МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

СОКОЛОВ
АРТЕМ ВІКТОРОВИЧ

УДК 004.056.55

МЕТОДОЛОГІЯ РОЗРОБКИ ЕФЕКТИВНОЇ КРИПТО-СТЕГАНОГРАФІЧНОЇ СИСТЕМИ

05.13.21 — Системи захисту інформації

Р Е Ф Е Р А Т
дисертації на здобуття наукового ступеня
доктора технічних наук

Львів — 2023

Дисертацією є рукопис.
Робота виконана в Національному університеті «Одеська політехніка» Міністерства освіти і науки України.

Науковий консультант: доктор технічних наук, професор
Кобозєва Алла Анатоліївна,
Національний університет «Одеська політехніка»,
завідувач кафедри кібербезпеки та програмного забезпечення, м. Одеса

Офіційні опоненти: доктор технічних наук, професор
Хорошко Володимир Олексійович
Національний авіаційний університет,
професор кафедри безпеки інформаційних технологій, м. Київ

заслужений діяч науки і техніки України, лауреат Державної премії України в галузі науки і техніки,
доктор технічних наук, професор
Шелест Михайло Євгенович,
Національний університет «Чернігівська політехніка»,
професор кафедри кібербезпеки та математичного моделювання, м. Чернігів

доктор технічних наук, професор
Мілов Олександр Володимирович,
Національний технічний університет «Харківський політехнічний інститут»,
професор кафедри кібербезпеки, м. Харків

Захист відбудеться «__» _____ 2023 р. о ____ на засіданні спеціалізованої вченої ради в Національному університеті «Львівська політехніка» за адресою: 79013, м. Львів, вул. Ст. Бандери, 12, ауд. 226.

З дисертацією можна ознайомитись у науково-технічній бібліотеці Національного університету “Львівська політехніка” за адресою: 79013, м. Львів, вул. Професорська, 1.

Реферат розісланий «__» _____ 2023 р.

Виконувач обов'язків вченого секретаря
спеціалізованої вченої ради,
д.т.н., проф. О.А. Нємкова

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Повсюдне впровадження інформаційних технологій в усі сфери людської діяльності, зокрема, бурхливий розвиток мобільних платформ, пристроїв Internet of Things (IoT), Internet of Battlefield Things (IoBT), безпілотних літальних апаратів (БПЛА), призводить до істотного збільшення значення методів захисту інформації у задачах забезпечення безпеки та комфорту як окремих громадян та організацій, так і у задачі забезпечення безпеки та добробуту держави.

Історично виділяють два основні напрямки розвитку конструктів, що лежать в основі побудови систем захисту інформації: криптографічний (заснований на ідеї перетворення інформації таким чином, що унеможливлює її отримання без знання спеціального ключа) та стеганографічний (заснований на ідеї приховування самого факту наявності інформації, що захищається). Тим не менш, на сьогодні провідні вітчизняні та зарубіжні дослідники сходяться на тому, що через істотне збільшення мультимедіа контенту, насамперед цифрових зображень (ЦЗ) та цифрових відео (ЦВ) у світовому трафіку, окреме застосування криптографічної або стеганографічної компоненти для побудови повноцінної сучасної системи захисту інформації є неефективним та недостатнім. Отже, теоретично і практично обумовленим сучасним трендом розвитку систем захисту інформації є використання двох невід'ємних, залежних одна від одної, впливаючих одна на одну, складових: криптографічної та стеганографічної, необхідність врахування зв'язку та взаємного впливу яких приводить до формування принципово нового поняття крипто-стеганографічної системи (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. Означене має негативні наслідки: подібні перетворення (сингулярне розкладання, дискретне косинусне перетворення (ДКП), вейвлет-перетворення та ін.) характеризуються значною обчислювальною складністю, збільшенням ймовірності помилок округлення, через які можливі спотворення додаткової інформації (ДІ), 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.

Зв’язок роботи з науковими програмами, планами, темами. Тематика роботи та її результати безпосередньо пов’язані зі Стратегією національної безпеки України від 14 вересня 2020 № 392/2020; Стратегією кібербезпеки України від 27 січня 2016 року №96/2016; Законом України Про основні засади забезпечення кібербезпеки України від 24.10.2020 №2163-VIII. 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 впроваджені 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 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).

Для досягнення поставленої мети в роботі 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: матричний аналіз, теорія інформації та кодування, теорія досконалих алгебраїчних конструкцій, загальний підхід до аналізу стану й технології функціонування інформаційних систем (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: теорія ФБЛ та теорія криптоаналізу. Для оцінки якісних і кількісних характеристик розроблених КСС використовувалися: теорія алгоритмів, методи математичного моделювання та методи оцінки стохастичної якості.

Наукова новизна отриманих результатів полягає у наступному:

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 примітиви 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 примітивів 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 примітивів на 12.5%.

На базі сконструйованих у дисертаційній роботі криптографічних примітивів, що засновані на ФБЛ, розроблено спосіб формування стеганографічного ключа, 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 роботи. Наукові результати і основні положення дисертації доповідалися та обговорювалися на 18 Міжнародних і Всеукраїнських конференціях, форумах, семінарах, у тому числі на семінарі при Вченій раді НАН України «Технічні засоби захисту інформації» (2020-2022 рр.).

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.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** розкрито сутність і стан наукової проблеми та обґрунтовано її актуальність, визначено мета й завдання роботи, показано наукову новизну та практичну значущість отриманих результатів, наведено інформацію про особистий внесок здобувача, апробацію та впровадження наукових результатів роботи.

У **першому розділі** на основі проведеного аналізу наукових джерел по темі дисертації встановлено, що проблема, яка полягає у забезпеченні ефективності роботи КСС в режимі реального часу на ресурсообмежених платформах не є вирішеною та залишається актуальною.

Встановлено, що для забезпечення всебічного захисту інформації, необхідністю є об’єднання криптографічного та стеганографічного підходу, що приводить до формування визначення КСС — складного комплексу, загальна стійкість якого не визначається лише стійкістю застосованого криптографічного чи стеганографічного перетворення. Стійкість усієї системи залежатиме від правильного узгодження криптографічної і стеганографічної складових системи. У сьогоденні науковці здебільше розглядають окремо криптографічні та стеганографічні складові, при цьому питання їх одночасного ефективного функціонування із врахуванням сучасних особливостей інформації, що захищається, практично не розглядається. Окрім цього, при використанні КСС 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 й можливість їх роботи із ЦЗ та ЦВ у режимі реального часу, що є невід’ємною складовою багатьох сучасних інформаційних систем.

На сьогодні у відкритих літературних джерелах наведені лише концептуальні факти щодо необхідності об’єднання криптографічної та стеганографічної складових для організації ефективного захисту інформації. І хоча поняття КСС не є новим, 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.

Ефективність стеганографічних систем забезпечується, як правило, за рахунок використання 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 можуть функціонувати на ресурсообмежених платформах.

Для оцінки і порівняння якості криптографічних складових, сьогодні використовується лише підхід, заснований на математичному апараті компонентних булевих функцій, якими не обмежуються можливості криптоаналітика під час здійснення атак криптоаналізу, що призводить до необхідності розгляду представлення конструкцій криптографічних алгоритмів всіма можливими способами. Такий підхід обумовлює необхідність створення набору критеріїв криптографічної якості ФБЛ для простих значень q та значень q, що є степенем простого числа p: $q = p^k$. Встановлено, що у сучасних відкритих літературних джерелах фактично відсутні методи синтезу криптографічних примітивів, які б одночасно задовольняли як критеріям криптографічної якості їх компонентних булевих функцій, так і компонентних ФБЛ, а також ефективних 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.

Таким чином, залишаються актуальними питання побудови ефективних КСС, що забезпечують можливість роботи на ресурсообмежених платформах, шляхом розробки відповідної науково-обґрунтованої методології.

Другий розділ присвячений розробці загального теоретичного базису забезпечення певних властивостей стеганографічних методів, основ кодового управління вбудовуванням ДІ в просторовій області контейнера.

Забезпечення ефективності стеганографічної компоненти КСС вимагає апріорне забезпечення заданих властивостей стеганоповідомлення, зокрема стійкість до атак проти вбудованого повідомлення, надійність сприйняття, що потребує наявності відповідних достатніх умов. З урахуванням високої обчислювальної ефективності, прозорості взаємозв'язку з просторовою областю, а також відповідності архітектурним особливостям сучасних процесорів, перспективним для сучасних КСС є використання простору перетворень Уолша-Адамара.

Для проведення стеганоперетворення в роботі використовується блоковий підхід, коли вбудова ДІ робиться в окремі блоки, що отримуються в результаті розбивки матриці контейнера. Це, з урахуванням мети роботи, обумовлено декількома причинами: відносною простотою забезпечення стійкості відповідних стеганометодів до стиску з втратами для можливості збереження стеганоповідомлення в найбільш поширених форматах; забезпеченням незначної обчислювальної складності при послідовній реалізації алгоритму, яка для контейнера з $n \times n$-матрицею визначається як $\underline{O}\left(n^2\right)$; можливістю легкого розпаралелювання процесу шляхом одночасного стеганоперетворення декількох блоків.

Нехай X — матриця блоку контейнера розміру $N \times N$. Перетворення Уолша-Адамара для X відповідає формулі:

$$W = H'_N X H'^T_N, \qquad (1)$$

де H'_N — нормована матриця Уолша-Адамара порядку $N{=}2^k$, $H'_N = (1/N)H_N$, H_N будується у відповідності з конструкцією Сильвестра

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

Для отримання достатніх умов забезпечення певних властивостей стеганоповідомлення в просторі перетворення Уолша-Адамара встановлено взаємозв’язок між трансформантами областей, де такі умови наявні, а саме ДКП, сингулярного розкладання матриці блока та перетворення Уолша-Адамара. Кожна з функцій Уолша, не бувши гармонійною, характеризується частістю, яка є аналогом частоти для гармонійних функцій. Більше того, кожна з функцій Уолша має природну відповідність з гармонікою на часовому проміжку $t \in [0,1]$, при якому частість функції Уолша буде тим більшою, чим більша частота відповідної гармоніки. Позначимо як $H_N(i,:)$—*i*-ий рядок матриці H_N, відповідність між початковими рядками H_N та гармонійними функціями матиме вигляд

$$\begin{gathered} H_N(1,:) \;\to\; \sin(\pi t), H_N(2,:) \;\to\; \sin(N\pi t), H_N(3,:) \;\to\; \sin(N/2\pi t), \\ H_N(4,:) \;\to\; \cos(N/2\pi t), \ldots \text{і т.д.} \end{gathered} \tag{3}$$

Найбільшу частість серед рядків матриці Уолша-Адамара завжди матиме $H_N(2,:)$, для якої $\overline{\eta} = N/2 = 2^{k-1}$; найбільшу частоту з усіх відповідних гармонік (3) має гармоніка $\sin(N\pi t)$, що їй відповідає. Нехай $X = E$, де E — одинична матриця відповідного розміру. У цьому випадку результат співвідношення (1) не залежатиме від матриці зображення, а визначатиметься тільки коефіцієнтами матриці Уолша-Адамара

$$\begin{aligned} H'_N H'_N &= \frac{1}{N^2}\begin{pmatrix} H_N(1,:) \\ H_N(2,:) \\ \ldots\ldots\ldots\ldots \\ H_N(N,:) \end{pmatrix} \cdot \left((H_N(1,:))^T, (H_N(2,:))^T, \ldots, (H_N(N,:))^T \right) = \\ &= \frac{1}{N^2}\begin{pmatrix} H_N(1,:)(H_N(1,:))^T, H_N(1,:)(H_N(2,:))^T, \;\ldots, H_N(1,:)(H_N(N,:))^T \\ H_N(2,:)(H_N(1,:))^T, H_N(2,:)(H_N(2,:))^T, \;\ldots, H_N(2,:)(H_N(N,:))^T \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ H_N(N,:)(H_N(1,:))^T, H_N(N,:)(H_N(2,:))^T, \;\ldots, H_N(N,:)(H_N(N,:))^T \end{pmatrix}. \end{aligned} \tag{4}$$

З урахуванням (3) та (4), відповідності між функціями Уолша та гармоніками, а також формул перетворення добутку тригонометричних функцій у суму доведено:

Твердження 1. У матрицях W (1) високочастотним/низькочастотним складовим блоку ЦЗ будуть відповідати елементи, які знаходяться на перетинанні рядків і стовпців, що відповідають дискретним функціям Уолша з найбільшими/найменшими частостями.

Відповідно до Твердження 1 у матриці W (2) елемент (2,2) буде відповідати найбільш високочастотній складовій *X*, частина високочастотних складових буде локалізована в межах другого рядка і другого стовпця матриці W, незалежно від її розміру, де низькочастотні складові відсутні.

Для отримання точної відповідності між трансформантами Уолша-Адамара та ДКП, розв’язку задачі синтезу кодових слів для забезпечення кодового управління

вбудовуванням ДІ в роботі встановлено взаємозв'язок між одновимірним та двовимірним перетвореннями Уолша-Адамара та ДКП.

Для зручності представлення наступних викладок введемо таке позначення: оператор $\tilde{A}$ означає перетворення матриці A порядку N у вектор-рядок довжини N^2 шляхом послідовної конкатенації рядків вихідної матриці.

Нехай $b_i(k)$ — повний двійковий код довжини n, де $i = 0,1,...,n-1$, $n = \log_2 N$, $k = 0,1,...,N-1$, а одновимірне перетворення Уолша-Адамара деякого вектора Y довжини N задається за допомогою наступного співвідношення

$$V_\omega = \sum_{x=0}^{N-1} Y_x (-1)^{\sum_{i=0}^{n-1} b_i(x) b_i(\omega)}, \; x, \omega = 0,1,...,N-1, \tag{5}$$

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

Розрахункове співвідношення, що визначає двовимірне перетворення Уолша-Адамара матриці X розміру $N \times N$ має вигляд

$$W_{u,v} = \frac{1}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} X_{x,y} \left[(-1)^{\sum_{i=0}^{n-1} b_i(x) b_i(u) + b_i(y) b_i(v)} \right], \; u, v = 0,1,...,N-1. \tag{6}$$

Вираз (5) щодо векторів-рядків і отриманих в результаті рядкової конкатенації матриць W і X у вектори-рядки $\tilde{W}$ та $\tilde{X}$, відповідно, може бути записаний наступним чином

$$\tilde{W}_w = \frac{1}{N} \sum_{z=0}^{N^2-1} \tilde{X}_z \cdot (-1)^{\sum_{i=0}^{n-1} b_i(z//N) b_i(w//N) + b_i(z \bmod N) b_i(w \bmod N)}, \tag{7}$$

де $z, w = 0,1,...,N^2-1$ — індекс векторів-рядків $\tilde{X}$ та $\tilde{W}$, відповідно, а символ // позначає операцію цілочисельного ділення.

Частина виразу (7) $b_i(z//N) b_i(w//N)$ 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 (7) $b_i(z \bmod N) b_i(w \bmod N)$ 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 (7) 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 (5) 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 $1/N$, одновимірному перетворенню вектора $\tilde{X}$, що доводить наступне твердження.

Твердження 2. Трансформанти двовимірного перетворення Уолша-Адамара блока X при їх поданні у вигляді вектора-рядка можуть бути знайдені за допомогою наступного співвідношення

$$\tilde{W} = \tilde{X}\, A_1, \qquad (8)$$

де A_1 — матриця порядку N^2, що являє собою матрицю Уолша-Адамара H_{N^2} порядку N^2, яка побудована відповідно до конструкції Сільвестра з точністю до коефіцієнта $1/N$.

Зауваження. Вираз (8) є справедливим і для інших двовимірних перетворень, наприклад, ДКП, однак його обчислення потребує додаткового знаходження матриці A_1.

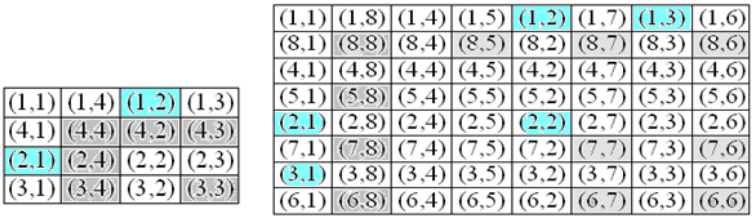


Рис.1. Відповідність між трансформантами Уолша-Адамара та ДКП для *N*×*N*-блоків ЦЗ: а — $N = 4$; б — $N = 8$

На основі проведених досліджень з урахуванням Тверджень 1,2 в роботі встановлено взаємозв'язок між трансформантами Уолша-Адамара та частотними складовими блока ЦЗ, який наочно представлений на рис. 1, на прикладі практично-значущих розмірів матриці перетворення $N = 4;8$.

Встановлений зв'язок дозволив отримати в області перетворення Уолша-Адамара достатні умови забезпечення певних властивостей стеганоповідомлень, незалежно від використовуваного стеганоалгоритму та області ЦЗ-контейнера, що задіюється безпосередньо для вбудови ДІ.

Твердження 3 ***(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, що відповідають високочастотним складовим блоку (локалізація наведена на рис. 1 для $N \times N$-блоків розміру $N \in \{4,8\}$ за допомогою сірої заливки).

Твердження 4 ***(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 перетворень Уолша-Адамара його результатом було збурення елементів, що відповідають низькочастотним складовим блоку (локалізація наведена на рис. 1 для $N \times N$-блоків розміру $N \in \{4,8\}$ за допомогою блакитної заливки).

Отримані результати є теоретичною основою для кодового управління частотними складовими, що зазнають збурення в результаті вбудовування інформації. Сутність кодового управління вбудовуванням інформації, дозволяє забезпечити задані властивості стеганоповідомлення у просторовій області при незначних обчислювальних витратах і збуреннях, що вносяться у контейнер під час адитивного вбудовування: ± 1. При цьому, в кожний блок контейнера вбудовується один біт ДІ, який рівномірно розподіляється між елементами даного блоку.

Нехай блок $X = \|x_{i,j}\|, i, j, = 0,1,..., N-1$ деякого ЦЗ або кадру ЦВ є матрицею розміру $N \times N$, тоді як d — біт ДІ, який має бути вбудований у даний блок

зображення. У відповідність даному біту ставиться кодове слово T, розміру $N \times N$ за допомогою якого відбувається вбудовування біта d.

Тоді блок стеганоповідомлення M, матиме вигляд

$$\tilde{M} = \tilde{X} + \tilde{T}. \quad (9)$$

Розглянемо, враховуючи Твердження 2, перетворення Уолша-Адамара вектора-рядка M

$$\tilde{W} = \tilde{M} H_{N^2} = (\tilde{X} + \tilde{T}) H_{N^2} = \tilde{X} H_{N^2} + \tilde{T} H_{N^2}. \quad (10)$$

Вираз (10) дозволяє зробити фундаментальний висновок про природу збурення трансформант Уолша-Адамара в стеганоповідомленні після адитивного вбудовування в нього ДІ — величина і локалізація подібних збурень залежатиме від конкретного виду доданку $\tilde{T} H_{N^2}$, що являє собою трансформанти Уолша-Адамара вектора-рядка $\tilde{T}$, за допомогою якого закодовано біт ДІ d.

Отже, для здійснення кодового управління вбудовуванням ДІ, її біти мають попередньо кодуватися такими кодовими словами розміру $N \times N$, що забезпечують вибірковий вплив на ту чи іншу трансформанту Уолша-Адамара, і, таким чином, на трансформанту ДКП. Застосування такого попереднього кодування дозволяє, обмеживши вплив на кожен конкретний елемент контейнера одиничною амплітудою, здійснювати зосереджений вплив на задану трансформанту перетворення Уолша-Адамара обраного блоку розміру $N \times N$, тим самим забезпечуючи задані властивості стеганоперетворення в залежності від того, на яку саме трансформанту такий вплив здійснюється.

Таким чином, маючи обчислювальну складність та величину збурень контейнера, що еквівалентні класичному методу LSB-matching, стає можливим формування гнучкості забезпечення заданих властивостей стеганоповідомлення, як у стеганографічних методів, що працюють в областях перетворень.

Не обмежуючи загальності для класифікації можливих кодових слів, які призводять до збурення тієї чи іншої трансформанти Уолша-Адамара, було запропоновано визначення елементарної структури.

Визначення 1. Елементарною структурою вектору трансформант Уолша-Адамара назвемо набір різних спектральних компонент із зазначенням їх частот у векторі.

Таким чином, шляхом конструювання кодових слів, за допомогою яких представляються елементи ДІ, стає можливим здійснювати передбачуваний та контрольований вплив на будь-які задані трансформанти контейнера.

Найбільшу практичну цінність становить максимізація впливу на ту чи іншу трансформанту Уолша-Адамара, яка може бути забезпечена через застосування кодових слів, що володіють елементарною структурою $\{N(1), 0(N-1)\}$, де перед круглими дужками вказано амплітуду наявної трансформанти Уолша-Адамара, а у круглих дужках — кількість разів, які вона зустрічається. 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 у матриці Уолша-Адамара. На основі даного вектору-рядка,

відповідно до Твердження 2 може бути сформована матриця кодового слова D, що представляє черговий елемент ДІ.

Додавання такого кодового слова до матриці-блоку контейнера (9) відповідно до (10) призведе до цілеспрямованого впливу на заданий коефіцієнт перетворення Уолша-Адамара, а отже, враховуючі дані, представлені на рис. 1, і на задану частотну складову контейнера. Таким чином, враховуючі Твердження 3 і Твердження 4, шляхом конструювання ансамбля кодових слів, що впливають на задану трансформанту Уолша-Адамара, забезпечуються необхідні властивості стеганоповідомлення, при збереженні мінімального (у межах амплітуди, що дорівнює 1) випливу на кожен конкретний елемент контейнера, та здійсненні вбудовування у просторовій області контейнера.

$$T_1^+ = \begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \end{bmatrix}, \quad W_1^+ = \begin{bmatrix} 0 & 0 & 16 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix};$$

$$T_2^+ = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \end{bmatrix}, \quad W_2^+ = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix};$$

$$T_3^+ = \begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \end{bmatrix}, \quad W_3^+ = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 16 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix};$$

$$T_4^+ = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \quad W_4^+ = \begin{bmatrix} 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Рис. 2. Набір кодових слів порядку $N = 4$, що забезпечують стійкість до атак проти вбудованого повідомлення

На рис. 2 представлено кодові слова, що забезпечують стійкість до атак проти вбудованого повідомлення. Подібним чином можуть бути побудовані кодові слова будь-якого необхідного порядку N, що забезпечують будь-які необхідні властивості стеганоповідомлення.

Результати, що отримані в розділі 2, належать теоретичній складовій методології, що розроблюється у роботі та дозволяють сформувати теоретичний базис для кодового управління вбудовуванням ДІ.

У **третьому розділі** на основі розробленого теоретичного базису виконується розробка стеганографічних методів з кодовим управлінням вбудовуванням ДІ на основі бінарних та багаторівневих кодових слів розміру $\mu \times \mu$, що дозволяють забезпечити задані властивості стеганоповідомлення, здійснюючі стеганоперетворення у просторовій області. Стеганографічний метод з кодовим управлінням вбудовуванням ДІ на основі бінарних кодових слів представлений на рис. 3. Результати тестування стеганографічного методу з кодовим управлінням вбудовуванням на основі бінарних кодових слів $T_{b,\mu,(n,m)}$, що цілеспрямовано впливають на задані трансформанти Уолша-Адамара (n,m) під впливом різних атак проти вбудованого повідомлення представлені на рис. 4.

Встановлений зв'язок 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 більшості кодових слів (рис. 2) є вплив не тільки на бажану трансформанту ДКП, але і на деякі інші трансформанти ДКП, що зменшує селективність впливу на ту чи іншу частотну складову матриці-блоку контейнера.

Нехай

$$E = \sum_{i=1}^{\mu} \sum_{j=1}^{\mu} t_{i,j}^2 , \tag{11}$$

Вбудовування ДІ

Крок 1. Розбити стандартним чином $m \times n$-матрицю контейнера P на $\mu \times \mu$-блоки. Нехай B — довільний блок, що використовується для вбудовування ДІ.

Крок 2. Визначити J — загальна кількість кодових слів;

$$\lambda = \log_2 J$$

— кількість біт ДІ, що вбудовуються в кожний черговий блок контейнера.

Крок 3. Сформувати $m/\mu \times n/\mu$-матрицю ДІ $\overline{D}$, кожний елемент d_{ij} якої визначається λ бітами ДІ, що вбудовуються у відповідний блок B.

Крок 4. Провести кодування $\overline{D}$ шляхом подання кожного d_{ij} за допомогою кодових слів $\{T_i^+\}$ та їх інверсій $\{T_i^-\}$. Результат — $m \times n$-матриця D.

Крок 5. Вбудувати ДІ в контейнер відповідно до формули:

$$M = P + D,$$

де M — матриця стеганоповідомлення.

Декодування ДІ

Крок 1. Побудувати $m \times n$-матрицю:

$$W = \overline{M} - P,$$

де $\overline{M}$ — матриця можливо збуреного стеганоповідомлення.

Розбити W стандартним чином на $\mu \times \mu$-блоки Δ_r, $r = 1, 2, \ldots, mn$.

Крок 2. Для кожної T_i^+ і кожної Δ_r розрахувати

$$\sigma_j = \sum_{k=0}^{\mu-1}\sum_{l=0}^{\mu-1} \Delta_r(l,k) T_i^+(l,k), \quad j = 0,1,\ldots, J/2-1.$$

Крок 3. Для кожного Δ_r визначити:

$$\sigma_{\tilde{j}} = \max_j \sigma_j,$$

при цьому $T_{\tilde{j}}^?$ - декодоване кодове слово, знак знайденого максимуму відповідає знаку, з яким $T_{\tilde{j}}^?$ було вбудовано (прямий або інверсний вигляд).

Рис. 3. Стеганографічний метод з кодовим управлінням вбудовуванням для бінарних кодових слів

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 $|c_{n,m}|$ та зменшенні $\sum_{i=0}^{\mu-1}\sum_{j=0}^{\mu-1} |c_{i,j}|$.

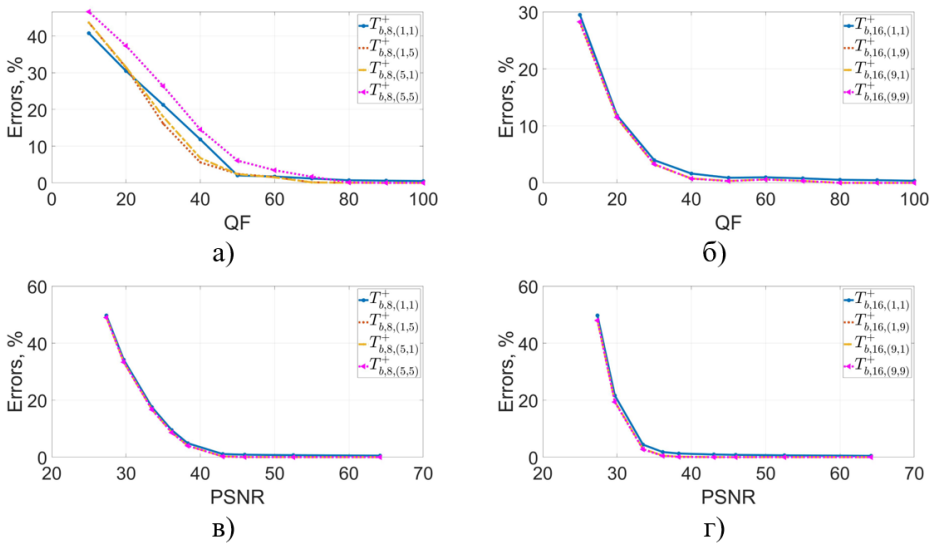


Рис. 4. Кількість помилок при декодуванні стеганоповідомлення: а) під атакою стисненням JPEG, розмір блоку $\mu = 8$, б) під атакою стисненням JPEG, розмір блоку $\mu = 16$, в) під атакою зашумленням, розмір блоку $\mu = 8$, г) під атакою зашумленням, розмір блоку $\mu = 16$

енергії застосовуваних кодових слів, $t_{i,j}$ — елементи кодового слова.

Для кількісної оцінки селективності впливу кодового слова на частотні складові стеганоповідомлення введено коефіцієнт селективності

$$\kappa = \frac{|c_{n,m}|}{\sum_{i=0}^{\mu-1}\sum_{j=0}^{\mu-1}|c_{i,j}|}, \quad (12)$$

де $c_{i,j}$, $i, j = 1,2,\ldots,\mu$ — коефіцієнти ДКП кодового слова T, n,m — індекси по рядкам і стовбцям трансформанти ДКП, на яку зосереджено вплив кодового слова T.

З визначення (12) безпосередньо випливає, що при фіксованому розмірі кодового слова зі

Показано, що результат «розсіювання» впливу кодового слова наростатиме зі зростанням його розміру.

Для забезпечення найвищої селективності кодових слів, що конструюються, необхідно будувати їх таким чином, щоб обрана трансформанта ДКП приймала задане значення $\alpha \neq 0$, у той час як інші трансформанти повинні дорівнювати нулю. Це завдання зводиться до розв'язання системи з N^2 рівнянь, яку в матричному вигляді можна записати як

$$V \cdot A_1 = Z, \tag{13}$$

де матриця A_1 розраховується для ДКП відповідно до Твердження 2, 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

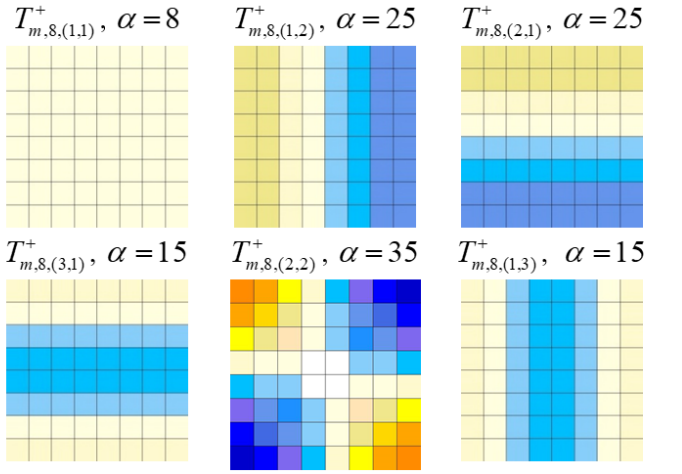
$$Z = (0 \quad \ldots \quad \alpha \quad \ldots \quad 0). \tag{14}$$

Рішення системи (13) для трансформанти ДКП (1,2) після представлення отриманого результату у вигляді матриці розміру 4×4, а також його трансформанти ДКП мають вигляд

$$T^{+}_{m',4,(1,2)} = \begin{bmatrix} 0.327\alpha & 0.135\alpha & -0.135\alpha & -0.327\alpha \\ 0.327\alpha & 0.135\alpha & -0.135\alpha & -0.327\alpha \\ 0.327\alpha & 0.135\alpha & -0.135\alpha & -0.327\alpha \\ 0.327\alpha & 0.135\alpha & -0.135\alpha & -0.327\alpha \end{bmatrix}, C^{+}_{m',4,(1,2)} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \alpha = 1. \tag{15}$$

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 мати цілі компоненти, що призводить до необхідності попереднього округлення кодових слів, побудованих за допомогою вирішення системи рівнянь (13), в результаті чого отримуємо недвійкові кодові слова із цілими елементами, які назвемо багаторівневими. Побудовані кодові слова, спрямовані на модифікацію інших трансформант ДКП і які мають високі значення коефіцієнта селективності.



Розшифровка кольорів

	1		2		3		4
	5		6		7		8
	–1		–2		–3		–4
	–5		–6		–7		–8

Рис. 5. Кодові слова з високою селективністю для $\mu = 16$

Для випадку розміру блоку $\mu = 16$ кодові слова $T_{m,16,(n,m)}$, що цілеспрямовано впливають на різні трансформанти ДКП (n,m), наведені на рис. 5.

Застосування багаторівневих кодових слів дозволяє досягти істотного підвищення коефіцієнта селективності порівняно з використанням їх бінарних аналогів і, як наслідок, забезпечує підвищення ефективності методу з кодовим управлінням вбудовуванням ДІ.

Основні кроки запропонованого стеганографічного методу з кодовим управлінням вбудовуванням на основі багаторівневих кодових слів

Вбудовування ДІ.

Крок 1. Розбити стандартним чином $m \times n$-матрицю контейнера P на $\mu \times \mu$-блоки, що не перетинаються. Нехай B — довільний блок, що використовується для вбудовування ДІ.

Крок 2. Задати цільову трансформанту ДКП (k,l), і значення амплітуди впливу α. Побудувати вектор Z (14) і матрицю $A1_{\mu^2}$.

Крок 3. Розв'язати систему рівнянь (13). Результат — вектор V.

Крок 4. Округлити елементи V до найближчого цілого, записати у вигляді m-кової $\mu \times \mu$-матриці. Результат — кодові слова $T^{+}_{m,\mu,(k,l)}$, $T^{-}_{m,\mu,(k,l)}$.

Крок 5. Вбудувати у блок B черговий біт ДІ p

$$\text{Якщо}: p = 0$$
$$\text{то}: M = B + T^{+}_{m,\mu,(k,l)},$$
$$\text{інакше}: M = B + T^{-}_{m,\mu,(k,l)}.$$

Вилучення ДІ

Крок 1. Побудувати $m \times n$-матрицю:

$$W = \overline{M} - P,$$

де $\overline{M}$ — матриця можливо збуреного стеганоповідомлення.
Розбити W стандартним чином на $\mu \times \mu$-блоки Δ_r, $r = 0,1,\ldots,mn-1$.

Крок 2. Для кожного Δ_r вилучити відповідний біт $\overline{p}$ ДІ

$$\overline{p} = sign\left(\sum_{i,j=0}^{\mu-1} \Delta_r(i,j) T^{+}_{m,\mu,(k,l)}(i,j) \right).$$

Рис. 6. Стеганографічний метод з кодовим управлінням вбудовуванням для багаторівневих кодових слів

представлені на рис. 6.

Результати тестування стеганографічного методу з кодовим управлінням на основі багаторівневих кодових слів в умовах різноманітних атак проти вбудованого повідомлення представлені на рис. 7.

У табл. 1 наведені значення коефіцієнта селективності для багаторівневих кодових слів у порівнянні з бінарними кодовими словами.

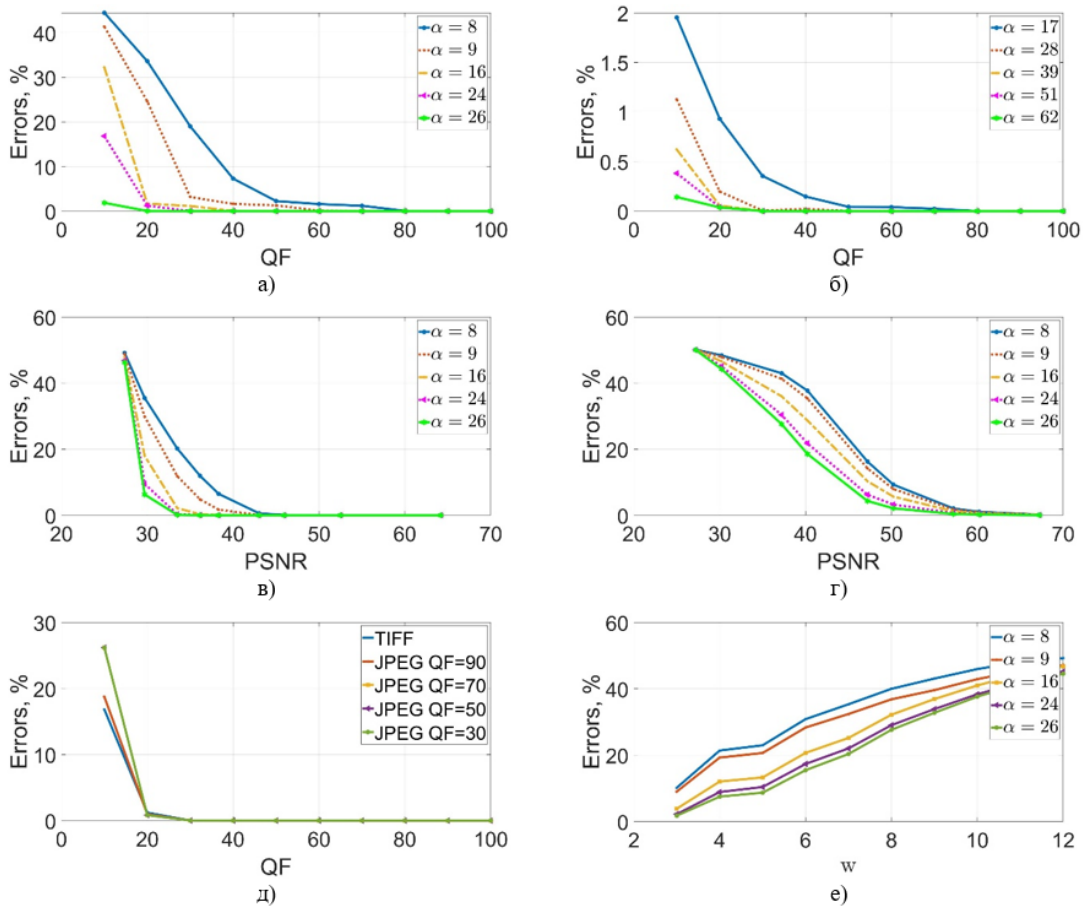


Рис. 7. Кількість помилок при декодуванні стеганоповідомлення із застосуванням багаторівневих кодових слів: а) під атакою стисненням JPEG, розмір блоку μ=8, б) під атакою стисненням JPEG, розмір блоку μ=16, в) під атакою зашумленням білим гаусівським шумом, розмір блоку μ=8, г) під атакою зашумленням шумом «salt&pepper», розмір блоку μ=8, д) під атакою стисненням JPEG, для різних форматів контейнерів при α=25, е) під атакою розмиттям при розмірі вікна w, розмір блоку μ=8

Таблиця 1

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	$T^{+}_{b,8,(3,1)}$	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
(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. 1 показує, що застосування багаторівневих кодових слів дозволяє досягти істотного підвищення коефіцієнта селективності порівняно з використанням їх бінарних аналогів і, як наслідок, забезпечує підвищення ефективності методу з кодовим управлінням вбудовуванням ДІ.

Результати порівняльного аналізу ефективності алгоритмічної реалізації розроблених методів із сучасними аналогами, представлені в табл. 2.

Таблиця 2

Результати порівняльного аналізу розроблених методів 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													
$\mu=4, \lambda=1$	46.0	39.4	33.0	26.9	20.8	16.2	9.4	3.0	0.8	0.6	48.1	1/16	S
$\mu=8, \lambda=1$	43.6	31.4	16.1	5.6	2.4	1.6	0.1	0	0	0	48.1	1/64	S
Стеганографічний метод з кодовим управлінням на основі багаторівневих кодових слів													
$T^{+}_{m,8,(1,2)}, \alpha=8$	44.5	33.6	19.0	7.3	2.3	1.6	1.2	0.1	0	0	49.32	1/64	S
$T^{+}_{m,8,(1,2)}, \alpha=16$	32.2	1.7	1.2	0	0	0	0	0	0	0	41.6	1/64	S
$T^{+}_{m,8,(1,2)}, \alpha=26$,	1.9	0	0	0	0	0	0	0	0	0	37	1/64	S
$T^{+}_{m,8,(1,2)}, \alpha=32$,	1.6	0	0	0	0	0	0	0	0	0	35.6	1/64	S
Сучасні аналоги													
Li, 2021 р.	—	—	0.02	—	0.02	—	0.01	—	0.01	0.01	~27.1	0.01	NN
Wang, 2021 р.	—	—	0	—	0	—	—	0	—	0	~38.5	0.01	DCT
Zhu, 2019 р.	—	—	—	—	—	—	33.9	7.4	0.3	—	~45	<1/8	DCT
Chanu, 2014 р.	—	—	—	—	23.88	14.1	2.76	0.08	0.08	—	~32.7	1/16	SVD
Мельник, 2012 р.	13	7	5	4	2	2	2	2	2	—	~ 34.7	1/64	SVD
Chang, 2007 р.	—	—	—	—	24.7	14.4	2.71	0.2	0.1	—	~32.7	1/64	SVD

У табл. 2. прийняті такі умовні позначення: S — просторова область, DCT — область трансформант ДКП блоків зображення, SVD — область сингулярного

розкладання блоків зображення, NN — стеганоперетворення відбувається засобами нейронної мережі.

Аналіз даних, представлених у табл. 2 показує, що представлені стеганографічні методи з кодовим управлінням вбудовуванням демонструють результати, що перевищують результати найкращих існуючих сучасних аналогів. Так, при застосуванні багаторівневого кодового слова $T^{+}_{m,8,(1,2)}$ і пропускний спроможності 1/64, під впливом атаки стисненням алгоритмом JPEG із коефіцієнтом якості $QF=10$, розроблений стеганографічний метод допускає 1.6% помилок, тоді як найкращий з існуючих аналогів при рівнозначних або гірших інших параметрах має цей показник на рівні 13%. Відзначимо, що сучасний аналог — алгоритм Wang, хоча і характеризується досить високою стійкістю до атак проти вбудованого повідомлення при забезпеченні високого рівня надійності сприйняття, є надзвичайно чутливим до властивостей обраного контейнера, що робить більш як 50% контейнерів непридатними для вбудовування. Такий недолік фактично унеможливлює застосування даного методу з потоковими контейнерами.

На відміну від більшості аналогів, у розробленому стеганографічну методі вбудовування відбувається у просторовій області, без необхідності застосування ресурсномістких перетворень, що закладає основи його застосування при побудові КСС, які працюють з потоковим контейнером у режимі реального часу.

Таким чином, 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%.

Четвертий розділ дисертації присвячений вирішенню задачі підвищення пропускної спроможності КСС за рахунок розробки стеганографічних методів з множинним доступом.

Одним з основних використовуваних сьогодні методів забезпечення множинного доступу до прихованого каналу є застосування технології MC-CDMA. Незважаючи на високу ефективність та перспективність використання технології кодового розподілу у стеганоканалах, це питання залишається досить малодослідженим. У літературі 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 призводить до неможливості застосування ефективних кодів, основаних на відомій статистиці вихідного алфавіту для кодування сигналу у груповому тракті.

У розділі доведено два фундаментальні твердження, які визначають ймовірність появи тих чи інших коефіцієнтів перетворення Уолша-Адамара, і, таким чином, дозволяють зробити процес їх попереднього кодування детермінованим.

Твердження 5. Множина значень $\{0,\pm2,...,\pm N\}$, які може приймати розбаланс Δ двійкових послідовностей, становить множину можливих значень коефіцієнтів перетворення Уолша-Адамара.

Твердження 6. Імовірність появи коефіцієнта перетворення Уолша-Адамара із заданим значенням ω_i визначається як

$$p(\omega_i) = p(-\omega_i) = \frac{C_N^{\frac{N-\omega_i}{2}}}{2^N}. \quad (16)$$

Використовуючи Твердження 6, стає можливою побудова ефективного коду на основі відомої статистики вихідного алфавіту, а також розрахунок середньої довжини кодового слова l_{av} для будь-якого необхідного значення N.

Відповідно до теореми Шеннона про кодування джерела, середня довжина кодового слова, необхідна для кодування символу його алфавіту не перевищує інформаційну ентропію даного алфавіту $l_{av} \geq H(\{\omega_i\})$, де

$$H(\{\omega_i\})_N = -\sum_{i=0}^{N} p(\omega_i) \cdot \log_2 p(\omega_i). \quad (17)$$

На основі Твердження 6 при довільному значенні N маємо таку нерівність

$$l_{av} \geq -\sum_{i=0}^{N} \frac{C_N^{\frac{N-\omega_i}{2}}}{2^N} \cdot \log_2 \frac{C_N^{\frac{N-\omega_i}{2}}}{2^N}, \quad \omega_i = 0, \pm 2, ..., \pm N - 1. \quad (18)$$

При заданому N права частина виразу (18) становить нижню границю кількості двійкових розрядів, необхідних для кодування одного коефіцієнта перетворення Уолша-Адамара.

У табл. 3 наведені обчислені імовірнісні характеристики коефіцієнтів перетворення Уолша-Адамара для 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 3

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

Встановлено, що для випадку кількості каналів, що розділяються $N = 4$, бент-послідовності можуть бути використані 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. При цьому пропонується таблиця кодування С-кодом, побудована відповідно до таких правил.

Правило 1. Кожне кодове слово, яке відповідає бент-послідовності, кодується кодовим словом в конкатенації з самим собою.

Правило 2. Кожне кодове слово, яке не відповідає бент-послідовності, кодується конкатенацією кодового слова, що відповідає бент-послідовності, та його інверсії.

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, тобто: порівняно з використанням коду Гаффмана для кодування коефіцієнтів перетворення Уолша-Адамара, запропонований код дозволяє упаковувати коефіцієнти Уолша-Адамара на 6,25% ефективніше; 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.

Однак, фундаментальними недоліками застосування технології MC-CDMA для організації множинного доступу до прихованого каналу зв'язку є той факт, що число абонентів є строго регламентованим і дорівнює $N = 2^k = 2,4,8,16,....$, а також дезінтегрованість технології MC-CDMA із стеганографічним методом, тобто технологія MC-CDMA не показує, як саме має відбуватися вбудовування та вилучення додаткової інформації.

Вбудовування інформації

Крок 1. Сформувати ансамблі:

— кодових слів $\{f_j\}$ розміру $\mu/2 \times \mu/2$ на основі рядів $H(i,:), i = 0,1,...,(\mu/2)^2$

— частотних розстановок $\{[i_1,i_2,i_3,i_4]_z\}$, $z = 1,2,...,q(q-1)$ на основі РС-коду над полем $GF(q)$.

Крок 2. Для абонентів A_z, сформувати кодові слова T_z^+ та T_z^- розміру $\mu \times \mu$ згідно до конструкції $\begin{array}{|c|c|}\hline f_{i_1} & f_{i_2} \\ \hline f_{i_3} & f_{i_4} \\ \hline \end{array}$ та особистої розстановки $[i_1,i_2,i_3,i_4]_z$

Крок 3. Кожний абонент A_z розбиває стандартним чином $m \times n$-матрицю контейнера P на $\mu \times \mu$-блоки. У черговий блок B вбудовується один біт $d_{z,k}$, $k = 1,2,...,mn/\mu^2$ ДІ як

$$\begin{array}{l} \text{Якщо}: d_{z,k} = 0 \\ \text{то}: M = B + T_z^+, \\ \text{інакше}: M = B + T_z^-. \end{array}$$

Вилучення інформації

Крок 1. Абонент A_z відповідно до особистої розстановки $[i_1,i_2,i_3,i_4]_z$ вибирає рядки $\{H(i_1,:)\},\{H(i_2,:)\},\{H(i_3,:)\},\{H(i_4,:)\}$.

Крок 2. Абонент A_z будує $m \times n$-матрицю:

$$W = \overline{M} - P,$$

де $\overline{M}$ — матриця можливо збуреного стеганоповідомлення. Розбиває W стандартним чином на $\mu \times \mu$-блоки Δ_r, $r = 1,2,\ldots,mn$.

Крок 3. Кожний $\mu \times \mu$-блок Δ_r розбивається на 4 $\mu/2 \times \mu/2$-підблоки, які представляється у вигляді вектора $\{\delta_{z,j}\}, i = \{1,2,3,4\}$ довжини $(\mu/2)^2$.

Крок 4. Абонент A_z обчислює вектор P, відповідно до наступної формули

$$P_{z,k} = [p_1 \quad p_2 \quad p_3 \quad p_4], p_i = \sum_{k=1}^{\mu^2} \delta_{j,k} h_{j,k}, i = \{1,2,3,4\}.$$

Крок 5. Абонент A_z обчислює призначений йому біт даних, вбудований у блок Δ_r за допомогою наступної формули $d_{z,k} = sign\left(\sum_{i=1}^{4} p_i\right)$.

Рис. 8. Стеганографічний метод з множинним доступом на основі технології частотних розстановок

Наступним кроком на шляху розвитку стеганографічних методів з множинним доступом, який дозволяє усунути недоліки методу розподілу каналів на основі технології MC-CDMA, є використання технології кодового управління, а також технології частотних розстановок, що застосовується для побудови адресних асинхронних систем зв'язку. В розділі представлено стеганографічний метод з множинним доступом на основі технології частотних розстановок (рис. 8). 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. На рис. 9 показано графік, що демонструє ефект впливу внутрішньосистемних перешкод на

точність передавання інформації в залежності від кількості одночасно працюючих абонентів для частотних розстановок над полями Галуа $GF(5)$ та $GF(13)$.

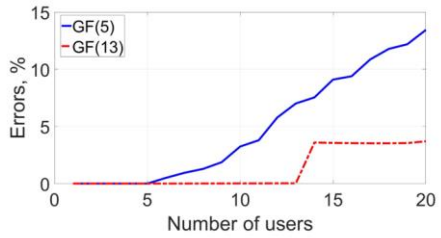


Рис. 9. Графік залежності рівня помилок у системі, що виникають внаслідок дії внутрішньосистемних перешкод від кількості абонентів

Застосування частотних розстановок на основі РС-коду над полем $GF(5)$ дозволяє 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 $N=20$ рівень внутрішньосистемних перешкод залишається прийнятним, а кількість помилок, що виникають, не перевищує 3.7%.

У разі необхідності максимізації кількості одночасно працюючих у стеганографічній системі з множинним доступом абонентів у роботі представлено новий стеганографічний метод, заснований на застосуванні кодового управління, однак із задіянням запропонованої технології частотно-просторових матриць.

Сутність ідеї стеганографічного методу на основі частотно-просторових матриць полягає в наступному. Операції вбудовування та вилучення інформації в даному методі засновані на стандартному розбитті зображення на блоки Q_k розміру $\mu\times\mu=16\times16$. Кожен з отриманих блоків поділяється ще на 16 блоків q_i, $i=1,2,...,16$, розміру 4×4

$$Q_k=\begin{array}{|c|c|c|c|}\hline q_1 & q_2 & q_3 & q_4\\ \hline q_5 & q_6 & q_7 & q_8\\ \hline q_9 & q_{10} & q_{11} & q_{12}\\ \hline q_{13} & q_{14} & q_{15} & q_{16}\\ \hline\end{array}. \qquad (19)$$

Розділення каналів користувачів відбувається за двома ознаками: частотною та просторовою: 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, що впливають на задану трансформанту Уолша-Адамара.

У розділі представлені методи синтезу кодових слів S-кодів, F-кодів та метод їх суперпозиції. 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.

Основні кроки стеганометоду з множинним доступом на основі просторово-частотних кодів представлені на рис. 10. Загальна кількість зареєстрованих у стеганографічній системі з множинним доступом на основі просторово-частотних розстановок абонентів дорівнює $J=4800$, тоді як характеристики розробленого стеганографічного методу безпосередньо залежать від кількості абонентів, що одночасно здійснюють передачу інформації.

Вбудовування ДІ

Крок 1. Сформувати ансамблі:

— кодових слів $\{f_i\}$ розміру $\mu/4\times\mu/4$ на основі рядків $H(i,:), i=0,1,...,(\mu/4)^2$

— просторових розстановок $\{s_{z_1}\}, z_1=1,2,...J_S$, ваги Геммінга $w=4$;

— частотних розстановок $\{C_{z_2}\}, z_2=1,2,...J_F$ на основі РС-коду над $GF(q)$.

Крок 2. Привласнити абонентам A_z, $z=J_SJ_F$ унікальний код $\{s_{z_1},C_{z_2}\}$.

Крок 3. На основі $\{s_{z_1},C_{z_2}\}$ абоненти A_z формують кодові слова T_z^+ та T_z^-.

Крок 4. Абонент A_z розбиває стандартним чином $m\times n$-матрицю контейнера P на $\mu\times\mu=16\times16$-блоки. У черговий блок B вбудовується один біт $d_{z,k}$, $k=1,2,...,mn/\mu^2$ ДІ як

$$\begin{aligned}&\text{Якщо: } d_{z,k}=0\\&\text{то: } M=B+T_z^+,\\&\text{інакше: } M=B+T_z^-.\end{aligned}$$

Алгоритм вилучення інформації

Крок 1. Абонент A_z будує $m\times n$-матрицю:

$$W=\overline{M}-P,$$

де $\overline{M}$ — матриця можливо збуреного стеганоповідомлення. Розбиває W стандартним чином на $\mu\times\mu=16\times16$-блоки Δ_r, $r=1,2,\ldots,mn$.

Крок 2. Кожний $\mu\times\mu$-блок Δ_r розбивається на 16 $\mu/4\times\mu/4$-підблоків, серед яких обираються $w=4$ блоки відповідно до кодового слова s_{z_1}. Обрані блоки представляються у вигляді векторів $\{\delta_{z,i}\}, i=1,2,...,16$ довжини $(\mu/4)^2$.

Крок 3. Абонент A_z відповідно до C_{z_2} вибирає рядки матриці Уолша-Адамара H_{16} $\{H(i_1,:)\},\{H(i_2,:)\},\{H(i_3,:)\},\{H(i_4,:)\}$.

Крок 4. Абонент A_z обчислює вектор P відповідно до наступної формули

$$P_{z,k}=[p_1\quad p_2\quad p_3\quad p_4],\ p_i=\sum_{k=1}^{\mu^2}\delta_{j,k}h_{j,k},\ i=\{1,2,3,4\}.$$

Крок 5. Абонент A_z обчислює призначений йому біт даних, вбудований у блок Δ_r за допомогою наступної формули $d_{z,k}=sign\left(\sum_{i=1}^{4}p_i\right)$.

Рис. 10. Стеганографічний метод з множинним доступом на основі просторово-частотних кодів

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.

На рис. 11 для розробленого методу представлено графік залежності кількості помилок у стеганоканалі, що виникають внаслідок дії внутрішньосистемних перешкод від кількості абонентів, що одночасно працюють.

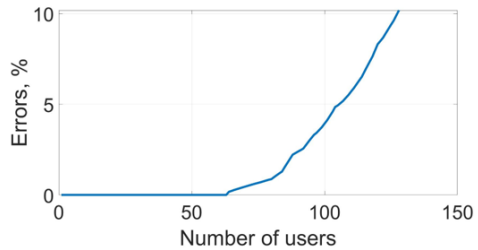


Рис. 11. Графік залежності кількості помилок у стеганоканалі, що виникають внаслідок дії внутрішньосистемних перешкод від кількості абонентів, що одночасно працюють

Отже, четвертий розділ присвячено розвитку теоретичної та практичної складової методології, запропоновано стеганографічні методи з множинним доступом, що дозволяють підвищити пропускну спроможність КСС за рахунок одночасної передачі інформації, що надходить від різних абонентів у прихованому каналі зв'язку. 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.

П'ятий розділ присвячено розробці теоретичного базису оцінки криптографічної якості ФБЛ з метою створення основи розробки криптографічних примітивів та способу формування стеганографічного ключа із застосуванням спеціалізованих шифрів для підвищення криптостійкості КСС.

Криптографічна складова є невід'ємною частиною КСС, формування якої потребує врахування її роботи у складі всієї системи. Основою для адаптації роботи криптографічної компоненти у складі КСС є математичний апарат ФБЛ.

У відкритих літературних джерелах на сьогодні фактично відсутні критерії та показники, які дозволяють досліджувати криптографічну якість ФБЛ, що унеможливлює як їх застосування для задач підвищення криптографічної якості КСС, так і оцінку стійкості існуючих криптографічних примітивів у разі здійснення атак на них із використанням ФБЛ. Дослідження якості компонентних ФБЛ криптографічних примітивів обумовлюють можливості їх подальшого вдосконалення (насамперед, через дослідження компонентних ФБЛ з основою $q = 2^k$, що відповідає довжинам примітивів розповсюджених сьогодні шифрів), а також створення нових спеціалізованих шифрів, що працюють над алфавітом $\{0,1,...,q-1\}$ для задач інтеграції компонентів КСС.

У роботі представлено чотири критерії криптографічної якості ФБЛ, що дозволяють всебічно оцінити їх якість: критерій максимізації алгебраїчної нелінійності, критерій максимізації дистанційної нелінійності, критерій розповсюдження, критерій незалежності виходу ФБЛ від її вхідних змінних.

Критерій максимізації алгебраїчної степені нелінійності засновано на методі уявлення компонентних ФБЛ криптографічних примітивів у вигляді алгебраїчної нормальної форми (АНФ). В роботі розроблено математичний апарат синтезу АНФ над розширеними полями $GF(q)$ для практично цінних з точки зору дослідження конструкцій сучасних шифрів значень $q = 4^k, q = 16^k$.

Оскільки існує єдиний первісний незвідний поліном $f(x) = x^2 + x + 1$ степеню $k = 2$, а отже таблиця множення у полі $GF(2^2)$ може бути побудована лише одним способом

+	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

. (20)

З метою обчислення коефіцієнтів АНФ конкретно заданої 4-функції, використовуються наступні матричні рівняння

$$A = L_4 F,\ F = L_4^{-1} A, \tag{21}$$

де L_4 — матриця перетворення Ріда-Маллера.

Доведено існування наступного рекурентного правила побудови прямих та зворотних матриць перетворення Ріда-Маллера довільного порядків $q = 4^k, q = 16^k$, яке для значення основи $q = 4$ має наступний вигляд

$$L_{4^k}^{-1} = \begin{bmatrix} L_{4^{k-1}}^{-1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ L_{4^{k-1}}^{-1} & L_{4^{k-1}}^{-1} & L_{4^{k-1}}^{-1} & L_{4^{k-1}}^{-1} \\ L_{4^{k-1}}^{-1} & 2L_{4^{k-1}}^{-1} & 3L_{4^{k-1}}^{-1} & L_{4^{k-1}}^{-1} \\ L_{4^{k-1}}^{-1} & 3L_{4^{k-1}}^{-1} & 2L_{4^{k-1}}^{-1} & L_{4^{k-1}}^{-1} \end{bmatrix},\ L_{4^k} = \begin{bmatrix} L_{4^{k-1}} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & L_{4^{k-1}} & 3L_{4^{k-1}} & 2L_{4^{k-1}} \\ \mathbf{0} & L_{4^{k-1}} & 2L_{4^{k-1}} & 3L_{4^{k-1}} \\ L_{4^{k-1}} & L_{4^{k-1}} & L_{4^{k-1}} & L_{4^{k-1}} \end{bmatrix}, \tag{22}$$

де під $\mathbf{0}$ розуміється нульова матриця порядку 4^{k-1}.

Застосування (21), а також конструкцій рекурентної побудови прямих та зворотних матриць перетворення Ріда-Маллера (22) дозволяє визначати та порівнювати алгебраїчні степені нелінійності компонентних q-функцій, на яких засновані сучасні криптографічні алгоритми.

Дистанційну нелінійність ФБЛ запропоновано вимірювати як степінь несхожості даної алгебраїчної структури з множиною структур, які прийнято вважати лінійними. В якості таких структур виступають багатозначні аналоги функцій Уолша, функції Віленкіна-Крестенсона. 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

$$NL = \begin{cases} q^k - \max\left\{\left|\Omega(\omega)\right|\right\}, & q > 2; \\ 2^{k-1} - \dfrac{1}{2}\max\left\{\left|W(\omega)\right|\right\}, & q = 2, \end{cases} \tag{23}$$

де $W(\omega)$ — коефіцієнти перетворення Уолша-Адамара, що є окремим випадком перетворення Віленкіна-Крестенсона для булевих функцій.

Вираз (23) є визначенням q-нелінійності ФБЛ. Використовуючи формулу (23), стає можливим виконати оцінку q-нелінійності таких криптографічних примітивів, 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. Спираючись на отримані результати, введено уточнене визначення бент-послідовностей для довільного значення q.

Визначення 2. 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 $h_i \in \{e^{j\frac{2\pi}{m}\nu}\}$, $\nu = 0,1,...,m-1$, якщо вона має рівномірно розподілені модулі трансформант Віленкіна-Крестенсона, які представимо в матричній формі

$$\left|\Omega_B(\omega)\right| = \left|H \cdot \overline{V}_N\right| = const\,, \omega = \overline{0, N-1}, \tag{24}$$

де V_N — матриця Віленкіна-Крестенсона порядку N над алфавітом $h_i \in \{e^{j\frac{2\pi}{m}\nu}\}$, $\nu = 0,1,...,m-1$.

У розділі обґрунтовано метод оцінки нелінійності ФБЛ в часовій області, що засновано на визначенні розбалансу ФБЛ.

Для послідовності f 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.

Визначення 3. Розбалансом послідовності f назвемо значення модуля суми поелементних добутків елементів вектора K на відповідні їм елементи експоненційного алфавіту $\{z_0, z_1, ..., z_{q-1}\}$

$$\Delta(f) = \left|K_0 z_0 + K_1 z_1 + ... + K_{q-1} z_{q-1}\right|. \tag{25}$$

Визначення 3 покладено в основу розрахунку дистанційної нелінійності ФБЛ. На основі Визначення 3 запропоновано метод обчислення нелінійності ФБЛ для довільного значення q у вигляді конкретних кроків, які представлені на рис. 12.

Крок 1. Записати повну множину лінійних функцій

$$\{A_j\} = (X \cdot X^T) \bmod q,$$

де X — матриця, що складена з усіх можливих q-ічних векторів довжини k.

Крок 2. Обчислити значення розбалансу суми повної множини афінних функцій і даної ФБЛ.

Крок 3. Обчислити значення нелінійності досліджуваної ФБЛ

$$N_f = \begin{cases} q^k - \max\left\{\Delta(f \underset{q}{\oplus} A_j)\right\}, & j = 1,2,...,q^{k+1}, \quad q > 2; \\ 2^{k-1} - \dfrac{1}{2}\max\left\{\Delta(f \underset{q}{\oplus} A_j)\right\}, & j = 1,2,...,2^{k+1}, \quad q = 2. \end{cases}$$

Рис. 12. Метод обчислення нелінійності ФБЛ у часовій області

З точки зору оцінки криптографічної якості ФБЛ важливим є питання розробки методу вимірювання диференціальних властивостей ФБЛ. Диференціальні властивості булевих функцій є найважливішим критерієм криптографічної якості, який враховується при конструюванні сучасних криптографічних S-блоків. В роботі введено визначення та запропоновано методи розрахунку показників стійкості q-функції до атак диференційного криптоаналізу, серед яких найбільшою практичною цінністю характеризується суворий лавинний критерій (СЛК) ФБЛ.

На рис. 13 показано основні кроки методу дослідження відповідності q-функції умовам СЛК, який дозволяє визначати та порівнювати якість компонентних q-функцій сучасних шифрів у сенсі їх диференційних властивостей, а також є теоретичною основою запропонованих методів синтезу криптографічних примітивів, що відповідають СЛК компонентних q-функцій.

Крок 1. Сформувати множину векторів $\{u_h\}$, $h = 1,2,...(q-1)\cdot\log_q N$ над алфавітом $\{0,1,...,q-1\}$ одиничної ваги $\varpi(u) = 1$, де вага $\varpi(u)$ q-значного вектору визначається як кількість його ненульових компонент.

Крок 2. Розрахувати похідні функції f у напрямку кожного з векторів u відповідно до наступної формули

$$D_u f(x) = f(x \underset{q}{\oplus} u) - f(x) \,(\bmod q)$$

де $\underset{q}{\oplus}$ означає додавання по модулю q.

Крок 3. Перевірити збалансованість кожної з побудованих похідних, тобто

Якщо : $p(D_u f(x) = i(\bmod q)) = 1/q$ *для* $\forall i = 0,1,...,q-1, u \in \{u_h\}$,

то : q-функція f відповідає СЛК,

інакше : q-функція f не відповідає СЛК.

Рис. 13. Метод знаходження відповідності СЛК q-функції f довжини N

Іншим важливим критерієм криптографічної якості є незалежність виходу криптографічного примітиву від її входу. Для чисельного визначення такого взаємозв'язку використовується поняття матриці коефіцієнтів кореляції. Поняття оптимальності матриці коефіцієнтів кореляції $\|R\| = \rho_{\nu,\mu}$ S-блока є універсальним як для його уявлення булевими функціями, так і ФБЛ і розраховується відповідно до запропонованої формули

$$\rho_{\nu,\mu} = \frac{\sum_{t=1}^{N} x_\nu y_\mu - \dfrac{\sum_{t=1}^{N} x_\nu \sum_{t=1}^{N} y_\mu}{N}}{\sqrt{\left[\sum_{t=1}^{N} x_\nu{}^2 - \dfrac{\left(\sum_{t=1}^{N} x_\nu\right)^2}{N}\right] \cdot \left[\sum_{t=1}^{N} y_\mu{}^2 - \dfrac{\left(\sum_{t=1}^{N} y_\mu\right)^2}{N}\right]}}, \quad \nu,\mu = 1,2,...,k, \tag{26}$$

де x_ν — ν-й вектор вхідної інформації криптографічного примітиву, y_μ — μ-й вектор вихідної інформації криптографічного примітиву.

Поняття матриці коефіцієнтів кореляції пов'язане із визначенням кореляційного імунітету його компонентних функцій. Відомо, що у двійковому випадку, оптимальність матриці коефіцієнтів кореляції (26), тобто тотожна рівність всіх її елемнтів нулю $\rho_{\nu,\mu}=0, \forall \nu,\mu \in \{1,2,...,k\}$, можлива тільки тоді, коли всі компонентні булеві функції є кореляційно імунними. У роботі доведено, що для випадку представлення криптографічного примітиву за допомогою компонентних ФБЛ, означене не є істинним. Тобто навіть ті криптографічні примітиви, що характеризуються оптимальною матрицею коефіцієнтів кореляції (26) потребують додаткового дослідження своїх компонентних ФБЛ на їх кореляційний імунітет. На рис. 14 представлено запропонований метод дослідження відповідності ФБЛ критерію кореляційного імунітету. Представлений метод дозволяє досліджувати та порівнювати ФБЛ, що входять до складу криптоалгоритмів, за критерієм їх кореляційного імунітету порядку $m=1$.

Крок 1. Знайти всі підфункції $\{f_i'\}$ $k-1$ змінних функції f шляхом підстановки у f значень з множини $\{0,1,...q-1\}$ почергово замість змінних $x_i, i=1,2,...,k$.

Крок 2. Перевірити розбаланс кожної підфункції з $\{f_i'\}$

Якщо : $\Delta_{f'}=\Delta_f/q$ для $\forall f_i, i=1,2,...,k,$

то : q-функція f відповідає критерію кореляційного імунітету,

інакше : q-функція f не відповідає відповідає критерію кореляційного імунітету.

Рис. 14. Метод знаходження відповідності критерію кореляційного імунітету порядку $m=1$ *q*-функції f довжини N

Проведені у розділі дослідження відносяться до теоретичної складової розробленої методології та дозволяють визначати та порівнювати криптографічну якість шифрів та їх складових частин при уявленні за допомогою будь-яких можливих основ уявлення q, що створює передумови для розробки криптографічних примітивів та шифрів, що володіють більшою крипостійкістю та підвищують ефективність КСС.

Шостий розділ роботи присвячено розробці методів підвищення криптографічної захищеності КСС на основі розроблених у попередньому розділі критеріїв криптографічної якості ФБЛ.

Запропоновано ефективні методи синтезу криптографічних примітивів, що відповідають як критеріям криптографічної якості булевих функцій, так і критеріям криптографічної якості ФБЛ. Зокрема, метод синтезу максимально нелінійних S-блоків довжини $N=16$ у сенсі компонентних булевих функцій та 4-функцій, який представлено на рис. 15.

Крок 1. Побудувати множину максимально нелінійних 4-функцій.

Крок 1.1. Перебравши повну множину булевих функцій довжини N потужності $J=2^N$, відібрати з них такі, які є збалансованими і при цьому мають найбільшу нелінійність $N_{2f}\to\max$.

Крок 1.2. Виконати конкатенацію знайдених нелінійних булевих функцій в 4-функцію і виміряти її нелінійність.

Крок 2. Вибрати задану компонентну 4-функцію f_{41} і добудувати до неї пару так, щоб вони складали бієктивний S-блок.

Крок 3. Відсіяти всі такі S-блоки, друга компонентна 4-функція яких не володіє максимальним значенням 4-нелінійності $N_{4f}\to\max$.

Рис. 15. Метод синтезу максимально нелінійних S-блоків у сенсі компонентних булевих та 4-функцій

Представлено метод синтезу S-блоків, що відповідають СЛК компонентних 4-функцій та максимальному лавинному критерію компонентних булевих функцій, який представлено на рис. 16.

Із застосуванням представленого методу отримано $J=245760$ S-блоків довжини $N=256$, що задовольняють СЛК компонентних 4-функцій, серед яких існує точно $J_1=3968$ S-блоків, що одночасно задовольняють і критерію максимального лавинного ефекту компонентних булевих функцій.

Розроблено метод синтезу S-блоків довжини $N=32$, що задовольняють критерію розповсюдження помилки вищих порядків PC(m). А саме, шляхом застосування запропонованого алгоритму класифікації елементарних структур векторів трансформант Уолша-Адамара (згідно до Визначення 1), знайдено типи елементарних структур трансформант Уолша-Адамара (табл. 4) булевих функцій довжини $N=32$, що допускають відповідність булевих функцій критерію розповсюдження помилки.

Крок 1. Використовуючи регулярний метод синтезувати множину S-блоків довжини $N=16$, потужності $J=245760$, що задовольняють СЛК компонентних 4-функцій.

Крок 2. Задати функцію F_m, яка є старшою компонентною 4-функцією в розкладанні S-блоку на 4-функції.

Крок 3. Сформувати множину із 4-х перестановок відповідно до наступного правила

$$p_j = x \underset{4}{\oplus} (j \circ d), \quad x = 0,1,\ldots,N-1, \quad j = 0,1,2,3,$$

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.

Крок 4. Отримати функцію G_1 довжини $4N$ за наступним правилом

$$G_1[F_m] = \left\{ F_m \underset{4}{\oplus} c_1 \mid F_m(p_1) \underset{4}{\oplus} c_2 \mid F_m(p_1) \underset{4}{\oplus} c_3 \mid F_m(p_1) \underset{4}{\oplus} c_4 \right\},$$

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 $c_1=0, c_2=1, c_3=2, c_4=3$.

Крок 5. Збільшити довжину S-блоку до значення $4N$, використовуючи наступну конструкцію

$$G_0 = \{ S \mid S(p_1) \mid S(p_2) \mid S(p_3) \}.$$

Крок 6. Побудувати новий S-блок довжини $4N$, що задовольняє суворому лавинному критерію компонентних 4-функцій за наступним правилом

$$S_1 = \left\{ G_1 \cdot 4^k + G_0 \right\}, k = \log_4 N.$$

Рис. 16. Метод синтезу S-блоків, що відповідають СЛК компонентних 4-функцій та максимальному лавинному критерію компонентних булевих функцій

Таблиця 4

Елементарні структури булевих функцій $k=5$ змінних

№	Елементарна структура	N_f	Потужність класу	Кількість булевих функцій, які відповідають PC(m)			
				1	2	3	4
18	{16(1),12(2),8(4),4(14),0(11)}	8	213 319 680	737280	0	0	0
19	{16(2),12(2),4(14), 0(14)}	8	3 809 280	163840	0	0	0
20	{16(2),8(4), 4(16),0(10)}	8	19 998 720	645120	0	0	0
21	{16(2),8(8),0(22)}	8	1 666 560	94720	0	0	0
22	{16(4),0(28)}	8	9 920	2560	0	0	0
23	{16(1),12(1),8(6),4(15),0(9)}	8	284 426 240	276480	0	0	0
31	{12(4),8(4),4(12),0(12)}	10	115 548 160	1904640	0	0	0
32	{12(4),4(28)}	10	31 744 000	1310720	0	0	0
34	{12(3),8(6),4(13),0(10)}	10	426 639 360	1966080	0	0	0
35	{12(2),8(8),4(14),0(8)}	10	666 624 000	12697600	0	0	0
36	{12(1),8(10),4(15),0(6)}	10	170 655 744	2654208	12288	0	0
39	{8(12),4(16),0(4)}	12	13 332 480	3440640	0	0	0
40	{8(16),0(16)}	12	14 054 656	1628672	228352	10752	1792

Отже, 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 помилки. 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. Ці булеві функції мають найбільшу відстань нелінійності, а також найвищий можливий (PC(4)) порядок критерію розповсюдження серед усіх булевих функцій довжини $N=32$.

На основі знайденого класу та алгоритму Кіма побудови S-блоків було побудовано бієктивні S-блоки з відстанню нелінійності $N_f = 12$, які задовольняють критерію розповсюдження помилки $\mathrm{PC}(4)$, тобто є оптимальними з точки зору критерію високої відстані нелінійності та критерію розповсюдження помилки серед можливих S-блоків довжини $N = 32$.

Доведено твердження, що визначає умову відповідності S-блока на основі 3-функцій критерію ідеальності матриці коефіцієнтів кореляції.

Твердження 7. 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 $m = 1$.

Синтезовано повну множину S-блоків довжини $N = 9$, що володіють ідеальною матрицею коефіцієнтів кореляції, а також розроблено метод рекурентного збільшення довжини S-блоків на онові конструкції Кіма (рис. 17), в результаті чого синтезовано повну множину з $|\Omega_9| = 264$ оптимальних S-блоків довжини $N = 9$, розробленим методом отримано $2 \cdot 4 \cdot 264 = 2112$ оптимальних S-блоків довжини $N = 27$, $2 \cdot 9 \cdot 2112 = 38016$ оптимальних S-блоків довжини $N = 81$, $2 \cdot 16 \cdot 38016 = 1216512$ оптимальних S-блоків довжини $N = 243$ і т.д. Побудовано та досліджено множини S-блоків конструкції Ніберг над полями $GF(p^k)$, $p \neq 2$.На основі запропонованих високоякісних криптографічних примітивів розроблено блоковий симетричний шифр для прекодера ДІ, а також розроблено концептуальну модель спеціалізованого шифру,

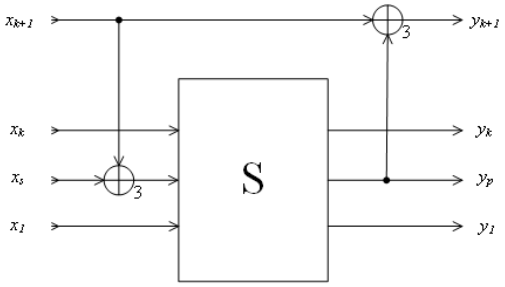


Рис. 17. Модифікована конструкція Кіма для 3-функцій

що оперує над алфавітом $\{0,1,-1\}$, що характеризується ефективним знищенням статистики вихідного тексту та великою кількістю ітерацій, що необхідні для зламу.

Розвиток теоретичних засад криптографічної стійкості ФБЛ, спеціалізований шифр, що оперує над алфавітом $\{0,1,-1\}$ та стеганографічний метод з кодовим управлінням вбудовуванням ДІ є основою для розробки нових рішень щодо підвищення криптографічної захищеності КСС. Запропоновано модифікацію структурної схеми КСС (рис. 18).

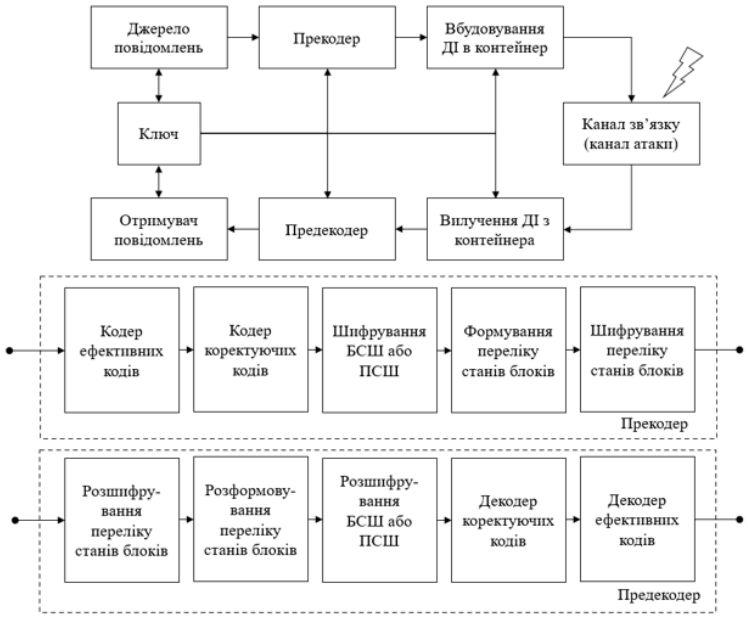


Рис. 18. Структурна схема КСС із застосуванням стеганографічного методу з кодовим управлінням вбудовуванням ДІ та шифруванням послідовності переліку станів блоків

Докладніше робота зв'язки пристроїв формування послідовності переліку станів блоків та її шифрування може бути представлена у вигляді конкретних кроків (рис. 19).

Відзначимо переваги запропонованого підходу до вбудовування ДІ з шифруванням послідовності переліку станів блока:

1. при використанні підходу до вбудовування ДІ з шифруванням послідовності 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^-) 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.

Теоретично доведена висока ефективність вбудовування інформації у просторовій області. Так, оскільки запропонований стеганографічний метод є блоковим, то для розміру контейнера $N \times N$ і розміру блока $\mu \times \mu$ обчислювальна складність операцій вбудовування та вилучення складатиме $\lceil N/\mu \rceil \times \lceil N/\mu \rceil \times C = O(N^2)$. В роботі показано, що для операції вбудовування ДІ $C = \mu^2$, тоді як для операції вилучення ДІ — $C = 2\lambda\mu^2$.

Крок 1. Кожному $\mu \times \mu$-блоку B_r, $r = 1,2,\ldots, mn/\mu^2$ контейнера розміру $m \times n$ поставити у відповідність елемент матриці станів Σ'_{ij}, $i = 1,2,\ldots,m/\mu$, $j = 1,2,\ldots,n/\mu$

Якщо : $d_k = 0$
то : $\Sigma'_{ij} = 1$
Якщо : $d_k = 1$
то : $\Sigma'_{ij} = -1$
інакше : $\Sigma'_{ij} = 0$.

при цьому індекси i, j змінюються у зіг-заг порядку, а $k = 1,2,\ldots,J$, де $J \le mn/\mu^2$ — кількість біт ДІ, що вбудовується

Крок 2. Сформувати послідовність $\{S_r\}$, $\forall S_r \in \{0, \pm 1\}$ шляхом порядкового зчитування Σ'_{ij}.

Крок 3. Зашифрувати послідовність $\{S_r\}$. Результат — зашифрована послідовність $\{C_r\} = E(\{S_r\})$ над алфавітом $\{0, \pm 1\}$.

Крок 4. Виконати вбудовування ДІ у черговий блок B_r

Якщо : $C_r = 1$
то : у блок B_r вбудовується кодове слово T^+
Якщо : $C_r = -1$
то : у блок B_r вбудовується кодове слово T^-
інакше : вбудовування не відбувається.

Рис. 19. Метод формування та шифрування послідовності переліку станів

При цьому, для найшвидшого перетворення, з множини найбільш вживаних при побудові стеганографічних методів перетворень, що дозволяють забезпечити заданий рівень ефективності стеганографічного методу, а саме, вейвлет-перетворення, значення C дорівнює μ^2.

Тобто, при чотирикратному перетворенні, що необхідно для підтримки операцій вбудовування та вилучення ДІ, стеганографічний метод з кодовим

управлінням гарантовано потребує у 4/3 рази менше операцій тільки від безпосередньої кількості операцій, які мають бути затрачені на виконання необхідних перетворень.

Отже, можемо сформулювати наступне твердження:

Твердження 8. Стеганографічний метод із кодовим управлінням вбудовуванням має меншу обчислювальну складність за будь-який стеганографічний алгоритм, що працює в області перетворень контейнера або перетворень блоків контейнера.

Окрім цього 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 майже всіх практично застосовуваних 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.

Результати вимірювання швидкодії розробленої КСС на найбільш розповсюджених у сучасних ресурсообмежених пристроях процесорах, а також на платформі AMD Ryzen 3 3200G, показані в табл. 5. 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 5

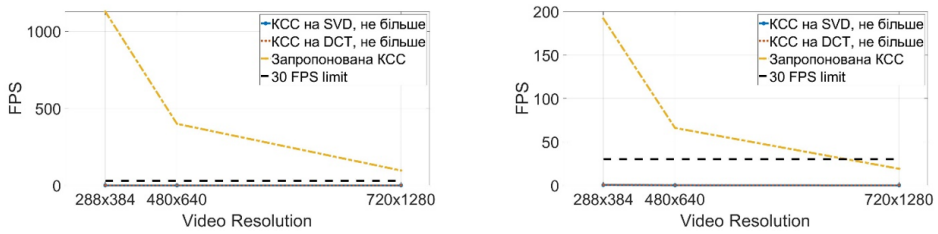
Показники швидкодії моделі КСС для різних розподільних здатностей потокових контейнерів

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
	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
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
	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. 5 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. 5 також вказано експериментально встановлені значення мінімально необхідного значення Single Thread ARM процесора для підтримки роботи КСС у режимі вбудовування або вилучення ДІ.



а) б)

Рис. 20. Графіки залежності FPS КСС у режимі вбудовування від розміру потокового контейнера, а) — платформа Raspberry Pi 4, б) — настільна платформа на основі AMD Ryzen 3

На рис. 20 представлено графіки залежності кількості FPS, що здатна обробити КСС в режимі вбудовування від розміру контейнера як для запропонованої ефективної КСС, так і для КСС, що засновані на застосуванні простору сингулярного розкладення матриць-блоків контейнеру і ДКП. При цьому, не обмежуючи загальності, на рис. 20 відображені лише обчислювальні затрати на безпосередньо пряме та зворотне перетворення, а також операції шифрування/розшифрування за криптоалгоритмом AES-128, який є розповсюдженим у сучасних КСС.

Аналіз даних рис. 20 показує, що КСС, засновані на застосуванні простору сингулярного розкладення матриць-блоків контейнеру і ДКП, на відміну від запропонованої КСС, не здатні досягти навіть значення у 1 FPS в режимі вбудовування, що повністю унеможливлює їх застосування у режимі реального часу на ресурсообмежених платформах.

Отже, запропонована на основі розробленої науково-обґрунтованої методології реалізація КСС характеризується показниками ефективності, що перевищують відомі сучасні аналоги, підвищеним рівнем криптостійкості за рахунок застосування криптографічних примітивів, що володіють високою криптографічною якістю у сенсі їх представлення компонентними ФБЛ, а також через застосування операції шифрування послідовності переліку станів. При цьому завдяки тому, що здійснення операцій вбудовування та вилучення інформації відбувається у просторовій області, запропонована КСС володіє гарантовано нижчим рівнем обчислювальної складності, і, таким чином, може бути імплементована на сучасних ресурсообмежених платформах.

Отримані в шостому розділі дисертації результати, шляхом розробки S-блоків із врахуванням їх можливого представлення із застосуванням математичного апарату ФБЛ, 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%.

При цьому, побудовані у розділі криптографічні примітиви, на відміну від відомих існуючих аналогів, враховують криптографічну якість не тільки компонентних булевих функцій, а і компонентних ФБЛ. Таким чином, в розділі закінчено розробку як теоретичної, так і практичної складових методології побудови ефективних КСС, узагальнена схема якої представлена на рис. 21.

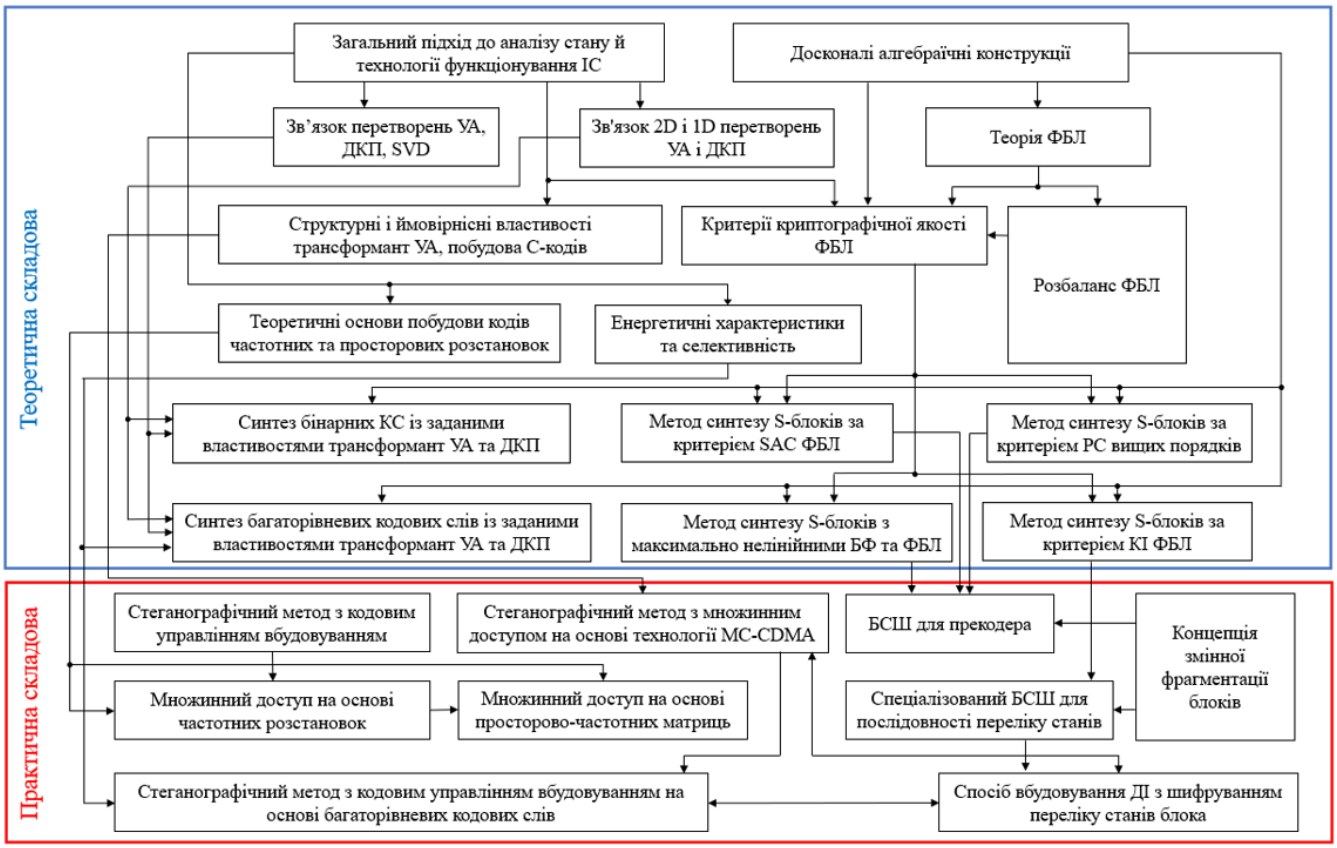


Рис. 21. Узагальнена схема методології розробки ефективних КСС

У табл. 6 наведено результати порівняльного аналізу відомих існуючих КСС із побудованою, відповідно до запропонованої методології.

Таблиця 6

Порівняльний аналіз відомих КСС з розробленою

Критерій / КСС	**Mukherjee (2015)**	**Shifa (2018)**	**CSRT (2018)**	**Seethalakshmi (2016)**	**Запропонована КСС**
Стійкість до атак проти вбудованого повідомлення	—	—	Немає даних	—	+
Забезпечення надійності сприйняття	+	+	+	+	+
Пропускна спроможність	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
Робота з потоковим контейнером в режимі реального часу	—	—	—	—	+
Реалізація на ресурсообмежених платформах	—	—	—	—	+

Аналіз даних табл. 6 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. 7.

Таблиця 7

Порівняння показників ефективності побудованої за розробленою методологією КСС із кращими існуючими аналогами

Критерій ефективності	Показник ефективності	Приріст ефективності	
Криптостійкість	Нелінійність	до 21.55%	можливість врахування криптографічної якості ФБЛ
	Лавинні властивості	до 9.375%	
	Кореляційний зв'язок векторів виходу та входу	до 12.5%	
	Алгебраїчна нелінійність	співпадає	
Швидкодія	Обчислювальна складність	в $\frac{4\mu}{3}$ разів	
Стійкість до атак проти вбудованого повідомлення	Кількість помилок при декодуванні ДІ в умовах атаки	в 8.125 разів	
Забезпечення надійності сприйняття стегано-повідомлення	PSNR, дБ	на 3%	
Пропускна спроможність стеганоканалів КСС у відсутності множинного доступу	$1/\mu^2$ (біт/піксель)	достатня	
Забезпечення можливості одночасного користування КСС декількома користувачами	Кількість каналів множинного доступу	у 1200 разів (зареєстрованих), у 16 разів (одночасно працюючих)	
Пропускна спроможність групового тракту	Середня довжина кодового слова l_{av}	на 6.25%	

Аналіз даних, представлених у табл. 7 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 примітивів при їх представленні за допомогою ФБЛ.

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.

СПИСОК РОБІТ АВТОРА ЗА ТЕМОЮ 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.

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**)

АНОТАЦІЯ

Соколов А.В. Методологія розробки ефективної крипто-стеганографічної системи. — Рукопис.

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. Відсутність аналогічних рішень в Україні та за кордоном робить результати досліджень пріоритетними. Отримані наукові результати мають фундаментальне (теоретичне) та прикладне (практичне) значення для розвитку та вдосконалення крипто-стеганографічних систем.

В роботі побудовано теоретичний базис для побудови крипто-стеганографічних систем, який надає можливість формування необхідних властивостей стеганоповідомлення при вбудовуванні інформації у просторовій області за рахунок реалізації концепції кодового управління вбудовуванням інформації. В контексті підвищення крипостійкості крипто-стеганографічних систем в роботі представлено теоретичний базис оцінки та підвищення криптографічної якості шифрів на основі математичного апарату функцій багатозначної логіки, що є основою підвищеннярівня імплементації шифрами дифузії та конфузії, підвищення їх ефективності та криптостійкості, а також узгодженості криптографічної і стеганографічної компоненти крипто-стеганографічних систем.

На основі побудованого теоретичного базису розроблено стеганографічні методи з кодовим управлінням вбудовуванням, а також спеціалізовані шифри для забезпечення узгодженості криптографічної та стеганографічної складової крипто-стеганографічних систем. Встановлено простоту алгоритмічної реалізації представлених методів, доведено можливість роботи крипто-стеганографічної системи на основі розробленої методології у режимі реального часу на ресурсообмежених платформах.

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.

The dissertation for the Doctor’s degree of Engineering Sciences in the specialty 05.13.21 — Information protection systems. — Lviv Polytechnic National University of the 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 code control of cryptographically protected additional information embedding in the spatial domain of the container. In the dissertation relationship between the transformants of the two-dimensional, one-dimensional Walsh-Hadamard transform and the discrete cosine transform, as well as the components of the singular value decomposition of the container block, is established, based on which formal sufficient conditions for the given properties of the steganographic message are obtained, and the theoretical foundations for the formation of steganographic methods with code control are developed.

The theoretical basis for the synthesis of effective codewords was formed, as well as indicators of energy and selectivity of the codeword were introduced and researched, which made it possible to synthesize multi-level codewords, which ensure the effectiveness of steganographic methods with code control developed on their basis. Two steganographic methods with code control of additional information embedding using binary and multi-level codewords have been created, which ensures their effectiveness, which exceeds modern analogs, in particular, in the conditions of a streaming container.

Using the developed theoretical basis, Reed-Solomon codes, and the developed codes of spatial arrangements, two steganographic methods with multiple access are proposed, which allow, while preserving the advantages of code control, to support the registration in the system of up to several thousand users and the simultaneous operation of several tens of users.

In the context of increasing the cryptographic strength of crypto-steganographic systems, the theoretical basis for ensuring the cryptographic quality of many-valued logic functions was built, which includes the following criteria: algebraic nonlinearity, distance nonlinearity, the avalanche effect criterion, the criterion of output independence from input variables, which made it possible to implement a justified choice of many-valued logic functions for the tasks of building specialized block symmetric ciphers for encrypting the states list sequence when using the steganographic method with code control of the additional information embedding. Based on the developed cryptographic quality criteria for many-valued logic functions, the sets of S-boxes of practically valuable lengths have been synthesized that 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 in terms of the criterion of independence of the output of the component many-valued logic functions from their input variables, which makes it possible to increase the cryptographic quality of cipher constructions used in crypto-steganographic systems.

Ready for practical implementation block symmetric cipher has been developed, the use of which allows to accelerate the destruction of the statistics of the plaintext, which made it possible to reduce the number of necessary iterations of the main step of cryptographic transformation, and, therefore, the computational costs for the operation of preliminary encryption of additional information in the preliminary coder of the crypto-steganographic system.

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

Algorithmic implementations of steganographic methods with code control of information embedding are characterized by realization simplicity, as well as the flexibility of setting properties of steganographic message by certain codewords choosing.

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