НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

СОКОЛОВ АРТЕМ ВІКТОРОВИЧ

УДК 004.056.55

ДИСЕРТАЦІЯ

МЕТОДОЛОГІЯ РОЗРОБКИ ЕФЕКТИВНОЇ КРИПТО-СТЕГАНОГРАФІЧНОЇ СИСТЕМИ

05.13.21 — Системи захисту інформації
(шифр і назва спеціальності)

05 — Технічні науки
(галузь знань)

Подається на здобуття наукового ступеня доктора технічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело _____ Соколов А.В.

Науковий консультант: Кобозєва Алла Анатоліївна,
доктор технічних наук, професор

Львів — 2023

АНОТАЦІЯ

Соколов А.В. Методологія розробки ефективної крипто-стеганографічної системи. — Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 — Системи захисту інформації. — Національний університет «Львівська політехніка» Міністерства освіти і науки України, Львів, 2023.

В роботі вирішено важливу науково-практичну проблему, що полягає у забезпеченні ефективності роботи крипто-стеганографічних систем в режимі реального часу на ресурсообмежених платформах, шляхом розробки відповідної науково-обґрунтованої методології, орієнтованої на управління вбудовуванням криптозахищеної додаткової інформації у просторовій області контейнера.

При цьому під ефективністю роботи крипто-стеганографічної системи розуміється її відповідність базовим вимогам: крипостійкість, швидкодія, стійкість до атак проти вбудованого повідомлення, забезпечення надійності сприйняття, забезпечення значної пропускної спроможності.

Для досягнення поставленої мети в роботі розв’язуються задачі, основні з яких наступні:

1. провести аналіз сучасного стану теоретичних засад та практичних рішень з розробки ефективних стеганографічних методів, що забезпечують можливість роботи з потоковим контейнером, а також способів забезпечення криптографічної стійкості таких методів;
2. розробити загальний теоретичний базис забезпечення певних властивостей стеганографічних методів;

3. розробити теоретичні основи кодового управління вбудовуванням ДІ в просторовій області контейнера, що забезпечує певні властивості стеганоповідомлення;

4. розробити просторові стеганографічні методи з кодовим управлінням на основі бінарних та багаторівневих кодових слів;

5. розробити стеганографічні системи з множинним доступом з використанням: кодів постійної амплітуди, частотних розстановок, просторово-частотних кодів, стеганографічних методів з кодовим управлянням;

6. розробити теоретичні основи підвищення криптографічної захищеності КСС;

7. розробити методи синтезу S-блоків підстановки на основі ФБЛ практично цінних довжин, що відповідають критеріям криптографічної якості;

8. розробити методи підвищення криптографічної захищеності КСС;

9. розробити алгоритмічні реалізації запропонованих методів; провести оцінку їх ефективності, в тому числі, порівняльну.

Розв’язок задач 1,2,3,6 дозволив сформувати теоретичну складову розробленої методології, для чого використовувалися методи матричного аналізу та досконалі алгебраїчні конструкції. Розв’язок задач 4,5,7,8,9 дозволив сформувати практичну складову розробленої методології.

В роботі отримані нові наукові результати, основні з яких наступні:

1. *Вперше* на основі ЗПАІС встановлено взаємозв’язок між трансформантами двовимірного, одновимірного перетворення Уолша-Адамара та дискретного косинусного перетворення і складовими сингулярного розкладання матриці, що дало можливість отримання формальних достатніх умов для заданих властивостей стеганоповідомлення, а також теоретичних основ для формування стеганографічних методів з кодовим управлінням.

2. *Вперше* на основі встановленого взаємозв'язку між трансформантами перетворення Уолша-Адамара, ДКП та сингулярним розкладанням матриці сформульовано достатні умови забезпечення надійності сприйняття та нечутливості стеганоповідомлення до збурних дій в області перетворення Уолша-Адамара, що дозволило сформувати основи теоретичного базису створення стеганографічних методів з кодовим управлінням вбудовуванням ДІ в просторовій області, забезпечуючи задані властивості КСС в умовах реального часу з використанням ресурсообмежених платформ.

3. *Вперше* на основі встановленого взаємозв'язку між перетвореннями Уолша-Адамара, ДКП та сингулярним розкладанням матриці сформовано теоретичний базис синтезу ефективних кодових слів та впроваджено і досліджено показники енергії E та селективності κ кодового слова, які дозволили синтезувати багаторівневі кодові слова, що забезпечують ефективність розроблених на їх основі стеганографічних методів з кодовим управлінням вбудовуванням ДІ, яка перевищує ефективність сучасних аналогів.

4. *Вперше* на основі розробленого теоретичного базису створено два стеганографічних методи з кодовим управлінням вбудовуванням ДІ з застосуванням бінарних та багаторівневих кодових слів, ефективність яких перевищує сучасні аналоги, зокрема в умовах потокового контейнера, та, на відміну від існуючих аналогів, забезпечує можливість ефективної роботи КСС в умовах реального часу з використанням ресурсообмежених платформ.

5. *Вперше* на основі концепції кодового управління вбудовуванням ДІ та запропонованих криптографічних примітивів розроблено спосіб формування стеганографічного ключа, який, на відміну від існуючих аналогів, дозволив забезпечити взаємозв'язок та врахувати взаємовплив криптографічної та стеганографічної складової КСС, наслідком чого стало забезпечення можливості її ефективної роботи з потоковим контейнером на ресурсообмежених платформах в режимі реального часу.

6. *Вперше* на основі ЗПАІС та теорії ФБЛ запропоновано науково-обґрунтовану методологію розробки КСС, яка забезпечує високу ефективність КСС, зокрема на ресурсообмежених платформах, на відміну від існуючих сучасних аналогів.

7. *Подальший розвиток* отримала технологія множинного доступу до прихованого каналу зв'язку за рахунок: використання розроблених кодів постійної амплітуди в технології MC-CDMA, двох запропонованих стеганографічних методів з множинним доступом, які базуються на кодах Ріда-Соломона та розроблених кодах просторових розстановок, що дозволило при збереженні переваг кодового управління забезпечити, на відміну від існуючих аналогів, підтримку роботи в системі до кількох тисяч користувачів та одночасну роботу кількох десятків користувачів, підвищити пропускну спроможність групового тракту в порівнянні з аналогами.

8. *Удосконалено* математичний підхід до оцінки якості криптографічних примітивів шляхом використання теорії ФБЛ, в результаті чого побудовано теоретичний базис забезпечення криптографічної якості ФБЛ, який включає наступні критерії: алгебраїчна нелінійність, дистанційна нелінійність, критерій лавинного ефекту, критерій незалежності виходу від вхідних змінних, що дозволило обґрунтувати вибір ФБЛ для задач формування стеганографічного ключа при використанні стеганографічного методу з кодовим управлінням вбудовуванням ДІ.

9. *Удосконалено* криптографічні примітиви на основі розроблених критеріїв криптографічної якості ФБЛ шляхом синтезу множин S-блоків практично цінних довжин, що володіють максимально можливим рівнем нелінійності як компонентних булевих функцій, так і компонентних ФБЛ, задовольняють критерію розповсюдження помилки найвищих порядків, а також є оптимальними з точки зору критерію незалежності виходу компонентних ФБЛ від їх вхідних змінних, що дало можливість підвищити криптографічну якість конструкцій шифрів КСС.

10. *Удосконалено* БСШ прекодера на основі запропонованих криптографічних примітивів та концепції змінної фрагментації блоків, що дозволило прискорити, в порівнянні з аналогами, формування блоком, який оброблюється, властивостей псевдовипадкової послідовності, знизити обчислювальні затрати на роботу прекодера, підвищити криптографічну стійкість КСС в порівнянні з існуючими аналогами.

Практична цінність роботи полягає в доведенні отриманих наукових результатів до конкретних методів та алгоритмів, що можуть бути використані у практичних системах захисту інформації, в тому числі тих, що передбачають розгортання на ресурсообмежених платформах та потребують роботи із потоковими контейнерами в режимі реального часу.

Алгоритмічні реалізації стеганографічних методів з кодовим управлінням вбудовуванням інформації характеризуються простотою реалізації, а також гнучкістю настроювання властивостей за допомогою вибору тих чи інших кодових слів. Методи дозволяють забезпечити кількість помилок на рівні 1.6% при вилученні ДІ під дією атаки стиском проти вбудованого повідомлення з коефіцієнтом якості QF=10, що у 8.125 разів краще за подібний показник найкращого відомого аналогу. При цьому значення показника PSNR складає 35.6 дБ, що на 3% перевершує значення найкращого відомого аналогу, який володіє сумірним рівнем стійкості до атак проти вбудованого повідомлення.

Алгоритмічні реалізації методів синтезу криптографічних конструкцій та криптоалгоритми на їх основі характеризуються можливостю синтезу S-блоків, що відповідають критеріям криптографічної якості (критерій високої алгебраїчної нелінійності, критерій високої дистанційної нелінійності, суворий лавинний критерій, критерій відсутності кореляційного зв’язку векторів виходу і входу) як в сенсі представлення компонентними булевими функціями, так і компонентними функціями багатозначної логіки.

Алгоритмічна реалізація крипто-стеганографічної системи, що побудована а основі розробленої методології характеризується високою ефективністю та можливістю роботи в режимі реального часу, навіть, на ресурсообмежених платформах. При роботі з ЦВ роздільної здатності 400p/720p/1080p/1140p швидкість роботи КСС становить 1815/825/354/257 fps в режимі вбудовування та 236/106/47/33 fps в режимі вилучення ДІ на найпоширенішій IoT платформі Raspberry Pi 4 під керуванням Raspbian Pi OS.

Практичне значення отриманих результатів підтверджено актами впровадження в діяльність НУ «Одеська політехніка», ТОВ Компанія «Планета-Юг», ТОВ «Телекарт-прилад», ТОВ «Бізнес-центр НТЦ», ТОВ «Продукт – Постачання».

Отримані наукові результати мають як теоретичне, так і практичне значення для розвитку та удосконалення систем захисту інформації.

Ключові слова: криптографія, стеганографія, крипто-стеганографічна система, шифрування, вбудовування інформації, перетворення Уолша-Адамара, функції багатозначної логіки.

ABSTRACT

Sokolov A.V. Methodology for developing an effective crypto-steganographic system. — Manuscript.

Thesis for the Doctor's degree of Engineering Sciences in specialty 05.13.21 — Information protection systems. — Lviv Polytechnic National University, Ministry of Education and Science of Ukraine, Lviv, 2023.

An important scientific and practical problem of ensuring the effectiveness of crypto-steganographic systems in real time on resource-limited platforms has been solved by developing an appropriate scientifically based methodology, focused on managing the embedding of cryptographically protected additional information in the spatial domain of the container.

The effectiveness of the crypto-steganographic system means its compliance with the basic requirements: cryptographic robustness, performance, resistance to attacks against the embedded message, ensuring the reliability of perception, and ensuring the necessary bandwidth.

To achieve the purpose of the work, the following main tasks have been solved:

1. analysis of the current state of theoretical foundations and practical solutions for the development of effective steganographic methods that provide the possibility of working with a streaming container, as well as ways to ensure the cryptographic stability of such methods;

2. development of a general theoretical basis for ensuring certain properties of steganographic methods;

3. development of the theoretical foundations of code control of the additional information embedding in the spatial domain of the container, which provides certain properties of steganographic messages;

4. development of the spatial steganographic methods with code control based on binary and multi-level codewords;

5. development of the steganographic systems with multiple access using: codes of constant amplitude, frequency arrangements, spatial-frequency codes, and steganographic methods with code control;

6. development of the theoretical foundations for increasing the cryptographic stability of crypto-steganographic system;

7. development of the methods for synthesis of cryptographic substitution boxes based on many-valued logic functions of practically valuable lengths that correspond to the criteria of cryptographic quality;

8. development of the methods for increasing the cryptographic security of the crypto-steganographic systems;

9. development of the algorithmic implementations of the proposed methods; performing of the assessment of their effectiveness, including a comparative one.

The following new main scientific results were obtained in the work:

1. *For the first time*, based on a general approach to the analysis of the state and technology of the functioning of information systems, the relationship between the transformants of the two-dimensional, one-dimensional Walsh-Hadamard transform, discrete cosine transformation, and the components of the singular value decomposition of the matrix was established, which made it possible to obtain formal sufficient conditions for the specified properties of the steganographic message, as well as theoretical foundations for the formation of steganographic methods with code control.

2. *For the first time*, based on the established relationship between the transformants of the Walsh-Hadamard transform, the discrete cosine transform, and the singular value decomposition of the matrix, sufficient conditions for ensuring the reliability of perception and the insensitivity of the steganographic message to disturbing influence in the domain of the Walsh-Hadamard transform were formulated, which made it possible to form the foundations of the theoretical basis for the development of steganographic methods with code control by

embedding additional information in the spatial domain, ensuring the given properties of the crypto-steganographic system in real-time conditions using resource-constrained platforms.

3. *For the first time*, based on the established relationship between the Walsh-Hadamard transform, the discrete cosine transform, and the singular value decomposition of the matrix, a theoretical basis for the synthesis of effective codewords was formed, and indicators of energy E and selectivity κ of the codeword were introduced and researched, which made it possible to synthesize multi-level codewords that ensure the effectiveness of the developed on their basis steganographic methods with code control, which exceeds the effectiveness of modern analogs.

4. *For the first time*, based on the developed theoretical basis, two steganographic methods with code control of the embedding of additional information using binary and multi-level codewords were developed, which ensures their effectiveness, which exceeds modern analogs, in particular, in the conditions of a streaming container and, unlike existing analogs, provides the possibility of effective operation of the crypto-steganographic system in real-time conditions using resource-constrained platforms.

5. *For the first time*, based on the concept of code control of additional information embedding and the proposed cryptographic primitives, a method for formation of steganographic key was developed, which, in contrast to existing analogs, made it possible to ensure the relationship and take into account the mutual influence of the cryptographic and steganographic components of the crypto-steganographic system, as a result of which it became possible to provide the possibility of its effective operation with the streaming container on resource-constrained platforms in real-time.

6. *For the first time*, based on a general approach to the analysis of the state and technology of the functioning of information systems and the theory of many-valued logic functions, a scientifically based methodology for the development of a

crypto-steganographic system is proposed, which ensures its high effectiveness, in particular on resource-constrained platforms, in contrast to existing modern analogs.

7. The technology of multiple access to the hidden communication channel was *further developed* due to: the use of developed constant amplitude codes in the MC-CDMA technology, two proposed steganographic methods with multiple access, which are based on Reed-Solomon codes, and developed codes of spatial arrangements, which made it possible, while preserving the advantages of code control, to provide, in contrast to existing analogs, the support of registration in the system up to several thousand users and the simultaneous operation of several tens of users, as well as to increase the bandwidth of the baseband section in comparison with analogs.

8. The mathematical approach for estimation of the quality of cryptographic primitives by using the theory of many-valued logic functions was *improved*, as a result of which a theoretical basis for ensuring the cryptographic quality of many-valued logic functions was constructed, which includes the following criteria: algebraic nonlinearity, distance nonlinearity, the criterion of the avalanche effect, the criterion of independence of output from input variables, which allowed to justify the choice of many-valued logic functions for the tasks of formation of steganographic key when using the steganographic method with code control of the additional information embedding.

9. The cryptographic primitives have been *improved* based on the developed criteria for cryptographic quality of many-valued logic functions by synthesizing sets of S-boxes of practically valuable lengths, which have the maximum possible level of nonlinearity of both component Boolean functions and component many-valued logic functions, satisfy the error propagation criterion of the highest orders, and are also optimal from the point of view of the criterion of independence of the output of component many-valued logic functions from their input variables, which

made it possible to improve the cryptographic quality of the constructions of crypto-steganographic system ciphers.

10. The precoder BSC has been *improved* with help of the proposed cryptographic primitives and the concept of variable fragmentation of blocks, which made it possible to accelerate, in comparison with analogs, the formation of properties of a pseudo-random sequence by the block being processed, to reduce the computational costs of the precoder, and to increase the cryptographic stability of the crypto-steganographic system in comparison with existing analogs.

The practical value of the work consists in bringing the obtained scientific results to specific methods and algorithms that can be used in practical information protection systems, including those that involve deployment on resource-limited platforms and require operation with streaming containers in real-time.

Algorithmic implementations of steganographic methods with code control of information embedding are characterized by simplicity of implementation, as well as the flexibility of setting properties by choosing certain codewords. The methods make it possible to ensure the number of errors at the level of 1.6% when extracting additional information under the action of a compression attack against an embedded message with a quality factor of QF=10, which is 8.125 times better than the similar indicator of the best-known analog. At the same time, the value of the PSNR indicator is 35.6 dB, which is 3% higher than the value of the best-known analog, which has a reasonable level of resistance to attacks against embedded messages.

Algorithmic implementations of methods for synthesizing cryptographic structures and based on them cryptographic algorithms are characterized by the possibility of synthesizing S-boxes that correspond to the criteria of cryptographic quality (criterion of high algebraic nonlinearity, the criterion of high distance nonlinearity, strict avalanche criterion, criterion of absence of correlation between output and input vectors) as in the sense of representation by component Boolean functions and component functions of many-valued logic.

The algorithmic implementation of the crypto-steganographic system built based on the developed methodology is characterized by high efficiency and the ability to operate in real-time, even on resource-constrained platforms. When operating with video resolutions 400p/720p/1080p/1140p, the performance of the crypto-steganographic system is 1815/825/354/257 fps in the embedding mode and 236/106/47/33 fps in the additional information extraction mode on the most common IoT platform Raspberry Pi 4 controlled by Raspbian Pi OS.

The practical significance of the obtained results is confirmed by the acts of implementation into the activities of Odesa Polytechnic National University, Planeta-Yug Ltd, Telekart-Prylad Ltd, Business Center of NTC Ltd, and Product – Supply Ltd.

The obtained scientific results have both theoretical and practical significance for the development and improvement of information protection systems.

Keywords: cryptography, steganography, crypto-steganographic system, encryption, information embedding, Walsh-Hadamard transform, many-valued logic functions.

Список публікацій здобувача:

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Kobozeva A. A., Sokolov A. V. The Sufficient Condition for Ensuring the Reliability of Perception of the Steganographic Message in the Walsh-Hadamard Transform Domain. *Problemele Energeticii Regionale*. 2022. 54 (2). P. 84-100. (**Scopus & Web of Science**)

2. Kobozeva A.A., Sokolov A.V. Efficient Coding of the Embedded Signal in Steganographic Systems with Multiple Access. *Problemele energeticii regionale*. 2021. No. 2 (50). P. 101-113. (**Scopus & Web of Science**)

3. Kobozeva A.A., Sokolov A.V. Robust Steganographic Method with Code-Controlled Information Embedding. *Problemele energeticii regionale*. 2021. No. 4 (52). P. 115-130. (**Scopus & Web of Science**)

4. Sokolov A. V., Zhdanov O. N Synthesis of highly nonlinear S-boxes satisfying higher order propagation criterion. *Journal of Discrete Mathematical Sciences and Cryptography*. 2020. P. 1-15. DOI: 10.1080/09720529.2019.1681675 (**Scopus & Web of Science**)

5. Sokolov A. V., Zhdanov O. N. Correlation immunity of three-valued logic functions. *Journal of Discrete Mathematical Sciences and Cryptography*. 2020. P. 1-17. DOI: 10.1080/09720529.2020.1781882 (**Scopus & Web of Science**)

6. Sokolov A. V., Zhdanov O.N. Regular synthesis method of a complete class of ternary bent-sequences and their nonlinear properties. *Journal of Telecommunication, Electronic and Computer Engineering*. 2016. Vol. 8, No. 9. P. 39-43. (**Scopus**)

7. Zhdanov O. N., Sokolov A. V. Block symmetric cryptographic algorithm based on principles of variable block length and many-valued logic. *Far East Journal of Electronics and Communications*. 2016. Vol. 16, No. 3. P. 573-589. DOI: 10.17654/EC016030573 (**Scopus**)

8. Жданов О. Н., Соколов А. В. О распространении конструкции Ниберг на поля Галуа нечетной характеристики. *Известия высших учебных заведений. Радиоэлектроника*. 2017. Т. 60, №12. С. 696-703. DOI: 10.20535/S0021347017120032 [Перекладений варіант: Zhdanov O. N., Sokolov A. V. Extending Nyberg construction on Galois fields of odd characteristic. *Radioelectronics and Communications Systems*. 2017. Vol. 60, No. 12. P. 538-544. DOI: 10.3103/S0735272717120032 (**Scopus**)]

9. Соколов А. В., Барабанов Н. А. Алгоритм устранения спектральной эквивалентности компонентных булевых функций S-блоков конструкции Ниберг. *Известия высших учебных заведений. Радиоэлектроника*. 2015. Т. 58, № 5. С. 41-49. DOI: 10.20535/S0021347015050040 [Перекладений варіант:

Sokolov A. V., Barabanov N. A. Algorithm for removing the spectral equivalence of component Boolean functions of Nyberg-design S-boxes. *Radioelectronics and Communications Systems*. 2015. Vol. 58, No. 5. P. 220-227. DOI: 10.3103/S0735272715050040 (**Scopus**)]

10. Мазурков М. И., Соколов А. В., Барабанов Н. А. Метод синтеза бент-последовательностей в базисе Виленкина-Крестенсона. *Известия высших учебных заведений. Радиоэлектроника*. 2016. Т. 59, № 11. С. 47-55. DOI: 10.20535/S0021347016110054 [Перекладений варіант: Mazurkov M. I., Sokolov A. V., Barabanov N. A. Synthesis method for bent sequences in the Vilenkin-Chrestenson basis. *Radioelectronics and Communications Systems*. 2016. Vol. 59, No. 11. P. 510-517. DOI: 10.3103/S0735272716110054 (**Scopus**)]

11. Mazurkov M. I., Sokolov A. V., Tsevukh I. V. Synthesis method for families of constant amplitude correcting codes based on an arbitrary bent-square. *Journal of Telecommunication, Electronic and Computer Engineering*. 2017. Vol. 2, No. 9. P. 99-103. (**Scopus**)

12. Мазурков М. И., Соколов А. В. Алгоритм синтеза экономичных схем S-блоков подстановки на основе клеточных автоматов. *Известия высших учебных заведений. Радиоэлектроника*. 2016. Т. 59, № 5. С. 27-37. DOI: 10.20535/S0021347016050034 [Перекладений варіант: Mazurkov M. I., Sokolov A. V. Algorithm for synthesis of efficient S-boxes based on cellular automata. *Radioelectronics and Communications Systems*. 2016. Vol. 59, No. 5. P. 212-220. DOI: 10.3103/S0735272716050034 (**Scopus**)]

13. Sokolov A. V. Regular synthesis method of the sequences of length N=24 with optimal PAPR of Walsh-Hadamard spectrum. *Far East Journal of Electronics and Communications*. 2016. Vol. 16, No. 2. P. 459-469. DOI: 10.17654/EC016020459 (**Scopus**)

14. Мазурков М. И., Соколов А. В. Конструктивные методы синтеза двоичного корректирующего кода длины 32 для технологии MC-CDMA. *Известия высших учебных заведений. Радиоэлектроника*. 2019. Т. 62, No. 3.

С. 123-135. DOI: 10.20535/S0021347019030014 [Перекладений варіант: Mazurkov M. I., Sokolov A. V. Constructive synthesis methods of binary error correcting code of length 32 for MC-CDMA technology. *Radioelectronics and Communications Systems*. 2019. Vol. 62, No. 3. P. 97-108. DOI: 10.3103/S0735272719030014 (**Scopus**)]

15. Sokolov A. V., Tsevukh I.V. Construction Method for Infinite Families of Bent Sequences. *Journal of Telecommunication, Electronic and Computer Engineering*. 2018. Vol. 10, No. 2. P. 51-54. (**Scopus**)

16. Sokolov A. V. Synthesis method of ternary bent-functions of three variables. *Radio Electronics, Computer Science, Control*. 2020. No. 1. P. 82-89. DOI: 10.15588/1607-3274-2020-1-9 (**Web of Science**)

17. Sokolov A. V., Zhdanov O. N. Avalanche Characteristics of Cryptographic Functions of Ternary Logic. *Radio Electronics, Computer Science, Control*. 2019. No.4(51). P.177-185. DOI: 10.15588/1607-3274-2019-4-17 (**Web of Science**)

18. Соколов А. В. Регулярный метод синтеза базовых бент-квадратов произвольного порядка. *Наука и техника*. 2016. Т. 15, №4. С. 345-352. DOI: 10.21122/2227-1031-2016-15-4-345–352 (**Web of Science**).

19. Sokolov A.V. Properties of the full class of quaternary bent-functions of two variables. *Journal of Discrete Mathematical Sciences and Cryptography*. 2021. P. 1-14. (**Scopus & Web of Science**)

20. Sokolov A.V., Radush V.V. A method for synthesis of S-boxes with good avalanche characteristics of component Boolean and quaternary functions. *Journal of Discrete Mathematical Sciences and Cryptography*. 2022. P. 1-12. (**Scopus & Web of Science**)

21. Sokolov A. V., Radush V. V. Avalanche characteristics of Nyberg construction S-boxes represented by the many-valued logic functions. *Informatics and Mathematical Methods in Simulation*. 2019. Vol. 9, No. 3. P. 111-119. DOI: 10.15276/imms.v9.no3.111

22. Соколов А. В., Жданов О. Н., Барабанов Н. А. Генератор псевдослучайных ключевых последовательностей на основе тройственных наборов бент-функций. *Проблемы физики, математики и техники*. 2016. №1(26). С. 85-91.

23. Соколов А. В., Жданов О. Н. Класс совершенных троичных решеток. *Системный анализ и прикладная информатика*. 2018. №2. С. 47-54. DOI: 10.21122/2309-4923-2018-2-47-54

24. Zhdanov O. N., Sokolov A. V. Spectral and Nonlinear Properties of the Sum of Boolean Functions. *Journal of Telecommunication, Electronic and Computer Engineering*. 2019. Vol. 11, No. 2. P. 31-35.

25. Соколов А. В., Жданов О. Н. Нелинейные преобразования конструкции Ниберг над изоморфными представлениями полей Галуа. *«Системный анализ и прикладная информатика»*. 2017. №3. С. 59-67. DOI: 10.21122/2309-4923-2017-3-59-67

26. Жданов О. Н., Соколов А. В. Метод синтеза базовых троичных бент-квадратов на основе оператора триадного сдвига. *Системный анализ и прикладная информатика*. 2017. № 1. С. 77-85. DOI: 10.21122/2309-4923-2017-1-77-85

27. Соколов А .В., Жданов О. Н., Айвазян А. О. Методы синтеза алгебраической нормальной формы функций многозначной логики. *Системный анализ и прикладная информатика*. 2016. №1. С. 69-76.

28. Жданов О. Н., Соколов А. В. Алгоритм построения оптимальных по критерию нулевой корреляции недвоичных блоков замен. *Проблемы физики, математики и техники*. 2015. № 3(24). С. 94-97.

29. Соколов А. В., Цевух И. В. О существовании бинарных С-кодов длины N=32 с заданным значением пик-фактора спектра Уолша–Адамара. *Проблемы физики, математики и техники*. 2017. № 2(31). С. 91-95.

30. Соколов А. В., Красота Н. И. Сильно нелинейные подстановки: метод синтеза S-блоков, обладающих максимальной 4-нелинейностью. *Наукові праці ОНАЗ ім. О.С. Попова*. 2017. № 1. С. 145-154.

31. Sokolov, A.V. Effect of binary orthogonal transform type on the cardinality and structure of constant amplitude codes for the MC-CDMA technology. *Informatics & Mathematical Methods in Simulation*. 2019. Vol. 9. No. 1-2. P. 5-14.

32. Соколов А. В. Метод синтеза полного класса бент-функций шести переменных. *Проблемы физики, математики и техники*. 2016. №4(29). С. 94-102.

33. Соколов А. В., Гаркуша А. А. Бесконечные семейства последовательностей Пэли с оптимальным пик-фактором спектра Уолша-Адамара. *Научные труды ОНАС им. А.С. Попова*. 2016. №2. С. 163-169.

34. Мазурков М. И., Соколов А. В., Барабанов Н. А. О влиянии вида ортогонального преобразования на пик-фактор спектра сигналов в системах с CDMA. *Информатика и математические методы в моделировании*. 2015. Т. 5, №1. С. 28-37.

35. Мазурков М. И., Соколов А. В. Рекуррентные методы синтеза последовательностей с оптимальным пик-фактором спектра Уолша-Адамара. *Информатика и математические методы в моделировании*. 2015. Т. 5, № 4. С. 203-209.

36. Соколов А. В., Барабанов Н. А. Системы ортогональных бифазных сигналов на основе бент-последовательностей. *Научные труды ОНАС им. А.С. Попова*. 2015. №1. С. 127-133.

37. Соколов А. В. Конструктивный метод синтеза последовательностей длины N = 20 с оптимальным спектром Уолша-Адамара. *Научные труды ОНАС им. А.С. Попова*. 2015. №2. С. 118-126.

38. Соколов А. В. Процессорно-ориентированные нелинейные преобразования на основе полных классов изоморфных и автоморфных

представлений полей GF(512) и GF(1024). *Системный анализ и прикладная информатика*. 2015. № 4. С. 55-60.

39. Sokolov A. V. Nyberg construction nonlinear transforms based on all isomorphic representations of the Galois field GF(512) [Электронный ресурс]. *Проблеми телекомунікацій*. 2015. № 2 (17). С. 68-75.

40. Sokolov A.V., Isakov D.A. Authenticated encryption mode with blocks skipping. *System analysis and applied information science*. 2021. Vol. 3. P. 59-65.

41. Соколов А.В., Корж А.О. Исследование режимов шифрования с пропуском блоков. *Информатика и математические методы в моделировании*. 2020. Т. 10, №. 1-2. С. 100-108.

42. Судаков А.Ю., Соколов А.В. Розробка системи безпеки клієнт-серверного застосунку на базі операційної системи Android. *Інформатика та математичні методи в моделюванні*. 2020. Т. 10, № 3/4. С. 197-207.

43. Sokolov A.V. Multiple access steganographic method based on code control and frequency arrangements. *Informatics and Mathematical Methods in Simulation*. 2021. Vol. 11, No. 3. P. 147-161.

44. Kobozeva A.A., Sokolov A.V. Theoretical foundations for constructing effective codewords for the code-controlled information embedding steganographic method. *Radiotekhnika*. 2021. 4(207). P. 27–39. https://doi.org/10.30837/rt.2021.4.207.02.

45. Sokolov A.V. The steganographic method with multiple access based on frequency-spatial matrices. *Informatics and Mathematical Methods in Simulation*. 2022. Vol. 12, No. 1/2. P. 5-14.

46. Юровских Д.А., Соколов А.В., Троицкий Б.С. Полуторабайтные нелинейные преобразования конструкции Ниберг. *Информатика и математические методы в моделировании*. 2016. Т. 6, № 2. С. 142-148.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

47. Bakunina E.V., Sokolov A.V. The Pseudorandom Key Sequences Generator Based on IV-Sets of Quaternary Bent-Sequences. *The Fifth International Workshop on Computer Modeling and Intelligent Systems*, Zaporizhzhia, Ukraine, May 12, 2022. P. 144-153. (**Scopus**)

48. Kazakova N. F., Sokolov A. V. Spectral and Nonlinear Properties of the Complete Quaternary Code. *Cybersecurity Providing in Information and Telecommunication Systems* : Proc., 7 July 2020. Kyiv, Ukraine, 2020. P. 76-86. (**Scopus**)

49. Sokolov A. V., Zhdanov O. N. Prospects for the Application of Many-Valued Logic Functions in Cryptography. *Advances in Computer Science for Engineering and Education* : Proceedings, January 2018. Kyiv, Ukraine, 2018. P. 331-339. DOI: 10.1007/978-3-319-91008-6_33 (**Scopus**)

50. Sokolov A. V. Interrelation Between the Class of Bent-Sequences and the Class of Perfect Binary Arrays. Proceedings of the *Second International Workshop on Computer Modeling and Intelligent Systems 2018*. Zaporizhzhia, Ukraine, 2019. P. 339-349. (**Scopus**)

51. Kazakova N.F., Karpinski M., Sokolov A.V., Gancarczyk T. Nonlinearity of Many-Valued Logic Component Functions of Modern Cryptographic Algorithms S-boxes. *Procedia Computer Science*. 2021. Vol. 192. P. 2731-2741. (**Scopus, Web of Science**)

52. Sokolov A., Kazakova N., Kuzmenko L., Mahomedova M. Prerequisites for developing a methodology for estimating and increasing cryptographic strength based on many-valued logic functions. *CEUR Workshop Proceedings*, 2021. 2923. pp. 107–116. (**Scopus**)

53. Соколов А. В., Оверчук Ю. С. О возможности синтеза алгебраической нормальной формы четверичных функций над полем GF(4). *Проблеми кібербезпеки інформаційно-телекомунікаційних систем* : зб. матеріалів першої міжнародної наук.-практ. конф., 5-6 квітня 2018 р. Київ. С. 384–388.

54. Соколов А. В., Жданов О. Н., Барабанов Н. А. Построение троичных бент-последовательностей. *Радиоэлектроника и молодежь в XXI веке* : сб. материалов XIX международного молодежного форума, 20-22 апреля 2015 г. Харьков, 2015. т. 3. С.131-132.

55. Соколов А. В., Корж А. О., Лопуленко О. В. Модифікований алгоритм шифрування зі змінною фрагментацією блоків. *WayScience* : матеріали VII міжнародної наук.-практ. конф., 6-7 червня 2019, Дніпро, 2019. С. 1592-1596.

56. Kazakova N., Sokolov A., Troyanskiy A. Correlation Immunity of Many-Valued Logic Component Functions of Modern Cryptographic Algorithm S-Boxes. *International Scientific and Practical Conference «Intellectual Systems and Information Technologies»*: Conference Proceedings / Odessa State Environmental University. Odessa, September 13-19, 2021. P. 268-275.

57. Соколов А. В., Авєкін В. В., Жук В. Г. Метод синтезу четвіркових бент-квадратів Агієвича. *Современные информационные и электронные технологии* : сб. материалов 18 международной науч.-практ. конф. 22-26 мая 2017 г. Одесса, 2017. С.152–153.

58. Соколов А. В., Ефимов О. И., Годунов А. И. О множестве линейных и нелинейных троичных последовательностей де Брейна длиной N = 9. *Современные информационные и электронные технологии* : сб. материалов 18 международной науч.-практ. конф. 22-26 мая 2017 г. Одесса, 2017. С.154–155.

59. Юровских Д. А., Соколов А. В., Шипунова А. О. Полуторабайтные нелинейные преобразования конструкции Ниберг. *Современные информационные и электронные технологии* : сб. материалов 17 международной науч.-практ. конф. 23—27 мая 2016 г. Одесса : ОНПУ, 2016. С. 137–138.

60. Соколов А. В., Гаркуша А. А. Исследование пик-фактора спектра Уолша–Адамара полного кода длины *N*=28. *Современные информационные и*

электронные технологии : сб. материалов 17 международной науч.-практ. конф. 23–27 мая 2016 г. Одесса : ОНПУ, 2016. С. 79–80.

61. Соколов А. В., Ткаченко М. В. Модифицированный генератор ключевых последовательностей на основе дуальных пар бент-функций. *Современные информационные и электронные технологии* : сб. материалов 17 международной наук.-практ. конф. 23—27 мая 2016 г. Одесса : ОНПУ, 2016. С. 139–140.

62. Соколов А. В., Юровских Д. А. Полуторабайтные экономичные нелинейные преобразования на основе последовательностей де Брейна. *Радиоэлектроника и молодежь в XXI столетии* : сб. материалов 20 юбилейного молодежного форума, 19-21 апреля 2016 г. Харьков, 2016. т.3. С. 97-98.

63. Соколов А. В., Барабанов Н. А. Системы ортогональных бифазных сигналов на основе бент-последовательностей длины 16. *Современные информационные и электронные технологии* : сб. материалов XVI международной наук.-практ. конф. 25–29 мая 2015 г. Одесса, 2015. С. 139 – 140. С. 75-76.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

№	Позначення	Розшифровка
1	AES	Advanced Encryption Standard
2	FPS	Frames Per Second
3	IoBT	Internet of Battlefield Things
4	IoT	Internet of Things
5	JPEG	Joint Photographic Experts Group
6	LSB	Least Significant Bit
7	MC-CDMA	Multi-Code Code Division Multiple Access
8	MSE	Mean Square Error
9	NRCS	Natural Resources Conservation Service
10	PC	Propagation Criterion, Критерій Розповсюдження Помилки
11	PLD, ПЛІС	Programmable Logic Device, Програмовані логічні інтегральні схеми
12	PSNR	Peak Signal-To-Noise Ratio
13	RGB	Red, Green, Blue
14	SNR	Signal to Noise Ratio
15	TIFF	Tagged Image File Format
16	АНФ	Алгебраїчна Нормальна Форма
17	БПЛА	Безпілотний літальний апарат
18	БСШ	Блоковий симетричний шифр
19	ДІ	Додаткова інформація
20	ДКП	Дискретне косинусне перетворення
21	ДП	Джерело Повідомлень
22	ДПФ	Дискретне перетворення Фур’є
23	ЕЦП	Електронний цифровий підпис

24	ЗПАІС	Загальний підхід до аналізу стану й технології функціонування інформаційних систем
25	КІ	Кореляційний імунітет
26	КСС	Крипто-стеганографічна система
27	ОЗП	Оперативний запам’ятовуючий пристрій
28	ОП	Одержувач Повідомлень
29	ПВП	Псевдовипадкова послідовність
30	ПСШ	Потоковий Симетричний Шифр
31	РС-код	Код Ріда-Соломона
32	СЛК	Суворий лавинний критерій
33	СНВ	Сингулярний вектор
34	СНЧ	Сингулярне число
35	ФБЛ	Функція багатозначної логіки
36	ЦВ	Цифрове відео
37	ЦЗ	Цифрове зображення
38	ЦП	Центральний процесор

ВСТУП

Актуальність теми. Протягом останніх десятиліть розвиток людства призвів до глибшого впровадження інформаційних технологій в усі сфери життя суспільства. Сучасні інформаційні системи, що працюють з даними, представленими у цифровому вигляді, є невід'ємною частиною практично всіх сфер людського життя, починаючи від економічних процесів і побутової техніки, що є частиною Інтернету речей, закінчуючи сучасними видами озброєнь, характеристики яких вдається суттєво покращити за рахунок впровадження інформаційних технологій.

Однак, дослідження та практичний досвід, набутий під час використання інформаційних технологій, призводить до переконливого висновку, що усі переваги від їх використання можуть бути легко зведені нанівець, або навіть перетворені у суттєві недоліки при недостатній увазі захисту інформації, що обертається в інформаційних системах. У купі із повсюдним використанням інформаційних технологій у житті суспільства такі вади захисту інформації можна розглядати в якості надзвичайно серйозного, а часто і екзистенційного виклику як окремим користувачам інформаційних технологій, так і організаціям і цілим державам, які використовують такі технології.

Історично було створено та виокремлено два основних напрямку розвитку конструктів, що складають основу всіх практично реалізованих систем захисту інформації: криптографічний, який засновано на ідеї її перетворення таким чином, що унеможливлює її отримання без знання спеціального ключа, та стеганографічний, який засновано на ідеї приховування самого факту наявності інформації, що захищається.

Численні вітчизняні та зарубіжні наукові дослідження, а також величезний досвід практиків в галузі інформаційної безпеки показують, що забезпечення надійного захисту інформації сьогодні неможливо без

інтегрального одночасного використання двох невід'ємних, залежних одна від одної, впливаючих одна на одну, складових: криптографічної та стеганографічної, необхідність врахування зв'язка та взаємного впливу яких приводить до формування принципово нового сучасного поняття КСС.

В сучасних умовах на практиці зростає частота використання при організації стеганографічного каналу зв'язку потокових контейнерів, зокрема ЦВ (що обов'язково повинно враховуватися при розробках сучасних КСС), хоча на сьогодні, як свідчать відкриті джерела, відчувається значний брак відповідних стеганометодів, що обумовлено, у першу чергу, складністю задачі, орієнтованістю (для забезпечення певних властивостей стеганоповідомлення) математичних базисів методів, здебільшого, на області перетворення контейнерів, що має негативні наслідки: подібні перетворення (сингулярне розкладання, дискретне косинусне перетворення (ДКП), вейвлет-перетворення та ін.) характеризуються значною обчислювальною складністю, часто призводить до збільшення помилок округлення, через які можливі спотворення інформації, що захищається, а також зниженням ймовірності забезпечення надійності сприйняття стеганоповідомлення за рахунок непередбачуваності амплітуди змін у просторовій області при впливі на (блоки) ЦЗ або кадра ЦВ у просторі перетворень. На сьогодні у відкритих джерелах фактично відсутні теоретичні засади, які б дозволяли керувати впливом на конкретні частотні складові контейнерів і, таким чином, забезпечувати задані властивості стеганоповідомлення без переходу в ту чи іншу області перетворення.

Надзвичайно актуальним сьогодні є забезпечення можливості роботи КСС не тільки в режимі реального часу, а й на ресурсообмежених пристроях. Приклади таких КСС в відкритих джерелах відсутні.

Згідно з RFC 7228 під ресурсообмеженими пристроями розуміються пристрої з обмеженою доступною потужністю, геометричними розмірами, обчислювальними здатностями, пам'яттю, ресурсами живлення, тощо. Фізичним

втіленням ресурсообмеженних пристроїв у сучасному світі є: мобільні телефони, кишенькові комп’ютери, пристрої IoT та IoBT, БПЛА тощо.

Наявні вимоги до КСС вкрай ускладнюють, а іноді взагалі унеможливлюють застосування областей перетворень інформаційних контентів, що використовуються в якості контейнерів, в режимі реального часу на ресурсообмежених пристроях, суттєво зменшуючи час автономності роботи таких пристроїв, що є неприпустимим.

Формування цілісної КСС в умовах розвитку методів криптоаналізу, зокрема, квантового криптоаналізу та криптоаналітичних атак, заснованих на функціях багатозначної логіки (ФБЛ) потребує підвищення криптографічної якості застосованих в ній криптоалгоритмів та криптографічних примітивів при їх представленні будь-яким способом: як за допомогою булевих функцій, так і за допомогою ФБЛ. На сьогодні в літературі фактично відсутні критерії криптографічної якості компонентних ФБЛ сучасних криптографічних примітивів, методи побудови криптографічних примітивів та алгоритмів, що володіють високою криптографічною якістю як в разі їх представлення за допомогою булевих функцій, так і ФБЛ, що фактично зменшує якість застосовуваних криптографічних конструкцій та імплементацію ними концепцій дифузії та конфузії, збільшує кількість необхідних раундів основного кроку криптоперетворення, унеможливлює більш тісну інтеграцію криптографічної та стеганографічної складової КСС.

Таким чином, на сьогодні склалося об’єктивне протиріччя між наявною необхідністю використання ресурсообмежених платформ при реалізації КСС, що, між іншим, передбачає застосування «нескладних» в обчислювальному сенсі методів та застосуванням ресурсномістких перетворень контейнера, що сьогодні має місце, для забезпечення ефективності крипто-стеганографічних систем, яке обумовлює важливу науково-практичну проблему, що полягає у необхідності забезпечення ефективності КСС при їх роботі в режимі

реального часу на ресурсообмежених пристроях. Означене обумовлює актуальність теми дисертаційного дослідження.

Вагомі теоретичні та практичні результати, пов'язані з вирішенням задачі підвищення ефективності криптографічних та стеганографічних компонент КСС, а також концептуальним засадам їх об'єднання належать відомим в галузі інформаційної безпеки вченим України: А.А. Кобозєва, В.О. Хорошко, М.Є. Шелест, В.К. Задірака, А.М. Кудін, М.І. Мазурков, І.Д. Горбенко, О.В. Мілов, І.В. Лисицька, Р.В. Олійников, А.Г. Ростовцев, Ю.Н. Зайко, а також їх закордонним колегам: M.Rakhra, Y.Wang, Y.Zhang, R.C. Stankovic, C. Moraga, W. Maier, K. Nyberg, K. Kim, S. Bhattacharyya, H. Sheidaeian. Тим не менш, незважаючи на отримані результати, зазначена проблема залишається актуальною не тільки для України, але і для світової наукової спільноти.

Проблема, що розв'язується в дисертації: полягає у вирішенні протиріччя між наявною необхідністю використання ресурсообмежених платформ при реалізації КСС, що, між іншим, передбачає застосування «нескладних» в обчислювальному сенсі методів та застосуванням ресурсномістких перетворень контейнера, що сьогодні має місце, для забезпечення ефективності крипто-стеганографічних систем.

Ефективність роботи КСС оцінюється в роботі за допомогою наступних критеріїв: криптостійкість, обчислювальні (часові) витрати, стійкість до атак проти вбудованого повідомлення, надійність сприйняття стеганоповідомлення, достатня пропускна спроможність прихованого криптозахищеного каналу зв'язку при відсутності множинного доступу, забезпечення можливості одночасного користування КСС декількома користувачами, пропускна спроможність групового тракту. При цьому під достатньою розуміється пропускна спроможність, не менша за $1/\mu^2$ біт/піксель, де μ — розмір блоку, що є результатом стандартної розбивки матриці ЦЗ (кадра ЦВ).

Зв'язок роботи з науковими програмами, планами, темами. Тематика роботи та очікувані результати безпосередньо пов’язані зі Стратегією національної безпеки України від 14 вересня 2020 № 392/2020 у контексті п. 52 «Основне завдання розвитку системи кібербезпеки — гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації»; Стратегією кібербезпеки України від 27 січня 2016 року №96/2016 у контексті п. 4.1. «Розвиток безпечного, стабільного і надійного кіберпростору має полягати, насамперед, у … розвитку та вдосконаленні системи технічного і криптографічного захисту інформації»; Законом України Про основні засади забезпечення кібербезпеки України від 24.10.2020 №2163-VIII у контексті п.3 Статті 8 «Національна система кібербезпеки», а саме «Функціонування національної системи кібербезпеки забезпечується шляхом … розвитку та вдосконалення системи технічного і криптографічного захисту інформації».

Результати досліджень дисертаційної роботи використовувалися під час виконання НДР №0111U009481«Підвищення ефективності методів цифрової обробки сигналів в радіотехнічних системах», НДР №0116U004923 «Оптимізація методів цифрової обробки інформації в корпоративних мережах та радіотехнічних системах», НДР №710-59 «Методи і технології радіаційного керування параметрами та стійкістю активних елементів електроніки до іонізуючих випромінювань», а також в діяльність підприємств ТОВ Компанія «Планета-Юг», ТОВ «Телекарт-прилад», ТОВ «Бізнес-центр НТЦ», ТОВ «Продукт – Постачання».

Мета і завдання дослідження. *Метою* роботи є вирішення важливої науково-прикладної проблеми, що полягає у забезпеченні ефективності роботи КСС, зокрема, в режимі реального часу на ресурсообмежених платформах шляхом розробки науково-обґрунтованої методології, що орієнтована на управління вбудовуванням криптозахищеної ДІ у просторовій області контейнера.

Ефективність роботи КСС оцінюється в роботі за допомогою наступних критеріїв: криптостійкість, обчислювальні (часові) витрати, стійкість до атак проти вбудованого повідомлення, надійність сприйняття стеганоповідомлення, достатня пропускна спроможність прихованого криптозахищеного каналу зв'язку з забезпеченням можливості одночасного користування КСС декількома користувачами. При цьому під достатньою розуміється пропускна спроможність, не менша за $1/\mu^2$ біт/піксель, де μ — розмір блоку, що є результатом стандартної розбивки матриці ЦЗ (кадра ЦВ).

Досягнення поставленої мети необхідно розв'язати наступні задачі:

1. провести аналіз сучасного стану теоретичних засад та практичних рішень з розробки ефективних стеганографічних методів, що забезпечують можливість роботи з потоковим контейнером, а також способів забезпечення криптографічної стійкості таких методів;
2. розробити загальний теоретичний базис забезпечення певних властивостей стеганографічних методів;
3. розробити теоретичні основи кодового управління вбудовуванням ДІ в просторовій області контейнера, що забезпечує певні властивості стеганоповідомлення;
4. розробити просторові стеганографічні методи з кодовим управлінням на основі бінарних та багаторівневих кодових слів;
5. розробити стеганографічні системи з множинним доступом з використанням: кодів постійної амплітуди, частотних розстановок, просторово-частотних кодів, стеганографічних методів з кодовим управлянням;
6. розробити теоретичні основи підвищення криптографічної захищеності КСС;
7. розробити методи синтезу S-блоків підстановки на основі ФБЛ практично цінних довжин, що відповідають критеріям криптографічної якості;

8. розробити методи підвищення криптографічної захищеності КСС;

9. розробити алгоритмічні реалізації запропонованих методів; провести оцінку їх ефективності, в тому числі, порівняльну.

Об’єкт дослідження — процеси створення КСС.

Предмет дослідження — теоретичні засади та методи створення КСС з використанням просторової області контейнера.

Методи дослідження. Для розробки теоретичної складової підходу кодового управління вбудовуванням інформації використовувалися методи матричного аналізу, теорії інформації та кодування, теорії досконалих алгебраїчних конструкцій, ЗПАІС. Для розробки стеганографічних методів з кодовим управлінням на основі бінарних та багаторівневих кодових слів, а також методів з кодовим управлінням, що забезпечують множинний доступ до прихованого каналу зв’язку — матричний аналіз, методи теорії полів Галуа, теорії кодування (коди Ріда-Маллера та коди Ріда-Соломона). Для розробки теоретичних основ підвищення криптографічної стійкості стеганоповідомлень використовувалися методи теорії ФБЛ та теорії криптоаналізу. Для оцінки якісних і кількісних характеристик розроблених стеганографічних методів з кодовим управлінням використовувалися теорія алгоритмів, методи математичного моделювання та методи оцінки стохастичної якості.

Наукова новизна отриманих результатів.

1. *Вперше* на основі ЗПАІС встановлено взаємозв’язок між трансформантами двовимірного, одновимірного перетворення Уолша-Адамара та дискретного косинусного перетворення і складовими сингулярного розкладання матриці, що дало можливість отримання формальних достатніх умов для заданих властивостей стеганоповідомлення, а також теоретичних основ для формування стеганографічних методів з кодовим управлінням.

2. *Вперше* на основі встановленого взаємозв’язку між трансформантами перетворення Уолша-Адамара, ДКП та сингулярним розкладанням матриці сформульовано достатні умови забезпечення надійності сприйняття та нечутливості стеганоповідомлення до збурних дій в області перетворення Уолша-Адамара, що дозволило сформувати основи теоретичного базису створення стеганографічних методів з кодовим управлінням вбудовуванням ДІ в просторовій області, забезпечуючи задані властивості КСС в умовах реального часу з використанням ресурсообмежених платформ.

3. *Вперше* на основі встановленого взаємозв’язку між перетвореннями Уолша-Адамара, ДКП та сингулярним розкладанням матриці сформовано теоретичний базис синтезу ефективних кодових слів та впроваджено і досліджено показники енергії E та селективності κ кодового слова, які дозволили синтезувати багаторівневі кодові слова, що забезпечують ефективність розроблених на їх основі стеганографічних методів з кодовим управлінням вбудовуванням ДІ, яка перевищує ефективність сучасних аналогів.

4. *Вперше* на основі розробленого теоретичного базису створено два стеганографічних методи з кодовим управлінням вбудовуванням ДІ з застосуванням бінарних та багаторівневих кодових слів, ефективність яких перевищує сучасні аналоги, зокрема в умовах потокового контейнера, та, на відміну від існуючих аналогів, забезпечує можливість ефективної роботи КСС в умовах реального часу з використанням ресурсообмежених платформ.

5. *Вперше* на основі концепції кодового управління вбудовуванням ДІ та запропонованих криптографічних примітивів розроблено спосіб формування стеганографічного ключа, який, на відміну від існуючих аналогів, дозволив забезпечити взаємозв’язок та врахувати взаємовплив криптографічної та стеганографічної складової КСС, наслідком чого стало забезпечення можливості її ефективної роботи з потоковим контейнером на ресурсообмежених платформах в режимі реального часу.

6. *Вперше* на основі ЗПАІС та теорії ФБЛ запропоновано науково-обґрунтовану методологію розробки КСС, яка забезпечує високу ефективність КСС, зокрема на ресурсообмежених платформах, на відміну від існуючих сучасних аналогів.

7. *Подальший розвиток* отримала технологія множинного доступу до прихованого каналу зв'язку за рахунок: використання розроблених кодів постійної амплітуди в технології MC-CDMA, двох запропонованих стеганографічних методів з множинним доступом, які базуються на кодах Ріда-Соломона та розроблених кодах просторових розстановок, що дозволило при збереженні переваг кодового управління забезпечити, на відміну від існуючих аналогів, підтримку роботи в системі до кількох тисяч користувачів та одночасну роботу кількох десятків користувачів, підвищити пропускну спроможність групового тракту в порівнянні з аналогами.

8. *Удосконалено* математичний підхід до оцінки якості криптографічних примітивів шляхом використання теорії ФБЛ, в результаті чого побудовано теоретичний базис забезпечення криптографічної якості ФБЛ, який включає наступні критерії: алгебраїчна нелінійність, дистанційна нелінійність, критерій лавинного ефекту, критерій незалежності виходу від вхідних змінних, що дозволило обґрунтувати вибір ФБЛ для задач формування стеганографічного ключа при використанні стеганографічного методу з кодовим управлінням вбудовуванням ДІ.

9. *Удосконалено* криптографічні примітиви на основі розроблених критеріїв криптографічної якості ФБЛ шляхом синтезу множин S-блоків практично цінних довжин, що володіють максимально можливим рівнем нелінійності як компонентних булевих функцій, так і компонентних ФБЛ, задовольняють критерію розповсюдження помилки найвищих порядків, а також є оптимальними з точки зору критерію незалежності виходу компонентних ФБЛ від їх вхідних змінних, що дало можливість підвищити криптографічну якість конструкцій шифрів КСС.

10. *Удосконалено* БСШ прекодера на основі запропонованих криптографічних примітивів та концепції змінної фрагментації блоків, що дозволило прискорити, в порівнянні з аналогами, формування блоком, який оброблюється, властивостей псевдовипадкової послідовності, знизити обчислювальні затрати на роботу прекодера, підвищити криптографічну стійкість КСС в порівнянні з існуючими аналогами.

Практичне значення отриманих результатів.

Практична цінність роботи базується на тому факті, що отримані наукові результати були доведені до конкретних методів та алгоритмів, які можуть бути використані або вже використовуються у прикладних системах захисту інформації. Розроблені методи характеризуються високою швидкодією та простотою алгоритмічної реалізації, яка витікає з їх роботи у просторовій області та робить їх придатними для роботи з потоковими контейнерами з використанням ресурсообмежених платформ.

Алгоритмічна реалізація стеганографічного методу з кодовим управлінням вбудовуванням ДІ дозволяє забезпечити кількість помилок на рівні 1.6% при вилученні ДІ під дією атаки стиском проти вбудованого повідомлення з коефіцієнтом якості $QF = 10$, що у 8.125 разів менше за подібний показник найкращого відомого аналогу. При цьому значення показника PSNR складає 35.6 дБ, що на 3% перевершує значення найкращого відомого аналогу, який володіє сумірним рівнем стійкості до атак проти вбудованого повідомлення.

Алгоритмічна реалізація розробленого стеганографічного метода з кодовим управлінням вбудовуванням ДІ на основі просторово-частотних матриць дозволяє забезпечити кількість зареєстрованих у системі абонентів, що дорівнює $J = 4800$, а також кількість одночасно працюючих абонентів при нульовому рівні внутрішньосистемних перешкод, що дорівнює $J = 64$. Таким чином розроблений метод дозволяє отримати у 1200 разів більше

зареєстрованих абонентів та у 16 разів більше одночасно працюючих абонентів при відсутності внутрішньосистемних перешкод.

Розроблений метод синтезу максимально нелінійних S-блоків як у сенсі компонентних булевих функцій, так і ФБЛ дозволяє синтезувати криптографічні конструкції з 4-нелінійністю $N_{4f} = 10.3431$, що до 21.55% перевищує значення найкращих відомих аналогів. Метод синтезу S-блоків, що відповідають суворому лавинному критерію компонентних 4-функцій та критерію максимального лавинного ефекту компонентних булевих функцій дозволяє покращити лавинні властивості криптографічних конструкцій на 9.375% у порівнянні з найкращими відомими аналогами, тоді як метод синтезу S-блоків з ідеальними матрицями коефіцієнтів кореляції $\left|R_{ij}\right| = 0, i, j = 1, 2, ..., k$ дозволяє покращити кореляційні властивості синтезованих криптографічних конструкцій на 12.5%.

На базі сконструйованих у дисертаційній роботі криптографічних примітивів, що засновані на ФБЛ, розроблено спеціалізований шифр для шифрування послідовності переліку станів, а також удосконалений БСШ прекодера, які на відміну від відомих існуючих аналогів, враховують криптографічну якість не тільки компонентних булевих функцій, а і компонентних ФБЛ.

Зменшення кількості необхідних для роботи стеганографічного методу з кодовим управлінням вбудовуванням операцій у $4\mu/3$ порівняно із найкращим аналогом дозволило реалізацію розробленої КСС в умовах обмежених технічних ресурсів, зокрема при роботі із потоковим контейнером в режимі реального часу. При роботі з ЦВ роздільної здатності 400p/720p/1080p/1140p швидкість роботи КСС становить 1815/825/354/257 fps в режимі вбудовування та 236/106/47/33 fps в режимі вилучення ДІ на найпоширенішій IoT платформі Raspberry Pi 4 під керуванням Raspbian Pi OS. При цьому експериментально встановлено мінімально необхідні значення кількості операцій Single Thread ARM процесорів необхідні для

роботи розробленої КСС, які при роботі з ЦВ роздільної здатності 400p/720p/1080p/1140p і частоти 30 fps для операції вбудовування ДІ, складають 7.4/16.6/37.3/52.5/149.2/437.9 MOps/Sec та 53.5/120.3/270.6/380.8/1082.4/4329.6 MOps/Sec для операції вилучення ДІ, що відповідає характеристикам переважної більшості застосовуваних на сучасних ресурсообмежених пристроях процесорів.

Особистий внесок здобувача. Роботи [13,16,18-19,31,32,37,38-39,43,45] виконані автором самостійно. З робіт, які написані у співавторстві, автору належать: отримання достатніх умов забезпечення заданих властивостей стеганоповідомлення [1], теоретичний базис синтезу ефективних кодових слів [2,44], стеганографічний метод з кодовим управлінням вбудовуванням ДІ [3], метод синтезу максимально-нелінійних S-блоків, що відповідають критерію розповсюдження помилки максимального порядку [4], критерій незалежності виходу ФБЛ від вхідних змінних [5], критерій нелінійності ФБЛ [6, 10, 15], критерій розповсюдження помилки та суворий лавинний критерій ФБЛ [17], метод синтезу АНФ ФБЛ [27], методи синтезу множин S-блоків, що задовольняють критеріям криптографічної якості компонентних булевих функцій та ФБЛ [8,12,20,21,24,25,28,30,46], дослідження властивостей ФБЛ [22,23,24,26,32,36], спеціалізований БСШ для шифрування послідовності переліку станів [7], визначення елементарної структури коефіцієнтів перетворення Уолша-Адамара [9], методи синтезу С-кодів для технології множинного доступу до прихованого каналу зв’язку на основі технології Multi-Code Code-Division Multiple Access [11,14,29,33,34,35], режими роботи криптоалгоритмів на пристроях з обмеженими ресурсами [40,41], дослідження властивостей компонентів КСС при їх практичній імплементації [42].

Апробація результатів дисертації. Матеріали дисертації доповідалися і обговорювалися:

1. На міжнародній науково-практичній конференції «Сучасні електронні та інформаційні технології», м. Одеса, 25—29 травня 2015 р.

2. На 19-му молодіжному форумі «Радіоелектроніка та молодь у XXI столітті», м. Харків, 20—22 квітня 2015.

3. На 17-й міжнародній науково-практичній конференції «Сучасні інформаційні та електронні технології», м. Одеса,23—27 травня 2016 р.

4. На 20-му ювілейному молодіжному форумі «Радіоелектроніка та молодь у XXI столітті», м. Харків, 19—21 квітня 2016.

5. На 18-й міжнародній науково-практичній конференції «Сучасні інформаційні та електронні технології», м. Одеса, 22—26 травня 2017 р.

6. На V міжнародній науково-технічній конференції «Информационные технологии в образовании, науке и производстве», м. Мінськ, 18-19 листопада 2017 р.

7. На першій міжнародній науково-практичній конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем», м. Київ, 5-6 квітня 2018 р.

8. На міжнародній конференції «Theory and Applications of Fuzzy Systems and Soft Computing», м. Київ, січень 2018 року.

9. На другій міжнародній конференції «Computer Modeling and Intelligent Systems», м. Запоріжжя, 2 квітня 2019 року.

10. На сьомій міжнародній науково-практичній інтернет-конференції «Сучасний рух науки», м. Дніпро, 6-7 червня 2019 р.

11. На міжнародній конференції «Cybersecurity Providing in Information and Telecommunication Systems», м. Київ, 7 липня, 2020 р.

12. Міжнародна науково-практична конференція «Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру», м. Одеса, 21 травня 2021 року.

13. На міжнародній конференції «Knowledge-Basedand Intelligent Information & Engineering Systems: Proceedings of the 25th International Conference», 8-10 вересня 2021, м. Щецин, Польща.

14. На міжнародній конференції «Cybersecurity Providing in Information and Telecommunication Systems», м. Київ, 28 січня 2021 р.

15. На міжнародній конференції «Engineer of XXI Century», м. Більсько-Бяла, Польща, 10 грудня 2021 р.

16. На міжнародній науково-практичній конференції «Intellectual Systems and Information Technologies», м. Одеса, 13-19 вересня 2021 р.

17. На міжнародній конференції «Computer Modeling and Intelligent Systems», м. Запоріжжя, 12 травня 2022 р.

Публікації. За результатами досліджень, які викладені в даній дисертаційній роботі, опубліковано 63 наукові роботи, з них 22 статті у фахових виданнях України, 29 в міжнародних виданнях, 26 статей у виданнях, що входять до наукометричних баз Scopus та/або Web of Science (з яких 5 статей є перекладами статей у фахових виданнях України), 17 публікацій у збірниках праць міжнародних та регіональних конференцій.

Структура та обсяг дисертації. Дисертація складається зі вступу, шести розділів, загальних висновків, списку використаної літератури до кожного розділу, загалом 336 літературних джерел, додатків на 6 сторінках, 57 рисунків і 45 таблиць — всього 377 сторінки. Основний текст дисертації складається з 331 сторінок.

Розділ 1.

ДОСЛІДЖЕННЯ ЕВОЛЮЦІЇ ПІДХОДІВ ДО ЗАСТОСУВАННЯ КРИПТОГРАФІЧНИХ ТА СТЕГАНОГРАФІЧНИХ ЗАСОБІВ У СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Дослідження еволюції систем захисту інформації дозволяє виділити дві принципово різні концепції, що покладено в основу даного процесу: приховування самого факту наявності конфіденційної інформації або її перетворення таким чином, щоб її сприйняття без знання секретного ключа стало неможливим. Різні епохи розвитку науки і техніки характеризувалися різними способами імплементації цих двох концепцій щодо захисту інформації. На сьогодні, із значним прогресом інформаційних технологій став доступним потужний інструментарій для реалізації вказаних концепцій, в результаті чого вони тією чи іншою мірою лежать в основі будь-якої практично реалізованої системи захисту інформації. Саме якість реалізації або однієї, або відразу двох цих концепцій визначають ефективність всієї системи захисту інформації якою складною та всеосяжною вона б не була.

Метою поточного розділу є огляд найсучасніших підходів до створення стеганографічних та криптографічних систем захисту інформації, а також шляхів їх поєднання.

Для досягнення мети розділу необхідно вирішити наступні задачі:

1. Провести огляд методів побудови стеганографічних систем захисту інформації, вимог до їх якості та особливостей застосування у сучасних інформаційних системах.

2. Провести огляд методів побудови криптографічних систем захисту інформації та вимог до їх якості.

3. Провести аналітичний огляд способів об’єднання стеганографічної та криптографічної складової для формування крипто-стеганографічних систем захисту інформації.

1.1. Поняття крипто-стеганографічної системи

Бурхливий розвиток інформаційних технологій та їх повсюдне впровадження в усі сфери людської діяльності призвело до формування суттєвої вразливості таких систем до можливих неправомірних впливів. Зловмисний вплив на інформаційну систему може призвести до катастрофічних наслідків для такої системи, і, за відсутності належного захисту інформаційної системи, результуючі можливі збитки такого впливу залежатимуть лише від сфери, в якій ця інформаційна система використовується: починаючи від спотворення та витоку особистих та корпоративних даних, фінансової та комерційної таємниці, закінчуючи можливими впливами на інформацію, яка є життєво важливою для національної безпеки та обороноздатності країни [1].

Така важливість та актуальність задачі забезпечення захисту інформації призвела до пильної уваги сучасних дослідників до задачі забезпечення її захисту. На сьогодні, представлені системи захисту інформації є комплексними [2], орієнтуються на специфічні параметри інформаційної системи, захист якої вони забезпечують. Тем не менш, основні складові частини на які ґрунтуються їх захисні можливості є незмінними, та такими, що спираються на багатовіковий людський досвід рішення задач захисту інформації [3, 4]. Для формування таких базисних елементів систем захисту інформації сьогодні існують два основні підходи, на основі яких створено відповідні галузі науки [5]:

криптографія — наука про методи забезпечення неможливості читання інформації сторонніми особами, неможливості непомітної її зміни, перевірки її автентичності;

стеганографія — наука про методи приховування самого факту передавання або зберігання інформації.

На сьогоднішній день, обидва напрямки зазнали суттєвого розвитку, в результаті чого, для кожного з них було створено інструментарії для вирішення того чи іншого завдання у практично реалізованих комплексних системах захисту інформації.

Тим не менш, сучасні вітчизняні та закордонні дослідники приходять до висновку неможливості окремого застосування криптографічних або стеганографічних компонентів систем захисту інформації. Так, невід'ємною складовою прекодера будь-якої стеганографічної системи є блок попереднього шифрування ДІ для рішення задачі неможливості її читання без знання секретного ключа, а також задачі руйнації статистичних особливостей ДІ перед її вбудовуванням у контейнер, що є необхідним для зниження ризиків детектування ДІ при відмінності її властивостей від властивостей ПВП.

З іншого боку, суттєві зміни, що сталися у глобальному трафіку в сторону величезного збільшення мультимедіа контенту, в першу чергу, ЦЗ та ЦВ, а також бурхливий розвиток та впровадження мобільних пристроїв, пристроїв IoT, IoBT, БПЛА робить використання лише криптографічного захисту інформації не тільки недостатнім, але ж і нераціональним, через невикористані можливості застосування потенційних прихованих каналів передачі інформації у ЦЗ і ЦВ, що генеруються та передаються зазначеними пристроями.

Отже, з перерахованого стає очевидним той факт, що для забезпечення всебічного захисту інформації, необхідністю є об'єднання криптографічного

та стеганографічного підходу. Дослідження, спрямовані на таке об’єднання проводилися як закордонними [6…12] так і вітчизняними [13] дослідниками.

Так, у фундаментальній роботі [13] вітчизняним дослідником академіком Задіракою В.Г. підкреслюється необхідність об’єднання застосувань криптографічної та стеганографічної складової у системах захисту інформації та вводиться фундаментальне визначення крипто-стеганографічної системи:

крипто-стеганографічна система (КСС) — складний комплекс, загальна стійкість якого не визначається лише стійкістю застосованого криптографічного чи стеганографічного перетворення. Стійкість усієї системи залежатиме від правильного узгодження криптографічної і стеганографічної складових системи.

Тим не менш, у сьогоденні науковці здебільше розглядають криптографічні та стеганографічні складові таких крипто-стеганографічних систем окремо, при цьому їх одночасне функціонування із врахуванням сучасних особливостей інформації, що захищається, не розглядаються взагалі. Окрім цього, при використанні крипто-стеганографічних систем в сучасних умовах, зокрема на мобільних пристроях, пристроях IoT, IoBT, БПЛА, важливими є не тільки вимоги до ефективності захисту проти існуючих загроз, які вони забезпечують, а і можливість їх роботи із ЦЗ та ЦВ у режимі реального часу, що є невід’ємною складовою багатьох сучасних інформаційних систем.

Зважаючи на тенденцію до суттєвого збільшення використання ЦЗ та ЦВ сучасними інформаційними системами, вимогу до їх обробки та передачі в режимі реального часу, активне впровадження автономних пристроїв із обмеженими обчислювальними можливостями, раціональним вбачається курс на інтеграцію криптографічної та стеганографічної складових крипто-стеганографічних систем задля об’єднання їх можливостей для протидії

існуючим викликам у необхідних режимах і для їх використання із врахуванням особливостей інформації, що захищається.

Зважаючи на той факт, що на сьогодні у відкритих літературних джерелах наведені лише концептуальні факти щодо необхідності об’єднання криптографічної та стеганографічної складових КСС, а всі вагомі результати щодо побудови та використання криптографічних та стеганографічних компонентів систем захисту інформації розроблені, досліджені та протестовані окремо, огляд найголовніших відомих результатів, що складатимуть основу подальших досліджень проведено у окремих підрозділах.

1.2. Огляд сучасних стеганографічних методів захисту інформації

Сьогодні створено чимало інструментів цифрової стеганографії для вирішення різноманітних завдань, пов’язаних із забезпеченням стеганографічного захисту інформації. При цьому, існують інструменти, здатні працювати із різноманітними типами контейнерів: ЦЗ, ЦВ, звук, інші контейнери. Тем не менш, зважаючи на особливості сьогоднішнього інформаційного трафіку, найбільш важливими є стеганографічні методи, адаптовані для роботи саме із ЦЗ і ЦВ. Класифікацію [14] таких стеганографічних інструментів представлено на рис. 1.1.

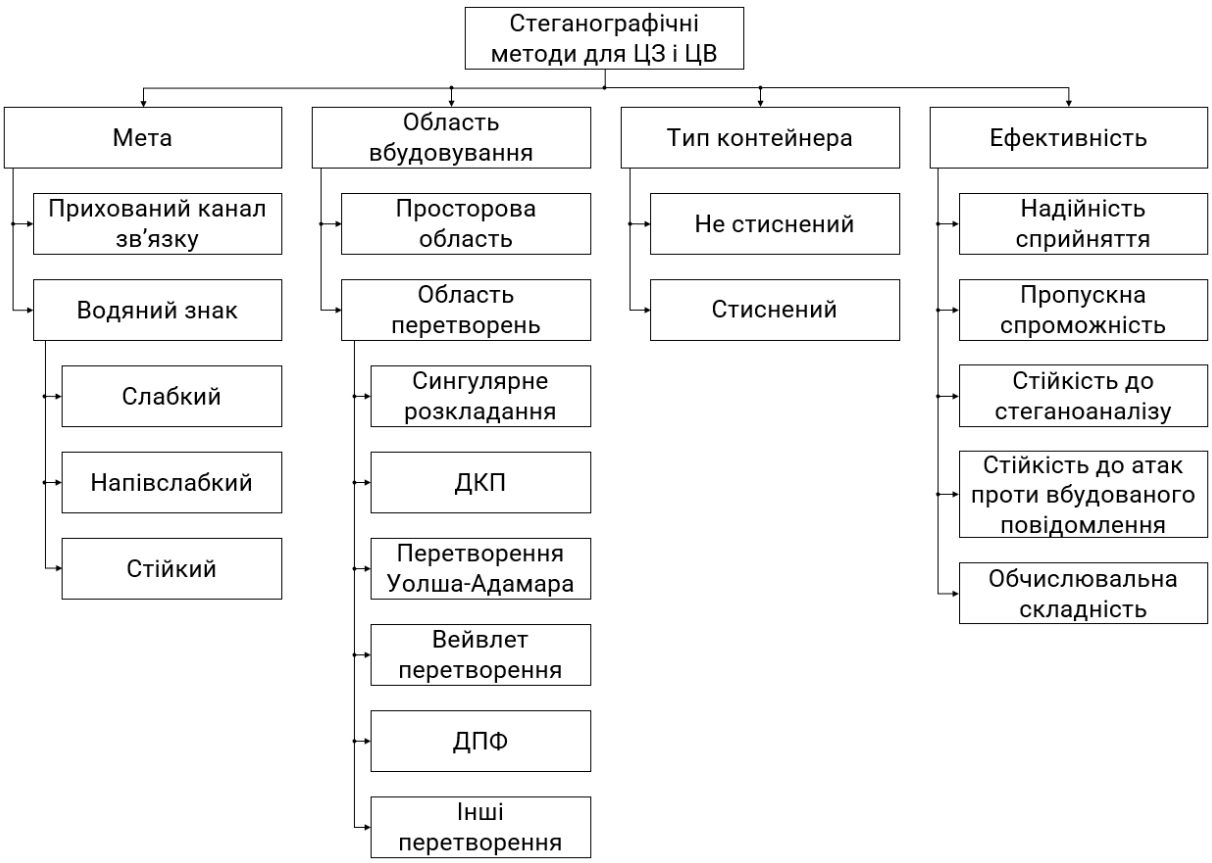


Рис. 1.1. — Класифікаційна схема стеганографічних методів, що застосовуються для роботи з ЦЗ та ЦВ

Найбільший інтерес, з огляду на побудову КСС, являють саме стеганографічні методи організації прихованого каналу зв'язку, тоді як зважаючи на особливості функціонування сучасних інформаційних систем, у яких передбачено механізми стиску ЦЗ та ЦВ при їх передаванні, важливою є властивість стеганографічного методу протидіяти атакам проти вбудованого повідомлення.

На рис. 1.2. показано узагальнену структурну схему стеганографічної системи, призначеної для передавання інформації.

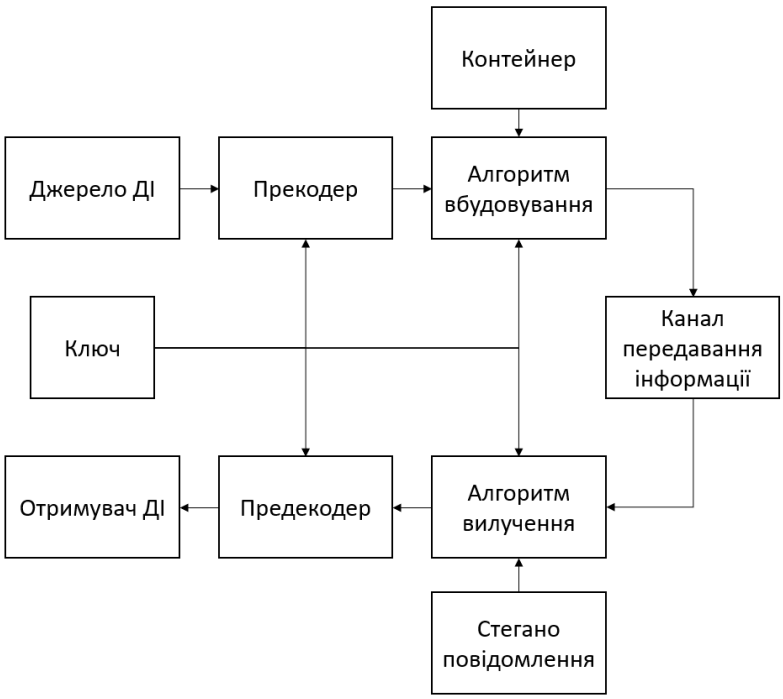


Рис. 1.2. — Структурна схема стеганографічної системи передавання інформації

Відзначимо при цьому, що функціонування стеганографічних систем на практиці, зазвичай потребує їх відповідності всім вказаним на рис. 1.1. вимогам до ефективності.

Забезпечення надійності сприйняття є очевидною вимогою до ефективності роботи стеганографічної системи і передбачає неможливість детектування наявності ДІ в контейнері при суб'єктивному ранжуванні стеганоповідомлення. Сьогодні задля математичного виміру степеню забезпечення надійності сприйняття впроваджено досить багато різних показників та створено досить багато моделей сприйняття ЦЗ та ЦВ людиною, наприклад [15-19]. Тим не менш, завдання оцінки надійності сприйняття стеганоповідомлень сьогодні не є вирішеним остаточно, насамперед, через складність механізмів сприйняття ЦЗ та ЦВ людиною, тоді як найбільш вживаним способом оцінювання надійності сприйняття стеганоповідомлень лишається використання різницевих показників, одним з

найпоширеніших серед яких є пікове відношення «сигнал-шум» PSNR, який для кожної кольорової компоненти ЦЗ, або кадру ЦВ визначається як[20]

$$PSNR = 20\lg\left(\frac{255}{\sqrt{MSE}}\right), \tag{1.1}$$

де

$$MSE = \frac{1}{nm}\sum_i\sum_j \left|X(i,j) - M(i,j)\right|^2, \tag{1.2}$$

а X являє собою $n \times m$-матрицю вихідного зображення, тоді як M — матриця стеганоповідомлення відповідного розміру.

На сьогодні існують ряд стеганографічних методів, спрямованих на максимізацію показника надійності сприйняття стеганоповідомлення, наприклад [20…21], однак, загальним недоліком цих методів є те, що максимізація надійності сприйняття призводить до необхідності зосередження ДІ в області найвищих частотних складових ЦЗ / кадра ЦВ, що суттєво знижує, або, навіть зводить нанівець стійкість стеганоповідомлення до атак проти вбудованої ДІ.

Наступним критерієм ефективності стеганографічних систем є критерій максимізації пропускної спроможності прихованого каналу зв’язку. Під пропускною спроможністю прихованого каналу зв’язку розуміють максимальну кількість інформації, яка може бути вкладена в один елемент контейнера [22]. Відзначимо при цьому, що існують різні підходи до визначення пропускної спроможності через врахування можливих збурних дій на стеганоповідомлення при його передаванні та різних рівнів захисту від них, що може забезпечити конкретний стеганографічний метод. Вибір конкретного підходу обумовлений метою захисту інформації, моделями порушника, його можливостями, реалізованими ним атаками на стеганосистеми, видом використовуваних контейнерів і прихованих повідомлень і багатьма іншими факторами.

На сьогодні створено низку стеганографічних методів [23…30], що орієнтовані на досягнення якнайбільшої пропускної спроможності прихованого каналу зв’язку. Тим не менш, збільшення пропускної спроможності тісно пов’язане із погіршенням надійності сприйняття стеганоповідомлення та зменшенням його резистивності до атак проти вбудованого повідомлення та стеганоаналітичних атак.

Наступною вимогою є стійкість стеганоповідомлення до атак стеганоаналізу. Найчастіше метою стеганоаналітичних атак [31] є виявлення самого факту наявності вбудованого повідомлення, однак, існують різновиди стеганоаналітичних атак, що спрямовані на вилучення прихованої ДІ із стеганоповідомлення.

На рис. 1.3. представлена класифікація сучасних стеганоаналітичних методів.

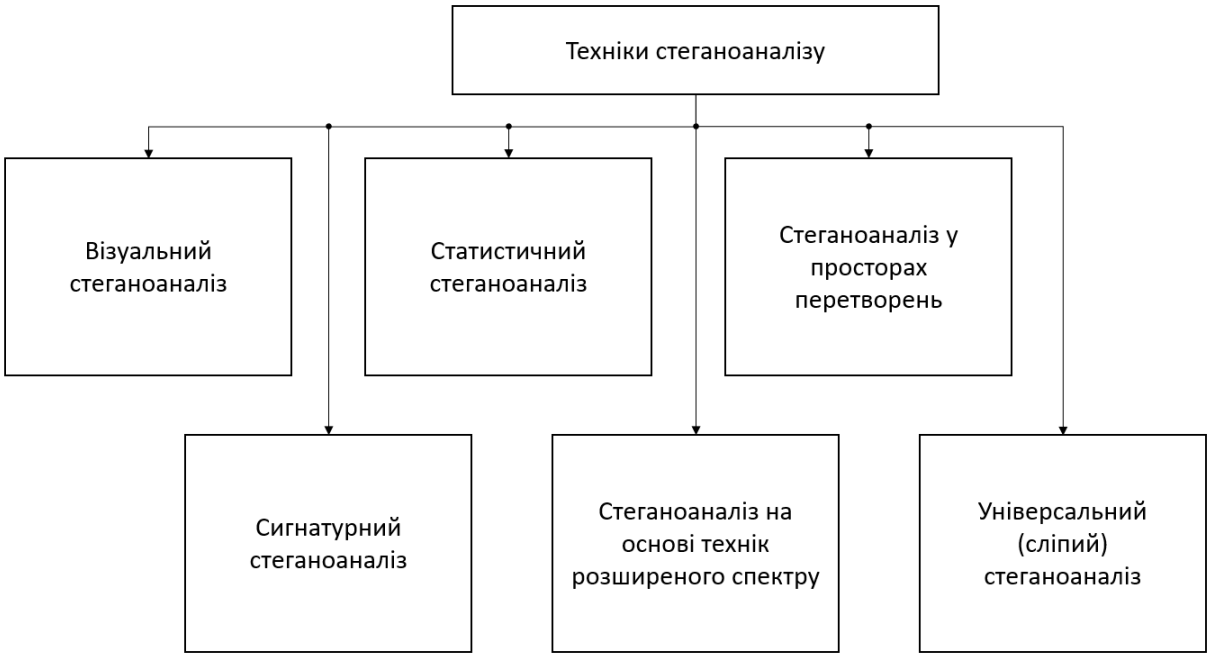


Рис. 1.3. — Класифікаційна схема стеганоаналітичних методів

Сьогодні створено низку стеганографічних методів, що декларують певний рівень стійкості до відомих стеганоаналітичних атак. До таких методів слід віднести, наприклад,[32].

Важливою у сьогоденні є вимога до стійкості стеганографічного методу до можливих атак проти вбудованого повідомлення. Класифікація [14] типових атак проти вбудованого повідомлення представлена на рис. 1.4.

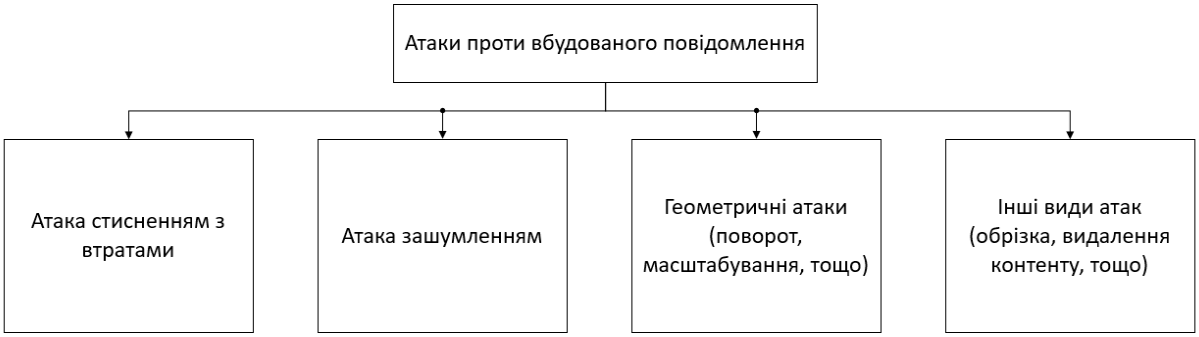


Рис. 1.4. — Класифікаційна схема типових атак проти вбудованого повідомлення

Однією з найголовніших атак, з якою пов’язане використання сучасних стеганографічних систем, є атака стисненням з втратами, адже стеганоповідомлення при передавання каналами зв’язку сьогодні найчастіше зазнають стиску одним з відомих алгоритмів стиснення ЦЗ або ЦВ. Цей факт ставить у пріоритет вимогу забезпечення стійкості стеганографічних методів, що розробляються, до вказаного виду атак проти вбудованого повідомлення. Відзначимо, що надання стеганоповідомленню стійкості до атак проти вбудованого повідомлення часто призводить до зниження надійності сприйняття стеганоповідомлення через те, що забезпечення такої стійкості вимагає вбудовування ДІ здебільшого у низькі та середні частотні складові контейнера, які з одного боку є найменш чутливими до атак проти вбудованого повідомлення, а з іншого — щонайкраще сприймаються при суб’єктивному ранжуванні. Забезпечення стійкості стеганоповідомлення до можливих атак проти вбудованої ДІ також найчастіше веде до суттєвого зменшення пропускної спроможності стеганографічної системи. До

стеганографічних методів, що забезпечують стійкість стеганоповідомлення до атак проти вбудованої ДІ, можна віднести, наприклад, [33…36].

Важливо відзначити, що забезпечення вбудовування ДІ в низькочастотні та середньочастотні складові контейнера найбільш просто досягти із застосуванням областей перетворення контейнера: ДКП, вейвлет-перетворення, спектрального/сингулярного розкладання матриць-блоків контейнера. Наслідком цієї обставини є те, що більшість відомих сьогодні стеганографічних методів, що позиціонуються як стійкі до атак на вбудовану ДІ виконують вбудовування та вилучення інформації у зазначених областях перетворень, адже саме в них насьогодні сформульовано достатні умови для забезпечення такої стійкості [37…38].

Розглянемо найголовніші перетворення, які застосовуються для розробки сучасних стеганографічних методів, що володіють стійкістю до атак проти вбудованого повідомлення. Найпоширенішим з таких перетворень є ДКП, яке визначається наступним співвідношенням

$$S = C_N X C_N^T, \tag{1.3}$$

де X — фрагмент вихідного зображення розміру $N \times N$,

C_N — $N \times N$-матриця ДКП, елементи $C(i, j),\ i, j = 0,1,..., N-1$ якої обчислюються відповідно до формули

$$C(i, j) = \begin{cases} \dfrac{1}{\sqrt{N}}, & \text{при } i = 0; \\ \sqrt{\dfrac{2}{N}} \cos(2j+1) \cdot i \cdot \pi, & \text{при } i > 0. \end{cases} \tag{1.4}$$

Трансформанти ДКП показують розподіл контенту блоку зображення по частотним складовим. При цьому відомо [38], що чутливість стеганоповідомлення до збурювальних впливів залежить від того, які саме частотні складові зазнали збурення в процесі стеганоперетворення. Так, гарантована стійкість стеганографічного методу до атак проти вбудованого повідомлення забезпечується за рахунок збурення низькочастотних

складових контейнера. Такі зміни з великою ймовірністю негативно відіб'ються на надійності сприйняття стеганоповідомлення, через що на практиці часто використовується «компромісний варіант», коли вбудовування ДІ проводиться таким чином, щоб збурення зазнали середньочастотні складові цифрового контенту. Однак, такий підхід забезпечує стійкість стеганографічного метода лише до незначних збурювальних впливів, в той час як в реаліях атаки проти вбудованого повідомлення можуть бути значними (наприклад, стиснення стеганоповідомлення з малим коефіцієнтом якості).

Розподілення частотних складових у матриці трансформант ДКП блока X наведено на рис. 1.5.

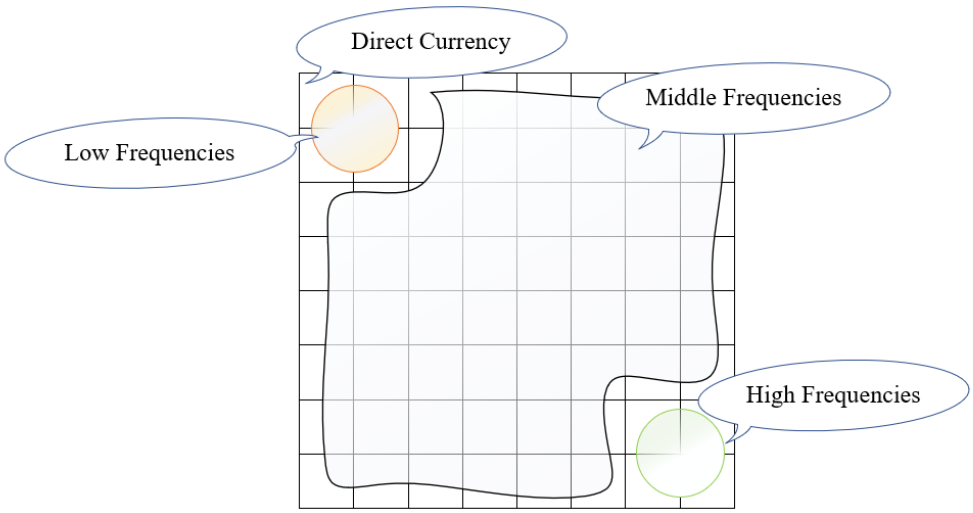


Рис. 1.5. — Розподілення частотних складових у трансформантах ДКП

Насьогодні існує досить багато стеганографічних методів, які для своєї роботи використовують область перетворень ДКП, наприклад [39…45].

Перспективним видом перетворень, що використовується для побудови сучасних стеганографічних методів, є двовимірне перетворення Уолша-Адамара, яке задається за допомогою наступного співвідношення

$$W_X = H'_N X H'^T_N, \qquad (1.5)$$

де $H'_N = \frac{1}{\sqrt{N}} H_N$, X — матриця розміру $N \times N$, а матриця Адамара H_N порядку N визначається за допомогою конструкції Сильвестра

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix}, \; H_1 = 1. \tag{1.6}$$

Зазначимо, що окрім двовимірного перетворення Уолша-Адамара в теорії сигналів і криптографії широко застосовується одновимірне перетворення Уолша-Адамара вектора-рядка довжини N, яке записується як

$$V = YH_N. \tag{1.7}$$

Перетворення Уолша-Адамара характеризується великою швидкодією та стало основою побудови деяких стеганографічних методів, серед яких [46…53].

Іншим видом перетворень, на якому засновані найефективніші з відомих сьогодні стеганографічних методів, що характеризуються стійкістю до атак проти вбудованого повідомлення є сингулярне розкладання.

Під сингулярним розкладанням матриці-блока X розміру $N \times N$ розуміють його уявлення у вигляді [37]

$$X = U\Sigma V^T, \tag{1.8}$$

де U, V ортогональні матриці розміру $N \times N$,

стовпці $u_1,...,u_8$ матриці U, називають лівими СНВ, стовпці $v_1,...,v_8$ матриці V називають правими СНВ матриці X, тоді як $\Sigma = diag(\sigma_1,...,\sigma_8)$ — діагональна матриця СНЧ.

У роботі [37] були сформульовані формальні достатні умови забезпечення надійності сприйняття стеганоповідомлення в області сингулярного розкладання (блоків) матриці контейнера, що робить використання саме цієї області перетворень блоків контейнера найбільш зручним с точки зору забезпечення стійкості стеганоповідомлення до атак проти вбудованої ДІ. Це послужило базисом для створення найкращих, з

точки зору захищеності від атак проти вбудованого ДІ, стеганографічних методів [32…36, 54…64].

Однак, незважаючи на всі переваги, використання областей перетворень для роботи стеганографічних алгоритмів не позбавлено суттєвого недоліку, який полягає у необхідності виконання прямого та зворотного перетворення, що пов’язано із суттєвими обчислювальними витратами. Нажаль, найвибагливішим до обчислювальних ресурсів є саме сингулярне розкладання, що веде до невідповідності таких методів критерію мінімізації необхідних для роботи стеганографічного методу обчислювальних ресурсів. Це, у свою чергу, практично унеможливлює використання ефективних стеганографічних методів в областях перетворень на обмежених у ресурсах платформах: мобільних пристроях, пристроях IoT та IoBT, а також, БПЛА.

Дослідниками у роботах [65…66] підкреслювалася висока актуальність розробки стеганографічних методів, що є стійкими до атак проти вбудованого повідомлення та працюють у просторовій області, таким чином, виключаючи необхідність додаткових перетворень при вбудовуванні та вилученні стеганоповідомлень. На сьогодні, існують низка нестійких до атак проти вбудованої ДІ, стеганографічних методів, що працюють в просторовій області [67…74]. У роботі [75] на основі умови забезпечення стійкості сприйняття в області сингулярних розкладань матриць блоків контейнера [37] створено достатню умову забезпечення стійкості стеганоалгоритмів до збурних дій, що реалізується у просторовій області контейнера, на основі чого було побудовано стеганографічні алгоритми [75…77], що оперують у часовій області та характеризуються стійкістю до атак проти вбудованого повідомлення. Тим не менш, побудовані алгоритми основані на зміні інтенсивності пікселів блоків контейнера у певних межах, що не дає змогу керувати впливом стеганографічного методу на необхідні частотні складові блоків контейнера, а, отже, і характеристиками стеганографічного методу з

метою досягнення його відповідності критеріям ефективності. Окрім того, зазначені стеганографічні методи вимагають досить суттєвого впливу на блоки зображень (значення амплітуди збурних дій може сягати 9), що негативно відзначається на надійності сприйняття зображення, а так само ці алгоритми характеризуються зменшенням ефективності при наявності у контейнері областей з малими перепадами значень яскравості.

Отже, питання розробки ефективних стеганографічних методів, які працюють у просторовій області контейнера до сьогодення залишаються не вирішеними, що суттєво стримує подальший розвиток КСС.

1.3. Огляд сучасних криптографічних методів захисту інформації

Метою криптографічних методів захисту інформації є її перетворення таким чином, щоб унеможливити її читання неавторизованим користувачем. При цьому, при суто криптографічному захисті, сам факт передачі інформації не приховується. На рис. 1.6. представлено класифікацію сучасних криптографічних алгоритмів.

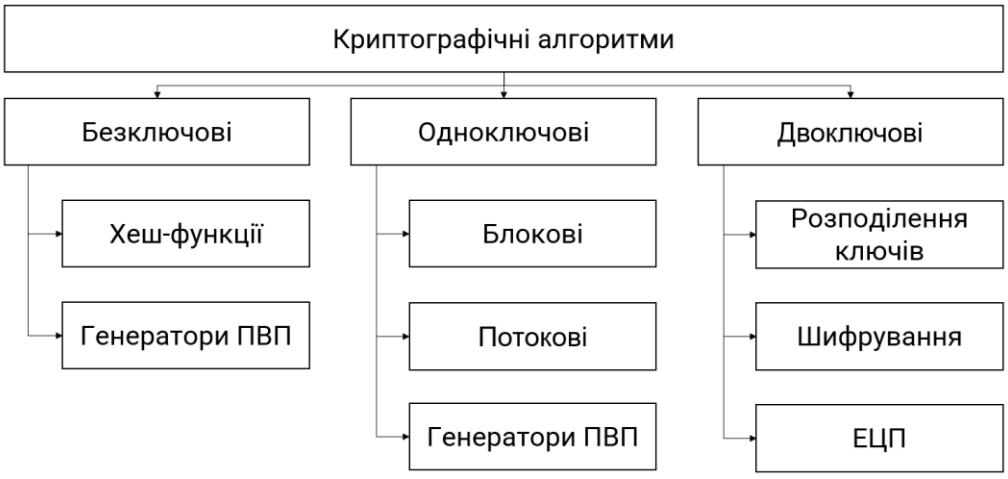


Рис. 1.6. — Класифікація сучасних криптографічних алгоритмів

На сьогодні, у практичних системах захисту інформації, безключові криптографічні алгоритми найчастіше використовуються для контролю цілісності інформації, у системах парольного захисту, для генерації модифікаторів вхідних значень хеш-функцій та векторів ініціалізації, тощо. З іншого боку, двоключові (асиметричні) криптографічні алгоритми через їх значну обчислювальну складність та необхідність використання довших ключів, у порівнянні із одноключовими (симетричними) криптоалгоритмами, використовуються більшою мірою на етапі розподілення ключової інформації або для організації систем електронного цифрового підпису.

Основним криптографічним засобом, призначеним для шифрування, що застосовується для захисту великих обсягів даних, які передаються та зберігаються, є симетричні криптографічні алгоритми, насамперед, блокові.

Будь-який сучасний криптографічний алгоритм, поза залежністю від його місця у класифікації на рис. 1.6., засновано на основоположних принципах, запропонованих К. Шенноном: дифузії та конфузії [78].

Визначення 1.3.1. Дифузія — метод, при якому надмірність в статистиці вхідних даних «розподіляється» по всій структурі вихідних даних.

Визначення 1.3.2. Конфузія — метод, при якому залежність ключа і вихідних даних робиться якомога більш складною, зокрема, нелінійною.

Однак, подібно до теореми Шеннона про кодування дискретного джерела, принципи дифузії та конфузії дають лише вербальне уявлення про якість криптографічних конструкцій та побудованих на їх основі криптографічних алгоритмів, проте не надають ані конкретні методи оцінки якості криптографічних примітивів та криптографічних алгоритмів, ані методи побудови криптографічних примітивів та алгоритмів, які б найкращим чином імплементовували ці принципи.

Питання побудови криптографічних алгоритмів та примітивів тісно пов’язане із питанням оцінки криптографічної якості конструкцій, на яких вони засновані. Так, вибір тієї чи іншої конструкції для застосування у

криптоалгоритмі залежить від розуміння розробниками даного алгоритму степені імплементації принципів дифузії і конфузії, яку дана конкретна конструкція здатна забезпечити.

З часів формулювання К. Шенноном принципів дифузії та конфузії було зроблено чимало спроб створити всебічну теорію оцінки якості криптографічних алгоритмів та примітивів на їх основі, яка б була орієнтована на оцінку спроможності складових частин криптоалгоритмів та їх суперпозицій протистояти можливим атакам за допомогою сучасних методів криптоаналізу [79…88].

Так, на цей час створено чимало підходів до оцінки криптографічної якості, зокрема на основі аналізу стохастичних властивостей вихідних послідовностей криптографічних алгоритмів [89, 90], до яких можуть, наприклад, застосовуватися тести стохастичної якості [91, 92]. Відомий також підхід, який передбачає створення та дослідження міри імплементації криптоалгоритмом принципів дифузії та конфузії на основі дослідження його зменшених копій [93…95], який було застосовано до криптоалгоритмів Калина [96, 97], Rijndael [98] та інших [99]. Відомий також спосіб оцінки якості імплементації криптоалгоритмом принципів дифузії та конфузії на основі дослідження швидкості наближення шифру до стаціонарного стану, властивого випадковій підстановці [100], інші загальні підходи [101…111], а також підходи, застосовні для конкретних криптографічних алгоритмів [112…118].

На рис. 1.7. представлено схему, яка являє собою класифікацію основних підходів до дослідження криптографічної якості криптоалгоритмів.

Рис. 1.7. — Класифікація основних підходів до дослідження криптографічної якості криптоалгоритмів

Серед підходів, означених на рис. 1.7 загальноприйнятим на сьогодні є підхід до синтезу і аналізу криптографічних примітивів передбачає їх опис за допомогою компонентних булевих функцій [119…121], до яких потім застосовується набір критеріїв криптографічної якості.

Побудова сучасних БСШ передбачає ітеративне використання криптографічних примітивів [122,123]. На рис. 1.8. наведено класифікацію основних криптографічних примітивів, що використовуються сьогодні для побудови симетричних криптографічних алгоритмів.

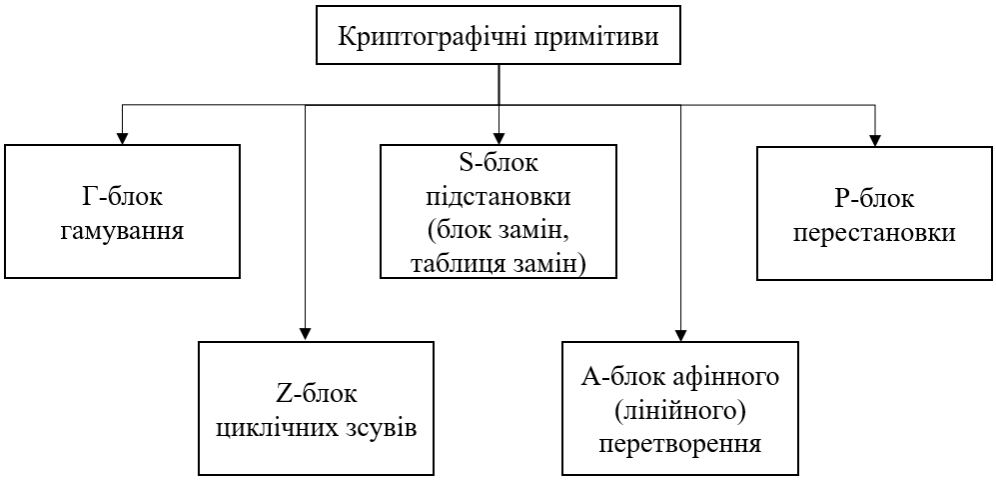


Рис. 1.8. — Класифікація криптографічних примітивів

Багато шифрів використовують у своєму складі декілька із зазначених на рис. 1.8. криптографічних примітивів, але найважливішими з них є S-блоки та P-блоки. При цьому, за своєю побудовою та за своїми властивостями, вирішальний вплив на якість криптографічного перетворення та на його швидкодію має саме S-блок.

Вичерпну інформацію щодо визначення S-блоку, його різновиди, а також існуючі сьогодні методи його уявлення можна знайти у роботах [119, 120].

Саме через важливість такої криптографічної конструкції, як S-блок для функціонування криптографічних алгоритмів, найбільша увага дослідників в області криптографії сконцентрована, з одного боку, на вдосконаленні існуючого інструментарію оцінки криптографічної якості S-блоків, а з іншого — вдосконаленню методів побудови великих множин S-блоків, які б володіли високим рівнем криптографічної якості. При цьому, найголовнішу роль у цих двох процесах відіграє загальноприйнятий підхід до оцінки криптографічної якості S-блоків, що заснований на їх уявленні за допомогою компонентних булевих функцій. Основні визначення та дані щодо застосування математичного апарату булевих функцій наведено в роботі [121]. Тим не менш, останні дослідження показують, що застосування

математичного апарату булевих функцій при роботі з криптографічними примітивами не може вважатися вичерпним.

Так, при здійсненні атаки на криптографічний алгоритм криптоаналітик не обмежений в обраному математичному апараті, за допомогою якого здійснюється подання конструкцій криптографічного алгоритму. Можливості подання конструкцій криптографічних алгоритмів за допомогою ФБЛ обумовлені їх довжинами. Для найбільш розповсюджених довжин криптографічних примітивів, що застосуються у сучасних криптоалгоритмах, можливі подання за допомогою ФБЛ наведено на рис. 1.9.

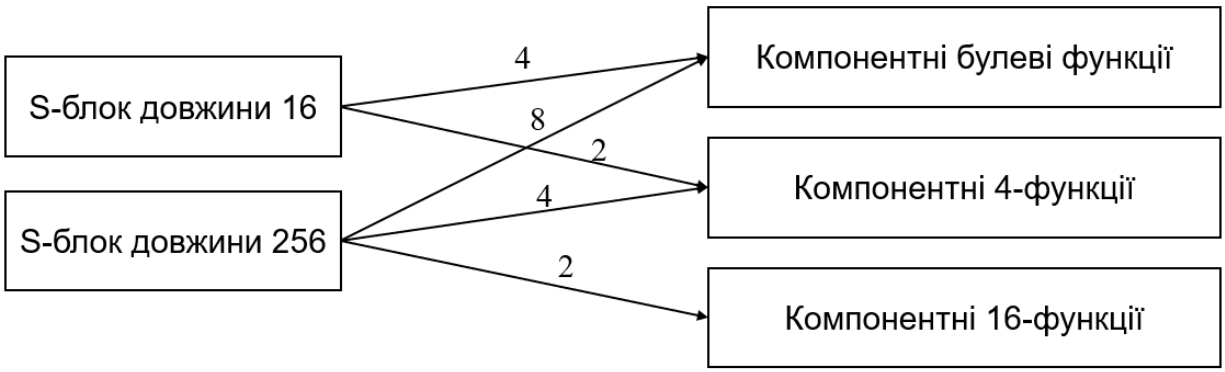


Рис. 1.9. — Можливі уявлення S-блоків для найбільш розповсюджених довжин N

Сутність існування можливості уявлення конструкцій S-блока за допомогою компонентних булевих функцій та компонентних ФБЛ можна прояснити за допомогою табл. 1.1.

Таблиця 1.1. — Уявлення S-блока довжини $N = 16$ за допомогою компонентних ФБЛ

5	**9**	**2**	**4**	**8**	**7**	**3**	**10**	**15**	**1**	**13**	**11**	**6**	**14**	**0**	**12**
1	1	0	0	0	1	1	0	1	1	1	1	0	0	0	0
0	0	1	0	0	1	1	1	1	0	0	1	1	1	0	0
1	0	0	1	0	1	0	0	1	0	1	0	1	1	0	1
0	1	0	0	1	0	0	1	1	0	1	1	0	1	0	1
1	1	2	0	0	3	3	2	3	1	1	3	2	2	0	0
1	2	0	1	2	1	0	2	3	0	3	2	1	3	0	3

На сьогодні в криптографії склалося повне розуміння щодо можливих критеріїв криптографічної якості, які можуть бути застосовані до компонентних булевих функцій криптографічної конструкції із метою визначення її криптографічної якості, яка чисельно показує наскільки криптографічна конструкція здатна імплементувати концепції дифузії та конфузії. Тим не менш, питання визначення якості криптографічних конструкцій при їх уявленні за допомогою ФБЛ фактично не знайшли свого цілісного рішення у наявних відкритих літературних джерелах. У табл. 1.2. представлено аналітичний огляд відомих доробків щодо критеріїв криптографічної якості булевих функцій та ФБЛ.

Таблиця 1.2. — Огляд критеріїв криптографічної якості булевих функцій та ФБЛ

Критерій	**Булеві функції**	**ФБЛ**
Алгебраїчний степінь нелінійності	Існує добре пророблений математичний апарат знаходження АНФ булевих функцій, за допомогою якої може бути визначено алгебраїчний степінь нелінійності.	Представлено метод знаходження АНФ ФБЛ для простих значень p [126]. Для найважливіших значень p^k, методи синтезу АНФ ФБЛ не представлені.

Продовження табл. 1.2.

	Відомо чимало робіт, спрямованих на синтез булевих функцій, що характеризуються високими алгебраїчними степенями нелінійності [122…124], а також робіт, які присвячені питанням синтезу S-блоків, що складаються з таких булевих функцій, наприклад, [125].	Не визначено критерії криптографічної якості компонентних ФБЛ криптографічних примітивів. Недостатньо дослідженими є і множини афінних ФБЛ та їх взаємозв'язок з функціями Віленкіна-Крестенсона. Наявні методи фактично не дозволяють проводити дослідження алгебраїчної нелінійності криптографічних конструкцій при їх уявленні ФБЛ.
Відстань нелінійності	На сьогодні можливо говорити про формування теорії нелінійності булевих функцій, яка містить як традиційні підходи, що базуються на визначенні нелінійності першого (відносно множини афінних функцій [127, 128]), так і нетрадиційних способів визначення нелінійності, наприклад, [129]. Існують методи вимірювання нелінійності булевих функцій як в часовій області, так і в області перетворень Уолша-Адамара [120]. Розроблено чимало методів синтезу високонелінійних булевих функцій [130…134].	На сьогоднішній день відомі визначення максимально-нелінійних ФБЛ [152], а також методи їх синтезу [153, 154]. Тим не менш, на сьогодні не відомі способи чисельної оцінки рівня нелінійності криптографічних конструкцій, уявлених за допомогою ФБЛ, що не дає змоги визначати та порівнювати їх криптографічну якість.

Продовження табл. 1.2.

	Добре проробленими є також питання синтезу високонелінійних S-блоків [135…140]. Булеві функції, що характеризуються максимальним рівнем нелінійності, називаються бент-функціями [141…146] та займають особливе місце у криптографії, зокрема для генерації ПВП [147…149] і високоякісних S-блоків [150]. Дослідженню та розробці методів синтезу бент-функцій присвячено чимало робіт, однак, вони лишаються одними з найбільш цікавих та непередбачуваних математичних конструкцій. Розроблено регулярні методи синтезу повного класу бент-функцій довжини $N=16$, потужність якого складає $J_{16}=896$ [144], а також повного класу бент-функцій довжини $N=64$, потужність якого складає $J_{64}=5\,425\,430\,528$ [151].	Відсутні також і методи синтезу криптографічних примітивів, що є високонелінійними як при їх уявленні за допомогою булевих функцій, так і за допомогою ФБЛ.
Критерій поширення помилки	Математичний апарат визначення відповідності булевих функцій і криптографічних конструкцій критерію поширення помилки є добре проробленим [121]. Чисельне визначення відповідності криптографічної конструкції критерію поширення помилки здійснюється на основі математичного апарату похідних булевих функцій [121, 155…158].	На сьогодні у відкритих літературних джерелах інформація щодо дослідження компонентних ФБЛ криптографічних конструкцій на предмет їх відповідності критерію поширення помилки, суворому лавинному критерію та критерію максимального лавинного ефекту, відсутня.

Продовження табл. 1.2.

	Через різноманітність вимог до криптографічних конструкцій створено похідні критерія поширення помилки: суворий лавинний критерій та критерій максимального лавинного ефекту [159, 160]. Чимало робіт присвячено синтезу множин булевих функцій [161, 162], а також криптографічних S-блоків [150,163], що відповідають суворому лавинному критерію. Окремий інтерес сучасних дослідників становлять методи синтезу S-блоків, що відповідають критерію поширення помилки вищих порядків [164].	Відсутні також і методи синтезу криптографічних конструкцій, що задовольняють зазначеним критеріям, при їх уявлення як у вигляді компонентних ФБЛ, так і у вигляді компонентних булевих функцій.
Кореляційний взаємозв'язок виходу і входу S-блока	Введені визначення кореляційного імунітету булевих функцій як в часовій області, так і в області перетворень Уолша-Адамара [121]. Введено визначення матриці коефіцієнтів кореляції криптографічних конструкцій [120], яке дозволяє чисельно оцінювати та порівнювати між собою степінь кореляційного зв’язку виходу та входу довільних криптографічних конструкцій. Встановлено взаємозв’язок між кореляційним імунітетом компонентних булевих функцій та матрицею коефіцієнтів кореляції [165-169].	Введено визначення кореляційного імунітету ФБЛ [170]. Тим не менш, методи дослідження та порівняння степеню відповідності криптографічних конструкцій критерію кореляційного імунітету лишаються невідомими. Невідомим також є взаємозв’язок матриць коефіцієнтів кореляції векторів виходу та входу криптографічних конструкцій з їх компонентними ФБЛ.

Продовження табл. 1.2.

		В літературі також відсутні методи синтезу криптографічних конструкцій, що задовольняють як критерію кореляційного імунітету компонентних булевих функцій, так і компонентних ФБЛ.
Лінійна надмірність компонентних функцій криптографічних конструкцій	Дослідження компонентних булевих функцій деяких криптографічних примітивів, наприклад, конструкції Ніберг [174] показує, що вони мають між собою певний математичний зв'язок. Такий зв'язок послаблює рівень конфузії, який може забезпечити досліджуваний криптографічний примітив, і, відповідно, посилює можливості криптоаналітика щодо опису криптоалгоритму в цілому. Дослідження, які були проведені в роботі [175] дозволили математично описати цей зв'язок за допомогою визначення афінної еквівалентності. Однак, у загальному випадку задача афінної класифікації булевих функцій є складною. В даний час встановлено, що для булевих функцій $k = 5$ змінних існує 48 класів афінної еквівалентності [176], тоді як для булевих функцій $k = 6$ змінних існує $150\,357$ класів афінної еквівалентності [177].	У відкритих джерелах інформація щодо дослідження лінійної надмірності компонентних ФБЛ криптографічних конструкцій, відсутня.

Закінчення табл. 1.2.

	Відзначимо, що складним є не тільки завдання повної класифікації булевих функцій з точки зору афінної еквівалентності, але також і завдання визначення афінної еквівалентності двох конкретно заданих компонентних булевих функцій, що ускладнює завдання пошуку оптимальних, з точки зору критерію відсутності лінійної надмірності, структур Q-послідовностей. У роботі [178] був запропонований новий метод визначення еквівалентності компонентних булевих функцій, який набагато спрощує практичну задачу визначення афінної еквівалентності компонентних булевих функцій криптографічних конструкцій.	

Порівняльний аналіз результатів наявних в літературі методів дослідження якості криптографічних конструкцій при їх уявленні за допомогою компонентних булевих функцій та ФБЛ, що наведені у табл. 1.2., дозволяє дійти висновку, що із наявним інструментарієм задача оцінки та підвищення криптографічної якості компонентних ФБЛ існуючих криптографічних алгоритмів, а також криптоалгоритмів та їх конструкцій, що розроблюються, не може бути вирішена.

При цьому, на сьогодні вже розроблено атаки на БСШ із застосуванням математичного апарату ФБЛ [171]. З іншого боку, дослідження компонентних ФБЛ криптографічних конструкцій є актуальним і в світлі динамічного розвитку квантової криптографії, що вже сьогодні

дозволяє говорити про формування постквантових криптографічних методів, які будуть актуальними при появі квантових комп'ютерів і здійсненні з їх допомогою квантових атак [172…178]. Відомо чимало адаптацій квантових атак до структури існуючих способів побудови криптографічних алгоритмів, наприклад, узагальненої мережі Фейстеля [179], або до конкретних блокових симетричних шифрів, наприклад, AES [180…186].

Ключем сучасного симетричного алгоритму шифрування є псевдовипадкова послідовність, отже, при досить великій довжині ключа потрібно використання атаки методом «грубої сили» або використання будь-якої структурної вразливості для злому криптоалгоритма, на відміну від використання алгоритмічних атак, наприклад, за допомогою алгоритму Шора [187], який може бути застосований для злому алгоритмів асиметричного шифрування. Даний факт робить особливо актуальним, в умовах постквантової криптографії, детальне дослідження і вдосконалення їх структури. Оскільки квантові комп’ютери ефективно оперують недвійковими даними [188…189], інтерес являє дослідження всіх можливих уявлень криптографічних алгоритмів, особливо за допомогою ФБЛ.

Методи ФБЛ, дослідження яких бере початок в історичній роботі [190], сьогодні стали основою для синтезу сигнальних конструкцій [191…194], створення електронних (у тому числі, наноелектронних) пристроїв на основі засад ФБЛ [195…199], застосуються також для розробки коригувальних і ефективних кодів [200]. Відомо також застосування недвійкових конструкцій для зниження пік-фактору сигналів при використанні технології кодового розділення каналів MC-CDMA у системах зв’язку [201], а так само і в стеганографії [202…204].

Перехід від двійкової логіки до багатозначної відкриває нові можливості, у роботі показано, що застосування криптографічних конструкцій, які характеризуються високою якістю як з точки зору компонентних булевих функцій, так і з точки зору ФБЛ, дозволяє значно

підвищити імплементацію криптоалгоритмами концепцій дифузії і конфузії, а, отже, підвищити ефективність криптографічних перетворень, зменшити необхідну кількість застосувань криптографічних примітивів для забезпечення високої якості криптограм.

Окрім цього, криптографічні конструкції, що розроблені із застосуванням математичного апарату ФБЛ характеризуються більшою відповідністю сучасній парадигмі побудови багатоядерних процесорів, значною алгоритмічністю. Використання ФБЛ відкриває можливості щодо гармонійного поєднання криптографічного захисту інформації з іншими компонентами, насамперед, його узгодження із стеганографічною складовою.

1.4. Висновки

Таким чином, у першому розділі дисертаційної роботи було проведено аналіз наукової літератури за темою дисертації, зокрема проаналізовано сучасні підходи до побудови стеганографічних систем, криптографічних систем та КСС. Проведене дослідження еволюції підходів до створення КСС, стеганографічних та криптографічних компонентів систем захисту інформації дозволяє виділити наступне:

1. Дослідниками показано, що формування сучасних систем захисту інформації має відбуватися із залученням як криптографічної, так і стеганографічної складової. Незважаючи на те, що на сьогодні введено визначення КСС та встановлено, що ефективність такої системи залежатиме, насамперед, від узгодження роботи криптографічної та стеганографічної складової, проблеми такого узгодження, а також одночасного функціонування даних компонент КСС в сучасній літературі не розглядаються.

2. Проведено аналіз вимог до побудови сучасних стеганографічних систем, зокрема встановлено, що для забезпечення ефективності стеганографічних систем із використанням існуючих методів виникає необхідність застосування ресурсномістких перетворень (насамперед, сингулярного розкладання матриць-блоків контейнера, ДКП, ДПФ, перетворення Уолша-Адамара, вейвлет-перетворень і т.д.), що стає у протиріччя з необхідністю застосування таких стеганографічних методів для побудови КСС, що застосовуються на ресурсообмежених платформах. Наявність даного протиріччя гальмує розвиток та широке застосування КСС, які характеризуються значно більшою ефективністю у порівнянні із застосуванням лише криптографічного, або лише стеганографічного захисту інформації, та створює передумови для формування методології розробки ефективних крипто-стеганографічних систем захисту інформації.

3. Ефективність роботи КСС визначається степенем узгодженості її стеганографічної та криптографічної складової, а також, значною мірою, крипостійкістю конструкцій, що застосовані в ній. Огляд літературних джерел показує, що для оцінки і порівняння криптографічної якості криптографічних компонент КСС, сьогодні використовується лише математичний апарат компонентних булевих функцій, до яких застосовуються критерії криптографічної якості. Тим не менш, криптоаналітик не є обмеженим застосуванням лише математичного апарату булевих функцій під час здійснення атак криптоаналізу, що призводить до необхідності розгляду можливого уявлення конструкцій криптографічних алгоритмів всіма можливими способами, тобто за допомогою математичного апарату ФБЛ. Такий підхід обумовлює необхідність створення набору критеріїв криптографічної якості ФБЛ для простих значень q та значень q, що є степенем простого числа $q = p^k$. У сучасних відкритих літературних джерелах фактично відсутні методи синтезу криптографічних конструкцій, які б одночасно задовольняли як критеріям криптографічної якості їх

компонентних булевих функцій, так і компонентних ФБЛ, а також БСШ на їх основі, що здатні працювати із алфавітом $\{0,1,...,q-1\}$ для значень $q>2$, що є важливим для об'єднання роботи криптографічної та стеганографічної складових КСС.

Отже, побудова КСС вимагає забезпечення ефективної та узгодженої роботи як стеганографічної, так і криптографічної складової. При цьому, в реаліях сучасних інформаційних систем важливою умовою роботи КСС є їх висока обчислювальна ефективність, що пояснюється необхідністю їх функціонування в платформах, що є обмеженими у обчислювальних ресурсах. Повсюдне впровадження та застосування платформ, що є обмеженими у обчислювальних ресурсах з одного боку, та необхідна складність виконуваних перетворень для забезпечення високої ефективності (насамперед, захисту від атак проти вбудованого повідомлення) з іншого, призводить то суттєвого гальмування практичного використання КСС, навіть до повного усунення їх стеганографічної складової, тобто використання суто криптографічного захисту інформації, що призводить до зниження ефективності всієї системи захисту інформації.

Разом с тим встановлено, що підвищення ефективності КСС має на увазі і підвищення ефективності її криптографічної складової. Об'єктивний розвиток методів криптоаналізу та останні дослідженні в області досконалих алгебраїчних конструкцій показують, що подальше підвищення ефективності сучасних криптоалгоритмів потребує розгляду їх конструкцій не тільки із застосуванням математичного апарату булевих функцій, а також із застосуванням їх розкладання на компонентні ФБЛ.

Застосування ФБЛ є основою подальшого підвищення дифузії та конфузії, що забезпечує криптоалгоритм, а також базою для більшого узгодження із стеганографічною складовою КСС.

Таким чином, проведені дослідження відкритих літературних джерел вказують на існування об'єктивного протиріччя у побудові систем захисту

інформації, між наявною необхідністю використання ресурсообмежених платформ при реалізації КСС, що, між іншим, передбачає застосування «нескладних» в обчислювальному сенсі методів та застосуванням ресурсномістких перетворень контейнера, що сьогодні має місце, для забезпечення ефективності крипто-стеганографічних систем.

Вирішення цього протиріччя лежить у площині формування методології розробки КСС, яка базується на кодовому управлінні вбудовуванням інформації у часовій області із тісною інтеграцією криптографічного захисту інформації.

Список використаних джерел у першому розділі

1. Vakulyk O. et al. Cybersecurity as a component of the national security of the state. *Journal of Security & Sustainability Issues*. 2020. Vol. 9, No. 3. P. 775-784.

2. Хорошко В. О. та ін. Проєктування комплексних систем захисту інформації. Видавництво Львівської політехніки, 2020. 317 с.

3. Naser S. M. Cryptography: From The Ancient History to Now, It’s Applications and a New Complete Numerical Model. *International Journal of Mathematics and Statistics Studies*. 2021. Vol. 9, No. 3. P. 11-30.

4. Kiss G. et al. How to teach the history of cryptography and steganography. *Educaţia Plus*. 2018. Vol. 20, No. 2. P. 13-23.

5. Schneier B., Applied Cryptography: Protocols, Algorithms and Source Code in C. Wiley. 2015. 784 p.

6. Mohammed M. H. Analysis on Contribution of Cryptography and Steganography in Protecting Information in Diverse Environments. *Proceedings of Third International Conference on Communication, Computing and Electronics Systems*. Singapore: Springer, 2022. P. 153-158.

7. Sangeetha R., Koteeswari G., Phil M. Securing Data in IOT using Cryptography & Steganography Techniques. *Int. J. Res. Eng. Sci*. 2021. Vol. 9. P. 1-5.

8. Adee R., Mouratidis H. A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography. *Sensors*. 2022. Vol. 22. No. 3. P. 1109.

9. Abel K. D. et al. Data Security Using Cryptography and Steganography Technique on the Cloud. *Computational Intelligence in Machine Learning*. Singapore: Springer, 2022. P. 475-481.

10. ALRikabi H. T. H. S., Hazim H. T. Enhanced data security of communication system using combined encryption and steganography. *iJIM*. 2021. Vol. 15, No. 16. P. 145.

11. Rakhra M. et al. A Review on Data hiding using Steganography and Cryptography. *9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)*. IEEE, 2021. P. 1-4.

12. Antonio H., Prasad P. W. C., Alsadoon A. Implementation of cryptography in steganography for enhanced security. *Multimedia Tools and Applications*. 2019. Vol. 78. No. 23. P. 32721-32734.

13. Задирака В. К. Сучасні методи розв’язання задач інформаційної безпеки. *Вісн. НАН України*. 2014. № 5. С. 65-69.

14. Evsutin O., Melman A., Meshcheryakov R. Digital Steganography and Watermarking for Digital Images: A Review of Current Research Directions. *IEEE Access*. 2020. No. 8. P. 166589-166611. doi: 10.1109/ACCESS.2020.3022779

15. Нариманова Е. В. и др. Методика количественной оценки надежности восприятия цифрового изображения. *Інформатика та математичні методи в моделюванні*. 2014. №. 4. С. 332-336.

16. Setiadi D. R. I. M. PSNR vs SSIM: imperceptibility quality assessment for image steganography. *Multimedia Tools and Applications*. 2021. Vol. 80, No. 6. P. 8423-8444.

17. Sara U., Akter M., Uddin M. S. Image quality assessment through FSIM, SSIM, MSE and PSNR—a comparative study. *Journal of Computer and Communications*. 2019. Vol. 7, No. 3. P. 8-18.

18. Baig M. A., Moinuddin A. A., Khan E. PSNR of highest distortion region: an effective image quality assessment method. *International Conference on Electrical, Electronics and Computer Engineering*. IEEE, 2019. P. 1-4.

19. Гонсалес Р., Вудс Р. Цифровая обработка изображений. М.: Техносфера, 2012. 1104 с.

20. Singh N. High PSNR based image steganography. *Int J Adv Eng Res Sci*. 2019. Vol. 6, No. 1. P. 109-115.

21. Kumari N., Todwal V. High PSNR based Video Steganography by DWT-BCH Method. *International Journal of Innovative Science and Research Technology*. Vol. 4, Issue 5. P. 41-48.

22. Грибунин В., Оков И., Туринцев И. Цифровая стеганография. Солон-Пресс, 2002. 272 с.

23. Duan X. et al. High-capacity image steganography based on improved Xception. *Sensors*. 2020. Vol. 20, No. 24. P. 7253.

24. Paul G. et al. A PVD based high capacity steganography algorithm with embedding in non-sequential position. *Multimedia Tools and Applications*. 2020. Vol. 79, No. 19. P. 13449-13479.

25. Lu S. P. et al. Large-capacity image steganography based on invertible neural networks. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2021. P. 10816-10825.

26. Swain G. Very high capacity image steganography technique using quotient value differencing and LSB substitution. *Arabian Journal for Science and Engineering*. 2019. Vol. 44, No. 4. P. 2995-3004.

27. Chen B. et al. High-capacity robust image steganography via adversarial network. *KSII Transactions on Internet and Information Systems (TIIS)*. 2020. Vol. 14, No. 1. P. 366-381.

28. Wang Y., Tang M., Wang Z. High-capacity adaptive steganography based on LSB and Hamming code. *Optik*. 2020. Vol. 213. P. 164685.

29. Farrag S., Alexan W. A high capacity geometrical domain based 3d image steganography scheme. *International Conference on Advanced Communication Technologies and Networking (CommNet)*. IEEE, 2019. P. 1-7.

30. Tyagi S., Dwivedi R. K., Saxena A. K. High capacity steganography protected using Shamir's threshold scheme and permutation framework. *Int. J. Innov. Technol. Exploring Eng*. 2019. Vo. 8, No. 9. P. 784-795.

31. Jung K. H. A Study on Machine Learning for Steganalysis. *Proceedings of the 3rd International Conference on Machine Learning and Soft Computing*, 2019. P. 12-15.

32. Zhang Y. et al. A robust image steganography method resistant to scaling and detection. *Journal of Internet Technology*. 2018. Vol. 19, No. 2. P. 607-618.

33. Zhu Z., Zheng N., Qiao T., Xu M. Robust Steganography by Modifying Sign of DCT Coefficients. *IEEE Access*. 2019. Vol. 7. P. 168613-168628. doi: 10.1109/access.2019.2953504

34. Мельник М.А. Стеганоалгоритм, устойчивый к сжатию. *Інформаційна безпека*. 2012. Т. 2, №8. С. 99-106.

35. Chang C.C., Lin C.C., Hu Y.S. An SVD oriented watermark embedding scheme with high qualities for the restored images. *International journal of innovative computing, information & control*. 2007.Vol. 3, No. 3. P. 609-620.

36. Chanu Y. J., Singh Kh. M., Tuithung T. A Robust Steganographic Method based on Singular Value Decomposition. *International Journal of Information & Computation Technology*. 2014. Vol. 4, No. 7. P. 717-726.

37. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности. К.: Изд. ГУИКТ, 2010. 251 с.

38. Lu Leng, Jiashu Zhang, Jing Xu et al. Dynamic weighted discrimination power analysis: A novel approach for face and palmprint recognition in DCT domain. *International Journal of Physical Sciences*. 2010. No. 5(17) P.467-471.

39. Dai H., Cheng J., Li Y. A novel steganography algorithm based on quantization table modification and image scrambling in DCT domain. *International Journal of Pattern Recognition and Artificial Intelligence*. 2021. Vol. 35, No. 01. P. 2154001.

40. Chowdhuri P., Jana B., Giri D. Secured steganographic scheme for highly compressed color image using weighted matrix through DCT. *International Journal of Computers and Applications*. 2021. Vol. 43, No. 1. P. 38-49.

41. Patel R., Lad K., Patel M. Novel DCT and DST based video steganography algorithms over non-dynamic region in compressed domain: a comparative analysis. *International Journal of Information Technology*. 2022. Vol. 14, No. 3. P. 1649-1657.

42. Khatavkar M. M. D., MALI A. S. A Image Security with Image Steganography Using Dct Coefficient and Encryption. *International Journal of Innovations in Engineering Research and Technology*. Vol. 3, No. 9. P. 1-8.

43. Ayub N., Selwal A. An improved image steganography technique using edge based data hiding in DCT domain. *Journal of Interdisciplinary Mathematics*. 2020. Vol. 23, No. 2. P. 357-366.

44. Zhang X., Peng F., Long M. Robust coverless image steganography based on DCT and LDA topic classification. *IEEE Transactions on Multimedia*. 2018. Vol. 20, No. 12. P. 3223-3238.

45. Jia J. et al. An adaptive JPEG double compression steganographic scheme based on irregular DCT coefficients distribution. *IEEE Access*. 2019. Vol. 7. P. 119506-119518.

46. Bhattacharyya S., Mondal S., Sanyal G. A Robust Image Steganography using Hadamard Transform. *International Conference on Information Technology in Signal and Image Processing*, Mumbai, 2013. P. 416-426.

47. Sheidaeian H., Zolfaghari B., Zobeiri M. An Efficient and Secure Approach to Multi-User Image Steganography Using CRC-Based CDMA. *International Conference on Signal Acquisition and Processing*. Singapore, 2011. Vol. 2. P. 1-5.

48. Amirtharajan R., Rayappan J. B. B. Covered CDMA multi-user writing on spatially divided image. *International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE)*, 2011. P. 1-5. doi: wirelessvitae.2011.5940912

49. Sneha P. S., Sankar S., Kumar A. S. A chaotic colour image encryption scheme combining Walsh–Hadamard transform and Arnold–Tent maps. *Journal of Ambient Intelligence and Humanized Computing*. 2020. Vol. 11, No. 3. P. 1289-1308. doi: 10.1007/s12652-019-01385-0

50. Prabha K., Sam I. S. Robust color image watermarking by elliptical phase modification based on Walsh Hadamard Transform and Triangular Vertex Transform. *Sādhanā*. 2021. Vol. 46, No. 1. P. 1-16.

51. Prabha K., Sam I. S. A novel blind color image watermarking based on Walsh Hadamard Transform. *Multimedia Tools and Applications*. 2020. Vol. 79, No. 9. P. 6845-6869.

52. Helal S., Salem N. A Hybrid Watermarking Scheme Using Walsh Hadamard Transform and SVD. *Procedia Computer Science*. 2021. Vol. 194. P. 246-254.

53. Zhang Y. Q., Zhong K., Wang X. Y. High-Capacity Image Steganography based on Discrete Hadamard Transform. *IEEE Access*. 2022. Vol. 10. P. 65141-65155. doi: 10.1109/ACCESS.2022.3181179

54. Arunkumar S. et al. SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images. *Measurement*. 2019. Vol. 139. P. 426-437.

55. Wang Z. et al. Robust JPEG Image Steganography Based on SVD and QIM in Stationary Wavelet Domain. *International Conference on Artificial Intelligence and Security*. Springer, Cham, 2021. P. 551-560.

56. Zaidan F. K. Digital Image Steganography Scheme Based on DWT and SVD. *Diyala Journal of Engineering Sciences*. 2020. Vol. 13, No. 4. P. 10-17.

57. Yousif A. J. Image Steganography Based on Wavelet Transform and Color Space Approach. *Diyala Journal of Engineering Sciences*. 2020. Vol. 13, No. 3. P. 23-34.

58. Abdallah H. A. et al. An embedding approach using orthogonal matrices of the singular value decomposition for image steganography. *Multimedia Tools and Applications*. 2020. Vol. 79, No. 11. P. 7175-7191.

59. Zainol Z. et al. A new chaotic image watermarking scheme based on SVD and IWT. *IEEE Access*. 2020. Vol. 8. P. 43391-43406.

60. Ahmadi S. B. B., Zhang G., Wei S. Robust and hybrid SVD-based image watermarking schemes. *Multimedia Tools and Applications*. 2020. Vol. 79, No. 1. P. 1075-1117.

61. Abdulazeez A. M. et al. Robust watermarking scheme based LWT and SVD using artificial bee colony optimization. *Indonesian Journal of Electrical Engineering and Computer Science*. 2021. Vol. 21, No. 2. P. 1218-1229.

62. Arora S. M. et al. A DWT-SVD based robust digital watermarking for digital images. *Procedia computer science*. 2018. Vol. 132. P. 1441-1448.

63. He Y., Hu Y. A proposed digital image watermarking based on DWT-DCT-SVD. *2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*. IEEE, 2018. P. 1214-1218.

64. Roy S., Pal A. K. A hybrid domain color image watermarking based on DWT–SVD. *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*. 2019. Vol. 43, No. 2. P. 201-217.

65. Костырка О. В. Анализ преимуществ пространственной области цифрового изображения-контейнера для стеганопреобразования. *Інформатика та математичні методи в моделюванні*. 2013. № 3. С. 275-282.

66. Alyousuf F. Q. A., Din R., Qasim A. J. Analysis review on spatial and transform domain technique in digital steganography. *Bulletin of Electrical Engineering and Informatics*. 2020. Vol. 9, No. 2. P. 573-581.

67. Santoso H. A. et al. An improved message capacity and security using divide and modulus function in spatial domain steganography. *International conference on information and communications technology*. IEEE, 2018. P. 186-190.

68. Abdulwahedand M. N., Mustafa S. T., Rahim M. S. M. Image Spatial Domain Steganography: A study of Performance Evaluation Parameters. *IEEE 9th International Conference on System Engineering and Technology*. IEEE, 2019. P. 309-314.

69. Hu X., Ni J., Shi Y. Q. Efficient JPEG steganography using domain transformation of embedding entropy. *IEEE Signal Processing Letters*. 2018. Vol. 25, No. 6. P. 773-777.

70. Shah P. D., Bichkar R. S. A secure spatial domain image steganography using genetic algorithm and linear congruential generator. *International conference on intelligent computing and applications*. Springer, Singapore, 2018. P. 119-129.

71. Nisha C. D., Monoth T. Analysis of spatial domain image steganography based on pixel-value differencing method. *Soft computing for problem solving*. Springer, Singapore, 2020. P. 385-397.

72. Astuti Y. P. et al. Simple and secure image steganography using LSB and triple XOR operation on MSB. *International Conference on Information and Communications Technology*. IEEE, 2018. P. 191-195.

73. Paul G. et al. An efficient multi-bit steganography algorithm in spatial domain with two-layer security. *Multimedia Tools and Applications*. 2018. Vol. 77, No. 14. P. 18451-18481.

74. Jayapandiyan J. R., Kavitha C., Sakthivel K. Enhanced least significant bit replacement algorithm in spatial domain of steganography using character sequence optimization. *IEEE Access*. 2020. Vol. 8. P. 136537-136545.

75. Кобозева, А.А. Стеганопреобразование пространственной области изображения контейнера, устойчивое к атакам против встроенного сообщения. Проблемы региональной энергетики. / А.А. Кобозева, О.В.

Костырка, Е.Ю. Лебедева // Электронный журнал Академии наук республики Молдова. – 2014. – №1(24). – С. 1 – 12.

76. Рудницький В.М., Костирка О.В. Стійке стеганоперетворення в просторовій області зображення-контейнера. *Інформатика та математичні методи в моделюванні*. 2013. Т. 3, № 4, С. 353-360.

77. Костирка О.В. Модифікація стійкого до збурних дій стеганоперетворення просторової області зображення-контейнера. *Інформатика та математичні методи в моделюванні*. 2016. Т. 6, № 1, С. 85-93.

78. Shannon C. E. A Mathematical Theory of Cryptography. USA : Bell System Technical Memo, 1945, MM 45-110-02.

79. Авдошин С. М., Савельева А. А. Криптоанализ: современное состояние и перспективы развития. *Информационные технологии*. 2007. №. 3. С. 1-32.

80. Stamp M., Low R. M. Applied cryptanalysis: breaking ciphers in the real world. John Wiley & Sons, 2007. 401 p.

81. Исследование дифференциальных свойств блочно-симметричных шифров / Сорока Л. С. и др. *Системи обробки інформації*. 2010. №. 6. С. 286-294.

82. Courtois N., Pieprzyk J. Cryptanalysis of block ciphers with over-defined systems of equations. Proceedings of ASIACRYPT, Springer, Heidelberg, LNCS, 2002. Vol. 2501, P. 267-287.

83. Роенко Д. В. Обзор криптографических атак на алгоритмы блочного шифрования. *Физико-математические и технические науки как фундамент становления постиндустриального общества*, 2020. С. 49-53.

84. Пестунов А. И. Статистический анализ современных блочных шифров. *Вычислительные технологии*. 2007. Т. 12, №. 2. С. 122-129.

85. Исследование возможности применения генетических алгоритмов для реализации криптоанализа блочных криптосистем / Чернышев Ю. О. и др.

Вестник Донского государственного технического университета. 2015. Т. 15, №. 3 (82). С. 65-72.

86. Городилова А. А. От криптоанализа шифра к криптографическому свойству булевой функции. *Прикладная дискретная математика*. 2016. №. 3 (33). С. 16-44.

87. Фатхи В. А., Сергеев А. С. Исследование возможности применения алгоритма муравьиных колоний для реализации криптоанализа шифров перестановок. *Вестник Донского государственного технического университета*. 2011. Т. 11, №. 1. С. 10-20.

88. Gaines H. F. Cryptanalysis: A study of ciphers and their solution. Courier Corporation, 2014. 256 p.

89. Schindler W., Killmann W. Evaluation criteria for true (physical) random number generators used in cryptographic applications. International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2002. P. 431-449.

90. Innokentievich T. P., Vasilevich M. V. The Evaluation of the cryptographic strength of asymmetric encryption algorithms. Second Russia and Pacific Conference on Computer Technology and Applications (RPC), IEEE, 2017. P. 180-183.

91. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / A. Rukhin, J. Soto, J. Nechvatal et al. National Institute of Standards and Technology Special Publication, 2010. 131 p.

92. Иванов М. А., Чугунков И. В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. М.: КУДИЦ-ОБРАЗ, 2003. 240 с.

93. Евсеев С., Остапов С., Королев Р. Использование мини-версий для оценки стойкости блочно-симметричных шифров. *Науковий журнал «Безпека інформації»*. 2017. Т. 23, № 2. С.100-108.

94. Исследование криптографических показателей уменьшенных моделей шифров DES и ГОСТ / В. И. Долгов и др. *Прикладная радиоэлектроника: науч.-техн. журн.*, 2011. Т. 10, № 1. С. 127-134.

95. Лисицкая И. В. О новой методике оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа. *Системи обробки інформації*. 2011. №. 4. С. 167-173.

96. Криптографические свойства уменьшенной версии шифра "Калина" / Долгов В. И. и др. *Прикладная радиоэлектроника*. 2010. Т. 9, № 3. С. 349-354.

97. Руженцев В. И., Чичмарь С. В., Савин Д. И. Комбинаторные свойства уменьшенной версии шифра «Калина». *Прикладная радиоэлектроника*. 2010. Т. 9, № 3. С. 346-348.

98. Долгов В. И., Лисицкая И. В., Хряпин Д. Э. Атака на полный дифференциал уменьшенной версии БСШ Rijndael. *Прикладная радиоэлектроника*. 2010. Т. 9, № 3. С. 355-360.

99. Исследование криптографических свойств нелинейных узлов замены уменьшенных версий некоторых шифров / Долгов В. И. и др. *Прикладная радиоэлектроника*, 2009. Т. 8, № 3. С. 268-277.

100. Лисицкая И. В., Лисицкий К. Е. О приходе итеративных шифров к стационарному состоянию, свойственному случайной подстановке. *Прикладная радиоэлектроника*. 2013. Т. 12, № 2. С. 230-235.

101. Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа / Горбенко И. Д. и др. *Прикладная радиоэлектроника*. 2010. Том 9, № 3. С. 312-320.

102. Jorstad N. D., Landgrave T. S. Cryptographic algorithm metrics. 20th National Information Systems Security Conference, 1997. – С. 1-38.

103. Якимчук О., Яковлєв С. Параметр, який характеризує стійкість S-блоків до аналізу усічених диференціалів. *INTERNET-EDUCATION-SCIENCE* : зб. мат. XII міжнародної науково-практичної конференції, 26-29 травня 2020, Україна, Вінниця: ВНТУ, 2020 С. 129-131.

104. Науменко О. В. Порівняльний аналіз криптографічних властивостей блоків підстановки деяких сучасних стандартів блокового шифрування. *Теоретичні і прикладні проблеми фізики, математики та інформатики* : Зб. матеріалів XV Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених, 25-27 травня 2017 року, м. Київ: ВПІ ВПК «ПОЛІТЕХНІКА», 2017. С. 103-105.

105. Юкальчук, А.А. Критерии и показатели эффективности нелинейных преобразований симметричных криптоалгоритмов. *Системи обробки інформації*. 2006. Вип. 3(52). С. 186-190.

106. Холоша А.А. Об одном подходе к анализу качества блока подстановки битовых векторов. *Збірник наукових праць ІПМЕ НАН України*. 1998. Вип. 2. С.59-74.

107. Кирюхин В. А. Атака методом бумеранга на связанных ключах на 5 раундах шифра Кузнечик. *Обозрение прикладной и промышленной математики*. 2019. Т. 26, №. 3. С. 268-270.

108. Зайко, Ю.Н. Криптография глазами физика. Изв. Саратовского ун-та. 2009. Т. 9, № 2. С. 34-48.

109. Маро Е. А. Исследование надежности блочных криптографических алгоритмов с помощью методологии SAT. *Известия Южного федерального университета. Технические науки*. 2019. №. 5 (207). С. 33-45.

110. Tanaka H., Kaneko T., Sugio N. Cipher strength evaluation apparatus : пат. США 7460665. опубл. 2008.

111. Ding C., Xiao G., Shan W. The stability theory of stream ciphers. LNCS. vol. 561. Springer, Heidelberg, 1991. 194 p.

112. Кузнецов А. А., Лисицкая И. В., Исаев С. А. Линейные свойства блочных симметричных шифров, представленных на украинский конкурс. *Прикладная радиоэлектроника*. 2011. Том 10, № 2. С. 135-140.

113. Настенко А. А. Показатели статистической безопасности украинских блочных симметричных шифров. *Технологический аудит и резервы производства*. 2012. Т. 5, №. 2. С. 19-20.

114. Ковальчук Л. В., Кучинська Н. В. Оцінки практичної стійкості модифікацій нових стандартів блокового шифрування відносно цілочисельного різницевого криптоаналізу. *Математичне та комп'ютерне моделювання. Серія: Фізико-математичні науки*. 2017. №. 15. С. 69-74.

115. Easttom C. An Examination of Inefficiencies in Key Dependent Variations of the Rijndael S-Box. *Electrical Engineering (ICEE)*, Iranian Conference on. IEEE, 2018. P. 1658-1663.

116. Improved cryptanalysis of Rijndael / Ferguson N. et al. *International Workshop on Fast Software Encryption*. Springer, Berlin, Heidelberg, 2000. P. 213-230.

117. On the security of Rijndael-like structures against differential and linear cryptanalysis / Park S. et al. *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, Berlin, Heidelberg, 2002. P. 176-191.

118. Cryptanalysis of Rijndael S-box and improvement / Jing-mei L. et al. *Applied Mathematics and Computation*. 2005. Vol. 170, No. 2. P. 958-975.

119. Жданов О. Н. Методика выбора ключевой информации для алгоритма блочного шифрования. М.: ИНФРА-М, 2013 г. 90 с.

120. Соколов А. В. Новые методы синтеза нелинейных преобразований современных шифров. Lap Lambert Academic Publishing. Germany, 2015. 100 с.

121. Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 472 с.

122. Sharma D. K., Pandey R. New Constructions of balanced Boolean functions with maximum algebraic immunity, high nonlinearity and optimal algebraic degree. *Walailak Journal of Science and Technology*. 2020. Vol. 17. No. 7. P. 639-654.

123. Carlet C., Feng K. An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity. *International Conference on the Theory and Application of Cryptology and Information Security* : Springer, Berlin, Heidelberg, 2008. P. 425-440.

124. Tang D., Carlet C., Tang X. Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks. *IEEE transactions on information theory*. 2012. Vol. 59, No. 1. P. 653-664.

125. Sattarov A. B., Abdurahimov B. F. An algorithm for constructing S-boxes for block symmetric encryption. *Universal Journal of Mathematics and Applications*. 2018. Vol. 1, No. 1. P. 29-32.

126. Stankovic R. S., Astola J.T., Moraga C. Representation of Multiple-Valued Logic Functions. Morgan and Claypool Publishers, Synthesis lectures on digital circuits and systems, 2012. 154 p.

127. Maier W., Staffelbach O. Nonlinearity criteria for cryptographic functions. In Advances in Cryptology, EUROCRYPT'89, Lecture Notes in Computer Science, Springer-Verlag, 1990. Vol.434. P .549-562.

128. Cooke B. Reed Muller error correcting codes. *MIT undergraduate journal of mathematics.* 1999. Vol. 1, No. 06. P. 21-26.

129. Yan H., Tang D. Improving lower bounds on the second-order nonlinearity of three classes of Boolean functions. *Discrete Mathematics*. 2020. Vol. 343, No. 5. P. 111698.

130. Tang D., Zhang W., Tang X. Construction of balanced Boolean functions with high nonlinearity and good autocorrelation properties. *Designs, codes and cryptography*. 2013. Vol. 67, No. 1. P. 77-91.

131. Sarkar P., Maitra S. Construction of nonlinear Boolean functions with important cryptographic properties. *International Conference on the Theory and Applications of Cryptographic Techniques* : Springer, Berlin, Heidelberg, 2000. P. 485-506.

132. Filiol E., Fontaine C. Highly nonlinear balanced Boolean functions with a good correlation-immunity. *International Conference on the Theory and Applications of Cryptographic Techniques* : Springer, Berlin, Heidelberg, 1998. P. 475-488.

133. Sarkar P., Maitra S. Nonlinearity bounds and constructions of resilient Boolean functions. *Annual International Cryptology Conference* : Springer, Berlin, Heidelberg, 2000. P. 515-532.

134. Carlet C., Crama Y., Hammer P. L. Boolean Functions for Cryptography and Error-Correcting Codes. Cambridge University Press, 2010. 148 p.

135. Мазурков М.И., Соколов А.В. Нелинейныепреобразования на основеполныхклассовизоморфных и автоморфных представлений поля GF(256). *Известиявысшихучебных заведений. Радиоэлектроника*. 2013. Т. 56, № 11. С. 16-24.

136. Мазурков М.И., Соколов А.В. Нелинейные S-блоки подстановки на основекомпозиционныхкодовстепенныхвычетов. *Известиявысшихучебных заведений. Радиоэлектроника*. 2013. Т. 56, № 9. С. 34-43.

137. Rodinko M., Oliynykov R., Gorbenko Y. Improvement of the high nonlinear S-boxes generation method. Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T) : IEEE, 2016. P. 63-66.

138. Generation of highly nonlinear and dynamic AES substitution-boxes (S-boxes) using chaos-based rotational matrices / Malik M. S. M. et al. *IEEE Access*. 2020. Vol. 8. P. 35682-35695.

139. Nyberg K. Perfect nonlinear S-boxes. Workshop on the Theory and Application of of Cryptographic Techniques : Springer, Berlin, Heidelberg, 1991. P. 378-386.

140. Shah T., Shah D. Construction of highly nonlinear S-boxes for degree 8 primitive irreducible polynomials over $\mathbb{Z}2$. *Multimedia Tools and Applications*. 2019. Vol. 78. No. 2. P. 1219-1234.

141. Rothaus O. S. On “bent” functions. *J. Comb. Theory Ser*. A.1976. No. 20(3). P.300-305.

142. Токарева Н. Н. Бент-функции: результаты и приложения. Обзор работ. *Приклад. дискрет. математика*. 2009. № 1(3). С. 15-37.

143. A new lower bound on the second-order nonlinearity of a class of monomial bent functions / Tang D. et al. *Cryptography and Communications*. 2020. Vol. 12. No. 1. P. 77-83.

144. Мазурков М. И., Соколов А. В. Регулярные привила построенияполногокласса бент-последовательностейдлины 16. *Труды ОНПУ*. 2013. №2(41). С. 231-237.

145. Mesnager S. Bent functions. Springer International Publishing, 2016. 544 p.

146. Carlet C., Mesnager S. Four decades of research on bent functions. *Designs, Codes and Cryptography*. 2016. Vol. 78, No. 1. P. 5-50.

147. Агафонова И. В. Криптографические свойства нелинейных булевых функций. *Семинар по дискрет. гармон. анализу и геометр. моделированию* : СПб.: DHA&CAGD, 2007. С. 1—24.

148. Мазурков М. И., Соколов А. В., Барабанов Н. А. Генератор ключевыхпоследовательностей на основедуальных пар бент-функций. Праці Одеського політехнічного університету, 2013. №3. С. 150-156.

149. Соколов А. В. Быстродействующий генератор ключевыхпоследовательностей на основеклеточныхавтоматов. *Труды ОНПУ*, 2014. №1(43). С. 180 -186.

150. Соколов А. В. Конструктивный метод синтезанелинейных S-блоковподстановки, соответствующих строгому лавинному критерию. *Известия высшихучебных заведений. Радиоэлектроника*. 2013. Т. 56, № 8. С. 43-52.

151. Соколов А. В. Метод синтеза полного класса бент-функций шести переменных. *Проблемыфизики, математики и техники*. 2016. №4(29). С. 94-102.

152. Potapov V. N. On q-ary bent and plateaued functions. *Designs, Codes and Cryptography*. 2020. Vol. 88, No. 10. P. 2037-2049.

153. Stanković M. et al. Construction of Ternary Bent Functions From Ternary Linear Functions. *IEEE 52nd International Symposium on Multiple-Valued Logic (ISMVL)*. IEEE, 2022. P. 50-55.

154. Stanković R. S. et al. Construction of ternary bent functions by FFT-like permutation algorithms. *IEICE Transactions on Information and Systems*. 2021. Vol. 104, No. 8. P. 1092-1102.

155. Propagation characteristics of Boolean functions / Preneel B. et al. *Workshop on the Theory and Application of Cryptographic Techniques* : Berlin, Heidelberg : Springer, 1990. P. 161-173.

156. Forrié R. The strict avalanche criterion: spectral properties of Boolean functions and an extended definition. *Conference on the Theory and Application of Cryptography* : New York, NY : Springer, 1988. P. 450-468.

157. Cusick T. W. Boolean functions satisfying a higher order strict avalanche criterion. *Workshop on the Theory and Application of Cryptographic Techniques* : Berlin, Heidelberg : Springer, 1993. P. 102-117.

158. Cusick T. W., Stanica P. Cryptographic Boolean functions and applications. Academic Press, 2017. 283 p.

159. Chandrasekharappa T.G.S, Prema K.V., Shama Kumara. S-boxes generated using Affine Transformation giving Maximum Avalanche Effect. *Internation Journal of Computer Science and Engineering*. Vol.3, No.9. 2011. P. 3185-3193.

160. Мазурков М.И., Соколов А.В. Нелинейные S-блоки конструкции Ниберг с максимальным лавинным эффектом. *Известия высших учебных заведений. Радиоэлектроника*. 2014. Т. 57, № 6. С. 47-55.

161. Design of Boolean Function from a Great Number of Variables Satisfying Strict Avalanche Criterion / Bardis E. G. et al. Resent advances in signal processing and communications-IMACS/IEEE. 1999. P. 107-112.

162. Seberry J., Zhang X. M. Highly nonlinear 0–1 balanced Boolean functions satisfying strict avalanche criterion. *International Workshop on the Theory and*

Application of Cryptographic Techniques :Berlin, Heidelberg : Springer, 1992. P. 143-155.

163. Kim K. Construction of DES-like S-boxes Based on Boolean Functions Satisfying the SAC. International Conference on the Theory and Application of Cryptology : Berlin, Heidelberg : Springer, 1991. P. 59-72.

164. Kurosawa K., Satoh T. Generalization of higher order SAC to vector output Boolean functions. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*. 1998. Vol. 81, No. 1. P. 41-47.

165. Fon-Der-Flaass D. G. A bound on correlation immunity. *SibirskieEhlektronnyeMatematicheskieIzvestiya* [electronic only]. 2007. Vol. 4. P. 133-135.

166. Tarannikov Y., Korolev P., Botev A. Autocorrelation coefficients and correlation immunity of Boolean functions. *International Conference on the Theory and Application of Cryptology and Information Security* : Berlin, Heidelberg : Springer, 2001. P. 460-479.

167. Liu M., Lu P., Mullen G. L. Correlation-immune functions over finite fields. *IEEE Transactions on Information Theory*. 1998. Vol. 44, №. 3. P. 1273-1276.

168. Alekseev E. K., Karelina E. K. Classification of correlation-immune and minimal correlation-immune Boolean functions of 4 and 5 variables. *Discrete Mathematics and Applications*. 2015. Vol. 25, No. 4. P. 193-202.

169. Karelina E. K. On a method of synthesis of correlation-immune Boolean functions. *Discrete Mathematics and Applications*. 2020. Vol. 30, No. 2. P. 79-91.

170. Gopalakrishnan K., Stinson D. R. Three characterizations of non-binary correlation-immune and resilient functions, Designs, Codes and Cryptography, 5, P. 241-251.

171. Baigneres T., Stern J., Vaudenay S. Linear cryptanalysis of non binary ciphers. Proceedings of the *International Workshop on Selected Areas in Cryptography*, Berlin, Heidelberg : Springer, 2007. P. 184-211.

172. Bernstein D. J., Lange T. Post-quantum cryptography. *Nature*. 2017. Vol. 549, No. 7671. P. 188-194.

173. Roetteler M., Svore K. M. Quantum computing: Codebreaking and beyond. *IEEE Security & Privacy*. 2018. Vol. 16, No. 5. P. 22-36.

174. Report on post-quantum cryptography / Chen L. et al. US Department of Commerce, National Institute of Standards and Technology, 2016. Vol. 12. P. 1-10.

175. Chen Y. A., Gao X. S. Quantum algorithms for Boolean equation solving and quantum algebraic attack on cryptosystems. *Journal of Systems Science and Complexity*. 2021. P. 1-34.

176. Evolution of an emerging symmetric quantum cryptographic algorithm / Jasim O. K. et al. *arXiv preprint*. 1503.04796. 2015. P. 1-11.

177. The impact of quantum computing on present cryptography / Mavroeidis V. et al. *International Journal of Advanced Computer Science and Applications*. Vol. 9, No. 3, 2018. P. 1-10.

178. Quantum attacks without superposition queries: the offline Simon's algorithm / Bonnetain X. et al. Proceedings of the *International Conference on the Theory and Application of Cryptology and Information Security*, Cham : Springer, 2019. P. 552-583.

179. Ito G., Iwata T. Quantum Distinguishing Attacks against Type-1 Generalized Feistel Ciphers. *IACR Cryptol. ePrint Arch*. 2019. Vol. 2019. P. 327.

180. Bonnetain X., Naya-Plasencia M., Schrottenloher A. Quantum security analysis of AES. IACR Transactions on Symmetric Cryptology, Ruhr Universität Bochum. 2019. P. 55-92.

181. Implementing Grover oracles for quantum key search on AES and LowMC / Jaques S. et al. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*Cham : Springer, 2020. P. 280-310.

182. Davenport J. H., Pring B. Improvements to quantum search techniques for block-ciphers, with applications to AES. *Selected Areas in Cryptography-SAC*. 2020. P. 1-24.

183. Grassl M. et al. Applying Grover's algorithm to AES: quantum resource estimates. *arXiv preprint*.1512.04965. 2015. P. 1-13.

184. Neve M., Seifert J. P. Advances on access-driven cache attacks on AES. *International Workshop on Selected Areas in Cryptography*, Berlin, Heidelberg : Springer, 2006. P. 147-162.

185. Quantum Collision Attacks on AES-Like Hashing with Low Quantum Random Access Memories / Xiaoyang Dong et al. *Advances in Cryptology – ASIACRYPT 2020 Lecture Notes in Computer Science*. 2020. P. 727-757

186. Observations on the Quantum Circuit of the SBox of AES / Zou J. et al. *IACR Cryptol. ePrint Arch*. 2019. Vol. 2019. P. 1245.

187. A many-valued approach to quantum computational logics / Dalla Chiara M. L. et al. *Fuzzy Sets and Systems*. 2018. Vol. 335. P. 94-111.

188. A many-valued approach to quantum computational logics / Dalla Chiara M. L. et al. *Fuzzy Sets and Systems*. 2018. Vol. 335. P. 94-111.

189. Bechmann-Pasquinucci H., Peres A. *Quantum cryptography with 3-state systems*. *Physical Review Letters*. 2000. Vol. 85, No. 15. P. 3313.

190. Łukasiewicz J. Aristotelian syllogistics from the point of view of modern formal logic. Moscow : Foreign literature, 1959. 313 p.

191. Large families of quaternary sequences with low correlation / Kumar P. V. et al. *IEEE Transactions on Information Theory*. 1996. Vol. 42, No. 2. P. 579-592.

192. New quaternary sequences of even length with optimal auto-correlation / Su W. et al. *Science China Information Sciences*. 2018. Vol. 61, No. 2. P. 022308.

193. New construction of quaternary sequences with ideal autocorrelation from Legendre sequences / Kim Y. S. et al. Proceedings of the *IEEE International Symposium on Information Theory*, IEEE, 2009. P. 282-285.

194. New quaternary sequences with ideal autocorrelation constructed from binary sequences with ideal autocorrelation / Jang J. W. et al. Proceedings of the *IEEE International Symposium on Information Theory*, IEEE, 2009. P. 278-281.

195. Hosseini S. A., Etezadi S. A novel very low-complexity multi-valued logic comparator in nanoelectronics. *Circuits, Systems, and Signal Processing*. 2020. Vol. 39, No. 1. P. 223-244.

196. Choi B., Shukla K. Multi-valued logic circuit design and implementation. *International Journal of Electronics and Electrical Engineering*. 2015. Vol. 3, No. 4. P. 256-262.

197. Multi-Valued Logic Circuits Based on Organic Anti-ambipolar Transistors / Kobashi K. et al. *Nano letters*. 2018. Vol. 18, No. 7. P. 4355-4359.

198. Multi-valued and fuzzy logic realization using TaOxmemristive devices / Bhattacharjee D. et al. *Scientific reports*. 2018. Vol. 8, No. 1. P. 1-10.

199. Sarica F., Morgül A. Basic circuits for multi-valued sequential logic. *Analog Integrated Circuits and Signal Processing*. 2013. Vol. 74, No. 1. P. 91-96.

200. Zhenxian Fang, Ying Liu. Ternary Error Correcting Codes. *Chinese Science Abstracts Series A*. 1995. P.54.

201. Schmidt K. U. Quaternary constant-amplitude codes for multicode CDMA. *IEEE Transactions on Information Theory*. 2009. Vol. 55, No. 4. P. 1824-1832.

202. Zhuo Z., Zhong N. A new kind of steganography schemes for image. *International Journal of Electronic Security and Digital Forensics*. 2017. Vol. 9, No. 1. P. 35-44.

203. Jouhari H. New steganographic schemes using binary and quaternary codes. UNIVERSITÉ MOHAMMED V-AGDAL, Faculté des Sciences, 2013. 130 p.

204. Rifà-Pous H., Rifà J., Ronquillo L. Z2Z4 additive perfect codes in Steganography. *Advances in Mathematics of Communications*. – 2011. – Т. 5. – №. 3. – С. 425.

Розділ 2.

РОЗРОБКА ТЕОРЕТИЧНИХ ОСНОВ ЗБЕЗПЕЧЕННЯ ЗАДАНИХ ВЛАСТИВОСТЕЙ СТЕГАНОПОВІДОМЛЕННЯ У ПРОСТОРОВІЙ ОБЛАСТІ

Формування ефективної КСС передбачає застосування інструментарію стеганографічної складової, яка, на відміну від криптографічної, дозволяє не тільки захистити інформацію від можливого читання зловмисниками, а й приховати від неавторизованих користувачів сам факт її передачі.

До сучасних стеганографічних методів сьогодні висувається ряд вимог, серед яких одними з найважливіших є: криптостійкість, швидкодія, стійкість до атак проти вбудованого повідомлення, забезпечення надійності сприйняття, забезпечення значної пропускної спроможності прихованого криптозахищеного каналу зв’язку.

Для побудови ефективної стеганографічної системи важливою є наявність можливості апріорного забезпечення вимог щодо забезпечення надійності сприйняття та стійкості до атак проти вбудованого повідомлення за допомогою використання відповідних достатніх умов. Достатні умови забезпечення надійності сприйняття й нечутливості стеганоповідомлення сформовані в частотній області ЦЗ [1], а також в областях сингулярного (спектрального) розкладання його матриці (матриць) [2]. При використанні інших областей ЦЗ для проведення стеганоперетворення і, як наслідок, для забезпечення певних вимог до стеганоповідомлення, незручним є використання наявних достатніх умов, оскільки їх використання вимагає значної кількості додаткових операцій для переведення зображення в частотну область чи область сингулярного (спектрального) розкладання відповідної матриці (матриць). Підвищення обчислювальної складності приводить до ускладнень (аж до неможливості) використання стеганоалгоритмів в режимі реального часу для потокового контейнеру.

Як показали дослідження, основою для формування кодових слів, що здатні забезпечити задані властивості стеганографічного методу у просторовій області є перетворення Уолша-Адамара. Враховуючи характеристики перетворення Уолша-Адамара, наявність достатніх умов забезпечення певних вимог для стеганоалгоритму (стеганоповідомлення) в цій області становить основу теоретичного базису для створення технології кодового управління вбудовуванням інформації.

Метою розділу є розробка теоретичного базису для побудови ефективних стеганографічних методів з використанням перетворення Уолша-Адамара.

Для досягнення мети необхідно розв’язати наступні задачі:

1. Встановлення взаємозв'язку між областю перетворень Уолша-Адамара та частотною областю цифрового зображення (областю дискретного косинусного перетворення), а також складовими сингулярного розкладання відповідної матриці.

2. Встановлення взаємозв’язку між двовимірним та одновимірним перетворенням Уолша-Адамара.

4. Отримання достатніх умов забезпечення заданих властивостей стеганоповідомлення в області перетворення Уолша-Адамара.

5. Розробка теоретичного базису кодового управляння вбудовуванням інформації з метою забезпечення стійкості стеганоповідомлення до атак стисненням.

2.1. Перспективи застосування перетворення Уолша-Адамара у сучасних стеганографічних системах для оцінки надійності сприйняття стеганоповідомлення

В даний час теорія і практика стеганографії стрімко розвивається [3], в рамках чого розробляється, вдосконалюється багато стеганографічних

методів захисту інформації, заснованих на найрізноманітніших математичних конструкціях, починаючи від класичного методу LSB, що забезпечує ефективне вбудовування додаткової інформації в контейнер, як правило, в просторовій / часовій області [4], закінчуючи методами, які використовують простір перетворень контейнера [5…9] (дискретного косинусного перетворення (ДКП), дискретного вейвлет-перетворення, перетворення Фур'є, області різних розкладань матриці (сингулярного, спектрального та ін.), а також перетворення Уолша-Адамара [10…11]) для вбудовування додаткової інформації.

Розвиток стеганографії тягне за собою розвиток методів стеганоаналіза, основним завданням якого є виявлення наявності додаткової інформації в інформаційному контенті [12], що дуже ускладнює в сучасних умовах задачу задоволення вимозі надійного приховання самого факту організації прихованого каналу зв'язку, а також збільшує кількість і частоту застосування різноманітних атак проти вбудованого повідомлення, що затосовуються активним порушником навіть тоді, коли він не в змозі не тільки декодувати, а й встановити факт наявності ДІ. В силу цього для сучасних стеганографічних методів зростає актуальність вимоги надійності сприйняття стеганоповідомлення (забезпечення відсутності візуальних відмінностей між контейнером і стеганоповідомленням, при цьому сьогодні тут мова йде не тільки про появу явних артефактів у стеганоповідомленні, а й про виникнення будь-яких відмінностей, які без наявності контейнера можуть і не сприйматися як зміни оригіналу: зміна яскравості, відтінків кольору, незначного згладжування контурів і т.д., однак стають визначними при безпосередньому порівнянні з контейнером), а також забезпечення його нечутливості до збурних дій при організації прихованого каналу зв'язку [13].

Гарантоване забезпечення надійності сприйняття стеганоповідомлення робить таким «живучим» і широко використовуваним метод модифікації найменшого значущого біта.

Кількісна оцінка надійності сприйняття стеганоповідомлення сьогодні відбувається з використанням стандартних різницевих показників спотворення [14]: MSE, SNR, PSNR, хоча вони часто виявляються необ'єктивними, оскільки не можуть повною мірою врахувати особливості людського зору. Особливо яскраво така можлива необ'єктивність проявляється у випадках, коли зміни цифрового контенту відбуваються в його локальних (малих за розміром) областях. Тут формальна кількісна оцінка спотворення може бути задовільною при явній наявності артефактів (рис. 1 (б)), в той час як значення різницевих показників в разі відсутності явних візуальних спотворень можуть бути низькими (рис. 1 (в)).

В якості контейнера у розділі далі розглядається ЦЗ або кадр ЦВ, які в умовах даної задачі нічим принципово не відрізняються в тому сенсі, що формальним поданням кожного є одна (зображення в градаціях сірого) або кілька (кольорове зображення) двовимірних матриць, а будь-які зміни оригінального контенту, в тому числі і стеганоперетворення, може розглядатися як збурення відповідної матриці (матриць).

а б в

Рис. 2.1. — Ілюстрація недосконалості різницевих показників для оцінки візуальних спотворень ЦЗ: а — вихідне ЦЗ, б — спотворене ЦЗ (PSNR = 52 dB), в — спотворене за допомогою гаусівського шуму ЦЗ (PSNR = 28 dB)

В існуючих стеганографічних методах часто зустрічаються обмеження на область їх застосування саме через те, що для якихось ЦЗ-контейнерів надійність сприйняття стеганоповідомлення, що формується, може

порушуватися, або може не забезпечуватися стійкість до якихось конкретних атак проти вбудованого повідомлення (зокрема до атаки стиском, що не дає змогу використовувати відповідний алгоритм в умовах збереження стеганоповідомлення з втратами). Це найчастіше відбувається в силу того, що при розробці стеганоалгоритму не враховуються формальні достатні умови такого забезпечення (або такі формальні умови в використовуваної області контейнера не знайдені), а оцінка властивостей алгоритму (надійності сприйняття, стійкості до збурних дій) робиться вже a posteriori, по факту. Така ситуація не дає в повній мірі можливості використання випадкового контейнера, є недоліком відповідних методів. Необхідно зауважити, що формальний математичний апарат для забезпечення надійності сприйняття стеганоповідомлення, стійкості до атак проти вбудованого повідомлення отримав свій розвиток стосовно стеганографії не так давно [2]. До цього, зокрема для забезпечення відсутності наявних відмінностей стеганоповідомлення і контейнера все обмежувалося урахуванням особливостей людського зору: зміни сильніше сприймаються в областях ЦЗ з малими перепадами значень яскравості, або фонових, що відповідають низькочастотній складовій. В [2] з використанням математичного апарату теорії збурень і матричного аналізу були отримані достатні умови забезпечення надійності сприйняття, нечутливості до збурних дій стеганоповідомлення, що формується, врахування яких дозволяло апріорно забезпечити / перевірити виконання цих властивостей в області сингулярного (або спектрального) розкладання відповідної матриці. З урахуванням можливого забезпечення єдиності таких розкладів отримані достатні умови можуть бути застосовані незалежно від обраної безпосередньої області стеганоперетворення (просторової, частотної, різних розкладань), однак на практиці все ж доцільним є отримання таких достатніх умов в кожній з областей ЦЗ, де можливе проведення стеганоперетворення, що дасть можливість уникати переходу в область сингулярного (спектрального)

розкладання матриці для аналізу степеню забезпечення надійності сприйняття чи чутливості стеганоповідомлення, якщо стеганоперетворення відбувається в іншій області контейнера.

Зважаючи на високу обчислювальну ефективність, а також відповідність архітектурним особливостям сучасних процесорів, перспективними для сучасних засобів захисту інформації є стеганографічні методи, засновані на використанні простору перетворень Уолша-Адамара.

На сьогодні в літературі відсутнє строге обґрунтування впливу модифікації того чи іншого коефіцієнта результату двовимірного перетворення Уолша-Адамара на спотворення, що виникають у зображенні-контейнері, на чутливість отриманого зображення-стеганоповідомлення до збурних дій. Ця обставина істотно ускладнює розвиток перспективних стеганографічних методів, заснованих на використанні властивостей перетворення Уолша-Адамара.

2.2. Зв'язок перетворення Уолша-Адамара та дискретного косинусного перетворення

Базовим перетворенням, що використовується в багатьох сучасних алгоритмах стиснення графічної інформації, а також стеганографічних алгоритмах, є ДКП, яке можемо записати в матричній формі

$$S=C_N X C_N^T, \tag{2.1}$$

де X — фрагмент вихідного зображення розміру $N\times N$,

C — $N\times N$-матриця дискретного косинусного перетворення, елементи якої $C(i,j)$, $i, j=0,1,...,N-1$ обчислюються відповідно до формули

$$C(i,j)=\begin{cases}\dfrac{1}{\sqrt{N}}, & \text{при } i=0;\\ \sqrt{\dfrac{2}{N}}\cos(2j+1)\cdot i\cdot\pi, & \text{при } i>0.\end{cases} \tag{2.2}$$

У результуючій матриці S (2.1) ДКП має місце наступний розподіл частотних складових, схематично показаний на рис. 2.2[1].

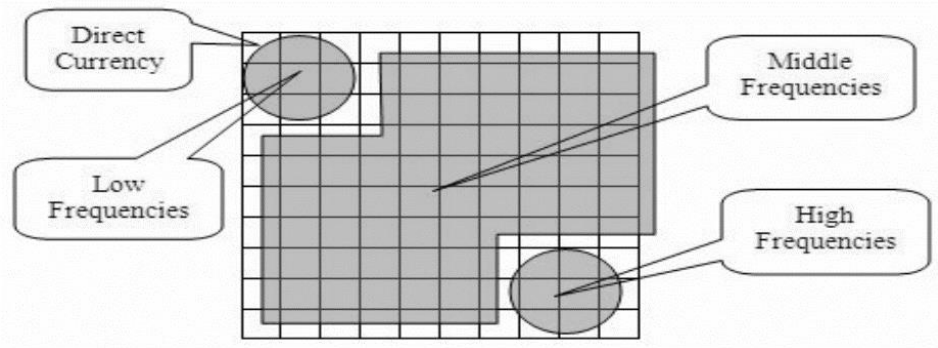


Рис. 2.2 — Розподіл частотних складових у трансформантах ДКП

Загальновідомо [12], що модифікація високочастотних складових (розташованих у правому нижньому куті матриці трансформант ДКП) веде до найменших візуальних спотворень вихідного зображення, тоді як модифікація середніх частот відповідає більш значним спотворенням. Найбільші спотворення вихідного зображення відбуваються за модифікації низькочастотних складових (лівий верхній кут) матриці трансформант ДКП.

Часто використовуваним у криптографії [15] та теорії сигналів [16] є ще один вид перетворення — дискретне перетворення Уолша-Адамара, яке в матричній формі можна записати у вигляді наступного матричного добутку

$$V=YH_N, \tag{2.3}$$

де H_N — матриця Уолша-Адамара порядку $N=2^k$, яка може бути побудована відповідно до конструкції Сільвестра

$$H_{2^k}=\begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix}, \tag{2.4}$$

де $H_1=1$, а Y — вектор-рядок довжини N.

Вираз (2.3) являє собою одновимірне перетворення Уолша-Адамара, у той час як у додатках обробки графічної інформації, зокрема, для завдань

стеганографії, поширення набуло двовимірне дискретне перетворення Уолша-Адамара, яке визначається як

$$W = H'_N X H'^T_N, \tag{2.5}$$

де $H'_N = \frac{1}{N} H_N$, а X — матриця розміру $N \times N$.

Знайдемо зв'язок між елементами матриці-результату перетворення Уолша-Адамара та частотними складовими матриці *X*. Зокрема, найбільший інтерес в сенсі забезпечення надійності сприйняття стеганоповідомлення представляє локалізація образів високочастотних складових матриці X ЦЗ. Кожна з функцій Уолша, не бувши гармонійною, характеризується частістю [17], яка є аналогом частоти для гармонійних функцій, і в разі останніх ці дві характеристики збігаються. Відповідно до [17], якщо число змін знаку в інтервалі часу функції f дорівнює η, то частість $\bar{\eta}$ функції f визначається як $\eta/2$ або $(\eta+1)/2$ при η парному або непарному, відповідно. Більше того, кожна з функцій Уолша має природну відповідність з гармонікою на часовому проміжку $t \in [0,1]$ [17], при якому частість функції Уолша буде тим більшою, чим більша частота відповідної гармоніки.

Позначимо як $H_N(i,:)$—*i*-ий рядок матриці H_N. У прийнятих позначеннях з урахуванням (2.4) відповідність між початковими рядками H_N та гармонічними функціями матиме вигляд

$$\begin{aligned} H_N(1,:) &\rightarrow \sin(\pi t); \\ H_N(2,:) &\rightarrow \sin(N\pi t); \\ H_N(3,:) &\rightarrow \sin\left(\frac{N}{2}\pi t\right); \\ H_N(4,:) &\rightarrow \cos\left(\frac{N}{2}\pi t\right); \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \end{aligned} \tag{2.6}$$

і т.д.

Найбільшу частість серед рядків матриці (2.4), які є дискретними функціями Уолша, упорядкованими за Адамаром, завжди матиме $H_N(2,:)$, для якої $\overline{\eta} = N/2 = 2^{k-1}$; найбільшу частоту з усіх відповідних гармонік (2.6) має гармоніка $\sin(N\pi t)$, що їй відповідає.

Для найяснішого уявлення про зв'язки між частотними складовими і складовими матриці, що є результатом перетворення Уолша-Адамара, припустимо, що *X*=*E*, де *E* — одинична матриця відповідного розміру. У цьому випадку результат співвідношення (2.5) не залежатиме від матриці зображення, а визначатиметься тільки коефіцієнтами матриці Уолша-Адамара

$$W = H'_N X H'^T_N = H'_N H'_N . \tag{2.7}$$

Співвідношення (2.7) можна переписати у вигляді

$$H'_N H'_N = \frac{1}{N^2}\begin{pmatrix} H_N(1,:) \\ H_N(2,:) \\ \dots\dots\dots \\ H_N(N,:) \end{pmatrix} \cdot \left(\left(H_N(1,:)\right)^T, \left(H_N(2,:)\right)^T, \dots, \left(H_N(N,:)\right)^T \right) =$$
$$= \frac{1}{N^2}\begin{pmatrix} H_N(1,:)\left(H_N(1,:)\right)^T, H_N(1,:)\left(H_N(2,:)\right)^T, & \dots, H_N(1,:)\left(H_N(N,:)\right)^T \\ H_N(2,:)\left(H_N(1,:)\right)^T, H_N(2,:)\left(H_N(2,:)\right)^T, & \dots, H_N(2,:)\left(H_N(N,:)\right)^T \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots & \\ H_N(N,:)\left(H_N(1,:)\right)^T, H_N(N,:)\left(H_N(2,:)\right)^T, & \dots, H_N(N,:)\left(H_N(N,:)\right)^T \end{pmatrix}. \tag{2.8}$$

З урахуванням (2.8), відповідності (2.6) між функціями Уолша та відповідними гармоніками, а також відомих формул перетворення добутку тригонометричних функцій у суму, сформулюємо наступну гіпотезу.

Умова А: у матриці (2.5), що є результатом перетворення Уолша-Адамара, елемент (2,2) буде відповідати найбільш високочастотній складовій *X*, частина високочастотних складових буде локалізована в межах другого рядка і другого стовпця матриці (2.5), незалежно від її розміру. У межах другого рядка та другого стовпця низькочастотні складові відсутні. Взагалі ж у матрицях, що є результатом перетворення Уолша-Адамара, високочастотним складовим відповідатимуть елементи, що стоять на

перетині рядків і стовпців, що відповідають дискретним функціям Уолша з найбільшими частостями. Таким чином, для локалізації елементів, що відповідають високочастотним складовим блоку (матриці) ЦЗ, достатньо серед функцій Уолша визначити функції з найбільшими частостями. Так з урахуванням частості дискретних функцій Уолша, упорядкованих за Адамаром, що використовуються для перетворення матриць розміру $l \times l$, де $l \in \{4,8,16\}$, вказаних в табл. 2.1, можна стверджувати, що високочастотним складовим сигналу в матриці розміру 4×4 будуть відповідати в матриці (2.5) елементи, що стоять на позиціях (виписані в порядку зменшення частоти): (2,2), (2,4) і (4,2); в матриці розміру 8×8: (2,2), (2,6) та (6,2), (2,8) та (6,8) і (6,6); в матриці розміру 16×16: (2,2), (2,10) та (10,2), (2,14) та (14,2), (2,6) і (6,2) і т.д. У порядку зменшення частоти можна виписати всі елементи матриці, а не тільки ті, які відповідають високочастотним. Зазначимо, що якщо частості функцій однакові, то при виявленні відповідності високочастотним складовим перевагу слід віддати тій, яка має більше значення η.

Таблиця 2.1. Відповідність між значеннями η і $\bar{\eta}$ для функцій Уолша, упорядкованих за Адамаром, для різних розмірів матриць Уолша-Адамара

l=4	Номер рядка	1				2				3				4			
	$\eta / \bar{\eta}$	0/0				3/2				1/1				2/1			
l=8	Номер рядка	1		2		3		4		5		6		7		8	
	$\eta / \bar{\eta}$	0/0		7/4		3/2		4/2		1/1		6/3		2/1		5/3	
l=16	Номер рядка	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	$\eta / \bar{\eta}$	0/0	15/8	7/4	8/4	3/2	12/6	4/2	11/6	1/1	14/7	6/3	9/5	2/1	13/7	5/3	10/5

Для практичного підтвердження висунутої гіпотези в середовищі MatLAB було проведено обчислювальний експеримент, в якому було задіяно

1000 ЦЗ з традиційних баз зображень у форматі як із втратами (Jpeg) (база NRCS [18]), так і без втрат (TIFF) (бази img_Nikon_D70s[19], 4cam_auth [20]). Зображення розглядалися розміром 400x400 пікселів. В ході експерименту кожне ЦЗ розбивалося стандартним чином на $l \times l$-блоки, де $l \in \{4,8,16\}$ (розміри блоків обрані як найбільш часто використовувані в блокових стеганографічних методах), для кожного блоку виконувалося перетворення Уолша-Адамара (2.5) (результат — блок B_{WA}) і дискретне косинусне перетворення (результат — блок B_{DCT}). Потім певний елемент (i,j) (для всіх блоків ЦЗ — один і той же елемент(i,j)) піддавався збуренню (результат — блок $\overline{B}_{DCT}$), після чого відновлювався шляхом зворотного косинусного перетворення збурений блок $\overline{B}$. Для $\overline{B}$ будувалося перетворення Уолша-Адамара (результат — блок $\overline{B}_{WA}$), після чого шляхом порівняння $\overline{B}_{WA}$ і B_{WA} знаходився найбільш збурений елемент B_{WA}.По всіх блоках ЦЗ визначався такий елемент B_{WA}, який частіше за інших мав максимальне збурення в результаті збурення елемента (i,j) B_{DCT}, а також кількісна характеристика цієї частоти, для чого для кожного ЦЗ будувалася $l \times l$-матриця максимального збурення R, елемент $R_{ij}, i, j = 0,1,...,l-1$, якої дорівнював кількості блоків ЦЗ, для яких максимальний по абсолютній величині елемент матриці $\overline{B}_{WA} - B_{WA}$ знаходиться на позиції (i,j). Результати експерименту, які повністю відповідають теоретичним положенням, обґрунтованим вище, наведено в табл. 2.2 та на рис. 2.3 (локалізація високочастотних складових виділена заливкою відповідних елементів), при цьому значення елементів матриці R не залежали від величини збурної дії на елементи B_{DCT} (під час експерименту збурення становили $\pm 1\%; \pm 10\%; \pm 100\%$, а залежали лише від їх локалізації в B_{DCT}, що підтверджує точність встановленої відповідності між елементами частотної області і області перетворення Уолша-Адамара. Зауважимо, що оскільки низькочастотним складовим відповідають не тільки елементи

першого стовпця матриці, що є результатом перетворення Уолша-Адамара (рис. 2.3), то очевидно, що метод, запропонований у [10], як уже зазначалося вище, не може гарантовано забезпечити надійність сприйняття стеганоповідомлення, що формується.

Зазначимо, що для деяких блоків ЦЗ однакове максимальне збурення в блоках виду (2.5) досягалося одночасно в кількох елементах, що враховувалося під час проведення експерименту. Поведінка ЦЗ у різних форматах зберігання (із втратами і без втрат) тут дещо відрізнялася. Так для більшості ЦЗ у форматі з втратами кількість блоків, де максимальне збурення в матриці (2.5) відбувалося в одному єдиному елементі, що відповідає теоретичним передумовам, часто збігалося із загальною кількістю блоків або відрізнялося незначно (менше 1.5%), тоді як в інших елементах максимум збурення в блоках взагалі не досягався. Для ЦЗ у форматі без втрат шуканий елемент в області перетворення Уолша-Адамара, що відповідає конкретному частотному коефіцієнту, визначався за абсолютним максимумом блоків, де він зазнавав максимального збурення; цей максимум досягався і в інших елементах перетвореного блоку.

Дана картина очевидно є наслідком того, що для ЦЗ у форматі з втратами високочастотні коефіцієнти в результаті квантування та округлення в процесі збереження та відновлення зображення стають за значенням порівнянними з нулем. Через це навіть за малого абсолютного збурення їхнє відносне збурення буде значним. Наслідком цього факту є те, що отримана нижче достатня умова краще працюватиме для ЦЗ у форматі із втратами. Ілюстрацію наведено на рис. 2.4. Матриця ЦЗ розміру 400×400, спочатку збереженого у форматі Tiff, а потім перезбереженого у формат Jpeg, розбивалася на блоки 8×8, збуренню піддавався в кожному блоці B_{DCT} елемент (8,8).

Таблиця 2.2. — Відповідність між високочастотними складовими блоку ЦЗ та елементами його результату перетворення Уолша-Адамара

Розмір блоку l	Елемент (i,j), що зазнав збурення у B_{DCT} / елемент (m,n), що зазнав максимального збурення у B_{WA} у максимальній кількості блоків ЦЗ при збуренні (i,j) у B_{DCT} (кількість блоків ЦЗ (%), в яких максимальне збурення у B_{WA} зазнав елемент (m,n))		
4	(4,4)/(2,2) (97.3%)	(4,3)/(2,4) (95.6%)	(3,4)/(4,2) (96.1%)
8	(8,8)/(2,2) (99.4%)	(8,7)/(2,6) (99.4%)	(7,8)/(6,2) (99.4%)
16	(16,16)/(2,2) (99.8%)	(16,15)/(2,10) (99.9%)	(15,16)/(10,2) (99.9%)

Таким чином, для матриці, що є результатом перетворення Уолша-Адамара матриці X довільного розміру, можна точно встановити елементи, що відповідають високочастотним складовим матриці X. Стеганоперетворення, результатом якого є збурення цих елементів в області перетворення Уолша-Адамара, забезпечить надійність сприйняття одержуваного стеганоповідомлення.

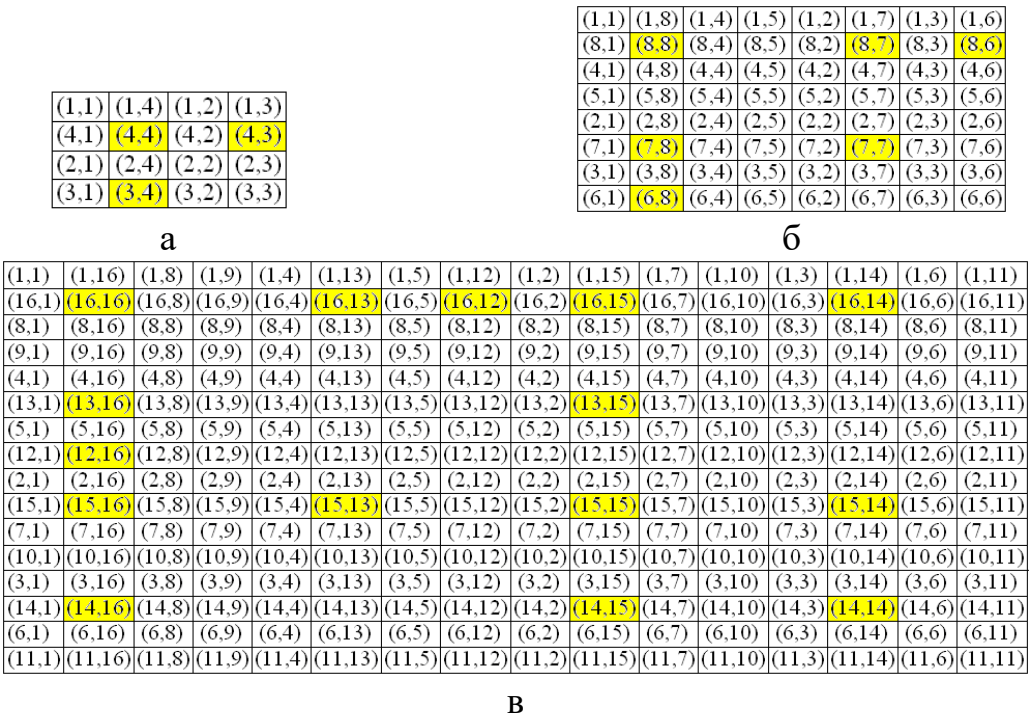
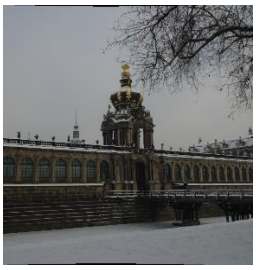


Рис. 2.3. — Відповідність елементів B_{WA} через елементи блоків B_{DCT} різного розміру l: а – l = 4; б - l = 8; в - l = 16;



8	8	8	8	8	8	8	8
8	2500	8	8	8	8	8	8
8	8	8	8	8	8	8	8
8	8	8	8	8	8	5	8
8	8	8	8	8	8	8	8
8	8	8	8	8	8	8	8
8	8	8	5	8	8	8	8
8	8	8	8	8	8	8	5

10	0	0	0	0	0	0	0
0	2490	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

а б в

Рис. 2.4. — а — вихідне ЦЗ у форматі без втрат; б — матриця R для ЦЗ у форматі TIFF; в — матриця R для вихідного ЦЗ, перезбереженого у формат Jpeg

Дещо інший погляд на встановлення відповідності між областями перетворення Уолша-Адамара та ДКП, що призводить до тих самих результатів, запропонований нижче.

Для вивчення фізичної сутності трансформант двовимірного перетворення Уолша-Адамара (2.5) та їх взаємозв'язку з трансформантами ДКП (2.1) зручно розглянути їхнє подання за допомогою векторів-рядків.

Розглянемо вектори-рядки V та Y довжини N^2, які є результатом послідовної конкатенації рядків матриць W та X (2.5) розміру $N \times N$, відповідно. Тут має місце таке твердження.

Твердження 2.1. Трансформанти двовимірних перетворень ДКП (2.1) і Уолша-Адамара (2.5) при їх поданні у вигляді вектора-рядка можуть бути знайдені за допомогою наступного співвідношення

$$V = YA_1, \tag{2.9}$$

де A_1 — матриця порядку N^2, елементи якої є коефіцієнтами при елементах $x_{i,j}$ матриці X після розкриття добутку (2.1) або (2.5).

Доказ **Твердження 2.1.** є очевидним.

При цьому у разі використання двовимірного перетворення Уолша-Адамара (2.5) справедливо наступне.

Твердження 2.2. У разі двовимірного перетворення Уолша-Адамара матрицею A_1 є матриця Уолша-Адамара H_{N^2} порядку N^2, побудована відповідно до конструкції Сільвестра (2.4) з точністю до коефіцієнта $\frac{1}{N}$.

Для доказу **Твердження 2.2.** скористаємося визначеннями одновимірного та двовимірного перетворення Уолша-Адамара через повний двійковий код $b_i(k)$ довжини n, де $i = 0,1,...,n-1$, $n = \log_2 N$, $k = 0,1,...,N-1$.

При цьому одновимірне перетворення Уолша-Адамара вектора Y задається за допомогою наступного співвідношення

$$V_\omega = \sum_{x=0}^{N-1} Y_x (-1)^{\sum_{i=0}^{n-1} b_i(x) b_i(\omega)}, \qquad (2.10)$$

де сума $\sum_{i=0}^{n-1} b_i(x) b_i(\omega)$ є скалярним добутком кодових слів повного коду з номерами x і ω.

Співвідношення, що визначає двовимірне перетворення Уолша-Адамара матриці X має вигляд

$$W_{u,v} = \frac{1}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} X_{x,y} \left[(-1)^{\sum_{i=0}^{n-1} b_i(x) b_i(u) + b_i(y) b_i(v)} \right], \qquad (2.11)$$

Перепишемо вираз (2.11) щодо векторів-рядків і отриманих в результаті рядкової конкатенації матриць W і X

$$V_w = \frac{1}{N} \sum_{z=0}^{N^2-1} Y_z \cdot (-1)^{\sum_{i=0}^{n-1} b_i(z//N) b_i(w//N) + b_i(z \bmod N) b_i(w \bmod N)}, \qquad (2.12)$$

де $z = 0,1,...,N^2-1$, а символ $//$ позначає операцію цілочисельного ділення.

У виразі (2.12) частина виразу під сумою $b_i(z//N) b_i(w//N)$ визначає дублювання скалярного добутку кодових слів повного коду з номерами z і w N разів (еквівалентно низькочастотній частини повного коду довжини $n' = \log_2 N^2 = 2\log_2 N$), в той час як частина виразу під сумою

$b_i(z \bmod N) b_i(w \bmod N)$ призводить до формування скалярного добутку кодових слів повного коду з номерами z і w при кожній зміні значення (еквівалентно високочастотній частини повного коду довжини $n' = \log_2 N^2 = 2\log_2 N$).

Таким чином, у виразі (2.12) сума $\sum_{i=0}^{n-1} b_i(z//N) b_i(w//N) + b_i(z \bmod N) b_i(w \bmod N)$ еквівалентна сумі $\sum_{i=0}^{n'-1} b_i(x) b_i(\omega)$ у виразі (2.10) одновимірного перетворення Уолша-Адамара при використанні повного коду b_i з довжиною кодового слова $n' = 2\log_2 N$, в той час як двовимірне перетворення Уолша-Адамара матриці X відповідає, з точністю до коефіцієнта $\frac{1}{N}$, одновимірному перетворенню вектора Y, який є послідовною конкатенацією рядків матриці X, що доводить **Твердження 2.2**.

Розглянемо також конкретний приклад роботи **Твердження 2.2.** за допомогою прямого розкриття добутку (2.5), яке, наприклад, виконаємо для матриць W, X, H_4 порядку $N = 4$

$$W = H_N X H_N^T = \begin{bmatrix} + & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & + \end{bmatrix} \begin{bmatrix} x_{11} & x_{12} & x_{13} & x_{14} \\ x_{21} & x_{22} & x_{23} & x_{24} \\ x_{31} & x_{32} & x_{33} & x_{34} \\ x_{41} & x_{42} & x_{43} & x_{44} \end{bmatrix} \begin{bmatrix} + & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & + \end{bmatrix} =$$

$$\begin{bmatrix} x_{11}+x_{12}+x_{13}+x_{14}+x_{21}+x_{22}+x_{23}+x_{24}+ & x_{11}-x_{12}+x_{13}-x_{14}+x_{21}-x_{22}+x_{23}-x_{24}+ \\ +x_{31}+x_{32}+x_{33}+x_{34}+x_{41}+x_{42}+x_{43}+x_{44} & +x_{31}-x_{32}+x_{33}-x_{34}+x_{41}-x_{42}+x_{43}-x_{44} \\ x_{11}+x_{12}+x_{13}+x_{14}-x_{21}-x_{22}-x_{23}-x_{24}+ & x_{11}-x_{12}+x_{13}-x_{14}-x_{21}+x_{22}-x_{23}+x_{24}+ \\ +x_{31}+x_{32}+x_{33}+x_{34}-x_{41}-x_{42}-x_{43}-x_{44} & +x_{31}-x_{32}+x_{33}-x_{34}-x_{41}+x_{42}-x_{43}+x_{44} \\ x_{11}+x_{12}+x_{13}+x_{14}+x_{21}+x_{22}+x_{23}+x_{24}- & x_{11}-x_{12}+x_{13}-x_{14}+x_{21}-x_{22}+x_{23}-x_{24}- \\ -x_{31}-x_{32}-x_{33}-x_{34}-x_{41}-x_{42}-x_{43}-x_{44} & -x_{31}+x_{32}-x_{33}+x_{34}-x_{41}+x_{42}-x_{43}+x_{44} \\ x_{11}+x_{12}+x_{13}+x_{14}-x_{21}-x_{22}-x_{23}-x_{24} & x_{11}-x_{12}+x_{13}-x_{14}-x_{21}+x_{22}-x_{23}+x_{24}- \\ -x_{31}-x_{32}-x_{33}-x_{34}+x_{41}+x_{42}+x_{43}+x_{44} & -x_{31}+x_{32}-x_{33}+x_{34}+x_{41}-x_{42}+x_{43}-x_{44} \end{bmatrix} \quad (2.13)$$

$$\begin{bmatrix} x_{11}+x_{12}-x_{13}-x_{14}+x_{21}+x_{22}-x_{23}-x_{24}+ & x_{11}-x_{12}-x_{13}+x_{14}+x_{21}-x_{22}-x_{23}+x_{24}+ \\ +x_{31}+x_{32}-x_{33}-x_{34}+x_{41}+x_{42}-x_{43}-x_{44} & +x_{31}-x_{32}-x_{33}+x_{34}+x_{41}-x_{42}-x_{43}+x_{44} \\ x_{11}+x_{12}-x_{13}-x_{14}-x_{21}-x_{22}+x_{23}+x_{24}+ & x_{11}-x_{12}-x_{13}+x_{14}-x_{21}+x_{22}+x_{23}-x_{24}+ \\ +x_{31}+x_{32}-x_{33}-x_{34}-x_{41}-x_{42}+x_{43}+x_{44} & +x_{31}-x_{32}-x_{33}+x_{34}-x_{41}+x_{42}+x_{43}-x_{44} \\ x_{11}+x_{12}-x_{13}-x_{14}+x_{21}+x_{22}-x_{23}-x_{24}- & x_{11}-x_{12}-x_{13}+x_{14}+x_{21}-x_{22}-x_{23}+x_{24}- \\ -x_{31}-x_{32}+x_{33}+x_{34}-x_{41}-x_{42}+x_{43}+x_{44} & -x_{31}+x_{32}+x_{33}-x_{34}-x_{41}+x_{42}+x_{43}-x_{44} \\ x_{11}+x_{12}-x_{13}-x_{14}-x_{21}-x_{22}+x_{23}+x_{24}- & x_{11}-x_{12}-x_{13}+x_{14}-x_{21}+x_{22}+x_{23}-x_{24}- \\ -x_{31}-x_{32}+x_{33}+x_{34}+x_{41}+x_{42}-x_{43}-x_{44} & -x_{31}+x_{32}+x_{33}-x_{34}+x_{41}-x_{42}-x_{43}+x_{44} \end{bmatrix}.$$

Виконуючи послідовну конкатенацію рядків векторів W і X, а також записуючи коефіцієнти при елементах x_{ij} в результуючій матриці виразу (2.13), не важко переписати вираз (2.5) щодо векторів V і Y довжини N^2

$$V = \begin{bmatrix} w_{11} \\ w_{12} \\ w_{13} \\ w_{14} \\ w_{21} \\ w_{22} \\ w_{23} \\ w_{24} \\ w_{31} \\ w_{32} \\ w_{33} \\ w_{34} \\ w_{41} \\ w_{42} \\ w_{43} \\ w_{44} \end{bmatrix} = A_1 Y^T = \begin{bmatrix} + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + \\ + & - & + & - & + & - & + & - & + & - & + & - & + & - & + & - \\ + & + & - & - & + & + & - & - & + & + & - & - & + & + & - & - \\ + & - & - & + & + & - & - & + & + & - & - & + & + & - & - & + \\ + & + & + & + & - & - & - & - & + & + & + & + & - & - & - & - \\ + & - & + & - & - & + & - & + & + & - & + & - & - & + & - & + \\ + & + & - & - & - & - & + & + & + & + & - & - & - & - & + & + \\ + & - & - & + & - & + & + & - & + & - & - & + & - & + & + & - \\ + & + & + & + & + & + & + & + & - & - & - & - & - & - & - & - \\ + & - & + & - & + & - & + & - & - & + & - & + & - & + & - & + \\ + & + & - & - & + & + & - & - & - & - & + & + & - & - & + & + \\ + & - & - & + & + & - & - & + & - & + & + & - & - & + & + & - \\ + & + & + & + & - & - & - & - & - & - & - & - & + & + & + & + \\ + & - & + & - & - & + & - & + & - & + & - & + & + & - & + & - \\ + & + & - & - & - & - & + & + & - & - & + & + & + & + & - & - \\ + & - & - & + & - & + & + & - & - & + & - & + & + & - & - & + \end{bmatrix} \begin{bmatrix} x_{11} \\ x_{12} \\ x_{13} \\ x_{14} \\ x_{21} \\ x_{22} \\ x_{23} \\ x_{24} \\ x_{31} \\ x_{32} \\ x_{33} \\ x_{34} \\ x_{41} \\ x_{42} \\ x_{43} \\ x_{44} \end{bmatrix}. \quad (2.14)$$

Аналізуючи вирази (2.10) і (2.11), можна дійти висновку, кожен коефіцієнт w_{ij} матриці трансформант Уолша-Адамара W показує ступінь «присутності» в матриці X тієї чи іншої частотної складової, які являють собою всі можливі суперпозиції рядків вихідної матриці Уолша-Адамара H_4. При цьому, зважаючи на структурні особливості матриць Уолша-Адамара, ці суперпозиції збігаються з рядками матриці Уолша-Адамара порядка N^2, тобто, у нашому випадку H_{16}.

Зазначене не є правильним для матриць ДКП, тобто для заданої матриці C_N матриця A_1 відповідає матриці ДПК порядку N^2, тобто $A_1 \neq C_{N^2}$. Однак, проводячи обчислення, подібні до обчислень, проведених в (2.10), не важко знайти матрицю A_1 і для ДКП.

Таким чином, як і у разі перетворення Уолша-Адамара, вираз (2.1) може бути переписаний щодо векторів-рядків P і Y довжини N^2, отриманих шляхом послідовної конкатенації рядків матриць S і X, відповідно.

Далі, розглянемо конкретний приклад на основі матриці ДКП порядку $N = 4$, побудованої відповідно до (2.2)

$$C_4 = \begin{bmatrix} 0.5 & 0.5 & 0.5 & 0.5 \\ 0.65 & 0.27 & -0.27 & -0.65 \\ 0.5 & -0.5 & -0.5 & 0.5 \\ 0.27 & -0.65 & 0.65 & -0.27 \end{bmatrix}, \qquad (2.15)$$

для якої знайдемо матрицю A_1, після чого перепишемо вираз (2.1) щодо векторів-рядків P і Y

$$P=\begin{bmatrix} s_{11}\\ s_{12}\\ s_{13}\\ s_{14}\\ s_{21}\\ s_{22}\\ s_{23}\\ s_{24}\\ s_{31}\\ s_{32}\\ s_{33}\\ s_{34}\\ s_{41}\\ s_{42}\\ s_{43}\\ s_{44} \end{bmatrix}=YA_1=\begin{bmatrix} y_{11}\\ y_{12}\\ y_{13}\\ y_{14}\\ y_{21}\\ y_{22}\\ y_{23}\\ y_{24}\\ y_{31}\\ y_{32}\\ y_{33}\\ y_{34}\\ y_{41}\\ y_{42}\\ y_{43}\\ y_{44} \end{bmatrix}^T \begin{bmatrix} 0.25 & 0.33 & 0.25 & 0.14 & 0.33 & 0.43 & 0.33 & 0.18\\ 0.25 & 0.14 & -0.25 & -0.33 & 0.33 & 0.18 & -0.33 & -0.43\\ 0.25 & -0.14 & -0.25 & 0.33 & 0.33 & -0.18 & -0.33 & 0.43\\ 0.25 & -0.33 & 0.25 & -0.14 & 0.33 & -0.43 & 0.33 & -0.18\\ 0.25 & 0.33 & 0.25 & 0.14 & 0.14 & 0.18 & 0.14 & 0.07\\ 0.25 & 0.14 & -0.25 & -0.33 & 0.14 & 0.07 & -0.14 & -0.18\\ 0.25 & -0.14 & -0.25 & 0.33 & 0.14 & -0.07 & -0.14 & 0.18\\ 0.25 & -0.33 & 0.25 & -0.14 & 0.14 & -0.18 & 0.14 & -0.07\\ 0.25 & 0.33 & 0.25 & 0.14 & -0.14 & -0.18 & -0.14 & -0.07\\ 0.25 & 0.14 & -0.25 & -0.33 & -0.14 & -0.07 & 0.14 & 0.18\\ 0.25 & -0.14 & -0.25 & 0.33 & -0.14 & 0.07 & 0.14 & -0.18\\ 0.25 & -0.33 & 0.25 & -0.14 & -0.14 & 0.18 & -0.14 & 0.07\\ 0.25 & 0.33 & 0.25 & 0.14 & -0.33 & -0.43 & -0.33 & -0.18\\ 0.25 & 0.14 & -0.25 & -0.33 & -0.33 & -0.18 & 0.33 & 0.43\\ 0.25 & -0.14 & -0.25 & 0.33 & -0.33 & 0.18 & 0.33 & -0.43\\ 0.25 & -0.33 & 0.25 & -0.14 & -0.33 & 0.43 & -0.33 & 0.18 \end{bmatrix}$$

$$\begin{bmatrix} 0.25 & 0.33 & 0.25 & 0.14 & 0.14 & 0.18 & 0.14 & 0.07\\ 0.25 & 0.14 & -0.25 & -0.33 & 0.14 & 0.07 & -0.14 & -0.18\\ 0.25 & -0.14 & -0.25 & 0.33 & 0.14 & -0.07 & -0.14 & 0.18\\ 0.25 & -0.33 & 0.25 & -0.14 & 0.14 & -0.18 & 0.14 & -0.07\\ -0.25 & -0.33 & -0.25 & -0.14 & -0.33 & -0.43 & -0.33 & -0.18\\ -0.25 & -0.14 & 0.25 & 0.33 & -0.33 & -0.18 & 0.33 & 0.43\\ -0.25 & 0.14 & 0.25 & -0.33 & -0.33 & 0.18 & 0.33 & -0.43\\ -0.25 & 0.33 & -0.25 & 0.14 & -0.33 & 0.43 & -0.33 & 0.18\\ -0.25 & -0.33 & -0.25 & -0.14 & 0.33 & 0.43 & 0.33 & 0.18\\ -0.25 & -0.14 & 0.25 & 0.33 & 0.33 & 0.18 & -0.33 & -0.43\\ -0.25 & 0.14 & 0.25 & -0.33 & 0.33 & -0.18 & -0.33 & 0.43\\ -0.25 & 0.33 & -0.25 & 0.14 & 0.33 & -0.43 & 0.33 & -0.18\\ 0.25 & 0.33 & 0.25 & 0.14 & -0.14 & -0.18 & -0.14 & -0.07\\ 0.25 & 0.14 & -0.25 & -0.33 & -0.14 & -0.07 & 0.14 & 0.18\\ 0.25 & -0.14 & -0.25 & 0.33 & -0.14 & 0.07 & 0.14 & -0.18\\ 0.25 & -0.33 & 0.25 & -0.14 & -0.14 & 0.18 & -0.14 & 0.07 \end{bmatrix}. \quad (2.16)$$

Використовуючи отримані одновимірні уявлення ДКП, і також двовимірного перетворення Уолша-Адамара, ми можемо встановити взаємозв'язок між трансформантами обох перетворень. Зазначимо, проте, що через різницю у природі базисних функцій ДКП і перетворення Уолша-Адамара, вплив зміни того чи іншого коефіцієнта в області перетворень Уолша-Адамара впливатиме на ряд коефіцієнтів у просторі ДКП, і навпаки.

Тим не менш, як показують дослідження, можливо встановити коефіцієнти ДКП та двовимірного перетворення Уолша-Адамара, які мають один на одного найбільший вплив.

Відповідно до визначення частоти [17] знайдемо значення числа зміни знаку η для кожного рядка матриці A_1 (2.13), обчисленої нами для трансформант ДКП матриці порядку $N = 4$. Дані про кількість змін знаку η для рядків матриці A_1 (2.14) наведено в табл. 2.3.

Таблиця 2.3 — Значення η для матриці ДКП

№ строки	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
A_1 (10)	0	7	8	15	1	6	9	14	2	5	10	13	3	4	11	12

Аналізуючи дані табл. 2.3 і порівнюючи їх з даними табл. 2.1 ми можемо встановити відповідність між частотами (частостями) базисних функцій ДКП і перетворення Уолша-Адамара, таким чином, зробивши висновок про те, модифікація яких трансформант перетворення Уолша-Адамара призводить до найбільшої зміни тих чи інших трансформант ДКП. Дану відповідність, для зручності, запишемо у вигляді наступного виразу

$$\begin{matrix} s_{11} & s_{12} & s_{13} & s_{14} & s_{21} & s_{22} & s_{23} & s_{24} & s_{31} & s_{32} & s_{33} & s_{34} & s_{41} & s_{42} & s_{43} & s_{44} \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ w_{11} & w_{13} & w_{14} & w_{12} & w_{31} & w_{33} & w_{34} & w_{32} & w_{41} & w_{43} & w_{44} & w_{42} & w_{21} & w_{23} & w_{24} & w_{22} \end{matrix}. \quad (2.17)$$

Отримана відповідність (2.17) повністю збігається з результатами, представленими на рис. 2.2. Вираз (2.17) дозволяє встановити відповідність між трансформантами Уолша-Адамара і ДКП, а також показує, які трансформанти Уолша-Адамара найбільше впливають на якість вихідного зображення.

2.3. Зв'язок перетворення Уолша-Адамара та сингулярного розкладання матриці

Як було зазначено, формальні достатні умови забезпечення надійності сприйняття стеганоповідомлення вже пропонувалися раніше в області

сингулярного (спектрального) розкладання (блоків) матриці контейнера [13], відповідно до яких надійність сприйняття стеганоповідомлення забезпечуватиметься у разі, якщо сингулярні вектори (блоків) матриці (власні вектори симетричної матриці), збурені в результаті стеганоперетворення, відповідають малим сингулярним числам (малим за модулем власним значенням симетричної матриці (симетричних блоків матриці)) або сингулярним числам, які мають малі відокремленості (власним значенням симетричної матриці (малі абсолютні відокремленості). При цьому, чим менше збурення сингулярних чисел (власних значень симетричної матриці), відокремленості (абсолютні відокремленості) і значення сингулярних чисел (модулі власних значень симетричної матриці), які відповідають збуреним сингулярним векторам (власним векторам симетричної матриці), тим більше ймовірність дотримання надійності сприйняття стеганоповідомлення. При цьому у разі застосування достатньої умови до блоків матриці блоки утворюються шляхом її стандартного розбиття [22].

Розглянемо для визначеності повний набір параметрів, який повністю визначає ЦЗ і складається з СНЧ і СНВ сукупності $l \times l$-блоків ЦЗ, що не перетинаються, [2], довільний з яких — B. Достатня умова, згадана вище, з урахуванням того, що в матриці ЦЗ (кадра ЦВ) СНЧ не просто пов'язані співвідношенням: $\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_l \geq 0$ а це співвідношення можна уточнити

$$\sigma_1 >> \sigma_2 \geq ... \geq \sigma_l \geq 0, \qquad (2.18)$$

при цьому відокремленість σ_i обчислюється за формулою [21]: $svdgap(i, B) = \min\limits_{j \neq i} |\sigma_i - \sigma_j|$, відповідно до якої $svdgap(1, B) = \sigma_1 - \sigma_2 >> svdgap(i, B),\ i > 1$, при цьому відокремленість найменших за значенням СНЧ може бути значно менше одиниці (аж до порівнянності з 0), що призводить до того, що СНЧ, про які йдеться в достатній умові — це найменші за значенням СНЧ. Розглянемо сингулярне розкладання матриці B у формі зовнішніх добутків [21]

$$B = \sum_{i=1}^{l} \sigma_i u_i v_i^T , \qquad (2.19)$$

яке дає уявлення B у вигляді суми матриць одиничного рангу, кожна з яких відповідає своїй сингулярній трійці (σ_i, u_i, v_i). З урахуванням цього, а також (2.16), згадану достатню умову можна сформулювати в дещо іншій формі: надійність сприйняття стеганоповідомлення буде забезпечуватися в тому випадку, коли при формальному поданні стеганоперетворення в області сингулярного розкладання блоків матриці це виразиться в збуренні в матрицях одиничного рангу, що відповідають найменшим за значенням СНЧ у (2.17).

Необхідно відзначити, що за достатньої умови, сформульованої в області сингулярного розкладання матриці, ми не маємо такого чіткого поділу по частотним складовим, як в області ДКП або перетворення Фур'є, оскільки кожна сингулярна трійка (і відповідна їй однорангова матриця) несе в собі інформацію про всі частоти, але у різній мірі. Так сингулярні трійки, що відповідають мінімальним/максимальним/середнім за значенням СНЧ, відповідають головним чином високочастотним/низькочастотним/середньочастотним складовим. Розподіл частот між сингулярними трійками більш «м'який», ніж у частотній області, що дає свої переваги в стеганографії [2].

Можна припустити, що відсутність чіткого розподілу на частоти призведе і до більш «м'якої» відповідності між сингулярними трійками матриці та елементами матриці-результату перетворення Уолша-Адамара, дасть можливість для «більшого маневру» в процесі стеганоперетворення, не погіршуючи надійність сприйняття стегноповідомлення, розширюючи можливу область перетворення.

Для підтвердження було проведено обчислювальний експеримент, у якому були задіяні традиційні бази зображень у форматі як із втратами (Jpeg) (база NRCS [18]), так і без втрат (TIFF) (бази img_Nikon_D70s [19],

4cam_auth [20]). У ході експерименту збурення вносилися в матрицю $\sigma_4 u_4 v_4^T$ (для блоків розміру 4×4), в матриці $\sigma_7 u_7 v_7^T$ та $\sigma_8 u_8 v_8^T$ (для блоків розміром 8×8), в матриці $\sigma_i u_i v_i^T$, $i\in\{13,14,15,16\}$ (для блоків розміром 16×16). В результаті було розширено область можливого збурення блоків ЦЗ в області перетворення Уолша-Адамара, що дає можливість збереження надійності сприйняття стеганоповідомлення (рис. 2.5).

Отримана картина є абсолютно природною. Додаткове розширення області можливого збурення без порушення надійності сприйняття відбувається, по суті, за рахунок підключення елементів, які можна віднести до таких, які відповідають середньочастотній складовій, яка, як відомо, зі значною ймовірністю не порушує надійність сприйняття.

(1,1)	(1,4)	(1,2)	(1,3)
(4,1)	(4,4)	(4,2)	(4,3)
(2,1)	(2,4)	(2,2)	(2,3)
(3,1)	(3,4)	(3,2)	(3,3)

а

(1,1)	(1,8)	(1,4)	(1,5)	(1,2)	(1,7)	(1,3)	(1,6)
(8,1)	(8,8)	(8,4)	(8,5)	(8,2)	(8,7)	(8,3)	(8,6)
(4,1)	(4,8)	(4,4)	(4,5)	(4,2)	(4,7)	(4,3)	(4,6)
(5,1)	(5,8)	(5,4)	(5,5)	(5,2)	(5,7)	(5,3)	(5,6)
(2,1)	(2,8)	(2,4)	(2,5)	(2,2)	(2,7)	(2,3)	(2,6)
(7,1)	(7,8)	(7,4)	(7,5)	(7,2)	(7,7)	(7,3)	(7,6)
(3,1)	(3,8)	(3,4)	(3,5)	(3,2)	(3,7)	(3,3)	(3,6)
(6,1)	(6,8)	(6,4)	(6,5)	(6,2)	(6,7)	(6,3)	(6,6)

б

(1,1)	(1,16)	(1,8)	(1,9)	(1,4)	(1,13)	(1,5)	(1,12)	(1,2)	(1,15)	(1,7)	(1,10)	(1,3)	(1,14)	(1,6)	(1,11)
(16,1)	(16,16)	(16,8)	(16,9)	(16,4)	(16,13)	(16,5)	(16,12)	(16,2)	(16,15)	(16,7)	(16,10)	(16,3)	(16,14)	(16,6)	(16,11)
(8,1)	(8,16)	(8,8)	(8,9)	(8,4)	(8,13)	(8,5)	(8,12)	(8,2)	(8,15)	(8,7)	(8,10)	(8,3)	(8,14)	(8,6)	(8,11)
(9,1)	(9,16)	(9,8)	(9,9)	(9,4)	(9,13)	(9,5)	(9,12)	(9,2)	(9,15)	(9,7)	(9,10)	(9,3)	(9,14)	(9,6)	(9,11)
(4,1)	(4,16)	(4,8)	(4,9)	(4,4)	(4,13)	(4,5)	(4,12)	(4,2)	(4,15)	(4,7)	(4,10)	(4,3)	(4,14)	(4,6)	(4,11)
(13,1)	(13,16)	(13,8)	(13,9)	(13,4)	(13,13)	(13,5)	(13,12)	(13,2)	(13,15)	(13,7)	(13,10)	(13,3)	(13,14)	(13,6)	(13,11)
(5,1)	(5,16)	(5,8)	(5,9)	(5,4)	(5,13)	(5,5)	(5,12)	(5,2)	(5,15)	(5,7)	(5,10)	(5,3)	(5,14)	(5,6)	(5,11)
(12,1)	(12,16)	(12,8)	(12,9)	(12,4)	(12,13)	(12,5)	(12,12)	(12,2)	(12,15)	(12,7)	(12,10)	(12,3)	(12,14)	(12,6)	(12,11)
(2,1)	(2,16)	(2,8)	(2,9)	(2,4)	(2,13)	(2,5)	(2,12)	(2,2)	(2,15)	(2,7)	(2,10)	(2,3)	(2,14)	(2,6)	(2,11)
(15,1)	(15,16)	(15,8)	(15,9)	(15,4)	(15,13)	(15,5)	(15,12)	(15,2)	(15,15)	(15,7)	(15,10)	(15,3)	(15,14)	(15,6)	(15,11)
(7,1)	(7,16)	(7,8)	(7,9)	(7,4)	(7,13)	(7,5)	(7,12)	(7,2)	(7,15)	(7,7)	(7,10)	(7,3)	(7,14)	(7,6)	(7,11)
(10,1)	(10,16)	(10,8)	(10,9)	(10,4)	(10,13)	(10,5)	(10,12)	(10,2)	(10,15)	(10,7)	(10,10)	(10,3)	(10,14)	(10,6)	(10,11)
(3,1)	(3,16)	(3,8)	(3,9)	(3,4)	(3,13)	(3,5)	(3,12)	(3,2)	(3,15)	(3,7)	(3,10)	(3,3)	(3,14)	(3,6)	(3,11)
(14,1)	(14,16)	(14,8)	(14,9)	(14,4)	(14,13)	(14,5)	(14,12)	(14,2)	(14,15)	(14,7)	(14,10)	(14,3)	(14,14)	(14,6)	(14,11)
(6,1)	(6,16)	(6,8)	(6,9)	(6,4)	(6,13)	(6,5)	(6,12)	(6,2)	(6,15)	(6,7)	(6,10)	(6,3)	(6,14)	(6,6)	(6,11)
(11,1)	(11,16)	(11,8)	(11,9)	(11,4)	(11,13)	(11,5)	(11,12)	(11,2)	(11,15)	(11,7)	(11,10)	(11,3)	(11,14)	(11,6)	(11,11)

в

Рис. 2.5. — Локалізація області можливого збурення в результаті стеганоперетворення в області перетворення Уолша-Адамара для $l\times l$-блоків ЦЗ: а — $l=4$; б — $l=8$; в — $l=16$

2.4. Достатня умова забезпечення надійності сприйняття стеганоповідомлення

Виходячи з отриманих у роботі результатів, може бути сформульована ***Достатня умова забезпечення надійності сприйняття стеганоповідомлення.*** Для забезпечення надійності сприйняття стеганоповідомлення достатньо проводити вбудовування додаткової інформації таким чином, щоб в області перетворення Уолша-Адамара його результатом було збурення елементів, локалізація яких наведена на рис. 2.5 для $l \times l$-блоків розміру $l \in \{4,8,16\}$, при цьому саме вбудовування ДІ може здійснюватися не тільки безпосередньо в області Уолша-Адамара, а й у будь-якій іншій області контейнера (просторовій, перетворення). При необхідності використання блоків іншого розміру рекомендується проводити вбудовування ДІ таким чином, щоб результатом його було збурення елементів в області перетворення Уолша-Адамара в межах другого стовпця та другого рядка перетвореної матриці. Для точнішої локалізації можливих збурень необхідно провести додаткові дослідження з урахуванням умови *A*.

Для практичної перевірки отриманої достатньої умови було проведено обчислювальний експеримент, у якому були задіяні ЦЗ з перерахованих раніше баз. Збурення вносилося в матрицю блока в області перетворення Уолша-Адамара. Збурення кожного елемента бралися з множини {+1, -1}, з урахуванням того, що ДІ при організації прихованого каналу зв'язку, як правило, являє собою бінарну послідовність. Експеримент проводився для блоків 8×8. Результати представлені у табл. 2.4.

Таблиця 2.4 — Вплив збурення елементів блока в області перетворення Уолша-Адамара на PSNR зображення

Збурені елементи блоку в області перетворення Уолша-Адамара	(2,2)	(2,6)&(6,2)	(2,8)/(8,2)	(2,4)&(4,2)	(2,2)&(2,8)&(8,2) &(2,6)&&(6,2) &(2,4)&(4,2)	(6,6)	(8,8)	(6,6)& (6,8)& (8,6)&(8,8)	(2,2)&(2,8)&(8,2)& (2,6)&&(6,2)&(2,4) &(4,2)&&(6,6)& (6,8)&(8,6)& &(8,8)
PSNR (*dB*)	48.1	45.2	45.1	45.1	39.7	48.0	48.0	42.1	37.7

Отримані результати перебувають у повній відповідності з теоретичними висновками, практично підтверджують дієвість отриманої достатньої умови дотримання надійності сприйняття стеганоповідомлення. Наочна ілюстрація наведена на рис. 2.6 де величина збурення елементів в матрицях, що є результатом перетворення Уолша-Адамара 8×8-блоків ЦЗ, склала ±1. Жодних артефактів, відмінностей від оригіналу на збуреному ЦЗ (рис. 2.6 (б)) шляхом суб'єктивного ранжування не виявляється.

а б

Рис. 2.6. — Ілюстрація дієвості отриманої достатньої умови дотримання надійності сприйняття стеганоповідомлення: а – оригінальне ЦЗ; б - ЦЗ, отримане в результаті збурення всіх елементів другого стовпця і другого рядка в кожному блоці, що є результатом перетворення Уолша-Адамара 8×8-блоків ЦЗ

Зауваження. Отримана достатня умова завдяки використаному математичному підходу дає можливість для недопущення локальних порушень надійності сприйняття, пов'язаних не тільки із стеганоперетворенням (рис. 2.1), але і там, де різницеві показники виявляються часто недієздатними.

Ілюстрація наведеного зауваження представлена на рис. 2.7, де на оригінальному ЦЗ змінено значення яскравості лише одного пікселя. При значних розмірах ЦЗ така зміна візуально на зображенні взагалі не визначається, але вона може бути виявлена при ретельному візуальному аналізі, включаючи використання існуючих програмних засобів.

а

б

Рис. 2.7. — Локальні зміни ЦЗ: а — оригінальне зображення з виділеною оригінальною 8×8-областю; б — зображення, цілісність якого порушена в межах виділеної 8×8-області

Аналізуючи 8×8-блок B, що містить змінений піксель, було встановлено, що зміни в області перетворення Уолша-Адамара зазнали всі елементи, збурення яких склали ≈ 3.1 (матриця (2.5) для блоку B, модулі елементів якої (за винятком (1,1)) менше 1, представлена у (2.20)), що не задовольняє отриманій достатній умові та очікувано призводить до можливості встановлення порушення надійності сприйняття.

$$W=\begin{bmatrix} 251.0781 & 0.1094 & 0.1719 & 0.3281 & -0.2656 & 0.0156 & -0.0469 & -0.0156 \\ -0.0156 & 0.0156 & -0.0469 & -0.0156 & -0.1094 & 0.0469 & -0.0156 & 0.0156 \\ 0.0781 & -0.0156 & -0.0781 & -0.0469 & -0.3281 & 0.0781 & 0.1406 & 0.0469 \\ -0.1406 & 0.0156 & 0.0781 & -0.0156 & -0.0469 & -0.0156 & 0.0469 & -0.0469 \\ -0.1719 & 0.1094 & 0.2969 & -0.0469 & -0.3906 & 0.1406 & 0.3281 & 0.1094 \\ 0.0469 & 0.0781 & 0.0156 & 0.0469 & 0.0781 & -0.0156 & 0.0469 & 0.0781 \\ 0.0156 & 0.0469 & 0.1094 & 0.0156 & -0.0156 & 0.0156 & 0.0781 & 0.1094 \\ 0.1094 & -0.1094 & -0.0469 & -0.0156 & 0.0781 & -0.0156 & -0.0781 & -0.0469 \end{bmatrix}. \quad (2.20)$$

Таким чином, отримана достатня умова може бути використана не тільки для забезпечення надійності сприйняття стеганоповідомлення, але і як інструмент, який дасть можливість навіть за відсутності візуальної картинки робити висновки про можливу з великою ймовірністю появу артефактів на зображенні, кадрі цифрового відео, в тому числі, у малій локальній області (аж до зміни одного пікселя).

2.5. Достатня умова забезпечення нечутливості стеганоповідомлення до збурних дій

Такі збурні дії як стиск із втратами, накладання шуму та розмиття часто використовуються для атаки на стеганоповідомлення з метою руйнування ДІ, що вбудована в нього. Перераховані збурні дії, призводять до зміни, головним чином, високочастотних складових зображення, таким чином, якщо ДІ буде зосереджена в низькочастотних або середньочастотних складових стеганоповідомлення, воно буде максимально стійким до перерахованих атак.

Подальший розгляд почнемо з прикладу найпоширенішоїзбурної дії — атаки стисненням з використанням алгоритму стиснення JPEG.

Відомо [1], що з метою максимізації якості візуального сприйняття зображення найменший збурний вплив алгоритм JPEG чинить на низькочастотні і середньочастотні компоненти ДКП.

Ґрунтуючись на введених раніше визначеннях, а також результатах роботи [12], амплітуда змін, що вносяться в трансформанти ДКП зображення при його збуренні стисненням із втратами, розмиванням або зашумленням пропорційна частоті відповідної компоненти зображення. Так, найменшою амплітудою зміни при зазначених атаках характеризуються трансформанти ДКП, що відповідають низькочастотним та середньочастотним складовим.

Перерахуємо у порядку зростання частоти трансформанти ДКП розмірів $4\times4, 8\times8, 16\times16$: (1,1); (1,2); (2,1); (3,1); (2,2); (1,3) і т.д.

Відповідно до даних рис. 2.5. наведемо відповідні зазначеним трансформантам ДКП трансформанти Уолша-Адамара для практично цінних розмірів блоку перетворення $n\times n$, $n\in\{4,8,16\}$

ДКП	Перетворення Уолша-Адамара
$(1,1);\ (1,2);\ (2,1);$ $(3,1);\ (2,2);\ (1,3)...$	$4\times4:(1,1);\ (1,3);\ (3,1);\ (4,1);\ (3,3);\ (1,4)...$ $8\times8:(1,1);\ (1,5);\ (5,1);\ (7,1);\ (5,5);\ (1,7)...$ $16\times16:(1,1);\ (1,9);\ (9,1);\ (13,1);\ (9,9);\ (1,13)...$

. (2.21)

Зрозуміло, що подібним чином можуть бути виписані всі трансформанти Уолша-Адамара у порядку зростання частоти компоненти, яку вони представляють. Однак, з практичної точки зору, для завдань формулювання достатньої умови забезпечення нечутливості зображень до збурень, найбільший інтерес представляють саме представлені вище низькочастотні та середньочастотні компоненти.

Для емпіричного підтвердження співвідношення (2.21) стосовно атак накладенням шуму проведемо наступний експеримент, на основі бази зображень без втрат у форматі TIFF (база NRCS [18]). До кожного

зображення будемо застосовувати накладання адитивного білого гаусівського шуму зі стандартним значенням математичного сподівання $M = 0$ та дисперсією $\sigma^2 = 10^{-5}$. Після цього знаходитимемо перетворення Уолша-Адамара для кожного блоку розміру $n \times n$, $n \in \{4,8,16\}$ (розбиття зображення на блоки виконується таким чином, щоб вони не перетиналися), досліджуваних зображень до і після накладання шуму з наступним знаходженням різниці (у відсотках) і усередненням результатів. Наведемо отриману матрицю для розміру блоку 4×4

$$\Delta_4 = \begin{bmatrix} 2.97 & 68.72 & 48.43 & 66.59 \\ 64.92 & 110.17 & 85.83 & 101.4 \\ 45.11 & 86.01 & 62.55 & 77.3 \\ 63.42 & 100.48 & 75.9 & 88.2 \end{bmatrix}, \quad (2.22)$$

для розміру блоку 8×8

$$\Delta_8 = \begin{bmatrix} 8.31 & 82.87 & 54.35 & 80.92 & 40.96 & 81.45 & 57.66 & 78.72 \\ 74.65 & 158.6 & 119.95 & 137.89 & 101.42 & 146.5 & 114.84 & 141.17 \\ 48.44 & 120.1 & 82.38 & 97.03 & 67.33 & 108.64 & 78.72 & 101.64 \\ 75.46 & 136 & 96.33 & 114.42 & 84.14 & 123.57 & 93.44 & 113.24 \\ 35.33 & 100.93 & 68.07 & 87.32 & 52.91 & 90.58 & 64.46 & 88.14 \\ 75.66 & 145.73 & 107.2 & 125.34 & 88.65 & 132.43 & 100.28 & 127.73 \\ 53.3 & 114.43 & 78.85 & 97.23 & 63.09 & 101.07 & 73.06 & 97.42 \\ 73.53 & 139.89 & 99.46 & 112.29 & 85.08 & 126.84 & 95.03 & 117.41 \end{bmatrix}, \quad (2.23)$$

а також для розміру блоку 16×16

$$\Delta_{16} = \begin{bmatrix} 23 & 92 & 59 & 89 & 42 & 91 & 63 & 90 & 31 & 92 & 61 & 91 & 45 & 92 & 63 & 89 \\ 78 & 209 & 155 & 173 & 130 & 184 & 145 & 181 & 111 & 198 & 149 & 176 & 126 & 189 & 146 & 179 \\ 49 & 155 & 104 & 118 & 83 & 131 & 95 & 126 & 70 & 143 & 98 & 119 & 80 & 136 & 97 & 124 \\ 83 & 171 & 117 & 128 & 99 & 145 & 107 & 135 & 91 & 158 & 111 & 131 & 96 & 151 & 109 & 133 \\ 33 & 128 & 84 & 103 & 64 & 106 & 76 & 105 & 52 & 117 & 78 & 103 & 61 & 110 & 76 & 105 \\ 83 & 183 & 130 & 147 & 104 & 155 & 114 & 152 & 92 & 169 & 122 & 148 & 99 & 159 & 116 & 151 \\ 57 & 144 & 95 & 111 & 74 & 116 & 82 & 114 & 64 & 129 & 88 & 112 & 69 & 120 & 83 & 113 \\ 82 & 179 & 123 & 135 & 102 & 152 & 111 & 143 & 90 & 165 & 116 & 137 & 98 & 157 & 114 & 141 \\ 24 & 113 & 72 & 97 & 54 & 98 & 68 & 95 & 42 & 103 & 68 & 96 & 51 & 100 & 67 & 95 \\ 83 & 197 & 142 & 160 & 117 & 170 & 129 & 166 & 98 & 183 & 134 & 161 & 111 & 175 & 130 & 165 \\ 54 & 149 & 98 & 113 & 78 & 124 & 88 & 119 & 65 & 135 & 91 & 114 & 73 & 128 & 90 & 117 \\ 84 & 173 & 118 & 132 & 100 & 147 & 107 & 137 & 90 & 159 & 111 & 133 & 96 & 152 & 110 & 135 \\ 40 & 125 & 81 & 101 & 61 & 103 & 72 & 102 & 50 & 112 & 74 & 100 & 57 & 105 & 72 & 101 \\ 84 & 188 & 134 & 153 & 107 & 160 & 120 & 158 & 94 & 174 & 126 & 154 & 102 & 165 & 121 & 157 \\ 57 & 145 & 97 & 114 & 75 & 118 & 84 & 117 & 65 & 131 & 90 & 114 & 71 & 123 & 86 & 116 \\ 82 & 177 & 121 & 132 & 101 & 149 & 110 & 141 & 89 & 163 & 114 & 134 & 97 & 155 & 112 & 139 \end{bmatrix}. \quad (2.24)$$

Аналіз матриць (2.22), (2.23), (2.24) показує, що найменші збуренні трансформанти Уолша-Адамара, дійсно відповідають коефіцієнтам зазначеним в (2.21), що представляють низькочастотні і середньочастотні складові.

В результаті проведення аналогічного експерименту для випадку атаки розмиттям зображення були отримані матриці, аналогічні матрицям (2.22), (2.23), (2.24).

Таким чином, враховуючи результати відповідності між трансформантамиУолша-Адамара, коефіцієнтами ДКП, сингулярними трійками, отримані в попередніх підрозділах, а також результати проведених експериментів може бути сформульована і

Достатня умова забезпечення нечутливості стеганоповідомлення до збурних дій. Для забезпечення нечутливості стеганоповідомлення до збурних дій достатньо проводити вбудовування додаткової інформації таким чином, щоб в області перетворення Уолша-Адамара його результатом було збурення елементів, локалізація яких наведена у (2.21) для $l \times l$-блоків розміру $l \in \{4,8,16\}$, при цьому саме вбудовування ДІ може здійснюватися не тільки безпосередньо в області Уолша-Адамара, а й у будь-якій іншій області контейнера (просторовій, перетворення).

2.6 Кодове управління частотними складовими, що зазнають збурення внаслідок вбудовування інформації

Як показують дослідження, отримані результати можуть стати основою для кодового управлінням частотними складовими, що зазнають збурення в результаті вбудовування інформації при їх комбінації з класичним методом LSB-matching [24], який гарантує забезпечення надійності сприйняття стеганоповідомлення та передбачає послідовне поелементне підсумовування

елементів контейнера $x_{i,j} \in \{0,1,...,255\}$ з додатковою інформацією, що вбудовується $d_i \in \{+1,0,-1\}$.

Розглянемо теоретичну основу можливості кодового управління частотними складовими без переходу до частотної області. Нехай блок $X = \|x_{i,j}\|, i, j, = 0,1,...,N-1$ деякого зображення є матрицею розміру $N \times N$, тоді як результат додаткового кодування ДІ — вектор $D = \{d_k\}, k = 0,1,...,N^2 - 1.$

Шляхом послідовної конкатенації рядків матриці X отримуємо новий вектор-рядок Y. Тоді результуюче стеганоповідомлення матиме вигляд

$$M = Y + D. \tag{2.25}$$

Розглянемо тепер перетворення Уолша-Адамара вектора-рядка M, відповідно до виразу (2.5)

$$V = MH_{N^2} = (Y + D)H_{N^2} = YH_{N^2} + DH_{N^2}. \tag{2.26}$$

Вираз (2.22) дозволяє зробити фундаментальний висновок про природу збурення трансформант Уолша-Адамара в стеганоповідомленні після вбудовування в нього додаткової інформації — величина і локалізація подібних збурень залежатиме від конкретного виду доданку DH_{N^2}, який являє собою трансформанти Уолша-Адамара додаткової інформації, що вбудовується. У свою чергу, конкретна локалізація і амплітуда внесених у трансформанти Уолша-Адамара стеганоповідомлення збурень буде залежати від виду вбудовуваної у вектор-рядок Y, а значить, і в блок X, послідовності D.

З огляду на бінарну природу послідовності D для визначення таких її видів, які призводять до забезпечення нечутливості стеганоповідомлення до збурювальних впливів, скористаємося визначенням елементарної структури [27].

Визначення 2.1. Елементарною структурою вектора трансформант Уолша-Адамара назвемо набір різних спектральних компонент із зазначенням їх частот у векторі.

Наприклад, розглянемо вектор $T=[++--++--++--++--]$ довжини $N=16$, і також його вектор трансформант Уолша-Адамара $W=[0,0,16,0,0,0,0,0,0,0,0,0,0,0,0,0]$, який має елементарну структуру $\{16(1),0(15)\}$, де у круглих дужках зазначено кількість разів, яка наведена компонента зустрічається у векторі трансформант Уолша-Адамара. Це з урахуванням (2.22) говорить про те, що якщо в якості вектора *D*, що є результатом додаткового кодування ДІ, використовувати рядки матриці Уолша-Адамара, то за рахунок вибору конкретного рядка можливо управляти локалізацією відповідного збурення в області Уолша-Адамара, а значить, з урахуванням інформації, поданої на рис. 2.5, і в області трансформант ДКП контейнера.

Відомо, що елементарною структурою $\{N(1),0(N-1)\}$ характеризуються двійкові вектори, які є рядками матриці Уолша-Адамара порядку N та їх інверсії, при цьому значення, що дорівнює N ($-N$ у разі інверсії рядка матриці Уолша-Адамара) стоїть на позиції, що відповідає номеру рядка Уолша-Адамара.

Розглянемо конкретний приклад. Нехай задана матриця-фрагмент вихідного зображення, для якої відповідно до виразу (2.3) знайдемо трансформанти Уолша-Адамара (з точністю до коефіцієнта $1/N$)

$$X=\begin{bmatrix}127 & 123 & 119 & 119\\ 124 & 125 & 124 & 124\\ 123 & 122 & 123 & 124\\ 123 & 121 & 122 & 125\end{bmatrix}, W_X=\begin{bmatrix}1968 & 2 & 8 & 10\\ -8 & 6 & 12 & 2\\ 2 & 4 & 18 & -4\\ -10 & 4 & 10 & 8\end{bmatrix}. \qquad (2.27)$$

На основі матриці-контейнера X отримаємо стеганоповідомлення M виконуючи додавання з послідовністю $T=[++--++--++--++--]$, яка являє собою третій рядок матриці Уолша-Адамара порядку $N^2=16$.

Відповідно до встановленої у цьому розділі відповідності між двовимірним і одновимірним перетворенням Уолша-Адамара, представимо зазначену послідовність у вигляді матриці порядку $N = 4$ шляхом її поділу на сегменти довжини $N = 4$ та їх наступної вертикальної конкатенації.

Представимо також результат перетворення Уолша-Адамара (з точністю до коефіцієнта $1/N$) отриманого стеганоповідомлення, обчислений відповідно до (2.5)

$$
\begin{gathered}
M = X + D = \\
= \begin{bmatrix} 127 & 123 & 119 & 119 \\ 124 & 125 & 124 & 124 \\ 123 & 122 & 123 & 124 \\ 123 & 121 & 122 & 125 \end{bmatrix} + \begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \end{bmatrix} = \\
= \begin{bmatrix} 128 & 124 & 118 & 118 \\ 125 & 126 & 123 & 123 \\ 124 & 123 & 122 & 123 \\ 124 & 122 & 121 & 124 \end{bmatrix}; \\
W_M = \begin{bmatrix} 1968 & 2 & 24 & 10 \\ -8 & 6 & 12 & 2 \\ 2 & 4 & 18 & -4 \\ -10 & 4 & 10 & 8 \end{bmatrix}.
\end{gathered}
\tag{2.28}
$$

Аналізуючи (2.23) і (2.24) неважко помітити, що зміни зазнала лише трансформанта Уолша-Адамара (1,3), або відповідна їй третя трансформанта Уолша-Адамара у разі одновимірного уявлення.

Відповідно до даних, представлених на рис. 2.5, зазначена трансформанта Уолша-Адамара відповідає (1,2) трансформанті ДКП, таким чином, вбудовування додаткової інформації збурило, головним чином, цю складову.

Наведений приклад наочно ілюструє теоретичні можливості кодового управління частотними складовими, у які виконується вбудовування інформації.

2.7. Забезпечення стійкості стеганометоду до атаки стисненням

З практичної точки зору інтерес являє побудова кодових слів різної довжини, насамперед практично важливих довжин $4\times4, 8\times8$, що змінюють лише ті складові контейнеру, які були отримані у достатній умові забезпечення надійності стеганоповідомлення до збурних впливів.

Відповідно до встановленої відповідності між двовимірним і одновимірним перетворенням Уолша-Адамара в якості таких кодових слів візьмемо 5, 33, 37 і 1-ший рядки матриці Уолша-Адамара порядку $N^2=64$ (у вигляді відповідних їм матриць порядку $N=8$), для кожної з яких у виразі (2.25) наведемо відповідну матрицю трансформант Уолша-Адамара (з точністю до коефіцієнта $1/N$).

$$T_1^+=\begin{bmatrix}1&1&1&1&-1&-1&-1&-1\\1&1&1&1&-1&-1&-1&-1\\1&1&1&1&-1&-1&-1&-1\\1&1&1&1&-1&-1&-1&-1\\1&1&1&1&-1&-1&-1&-1\\1&1&1&1&-1&-1&-1&-1\\1&1&1&1&-1&-1&-1&-1\\1&1&1&1&-1&-1&-1&-1\end{bmatrix},\quad W_1^+=\begin{bmatrix}0&0&0&0&64&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\end{bmatrix};$$

$$T_2^+=\begin{bmatrix}1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1\\-1&-1&-1&-1&-1&-1&-1&-1\\-1&-1&-1&-1&-1&-1&-1&-1\\-1&-1&-1&-1&-1&-1&-1&-1\\-1&-1&-1&-1&-1&-1&-1&-1\end{bmatrix},\ W_2^+=\begin{bmatrix}0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\64&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\end{bmatrix};\qquad(2.29)$$

$$T_3^+=\begin{bmatrix}1&1&1&1&-1&-1&-1&-1\\1&1&1&1&-1&-1&-1&-1\\1&1&1&1&-1&-1&-1&-1\\1&1&1&1&-1&-1&-1&-1\\-1&-1&-1&-1&1&1&1&1\\-1&-1&-1&-1&1&1&1&1\\-1&-1&-1&-1&1&1&1&1\\-1&-1&-1&-1&1&1&1&1\end{bmatrix},\ W_3^+=\begin{bmatrix}0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&64&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\end{bmatrix};$$

$$T_4^+=\begin{bmatrix}1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1\end{bmatrix},\quad W_4^+=\begin{bmatrix}64&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\end{bmatrix}.$$

Зазначимо також, що крім представлених кодових слів вдається визначити кодові слова, які впливають одночасно на 4 частотні складові, тобто такі, що володіють елементарною структурою $\{N/2(4),0(N-4)\}$.

Ми представляємо у виразі (2.26) зазначені кодові слова довжини $N=64$, що впливають одночасно на складові (1,5), (5,1), (5,5) та (1,1), а також відповідні їм матриці трансформант Уолша-Адамара (з точністю до коефіцієнта $1/N$)

$$
T_5^+ = \begin{bmatrix}
1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1\\
1&1&1&1&-1&-1&-1&-1\\
1&1&1&1&-1&-1&-1&-1\\
1&1&1&1&-1&-1&-1&-1\\
1&1&1&1&-1&-1&-1&-1
\end{bmatrix},\quad
W_5^+ = \begin{bmatrix}
32&0&0&0&32&0&0&0\\
0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0\\
32&0&0&0&-32&0&0&0\\
0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0
\end{bmatrix};
$$

$$
T_6^+ = \begin{bmatrix}
1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1\\
-1&-1&-1&-1&1&1&1&1\\
-1&-1&-1&-1&1&1&1&1\\
-1&-1&-1&-1&1&1&1&1\\
-1&-1&-1&-1&1&1&1&1
\end{bmatrix},\quad
W_6^+ = \begin{bmatrix}
32&0&0&0&-32&0&0&0\\
0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0\\
32&0&0&0&32&0&0&0\\
0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0
\end{bmatrix};
\qquad (2.30)
$$

$$
T_7^+ = \begin{bmatrix}
1&1&1&1&-1&-1&-1&-1\\
1&1&1&1&-1&-1&-1&-1\\
1&1&1&1&-1&-1&-1&-1\\
1&1&1&1&-1&-1&-1&-1\\
1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1
\end{bmatrix}\quad
W_7^+ = \begin{bmatrix}
32&0&0&0&32&0&0&0\\
0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0\\
-32&0&0&0&32&0&0&0\\
0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0
\end{bmatrix};
$$

$$
T_8^+ = \begin{bmatrix}
-1&-1&-1&-1&1&1&1&1\\
-1&-1&-1&-1&1&1&1&1\\
-1&-1&-1&-1&1&1&1&1\\
-1&-1&-1&-1&1&1&1&1\\
1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1
\end{bmatrix}\quad
W_8^+ = \begin{bmatrix}
32&0&0&0&-32&0&0&0\\
0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0\\
-32&0&0&0&-32&0&0&0\\
0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0
\end{bmatrix}.
$$

Окрім розміру кодових слів 8×8, які забезпечують селективний вплив на трансформанти Уолша-Адамара матриці контейнера практичний інтерес являє побудова таких кодових слів розміру 4×4.

Наведемо кодові слова, що дозволяють вбудовувати інформацію в дані коефіцієнти, а також відповідні їм матриці трансформант Уолша-Адамара (з точністю до коефіцієнта $1/N$)

$$
\begin{aligned}
T_1^+ &= \begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \end{bmatrix}, \quad W_1^+ = \begin{bmatrix} 0 & 0 & 16 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}; \\
T_2^+ &= \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \end{bmatrix}, \quad W_2^+ = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}; \\
T_3^+ &= \begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \end{bmatrix}, \quad W_3^+ = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 16 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}; \\
T_4^+ &= \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \quad W_4^+ = \begin{bmatrix} 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.
\end{aligned}
\tag{2.31}
$$

При цьому, як у випадку розміру кодового слова 8×8, можуть бути знайдені кодові слова, що допускають вбудовування інформації у всі обрані чотири частотні складові одночасно (їх трансформанти Уолша-Адамара наведені з точністю до коефіцієнта $1/N$)

$$
\begin{aligned}
T_5^+ &= \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \end{bmatrix}, \quad W_5^+ = \begin{bmatrix} 8 & 0 & 8 & 0 \\ 0 & 0 & 0 & 0 \\ 8 & 0 & -8 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}; \\
T_6^+ &= \begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \quad W_6^+ = \begin{bmatrix} 8 & 0 & 8 & 0 \\ 0 & 0 & 0 & 0 \\ -8 & 0 & 8 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}; \\
T_7^+ &= \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \end{bmatrix}, \quad W_7^+ = \begin{bmatrix} 8 & 0 & -8 & 0 \\ 0 & 0 & 0 & 0 \\ 8 & 0 & 8 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}; \\
T_8^+ &= \begin{bmatrix} -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \quad W_8^+ = \begin{bmatrix} 8 & 0 & -8 & 0 \\ 0 & 0 & 0 & 0 \\ -8 & 0 & -8 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.
\end{aligned}
\tag{2.32}
$$

Аналогічним чином можуть бути побудовані і кодові слова розміру 16×16, які впливають на задані трансформанти перетворення Уолша-Адамара. Для стислості наведемо у вигляді табл. табл. 2.5 із позначенням трансформанті ДКП, на яку здійснює максимальний вплив відповідне кодове слово.

Таблиця 2.5 — Кодові слова розміру 16×16, що здійснюють вплив на задані трансформанти Уолша-Адамара

(1,1)	(1,9)
1 1	1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1
(9,1)	(9,9)
1 -1 -1	1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1
(1,1), (1,9), (9,1), (9,9)	(1,1), (1,9), (9,1), (9,9)
1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1	1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1

Закінчення таблиці 2.5

(1,1), (1,9), (9,1), (9,9)	(1,1), (1,9), (9,1), (9,9)
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	-1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	-1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	-1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	-1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	-1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	-1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	-1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	-1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1
-1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
-1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
-1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
-1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
-1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
-1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
-1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
-1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

Кодові слова (2.29), (2.30) розміру 8×8, (2.31, 2.32) розміру 4×4, а також табл. 2.5 є основою для подальшої побудови стеганографічного методу з кодовим управлінням вбудовуванням.

2.8. Висновки

В розділі розроблені теоретичні основи для побудови ефективних стеганографічних методів, що задовольняють певним вимогам, з використанням перетворення Уолша-Адамара, ході чого:

1. Встановлено зв’язок між трансформантами перетворенням Уолша-Адамара та коефіцієнтами дискретного косинусного перетворення, який теоретично обґрунтований двома способами: за допомогою врахування відповідності між функціями Уолша-Адамара та гармоніками, а також шляхом встановлення відповідності між двовимірним та одновимірним перетворенням Уолша-Адамара. Обидва способи дали однакові результати, що підтверджуються проведеними емпіричними дослідженнями. При цьому в роботі виведена конкретна локалізація трансформант, які відповідають високочастотним, низькочастотним складникам для матриць Уолша-Адамара практично цінних розмірів $N = 4,8,16$.

2. Встановлено звязок трансформант перетворення Уолша-Адамара та сингулярних трійок (блоків) матриці ЦЗ, що дало можливість, використовуючи існуючу достатню умову забезпечення надійності сприйняття стеганоповідомлення в області сингулярного розкладання матриці, розширити область можливих збурень в результаті стеганоперетворення, в порівнянні з тією, що визначалася лише високочастотними складовими.

3. На підставі проведених досліджень одержано достатню умову забезпечення надійності сприйняття стеганоповідомлення в області перетворення Уолша-Адамара, яка може бути використана незалежно від того, в якій області контейнера (просторовій, перетворення) відбувається вбудовування додаткової інформації. Отримана достатня умова дозволяє зробити висновки про можливу з великою ймовірністю появу артефактів на зображенні, кадрі цифрового відео, у тому числі, у малій локальній області (аж до зміни одного пікселя), навіть у тому випадку, коли візуально під час перегляду ЦЗ зроблені зміни не візуалізуються.

4. На підставі проведених досліджень одержано достатню умову забезпечення нечутливості стеганоповідомлення до збурних дій, насамперед, таких як стиснення із втратами, накладання шуму та розмиття в області перетворення Уолша-Адамара, яке може бути використане незалежно від того, в якій області контейнера (просторовій, перетворення) відбувається вбудовування додаткової інформації.

5. Сформовано теоретичний базис кодового управління вбудовуванням інформації, сутність якого полягає в попередньому кодуванні ДІ за допомогою кодових слів із заданими властивостями трансформант Уолша-Адамара, вбудовування яких призводить до строго певного впливу на трансформанти Уолша-Адамара, і, відповідно, на трансформанти ДКП контейнеру. Таким чином, маніпулюючи властивостями застосовуваних кодів, стає можливим впливати на властивості стеганоповідомлення,

наприклад, на його здатність протистояти атаці стисненням, в просторовій області контейнера.

Отримані в даному розділі результати, у сукупності з перевагами перетворення Уолша-Адамара, такими як приналежність елементів його базисних векторів бінарному алфавіту, а також простота побудови матриць перетворення, зумовлюють перспективність розвитку та практичного застосування перетворення Уолша-Адамара для оцінки ефективності існуючих та розробки нових перспективних методів стеганографії та стеганоаналізу.

Список використаних джерел у другому розділі

1. Lu Leng, Jiashu Zhang, Jing Xu et al. Dynamic weighted discrimination power analysis: A novel approach for face and palmprint recognition in DCT domain. International Journal of Physical Sciences. 2010. No. 5(17) P.467 – 471.

2. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности. К.: Изд. ГУИКТ, 2009. 251 с.

3. Towards robust image steganography / J. Tao et al. *IEEE Transactions on Circuits and Systems for Video Technology*. 2019. 29(2). P. 594–600.

4. Veena S.T., Arivazhagan S. Universal secret payload location identification in spatial LSB stego images. *Annals of Telecommunications*. 2019. 74. P. 273–286.

5. Dai H., Cheng J., Li Y. A Novel Steganography Algorithm Based on Quantization Table Modification and Image Scrambling in DCT Domain. *International Journal of Pattern Recognition and Artificial Intelligence*. 2021. Vol. 35. No. 01. P. 2154001.

6. Khatavkar M. M. D., MALI A. S. A Image Security with Image Steganography Using Dct Coefficient and Encryption. *International Journal of Innovations in Engineering Research and Technology*. 2021. Vol. 3. No. 9. P. 1-8.

7. Kaur R., Singh B. A hybrid algorithm for robust image steganography. *Multidimensional Systems and Signal Processing*. 2021. Vol. 32. No. 1. P. 1-23.

8. Vakani H. et al. DCT-in-DCT: A Novel Steganography Scheme for Enhanced Payload Extraction Quality. *IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT)*. IEEE, 2021. P. 201-206.

9. Chowdhuri P., Jana B., Giri D. Secured steganographic scheme for highly compressed color image using weighted matrix through DCT. *International Journal of Computers and Applications*. 2021. Vol. 43. No. 1. P. 38-49.

10. Sheidaeian H., Zolfaghari B., Zobeiri M. An Efficient and Secure Approach to Multi-User Image Steganography Using CRC-Based CDMA. *International Conference on Signal Acquisition and Processing*. Singapore, 2011. Vol. 2. P. 1-5.

11. Bhattacharyya S., Mondal S., Sanyal G. A Robust Image Steganography using Hadamard Transform. *International Conference on Information Technology in Signal and Image Processing*. Mumbai, 2013. P. 416-426.

12. Karampidis K., Kavallieratou E., Papadourakis G. A review of image steganalysis techniques for digital forensics. *Journal of Information Security and Applications.* 2018. 40. P. 217–235.

13. Saleh M.E., Aly A.A., Omara F.A. Data security using cryptography and steganography techniques. *International Journal of Advanced Computer Science and Applications*. 2016. 7(6).P. 390–397.

14. A. Yahya, "Steganography Techniques", Steganography Techniques for Digital Images, pp. 9-42, 2019.

15. Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 472 с.

16. Мазурков М.И. Системы широкополосной радиосвязи. Одесса : Наука и Техника, 2010. с. 340

17. Баженов А.В. Цифровые методы реализации пространственно-временной обработки сигналов в авиационных радиоэлектронных комплексах. Ставрополь: СВВАИУ, 2006. 219 с.

18. NRCS Photo Gallery // United States Department of Agriculture. URL: https://www.nrcs.usda.gov/wps/portal/nrcs/main/national/newsroom/multimedia/

19. Gloe T., Böhme R. The “Dresden Image Database” for benchmarking digital image forensics. Proceedings of the 2010 ACM Symposium on Applied Computing (SAC 10). New York, 2010.P. 1585–1591.

20. Hsu Y., Chang S. Detecting image splicing using geometry invariants and camera characteristics consistency. 2006 IEEE International Conference on Multimedia and Expo, Toronto, 2006.P. 549–552.

21. Деммель Дж. Вычислительная линейная алгебра / Дж.Деммель; пер.с англ. Х.Д.Икрамова. М.: Мир, 2001. 430 с.

22. Гонсалес Р., Вудс Р. Цифровая обработка изображений. М.: Техносфера, 2012. 1104 с.

23. Нариманова и др. Методика количественной оценки надежности восприятия цифрового изображения. 2014. ИМММ. Т.4, №4, С. 332-336.

24. Мерзлякова Е. Ю. Построение стеганографических систем для растровых изображений, базирующихся на теоретико-информационных принципах: автореферат диссертации на соискание ученой степени кандидата технических наук, специальность 05.13.19 – Методы и системы защиты информации. Информационная безопасность. Сибирский государственный университет телекоммуникаций и информатики. Новосибирск, 2011. 16 с.

Розділ 3.

РОЗРОБКА СТЕГАНОГРАФІЧНИХ МЕТОДІВ З КОДОВИМ УПРАВЛІННЯМ ВІБУДОВУВАННЯ ДОДАТКОВОЇ ІНФОРМАЦІЇ

В даний час існує і розробляється велика кількість стеганографічних методів, які ґрунтуються на різних математичних конструкціях і перетвореннях. Однак, саме використання властивостей перетворення Уолша-Адамара для побудови та дослідження стеганографічних методів, що працюють у просторовій (часовій) області є перспективним з огляду на максимальне спрощення алгоритмічної реалізації таких стеганографічних методів та зниження обчислювальних ресурсів, що необхідні для вбудовування та вилучення додаткової інформації.

Наукові експерименти, проведені в Розділі 2 чітко вказують на те, що використання саме властивостей перетворення Уолша-Адамара може слугувати базисом для побудови стеганографічних методів, що здійснюють вбудовування додаткової інформації у просторовій (часовій) області та дозволяють отримати стійкість стеганоповідомлень до можливих збурних дій, наприклад, атак стисненням із втратами, зашумленням та розмиттям стеганоповідомлення.

Метою цього розділу є розробка стеганоперетворення просторової області ЦЗ з кодовим управлінням, яке дозволить забезпечити певні властивості метода.

Для досягнення мети розділу необхідно вирішити наступні задачі:

1. розробити стеганоперетворення просторової області ЦЗ з кодовим управлінням, заснованим на властивості лінійності перетворення Уолша-Адамара, яке дозволить забезпечити певні властивості метода.

2. ввести та дослідити показники енергії та селективності кодових слів, що застосовуються в методі з кодовим управлінням вбудовуванням інформації;

3. розробити та синтезувати багаторівневі кодові слова для стеганоперетворення з кодовим управлінням, які забезпечать підвищену стійкість до збурних дій;

4. провести оцінку ефективності, в тому числі, порівняльну, алгоритмічної реалізації методу в умовах різноманітних атак проти вбудованого повідомлення;

3.1. Розробка стеганографічного методу, стійкого до атак проти вбудованого повідомлення

Вбудовування ДІ може здійснюватися в різних областях контейнера: просторовій (часовій) [1…10], областях різних перетворень, зокрема, частотній [11…19], області сингулярного (спектрального розкладання) відповідних матриць [20…23], області перетворення Уолша-Адамара [24, 25] та ін.

Класичним стеганографічним методом прийнято вважати метод LSB [26], в основі якого лежить модифікація одного або кількох найменших значущих біт значень яскравості пікселів зображення. До безперечних переваг цього методу необхідно віднести гарантоване забезпечення надійності сприйняття стеганоповідомлення, а також простоту реалізації процедури вбудовування та вилучення інформації. Недоліками зазначеного методу є його нестійкість до атак проти вбудованого повідомлення, зокрема до найпоширенішої на сьогоднішній день атаки стисненням.

Стійкість стеганометода забезпечується, як правило, в областях перетворення ЦЗ, хоча така вимога, зважаючи на [27], не є необхідною, більше того, використання області різних перетворень, як зазначено в роботі

[28], підвищує обчислювальну складність алгоритму через необхідність переходу з просторової області в область обраного перетворення та назад, а також сприяє накопиченню додаткової обчислювальної похибки, що ускладнює використання таких методів у режимі реального часу. Основною причиною переваги використання вбудовування ДІ у областях перетворення контейнера, очевидно, є той факт, що забезпечити тут стійкість методу до атак проти вбудованого повідомлення легше, ніж у просторовій області [28], спираючись на наявні достатні умови такої стійкості, проте не існує жодних принципових заперечень для забезпечення стійкості до збурних дій при організації стеганоперетворення в просторовій області контейнера.

Дослідження, представлені в цьому розділі, показують можливості використання властивостей перетворення Уолша-Адамара для побудови нового стеганографічного методу, що працює в просторовій області контейнера, який поєднує забезпечення високої надійності сприйняття, властивої методу LSB, а також високу стійкість до атак, спрямованих на руйнування стеганоповідомлення, насамперед, до атаки стисненням.

Розроблений у даному розділі метод, на відміну від відомих аналогів, заснованих на вбудовуванні інформації в області сингулярного розкладання блоків зображення [20…22], характеризується значно більш високою надійністю сприйняття стеганоповідомлення, тоді як на відміну від методу [4] — більшою стійкістю стеганоповідомлення до атак стисненням. Крім того, розроблений метод, на відміну від аналогів [4, 20…22], виконує вбудовування та вилучення додаткової інформації в просторовій області, що зумовлює ефективність його алгоритмічної реалізації та високу швидкодію.

Вбудовування ДІ

Крок 1. Виконуємо сегментацію вихідного зображення P розміру $m \times n$ на блоки $\mu \times \mu$.

Крок 2. Кожному блоку вихідного зображення $\mu \times \mu$, задіяному в процесі стеганоперетворення, ставимо у відповідність λ біт ДІ, таким чином

отримуємо матрицю ДІ D розміру $\frac{m}{\mu}\times\frac{n}{\mu}$, кожен елемент якої містить λ біт інформації. При цьому $\lambda=\log_2 J$, де J — кількість кодових слів, що використовуються.

Крок 3. Будуємо таблицю відповідності половини комбінацій із λ біт ДІ кодовим словам $\{T_i^+\}$, тоді як друга половина комбінацій із λ біт ДІ кодується за допомогою інверсій кодових слів $\{T_i^-\}$. Відзначимо, що така таблиця може бути частиною ключа. Отримуємо закодовану матрицю ДІ шляхом подання кожного її елемента з λ біт ДІ за допомогою кодових слів $\{T_i^+\}$ та $\{T_i^-\}$.

Крок 4. Виконуємо вбудовування інформації шляхом підсумовування матриці контейнера P з кодовою матрицею, що була отримана на *Кроці 3*, в результаті чого отримуємо стеганоповідомлення M, тобто

$$M = P + D. \tag{3.1}$$

Декодування ДІ

Крок 1. Вилучення інформації відбувається шляхом віднімання з матриці можливо збуреного стеганоповідомлення $\overline{M}$ матриці контейнера P, що є частиною секретного ключа. В результаті вилучення, для кожного i-го блоку розміру $\mu\times\mu$ отримуємо матрицю Δ_i

$$\{\Delta_i\}=\overline{M}-P,\quad i=0,1,...,mn-1. \tag{3.2}$$

Крок 2. Для кожної матриці T_i^+ робимо поелементне множення кожної отриманої на *Кроці 1* матриці Δ_i на матрицю T_i^+, після чого знаходимо суму всіх елементів результуючої матриці кожного кодового слова T_i^+, тобто розраховуємо значення $\sigma_j=\sum_{l=0}^{\mu-1}\sum_{k=0}^{\mu-1}\Delta_i(l,k)T^+(l,k),\ j=0,1,...,J/2-1.$

Крок 3. Серед отриманої для кожного блоку множини значень σ_j знаходимо максимальне за модулем значення. При цьому індекс знайденого значення буде відповідати індексу декодованого кодового слова $T_i^?$, в той час

як знак знайденого максимуму буде відповідати знаку, з яким вказане кодове слово було вбудовано (прямий або інверсний вигляд).

Зазначимо, що *Крок 2* та *Крок 3* у частині декодування ДІ в представленому методі, по суті, реалізують алгоритм оптимального прийому [29].

Зауваження. Зважаючи на те, що більшість використовуваних зображень сьогодні представлені з використанням моделі RGB, де для кодування кожного кольору відводиться 1 байт (кожна складова кольору представляється числами в діапазоні $[0,...,255]$), у разі наявності в блоці граничних для даного діапазону значень (0 або 255), вказаний блок не використовується в процесі стеганоперетворення у разі застосування розробленого стеганографічного методу.

Ґрунтуючись на запропонованому стеганографічному методі, представимо на рис. 3.1 загальну структурну схему стеганографічної системи з кодовим управлінням частотними складовими.

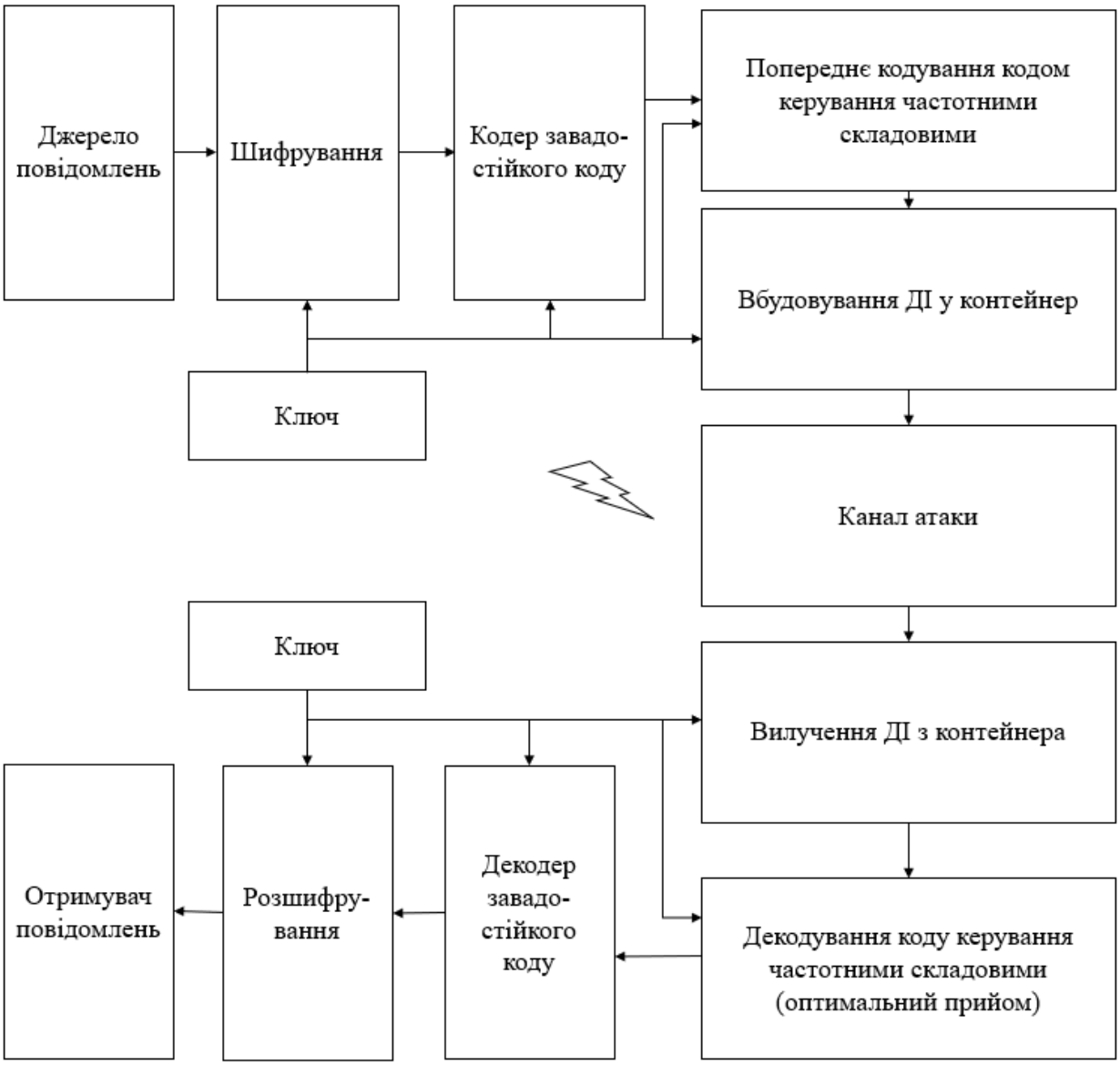


Рис. 3.1. — Структурна схема стеганографічної системи з кодовим управлінням вбудовуванням інформації

Експеримент 1.1. Заданням даного експерименту є дослідження стійкості стеганографічного методу з кодовим управлінням при вбудовуванні інформації за допомогою кодових слів (2.29) та (2.30), що здійснюють вплив на різні трансформанти Уолша-Адамара. Для здійснення експерименту було обрано базу NRCS [30] з 500 зображень у форматі TIFF. Після цього кожне зображення було сегментоване на блоки 8×8, у кожний з яких вбудовувався $\lambda=1$ біт ДІ.

На рис. 3.2. представлені графіки залежності кількості помилок, що виникають (у відсотках від загальної кількості біт ДІ) від степеню стиснення QF зображення алгоритмом JPEG для кожної з розглянутих трансформант Уолша-Адамара, що дозволяє оцінити ефективність їх використання для протистояння атакам стисненням на стеганоповідомлення. При цьому, через те, що всі кодові слова (2.30), які використовують одночасно всі частотні складові показують практично еквівалентні результати, на графіку (рис. 3.2) вони показані однією кривою.

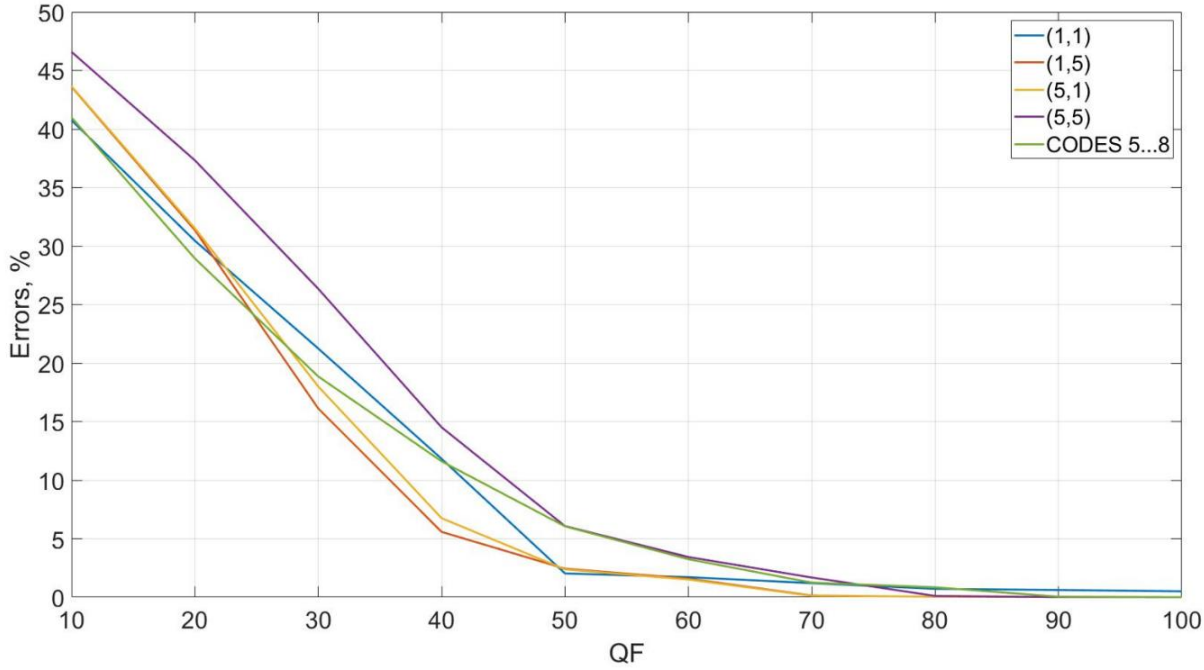


Рис. 3.2. — Графік залежності кількості помилок, що виникають, від степеню QF стиснення стеганоповідомлення алгоритмом JPEG для різних трансформант Уолша-Адамара, в які здійснюється вбудовування

Аналіз даних, представлених на рис. 3.2 показує, що вбудовування інформації як з використанням кодових слів (2.29), так і кодових слів (2.30) формує стеганоповідомлення, нечутливе до атаки стисненням. При цьому, при стисненні з коефіцієнтом QF=60% (на практиці вкрай нечасто використовуються більші степені стиснення), відсоток помилок, що

виникають, не перевищує 5%, що є показником високої стійкості стеганографічного методу.

Фізична сутність стійкості запропонованого методу до атак стисненням полягає в накопиченні енергії сигналу, що вбудовується, у заданій частотній складовій блоку, незважаючи на те, що амплітуда впливу на кожен окремий піксель є незначною (± 1). Такий спосіб вбудовування інформації дозволяє досягти високих показників стійкості до атаки стиском при гарантованому збереженні високого рівня надійності сприйняття, порівнянного з рівнем, що забезпечується методом LSB-matching.

Зворотною стороною збільшення стійкості запропонованого методу є зменшення його пропускної спроможності порівняно з методом LSB-matching. Тим не менш, оскільки пропускна здатність запропонованого методу визначається параметром λ, для конкретної алгоритмічної реалізації вона може бути підвищена за рахунок збільшення числа біт, що вбудовуються в кожен блок повідомлення.

Експеримент 1.2. Завданням даного експерименту є дослідження стійкості стеганографічного методу з кодовим управлінням при вбудовуванні більше одного біту інформації на блок. В якості бази експерименту використовувалися 500 зображень NRCS у форматі TIFF, в кожне з яких виконувалося вбудовування інформації. Зазначимо, що для значення $\lambda = 1$ вбудовування виконувалося за допомогою кодового слова (1,5), тоді як при $\lambda = 2,3$ використовувалися кодові слова (2.30), а при $\lambda = 4$ використовувалися всі кодові слова (2.29) і (2.30).

На рис. 3.3 показаний графік залежності кількості помилок, що виникли при декодуванні ДІ, від степені *QF* стиснення зображення-стеганоповідомлення алгоритмом JPEG при різних значеннях кількості вбудованих біт λ в блок зображення, що визначають різні значення пропускної спроможності λ / μ^2.

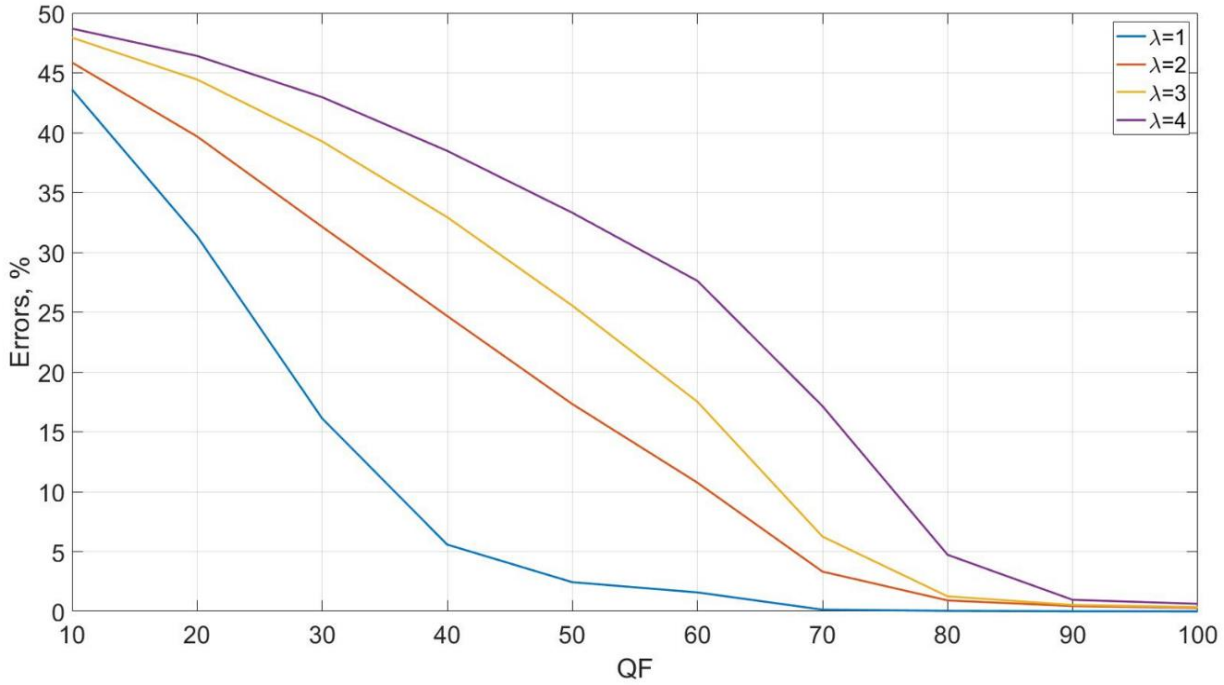


Рис. 3.3. — Графік залежності кількості помилок, що виникають, від степеню QF стиснення стеганоповідомлення алгоритмом JPEG для різних значень λ

Аналіз даних, представлених на рис. 3.3. показує очікуване збільшення кількості помилок, зі збільшенням пропускної спроможності, яке обумовлено появою шумів неортогональності зі збільшенням кількості застосовуваних кодових слів. Таким чином, значення $\lambda>1$ можуть використовуватися у разі необхідності організації стеганографічних каналів передачі інформації з високими вимогами до пропускної спроможності, і невисокими вимогами до якості передачі інформації**.** Зазначимо, що крім збільшення кількості біт, що вбудовуються в один блок контейнера, для підвищення пропускної спроможності може бути зменшений розмір блоку μ, в який відбувається вбудовування кванта інформації.

Експеримент 1.3. Завданням даного експерименту є дослідження стійкості методу з кодовим управлінням при використанні кодових слів розміру 4×4. В якості бази експерименту використовувалася база NRCS з 500 зображень у форматі TIFF, в кожне з яких виконувалося вбудовування додаткової інформації із використанням кодових слів (2.31) та (2.32). При

цьому кодові слова (2.32) відповідають одній кривій на графіці рис. 3.4., зважаючи на їх подібні результати.

На рис. 3.4. представлені графіки залежності кількості помилок під час декодування інформації при її кодуванні кодовими словами розміру 4×4.

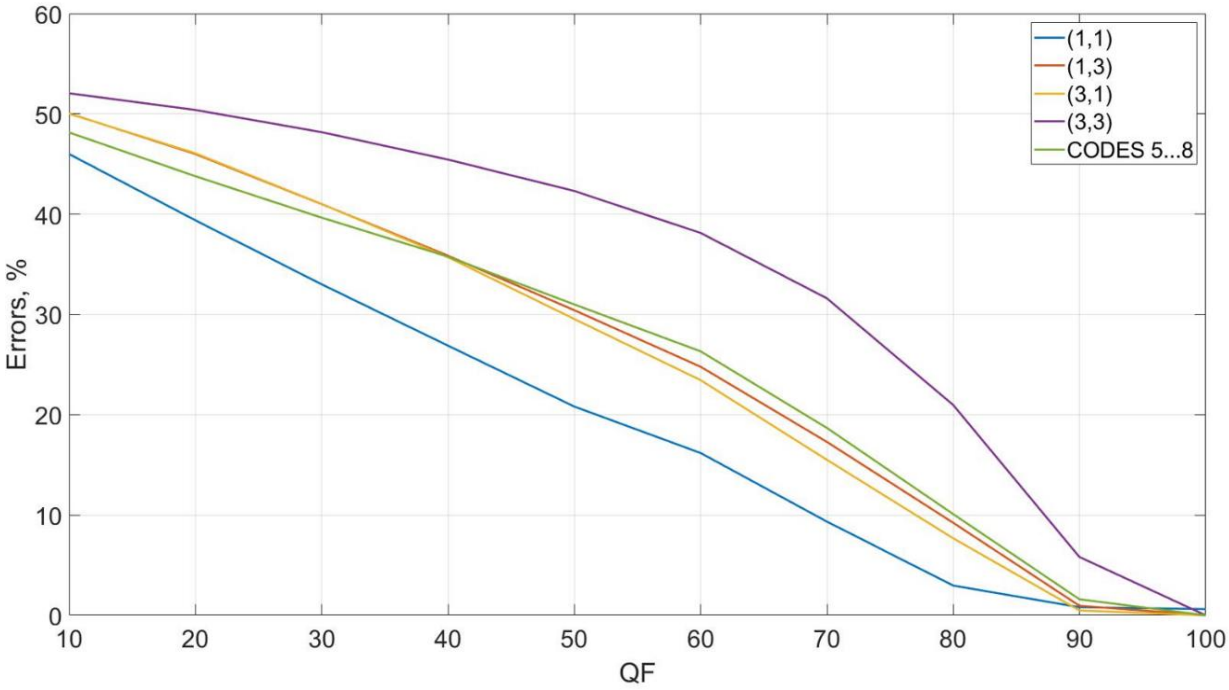


Рис. 3.4. — Графік залежності кількості помилок, що виникають, від степеню QF стиснення зображення алгоритмом JPEG для $\mu=4$

Аналіз даних, представлених на рис. 3.4. показує, що при пропускній спроможності $1/16$ при використанні кодового слова T_4^+, $\mu=4$, стійкість стеганографічного каналу до стиснення алгоритмом JPEG навіть перевершує стійкість стеганографічного каналу при використанні всіх кодових слів (2.29) і (2.30) для досягнення значень $\lambda=4$, $\mu=8$. Таким чином, для досягнення значення пропускної спроможності рівного $1/16$, використання кодового слова T_4^+ і значення $\mu=4$ є більш доцільним, ніж використання значення розміру блоку $\mu=8$. Тим не менш, використання кодових слів T_1^+, T_2^+ і $T_5^+, T_6^+, T_7^+, T_8^+$ показує практично подібні результати з випадком застосування

розробленого методу з параметрами $\lambda=4$, $\mu=8$, в той час як використання кодового слова T_3^+ при $\mu=4$ показує найгірші результати.

Експеримент 1.4. Завданням даного експерименту є дослідження стійкості стеганографічного методу з кодовим управлінням при використанні кодових слів розміру 16×16. В якості бази експерименту використовувалася база NRCS [30] з 500 зображень у форматі TIFF, в кожне з яких виконувалося вбудовування додаткової інформації із використанням кодових слів табл. 2.5. На рис. 3.5. представлено графік залежності кількості помилок при декодуванні вбудованого повідомлення від степеню стиснення стеганоповідомлення алгоритмом JPEG під час проведення атаки.

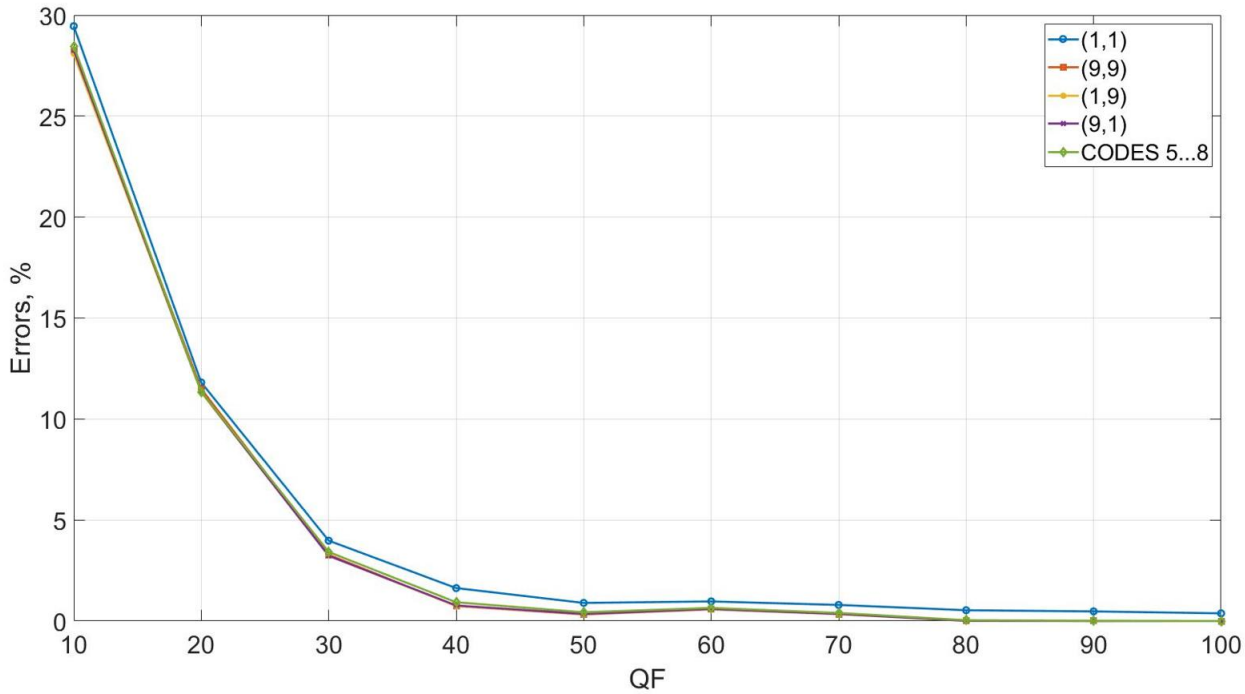


Рис. 3.5 — Графік залежності кількості помилок, що виникають, від степеню QF стиснення зображення алгоритмом JPEG для $\mu=16$

Аналіз даних рис. 3.5 дозволяє дійти висновку, що використання кодових слів розміру 16×16 забезпечує високий рівень стійкості розробленого стеганографічного методу. Так, навіть при атаці з рівнем стиску $QF=30$ для будь-якого кодового слова кількість помилок при декодуванні не перевищує 5%.

Однак, така стійкість досягається за рахунок зниження пропускної спроможності стеганографічного методу до значення $1/256$.

Експеримент 1.5. Завданням даного експерименту є дослідження стійкості стеганографічного методу з кодовим управлінням до атак зашумленням. В якості бази експерименту використовувалася база NRCS [30] з 500 зображень у форматі TIFF, в кожне з яких виконувалося вбудовування інформації за допомогою кодових слів розмірів μ={4,8,16}, після чого зображення піддавалося зашумленню гаусівським шумом з математичним очікуванням $M[X]=0$ і дисперсією $D[X]=\sigma^2$, а також шумом типу «salt&pepper». Після зашумлення виконувалося вимірювання PSNR зашумленого зображення по відношенню до вихідного відповідно до формули

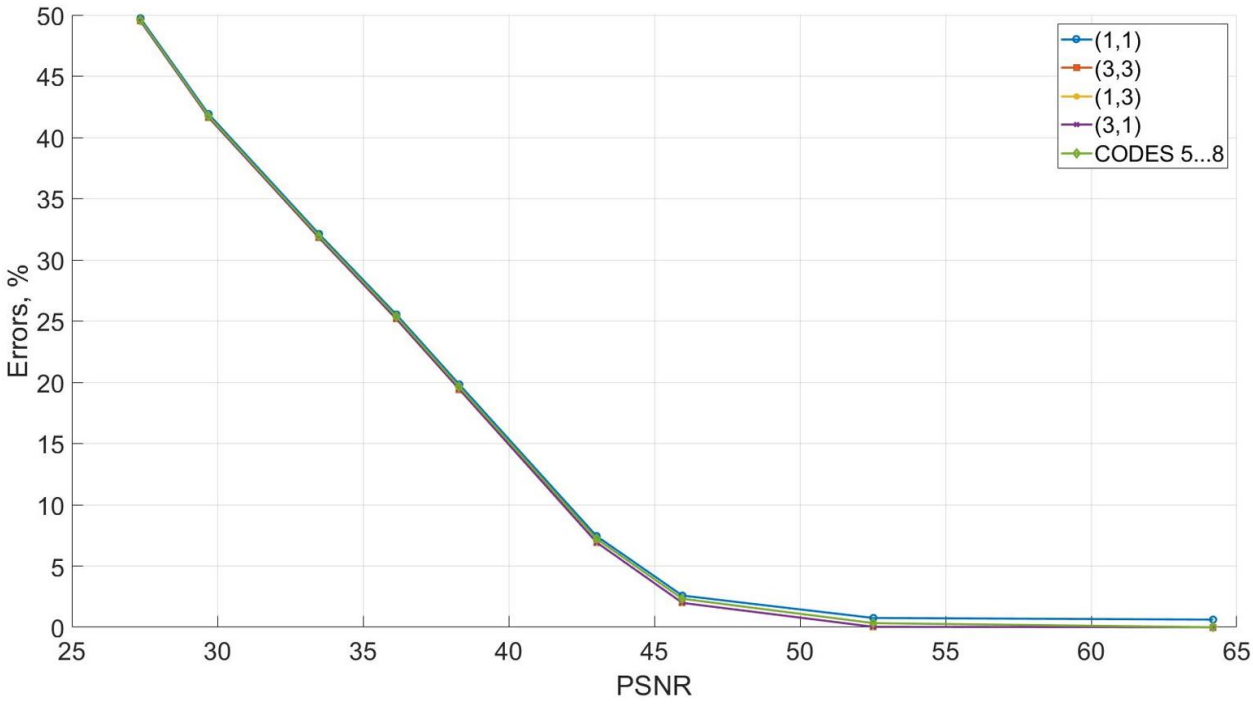
$$PSNR = 20\lg\left(\frac{255}{\sqrt{MSE}}\right), \tag{3.3}$$

де

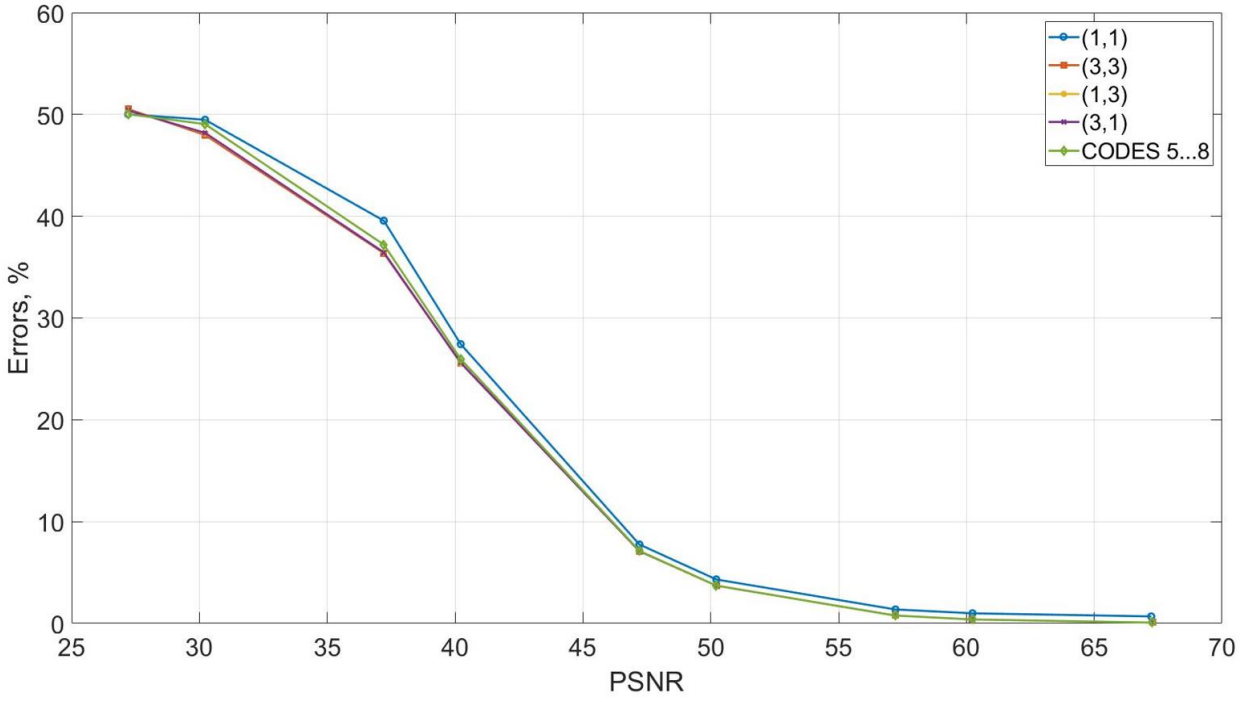
$$MSE = \frac{1}{nm}\sum_i\sum_j \left|X(i,j) - M(i,j)\right|^2, \tag{3.4}$$

а також здійснювалося вилучення ДІ з зашумленого стеганоповідомлення з вимірюванням кількості помилок при декодуванні.

На рис. 3.6. показано графік залежності кількості помилок при декодуванні ДІ при її вилученні від степеню зашумленості стеганоповідомлення гаусівським шумом (а) та шумом типу «salt&pepper» (б), який виражено у PSNR для блоків розміру 4×4 при використанні гаусівського шуму.



а)

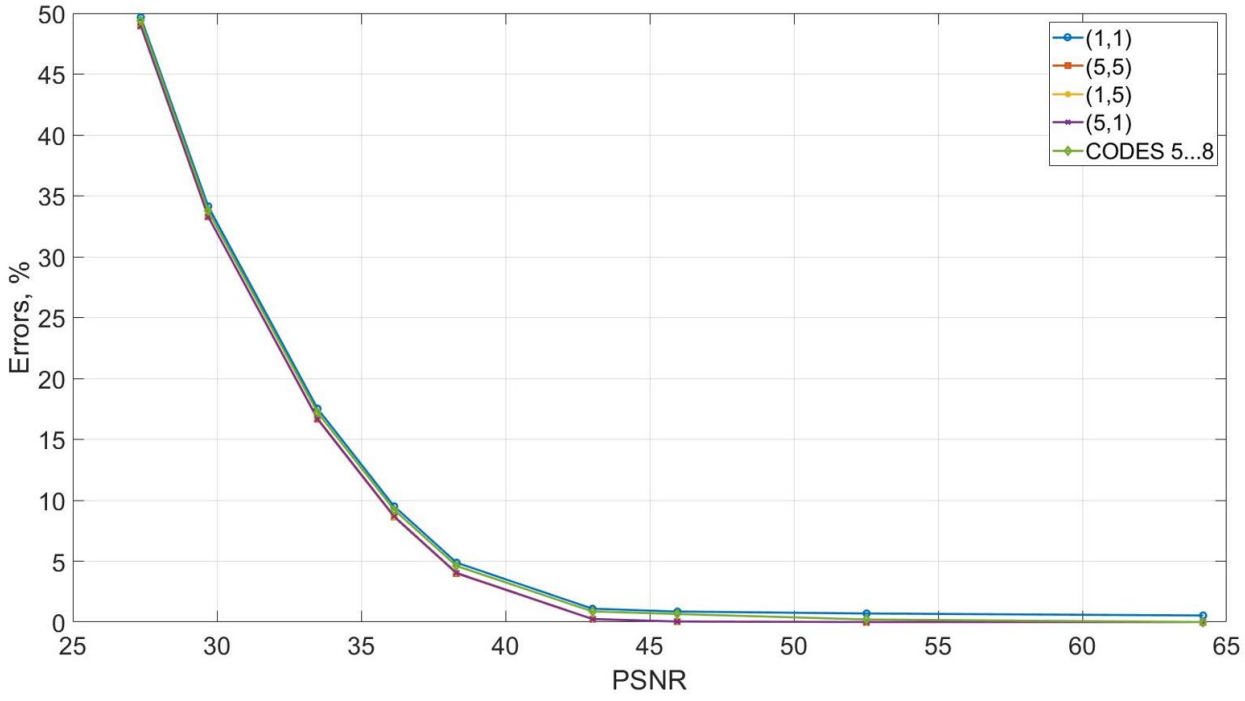


б)

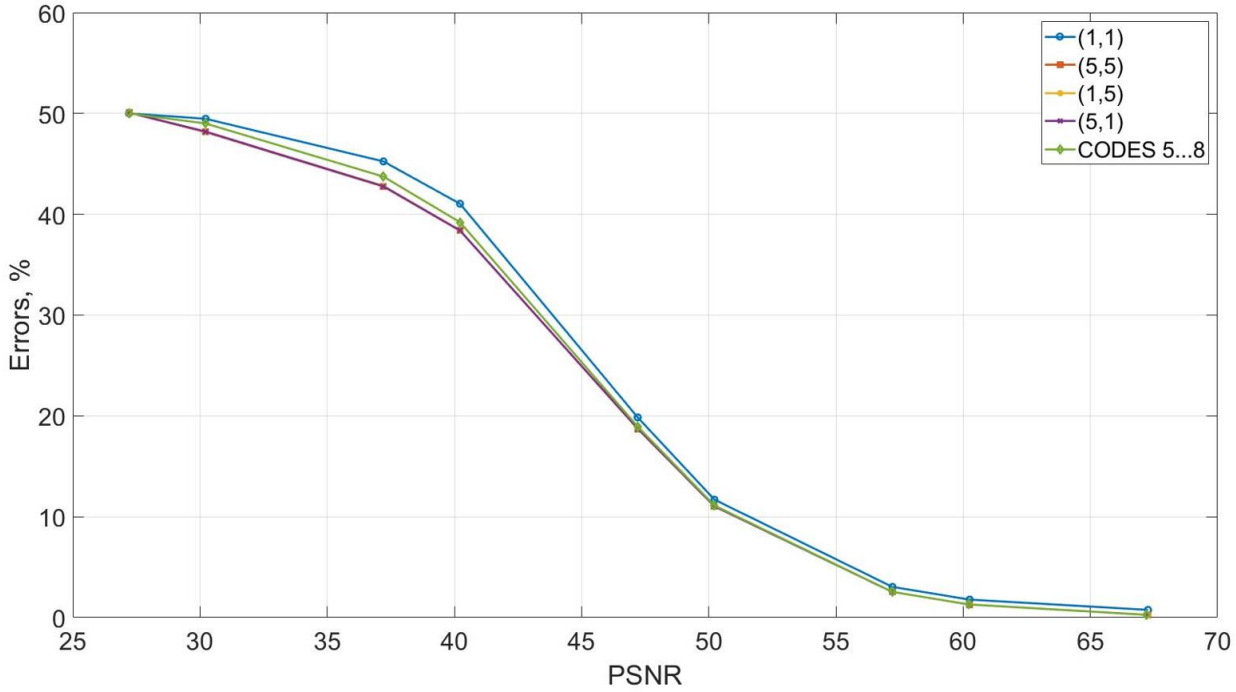
Рис. 3.6. — Графік залежності кількості помилок при декодуванні зашумленого стеганоповідомлення від PSNR при використанні кодових слів розміру 4×4: а) — зашумлення гаусівським шумом, б) — зашумлення шумом типу «salt&pepper»

Аналіз даних рис. 3.6. показує, що практично всі досліджені кодові слова розміру 4×4 дають ідентичний рівень захисту від гаусівського шуму та шуму типу «salt&pepper», та дозволяють декодувати ДІ при спотворенні стеганоповідомлення до рівня $PSNR = 50$ дБ з кількістю помилок, що не перевищує 5%.

На рис. 3.7 показано графік залежності при декодуванні ДІ при її вилученні від степеню зашумленості стеганоповідомлення гаусівським шумом (а) та шумом типу «salt&pepper» (б), який виражено у PSNR для блоків розміру 8×8.



а)

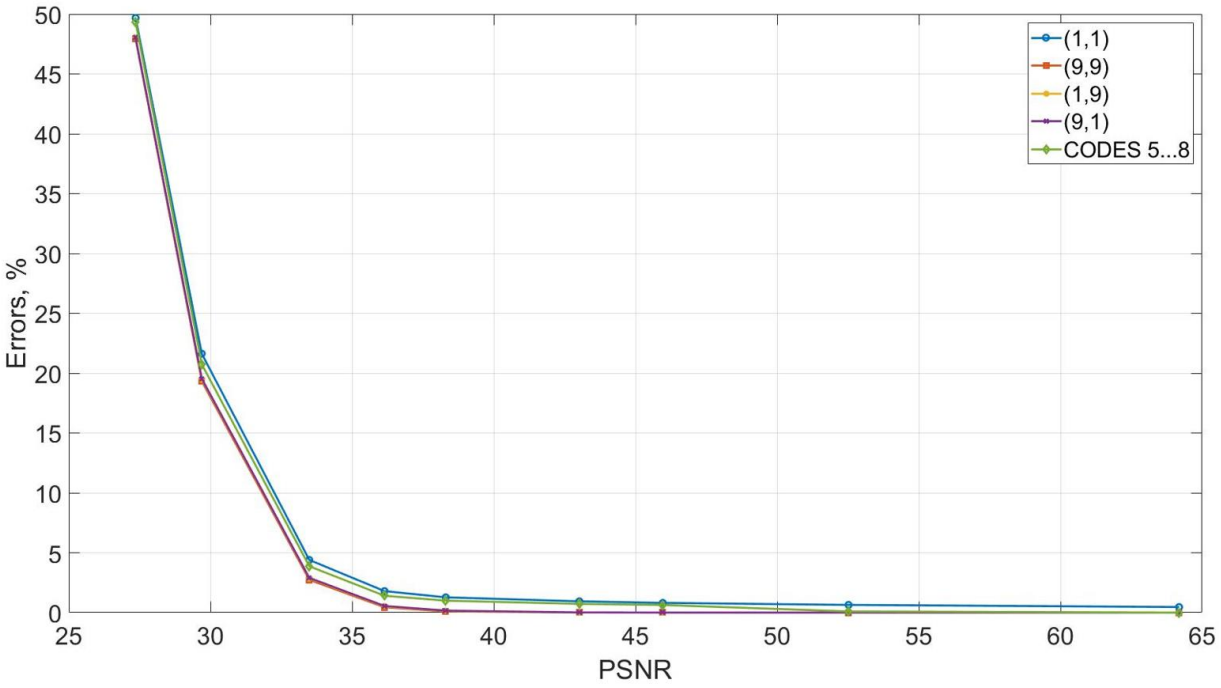


б)

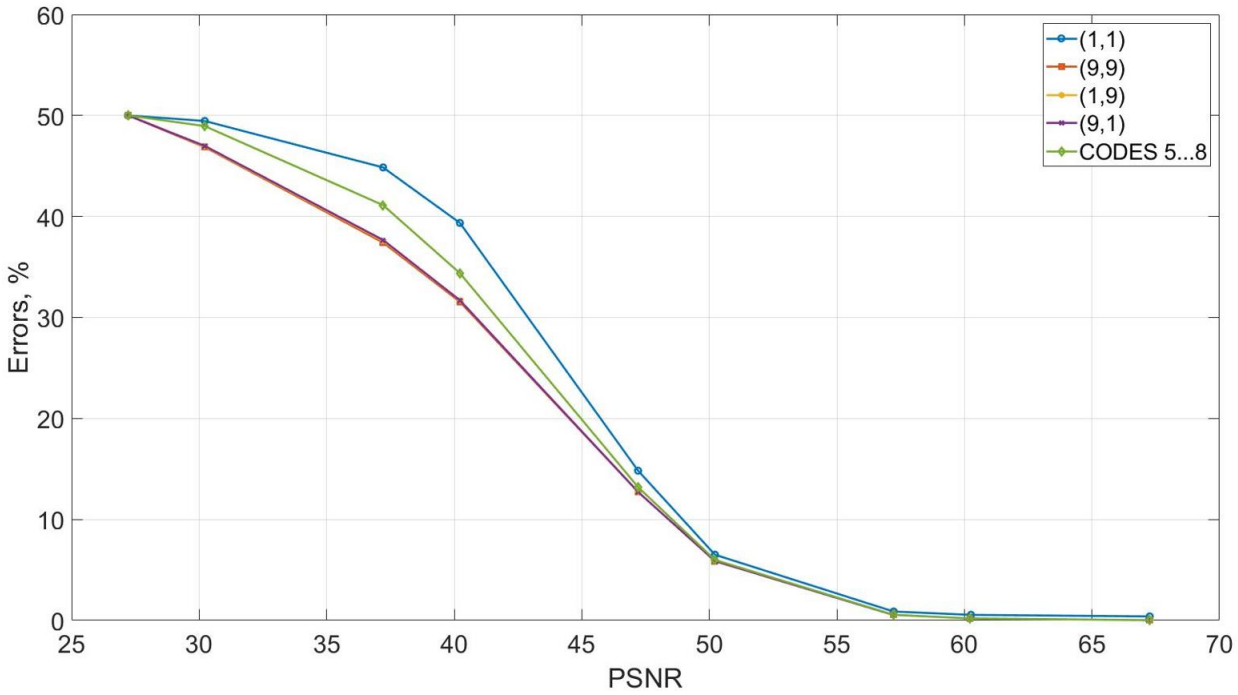
Рис. 3.7. — Графік залежності кількості помилок при декодуванні зашумленого стеганоповідомлення від PSNR при використанні кодових слів розміру 8×8: а) — зашумлення гаусівським шумом, б) — зашумлення шумом типу «salt&pepper»

Аналіз даних, представлених на рис. 3.7 показує, що розроблений стеганографічний метод з кодовим управлінням забезпечує рівень стійкості до виникнення помилок у стеганоповідомленні на рівні менше за 5% при зашумленні гаусівським шумом з $\mathrm{PSNR} = 43$ дБ або зашумленні на рівні $\mathrm{PSNR} = 57$ дБ для випадку шуму «salt&pepper».

На рис. 3.8 показано графік залежності при декодуванні ДІ при її вилученні від степеню зашумленності стеганоповідомлення, який виражено у PSNR для блоків розміру 8×8 при використанні гаусівського шуму (а) та шуму типу «salt&pepper» (б).



а)

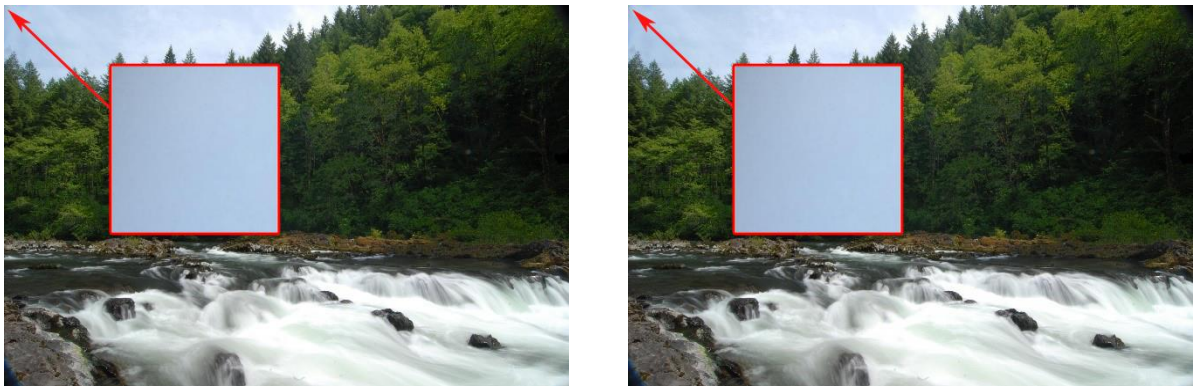


б)

Рис. 3.8. — Графік залежності кількості помилок при декодуванні зашумленного стеганоповідомлення від PSNR при використанні кодових слів розміру 16×16 : а) — зашумлення гаусівським шумом, б) — зашумлення шумом типу «salt&pepper»

Аналіз даних, представлених на рис. 3.8. показує, що стійкість стеганографічного методу з кодовим управлінням на рівні 5% помилок, що виникають при декодуванні, досягається навіть при зашумленні стеганоповідомлення гаусівським шумом до рівня $\mathrm{PSNR} = 34$ дБ, або $\mathrm{PSNR} = 55$ дБ для випадку зашумлення шумом «salt&pepper».

На рис. 3.9 представлений приклад вбудовування ДІ в контейнер за допомогою розробленого стеганографічного методу, при цьому використані параметри $\lambda = 1$, $\mu = 8$, а також для вбудовування інформації застосовано кодове слово T_2^+. Розмір контейнера становить 2592x3872, при цьому вбудовування інформації відбувалося в кожну колірну складову. Таким чином, загальний обсяг вбудованої інформації для даного контейнера склав 470 448 біт.



а) б)

Рис. 3.9. — Приклад використання розробленого стеганографічного методу: а) контейнер; б) стеганоповідомлення

Суб'єктивне ранжування зображень, що представлені на рис. 3.9. не дозволяє виявити артефакти, або будь-які інші відмінності стеганоповідомлення від вихідного контейнера. Даний факт є очікуваним, оскільки результатом стеганоперетворення є збурення значень яскравості пікселів контейнера на ± 1.

Зауваження. Обчислювальна складність алгоритмічної реалізації розробленого методу визначається кількістю блоків, що використовуються в процесі стеганоперетворення, і в найгіршому випадку складе $\underline{O}(nm)$ операцій. З урахуванням блоковості методу очевидним є його внутрішній паралелізм, що разом із використанням просторової області для стеганоперетворення забезпечує потенційну можливість його використання в режимі реального часу для потокового контейнера.

3.2. Теоретичні основи формування ефективних кодових слів для стеганографічного методу з кодовим управлінням

Застосування методу кодового управління вбудовуванням передбачає використання в якості матриці D розміру $\mu \times \mu$ у (3.1), яка є результатом кодування біта ДІ, таких кодових слів, які б селективно модифікували ті частотні складові $\mu \times \mu$-блоку контейнера, що збурюються найменше при атаках проти вбудованого повідомлення (у разі атак стисненням з втратами, зашумленням або розмиттям йдеться про складові, що відповідають низьким і середнім частотам).

При цьому збурювальна дія, яку чинить атака на вбудоване повідомлення, так само, як і вбудовування ДІ, може бути представлена у вигляді адитивної матриці збурення, таким чином, для випадку атакованого стеганоповідомлення вираз (3.1) набуває вигляду

$$M' = X + D + \varepsilon, \tag{3.5}$$

де ε — матриця помилки, що вноситься атакою, M' — матриця збуреного стеганоповідомлення.

Зрозуміло, що якщо елемент матриці помилки ε буде протилежним елементу матриці D і буде дорівнювати або перевищить його по амплітуді,

на стороні декодера відбудеться помилка при декодуванні зазначеного елемента кодового слова. Позначимо можливість такої події як p_e.

Для зменшення негативного результату від впливу можливих збурень та підвищення стійкості стеганографічного методу з кодовим управлінням можна використовувати збільшення енергії застосовуваних кодових слів, яку визначимо наступним чином

$$E = \sum_{i=1}^{\mu} \sum_{j=1}^{\mu} t_{i,j}^2 , \tag{3.6}$$

де $t_{i,j}$ — елементи застосовуваного кодового слова.

У Розділі 2 для побудови конкретних кодових слів, з використанням прямої відповідності між трансформантами перетворення Уолша-Адамара та трансформантами ДКП, з огляду на максимізацію стійкості стеганографічного методу з кодовим управлінням вбудовуванням були обрані трансформанти перетворення Уолша-Адамара, що відповідають низькочастотним та середньочастотним складовим блоку ЦЗ (2.21).

Ґрунтуючись на даних (2.21), в якості кодових слів було запропоновано використовувати матричне уявлення рядків матриці Уолша-Адамара порядку N^2. Наприклад, для впливу на трансформанту ДКП (1,2) 4×4-блоків, в якості кодового слова використовується матричне уявлення третього рядка матриці Уолша-Адамара порядку $N=16$, яке для наочності наведемо разом з його трансформантами перетворення Уолша-Адамара (х.5), а також трансформантами ДКП (2.1)

$$T^{+}_{b,4,(1,2)} = \begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \end{bmatrix}, W^{+}_{b,4,(1,2)} = \begin{bmatrix} 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$
$$C^{+}_{b,4,(1,2)} = \begin{bmatrix} 0 & 3.7 & 0 & -1.53 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \tag{3.7}$$

де індекс $b,4,(1,2)$ позначає: b — бінарний характер кодового слова, 4 — порядок матриці кодового слова, (1,2) — трансформанта ДКП, на яку дане кодове слово має найбільший вплив.

Зважаючи на те, що кодове слово $T^{+}_{b,4,(1,2)}$ складається виключно з елементів, що належать множині $\{\pm 1\}$, його енергія, відповідно до (3.6) дорівнює $E = 16$.

Аналіз виразу (3.7) показує, що кодове слово $T^{+}_{b,4,(1,2)}$ має винятковий вплив на трансформанту (1,3) перетворення Уолша-Адамара. Тим не менш, зв'язок, встановлений у Розділі 2 між трансформантами Уолша-Адамара і трансформантами ДКП, не є взаємно однозначним, йдеться про те, що задана трансформанта Уолша-Адамара пов'язана з певною трансформантою ДКП «головним чином». Ця обставина призводить до того, що у перетворенні ДКП кодового слова $T^{+}_{b,4,(1,2)}$ є вплив не тільки на бажану трансформанту (1,2), але і на трансформанту (1,4). Іншими словами, забезпечуючи селективний вплив на трансформанту Уолша-Адамара (1,3), кодове слово $T^{+}_{b,4,(1,2)}$ не є селективним з точки зору впливу на трансформанту ДКП (1,2), тоді як значна частина його енергії витрачається на зміну трансформанти ДКП (1,4)), яка є більш високочастотною, і, відповідно, більшою мірою схильна до атак проти вбудованого повідомлення. З погляду стеганографії це можна розглядати як розподіл вбудованої ДІ, результатом додаткового кодування якої є $T^{+}_{b,4,(1,2)}$, за частотними складовими ДКП (1,2) і (1,4), або інакше, як уявлення ДІ у частотній області у вигляді збурень відповідних частотних коефіцієнтів.

На формальному рівні декодування ДІ буде тим ефективнішим, чим менше зміняться ці збурення частотних коефіцієнтів в результаті атаки проти вбудованого повідомлення, зокрема атаки стисненням. При цьому та «частина ДІ», формальним відображенням якої є збурення коефіцієнта (1,2) ДКП, є «захищенішою» від атаки стисненням, ніж частина, відображенням якої є збурення середньочастотного коефіцієнта (1,4). У зв'язку з цим для

блоку 4×4 актуальним завданням є забезпечення зменшення (мінімізації) збурення коефіцієнта ДКП (1,4) у результаті вбудовування ДІ для підвищення ефективності її декодування в умовах атак проти вбудованого повідомлення. Аналогічним є завдання й для блоків інших розмірів.

Подібні міркування справедливі і в тому випадку, якщо потрібне забезпечення стеганографічним методом з кодовим управлінням найбільшої надійності сприйняття за рахунок використання високочастотних складових ЦЗ. У такому випадку, буде потрібно забезпечення максимальної спрямованості впливу вже на такі коефіцієнти.

Для кількісної оцінки селективності впливу кодового слова на частотні складові стеганоповідомлення ми пропонуємо визначити коефіцієнт селективності κ наступним чином

$$\kappa = \frac{\left|C_{n,m}\right|}{\sum_{i=0}^{\mu-1}\sum_{j=0}^{\mu-1}\left|C_{i,j}\right|}. \qquad (3.7)$$

З визначення (3.7) безпосередньо випливає, що при фіксованому розмірі кодового слова зі збільшенням коефіцієнта селективності очікуваний «ефект» від використання конкретного кодового слова зростатиме (зокрема, збільшуватиметься стійкість стеганоперетворення до атак проти вбудованого повідомлення для відповідних кодових слів) при збільшенні $\left|C_{n,m}\right|$ та зменшенні $\sum_{i=0}^{\mu-1}\sum_{j=0}^{\mu-1}\left|C_{i,j}\right|$.

Результат «розсіювання» впливу кодового слова наростатиме зі зростанням його розміру. Справді, зі зростанням μ зменшуватиметься крок зміни аргументу косинусів, що використовуються в ДКП. Це призведе до того, що зростаюча енергія кодового слова, що впливає, головним чином, на низькі частоти (за побудовою кодового слова), перерозподілятиметься за більшою кількістю близьких низьких частот, які незначно відрізняються одна від одної, причому ця відмінність зменшується зі зростанням μ. При цьому

коефіцієнт ДКП (*n*,*m*) відповідає різним (низьким) частотам у блоках різного розміру, як випливає з формули (2.2). Назвемо це ефектом «близького сусіда». Ефект «близького сусіда» призведе до зниження значення коефіцієнта селективності зі зростанням μ, що визначається відповідно до (2.21) (табл. 3.1), де найголовнішим чином розглядається лише вплив на заданий частотний коефіцієнт (*n*,*m*), і до збільшення сумарного впливу на низькочастотних «близьких сусідів» (*n*,*m*), що буде показано нижче. Таким чином, зменшення κ зі зростанням μ у загальному випадку не відображає зниження стійкості відповідного стеганоперетворення до атаки проти вбудованого повідомлення, ілюстрацією чого є рис. 3.6, 3.7, 3.8, де стійкість стіганоповідомлення до атаки накладанням гаусівського шуму зростає зі зменшенням κ (збільшенням μ).

Таблиця 3.1 — Коефіцієнти селективності кодових слів, застосовуваних у Розділі 2

Трансформанта ДКП	Кодове слово, $\mu=4$	κ	Кодове слово, $\mu=8$	κ	Кодове слово, $\mu=16$	κ
(1,1)	$T^{+}_{b,4,(1,1)}$	1	$T^{+}_{b,8,(1,1)}$	1	$T^{+}_{b,16,(1,1)}$	1
(1,2)	$T^{+}_{b,4,(1,2)}$	0.7071	$T^{+}_{b,8,(1,2)}$	0.5603	$T^{+}_{b,16,(1,2)}$	0.4675
(2,1)	$T^{+}_{b,4,(2,1)}$	0.7071	$T^{+}_{b,8,(2,1)}$	0.5603	$T^{+}_{b,16,(2,1)}$	0.4675
(3,1)	$T^{+}_{b,4,(3,1)}$	1	$T^{+}_{b,8,(3,1)}$	0.7071	$T^{+}_{b,16,(3,1)}$	0.5603
(2,2)	$T^{+}_{b,4,(2,2)}$	0.5	$T^{+}_{b,8,(2,2)}$	0.314	$T^{+}_{b,16,(2,2)}$	0.2186
(1,3)	$T^{+}_{b,4,(1,3)}$	1	$T^{+}_{b,8,(1,3)}$	0.7071	$T^{+}_{b,16,(1,3)}$	0.5603

Як видно з табл. 3.1, при розмірі кодового слова $\mu=4$, значення коефіцієнта селективності $\kappa=1$ (абсолютна селективність) мають кодові слова $T^{+}_{b,4,(3,1)}$ і $T^{+}_{b,4,(1,3)}$. Розглянемо докладніше природу існування абсолютної селективності деяких кодових слів. Нехай задані кодові слова $T^{+}_{\mathbb{R},4,(2,1)}$ і $T^{+}_{b,4,(1,3)}$

над кільцем дійсних чисел, які мають коефіцієнт селективності $\kappa = 1$. Дані кодові слова можуть бути побудовані в результаті розв'язання наступних матричних рівнянь

$$CT^{+}_{\mathbb{R},4,(2,1)}C^{T} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ \alpha & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad CT^{+}_{\mathbb{R},4,(3,1)}C^{T} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \alpha & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \tag{3.8}$$

Вирішуючи зазначені матричні рівняння з використанням властивості взаємозв'язку між двовимірним та одновимірним ДКП, яка встановлена в Розділі 2, отримуємо наступні кодові слова

$$\begin{aligned} T^{+}_{\mathbb{R},4,(2,1)} &= \alpha \begin{bmatrix} 0.32665 & 0.32665 & 0.32665 & 0.32665 \\ 0.1353 & 0.1353 & 0.1353 & 0.1353 \\ -0.1353 & -0.1353 & -0.1353 & -0.1353 \\ -0.32665 & -0.32665 & -0.32665 & -0.32665 \end{bmatrix}; \\ T^{+}_{\mathbb{R},4,(3,1)} &= \alpha \begin{bmatrix} 0.25 & 0.25 & 0.25 & 0.25 \\ -0.25 & -0.25 & -0.25 & -0.25 \\ -0.25 & -0.25 & -0.25 & -0.25 \\ 0.25 & 0.25 & 0.25 & 0.25 \end{bmatrix}. \end{aligned} \tag{3.9}$$

Для випадку кодового слова $T^{+}_{\mathbb{R},4,(3,1)}$, приймаючи значення $\alpha = \sqrt{E}$ (де енергія кодового слова $T^{+}_{b,4,(3,1)}$ дорівнює $E = 16$), ми отримуємо точно кодове слово $T^{+}_{b,4,(3,1)}$, в той час як зазначене не є вірним для кодового слова $T^{+}_{\mathbb{R},4,(2,1)}$. Щоб перевести кодове слово $T^{+}_{\mathbb{R},4,(2,1)}$ на бінарний алфавіт $\{\pm 1\}$ потрібно спочатку прийняти значення $\alpha = \sqrt{E}$, після чого провести округлення елементів отриманої матриці до найближчого цілого. Зрозуміло, що операція округлення до найближчого цілого призведе до пошкодження вихідної структури кодового слова і, відповідно, розсіювання енергії на інші частотні складові.

У табл. 3.2 перераховані можливі кодові слова для $\mu = \{4,8,16\}$, що надають винятковий вплив на ту чи іншу трансформанту ДКП та характеризуються абсолютною селективністю.

Таблиця 3.2 — Кодові слова, які мають абсолютну селективність

Розмір 4×4	Розмір 8×8	Розмір 16×16
$T_{b,4,(1,1)}$, $T_{b,4,(1,3)}$, $T_{b,4,(3,1)}$, $T_{b,4,(3,3)}$	$T_{b,8,(1,1)}$, $T_{b,8,(1,5)}$, $T_{b,8,(5,1)}$, $T_{b,8,(5,5)}$	$T_{b,16,(1,1)}$, $T_{b,16,(1,9)}$, $T_{b,16,(9,1)}$, $T_{b,16,(9,9)}$

Не схильним до ефекту «близького сусіда» серед коефіцієнтів ДКП гарантовано є DC-коефіцієнт, оскільки він завжди визначається нульовою частотою, його властивості не залежать від розміру кодового слова, що підтверджує табл. 3.1 (для $T^{+}_{b,n,(1,1)}$ коефіцієнт селективності має максимальне значення, яке не змінюється зі зміною μ). Крім того, спираючись на результати досліджень, представлені, наприклад, в [31], можна стверджувати, що DC-коефіцієнти мають високу стійкість до зовнішніх впливів, чим можуть навіть перевершувати AC-коефіцієнти, тобто є кращими (бажаними) для організації стеганоперетворення. З огляду на це покажемо, що стійкість стеганоперетворення, організованого з використанням $T^{+}_{b,\mu,(1,1)}$, зростатиме зі зростанням μ.

Матриця $T^{+}_{b,\mu,(1,1)}$ є симетричною, для неї можлива побудова спектрального розкладання у формі зовнішніх добутків [32]

$$T^{+}_{b,\mu,(1,1)} = \sum_{i=1}^{\mu} \lambda_i u_i u_i^T , \tag{3.10}$$

де λ_i — дійсні власні значення $T^{+}_{b,\mu,(1,1)}$, а u_i — ортонормовані лексикографічно позитивні власні вектори, $i=\overline{1,\mu}$. Оскільки для $\forall\mu$: $rank\left(T^{+}_{b,\mu,(1,1)}\right)=1$, співвідношення (3.10) можна уточнити

$$T^{+}_{b,\mu,(1,1)} = \lambda_1 u_1 u_1^T , \tag{3.11}$$

де λ_1 — єдине ненульове власне значення $T^{+}_{b,\mu,(1,1)}$. Виходячи з теореми Фробеніуса [33], враховуючи нерозкладність і невід'ємність матриці $T^{+}_{b,\mu,(1,1)}$: $\lambda_1>0$. Використовуючи формули для обчислення енергії E $T^{+}_{b,\mu,(1,1)}$ через

власні значення матриці, а також через її елементи $T^{+}_{b,\mu,(1,1)}(i,j), i,j=\overline{1,\mu}$, маємо [27]

$$E=\sum_{i,j=1}^{\mu}\left(T^{+}_{b,\mu,(1,1)}(i,j)\right)^2=\mu^2=\sum_{i=1}^{\mu}\lambda_i^2=\lambda_1^2, \tag{3.12}$$

звідки

$$\lambda_1=\mu. \tag{3.13}$$

Тоді шляхом безпосередніх обчислень з (3.11) отримуємо $u_1=\left(\frac{1}{\sqrt{\mu}},\frac{1}{\sqrt{\mu}},...,\frac{1}{\sqrt{\mu}}\right)^T$, що являє собою *n*-оптимальний вектор простору R^{μ} [18], що позначається далі n^O, а сам вираз (3.11) перетворюється до виду

$$T^{+}_{b,\mu,(1,1)}=\mu\left(\frac{1}{\sqrt{\mu}},\frac{1}{\sqrt{\mu}},...,\frac{1}{\sqrt{\mu}}\right)^T\left(\frac{1}{\sqrt{\mu}},\frac{1}{\sqrt{\mu}},...,\frac{1}{\sqrt{\mu}}\right)=\mu n^O\left(n^O\right)^T. \tag{3.14}$$

Для $\mu\times\mu$-блоку F матриці ЦЗ можливе нормальне сингулярне розкладання, яке у формі зовнішніх добутків має вигляд [25]

$$F=\sum_{i=1}^{\mu}\sigma_i u_i v_i^T, \tag{3.15}$$

де σ_i — сингулярні числа F, $\sigma_1\ge\sigma_2\ge...\ge\sigma_{\mu}\ge 0$, u_i, v_i — відповідно ліві та праві ортонормовані сингулярні вектори, u_i — лексикографічно позитивні, $i=\overline{1,\mu}$. Показано [27], що для оригінальних ЦЗ: $u_1\approx v_1\approx n^O$.

Якщо F — блок матриці ЦЗ-контейнера, то стеганоперетворення з використанням кодового слова $T^{+}_{b,\mu,(1,1)}$ відповідно до (3.1) матиме вигляд

$$\begin{aligned}F+T^{+}_{b,\mu,(1,1)}&=\sum_{i=1}^{\mu}\sigma_i u_i v_i^T+\mu n^O\left(n^O\right)^T=\\&=\sigma_1 n^O\left(n^O\right)^T+\sum_{i=2}^{\mu}\sigma_i u_i v_i^T+\mu n^O\left(n^O\right)^T=\\&=\left(\sigma_1+\mu\right)n^O\left(n^O\right)^T+\sum_{i=2}^{\mu}\sigma_i u_i v_i^T.\end{aligned} \tag{3.16}$$

Таким чином, формально стеганоперетворення (3.1) може бути представлене у вигляді збурення максимального сингулярного числа блоку контейнера на величину, рівну розміру блоку (кодового слова). Відомо [27], що перша сингулярна трійка F відповідає в ЦЗ, головним чином низькочастотній складовій. Якщо подивитися на стеганоперетворення (3.16) у просторовій області $F + T^{+}_{b,\mu,(1,1)}$, то тут збурення кожного пікселя однакове, дорівнює ± 1 і не залежить від розміру блоку, але якщо проаналізувати результат стеганоперетворення відповідно до правої частини, то тут очевидним є висновок про те, що із зростанням μ збільшується збурення низькочастотної складової. Відомо, що для принципової можливості декодування ДІ збурення, яке зазнає контейнер при стеганоперетворенні, має бути більше, ніж збурення, яке зазнає стеганосоповідомлення в результаті атаки. У зв'язку з цим очевидно, що зі зростанням μ зростають можливості стеганоповідомлення протистояти сильнішій атаці, при цьому PSNR не змінюється.

Усі кодові слова, представлені в табл. 3.1, мають одиничний ранг, і навіть не бувши симетричними матрицями, можуть бути представлені у вигляді, аналогічному (3.11), але з використанням сингулярного розкладання у формі зовнішніх добутків

$$T^{+}_{b,\mu,(k,m)} = \sigma_1 u_1 v_1^T, \tag{3.17}$$

де $\sigma_1 > 0$ — єдине ненульове сингулярне число $T^{+}_{b,\mu,(k,m)}$, u_1, v_1 — відповідно лівий і правий сингулярний вектор, що відповідають σ_1. Отже, будь-яке кодове слово, зокрема і $T^{+}_{b,\mu,(1,1)}$, визначається єдиною сингулярною трійкою, що відповідає максимальному СНЧ, тобто орієнтовані, переважно, на низькі частоти, що формально демонструє досягнення мети їх побудови. При збільшенні μ перша сингулярна трійка, з урахуванням ефекту «близького сусіда», відповідатиме все більшій кількості близьких низьких частот (за

розглянутим вище винятком $T^{+}_{b,\mu,(1,1)}$), і хоча селективність (3.7) і падатиме, але сумарний внесок низькочастотних коефіцієнтів ДКП зростатиме, враховуючи властивості першої сингулярної трійки. У цьому випадку при зростанні μ збільшуватиметься збурення та кількість збурених низькочастотних коефіцієнтів, враховуючи ефект «близького сусіда» (при цьому низькочастотними для визначеності та одноманітності для будь-якого μ будемо вважати коефіцієнти ДКП, що належать верхньому лівому трикутнику матриці ДКП (рис. 3.10), включаючи той, на який початково і спрямоване кодове слово, в результаті стеганоперетворення (3.1), забезпечуючи цим підвищення стійкості до атак проти вбудованого повідомлення.

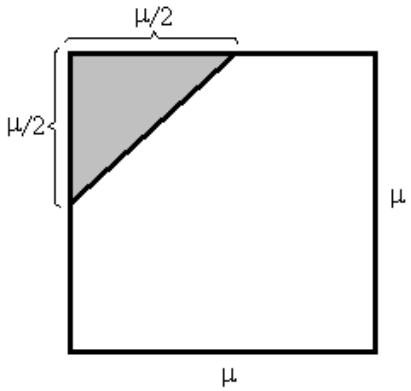


Рис. 3.10 — Матриця коефіцієнтів ДКП $T^{+}_{b,\mu,(1,1)}$ з виділеною областю коефіцієнтів, що розглядаються як низькочастотні

Вищевикладене проілюструємо за допомогою табл. 3.3, де представлені дані щодо значень коефіцієнта η відношення суми модулів низькочастотних коефіцієнтів ДКП до суми модулів решти всіх коефіцієнтів ДКП для кодових слів, застосованих у стеганографічному методі з кодовим управлінням.

Таблиця 3.3 — Значення η для кодових слів при різних значеннях μ

Трансформанта ДКП	Кодове слово, $\mu = 4$	η	Кодове слово, $\mu = 8$	η	Кодове слово, $\mu = 16$	η
(1,2)	$T^{+}_{b,4,(1,2)}$	2.4142	$T^{+}_{b,8,(1,2)}$	3.1165	$T^{+}_{b,16,(1,2)}$	3.8739
(2,1)	$T^{+}_{b,4,(2,1)}$	2.4142	$T^{+}_{b,8,(2,1)}$	3.1165	$T^{+}_{b,16,(2,1)}$	3.8739
(3,1)	$T^{+}_{b,4,(3,1)}$	-	$T^{+}_{b,8,(3,1)}$	2.4142	$T^{+}_{b,16,(3,1)}$	3.1165
(2,2)	$T^{+}_{b,4,(2,2)}$	-	$T^{+}_{b,8,(2,2)}$	0.4576	$T^{+}_{b,16,(2,2)}$	0.9305
(1,3)	$T^{+}_{b,4,(1,3)}$	-	$T^{+}_{b,8,(1,3)}$	2.4142	$T^{+}_{b,16,(1,3)}$	3.1165

Аналіз даних табл. 3.3 підтверджує, що зі збільшенням розміру кодових слів μ збільшується концентрація їх енергії в низькочастотних складових, що призводить до збільшення стійкості стеганографічного методу з кодовим управлінням до атак проти вбудованого повідомлення.

Зазначене повністю узгоджується з положеннями теорії кодування [27], відповідно до якої

$$p_{e\,decode} \le 1 - p_{correct} - p_{corrected} = 1 - \sum_{i=1}^{t} C_n^i p_e^t (1 - p_e)^{N-1}, \qquad (3.18)$$

де $p_{e\,decode}$ — ймовірність помилки декодування, $p_{correct}$ — ймовірність правильного прийому кодового слова, $p_{corrected}$ — ймовірність успішного виправлення помилки в кодовому слові, $t = \dfrac{d-1}{2}$ — кількість помилок, які можуть бути гарантовано виправлені кодом, d — кодова відстань коду, що використовується, $N = \mu^2$ — довжина кодових слів використовуваного коду.

Зважаючи на те, що у стеганографічному методі з кодовим управлінням використовується код, що складається з пари кодових слів, одне з яких є інверсією іншого, його кодова відстань дорівнює $d = N$, а отже $t = \dfrac{N-1}{2}$.

На рис. 3.11 представлені графіки залежності ймовірності помилки декодування від довжини кодового слова при різних значеннях ймовірності помилки у символі кодового слова p_e.

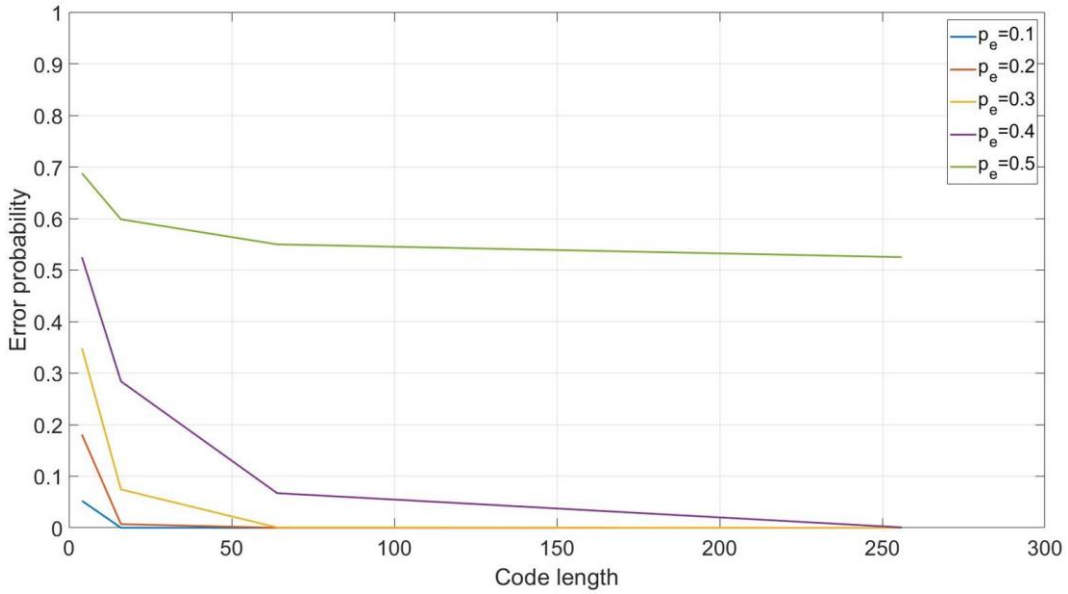


Рис. 3.11 — Графіки залежності ймовірності помилки декодування $p_{e\,decode}$ від довжини кодового слова N

Аналіз даних, поданих на рис. 3.11 показує зменшення ймовірності помилки декодування зі зростанням довжини кодового слова. При цьому для значень ймовірності помилки декодування $p_e \le 0.3$ для довжини кодового слова $N = 64$, що відповідає значенню $\mu = 8$, ймовірність помилки декодування фактично досягає нульової позначки.

Отримані результати говорять про те, що збільшення довжини кодового слова є однією з можливостей для підвищення стійкості стеганоперетворення до атак проти вбудованого повідомлення, хоча тут можливості не є безмежними, оскільки збільшення довжини кодового слова тягне за собою зменшення пропускної спроможності прихованого каналу зв'язку, що формується.

Практичним підтвердженням одержаних теоретичних висновків є результати обчислювальних експериментів, частина яких представлена на рис. 3.6, рис. 3.7, рис. 3.8.

Таким чином, підвищення стійкості методу кодового управління до можливих атак стисненням із втратами, зашумленням та розмиттям безпосередньо пов'язане з трьома завданнями: підвищення енергії кодового слова, яке може бути досягнуто шляхом збільшення значень модулів його елементів, збільшення рівня селективності кодового слова, а також нарощування довжини використовуваних кодових слів.

Однак очевидним тут є те, що у разі збільшення енергії кодового слова, погіршується надійність сприйняття стеганоповідомлення, у разі збільшення розміру кодових слів, що використовуються, — падає пропускна здатність прихованого каналу зв'язку. Підвищення селективності використовуваних кодових слів у загальному випадку є завданням оптимізації їх структури, яка не призводить до погіршення характеристик стеганографічного методу.

3.3. Багаторівневі коди для підвищення стійкості стеганографічного методу з кодовим управлінням

Задля вирішення завдання підвищення селективності кодових слів розглянемо докладніше особливості структури ДКП. Для спрощення математичних викладок запишемо двовимірне ДКП виду (2.1) за допомогою одномірного перетворення $\tilde{S} = \tilde{X}A1_{N^2}$.

Матриця $A1_{N^2}$ може бути побудована відповідно до методики, яку викладено у Розділі 2.

Для забезпечення найвищої селективності кодових слів, що конструюються, нам необхідно будувати їх таким чином, щоб необхідна трансформанта ДКП приймала задане значення $\alpha \neq 0$, у той час як інші

трансформанти повинні дорівнювати нулю. Це завдання можна звести до завдання розв'язання системи з N^2 рівнянь, яку в матричному вигляді можна записати як

$$V \cdot A1 = Z, \tag{3.19}$$

де V — вектор-рядок, що представляє шукане кодове слово, Z — вектор-рядок, що складається з усіх нулів і значення α на позиції $N \cdot n + m$, що відповідає (n,m) трансформанті ДКП при їх представленні за допомогою двовимірного ДКП, тобто

$$Z = \begin{pmatrix} 0 & \dots & \alpha & \dots & 0 \end{pmatrix}. \tag{3.20}$$

Рішення системи (3.19) для трансформанти ДКП (1,2), що розглядається для наочності викладу, після представлення отриманого результату у вигляді матриці розміру 4×4 має вигляд

$$T^{+}_{m',4,(1,2)} = \begin{bmatrix} 0.327\alpha & 0.135\alpha & -0.135\alpha & -0.327\alpha \\ 0.327\alpha & 0.135\alpha & -0.135\alpha & -0.327\alpha \\ 0.327\alpha & 0.135\alpha & -0.135\alpha & -0.327\alpha \\ 0.327\alpha & 0.135\alpha & -0.135\alpha & -0.327\alpha \end{bmatrix},$$
$$C^{+}_{m',4,(1,2)} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \alpha = 1. \tag{3.21}$$

Отже побудоване кодове слово має коефіцієнт селективності $\kappa = 1$ щодо трансформанти ДКП (1,2), тобто при використанні кодового управління вбудовуванням, теоретично забезпечує вбудовування інформації виключно в цю частотну складову.

Тим не менш, в реальних умовах, пікселі контейнера представлені цілими числами, тоді як їхня розрядність обмежена, найчастіше, одним байтом. Отже, кодове слово, за допомогою якого відбувається вбудовування, має бути цілим, тобто ідеальним з точки зору забезпечення максимальної селективності був би вибір такого α, яке б у прикладі (3.21) приводило до цілих значень 0.135α і 0.327α. Однак на практиці такий вибір найчастіше виявляється неприйнятним з урахуванням майбутнього адитивного

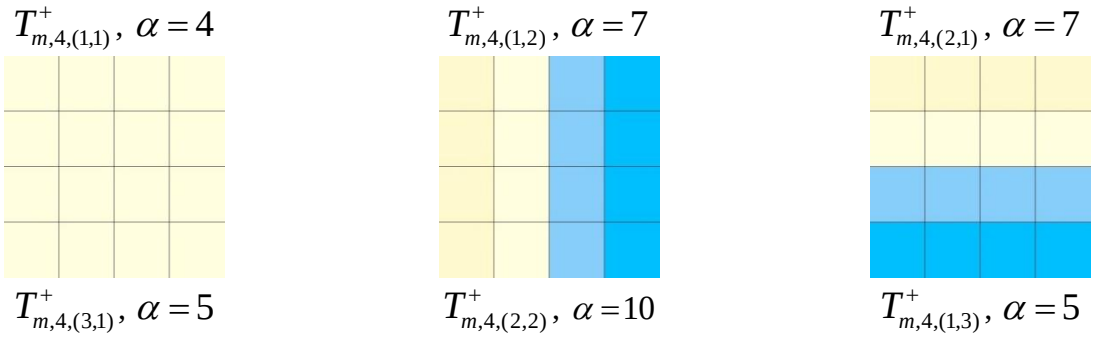
вбудовування ДІ (3.1): для забезпечення надійності сприйняття стеганоповідомлення елементи кодового слова не можуть бути великими. З урахуванням цього одержувані для конкретного значення α елементи $T^{+}_{m',4,(1,2)}$ для отримання кодового слова $T^{+}_{m,4,(1,2)}$ округлятимуться до найближчого цілого. Так для $\alpha = 7$ маємо

$$T^{+}_{m,4,(1,2)} = \begin{bmatrix} 2 & 1 & -1 & -2 \\ 2 & 1 & -1 & -2 \\ 2 & 1 & -1 & -2 \\ 2 & 1 & -1 & -2 \end{bmatrix}, C^{+}_{m,4,(1,2)} = \begin{bmatrix} 0 & 6.3086 & 0 & -0.448 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \qquad (3.22)$$

де індекс m означає багаторівневу природу кодового слова.

Аналіз (3.22) призводить до висновку, що коефіцієнт селективності кодового слова $T^{+}_{m,4,(1,2)}$ дорівнює κ =0.9337, що значно перевищує коефіцієнт селективності кодового слова $T^{+}_{b,4,(1,2)}$.

Аналогічним чином можуть бути побудовані і кодові слова, спрямовані на модифікацію інших трансформант ДКП і які мають високі значення коефіцієнта селективності. Для випадку розміру блоку $\mu = 4$ наведемо вказані кодові слова на рис. 3.12, причому в табл. 3.4 наведена розшифровка кольорів, що використовуються на рис. 3.12, а також у наступних рисунках, які показують структуру кодових слів.



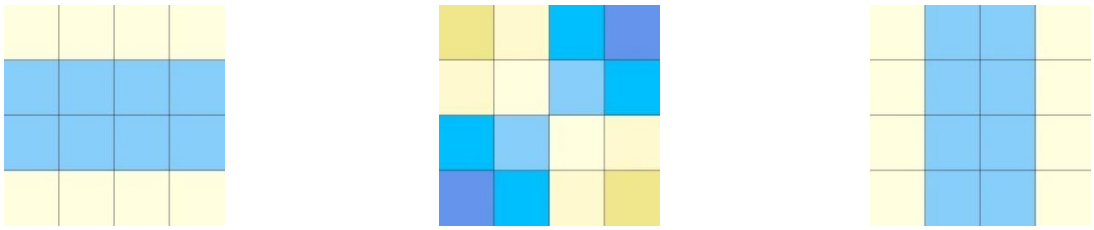


Рис. 3.12 — Кодові слова з високою селективністю для $\mu = 4$

Таблиця 3.4 — Розшифровка кольорів

	1		2		3		4		0
	5		6		7		8		
	–1		–2		–3		–4		
	–5		–6		–7		–8		

Слід зазначити, що коефіцієнт селективності κ у загальному випадку залежить від значення α, тобто від розкиду амплітуд у кодовому слові. Розглянемо, наприклад, кодове слово $T^{+}_{m',4,(2,2)}$, що впливає на трансформанту ДКП (2,2)

$$T^{+}_{m',4,(2,2)} = \begin{bmatrix} 0.43\alpha & 0.18\alpha & -0.18\alpha & -0.43\alpha \\ 0.18\alpha & 0.07\alpha & -0.07\alpha & -0.18\alpha \\ -0.18\alpha & -0.07\alpha & 0.07\alpha & 0.18\alpha \\ -0.43\alpha & -0.18\alpha & 0.18\alpha & 0.43\alpha \end{bmatrix}. \quad (3.23)$$

У (3.24) ми наводимо варіанти кодових слів $T^{+}_{m',4,(2,2)}$ при різних значеннях α, а також значення коефіцієнтів селективності, які досягаються при даному значенні α

$$T^{+}_{m,4,(2,2)} = \begin{bmatrix} 2 & 1 & -1 & -2 \\ 1 & 0 & 0 & -1 \\ -1 & 0 & 0 & 1 \\ -2 & -1 & 1 & 2 \end{bmatrix}, \alpha = 4, \kappa = 0.8536;$$

$$T^{+}_{m,4,(2,2)} = \begin{bmatrix} 4 & 2 & -2 & -4 \\ 2 & 1 & -1 & -2 \\ -2 & -1 & 1 & 2 \\ -4 & -2 & 2 & 4 \end{bmatrix}, \alpha = 9, \kappa = 0.8717; \quad (3.24)$$

$$T^{+}_{m,4,(2,2)} = \begin{bmatrix} 8 & 3 & -3 & -8 \\ 3 & 1 & -1 & -3 \\ -3 & -1 & 1 & 3 \\ -8 & -3 & 3 & 8 \end{bmatrix}, \alpha = 18, \kappa = 0.9189.$$

Таким чином, зі збільшенням значення α значно збільшується і коефіцієнт селективності κ. Аналогічна картина спостерігається з іншими кодовими словами, крім тих, для яких $\kappa = const = 1$.

Оскільки при великих значеннях α спотворення, що вносяться кодовим словом у контейнер, стають неприпустимо великими, з практичної точки зору мають сенс тільки такі значення коефіцієнта α, які не призводять до появи в кодових словах елементів, амплітуда яких перевищує значення 8.

Зазначимо, що абсолютно аналогічно випадку розміру блока $\mu = 4$ можуть бути побудовані кодові слова і для випадку розміру блоку $\mu = 8$.

На рис. 3.13 представлені кодові слова, що забезпечують високу селективність для випадку розміру блоку $\mu = 8$.

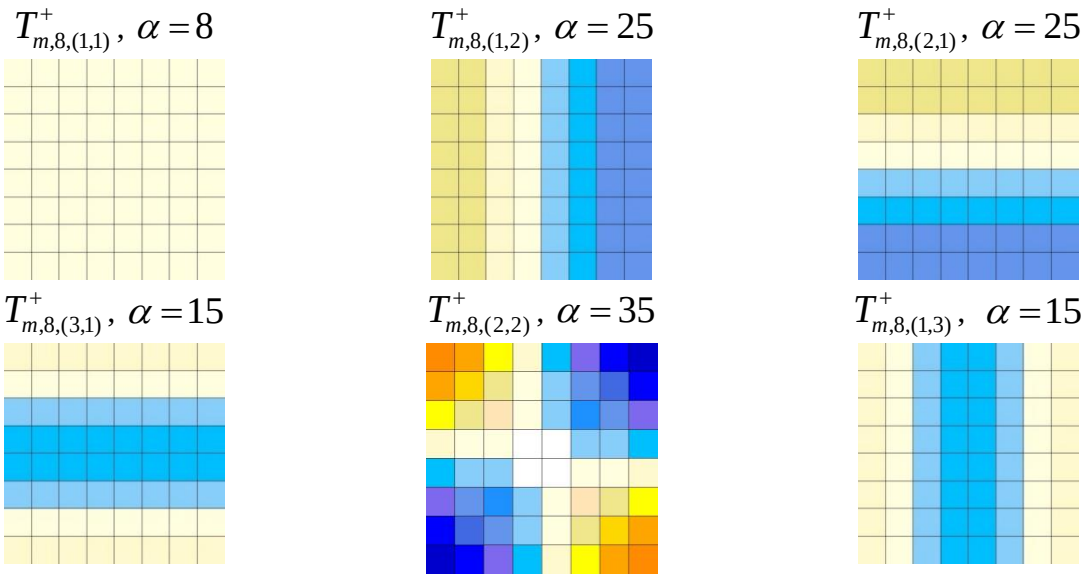


Рис. 3.13 — Кодові слова з високою селективністю для $\mu = 8$

На рис. 3.14 ми наводимо кодові слова, що забезпечують високу селективність для випадку розміру блоку $\mu = 16$.

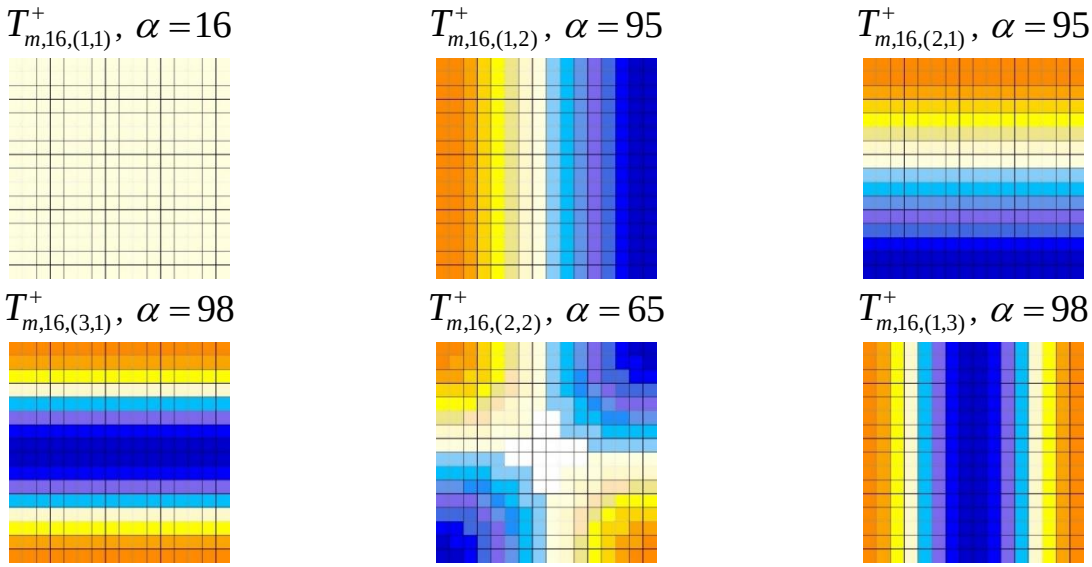


Рис. 3.14 — Кодові слова з високою селективністю для $\mu = 16$

У табл. 3.5 ми наводимо значення коефіцієнта селективності для багаторівневих кодових слів, зображених на рис. 3.12, рис. 3.13 та рис. 3.14, а також для їх бінарних аналогів.

Таблиця 3.5 — Коефіцієнти селективності багаторівневих та бінарних кодових слів

Трансформанта ДКП	Кодове слово, $\mu = 4$	κ	Кодове слово, $\mu = 8$	κ	Кодове слово, $\mu = 16$	κ
(1,1)	$T^{+}_{m,4,(1,1)}$	1	$T^{+}_{m,8,(1,1)}$	1	$T^{+}_{m,16,(1,1)}$	1
	$T^{+}_{b,4,(1,1)}$	1	$T^{+}_{b,8,(1,1)}$	1	$T^{+}_{b,16,(1,1)}$	1
(1,2)	$T^{+}_{m,4,(1,2)}$	0.9336	$T^{+}_{m,8,(1,2)}$	0.8710	$T^{+}_{m,16,(1,2)}$	0.9224
	$T^{+}_{b,4,(1,2)}$	0.7071	$T^{+}_{b,8,(1,2)}$	0.5603	$T^{+}_{b,16,(1,2)}$	0.4675
(2,1)	$T^{+}_{m,4,(2,1)}$	0.9336	$T^{+}_{m,8,(2,1)}$	0.8710	$T^{+}_{m,16,(2,1)}$	0.9224
	$T^{+}_{b,4,(2,1)}$	0.7071	$T^{+}_{b,8,(2,1)}$	0.5603	$T^{+}_{b,16,(2,1)}$	0.4675
(3,1)	$T^{+}_{m,4,(3,1)}$	1	$T^{+}_{m,8,(3,1)}$	0.9336	$T^{+}_{m,16,(3,1)}$	0.9398
	$T^{+}_{b,4,(3,1)}$	1	$T^{+}_{m,8,(2,2)}$	0.7071	$T^{+}_{b,16,(3,1)}$	0.5603
(2,2)	$T^{+}_{m,4,(2,2)}$	0.8717	$T^{+}_{m,8,(2,2)}$	0.8349	$T^{+}_{m,16,(2,2)}$	0.6859
	$T^{+}_{b,4,(2,2)}$	0.5	$T^{+}_{b,8,(2,2)}$	0.314	$T^{+}_{b,16,(2,2)}$	0.2186

Закінчення табл. 3.5

(1,3)	$T^{+}_{m,4,(1,3)}$	1	$T^{+}_{m,8,(1,3)}$	0.9336	$T^{+}_{m,16,(1,3)}$	0.9398
	$T^{+}_{b,4,(1,3)}$	1	$T^{+}_{b,8,(1,3)}$	0.7071	$T^{+}_{b,16,(1,3)}$	0.5603

Аналіз даних табл. 3.5 показує, що застосування багаторівневих кодових слів дозволяє досягти істотного підвищення коефіцієнта селективності порівняно з використанням їх бінарних аналогів і, як наслідок, теоретично забезпечує підвищення ефективності методу з кодовим управлінням вбудовуванням ДІ.

Основні кроки пропонованого стеганографічного методу з кодовим управлінням вбудовуванням на основі багаторівневих кодових слів, є наступними.

Вбудовування ДІ.

Крок 1. Провести розбиття вихідного зображення-контейнера на $\mu \times \mu$-блоки, що не перетинаються, де $\mu = 2^n$, n — натуральне число.

Крок 2. Виходячи з необхідних властивостей стеганоповідомлення, вибрати цільову трансформанту ДКП (k,l), на яку необхідно зробити вплив, і значення коефіцієнта α. Побудувати вектор Z (3.20) та матрицю $A1_{\mu^2}$ згідно з матеріалами Розділу 2.

Крок 3. Розв'язати систему рівнянь (3.19). Результат — вектор-рядок V.

Крок 4. Виконати округлення елементів V до найближчого цілого з подальшим перетворенням у $\mu \times \mu$-матрицю. Результат — кодове слово $T^{+}_{m,\mu,(k,l)}$ для додаткового кодування символу «0», його інверсія $T^{-}_{m,\mu,(k,l)}$ — для додаткового кодування символу «1».

Крок 5. Нехай X — черговий $\mu \times \mu$-блок контейнера, задіяний в стеганоперетворенні, в який вбудовується черговий біт додаткової інформації p

$$\begin{aligned} &\text{Якщо}: p = 0 \\ &\text{то}: M = X + T^{+}_{m,\mu,(k,l)}, \\ &\text{інакше}: M = X + T^{-}_{m,\mu,(k,l)}. \end{aligned} \tag{3.25}$$

Вилучення ДІ

Крок 1. Здійснити розбиття вихідного зображення-стеганоповідомлення на $\mu \times \mu$-блоки, що не перетинаються.

Крок 2. Нехай $\overline{M}$ — черговий $\mu \times \mu$-блок можливо збуреного стеганоповідомлення, задіяний в стеганоперетворенні, що відповідає $\mu \times \mu$-блоку X контейнера.

2.1. Побудувати матрицю $\Delta = \overline{M} - X$, з елементами $\Delta(i, j),\ i, j = 0,1,..., \mu - 1$.

2.2. Вилучення біта $\overline{p}$ ДІ з блоку $\overline{M}$

$$\overline{p} = sign\left(\sum_{i,j=0}^{\mu-1} \Delta(i, j) T^{+}_{m,\mu,(k,l)}(i, j) \right). \tag{3.26}$$

Зазначимо, що *Крок 2.2* в алгоритмі вилучення інформації, по суті, реалізує алгоритм оптимального прийому [29].

На основі представлених даних та сконструйованих кодових слів проведемо ряд експериментів, для дослідження ефективності розробленого методу.

Експеримент 3.1. Завданням, яке вирішується за допомогою даного експерименту є практичне підтвердження впливу коефіцієнта селективності на стійкість стеганографічного методу до збурювальних впливів. Для проведення експерименту було обрано 500 зображень у форматі TIFF з бази NRCS [30], у які проводилося вбудовування інформації з використанням кодового слова $T^{+}_{m,8,(1,2)}$, а також відповідного бінарного кодового слова $T^{+}_{b,8,(1,2)}$

$$T^{+}_{m,8,(1,2)} = \begin{bmatrix} 2 & 1 & 1 & 0 & 0 & -1 & -1 & -2 \\ 2 & 1 & 1 & 0 & 0 & -1 & -1 & -2 \\ 2 & 1 & 1 & 0 & 0 & -1 & -1 & -2 \\ 2 & 1 & 1 & 0 & 0 & -1 & -1 & -2 \\ 2 & 1 & 1 & 0 & 0 & -1 & -1 & -2 \\ 2 & 1 & 1 & 0 & 0 & -1 & -1 & -2 \\ 2 & 1 & 1 & 0 & 0 & -1 & -1 & -2 \\ 2 & 1 & 1 & 0 & 0 & -1 & -1 & -2 \end{bmatrix}, \alpha = 9, \kappa = 0.6937,$$

$$T^{+}_{b,8,(1,2)} = \begin{bmatrix} 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \end{bmatrix}. \quad (3.27)$$

Після вбудовування інформації, зображення було піддано атаці стиском з втратами за допомогою алгоритму JPEG з різними коефіцієнтами якості QF. Після виконання стиснення виконувалося вилучення інформації з підрахунком кількості помилок (у відсотках по відношенню до загальної кількості вилучених біт). Результуючий графік наведено на рис. 3.15.

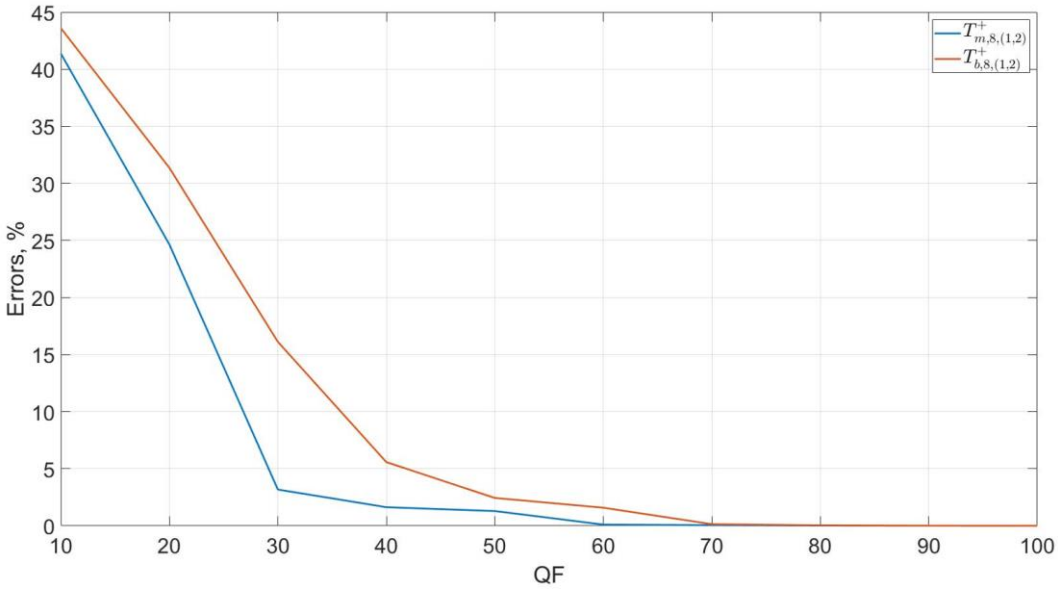


Рис. 3.15 — Графік залежності кількості помилок при вилученні додаткової інформації від коефіцієнта якості QF, що використовується при стисненні стеганоповідомлення

Аналіз даних, поданих на рис. 3.15 показує, що два кодових слова, навіть володіючи однаковою сумарною амплітудою впливу, і впливаючи на один і той же коефіцієнт ДКП, можуть показувати різні рівні стійкості до атаки стисненням у разі різного значення коефіцієнта селективності κ. Таким чином, проведений експеримент на практиці підтверджує підвищення ефективності декодування ДІ при переході від бінарного до багаторівневого кодового слова (що призводить до зростання селективності) в умовах атаки стисненням.

Експеримент 3.2. Завданням даного експерименту є дослідження впливу α (коефіцієнта селективності у разі використання багаторівневих кодових слів) на ефективність розробленого стеганографічного методу. Для проведення експерименту вбудовування ДІ виконувалося в 500 зображень з бази NRCS [30], після чого вони піддавалися стиску алгоритмом JPEG з різними коефіцієнтами якості. Для вбудовування інформації були побудовані варіанти кодових слів $T^{+}_{m,4,(1,2)}$, $T^{+}_{m,8,(1,2)}$ і $T^{+}_{m,16,(1,2)}$, для різних α, використовуючи

$$T^{+}_{m',4,(1,2)} = \alpha \begin{bmatrix} 0.33 & 0.14 & -0.14 & -0.33 \\ 0.33 & 0.14 & -0.14 & -0.33 \\ 0.33 & 0.14 & -0.14 & -0.33 \\ 0.33 & 0.14 & -0.14 & -0.33 \end{bmatrix};$$

$$T^{+}_{m',8,(1,2)} = \alpha \begin{bmatrix} 0.17 & 0.15 & 0.1 & 0.03 & -0.03 & -0.1 & -0.15 & -0.17 \\ 0.17 & 0.15 & 0.1 & 0.03 & -0.03 & -0.1 & -0.15 & -0.17 \\ 0.17 & 0.15 & 0.1 & 0.03 & -0.03 & -0.1 & -0.15 & -0.17 \\ 0.17 & 0.15 & 0.1 & 0.03 & -0.03 & -0.1 & -0.15 & -0.17 \\ 0.17 & 0.15 & 0.1 & 0.03 & -0.03 & -0.1 & -0.15 & -0.17 \\ 0.17 & 0.15 & 0.1 & 0.03 & -0.03 & -0.1 & -0.15 & -0.17 \\ 0.17 & 0.15 & 0.1 & 0.03 & -0.03 & -0.1 & -0.15 & -0.17 \\ 0.17 & 0.15 & 0.1 & 0.03 & -0.03 & -0.1 & -0.15 & -0.17 \end{bmatrix};$$

$$T^{+}_{m',16,(1,2)} = \alpha \left[\begin{matrix} 0.09 & 0.08 & 0.08 & 0.07 & 0.06 & 0.04 & 0.03 & 0.01 \\ 0.09 & 0.08 & 0.08 & 0.07 & 0.06 & 0.04 & 0.03 & 0.01 \\ 0.09 & 0.08 & 0.08 & 0.07 & 0.06 & 0.04 & 0.03 & 0.01 \\ 0.09 & 0.08 & 0.08 & 0.07 & 0.06 & 0.04 & 0.03 & 0.01 \\ 0.09 & 0.08 & 0.08 & 0.07 & 0.06 & 0.04 & 0.03 & 0.01 \\ 0.09 & 0.08 & 0.08 & 0.07 & 0.06 & 0.04 & 0.03 & 0.01 \\ 0.09 & 0.08 & 0.08 & 0.07 & 0.06 & 0.04 & 0.03 & 0.01 \\ 0.09 & 0.08 & 0.08 & 0.07 & 0.06 & 0.04 & 0.03 & 0.01 \\ 0.09 & 0.08 & 0.08 & 0.07 & 0.06 & 0.04 & 0.03 & 0.01 \\ 0.09 & 0.08 & 0.08 & 0.07 & 0.06 & 0.04 & 0.03 & 0.01 \\ 0.09 & 0.08 & 0.08 & 0.07 & 0.06 & 0.04 & 0.03 & 0.01 \\ 0.09 & 0.08 & 0.08 & 0.07 & 0.06 & 0.04 & 0.03 & 0.01 \\ 0.09 & 0.08 & 0.08 & 0.07 & 0.06 & 0.04 & 0.03 & 0.01 \\ 0.09 & 0.08 & 0.08 & 0.07 & 0.06 & 0.04 & 0.03 & 0.01 \\ 0.09 & 0.08 & 0.08 & 0.07 & 0.06 & 0.04 & 0.03 & 0.01 \\ 0.09 & 0.08 & 0.08 & 0.07 & 0.06 & 0.04 & 0.03 & 0.01 \end{matrix}\right. \qquad (3.28)$$

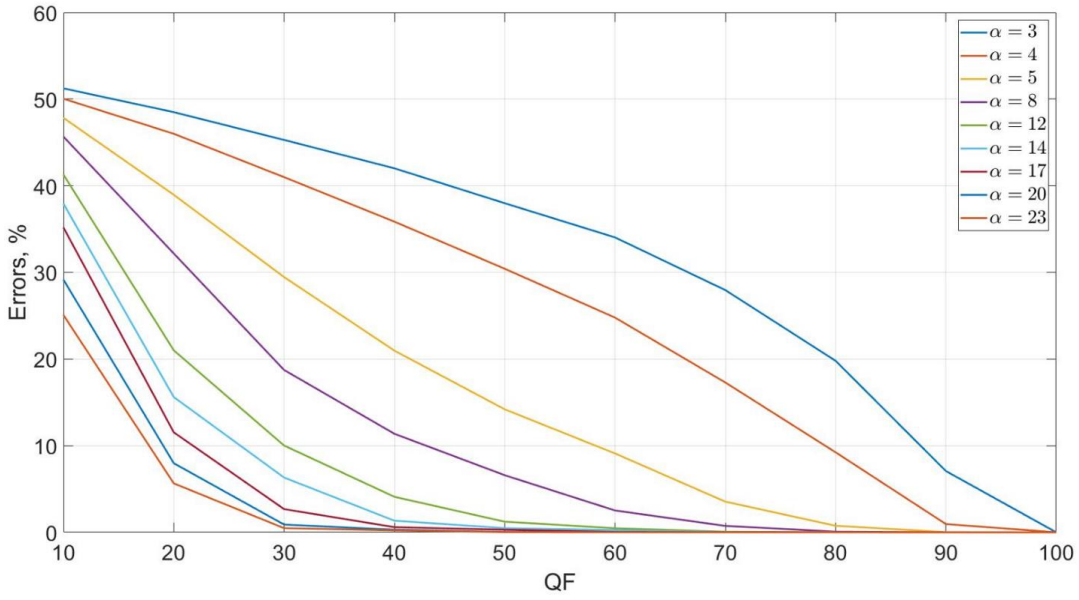
$$\left.\begin{matrix} -0.01 & -0.03 & -0.04 & -0.06 & -0.07 & -0.08 & -0.08 & -0.09 \\ -0.01 & -0.03 & -0.04 & -0.06 & -0.07 & -0.08 & -0.08 & -0.09 \\ -0.01 & -0.03 & -0.04 & -0.06 & -0.07 & -0.08 & -0.08 & -0.09 \\ -0.01 & -0.03 & -0.04 & -0.06 & -0.07 & -0.08 & -0.08 & -0.09 \\ -0.01 & -0.03 & -0.04 & -0.06 & -0.07 & -0.08 & -0.08 & -0.09 \\ -0.01 & -0.03 & -0.04 & -0.06 & -0.07 & -0.08 & -0.08 & -0.09 \\ -0.01 & -0.03 & -0.04 & -0.06 & -0.07 & -0.08 & -0.08 & -0.09 \\ -0.01 & -0.03 & -0.04 & -0.06 & -0.07 & -0.08 & -0.08 & -0.09 \\ -0.01 & -0.03 & -0.04 & -0.06 & -0.07 & -0.08 & -0.08 & -0.09 \\ -0.01 & -0.03 & -0.04 & -0.06 & -0.07 & -0.08 & -0.08 & -0.09 \\ -0.01 & -0.03 & -0.04 & -0.06 & -0.07 & -0.08 & -0.08 & -0.09 \\ -0.01 & -0.03 & -0.04 & -0.06 & -0.07 & -0.08 & -0.08 & -0.09 \\ -0.01 & -0.03 & -0.04 & -0.06 & -0.07 & -0.08 & -0.08 & -0.09 \\ -0.01 & -0.03 & -0.04 & -0.06 & -0.07 & -0.08 & -0.08 & -0.09 \\ -0.01 & -0.03 & -0.04 & -0.06 & -0.07 & -0.08 & -0.08 & -0.09 \\ -0.01 & -0.03 & -0.04 & -0.06 & -0.07 & -0.08 & -0.08 & -0.09 \end{matrix}\right].$$

У табл. 3.6 показані варіанти кодових слів для різних значень α і, відповідно, коефіцієнта селективності κ.

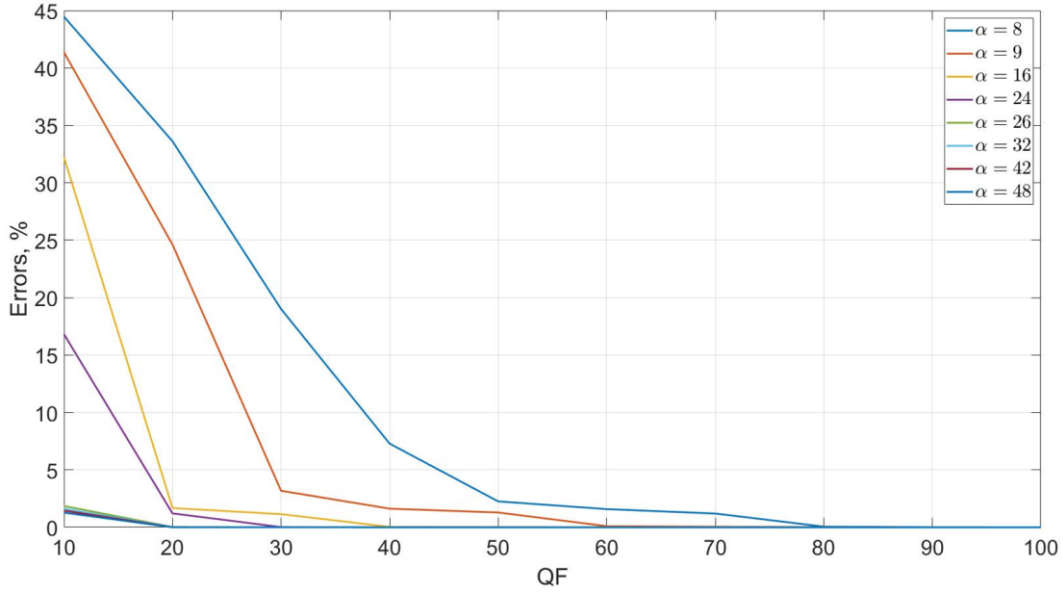
Таблиця 3.6 — Кодові слова $T^{+}_{m,4,(1,2)}$, $T^{+}_{m,8,(1,2)}$, $T^{+}_{m,16,(1,2)}$ з різними значеннями α і κ

4×4		8×8		16×16	
α	κ	α	κ	α	κ
3	0.7071	8	0.6937	17	0.5902
4	0.7071	9	0.6937	28	0.7226
5	0.9336	16	0.7980	39	0.7879
8	0.9336	24	0.8710	51	0.8413
12	0.9336	26	0.9387	62	0.8206
14	0.9880	32	0.9398	73	0.8996
17	0.9336	42	0.9387	85	0.8806
20	0.9880	48	0.9398	96	0.9046
23	0.9672	—	—	—	—

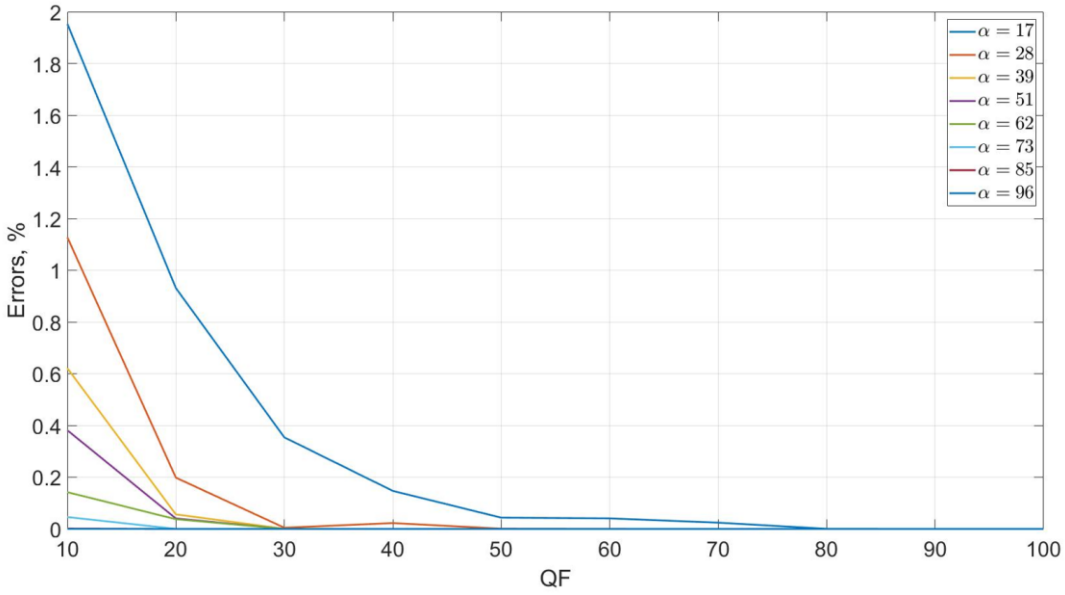
Далі, для отриманих стеганоповідомлень виконувалося вилучення інформації з подальшою оцінкою кількості помилок, що трапилися. На рис. 3.16 представлені графіки залежності кількості помилок від коефіцієнта якості QF для кожного значення α, що розглядається в експерименті.



а)



б)



в)

Рис. 3.16 — Графік залежності кількості помилок при декодуванні ДІ від коефіцієнта якості при використанні кодових слів (3.28) з коефіцієнтами з табл. 3.6: а) — $\mu = 4$; б) — $\mu = 8$; в) — $\mu = 16$

Аналіз даних рис. 3.16 показує, що вбудовування інформації з кодовим управлінням за допомогою кодового слова $T^{+}_{m,4,(1,2)}$ з коефіцієнтами $\alpha \geq 17$, практично дозволяє уникнути виникнення помилок при вилученні ДІ, в умовах атаки стисненням з коефіцієнтами якості $QF \geq 30$. При цьому

використання представлених кодових слів дозволяє отримати пропускну здатність, що дорівнює $1/16$ біт/піксель.

Вбудовування інформації за допомогою методу з кодовим управлінням з використанням кодового слова $T^{+}_{m,8,(1,2)}$ з коефіцієнтами $\alpha > 26$, дозволяє майже уникнути виникнення помилок при вилучення ДІ, за умов атаки стисненням з коефіцієнтами якості $\alpha > 26$. При цьому пропускна здатність стеганоканалу становить $1/64$ біт/піксель.

Використання ж кодового слова $T^{+}_{m,16,(1,2)}$ будь-якої представленої його модифікації, дозволяє фактично повністю уникнути виникнення помилок при декодуванні ДІ навіть при дуже маленьких значеннях коефіцієнта якості QF. Однак, при використанні даних кодових слів пропускна здатність дорівнюватиме $1/256$ біт/піксель.

Таким чином, в рамках заданого значення розміру блоку μ, збільшення α, що призводять до збільшення коефіцієнта селективності κ, дозволяє забезпечити більшу стійкість запропонованого стеганографічного методу до атак стисненням.

Експеримент 3.3. Завданням цього експерименту є оцінка ефективності запропонованого методу залежно від формату контейнера. В якості контейнерів було обрано по 500 зображень у форматі JPEG, збережених з коефіцієнтами якості $QF = \{90, 70, 50, 30\}$. Для даних зображень проводилося вбудовування інформації за допомогою кодового слова

$$T^{+}_{m,8,(1,2)} = \begin{bmatrix} 4 & 4 & 2 & 1 & -1 & -2 & -4 & -4 \\ 4 & 4 & 2 & 1 & -1 & -2 & -4 & -4 \\ 4 & 4 & 2 & 1 & -1 & -2 & -4 & -4 \\ 4 & 4 & 2 & 1 & -1 & -2 & -4 & -4 \\ 4 & 4 & 2 & 1 & -1 & -2 & -4 & -4 \\ 4 & 4 & 2 & 1 & -1 & -2 & -4 & -4 \\ 4 & 4 & 2 & 1 & -1 & -2 & -4 & -4 \\ 4 & 4 & 2 & 1 & -1 & -2 & -4 & -4 \end{bmatrix}, \qquad (3.29)$$

після чого проводилося повторне стиснення алгоритмом JPEG та подальше вилучення інформації. Графіки залежності кількості помилок від степеню повторного стиснення наведено на рис. 3.17.

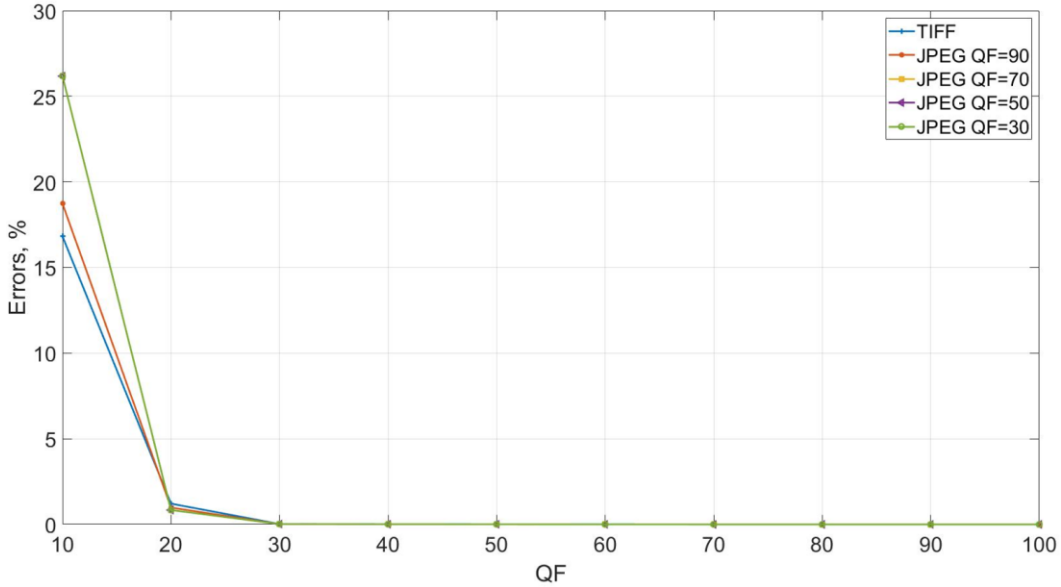


Рис. 3.17 — Графік залежності кількості помилок при декодуванні ДІ від коефіцієнта якості QF, що використовується при атаці стисненням, для контейнерів у різних форматах зберігання

Аналіз даних рис. 3.17 показує, що формат контейнера (TIFF — без втрат або JPEG — з різними коефіцієнтами якості QF) практично не впливає на ефективність стеганографічного методу з кодовим управлінням. Так, лінії графіків для контейнерів з коефіцієнтами якості $QF = \{70, 50, 30\}$ практично збігаються одна з одною. В інших випадках, відмінності у використанні контейнерів у форматі зі стисненням або без стиснення незначні і виявляються лише при значеннях коефіцієнта якості контейнера $QF < 30$, які дуже рідко використовуються на практиці.

Експеримент 3.4. Завданням даного експерименту є оцінка ефективності розробленого методу за умов атаки зашумленням [34]. Для проведення даного експерименту проводилося вбудовування ДІ в 500 зображень з бази NRCS [30], після чого вони піддавались зашумленню

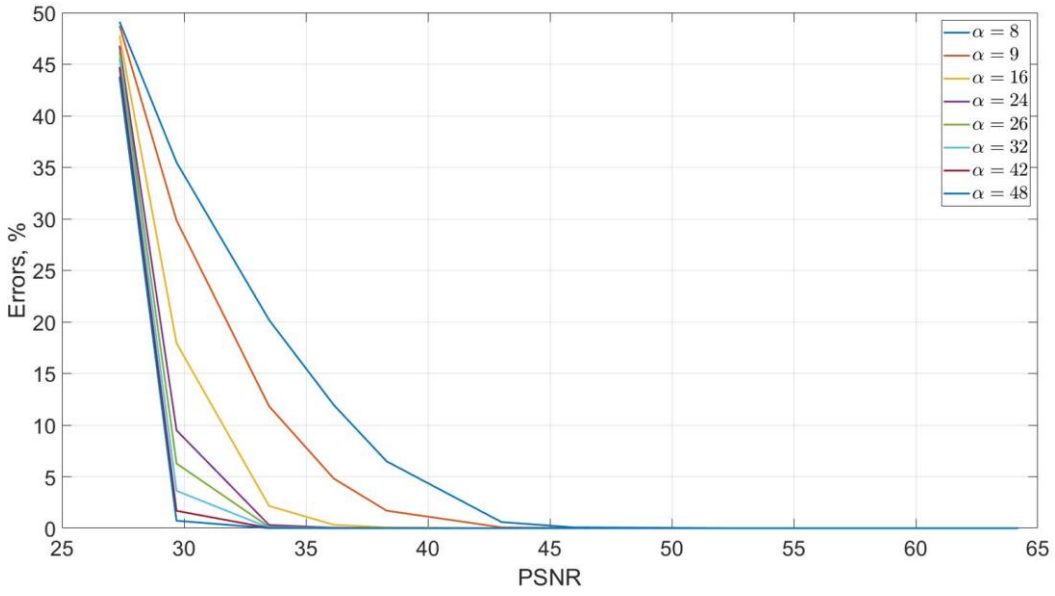
адитивним білим гауссівським шумом з математичним очікуванням $M[X]=0$ і дисперсією $D[X]=\sigma^2$, а також шумом «salt&pepper». На рис. 3.18 наведено графіки залежності кількості помилок при декодуванні ДІ від інтенсивності шуму, що оцінюється показником PSNR, який обчислюється за формулою

$$\mathrm{PSNR}=20\lg\left(\frac{255}{\sqrt{MSE}}\right), \tag{3.30}$$

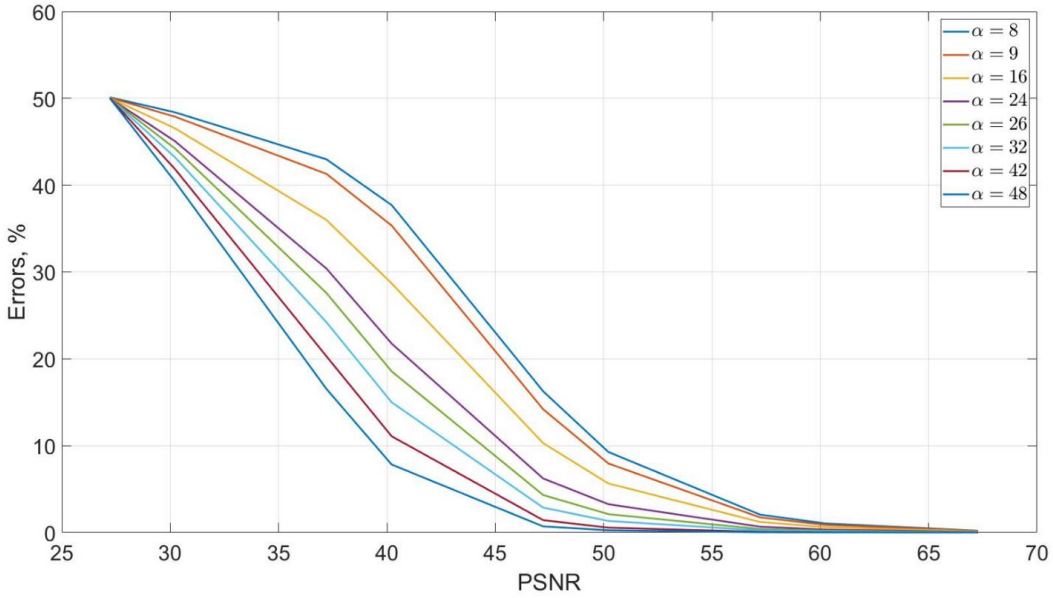
де

$$MSE=\frac{1}{nm}\sum_i\sum_j\left|Y(i,j)-H(i,j)\right|^2. \tag{3.31}$$

де Y — матриця зображення до збурювального впливу, H — матриця зображення після збурювального впливу.



а)



б)

Рис. 3.18 — Графік залежності кількості помилок при декодуванні ДІ від PSNR за умови атаки зашумленням при використанні кодових слів розміру 8×8 (3.28) з коефіцієнтами (табл. 3.6): а) — гаусівський шум; б) — шум "salt&pepper"

Аналіз даних рис. 3.18 показує, що для кодового слова $T^{+}_{m,8,(1,2)}$ з коефіцієнтами $\alpha \geq 16$ помилок при вилученні інформації практично не відбувається під впливом атаки зашумленням за допомогою адитивного білого гаусівського шуму з $\mathrm{PSNR} = 33\text{дБ}$, а також шуму типу «salt&pepper» з $\mathrm{PSNR} = 57\text{дБ}$.

Таким чином, при фіксованому значенні розміру блоку μ збільшення значення α призводить до збільшення стійкості запропонованого стеганографічного методу до атак зашумленням.

Експеримент 3.5. Завданням експерименту є оцінка ефективності розробленого методу під час використання багаторівневих кодових слів (3.28) з коефіцієнтами (табл. 3.6) за умови атаки розмиттям. Для проведення даного експерименту проводилося вбудовування ДІ в 500 зображень з бази NRCS [30], після чого вони піддавалися атаці розмиттям з вікном фільтра, рівним w. Далі, для отриманих стеганоповідомлень виконувалося вилучення

інформації з подальшою оцінкою кількості помилок, що трапилися. На рис. 3.19 показаний графік залежності кількості помилок при декодуванні стеганоповідомлення при різних значеннях розміру w вікна фільтра.

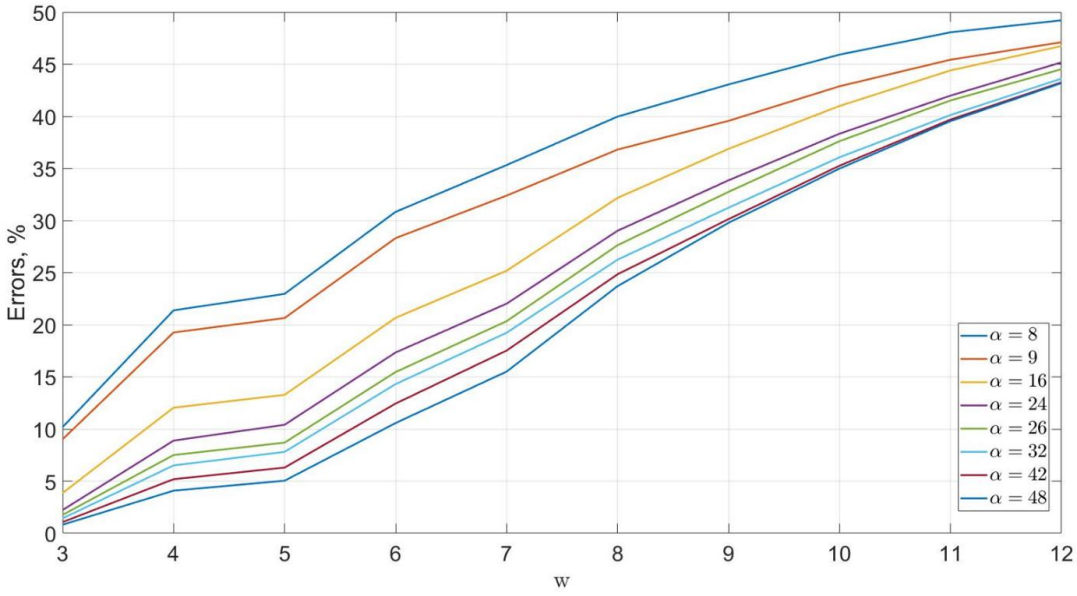


Рис. 3.19 — Графік залежності кількості помилок при декодуванні стеганоповідомлення від розміру вікна w при використанні кодових слів розміру 8×8 (3.28) та значень параметра (табл. 3.6)

Аналіз даних рис. 3.19 показує, що стеганографічний метод з кодовим управлінням вбудовуванням має також значну стійкість до атак розмиттям при значенні $\alpha \geq 16$ та розмірі вікна $w \leq 4$.

На рис. 3.20 представлено приклад вбудовування інформації в контейнер розміру 3872x2592 за допомогою стеганографічного методу з кодовим управлінням з використанням кодового слова (3.29). Вбудовування виконувалося у всі колірні компоненти, при цьому обсяг вбудованої інформації становив 470448 біт $= 57.4277$ Кб.

а) б)

Рис. 3.20 — Приклад вбудовування інформації за допомогою кодового слова (3.29): а) — вихідне зображення-контейнер, б) — стеганоповідомлення

Аналіз даних рис. 3.20 шляхом суб'єктивного ранжування не дозволяє визначити жодних артефактів або відмінностей стеганоповідомлення від вихідного контейнера.

3.4. Характеристики та порівняльний аналіз стеганографічного методу з кодовим управлінням

Стеганографічний метод з кодовим управлінням з використанням бінарних кодових слів, який описаний у підрозділі 3.1 характеризується дуже низьким впливом на вихідне зображення, через те, що абсолютна зміна в кожному пікселі при вбудовуванні інформації, не перевищує за амплітудою значення 1. Очевидно, що вбудовування інформації за допомогою багаторівневих кодових слів може збільшити вплив на пікселі зображення, однак, як показують подальші викладки, він залишається невеликим і строго контрольованим.

Кількісна оцінка спотворення ЦЗ-контейнера через вбудовування ДІ розробленим методом, проводиться з використанням різницевого показника PSNR, який визначається згідно до виразу (3.3).

Для варіанту стеганографічного методу з кодовим управлінням, який представлено у підрозділі 3.1 (на основі бінарних кодових слів), PSNR не залежить від виду обраного слова, а також від величини пропускної спроможності каналу прихованого зв'язку, розміру ЦЗ. Оскільки величина зміни у кожному з пікселів дорівнює 1 за модулем, то

$$MSE = \frac{1}{nm}\sum_i\sum_j \left|X(i,j) - M(i,j)\right|^2 = \\ = \frac{1}{nm}\sum_i\sum_j 1^2 = 1, \tag{3.32}$$

тоді

$$\mathrm{PSNR} = 20\lg(255) = 48.1308\, dB, \tag{3.33}$$

що говорить про практично достовірний факт забезпечення надійності сприйняття стеганоповідомлення для довільного ЦЗ-контейнера.

Отже, розроблений метод дозволив підвищити ефективність стеганографічної системи у порівнянні з існуючими аналогами: PSNR розробленого методу на $3.1308\,\mathrm{dB}$ вище ніж у методу [4], і більш ніж на $15.4708\,\mathrm{dB}$ вище, ніж у методу [21]. При цьому, при значенні коефіцієнта якості $QF = 70$ (що відповідає мінімальним рівням якості, застосовуваним у більшості сучасних систем передачі та обробки інформації), розроблений метод забезпечує на 33.7% меншу кількість помилок при декодуванні ДІ ніж метод [4], і на 2.57% менше помилок, ніж метод [21].

Розглянемо значення показника PSNR для варіанту стеганографічного методу з кодовим управлінням на основі багаторівневих кодових слів, який також є статичним та залежить лише від виду кодового слова, яке застосовується.

Нехай $K = [k_0, k_1, ..., k_{q-1}]$ — вектор, координати якого показують кількість значень $|t_i|$ у кодовому слові. Тоді, очевидно,

$$MSE = \frac{1}{\mu^2}\sum_{i=0}^{q-1} k_i |t_i|, \tag{3.34}$$

при цьому, через те, що для вбудовування інформації в кожен із блоків використовується однакове кодове слово, значення PSNR окремо взятого блоку буде відповідати значенню PSNR для всього зображення.

Таким чином, PSNR стеганоповідомлень, отриманих за допомогою стеганографічного методу з кодовим управлінням буде залежати тільки від виду кодового слова, що застосовується. Ми представляємо значення кожного з кодових слів $T^{+}_{m,8,(1,2)}$ розміру 8×8 з (3.28) для значень параметра (табл. 3.6)

α	$PSNR$
8	49.3802
9	46.3699
16	41.5987
24	38.4694 .
26	37.0757
32	35.6388
42	34.0654
48	32.6285

(3.35)

Результати порівняльного аналізу ефективності алгоритмічної реалізації розробленого методу із сучасними аналогами представлені в табл. 3.7. У табл. 3.7. прийняті такі умовні позначення: S — вбудовування інформації відбувається в просторовій області, DCT — вбудовування інформації відбувається в області трансформант ДКП блоків зображення, SVD — вбудовування інформації відбувається в області сингулярного розкладання блоків зображення.

Таблиця 3.7. — Результати порівняльного аналізу запропонованого стеганографічного методу із сучасними аналогами

Алгоритм / Метод	% помилок при заданому рівні *QF*										PSNR, dB	R	Обл. вбуд.
	10	20	30	40	50	60	70	80	90	100			
Стеганографічний метод з кодовим управлінням на основі бінарних кодових слів													
Метод с кодовим упр., $\mu=4$, $\lambda=1$, T_4^+	45.9923	39.3865	33.0043	26.8885	20.8169	16.1856	9.3461	2.9669	0.8089	0.6163	48.1	1/16	S
Метод с кодовим упр., $\mu=8$, $\lambda=1$, T_1^+	43.6133	31.3537	16.1266	5.5792	2.4352	1.5825	0.1392	0.0395	0.0055	0	48.1	1/64	S
Стеганографічний метод з кодовим управлінням на основі багаторівневих кодових слів													
Метод с кодовим упр., $T_{m,8,(1,2)}^+$, $\alpha=8$	44.4682	33.6170	19.0141	7.2899	2.2569	1.5852	1.2001	0.0600	0.0117	0	49.32	1/64	S
Метод с кодовим упр., $T_{m,8,(1,2)}^+$, $\alpha=16$	32.2259	1.6770	1.1473	0.0412	0.0246	0.0148	0.0073	0.0017	0.0001	0	41.6	1/64	S
Метод с кодовим упр., $T_{m,8,(1,2)}^+$, $\alpha=26$	1.8554	0.03	0.0116	0.0062	0.0037	0.0023	0.001	0.0002	0	0	37	1/64	S

Закінчення табл. 3.7.

Метод с кодовим упр., $T^{+}_{m,8,(1,2)}$, $\alpha = 32$	1.6249	0.0165	0.0063	0.0035	0.0021	0.0012	0.0005	0.0002	0	0	35.64	1/64	S
Інші стеганографічні методи та алгоритми, стійкі до атак стиском, зашумленням та розмиттям													
Алгоритм [4]	—	—	—	—	—	—	33.85(QF=75)	7.39(QF=85)	0.34(QF=95)	—	~45	<1/8	DCT
Алгоритм [20]	13	7	5	4	2	2	2	2	2	—	~ 34.7	1/64	SVD
Алгоритм [21]	—	—	—	—	24.74	14.24	2.71	0.2	0.05	—	~ 32.7	1/64	SVD
Алгоритм [22]	—	—	—	—	23.88	14.12	2.76	0.08	0.08	—	~ 32.7	1/16	SVD

Аналіз даних, представлених у табл. 3.7 дозволяє зробити висновок про те, що розроблений стеганографічний метод при збереженні високої надійності сприйняття стеганоповідомлення дозволяє отримати значну стійкість до атак стисненням. При практично цінних значеннях коефіцієнта $QF \geq 60$, кількість помилок при декодуванні у розробленого методу нижче, ніж у сучасних аналогів.

Аналіз даних, представлених у табл. 3.7 дозволяє прийти до висновку, що використання багаторівневих кодових слів у методі з кодовим управлінням вбудовуванням дозволяє збільшити його ефективність (менший відсоток помилок при декодуванні стеганоповідомлення, що зазнає атаки стисненням при $QF \geq 60$, більш високе значення PSNR=49.32), а також збільшити асортимент кодових слів, що дозволяють зробити акцент на підвищенні надійності сприйняття чи стійкості методу з кодовим управлінням вбудовуванням. При цьому застосування стеганографічного методу з кодовим управлінням вбудовуванням забезпечує найкраще серед усіх розглянутих аналогів співвідношення надійність сприйняття / стійкість до атак, а також простоту алгоритмічної реалізації та найвищу швидкодію, що пояснюється вбудовуванням інформації у просторовій області.

Безперечною перевагою розробленого стеганографічного методу в порівнянні з аналогами також є те, що вбудовування та вилучення інформації відбувається тут у просторовій області зображення, внаслідок чого відсутні додаткові обчислювальні витрати для переходу в область перетворення та назад.

3.5. Висновки

В третьому розділі розроблено теоретичні та практичні складові методології, запропоновано та досліджено ефективні стеганографічні методи, що забезпечують вбудовування ДІ у просторовій області контейнера. Отримані результати дозволили підвищити стійкість до атак проти вбудованого повідомлення у разі атаки стиском найбільшої сили (QF=10) у 8.125 разів, при цьому оцінка надійності сприйняття покращена на 3%.

Відзначимо основні результати проведених досліджень:

1. На основі сформульованого у Розділі 2 теоретичного базису розроблено стеганографічний метод, для якого побудовано множину кодових

слів практично цінних порядків $N=4$ і $N=8$, що забезпечують найкращу стійкість стеганоповідомлення до атаки стисненням.

2. Експериментальні дослідження, а також проведений порівняльний аналіз алгоритмічних реалізацій розробленого стеганографічного методу з сучасними аналогами показав, що він здатний забезпечити надійність сприйняття стеганоповідомлення (показник PSNR є постійним і дорівнює 48.1308 дБ, що перевищує значення PSNR всіх розглянутих у роботі сучасних аналогів), а також низьку ймовірність помилок при декодуванні ДІ, яка при рівнях якості $QF \geq 60$ нижче, ніж у розглянутих аналогів. При цьому, на відміну від розглянутих аналогів, розроблений метод здійснює вбудовування ДІ в просторовій області, що визначає простоту його алгоритмічної реалізації та високу швидкодію, наслідком чого є потенційна можливість його використання в режимі реального часу для потокового контейнера.

3. Введено та обґрунтовано визначення енергії та коефіцієнта селективності кодового слова, що застосовується у стеганографічному методі з кодовим управлінням. Розраховано значення коефіцієнта селективності кодових слів на основі рядків матриці Уолша-Адамара, що застосовуються у методі з кодовим управлінням. Встановлено та обґрунтовано існування кодових слів, які мають абсолютну селективність. Встановлено, що зі зростанням розміру застосовуваних блоків є тенденція до зменшення коефіцієнта селективності з огляду на наявність ефекту «близького сусіда», яка, проте, відбувається за рахунок залучення трансформант із близькими за значенням частотами, що мають подібну стійкість до можливих атак на вбудоване повідомлення. При цьому відношення суми модулів низькочастотних коефіцієнтів ДКП до суми модулів решти всіх коефіцієнтів ДКП зростає зі збільшенням розміру кодового слова. Доведено, а також практично підтверджено, що збільшення розміру кодового слова призводить до збільшення стійкості стеганоперетворення з кодовим управлінням.

4. Представлено набір багаторівневих кодових слів практично цінних розмірів 4×4, 8×8 і 16×16, що забезпечують високі значення коефіцієнта селективності, і впливають з високим степенем вибірковості на задані трансформанти ДКП. Зазначений набір кодових слів забезпечує високий рівень гнучкості стеганографічного методу з кодовим управлінням, який дозволяє «заточити» його під вирішення наступних завдань: забезпечення найкращої надійності сприйняття стеганоповідомлення; забезпечення найкращої стійкості стеганографічного методу до атак стисненням, зашумленням, розмиттям; забезпечення найкращої пропускної спроможності.

5. Проведено дослідження роботи стеганографічного методу з кодовим управлінням вбудовуванням на основі представлених багаторівневих кодових слів, які показують високий рівень стійкості до атак стисненням, зашумленням та розмиттям при забезпеченні високої пропускної спроможності та надійності сприйняття. Так, порівняльний аналіз розробленого методу з відомими аналогами дозволив встановити, що він забезпечує найкраще серед усіх розглянутих аналогів співвідношення надійність сприйняття / стійкість до атак. При цьому використання багаторівневих кодових слів дозволяє отримати кращі результати (при значенні стиснення $QF \geq 60$, більше на 4.32 дБ значення PSNR при меншій кількості помилок при вилученні інформації зі стисненого повідомлення) порівняно з використанням бінарних кодових слів.

Список використаних джерел у третьому розділі

1. Hussain M. et al. Image steganography in spatial domain: A survey. Signal Processing: Image Communication, 2018. Vol. 65. pp. 46-66. doi: 10.1016/j.image.2018.03.012

2. Samidha D., Agrawal D. Random image steganography in spatial domain. International Conference on Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System, 2013. pp. 1-3. doi: 10.1109/icevent.2013.6496564

3. Hu D. et al. A spatial image steganography method based on nonnegative matrix factorization. IEEE signal processing letters, 2018. Vol. 25, No. 9. pp. 1364-1368. doi: 10.1109/lsp.2018.2856630

4. Zhu Z., Zheng N., Qiao T., Xu M. Robust Steganography by Modifying Sign of DCT Coefficients. IEEE Access, 2019. Vol. 7. pp. 168613-168628. doi: 10.1109/access.2019.2953504

5. Hamid N. et al. Enhancing visual quality of spatial image steganography using SqueezeNet deep learning network //Multimedia Tools and Applications. 2021. Vol. 80. No. 28. P. 36093-36109.

6. Maji G., Mandal S., Sen S. Cover independent image steganography in spatial domain using higher order pixel bits //Multimedia Tools and Applications. 2021. Vol. 80. No. 10. P. 15977-16006.

7. Karthikeyan N. et al. Enhancing the confidentiality of text embedding using image steganography in spatial domain //AIP Conference Proceedings. AIP Publishing LLC, 2021. Vol. 2387. No. 1. P. 140013.

8. Gajabe R., Ali S. T. Secret Key-Based Image Steganography in Spatial Domain //International Journal of Image and Graphics. 2021. P. 2250014.

9. Rashid M., Arora B. Image Steganography Using Bit Differencing Technique //Proceedings of Second International Conference on Computing, Communications, and Cyber-Security. Springer, Singapore, 2021. P. 833-843.

10. Navadiya C., Sanghani N. Comparative Survey of Digital Image Steganography Spatial Domain Techniques //Data Science and Intelligent Applications. Springer, Singapore, 2021. P. 491-497.

11. Bansal D., Chhikara R. An improved DCT based steganography technique. International Journal of Computer Applications. 2014. Vol. 102, No.14. pp. 46-49. doi: 10.5120/17887-8861

12. Walia E., Jain P., Navdeep N. An analysis of LSB & DCT based steganography. Global Journal of Computer Science and Technology. 2010. 2010. Vol. 10, Issue 1. pp. 4-8.

13. Rachmawanto E. H. et al. Secure image steganography algorithm based on dct with otp encryption. Journal of Applied Intelligent System, 2017. Vol. 2, No. 1. pp. 1-11. doi: 10.33633/jais.v2i1.1330

14. Varuikhin V., Levina A. Continuous Wavelet Transform Applications In Steganography. Procedia Computer Science. 2021. Vol. 186. P. 580-587.

15. Lingamallu N. S., Veeramani V. Secure and covert communication using steganography by Wavelet Transform. Optik. 2021. Vol. 242. – P. 167167.

16. Mathivanan P., Balaji Ganesh A. ECG steganography based on tunable Q-factor wavelet transform and singular value decomposition. International Journal of Imaging Systems and Technology. 2021. Vol. 31. No. 1. P. 270-287.

17. Kumar M., Hussaini T. A Neural Network Based Image Steganography Method using Cyclic Chaos and Integer Wavelet Transform. 2021 Asian Conference on Innovation in Technology (ASIANCON). – IEEE, 2021. P. 1-6.

18. Ambika, Biradar R. L. A robust low frequency integer wavelet transform based fractal encryption algorithm for image steganography. International Journal of Advanced Intelligence Paradigms. 2021. Vol. 19. No. 3-4. P. 342-356.

19. Sharafi J., Khedmati Y., Shabani M. M. Image steganography based on a new hybrid chaos map and discrete transforms //Optik. 2021. Vol. 226. P. 165492.

20. Мельник М.А. Стеганоалгоритм, устойчивый к сжатию. Інформаційнабезпека. 2012. №2(8). С. 99-106.

21. Chang C.C., Lin C.C., Hu Y.S. An SVD oriented watermark embedding scheme with high qualities for the restored images. International journal of innovative computing, information & control, 2007.Vol. 3, No. 3. pp. 609-620.

22. Chanu Y. J., Singh Kh. M., Tuithung T. A Robust Steganographic Method based on Singular Value Decomposition. International Journal of Information & Computation Technology, 2014. Vol. 4, No. 7. pp. 717-726.

23. Abdallah H. A., Hadhoud M. M., Shaalan A. A. An efficient SVD image steganographic approach. International Conference on Computer Engineering & Systems, 2009. pp. 257-262. doi: 10.1109/icces.2009.5383271

24. Bhattacharyya S., Mondal S., Sanyal G. A Robust Image Steganography using Hadamard Transform. International Conference on Information Technology in Signal and Image Processing, Mumbai, 2013. pp. 416-426.

25. Sneha P. S., Sankar S., Kumar A. S. A chaotic colour image encryption scheme combining Walsh–Hadamard transform and Arnold–Tent maps. Journal of Ambient Intelligence and Humanized Computing, 2020. Vol. 11, No. 3. pp. 1289-1308. doi: 10.1007/s12652-019-01385-0

26. Курс К. С., Сабирзянова Э. И., Кротова Е. Л. LSB-стеганография. Автоматизированные системы управления и информационные технологии. 2020. С. 465-472.

27. Кобозева А. А., Хорошко В. А. Анализ информационной безопасности. К.: Изд. ГУИКТ, 2009. 251 с.

28. Костырка О.В. Анализ преимуществ пространственной области цифрового изображения-контейнера для стеганопреобразования. Інформатика та математичніметоди в моделюванні. №3. С. 275-282.

29. Мазурков М. И. Системы широкополосной радиосвязи. Одесса : Наука и Техника, 2010. с. 340.

30. NRCS Photo Gallery // United States Department of Agriculture. URL: https://www.nrcs.usda.gov/wps/portal/nrcs/main/national/newsroom/multimedia/

31. Прохожев Н. Н., Михайличенко О. В., Коробейников А. Г. Влияние внешних воздействий на DC коэффициенты матриц ДКП в полутоновых изображениях. Научно-технический вестник информационных технологий, механики и оптики. 2008. №56. С. 57-62.

32. Деммель Дж. Вычислительная линейная алгебра. М.: Мир, 2001. 430 с.

33. Гантмахер Ф. Р. Теория матриц. М.: «Наука» 1966. 576 с.

Westfeld A., Pfitzmann A. Attacks on steganographic systems //International workshop on information hiding. – Springer, Berlin, Heidelberg, 1999. pp. 61-76.

Розділ 4.

РОЗРОБКА СТЕГАНОГРАФІЧНИХ СИСТЕМ З МНОЖИННИМ ДОСТУПОМ НА ОСНОВІ ПЕРЕТВОРЕННЯ УОЛША-АДАМАРА

Більшість сучасних стеганографічних методів дозволяють організувати прихований стеганографічний канал лише між парою абонентів.

При цьому для вирішення низки практичних завдань виникає необхідність організації множинного доступу до прихованого каналу, що допускає одночасну роботу множини авторизованих користувачів при забезпеченні ефективного приховування самого факту передачі інформації.

Сьогодні відомі [1…3] методи організації прихованого стеганографічного каналу передачі інформації з множинним доступом, що засновані на технології MC-CDMA [4] із використанням перетворення Уолша-Адамара.

Однак, як показують дослідження, наявні методи володіють низкою недоліків, серед яких є той факт, що число абонентів є строго регламентованим і має дорівнювати $N = 2^k = 2,4,8,16,...$, а також додаткова інформація від кожного з абонентів має вбудовуватися одночасно. Суттєвим недоліком використання технології MC-CDMA є і дезінтегрованість поділу каналів із застосовуваним стеганографічним методом, тобто, технологія MC-CDMA не показує, як конкретно має відбуватися вбудовування та вилучення додаткової інформації.

Проведені дослідження показують, що існуючі методи організації стеганографічних систем з множинним доступом можуть бути суттєво покращені, а також створені нові методи, засновані на результатах, отриманих у попередніх розділах.

Метою цього розділу є розробка методів забезпечення множинного доступу до стеганографічного каналу, що забезпечують високу надійність сприйняття та гнучкість розподілення ресурсів.

Для досягнення мети розділу необхідно вирішити наступні задачі:

1. розробити теоретичні засади підвищення ефективності стеганографічної системи передавання інформації з множинним доступом на основі перетворення Уолша-Адамара, на базі яких виконати синтез ефективних кодів для кодування векторів даних;
2. розробити стеганографічний метод з множинним доступом на основі кодового управління та частотних розстановок;
3. розробити стеганографічний метод з множинним доступом на основі частотно-просторових матриць.

4.1. Підвищення ефективності стеганографічного методу з множинним доступом на основі технології MC-CDMA

Одним із ефективних способів організації множинного доступу в стеганоканалі є використання технології кодового розподілу каналів MC-CDMA [4] на основі перетворення Уолша-Адамара. Технологія MC-CDMA [4…6] надає значну гнучкість розподілу ресурсів стеганоканалу між користувачами. Так, для деяких більш пріоритетних користувачів може бути виділено кілька каналів зв'язку, що призведе до кратного збільшення пропускної спроможності стеганоканалу для даних користувачів.

Проте, незважаючи на високу ефективність та перспективність використання технології кодового розподілу у стеганоканалах, це питання залишається досить малодослідженим. У літературі [1,2] представлені лише дані про організацію окремих випадків стеганосистем на основі технології кодового розподілу каналів MC-CDMA з числом абонентів $N=4$, і тільки на

основі кодів Гаффмана, при цьому фундаментальні параметри кодування групового сигналу, так само як і питання оптимізації вибору числа каналів N з точки зору мінімізації значення середнього числа двійкових розрядів для представлення елемента групового сигналу залишаються невідомими, що ставить завдання подальшого дослідження та вдосконалення цього стеганографічного методу.

Розглянемо особливості функціонування технології MC-CDMA для організації множинного доступу в стеганоканалі.

Виберемо для організації кодового розподілу каналів ортогональне перетворення Уолша-Адамара. Безперечною перевагою перетворення Уолша-Адамара є те, що елементи його базисних векторів приймають лише значення бінарного алфавіту $\{\pm 1\}$, що відповідає бінарній природі інформації, яка вбудовується. Ця обставина, разом із простотою правил побудови матриць перетворення Уолша-Адамара, дозволяє значно спростити як програмну, так і апаратну реалізацію алгоритмів вбудовування і вилучення додаткової інформації.

Розглянемо докладніше принципи технології MC-CDMA, що застосовуються у стеганографічних системах з множинним доступом (рис. 4.1). Так, біти вихідних даних d_i, що надходять по кожному каналу змінюють знак однієї з ортогональних функцій W_i. Далі відбувається множення на деяку константу g_i (найчастіше приймають $g_i = 1$) та підсумовування. Отриманий сигнал і являє собою додаткову інформацію, що має бути надалі вбудована у стеганоповідомлення [4].

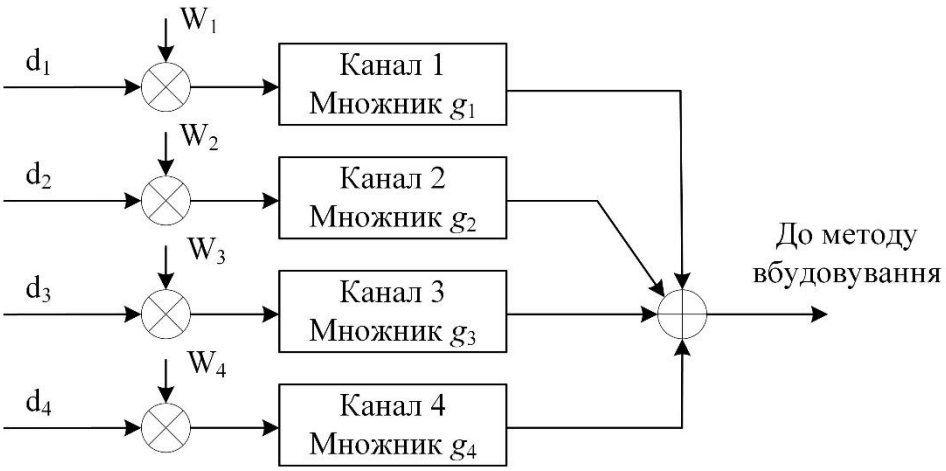


Рис. 4.1 — Схема ущільнення каналів за технологією MC-CDMA

Розглянемо конкретний приклад. Нехай, $d_1 = [1,1]$, $d_2 = [-1,-1]$, $d_3 = [-1,1]$, $d_4 = [1,-1]$, тоді як в якості системи ортогональних функцій обрані функції Уолша довжини $N = 2^k$, впорядковані за Адамаром [3]

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix}, \tag{4.1}$$

де $H_1 = 1$.

Для нашого випадку $k = 4$, таким чином, маємо систему функцій

$$\begin{cases} W_1 = +1,+1,+1,+1; \\ W_2 = +1,-1,+1,-1; \\ W_3 = +1,+1,-1,-1; \\ W_4 = +1,-1,-1,+1. \end{cases} \tag{4.2}$$

Виконуючи перетворення (рис. 4.1) отримуємо результуючий сигнал, який подається на вхід стеганографічного методу для подальшого вбудовування

$$\begin{array}{cccc|cccc} +1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 \\ -1 & +1 & -1 & +1 & -1 & +1 & -1 & +1 \\ -1 & -1 & +1 & +1 & +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 & -1 & +1 & +1 & -1 \\ \hline 0 & 0 & 0 & 4 & 0 & 4 & 0 & 0 \end{array}. \tag{4.3}$$

Кожен користувач, отримавши послідовність $S=[0,0,0,4,0,4,0,0]$ після вилучення зі стеганоповідомлення на приймальній стороні може виділити повідомлення, яке призначено конкретно йому відповідно до формули [4]

$$d_\alpha = \frac{\sum_{i=0}^{N} S \cdot W_\alpha}{g_\alpha N}. \tag{4.4}$$

Наприклад, можемо виділити вихідне повідомлення передане другим каналом

$$\begin{array}{cccccc} \times & 0 & 0 & 0 & 4 \\ & +1 & -1 & +1 & -1 \\ \hline & 0 & 0 & 0 & -4 \end{array} \quad \begin{array}{cccccc} \times & 0 & 4 & 0 & 0 \\ & +1 & -1 & +1 & -1 \\ \hline & 0 & -4 & 0 & 0 \end{array}. \tag{4.5}$$

Обчислюючи суму, і розділивши її на $g_2 N$ одержуємо вихідний сигнал $d_2=[-1,-1]$.

Загалом схема стеганосистеми з множинним доступом з використанням технології MC-CDMA має вигляд, зображений на рис. 4.2 [1].

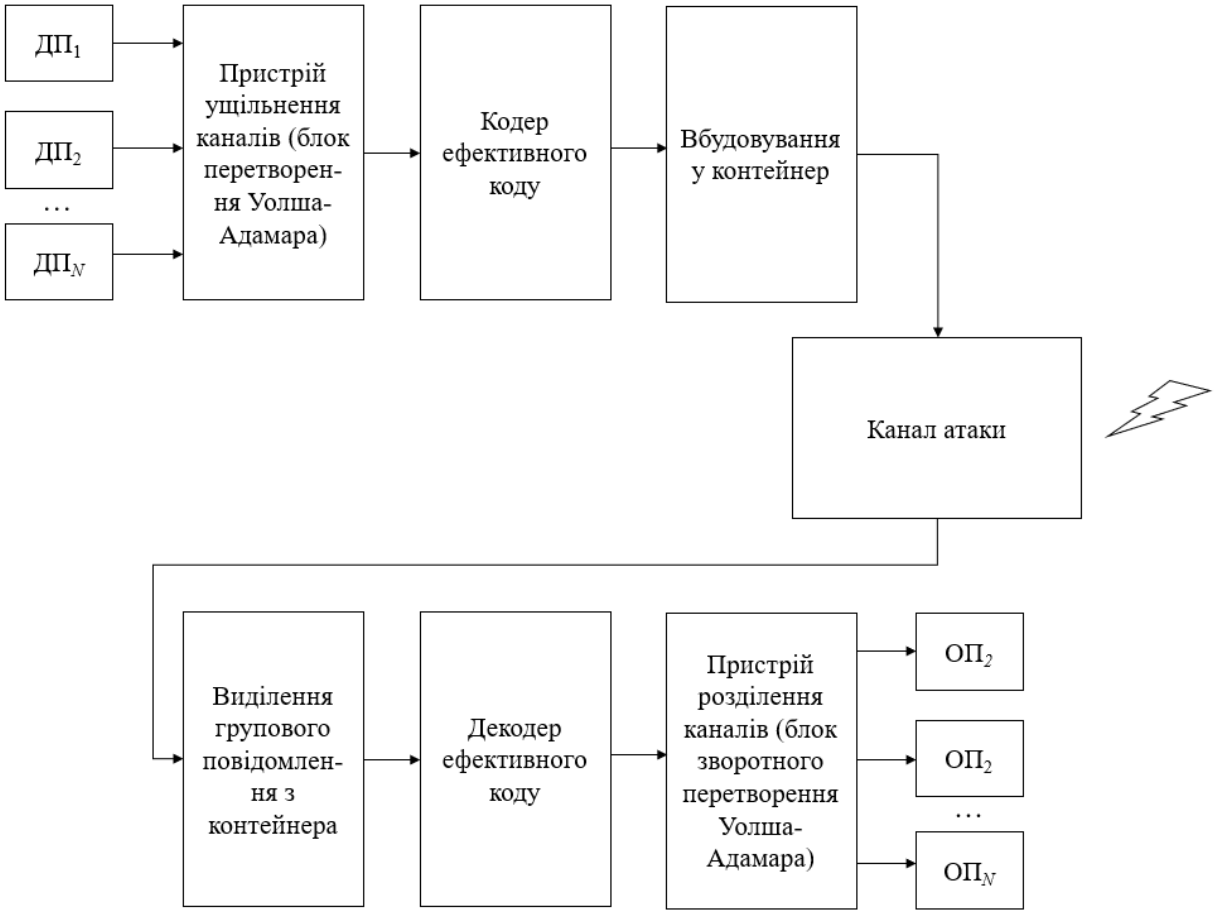


Рис. 4.2. — Структурна схема стеганосистеми з множинним доступом із використанням технології MC-CDMA

Розглянемо докладніше принципи функціонування пристрою ущільнення каналів. Відповідно до технології MC-CDMA біти вхідних даних d_i, що надходять по кожному каналу, змінюють знак однієї з ортогональних функцій W_i.

Виходячи з обраного виду ортогонального перетворення для побудови матриць Уолша-Адамара порядку $N=2^k$, рядки (стовпці) яких є зазначеними функціями Уолша, будемо використовувати конструкцію Сильвестра [1].

Таким чином, груповий сигнал, який повинен бути вбудований у контейнер у стеганосистемах з кодовим розподілом каналів на основі технології MC-CDMA, фактично є послідовністю коефіцієнтів перетворення Уолша-Адамара вектора даних від кожного з користувачів $\{d_i\}$[7].

Ця обставина веде до необхідності застосування ефективного кодування коефіцієнтів перетворення Уолша-Адамара задля забезпечення зручності подальшого вбудовування.

У роботі [1] для здійснення операції ефективного кодування коефіцієнтів перетворення Уолша-Адамара запропоновано використовувати ефективні коди Гаффмана [8, 9], що вимагають попереднього збору статистики появи символів алфавіту, що кодується.

Це завдання було вирішено у роботі [1] за допомогою повного перебору для значення $N=4$. Проте зазначимо, що для практично цінних значень числа каналів $N>32$ застосування методу повного перебору для отримання статистики появи коефіцієнтів перетворення Уолша-Адамара утруднено з обчислювальної точки зору, що обумовлює необхідність розробки відповідного теоретичного базису.

Розглянемо основні визначення теорії кодування, необхідні нам для подальших досліджень.

Визначення 4.1 [9]. Вагою Гемінга w_t бінарної послідовності називається кількість символів "–1" у ній.

Визначення 4.2 [10]. Розбалансом Δ бінарної послідовності називається різниця числа її символів «+1» та «–1»

$$\Delta = K^+ - K^-, \tag{4.6}$$

де K^+ і K^- число символів «+1» і «–1», відповідно, що містяться в бінарній послідовності.

На основі розглянутих визначень сформулюємо твердження, що визначають можливі значення коефіцієнтів перетворення Уолша-Адамара.

Твердження 4.1. Множина значень $\{0,\pm 2,...,\pm N\}$, які може приймати розбаланс Δ двійкових послідовностей, становить множину можливих значень коефіцієнтів перетворення Уолша-Адамара.

Доказ. Відповідно до визначення перетворення Уолша-Адамара (х.4) кожен коефіцієнт перетворення Уолша-Адамара кодового слова T, яке

належить множині кодових слів повного коду, є скалярним добутком вихідного кодового слова на відповідну функцію Уолша-Адамара (стовпець матриці Уолша-Адамара). Таким чином, відповідно до **Визначення 4.2**, кожен коефіцієнт перетворення Уолша-Адамара є розбалансом поелементного добутку вихідного кодового слова на відповідну функцію Уолша-Адамара.

З огляду на те, що довжина послідовності дорівнює N, а всі її елементи $t_i \in \{\pm 1\}$, то розбаланс послідовності ваги w_t дорівнює

$$\Delta = (N - w_t) - w_t = N - 2w_t . \tag{4.7}$$

Зважаючи на те, що можливі значення ваги $w_t \in \{0,1,...N\}$, доходимо висновку, що значення розбалансу належать множині $\Delta \in \{0, \pm 2, ..., \pm N\}$.

Твердження 4.2. Імовірність появи коефіцієнта перетворення Уолша-Адамара із заданим значенням ω_i визначається як

$$p(\omega_i) = p(-\omega_i) = \frac{C_N^{\frac{N-\omega_i}{2}}}{2^N} . \tag{4.8}$$

Доказ. Розглянемо перший коефіцієнт перетворення Уолша-Адамара, що є розбалансом добутку послідовності T на перший стовпець матриці Уолша-Адамара (відповідно до доказу **Твердження 4.1**), який за побудовою складається з символів «+1», тобто $[+1+1...+1]^T$. Таким чином, очевидно що даний коефіцієнт є розбалансом послідовності T.

З іншого боку, кількість послідовностей довжини N із заданою вагою w_t дорівнює $J_{w_t} = C_N^{w_t}$.

Нехай вага послідовності T дорівнює w_t, тоді відповідно до (4.7) значення її ваги може бути виражено через розбаланс як $w_t = \frac{N - \Delta}{2}$. З огляду на дію **Твердження 4.1.** можливі значення коефіцієнтів перетворення Уолша-Адамара дорівнюють значенням розбалансу послідовності T, і належать множині $\omega_i \in \{0, \pm 2, ..., \pm N\}$. Отже кількість значень першого

коефіцієнта перетворення Уолша-Адамара дорівнює кількості послідовностей із заданим розбалансом $J(\omega_i)=C_N^{\frac{N-\omega_i}{2}}$.

Покажемо, що це правильно для будь-якого коефіцієнта перетворення Уолша-Адамара.

Розглянемо повний бінарний код потужності $J=2^N$, кожне кодове слово якого має довжину N

$$\begin{matrix}[+1 & +1 & \dots & +1]\\ [+1 & +1 & \dots & -1]\\ \vdots & \vdots & & \vdots\\ [-1 & -1 & \dots & -1]\end{matrix}. \qquad (4.9)$$

Коефіцієнти перетворення Уолша-Адамара, що залишилися, знаходяться як значення розбалансів добутків відповідної функції Уолша (стовпця матриці Уолша-Адамара) на послідовності з повного коду

$$\begin{matrix}[h_N & h_{N-1} & \dots & h_1]\\ \times & \times & & \times\\ [+1 & +1 & \dots & +1]\\ [+1 & +1 & \dots & -1]\\ \vdots & \vdots & & \vdots\\ [-1 & -1 & \dots & -1]\end{matrix}. \qquad (4.10)$$

Очевидно, що ця операція (відома в теорії сигналів як побудова похідної системи сигналів [11]), застосована до повного коду, збереже всі його кодові слова з точністю до їх послідовності. Ця обставина обумовлена відсутністю стовпців повного коду, які є інверсією один одного, що веде до того, що будь-яке знакове кодування стовпців повного коду зберігає всі його кодові слова.

Отже, незмінною залишиться і кількість кодових слів повного коду, що мають задане значення розбалансу Δ і, відповідно, частоти появи того чи іншого значення коефіцієнтів перетворення Уолша-Адамара ω_i. Зважаючи на те, що загальна кількість коефіцієнтів перетворення Уолша-Адамара в одному векторі становить N, то частота появи того чи іншого значення коефіцієнта перетворення Уолша-Адамара становить $J(\omega_i)=NC_N^{\frac{N-\omega_i}{2}}$. А, отже,

ймовірність появи того чи іншого коефіцієнта перетворення Уолша-Адамара дорівнюватиме відношенню частот появи даного коефіцієнта до загальної кількості коефіцієнтів перетворення Уолша-Адамара повного коду $p(\omega_i)=\frac{NC_N^{\frac{N-\omega_i}{2}}}{N2^N}=\frac{C_N^{\frac{N-\omega_i}{2}}}{2^N}$.

Відзначимо також, що властивість рівності ймовірностей появи рівних за амплітудою, але протилежних за знаком коефіцієнтів перетворення Уолша-Адамара $p(\omega_i)=p(-\omega_i)$ легко довести, розкривши число сполучень у чисельнику формули (4.7)

$$p(\omega_i)=\frac{C_N^{\frac{N-\omega_i}{2}}}{2^N}= \\ =\frac{1}{2^N}\frac{N!}{\left(\frac{N-\omega_i}{2}\right)!\left(N-\frac{N-\omega_i}{2}\right)!}= \\ =\frac{1}{2^N}\frac{N!}{\left(\frac{N-\omega_i}{2}\right)!\left(\frac{N+\omega_i}{2}\right)!}, \tag{4.11}$$

і з іншого боку

$$p(-\omega_i)=\frac{C_N^{\frac{N+\omega_i}{2}}}{2^N}= \\ =\frac{1}{2^N}\frac{N!}{\left(\frac{N+\omega_i}{2}\right)!\left(N-\frac{N+\omega_i}{2}\right)!}= \\ =\frac{1}{2^N}\frac{N!}{\left(\frac{N+\omega_i}{2}\right)!\left(\frac{N-\omega_i}{2}\right)!}. \tag{4.12}$$

Розглянемо приклад роботи **Твердження 4.2.** При $N=16$ і $\omega_i=2$ отримуємо, що можливість появи даного коефіцієнта дорівнює $p(2)=\frac{C_{16}^{\frac{16-2}{2}}}{2^{16}}=\frac{C_{16}^{7}}{2^{16}}=0.1746$, що відповідає фактично отриманому результату.

Відповідно до (4.8) обчислимо решту ймовірностей появи коефіцієнтів перетворення Уолша-Адамара для цього значення $N=16$, для кожного з яких побудуємо кодові слова коду Гаффмана (табл. 4.1.).

Таблиця 4.1. — Код Гаффмана для коефіцієнтів перетворення Уолша-Адамара при $N=16$

Символ	Ймовірність появи	Код	Довжина кодового слова
ω_0	0.1964	11	2
ω_1	0.1746	001	3
ω_2	0.1746	000	3
ω_3	0.1222	100	3
ω_4	0.1222	011	3
ω_5	0.0667	0101	4
ω_6	0.0667	0100	4
ω_7	0.0278	10100	5
ω_8	0.0278	1011	4
ω_9	0.0085	1010100	7
ω_{10}	0.0085	101011	6
ω_{11}	0.0018	101010100	9
ω_{12}	0.0018	10101011	8
ω_{13}	0.0002	10101010100	11
ω_{14}	0.0002	1010101011	10
ω_{15}	0.0000153	101010101011	12
ω_{16}	0.0000153	101010101010	12

Аналіз представлених у табл. 4.1. даних приводить до висновку, що середня довжина кодового слова необхідного для передачі одного коефіцієнта перетворення Уолша-Адамара при кількості каналів, що розділяються $N=16$, становить $l_{av}=3.1041$.

Використовуючи **Твердження 4.2.**, неважко розрахувати l_{av} і для інших значень N. Тим не менш, l_{av} залежить від особливостей коду Гаффмана. Відповідно до теореми Шеннона про кодування джерела [12], середня довжина кодового слова, необхідна для кодування символу його алфавіту не перевищує інформаційну ентропію даного алфавіту $l_{av} \geq H(\{\omega_i\})$, де

$$H(\{\omega_i\})_N = -\sum_{i=0}^{N} p(\omega_i) \cdot \log_2 p(\omega_i). \qquad (4.13)$$

Таким чином, при довільному значенні N маємо таку нерівність

$$l_{av} \geq -\sum_{i=0}^{N} \frac{C_N^{\frac{N-\omega_i}{2}}}{2^N} \cdot \log_2 \frac{C_N^{\frac{N-\omega_i}{2}}}{2^N}, \quad \omega_i = 0, \pm 2, ..., \pm N - 1. \qquad (4.14)$$

При заданому N права частина виразу (4.14) становить нижню границю кількості двійкових розрядів, необхідних для кодування одного коефіцієнта перетворення Уолша-Адамара.

У табл. 4.2. наведені обчислені відповідно до (4.8) імовірнісні характеристики коефіцієнтів перетворення Уолша-Адамара для інших практично цінних значень числа каналів, що розділяються $N = 2, 4, 8, 16, 32, 64, 128, 256, 512$, а також значення l_{av} і $H(\{\omega_i\})$.

Таблиця 4.2. — Середня довжина кодового слова Гаффмана в залежності від значення N

N	Кількість різних ω_i	$p(\omega_0)$	$p(\omega_N)$	l_{av}	$H(\{\omega_i\})_N$
2	3	0.5	0.25	1.5	1.5
4	5	0.375	0.0625	2.125	2.0306
8	9	0.2734375	0.0039	2.5859	2.5442
16	17	0.196380615234375	0.000015258789063	3.1041	3.0465
32	33	0.139949934091419	0.000000000232831	3.5665	3.5470
64	65	0.099346753747967	$5.4 \cdot 10^{-20}$	4.0899	4.0471
128	129	0.070386092170015	$2.9 \cdot 10^{-39}$	4.5656	4.5471
256	257	0.049819109936140	$8.6 \cdot 10^{-78}$	5.0898	5.0471
512	513	0.035244635485839	$7.5 \cdot 10^{-155}$	5.5664	5.5471

Для наочності, на основі даних табл. 4.2., на рис. 4.3. побудований графік залежності середньої довжини кодового слова Гаффмана, необхідної для кодування одного коефіцієнта перетворення Уолша-Адамара, а також інформаційної ентропії (4.14) від кількості каналів N, що розділяються.

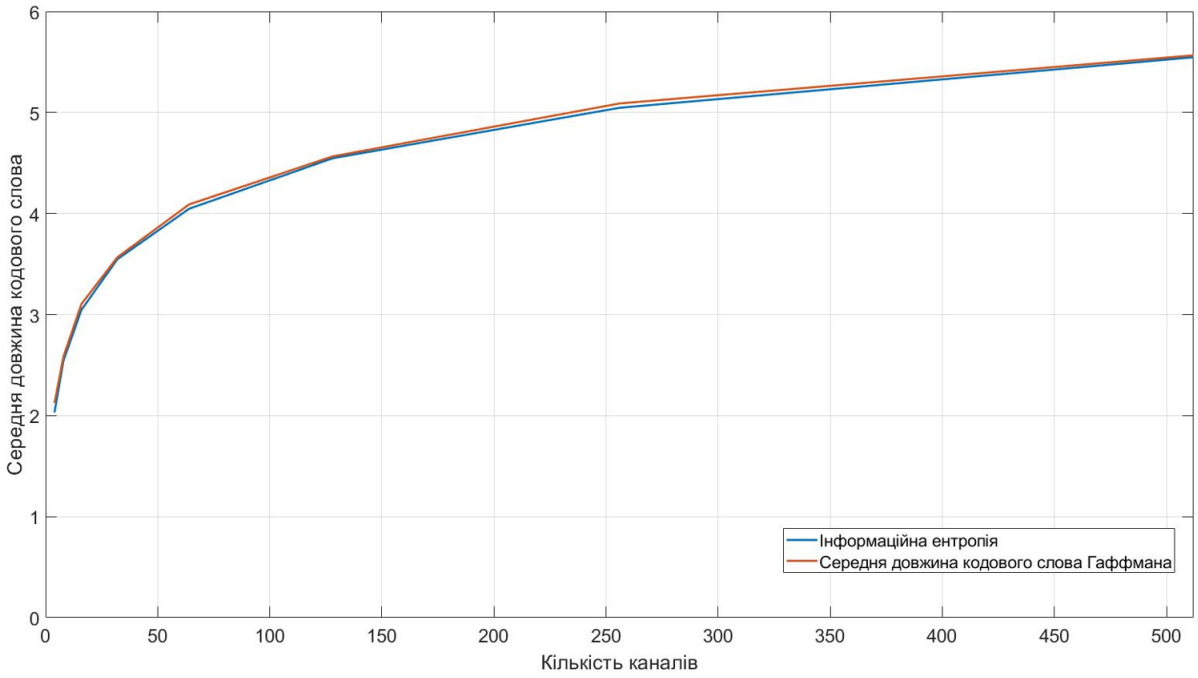


Рис. 4.3. — Графік залежності середньої довжини кодового слова від кількості каналів N, що розділяються

Аналіз даних рис. 4.3. свідчить про наростання середньої довжини кодового слова при зростанні кількості каналів N, що розділяються, що говорить про зростання надмірності в поданні інформації, що передається при збільшенні числа каналів, що розділяються за допомогою технології MC-CDMA.

Розглянемо послідовність елементів, які є різницею $\{\delta_i\} = H(\{\omega_i\})_N - H(\{\omega_i\})_{N/2}$ для значень $N = 4,8,16,32,64,128,256,512$

$$\{\delta_i\} = [0.53063906,\ 0.51355844,\ 0.50235205,\ 0.50042043,\ 0.50009527,\ 0.50002286,\ 0.50000560]. \quad (4.15)$$

Аналіз емпірично побудованої послідовності (4.15) дозволяє стверджувати, що зі зростанням числа каналів N, що розділяються, збільшення в інформаційній ентропії коефіцієнтів перетворення Уолша-Адамара (а, значить, і в мінімально можливому значенні середньої довжини кодового слова l_{av}) прямує до значення $1/2$ при кожному подвоєнні величини N.

Проведені дослідження дозволили встановити, що при значенні кількості каналів, що розділяються $N=4$, застосування ефективного коду Гаффмана не є найбільш ефективним способом кодування коефіцієнтів перетворення Уолша-Адамара.

Встановлено, що для підвищення ефективності кодування коефіцієнтів перетворення Уолша-Адамара може бути використаний спеціальний клас досконалих алгебраїчних конструкцій — бент-послідовностей.

Визначення 4.3 [13, 14]. Бінарна послідовність $B=[b_0,b_1,\cdots,b_i,\cdots,b_{N-1}]$, де $b_i\in\{\pm1\}$ — коефіцієнти, парної довжини $N=2^{2k}$, $i=0,1,...,N-1$; N — порядок матриці Уолша-Адамара, називається бент-послідовністю (БП), якщо вона має рівномірний за модулем спектр Уолша-Адамара $W_B(\omega)$, який представимо в матричній формі

$$S_B(\varpi)=BH,\ \varpi=0,1,...,N-1, \tag{4.16}$$

де H — матриця Уолша-Адамара порядку N.

Виходячи з визначення, кожен коефіцієнт перетворення Уолша-Адамара бент-послідовності $S_B(\varpi=0),S_B(\varpi=1),...,S_B(\varpi=N-1)$ набуває значень з множини $\left\{\pm\sqrt{N}\right\}$. Таким чином, вектор коефіцієнтів перетворення Уолша-Адамара бент-послідовності є, за своєю суттю, бінарною послідовністю, відображеною на алфавіт $\left\{\pm\sqrt{N}\right\}$, так як кожен його елемент набуває лише одного з двох можливих значень, які відрізняються знаком.

Зрозуміло, що коефіцієнти перетворення Уолша-Адамара бент-послідовності є виключно зручними для вбудовування інформації у контейнер.

Тим не менш, бент-послідовності є вкрай непередбачуваними та складними математичними об'єктами через свою максимально можливу нелінійність.

Сьогодні у відкритій літературі недоступні як методи синтезу бент-послідовностей для довільної довжини N, так і точна оцінка кількості бент-послідовностей для довжин $N \geq 1024$.

Зазначимо, однак, що класи бент-послідовностей для довжин $N \leq 64$ сьогодні досить добре вивчені [13…15], зокрема розроблено ефективні методи їх синтезу.

У табл. 4.3. представлені потужності класів бент-послідовностей для практично цінних довжин, а також відсотковий вміст бент-послідовностей у повному коді відповідної довжини.

Таблиця 4.3. — Потужності класів бент-послідовностей

N	Потужність повного коду	Кількість БП	% вмісту БП у повному коді
4	$2^4 = 16$	8	50
16	$2^{16} = 65536$	896	1.37
64	$2^{64} =$ 18446744073709551616	5425430	$2.94 \cdot 10^{-11}$
256	2^{256}	99270589265934370305785861242880	$8.57 \cdot 10^{-44}$

Аналіз даних, представлених у табл. 4.3. дозволяє зробити висновок про те, що відсоток вмісту бент-послідовностей у повному коді стрімко зменшується зі зростанням числа N.

Проте, у разі $N=4$ маємо унікальну ситуацію, коли половина всіх послідовностей є бент-послідовностями, тобто задовольняють умовам **Визначення 4.3.**

Даний факт може бути використаний для збільшення кількості інформації, що вбудовується в контейнер в стеганосистемах з кодовим розподілом каналів при $N=4$ наступним чином: груповий сигнал може бути підданий перетворенню за допомогою С-коду ще до знаходження його коефіцієнтів перетворення Уолша-Адамара.

Визначення 4.4 [4]. С-кодом називається код, кожне кодове слово якого має задане (зазвичай, мінімально можливе) значення пік-фактора (peak-to-average-power-ratio) κ, який визначається як

$$\kappa = \frac{P_{\max}}{P_{av}} = \frac{1}{N} \max_t \left\{ \left| S_c(t) \right|^2 \right\}, \qquad (4.17)$$

де $P_{\max}$ — максимальна потужність сигналу $S_c(t)$, P_{av} — середня потужність сигналу $S_c(t)$.

Багато уваги дослідників приділяється проблемі синтезу С-кодів для технології MC-CDMA [16…19]. С-коди можуть успішно використовуватися в стеганографічних системах, заснованих на технології MC-CDMA.

Таким чином, схема стеганосистеми з розподілом каналів з використанням технології MC-CDMA (рис. 4.2.) набуває вигляду, показаного на рис. 4.4.

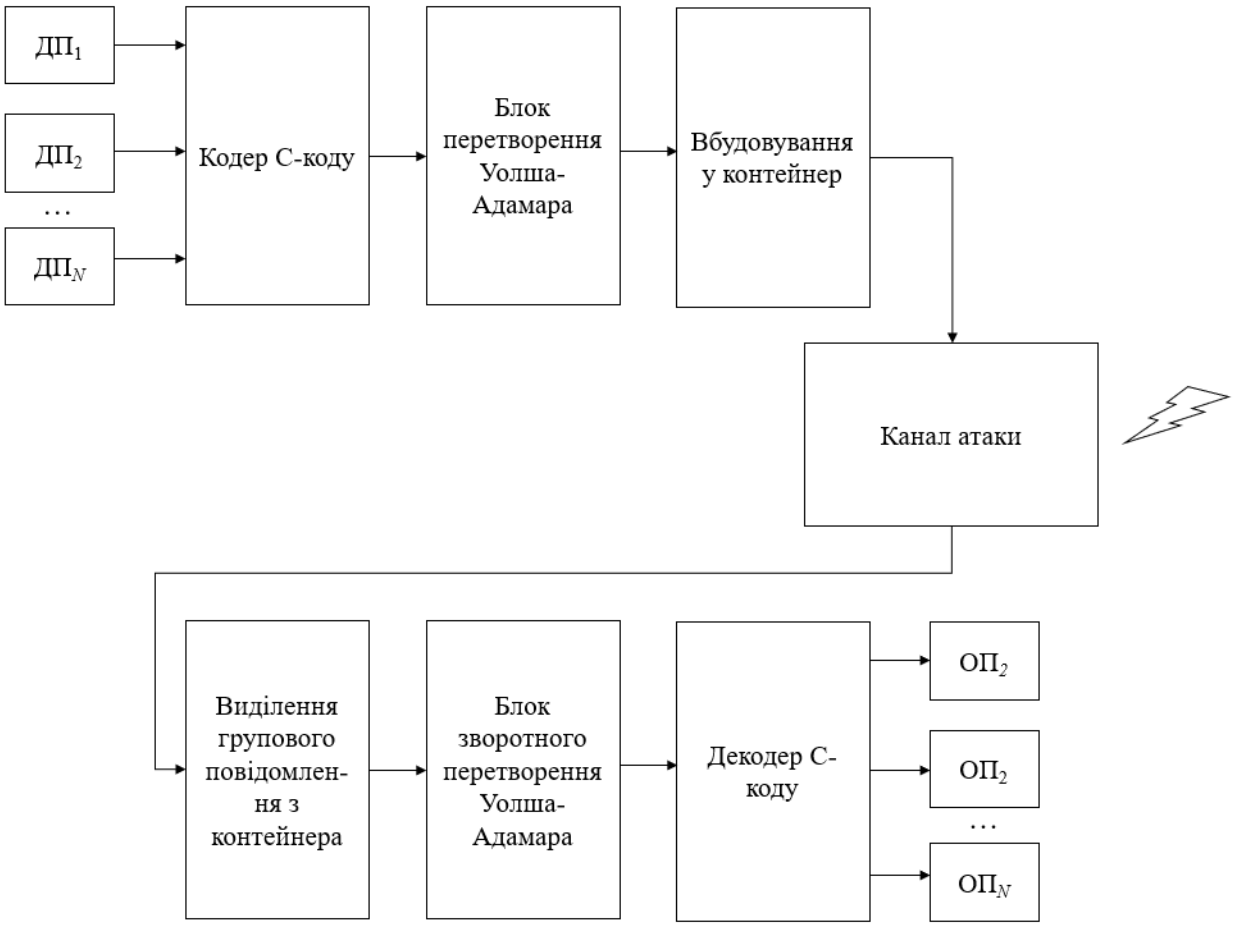


Рис. 4.4. — Схема стеганосистеми з використанням технології MC-CDMA та С-коду

При цьому пропонується таблиця кодування С-кодом, побудована відповідно до таких правил.

Правило 1. Кожне кодове слово, яке відповідає бент-послідовності, кодується двома такими кодовими словами.

Правило 2. Кожне кодове слово, яке не відповідає бент-послідовності, кодується кодовим словом, що відповідає бент-послідовності та її інверсії.

Зрозуміло, що при цьому вихідні кодові слова можуть бути закодовані кодовими словами С-коду з точністю до перестановок вихідних кодових слів усередині класу бент-послідовностей і послідовностей, що залишилися та не є бент-послідовностями.

Один із варіантів кодування зображений у табл. 4.4. При цьому жирним шрифтом виділено кодові слова, закодовані відповідно до *Правила 1*.

Таблиця 4.4. — Спосіб кодування кодових слів повного коду С-кодом

Вихідне кодове слово	Кодове слово після перетворення С-кодом	Вихідне кодове слово	Кодове слово після перетворення С-кодом
0000	1000 1110	0001	**0001 0001**
0011	0100 1011	0010	**0010 0010**
0101	0010 1101	0100	**01000100**
0110	0001 1110	0111	**01110111**
1010	0111 1000	1000	**10001000**
1100	1011 0100	1001	**10011001**
1101	1101 0010	1011	**10111011**
1111	1110 0001	1110	**11101110**

Неважко бачити, що кодова відстань такого коду [20] дорівнює $d_c = 2$. Зважаючи на те, що $d_c = f + 1$, де f — кількість виявлених кодом помилок, представлений в табл. 4.4. код може виявляти як мінімум одноразову помилку, підтверджуючи цим цілісність вбудованої інформації.

При цьому середня довжина кодового слова, необхідна для кодування в кожному кадрі одного каналу передачі інформації, становить 2 біти замість 2.125 біта, як це необхідно в системі з використанням кодів Гаффмана [1], тобто:

a. порівняно з використанням коду Гаффмана для кодування коефіцієнтів перетворення Уолша-Адамара, запропонований код дозволяє упаковувати коефіцієнти Уолша-Адамара на 6,25% ефективніше;

b. на відміну від випадку використання коду Гаффмана для кодування коефіцієнтів перетворення Уолша-Адамара, запропонований код дозволяє детектувати як мінімум одну помилку, що підтверджує цілісність вбудованої інформації.

4.2. Розробка стеганографічного методу з множинним доступом на основі кодового управління та частотних розстановок

Як показано в даному розділі, наступним кроком на шляху розвитку стеганографічних методів з множинним доступом, який дозволяє усунути недоліки стеганографічного методу на основі технології MC-CDMA, є використання технології кодового управління [21], а також технології частотних розстановок, що застосовується для побудови адресних асинхронних систем зв'язку на основі частотно-часових матриць (ЧЧМ-сигналів) [10]. Подібні системи використовуються в наземних, супутникових та інших системах зв'язку, в системах командного радіоуправління та управління повітряним рухом.

У табл. 4.5. ми наводимо набір кодових слів, які ми будемо використовувати для побудови стеганографічного методу з множинним доступом на основі кодового управління та частотних розстановок. Наведені кодові слова впливають на трансформанти (1,2), (1,4), (2,1), (2,2), (2,3), (2,4), (3,2), (3,3), (3,4), (4,1), (4,2), (4,3), (4,4), (за виключенням найбільш низькочастотних трансформант (1,1), (1,3), (3,1)). Така кількість застосовуваних частотних складових зумовлена тим, що ми розглядаємо застосування двох кодів частотних розстановок: перший код, передбачає найбільшу кількість абонентів, що розділяються, з використанням 13 частотних складових, у той час як другий код — використання п'яти частотних складових і забезпечує найкращу надійність сприйняття.

Зазначимо, що застосування представлених у табл. 4.5 кодових слів забезпечує цілеспрямований вплив на відповідну трансформанту Уолша-Адамара, причому інші трансформанти залишаються незмінними.

Таблиця 4.5 — Кодові слова, спрямовані на модифікацію заданих трансформант перетворення Уолша-Адамара

$T^{+}_{4,(1,2)}$	$T^{+}_{4,(1,4)}$	$T^{+}_{4,(2,1)}$	$T^{+}_{4,(2,2)}$
$\begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \end{bmatrix}$
$T^{+}_{4,(2,3)}$	$T^{+}_{4,(2,4)}$	$T^{+}_{4,(3,2)}$	$T^{+}_{4,(3,3)}$
$\begin{bmatrix} 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \end{bmatrix}$
$T^{+}_{4,(3,4)}$	$T^{+}_{4,(4,1)}$	$T^{+}_{4,(4,2)}$	$T^{+}_{4,(4,3)}$
$\begin{bmatrix} 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 \end{bmatrix}$
$T^{+}_{4,(4,4)}$	–	–	–
$\begin{bmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$	–	–	–

Кожне кодове слово, показане у табл. 4.5. являє собою частотну складову для першого коду частотних розстановок f_{1i} і другого f_{2i}, відповідно

$$
\begin{array}{lcllcl}
T^{+}_{4,(1,2)} & \leftrightarrow & f_{10} & & & \\
T^{+}_{4,(1,4)} & \leftrightarrow & f_{11} & & & \\
T^{+}_{4,(2,1)} & \leftrightarrow & f_{12} & & & \\
T^{+}_{4,(2,2)} & \leftrightarrow & f_{13} & & & \\
T^{+}_{4,(2,3)} & \leftrightarrow & f_{14} & T_{4,(2,2)} & \leftrightarrow & f_{20} \\
T^{+}_{4,(2,4)} & \leftrightarrow & f_{15} & T_{4,(2,3)} & \leftrightarrow & f_{21} \\
T^{+}_{4,(3,2)} & \leftrightarrow & f_{16}, & T_{4,(2,4)} & \leftrightarrow & f_{22}. \\
T^{+}_{4,(3,3)} & \leftrightarrow & f_{17} & T_{4,(3,2)} & \leftrightarrow & f_{23} \\
T^{+}_{4,(3,4)} & \leftrightarrow & f_{18} & T_{4,(4,2)} & \leftrightarrow & f_{24} \\
T^{+}_{4,(4,1)} & \leftrightarrow & f_{19} & & & \\
T^{+}_{4,(4,2)} & \leftrightarrow & f_{110} & & & \\
T^{+}_{4,(4,3)} & \leftrightarrow & f_{111} & & & \\
T^{+}_{4,(4,4)} & \leftrightarrow & f_{112} & & &
\end{array}
\qquad (4.18)
$$

Дані частотні складові f_i розміру $\frac{\mu}{2}\times\frac{\mu}{2}=4\times 4$ використовуються в стеганографічному методі як чіпи, для формування унікальних для кожного абонента кодових слів розміру $\mu\times\mu$ відповідно до правила частотних розстановок

$$
\begin{array}{|c|c|}
\hline
f_{i_1} & f_{i_2} \\
\hline
f_{i_3} & f_{i_4} \\
\hline
\end{array}, \qquad (4.19)
$$

де вектор індексів $[i_1,i_2,i_3,i_4]$ є унікальним для кожного абонента та визначається відповідною частотною розстановкою.

У сучасних асинхронних адресних системах зв'язку для побудови кодів частотних розстановок з добрими кореляційними властивостями набули поширення недвійкові циклічні коди Боуза-Чоудхурі-Хоквінгема — коди Ріда-Соломона (РС-коди) [10].

У запропонованому методі, розглядаючи приклад довжини блоку $\mu\times\mu=8\times 8$, ми представляємо два варіанти формування коду частотних розстановок: перший — над полем $GF(13)$, що дозволяє забезпечити максимальну кількість абонентів, що розділяються, при збереженні прийнятної надійності сприйняття, а також другий — над полем $GF(5)$, що

дозволяє забезпечити найкращу надійність сприйняття при меншій кількості абонентів, що розділяються.

Сформуємо перший код частотних розстановок на основі РС-коду над полем $GF(13)$ з наступними параметрами: довжина коду $N=12$, кількість інформаційних розрядів $K=2$, первісний елемент $\theta=2$, кодова відстань $d=12-2+1=11$. Породжуючий поліном даного коду визначається наступним співвідношенням

$$g(z)=\prod_{i=1}^{d-1}(z-\theta^i)=\prod_{i=1}^{10}(z-2^i)=$$
$$(z-2)(z-4)(z-8)(z-3)(z-6)(z-12)(z-11)(z-9)(z-5)(z-10)= \quad (4.20)$$
$$11+7z+12z^2+9z^3+3z^4+4z^5+6z^6+10z^7+5z^8+8z^9+z^{10}.$$

На основі породжуючого полінома (4.20) побудуємо породжуючу матрицю, перший рядок якої складається з коефіцієнтів породжуючого полінома, у той час як наступні $K-1$ рядків визначаються за допомогою нециклічного зсуву вправо на 1 попереднього рядка, при цьому всі незаповнені елементи породжуючої матриці вважаються рівними 0

$$G=\begin{bmatrix} 11 & 7 & 12 & 9 & 3 & 4 & 6 & 10 & 5 & 8 & 1 & 0 \\ 0 & 11 & 7 & 12 & 9 & 3 & 4 & 6 & 10 & 5 & 8 & 1 \end{bmatrix}. \quad (4.21)$$

Перший рядок породжуючої матриці G назвемо базовим кодовим словом і позначимо як C_1. Ґрунтуючись на властивості подвійної циклічності РС-кодів, решту кодових слів ми можемо побудувати шляхом циклічних зсувів базового кодового слова за часом і частотою. Далі, кожне з кодових слів РС-коду піддається усіченню, внаслідок чого отримуємо перші чотири його символи — частотну розстановку.

При цьому загальна кількість доступних частотних розстановок, сформованих за допомогою РС-коду над полем $GF(q)$, становить

$$J=q(q-1)=13\cdot 12=156. \quad (4.22)$$

Для стислості в табл. 4.6. дані частотні розстановки представлені в тринадцятковому вигляді ($10\to A, 11\to B, 12\to C$).

Таблиця 4.6. — Код частотних розстановок на базі РС-коду над полем $GF(13)$ у вигляді циклічних зсувів за часом і частотою базового кодового слова C_1

B7C9	7C93	C934	9346	346A	46A5	6A58	A581	5810	810B	10B7	0B7C
C80A	80A4	0A45	A457	457B	57B6	7B69	B692	6921	921C	21C8	1C80
091B	91B5	1B56	B568	568C	68C7	8C7A	C7A3	7A32	A320	3209	2091
1A2C	A2C6	2C67	C679	6790	7908	908B	08B4	8B43	B431	431A	31A2
2B30	B307	3078	078A	78A1	8A19	A19C	19C5	9C54	C542	542B	42B3
3C41	C418	4189	189B	89B2	9B2A	B2A0	2A06	A065	0653	653C	53C4
4052	0529	529A	29AC	9AC3	AC3B	C3B1	3B17	B176	1764	7640	6405
5163	163A	63AB	3AB0	AB04	B04C	04C2	4C28	C287	2875	8751	7516
6274	274B	74BC	4BC1	BC15	C150	1503	5039	0398	3986	9862	8627
7385	385C	85C0	5C02	C026	0261	2614	614A	14A9	4A97	A973	9738
8496	4960	9601	6013	0137	1372	3725	725B	25BA	5BA8	BA84	A849
95A7	5A71	A712	7124	1248	2483	4836	836C	36CB	6CB9	CB95	B95A
A6B8	6B82	B823	8235	2359	3594	5947	9470	470C	70CA	0CA6	CA6B

Таким чином, із застосуванням способу додаткового кодування інформації кодовими словами з використанням частотних розстановок на основі РС-коду, представлених у табл. 4.6. теоретично можливо забезпечити роботу 156 абонентів у стеганоканалі.

Наприклад, у цьому випадку перший абонент у системі буде передавати інформацію з використанням частотної розстановки $[B7C9] \to [11 \;\; 7 \;\; 12 \;\; 9]$, на основі якої, відповідно до (4.18) формуємо кодові слова виду (4.19) $[f_{111} \;\; f_{17} \;\; f_{112} \;\; f_{19}] = [T^{+}_{4,(4,3)}, \;\; T^{+}_{4,(3,3)}; \;\; T^{+}_{4,(4,4)}, \;\; T^{+}_{4,(4,1)}]$, де символ «,» означає горизонтальну конкатенацію, а символ «;» — вертикальну. Таким чином, перший абонент в системі проводить кодування інформації за допомогою наступних кодових слів (T_1^+ для передачі біта 0 і T_1^- для передачі біта 1)

$$T_1^+ = \left[\begin{array}{cccc|cccc} 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ \hline 1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \\ -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \end{array}\right], \quad T_1^- = \left[\begin{array}{cccc|cccc} -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\ \hline -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \end{array}\right]. \quad (4.23)$$

Приступимо тепер до формування другого коду частотних розстановок, для чого побудуємо РС-код над полем Галуа $GF(5)$ з параметрами: довжина коду $N=4$, кількість інформаційних розрядів $K=2$, первісний елемент $\theta=3$, кодова відстань $d=N-K+1=3$. Визначимо породжуючий поліном даного коду

$$g(z)=\prod_{i=1}^{d-1}(z-\theta^i)=\prod_{i=1}^{2}(z-3^i)=2+3z+z^2. \qquad (4.24)$$

Аналогічно випадку першого коду частотних розстановок, на основі породжуючого полінома (4.24), побудуємо породжуючу матрицю

$$G=\begin{bmatrix}2 & 3 & 1 & 0\\ 0 & 2 & 3 & 1\end{bmatrix}, \qquad (4.25)$$

на основі якої побудуємо всі $J=20$ кодових слів коду Ріда-Соломона (табл. 4.7.). Зважаючи на те, що кожне з даних кодових слів має довжину $N=4$, що відповідає конструкції (4.19), для цього коду кодові слова не потребують усічення і можуть бути використані в незмінному вигляді.

Таблиця 4.7. — Подання РС-коду над полем $GF(5)$

$C_1=[2\ \ 3\ \ 1\ \ 0]$	$C_6=[3\ \ 1\ \ 0\ \ 2]$	$C_{11}=[1\ \ 0\ \ 2\ \ 3]$	$C_{16}=[0\ \ 2\ \ 3\ \ 1]$
$C_2=[3\ \ 4\ \ 2\ \ 1]$	$C_7=[4\ \ 2\ \ 1\ \ 3]$	$C_{12}=[2\ \ 1\ \ 3\ \ 4]$	$C_{17}=[1\ \ 3\ \ 4\ \ 2]$
$C_3=[4\ \ 0\ \ 3\ \ 2]$	$C_8=[0\ \ 3\ \ 2\ \ 4]$	$C_{13}=[3\ \ 2\ \ 4\ \ 0]$	$C_{18}=[2\ \ 4\ \ 0\ \ 3]$
$C_4=[0\ \ 1\ \ 4\ \ 3]$	$C_9=[1\ \ 4\ \ 3\ \ 0]$	$C_{14}=[4\ \ 3\ \ 0\ \ 1]$	$C_{19}=[3\ \ 0\ \ 1\ \ 4]$
$C_5=[1\ \ 2\ \ 0\ \ 4]$	$C_{10}=[2\ \ 0\ \ 4\ \ 1]$	$C_{15}=[0\ \ 4\ \ 1\ \ 2]$	$C_{20}=[4\ \ 1\ \ 2\ \ 0]$

Стеганографічна система з множинним доступом на основі представленого коду Ріда-Соломона (табл. 4.7.) може теоретично забезпечити роботу $J=20$ абонентів з використанням п'яти частотних складових.

На основі викладеного теоретичного матеріалу представимо алгоритми вбудовування та вилучення інформації для розробленого стеганографічного методу з множинним доступом.

Алгоритм вбудовування інформації

Крок 1. Формується ансамбль кодових слів розміру $\frac{\mu}{2}\times\frac{\mu}{2}$ (табл. 4.5.), що впливають цілеспрямовано на задані трансформанти перетворення Уолша-Адамара, а також ансамбль частотних розстановок на основі РС-коду над полем $GF(q)$ (табл. 4.6. або табл. 4.7.). Вибір основи q залежить від кількості абонентів, що розділяються, а також від кількості модифікованих трансформант Уолша-Адамара, які беруть участь у передачі інформації.

Крок 2. Кожному зареєстрованому в стеганосистемі абоненту A_z, $z=1,2,...,J$ для передачі інформації по стеганоканалу виділяється частотна розстановка, на основі якої, відповідно до конструкції (4.19) і табл. 4.5., абонент формує кодові слова T_z^+ та T_z^- розміру $\mu\times\mu$.

Крок 3. Кожен з абонентів A_z розбиває зображення-контейнер на блоки розміру $\mu\times\mu$ і здійснює вбудовування одного біта $d_{z,k}$ ДІ у кожен із блоків контейнера X_k шляхом застосування операції підсумовування, тобто кожен блок стеганоповідомлення обчислюється як

$$M_k = X_k + D_k . \qquad (4.26)$$

Безперечною перевагою представленого стеганографічного методу є той факт, що різні абоненти, з використанням своєї частотної розстановки можуть здійснювати вбудовування інформації незалежно один від одного в будь-який зручний для них час. При цьому кількість абонентів, що одночасно функціонують в системі, також може бути легко масштабована.

Зауваження. З огляду на те, що більшість використовуваних зображень сьогодні представлені з використанням моделі RGB, де для кодування кожного кольору відводиться 1 байт (кожна колірна складова представляється числами в діапазоні $[0,...,255]$), у разі наявності в блоці

граничного для даного діапазону значень (0 або 255), вказаний блок не використовується в процесі стеганоперетворення у разі застосування розробленого стеганографічного методу.

Розглянемо конкретний приклад вбудовування інформації за допомогою представленого стеганографічного методу.

Нехай сформовано ансамбль кодових слів розміру 4×4, що складається з кодових слів $T_{4,(2,2)}, T_{4,(2,3)}, T_{4,(2,4)}, T_{4,(3,2)}, T_{4,(4,2)}$, а також ансамбль із $J=20$ частотних розстановок (табл. 4.7.). Розглянемо роботу двох абонентів A_1 та A_2, яким присвоєно частотні розстановки $C_1=\begin{bmatrix}2 & 3 & 1 & 0\end{bmatrix}$ та $C_2=\begin{bmatrix}3 & 4 & 2 & 1\end{bmatrix}$ по вбудовуванню бітів інформації $d_{1,k}=1, d_{2,k}=-1$ в блок зображення-контейнера

$$X_k=\begin{bmatrix}213 & 214 & 215 & 216 & 215 & 214 & 214 & 214\\ 214 & 215 & 215 & 216 & 215 & 214 & 216 & 214\\ 214 & 214 & 215 & 215 & 214 & 213 & 214 & 214\\ 215 & 215 & 216 & 217 & 214 & 214 & 214 & 214\\ 214 & 214 & 215 & 215 & 214 & 217 & 216 & 216\\ 214 & 214 & 215 & 215 & 216 & 216 & 214 & 216\\ 215 & 216 & 215 & 216 & 215 & 215 & 214 & 216\\ 214 & 216 & 215 & 214 & 215 & 215 & 216 & 215\end{bmatrix}. \qquad (4.27)$$

На основі заданої частотної розстановки C_1, а також ансамблю кодових слів розміру 4×4, перший абонент формує кодові слова розміру 8×8, призначені для передачі біта $d_{1,k}$ ДІ

$$T_1^+ = \left[\begin{array}{cccc|cccc} 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 \\ \hline 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 \end{array}\right],$$

$$T_1^- = \left[\begin{array}{cccc|cccc} -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\ \hline -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 \end{array}\right], \quad (4.28)$$

у той час як другий абонент генерує свої кодові слова на основі частотної розстановки C_2

$$T_2^+ = \left[\begin{array}{cccc|cccc} 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ \hline 1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 \end{array}\right],$$

$$T_2^- = \left[\begin{array}{cccc|cccc} -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ \hline -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 \end{array}\right]. \quad (4.29)$$

Ґрунтуючись на (4.28), перший абонент виконує вбудовування біта інформації $d_{1,k} = 1$, тоді як другий абонент виконує вбудовування біта інформації $d_{2,k} = -1$, внаслідок чого отримуємо стеганоповідомлення

$$M_k = X_k + T_1^+ + T_2^- =$$

$$= \begin{bmatrix} 213 & 214 & 213 & 218 & 215 & 214 & 214 & 214 \\ 212 & 217 & 215 & 216 & 217 & 212 & 218 & 212 \\ 216 & 212 & 215 & 215 & 214 & 213 & 214 & 214 \\ 215 & 215 & 218 & 215 & 212 & 216 & 212 & 216 \\ 214 & 216 & 215 & 213 & 214 & 215 & 218 & 216 \\ 214 & 212 & 215 & 217 & 216 & 218 & 212 & 216 \\ 215 & 218 & 215 & 214 & 215 & 213 & 216 & 216 \\ 214 & 214 & 215 & 216 & 215 & 217 & 214 & 215 \end{bmatrix}. \qquad (4.30)$$

Зазначимо при цьому, що степінь збурення зображення-контейнера при вбудовуванні інформації представленим способом залежить від таких факторів: кількості абонентів, що одночасно здійснюють передачу ДІ, конкретних значень бітів ДІ.

Перейдемо до алгоритму вилучення інформації.

Алгоритм вилучення інформації

Крок 1. Відповідно до взаємозв'язку між двовимірним і одновимірним перетворенням Уолша-Адамара кожен абонент A_z стеганографічної системи, відповідно до виданого йому коду частотних розстановок вибирає рядки матриці Уолша-Адамара H_{N^2} порядку N^2, які позначаються як $\{h_{z,1}\},\{h_{z,2}\},\{h_{z,3}\},\{h_{z,4}\}$.

Крок 2. Абонент знаходить матрицю різниці стеганоповідомлення M та зображення-контейнера X, розбиває отриману матрицю різниці на блоки Δ_k розміру $\mu \times \mu$.

Крок 3. Кожний із блоків матриці різниці абонент розбиває ще на 4 підблоки розміру $\frac{\mu}{2} \times \frac{\mu}{2}$ відповідно до конструкції (4.19). Шляхом послідовної конкатенації рядків кожен із чотирьох підблоків представляється у вигляді вектора $\{\delta_{z,i}\}, i = \{1,2,3,4\}$ довжини μ^2.

Крок 4. Абонент A_z обчислює вектор P відповідно до наступної формули

$$P_{z,k} = [\,p_1 \quad p_2 \quad p_3 \quad p_4\,],$$
$$p_i = \sum_{k=1}^{\mu^2} \delta_{j,k} h_{j,k},\ i = \{1,2,3,4\}. \tag{4.31}$$

Крок 5. Абонент обчислює призначений йому біт даних, вбудований у блок Δ_i за допомогою наступної формули

$$d_{z,k} = sign\left(\sum_{i=1}^{4} p_i\right). \tag{4.32}$$

Як приклад виконаємо вилучення інформації, вбудованої першим і другим абонентами в стеганоповідомлення (4.30). Для цього відповідно до виділених кодів частотних розстановок формуємо множину функцій Уолша для першого абонента

$$\begin{aligned}
\{h_{1,1}\} &= \{+1-1-1+1-1+1+1-1+1-1-1+1-1+1+1-1\};\\
\{h_{1,2}\} &= \{+1-1+1-1+1-1+1-1-1+1-1+1-1+1-1+1\};\\
\{h_{1,3}\} &= \{+1+1-1-1-1-1+1+1+1+1-1-1-1-1+1+1\};\\
\{h_{1,4}\} &= \{+1-1+1-1-1+1-1+1+1-1+1-1-1+1-1+1\},
\end{aligned} \tag{4.33}$$

а також для другого абонента

$$\begin{aligned}
\{h_{2,1}\} &= \{+1-1+1-1+1-1+1-1-1+1-1+1-1+1-1+1\};\\
\{h_{2,2}\} &= \{+1-1+1-1-1+1-1+1-1+1-1+1+1-1+1-1\};\\
\{h_{2,3}\} &= \{+1-1-1+1-1+1+1-1+1-1-1+1-1+1+1-1\};\\
\{h_{2,4}\} &= \{+1+1-1-1-1-1+1+1+1+1-1-1-1-1+1+1\}.
\end{aligned} \tag{4.34}$$

Далі, обидва абоненти обчислюють матрицю різниці стеганоповідомлення та зображення-контейнера, і розбивають її на блоки розміру $\mu \times \mu$. У разі нашого прикладу, розглянутий блок матиме вигляд

$$\Delta_k = M_k - X_k = \begin{bmatrix}
0 & 0 & -2 & 2 & 0 & 0 & 0 & 0\\
-2 & 2 & 0 & 0 & 2 & -2 & 2 & -2\\
2 & -2 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 2 & -2 & -2 & 2 & -2 & 2\\
0 & 2 & 0 & -2 & 0 & -2 & 2 & 0\\
0 & -2 & 0 & 2 & 0 & 2 & -2 & 0\\
0 & 2 & 0 & -2 & 0 & -2 & 2 & 0\\
0 & -2 & 0 & 2 & 0 & 2 & -2 & 0
\end{bmatrix}. \tag{4.35}$$

Ґрунтуючись на отриманій матриці Δ_k, перший і другий абоненти виділяють відповідні вектори $\{\delta_{z,i}\}, i=\{1,2,3,4\}$

$$\begin{aligned}
\{\delta_{1,1}\} &= \begin{bmatrix} 0 & 0 & -2 & 2 & -2 & 2 & 0 & 0 & 2 & -2 & 0 & 0 & 0 & 0 & 2 & -2 \end{bmatrix}; \\
\{\delta_{1,2}\} &= \begin{bmatrix} 0 & 0 & 0 & 0 & 2 & -2 & 2 & -2 & 0 & 0 & 0 & 0 & -2 & 2 & -2 & 2 \end{bmatrix}; \\
\{\delta_{1,3}\} &= \begin{bmatrix} 0 & 2 & 0 & -2 & 0 & -2 & 0 & 2 & 0 & 2 & 0 & -2 & 0 & -2 & 0 & 2 \end{bmatrix}; \\
\{\delta_{1,4}\} &= \begin{bmatrix} 0 & -2 & 2 & 0 & 0 & 2 & -2 & 0 & 0 & -2 & 2 & 0 & 0 & 2 & -2 & 0 \end{bmatrix}.
\end{aligned} \tag{4.36}$$

Далі, використовуючи (4.31), а також свій набір векторів $\{h_{1,i}\}$ (4.33), перший абонент обчислює вектор $P_{1,k}$, а також, відповідно до виразу (4.32), біт даних, що призначається йому

$$P_{1,k} = \begin{bmatrix} 16 & 16 & 16 & 16 \end{bmatrix} \rightarrow d_{1,k} = 1. \tag{4.37}$$

Аналогічним чином, вектор $P_{2,k}$, а також біт даних, що призначається йому, обчислює і другий абонент

$$P_{2,k} = \begin{bmatrix} -16 & -16 & -16 & -16 \end{bmatrix} \rightarrow d_{2,k} = -1. \tag{4.38}$$

Однією з найважливіших властивостей розробленого стеганографічного методу є можливість одночасної роботи такої кількості абонентів, яка потрібна в даний момент, при загальній кількості зареєстрованих абонентів J, кожному з яких виділено свою частотну розстановку. Тим не менш, при збільшенні кількості абонентів, що одночасно працюють у системі, збільшується інформаційне навантаження на зображення-контейнер, і, відповідно, погіршується якість сприйняття стегноповідомлення. Задля чисельного вимірювання якості сприйняття стеганоповідомлення ми приймемо показник PSNR [22], який визначається відповідно до наступної формули

$$PSNR = 20\lg\left(\frac{255}{\sqrt{MSE}}\right), \tag{4.39}$$

де

$$MSE = \frac{1}{nm}\sum_i\sum_j \left| X(i,j) - M(i,j) \right|^2. \tag{4.40}$$

На рис. 4.5. представлено графік залежності PSNR стеганоповідомлення від кількості одночасно працюючих у системі абонентів. Для побудови графіка проводився експеримент з використанням 500 зображень у форматі TIFF без втрат з бази NRCS [23], в кожне з яких проводилося вбудовування інформації, що надходила від різної кількості абонентів, після чого вимірювався PSNR отриманого стеганоповідомлення.

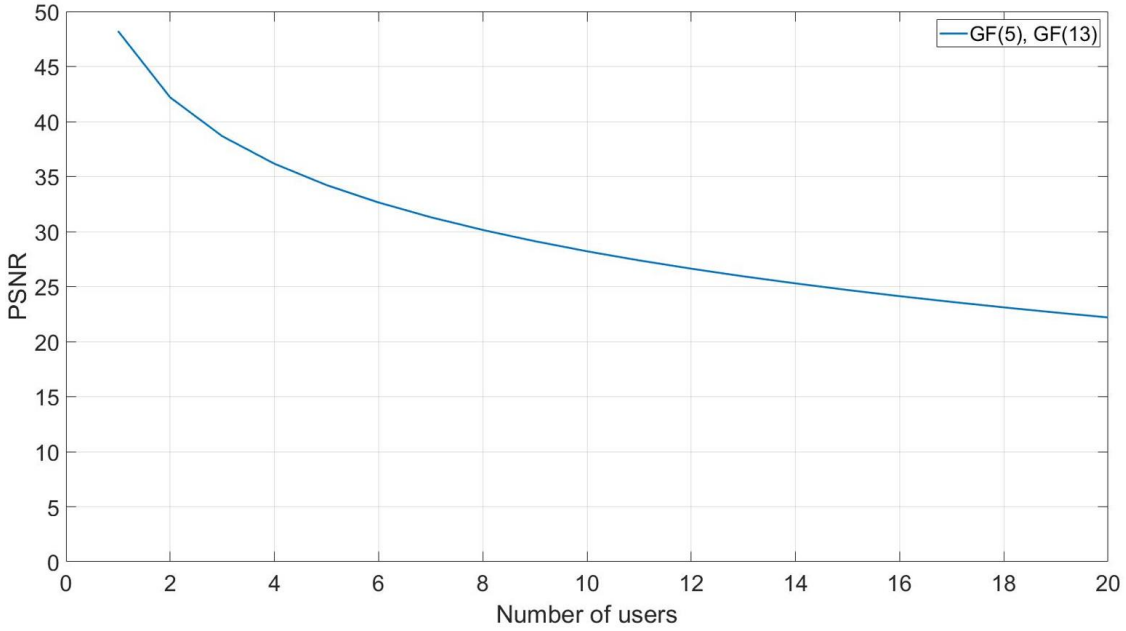


Рис. 4.5. — Графік залежності PSNR стеганоповідомлення від кількості абонентів, що одночасно передають інформацію

Аналіз даних рис. 4.5. показує, що збільшення кількості одночасно працюючих абонентів призводить до падіння PSNR стеганоповідомлення, при цьому даний процес є однаковим як для випадку застосування коду частотних розстановок на основі РС-коду над полем $GF(5)$, так і над полем $GF(13)$. Зазначимо при цьому, що при кількості абонентів, що одночасно працюють $N \le 8$, значення PSNR залишаються на допустимому рівні. У разі використання частотних розстановок на основі РС-коду над полем $GF(5)$ вбудовування інформації відбувається у високочастотні складові, тому навіть

при значенні $PSNR \approx 30 дБ$ надійність сприйняття зберігається на достатньому рівні, що можна наочно побачити на рис. 4.6.

При цьому на рис. 4.6. в синю RGB складову зображення розміру 2592x3872 при загальній кількості каналів, що розділяються $N = 20$, вбудовано в цілому $20 \cdot 324 \cdot 484 = 3136320$ бит $= 382.85$ КБ інформації.

а) б)

Рис. 4.6. — Приклад стеганоповідомлення з вбудованою інформацією від $N = 20$ абонентів (а), а також вихідного контейнера (б)

Суб'єктивне ранжування зображень, показаних на рис. 4.6. не дозволяє виявити у стеганоповідомленні ніяких артефактів або візуальних відмінностей від вихідного зображення-контейнера.

Особливістю асинхронних адресних систем зв'язку, що знайшла своє відображення і в розробленому стеганографічному методі з множинним доступом, є наявність внутрішньосистемних перешкод: формуючи загальний потік, імпульси інших каналів можуть випадково утворювати кодову комбінацію даного каналу, призводячи до появи відповідної перешкоди. Іншим типом внутрішньосистемних перешкод є інтерференційне придушення та нелінійне придушення імпульсів.

Проведені експерименти показують, що внутрішньосистемні перешкоди виявляються тоді, коли кількість абонентів, що одночасно

функціонують в системі, перевищує значення q. На рис. 4.7. показана залежність кількості помилок, що виникають у каналі зв'язку (кожного з користувачів) залежно від кількості функціонуючих в системі абонентів для кодів частотних розстановок на основі РС-кодів над полями $GF(5)$ та $GF(13)$.

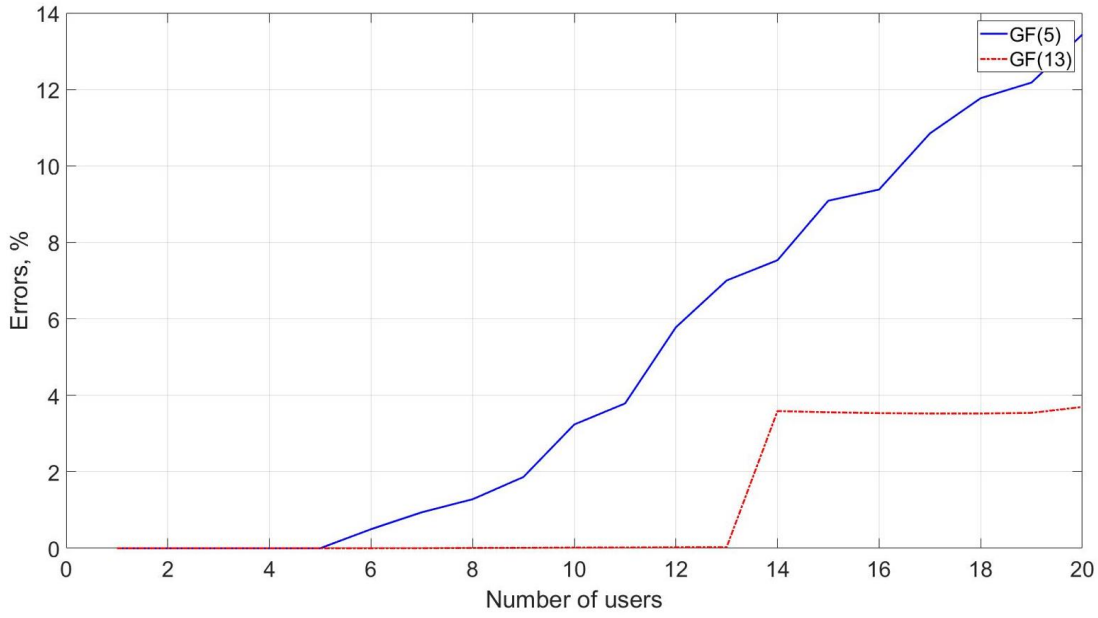


Рис. 4.7. — Графіки залежності відсотка помилок, що виникають в результаті внутрішньосистемних перешкод від кількості абонентів

Аналіз даних рис. 4.7. показує, що частотні розстановки на основі РС-коду над полем $GF(5)$ дозволяють забезпечити одночасну роботу $N=5$ абонентів без виникнення внутрішньосистемних перешкод, у той час як частотні розстановки на основі РС-коду над полем $GF(13)$ дозволяють забезпечити одночасну роботу $N=13$ абонентів без виникнення внутрішньосистемних перешкод, однак навіть для значення кількості одночасно працюючих абонентів $N=20$ для даних частотних розстановок (табл. 4.6.) рівень внутрішньосистемних перешкод залишається прийнятним, а кількість помилок, що виникають, не перевищує 3.7%.

4.3. Стеганографічний метод з множинним доступом на основі кодового управління та частотно-просторових матриць

У разі необхідності максимізації кількості одночасно працюючих у стеганографічній системі з множинним доступом абонентів ми представляємо новий стеганографічний метод, також заснований на застосуванні кодового управління, однак із задіянням запропонованої технології частотно-просторових матриць.

Для реалізації ідеї стеганографічного методу з множинним доступом на основі кодового управління [21] та частотно-просторових матриць, нам знадобляться кодові слова розміру 4×4, які цілеспрямовано впливають на кожну з можливих трансформант Уолша-Адамара (n,m), а також відповідні їм частотні складові $f_i, i=1,2,...,16$, які представлені в табл. 4.8.

Таблиця 4.8. — Кодові слова для цілеспрямованого впливу на кожну з трансформант Уолша-Адамара

$T^{+}_{4,(1,1)} \leftrightarrow f_0$	$T^{+}_{4,(1,2)} \leftrightarrow f_1$	$T^{+}_{4,(1,3)} \leftrightarrow f_2$	$T^{+}_{4,(1,4)} \leftrightarrow f_3$
$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$
$T^{+}_{4,(2,1)} \leftrightarrow f_4$	$T^{+}_{4,(2,2)} \leftrightarrow f_5$	$T^{+}_{4,(2,3)} \leftrightarrow f_6$	$T^{+}_{4,(2,4)} \leftrightarrow f_7$
$\begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \end{bmatrix}$
$T^{+}_{4,(3,1)} \leftrightarrow f_8$	$T^{+}_{4,(3,2)} \leftrightarrow f_9$	$T^{+}_{4,(3,3)} \leftrightarrow f_{10}$	$T^{+}_{4,(3,4)} \leftrightarrow f_{11}$
$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \end{bmatrix}$

Закінчення табл. 4.8.

$T^{+}_{4,(4,1)} \leftrightarrow f_{12}$	$T^{+}_{4,(4,2)} \leftrightarrow f_{13}$	$T^{+}_{4,(4,3)} \leftrightarrow f_{14}$	$T^{+}_{4,(4,4)} \leftrightarrow f_{15}$
$\begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$

Розглянемо сутність ідеї стеганографічного методу на основі частотно-просторових матриць. Операції вбудовування та вилучення інформації в даному методі засновані на розбитті зображення на блоки Q_k розміру $\mu \times \mu = 16 \times 16$. Кожен з отриманих блоків поділяється ще на 16 блоків q_i, $i = 1,2,...,16$, розміру 4×4

$$Q_k = \begin{array}{|c|c|c|c|} \hline q_1 & q_2 & q_3 & q_4 \\ \hline q_5 & q_6 & q_7 & q_8 \\ \hline q_9 & q_{10} & q_{11} & q_{12} \\ \hline q_{13} & q_{14} & q_{15} & q_{16} \\ \hline \end{array}. \qquad (4.41)$$

Розділення каналів користувачів відбувається за двома ознаками: частотною та просторовою. Іншими словами, кожному користувачеві виділяється 2 кодових слова: кодове слово S-коду просторових розстановок і кодове слово F-коду частотних розстановок. При цьому кодове слово S-коду визначає номери блоків q_i, в які даний користувач може проводити вбудовування інформації, в той час як кодове слово F-коду визначає ті трансформанти Уолша-Адамара, в які даний користувач може вбудовувати інформацію з використанням кодових слів, представлених у табл. 4.8.

Для вирішення завдання конструювання S-кодів просторових розстановок, кожне кодове слово якого містить 16 двійкових компонент, які показують, чи є дана просторова складова активною (значення елемента кодового слова $s_i = 1$) або пасивною (значення елемента кодового слова $s_i = 0$) прийнятий підхід заснований на тотальному випробуванні. У нашому випадку з метою максимізації кількості одночасно функціонуючих абонентів,

а також забезпечення найбільшої надійності сприйняття, використовуються кодові слова просторового S-коду ваги Хеммінга $wt(\{s_i\})=4$. Загальна кількість двійкових векторів довжини $N=16$ та ваги $wt(\{s_i\})=4$ визначається кількістю розстановок $C_{16}^{4}=1820$ і становлять код із кількістю збігів активних складових $\lambda \le 3$.

Для вирішення задачі мінімізації внутрішньосистемних завад, викликаних інтерференцією кодових слів від різних користувачів, необхідно на основі повного коду векторів довжини $N=16$ та ваги $wt(\{s_i\})=4$ побудувати просторовий S-код, кодові слова якого характеризуються кількістю збігів активних складових $\lambda \le 1$.

Як показують експерименти, потужність коду, що конструюється, буде залежати від порядку вибору кодових слів при його конструюванні. Скористаємося таким підходом:

Крок 1. Зафіксуємо перші чотири можливі кодові слова повного коду довжини $N=16$ і ваги $wt(\{s_i\})=4$, що мають число збігів активних складових $\lambda=0$, таким чином, підключаючи нових абонентів за допомогою даних кодових слів, ми забезпечимо повну відсутність внутрішньосистемних завад

$$S'=\begin{bmatrix}\{s_{1,i}\}\\ \{s_{2,i}\}\\ \{s_{3,i}\}\\ \{s_{4,i}\}\end{bmatrix}=\begin{bmatrix}\{1111000000000000\}\\ \{0000111100000000\}\\ \{0000000011110000\}\\ \{0000000000001111\}\end{bmatrix}, i=1,...,16. \qquad (4.42)$$

Крок 2. Виконуючи вибірку кодових слів з множини векторів довжини $N=16$ і ваги $wt(\{s_i\})=4$, добудовуємо ще 16 кодових слів, які мають число збігів $\lambda \le 1$ між собою і відносно кодових слів (4.42). В результаті отримуємо наступний ансамбль потужності $J_S=20$

$$S=\begin{bmatrix}\{s_{1,i}\}\\ \{s_{2,i}\}\\ \{s_{3,i}\}\\ \{s_{4,i}\}\\ \{s_{5,i}\}\\ \{s_{6,i}\}\\ \{s_{7,i}\}\\ \{s_{8,i}\}\\ \{s_{9,i}\}\\ \{s_{10,i}\}\\ \{s_{11,i}\}\\ \{s_{12,i}\}\\ \{s_{13,i}\}\\ \{s_{14,i}\}\\ \{s_{15,i}\}\\ \{s_{16,i}\}\\ \{s_{17,i}\}\\ \{s_{18,i}\}\\ \{s_{19,i}\}\\ \{s_{20,i}\}\end{bmatrix}=\begin{bmatrix}\{1111000000000000\}\\ \{0000111100000000\}\\ \{0000000011110000\}\\ \{0000000000001111\}\\ \{1000100010001000\}\\ \{0100010001001000\}\\ \{0010001000101000\}\\ \{0001000100011000\}\\ \{0010010010000100\}\\ \{0001100001000100\}\\ \{1000000100100100\}\\ \{0100001000010100\}\\ \{0001001010000010\}\\ \{0010000101000010\}\\ \{0100100000100010\}\\ \{1000010000010010\}\\ \{0100000110000001\}\\ \{1000001001000001\}\\ \{0001010000100001\}\\ \{0010100000010001\}\end{bmatrix},\ i=1,...,16, \qquad (4.43)$$

який буде використовуватися в якості S-кода.

Як основа для конструювання F-коду частотних розстановок використовуються двічі циклічні коди Ріда-Соломона [10]. З метою максимізації числа абонентів, які можуть одночасно працювати у стеганографічному каналі, раціональним є використання всіх доступних частотних складових. У цих цілях, для формування частотних розстановок використовуємо РС-код другого порядку над розширеним полем Галуа $GF(2^4)$, який має наступні характеристики: довжина кодового слова $N=15$, кількість інформаційних розрядів $K=2$, кодова відстань $d=N-K+1=15-2+1=14$.

Зазначимо, що поле $GF(2^4)$ має два ізоморфні уявлення, які визначаються двома первісними незвідними поліномами $h_1(x)=x^4+x+1$ і $h_2(x)=x^4+x^3+1$. Однак, з точки зору техніки побудови стеганографічного методу з множинним доступом, вибір конкретного ізоморфізму поля Галуа не має визначального значення, тому будемо використовувати арифметику

розширеного поля Галуа, що визначається первісним незвідним поліномом $h_1(x)$. В цьому випадку, таблиці складання та множення в полі $GF(2^4)$ матимуть вигляд

+	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	D
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	0	3	2	5	4	7	6	9	8	B	A	D	C	F	E
2	2	3	0	1	6	7	4	5	A	B	8	9	E	F	C	D
3	3	2	1	0	7	6	5	4	B	A	9	8	F	E	D	C
4	4	5	6	7	0	1	2	3	C	D	E	F	8	9	A	B
5	5	4	7	6	1	0	3	2	D	C	F	E	9	8	B	A
6	6	7	4	5	2	3	0	1	E	F	C	D	A	B	8	9
7	7	6	5	4	3	2	1	0	F	E	D	C	B	A	9	8
8	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7
9	9	8	B	A	D	C	F	E	1	0	3	2	5	4	7	6
A	A	B	8	9	E	F	C	D	2	3	0	1	6	7	4	5
B	B	A	9	8	F	E	D	C	3	2	1	0	7	6	5	4
C	C	D	E	F	8	9	A	B	4	5	6	7	0	1	2	3
D	D	C	F	E	9	8	B	A	5	4	7	6	1	0	3	2
E	E	F	C	D	A	B	8	9	6	7	4	5	2	3	0	1
F	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0

×	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	0	2	4	6	8	A	C	E	3	1	7	5	B	9	F	D
3	0	3	6	5	C	F	A	9	B	8	D	E	7	4	1	2
4	0	4	8	C	3	7	B	F	6	2	E	A	5	1	D	9
5	0	5	A	F	7	2	D	8	E	B	4	1	9	C	3	6
6	0	6	C	A	B	D	7	1	5	3	9	F	E	8	2	4
7	0	7	E	9	F	8	1	6	D	A	3	4	2	5	C	B
8	0	8	3	B	6	E	5	D	C	4	F	7	A	2	9	1
9	0	9	1	8	2	B	3	A	4	D	5	C	6	F	7	E
A	0	A	7	D	E	4	9	3	F	5	8	2	1	B	6	C
B	0	B	5	E	A	1	F	4	7	C	2	9	D	6	8	3
C	0	C	B	7	5	9	E	2	A	6	1	D	F	3	4	8
D	0	D	9	4	1	C	8	5	2	F	B	6	3	E	A	7
E	0	E	F	1	D	3	2	C	9	7	6	8	4	A	B	5
F	0	F	D	2	9	6	4	B	1	E	C	3	8	7	5	A

(4.44)

Прийнявши значення первісного елемента $\theta = 2$, сконструюємо породжуючий поліном РС-коду над полем $GF(2^4)$

$$g(z) = \prod_{i=1}^{d-1}(z-\theta^i) = \prod_{i=1}^{13}(z-2^i) =$$
$$(z+2)(z+4)(z+8)(z+3)(z+6)(z+12)(z+11)\times$$
$$\times(z+5)(z+10)(z+7)(z+14)(z+15)(z+13) = \quad (4.45)$$
$$= 2+6z+14z^2+13z^3+11z^4+7z^5+12z^6+$$
$$+9z^7+3z^8+4z^9+10z^{10}+5z^{11}+8z^{12}+z^{13}.$$

На основі отриманого породжуючого полінома запишемо породжуючу матрицю РС-коду

$$G = \begin{bmatrix} 2 & 6 & 14 & 13 & 11 & 7 & 12 & 9 & 3 & 4 & 10 & 5 & 8 & 1 & 0 \\ 0 & 2 & 6 & 14 & 13 & 11 & 7 & 12 & 9 & 3 & 4 & 10 & 5 & 8 & 1 \end{bmatrix}, \quad (4.46)$$

перший рядок якої є базовим кодовим словом, на основі якого, використовуючи властивості подвійної циклічності кодів Ріда-Соломона, можливо побудувати решту всіх кодових слів, застосовуючи операцію циклічного зсуву за часом і циклічного зсуву за частотою (з використанням

арифметики поля Галуа $GF(2^4)$). При цьому загальна кількість кодових слів збудованого нами коду частотних розстановок визначається як

$$J = q(q-1) = 16 \cdot 15 = 240. \qquad (4.47)$$

З огляду на те, що довжина кожної частотної розстановки відповідно до побудови стеганографічного методу повинна становити $n = 4$, зробимо усічення кожного кодового слова РС-коду до зазначеної довжини, отримані в результаті кодові слова представлені в табл. 4.9. При цьому, для стислості кодові слова записані у шістнадцятковому вигляді.

Таблиця 4.9. — Усічені кодові слова РС-коду над полем $GF(2^4)$

26ED	6EDB	EDB7	DB7C	B7C9	7C93	C934	934A	34A5	4A58	A581	5810	8102	1026	026E
37FC	7FCA	FCA6	CA6D	A6D8	6D82	D825	825B	25B4	5B49	B490	4901	9013	0137	137F
04CF	4CF9	CF95	F95E	95EB	5EB1	EB16	B168	1687	687A	87A3	7A32	A320	3204	204C
15DE	5DE8	DE84	E84F	84FA	4FA0	FA07	A079	0796	796B	96B2	6B23	B231	2315	315D
62A9	2A9F	A9F3	9F38	F38D	38D7	8D70	D70E	70E1	0E1C	E1C5	1C54	C546	5462	462A
73B8	3B8E	B8E2	8E29	E29C	29C6	9C61	C61F	61F0	1F0D	F0D4	0D45	D457	4573	573B
408B	08BD	8BD1	BD1A	D1AF	1AF5	AF52	F52C	52C3	2C3E	C3E7	3E76	E764	7640	6408
519A	19AC	9AC0	AC0B	C0BE	0BE4	BE43	E43D	43D2	3D2F	D2F6	2F67	F675	6751	7519
AE65	E653	653F	53F4	3F41	F41B	41BC	1BC2	BC2D	C2D0	2D09	D098	098A	98AE	8AE6
BF74	F742	742E	42E5	2E50	E50A	50AD	0AD3	AD3C	D3C1	3C18	C189	189B	89BF	9BF7
8C47	C471	471D	71D6	1D63	D639	639E	39E0	9E0F	E0F2	0F2B	F2BA	2BA8	BA8C	A8C4
9D56	D560	560C	60C7	0C72	C728	728F	28F1	8F1E	F1E3	1E3A	E3AB	3AB9	AB9D	B9D5
EA21	A217	217B	17B0	7B05	B05F	05F8	5F86	F869	8694	694D	94DC	4DCE	DCEA	CEA2
FB30	B306	306A	06A1	6A14	A14E	14E9	4E97	E978	9785	785C	85CD	5CDF	CDFB	DFB3
C803	8035	0359	3592	5927	927D	27DA	7DA4	DA4B	A4B6	4B6F	B6FE	6FEC	FEC8	EC80
D912	9124	1248	2483	4836	836C	36CB	6CB5	CB5A	B5A7	5A7E	A7EF	7EFD	EFD9	FD91

З метою максимізації кількості доступних розділених каналів зв'язку в загальному стеганоканалі в запропонованому методі використовується правило суперпозиції кодових слів просторового S-коду та частотного F-коду шляхом накладання частотних складових F-коду на активні позиції S-коду.

Таким чином, загальна кількість абонентів, які можуть бути зареєстровані та теоретично одночасно передавати інформацію у стеганоканалі становить

$$J = J_S J_F = 20 \cdot 240 = 4800. \qquad (4.48)$$

Розглянемо конкретний приклад. Нехай абоненту A_1 виділено кодове слово S-коду $\{s_{1,i}\}=\{1111000000000000\}$, а також кодове слово F-коду $C_1=\{26\text{ED}\}=\{2\ \ 6\ \ 14\ \ 13\}$. Для отримання кодових слів T^+ та T^-, що використовуються для вбудовування інформаційних символів «0» та «1», відповідно, абонент виконує суперпозицію виділених йому кодових слів S-коду та F-коду, для чого слідує наступному алгоритму:

Крок 1. Подати кодове слово S-коду у вигляді матриці розміру 4×4 шляхом послідовного заповнення її рядків.

Крок 2. Послідовно записати у активні позиції отриманої на *Кроці 1* матриці частотні компоненти, індекси яких визначаються значеннями виданого кодового слова.

Виконуючи *Крок 1* та *Крок 2* представленого алгоритму для нашого прикладу, отримуємо наступну конструкцію

$$T^{+\prime}=\begin{bmatrix} f_2 & f_6 & f_{14} & f_{13} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \qquad (4.49)$$

Крок 3. Провести підстановку конкретних кодових слів $T_{4,(n,m)}$, поданих у табл. 4.8. на основі їх відповідності частотним складовим. При цьому замість значень «0» в матриці (4.49) проводиться підстановка нульових матриць розміру 4×4. В результаті отримуємо кодове слово для кодування даним абонентом символу «0».

Крок 4. Для формування кодового слова T^- виконуємо інверсію кодового слова T^+, отриманого на *Кроці 3*.

У разі нашого прикладу отримуємо наступні кодові слова T^+ та T^-

$$T^{+}=\left[\begin{array}{c|c|c|c}
1\,1{-1}{-1} & 1\;1{-1}{-1} & 1\;1{-1}{-1} & 1{-1}\;1{-1}\\
1\,1{-1}{-1} & {-1}{-1}\;1\;1 & {-1}{-1}\;1\;1 & {-1}\;1{-1}\;1\\
1\,1{-1}{-1} & 1\;1{-1}{-1} & {-1}{-1}\;1\;1 & {-1}\;1{-1}\;1\\
1\,1{-1}{-1} & {-1}{-1}\;1\;1 & 1\;1{-1}{-1} & 1{-1}\;1{-1}\\
\hline
0000 & 0000 & 0000 & 0000\\
0000 & 0000 & 0000 & 0000\\
0000 & 0000 & 0000 & 0000\\
0000 & 0000 & 0000 & 0000\\
\hline
0000 & 0000 & 0000 & 0000\\
0000 & 0000 & 0000 & 0000\\
0000 & 0000 & 0000 & 0000\\
0000 & 0000 & 0000 & 0000\\
\hline
0000 & 0000 & 0000 & 0000\\
0000 & 0000 & 0000 & 0000\\
0000 & 0000 & 0000 & 0000\\
0000 & 0000 & 0000 & 0000
\end{array}\right],\tag{4.50}$$

$$T^{-}=\left[\begin{array}{c|c|c|c}
{-1}{-1}{+1}{+1} & {-1}{-1}{+1}{+1} & {-1}{-1}{+1}{+1} & {-1}{+1}{-1}{+1}\\
{-1}{-1}{+1}{+1} & {+1}{+1}{-1}{-1} & {+1}{+1}{-1}{-1} & {+1}{-1}{+1}{-1}\\
{-1}{-1}{+1}{+1} & {-1}{-1}{+1}{+1} & {+1}{+1}{-1}{-1} & {+1}{-1}{+1}{-1}\\
{-1}{-1}{+1}{+1} & {+1}{+1}{-1}{-1} & {-1}{-1}{+1}{+1} & {-1}{+1}{-1}{+1}\\
\hline
0000 & 0000 & 0000 & 0000\\
0000 & 0000 & 0000 & 0000\\
0000 & 0000 & 0000 & 0000\\
0000 & 0000 & 0000 & 0000\\
\hline
0000 & 0000 & 0000 & 0000\\
0000 & 0000 & 0000 & 0000\\
0000 & 0000 & 0000 & 0000\\
0000 & 0000 & 0000 & 0000\\
\hline
0000 & 0000 & 0000 & 0000\\
0000 & 0000 & 0000 & 0000\\
0000 & 0000 & 0000 & 0000\\
0000 & 0000 & 0000 & 0000
\end{array}\right].$$

Отримані кодові слова T^{+} та T^{-} використовуються для вбудовування інформаційних символів «0» та «1», відповідно. Вбудовування інформації кожен користувач виконує незалежно від інших користувачів у той час, який є зручним для нього. Розглянемо алгоритми вбудовування та вилучення інформації.

Алгоритм вбудовування інформації

Крок 1. Кожному з абонентів стеганографічної системи привласнюється свій унікальний код $\{\{s_{z_1,i}\},C_{z_2}\}$, що складається з кодового слова S-коду просторових розстановок і кодового слова F-коду частотних розстановок.

Крок 2. На основі отриманого набору $\{\{s_{z_1,i}\},C_{z_2}\}$, з урахуванням (4.41), а також кодових слів $f_i, i=1,2,...,16$, кожен з абонентів формує кодові слова T^{+} та T^{-}, за допомогою яких буде відбуватися передача інформації.

Крок 3. Кожен з абонентів A_z розбиває зображення-контейнер на блоки розміру $\mu \times \mu = 16 \times 16$ і здійснює вбудовування одного біта $d_{z,k}$ ДІ у кожен із блоків контейнера X_k шляхом застосування операції підсумовування, тобто кожен блок стеганоповідомлення обчислюється як

$$M_k = X_k + D_k . \tag{4.51}$$

Алгоритм вилучення інформації

Крок 1. Абонент, який прийняв стеганоповідомлення розбиває його на блоки M_k розміру $\mu \times \mu = 16 \times 16$, кожен з яких послідовно піддається обробці з метою отримання біта інформації $d_{z,k}$, призначеного для даного абонента.

Крок 2. Абонент знаходить матрицю різниці Δ_k між кожним блоком прийнятого стеганоповідомлення M_k та зображення-контейнера X_k.

Крок 3. Кожен із блоків матриці різниці Δ_k абонент розбиває ще на 16 підблоків розміру $\frac{\mu}{4} \times \frac{\mu}{4} = 4 \times 4$ відповідно до конструкції (4.41). З отриманих підблоків абонент вибирає ті, номер яких відповідає номерам позицій кодового слова S-коду просторових розстановок $\{s_{z_1,i}\}$, на яких воно приймає значення 1 (при його поданні у вигляді матриці розміру 4×4 шляхом послідовного заповнення її рядків). Зважаючи на те, що всі кодові слова S-коду мають вагу $w = 4$, кожен з абонентів на цьому кроці вибирає чотири підблоки розміру 4×4. Кожний із отриманих підблоків абонент представляє як вектор $\{\delta_{z,i}\}, i = 1,2,...,16$ довжини $4^2 = 16$ шляхом послідовної конкатенації його рядків.

Крок 4. Відповідно до виданого абоненту коду частотних розстановок C_{z_2} він вибирає рядки матриці Уолша-Адамара H_{16}, які позначаються як $\{h_{z,1}\},\{h_{z,2}\},\{h_{z,3}\},\{h_{z,4}\}$.

Крок 5. Абонент A_z обчислює вектор P відповідно до наступної формули

$$P_{z,k} = [p_1 \quad p_2 \quad p_3 \quad p_4],$$
$$p_i = \sum_{k=1}^{\mu^2} \delta_{j,k} h_{j,k}, i = \{1,2,3,4\}. \tag{4.52}$$

Крок 6. Абонент обчислює призначений йому біт даних вбудований у блок Δ_i за допомогою наступної формули

$$d_{z,k} = sign\left(\sum_{i=1}^{4} p_i\right). \tag{4.53}$$

За побудовою запропонованого стеганографічного методу стає ясно, що PSNR стеганоповідомлення буде залежати від кількості абонентів в системі, які одночасно здійснюють передачу інформації, а також від виду кодових слів S-коду і F-коду. При підключенні абонентів у порядку представлення кодових слів (4.43) та табл. 4.8. графік залежності PSNR від кількості абонентів, що одночасно функціонують в системі, буде мати вигляд, представлений на рис. 4.8.

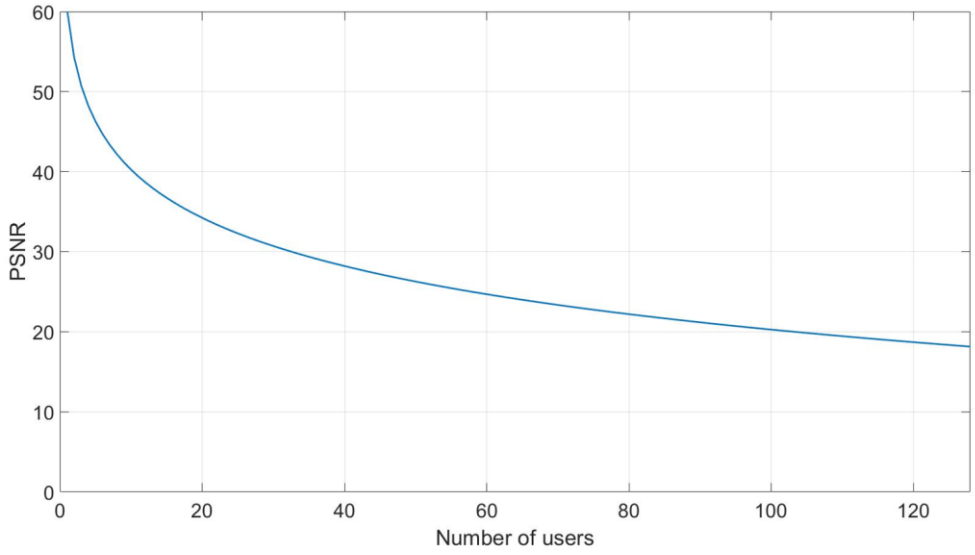


Рис. 4.8. — Графік залежності PSNR стеганоповідомлення від кількості абонентів, що одночасно передають інформацію по стеганоканалу

Аналіз даних рис. 4.8 показує, що при кількості абонентів, що одночасно передають інформацію $N \le 32$, вдається досягти значення PSNR

більше 30 дБ. При одночасній роботі $N \leq 100$ абонентів рівень PSNR стеганоповідомлення не опускається нижче 20 дБ.

З огляду на те, що кодові слова S-коду просторових розстановок (4.43) допускають не більше одного збігу в просторі так само, як і кодові слова F-коду частотних розстановок (табл. 4.8.) допускають не більше одного збігу за частотою, очевидним є виникнення в стеганографічній системі внутрішньосистемних завад, рівень яких буде прямо пропорційний кількості абонентів, що одночасно передають інформацію. Ясно також, що рівень внутрішньосистемних завад залежатиме від конкретних кодових слів S-коду та F-коду абонентів, які в даний час передають інформацію через стеганоканал.

На рис. 4.9 представлений графік залежності кількості помилок у стеганоканалі, що виникають внаслідок дії внутрішньосистемних завад від кількості абонентів, що одночасно працюють, при їх підключенні в порядку подання кодових слів (4.43) і табл. 4.8.

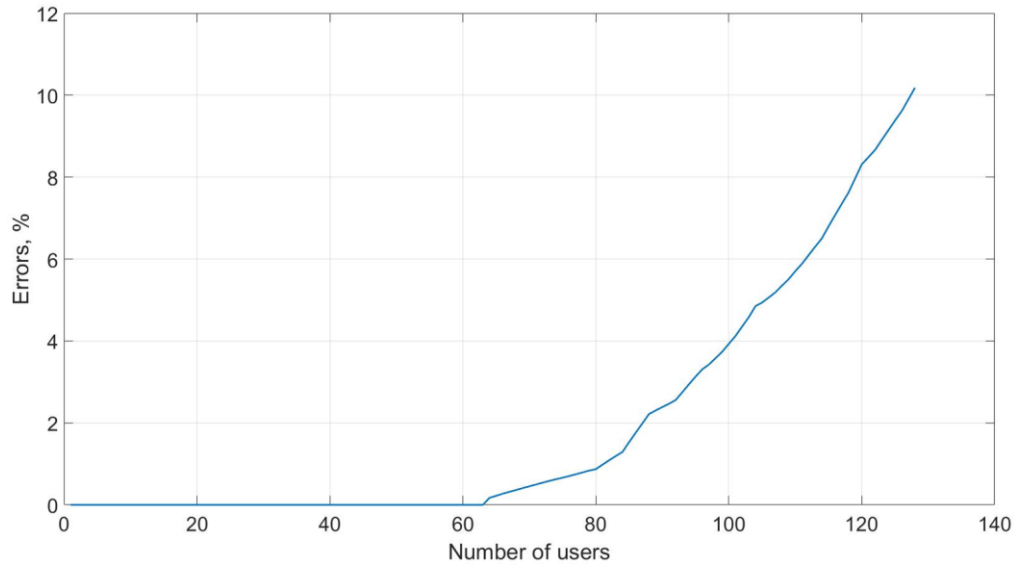


Рис. 4.9. — Графік залежності кількості помилок у стеганоканалі, що виникають внаслідок дії внутрішньосистемних завад від кількості абонентів, що одночасно працюють

Аналіз даних рис. 4.9. показує, що при обраному порядку підключення абонентів та їх кількості $N \leq 64$ внутрішньосистемні завади відсутні, у результаті вся інформація передається без спотворень. У разі кількості абонентів $N \leq 100$ кількість помилок, що виникають внаслідок дії внутрішньосистемних завад не перевищує рівня 4%, що є допустимим.

4.4. Висновки

Отримані у розділі результати дозволили підвищити пропускну спроможність стеганографічних методів з множинним доступом на основі технології MC-CDMA на 6.25%, а також розробити стеганографічні методи з кодовим управлінням вбудовуванням ДІ, що забезпечують множинний доступ до стеганоканалу і дозволяють підвищити кількість зареєстрованих у системі абонентів у 1200 разів та кількість одночасно працюючих абонентів у 16 разів.

Відзначимо основні результати проведених досліджень у вигляді конкретних пунктів:

1. Подальший розвиток отримали методи побудови стеганографічних систем з множинним доступом на основі перетворення Уолша-Адамара. Виведені і доведені співвідношення, що визначають як можливі значення коефіцієнтів перетворення Уолша-Адамара для заданого значення числа каналів N, що розділяються, так і ймовірності появи заданих значень коефіцієнтів перетворення Уолша-Адамара. Зазначені співвідношення дозволяють строго теоретично розрахувати імовірнісні характеристики алфавіту коефіцієнтів перетворення Уолша-Адамара для довільного значення числа каналів, що розділяються, що виключає необхідність набору відповідної статистики перебірним методом при побудові ефективних кодів.
2. Для стеганографічних систем, що використовують технологію MC-CDMA, проведено дослідження залежності середньої довжини кодового

слова від числа каналів N, що розділяються. Для практично обґрунтованих значень кількості каналів N, що розділяються, визначені середні довжини кодового слова Гаффмана. Емпірично показано, що зі зростанням числа каналів, що розділяються, збільшення в інформаційній ентропії коефіцієнтів-перетворення Уолша-Адамара прямує до значення $1/2$ при кожному подвоєнні величини N. Для практично цінного числа каналів, що розділяються $N=4$, запропонований ефективний метод кодування коефіцієнтів перетворення Уолша-Адамара за допомогою кодових слів С-коду, заснованого на бент-послідовностях. Порівняно з використанням коду Гаффмана для кодування коефіцієнтів перетворення Уолша-Адамара, запропонований код дозволяє упаковувати коефіцієнти Уолша-Адамара на 6,25% ефективніше, а також детектувати як мінімум одну помилку, що підтверджує цілісність вбудованої інформації. Таким чином, при використанні запропонованого ефективного методу кодування надмірність, що вноситься в інформацію, що передається по стеганоканалу, витрачається не тільки на ущільнення каналів, але і на додавання коректуючих властивостей.

3. На відміну від відомих аналогів, що здійснюють кодовий розподіл каналів незалежно від вбудовування інформації в контейнер, у цьому розділі розроблено повноцінний стеганографічний метод з множинним доступом на основі кодового управління та частотних розстановок. Розроблений стеганографічний метод забезпечує роздільне вбудовування (або його відсутність) інформації кожним користувачем у будь-який зручний для нього час з використанням особистої частотної розстановки. При цьому, як коди частотних розстановок запропоновано використовувати РС-коди над полями $GF(5)$ і $GF(13)$, що забезпечують максимальну надійність сприйняття і найбільшу кількість одночасно працюючих абонентів. Досліджено характеристики розробленого методу, в рамках чого показано, що PSNR результуючого зображення залежить від кількості абонентів, що одночасно

передають інформацію через стеганографічний канал. При кількості абонентів, що одночасно працюють $N \le 8$, значення PSNR залишаються на допустимому рівні. Виявлено наявність внутрішньосистемних завад у стеганографічному каналі при кількості абонентів, що одночасно передають інформацію $N > q$. Однак, у разі використання частотних розстановок на основі РС-кодів над полем $GF(13)$ при кількості абонентів $N = 20$ кількість генерованих внутрішньосистемними завадами помилок не перевищує 3.7%.

4. Запропоновано повноцінний стеганографічний метод з множинним доступом на основі частотно-просторових матриць, який забезпечує роздільне вбудовування (або його відсутність) інформації кожним абонентом у зручний для нього час. Розподіл каналів абонентів відбувається за двома ознаками: просторовою та частотною, на основі S-кодів просторових розстановок та F-кодів частотних розстановок. Побудований S-код просторових розстановок потужності $J_S = 20$, що володіє властивістю не більше одного збігу, а також F-код частотних розстановок на основі коду Ріда-Соломона потужності $J_F = 240$ над полем $GF(2^4)$, що також володіє властивістю не більше одного збігу. Загальна кількість зареєстрованих у стеганографічній системі з множинним доступом абонентів дорівнює $J = 4800$, тоді як характеристики розробленого стеганографічного методу безпосередньо залежать від кількості абонентів, що одночасно здійснюють передачу інформації. Так, при кількості абонентів, що одночасно передають інформацію $N \le 32$, значення PSNR не перевищує рівня в 30 дБ, у той час як при кількості абонентів $N \le 64$ не виникає внутрішньосистемних завад. Запропонований стеганографічний метод з множинним доступом характеризується гнучкістю в розподіленні ресурсів стеганоканалу: у разі необхідності, пропускна спроможність стеганоканалу може бути збільшена зі зменшенням значень PSNR, або ж, навпаки, може бути збільшена надійність сприйняття стеганоповідомлення за рахунок зменшення кількості одночасно

працюючих в системі абонентів. При цьому вбудовування інформації в контейнер кожним із користувачів відбувається незалежно.

Список використаних джерел у четвертому розділі

1. Sheidaeian H., Zolfaghari B., Zobeiri M. An Efficient and Secure Approach to Multi-User Image Steganography Using CRC-Based CDMA. International Conference on Signal Acquisition and Processing. Singapore, 2011. Vol. 2. P. 1-5.

2. Amirtharajan R., Rayappan J. B. B. Covered CDMA multi-user writing on spatially divided image. International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace &Electronic Systems Technology (Wireless VITAE), 2011. P. 1-5.

3. Цветков К. Ю., Федосеев В. Е., Коровин В. М., Абазина Е. С. Модель кодера скрытого канала с кодовым уплотнением с использованием сигнальных последовательностей Франка-Уолша, Франка-Крестенсона. Труды Научно-исследовательского института радио. 2015. №. 1. С. 2-11.

4. Paterson K. G. On codes with low peak-to-average power ratio for multicode CDMA. HP LaboratoriesTechnicalReport HPL-2001-115, May 2001. P. 1-16.

5. Paterson K. G. Sequences for OFDM and Multi-code CDMA: two problems in algebraic coding theory, Sequences and their applications. Seta 2001. Second Int. Conference (Bergen, Norway, May 13–17, 2001). Proc. Berlin: Springer, 2002, P. 46-71.

6. Wada T., Yamazato T., Katayama M., Ogawa A. A constant amplitude coding for orthogonal multi-code CDMA systems. IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences. 1997. Vol. 80, No. 12. P. 2477-2484.

7. Schmidt K. Quaternary Constant-Amplitude Codes for Multicode CDMA, IEEE International Symposium on Information Theory. Nice, 2007, P. 2781-2785.

8. McEliece R. The theory of information and coding. CambridgeUniversityPress, 2002. 400 p.

9. Мазурков М. І. Основи теорії передавання інформації. Одеса: Наука і Техніка, 2005, с. 168.

10. Мазурков М. И. Системы широкополосной радиосвязи. Одесса: Наука и Техника , 2010. 340 с.

11. Горбенко И. Д. и др. Метод синтеза производных систем сигналов на основе криптографических дискретных последовательностей символов. Радиотехника. 2017. Вып. 188. С. 107-115.

12. Shannon C. E. A Mathematical Theory of Cryptography. USA : Bell System Technical Memo, 1945, MM 45-110-02.

13. Токарева Н. Н. Бент-функции: результаты и приложения. Обзорработ. Приклад. дискрет. математика. Томск, 2009. Сер. №1(3). С. 15—37.

14. Мазурков М. И., Соколов А. В. Регулярные привила построения полного класса бент-последовательностей длины 16. Труды ОНПУ. 2013. №2(41). С. 231-237.

15. Langevin P., Leander G. Counting all bent functions in dimension eight 99270589265934370305785861242880. Designs, CodesandCryptography. 2011. Vol. 59. No. 1. P. 193-205.

16. Мазурков М. И., Соколов А. В. Конструктивные методы синтеза двоичного корректирующего кода длины 32 для технологии MC-CDMA. Известия ВУЗов. Радиоэлектроника, 2019. Т. 62, №3. С. 123-135.

17. Соколов А. В., Цевух И. В. О существовании бинарных С-кодов длины N=32 с заданным значением пик-фактора спектра Уолша–Адамара. ПФМТ, 2017. № 2(31). С. 91-95.

18. Соколов А. В., Гаркуша А. А. Бесконечные семейства последовательностей Пэли с оптимальным пик-фактором спектра Уолша-Адамара. Научные труды ОНАС им. АС Попова, 2016. №2, 2016. С. 163-169.

19. Соколов А. В. Конструктивный метод синтеза последовательностей длины N = 20 с оптимальным спектром Уолша-Адамара. Научные труды ОНАС им. А.С. Попова, 2015. №2. С. 118—126.

20. Fu H., Kong X., Wang Z. Binary code reranking method with weighted hamming distance. Multimedia tools and applications, 2016. Vol. 75. No. 3. P. 1391-1408.

21. Kobozeva A. A., Sokolov A. V. Robust Steganographic Method with Code-Controlled Information Embedding. Problemele energeticii regionale. 2021. No. 4 (52). P. 115-130.

22. Кобозева А. А., Хорошко В. А. Анализ информационной безопасности. К.: Изд. ГУИКТ, 2009. 251 с.

23. NRCS Photo Gallery // United States Department of Agriculture. URL: https://www.nrcs.usda.gov/wps/portal/nrcs/main/national/newsroom/multimedia/

Розділ 5.
ЗАСТОСУВАННЯ ФУНКЦІЙ БАГАТОЗНАЧНОЇ ЛОГІКИ ДЛЯ ПІДВИЩЕННЯ КРИПТОГРАФІЧНОЇ ЗАХИЩЕННОСТІ КРИПТО-СТЕГАНОГРАФІЧНИХ СИСТЕМ

Як випливає з аналітичних досліджень, результати яких представлені у Розділі 1, криптографічна складова є невід'ємною частиною сучасних крипто-стеганографічних систем. Таким чином, підвищення ефективності крипто-стеганографічних систем потребує вдосконалення та підвищення ефективності їх криптографічної складової.

Математичною основою конструювання та використання всіх сучасних криптографічних алгоритмів є теорія булевих функцій, яка застосовується для вибору конструкцій криптографічних алгоритмів (насамперед, їх S-блоків) таким чином, щоб вони задовольняли критеріям криптографічної якості: критерію максимізації алгебраїчної нелінійності, критерію максимізації дистанційної нелінійності, суворому лавинному критерію, критерію кореляційного імунітету, тощо. Саме відповідність переліченим критеріям забезпечує імплементацію шифром методів дифузії та конфузії. Тим не менш, криптоаналітик не є обмеженим застосуванням математичного апарату теорії булевих функцій під час здійснення атак на шифр, та може уявляти його конструкції будь-яким чином, в тому числі, за допомогою математичного апарату функцій багатозначної логіки (ФБЛ). Як показують численні проведені дослідження [1…3], математичний апарат ФБЛ є основою для подальшого підвищення криптографічної якості конструкцій, що застосовуються у сучасних шифрах, отже, і їх ефективності.

Основою для застосування математичного апарату ФБЛ у криптографії є розробка та обґрунтування критеріїв криптографічної якості ФБЛ.

Метою цього розділу, є створення базисних елементів теорії криптографічної якості ФБЛ.

Для досягнення цієї мети мають бути вирішені наступні задачі:

1. розробити метод уявлення ФБЛ у вигляді алгебраїчної нормальної форми для значень основ $q = p$ і $q = p^k$, де p — просте число;

2. розробити критерії оцінки нелінійності ФБЛ в сенсі степеню віддалення від множини афінних функцій (функцій Віленкіна-Крестенсона і їх знакових кодувань);

3. розробити критерії оцінки лавинних властивостей ФБЛ;

4. розробити критерії оцінки кореляційного імунітету ФБЛ.

5.1. Загальні засади уявлення та опису ФБЛ

Введемо необхідне нам визначення ФБЛ.

Визначення 5.1.1 [2]. Функцією q-значної логіки (далі q-функція) k змінних називається відображення $\{0,1,2,...,q-1\}^k \to \{0,1,2,...,q-1\}$.

Визначення ФБЛ є більш загальним за визначення булевих функцій. Так, при підстановці значення $q = 2$ у **Визначення 5.1.1.** отримаємо відоме визначення булевих функцій.

Одним із зручних і поширених способів уявлення ФБЛ, так само, як і для функцій двійкової логіки, є таблиця істинності, яка ставить у відповідність кожному з наборів число, яке належить алфавіту $\{0,1,2,...,q-1\}$.

Наприклад, визначимо функцію тризначної логіки за допомогою таблиці істинності довжини $N = 3^k = 9$

x:	00	01	02	10	11	12	20	21	22
$f(x)$	0	0	0	1	1	1	2	2	2.

(5.1)

Аналогічно до двійкового випадку таблиці істинності для стислості часто приводять без відповідних їм значенням аргументів, маючи на увазі лексикографічний порядок проходження, так таблицю істинності (5.1) можна представити вектором

$$f(x) = \{000111222\}. \tag{5.2}$$

Існує також експоненційна форма [4] подання ФБЛ, яка передбачає їх визначення над алфавітом

$$F_i \in \left\{ e^{j\frac{2\pi}{q}\nu} \right\}, \nu = 0,1,...,q-1. \tag{5.3}$$

Кожний елемент експоненційної форми (5.3) однозначно відповідає елементам алфавіту $f_i \in \{0,1,...,q-1\}$.

Для ФБЛ визначено перетворення Віленкіна-Крестенсона, як добуток експоненційної таблиці істинності ФБЛ та матриці Віленкіна-Крестенсона

$$\Omega = FV^T \tag{5.4}$$

де T — оператор транспонування, а рядки матриці Віленкіна-Крестенсона будуються відповідно до наступного виразу [4, 5]

$$v_t(x) = \mathrm{e}^{\frac{2\pi}{q}\sum_{i=1}^{k} t_i x_i}, \tag{5.5}$$

де t_i — i-й розряд числа записаного в позиційній q-ічній системі числення,

k — число розрядів в q-ічному поданні значення N, яке визначає довжину вибіркових відліків сигналу, причому $N = q^k$.

Згідно до (5.5) запишемо матрицю Віленкіна-Крестенсона для значень $q = 3,\ N = 9$

$$V_9 = \begin{bmatrix} e^{j0} & e^{j0} & e^{j0} & e^{j0} & e^{j0} & e^{j0} & e^{j0} & e^{j0} & e^{j0} \\ e^{j0} & e^{j\frac{2\pi}{3}} & e^{j\frac{4\pi}{3}} & e^{j0} & e^{j\frac{2\pi}{3}} & e^{j\frac{4\pi}{3}} & e^{j0} & e^{j\frac{2\pi}{3}} & e^{j\frac{4\pi}{3}} \\ e^{j0} & e^{j\frac{4\pi}{3}} & e^{j\frac{2\pi}{3}} & e^{j0} & e^{j\frac{4\pi}{3}} & e^{j\frac{2\pi}{3}} & e^{j0} & e^{j\frac{4\pi}{3}} & e^{j\frac{2\pi}{3}} \\ e^{j0} & e^{j0} & e^{j0} & e^{j\frac{2\pi}{3}} & e^{j\frac{2\pi}{3}} & e^{j\frac{2\pi}{3}} & e^{j\frac{4\pi}{3}} & e^{j\frac{4\pi}{3}} & e^{j\frac{4\pi}{3}} \\ e^{j0} & e^{j\frac{2\pi}{3}} & e^{j\frac{4\pi}{3}} & e^{j\frac{2\pi}{3}} & e^{j\frac{4\pi}{3}} & e^{j0} & e^{j\frac{4\pi}{3}} & e^{j0} & e^{j\frac{2\pi}{3}} \\ e^{j0} & e^{j\frac{4\pi}{3}} & e^{j\frac{2\pi}{3}} & e^{j\frac{2\pi}{3}} & e^{j0} & e^{j\frac{4\pi}{3}} & e^{j\frac{4\pi}{3}} & e^{j\frac{2\pi}{3}} & e^{j0} \\ e^{j0} & e^{j0} & e^{j0} & e^{j\frac{4\pi}{3}} & e^{j\frac{4\pi}{3}} & e^{j\frac{4\pi}{3}} & e^{j\frac{2\pi}{3}} & e^{j\frac{2\pi}{3}} & e^{j\frac{2\pi}{3}} \\ e^{j0} & e^{j\frac{2\pi}{3}} & e^{j\frac{4\pi}{3}} & e^{j\frac{4\pi}{3}} & e^{j0} & e^{j\frac{2\pi}{3}} & e^{j\frac{2\pi}{3}} & e^{j\frac{4\pi}{3}} & e^{j0} \\ e^{j0} & e^{j\frac{4\pi}{3}} & e^{j\frac{2\pi}{3}} & e^{j\frac{4\pi}{3}} & e^{j\frac{2\pi}{3}} & e^{j0} & e^{j\frac{2\pi}{3}} & e^{j0} & e^{j\frac{4\pi}{3}} \end{bmatrix}, \quad (5.6)$$

тоді подання 3-функції (5.1) у вигляді коефіцієнтів перетворення Віленкіна-Крестенсона матиме вигляд $Q = [0 \quad 0 \quad 0 \quad 9 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0]$.

Найважливішим інструментом, покладеним в основу багатьох методів оцінки криптографічних властивостей булевих функцій, є поліном Жегалкіна або АНФ. Так, за допомогою АНФ оцінюється алгебраїчний степінь нелінійності S-блоків підстановки, вводиться поняття відстані нелінійності [6]. На основі АНФ булевих функцій запропонований метод побудови таких досконалих алгебраїчних конструкцій, як бент-функції [7…14], які відіграють істотну роль в теорії кодування і криптографії. АНФ також є основою побудови важливих в теорії кодування коректувальних кодів Ріда-Маллера [16…18].

Відзначимо також, що АНФ булевих функцій важливі для реалізації ПЛІС. Ще одним застосуванням АНФ є побудова генераторів псевдовипадкових ключових послідовностей [19].

З перерахованого вже зрозуміла актуальність побудови методів синтезу АНФ довільної q-функції для задач оцінки рівня її алгебраїчної нелінійності.

Далі ми наводимо методи визначення АНФ ФБЛ для значень $q = 3$ та $q = 2^k$, які є необхідними в контексті досліджень, що проводяться в даному розділі. На основі **Визначення 5.1.1** введемо визначення 3-функції.

Визначення 5.1.2. Функція тризначної логіки (3-функція) — це відображення $\{0,1,2\}^k \to \{0,1,2\}$, тобто правило, яке однозначно зіставляє вектору з k координат, які приймають значення 0,1,2 значення 0,1 або 2.

Аналогічно до поліномів Жегалкіна для випадку булевих функцій ми вводимо визначення алгебраїчної нормальної форми q-функцій.

Визначення 5.1.3. Алгебраїчною нормальною формою q-функції називається поліном Ф над Z_q степеню $\deg(\Phi) < q$ з коефіцієнтами $a_i \in \{0,1,...,q-1\}$, що містить операції «Сума по модулю q» і «Множення по модулю q».

Приклад. Розглянемо 3-функції $k = 2$ змінних, таблиця істинності яких має довжину $N = 9$ і може бути представлена в загальному вигляді

$$f = \{f_{00}, f_{01}, f_{02}, f_{10}, f_{11}, f_{12}, f_{20}, f_{21}, f_{22}\}. \tag{5.7}$$

З іншого боку, відповідно до **Визначення 5.1.3** для 3-функцій двох змінних можна виписати поліном АНФ в загальному вигляді

$$\begin{aligned} f(x_1, x_2) = a_{00} + a_{01}x_2 + a_{02}x_2^{\,2} + a_{10}x_1 + a_{11}x_1x_2 + a_{12}x_1x_2^{\,2} + \\ + a_{20}x_1^{\,2} + a_{21}x_1^{\,2}x_2 + a_{22}x_1^{\,2}x_2^{\,2}, \end{aligned} \tag{5.8}$$

де $a_{ij} \in \{0,1,2\}$ – шукані коефіцієнти.

Для того щоб зв'язати шукані коефіцієнти a_{ij} з елементами таблиці істинності 3-функції (5.7), записуємо відповідну систему рівнянь

$$\begin{cases} f_{00} = a_{00}; \\ f_{01} = a_{00} + a_{01} + a_{02}; \\ f_{02} = a_{00} + 2a_{01} + a_{02}; \\ f_{10} = a_{00} + a_{10} + a_{20}; \\ f_{11} = a_{00} + a_{01} + a_{10} + a_{02} + a_{11} + a_{20} + a_{12} + a_{21} + a_{22}; \\ f_{12} = a_{00} + 2a_{01} + a_{10} + a_{02} + 2a_{11} + a_{20} + a_{12} + 2a_{21} + a_{22}; \\ f_{20} = a_{00} + 2a_{10} + a_{20}; \\ f_{21} = a_{00} + a_{01} + 2a_{10} + a_{02} + 2a_{11} + a_{20} + 2a_{12} + a_{21} + a_{22}; \\ f_{22} = a_{00} + 2a_{01} + 2a_{10} + a_{02} + a_{11} + a_{20} + 2a_{12} + 2a_{21} + a_{22}, \end{cases} \tag{5.9}$$

де знак «+» слід розуміти як складання по модулю 3.

Представляючи знайдену систему рівнянь в матричній формі, отримуємо, відповідно, матрицю L_9^{-1} для випадку 3-функцій двох змінних

$$L_9^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 & 2 & 1 & 1 & 2 & 1 \\ 1 & 0 & 0 & 2 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 2 & 2 & 2 & 1 & 1 & 1 \\ 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 \end{bmatrix}. \qquad (5.10)$$

Проведені емпіричні дослідження дозволили встановити: побудова матриць зворотного перетворення АНФ L_n^{-1} порядку N, кратного трьом, може бути здійснено у відповідності з наступною рекурентною формулою

$$L_{3n}^{-1} = \begin{bmatrix} L_n^{-1} & 0 & 0 \\ L_n^{-1} & L_n^{-1} & L_n^{-1} \\ L_n^{-1} & 2L_n^{-1} & L_n^{-1} \end{bmatrix}, \; L_1^{-1} = [1], \qquad (5.11)$$

де під знаком «0» розуміється нульова матриця порядку n.

Обчислювальні експерименти, проведені в середовищі MatLAB, дозволили підтвердити правильність висунутої гіпотези для практично цінних значень $n < 6$.

Для знаходження матриці прямого перетворення (необхідної для розрахунку коефіцієнтів АНФ) матриця L_n^{-1} повинна бути обернена

$$L = (L^{-1})^{-1} = \mathrm{adj}(L) \cdot \det{}^{-1}(L), \qquad (5.12)$$

де $\mathrm{adj}(L)$ — союзна матриця над алфавітом $\{0,1,2\}$,

$\det^{-1}(L)$ — елемент, зворотний до визначника матриці.

Для матриці (5.10), тобто для випадку 3-функцій двох змінних, зворотна матриця має такий вигляд

$$L_9 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 2 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}. \qquad (5.13)$$

Відзначимо важливу властивість: на відміну від випадку булевих функцій, для q-функцій при $q > 2$ матриці прямого і зворотного перетворення АНФ не збігаються.

Ґрунтуючись на (5.11), (5.12) і (5.13), можемо записати регулярний метод знаходження АНФ 3-функцій довільної кількості змінних у вигляді кроків.

Крок 1. Ґрунтуючись на (5.11) з урахуванням (5.10) знайти матрицю зворотного перетворення L_n^{-1} необхідного порядку $n = 3^k$.

Крок 2. На основі (5.12) або ж з використанням одного з відомих алгоритмів обернення матриць над алфавітом $\{0,1,...,q-1\}$ [20] знайти матрицю $n = 3^k$.

Крок 3. Знайти всі коефіцієнти АНФ 3-функцій шляхом множення матриці перетворення порядку $n = 3^k$ на таблицю істинності 3-функції f. При цьому природним є і зворотне перетворення

$$A = f \cdot L_n, \quad f = A \cdot L_n^{-1}, \qquad (5.14)$$

Вираз (5.14) повністю визначає пряме і зворотне перетворення Ріда-Маллера для випадку функцій багатозначної логіки, що дозволяє шляхом простого матричного множення отримати коефіцієнти АНФ довільної булевої функції.

Розглянемо приклад, який ілюструє роботу запропонованого методу. Нехай, наприклад, задана 3-функція п'яти змінних у вигляді своєї таблиці істинності

$$f = \{000222111000222111000222111000222111 \\ 000222111000222111000222111000222111000 \\ 222111000222111000222111000222111111000 \\ 211102022111101022011100022211100120211 \\ 002212000222111000222111000222111222111 \\ 002221100202221120102221110002221210012 \\ 2101002\}. \quad (5.15)$$

Шляхом множення таблиці істинності 3-функції (5.15) на матрицю L_{243}, побудовану відповідно до (5.11) та (5.12), одержуємо коефіцієнти АНФ 3-функції

$$A = \{000200000000000000000000000000000000000 \\ 000000000000000000000000000000000000000 \\ 000000000000000000000000000000000000000 \\ 000010000000000001000000000000000000000 \\ 000000000000000000000000000001000000000 \\ 000000000000000000000\}, \quad (5.16)$$

а також, власне, АНФ

$$\Phi(x_1, x_2, x_3, x_4, x_5) = 2x_4 + x_1x_2^{\,2} + x_1x_2^{\,2}x_3x_4x_5 + x_1^{\,2}x_2x_3x_4^{\,2}x_5^{\,2}. \quad (5.17)$$

Підстановка всіх можливих значень $\{x_1, x_2, x_3, x_4, x_5\} \in \{0,1,2\}$ в (5.17) дозволяє знову повернутися до таблиці істинності (5.15), що підтверджує правильність отриманої АНФ.

Відзначимо, що подібно до перетворення Ріда-Маллера для булевих функцій, застосування розробленого регулярного методу знаходження АНФ 3-функцій за обчислювальною складністю еквівалентно множенню матриці на вектор над скінченним полем, за умови, що матриця перетворення знайдена завчасно. Дана властивість запропонованого методу обумовлює його високу практичну цінність.

Для вирішення задач цього розділу необхідною є також розробка методу синтезу АНФ ФБЛ у полях $GF(2^k)$ [21]. Це завдання, окрім цього, є необхідним для визначення якості криптографічних конструкції, яке було проведено автором, в роботах [22…25], та побудови криптографічно високоякісних примітивів, що є частинами блокових симетричних шифрів, що було виконано автором, наприклад, в роботах [26…28].

Далі, проаналізуємо приклад знаходження АНФ для ізоморфних уявлень поля $GF(4)$ [21]. Слід зазначити, що абсолютно аналогічно можуть бути розглянуті будь-які інші поля $GF(p^k)$.

На підставі аналізу літературних джерел можливо зробити висновок, що математичний апарат синтезу АНФ 4-функцій над полем $GF(4)$ на сьогодні не розроблений. Дана обставина унеможливлює застосування такого критерію криптографічної якості, як алгебраїчний степінь нелінійності 4-функцій, який відіграє значну роль у протидії атакам лінійного криптоаналізу [29…31].

З метою розробки методу синтезу АНФ ФБЛ над розширеними полями Галуа введемо наступне твердження.

Твердження 5.1.1. Будь-яку 4-функцію можна єдиним чином представити за допомогою АНФ над полем $GF(4)$, тобто за допомогою полінома, що містить операції додавання і множення в полі $GF(4)$.

Відомо, що існує єдиний первісний незвідний поліном $f(x) = x^2 + x + 1$ степеню $k = 2$ [32], а отже таблиця множення у полі $GF(4)$ може бути побудована лише одним способом. Наведемо таблицю складання та таблицю множення у полі $GF(4)$

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

,

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

. (5.18)

Наприклад, розглянемо 4-функції однієї змінної x_1. У загальному випадку АНФ 4-функції однієї змінної має вигляд

$$\Phi(x_1) = a_0 + a_1 x_1 + a_2 x_1^2 + a_3 x_1^3, \quad (5.19)$$

тоді як набір коефіцієнтів α_i визначається конкретно для кожної 4-функції однієї змінної $f(x_1)=\{f_0 \quad f_1 \quad f_2 \quad f_3\}$, представленої у вигляді таблиці істинності.

Наступна система рівнянь пов'язує коефіцієнти α_i з елементами таблиці істинності f_j

$$\begin{cases} f_0 = a_0; \\ f_1 = a_0 + a_1 + a_2 + a_3; \\ f_2 = a_0 + 2a_1 + 3a_1 + a_3; \\ f_3 = a_0 + 3a_1 + 2a_2 + a_3. \end{cases} \tag{5.20}$$

Запишемо систему рівнянь (5.20) в матричній формі

$$F = L_4^{-1}A, \text{ где } F = \begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \end{bmatrix}, \; A = \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}, \tag{5.21}$$

де $L_4^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 3 & 2 & 1 \end{bmatrix}$ — обернена матриця перетворення Ріда-Маллера.

З метою обчислення коефіцієнтів АНФ конкретно заданої 4-функції, зручно використовувати наступне матричне рівняння $A = L_4 F$, де L_4 — матриця перетворення Ріда-Маллера.

Далі для знаходження матриці L_4, необхідно знайти зворотну матрицю для L_4^{-1} над полем $GF(4)$. У такому випадку матриця L_4 буде мати вигляд

$$L_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 3 & 2 \\ 0 & 1 & 2 & 3 \\ 1 & 1 & 1 & 1 \end{bmatrix}. \tag{5.22}$$

Аналогічним (5.22) чином може бути записаний загальний вигляд АНФ 4-функцій двох змінних

$$\begin{aligned}\Phi(x_1,x_2) = a_0 + a_{01}x_2 + a_{02}x_2^2 + a_{03}x_2^3 + a_{10}x_1 + a_{11}x_1x_2 + \\ + a_{12}x_1x_2^2 + a_{13}x_1x_2^3 + a_{20}x_1^2 + a_{21}x_1^2x_2 + a_{22}x_1^2x_2^2 + \\ a_{23}x_1^2x_2^3 + a_{30}x_1^3 + a_{31}x_1^3x_2 + a_{32}x_1^3x_2^2 + a_{33}x_1^3x_2^3.\end{aligned} \quad (5.23)$$

Записуючи систему рівнянь і отримуючи пряму і зворотну матриці перетворення Ріда-Маллера для випадку четвіркових функцій двох змінних, запишемо рекурентні правила їх формування для четвіркових функцій довільного числа змінних k

$$L_{4^k}^{-1} = \begin{bmatrix} L_{4^{k-1}}^{-1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ L_{4^{k-1}}^{-1} & L_{4^{k-1}}^{-1} & L_{4^{k-1}}^{-1} & L_{4^{k-1}}^{-1} \\ L_{4^{k-1}}^{-1} & 2L_{4^{k-1}}^{-1} & 3L_{4^{k-1}}^{-1} & L_{4^{k-1}}^{-1} \\ L_{4^{k-1}}^{-1} & 3L_{4^{k-1}}^{-1} & 2L_{4^{k-1}}^{-1} & L_{4^{k-1}}^{-1} \end{bmatrix}, \; L_{4^k} = \begin{bmatrix} L_{4^{k-1}} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & L_{4^{k-1}} & 3L_{4^{k-1}} & 2L_{4^{k-1}} \\ \mathbf{0} & L_{4^{k-1}} & 2L_{4^{k-1}} & 3L_{4^{k-1}} \\ L_{4^{k-1}} & L_{4^{k-1}} & L_{4^{k-1}} & L_{4^{k-1}} \end{bmatrix}, \quad (5.24)$$

де під $\mathbf{0}$ розуміється нульова матриця порядку 4^{k-1}.

Наступним практично важливим завданням є знаходження АНФ ФБЛ над розширеним полем $GF(2^4)$. При цьому, оскільки у розширеному полі Галуа $GF(2^4)$ існують 2 первісні незвідні поліноми $g_1(x) = 19_{10} = x^4 + x + 1$ та $g_1(x) = 25_{10} = x^4 + x^3 + 1$ [32], то, відповідно, можливі дві ізоморфні форми уявлення АНФ компонентних 16-функцій, які можуть бути використані криптоаналітиком для апроксимації конструкцій криптоалгоритма.

При цьому, для побудови матриці інверсного перетворення Ріда-Маллера у полі $GF(2^4)$, арифметика якого визначається первісним незвідним поліномом $g_1(x)$, призначена наступна рекурентна конструкція

$$L_{16^k,19}^{-1} = L_{16,19}^{-1} \otimes L_{16^{k-1},19}^{-1}, \quad (5.25)$$

де $\otimes$ — символ добутку Кронекера, а

$$L_{16,19}^{-1}=\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\
1 & 2 & 4 & 8 & 3 & 6 & 12 & 11 & 5 & 10 & 7 & 14 & 15 & 13 & 9 & 1\\
1 & 3 & 5 & 15 & 2 & 6 & 10 & 13 & 4 & 12 & 7 & 9 & 8 & 11 & 14 & 1\\
1 & 4 & 3 & 12 & 5 & 7 & 15 & 9 & 2 & 8 & 6 & 11 & 10 & 14 & 13 & 1\\
1 & 5 & 2 & 10 & 4 & 7 & 8 & 14 & 3 & 15 & 6 & 13 & 12 & 9 & 11 & 1\\
1 & 6 & 7 & 1 & 6 & 7 & 1 & 6 & 7 & 1 & 6 & 7 & 1 & 6 & 7 & 1\\
1 & 7 & 6 & 1 & 7 & 6 & 1 & 7 & 6 & 1 & 7 & 6 & 1 & 7 & 6 & 1\\
1 & 8 & 12 & 10 & 15 & 1 & 8 & 12 & 10 & 15 & 1 & 8 & 12 & 10 & 15 & 1\\
1 & 9 & 13 & 15 & 14 & 7 & 10 & 5 & 11 & 12 & 6 & 3 & 8 & 4 & 2 & 1\\
1 & 10 & 8 & 15 & 12 & 1 & 10 & 8 & 15 & 12 & 1 & 10 & 8 & 15 & 12 & 1\\
1 & 11 & 9 & 12 & 13 & 6 & 15 & 3 & 14 & 8 & 7 & 4 & 10 & 2 & 5 & 1\\
1 & 12 & 15 & 8 & 10 & 1 & 12 & 15 & 8 & 10 & 1 & 12 & 15 & 8 & 10 & 1\\
1 & 13 & 14 & 10 & 11 & 6 & 8 & 2 & 9 & 15 & 7 & 5 & 12 & 3 & 4 & 1\\
1 & 14 & 11 & 8 & 9 & 7 & 12 & 4 & 13 & 10 & 6 & 2 & 15 & 5 & 3 & 1\\
1 & 15 & 10 & 12 & 8 & 1 & 15 & 10 & 12 & 8 & 1 & 15 & 10 & 12 & 8 & 1
\end{bmatrix}. \quad (5.26)$$

На основі матриці зворотного перетворення Ріда-Маллера (5.26) побудуємо також і матрицю прямого перетворення Ріда-Маллера у полі $GF(2^4)$, арифметика якого визначається первісним незвідним поліномом $g_1(x)$, яка також може бути збільшена до необхідного розміру за допомогою рекурентної конструкції

$$L_{16^k,19}=L_{16^k,19}\otimes L_{16^{k-1},19}, \quad (5.27)$$

де

$$L_{16,19}=\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 1 & 9 & 14 & 13 & 11 & 7 & 6 & 15 & 2 & 12 & 5 & 10 & 4 & 3 & 8\\
0 & 1 & 13 & 11 & 14 & 9 & 6 & 7 & 10 & 4 & 15 & 2 & 8 & 3 & 5 & 12\\
0 & 1 & 15 & 8 & 10 & 12 & 1 & 1 & 12 & 8 & 8 & 10 & 15 & 12 & 15 & 10\\
0 & 1 & 14 & 9 & 11 & 13 & 7 & 6 & 8 & 3 & 10 & 4 & 12 & 5 & 2 & 15\\
0 & 1 & 7 & 7 & 6 & 6 & 6 & 7 & 1 & 6 & 1 & 7 & 1 & 7 & 6 & 1\\
0 & 1 & 10 & 12 & 8 & 15 & 1 & 1 & 15 & 12 & 12 & 8 & 10 & 15 & 10 & 8\\
0 & 1 & 5 & 4 & 2 & 3 & 7 & 6 & 10 & 11 & 15 & 14 & 8 & 9 & 13 & 12\\
0 & 1 & 11 & 13 & 9 & 14 & 6 & 7 & 12 & 5 & 8 & 3 & 15 & 2 & 4 & 10\\
0 & 1 & 12 & 10 & 15 & 8 & 1 & 1 & 8 & 10 & 10 & 15 & 12 & 8 & 12 & 15\\
0 & 1 & 6 & 6 & 7 & 7 & 7 & 6 & 1 & 7 & 1 & 6 & 1 & 6 & 7 & 1\\
0 & 1 & 3 & 2 & 5 & 4 & 6 & 7 & 15 & 14 & 12 & 13 & 10 & 11 & 9 & 8\\
0 & 1 & 8 & 15 & 12 & 10 & 1 & 1 & 10 & 15 & 15 & 12 & 8 & 10 & 8 & 12\\
0 & 1 & 4 & 5 & 3 & 2 & 7 & 6 & 12 & 13 & 8 & 9 & 15 & 14 & 11 & 10\\
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15\\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix}. \quad (5.28)$$

Оскільки основне поле $GF(2^4)$ має два ізоморфних уявлення, АНФ компонентних 16-функцій також можна записати згідно до таблиці множення, визначеної поліномом $g_2(x)$. Таким чином, вирази (5.25) і (5.27) набувають вигляд

$$L^{-1}_{16^k,25} = L^{-1}_{16,25} \otimes L^{-1}_{16^{k-1},25},\ L_{16^k,25} = L_{16^k,25} \otimes L_{16^{k-1},25} \tag{5.29}$$

де

$$L^{-1}_{16,25} = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 2 & 4 & 8 & 9 & 11 & 15 & 7 & 14 & 5 & 10 & 13 & 3 & 6 & 12 & 1 \\
1 & 3 & 5 & 15 & 8 & 1 & 3 & 5 & 15 & 8 & 1 & 3 & 5 & 15 & 8 & 1 \\
1 & 4 & 9 & 15 & 14 & 10 & 3 & 12 & 2 & 8 & 11 & 7 & 5 & 13 & 6 & 1 \\
1 & 5 & 8 & 3 & 15 & 1 & 5 & 8 & 3 & 15 & 1 & 5 & 8 & 3 & 15 & 1 \\
1 & 6 & 13 & 5 & 7 & 11 & 8 & 2 & 12 & 3 & 10 & 14 & 15 & 9 & 4 & 1 \\
1 & 7 & 12 & 15 & 6 & 11 & 3 & 9 & 13 & 8 & 10 & 4 & 5 & 2 & 14 & 1 \\
1 & 8 & 15 & 5 & 3 & 1 & 8 & 15 & 5 & 3 & 1 & 8 & 15 & 5 & 3 & 1 \\
1 & 9 & 14 & 3 & 2 & 11 & 5 & 6 & 4 & 15 & 10 & 12 & 8 & 7 & 13 & 1 \\
1 & 10 & 11 & 1 & 10 & 11 & 1 & 10 & 11 & 1 & 10 & 11 & 1 & 10 & 11 & 1 \\
1 & 11 & 10 & 1 & 11 & 10 & 1 & 11 & 10 & 1 & 11 & 10 & 1 & 11 & 10 & 1 \\
1 & 12 & 6 & 3 & 13 & 10 & 5 & 14 & 7 & 15 & 11 & 9 & 8 & 4 & 2 & 1 \\
1 & 13 & 7 & 8 & 12 & 10 & 15 & 4 & 6 & 5 & 11 & 2 & 3 & 14 & 9 & 1 \\
1 & 14 & 2 & 5 & 4 & 10 & 8 & 13 & 9 & 3 & 11 & 6 & 15 & 12 & 7 & 1 \\
1 & 15 & 3 & 8 & 5 & 1 & 15 & 3 & 8 & 5 & 1 & 15 & 3 & 8 & 5 & 1
\end{bmatrix}, \tag{5.30}$$

і

$$L_{16,25} = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 12 & 8 & 6 & 15 & 4 & 14 & 3 & 13 & 11 & 10 & 2 & 9 & 7 & 5 \\
0 & 1 & 6 & 15 & 13 & 3 & 9 & 2 & 5 & 7 & 10 & 11 & 4 & 14 & 12 & 8 \\
0 & 1 & 3 & 5 & 5 & 8 & 15 & 5 & 15 & 8 & 1 & 1 & 8 & 3 & 15 & 3 \\
0 & 1 & 13 & 3 & 7 & 5 & 14 & 4 & 8 & 12 & 11 & 10 & 9 & 2 & 6 & 15 \\
0 & 1 & 10 & 1 & 11 & 1 & 10 & 10 & 1 & 10 & 10 & 11 & 11 & 11 & 11 & 1 \\
0 & 1 & 5 & 8 & 8 & 15 & 3 & 8 & 3 & 15 & 1 & 1 & 15 & 5 & 3 & 5 \\
0 & 1 & 14 & 15 & 2 & 3 & 12 & 13 & 5 & 4 & 11 & 10 & 7 & 6 & 9 & 8 \\
0 & 1 & 7 & 5 & 12 & 8 & 2 & 9 & 15 & 6 & 10 & 11 & 14 & 4 & 13 & 3 \\
0 & 1 & 15 & 3 & 3 & 5 & 8 & 3 & 8 & 5 & 1 & 1 & 5 & 15 & 8 & 15 \\
0 & 1 & 11 & 1 & 10 & 1 & 11 & 11 & 1 & 11 & 11 & 10 & 10 & 10 & 10 & 1 \\
0 & 1 & 9 & 8 & 14 & 15 & 7 & 6 & 3 & 2 & 10 & 11 & 13 & 12 & 4 & 5 \\
0 & 1 & 8 & 15 & 15 & 3 & 5 & 15 & 5 & 3 & 1 & 1 & 3 & 8 & 5 & 8 \\
0 & 1 & 4 & 5 & 9 & 8 & 13 & 12 & 15 & 14 & 11 & 10 & 6 & 7 & 2 & 3 \\
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix}. \tag{5.31}$$

5.2. Розроблення методу визначення нелінійності ФБЛ

Відстань нелінійності булевих функцій прийнято визначати як степінь її віддаленості, в сенсі деякої метрики, від множини функцій, прийнятих за лінійні.

У двійковому випадку, в якості такої метрики, використовується метрика Гемінга. Опис методів знаходження відстані нелінійності функцій двійкової логіки викладено в роботах [6, 33…36].

Використання метрики Гемінга або метрики Лі для порівняння відстаней нелінійності ФБЛ не дозволяє створення коректного математичного опису критерію нелінійності. Як показали численні дослідження, наприклад, [37…38], вирішення цього завдання може бути здійснено за допомогою використання коефіцієнтів перетворення Віленкіна-Крестенсона.

Нелінійність функцій багатозначної логіки будемо вимірювати як степінь несхожості даної алгебраїчної структури з множиною структур, які прийнято вважати лінійними. В якості таких структур виступають багатозначні аналоги функцій Уолша [39] — функції Віленкіна-Крестенсона.

Розглянемо спочатку випадок 3-функцій. Для випадку $k = 2$ існує 3 лінійні функції, що задаються як $\varphi'(x_0) = \mathrm{a}_0\, x_0 \bmod 3$, для $a_0, x_0 \in \{0,1,2\}$

$$f_1 = [000], \quad f_2 = [012], \quad f_3 = [021]. \tag{5.32}$$

На основі отриманих лінійних функцій, а також однозначного перетворення $0 \to e^{j\cdot 0}, 1 \to e^{j\cdot\frac{2\pi}{3}}, 2 \to e^{j\cdot\frac{4\pi}{3}}$, яке встановлює зв'язок між символічною і експоненційною формою подання 3-функцій запишемо матрицю перетворення Віленкіна-Крестенсона [40…42], що є ортогональною, тобто $V_3 V_3^T = 3E$

$$V_3 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} e^{j\cdot 0} & e^{j\cdot 0} & e^{j\cdot 0} \\ e^{j\cdot 0} & e^{j\cdot\frac{2\pi}{3}} & e^{j\cdot\frac{4\pi}{3}} \\ e^{j\cdot 0} & e^{j\cdot\frac{4\pi}{3}} & e^{j\cdot\frac{2\pi}{3}} \end{bmatrix}, \tag{5.33}$$

де E — одинична матриця.

Коефіцієнти перетворення Віленкіна-Крестенсона дискретної послідовності знаходяться шляхом множення вектора-стовпця, що містить відліки сигналу, на комплексно-сполучену матрицю перетворення $\overline{V}$.

Проведені дослідження [37] дозволили знайти спрощене правило рекурентної побудови трійкових матриць Віленкіна-Крестенсона будь-якого порядку $\mu = 3^k$, $k \in \mathrm{N}$

$$V_{3^k} = \begin{bmatrix} V_{3^{k-1}} & V_{3^{k-1}} & V_{3^{k-1}} \\ V_{3^{k-1}} & \left(V_{3^{k-1}} + 1\right) \bmod 3 & \left(V_{3^{k-1}} + 2\right) \bmod 3 \\ V_{3^{k-1}} & \left(V_{3^{k-1}} + 2\right) \bmod 3 & \left(V_{3^{k-1}} + 1\right) \bmod 3 \end{bmatrix}. \tag{5.34}$$

Наприклад, розглянемо 3-функцію

$$A = \left\{ e^{j\cdot\frac{2\pi}{3}} \quad e^{j\cdot 0} \quad e^{j\cdot\frac{4\pi}{3}} \quad e^{j\cdot\frac{2\pi}{3}} \quad e^{j\cdot 0} \quad e^{j\cdot\frac{4\pi}{3}} \quad e^{j\cdot\frac{2\pi}{3}} \quad e^{j\cdot 0} \quad e^{j\cdot\frac{4\pi}{3}} \right\}, \tag{5.35}$$

яка має наступні коефіцієнти перетворення Віленкіна-Крестенсона

$$\Omega_A = A \cdot \overline{V}_9 = \left\{ 0 \quad 0 \quad 9e^{j\cdot\frac{2\pi}{3}} \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \right\}. \tag{5.36}$$

Кожен коефіцієнт перетворення Віленкіна-Крестенсона (5.36) характеризує «вміст» тієї чи іншої функції Віленкіна-Крестенсона (рядки матриці V_{3^k}) в досліджуваній послідовності.

Так як множина функцій Віленкіна-Крестенсона прийнята в якості множини найбільш лінійних функцій, можна оцінити величину лінійності досліджуваної функції за максимальним значенням коефіцієнтів перетворення Віленкіна-Крестенсона. Так, максимальний спектральний коефіцієнт (по модулю) послідовності (5.35) $L = \max\left\{\left|S\right|\right\} = 9$ назвемо

величиною лінійності. Дійсно, послідовність (5.35) є третім рядком матриці Віленкіна-Крестенсона, таким чином значення третього коефіцієнта вектора коефіцієнтів перетворення Віленкіна-Крестенсона (5.36) вийшло максимально можливим — рівним довжині.

Оскільки повний трійковий код можна розглядати як лінійний векторний простір, в якому функції Віленкіна-Крестенсона є ортонормованим базисом, то для перетворення Віленкіна-Крестенсона справедлива рівність Парсеваля [4]

$$\sum_{\omega=1}^{N}\left|\Omega(\omega)\right|^2 = 3^{2k}, \tag{5.37}$$

де k — число змінних, від яких залежить еквівалентна 3-функція, $k = \log_3 N$.

Відомо, що максимум зі значень коефіцієнтів перетворення Віленкіна-Крестенсона приймає найменше значення тоді, коли їх модулі рівні між собою. При цьому мінімальне значення дорівнює

$$\left|\Omega(\omega)\right| = \sqrt{\frac{3^{2k}}{3^k}} = 3^{k/2}, \quad \omega = 0,1,...,N-1. \tag{5.38}$$

В якості міри нелінійності 3-функцій раціональним є використання різниці максимально можливого значення коефіцієнтів перетворення Віленкіна-Крестенсона і поточного максимального значення спектра

$$NL = N - L = 3^k - \max\left\{\left|\Omega(\omega)\right|\right\}. \tag{5.39}$$

У табл. 5.3. представлено розподіл NL-коефіцієнтів для повного коду довжини $N = 9$.

Таблиця 5.3. — Розподіл NL-коефіцієнтів повного коду довжини $N = 9$

NL	0	1.4502	2.7550	3	3.8038	4.4174	6
Число векторів	27	486	1944	1944	4104	10692	486
Примітка	Афінні функції	—	—	—	—	—	Бент-функції

Відзначимо також, що вираз (5.39) є узагальненням відомої формули для обчислення відстані нелінійності булевих функцій

$$N_f = 2^{k-1} - \frac{1}{2}\max\left\{\left|W_f\right|\right\}, \tag{5.40}$$

де $\left|W_f\right|$ — модулі коефіцієнтів перетворення Уолша-Адамара булевої функції f.

Визначення нелінійності ФБЛ є актуальним завданням з огляду на побудову новітніх криптографічних алгоритмів. Тим не менш, використання введеного поняття нелінійності може бути використаним і для оцінки криптографічної якості конструкцій існуючих криптоалгоритмів, що працюють на основі двійкових принципів. Очевидно, S-блоки практично цінної довжини $N = 16$ можуть бути однозначно визначені за допомогою функцій 4-логіки, таким чином, доцільним та актуальним є визначення 4-нелінійності [43]. Проте, для інших довжин S-блоків можуть бути аналогічним чином введені визначення q-нелінійності, якщо їх довжина N може бути представлена у вигляді $N = q^k$, $k \in \mathbb{N}$.

Подібно до булевих функцій та 3-функцій, також можемо ввести визначення афінної 4-функції. Так, афінними є всі 4-функції, які мають вигляд

$$f\left(x_0,\ldots,x_{k-1}\right) = b + a_0x_0 + a_1x_1 + \ldots + a_{k-1}x_{k-1} (\mathrm{mod}\, 4) = \sum_{i=0}^{k-1} a_i x_i (\mathrm{mod}\, 4) + b, \tag{5.41}$$

де $a_i, b \in \{0,1,2,3\}$.

Наприклад, для випадку $k = 2$ можуть бути виписані всі афінні функції у вигляді таблиць істинності

$$\begin{Bmatrix} 0000 & 0123 & 0202 & 0321 \\ 1111 & 1230 & 1313 & 1032 \\ 2222 & 2301 & 2020 & 2103 \\ 3333 & 3012 & 3131 & 3210 \end{Bmatrix}. \tag{5.42}$$

Викреслюючи з даної множини всі такі рядки, які є лінійною комбінацією, з точки зору операції додавання зі значеннями 1, 2 або 3 по модулю 4, в результаті залишаться тільки чотири рядки

$$\begin{array}{ll} \varphi_1 = 0; & \{0000\}; \\ \varphi_5 = x_1; & \{0123\}; \\ \varphi_9 = 2x_1; & \{0202\}; \\ \varphi_{13} = 3x_1; & \{0321\}. \end{array} \tag{5.43}$$

Переходячи до експоненційної системі числення шляхом використання однозначного перетворення

$$\left\{ e^{j\frac{2\pi}{4}\cdot 0} \quad e^{j\frac{2\pi}{4}\cdot 1} \quad e^{j\frac{2\pi}{4}\cdot 2} \; e^{j\frac{2\pi}{4}\cdot 3} \right\} \to \left\{ e^{j0^\circ} \quad e^{j90^\circ} \quad e^{j180^\circ} \; e^{j270^\circ} \right\} \to \\ \to \{z_0 \quad z_1 \quad z_2 \quad z_3\}, \tag{5.44}$$

отримуємо матрицю Віленкіна-Крестенсона

$$V_4 = \begin{bmatrix} z_0 & z_0 & z_0 & z_0 \\ z_0 & z_1 & z_2 & z_3 \\ z_0 & z_2 & z_0 & z_2 \\ z_0 & z_3 & z_2 & z_1 \end{bmatrix} = \begin{bmatrix} e^{j\frac{2\pi}{4}\cdot 0} & e^{j\frac{2\pi}{4}\cdot 0} & e^{j\frac{2\pi}{4}\cdot 0} & e^{j\frac{2\pi}{4}\cdot 0} \\ e^{j\frac{2\pi}{4}\cdot 0} & e^{j\frac{2\pi}{4}\cdot 1} & e^{j\frac{2\pi}{4}\cdot 2} & e^{j\frac{2\pi}{4}\cdot 3} \\ e^{j\frac{2\pi}{4}\cdot 0} & e^{j\frac{2\pi}{4}\cdot 2} & e^{j\frac{2\pi}{4}\cdot 0} & e^{j\frac{2\pi}{4}\cdot 2} \\ e^{j\frac{2\pi}{4}\cdot 0} & e^{j\frac{2\pi}{4}\cdot 3} & e^{j\frac{2\pi}{4}\cdot 2} & e^{j\frac{2\pi}{4}\cdot 1} \end{bmatrix}. \tag{5.45}$$

Відзначимо, що метод побудови матриць Віленкіна-Крестенсона на основі афінних функцій є досить трудомістким, в той час, як метод [4] має на увазі поелементний синтез таких матриць. Аналіз структури матриці (5.45) дозволив вивести формулу рекурентної побудови матриць Віленкіна-Крестенсона будь-якого заданого порядку $N = 4^k$

$$V_{4^{k+1}} = \begin{bmatrix} V_{4^k} & V_{4^k} & V_{4^k} & V_{4^k} \\ V_{4^k} & V_{4^k}+1 & V_{4^k}+2 & V_{4^k}+3 \\ V_{4^k} & V_{4^k}+2 & V_{4^k} & V_{4^k}+2 \\ V_{4^k} & V_{4^k}+3 & V_{4^k}+2 & V_{4^k}+1 \end{bmatrix}, \tag{5.46}$$

де «+» — операція додавання по модулю 4, а матриці представлені в символічній формі, тобто підсумовування виконується щодо індексів z_i.

Наприклад, запишемо матрицю Віленкіна-Крестенсона порядку $N = 16$

$$V_{16}=\begin{bmatrix}
z_0 & z_0 & z_0 & z_0 & z_0 & z_0 & z_0 & z_0 & z_0 & z_0 & z_0 & z_0 & z_0 & z_0 & z_0 & z_0\\
z_0 & z_1 & z_2 & z_3 & z_0 & z_1 & z_2 & z_3 & z_0 & z_1 & z_2 & z_3 & z_0 & z_1 & z_2 & z_3\\
z_0 & z_2 & z_0 & z_2 & z_0 & z_2 & z_0 & z_2 & z_0 & z_2 & z_0 & z_2 & z_0 & z_2 & z_0 & z_2\\
z_0 & z_3 & z_2 & z_1 & z_0 & z_3 & z_2 & z_1 & z_0 & z_3 & z_2 & z_1 & z_0 & z_3 & z_2 & z_1\\
z_0 & z_0 & z_0 & z_0 & z_1 & z_1 & z_1 & z_1 & z_2 & z_2 & z_2 & z_2 & z_3 & z_3 & z_3 & z_3\\
z_0 & z_1 & z_2 & z_3 & z_1 & z_2 & z_3 & z_0 & z_2 & z_3 & z_0 & z_1 & z_3 & z_0 & z_1 & z_2\\
z_0 & z_2 & z_0 & z_2 & z_1 & z_3 & z_1 & z_3 & z_2 & z_0 & z_2 & z_0 & z_3 & z_1 & z_3 & z_1\\
z_0 & z_3 & z_2 & z_1 & z_1 & z_0 & z_3 & z_2 & z_2 & z_1 & z_0 & z_3 & z_3 & z_2 & z_1 & z_0\\
z_0 & z_0 & z_0 & z_0 & z_2 & z_2 & z_2 & z_2 & z_0 & z_0 & z_0 & z_0 & z_2 & z_2 & z_2 & z_2\\
z_0 & z_1 & z_2 & z_3 & z_2 & z_3 & z_0 & z_1 & z_0 & z_1 & z_2 & z_3 & z_2 & z_3 & z_0 & z_1\\
z_0 & z_2 & z_0 & z_2 & z_2 & z_0 & z_2 & z_0 & z_0 & z_2 & z_0 & z_2 & z_2 & z_0 & z_2 & z_0\\
z_0 & z_3 & z_2 & z_1 & z_2 & z_1 & z_0 & z_3 & z_0 & z_3 & z_2 & z_1 & z_2 & z_1 & z_0 & z_3\\
z_0 & z_0 & z_0 & z_0 & z_3 & z_3 & z_3 & z_3 & z_2 & z_2 & z_2 & z_2 & z_1 & z_1 & z_1 & z_1\\
z_0 & z_1 & z_2 & z_3 & z_3 & z_0 & z_1 & z_2 & z_2 & z_3 & z_0 & z_1 & z_1 & z_2 & z_3 & z_0\\
z_0 & z_2 & z_0 & z_2 & z_3 & z_1 & z_3 & z_1 & z_2 & z_0 & z_2 & z_0 & z_1 & z_3 & z_1 & z_3\\
z_0 & z_3 & z_2 & z_1 & z_3 & z_2 & z_1 & z_0 & z_2 & z_1 & z_0 & z_3 & z_1 & z_0 & z_3 & z_2
\end{bmatrix}. \qquad (5.47)$$

Наведемо далі приклад визначення нелінійності 4-функції. Нехай, задана довільна 4-функція довжини $N=16$ у вигляді своєї таблиці істинності

$$A=\{z_0\ \ z_1\ \ z_2\ \ z_3\ \ z_0\ \ z_1\ \ z_2\ \ z_3\ \ z_0\ \ z_1\ \ z_2\ \ z_3\ \ z_0\ \ z_1\ \ z_2\ \ z_3\}, \qquad (5.48)$$

знайдемо її коефіцієнти перетворення Віленкіна-Крестенсона

$$\Omega_A=A\cdot\overline{V}_{16}=\{0\ \ 16\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\}. \qquad (5.49)$$

Кожен коефіцієнт перетворення Віленкіна-Крестенсона (5.49) характеризує степінь вмісту відповідної функції Віленкіна-Крестенсона (рядка матриці V_N) в досліджуваній послідовності.

Оскільки множина функцій Віленкіна-Крестенсона є множиною найбільш лінійних функцій, можна виміряти степінь лінійності досліджуваної функції за допомогою максимального значення спектральних коефіцієнтів. Наприклад, в даному випадку коефіцієнт лінійності складає $L=\max\{|\Omega_A|\}=16.$

Через те, що послідовність (5.48) є другим рядком матриці Віленкіна-Крестенсона (5.47), модуль другого значення серед трансформант Віленкіна-Крестенсона (5.49) прийняв максимально можливе значення, яке дорівнює довжині N.

Оскільки повний четвірковий код може бути розглянутий як лінійний векторний простір, в якому функції Віленкіна-Крестенсона є ортонормованим базисом [4], для перетворення Віленкіна-Крестенсона є справедливою рівність Парсеваля

$$\sum_{\omega=1}^{N}\left|\Omega(\omega)\right|^2 = 4^{2k}, \tag{5.50}$$

де k — число змінних, від яких залежить еквівалентна 4-функція, $k = \log_4 N$.

Мінімальне ж значення коефіцієнтів перетворення Віленкіна-Крестенсона досягається тоді, коли їх значення постійні по модулю і рівні

$$\left|\Omega_{\min}(\omega)\right| = \sqrt{\frac{4^{2k}}{4^k}} = 4^{k/2}, \quad \omega = 0,1,...,N-1. \tag{5.51}$$

Таким чином, нелінійність функцій q-значної логіки оцінюється як різниця між максимально можливим значенням модуля коефіцієнта перетворення Віленкіна-Крестенсона і максимальним значенням (по модулю) перетворення Віленкіна-Крестенсона досліджуваної функції

$$NL = \begin{cases} q^k - \max\left\{\left|\Omega(\omega)\right|\right\}, & q > 2; \\ 2^{k-1} - \dfrac{1}{2}\max\left\{\left|W(\omega)\right|\right\}, & q = 2, \end{cases} \tag{5.52}$$

де $W(\omega)$ — коефіцієнти перетворення Уолша-Адамара, що є окремим випадком перетворення Віленкіна-Крестенсона для булевих функцій.

Вираз (5.52) є визначенням q-нелінійності функцій багатозначної логіки. Використовуючи формулу (5.52), стає можливим виконати оцінку q-нелінійності таких криптографічних конструкцій, як S-блоки.

Відомо, що послідовності, для яких максимум зі значень коефіцієнтів перетворення Віленкіна-Крестенсона приймає найменше значення, називаються бент-послідовностями, які мають численні застосування у криптографії [7…14, 44…45]. Спираючись на отримані результати, введемо уточнене визначення бент-послідовностей для довільного значення q.

Визначення 5.2.1. Для матриці Віленкіна-Крестенсона порядку $N = p^k$, p — просте число, $k \in \mathbb{N}$, бент-послідовністю називається послідовність $H = [h_0, h_1, \cdots, h_i, \cdots, h_{N-1}]$ над алфавітом $h_i \in \left\{ e^{j\frac{2\pi}{m}\nu} \right\}$, $\nu = 0,1,...,m-1$, якщо вона має рівномірно розподілені модулі трансформант Віленкіна-Крестенсона, які представимо в матричній формі

$$\left|\Omega_B(\omega)\right| = \left|H \cdot \overline{V}_N\right| = const\ ,\ \omega = \overline{0, N-1}, \tag{5.53}$$

де V_N — матриця Віленкіна-Крестенсона порядку N над алфавітом $h_i \in \left\{ e^{j\frac{2\pi}{m}\nu} \right\}$, $\nu = 0,1,...,m-1$.

Далі наведемо приклад дослідження нелінійності конкретної криптографічної конструкції. Розглянемо приклад S-блока підстановки довжини $N = 16$

$$S = [6 \quad 8 \quad 2 \quad 3 \quad 9 \quad 10 \quad 5 \quad 12 \quad 1 \quad 14 \quad 4 \quad 7 \quad 11 \quad 13 \quad 0 \quad 15]. \tag{5.54}$$

Представляючи даний S-блок у вигляді компонентних булевих функцій

$$F_2 = \begin{bmatrix} 0100110101001101 \\ 1000001101110101 \\ 1011010001011001 \\ 0001101010011101 \end{bmatrix}, \tag{5.55}$$

неважко знайти, що його 2-нелінійність дорівнює $N_{f_{2i}} = \min\{4,4,4,4\} = 4$.

Проте, цей S-блок можливо уявити у вигляді компонентних 4-функцій

$$F_4 = \begin{bmatrix} 1200221313112303 \\ 2023121012033103 \end{bmatrix}, \tag{5.56}$$

для кожної з яких знайдемо модулі трансформант Віленкіна-Крестенсона

$$\left|\Omega\right| = \begin{bmatrix} 0 & 4.472 & 6.325 & 4.472 & 2.828 & 2 & 0 & 6 \\ 0 & 2.828 & 4 & 6.325 & 2 & 4.472 & 2 & 2 \\ 5.657 & 2 & 2.828 & 6 & 2.828 & 6 & 0 & 2 \\ 2.828 & 0 & 2.828 & 4 & 4.472 & 4.472 & 8.246 & 4.472 \end{bmatrix}. \tag{5.57}$$

Застосовуючи формулу (5.52), а також методику оцінки нелінійності S-блоків, знаходимо, що 4-нелінійність дорівнює

$$N_{f_{4i}} = \min\{NL\} = \min\{9.675\ ,\ 7.754\} = 7.754. \qquad (5.58)$$

Отже запропонований критерій нелінійності функцій багатозначної логіки дозволяє оцінювати криптографічні конструкції, представлені за допомогою ФБЛ на предмет складності їх апроксимації множиною афінних функцій, а також створювати криптографічні алгоритми та їх складові частини, виходячи з необхідності максимізації нелінійності їх уявлень за всіма можливими основами q ФБЛ.

5.3. Обґрунтування методу оцінки нелінійності ФБЛ в часовій області

Скористаємося визначенням ваги 3-функції, яке у роботі [46] застосовується для визначення досконалих трійкових решіток.

Розглянемо довільну послідовність над алфавітом $\{0,1,...,q-1\}$

$$f_i \in \{0,1,...,q-1\}, \quad i = 0,1,...,N-1. \qquad (5.59)$$

Відзначимо, що елементи цієї послідовності можуть бути представлені в експоненційній формі, тобто над алфавітом (5.3).

Для даної послідовності введемо вектор $K = \{K_0, K_1, ..., K_{q-1}\}$, де K_u — це кількість появ символу $u \in \{0,1,...,q-1\}$ в послідовності f.

В якості характеристики послідовності f введемо таке визначення.

Визначення 5.3.1. Розбалансом послідовності f назвемо значення модуля суми поелементних добутків елементів вектора K на відповідні їм елементи експоненційного алфавіту $\{z_0, z_1, ..., z_{q-1}\}$

$$\Delta(f) = \left| K_0 z_0 + K_1 z_1 + ... + K_{q-1} z_{q-1} \right|. \qquad (5.60)$$

Відзначимо окремі випадки формули (5.60).

1. У разі булевих функцій, при $q = 2$ вираз (5.60) набуває вигляду

$$\Delta(f) = \left|K_0 z_0 + K_1 z_1\right| = \left|K_0 - K_1\right|, \tag{5.61}$$

що відповідає класичному визначенню разбаланса булевих функцій, який широко застосовується в теорії сигналів [47].

2. Для послідовності f над алфавітом $\{0,1,2\} \leftrightarrow \{z_0, z_1, z_2\}$ шляхом використання тригонометричної форми і формули модуля комплексного числа вираз (5.60) можна привести до виду

$$\Delta(f) = \left|K_0 z_0 + K_1 z_1 + K_2 z_2\right| = \\ = \sqrt{\left(1 \cdot K_0 - 0.5\left(K_1 + K_2\right)\right)^2 + \left(\frac{\sqrt{3}}{2} K_1 - \frac{\sqrt{3}}{2} K_2\right)^2}, \tag{5.62}$$

що відповідає формулі разбалансу трійкових послідовностей, яка введена в роботі [46].

Безпосередньо з розгляду виразу (5.60) випливає важливе твердження.

Твердження 5.3.1. Розбаланс суми q-функції f і q-функції-константи $A_0 = \left[a_0\ a_0 \ldots a_0\right],\quad a_0 \in \{0,1,\ldots,q-1\}$ дорівнює разбалансу вихідної q-функції f

$$\Delta(f + A_0) = \Delta(f). \tag{5.63}$$

Іншими словами, додавання константи не змінює значення разбаланса вихідної функції.

Доказ **Твердження 5.3.1.** стає очевидним при розгляді того факту, що додавання константи переведе значення елементів таблиці істинності функції в деякі інші відповідні їм значення над алфавітом $\{0,1,\ldots,q-1\}$. Таким чином, кожному z_k в послідовності до додавання константи буде відповідати своє z_i в послідовності після додавання константи і, таким чином, значення суми $K_0 z_0 + K_1 z_1 + \ldots + K_{q-1} z_{q-1}$ не зміниться.

Далі на прикладі 5-функцій розглянемо сутність перетворення Віленкіна-Крестенсона і встановимо його взаємозв'язок з введеним визначенням разбаланса.

Нехай, за допомогою своєї таблиці істинності, а також в експоненційній формі над алфавітом

$\left\{ z_0 = e^{j0}, z_1 = e^{j\frac{2\pi}{5}}, z_2 = e^{j\frac{4\pi}{5}}, z_3 = e^{j\frac{6\pi}{5}}, z_4 = e^{j\frac{8\pi}{5}} \right\}$ задана деяка 5-функція $k=1$ змінної

$$f_5 = [04321] \to \left[e^{j0}\ e^{j\frac{8\pi}{5}}\ e^{j\frac{6\pi}{5}}\ e^{j\frac{4\pi}{5}}\ e^{j\frac{2\pi}{5}} \right]. \tag{5.64}$$

Відповідно до виразу (5.5) побудуємо матрицю Віленкіна-Крестенсона порядку $N=5$ над алфавітом

$$V_5 = \begin{bmatrix} 0\,0\,0\,0\,0 \\ 0\,1\,2\,3\,4 \\ 0\,2\,4\,1\,3 \\ 0\,3\,1\,4\,2 \\ 0\,4\,3\,2\,1 \end{bmatrix} \to \begin{bmatrix} e^{j0} & e^{j0} & e^{j0} & e^{j0} & e^{j0} \\ e^{j0} & e^{j\frac{2\pi}{5}} & e^{j\frac{4\pi}{5}} & e^{j\frac{6\pi}{5}} & e^{j\frac{8\pi}{5}} \\ e^{j0} & e^{j\frac{4\pi}{5}} & e^{j\frac{8\pi}{5}} & e^{j\frac{2\pi}{5}} & e^{j\frac{6\pi}{5}} \\ e^{j0} & e^{j\frac{6\pi}{5}} & e^{j\frac{2\pi}{5}} & e^{j\frac{8\pi}{5}} & e^{j\frac{4\pi}{5}} \\ e^{j0} & e^{j\frac{8\pi}{5}} & e^{j\frac{6\pi}{5}} & e^{j\frac{4\pi}{5}} & e^{j\frac{2\pi}{5}} \end{bmatrix}. \tag{5.65}$$

Відповідно, вектор трансформант Віленкіна-Крестенсона обчислюється як добуток таблиці істинності досліджуваної функції (5.64) і транспонованої матриці Віленкіна-Крестенсона (5.65)

$$\Omega = f_5 V_5^{'} = \left[e^{j0}\ e^{j\frac{8\pi}{5}}\ e^{j\frac{6\pi}{5}}\ e^{j\frac{4\pi}{5}}\ e^{j\frac{2\pi}{5}} \right] \begin{bmatrix} e^{j0} & e^{j0} & e^{j0} & e^{j0} & e^{j0} \\ e^{j0} & e^{j\frac{8\pi}{5}} & e^{j\frac{6\pi}{5}} & e^{j\frac{4\pi}{5}} & e^{j\frac{8\pi}{5}} \\ e^{j0} & e^{j\frac{6\pi}{5}} & e^{j\frac{8\pi}{5}} & e^{j\frac{8\pi}{5}} & e^{j\frac{4\pi}{5}} \\ e^{j0} & e^{j\frac{4\pi}{5}} & e^{j\frac{8\pi}{5}} & e^{j\frac{8\pi}{5}} & e^{j\frac{6\pi}{5}} \\ e^{j0} & e^{j\frac{8\pi}{5}} & e^{j\frac{4\pi}{5}} & e^{j\frac{6\pi}{5}} & e^{j\frac{8\pi}{5}} \end{bmatrix}. \tag{5.66}$$

Врахуємо, що додаванню в групі $\Gamma_q = \{0,1,...,q-1\}$ відповідає множення в групі коренів з одиниці $z_k = e^{j\frac{2\pi}{q}k}$, $k \in \{0,1,...,q-1\}$. При цьому, розглядаючи модулі елементів вектора коефіцієнтів перетворення Віленкіна-Крестенсона бачимо, що кожен даний елемент буде являти собою не що інше, як розбаланс суми досліджуваної функції з відповідною функцією Віленкіна-Крестенсона

$$\Omega = \Delta(f + \nu_j), \quad j = 0,1,...,q^k - 1. \tag{5.67}$$

Таким чином, на основі введеного **Визначення 5.3.1.** разбаланса ФБЛ введемо визначення відстані нелінійності функції багатозначної логіки k змінних для довільного значення q

$$N_f = \begin{cases} q^k - \max\left\{\Delta(f \underset{q}{\oplus} A_j)\right\}, & j = 1,2,...,q^{k+1}, \quad q > 2; \\ 2^{k-1} - \dfrac{1}{2}\max\left\{\Delta(f \underset{q}{\oplus} A_j)\right\}, & j = 1,2,...,2^{k+1}, \quad q = 2, \end{cases} \tag{5.68}$$

де $\{A_j\}$ — множина лінійних функцій, що може бути побудована відповідно до правила

$$\{A_j\} = (X \cdot X^T) \bmod q, \tag{5.69}$$

де X — матриця, що складена з усіх можливих q-ічних векторів довжини k.

Відзначимо також, що множина лінійних функцій (5.69) збігається з множиною афінних функцій (5.41) при значенні коефіцієнта $a_0 = 0$. При цьому афінні функції, що залишилися при $a_0 \neq 0$ виключимо з розгляду в силу **Твердження 5.3.1.**

Таким чином, можемо записати метод обчислення нелінійності ФБЛ для довільного значення q у вигляді конкретних кроків.

Крок 1. Відповідно до формули (5.69) записати повну множину лінійних функцій.

Крок 2. Відповідно до формули (5.60) обчислити значення разбаланса суми повної множини афінних функцій і даної ФБЛ.

Крок 3. Відповідно до формули (5.68) обчислити значення нелінійності досліджуваної функції багатозначної логіки.

Відзначимо також, що запропонований метод розрахунку нелінійності булевих функцій передбачає побудову тільки лінійного коду замість всього афінного коду як при використанні класичного методу [33]. Це дозволяє домогтися економії пам'яті при обчисленні відстані нелінійності в 2 рази, що є особливо критичним при оцінці рівня нелінійності великих булевих функцій.

5.4. Обґрунтування критеріїв, що характеризують диференціальні властивості ФБЛ

З точки зору оцінки криптографічної якості ФБЛ важливим є питання розробки методики вимірювання диференціальних властивостей ФБЛ.

Диференціальні властивості булевих функцій є найважливішим критерієм криптографічної якості, який враховується при конструюванні сучасних криптографічних S-блоків [48…53]. Поширимо цей критерій на випадок ФБЛ, починаючи з прикладу 3-функцій. Кожна 3-функція k змінних може бути розглянута як блок перетворення з k входами і одним виходом. На рис. 5.1. показаний приклад схемного уявлення 3-функції двох змінних. При цьому передбачається, що $x_i, y \in \{0,1,2\}$.

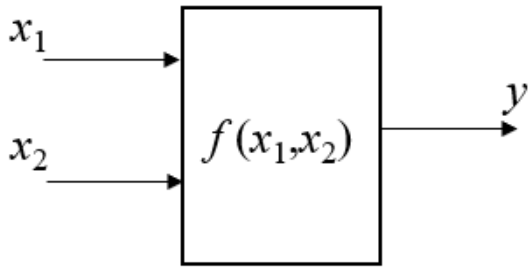


Рис. 5.1. — Схемне уявлення 3-функції двох змінних

Сутність вимірювання диференціальних властивостей ФБЛ полягає в спостереженні за зміною вихідного значення ФБЛ при певному впливі на її вхідні значення [54].

Розглянемо конкретний приклад. Нехай, за допомогою своєї таблиці істинності задана 3-функція двох змінних

$$f = \{0\ 1\ 2\ 0\ 1\ 2\ 2\ 1\ 0\}. \qquad (5.70)$$

Для того, щоб дослідити вплив кожного з входів 3-функції на її вихід, підключимо до її входів суматори (рис. 5.2.), на які подаємо деякі впливи

$d_1, d_2 \in \{0,1,2\}$. Очевидно, що значення $d_1, d_2 = 0$ означають відсутність впливу на входи 3-функції.

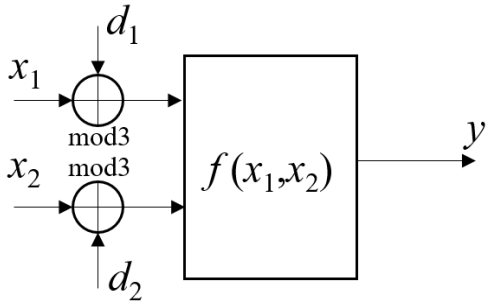


Рис 5.2. — Схема дослідження впливу входів 3-функції на її вихід

Почергово змінюючи значення коефіцієнтів d_1, d_2 отримаємо перегруповані значення вихідної 3-функції (5.70), представлені в табл. 5.4., при цьому під знаком $\oplus$ розуміється додавання по модулю 3.

Таблиця 5.4. — Знаходження значень 3-функції від аргументу з прирощенням

$f(x_1, x_2)$	$f(x_1, x_2 \oplus 1)$	$f(x_1, x_2 \oplus 2)$	$f(x_1 \oplus 1, x_2)$	$f(x_1 \oplus 2, x_2)$
$f(0,0)=0$	$f(0,1)=1$	$f(0,2)=2$	$f(1,0)=0$	$f(2,0)=2$
$f(0,1)=1$	$f(0,2)=2$	$f(0,0)=0$	$f(1,1)=1$	$f(2,1)=1$
$f(0,2)=2$	$f(0,0)=0$	$f(0,1)=1$	$f(1,2)=2$	$f(2,2)=0$
$f(1,0)=0$	$f(1,1)=1$	$f(1,2)=2$	$f(2,0)=2$	$f(0,0)=0$
$f(1,1)=1$	$f(1,2)=2$	$f(1,0)=0$	$f(2,1)=1$	$f(0,1)=1$
$f(1,2)=2$	$f(1,0)=0$	$f(1,1)=1$	$f(2,2)=0$	$f(0,2)=2$
$f(2,0)=2$	$f(2,1)=1$	$f(2,2)=0$	$f(0,0)=0$	$f(1,0)=0$
$f(2,1)=1$	$f(2,2)=0$	$f(2,0)=2$	$f(0,1)=1$	$f(1,1)=1$
$f(2,2)=0$	$f(2,0)=2$	$f(2,1)=1$	$f(0,2)=2$	$f(1,2)=2$

Таким чином, аналізуючи дані табл. 5.4. можна спостерігати динаміку зміни вихідного значення 3-функції при зміні її вхідних значень. При цьому, в двійковому випадку, дана дія є тривіальною, оскільки оперування зі значеннями з множини $\{0,1\}$ дозволяє зробити висновок щодо вихідного

значення — змінилося / не змінилося. У випадку трійкової логіки, очевидно, істотну роль грає ще й характер зміни вихідного значення. Можливі наступні варіанти:

1. Значення функції не змінилося. Позначимо цю подію символом 0.

2. Значення збільшилося (зменшилося) на 1 (по модулю 3). Позначимо ці події символами «+/–».

Позначимо описане перетворення символом δ і введемо такі базові визначення.

Визначення 5.4.1. Нехай величина $\nu(u)$ — кількість ненульових значень вектора u, тоді похідною 3-функції $f(X)$, де $X=\{x_1,x_2,...,x_k\}$ у напрямку u назвемо 3-функцію, що задається наступним виразом

$$D_u f=\delta(f(x),f(x+u)). \tag{5.71}$$

Визначення 5.4.2. Досліджувана 3-функція $f(X)$ відповідає критерію поширення в напрямку вектора u, якщо кількість нульових значень в його похідній $D_u f$ дорівнює кількості позитивних і дорівнює кількості негативних значень $K^0=K^+=K^-=\frac{N}{3}$.

Тобто, вектор ймовірностей зміни вихідних значень досліджуваної функції $f(X)$ при зміщенні її вхідних значень в напрямку вектора u має вигляд

$$P_u=\begin{bmatrix}\frac{K^0}{N} & \frac{K^+}{N} & \frac{K^-}{N}\end{bmatrix}=\begin{bmatrix}0 & + & -\\ 1/3 & 1/3 & 1/3\end{bmatrix}. \tag{5.72}$$

Визначення 5.4.3. Досліджувана 3-функція задовольняє критерію поширення порядку m, якщо вона відповідає критерію поширення у всіх напрямках u таких, що $1\le\nu(u)\le m$.

Визначення 5.4.4. Досліджувана 3-функція задовольняє суворому лавинному критерію, якщо вона задовольняє критерію поширення порядка $m=1$.

З огляду на введені визначення, знайдемо похідні 3-функції (5.70) і перевіримо, чи задовольняє вона суворому лавинному критерію (табл. 5.5.).

Таблиця 5.5. — Похідні 3-функції (5.70) за напрямками ваги $\nu(u)=1$

$f(x_1,x_2)$	$f(x_1,x_2\oplus 1)$	D_{01}	$f(x_1,x_2\oplus 2)$	D_{02}	$f(x_1\oplus 1,x_2)$	D_{10}	$f(x_1\oplus 2,x_2)$	D_{20}
$f(0,0)=0$	$f(0,1)=1$	–	$f(0,2)=2$	+	$f(1,0)=0$	0	$f(2,0)=2$	+
$f(0,1)=1$	$f(0,2)=2$	–	$f(0,0)=0$	+	$f(1,1)=1$	0	$f(2,1)=1$	0
$f(0,2)=2$	$f(0,0)=0$	–	$f(0,1)=1$	+	$f(1,2)=2$	0	$f(2,2)=0$	–
$f(1,0)=0$	$f(1,1)=1$	–	$f(1,2)=2$	+	$f(2,0)=2$	+	$f(0,0)=0$	0
$f(1,1)=1$	$f(1,2)=2$	–	$f(1,0)=0$	+	$f(2,1)=1$	0	$f(0,1)=1$	0
$f(1,2)=2$	$f(1,0)=0$	–	$f(1,1)=1$	+	$f(2,2)=0$	–	$f(0,2)=2$	0
$f(2,0)=2$	$f(2,1)=1$	+	$f(2,2)=0$	–	$f(0,0)=0$	–	$f(1,0)=0$	–
$f(2,1)=1$	$f(2,2)=0$	+	$f(2,0)=2$	–	$f(0,1)=1$	0	$f(1,1)=1$	0
$f(2,2)=0$	$f(2,0)=2$	+	$f(2,1)=1$	–	$f(0,2)=2$	+	$f(1,2)=2$	+

Таким чином, досліджувана функція не задовольняє суворому лавинному критерію.

Відзначимо, що завдання поширення критеріїв криптографічної якості на випадок ФБЛ дозволяє краще зрозуміти і вдосконалити існуючі системи двійкової криптографії. Так, для здійснення атаки на двійковий криптографічний алгоритм криптоаналітиком можуть бути використані будь-які описи криптоалгоритма, зокрема, математичний апарат ФБЛ.

Використовувані на практиці криптоалгоритми часто мають S-блоки довжини N, яка кратна 4, наприклад, $N=16$, як в криптоалгоритмі ДСТУ ГОСТ 28147:2009 [55], або $N=256$, як S-блоки конструкції Ніберг [56] в криптоалгоритмі AES [57]. S-блоки зазначених довжин можуть бути уявлені за допомогою функцій 4-логіки. Дана обставина вимагає дослідження всіх можливих форм представлення S-блоків, зокрема, за допомогою компонентних функцій багатозначної логіки. При цьому особливу практичну цінність має дослідження криптографічної якості S-блоків, уявлених у вигляді компонентних 4-функцій.

Наприклад, розглянемо S-блок, синтезований в [58], який є оптимальним з точки зору суворого лавинного критерію в двійковому сенсі. Його розкладання на компонентні булеві функції має такий вигляд

$$S=\left\{\begin{array}{cccccccccccccccc}4&7&2&14&1&13&8&11&15&12&6&10&5&9&3&0\\ \hline 0&1&0&0&1&1&0&1&1&0&0&0&1&1&1&0\\ 0&1&1&1&0&0&0&1&1&0&1&1&0&0&1&0\\ 1&1&0&1&0&1&0&0&1&1&1&0&1&0&0&0\\ 0&0&0&1&0&1&1&1&1&1&0&1&0&1&0&0\end{array}\right\}. \qquad (5.73)$$

Даний S-блок (5.73) може бути уявлений за допомогою двох компонентних 4-функцій

$$S=\left\{\begin{array}{cccccccccccccccc}4&7&2&14&1&13&8&11&15&12&6&10&5&9&3&0\\ \hline 0&3&2&2&1&1&0&3&3&0&2&2&1&1&3&0\\ 1&1&0&3&0&3&2&2&3&3&1&2&1&2&0&0\end{array}\right\}, \qquad (5.74)$$

криптографічні властивості яких також визначають властивості самого S-блоку, але вже на рівні четвіркової логіки.

Далі наведено загальну схему дослідження критерія поширення, для якої булева функція, 3-функція і 4-функція будуть окремими випадками.

Розглянемо q-функцію k змінних $f(x)$. Нехай $u=(u_1,u_2,...,u_k)$.

Визначення 5.4.5. Вагою $\varpi(u)$ q-значного вектора назвемо кількість його ненульових компонент.

Використовуючи **Визначення 5.4.5.**, запишемо більш загальну форму **Визначення 5.4.3.** і **Визначення 5.4.4.**

Визначення 5.4.6. Похідною функції f у напрямку вектора u назвемо функцію

$$D_u f(x)=f(x\underset{q}{\oplus}u)-f(x)\,(\mathrm{mod}\,q)\ , \qquad (5.75)$$

де $\underset{q}{\oplus}$ означає додавання по модулю q.

Визначення 5.4.7. Функція q-значної логіки $f(x)$ відповідає критерію поширення щодо вектора $u\in V_n$ — КР(u), якщо її похідна у напрямку u є збалансованою функцією, тобто значення $0,1,...,q-1$ приймаються з рівними

ймовірностями $p(D_u f(x) = i(\mathrm{mod}\, q)) = \frac{1}{q}$ для всіх $i = 0,1,...,q-1$. Таким чином, виконується рівність $K^0 = K^1 = ... = K^{q-1}$, де K^i — кількість наборів значень змінних, на яких похідна приймає значення i.

При цьому **Визначення 5.4.3.** і **Визначення 5.4.4.** узгоджені з **Визначенням 5.4.7.** Відповідно до введених визначень розглянемо приклад дослідження першої 4-функції S-блоку (5.74) на відповідність суворому лавинному критерію (табл. 5.6.).

Таблиця 5.6. — Приклад знаходження похідної 4-функції

$f(X)$	u=01	$D_{01}f$	u=02	$D_{02}f$	u=03	$D_{03}f$	u=10	$D_{10}f$	u=20	$D_{20}f$	u=30	$D_{30}f$
$f(00)=0$	3	3	2	2	2	2	1	1	3	3	1	1
$f(01)=3$	2	3	2	3	0	1	1	2	0	1	1	2
$f(02)=2$	2	0	0	2	3	1	0	2	2	0	3	1
$f(03)=2$	0	2	3	1	2	0	3	1	2	0	0	2
$f(10)=1$	1	0	0	3	3	2	3	2	1	0	0	3
$f(11)=1$	0	3	3	2	1	0	0	3	1	0	3	2
$f(12)=0$	3	3	1	1	1	1	2	2	3	3	2	2
$f(13)=3$	1	2	1	2	0	1	2	3	0	1	2	3
$f(20)=3$	0	1	2	3	2	3	1	2	0	1	1	2
$f(21)=0$	2	2	2	2	3	3	1	1	3	3	1	1
$f(22)=2$	2	0	3	1	0	2	3	1	2	0	0	2
$f(23)=2$	3	1	0	2	2	0	0	2	2	0	3	1
$f(30)=1$	1	0	3	2	0	3	0	3	1	0	3	2
$f(31)=1$	3	2	0	3	1	0	3	2	1	0	0	3
$f(32)=3$	0	1	1	2	1	2	2	3	0	1	2	3
$f(33)=0$	1	1	1	1	3	3	2	2	3	3	2	2

На підставі аналізу даних, що наведені в табл. 5.6. можна говорити про те, що перша компонентна 4-функція S-блока (5.74) не відповідає суворому лавинному критерію. Тобто бувши оптимальним з точки зору суворого лавинного критерію у двійковому сенсі, S-блок (5.74) не є оптимальним з точки зору суворого лавинного критерію у четвірковому сенсі.

5.5. Кореляційний імунітет ФБЛ

Відзначимо, що поняття оптимальності матриці коефіцієнтів кореляції S-блока пов'язане із поняттям кореляційного імунітету його компонентних функцій [59…68]. Введемо визначення кореляційного імунітету 3-функцій, яке базується на визначенні підфункції.

Визначення 5.5.1. Підфункцією q-функції $f(x)$, називається функція f', отримана підстановкою в f значень з множини $\{0,1,...q-1\}$ замість деяких змінних. Якщо підставимо в функцію f константи $\sigma_{i_1},\cdots,\sigma_{i_s}$ замість змінних $x_{i_1},\cdots,x_{i_s}$ відповідно, то отримана підфункція позначається $f^{\sigma_{i_1},\cdots,\sigma_{i_s}}_{x_{i_1},\cdots,x_{i_s}}$.

Також для визначення незалежності виходу 3-функції від її входу і для визначення кореляційного імунітету зручно скористатися поняттям разбаланса (5.60).

На основі поняття розбалансу введемо наступні визначення.

Визначення 5.5.2. Кажуть, що вихід 3-функції $f(x)$ є незалежним від групи своїх вхідних змінних $\{x_i\}$, $i=1,...,m$, якщо при підстановці замість цих змінних будь-яких констант $\sigma_{i_1},\cdots,\sigma_{i_s}\in\{0,1,...q-1\}$, розбаланс отриманих таким чином підфункцій становить $\Delta_{f'}=\dfrac{\Delta_f}{3^m}$.

Визначення 5.5.3. Кажуть, що 3-функція є кореляційно імунною порядка $m\le k$, якщо її вихід є незалежним від будь-якої групи з m її вхідних змінних, тобто розбаланс всіх її підфункцій $k-m$ змінних має становити $\Delta_{f'}=\dfrac{\Delta_f}{3^m}$.

Розглянемо приклад. Нехай задана 3-функція

$$f=\left\{\begin{array}{c|ccccccccc} x_1x_2 & 00 & 01 & 02 & 10 & 11 & 12 & 20 & 21 & 22 \\ \hline f(x_1x_2) & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 0 & 0 \end{array}\right\}. \qquad (5.76)$$

Відповідно до (5.60) розбаланс 3-функції (5.76) складає $\Delta_f = 0$, тобто вона є збалансованою. Таким чином, відповідно до **Визначення 5.5.2.**, для незалежності даної функції від будь-якої зі своїх вхідних змінних (x_1 або x_2), необхідно, щоб її підфункції, отримані шляхом підстановки в дані змінні будь-яких констант, були збалансованими.

Знайдемо всі підфункції $m = 1$ змінної 3-функції f

$$\begin{aligned} &f(0, x_2) = \{011\}; \quad f(x_1, 0) = \{012\}; \\ &f(1, x_2) = \{122\}; \quad f(x_1, 1) = \{120\}; \\ &f(2, x_2) = \{200\}; \quad f(x_1, 2) = \{120\}. \end{aligned} \tag{5.77}$$

Таким чином, вихід досліджуваної 3-функції є незалежним від змінної x_2, оскільки підстановка замість даної змінної будь-якої константи не змінює її розбаланс.

З метою ілюстрації роботи методу знаходження кореляційного імунітету розглянемо наступний приклад. Нехай задано 3-функцію довжини $N = 27$

$$f = \left\{ \begin{array}{c|ccccccccc} x_1x_2x_3 & 000 & 001 & 002 & 010 & 011 & 012 & 020 & 021 & 022 \\ \hline f(x_1x_2x_3) & 0 & 2 & 1 & 1 & 0 & 2 & 2 & 1 & 0 \end{array} \right.$$
$$\begin{array}{c|ccccccccc} x_1x_2x_3 & 100 & 101 & 102 & 110 & 111 & 112 & 120 & 121 & 122 \\ \hline f(x_1x_2x_3) & 1 & 0 & 2 & 2 & 1 & 0 & 0 & 2 & 1 \end{array} \tag{5.78}$$
$$\left. \begin{array}{c|ccccccccc} x_1x_2x_3 & 200 & 201 & 202 & 210 & 211 & 212 & 220 & 221 & 222 \\ \hline f(x_1x_2x_3) & 2 & 1 & 0 & 0 & 2 & 1 & 1 & 0 & 2 \end{array} \right\},$$

яку необхідно дослідити на відповідність критерію кореляційного імунітету порядку $m = 2$.

Використовуючи вираз (5.60), знаходимо: розбаланс 3-функції (5.78) дорівнює $\Delta_f = 0$, тобто дана функція є збалансованою. Відповідно до **Визначення 5.5.3.** для перевірки відповідності 3-функції (5.78) критерію кореляційного імунітету порядка $m = 2$ необхідно знайти всі її підфункції $k - m = 3 - 2 = 1$ змінної, яких існує 27, і переконатися, що вони також є збалансованими

$$
\begin{array}{l|l}
f(0,0,x_3)=\left\{\begin{matrix}000 & 001 & 002\\ 0 & 2 & 1\end{matrix}\right\} & f(0,x_2,0)=\left\{\begin{matrix}000 & 010 & 020\\ 0 & 1 & 2\end{matrix}\right\}\\
f(0,1,x_3)=\left\{\begin{matrix}010 & 011 & 012\\ 1 & 0 & 2\end{matrix}\right\} & f(0,x_2,1)=\left\{\begin{matrix}001 & 011 & 021\\ 2 & 0 & 1\end{matrix}\right\}\\
f(0,2,x_3)=\left\{\begin{matrix}020 & 021 & 022\\ 2 & 1 & 0\end{matrix}\right\} & f(0,x_2,2)=\left\{\begin{matrix}002 & 012 & 022\\ 1 & 2 & 0\end{matrix}\right\}\\
f(1,0,x_3)=\left\{\begin{matrix}100 & 101 & 102\\ 1 & 0 & 2\end{matrix}\right\} & f(1,x_2,0)=\left\{\begin{matrix}100 & 110 & 120\\ 1 & 2 & 0\end{matrix}\right\}\\
f(1,1,x_3)=\left\{\begin{matrix}110 & 111 & 112\\ 2 & 1 & 0\end{matrix}\right\} & f(1,x_2,1)=\left\{\begin{matrix}101 & 111 & 121\\ 0 & 1 & 2\end{matrix}\right\}\\
f(1,2,x_3)=\left\{\begin{matrix}120 & 121 & 122\\ 0 & 2 & 1\end{matrix}\right\} & f(1,x_2,2)=\left\{\begin{matrix}102 & 112 & 122\\ 2 & 0 & 1\end{matrix}\right\}\\
f(2,0,x_3)=\left\{\begin{matrix}200 & 201 & 202\\ 2 & 1 & 0\end{matrix}\right\} & f(2,x_2,0)=\left\{\begin{matrix}200 & 210 & 220\\ 2 & 0 & 1\end{matrix}\right\}\\
f(2,1,x_3)=\left\{\begin{matrix}210 & 211 & 212\\ 0 & 2 & 1\end{matrix}\right\} & f(2,x_2,1)=\left\{\begin{matrix}201 & 211 & 221\\ 1 & 2 & 0\end{matrix}\right\}\\
f(2,2,x_3)=\left\{\begin{matrix}220 & 221 & 222\\ 1 & 0 & 2\end{matrix}\right\} & f(2,x_2,2)=\left\{\begin{matrix}202 & 212 & 222\\ 0 & 1 & 2\end{matrix}\right\}
\end{array}
$$

(5.79)

$$
\begin{array}{l}
f(x_1,0,0)=\left\{\begin{matrix}000 & 100 & 200\\ 0 & 1 & 2\end{matrix}\right\}\\
f(x_1,0,1)=\left\{\begin{matrix}001 & 101 & 201\\ 2 & 0 & 1\end{matrix}\right\}\\
f(x_1,0,2)=\left\{\begin{matrix}002 & 102 & 202\\ 1 & 2 & 0\end{matrix}\right\}.\\
f(x_1,1,0)=\left\{\begin{matrix}010 & 110 & 210\\ 1 & 2 & 0\end{matrix}\right\}\\
f(x_1,1,1)=\left\{\begin{matrix}011 & 111 & 211\\ 0 & 1 & 2\end{matrix}\right\}\\
f(x_1,1,2)=\left\{\begin{matrix}012 & 112 & 212\\ 2 & 0 & 1\end{matrix}\right\}\\
f(x_1,2,0)=\left\{\begin{matrix}020 & 120 & 220\\ 2 & 0 & 1\end{matrix}\right\}\\
f(x_1,2,1)=\left\{\begin{matrix}021 & 121 & 221\\ 1 & 2 & 0\end{matrix}\right\}\\
f(x_1,2,2)=\left\{\begin{matrix}022 & 122 & 222\\ 0 & 1 & 2\end{matrix}\right\}
\end{array}
$$

Аналіз множини (5.79) призводить до висновку, що всі підфункції однієї змінної 3-функції (5.78) мають розбаланс $\Delta_{f'}=0$, а оскільки і $\Delta_f=0$, то дана 3-функція є кореляційно-імунною порядка $m=2$.

Доцільним є проведення досліджень кореляційних властивостей повної множини 3-функцій $k=2$ змінних, для чого необхідно буде розглядати їх підфункції $m=1$ змінної, довжина таблиць істинності яких дорівнює $n=3$.

Розглянемо повну множину 3-функцій довжини $n=3$ і потужності $J=3^n=3^3=27$ і визначимо можливі значення розбалансу 3-функцій в даній множині

$$\begin{array}{c|c} \Delta & J_\Delta \\ \hline 0 & 6 \\ \sqrt{3} & 18 \\ 3 & 3 \end{array}. \qquad (5.80)$$

Відповідно до **Визначення 5.5.2.**, для того щоб вихід 3-функції був незалежним від деякої її вхідної змінної, необхідно щоб розбаланс її підфункцій, отриманих підстановкою констант в цю змінну, становив $\Delta_{f'}=\frac{\Delta_f}{3^m}$. Оскільки в даному випадку розглядаються 3-функції двох змінних і, таким чином, досліджуємо підфункції f' однієї змінної, то для того, щоб вихід 3-функції був незалежний хоча-б від одного її входу, необхідно, щоб її розбаланс становив $\Delta_f=3^1\Delta_{f'}\in\{0,3,9\}$.

Результати досліджень повної множини 3-функцій довжини $n=3$ і потужності $J=3^n=3^3=27$, для кожної з яких визначено значення розбалансу 3-функцій в даній множині представлені в табл. 5.7.

Таблиця 5.7. — Результати досліджень рівня незалежності виходу 3-функцій довжини $N=9$ від їх входу

Рівень незалежності виходу 3-функції від її входу	3-функції, незалежні від змінної x_1	3-функції, незалежні від змінної x_2	3-функції з кореляційним імунітетом порядку $m=1$
$\Delta=0,\ J=1680$			
Кількість 3-функцій	216	216	12
$\Delta=3,\ J=4158$			
Кількість 3-функцій	972	972	216
$\Delta=9,\ J=3$			
Кількість 3-функцій	3	3	3

Критерій незалежності виходу ФБЛ від її вхідних значень та кореляційного імунітету ФБЛ може бути легко розповсюджений на випадок 4-функцій.

На основі визначення (5.60) розбалансу ФБЛ введемо визначення незалежності виходу 4-функції від її вхідних змінних, а також визначення кореляційного імунітету 4-функції.

Визначення 5.5.4. Підфункцією q-функції $f(x)$ називається функція f', отримана підстановкою значень із множини $\{0,1,...q-1\}$ замість деяких змінних. Якщо замість змінних $x_{i_1},\cdots,x_{i_s}$ у функцію f підставити константи $\sigma_{i_1},\cdots,\sigma_{i_s}$ відповідно, то отриману підфункцію позначимо як $f^{\sigma_{i_1},\cdots,\sigma_{i_s}}_{x_{i_1},\cdots,x_{i_s}}$.

Визначення 5.5.5. Кажуть, що вихід 4-функції $f(x)$ не залежить від групи її вхідних змінних $\{x_i\}$, $i=1,...,m$, якщо при підстановці будь-яких констант $\sigma_{i_1},\cdots,\sigma_{i_s}\in\{0,1,...q-1\}$ замість цих змінних розбаланс отриманих таким чином підфункцій дорівнює $\Delta_{f'}=\dfrac{\Delta_f}{4^m}$.

Визначення 5.5.6. 4-функцію $f(x)$ називають кореляційно імунною порядку $m\le k$, якщо її вихід незалежний від будь-якої групи її вхідних змінних, тобто розбаланс усіх її підфункцій $k-m$ змінних дорівнює $\Delta_{f'}=\dfrac{\Delta_f}{4^m}$.

Таким чином, використовуючи умови **Визначення 5.5.6.**, ми можемо перевірити компонентні функції будь-якого S-блока, наприклад,

S	4	2	12	1	10	9	7	15	11	13	3	14	5	6	8	0
f_{41}	0	2	0	1	2	1	3	3	3	1	3	2	1	2	0	0
f_{42}	1	0	3	0	2	2	1	3	2	3	0	3	1	1	2	0

(5.81)

на відповідність критерію кореляційного імунітету першого порядку. Наприклад, знайдемо підфункції $2-1=1$ змінної 4-функції f_1

$$
\begin{array}{l}
f_{41}'(x_1,0)=[0\quad 2\quad 3\quad 1]\\
f_{41}'(x_1,1)=[2\quad 1\quad 1\quad 2]\\
f_{41}'(x_1,2)=[0\quad 3\quad 3\quad 0]\\
f_{41}'(x_1,3)=[1\quad 3\quad 2\quad 0]\\
f_{41}'(0,x_2)=[0\quad 2\quad 0\quad 1]\\
f_{41}'(1,x_2)=[2\quad 1\quad 3\quad 3]\\
f_{41}'(2,x_2)=[3\quad 1\quad 3\quad 2]\\
f_{41}'(3,x_2)=[1\quad 2\quad 0\quad 0]
\end{array}. \qquad (5.82)
$$

Використовуючи **Визначення 5.5.6.**, легко визначити, що існують підфункції першої компонентної 4-функції S-блока (5.81), розбаланс яких не дорівнює 0, наприклад, розбаланс підфункції $f_{41}'(x_1,1)=[2\quad 1\quad 1\quad 2]$ дорівнює $\Delta(f_{41}'(x_1,1))=\sqrt{8}$. Легко помітити, що те саме вірно і для компонентної функції f_{42}. Таким чином, S-блок (5.81) не задовольняє критерію кореляційного імунітету компонентних 4-функцій (хоча, як нескладно встановити, задовольняє критерію кореляційного імунітету компонентних булевих функцій). Ця обставина може бути використана криптоаналітиком для виконання атак кореляційного аналізу на зазначену криптографічну конструкцію з використанням 4-функцій.

Підсумовуючи отримані результати за розробленими критеріями криптографічної якості ФБЛ, відзначимо, що вони можуть використовуватися як для синтезу нових криптографічних примітивів та шифрів на їх основі, так і для аналізу якості існуючих криптографічних алгоритмів, який проведено у роботах [22…25, 69…70].

5.6. Висновки

У п’ятому розділі запропоновано методи оцінки криптографічної якості ФБЛ, які на відміну від існуючих методів оцінки криптографічної якості булевих функцій, дозволяють визначати та порівнювати криптографічну

якість шифрів та їх складових частин при уявленні за допомогою будь-яких можливих основ уявлення q. В результаті цього отримано такі наукові і практичні результати:

1. запропоновано методи синтезу алгебраїчної нормальної форми ФБЛ, які, на відміну від існуючих методів, допускають знаходження коефіцієнтів АНФ для q-функцій при значеннях $q > 2$, що дозволило проводити дослідження алгебраїчних показників нелінійності ФБЛ. При цьому, визначено зворотне перетворення, яке дозволяє отримати таблицю істинності q-функцій при наявності вектору коефіцієнтів АНФ. Обчислювальна складність запропонованих методів практично еквівалентна складності операції множення матриці на вектор;

2. на основі коефіцієнтів перетворення Віленкіна-Крестенсона введено поняття NL-коефіцієнту, який, на відміну від існуючих визначень відстані нелінійності булевих функцій, відображає степінь нелінійності q-функцій для довільного значення q (степінь вмісту у компонентних q-функціях шифру афінних функцій), що дозволило проводити дослідження нелінійних властивостей ФБЛ. Розроблено метод оцінки нелінійності ФБЛ в часовій області, який є узагальненням відомого раніше методу оцінки відстані нелінійності булевих функцій на основі обчислення їх кодової відстані Гемінга з афінним кодом. Введено визначення разбаланса послідовностей над алфавітом $\{0,1,...,q-1\}$, яке є узагальненням визначення разбаланса двійкових послідовностей. При цьому доведено, що розбаланс суми послідовності над алфавітом $\{0,1,...,q-1\}$ і послідовності-константи дорівнює разбалансу вихідної послідовності;

3. на основі математичного апарату похідних ФБЛ введено критерій розповсюдження і суворий лавинний критерій, які, на відміну від існуючих аналогів, можуть бути застосовані для ФБЛ. Відповідність q-функції суворому лавинному критерію дозволяє говорити про її стійкість до атак

диференціального криптоаналізу, що є визначальним для її застосування в практичних криптоалгоритмах;

4. на основі математичного апарату підфункцій ФБЛ розроблено критерій відсутності статистичного взаємозв'язку між векторами виходу і входу S-блока підстановки, а також критерій кореляційного імунітету, що, на відміну від існуючих, можуть бути застосовані для ФБЛ. Введено визначення кореляційної незалежності виходу і входу ФБЛ, а також визначення кореляційного імунітету.

Проведені у даному розділі дослідження створюють передумови для розробки криптографічних примітивів та шифрів, що підвищують ефективність крипто-стеганографічних систем.

Список використаних джерел у 5 розділі

1. Sokolov A. V., Zhdanov O. N. Prospects for the Application of Many-Valued Logic Functions in Cryptography. *Advances in Computer Science for Engineering and Education* : Proceedings, January 2018. Kyiv, Ukraine, 2018. P. 331-339. DOI: 10.1007/978-3-319-91008-6_33

2. Stankovic R. S., Astola J.T., Moraga C. Representation of Multiple-Valued Logic Functions. Morgan and Claypool Publishers, Synthesis lectures on digital circuits and systems, 2012. 154 p.

3. Hui-bin T. C. L. U. A New Quaternary Chaotic Sequence Encryption Algorithm. *Microcomputer Information*. 2009. Vol. 2009. No. 36. P. 37.

4. Трахтман А.М., Трахтман В.А. Основы теории дискретных сигналов на конечных интервалах. М.: Сов.радио, 1975. 208 с.

5. Gajić D. B., Stanković R. S. Computation of the Vilenkin-Chrestenson Transform on a GPU. *Journal of Multiple-Valued Logic & Soft Computing*. 2015. Vo. 24, No.1-4. P. 317-340.

6. Логачев О.А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. М: Издательство МЦНМО, 2004. 472 с.

7. Rothaus O.S. On “bent” functions. *J. Comb. Theory Ser*. A. USA: Academic Press Inc, 1976. №20(3). P.300-305.

8. Токарева Н.Н. Бент-функции: результаты и приложения. Обзор работ. *Приклад. дискрет. математика*. Томск, 2009. Сер. №1(3). С. 15-37.

9. Мазурков М.И., Соколов А.В. Регулярные привила построения полного класса бент-последовательностей длины 16. *Труды ОНПУ*. 2013. №2(41). С.231-237.

10. Куценко А.В., Токарева Н.Н. Метрические свойства множества бент-функций в контексте дуальности. *Прикладная дискретная математика*. 2020. №. 49. С. 18-34.

11. Stănică P. et al. Bent and generalized bent Boolean functions. *Designs, codes and cryptography*. 2013. Vol 69, No. 1. P. 77-94.

12. Solé P., Tokareva N.N. On quaternary and binary bent functions. *Applied Discrete Mathematics*. 2009. No 1. P. 16-18.

13. Hou X., Langevin P. Results on bent functions. *Journal of combinatorial theory*, Series A, 1997. Vol. 80, No. 2. P. 232-246.

14. Zheng L. et al. Several new infinite families of bent functions via second order derivatives. *Cryptography and communications-discrete-structures Boolean functions and sequences*. 2020, P. 1143-1160.

15. Козловский А.В., Насыров А.М. Специфика применения структурных особенностей кодовых комбинаций полярных кодов и кодов Рида-Маллера. *Современные проблемы проектирования, производства и эксплуатации радиотехнических систем*. 2017. №. 1-2. С. 159-161.

16. Агафонова, И.В. Криптографические свойства нелинейных булевых функций. *Семинар по дискрет. гармон. анализу и геометр. моделированию*. СПб.: DHA & CAGD, 2007. С. 1-24.

17. Соколов А.В., Жданов О.Н., Барабанов Н.А. Генератор псевдослучайных ключевых последовательностей на основе тройственных

наборов бент-функций. *Проблемы физики, математики и техники*. 2016. №1(26). С. 85-91.

18. Соколов А.В. Быстродействующий генератор ключевых последовательностей на основе клеточных автоматов. *Труды ОНПУ*. 2014. №1(43). С. 180-186.

19. Соколов А.В., Жданов О.Н., Айвазян А.О. Методы синтеза алгебраической нормальной формы функций многозначной логики. *Системный анализ и прикладная информатика*. 2016. №1. С. 69-76.

20. Кормен Т., Лейзерсон Ч., Ривест Р., Штайн К. Алгоритмы: построение и анализ. М.: Вильямс, 2006. 1328 с.

21. Соколов А.В., Оверчук Ю.С. О возможности синтеза алгебраической нормальной формы четверичных функций над полем GF (4). Перша міжнародна науково-практична конференція *Проблеми кібербезпеки інформаційно-телекомунікаційних систем*, 2018. С. 384-388.

22. Kazakova N.F., Karpinski M., Sokolov A.V., Gancarczyk T. Nonlinearity of Many-Valued Logic Component Functions of Modern Cryptographic Algorithms S-boxes. Procedia Computer Science. Vol. 192. P. 2731-2741.

23. Sokolov A., Kazakova N., Kuzmenko L., Mahomedova M. Prerequisites for developing a methodology for estimating and increasing cryptographic strength based on many-valued logic functions. CEUR Workshop Proceedings, 2021. 2923. pp. 107–116.

24. Kazakova Nadiia, Sokolov Artem, Troyanskiy Alexander. Correlation Immunity of Many-Valued Logic Component Functions of Modern Cryptographic Algorithm S-Boxes. International Scientific and Practical Conference «Intellectual Systems and Information Technologies»: Conference Proceedings / Odessa State Environmental University. Odessa, 2021. P. 268-275.

25. Sokolov, A. Research methods for avalanche properties of many-valued logic component functions [Text] / A. Sokolov, N. Kazakova, O. Fraze-Frazenko // XI International Conference of Students, PhD Students and Young Scientists

“Engineer of XXI Century”, 10 december 2021, Bielsko-Biała, Akademia Techniczno-Humanistyczna w Bielsku-Białej, 2021 : materiały konf. — P. 209-218.

26. Sokolov A.V., Radush V.V. A method for synthesis of S-boxes with good avalanche characteristics of component Boolean and quaternary functions. Journal of Discrete Mathematical Sciences and Cryptography, P. 1-12.

27. Sokolov A.V. Zhdanov O.N. Synthesis of highly nonlinear S-boxes satisfying higher order propagation criterion. Journal of Discrete Mathematical Sciences and Cryptography. 2020. P. 1-15.

28. Красота Н.И., Соколов А.В. Методика оценки нелинейности S-блоков на основе четверичного преобразования Виленкина–Крестенсона. Труди 18-ой международной научно-практической конференции «Современные информационные и электронные технологии», 22-26 мая 2017 г. Одесса, 2017. С.150-151.

29. Mihailescu M.I., Nita S.L. Linear and Differential Cryptanalysis. *Pro Cryptography and Cryptanalysis*. Apress, Berkeley, CA. P. 457-481.

30. Liu Z. et al. New insights on linear cryptanalysis. *Science China Information Sciences*. 2020. Vol. 63, No. 1. P. 112104.

31. Тарасевич Д.А. Особенности дифференциального и линейного криптоанализа. *70-я научно-техническая конференция учащихся, студентов и магистрантов*, 15-20 апреля 2019 г., Минск: сборник научных работ: в 4 ч. Ч. 4. Минск: БГТУ, 2019. С. 198-201.

32. Мазурков М.І. Основи теорії передавання інформації. Одеса : Наука і Техніка, 2005. 168 с.

33. Maier W. Staffelbach O. Nonlinearity criteria for cryptographic functionsю In Advances in Cryptology — *EUROCRYPT’89*, Lecture Notes in Computer Science, Springer-Verlag, 1990. Vol.434. P.549-562.

34. Жданов О.Н. Методика выбора ключевой информации для алгоритма блочного шифрования. М.: ИНФРА-М, 2013. 90 с.

35. Соколов, А.В. Новые методы синтеза нелинейных преобразований современных шифров. Lap Lambert Academic Publishing, Germany, 2015. 100 с.

36. Гайнулин Н. А. Алгоритм вычисления нелинейности векторной булевой функции. *Информационные технологии и проблемы математического моделирования сложных систем*. 2015. №14. С. 27-32.

37. Sokolov A.V. Regular synthesis method of a complete class of ternary bent-sequences and their nonlinear properties. *Journal of Telecommunication, Electronic and Computer Engineering*. 2016. Vol. 8, No. 9. P. 39-43.

38. Zhdanov O.N., Sokolov A.V. Extending Nyberg construction on Galois fields of odd characteristic. *Radioelectronics and Communications Systems*. 2017. Vol. 60, No. 12. P. 538-544.

39. Мазурков М.И. Системы широкополосной радиосвязи. Одесса : Наука и Техника, 2010. 340 с.

40. Фарков Ю.А. фреймы Парсеваля и дискретное преобразование Виленкина Крестенсона. *Современные методы теории функций и смежные проблемы*. 2019. С. 270-270.

41. Гуренко В. В., Кудряшов Н. И., Лепкивкер А. М. Преобразование спектров дискретных сигналов в базис функций Виленкина-Крестенсона. *Технологии инженерных и информационных систем*. 2017. №2. С. 125-131.

42. Лабунец В.Г., Мартюгин С.А. Быстрые многопараметрические преобразования Уолша, Крестенсона-Виленкина и Хаара. *Вестник Южно-Уральского государственного университета*. Серия: Компьютерные технологии, управление, радиоэлектроника. 2016. Т. 16, №4. С. 136-142.

43. Соколов А.В., Красота Н.И. Сильно нелинейные подстановки: метод синтеза S-блоков, обладающих максимальной 4-нелинейностью. *Наукові праці ОНАЗ ім. О.С. Попова*. 2017. № 1. С. 145-154.

44. Mesnager S. Bent functions. Springer International Publishing, 2016. 561 p.

45. Carlet C., Mesnager S. Four decades of research on bent functions. *Designs, Codes and Cryptography*. 2016. Vol. 78, № 1. P. 5-50.

46. Соколов А.В., Жданов О.Н. Класс совершенных троичных решеток. *Системный анализ и прикладная информатика*. 2018. №2. С. 47-54.

47. Свердлик М.Б. Оптимальные дискретные сигналы. М.: Советское радио, 1975, 200 с.

48. Cusick T.W., Stanica P. Cryptographic Boolean functions and applications. Academic Press, 2017. 288 p.

49. Stanica P. Nonlinearity, local and global avalanche characteristics of balanced Boolean functions. *Discrete Mathematics*. 2002. Vol. 248, No. 1–3. P. 181-193.

50. Zhang X.M., Zheng Y. GAC—the criterion for global avalanche characteristics of cryptographic functions. *The Journal of Universal Computer Science*. Berlin, Heidelberg : Springer. 1996. P. 320-337.

51. Preneel B. et al. Propagation characteristics of Boolean functions. *Workshop on the Theory and Application of Cryptographic Techniques*. Berlin, Heidelberg : Springer, 1990. P. 161-173.

52. Cusick T.W. Boolean functions satisfying a higher order strict avalanche criterion. *Workshop on the Theory and Application of Cryptographic Techniques*. Berlin, Heidelberg : Springer, 1993. P. 102-117.

53. Stănică P., Sung S.H. Boolean functions with five controllable cryptographic properties. *Designs, Codes and Cryptography*. 2004. Vol. 31, No.2. P. 147-157.

54. Sokolov A.V., Zhdanov O.N. Strict avalanche criterion of four-valued functions as the quality characteristic of cryptographic algorithms strength. *Siberian Journal of Science and Technology*. 2019. Vol. 20, No. 2. P.183-190.

55. ГОСТ Р 34.12-2015. Криптографическая защита информации. Блочные шифры. М. Стандартинформ, 2015. 21 с.

56. Nyberg K. Differentially uniform mappings for cryptography. I Advances in cryptology. Proc. of *EUROCRYPT'93*. Lecture Notes in Compuer Springer-Verlag, 1994. Berlin, Heidelberg, New York. Vol. 765. P.55-65.

57. FIPS 197. [Electronic resource] Advanced encryption standard. — 2001. — http://csrc.nist.gov/publications/

58. Sokolov A.V. Constructive method for the synthesis of nonlinear S-boxes satisfying the strict avalanche criterion. *Radioelectronics and Communications Systems*. 2013. Vol. 56, No. 8. P. 415-423.

59. Sokolov A.V., Zhdanov O.N. Correlation immunity of three-valued logic functions. *Journal of Discrete Mathematical Sciences and Cryptography*. 2020. P. 1-17.

60. Mazurkov M.I. Synthesis method of optimal substitution constructions based on the criterion of zero correlation between the output and input data vectors. *Radioelectronics and Communications Systems*. 2012. Vol. 55, No. 12. P. 533-543.

61. Mazurkov M.I., Sokolov A.V. Method of S-boxes synthesis based on the criterion of zero correlation between the output and input data vectors and the strict avalanche criterion. *Radioelectronics and Communications Systems*. 2014. Vol. 57, No. 8. P. 376-381.

62. Gopalakrishnan K., Stinson D.R., Three characterizations of non-binary correlation-immune and resilient functions. *Designs, Codes and Cryptography.* 1995. No. 5, P. 241-251.

63. Siegenthaler T. Correlation-immunity of nonlinear combining functions for cryptographic applications (Corresp.). *IEEE Transactions on Information theory*. 1984. Vol. 30, No. 5. P. 776-780.

64. Picek S. et al. Correlation immunity of boolean functions: an evolutionary algorithms perspective. Proceedings of the 2015 *Annual Conference on Genetic and Evolutionary Computation*. 2015. P. 1095-1102.

65. Krotov D.S., Vorob'ev K.V. On unbalanced Boolean functions with best correlation immunity. *The Electronic Journal of Combinatorics*. 2020. P. 1-24.

66. Kudin S., Pasalic E. Efficient design methods of low-weight correlation-immune functions and revisiting their basic characterization. *Discrete applied mathematics*. 2020. Vol. 284. P. 150-157.

67. Chai J., Mesnager S., Wang Z. New characterizations for the multi-output correlation-immune Boolean functions. *Discrete Mathematics*. 2020. Vol. 343, No. 11. P. 112082.

68. Ge H., Sun Y., Zhuo Z. Constructions of 1-Resilient Boolean Functions with High Nonlinearity and Good Algebraic Degree. *Chinese Journal of Electronics*. 2020. Vol. 29, No. 4. P. 667-671.

69. Sokolov A.V. Djiofack Temgoua Vanissa Noel. Nonlinear Properties of Rijndael S-boxes Represented by the Many-Valued Logic Functions. Proceedings of the International Workshop on Cyber Hygiene, Kyiv, Ukraine, November 30, 2019. P. 96—106.

70. Sokolov A.V., Radush V.V. Avalanche characteristics of Nyberg construction S-boxes represented by the many-valued logic functions. Informatics & Mathematical Methods in Simulation, 2019. No. 9 (3). P. 111-119.

Розділ 6.

РОЗРОБКА МЕТОДІВ ПІДВИЩЕННЯ КРИПТОГРАФІЧНОЇ СТІЙКОСТІ КРИПТО-СТЕГАНОГРАФІЧНИХ СИСТЕМ

Розроблені у Розділі 5 критерії криптографічної якості ФБЛ є основою не тільки для оцінки криптографічної якості існуючих криптоалгоритмів та їх складових частин, а і базою для побудови нових високоякісних криптографічних примітивів та шифрів на їх основі для задач підвищення криптографічної стійкості крипто-стеганографічної системи, так само як і її адаптації для роботи з потоковим контейнером.

Як показують проведені дослідження, отримані результати стосовно критеріїв криптографічної якості ФБЛ є потужною основою не тільки для розробки шифрів, що характеризуються високою криптографічної якістю своїх складових частин при їх представленні як булевими функціями, так і ФБЛ, збільшеним рівнем реалізації концепції дифузії та конфузії, що дозволяє знизити кількість необхідних раундів, але і можливістю розробки недвійкових шифрів, що відкривають нові можливості для підвищення криптографічної захищеності крипто-стеганографічних систем.

Метою цього розділу є розробка криптографічних конструкцій для підвищення стійкості крипто-стеганографічних систем.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

1. розробити методи синтезу криптографічних примітивів, що характеризуються високою криптографічною якістю як при їх представленні за допомогою булевих функцій, так і при їх представленні за допомогою математичного апарату ФБЛ;

2. розробити адаптований для роботи у прекодерах крипто-стеганографічних систем шифр на основі криптографічних примітивів, що характеризуються високою криптографічної якістю як при їх представленні

за допомогою булевих функцій, та і при їх представленні за допомогою ФБЛ, а також на основі концепції шифрування зі змінною фрагментацією блоків;

3. розробити спосіб вбудовування ДІ з шифруванням переліку станів блока, що забезпечуватиме підвищену криптографічну стійкість вбудованого повідомлення;

4. на основі криптографічних примітивів заснованих на ФБЛ та концепції змінної фрагментації блоків розробити спеціалізований БСШ для шифрування послідовності переліку станів, що являє собою спосіб формування стеганографічного ключа.

6.1. Розроблення методів синтезу криптографічних примітивів для блоку шифрування крипто-стеганографічної системи

6.1.1. Метод синтезу S-блоків, максимально нелінійних у двійковому та четвірковому сенсі

При атаці на алгоритм шифрування криптоаналітик не обмежений у використовуваних засобах і може здійснювати апроксимацію елементів шифру будь-якими доступними способами, в тому числі і методами багатозначної логіки. Важливим з точки зору практики, є завдання розробки методів синтезу максимально нелінійних S-блоків практично цінної довжини $N = 16$, як в сенсі двійкової логіки, так і в сенсі ФБЛ.

Для даної довжини можливими є 2 способи представлення S-блоків: за допомогою булевих функцій та за допомогою ФБЛ. Метод синтезу S-блоків підстановки, що володіють максимальною нелінійністю (як 2-нелінійністю, так і 4-нелінійністю) заснований на наступному підході: спочатку на основі високонелілейних булевих функцій синтезуються 4-функції, що володіють максимально можливою 4-нелінійністю, після чого на їх основі виконується синтез S-блоків.

Запропонований метод синтезу S-блоків підстановки [1], що володіють максимальною нелінійністю, викладемо у вигляді кроків, супроводжуваних конкретними прикладами.

Крок 1. Побудувати множину максимально нелінійних 4-функцій.

Відзначимо, що пошук максимально нелінійних 4-функцій пов'язаний з перебором множини потужності $J_4^{16} = 4^{16} = 2^{32}$, що утруднено з обчислювальної точки зору. Запропоновано наступний алгоритм для синтезу максимально нелінійних 4-функцій на основі максимально нелінійних булевих функцій.

Крок 1.1. Перебравши повну множину булевих функцій довжини $N = 16$, потужності $J_2^{16} = 2^{16} = 65536$, відберемо з них такі, які є збалансованими і при цьому мають найбільшу 2-нелинейность $N_f = 4$. Всього таких булевих функцій існує $J_{Nf\,4} = 10920$ штук.

Крок 1.2. Виконуємо конкатенацію знайдених нелінійних булевих функцій в 4-функцію і вимірюємо її 4-нелінійність відповідно до (5.52).

Наприклад, нехай обрані наступні 2 булеві функції з множини булевих функцій, що побудовані на *Кроці 1.1.*, на основі яких неважко побудувати нову 4-функцію f_1

$$\begin{array}{lcccccccccccccccc} g_1 = & \{ & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \}; \\ g_2 = & \{ & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & \}; \\ f_1 = & \{ & 3 & 3 & 1 & 1 & 3 & 1 & 2 & 0 & 3 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & \}. \end{array} \qquad (6.1)$$

Дослідження показують наступний розподіл (табл. 6.1) 4-нелинейності в синтезованому класі з 10920^2 4-функцій.

Таблиця 6.1. — Розподіл 4-нелінійностей в синтезованому класі з 10920^2 4-функцій

4-нелінійність	3.3509	4	4.6863	5.2297	5.8020	6	7.0557	7.5147
Кількість 4-функцій	7168	53376	120832	387072	979968	1831936	6745472	7279104
4-нелінійність	7.7538	8	8.7889	9.6754	10	10.3431	11.5279	—
Кількість 4-функцій	12682240	12472448	27601920	42826240	3834880	2417600	6144	—

Виявляється, що у множині 4-функцій з 4-нелінійністю 11.5279 не існує збалансованих 4-функцій. Таким чином, максимальне значення 4-нелінійності, яким можуть володіти S-блоки з 2-нелинейностью $N_f = 4$, дорівнює 10.3431.

Крок 2. Вибрати задану компонентну 4-функцію і добудувати до неї пару так, щоб вони складали бієктивний S-блок підстановки.

Наприклад, розглянемо 4-функцію

$$\begin{array}{cccccccccccccccccc} & & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & \\ f_1 = & \{ & 3 & 3 & 1 & 1 & 3 & 1 & 2 & 0 & 3 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & \} \\ f_2 = & \{ & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * & \}. \end{array} \quad (6.2)$$

У позиціях, в яких функція $f_1 = 0$, 4-функція f_2 може приймати будь-яке з чотирьох можливих значень $\{0,1,2,3\}$ для того, щоб S-блок був бієктивним. Всього різних комбінацій, відповідно, може бути $4! = 24$. Розставимо один з можливих наборів функції f_2 в тих позиціях, де $f_1 = 0$

$$\begin{array}{cccccccccccccccccc} & & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & \\ f_1 = & \{ & 3 & 3 & 1 & 1 & 3 & 1 & 2 & 0 & 3 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & \} \\ f_2 = & \{ & * & * & * & * & * & * & * & 0 & * & * & * & * & * & 1 & 2 & 3 & \}. \end{array} \quad (6.3)$$

Аналогічним чином вибираємо один з $4! = 24$ наборів для функції f_2 на позиціях, де $f_1 = 1,2,3$. В результаті, наприклад, отримуємо наступну пару 4-функцій, що визначає S-блок

$$
\begin{array}{lcccccccccccccccc}
 & & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & \\
f_1 = & \{ & 3 & 3 & 1 & 1 & 3 & 1 & 2 & 0 & 3 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & \} \\
f_2 = & \{ & 0 & 1 & 0 & 1 & 3 & 2 & 1 & 0 & 2 & 3 & 2 & 3 & 0 & 1 & 2 & 3 & \} \\
S = & \{ & 3 & 7 & 1 & 5 & 15 & 9 & 6 & 0 & 11 & 13 & 10 & 14 & 2 & 4 & 8 & 12 & \}.
\end{array} \tag{6.4}
$$

Крок 3. Відсіваємо всі такі S-блоки, друга компонентна 4-функція яких не володіє 4-нелінійністю 10.3431.

Для нашого прикладу, задавши 4-функцію f_1 (6.2), ми можемо побудувати 5225 S-блоків, що володіють 4-нелінійністю 10.3431.

6.1.2. Метод синтезу S-блоків з хорошими лавинними характеристиками компонентних булевих та четвіркових функцій

Далі ми представляємо методи синтезу S-блоків будь-якої довжини N, що володіють хорошими лавинними характеристиками як з точки зору їх представлення булевими функціями, так і ФБЛ, що є важливим вихідним матеріалом для створення високоякісних шифрів. Запропонований метод є подальшим розвитком метода [2].

Метод представлено у вигляді кроків, що супроводжуються конкретним прикладом.

Крок 1. Як вихідний матеріал для розробленого методу використовується множина S-блоків довжини $N=16$, що задовольняють СЛК компонентних 4-функцій, яка побудована в [2]. Потужність цієї множини становить $J=245760$ бієктивних S-блоків.

Як приклад розглянемо S-блок

$$
S=\left[\begin{array}{c|cccccccccccccccc}
Q & 0 & 1 & 3 & 7 & 14 & 2 & 10 & 9 & 6 & 12 & 11 & 4 & 13 & 8 & 15 & 5 \\
\hline
f_{40} & 0 & 1 & 3 & 3 & 2 & 2 & 2 & 1 & 2 & 0 & 3 & 0 & 1 & 0 & 3 & 1 \\
f_{41} & 0 & 0 & 0 & 1 & 3 & 0 & 2 & 2 & 1 & 3 & 2 & 1 & 3 & 2 & 3 & 1
\end{array}\right]. \tag{6.5}
$$

Крок 2. Задається функція F_m, яка є старшою компонентною 4-функцією в розкладанні S-блоку на 4-функції.

У випадку S-блоку (6.5) дана компонентна 4-функція має вигляд

$$F_m=[0001302213213231]. \tag{6.6}$$

Крок 3. Формується множина із 4-х перестановок відповідно до наступного правила

$$p_j = x \underset{4}{\oplus} (j \circ d), \quad x = 0,1,...,N-1, \quad j = 0,1,2,3, \tag{6.7}$$

де d — один з векторів довжини $k = \log_4 N$ з 1 на одній зі своїх позицій, вектор x пробігає четвіркові уявлення чисел від 0 до $N-1$, під знаком $\underset{4}{\oplus}$ розуміється додавання по модулю 4, $\circ$ — символ поелементного множення четвіркового уявлення числа d на значення j.

У разі нашого прикладу $k = \log_4 16 = 2$, візьмемо значення $d = [0 \quad 1]$, відповідно, множина перестановок матиме вигляд

$$\begin{aligned}
p_0 &= [0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \quad 10 \quad 11 \quad 12 \quad 13 \quad 14 \quad 15]; \\
p_1 &= [1 \quad 2 \quad 3 \quad 0 \quad 5 \quad 6 \quad 7 \quad 4 \quad 9 \quad 10 \quad 11 \quad 8 \quad 13 \quad 14 \quad 15 \quad 12]; \\
p_2 &= [2 \quad 3 \quad 0 \quad 1 \quad 6 \quad 7 \quad 4 \quad 5 \quad 10 \quad 11 \quad 8 \quad 9 \quad 14 \quad 15 \quad 12 \quad 13]; \\
p_3 &= [3 \quad 0 \quad 1 \quad 2 \quad 7 \quad 4 \quad 5 \quad 6 \quad 11 \quad 8 \quad 9 \quad 10 \quad 15 \quad 12 \quad 13 \quad 14].
\end{aligned} \tag{6.8}$$

Зазначимо, що дані перестановки є окремим випадком перестановок *m*-зсуву [3].

Крок 4. Отримуємо функцію G_1 довжини $4N$ за наступним правилом

$$G_1[F_m] = \left\{ F_m \underset{4}{\oplus} c_1 \mid F_m(p_1) \underset{4}{\oplus} c_2 \mid F_m(p_1) \underset{4}{\oplus} c_3 \mid F_m(p_1) \underset{4}{\oplus} c_4 \right\}, \tag{6.9}$$

де $\{c_1, c_2, c_3, c_4\}$ — множина констант, яка повинна містити всі значення з множини $\{0,1,2,3\}$. За замовчуванням приймемо $c_1 = 0, c_2 = 1, c_3 = 2, c_4 = 3$.

У нашому прикладі отримуємо, що функція G_1 набуде наступного вигляду

$$\begin{aligned}
G_1 = [&000130221321323111211330032230 \\
&20232200120331131003331231002102 12].
\end{aligned} \tag{6.10}$$

Крок 5. Збільшуємо довжину S-блоку до значення $4N$, використовуючи наступну конструкцію

$$G_0 = \{ S \mid S(p_1) \mid S(p_2) \mid S(p_3) \}. \tag{6.11}$$

Крок 6. Будуємо новий бієктивний S-блок довжини $4N$, що задовольняє суворому лавинному критерію компонентних 4-функцій за наступним правилом

$$S_1 = \left\{ G_1 \cdot 4^k + G_0 \right\}, k = \log_4 N. \tag{6.12}$$

Для випадку нашого прикладу отримуємо наступний S-блок довжини $N = 64$

$$\begin{gathered} S_{64} = [0,1,3,23,62,2,42,41,22,60,43,20,61,40,63,21, \\ 17,19,39,16,18,58,57,14,12,59,36,38,56,15,37,13, \\ 35,55,32,33,10,9,30,34,11,52,54,28,31,53,29,8,7,48, \\ 49,51,25,46,50,26,4,6,44,27,5,45,24,47]. \end{gathered} \tag{6.13}$$

Неважко переконатися, що компонентні 4-функції S-блоку (6.13) відповідають умовам **Визначення 5.4.7.** і, відповідно, S-блок (6.13) відповідає СЛК у сенсі компонентних 4-функцій. При цьому отриманий S-блок має наступну матрицю ваг похідних компонентних булевих функцій

e_j	$wt\left(D_{1,k}\right)$	$wt\left(D_{2,k}\right)$	$wt\left(D_{3,k}\right)$	$wt\left(D_{4,k}\right)$	$wt\left(D_{5,k}\right)$	$wt\left(D_{6,k}\right)$
000001	32	40	32	24	32	40
000010	32	32	32	32	32	32
000100	32	32	32	32	32	32
001000	32	32	32	32	32	32
010000	32	40	32	24	32	24
100000	32	32	32	32	32	32

, (6.14)

тобто не відповідає СЛК компонентних булевих функцій.

Повторне застосування розробленого методу до S-блока (6.13) довжини $N = 64$ дозволяє отримати на його основі новий S-блок довжини $N = 256$

$$S_{256} = [0,1,3,87,254,2,170,169,86,252,171,84,253,168,255,85,81,\\ 83,167,80,82,250,249,14,12,251,164,166,248,15,165,13,163,247,\\ 160,161,10,9,94,162,11,244,246,92,95,245,93,8,7,240,241,243,\\ 89,174,242,90,4,6,172,91,5,173,88,175,145,147,231,144,146,58,\\ 57,78,76,59,228,230,56,79,229,77,227,55,224,225,74,73,158,\\ 226,75,52,54,156,159,53,157,72,71,48,49,51,153,238,50,154,68,\\ 70,236,155,69,237,152,239,64,65,67,151,62,66,234,233,150,60,\\ 235,148,61,232,63,149,35,119,32,33,138,137,222,34,139,116,\\ 118,220,223,117,221,136,135,112,113,115,217,46,114,218,132,\\ 134,44,219,133,45,216,47,128,129,131,215,126,130,42,41,214,\\ 124,43,212,125,40,127,213,209,211,39,208,210,122,121,142,140,\\ 123,36,38,120,143,37,141,199,176,177,179,25,110,178,26,196,\\ 198,108,27,197,109,24,111,192,193,195,23,190,194,106,105,22,\\ 188,107,20,189,104,191,21,17,19,103,16,18,186,185,206,204,187,\\ 100,102,184,207,101,205,99,183,96,97,202,201,30,98,203,180,\\ 182,28,31,181,29,200], \quad (6.15)$$

який також відповідає СЛК компонентних 4-функцій, і характеризується наступною матрицею ваг похідних компонентних булевих функцій

e_j	$wt(D_{1,k})$	$wt(D_{2,k})$	$wt(D_{3,k})$	$wt(D_{4,k})$	$wt(D_{5,k})$	$wt(D_{6,k})$	$wt(D_{7,k})$	$wt(D_{8,k})$
00000001	128	160	128	96	128	160	128	128
00000010	128	128	128	128	128	128	128	128
00000100	128	128	128	128	128	128	128	128
00001000	128	128	128	128	128	128	128	128
00010000	128	160	128	96	128	128	128	96
00100000	128	128	128	128	128	128	128	128
01000000	128	160	128	96	128	128	128	128
10000000	128	128	128	128	128	128	128	128

, (6.16)

тобто не відповідає СЛК компонентних булевих функцій.

Проведені експерименти показують, що на основі повної множини S-блоків довжини $N = 16$, яка була побудована у [2], шляхом застосування розробленого методу можуть бути отримані S-блоки практично цінної довжини $N = 256$, які відповідають одночасно СЛК компонентних 4-функцій і критерію максимального лавинного ефекту булевих функцій. При цьому, кількість даних S-блоків залежить від значення вибраних параметрів c_1, c_2, c_3, c_4, а також від вибраного вектору напрямку d. Наприклад, нехай задані наступні параметри: довжина S-блоку $N = 256$, параметри $c_1 = 0, c_2 = 1, c_3 = 2, c_4 = 3$ на першій і на другій ітерації застосування методу, а також значення $d = [0 \quad 1]$ на першій ітерації застосування методу і

$d=[0 \quad 0 \quad 1]$ на другій ітерації застосування методу. Отримуємо тоді, що з множини $J=245760$ S-блоків довжини $N=256$ отриманих на основі множини S-блоків довжини $N=16$ [2], що задовольняють СЛК компонентних 4-функцій існує точно $J_1=3968$ S-блоків, що одночасно задовольняють і критерію максимального лавинного ефекту компонентних булевих функцій. В якості прикладу наведемо один із даних S-блоків довжини $N=256$, компонентні 4-функції якого задовольняють СЛК, який побудований на основі S-блоку $S=[0,1,2,12,7,11,3,8,15,9,6,13,5,4,10,14]$

$$
\begin{gathered}
S_{256}=[1,2,252,0,171,3,168,87,169,86,253,255,84,170,254,85,82,12,\\
80,81,83,248,167,251,166,13,15,249,250,14,165,164,92,160,161,\\
162,8,247,11,163,93,95,9,246,94,245,244,10,240,241,242,172,7,\\
91,243,88,175,89,6,173,5,4,90,174,66,60,64,65,67,232,151,235,\\
150,61,63,233,234,62,149,148,76,144,145,146,56,231,59,147,77,\\
79,57,230,78,229,228,58,224,225,226,156,55,75,227,72,159,73,\\
54,157,53,52,74,158,49,50,236,48,155,51,152,71,153,70,237,239,\\
68,154,238,69,124,128,129,130,40,215,43,131,125,127,41,214,126,\\
213,212,42,208,209,210,140,39,123,211,120,143,121,38,141,37,36,\\
122,142,33,34,220,32,139,35,136,119,137,118,221,223,116,138,222,\\
117,114,44,112,113,115,216,135,219,134,45,47,217,218,46,133,\\
132,192,193,194,188,23,107,195,104,191,105,22,189,21,20,106,190,\\
17,18,204,16,187,19,184,103,185,102,205,207,100,186,206,101,98,\\
28,96,97,99,200,183,203,182,29,31,201,202,30,181,180,108,176,\\
177,178,24,199,27,179,109,111,25,198,110,197,196,26],
\end{gathered}
\tag{6.17}
$$

та його матрицю ваг похідних булевих функцій

e_j	$wt(D_{1,k})$	$wt(D_{2,k})$	$wt(D_{3,k})$	$wt(D_{4,k})$	$wt(D_{5,k})$	$wt(D_{6,k})$	$wt(D_{7,k})$	$wt(D_{8,k})$
00000001	128	160	128	160	128	128	128	160
00000010	128	128	128	128	128	128	128	128
00000100	128	128	128	128	128	128	128	128
00001000	128	128	128	128	128	128	128	128
00010000	128	160	128	160	128	128	128	128
00100000	128	128	128	128	128	128	128	128
01000000	128	160	128	160	128	128	128	128
10000000	128	128	128	128	128	128	128	128

, (6.18)

яка підтверджує, що даний S-блок (6.17) дійсно відповідає критерію максимального лавинного ефекту компонентних булевих функцій.

6.1.3. Метод синтезу максимально нелінійних S-блоків, що відповідають СЛК найвищих порядків

У цьому підрозділі для вирішення задачі підвищення криптографічної якості компонентів шифрів запропоновано метод синтезу максимально-нелінійних S-блоків, що задовольняють критерію розповсюдження найвищого порядку. Подібні S-блоки побудовано для значення довжини $N = 32$, при якому представлення криптографічних конструкцій можливо лише за допомогою булевих функцій. Дослідження криптографічних конструкцій, що відповідають критерію розповсюдження помилки вищих порядків присвячено чимало уваги дослідників [4, 5]. Однак, в літературі не представлені конкретні методи побудови S-блоків, що одночасно є максимально нелінійними, та задовольняють критерію розповсюдження вищих порядків. Далі наведемо розроблений метод синтезу S-блоків, які задовольняють критерію максимальної відстані нелінійності та критерію розповсюдження порядків $m > 1$ [6].

Раніше у Розділі 1 було введено визначення булевих бент-функцій. Відзначимо деякі властивості бент-функцій, які є важливими в контексті викладених далі досліджень:

Властивість 6.1.1. Відстань нелінійності бент-функції дорівнює

$$N_f = 2^{k-1} - 2^{k/2-1}. \qquad (6.19)$$

Властивість 6.1.2. Бент-функції існують лише для парної кількості змінних k.

Властивість 6.1.3. Нехай f є бент-функцією і g є афінною функцією. Тоді $f \oplus g$ є також бент-функцією.

Властивість 6.1.4. Бент-функції не врівноважені, тобто $K^{(0)} \neq K^{(1)}$, де $K^{(i)}$ кількість символів у таблиці істинності булевої функції.

Також у Розділі 1 було введено визначення булевих функцій, що задовольняють критерію розповсюдження. Відзначимо деякі важливі, в контексті виконуваних досліджень, властивості булевих функцій, що задовольняють критерію розповсюдження PC(m) порядку m.

Властивість 6.1.5. Нехай f — булева функція, яка задовольняє критерію розповсюдження $\mathrm{PC}(m)$, і g — афінна функція. Тоді $f \oplus g$ також задовольняє критерію розповсюдження $\mathrm{PC}(m)$.

Властивість 6.1.6. Бент-функції і лише вони задовольняють критерію розповсюдження $\mathrm{PC}(k)$ порядку k.

З практичної точки зору становлять інтерес булеві функції, що відповідають критерію розповсюдження, а також критерію високої нелінійності. У цьому світлі визначати відстань нелінійності через коефіцієнти перетворення Уолша-Адамара зручно, оскільки це дозволяє зменшити пошук булевих функцій, за допомогою розгляду лише множини булевих функцій, що задовольняють необхідному значенню відстані нелінійності.

Коефіцієнти перетворення Уолша-Адамара мають строго детерміновану структуру, що передбачає певні набори можливих значень. З точки зору практичного використання представляється зручною класифікація множин коефіцієнтів перетворення Уолша-Адамара, виходячи з їх елементарної структури [7].

Запропоноване у роботі [7] визначення елементарної структури дає можливість класифікувати вектори коефіцієнтів перетворення Уолша-Адамара на спектральні класи. Таким чином, вектори коефіцієнтів перетворення Уолша-Адамара в межах кожного спектрального класу характеризуються однаковою елементарною структурою.

Для різної довжини таблиць істинності булевих функцій існують різні множини можливих елементарних структур векторів коефіцієнтів перетворення Уолша-Адамара, які складають їх спектральну класифікацію.

Наприклад, у тривіальному випадку булевих функцій $k=1$ змінної довжини $N=2^k=2$ є всього $J=4$ булеві функції, кожну з яких представимо разом з відповідним вектором коефіцієнтів перетворення Уолша-Адамара

$$\begin{array}{lcl} f_1=\{0 \quad 0\} & \to & W_1=\{2 \quad 0\} \\ f_2=\{0 \quad 1\} & \to & W_2=\{0 \quad -2\} \\ f_3=\{1 \quad 0\} & \to & W_3=\{0 \quad 2\} \\ f_4=\{1 \quad 1\} & \to & W_4=\{-2 \quad 0\} \end{array}. \qquad (6.20)$$

Згідно з результатами [7], у наборі булевих функцій довжини $N=2$ існує лише один спектральний клас, який характеризується елементарною структурою $\{2(1),0(1)\}$. Це позначення елементарної структури слід розуміти так: число перед дужками характеризує абсолютне значення коефіцієнта перетворення Уолша-Адамара, тоді як число в дужках вказує, скільки разів воно зустрічається у векторі коефіцієнтів перетворення Уолша-Адамара.

Відстань нелінійності всіх булевих функцій (6.20) дорівнює $N_f=0$, тобто вони афінні. Очевидно також, що жодна з булевих функцій (6.20) не задовольняє критерію розповсюдження порядку $m=1$.

Ситуація змінюється при переході до булевих функцій $k=2$ змінних довжини $N=4$, загальна кількість яких становить $J=16$. У випадку векторів коефіцієнтів перетворення Уолша-Адамара довжини 4 існують дві можливі елементарні структури та відповідні спектральні класи. Ці елементарні структури наведені в табл. 6.2., для кожної з них наведено потужність відповідного спектрального класу та кількість булевих функцій, що задовольняють критерію розповсюдження порядків $m=1,2$.

Таблиця 6.2. — Елементарні структури булевих функцій $k=2$ змінних

Номер класу спектральних векторів	Набори абсолютних значень спектральних компонент	Потужність класу	Відстань нелінійності	Кількість булевих функцій, які відповідають критерію розповсюдження порядку m	
				$m=1$	$m=2$
1	$\{4(1), \quad 0(3)\}$	8	0	0	0
2	$\{2(4)\}$	8	1	8	8

Таким чином, у множині булевих функцій довжини $N=4$ є підклас булевих бент-функцій, що задовольняють критерію розповсюдження РС(2) порядку $m=2$ та мають максимальну відстань нелінійності $N_f=1$. Однак, відповідно до *Властивості 6.1.4.* бент-функції є неврівноваженими і непридатні для побудови бієктивних S-блоків. Іншими словами, дані, представлені в табл. 6.2., показують неможливість побудови бієктивних S-блоків довжини $N=4$, що задовольняють критерію розповсюдження.

Розглянемо далі булеві функції $k=3$ змінних, довжини $N=8$. У табл. 6.3. показана спектральна класифікація векторів перетворення Уолша-Адамара довжини $N=8$, а також обчислені нами кількості булевих функцій, що відповідають критерію розповсюдження порядків $m=1,2,3$.

Таблиця 6.3. — Елементарні структури булевих функцій $k=3$ змінних

Номер класу спектральних векторів	Набори абсолютних значень спектральних компонент	Потужність класу	Відстань нелінійності	Кількість булевих функцій, які відповідають критерію розповсюдження порядку m		
				$m=1$	$m=2$	$m=3$
1	$\{\pm 8(1),\quad 0(7)\}$	16	0	0	0	0
2	$\{\pm 6(1),\quad \pm 2(7)\}$	128	1	0	0	0
3	$\{\pm 4(4),\quad 0(4)\}$	112	2	64	16	0

Таким чином, з точністю до суми з афінною функцією для булевих функцій довжини $N=8$ існують $64/16=4$ булеві функції, що задовольняють критерію поширення порядку $m=1$

$$DC_{1,8}=[0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 1\ \ 0\ \ 0;\ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0;\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0;\ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1],\tag{6.21}$$

а також $16/16=1$ булева функція, що відповідає критерію розповсюдження порядку $m=2$

$$DC_{2,8}=[0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1]. \qquad (6.22)$$

Усі булеві функції довжини $N=8$, що задовольняють критерію поширення, належать до спектрального класу №3 і, відповідно, мають максимально можливу відстань нелінійності $N_f=2$.

Далі розглянемо булеві функції $k=4$ змінних довжини $N=16$. Для заданої довжини булевих функцій має місце представлена в табл. 6.4. класифікація. У табл. 6.4. представимо дані про кількість булевих функцій, які відповідають критерію розповсюдження порядків $m=1...4$.

Таблиця 6.4. — Елементарні структури булевих функцій $k=4$ змінних

Номер класу спектральних векторів	Набори абсолютних значень спектральних компонент	Потужність класу	Відстань нелінійності	Кількість булевих функцій, які відповідають критерію розповсюдження порядку m			
				$m=1$	$m=2$	$m=3$	$m=4$
1	$\{16(1),0(15)\}$	32	0	0	0	0	0
2	$\{14(1),2(15)\}$	512	1	0	0	0	0
3	$\{12(1),4(7),0(8)\}$	3840	2	0	0	0	0
4	$\{10(1),6(3),2(12)\}$	17920	3	0	0	0	0
5	$\{8(2),4(8),0(6)\}$	26880	4	2816	0	0	0
6	$\{8(4),0(12)\}$	1120	4	416	0	0	0
7	$\{6(6),2(10)\}$	14336	5	0	0	0	0
8	$\{4(16)\}$	896	6	896	896	896	896

Таким чином, для булевих функцій довжини $N=16$ існують $2816+416+896=4128$ булевих функцій, які задовольняють критерію розповсюдження порядку $m=1$. Спектральний клас булевих функцій №8 — це бент-функції, які відповідно до *Властивості 6.1.2.* задовольняють критерію розповсюдження порядку $m=k=\log_2 N=4$. Тим не менш, всі вони

неврівноваженими, і для довжини $N=16$ побудова S-блоків, що відповідають критерію розповсюдження порядку $m>1$, так само як і для булевих бент-функцій $k=2$ змінних, неможлива.

Далі розглянемо спектральну класифікацію булевих функцій довжини $N=32$. Зауважимо, що ця проблема для булевих функцій довжини $N=32$ пов'язана зі значними обчислювальними труднощами, оскільки передбачає розгляд множини з $J=2^{32}=4\,294\,967\,296$ елементів. Ця обставина вимагає використання конструктивного методу замість методу грубої сили. Даний конструктивний метод, із використанням АНФ описано у роботах [8].

Виходячи з цього, ми розглядаємо метод пошуку різних спектральних структур для векторів довжини 32 у вигляді кроків.

Крок 1. Розглянемо послідовність коефіцієнтів АНФ $\{a_i\}$ булевої функції п'яти змінних. Зафіксуємо в ній такі положення, які відповідають афінним функціям (табл. 6.5.). У табл. 6.5. використовуються такі позначення: **0** — нульове значення, ? — значення, яке можна змінювати під час пошуку.

Таблиця 6.5. — Позиції афінних доданків у послідовності довжини $N=32$

1	**2**	**3**	4	**5**	6	7	8	**9**	10	11	12	13	14	15	16
0	**0**	**0**	?	**0**	?	?	?	**0**	?	?	?	?	?	?	?
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	18	19	20	21	22	23	24	25	26	27	28	29	30	21	32
0	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Крок 2. Зробимо послідовну зміну в решті позицій, надаючи їм значення 0 або 1.

У разі довжини вихідної послідовності $N = 32$ на цьому етапі необхідно розглянути $2^{32}/2^6 = 2^{26} = 67\,108\,864$ різні послідовності, що обчислювально можливо.

Крок 3. З набору послідовностей, отриманих на *Кроці* 2, вибираємо ті, які мають різну елементарну структуру.

Результати використання запропонованого методу щодо послідовностей довжини $N = 32$ наведені в табл. 6.6. у вигляді спектральної класифікації, де представляємо кількості булевих функцій, що задовольняють критерію розповсюдження заданого порядку для кожного можливого спектрального класу.

Таблиця 6.6. — Елементарні структури булевих функцій $k = 5$ змінних

№	Набір абсолютних значень спектральних компонент	N_f	Потужність класу	Кількість булевих функцій, які відповідають критерію розповсюдження порядку m				
				1	2	3	4	5
1	{32(1), 0(31)}	0	64	0	0	0	0	0
2	{30(1),2(31)}	1	2 048	0	0	0	0	0
3	{28(1),4(15), 0(16)}	2	31 744	0	0	0	0	0
4	{26(1),6(7),2(24)}	3	317 440	0	0	0	0	0
5	{24(1),8(7),0(24)}	4	79 360	0	0	0	0	0
6	{24(1), 8(3), 4(16), 0(12)}	4	2 222 080	0	0	0	0	0
7	{22(1),10(3),6(4), 2(24)}	5	2 222 080	0	0	0	0	0
8	{22(1),10(1),6(10), 2(20)}	5	10 665 984	0	0	0	0	0
9	{20(1),12(3),4(12), 0(16)}	6	1 111 040	0	0	0	0	0
10	{20(1),8(6), 4(15), 0(10)}	6	28 442 624	0	0	0	0	0
11	{20(1),12(1),4(30)}	6	1 777 664	0	0	0	0	0
12	{20(1), 12(1), 8(4), 4(14), 0(12)}	6	26 664 960	0	0	0	0	0

Продовження табл. 6.6.

13	{18(1), 14(3), 2(28)}	7	317 440	0	0	0	0	0
14	{18(1), 14(1), 10(2), 6(6), 2(22)}	7	26 664 960	0	0	0	0	0
15	{18(1),10(3),6(9), 2(19)}	7	142 213 120	0	0	0	0	0
16	{18(1),10(1),6(15), 2(15)}	7	28 442 624	0	0	0	0	0
17	{18(1),14(1),6(12), 2(18)}	7	17 776 640	0	0	0	0	0
18	{16(1),12(2),8(4), 4(14),0(11)}	8	213 319 680	737280	0	0	0	0
19	{16(2),12(2),4(14), 0(14)}	8	3 809 280	163840	0	0	0	0
20	{16(2),8(4), 4(16),0(10)}	8	19 998 720	645120	0	0	0	0
21	{16(2),8(8),0(22)}	8	1 666 560	94720	0	0	0	0
22	{16(4),0(28)}	8	9 920	2560	0	0	0	0
23	{16(1),12(1),8(6), 4(15),0(9)}	8	284 426 240	276480	0	0	0	0
24	{16(1),8(12),0(19)}	8	17 776 640	0	0	0	0	0
25	{16(1),8(8),4(16),0(7)}	8	106 659 840	0	0	0	0	0
26	{14(3),10(1),6(7), 2(21)}	9	20 316 160	0	0	0	0	0
27	{14(2),10(4),6(4), 2(22)}	9	26 664 960	0	0	0	0	0
28	{14(2),10(2),6(10), 2(18)}	9	319 979 520	0	0	0	0	0
29	{14(1),10(5),6(7), 2(19)}	9	426 639 360	0	0	0	0	0
30	{14(1),10(3),6(13), 2(15)}	9	568 852 480	0	0	0	0	0
31	{12(4),8(4),4(12), 0(12)}	10	115 548 160	1904640	0	0	0	0
32	{12(4),4(28)}	10	31 744 000	1310720	0	0	0	0
33	{12(6),4(10),0(16)}	10	888 832	0	0	0	0	0
34	{12(3),8(6),4(13), 0(10)}	10	426 639 360	1966080	0	0	0	0
35	{12(2),8(8),4(14), 0(8)}	10	666 624 000	12697600	0	0	0	0

Закінчення табл. 6.6

36	{12(1),8(10),4(15), 0(6)}	10	170 655 744	2654208	12288	0	0	0
37	{10(6),6(10),2(16)}	11	449 748 992	0	0	0	0	0
38	{10(4),6(16),2(12)}	11	106 659 840	0	0	0	0	0
39	{8(12),4(16),0(4)}	12	13 332 480	3440640	0	0	0	0
40	{8(16),0(16)}	12	14 054 656	1628672	228352	10752	1792	0

Аналіз даних, представлених у табл. 6.6., показує, що для довжини булевих функцій $N = 32$ існує клас з 1792 (28 з точністю до суми з афінною функцією) булевих функцій, які мають максимальну відстань нелінійності та також задовольняють критерію розповсюдження. Більш детальне дослідження цього класу дозволило встановити, що він містить 768 (12 з точністю до суми з афінною функцією) збалансованих булевих функцій, придатних для побудови S-блоків

$$\begin{gathered}
\{00000011010110010110010100111111\};\\
\{00000011011001010101100100111111\};\\
\{00000101001110010110001101011111\};\\
\{00000101011000110011100101011111\};\\
\{00000110001101010101001110011111\};\\
\{00000110010100110011010110011111\};\\
\{00010001001011010100101101110111\};\\
\{00010001010010110010110101110111\};\\
\{00010010000111010100011110110111\};\\
\{00010010010001110001110110110111\};\\
\{00010100000110110010011111010111\};\\
\{00010100001001110001101111010111\}.
\end{gathered} \tag{6.23}$$

Ці булеві функції мають найбільшу відстань нелінійності, а також найвищий можливий ($\mathrm{PC}(4)$) порядок критерію розповсюдження серед усіх булевих функцій довжини $N = 32$.

На основі знайденого класу та алгоритму [9] стає можливим побудувати бієктивні S-блоки з відстанню нелінійності $N_f = 12$, які задовольняють критерію розповсюдження $\mathrm{PC}(4)$, наприклад

$$\begin{aligned}
S = [&24\ 12\ 18\ 22\ 14\ 26\ 27\ 31\ 20\ 15\ 30\ 21\ 29\ \ 6\ \ 8\ \ 3\ 28\ 23\\
&25\ \ 2\ 10\ \ 1\ 16\ 11\ \ 0\ \ 4\ \ 5\ 17\ \ 9\ 13\ 19\ \ 7].
\end{aligned} \tag{6.24}$$

S-блок (6.24), а також інші S-блоки, створені на основі побудованого набору булевих функцій (6.23) та алгоритму [9], є найкращими з точки зору критерію високої відстані нелінійності та критерію розповсюдження серед можливих S-блоків довжини $N = 32$ і можуть бути рекомендовані для практичного використання.

6.2. Модифікований алгоритм шифрування зі змінною фрагментацією блоків

Як відомо, багато сучасних алгоритмів шифрування використовують заміни по таблиці і операцію складання з раундовим ключем [10…19]. При цьому важливим є як розмір блоку, що замінюється, так і якість таблиці замін, які впливають на показники дифузії і конфузії.

Блок є об'єктом, над яким потрібно здійснити криптографічне перетворення. Однак блок тексту володіє своєю структурою, яка в більшій чи меншій мірі успадковує особливості текстів на природній мові. Тому робота з блоками незмінного, одного і того ж розміру в усіх раундах, не може гарантувати розсіювання таких особливостей по шифротексту, і для підвищення якості результуючого криптоперетворення доводиться ускладнювати раундові операції з блоками або збільшувати кількість раундів.

Далі представлено концепцію шифрування з динамічною зміною розмірів криптографічних примітивів в різних раундах та можливу реалізацію криптографічного алгоритму на її основі. А саме запропоновано проводити зашифрування тексту, застосовуючи заміни за таблицями різних розмірів в різних раундах. Більше того, як показують дослідження, складові частини шифрів, що відповідають різним критеріям легше побудувати для різних значень довжини вхідного блока. Отже, для поєднання переваг

використання різноманітних криптографічних конструкцій доцільною є зміна довжини блока, що шифрується, на протязі різних раундів шифрування.

Для найбільш ефективної організації подібних алгоритмів шифрування з динамічною зміною розмірів криптографічних примітивів довжина вхідного блоку алгоритма повинна бути складеним числом [20]. Наприклад, розглянемо блок відкритого тексту довжини $L = 120 = 2^3 \cdot 3 \cdot 5$ біт. Розбиття даного блоку відкритого тексту в алгоритмі шифрування може бути здійснено різними способами, наприклад, на сегменти зручної з обчислювальної точки зору довжини $\sigma = 6,8,10,12,15,20,30$ біт, при цьому в межах одного раунду розмір сегмента не змінюється.

На відміну від класичної мережі Фейстеля в запропонованому алгоритмі криптографічні примітиви застосовуються і до правої і до лівої частини вихідного блоку одночасно. Загальна схема основного кроку криптоперетворення запропонованого алгоритму представлена на рис. 6.1.

Опишемо запропонований симетричний алгоритм шифрування:

Загальна інформація:

Вхідний блок даних сегментується на фрагменти по 240 біт, та подається на вхід основного кроку криптоперетворення. Після цього, кожен фрагмент із 240 біт сегментується на дві частини: L_i та R_i. У базовій версії криптоалгоритму основний крок криптоперетворення повторюється 7 разів.

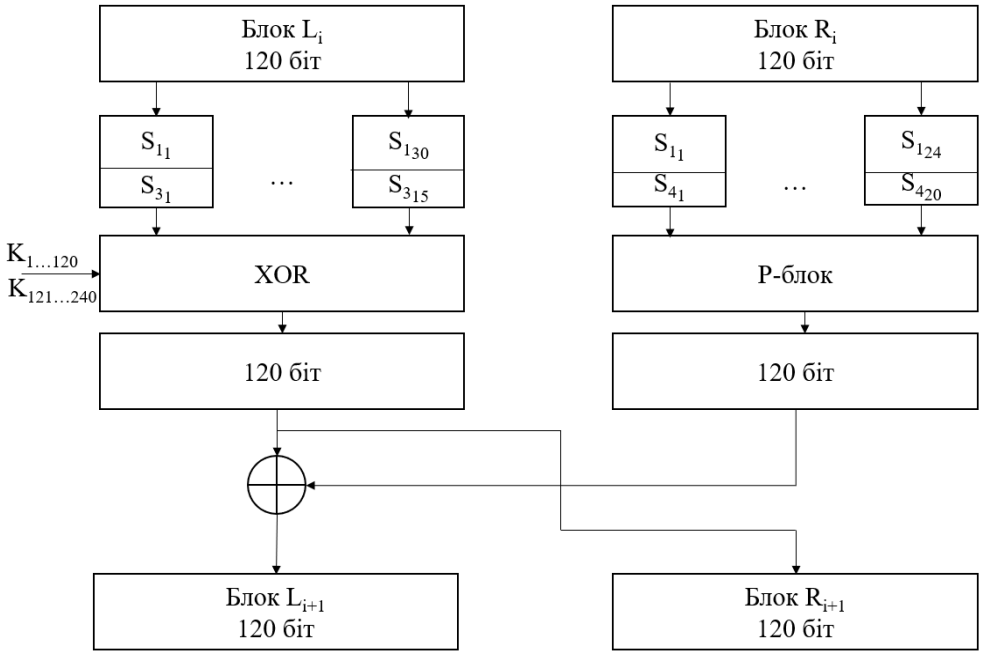


Рис. 6.1. — Основний крок криптоперетворення

S-блоки:

Застосовуються різні S-блоки для парних та непарних ітерацій основного кроку криптоперетворення. Так, на 1,3,5,7 ітерації використовуються наступні набори S-блоків:

$S_{1_1}...S_{1_{30}}$ — набір із 30 нелінійних у двійковому та четвірковому сенсі S-блоків довжини $N = 16$, метод синтезу представлено у Підрозділі 6.1.1. Таким чином, для застосування даних S-блоків вихідний фрагмент довжини 120 біт розбивається на $120 / \log_2(16) = 30$ частин по $\log_2(16) = 4$ біта кожна.

$S_{2_1}...S_{2_{24}}$ — набір із 24 максимально нелінійних S-блоків довжини $N = 32$, що відповідають критерію розповсюдження максимального порядку, алгоритм синтезу яких представлено у Підрозділі 6.1.3. Для застосування даних S-блоків вихідний фрагмент довжини 120 біт розбивається на $120 / \log_2(32) = 24$ частини по $\log_2(32) = 5$ біт кожна.

З іншого боку, на ітераціях 2,4,6 використовуються наступні набори S-блоків:

$S_{3_1}...S_{3_{15}}$ — набір із 15 S-блоків конструкції Ніберг довжини $N = 256$. Для застосування даних S-блоків вихідний фрагмент довжини 120 біт розбивається на $120 / \log_2(256) = 15$ частин по $\log_2(256) = 8$ біт кожна. Дослідження криптографічної якості S-блоків конструкції Ніберг при їх уявленні за допомогою компонентних ФБЛ виконано в роботах [21, 22].

$S_{4_1}...S_{4_{20}}$ — набір із 20 S-блоків довжини $N = 64$, що відповідають СЛК компонентних ФБЛ та критерію максимального лавинного ефекту компонентних булевих функцій. Метод синтезу таких S-блоків представлено в Підрозділі 6.1.2. Для застосування даних S-блоків вихідний фрагмент довжини 120 біт розбивається на $120 / \log_2(64) = 20$ частин по $\log_2(64) = 6$ біт кожна [23].

Складання з ключем:

Складання з ключем виконується наступним чином: ключ має загальну довжину 240 біт та розділюється на дві частини: на парних ітераціях виконується складання з першою частиною ключа, на непарних — із другою. Операція складання являє собою побітове виключне АБО.

P-блок:

У базовій версії запропонованого алгоритму використовується випадковий P-блок довжини $N = 240$.

Розшифрування:

Операція розшифровування виконується подібно до операції шифрування із наступними особливостями:

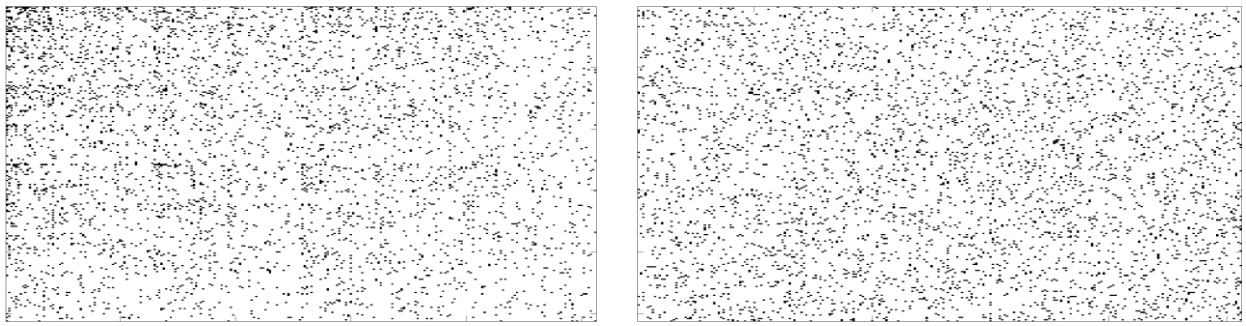
1. порядок слідування ітерацій обирається зворотним;

2. порядок виконання дій у основному кроці криптоперетворення обирається зворотним;

3. в якості S-блоків використовуються послідовності, що я зворотними до S-блоків, використаних під час шифрування;

4. в якості P-блоку використовується послідовність, що є зворотною до P-блоку, використаному під час шифрування.

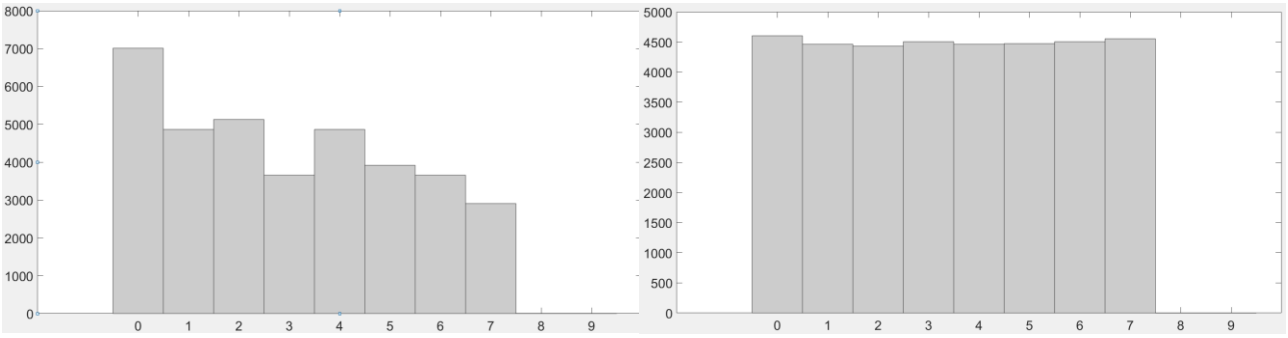
Проведемо серію показових тестів [24] для встановлення якісних характеристик розробленого нами криптографічного алгоритму. На рис. 6.2. показано динаміку зміни розподілення на площині при шифруванні текстової інформації.



а) б)

Рис. 6.2. — Динаміка зміни розподілення на площині при шифруванні текстової інформації (а) — вихідний текст, б) — перша ітерація)

На рис. 6.3. наведено динаміку зміни гістограми 3-грамного розподілу.



а) б)

Рис. 6.3. — Динаміка зміни гістограми 3-грамного розподілу (а) — вихідний текст, б) — перша ітерація)

Результати чисельних проведених експериментів за іншими тестами також підтверджують високу ефективність запропонованого криптоалгоритму, яка проявляється вже на першому раунді шифрування та

обумовлена високою якістю його складових, як у сенсі їх уявлення булевими функціями, так і ФБЛ.

Відзначимо, що розроблений шифр може працювати з будь-якими режимами шифрування, включно із новими економічними режимами, що запропоновані в роботах [25, 26].

6.3. Вбудовування ДІ з шифруванням переліку станів блока

Розвиток теоретичних засад криптографічної стійкості ФБЛ, який було проведено в Розділі 5 із поєднанням з методом вбудовування інформації з кодовим управлінням, який було представлено в Розділі 3, дозволяє розробку нових рішень щодо підвищення криптографічної захищеності крипто-стеганографічних систем. У поточному розділі запропоновано наступну модифікацію структурної схеми типової стеганосистеми, що показана на рис. 6.4.

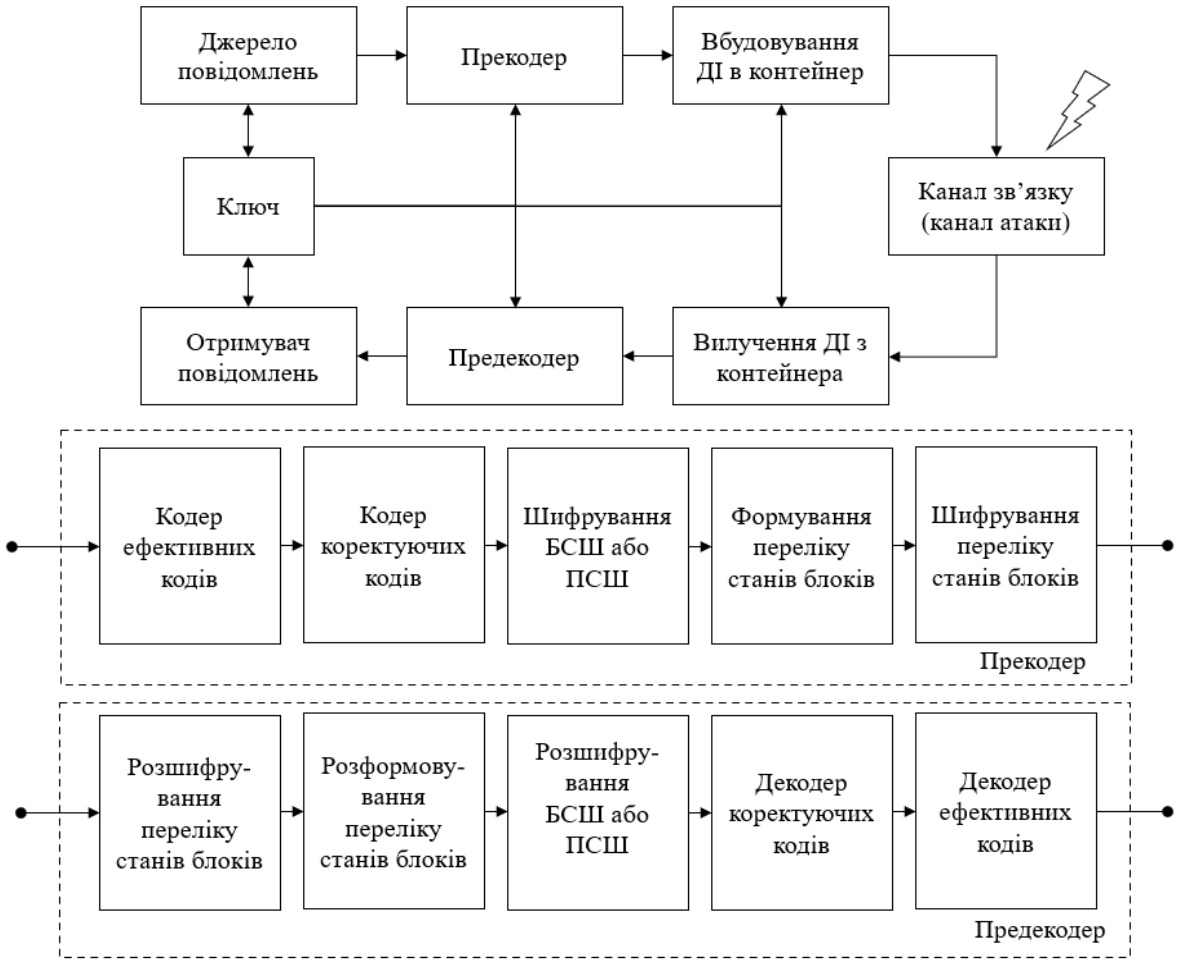


Рис. 6.4. — Структурна схема вбудовування ДІ із шифруванням переліку станів блоків

Основна відмінність запропонованої на рис. 6.4. схеми полягає у наборі компонентів прекодера і предекодера, який розглянемо докладніше. Перші 3 блоки прекодера є класичними для будь-яких систем передавання інформації: перед вбудовуванням ДІ проходить кодування ефективним кодом задля усунення природньої надмірності, після чого вона кодується коректуючим кодом, який впроваджує в неї штучну надмірність задля набуття можливості виявлення та корекції помилок. Отримана послідовність шифрується за допомогою БСШ або ПСШ. Оптимальним є використання запропонованого у Підрозділі 6.2 БСШ із підвищеним рівнем криптостійкості, що враховує можливість уявлення його конструкцій за допомогою ФБЛ. Результатом

роботи перших трьох блоків прекодера має стати двійкова послідовність, що відображається на бінарний алфавіт $\{\pm 1\}$.

Отримана бінарна послідовність над алфавітом $\{\pm 1\}$ поступає на вхід пристрою формування переліку станів блоків, що визначає, у які саме блоки відбуватиметься вбудовування ДІ, а які блоки залишатимуться порожніми. Після цього послідовність переліку станів шифрується, і вже зашифрована послідовність переліку станів визначає які данні вбудовуються (або не вбудовуються) у конкретний блок.

Розглянемо докладніше роботу зв’язки пристроїв формування переліку станів блоків та шифрування переліку станів блоків у вигляді конкретного алгоритму їх роботи.

При цьому необхідність виконання *Кроку 1* та *Кроку 2* представленого алгоритму визначається необхідністю протидії можливим криптоаналітичним атакам по відомим кінцівкам ДІ у разі меншої кількості ДІ у порівнянні з кількістю блоків зображення-контейнера, у яке відбувається вбудовування інформації.

Крок 1. Кожному блоку зображення-контейнера, який прийматиме участь в процесі вбудовування, ставиться у відповідність комірка у матриці станів Σ', у яку записуються біти вихідної послідовності відповідно до наступної схеми, показаної на рис. 6.5. При цьому у порожні комірки, якщо довжина бітової послідовності ДІ менша за кількість комірок матриці Σ', записується значення 0.

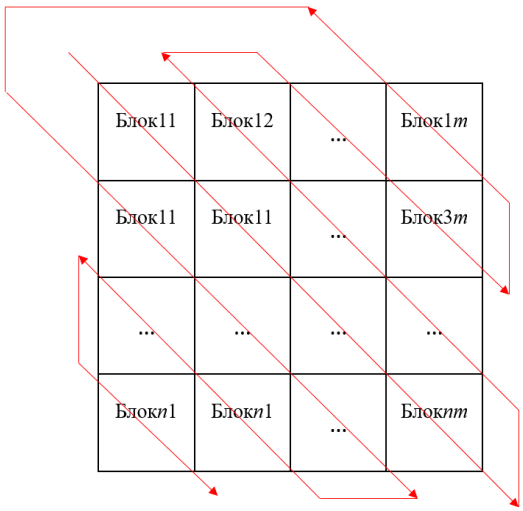


Рис. 6.5. — Схема заповнення комірок матриці Σ'

Крок 2. Виконується зчитування (по рядкам) послідовності переліку станів з матриці Σ' в результаті чого формується послідовність S довжини nm над алфавітом $\{0,\pm1\}$.

Крок 3. Виконується шифрування послідовності S над алфавітом $\{0,\pm1\}$ в результаті чого отримуємо нову послідовність $E(S)$ над алфавітом $\{0,\pm1\}$ довжини nm.

Крок 4. Послідовно виконується запис по рядках елементів зашифрованої послідовності $E(S)$ над алфавітом $\{0,\pm1\}$ у остаточну матрицю переліку станів Σ. Подальше вбудовування інформації у блоки зображення-контейнера відбувається за допомогою стеганографічного методу із кодовим управлінням вбудовуванням у відповідності до значень матриці Σ, які показують 3 можливих стани: вбудовується додатне кодове слово T^+, від'ємне кодове слово T^- або ж вбудовування у цей блок не відбувається.

Розглянемо роботу представленого алгоритму на конкретному прикладі. Нехай зображення-контейнер матиме розмір 32x32 пікселі, при цьому у нього необхідно виконати вбудовування 32 бітів ДІ

$$d_i = \{1,1,1,-1,-1,1,-1,1,1,1,-1,-1,1,1,1,-1,-1, \\ -1,1,-1,-1,1,1,1,-1,1,-1,1,-1,1,-1,-1\}, \quad (6.25)$$

за допомогою стеганографічного методу з кодовим управлінням вбудовуванням із використанням кодових слів розміру 4×4. Отже, записуємо у табл. 6.7. матрицю Σ', яка в нашому випадку матиме розмір $\frac{32}{4}\times\frac{32}{4}=8\times8$.

Таблиця 6.7. — Матриця Σ'

Блок 11 1	Блок 12 1	Блок 13 –1	Блок 14 1	Блок 15 –1	Блок 16 0	Блок 17 0	Блок 18 0
Блок 21 0	Блок 22 1	Блок 23 1	Блок 24 –1	Блок 25 –1	Блок 26 1	Блок 27 –1	Блок 28 0
Блок 31 0	Блок 32 0	Блок 33 1	Блок 34 1	Блок 35 –1	Блок 36 1	Блок 37 –1	Блок 38 –1
Блок 41 0	Блок 42 0	Блок 43 0	Блок 44 –1	Блок 45 –1	Блок 46 1	Блок 47 1	Блок 48 1
Блок 51 0	Блок 52 0	Блок 53 0	Блок 54 0	Блок 55 –1	Блок 56 –1	Блок 57 –1	Блок 58 1
Блок 61 0	Блок 62 0	Блок 63 0	Блок 64 0	Блок 65 0	Блок 66 1	Блок 67 1	Блок 68 –1
Блок 71 0	Блок 72 0	Блок 73 0	Блок 74 0	Блок 75 0	Блок 76 0	Блок 77 –1	Блок 78 1
Блок 81 0	Блок 82 0	Блок 83 0	Блок 84 0	Блок 85 0	Блок 86 0	Блок 87 0	Блок 88 1

Далі по рядках матриці Σ' зчитуємо послідовність переліку станів

$$\begin{gathered}S=\{1,1,-1,1,-1,0,0,0,0,1,1,-1,-1,1,-1,0,\\0,0,1,1,-1,1,-1,-1,0,0,0,-1,-1,1,1,1,\\0,0,0,0,-1,-1,-1,1,0,0,0,0,0,1,1,-1,\\0,0,0,0,0,0,-1,1,0,0,0,0,0,0,0,1\},\end{gathered}\tag{6.26}$$

яку шифруємо за допомогою блокового симетричного шифру, що оперує над алфавітом $\{0,\pm1\}$, в результаті чого отримуємо зашифровану послідовність переліку станів

$$\begin{gathered}E(S)=\{1,1,0,1,-1,0,0,-1,1,1,0,1,1,-1,1,0,\\-1,1,1,1,-1,0,1,1,1,1,1,-1,-1,0,1,0,\\0,0,0,1,1,0,1,0,-1,-1,1,1,0,-1,-1,-1,\\1,1,0,1,-1,0,0,-1,1,-1,-1,0,1,0,-1,1\}.\end{gathered}\tag{6.27}$$

На основі послідовності (6.27) будуємо матрицю Σ, представлену у табл. 6.8.

Таблиця 6.8. — Матриця Σ

Блок 11 1	Блок 12 1	Блок 13 0	Блок 14 –1	Блок 15 0	Блок 16 0	Блок 17 –1	Блок 18 1
Блок 21 1	Блок 22 1	Блок 23 0	Блок 24 1	Блок 25 1	Блок 26 –1	Блок 27 1	Блок 28 0
Блок 31 –1	Блок 32 1	Блок 33 1	Блок 34 1	Блок 35 –1	Блок 36 0	Блок 37 1	Блок 38 1
Блок 41 1	Блок 42 1	Блок 43 1	Блок 44 –1	Блок 45 –1	Блок 46 0	Блок 47 1	Блок 48 0
Блок 51 0	Блок 52 0	Блок 53 0	Блок 54 1	Блок 55 1	Блок 56 0	Блок 57 1	Блок 58 0
Блок 61 –1	Блок 62 –1	Блок 63 1	Блок 64 1	Блок 65 0	Блок 66 –1	Блок 67 –1	Блок 68 –1
Блок 71 1	Блок 72 1	Блок 73 0	Блок 74 1	Блок 75 –1	Блок 76 0	Блок 77 0	Блок 78 –1
Блок 81 1	Блок 82 –1	Блок 83 –1	Блок 84 0	Блок 85 1	Блок 86 0	Блок 87 –1	Блок 88 1

Матриця Σ (табл. 6.8.) визначатиме, яке кодове слово вбудовуватиметься (або не вбудовуватиметься) у відповідний блок зображення-контейнера.

Відзначимо переваги запропанованого підходу до вбудовування ДІ з шифруванням переліку станів блока:

1. при використанні підходу до вбудовування ДІ з шифруванням переліку станів блока, ДІ розподіляється як по тим блокам, у які відбувається її вбудовування, так і по тих, у які вбудовування не відбувається. Тобто, у такий спосіб стає можливим рівномірне розподілення ДІ по всьому зображенню-контейнеру, навіть якщо кількість ДІ менша за кількості блоків;

2. незалежно від кількості вбудованої ДІ (тобто від кількості блоків, в які вбудовуються кодові слова T^+ або T^-) ми отримуємо рівну ймовірність появи блоків в які вбудовано кодове слово T^+, T^- або вбудовування не

відбулося. Таким чином ми отримуємо максимальну невизначеність для супротивника: навіть якщо зловмисник отримає будь-яким способом оригінал зображення і зможе точно встановити в які блоки відбувалося вбудовування ДІ — він не зможе отримати інформацію навіть про те, скільки даних було вбудовано;

3. фактично відпадає необхідність зберігання довгого стеганошляху, так само як і необхідність у його формуванні, через те, що стеганошлях формується безпосередньо під час шифрування послідовності переліку станів;

4. для будь-якого зображення ми отримуємо однакові стандартні показники PSNR незалежно від кількості вбудованої ДІ, що є важливим під час використання потокового контейнеру задля уніфікації розподілення ДІ у кадрах потокового контейнеру та унеможливлення отримання інформації супротивником про розподілення ДІ у контейнері.

До можливих недоліків запропонованого підходу до вбудовування ДІ з шифруванням переліку станів блока можна віднести зменшення пропускної здатності прихованого каналу зв’язку у випадку, якщо кількість вбудовуваної ДІ значно менша кількості блоків зображення-контейнера, а також той факт, що стійкість стеганографічного методу із кодовим управлінням вбудовуванням до атак проти вбудованої ДІ може зменшуватися через невідомі позиції блоків, у які вбудовування ДІ не відбувалося, що, відповідно, приводить до необхідності їх локалізації під час вилучення ДІ.

Відзначимо при цьому, що для роботи зазначеного підходу до вбудовування ДІ з шифруванням переліку станів блока необхідним є використання криптографічних алгоритмів, що здатні оперувати над алфавітом $\{0,\pm1\}$, які можуть бути розроблені на основі результатів, представлених у Розділі 5.

6.4. Розроблення методів синтезу криптографічних примітивів на основі 3-функцій

6.4.1. Метод синтезу трійкових S-блоків з ідеальною матрицею коефіцієнтів кореляції

Розглянемо випадково згенерований S-блок довжини $N = 27$

$$S = [21\ \ 5\ \ 2\ \ 15\ \ 10\ \ 6\ \ 16\ \ 13\ \ 7\ \ 4\ \ 20\ \ 24\ \ 26\ \ 25\ \ 18\ \ 14\ \ 0\ \ 22\ \ 1\ \ 3\ \ 17\ \ 23\ \ 12\ \ 8\ \ 19\ \ 9\ \ 11], \tag{6.28}$$

для якого, відповідно до методики [27], обчислимо матрицю коефіцієнтів кореляції

$$\mathrm{P} = \begin{bmatrix} 0.11 & -0.22 & 0.11 \\ 0.11 & -0.06 & -0.06 \\ -0.16 & 0.06 & 0 \end{bmatrix}. \tag{6.29}$$

Як видно з (6.29), у даного випадково згенерованого S-блоку присутній кореляційний зв'язок між векторами виходу і входу, що спрощує завдання криптоаналітика.

Визначення 6.4.1 [27]. Нелінійне перетворення називається оптимальним, якщо всі його коефіцієнти кореляції дорівнюють нулю $\rho_{\nu,\mu} = 0, \quad \forall\, \nu, \mu = 1,2,...,k.$

Видається перспективною можливість реалізації двоетапної побудови S-блоків, яка запропонована в роботі [27]. На першому етапі генеруємо блок замін невеликої довжини, наприклад, довжини $N = 9$. На другому етапі, пропонується використання схеми Кіма [9], яка дозволяє з побудованих невеликих S-блоків отримати блоки потрібної довжини, при збереженні їх оптимальності.

У розділі 5 було встановлено зв’язок між критерієм незалежності виходу та входу S-блока та кореляційним імунітетом його компонентних q-функцій.

Наведемо результати щодо синтезу кореляційно імунних 3-функцій та S-блоків на їх основі.

Для дослідження кореляційного імунітету порядку $m=1$ для 3-функцій двох змінних розглянемо підфункції $m=1$ змінної, довжина таблиці істинності яких становить $N=3$.

Актуальною є задача розробки регулярного методу синтезу таких 3-функцій, вихід яких є незалежним від певної множини вхідних змінних. Представимо розроблений метод [28], який заснований на наступних правилах.

Правило 1. Синтез збалансованих ($\Delta=0$) 3-функцій довжини $N=9$, які є незалежними від входу x_1.

Розглянемо тривіальну монотонно зростаючу послідовність натуральних чисел від 0 до 2 $\alpha=\{012\}$. Сформуємо на її основі множину послідовностей довжини $N=9$ та потужності $J_1=6^2=36$ за наступним правилом

$$\mathrm{A}=\{P_i(\alpha)\quad P_j(\alpha)\quad P_l(\alpha)\},\quad i,j,l=1,...,6, \tag{6.30}$$

де P позначає операцію застосування однієї з шести перестановок елементів послідовності

$$P=\begin{Bmatrix}\{123\} & \{231\}\\ \{132\} & \{312\}\\ \{213\} & \{321\}\end{Bmatrix}. \tag{6.31}$$

Наприклад, вибираючи перестановки $P_i=P_j=P_1=\{123\}$, отримуємо першу послідовність, вихід якої не залежить від входу x_1

$$T_1=\{0\quad 1\quad 2\quad 0\quad 1\quad 2\quad 0\quad 1\quad 2\}. \tag{6.32}$$

Загальна кількість 3-функцій довжини $N=9$, вихід яких не залежить від входу x_1, які можуть бути синтезовані за допомогою *Правила 1* складає $J_1=6^3=216$, що становить повний клас таких послідовностей.

Правило 2. Синтез збалансованих ($\Delta = 0$) 3-функцій довжини $N = 9$, які є незалежними від входу x_2.

Повна множина 3-функцій, вихід яких не залежить від входу x_2 може бути побудована на основі повної множини 3-функцій, вихід яких не залежить від входу x_1 шляхом простої заміни змінних.

Розглянемо заміну змінних $x_1 \leftrightarrow x_2$ на прикладі послідовності (6.32)

$$\begin{array}{r|ccccccccc}
 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
x_1x_2 & 00 & 01 & 02 & 10 & 11 & 12 & 20 & 21 & 22 \\
f(x_1x_2) & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\
 & & & & & \Downarrow & & & & \\
 & 0 & 3 & 6 & 1 & 4 & 7 & 2 & 5 & 8 \\
x_2x_1 & 00 & 10 & 20 & 01 & 11 & 21 & 02 & 12 & 22 \\
f(x_1x_2) & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2
\end{array} . \qquad (6.33)$$

Таким чином, перестановка $P = \{0,3,6,1,4,7,2,5,8\}$ повністю визначає правило переходу від 3-функцій, вихід яких не залежить від входу x_1 до множини 3-функцій, вихід яких не залежить від входу x_2. Відповідно, потужність множини 3-функцій, вихід яких не залежить від входу x_2 дорівнює потужності множини 3-функцій, вихід яких не залежить від входу x_1 і дорівнює $J_2 = J_1 = 216$.

Правило 3. Синтез збалансованих ($\Delta = 0$) кореляційно-імунних порядку $m = 1$ 3-функцій довжини $N = 9$.

Синтез збалансованих кореляційно-імунних порядку $m = 1$ 3-функцій довжини $N = 9$ можна описати як послідовність наступних кроків.

Крок 1. Розглянемо монотонно зростаючу послідовність натуральних чисел від 0 до 2 $\alpha = \{012\}$, на основі якої сформуємо 6 послідовностей довжини $N = 9$ за допомогою наступних правил

$$\begin{aligned}
&\mathrm{A}_1 = \{\alpha \leftarrow (i+0) \quad \alpha \leftarrow (i+1) \quad \alpha \leftarrow (i+2)\}, \quad i \in \{0,1,2\}; \\
&\mathrm{A}_2 = \{\alpha \leftarrow (i+0) \quad \alpha \leftarrow (i+2) \quad \alpha \leftarrow (i+1)\}, \quad i \in \{0,1,2\},
\end{aligned} \qquad (6.34)$$

де символ $x \leftarrow l$ позначає оператор циклічного зсуву вектора x вправо на величину l. Всього на *Кроці 1* ми отримуємо 6 кореляційно-імунних 3-функцій.

Крок 2. До отриманих на *Кроці 1* послідовностей застосовуємо операцію заміни символів $\{1 \leftrightarrow 2, 2 \leftrightarrow 1\}$, таким чином отримуючи з кожної кореляційно-імунної 3-функції 2 кореляційно-імунні 3-функції.

Виконуючи *Крок 1* і *Крок 2*, загальна кількість отриманих кореляційно-імунних 3-функцій становить $J_3 = 2 \cdot 6 = 12$.

Правила синтезу не збалансованих 3-функцій, вихід яких є незалежним від їх вхідних змінних, наведені в роботі [28]. Тим не менш, найбільший інтерес, з точки зору конструювання S-блоків, представляють збалансовані 3-функції. Проведені дослідження дозволили встановити, що конструювання повної множини S-блоків можливо на основі 44-х 3-функцій, серед яких 12 3-функцій, вихід яких не залежить від входу x_1

$$\begin{array}{l}\{012120120\}\ \{021021210\}\ \{102102210\}\\ \{012201201\}\ \{021210021\}\ \{102210102\}\\ \{120012120\}\ \{201012201\}\ \{210021021\},\\ \{120120012\}\ \{201201012\}\ \{210102102\}\end{array} \qquad (6.35)$$

вихід ще 12 3-функцій є незалежним від входу x_2

$$\begin{array}{l}\{002221110\}\ \{020212101\}\ \{101212020\}\\ \{011122200\}\ \{022100211\}\ \{110221002\}\\ \{112001220\}\ \{200122011\}\ \{211100022\}.\\ \{121010202\}\ \{202010121\}\ \{220001112\}\end{array} \qquad (6.36)$$

Крім цього до складу повної множини S-блоків довжини $N = 9$, що володіють ідеальними кореляційними матрицями входить 12 кореляційно-імунних 3-функцій порядку $m = 1$

$$\begin{array}{l}\{012120201\}\ \{021102210\}\ \{102021210\}\\ \{012201120\}\ \{021210102\}\ \{102210021\}\\ \{120012201\}\ \{201012120\}\ \{210021102\},\\ \{120201012\}\ \{201120012\}\ \{210102021\}\end{array} \qquad (6.37)$$

а також 8 3-функцій загального вигляду (вихід яких є кореляційно залежним від кожного з входів)

$$\begin{array}{l}\{011221020\}\ \{020221011\}\ \{112100202\}\ \{202100112\}\\ \{020122110\}\ \{110122020\}\ \{202001211\}\ \{211001202\}.\end{array} \quad (6.38)$$

Проведені дослідження повної множини з $J = 264$ S-блоків довжини $N = 9,$ що володіють ідеальними матрицями коефіцієнтів кореляції, дозволили сформулювати наступне твердження.

Твердження 6.4.1. Для того, щоб S-блок довжини $N = 9$ володів ідеальною матрицею коефіцієнтів кореляції, необхідно і достатньо, щоб виконувалася одна з вимог:

1. Обидві його компонентні 3-функції повинні бути незалежні від вхідної змінної x_1 або x_2.

2. Хоча-б одна з його компонентних 3-функцій повинна бути кореляційно-імунною порядку $m = 1.$

На основі **Твердження 6.4.1.** повна множина з $J = 264$ S-блоків довжини $N = 9$ може бути класифікована на п'ять класів:

1. S-блоки, у яких вихід першої і другої компонентних 3-функцій є незалежними від входу x_1, потужність даного класу S-блоків становить $J_{S1} = 48$

$$\begin{array}{l}\{057624813\}\ \{318426750\}\ \{615237804\}\\ \{057813624\}\ \{318750426\}\ \{615804237\}\\ \{075264831\}\ \{372480156\}\ \{624057813\}\\ \{075831264\}\ \{372156480\}\ \{624813057\}\\ \{084273651\}\ \{426318750\}\ \{651273084\}\\ \{084651273\}\ \{426750318\}\ \{651084273\}\\ \{138462570\}\ \{408516732\}\ \{732408516\}\\ \{138570462\}\ \{408732516\}\ \{732516408\}\\ \{156372480\}\ \{462570138\}\ \{750318426\}.\\ \{156480372\}\ \{462138570\}\ \{750426318\}\\ \{237615804\}\ \{480372156\}\ \{813624057\}\\ \{237804615\}\ \{480156372\}\ \{813057624\}\\ \{264075831\}\ \{516408732\}\ \{831264075\}\\ \{264831075\}\ \{516732408\}\ \{831075264\}\\ \{273084651\}\ \{570462138\}\ \{804237615\}\\ \{273651084\}\ \{570138462\}\ \{804615237\}\end{array} \quad (6.39)$$

2. S-блоки, у яких вихід першої і другої компонентних 3-функцій є незалежними від входу x_2, потужність даного класу S-блоків становить $J_{S2} = 48$

$$\begin{array}{l}
\{026875431\}\ \{314758260\}\ \{620578134\} \\
\{028763541\}\ \{341785206\}\ \{628130574\} \\
\{062857413\}\ \{347125860\}\ \{602587143\} \\
\{068521743\}\ \{374152806\}\ \{608251473\} \\
\{082736514\}\ \{413857062\}\ \{682103547\} \\
\{086512734\}\ \{415637280\}\ \{680215437\} \\
\{134578620\}\ \{431875026\}\ \{734512086\} \\
\{143587602\}\ \{437215680\}\ \{743521068\} \\
\{145367820\}\ \{451673208\}\ \{745301286\}. \\
\{154376802\}\ \{457013862\}\ \{754310268\} \\
\{206785341\}\ \{473251608\}\ \{826031475\} \\
\{208673451\}\ \{475031826\}\ \{820367145\} \\
\{260758314\}\ \{514736082\}\ \{862013457\} \\
\{268310754\}\ \{541763028\}\ \{860125347\} \\
\{280637415\}\ \{547103682\}\ \{802376154\} \\
\{286301745\}\ \{574130628\}\ \{806152374\}
\end{array} \qquad (6.40)$$

3. S-блоки, у яких перша компонентна 3-функція є кореляційно-імунною порядку $m = 1$, а друга компонентна 3-функція є функцією загального вигляду (вихід якої є кореляційно залежним від кожного з входів), потужність даного класу S-блоків становить $J_{S3} = 48$

$$\begin{array}{l}
\{047581623\}\ \{317284650\}\ \{614257380\} \\
\{056482713\}\ \{326185740\}\ \{623158470\} \\
\{056824371\}\ \{326851074\}\ \{623581047\} \\
\{074851326\}\ \{371824056\}\ \{641527083\} \\
\{083527641\}\ \{380257614\}\ \{650428173\} \\
\{083752416\}\ \{380725146\}\ \{650284317\} \\
\{146725380\}\ \{416752083\}\ \{713482056\} \\
\{148703562\}\ \{418730265\}\ \{715460238\} \\
\{173428650\}\ \{472136805\}\ \{742163508\}. \\
\{175406832\}\ \{470158623\}\ \{740185326\} \\
\{238460715\}\ \{517064832\}\ \{814037562\} \\
\{238604571\}\ \{508163742\}\ \{832406175\} \\
\{247361805\}\ \{508631274\}\ \{832064517\} \\
\{265307841\}\ \{562037814\}\ \{841307265\} \\
\{265730418\}\ \{562703148\}\ \{805361247\} \\
\{274631508\}\ \{571604238\}\ \{805136472\}
\end{array} \qquad (6.41)$$

4. S-блоки, у яких перша компонентна 3-функція є функцією загального вигляду (вихід якої є кореляційно залежним від кожного з входів), а друга

компонентна 3-функція є кореляційно-імунною порядку $m=1$, потужність даного класу S-блоків становить $J_{S4}=48$

$$\begin{array}{l}
\{045783261\}\{270468351\}\{627510438\}\\
\{054873162\}\{270684135\}\{627105843\}\\
\{072486531\}\{342567180\}\{645123807\}\\
\{072864153\}\{348501726\}\{654213708\}\\
\{081576432\}\{351468270\}\{726501348\}\\
\{081765243\}\{357402816\}\{726015834\}\\
\{135684270\}\{432576081\}\{735024816\}\\
\{153864072\}\{438510627\}\{753204618\}\\
\{162387540\}\{450378261\}\{708321546\}\\
\{162873054\}\{456312807\}\{708213654\}\\
\{180567342\}\{531486072\}\{816402357\}\\
\{180675234\}\{537420618\}\{816024735\}\\
\{234675180\}\{540387162\}\{834015726\}\\
\{243765081\}\{546321708\}\{843105627\}\\
\{261378450\}\{618420537\}\{807312456\}\\
\{261783045\}\{618204753\}\{807123645\}
\end{array}. \qquad (6.42)$$

5. S-блоки, у яких обидві компонентні 3-функції є кореляційно-імунними порядку $m=1$, потужність даного класу S-блоків становить $J_{S4}=72$

$$\begin{array}{l}
\{048561723\}\{318750264\}\{615480237\}\\
\{048723561\}\{318264750\}\{615237480\}\\
\{057462813\}\{327165840\}\{624138570\}\\
\{057813462\}\{327840165\}\{624570138\}\\
\{075426831\}\{372156804\}\{642183507\}\\
\{075831426\}\{372804156\}\{642507183\}\\
\{084516732\}\{381705246\}\{651408273\}\\
\{084732516\}\{381246705\}\{651273408\}\\
\{138570624\}\{426075831\}\{723561048\}\\
\{138624570\}\{426831075\}\{723048561\}\\
\{156372804\}\{408651273\}\{732516084\}\\
\{156804372\}\{408273651\}\{732084516\}\\
\{165327840\}\{462057813\}\{750318264\}\\
\{165840327\}\{462813057\}\{750264318\}\\
\{183507642\}\{480237615\}\{705381246\}\\
\{183642507\}\{480615237\}\{705246381\}\\
\{237480615\}\{516084732\}\{813462057\}\\
\{237615480\}\{516732084\}\{813057462\}\\
\{246381705\}\{507183642\}\{831426075\}\\
\{246705381\}\{507642183\}\{831075426\}\\
\{264318750\}\{561048723\}\{840327165\}\\
\{264750318\}\{561723048\}\{840165327\}\\
\{273408651\}\{570624138\}\{804372156\}\\
\{273651408\}\{570138624\}\{804156372\}
\end{array}. \qquad (6.43)$$

Очевидно, що S-блоки (6.43) є найбільш стійкими до кореляційного криптоаналізу, оскільки їх вихід є незалежним одночасно від кожної з вхідних змінних. Дані S-блоки можуть бути рекомендовані до практичного використання в додатках, де необхідна максимальна незалежність виходу криптографічних конструкцій від їх входу.

6.4.2. Модифікація схеми Кіма для збільшення довжини оптимальних S-блоків

Схема Кіма в загальному вигляді представлена на рис. 6.6.

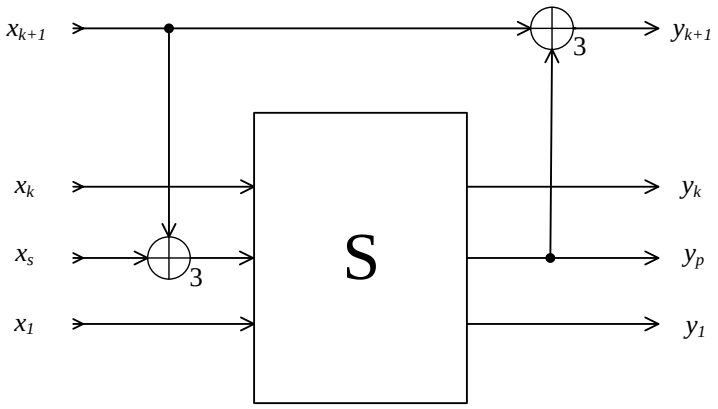


Рис. 6.6. — Схема Кіма

Приклад. Розглянемо один із побудованих вище оптимальних S-блоків довжини $N = 3^2 = 9$

$$S_9 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 0 & 2 & 6 & 8 & 7 & 5 & 4 & 3 & 1 \end{pmatrix}. \tag{6.44}$$

Обчислюючи його матрицю коефіцієнтів кореляції, отримуємо

$$\mathrm{P} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}. \tag{6.45}$$

Застосуємо до S-блока (6.44) схему рекурентного збільшення довжини (рис. 6.6.), яка, з огляду на довжину вихідного S-блока $N = 9$ і довжину необхідного S-блока $N = 27$ набуває вигляду (рис. 6.7).

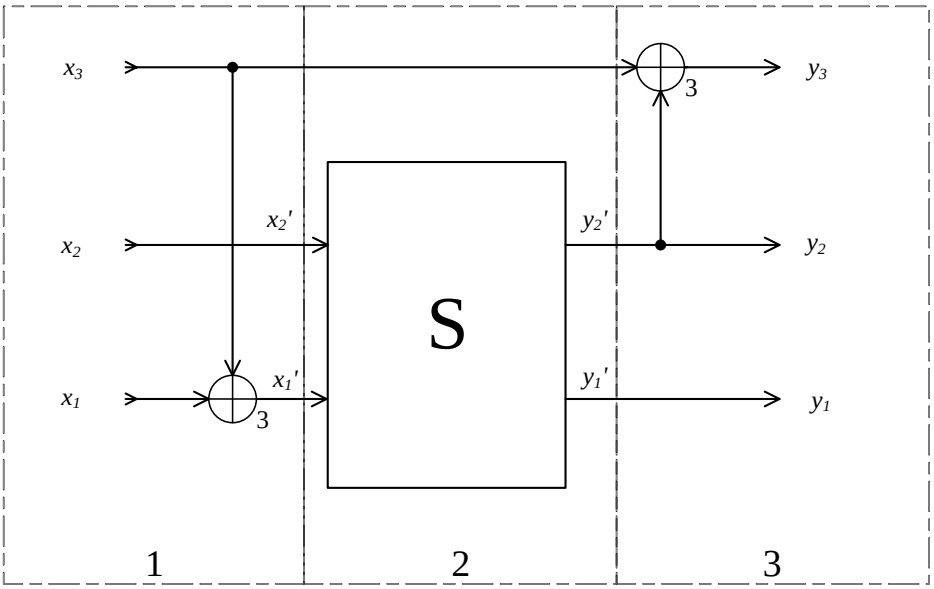


Рис. 6.7. — Схема Кіма для S-блока з двома входами

Розглянемо приклад роботи схеми Кіма за допомогою обчислення вихідних значень на конкретних ітераціях.

Значення нового S-блока на ітерації 0. Нехай на вхід схеми (рис. 6.7.) надійшло поєднання вихідних даних $X = (x_1, x_2, x_3)$

$$x_1 = 0, \quad x_2 = 0, \quad x_3 = 0 \quad \Rightarrow \quad X = 0, \tag{6.46}$$

тоді, обчислюючи суму в першому підблоку обчислень, отримуємо

$$x_1' = x_1 + x_3 = 0 + 0 = 0, \quad x_2' = 0, \tag{6.47}$$

після перетворення, у другому підблоці

$$S_9(0,0) = S_9(0) = 0, \; y_1' = 0, \quad y_2' = 0. \tag{6.48}$$

І нарешті, обчислення в третьому підблоці схеми

$$y_1 = y_1' = 0, \quad y_2 = y_2' = 0, \quad y_3 = x_3 + y_2' = 0 + 0 = 0 \quad \Rightarrow \quad S_{27}(0) = 0. \tag{6.49}$$

Покажемо обчислення значення нового S-блока на ще одній ітерації, наприклад, на ітерації 19. Нехай на вхід схеми (рис. 6.7.) надійшло поєднання вихідних даних $X = (x_1, x_2, x_3)$

$$x_1 = 1, \quad x_2 = 0, \quad x_3 = 2 \quad \Rightarrow \quad X = 19. \tag{6.50}$$

Тоді, обчислюючи суму в першому підблоці обчислень отримуємо

$$x_1' = x_1 + x_3 = 1 + 2 = 0, \quad x_2' = 0. \tag{6.51}$$

Після перетворення, у другому підблоці

$$S_9(0,0) = S_9(0) = 0,\ y_1' = 0,\quad y_2' = 0, \tag{6.52}$$

і нарешті, обчислення в третьому підблоці схеми

$$y_1 = y_1' = 0,\quad y_2 = y_2' = 2,\quad y_3 = x_3 + y_2' = 2 + 0 = 2 \quad \Rightarrow \quad S_{27}(19) = 18. \tag{6.53}$$

Таким чином, проводячи всі ітерації, в результаті отримуємо необхідний S-блок S_{27} довжини $N = 27$

$$S_{27} = [0,2,24,26,25,14,13,12,1,9,11,6,8,7,23,22,21,10,\\ 18,20,15,17,16,5,4,3,19]. \tag{6.54}$$

Відповідно до [27] отримуємо матрицю коефіцієнтів кореляції даного S-блока

$$R = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \tag{6.55}$$

що підтверджує відповідність S-блока (6.54) визначенню оптимальності [27].

Таким чином, наведемо алгоритм синтезу S-блоків, оптимальних за критерієм нульової кореляції між векторами виходу і входу.

Крок 1. Синтезувати всі S-блоки малої довжини $N = 9$, що відповідають критерію нульової кореляції між векторами виходу і входу.

Крок 2. Застосовуючи схему Кіма (рис. 6.6.) збільшити довжину S-блока в 3 рази. Відзначимо, що при цьому з'єднання в схемі Кіма можуть бути виконані k^2 різними способами.

Крок 3. Провести розмноження отриманої множини S-блоків, ґрунтуючись на збереженні оптимальності при перестановці стовпців в зворотному порядку. Таким чином, потужність нової множини буде $J_{3^{k+1}} = 2k^2 J_{3^k}$.

Крок 4. Якщо досягнута необхідна довжина S-блока, завершити роботу алгоритму, інакше перейти до *Кроку 2*.

Застосування рекурентного збільшення довжини дає змогу отримати оптимальні S-блоки будь-якої довжини $N = 3^k, k \in \mathbb{N}$. Відзначимо, що

використовуючи повну множину з $|\Omega_9| = 264$ S-блоків довжини $N = 9$, розробленим методом ми можемо отримати $2 \cdot 4 \cdot 264 = 2112$ S-блоків довжини $N = 27$, $2 \cdot 9 \cdot 2112 = 38016$ S-блоків довжини $N = 81$, $2 \cdot 16 \cdot 38016 = 1216512$ S-блоків довжини $N = 243$ і т.д.

Наприклад, після триразового застосування схеми Кіма отримаємо з вихідного S-блока наступний, який також є оптимальним

$$S_{243} = \{0,81,162,80,161,242,12,93,174,230,68,149,218,56,137,214,52,\\ 133,105,186,24,121,202,40,109,190,28,3,84,165,74,155,236,15,\\ 96,177,233,71,152,221,59,140,208,46,127,99,180,18,124,205,\\ 43,112,193,31,6,87,168,77,158,239,9,90,171,227,65,146,224,\\ 62,143,211,49,130,102,183,21,118,199,37,115,196,34,1,82,163,\\ 78,159,240,13,94,175,228,66,147,216,54,135,215,53,134,106,\\ 187,25,122,203,41,110,191,29,4,85,166,72,153,234,16,97,178,\\ 231,69,150,219,57,138,209,47,128,100,181,19,125,206,44,113,\\ 194,32,7,88,169,75,156,237,10,91,172,225,63,144,222,60,141,\\ 212,50,131,103,184,22,119,200,38,116,197,35,2,83,164,79,160,\\ 241,14,95,176,229,67,148,217,55,136,213,51,132,107,188,26,\\ 120,201,39,108,189,27,5,86,167,73,154,235,17,98,179,232,70,\\ 151,220,58,139,207,45,126,101,182,20,123,204,42,111,192,30,\\ 8,89,170,76,157,238,11,92,173,226,64,145,223,61,142,210,48,\\ 129,104,185,23,117,198,36,114,195,33\}. \quad (6.56)$$

Наступна ітерація дозволить отримати S-блок розміром $3^6 = 729$.

Існує можливість опрацювання S-блока у будь-якому поданні: у вигляді десяткового числа або у вигляді трійкового, а після виконання замін перехід (при необхідності) до двійкового (бітового) формату. Отримавши множину S-блоків з нульовими коефіцієнтами кореляції вихідних і вхідних векторів, можна вибрати з них S-блоки з максимально можливою нелінійністю, або ж ранжувати їх за іншими критеріями криптографічної якості.

Зауваження 1. Проведені міркування і обчислення з досить очевидними змінами можна провести для будь-якого простого q. При цьому чим більше q, тим менша кількість ітерацій потрібна для побудови блоків порівнянної довжини.

Так, наприклад, для побудови сімейства S-блоків підстановки довжини $N = 5^k$ може бути використаний первинний оптимальний S-блок

$$S_{25} = \{15,8,6,17,13,24,5,20,4,18,3,11,9,22,2,1,7,21,16,12,14,23,10,19,0\}. \quad (6.57)$$

6.4.2. Конструкція Ніберг над ізоморфними уявленнями полів Галуа характеристики $p = 3$

В цілому, S-блоки конструкції Ніберг володіють високою відстанню нелінійності, наближаються до відповідності критеріям розповсюдження помилки та рівномірного розподілу коефіцієнтів кореляції векторів виходу та входу.

Таким чином, S-блоки конструкції Ніберг ідеально підходять для застосування в криптоалгоритмах, заснованих на принципах багатозначної логіки. Відповідно, актуальною є задача конструювання їх множин і докладного вивчення їх криптографічних властивостей.

Одним з небагатьох недоліків конструкції Ніберг є мала кількість S-блоків, які можуть бути отримані таким методом. У полях $GF(2^k)$ даний недолік вдалося усунути шляхом розгляду всіх ізоморфних уявлень даного поля, при цьому криптографічні властивості побудованих S-блоків залишаються стабільними. Далі в цьому розділі показано, що такий підхід може бути поширений і на поля непарної характеристики. При цьому основні отримані результати по синтезу S-блоків конструкції Ніберг над усіма ізоморфними уявленнями трійкових полів Галуа наведено в роботі [29].

Як відомо, поля $GF(3^k)$ також можна представити у вигляді різних ізоморфних уявлень. Розглянемо поля $GF(3^k)$ і всі їх ізоморфні уявлення для значень $k = 2,3,4,5,6,7$, що відображає практично цінні довжини S-блоків. З урахуванням нових видів уявлення основного поля $GF(3^k)$, виходячи з [30], вираз, що визначає конструкцію Ніберг, набирає вигляду

$$y = x^{-1}\text{moddd}[f_1(z), f_2(z), p], \quad y, x \in GF(3^k), \quad (6.58)$$

де $f_1(z)$ — незвідний поліном, що визначає операцію мультиплікативного обернення в полі «нижнього рівня» $GF(q)$, $f_2(z)$ — в полі «верхнього рівня»,

тобто в розширенні поля $GF(q^k)$. Різні уявлення основного поля $GF(3^k)$, а також кількості нормованих незвідних і первісних поліномів, що існують в даних полях, наведені в табл. 6.9.

Таблиця 6.9. — Потужності множин незвідних і первісних поліномів над полями $GF(3^k)$

Основне поле	Можливі ізоморфні уявлення	Кількість незвідних поліномів	Кількість первісних поліномів	Загальна кількість S-блоків конструкції Ніберг
$GF(3^2)$	$GF(3^2)$	3	2	3
$GF(3^3)$	$GF(3^3)$	8	4	8
$GF(3^4)$	$GF(3^4) \Rightarrow GF(9^2)$	$18 \Rightarrow 36$	$8 \Rightarrow 16$	54
$GF(3^5)$	$GF(3^5)$	48	22	48
$GF(3^6)$	$GF(3^6), GF(9^3), GF(27^2)$	$116 \Rightarrow 240 \Rightarrow 351$	$48 \Rightarrow 96 \Rightarrow 144$	2000

Незвідні і первісні поліноми для полів $GF(3^k)$ отримано в роботі [31], знаходити поліноми для полів $GF(9^k)$ і $GF(27^k)$ можна з використанням методу, який розроблений у [32]. Нормовані незвідні і первісні поліноми максимального степеню наведені в табл. 6.10.

Таблиця 6.10. — Незвідні і первісні поліноми

Поле	Поліном $f_1(z)$	Поліноми $f_2(z)$
$GF(9^2)$	$f_1(z) = x^2 + x + 2$	84,86,87,88,**93**,94,**97**,98,**102**,103,**106**,107,109,110,**114**,**115**,121,**122**,**123**,125,127,128,**129**,**131**,136,137,**141**,**142**,145,146,**147**,**149**,157, **158**,**159**,161
	$f_1(z) = x^2 + 2x + 2$	84,85,87,89,**94**,95,**96**,97,**103**,104,**105**,106,109,110,**111**,**112**,118,119,**123**,**125**,**129**,131,133,**134**,136,137,**138**,**139**,**147**,149,151,**152**,154,155,**159**,**161**

Закінчення табл. 6.10

$GF(9^3)$	$f_1(z)=x^2+x+2$	**741**,742,**743**,**744**,**745**,746,748,749,**750**,**752**,**753**,**754**, 766,767,768,769,771,773,802,803,805,806,808,809, 812,814,818,821,823,827,829,**831**,**835**,838,**842**,845, 848,**851**,**853**,856,**858**,862,865,867,**871**,874,877,**879**, 884,**885**,**888**,892,895,899,901,904,908,911,**914**,**915**, 920,922,**925**,928,**932**,**934**,938,941,**942**,947,**950**,951, 956,**957**,962,964,**966**,**969**,**975**,977,**978**,982,983,**986**, 994,**995**,998,1001,**1006**,1007,**1011**,1013,**1014**,1019,**1** **024**,1025,1027,**1032**,**1033**,**1038**,1039,**1042**,1046,1051 ,1052,1054,1055,1057,**1065**,**1067**,1070,1072,1073,10 75,**1083**,1085,1088,1093,**1094**,**1096**,1099,**1105**,1106, 1109,**1113**,1115,1119,**1121**,1124,**1128**,1129,**1131**,113 7,**1139**,**1141**,1144,1145,**1146**,**1155**,1156,1160,1165,**1** **166**,**1167**,1171,1176,1178,1181,**1185**,**1186**,1189,**1194** ,1196,1198,**1203**,1205,1209,**1211**,**1213**,**1218**,**1221**,12 22,1225,1226,**1231**,1237,**1240**,1241,1243,1246,**1247**, **1254**,**1257**,1258,1261,1264,**1265**,1271,**1272**,**1274**,**128** **3**,**1284**,1286,1288,1291,1292,**1301**,1302,**1303**,1306,1 307,**1311**,1318,**1320**,1322,**1326**,**1330**,1331,1334,1335 ,1336,1342,**1344**,**1346**,1352,**1353**,1354,1361,**1362**,13 63,**1373**,1374,**1375**,1378,1379,1385,1390,**1392**,**1393**, 1396,1397,1403,1408,**1410**,1411,**1418**,**1420**,1421,142 4,1426,**1427**,1432,**1434**,1435,1444,1446,**1447**,**1452**,**1** **455**,1457
	$f_1(z)=x^2+2x+2$	**741**,**742**,743,**744**,745,**746**,748,749,**750**,**751**,**753**,**755**, 775,776,778,779,781,782,793,794,795,797,798,799, 812,815,817,821,824,826,829,**832**,**834**,838,**841**,843, 847,**849**,853,857,**858**,**861**,865,869,**872**,875,**877**,**881**, 883,886,**888**,892,896,898,901,905,907,911,**912**,**917**, 920,921,**926**,929,932,**933**,937,**939**,**942**,947,**949**,952, 955,**958**,**962**,965,**966**,971,**975**,976,**978**,982,983,**985**, **994**,995,997,1001,**1005**,**1007**,**1011**,1013,**1016**,1018,1 024,1025,1027,1033,**1034**,**1038**,1039,**1041**,1045,1051 ,**1052**,1056,**1057**,**1061**,1063,1064,**1065**,**1074**,1076,10 78,1082,**1086**,1087,1091,**1095**,1096,1101,**1102**,**1106**, **1111**,1112,**1113**,1118,1122,1123,1126,**1131**,**1133**,113 5,1136,1139,**1146**,**1147**,1150,1153,1154,1157,1162,**1** **167**,1168,1173,**1174**,1177,**1182**,1184,**1185**,**1191**,1192 ,1195,**1201**,1202,**1205**,1208,1213,**1214**,**1218**,**1221**,12 23,1225,1226,**1232**,1238,1240,**1241**,1243,**1245**,**1246**, **1255**,**1257**,1258,1262,1264,1265,1271,**1273**,1274,**128** **1**,**1284**,1286,1289,**1291**,1292,1297,1298,1303,1310,**1** **311**,**1313**,1315,1316,1321,1325,**1326**,1328,1337,1338 ,**1340**,**1344**,**1347**,1348,1355,**1356**,1358,**1363**,1366,**13** **67**,1369,**1372**,1373,**1381**,1383,**1385**,1387,1388,**1392**, 1400,**1401**,1402,1405,**1407**,1409,1414,**1416**,1418,**142** **6**,1428,**1430**,**1434**,1438,**1439**,1441,1443,1445,1451,**1** **452**,**1453**

Наведемо приклад дослідження нелінійних властивостей S-блока підстановки довжини $N=81$. Побудуємо S-блок над полем $GF(9^2)$ на основі (6.58) і поліномів $f_1(z)=x^2+x+2$, $f_2(z)=107_{10}=x^2+2x+8$

$$Q=\{0\ \ 1\ \ 2\ \ 5\ \ 8\ \ 3\ \ 7\ \ 6\ \ 4\ 37\ 49\ 21\ 67\ 59\ 65\ 19\ 50\ 36\ 74$$
$$15\ 71\ 11\ 72\ 70\ 53\ 46\ 34\ 32\ 43\ 80\ 75\ 39\ 27\ 64\ 26\ 68\ 17\ \ 9$$
$$69\ 31\ 55\ 44\ 60\ 28\ 41\ 66\ 25\ 57\ 73\ 10\ 16\ 63\ 58\ 24\ 61\ 40 \quad (6.59)$$
$$77\ 47\ 52\ 13\ 42\ 54\ 78\ 51\ 33\ 14\ 45\ 12\ 35\ 38\ 23\ 20\ 22\ 48$$
$$18\ 30\ 79\ 56\ 62\ 76\ 29\}.$$

Уявімо S-блок підстановки (6.59) у вигляді компонентних 3-функцій

$$f_1=\{00000000011022201120202211111221120200212121$$
$$12022002202121101221101011000101222 21\};$$
$$f_2=\{00000000012210122121112122001221012111100100$$
$$11202111020122211022012101222220200 20\};$$
$$f_3=\{00012122101111001002200220212211002120210220 \quad (6.60)$$
$$11210020122110212022210120101101202 10\};$$
$$f_4=\{01222010111012212020220121121200012220011201$$
$$20101110101122110000020022221000122 12\}.$$

Для кожної з 3-функцій (6.60) знайдемо коефіцієнти перетворення Віленкіна-Крестенсона. Наприклад, модулі спектральних коефіцієнтів перетворення Віленкіна-Крестенсона першої компонентної 3-функції мають вигляд

$$S_1=\{0\ \ 9\ \ 0\ \ 3\ \ 6\ 12\ \ 6\ 12\ \ 6\ 15\ \ 3\ \ 6\ \ 9\ \ 9\ \ 9\ 15\ 12\ \ 3$$
$$6\ \ 6\ \ 3\ \ 3\ \ 3\ 12\ 9\ \ 9\ \ 0\ \ 3\ \ 3\ \ 6\ 12\ 6\ \ 3\ \ 9\ \ 9\ \ 9\ 18\ \ 9$$
$$9\ 12\ \ 3\ \ 3\ \ 3\ \ 3\ 15\ 15\ 15\ \ 3\ \ 9\ 0\ \ 9\ \ 3\ \ 3\ \ 3\ 15\ 6\ 15\ \ 9 \quad (6.61)$$
$$9\ \ 9\ 12\ 15\ \ 6\ \ 3\ \ 3\ \ 3\ \ 6\ 15\ \ 6\ \ 9\ \ 9\ \ 9\ 18\ \ 0\ \ 9\ \ 15\ \ 3$$
$$15\ 12\ \ 6\ \ 3\}.$$

Для S-блока (6.59) максимум модуля по всім трансформантам Віленкіна-Крестенсона дорівнює $L=\max\{S\}=18$, і можливо обчислити коефіцієнт нелінійності по формулі $NL=q^k-\max\left\{\left|S\right|\right\}=3^4-18=63$, що складає 87.5% від максимального значення, оскільки для даної довжини коефіцієнт нелінійності бент-функцій дорівнює $NL_{\max}=3^4-\sqrt{3^4}=72$.

У табл. 6.11. представлені коефіцієнти нелінійності NL і коефіцієнти кореляції векторів виходу і входу ρ трійкових S-блоків конструкції Ніберг над різними ізоморфними уявленнями полів $GF(3^k)$.

Таблиця 6.11. — Якість S-блоків конструкції Ніберг над полями $GF(3^k)$

Поле	Ізоморфне уявлення		*NL*	ρ
$GF(3^2)$	$GF(3^2)$		3	0.8333
$GF(3^3)$	$GF(3^3)$		18	0.2222…0.3333
$GF(3^4)$	$GF(3^4)$		63	0.1667… 0.3333
	$GF(9^2)$		63	0.2037…0.3333
$GF(3^5)$	$GF(3^5)$		213	0.0617…0.1543
$GF(3^6)$	$GF(3^6)$		675	0.0453…0.0986
	$GF(9^3)$	Поліном $GF(9)\ x^2+x+2$	675	0.0432…0.0967
		Поліном $GF(9)\ x^2+2x+2$	675	0.0514…0.0967
	$GF(27^2)$	Поліном $GF(27)\ x^3+2x+1$	675	0.0885…0.0967
		Поліном $GF(27)\ x^3+x^2+2x+1$	675	0.0761…0.0967
		Поліном $GF(27)\ x^3+2x^2+1$	675	0.0885…0.0967
		Поліном $GF(27)\ x^3+2x^2+x+1$	675	0.0761…0.0967

Важливо зауважити, що коефіцієнти кореляції можуть відрізнятися для різних уявлень одного поля.

6.5. Концептуальна модель побудови блокового симетричного криптоалгоритма на основі ФБЛ

Описаний далі алгоритм шифрування характеризується динамічною зміною розмірів криптографічних примітивів в різних раундах та застосуванням ФБЛ.

Іншими словами, пропонується проводити зашифрування тексту, застосовуючи заміни за таблицями різних розмірів в різних раундах.

В даний час широко застосовується генерація високоякісних S-блоків в полі Галуа $GF(p^k)$, $k \in \mathbb{N}$, де k — розмір вхідного слова S-блока. При цьому найчастіше використовується поле характеристики $p = 2$. Перехід до характеристик $p > 2$ представляє інтерес як з дослідницької точки зору, так і з практичної. Наприклад, як показано в [27], конструювання таблиць замін в полі $GF(3^k)$ має свої особливості. Для полів характеристики $p > 3$ сказане справедливо в ще більшій мірі.

Для найбільш ефективної організації алгоритму шифрування з динамічною зміною розмірів криптографічних примітивів вибір довжини вхідного блоку алгоритму повинен бути складеним числом. Під час розробки концепції шифрування зі змінною фрагментацією блоків було розглянуто розмір блоку $L = 120 = 2^3 \cdot 3 \cdot 5$ біт. Розбиття даного блоку відкритого тексту в алгоритмі шифрування може бути проведено різними способами, наприклад, на сегменти зручної, з обчислювальної точки зору, довжини $\sigma = 6,8,10,12,15,20,30$ біт, при цьому в межах одного раунду розмір сегмента не змінюється.

Далі, під час викладення прикладу побудови алгоритму шифрування [33] на основі ФБЛ ми показуємо обчислювальні експерименти для трійкового випадку, а саме, для блоку довжини $N = 240$ тріт, тим не менше

отримані результати можуть бути легко поширені на інші алфавіти і довжини блоків.

Запропонований алгоритм шифрування включає 3 основні процедури: підстановки, перестановки, гамування. Послідовно опишемо кожну з даних процедур, які є оборотними, і тому використовуються як в алгоритмі шифрування, так і в алгоритмі розшифрування.

6.5.1. Алгоритм шифрування і розшифрування

Шифрування виконується ітеративно, при цьому допускається варіювати кількість раундів. Раундове перетворення складається з реалізації процедур гамування, підстановки або перестановки. Базова версія алгоритму шифрування включає в себе п'ять раундів, перший раунд складається з процедур гамування та перестановки, в той час як інші раунди включають процедури підстановки і гамування. Схема запропонованого алгоритму шифрування приведена на рис. 6.8.

Алфавіт: $A=\{0,1,...,q-1\}$, $q>2$. У цьому розділі ми детально розглянемо випадок $q=3$.

Вихідний текст: $\{x_i\}$, $i=0,1,...N-1$. У цьому розділі ми розглядаємо $N=240$.

Ключем є: $K=\{g_i,Q_l,E,a_i\}$, де a_i — змінні розбиття, які вибираються різними для кожної процедури, яка є частиною раунду шифрування; Q_l — послідовності підстановки; E — послідовність перестановки; $\{g_i\}$ — гамма послідовність.

Вихідний текст: $\{y_i\}$, $i=0,1,...N-1$.

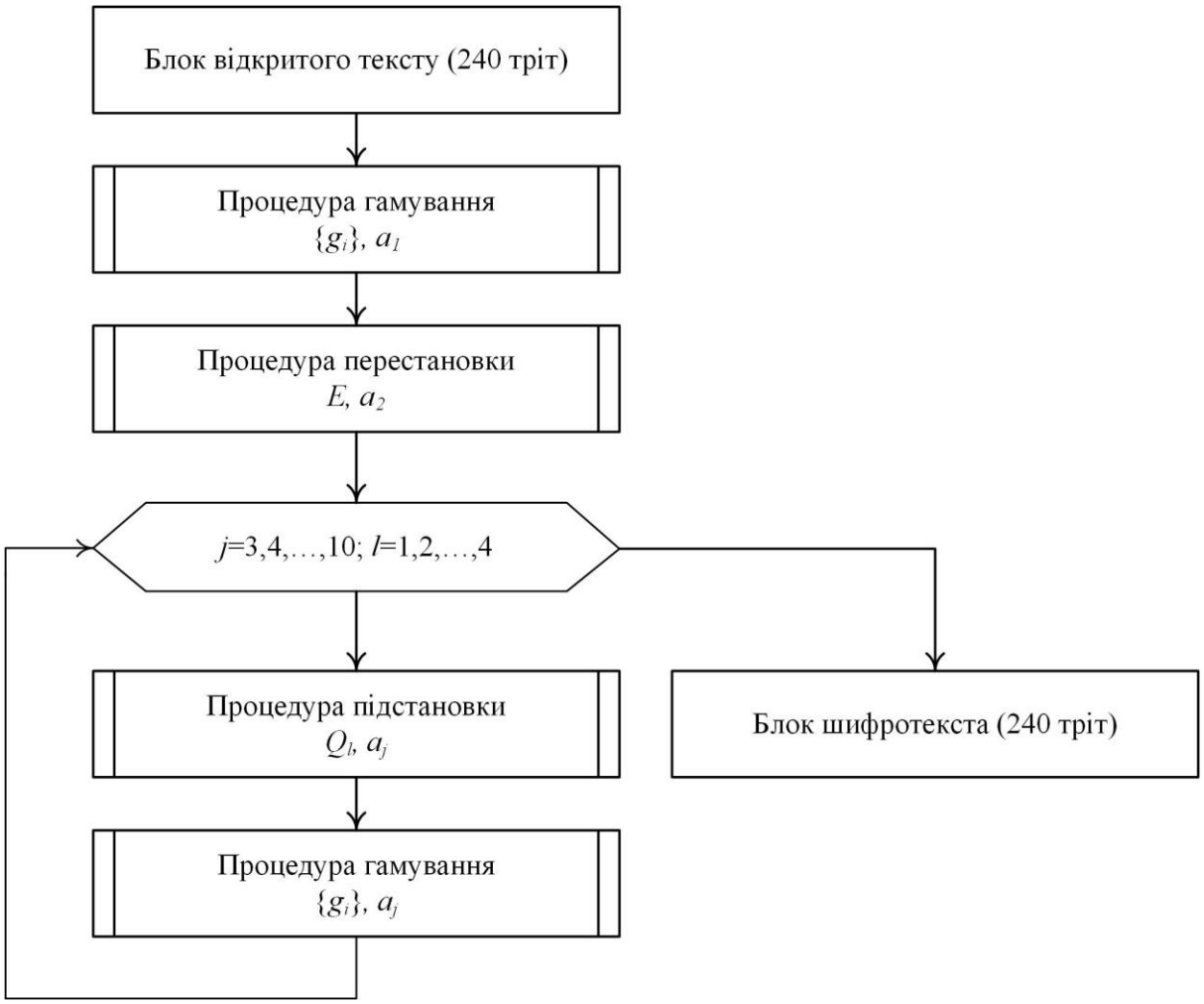


Рис. 6.8. — Алгоритм шифрування

Для організації раундів шифрування значення $\{a_i\}$ повинні бути вибрані з дільників числа N, а також повинні бути визначені підстановочні послідовності Q_1, Q_2, Q_3, Q_4 і перестановка E.

Алгоритм розшифрування являє собою зворотний порядок процедур, з яких складається алгоритм шифрування. Змінні розбиття процедур підстановки і перестановки повинні слідувати в зворотному порядку. Послідовності Q і перестановка E, а також гамма повинні бути інвертовані. Схема запропонованого алгоритму розшифрування показана на рис. 6.9.

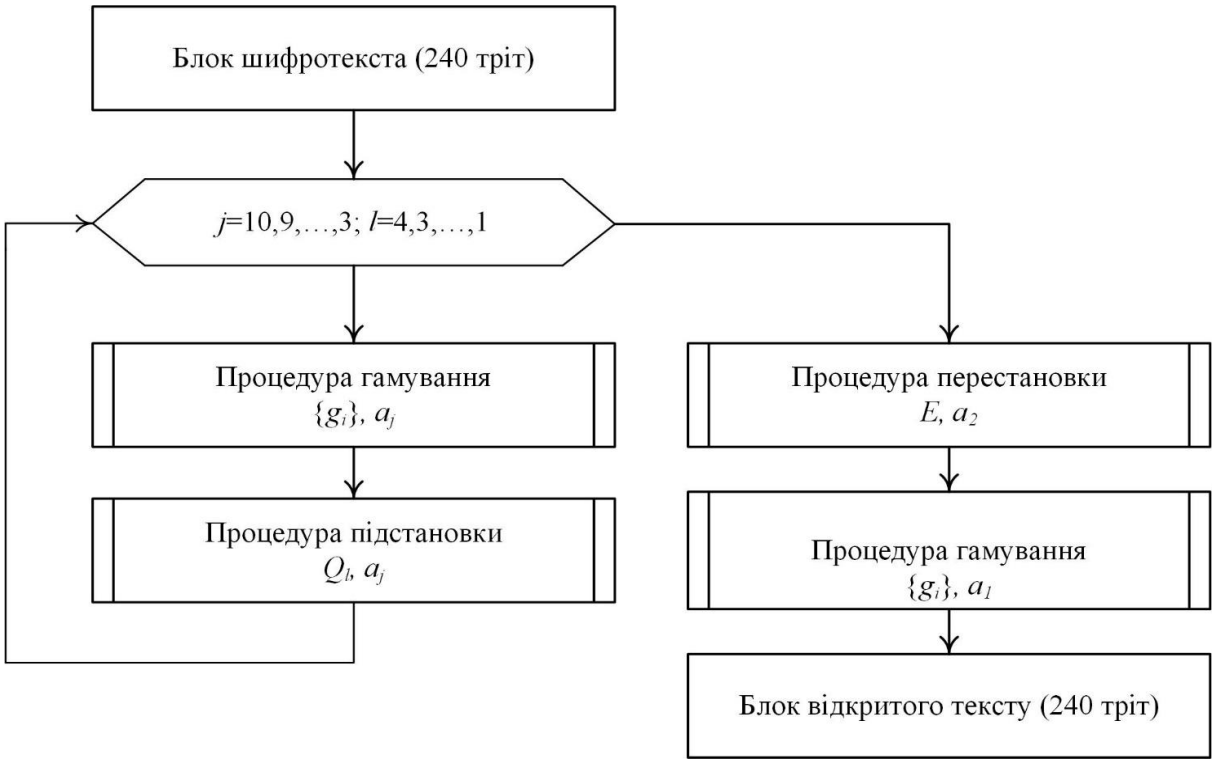


Рис. 6.9. — Алгоритм розшифрування

6.5.2. Процедура підстановки

Вхідні дані: блок вхідного тексту $\{x_i\}$, $i=1,2,...,N$ над алфавітом $x_i \in \{0,1,...,q-1\}$, змінна розбиття a, структура Q S-блока підстановки довжини q^a.

Вихідні дані: блок зашифрованого тексту $\{y_i\}$, $i=1,2,...,N$.

Позначення: для зручності процедуру підстановки будемо позначати як $y_i = S(x_i, Q, a), \quad i=1,2,...,N$.

Процедура підстановки призначена для реалізації концепції конфузії в криптографічному алгоритмі і заснована на принципі змінної довжини блоку. Уявімо процедуру у вигляді послідовності кроків, які будемо супроводжувати конкретним прикладом.

Наприклад, задаємося блоком трійкового вхідного тексту довжини $N=240$, який будемо використовувати в якості прикладу

$$x_i = \{220210112202212012221022121110101002112012201111211100121102110211221001212021011112112122110012201101021101111110020212010202220112120100211021111000001022111210210100221001200011111110101120221111112211211221110110200001121022101111100111\},\quad (6.62)$$

і значенням змінної розбиття $a = 4$, а також структурою оптимальної Q-послідовності, запропонованої в роботі [27] довжини 3^a

$$S=\{0\ 80\ 37\ 77\ 43\ 6\ 40\ 3\ 74\ 8\ 73\ 36\ 79\ 42\ 5\ 39\ 2\ 76\ 1\ 72\ 44\ 78\ 41\ 7\ 38\ 4\ 75\ 27\ 26\ 64\ 23\ 70\ 33\ 67\ 30\ 20\ 35\ 19\ 63\ 25\ 69\ 32\ 66\ 29\ 22\ 28\ 18\ 71\ 24\ 68\ 34\ 65\ 31\ 21\ 54\ 53\ 10\ 50\ 16\ 60\ 13\ 57\ 47\ 62\ 46\ 9\ 52\ 15\ 59\ 12\ 56\ 49\ 55\ 45\ 17\ 51\ 14\ 61\ 11\ 58\ 48\}. \quad (6.63)$$

Крок 1. Блок вхідного тексту розбивається на $\lambda = N/a$ сегментів довжини a кожен. Таким чином, отримуємо двовимірний масив, який зручно представити у вигляді матриці Λ порядку $\lambda \times a$, кожен рядок якої є сегментом вхідного тексту довжини a.

Розбиваємо вихідний сегмент даних на $\lambda = N/a = 240/4 = 60$ сегментів, які представимо у вигляді матриці розміру 60×4, у якій кожен рядок для наочності взятий у фігурні дужки, і поруч проставлені номери сегментів (рядків матриці Λ).

1.{2202}	11.{1122}	21.{1211}	31.{0202}	41.{2101}	51.{1121}
2.{1011}	12.{0111}	22.{2122}	32.{2201}	42.{0022}	52.{1221}
3.{2202}	13.{1211}	23.{1100}	33.{1212}	43.{1001}	53.{1101}
4.{2120}	14.{1001}	24.{1220}	34.{0100}	44.{2000}	54.{1020}
5.{1222}	15.{2110}	25.{1101}	35.{2110}	45.{1111}	55.{0001}
6.{1022}	16.{2111}	26.{0211}	36.{2111}	46.{1110}	56.{1210}
7.{1211}	17.{2210}	27.{0111}	37.{1000}	47.{1011}	57.{2210}
8.{1010}	18.{0121}	28.{1110}	38.{0010}	48.{2022}	58.{1111}
9.{1002}	19.{2021}	29.{0202}	39.{2211}	49.{1111}	59.{1100}
10.{1120}	20.{0111}	30.{1201}	40.{1210}	50.{1122}	60.{1111}

. (6.64)

Крок 2. Проводимо підстановку в кожному сегменті довжини a згідно із законом, який визначається Q-послідовністю, в результаті чого отримуємо нову матрицю $\Omega_j = Q(\Lambda_j)$ розміру $\lambda \times a$, де $j = 1,2,...,\lambda$ — номер рядка.

Для нашого прикладу отримуємо нову матрицю розміру 60×4.

1.{0122}	11.{0211}	21.{2112}	31.{1122}	41.{1201}	51.{1002}
2.{2121}	12.{1120}	22.{1211}	32.{1200}	42.{2202}	52.{1011}
3.{0122}	13.{2112}	23.{1022}	33.{1021}	43.{0222}	53.{0201}
4.{0110}	14.{0222}	24.{2102}	34.{0022}	44.{2000}	54.{2111}
5.{0210}	15.{1221}	25.{0201}	35.{1221}	45.{2120}	55.{2222}
6.{0202}	16.{0120}	26.{1112}	36.{0120}	46.{0221}	56.{0220}
7.{2112}	17.{1220}	27.{1120}	37.{1000}	47.{2121}	57.{1220}
8.{0212}	18.{0002}	28.{0221}	38.{2212}	48.{1202}	58.{2120}
9.{2101}	19.{2010}	29.{1122}	39.{0112}	49.{2120}	59.{1022}
10.{2110}	20.{1120}	30.{0200}	40.{0220}	50.{0211}	60.{2120}

. (6.65)

Крок 3. Виконуємо конкатенацію рядків матриці Ω, в результаті чого отримуємо послідовність елементів вихідного тексту $\{y_i\}$, $i = 1,2,...,N$

$$
\begin{aligned}
y_i = \{&0122212101220110021002022112021221012\\
&1100211112021120222122101201220000220101 1\\
&2021121211102221020201111211200221112202 0\\
&0112212001021002212210120100022120112022 0\\
&1201220202222000212002212121120221200211 1\\
&0021011020121112222022012202120102221 20\}.
\end{aligned}
\tag{6.66}
$$

Відзначимо, що статистика вхідного тексту в результаті виконання процедури підстановки зазнала змін. Так вхідний текст містив 63 символа «0», 114 символів «1» і 63 символа «2», тоді як після виконання всіх перетворень у вихідному тексті стало 67, 77, 96 символів «0», «1» і «2», відповідно. Таким чином, можна відзначити тенденцію, що намітилася на наближення статистики тексту до рівномірної.

Зауважимо також, що структура Q-послідовності може розглядається як елемент (довгострокового) ключа, і бути засекреченою.

Процедура зворотної підстановки повністю ідентична процедурі підстановки, за винятком того, що в разі, якщо Q-послідовність не є інволюцією, для здійснення зворотної підстановки повинна бути знайдена послідовність Q^{-1}, як зворотна перестановка до послідовності Q.

6.5.3. Процедура перестановки

Вхідні дані: блок вхідного тексту $\{x_i\}$, $i = 1,2,...,N$ над алфавітом $x_i \in \{0,1,...,q-1\}$, змінна розбиття a, структура перестановки E довжини a.

Вихідні дані: блок зашифрованого тексту $\{y_i\}$, $i = 1,2,...,N$.

Позначення: процедуру перестановки будемо коротко позначати як $y_i = P(x_i, E, a), \quad i = 1,2,...,N$.

Процедура перестановки призначена для реалізації концепції дифузії при шифруванні. У розробленому алгоритмі пропонується проводити вибір структури Е-послідовності, що визначає Р-блок випадковим чином і передавати її приймальній стороні як елемент ключової інформації.

Опишемо процедуру перестановки у вигляді послідовності кроків, для ясності викладу супроводжуваних конкретним прикладом, для чого задаємося блоком вихідних даних (6.62), значенням змінної розбиття $a = 30$, а також випадковою перестановкою

$$E = \{5\ \ 8\ \ 21\ \ 11\ \ 10\ \ 19\ \ 20\ \ 24\ \ 13\ \ 29\ \ 30\ \ 22\ \ 14\ \ 17\ \ 15\ \ 16\ \ 7\ \ 2\ \ 3\ \ 12\ \ 18\ \ 26\ \ 25\ \ 9\ \ 23\ \ 27\ \ 28\ \ 4\ \ 6\ \ 1\}. \tag{6.67}$$

Крок 1. Блок вхідного тексту розбиваємо на $\lambda = N/a$ сегментів довжини a кожен. Таким чином, отримуємо двовимірний масив, який зручно представити у вигляді матриці Λ порядку $\lambda \times a$, кожен рядок якої є сегментом вхідного тексту довжини a.

Розбиваємо вихідний сегмент даних на $\lambda = N/30 = 240/30 = 8$ сегментів, які представимо у вигляді матриці розміру 8×30

$$\Lambda = \begin{bmatrix} 220210112202212012221022121110 \\ 101002112011220111121110012110 \\ 211122100121202101111211212211 \\ 001220110102110111111002021201 \\ 020222011212010021102111100000 \\ 102211121021010022100120001111 \\ 111010112022111111221121122111 \\ 011020000112102210111111001111 \end{bmatrix}. \quad (6.68)$$

Крок 2. Проводимо перестановку стовпців матриці Λ відповідно до правила, визначеного перестановкою E, в результаті чого отримуємо нову матрицю $\Omega_{i,j} = \Lambda_{i,E_j}$, $i = 1,2,...,\lambda$, $j = 1,2,...,a$.

Отримуємо нову матрицю

$$\Omega = \begin{bmatrix} 111022222100112012022212211202 \\ 011101202101210110111102121021 \\ 201211112112002111111120122122 \\ 211011121010110110121200012200 \\ 212121010001120002021011100220 \\ 120201000111120010212001211211 \\ 111202211111111111121212221001 \\ 201111111111012201120000111000 \end{bmatrix}. \quad (6.69)$$

Крок 3. Виконуємо конкатенацію рядків матриці Ω, в результаті чого отримуємо послідовність елементів вихідного тексту $\{y_i\}$, $i = 1,2,...,N$.

Отримуємо вихідну послідовність

$$\begin{aligned} y_i = \{&111022222100112012022212211202011 \\ &101202101210110111102121021201211121 \\ &120021111111201221222110111210101101 \\ &012120001220021212101000112000202101 \\ &100220120201000111120010212001211211 \\ &112022111111111111212122210012011111 \\ &1111012201120000111000\}, \end{aligned} \quad (6.70)$$

статистика якої повністю збігається зі статистикою вхідного тексту.

Відзначимо, що при випадковому виборі перестановки E залишається ймовірність використання слабких перестановок. Проте, при досить великому значенні змінної розбиття дана ймовірність стає такою малою, що нею можна нехтувати [34].

Процедура зворотної перестановки повністю ідентична процедурі перестановки, за винятком того, що в разі, якщо E-послідовність не є інволюцією, для здійснення зворотної перестановки повинна бути знайдена послідовність E^{-1}, як зворотна перестановка до послідовності E.

6.5.4. Процедура гамування

Вхідні дані: блок вхідного тексту $\{x_i\}$, $i=1,2,...,N$ над алфавітом $x_i \in \{0,1,...,q-1\}$, гамма $\{g_i\}$ над алфавітом $g_i \in \{0,1,...,q-1\}$, змінна розбиття a.

Вихідні дані: блок зашифрованого тексту y_i, $i=1,2,...,N$.

Позначення: процедуру гамування будемо коротко позначати як $y_i = \Gamma(x_i, g_i, a)$, $i=1,2,...,N$.

Опишемо процедуру гамування у вигляді конкретних кроків, для ясності викладу супроводжуваних прикладом. Задаємося блоком вихідних даних (6.62), значенням змінної розбиття $a=40$, а також гамою

$$\begin{gathered}\{g_i\} = \{21022201110111100222000102001210101210101122120122111201121121121111211121212011101111011011012110201121121120201111120021021022201110111100222000102001210121010112212012211120112112112111121121212011101110110121102011211211202011111200210\}.\end{gathered} \tag{6.71}$$

Крок 1. Блок вхідного тексту розбиваємо на $\lambda = N/a$ сегментів довжини a кожен. Таким чином, отримуємо двовимірний масив, який зручно

представити у вигляді матриці Λ порядку $\lambda \times a$, кожен рядок якої є сегментом вхідного тексту довжини a.

Для нашого прикладу розбиваємо вихідний сегмент даних на $\lambda = {}^{240}\!/_{40} = 6$ сегментів, які представимо у вигляді матриці Λ розміру 6×40

$$\Lambda = \begin{bmatrix} 2202101122022120122210221211101010021120 \\ 1122011112111001211021112210012120210111 \\ 1211212211001220110102110111111002021201 \\ 0202220112120100211021111000001022111210 \\ 2101002210012000111111101011202211111122 \\ 1121122111011020000112102210111111001111 \end{bmatrix}. \qquad (6.72)$$

Крок 2. Аналогічним *Кроку 1* чином здійснюємо розбивку гами, представляючи її у вигляді матриці G розміру $\lambda \times a$. Для нашого прикладу, відповідно

$$G = \begin{bmatrix} 2102220111011110022200010200121010121010 \\ 1122120122111201121121121111211121212011 \\ 1011110110121102011211211202011111200210 \\ 2102220111011110022200010200121010121010 \\ 1122120122111201121121121111211121212011 \\ 1011110110121102011211211202011111200210 \end{bmatrix}. \qquad (6.73)$$

Крок 3. Розглядаючи кожен рядок матриць Λ і G як a-розрядне число, представлене в q-ічній системі числення здійснюємо порядкове складання матриць Λ і G по модулю q^a. Таким чином, при складанні елементів рядків матриць Λ і G враховуються всі перенесення, за винятком останнього, яке відкидається.

У нашому прикладі рядки розглядаються як 40-розрядні числа в трійковій системі числення (по модулю 3^{40}). Таким чином, можемо обчислити нову матрицю як порядкову суму представлених матриць Λ і G

$$\begin{bmatrix} 20120220101110002221110021112220202122 00 \\ 00212020112222101022200110220010121221 22 \\ 00001000212000221220210220201221202221 11 \\ 00122110002012110102211212001221100022 20 \\ 10002001022002020100022222001211101002 10 \\ 22100022212021220121010211121222222020 21 \end{bmatrix}. \quad (6.74)$$

Крок 4. Здійснюємо конкатенацію рядків обчисленої на *Кроці 3* матриці, в результаті чого отримуємо послідовність елементів вихідного тексту $\{y_i\}$, $i = 1,2,...,N$. Для нашого прикладу отримуємо вихідну послідовність

$$\begin{gathered} \{y_i\} = \{20120220101110002221110021112220202122000021202011222210102220011022001012212212200001000212000221220210220201221202221112200010002012110102211212001221100022010012211000201211010221121200122110002201000200102200202010002222200121110100210221 \\ 00022212021220121010211121222222020211\}. \end{gathered} \quad (6.75)$$

Відзначимо, що при розшифруванні необхідно використовувати зворотну гамуючу послідовність $\{g_i\}^{-1}$, яка буде мати різну структуру при різних значеннях змінної розбиття a. Обчислювати зворотну ключову послідовність зручно по матриці G. За правилами багатозначної арифметики для кожного рядка матриці G повинен бути знайдений додатковий код [35], для чого необхідно провести віднімання кожного рядка від числа $\overbrace{2222...2}^{a}$, а потім додати до одержаного числа 1.

Наприклад, знайдемо перший рядок матриці G^{-1}.

$$\begin{array}{l} - \underline{22222222222222222222222222222222222222} \\ \underline{21022201110111100222000102002121010121010} \\ + \underline{01200021112111122000222120221010121012120} \\ \underline{00000000000000000000000000000000000000001} \\ 01200021112111122000222120221010121012200 \end{array} \quad (6.76)$$

Аналогічним чином можемо знайти всю зворотну гаму $\{g_i\}^{-1}$.

6.6. Можливість використання крипто-стеганографічної системи із потоковим контейнером

Створення прихованого каналу передачі ДІ у потоковому контейнері є складним обчислювальним завданням, особливо, якщо мова йде про його використання на таких обмежених у обчислювальних ресурсах пристроях, як пристрої IoT, IoBT, мобільні пристрої, безпілотні літальні апарати та ін.

Отримані в дисертаційній роботі результати роблять можливим створення таких каналів передачі інформації за рахунок використання для роботи таких систем просторової області.

Далі ми доводимо, що такий підхід є гарантовано обчислювально більш ефективним, аніж використання областей перетворень.

Твердження 6.6.1. Стеганографічний алгоритм із кодовим управлінням вбудовуванням має меншу обчислювальну складність за будь-який стеганографічний алгоритм, що працює в області перетворень контейнера або перетворень блоків контейнера.

Доведення. Стеганографічні алгоритми, що використовують області перетворень, потребують виконання операцій прямого та зворотного перетворення контейнера (блоків контейнера).

Отже, для того, щоб довести справедливість **Твердження 6.6.1.** нам необхідно довести той факт, що виконання прямого та зворотного перенесення контейнера (його блока) в область перетворень має більшу складність за виконання вбудовування ДІ за допомогою методу вбудовування із кодовим управлінням. Наведемо для цього у табл. 6.12 порівняння складності найефективніших перетворень $N = n^2$ елементів, що використовуються у стеганографічних алгоритмах зі складністю стеганографічного алгоритму з кодовим управлінням вбудовуванням.

Для даного алгоритму складність вбудовування ДІ для блока розміру n визначається складністю підсумовування двох матриць, тобто $\mathrm{O}(n^2) = n^2$.

Проведемо далі оцінку обчислювальної складності алгоритму вилучення ДІ з контейнера. Для цього розрахуємо обчислювальну складність на кожному кроці цього алгоритму. На першому кроці для кожного блока стеганоповідомлення необхідно знайти матрицю різниць елементів контейнера та стеганоповідомлення, що потребує n^2 операцій віднімання. На другому кроці необхідно перемножити отриману на першому кроці матрицю різниць на кожне з λ кодових слів, після чого підсумувати отриманий результат. Оскільки кодові слова містять лише елементи ± 1, для реалізації цієї дії необхідно якнайбільше λn^2 операцій. При цьому на третьому кроці необхідно знайти максимум серед λ значень, що, взагалі, потребує $\lambda - 1$ операцій порівняння, і, відповідно, жодної додаткової операції, якщо в блок вбудовується лише 1 біт ДІ, тобто $\lambda = 1$.

Тобто обчислювальна складність алгоритму вилучення складатиме щонайбільше $O(n^2)$ із коефіцієнтом 2λ.

Таким чином загальна обчислювальна складність вбудовування та вилучення інформації складатиме $O(n^2)$ із коефіцієнтом $2\lambda + 1$, або $O(n^2)$ з коефіцієнтом 3 для випадку $\lambda = 1$.

У табл. 6.12 наведено результати порівняння обчислювальної складності чотирикратного застосування розповсюджених видів перетворень, що використовуються під час побудови стеганографічних алгоритмів (адже операції вбудовування та вилучення ДІ вимагатимуть по парі перетворень на кожну) та обчислювальної складності запропонованого стеганографічного алгоритму з кодовим управлінням вбудовуванням інформації.

Таблиця 6.12 — Порівняння складності переходу до найчастіше застосовуваних областей перетворення зі складністю вбудовування ДІ за допомогою стеганографічного алгоритму з кодовим управлінням

Перетворення	Складність перетворення	Складність перетворення x 4 / Загальна складність вбудовування та вилучення ДІ
ДКП	$O(n^2 \log_2 n^2)$ [36]	$\frac{4}{3}\log_2 n$
Дискретне перетворення Фур'є	$O(n^2 \log_2 n^2)$ [37]	$\frac{4}{3}\log_2 n$
Перетворення Уолша-Адамара	$O(n^2 \log_2 n^2)$ [38]	$\frac{4}{3}\log_2 n$
Вейвлет перетворення	$O(n^2)$ [39]	$\frac{4}{3}$
Сингулярне розкладання матриці	$O(n^3)$ [40]	$\frac{4}{3}n$

Аналіз даних табл. 6.12 доводить високу обчислювальну ефективність стеганографічного алгоритму з кодовим управлінням вбудовуванням інформації.

Відзначимо також, що при реалізації на реальних обчислювальних платформах стеганографічного методу з кодовим управлінням мова йде про імплементацію найпростішої операції інкременту або декременту значень яскравості пікселів зображення, тоді як при реалізації практично всіх вказаних в табл. 6.12 перетворень (окрім перетворення Уолша-Адамара та деяких видів вейвлет перетворення) йдеться про роботу з нецілочисельними операндами, та виконання як операцій множення, так і підсумовування, що ще більше ускладнює технічну реалізацію стеганографічних алгоритмів, що засновані на цих перетвореннях.

Також, на практиці, в більшості стеганографічних алгоритмів, що працюють в області перетворень, доводиться, окрім операцій прямого та зворотного перетворення, виконувати досить обчислювально складні

операції із вбудовування ДІ, які часто набагато складніші за саме перетворення (наприклад, вирішення систем рівнянь), що фактично унеможливлює імплементацію таких методів на обмежених у ресурсах платформах. Вказане визначає високу актуальність стеганографічного методу з кодовим управлінням вбудовуванням інформації.

Отже, наведене доводить, що використання стеганографічного алгоритму з кодовим управлінням вбудовуванням у просторовій області принципово дозволяє отримати меншу обчислювальну складність ніж у стеганографічних алгоритмів, що використовують області перетворень.

Результати вимірювання швидкодії розробленої КСС на найбільш розповсюджених у сучасних ресурсообмежених пристроях процесорах, а також на платформі AMD Ryzen 3 3200G показані в табл. 6.13. При цьому для кожного кадру потокового контейнера виконувалося вбудовування максимального обсягу ДІ у одну з кольорових компонент за допомогою кодових слів T_{16}, які забезпечують максимальну стійкість до атак проти вбудованого повідомлення, що є важливим при вбудовуванні інформації у потоковий контейнер.

Таблиця 6.13 —Показники швидкодії моделі КСС для різних розподільних здатностей потокових контейнерів

Тип потокового контейнеру			**400p**	**720p**	**1080p**	**1140p**	**4k**	**8k**
Загальна швидкість роботи КСС в режимі вбудовування ДІ, fps	AMD Ryzen 3 3200G		6826	2571	1356	962	326	73
	ASUS ZE620KL (Cortex A73)		2507	1118	493	356	125	31
	Raspberry Pi 4 (Cortex A72)		1815	825	354	257	90	23
	ASUS P028 (Cortex A53)		761	344	186	109	39	10
	Yarvik TAB275 (Cortex A8)		485	239	106	67	25	7
	Мінімально необхідне значення продуктивності Single Thread ARM процесора, MOps/Sec	30 fps	~7.4	~16.6	~37.3	~52.5	~149.2	~437.9
		60 fps	~14.8	~33.2	~74.6	~105	~298.4	~875.8

Закінчення табл. 6.13

Загальна швидкість роботи КСС в режимі вилучення ДІ, fps	AMD Ryzen 3 3200G		845	359	164	116	41	11
	ASUS ZE620KL (Cortex A73)		306	63	60	44	16	4
	Raspberry Pi 4 (Cortex A72)		236	106	47	33	12	3
	ASUS P028 (Cortex A53)		93	42	19	12	5	2
	Yarvik TAB275 (Cortex A8)		55	24	11	8	3	1
	Мінімально необхідне значення продуктивності Single Thread ARM процесора, MOps/Sec	30 fps	~53.5	~120.3	~270.6	~380.8	~1082.4	~4329.6
		60 fps	~107.0	~240.6	~541.2	~761.6	~2164.8	~8659.2

Аналіз даних, представлених у табл. 6.13 показує, що навіть непотужні і не орієнтовані на обробку ЦВ моделі процесорів серії ARM Cortex виявляються здатними підтримувати роботу розробленої ефективної КСС в режимі реального часу. При цьому очевидно, що застосування розробленої КСС на більш сучасних моделях процесорів, а більше того, на процесорах, що орієнтовані на обробку ЦВ, дозволить суттєво знизити навантаження на них, яке пов’язане із забезпеченням функціонування системи захисту інформації, а, отже, підвищити швидкодію інших операцій, збільшити час автономності пристроїв та їх енергоефективність.

У табл. 6.13 значення мінімально необхідної продуктивності обраховані на основі експериментальних даних, які були отримані під час підрахунку швидкодії КСС на платформах ARM Cortex. Мінімальна необхідна продуктивність Single Thread для підтримки роботи КСС із заданою розподільною здатністю контейнера у режимі реального часу сильно залежить від архітектури конкретного процесора.

При цьому слід зазначити наступні твердження:

1. стеганографічний метод вбудовування інформації з кодовим управлінням володіє очевидним внутрішнім паралелізмом (блоки контейнера можуть оброблятися незалежно один від одного), що дозволяє збільшити

швидкість вбудовування та вилучення інформації кратно кількості використовуваних обчислювальних пристроїв;

2. стеганографічний метод вбудовування інформації з кодовим управлінням не передбачає використання будь-яких специфічних операцій (окрім цілочисельних операцій підсумовування та невеликої кількості операцій множення елементів), а також володіє простою структурою, що спрощує та підвищує ефективність його апаратної реалізації, наприклад, за допомогою PLD. Зазначене є надзвичайно важливим з огляду на використання крипто-стеганографічних систем у пристроях IoT та IoBT.

У табл. 6.14 наведено результати порівняльного аналізу відомих існуючих КСС із побудованою, відповідно до запропонованої методології.

Таблиця 6.14 — Порівняльний аналіз відомих КСС з розробленою

Критерій / КСС	Mukherjee [41] (2015)	Shifa [42] (2018)	CSRT [43] (2018)	Seethalakshmi [44] (2016)	Запропонована КСС
Стійкість до атак проти вбудованого повідомлення	—	—	Немає даних	—	+
Забезпечення надійності сприйняття	+	+	+	+	+
Пропускна спроможність прихованого каналу	Залежить від контейнера	<1	1/8	<1	Фіксовані значення: 1/4, 1/8, 1/16, 1/64…
Криптоалгоритм	RSA + ГПКП	AES256-OFB	LOOK-UP Table	AES	БСШ прекодера + спец. БСШ послідовності переліку станів
Область вбудовування	Просторова	Просторова	DCT	Просторова + Integer Wavelet Transformation	Просторова
Можливість роботи з потоковим контейнером в режимі реального часу	—	—	—	—	+
Можливість реалізації на ресурсообмежених платформах	—	—	—	—	+

Аналіз даних табл. 6.14 підтверджує, що серед найкращих розглянутих існуючих аналогів, тільки розроблена КСС у повній мірі здатна забезпечити функціонування на ресурсообмежених платформах з потоковим контейнером при збереженні відповідності основним критеріям ефективності. Так, КСС Mukherjee, Shifa, Seethalakshmi передбачають попередній аналіз контейнера перед вбудовуванням ДІ, що потребує наявності значних обчислювальних ресурсів і заздалегідь відомого контейнера, таким чином унеможливлюючи їх застосування із потоковим контейнером в режимі реального часу на ресурсообмежених платформах. Окрім того, КСС Mukherjee потребує додаткової генерації та зберігання стеганошляху, тоді як КСС Mukherjee, Shifa, Seethalakshmi є нестійкими до атак проти вбудованої ДІ, що суперечить їх відповідності означеним критеріям ефективності, які висуваються до сучасних КСС. Незважаючи на те, що автори декларують значну швидкодію КСС CSRT при її апаратній реалізації, вона характеризується значним зростанням обсягу необхідної ключової інформації із зростанням обсягу ДІ, що також унеможливлює її роботу з потоковими контейнерами в режимі реального часу. Більш того, необхідність застосування ДКП, в силу Твердження 8, при рівних обчислювальних потужностях, завжди обмежуватиме показники швидкодії КСС, що застосовують області перетворень у порівнянні із запропонованою методологією розробки ефективної КСС.

Значення чисельного приросту ефективність КСС у порівнянні із найкращими відомими аналогами наведено в табл. 6.15.

Таблиця 6.15 — Порівняння показників ефективності побудованої за розробленою методологією КСС із кращими існуючими аналогами

<table>
<tr><th>Критерій ефективності</th><th>Показник ефективності</th><th colspan="2">Приріст ефективності</th></tr>
<tr><td rowspan="4">Криптостійкість</td><td>Нелінійність</td><td>до 21.55%</td><td rowspan="4">можливість врахування криптографічної якості ФБЛ</td></tr>
<tr><td>Лавинні властивості</td><td>до 9.375%</td></tr>
<tr><td>Кореляційний зв’язок векторів виходу та входу</td><td>до 12.5%</td></tr>
<tr><td>Алгебраїчна нелінійність</td><td>співпадає</td></tr>
<tr><td>Швидкодія</td><td>Обчислювальна складність</td><td colspan="2">в $\frac{4\mu}{3}$ разів</td></tr>
<tr><td>Стійкість до атак проти вбудованого повідомлення</td><td>Кількість помилок при декодуванні ДІ в умовах атаки</td><td colspan="2">в 8.125 разів</td></tr>
<tr><td>Забезпечення надійності сприйняття стегано-повідомлення</td><td>PSNR, дБ</td><td colspan="2">на 3%</td></tr>
<tr><td>Пропускна спроможність стеганоканалів КСС у відсутності множинного доступу</td><td>$1/\mu^2$ (біт/піксель)</td><td colspan="2">достатня</td></tr>
<tr><td>Забезпечення можливості одночасного користування КСС декількома користувачами</td><td>Кількість каналів множинного доступу</td><td colspan="2">у 1200 разів (зареєстрованих), у 16 разів (одночасно працюючих)</td></tr>
<tr><td>Пропускна спроможність групового тракту</td><td>Середня довжина кодового слова l_{av}</td><td colspan="2">на 6.25%</td></tr>
</table>

Аналіз даних, представлених у табл. 6.15 дозволяє дійти висновку про значне підвищення рівня ефективності розробленої КСС у порівнянні із найкращими відомими аналогами КСС, а також найкращими криптографічними та стеганографічними методами, які потенційно можуть бути об’єднаними у КСС. При цьому, на відміну від існуючих аналогів, КСС, що побудовані на основі розробленої методології, характеризуються значним

підвищенням швидкодії, що забезпечило принципову можливість їх роботи на ресурсообмежених пристроях. Окрім того, розроблена методологія забезпечує можливість множинного доступу до захищеного каналу КСС, так само як і надає можливості дослідження криптографічної якості застосовуваних конструкцій при їх представленні за допомогою ФБЛ.

Таким чином, в розділі закінчено розробку як теоретичної, так і практичної складових методології методології побудови ефективних КСС, узагальнена схема якої представлена на рис. 6.10.

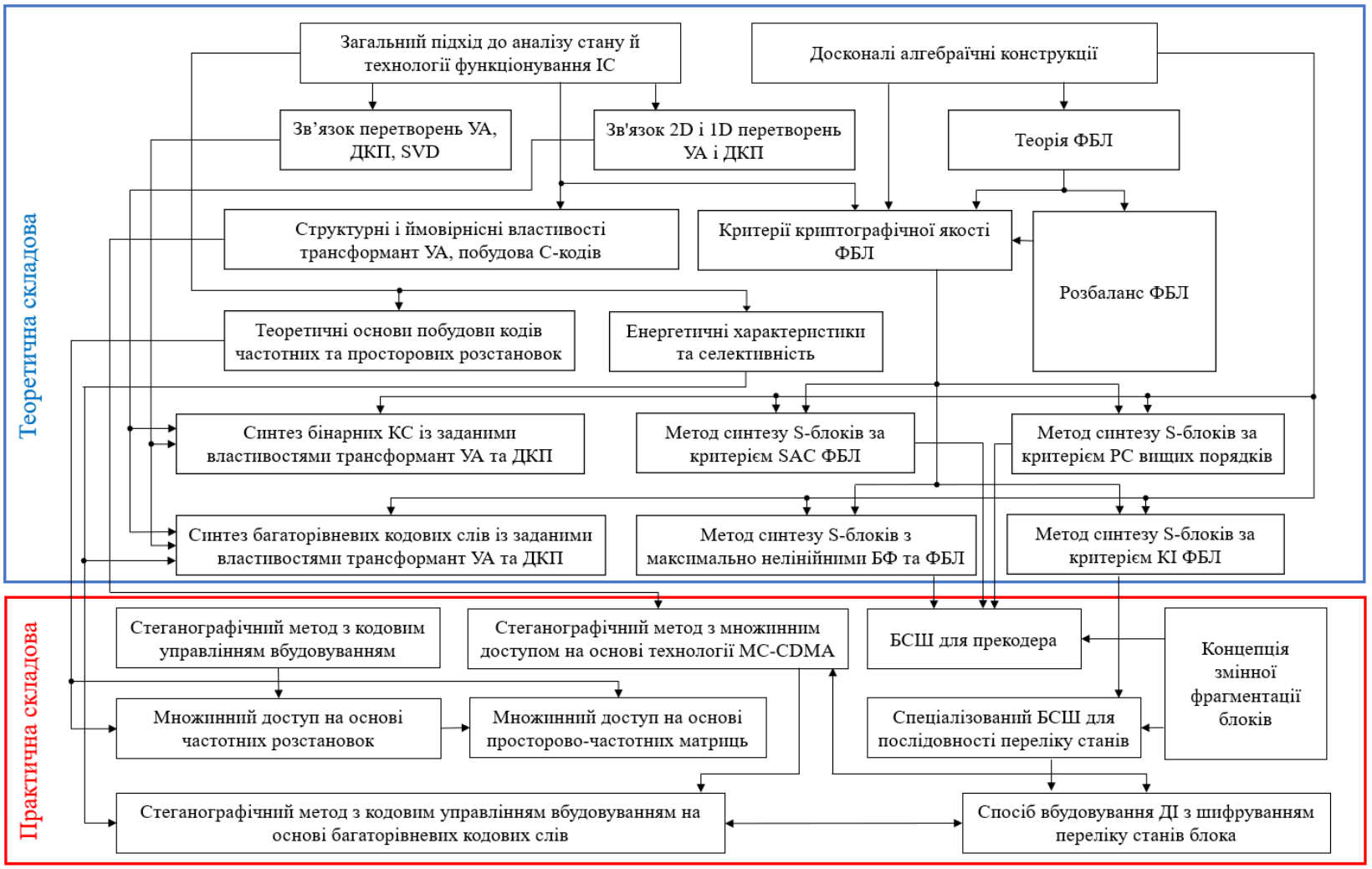


Рис. 6.10. — Узагальнена схема методології розробки ефективних КСС

6.7. Висновки

Отримані в шостому розділі дисертації результати, шляхом розробки S-блоків із врахуванням їх можливого представлення із застосуванням математичного апарату функцій багатозначної логіки, дозволили підвищити крипостійкість розробленої КСС, а саме у порівнянні з найкращими аналогами: підняти дистанційну нелінійність на 21.55%, покращити лавинні властивості на 9.375%, зменшити кореляційний зв'язок векторів виходу та входу на 12.5%.

Відзначимо основні результати проведених досліджень у вигляді конкретних пунктів:

1. На основі сформульованого у Розділі 5 теоретичного базису оцінки криптографічної якості ФБЛ створено методи синтезу криптографічних конструкцій, що володіють високою криптографічною якістю як у сенсі їх уявлення за допомогою булевих функцій, так і у сенсі їх уявлення за допомогою ФБЛ:

— на основі методу уявлення S-блоків за допомогою компонентних 4-функцій запропоновано конструктивний метод синтезу S-блоків довжини $N=16$, що дозволило отримати S-блоки, які володіють максимальним рівнем 4-нелінійності;

— розроблено рекурентний метод синтезу S-блоків, що задовольняють суворому лавинному критерію компонентних 4-функцій, що дозволяє отримувати S-блоки будь-якої заданої довжини $N=4^k$, зокрема, практично цінної довжини $N=256$. На основі відомої множини S-блоків довжини $N=16$ та потужності $J=245760$ отримано набір S-блоків довжини $N=64$ та набір S-блоків довжини $N=256$, компонентні 4-функції яких задовольняють суворому лавинному критерію. У побудованому наборі S-блоків довжини $N=256$, що задовольняють суворому лавинному критерію компонентних 4-функцій, знайдено S-блоки, які одночасно задовольняють і критерію максимального лавинного ефекту компонентних булевих функцій;

— на основі критерію розповсюдження помилки булевих функцій розроблено метод дослідження суворого лавинного критерію вищих порядків для булевих функцій, що дозволило для кожного спектрального класу булевих функцій $k = 1, 2, ..., 5$ змінних, які мають фіксовану елементарну структуру і, відповідно, фіксовану відстань нелінійності, обчислити кількості булевих функцій, що задовольняють критерію розповсюдження заданого порядку m. Знайдено клас з 12 (з точністю до суми з афінною функцією) врівноважених булевих функцій довжини $N = 32$, які мають максимальну відстань нелінійності та задовольняють критерію розповсюдження $\mathrm{PC}(4)$. Показано, що на основі цього набору булевих функцій можна синтезувати бієктивні криптографічні S-блоки довжини $N = 32$. Ці S-блоки є найкращими серед усієї множини S-блоків довжини $N = 32$ і потужності $J = 32! \approx 2.63 \cdot 10^{35}$ з точки зору критерію максимальної відстані нелінійності та критерію розповсюдження.

2. На основі розроблених криптографічних примітивів та концепції змінної фрагментації блоків створено готовий до практичної реалізації криптографічний алгоритм. При цьому спільне використання криптографічних примітивів, що володіють високим рівнем криптографічної якості як в сенсі їх уявлення за допомогою булевих функцій, так і за допомогою ФБЛ та їх об'єднання на основі сучасної концепції змінної фрагментації блоків, дозволяє суттєво підвищити ефективність блокових симетричних криптоалгоритмів, що доводиться експериментальними дослідженнями запропонованого криптоалгоритму: знищення статистики вихідного тексту, на відміну від існуючих аналогів, досягається вже на першій ітерації основного кроку криптоперетворення.

3. Запропоновано спосіб вбудовування ДІ за допомогою стеганографічного методу з кодовим управлінням вбудовуванням із шифруванням послідовності переліку станів блоків, який дозволяє підвищити

криптографічну захищеність крипто-стеганографічної системи за рахунок рівномірного розподілення ДІ по всім блокам контейнера (включаючи ті, в які вбудовування ДІ не відбувається) та, таким чином, досягти наступних переваг: за рахунок рівної ймовірності появи блоків, в які вбудовується кодове слово T^+, T^- та у які вбудовування не відбувається, вдається максимізувати невизначеність під час стеганоаналізу, що робить прихованим (зашифрованим) навіть об'єм вбудованої ДІ; відпадає необхідність формування та збереження стеганошляху, адже він формується під час шифрування послідовності переліку станів; уніфікуються показники PSNR для кадрів потокового контейнеру, що унеможливлює визначення місць концентрації ДІ у кадрах контейнера при її нерівномірному розподіленні.

4. На основі сформульованого у Розділі 5 теоретичного базису оцінки криптографічної якості ФБЛ створено методи синтезу криптографічних S-блоків довжини $N = 3^k$, що відповідають критеріям криптографічної якості компонентних 3-функцій та дозволяють синтез криптографічних алгоритмів, що оперують над алфавітом $\{0,1,-1\}$ для задач шифрування послідовності переліку станів для роботи стеганографічного методу з кодовим управлінням вбудовуванням інформації:

— на основі конструкції Кіма запропоновано метод синтезу S-блоків підстановки довжини $N = 3^k$, що дозволяє отримати множини S-блоків, які відповідають критерію відсутності кореляційного зв'язку векторів виходу і входу. Метод передбачає синтез невеликих S-блоків, що володіють оптимальними матрицями коефіцієнтів кореляції, після чого використовується алгоритм Кіма рекурентного збільшення довжини S-блока підстановки. Результати обчислювальних експериментів підтверджують ефективність розробленого методу для побудови S-блоків великої довжини, зокрема побудований S-блок підстановки довжини $N = 3^5 = 243$;

— на основі конструкції Ніберг побудовано повні множини S-блоків над усіма ізоморфними уявленнями полів $GF(p^k)$, $p=3,5$, що дозволило отримати великі множини високоякісних S-блоків більшого асортименту довжин. Побудовано та табульовано повні множини незвідних та первісних незвідних поліномів над полями $GF(3)$, $GF(5)$, $GF(9^k)$, $GF(27^k)$, а також $GF(25^k)$ для практично цінних значень k, які можуть бути використані не тільки для побудови S-блоків, але також і для побудови генераторів псевдовипадкових ключових послідовностей. Визначено основні показники криптографічної якості побудованих S-блоків. Побудовані S-блоки в силу своєї високої якості можуть бути рекомендовані для використання в новітніх криптографічних алгоритмах, заснованих на принципах багатозначної логіки.

5. На основі функцій багатозначної логіки та методу динамічної зміни розмірів криптографічних примітивів запропоновано новий алгоритм шифрування, що оперує над алфавітом $\{0,1,-1\}$ та заснований на трьох основних процедурах: Заміна, Перестановка та Гамування, що визначає його чітку структуру та простоту програмної або апаратної реалізації. Запропонований криптографічний алгоритм досягає значення кількості ітерацій, що необхідні для його зламу $\Psi = 3.2292 \cdot 10^{114}$, і може застосовуватися для задач шифрування послідовності переліку станів під час застосування стеганографічного методу з кодовим управлінням вбудовуванням інформації.

6. Сформульовано твердження із строгим доказом, що доводить більшу обчислювальну ефективність застосування стеганографічних методів, що оперують у просторовій області у порівнянні із стенографічними методами, що оперують у областях перетворень. Проведені обчислювальні експерименти дозволили встановити можливість використання крипто-

стенографічної системи для роботи з потоковими контейнерами у режимі реального часу.

Список використаних джерел у шостому розділі

1. Соколов А.В., Красота Н.И. Сильно нелинейные подстановки: метод синтеза S-блоков, обладающих максимальной 4-нелинейностью. *Наукові праці ОНАЗ ім. О.С. Попова*. 2017. № 1. С. 145-154.

2. Sokolov A.V. Zhdanov O.N. Strict avalanche criterion of four-valued functions as the quality characteristic of cryptographic algorithms strength. Siberian Journal of Science and Technology, 2019. Vol. 20, No. 2. P.183–190.

3. Мазурков М.И., Чечельницкий В.Я., Мельник М.А., Соколов А.В. Алгоритм синтеза оптимальных криптографических блоков подстановки на основе регулярных операторов децимации, перестановки и m-сдвига. *Одесский политехнический университет. Труды.* 2012. №1(38). С. 179—187.

4. Cusick T. W. Boolean functions satisfying a higher order strict avalanche criterion. *Workshop on the Theory and Application of of Cryptographic Techniques*. Berlin, Heidelberg : Springer, 1993. P. 102-117.

5. Lloyd S. Counting functions satisfying a higher order strict avalanche criterion. *Workshop on the Theory and Application of of Cryptographic Techniques*. Berlin, Heidelberg : Springer, 1989. P. 63-74.

6. Sokolov A. V., Zhdanov O. N. Synthesis of highly nonlinear S-boxes satisfying higher order propagation criterion. *Journal of Discrete Mathematical Sciences and Cryptography*. 2020. P. 1-15.

7. Соколов А. В., Барабанов Н. А. Алгоритм устранения спектральной эквивалентности компонентных булевых функций S-блоков конструкции Ниберг. *Известия высших учебных заведений. Радиоэлектроника*. 2015. Т. 58, № 5. С. 41-49.

8. Соколов А.В., Цевух И.В. О существовании бинарных С-кодов длины N=32 с заданным значением пик-фактора спектра Уолша–Адамара. *ПФМТ*, 2017. № 2(31). С. 91-95.

9. Kim K. Construction of DES-like S-boxes Based on Boolean Functions Satisfying the SAC. *International Conference on the Theory and Application of Cryptology* : Berlin, Heidelberg : Springer, 1991. P. 59-72.

10. FIPS 197. [Electronic resource] Advanced encryption standard. 2001. http://csrc.nist.gov/publications/

11. СТБ 34.101.31-2011. Информационные технологии и безопасность. Защита информации. Криптографические алгоритмы шифрования и контроля целостности. Минск, Госстандарт, 2011. 31 с.

12. ГОСТ 34.12-2018. Информационная технология. криптографическая защита информации. Блочные шифры. М. Стандартинформ, 2018. 17 с.

13. ГОСТ 28147—89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования, 1989. 32 с.

14. Enhancing speed of SIMON: A light-weight-cryptographic algorithm for IoT applications / Alassaf N. et al. *Multimedia Tools and Applications*. 2019. Vol. 78, No. 23. P. 32633-32657.

15. Implementation and analysis of new lightweight cryptographic algorithm suitable for wireless sensor networks / Koo W. K. et al. *International Conference on Information Security and Assurance*. IEEE, 2008. P. 73-76.

16. A new cryptographic algorithm for the real time applications / Omari A. H. et al. Proceedings of the *7th International Conference on Information Security and Privacy*-(ISP’08), Cairo, Egypt, from Dec. 2008. Vol. 29. P. 33-38.

17. A new advanced cryptographic algorithm system for binary codes by means of mathematical equation / Ksasy M. S. et al. *ICIC Exp. Lett*. 2018. Vol. 12, No. 2. P. 117-125.

18. Jamel S., Herawan T., Deris M. M. A cryptographic algorithm based on hybrid cubes. *International Conference on Computational Science and Its Applications*. Berlin, Heidelberg : Springer, 2010. P. 175-187.

19. A block cryptographic algorithm for wireless sensor networks based on hybrid chaotic map / Luo Y. et al. *IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems* (HPCC/SmartCity/DSS). IEEE, 2019. P. 2790-2797.

20. Жданов О. Н., Соколов А. В. Алгоритм шифрования с переменной фрагментацией блока. *Проблемы и достижения в науке и технике*. 2015. №2. С. 153-159.

21. Sokolov A.V. Djiofack Temgoua Vanissa Noel. Nonlinear Properties of Rijndael S-boxes Represented by the Many-Valued Logic Functions. *Proceedings of the International Workshop on Cyber Hygiene*, Kyiv, Ukraine, November 30, 2019. P. 96-106.

22. Sokolov A.V., Radush V.V. Avalanche characteristics of Nyberg construction S-boxes represented by the many-valued logic functions. *Informatics & Mathematical Methods in Simulation,* 2019. No. 9 (3). P. 111-119.

23. Sokolov A.V., Radush V.V. A method for synthesis of S-boxes with good avalanche characteristics of component Boolean and quaternary functions. *Journal of Discrete Mathematical Sciences and Cryptography*. 2022. P. 1-12.

24. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. М.: КУДИЦ-ОБРАЗ, 2003. 240 с.

25. Соколов А.В., Корж А.О. Исследование режимов шифрования с пропуском блоков. *Информатика и математические методы в моделировании.* Т. 10 (2020), №. 1-2. С. 100-108

26. Sokolov A.V., Isakov D.A. Authenticated encryption mode with blocks skipping. *System analysis and applied information science*. Vol. 3. P. 59-65.

27. Жданов О.Н. Соколов А.В. Алгоритм построения оптимальных по критерию нулевой корреляции недвоичных блоков замен. Проблемы физики, математики и техники, 2015. № 3(24). С. 94–97.

28. Sokolov A. V., Zhdanov O. N. Correlation immunity of three-valued logic functions. *Journal of Discrete Mathematical Sciences and Cryptography*. 2020. P. 1-17.

29. Соколов А. В., Жданов О. Н. Нелинейные преобразования конструкции Ниберг над изоморфными представлениями полей Галуа. *Системный анализ и прикладная информатика*. 2017. №3. С. 59-66.

30. Nyberg K. Differentially uniform mappings for cryptography. I Advances in cryptology / K. Nyberg // Proc. of EUROCRYPT’93. Berlin, Heidelberg, New York. 1994. Vol.765, Lecture Notes in Compuer Springer-Verlag. P.55-65.

31. Соколов А.В., Жданов О.Н., Барабанов Н.А. Генератор псевдослучайных ключевых последовательностей на основе тройственных наборов бент-функций. *Проблемы физики, математики и техники*. 2016. №1(26). С. 85-91.

32. Мазурков М.И. Конструктивный способ построения первообразных неприводимых полиномов над простыми полями Галуа. *Радиоэлектроника (Изв. вузов)*. 1999. №2. С. 41-45.

33. Zhdanov O. N., Sokolov A. V. Block symmetric cryptographic algorithm based on principles of variable block length and many-valued logic. *Far East Journal of Electronics and Communications*. 2015. Vol. 16, No. 3. P. 573-589.

34. Ростовцев А. Г. Большие подстановки для программных шифров. *Проблемы инф. безопасности. Компьютерные системы*. СПб, 2000. № 3. С. 31-34.

35. Behrooz Parhami. Computer Arithmetic: Algorithms and Hardware Designs. New York: Oxford University Press, 2000. 510 p.

36. Stanković, R. S., Astola, J. T. Reminiscences of the Early Work in DCT: Interview with K.R. Rao. Reprints from the Early Days of Information Sciences. Tampere International Center for Signal Processing. 2012.88 p.

37. Heideman M. T., Johnson D. H., Burrus C. S. Gauss and the history of the fast Fourier transform. *IEEE ASSP Magazine*. 1984. No. 1 (4). P. 14-21.

38. Fino B.J., Algazi V.R. Unified Matrix Treatment of the Fast Walsh–Hadamard Transform. *IEEE Transactions on Computers*. 1976. No. 25 (11). P. 1142-1146.

39. Baleanu D. Wavelet Transform and Complexity. IntechOpen. 2019. 124 p.

40. VasudevanV., Ramakrishna M.A Hierarchical Singular ValueDecomposition Algorithm for Low Rank Matrices. arXiv: 1710.02812v2, 2019. P. 1-8.

41. Mukherjee P., Srivastava S., Lall B., et al. Adaptive Crypto-Steganosystem for videos based on Information Content and Visual Perception. Fifth National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics, 2015. Patna, India. doi: 10.1109/NCVPRIPG.2015.7490047

42. Shifa A., Afgan M. S., Asghar M., et al. Joint Crypto-Stego Scheme for Enhanced Image Protection With Nearest-Centroid Clustering. IEEE Access, 2018. Vol. 6. P. 16189 – 16206. doi: 10.1109/ACCESS.2018.2815037

43. Desai L., Mali S. Crypto-Stego-Real-Time (CSRT) System for Secure Reversible Data Hiding. Hindawi VLSI Design. 2018. P. 1-8. doi: 10.1155/2018/4804729

44. Seethalakshmi K.S. Use of Visual Cryptography and Neural Networks to Enhance

Security in Image Steganography. Journal of Computer Engineering, Special Issue – AETM. 2016. P. 57-61.

ВИСНОВКИ

У дисертаційній роботі вирішено важливу науково-прикладну проблему, що полягає у забезпеченні ефективності роботи крипто-стеганографічних систем в режимі реального часу на ресурсообмежених платформах, шляхом розробки відповідної методології. Відсутність подібних рішень щодо побудови КСС у роботах вітчизняних та зарубіжних дослідників обумовлює пріоритетність отриманих результатів.

В рамках досягнення мети роботи були отримані наступні результати:

1. Вперше на основі ЗПАІС розроблено теоретичний базис забезпечення ефективної роботи КСС у просторовій області, в рамках чого створено універсальний теоретичний інструментарій, що включає встановлений взаємозв'язок між трансформантами ДКП, перетворення Уолша-Адамара та сингулярним розкладанням матриць, взаємозв'язок між двовимірним та одновимірним перетворенням Уолша-Адамара, а також достатні умови забезпечення необхідних властивостей стеганоповідомлення в області трансформант Уолша-Адамара, що разом з методами оцінки криптографічної якості ФБЛ стало теоретичною основою розробленої методології.

2. Вперше на основі теоретичного базису забезпечення ефективності роботи КСС у просторовій області сформовано концепцію кодового управління вбудовуванням інформації у просторовій області, яка, на відміну від існуючих аналогів, дає змогу забезпечити ефективність роботи КСС в режимі реального часу на ресурсообмежених платформах.

3. Вперше на основі теоретичного базису забезпечення ефективності роботи КСС у просторовій області введено поняття коефіцієнту селективності κ та енергії E кодового слова, на основі яких визначено критерії побудови кодових слів T^+, T^-, що дають можливість забезпечення необхідних властивостей стеганоповідомлення при вбудовування ДІ у просторовій області в режимі реального часу. Побудовано множини бінарних та багаторівневих кодових слів T^+, T^- практично цінних розмірів 4×4, 8×8 і

16×16, що забезпечують високі значення коефіцієнта селективності, і впливають з високим степенем вибірковості на задані трансформанти ДКП.

4. Вперше на основі теоретичного базису забезпечення ефективності роботи КСС у просторовій області побудовано два стеганографічні методи з кодовим управлінням вбудовуванням на основі бінарних та багаторівневих кодових слів. Розроблені методи характеризуються значеннями показників ефективності, що перевищують найкращі сучасні аналоги: дозволяє забезпечити кількість помилок на рівні 1.6% при вилученні ДІ під дією атаки стиском проти вбудованого повідомлення з коефіцієнтом якості $QF=10$, що у 8.125 разів краще за подібний показник найкращого відомого сьогодні аналогу. При цьому значення показника PSNR складає 35.6 дБ, що на 3% перевершує значення найкращого відомого аналогу, який володіє сумірним рівнем стійкості до атак проти вбудованого повідомлення.

5. Подальший розвиток отримала технологія забезпечення множинного доступу до прихованого каналу на основі технології MC-CDMA та кодового управління вбудовуванням інформації, в результаті чого на основі бент-послідовностей, кодів Ріда-Соломона та розроблених кодів просторових розстановок запропоновано застосування кодів постійної амплітуді, а також розроблено два стеганографічні методи з множинним доступом, що дозволило підвищити пропускну спроможність стеганографічного методу при застосуванні технології множинного доступу на 6.25% в порівнянні із застосуванням коду Гаффмана для кодування групового сигналу, забезпечити кількість зареєстрованих у системі абонентів, що дорівнює $J=4800$ (у 1200 разів перевищує найкращий відомий аналог), а також кількість одночасно працюючих абонентів при нульовому рівні внутрішньосистемних перешкод, що дорівнює $J=64$ (у 16 разів перевищує найкращий відомий аналог).

6. Удосконалено математичний підхід до оцінки якості примітивів на основі застосування теорії ФБЛ, в результаті чого розроблено теоретичний базис оцінки та підвищення якості криптографічних примітивів, який

включає набір критеріїв криптографічної якості, які, на відміну від існуючих аналогів, дозволяють оцінювати якість криптографічних примітивів при їх представленні за допомогою компонентних ФБЛ.

7. Удосконалено криптографічні примітиви на основі застосування математичного підходу до оцінки їх криптографічної якості шляхом представлення у вигляді ФБЛ, в рамках чого розроблено: метод синтезу повної множини S-блоків довжини $N=16$, що, на відміну від існуючих аналогів, володіють максимальною нелінійністю як у сенсі їх уявлення за допомогою компонентних булевих функцій, так і ФБЛ; метод синтезу S-блоків, що задовольняють СЛК ФБЛ; метод синтезу класу з 12 врівноважених булевих функцій довжини $N=32$, які мають максимальну відстань нелінійності та задовольняють критерію розповсюдження $\mathrm{PC}(4)$; метод синтезу S-блоків довжини $N=3^k$, що дозволило отримати великі множини S-блоків, які відповідають критерію відсутності кореляційного зв'язку векторів виходу і входу, що дозволило синтезувати криптографічні примітиви: з 4-нелінійністю $N_{4f}=10.3431$, що до 21.55% перевищує значення найкращих відомих аналогів; покращити лавинні властивості криптографічних примітивів на 9.375% у порівнянні з найкращими відомими аналогами; покращити кореляційні властивості синтезованих криптографічних примітивів на 12.5%.

8. Подальший розвиток отримала конструкція Ніберг в рамках чого побудовано та досліджено повні множини S-блоків над усіма ізоморфними уявленнями полів $GF(p^k)$, $p=3,5$, що дозволило отримати великі множини високоякісних S-блоків більшого асортименту довжин.

9. Удосконалено БСШ прекодера на основі спільного використання криптографічних примітивів, що володіють високим рівнем криптографічної якості компонентних булевих функцій і ФБЛ та їх об'єднання на основі концепції змінної фрагментації блоків шляхом розробки шифру прекодера КСС, який характеризується підвищеною ефективністю: знищення статистики

вихідного тексту, на відміну від існуючих аналогів, досягається вже на першій ітерації основного кроку криптоперетворення, що дозволяє прискорити роботу прекодера для забезпечення роботи КСС у режимі реального часу на ресурсообмежених платформах.

10. Вперше на основі запропонованих методів синтезу криптографічних примітивів і концепції змінної фрагментації блоків запропоновано спосіб формування стеганографічного ключа під час застосування стеганографічного методу з кодовим управлінням вбудовуванням інформації, що дозволило забезпечити взаємозв'язок криптографічної та стеганографічної складової КСС, підвищити її криптографічну стійкість, забезпечуючи її ефективність при роботі з потоковим контейнером на ресурсообмежених платформах в режимі реального часу.

11. Вперше на основі ЗПАІС, теорії ФБЛ запропоновано науково-обґрунтовану методологію розробки КСС, використання якої підтвердило забезпечення високої ефективності відповідної КСС, зокрема в режимі реального часу з потоковим контейнером на відміну від існуючих аналогів, для яких взагалі не передбачено можливості реалізації на ресурсообмежених платформах. Зменшення кількості необхідних для роботи стеганографічного методу з кодовим управлінням вбудовуванням операцій у $4\mu/3$ разів порівняно із найкращим аналогом дозволило реалізацію розробленої КСС в умовах обмежених технічних ресурсів, зокрема при роботі із потоковим контейнером в режимі реального часу. При роботі з ЦВ роздільної здатності 400p/720p/1080p/1140p швидкість роботи КСС становить 1815/825/354/257 fps в режимі вбудовування та 236/106/47/33 fps в режимі вилучення ДІ на найпоширенішій IoT платформі Raspberry Pi 4 під керуванням Raspbian Pi OS. При цьому експериментально встановлено мінімально необхідні значення кількості операцій Single Thread ARM процесорів необхідні для роботи розробленої КСС, які при роботі з ЦВ роздільної здатності 400p/720p/1080p/1140p і частоти 30 fps для операції вбудовування ДІ,

складають 7.4/16.6/37.3/52.5/149.2/437.9 MOps/Sec та 53.5/120.3/270.6/380.8/1082.4/4329.6 MOps/Sec для операції вилучення ДІ, що відповідає характеристикам переважної більшості застосовуваних на сучасних ресурсообмежених пристроях процесорів.

Додаток А

Документи, що підтверджують впровадження результатів дисертаційної роботи

ПЛАНЕТА ЮГ
ОДЕССА

Украина, 65020, г.Одесса, ул. 10 Апреля,16
Почтовый адрес: 65020, г. Одесса, ул. 10 Апреля, 16
Тел.: (048) 705-74-96, E-mail: office@ps.od.ua

Р/с UA423052990000026000014912325 в АО КБ "ПриватБанк"
г. Одесса МФО 305299, код ОКПО 30747868, индивидуальный налоговый номер плательщика НДС 307478615538, свидетельство: №23235396

Затверджую
Директор
ТОВ Компанія «Планета-Юг»
_____ В.О.Коробко
«10» жовтня 2022р.

АКТ

про впровадження результатів дисертаційних досліджень Соколова Артема Вікторовича в функціонування підприємства ТОВ Компанія «Планета-Юг».

Комісія у складі: директора - Коробко В.О., технічного директора - Каліновського Р.Ю., адміністратора системи- Лебеденко С.В. провела тестування та випробування програмної реалізації цілісної крипто-стеганографічної системи, що заснована на засадах кодового управління вбудовуванням інформації у просторовій області та шифруванні послідовності переліку станів при її роботі на ресурсообмежених платформах нашого підприємства.

Комісія ВСТАНОВИЛА:

1. Представлена КСС, на відміну від існуючих аналогів, що засновані на використанні областей перетворень для свого функціонування може бути розгорнута та ефективно здійснювати захист інформації при роботі з потоковим контейнером у режимі реального часу на ресурсообмежених платформах.

2. На обчислювальних вузлах обробки відеоінформації підприємства, що засновані на процесорах сімейства Intel Pentium на базі ядра Kaby Lake та об'ємом оперативної пам`яті 8 Гб під керуванням операційної системи Windows 10, вимірювання часу обробки відео показало наступні результати:

- швидкість роботи КСС в режимі вбудовування додаткової інформації (включно із операцією попереднього шифрування та шифрування послідовності переліку станів): 139 кадрів / с;
- швидкість роботи КСС в режимі вилучення додаткової інформації (включно із операцією розшифрування вилученої ДІ та розшифрування послідовності переліку станів): 65 кадрів / с.

3. Отримані результати вимірювання швидкості роботи КСС підтверджують її здатність обробки потокового контейнера в режимі реального часу із більш ніж двократним запасом для відео з кадровою частотою 30 кадрів на секунду.

4. Відзначається зручність програмної та можливої апаратної реалізації КСС через її чітку структуру та можливості розпаралелювання обчислень.

Впровадження розробленої КСС у діяльність організації дозволило підвищити захист інформації, що обертається в інформаційних системах підприємства без необхідності застосування потужних обчислювальних пристроїв для забезпечення обробки потокового контейнера в режимі реального часу.

Директор _____ В.О.Коробко

Технічний директор _____ Р.Ю. Каліновський

ЗАТВЕРДЖУЮ

Генеральний директор
ТОВ «ТЕЛЕКАРТ-ПРИЛАД»

О.С. Козлов

«22» 03 2020 року

АКТ

про впровадження та використання результатів дисертаційного дослідження
на здобуття наукового ступеня доктора технічних наук

СОКОЛОВА АРТЕМА ВІКТОРОВИЧА

Комісія у складі:
Дерев'янко Ю.П., заступник генерального директора – начальник СКБ,
Баранов С.В., заступник начальника СКБ по ОКР,

склала цей акт про те, що зазначені нижче результати, отримані в дисертаційній роботі Соколова А.В., використані та впроваджені у діяльність підприємства ТОВ «Телекарт-Прилад».

Зокрема, були використані та впроваджені:

– метод уявлення конструкцій криптографічних алгоритмів за допомогою математичного апарату функцій багатозначної логіки та методи оцінки їх криптографічної якості, зокрема: нелінійність, алгебраїчний степінь нелінійності, критерій розповсюдження, критерій кореляційного імунітету функцій багатозначної логіки, які були використані з метою оцінки криптографічної якості застосовуваних криптографічних конструкцій, що забезпечило їх обґрунтований вибір;

– елементи теорії синтезу досконалих алгебраїчних конструкцій багатозначної логіки, зокрема, бент-послідовностей та досконалих недвійкових решіток, що були використані у схемах криптографічних генераторів псевдовипадкових ключових послідовностей та дозволили підвищити якість генерованих ними послідовностей та підвищити число рівнів захисту;

- метод шифрування зі змінною фрагментацією блоків, який у поєднанні з використанням запропонованих високоякісних криптографічних примітивів, що побудовані на основі функцій багатозначної логіки (максимально нелінійних S-блоків, S-блоків що відповідають суворому лавинному критерію та кореляційно імунних S-блоків), дозволив підвищити ефективність використовуваних засобів криптографічного захисту інформації.

Впроваджені результати, крім зазначеного, шляхом застосування методів оцінки якості криптографічних конструкцій, уявлених за допомогою функцій багатозначної логіки, дозволили скоротити терміни виконання науково-дослідних проектів та призвели до зменшення витрат за рахунок економії коштів, призначених на виконання практичних експериментів.

Заступник генерального директора – начальник СКБ Дерев'янко Ю.П.

Заступник начальника СКБ по ОКР Баранов С.В.

Затверджую

Директор Дець І.О.

ТОВ «Продукт – Постачання»

«21» 11 2019 р.

АКТ

про впровадження результатів дисертаційних досліджень Соколова Артема Вікторовича в функціонування підприємства ТОВ «Продукт - Постачання».

Комісія у складі: голови: директора ТОВ «Продукт - Постачання» Дець І.О., а також головного інженера Гавва Н.Г. провела тестування та випробування алгоритму блокового симетричного криптоалгоритму на основі принципів багатозначної логіки та методу змінної фрагментації блоків.

Комісія ВСТАНОВИЛА:

1. Імплементований блоковий симетричний криптоалгоритм на основі принципів багатозначної логіки та методу змінної фрагментації блоків за рахунок використання функцій багатозначної логіки може ефективно здійснювати шифрування інформації навіть у режимі "Електронної кодової книги", що є недосяжним для сучасних блокових симетричних криптографічних алгоритмів. Можливість використання режиму "Електронної кодової книги" дозволила знизити затрати на використання програмно-апаратних модулів захисту інформації близько на 10%. При цьому рівень криптографічного захисту інформації цих модулів підвищився, адже, як показують проведені комісією підрахунки, запропонований криптографічний алгоритм досягає астрономічної величини числа рівнів захисту $\Psi = 3.2292 \cdot 10^{114}$, що в $2.8 \cdot 10^{37}$ разів перевищує число рівнів захисту криптографічного алгоритму AES256.

3. Надані на тестування повні класи S-блоків підстановки, що апроксимуються поліномами АНФ (алгебраїчної нормальної форми) максимального алгебраїчного степеню нелінійності, відповідають критерію високої нелінійності (у сенсі віддалення від функцій Віленкіна-Крестенсона), відповідають суворому лавинному критерію та відповідають критерію відсутності кореляційного зв'язку між векторами виходу і входу дозволяють говорити про можливість їх використання в якості (довгострокового ключа), який може бути оперативно змінений при необхідності, що модифікує структуру криптоалгоритму. Використання наданих методів синтезу криптографічних примітивів надають фактично необмежені можливості масштабування числа рівнів захисту розробленого криптоалгоритму, що дозволило підприємству адаптувати його для здійснення криптографічного захисту інформації з різним рівнем доступу.

Директор
Дець І.О. ...

Головний інженер
Гавва Н.Г. ...

Затверджую

Директор Коваленко Є.В.

ТОВ «Бізнес – Центр НТЦ»

«18» 12 2019 р.

АКТ

про впровадження результатів дисертаційних досліджень Соколова Артема Вікторовича в функціонування підприємства ТОВ «Бізнес - Центр НТЦ».

Директор Коваленко Є.В. провів тестування та випробування новітнього генератора псевдовипадкових ключових послідовностей на основі троїстих наборів 3-бент-послідовностей.

ВСТАНОВЛЕНО:

1. Імплементований генератор псевдовипадкових ключових послідовностей на основі троїстих наборів 3-бент-послідовностей дозволяє генерування гами, що повністю задовольняють критеріям стохастичної якості згідно до набору статистичних тестів NIST. При цьому виявляється, що максимальна амплітуда бічного пелюстка тритової автокореляційної функції в середньому у ~ 2 рази менша за амплітуду бічного пелюстка бітової автокореляційної функції класичних генераторів псевдовипадкових ключових послідовностей. Екстремальні нелінійні властивості 3-бент-послідовності дозволяють говорити про максимальний рівень реалізації конфузії у розробленому генераторі.

2. Результати тестування показують можливість використання розробленого генератора в якості потокового алгоритму шифрування (у схемі шифра Вернама з коротким ключем), при цьому програмно-апаратна реалізація такого генератора є значно простішою за реалізацію класичних блокових симетричних криптоалгоритмів типу «Калина» (ДСТУ 7624:2014), що дозволяє говорити про зменшення затрат на виготовлення криптографічних підсистем захисту інформації більш ніж на 25%.

3. Надані на тестування повні класи 3-бент-послідовностей (синтезовані за допомогою регулярних методів та класифіковані на троїсті набори) роблять можливим розглядати використані у генераторі бент-послідовності в якості (довгострокового) ключа, а також дозволяє легко змінювати криптографічну стійкість генератора в процесі його роботи за рахунок використання 3-бент-послідовностей більшою довжини.

Директор
ТОВ «Бізнес - Центр НТЦ» Є. КОВАЛЕНКО

ЗАТВЕРДЖУЮ
Проректор з наукової та науково-педагогічної роботи одеського нац ціонального політехнічного університету

Д.В. Дмитришин

«09» 02 2021 року

АКТ

про впровадження та використання результатів дисертаційного дослідження на здобуття наукового ступеня доктора технічних наук

СОКОЛОВА АРТЕМА ВІКТОРОВИЧА

Комісія в складі: зав. каф. радіоелектронних і телекомунікаційних систем (РТС), к.т.н. Цевуха І.В., доц. каф. РТС, к.т.н. Аверочкіна В.О., доц. каф. РТС, к.т.н. Садченка А.В. склала цей акт про те, що результати, отримані в дисертаційній роботі Соколова А.В., та які зазначені нижче, використані та впроваджені при виконанні науково-дослідної робіти за темою: «Підвищення ефективності методів цифрової обробки сигналів в радіотехнічних системах», номер в ОНПУ 60-57, державний реєстраційний номер 0111U009481.

Зокрема, були використані та впроваджені:

— методи проведення спектральної класифікації повного коду двійкових послідовностей, а також результати спектральної класифікації повного коду для довжин послідовностей $N = 16, 20, 24, 32$, що дозволило провести оцінку можливих потужностей С-кодів для зменшення значення PAPR у системах з використанням технології розділення каналів MC-CDMA;

-– методи та результати проведення спектральної класифікації повного коду недвійкових послідовностей довжини $N = 9$, які дозволили провести оцінку можливих потужностей недвійкових С-кодів, що використовуються для зменшення PAPR у системах з використанням технології розділення каналів MC-CDMA;

— елементи теорії синтезу недвійкових бент-послідовностей, які дозволили синтезувати повні множини цих досконалих алгебраїчних конструкцій, що стало основою для побудови С-кодів постійної амплітуди.

Впроваджені результати, крім зазначеного, дозволили скоротити терміни виконання науково-дослідної роботи за зазначеною темою та призвели до зменшення витрат за рахунок економії коштів, призначених на виконання практичних експериментів.

Науковий керівник НДР **І.В. Цевух**

Відповідальний виконавець НДР **А.В. Садченко**

ЗАТВЕРДЖУЮ
Проректор з наукової та науково-педагогічної роботи одеського національного політехнічного університету

_____ Д.В. Дмитриєнко

«09» 02 2021 року

АКТ

про впровадження та використання результатів дисертаційного дослідження
на здобуття наукового ступеня доктора технічних наук

СОКОЛОВА АРТЕМА ВІКТОРОВИЧА

Комісія в складі: зав. каф. радіоелектронних і телекомунікаційних систем (РТС), к.т.н. Цевуха І.В., доц. каф. РТС, к.т.н. Аверочкіна В.О., доц. каф. РТС, к.т.н. Садченка А.В. склала цей акт про те, що результати, отримані в дисертаційній роботі Соколова А.В., та які зазначені нижче, використані та впроваджені при виконанні науково-дослідної робіти за темою: «Оптимізація методів цифрової обробки інформації в корпоративних мережах та радіотехнічних системах», номер в ОНПУ 123-57, державний реєстраційний номер 0116U004923.

Були використані і впроваджені результати, що стосуються розробленої методології оцінки криптографічної якості елементів шифрів, які використовуються у телекомунікаційних та радіотехнічних системах, зокрема:

—критерій алгебраїчної степені нелінійності і показник відносної алгебраїчної степені нелінійності компонентних функцій багатозначної логіки, які дозволили провести оцінку алгебраїчної складності конструкцій криптографічних алгоритмів;

—критерій нелінійності і показник відносної алгебраїчної нелінійності компонентних функцій багатозначної логіки, які дозволили провести оцінку дистанційних властивостей криптографічних конструкцій щодо найбільш лінійних структур;

—критерій розповсюдження помилки та показники максимального та інтегрального відхилення від суворого лавинного критерію функцій багатозначної логіки, що дозволяють провести оцінку диференційних властивостей криптографічних конструкцій у сенсі компонентних функцій багатозначної логіки;

—критерій відсутності статистичного зв'язку виходу криптографічних конструкцій від їх вхідних змінних і показники максимального та інтегрального відхилення від критерію відсутності статистичного зв'язку виходу криптографічних конструкцій від їх вхідних змінних, які дозволяють оцінити кореляційні властивості криптографічних конструкцій у сенсі компонентних функцій багатозначної логіки.

Впроваджені результати, крім зазначеного, дозволили скоротити терміни виконання науково-дослідної роботи за зазначеною темою та призвели до зменшення витрат за рахунок економії коштів, призначених на виконання практичних експериментів.

Науковий керівник НДР **І.В. Цевух**

Відповідальний виконавець НДР **А.В. Садченко**