Міністерство освіти і науки України
Харківський національний університет імені В.Н. Каразіна
Навчально-науковий інституту комп’ютерних наук та штучного інтелекту
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

В.о. зав. кафедрою КІСМіТ
Марина ЄСІНА
“Допущено до захисту”

« »_____2025р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра

на тему: «Сучасні стеганографічні методи, дослідження та порівняльний аналіз»

оцінка «_____»

Голова ЕК

Мичуда Л.З.

Керівник: PhD. Шеханін К. Ю.

Рецензент: к.т.н. Олешко О. І.

Виконавець: студентка групи КБ-41
Капустенко А. Ю.

Харків 2025

РЕФЕРАТ

Пояснювальна записка до проекту бакалавра містить 56 сторінок, 10 рисунків 5 таблиць та 30 посилань на джерела.

Основною метою дослідження є обґрунтування доцільності комбінування цифрових методів стеганографії та криптографії з урахуванням практичної стійкості в умовах спотворення даних. Робота зосереджена на теоретичному аналізі сучасних підходів, оцінці їх ефективності, зокрема методу найменш значущих бітів (LSB), доповненого службовою інформацією, та алгоритму Fernet, що базується на AES.

Об’єктом дослідження є методи приховування даних у графічних контейнерах.

Предметом є аналіз стійкості та придатності модифікованих стеганографічних схем у контексті комбінованого захисту.

У роботі представлено огляд сучасного стану питання, класифікацію відповідних методів, порівняльні таблиці, моделі розміщення службових даних і результати симуляцій, що дозволяють оцінити рівень втрат при різних конфігураціях контейнерів.

Метод дослідження - порівняльно-аналітичний аналіз, доповнений емпіричними розрахунками та оцінкою ефективності схем.

Отримані результати можуть бути корисними при побудові систем інформаційної безпеки в умовах часткової втрати даних або необхідності прихованого обміну.

Ключові слова: СТЕГАНОГРАФІЯ, МЕТОД ЗАМІНИ НАЙМЕНШ ЗНАЧУЩИХ БІТІВ, LSB, МЕТОД КУТТЕРА-ДЖОРДАНА-БОССЕНА, МЕТОД ХРЕСТА, АТАКА ШЛЯХОМ ОБРІЗАННЯ ЗОБРАЖЕННЯ, КРИПТОГРАФІЯ, RSA.

ABSTRACT

The explanatory note for the bachelor's project contains 56 pages, 10 figures, 5 tables, and 30 references to sources.

The main objective of the research is to justify the feasibility of combining digital steganography and cryptography methods, taking into account practical robustness under data distortion conditions. The work focuses on the theoretical analysis of modern approaches and their effectiveness assessment, particularly the Least Significant Bit (LSB) method, enhanced with auxiliary service data, and the Fernet algorithm based on AES encryption.

The object of the study is data hiding methods in graphic containers.

The subject is the analysis of the resilience and applicability of modified steganographic schemes in the context of combined information protection.

The paper presents a review of the current state of the issue, a classification of relevant methods, comparative tables, models for embedding service data, and simulation results that allow for estimating message loss levels under various container configurations.

The research method is a comparative-analytical analysis, supported by empirical calculations and performance evaluation of the proposed schemes.

The obtained results may be useful for the development of information security systems under conditions of partial data loss or the need for covert communication.

Keywords: STEGANOGRAPHY, LEAST SIGNIFICANT BIT SUBSTITUTION METHOD, LSB, CUTTER-JORDAN-BOSSEN METHOD, CROSS METHOD, IMAGE CROPPING ATTACK, CRYPTOGRAPHY, RSA.

ЗМІСТ

ПЕРЕЛІК ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

КС - комп’ютерна стеганографія

ЦС - цифрова стеганографія

ЦВЗ - цифрові водяні знаки

НСД - несанкціонований доступ

НЗБ - найменш значущий біт

ПВЧ - псевдовипадкове число

ДКП - дискретне косинусне перетворення

ВСТУП

У сучасних умовах стрімкого розвитку інформаційних технологій та зростання обсягів електронного документообігу, проблеми конфіденційності, цілісності та автентичності цифрових даних набувають особливої актуальності. Однією з ключових загроз цифровій безпеці є можливість перехоплення, аналізу або модифікації інформаційного потоку без відома відправника чи одержувача. У зв'язку з цим традиційні криптографічні методи забезпечення безпеки інформації, хоч і залишаються актуальними, поступово доповнюються технологіями прихованого передавання, серед яких стеганографія займає провідне місце. Саме поєднання криптографічного та стеганографічного підходів дозволяє сформувати багаторівневий механізм захисту, що є не лише технічно ефективним, але й соціально значущим.

Науковий інтерес до проблем прихованої передачі інформації зумовлений не лише зростанням загроз у сфері кібербезпеки, але й практичною потребою захисту критичних відомостей у сфері журналістики, захисту прав людини, медицини, військової справи та інтелектуальної власності. Сучасні засоби інформаційної безпеки все частіше застосовуються в середовищах з обмеженими ресурсами - в мобільних пристроях, IoT-рішеннях, автономних сенсорних мережах. У цих умовах особливої цінності набувають методи, які поєднують високу криптостійкість із мінімальним навантаженням на апаратне забезпечення. До таких належать симетричні алгоритми шифрування та методи стеганографії на основі найменш значущих бітів (LSB).

Аналіз сучасної літератури [1-6; 13-15; 21-23] свідчить про активне застосування алгоритмів, що базуються на AES (Advanced Encryption Standard), серед яких особливе місце посідає бібліотека Fernet - готове програмне рішення, що поєднує симетричне шифрування, автентифікацію та контроль цілісності даних. У той самий час, метод LSB, попри свою простоту, демонструє на практиці досить високий рівень ефективності при обробці графічної інформації, особливо коли

йдеться про передавання невеликих обсягів повідомлень з вимогами до непомітності.

Наразі у відкритому доступі представлено чимало інструментів для стеганографічного приховування, однак більшість із них не орієнтовані на забезпечення комплексного захисту - як від виявлення прихованого факту комунікації, так і від несанкціонованого розшифрування вмісту. Саме тому дослідження, спрямоване на реалізацію комбінованого підходу шифрування з наступним вбудовуванням у мультимедійні файли, є актуальним як у теоретичному, так і в прикладному аспектах.

Об’єктом дослідження в бакалаврській роботі є процес прихованого передавання конфіденційної інформації в цифрових системах передачі даних.

Предметом дослідження є методи та алгоритми стеганографічного та криптографічного захисту, їх інтеграція в межах одного програмного рішення та оцінка ефективності такого поєднання в умовах часткової втрати контейнера.

Метою дослідження є теоретичне та емпіричне дослідження стійкості цифрових методів стеганографії та криптографії в умовах часткової втрати контейнера на прикладі модифікації методу LSB у поєднанні з алгоритмом Fernet.

Для досягнення поставленої мети необхідно розв’язати такі завдання:

- проаналізувати сучасні підходи до цифрового приховування інформації;
- провести класифікацію існуючих стеганографічних і криптографічних методів;
- обґрунтувати доцільність поєднання Fernet (AES) та модифікованого LSB;
- визначити стійкість такого підходу до обрізання/спотворення контейнера;
- порівняти результати з альтернативними методами на основі літератури та симуляцій.

Таким чином, ця робота покликана не лише поглибити розуміння можливостей комбінованого підходу захисту даних, але й дати практичні результати, які можуть бути використані для створення надійних, адаптивних рішень у сфері інформаційної безпеки.

1 ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОГО ПРИХОВУВАННЯ

1.1 Аналіз нормативно-правової бази у сфері захисту інформації

У сучасних умовах активного впровадження цифрових технологій, широкого поширення хмарних сервісів, мережевих сховищ та систем відеоспостереження особливої уваги набуває правове регулювання питань безпеки інформації. Водночас не менш важливою є проблема забезпечення конфіденційності під час передавання або зберігання даних із використанням стеганографічних або криптографічних методів. Оскільки такі методи безпосередньо пов’язані з обробкою візуальної та мультимедійної інформації, важливо враховувати як технічні, так і нормативні аспекти захисту даних.

З-поміж міжнародних документів, які становлять основу правового забезпечення інформаційної безпеки, ключове місце займає стандарт ISO/IEC 15444-8 (Secure JPEG 2000) - частина розширеної специфікації JPEG 2000, що розроблена в межах ініціативи ITU-T [19]. У цьому документі вперше на рівні міжнародного технічного регламенту визначено, яким чином може бути реалізоване шифрування в JPEG-контейнерах, зокрема - як можна додатково захищати зображення в процесі їх передавання або архівації. Застосування такого підходу дозволяє інтегрувати криптографічний захист на рівні стандартів, що особливо важливо у випадках, коли стеганографічні методи реалізуються поверх існуючих форматів зображень.

Додатково до міжнародних стандартів, у публікаціях [10] та [22] обґрунтовується важливість збереження структурної цілісності відеоданих у процесі їх стеганографічного або криптографічного опрацювання. Автори відзначають, що будь-яке втручання в бітову структуру візуального потоку має враховувати вимоги щодо допустимих змін - зокрема, недопущення втрат ключових ознак кадру або викривлення семантичного змісту. Це безпосередньо пов’язано з правовими нормами, що регулюють автентичність та достовірність цифрової інформації, особливо в контексті судово-експертної практики або кримінального процесу.

У згаданих роботах [23] і [24] пропонується концептуальний підхід до побудови криптокомпресійних систем, які передбачають одночасне застосування кількох методів захисту (наприклад, шифрування з одночасним стисненням), що відповідає сучасним вимогам до багаторівневої безпеки. Водночас наголошується на важливості узгодження таких методів із чинними стандартами, оскільки будь-які відхилення від формальних специфікацій можуть призвести до несумісності або недопустимих похибок під час передачі даних.

З української сторони правове регулювання базується на актах, які закріплюють загальні вимоги до обробки, передавання та збереження конфіденційної інформації. Зокрема, відповідно до Закону України «Про інформацію» та Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», розробка й використання засобів захисту має здійснюватися із забезпеченням технічної сумісності, контролю доступу та належного рівня криптографічного захисту. Окремі положення також узгоджуються із рекомендаціями Національного координаційного центру кібербезпеки при РНБО України.

У цьому контексті важливими є також практичні підходи, запропоновані в роботах [9], [11], [12], де акцент зроблено на реалізацію технологій безпечного кодування, зокрема - для відеоресурсів, що передаються через публічні канали зв’язку. При цьому особливе значення надається забезпеченню цілісності кодувального потоку, контролю над втратою структурної інформації, а також наявності засобів ідентифікації або виявлення модифікацій, які могли бути внесені під час несанкціонованого доступу.

Варто підкреслити, що нормативно-правова база в галузі захисту інформації постійно оновлюється відповідно до нових викликів. Так, актуальними залишаються підходи, пов’язані з контролем якості переданого контенту, що вказано у дослідженнях [4], де оцінюється взаємозв’язок між параметрами QoE та QoS, що опосередковано визначають вимоги до методів приховування інформації.

Таким чином, правова та нормативна база у сфері захисту інформації є багатокомпонентною та динамічною. Вона охоплює як технічні стандарти

міжнародного рівня (ISO/IEC, ITU-T), так і національне законодавство, а також прикладні дослідження, що деталізують конкретні технічні сценарії застосування. У межах цієї дипломної роботи дотримання відповідних вимог виступає не лише необхідною формальністю, а й гарантією того, що розроблене рішення має потенціал до масштабованого та легітимного впровадження у реальні інформаційно-комунікаційні системи.

1.2 Взаємозв'язок криптографії та стеганографії у сучасних системах захисту інформації

У сучасних умовах високої насиченості цифрового простору питання інформаційної безпеки вже не зводиться до простої задачі шифрування вмісту. Реальні загрози перехоплення, модифікації або блокування інформації потребують системного, багаторівневого підходу, в якому поєднуються засоби криптографічного захисту зі способами стеганографічного маскування самої передачі.

Криптографія, як метод захисту інформації через математичне перетворення її структури, традиційно виступає ядром безпеки. Вона дозволяє забезпечити конфіденційність, автентичність і цілісність даних у процесі зберігання чи передавання. Сучасні реалізації шифрування, зокрема алгоритм AES, покладено в основу численних прикладних протоколів, таких як TLS, SSH та Signal Protocol. У межах цієї роботи було обрано Fernet - перевірену реалізацію AES із вбудованим контролем цілісності, яка дозволяє забезпечити надійне симетричне шифрування повідомлень перед їх вбудовуванням у візуальні контейнери.

Стеганографія, своєю чергою, має іншу мету - приховати сам факт передавання інформації, маскуючи її серед звичайного цифрового шуму, зображень чи інших об'єктів. У результаті навіть якщо зловмисник отримає доступ до каналу передавання, він не зможе виявити сам факт передачі прихованого повідомлення. У поєднанні з криптографією це створює подвійну лінію захисту: повідомлення не лише зашифроване, а й непомітне.

У загальному вигляді взаємодія між криптографічним і стеганографічним рівнями зображена на рисунку 1.1. Секретний файл попередньо шифрується, після

чого результуючий бітовий потік вбудовується у відкритий цифровий контейнер (наприклад, зображення чи відеофайл) відповідно до заданого ключа. На стороні одержувача виконується зворотна процедура: за допомогою ключа декодування відбувається витяг прихованих даних із заповненого контейнера та їх розшифрування.

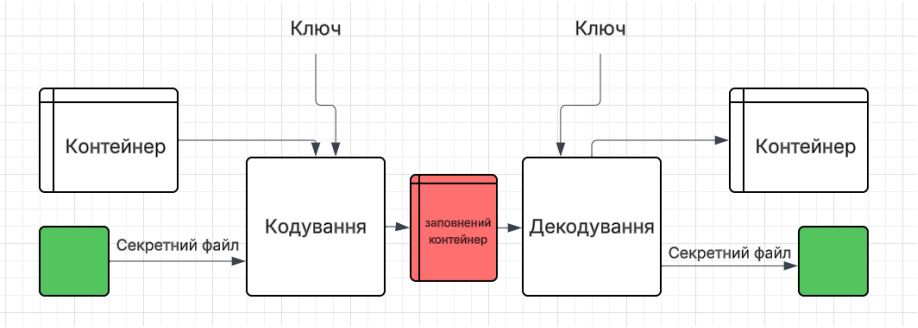

Рисунок 1.1 - Схема захисту інформації з використанням стеганографії

Така схема дозволяє побудувати двоетапну систему захисту, де одночасно забезпечується як конфіденційність змісту (через шифрування), так і непомітність передавання (через приховування). Це значно ускладнює як виявлення самої інформації, так і її несанкціоноване декодування.

У публікаціях [6], [7], [8], [23] запропоновано різні технічні рішення щодо реалізації такого підходу. У [6] представлено огляд методів шифрування на основі хаотичних відображень, які демонструють високу стійкість до криптоаналізу. Такі методи особливо ефективні в умовах, коли зашифровані повідомлення попередньо вбудовуються в цифрові зображення. Вони гарантують, що навіть у разі виявлення прихованого шару даних, декодування без початкового ключа буде практично неможливим.

У роботі [8] розглянуто використання клітинних автоматів як основи для зворотного шифрування з подальшим застосуванням до LSB-кодування. Завдяки поєднанню шифрування та стеганографії вдається досягти балансу між продуктивністю, енергоспоживанням і безпекою, що є критичним у мобільних або вбудованих системах.

У публікації [7] автори розглядають інноваційний підхід до захисту приватності, базуючись на використанні зворотного візуального перетворення

JPEG-зображень. У цьому випадку криптографічні та стеганографічні механізми інтегруються так, щоб не порушувати візуальну цілісність зображення. Це особливо важливо в системах, де перцептивна якість контенту відіграє вирішальну роль - наприклад, у захисті персональних фото або відео у відкритих каналах зв’язку.

У свою чергу, дослідження [23] представляє комплексну концепцію захисту візуального контенту, що реалізується через криптокомпресійну систему. Така система поєднує алгоритми стиснення, шифрування та вбудовану стеганографію в єдиний процес. Вона не лише забезпечує багаторівневий захист інформації, а й сприяє зменшенню обсягу переданих даних без втрати їхньої структури чи змісту.

Загалом поєднання стеганографічних і криптографічних технологій формує сучасні адаптивні стратегії захисту, де інформація не просто шифрується, а стає невидимою для потенційного зловмисника. Такий підхід повністю відповідає сучасним уявленням про інформаційну гігієну, цифрову обізнаність і кібербезпеку в умовах, коли загрози дедалі частіше мають не лише технічну, а й соціотехнічну природу.

Стеганографія як наука і практика приховування інформації має глибоке історичне коріння, що сягає задовго до появи комп’ютерних технологій. У давнину використовувалися численні хитромудрі методи, які дозволяли таємно передавати повідомлення, не викликаючи підозри в оточення. Наприклад, одним із відомих способів було нанесення тексту на дерев’яну дощечку, яку потім покривали шаром воску — поверх можна було написати інше повідомлення, а справжній текст залишався прихованим під шаром покриття. Інші методи передбачали використання симпатичних чорнил, що ставали видимими лише під дією тепла або хімічних реактивів, або приховування текстів у швах одягу, зачісках, на тілі.

Ці техніки, попри свою зовнішню простоту, втілювали фундаментальну ідею: зробити повідомлення непомітним для стороннього спостерігача, залишаючи можливість для адресата його розпізнати. Саме цей базовий принцип непомітності, а не лише шифрування змісту, ліг в основу сучасної цифрової стеганографії. У наш час історичні методи вже не є ефективними в традиційному сенсі, однак

концептуально вони залишаються актуальними, особливо в гібридних схемах захисту, де класичні фізичні носії поєднуються з цифровими технологіями для побудови багаторівневих каналів комунікації.

На рисунку 1.2 представлено узагальнену класифікацію традиційних підходів до стеганографії, які умовно поділяються на хімічні (використання органічних розчинів, ферментів, реактивів тощо) та фізичні методи (мікрографія, приховування предметів, маскування візуальних маркерів). Такі підходи можуть знаходити нове життя у контексті інформаційно-психологічних операцій, коли технічна непомітність інформації доповнюється її когнітивною непомітністю. У поєднанні з цифровими засобами стеганографія класичного типу може бути адаптована до нових умов, наприклад — у формі комбінованих каналів зв'язку, які використовують і матеріальні носії, і криптографічні схеми одночасно

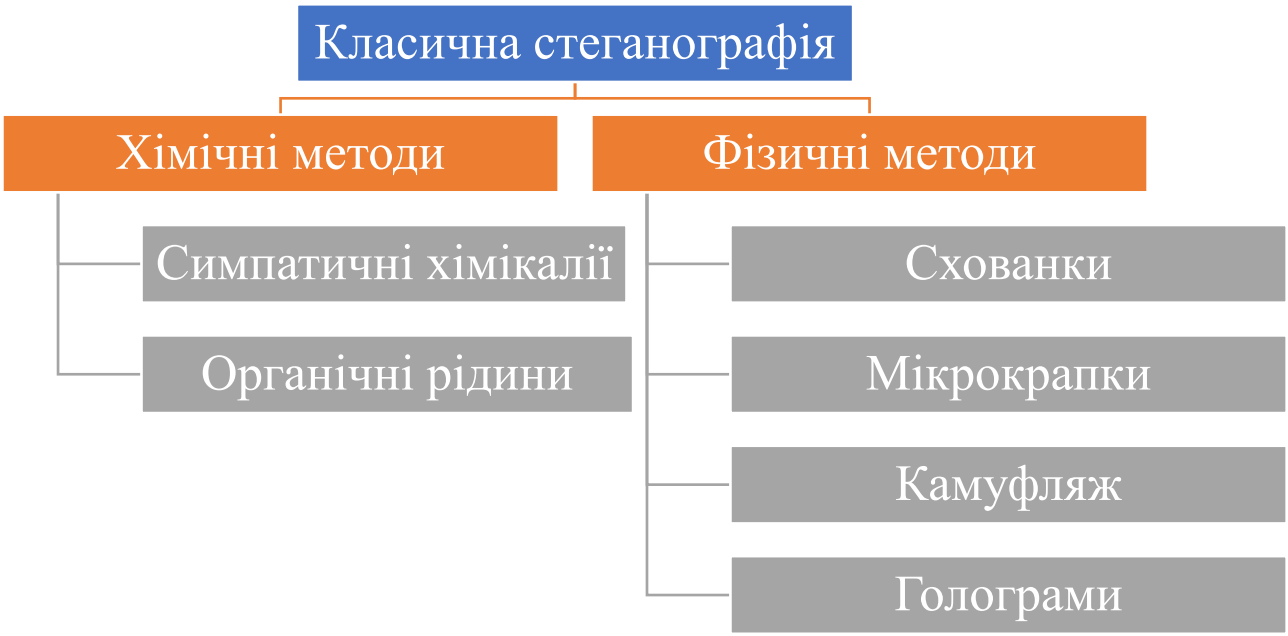

Рисунок 1.2 - Основні напрямки класичної стеганографії

Розглянуті методи демонструють, що ефективний захист інформації базується не на ізольованому використанні криптографії чи стеганографії, а на їх комбінованому застосуванні. Такий підхід дозволяє забезпечити як прихованість самої передачі, так і захист вмісту на рівні даних. Проте, для повноцінної реалізації подібних систем необхідно обрати конкретні алгоритми шифрування, які б

відповідали вимогам криптостійкості, продуктивності й сумісності з цифровими стеганографічними контейнерами.

У цьому контексті першочергове значення має аналіз симетричних алгоритмів шифрування, які завдяки своїй високій швидкодії, відносно невеликій обчислювальній складності та простоті апаратної й програмної реалізації, широко застосовуються в прикладних системах інформаційної безпеки. На відміну від асиметричних схем, симетричні алгоритми використовують один і той самий ключ як для шифрування, так і для дешифрування повідомлення, що забезпечує зручність інтеграції в системи з обмеженим доступом або з попередньо розподіленими ключами [6], [7].

Особливої актуальності симетричне шифрування набуває в умовах роботи із мультимедійними об’єктами, які вимагають обробки великих обсягів даних у режимі реального часу. У таких випадках навіть незначне збільшення обчислювального навантаження може негативно вплинути на загальну продуктивність системи. Саме тому подібні алгоритми активно застосовуються у вбудованих пристроях, мобільних застосунках, а також у стеганографічних реалізаціях, де зашифроване повідомлення вбудовується в цифровий контейнер із суворими обмеженнями на зміну структури файлу [8], [23].

Сучасні симетричні алгоритми, такі як AES, Blowfish, RC6 або ChaCha20, забезпечують високий рівень криптостійкості, підтверджений не лише академічними дослідженнями, а й багаторічною практикою використання у стандартизованих протоколах. У рамках цієї роботи особливу увагу приділено реалізації алгоритму Fernet, який базується на AES у режимі CBC та містить вбудовану перевірку цілісності даних. Цей алгоритм було обрано завдяки його практичності, простоті реалізації у Python-середовищі та відповідності вимогам до сучасної інформаційної безпеки у прикладних програмних продуктах [6], [23].

1.3 Алгоритми симетричного шифрування: огляд та застосування

Симетричні алгоритми шифрування є одним із фундаментальних напрямів криптографії, заснованих на принципі використання одного й того ж ключа як для шифрування, так і для розшифрування повідомлення. Попри значний розвиток

асиметричних систем, симетричні методи залишаються надзвичайно актуальними завдяки своїй високій швидкодії, ефективності в умовах обмежених обчислювальних ресурсів та простоті реалізації як у програмному, так і в апаратному середовищі [6], [7].

У загальному вигляді симетричне шифрування (рис. 1.3) передбачає існування множини допустимих ключів, з яких кожен визначає конкретну функцію перетворення відкритого тексту у зашифрований. Криптостійкість таких алгоритмів значною мірою залежить від кількості можливих ключів та складності математичних операцій, необхідних для перебору усіх варіантів. До переваг симетричних систем відносять високу продуктивність, незалежність безпеки від конкретного реалізованого програмного середовища, а також відсутність необхідності в обміні відкритими ключами через ненадійні канали зв’язку [8], [23].

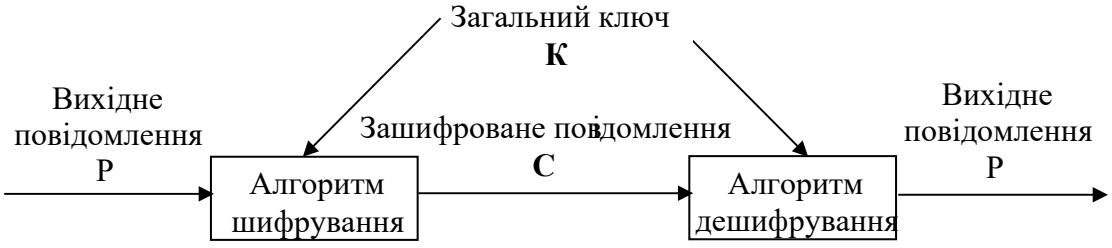

Рисунок 1.3 - Загальна схема симетричного шифрування

Класифікація симетричних алгоритмів здійснюється за кількома критеріями. Залежно від способу перетворення повідомлення виділяють потокові та блочні шифри. Потокові шифри обробляють вхідні дані побітово або побайтно, що забезпечує низьку затримку і добре підходить для потокової передачі. У той час як блочні шифри працюють із фіксованими блоками інформації (зазвичай 64 або 128 біт), що дозволяє реалізувати складніші схеми шифрування з підвищеною стійкістю.

Залежно від методу обробки відкритого тексту, симетричні шифри поділяються на кілька типів:

1) Моноалфавітні підстановки - кожен символ замінюється на інший за фіксованим правилом.

2) Багатоалфавітні підстановки - використовуються кілька алфавітів, що чергуються за певним законом.
3) Перестановки - символи відкритого тексту змінюють своє розташування.
4) Гамування - повідомлення комбінується з псевдовипадковою послідовністю (гамою).
5) Блочне шифрування - обробка інформації блоками із застосуванням складних нелінійних перетворень.

Серед сучасних симетричних алгоритмів найбільш відомими є:

- DES (Data Encryption Standard) - історичний стандарт, що має низьку криптостійкість через короткий ключ (56 біт);
- Triple DES (3DES) - удосконалення DES через потрійне шифрування, але знижена ефективність;
- AES (Advanced Encryption Standard) - сучасний міжнародний стандарт, що підтримує довжини ключа 128, 192 і 256 біт і забезпечує високу стійкість до атак;
- Blowfish - алгоритм із довільною довжиною ключа до 448 біт, зручний для реалізації;
- RC6, IDEA, Serpent, Twofish - альтернативи з різним ступенем криптографічної складності й швидкодії.

Оцінка надійності симетричних алгоритмів традиційно ґрунтується на понятті криптостійкості, яка визначає здатність алгоритму протистояти розшифруванню без знання ключа. Основними критеріями виступають:

- кількість можливих ключів;\
- об’єм необхідної вибірки для проведення атаки;
- складність математичної задачі, що лежить в основі шифрування;
- стійкість до атак на основі відомих відкритих або зашифрованих повідомлень.

Симетричні алгоритми шифрування залишаються ключовим інструментом у сучасних системах захисту даних, особливо у випадках, коли обидві сторони обміну перебувають у заздалегідь узгодженому, довіреному середовищі. Це

можуть бути як внутрішні сегменти корпоративних мереж, так і замкнені стеганографічні системи, де питання безпечного обміну ключами вирішується на рівні інфраструктури. В таких умовах симетричне шифрування демонструє високу продуктивність і мінімальні вимоги до ресурсів, що робить його оптимальним вибором для рішень, де критичною є швидкість та компактність реалізації без втрати рівня безпеки.

Завдяки цим властивостям симетричні шифри широко використовуються не лише в класичних IT-інфраструктурах, але й у стеганографічних системах, де крім конфіденційності важливо зберегти сам факт передачі даних у таємниці. На відміну від криптографії, яка унеможливлює розшифрування змісту без відповідного ключа, але не приховує сам факт наявності зашифрованого контенту, стеганографія спрямована на інше — приховати саме існування передаваного повідомлення. Це критично важливо в умовах, коли загроза перехоплення метаданих, моніторингу трафіку або відстеження цифрової активності користувачів стає дедалі реальнішою.

З огляду на це, доцільно перейти до аналізу базових принципів функціонування стеганографічних систем. Буде розглянуто ключові характеристики процесу приховування, типову архітектуру таких систем, а також їхню класифікацію за ступенем впливу на контейнер, рівнемнепомітності, стійкістю до атак і пропускною здатністю.

1.4 Принципи та моделі стеганографічного приховування інформації

Комп’ютерна стеганографія ґрунтується на ідеї непомітного вбудовування інформації в цифрові об’єкти без порушення їхньої основної функціональності. На відміну від криптографії, яка лише зашифровує повідомлення, стеганографія приховує сам факт його існування, що особливо важливо в умовах ризику перехоплення трафіку або цифрових артефактів.

Переважна більшість методів цифрової стеганографії базується на двох принципах: по-перше, можливості модифікації файлів, точність яких не є критичною, без втрати їхньої функціональності; по-друге, забезпечення такої модифікації, яка є візуально, аудіально чи текстуально непомітною для людини, і

може бути виявлена лише з використанням спеціалізованих програмно-аналітичних засобів [6], [7].

Стеганографічні системи функціонують за типовою моделлю, що включає відкритий текст, контейнер, механізм вбудовування, можливий стеганографічний ключ і алгоритм вилучення. Такий підхід дозволяє забезпечити цілісність інформації та її збереження під час передачі. Узагальнена схема функціонування подібних систем подана на рисунку 1.4.

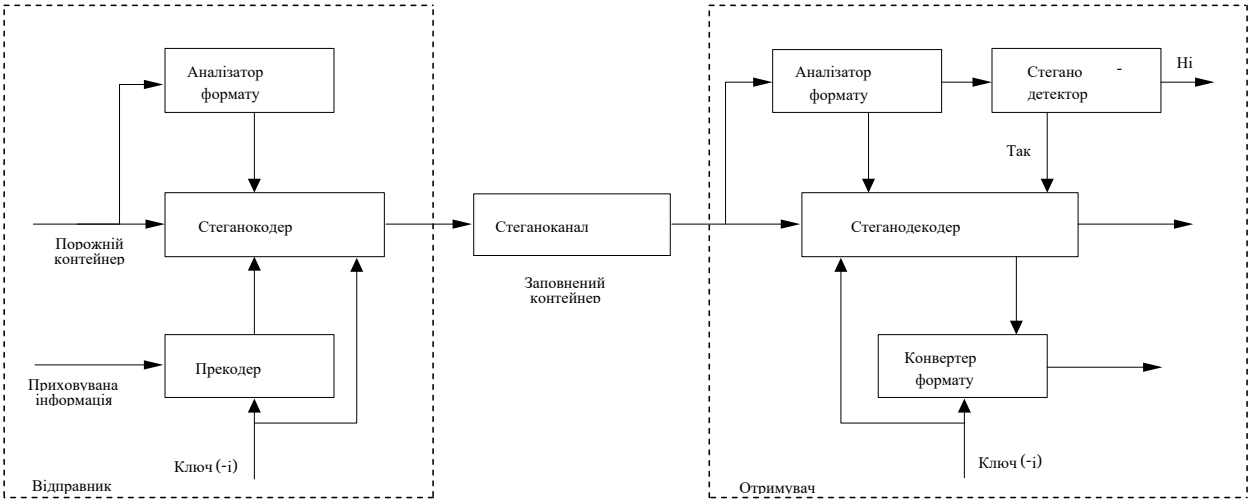

Рисунок 1.4 - Узагальнена модель стеганографічного приховування даних

Методи стеганографії класифікують за різними ознаками: за середовищем вбудовування (зображення, відео, аудіо, текст), за типом модифікації (просторова чи частотна область), а також за рівнем стійкості, прихованості, пропускної здатності та надійності передачі. Типову класифікацію сучасних комп’ютерних методів подано на рисунку 1.5.

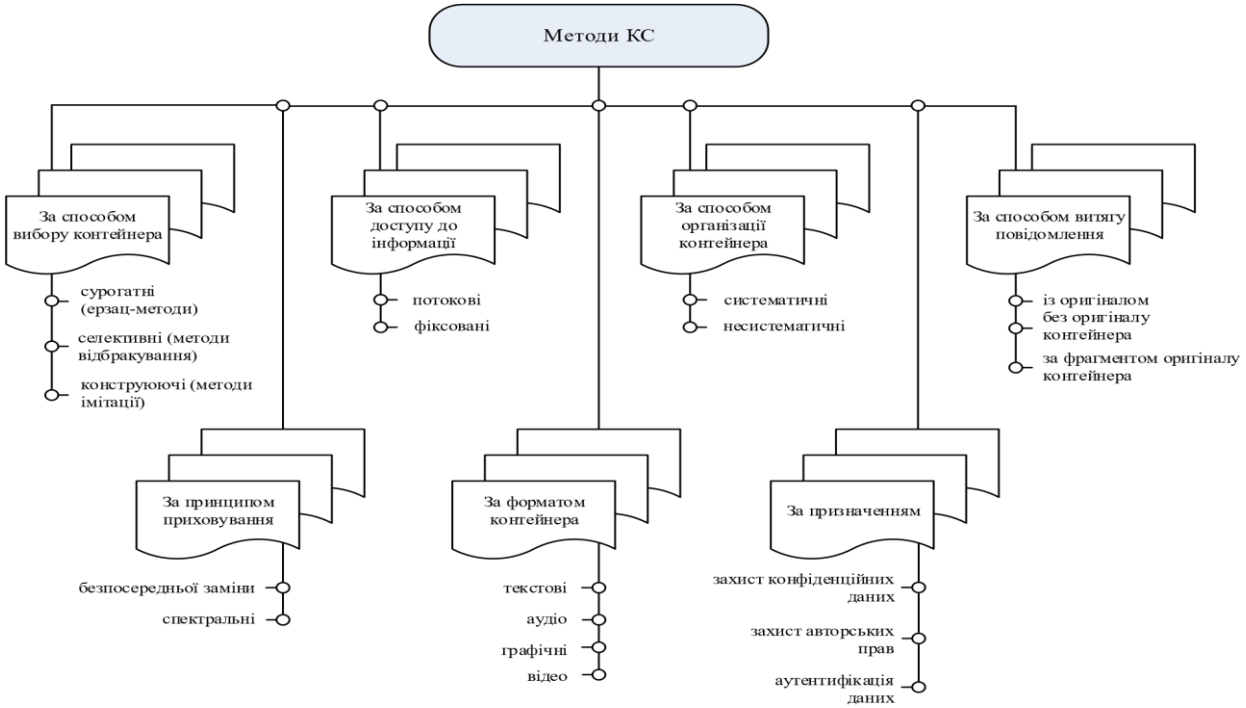

Рисунок 1.5 - Класифікація методів комп’ютерної стеганографії

Серед методів, що базуються на використанні специфічних властивостей форматів, виділяють такі підходи: модифікація зарезервованих полів, які зазвичай не використовуються програмами і можуть бути заповнені довільними даними; спеціальне форматування тексту, зокрема зміщення слів, абзаців або застосування шаблонного вибору символів; використання незадіяних областей пам’яті на цифрових або магнітних носіях, що не впливають на цілісність або доступність даних для користувача.

Попри простоту реалізації, ці методи характеризуються низькою пропускною здатністю та обмеженою надійністю. Зміна структури контейнера, його перекодування або конверсія формату можуть призвести до повної або часткової втрати прихованої інформації. Крім того, їх рівень прихованості не завжди забезпечує стійкість до сучасних методів виявлення, зокрема до статистичного аналізу або спектрального розкладу [6], [23].

Таким чином, ефективне стеганографічне приховування інформації базується на балансі між непомітністю змін, обсягом даних, які можливо вбудувати, і стійкістю до зовнішніх впливів. Розуміння цих принципів є передумовою для побудови надійної стеганосистеми, яка не лише виконує свою функцію, а й залишається прихованою від стороннього спостереження.

1.5 Висновки за розділом

У першому розділі було здійснено теоретичне обґрунтування ключових понять, що лежать в основі сучасних технологій прихованого захисту інформації. Розглянуто нормативно-правову базу, що регламентує захист даних, визначено місце криптографії у системі інформаційної безпеки та класифіковано основні напрями її застосування. Особливу увагу приділено симетричним алгоритмам шифрування, які, завдяки своїй ефективності, простоті та криптостійкості, становлять основу для багатьох стегокриптографічних рішень.

Проаналізовано сутність та функціональні характеристики комп’ютерної стеганографії, яка виступає як інструмент прихованого передавання інформації шляхом модифікації цифрових контейнерів без візуально помітних змін. Наведено принципи побудови стеганосистем і їхні структурні моделі, що включають елементи вбудовування та витягування повідомлень із використанням допоміжних ключів або детермінованих правил. Узагальнено підходи до класифікації методів за ознаками середовища, типу змін, рівня прихованості та стійкості до впливів.

Сформульовані положення закладають теоретичну основу для подальшого дослідження методів комп’ютерної стеганографії, реалізованих у вигляді прикладної системи, та дозволяють критично оцінити їхню ефективність у межах практичної реалізації, що буде розглянута в наступних розділах роботи.

2 ВИБІР ТА ОБҐРУНТУВАННЯ МЕТОДІВ ДЛЯ РЕАЛІЗАЦІЇ СИСТЕМИ

2.1 Вибір криптографічного методу: аналіз можливостей Fernet (AES)

Одним із ключових етапів побудови стеганографічної системи є вибір криптографічного методу, що забезпечує конфіденційність повідомлення ще до його вбудовування в контейнер. Для досягнення надійного рівня безпеки сучасні стеганосистеми комбінують криптографічні та стеганографічні перетворення, створюючи багаторівневий захист даних. У цьому контексті особливої актуальності набувають симетричні алгоритми шифрування, які дозволяють досягти високої швидкодії, гнучкості та сумісності з мультимедійними форматами.

Серед множини сучасних алгоритмів особливу увагу привертає стандарт AES (Advanced Encryption Standard), який підтримує довжину ключа 128, 192 і 256 біт, працює з блоками даних по 128 біт і має високий рівень криптостійкості [6]. Його перевагами є стійкість до статистичного й диференційного аналізу, ефективність реалізації на різних апаратних архітектурах і відкритість алгоритму, що сприяє його широкому впровадженню в індустріальних і дослідницьких застосуваннях.

У рамках даної роботи обґрунтовано вибір високорівневої реалізації AES - криптографічного інтерфейсу Fernet, який є частиною бібліотеки cryptography у Python. Fernet базується на AES у режимі CBC з довжиною ключа 128 біт і застосовує HMAC на SHA-256 для перевірки цілісності даних. Така комбінація забезпечує не лише шифрування, але й автентифікацію повідомлення, що є додатковим захистом від несанкціонованого модифікування інформації під час передавання або зберігання [23]. Важливою перевагою алгоритму Fernet є його висока доступність для інтеграції у програмні середовища. Завдяки автоматизованому керуванню ініціалізаційним вектором, вбудованій функції генерації ключа, простому синтаксису та підтримці типових типів даних, реалізація шифрування за допомогою Fernet не потребує глибокого криптографічного досвіду від розробника, що значно підвищує надійність і зменшує ризик помилок. Це особливо важливо в умовах використання шифрування як допоміжного етапу перед вбудовуванням повідомлення в цифрове зображення методом LSB.

Архітектура блочного шифрування AES, що лежить в основі алгоритму Fernet, представлена на рисунку 2.1. Вона включає попередню трансформацію, набір раундів шифрування та механізм розширення ключа, завдяки якому генеруються раундові ключі K0,K1,...,KnK_0, K_1, ..., K_nK0,K1,...,Kn, що використовуються в кожному циклі перетворення. Такий підхід забезпечує високу ступінь дифузії та ускладнює криптоаналіз навіть при обмеженій довжині ключа.

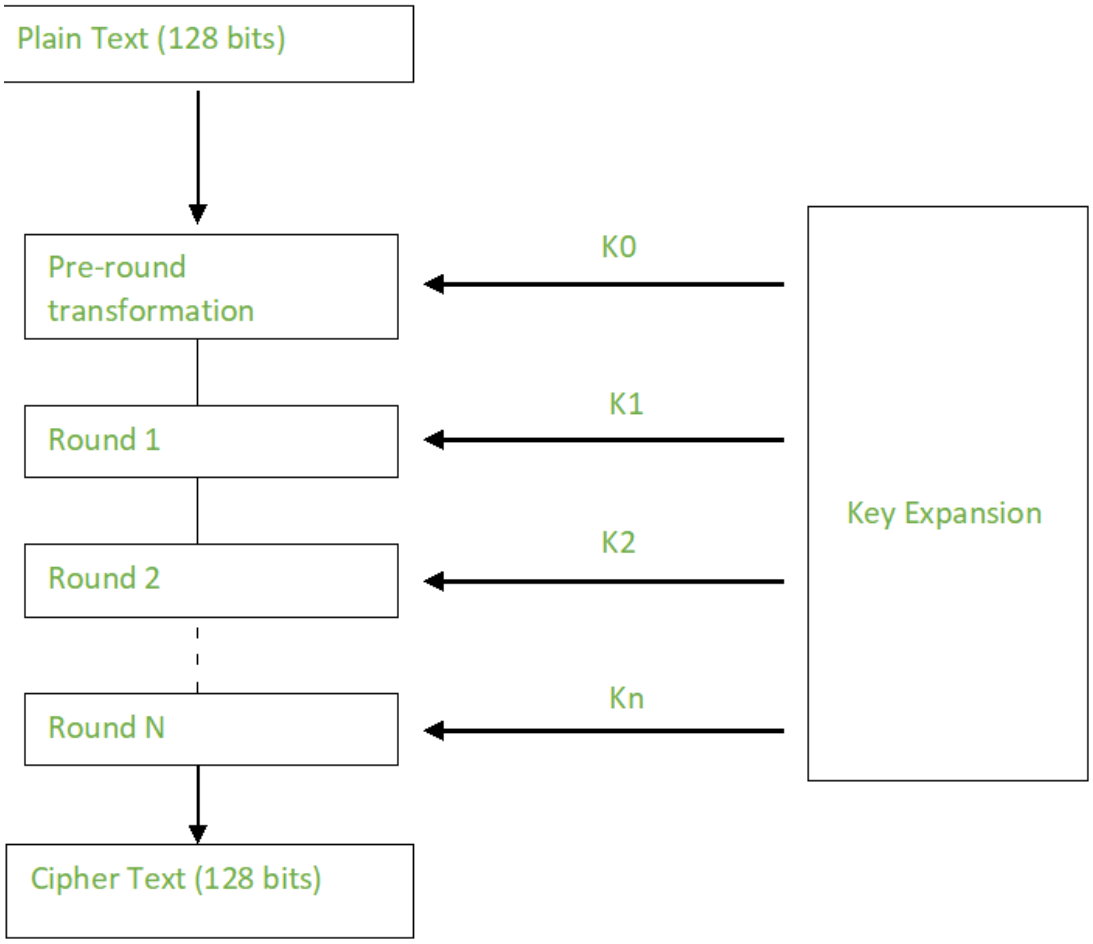

Рисунок 2.1 - Загальна структура роботи шифрування AES із розширенням ключа

У межах реалізації Fernet ці раунди приховані за рівнем абстракції бібліотеки, однак алгоритм використовує повноцінну AES-схему з режимом CBC і контрольну суму HMAC, що дозволяє забезпечити не лише шифрування, а й перевірку цілісності даних.

Окрему увагу слід звернути на особливості реалізації Fernet як високорівневого інтерфейсу над AES: бібліотека cryptography не лише автоматизує процес генерації ключів та ініціалізаційного вектора, а й враховує сучасні вимоги до захисту від типових векторів атак, таких як повторне використання ключа, модифікація шифротексту чи підміна автентичності повідомлення. Зокрема, за замовчуванням у структурі шифротексту використовується HMAC на SHA-256 для перевірки цілісності, а також вбудовується мітка часу, що може використовуватись як механізм обмеження строку дії зашифрованого повідомлення або токена.

Таким чином, Fernet не варто розглядати лише як обгортку до AES - це повноцінний криптографічний контейнер, що поєднує функції шифрування, цілісності та структурованого форматування, придатний для безпечного вбудовування в цифрові носії. Його ключові компоненти, принципи функціонування та практичне призначення узагальнено у таблиці 2.1.

Таким чином, вибір Fernet як програмної реалізації AES у цій роботі є обґрунтованим з погляду криптографічної стійкості, сумісності з форматом прихованого передавання, зручності реалізації в Python-середовищі та відповідності вимогам до сучасного багаторівневого захисту інформації.

Таблиця 2.1 - Функціональні компоненти алгоритму Fernet

Компонент	Призначення
1	2
AES у режимі CBC	Блочне шифрування даних з використанням 128-бітового ключа та ініціалізаційного вектора (IV); забезпечує конфіденційність повідомлення.
HMAC на SHA-256	Генерує контрольну суму для перевірки цілісності зашифрованого повідомлення; захищає від модифікації.
Ініціалізаційний вектор (IV)	Випадково згенерований для кожного шифрування; гарантує унікальність результату навіть при однаковому ключі та повідомленні.

Подовження таблиці 2.1

Компонент	Призначення
1	2
Base64-форматування	Кодування результуючого токена у формат, зручний для передавання через текстові канали або вбудовування в мультимедіа.
Позначка часу (timestamp)	Опціонально вбудовується в токен; дозволяє реалізовувати обмеження строку дії повідомлення.
Генератор ключів (Fernet.generate_key)	Створює криптографічно стійкий симетричний ключ, що використовується для шифрування й дешифрування.

Як видно з таблиці 2.1, алгоритм Fernet поєднує низку важливих функцій, які суттєво розширюють можливості базового AES-шифрування та роблять його зручним і надійним інструментом для застосування в умовах сучасних цифрових загроз. Зокрема, автоматизоване управління ключами, автентифікація даних через HMAC, підтримка мітки часу й форматування результату у вигляді зручного для передачі токена забезпечують відповідність Fernet принципам надійності, цілісності та повторного використання.

Важливо й те, що реалізація Fernet легко інтегрується у програмні рішення, пов’язані з мультимедійною інформацією, зокрема в стеганографічні системи. Завдяки сталому вихідному формату та підтримці текстових і бінарних повідомлень, результат шифрування легко адаптується до особливостей зображень, аудіофайлів чи відеопотоків як контейнерів для прихованого вбудовування.

Таким чином, обґрунтованість вибору Fernet полягає не лише в його теоретичних перевагах, але й у високій практичній сумісності з методами стеганографії, які будуть розглянуті в наступному підпункті. Подальший аналіз буде присвячено оцінці доцільності використання методу Least Significant Bit (LSB), який забезпечує приховування шифрованого повідомлення у цифрових зображеннях без помітного впливу на їх візуальну якість.

2.2 Обґрунтування вибору методу LSB для стеганографії

Одним із найбільш поширених і практично застосовуваних методів цифрової стеганографії є метод заміни найменш значущого біта (Least Significant Bit, LSB). Його популярність пояснюється простотою реалізації, високою прихованістю змін і сумісністю з графічними форматами, які зберігають значний обсяг непомітних для людського сприйняття даних. Суть цього методу полягає у заміні останніх (найменш значущих) бітів байтів, що описують окремі пікселі в графічному зображенні, на біти прихованого повідомлення. Таке перетворення забезпечує мінімальну візуальну різницю між вихідним і модифікованим контейнером, що майже не фіксується навіть високоточними пристроями відтворення [21].

Для прикладу, розглянемо 8-бітне зображення у відтінках сірого, де значення 00000000b відповідає чорному кольору, а 11111111b - білому. Якщо вбудовувати 1 байт інформації (наприклад, 01101011b), то, використовуючи по 2 молодших біта в кожному пікселі, потрібно змінити чотири пікселі. Припустимо, що всі пікселі мали значення 00000000b. Після вбудовування вони набудуть вигляду 00000001b, 00000010b, 00000010b, 00000011b, що еквівалентно змінам яскравості лише на 1, 2, 2 і 3 з 255 градацій відповідно. Такі зміни залишаються непомітними для людського зору, особливо на фоні шуму, присутнього в оригінальному зображенні [6], [21].

Для підвищення ефективності методу LSB як контейнер доцільно використовувати зображення у форматі BMP високої роздільної здатності з глибиною кольору 24 або 32 біти. Приховане повідомлення може бути представлене як текст, а також як графічне зображення з розширенням BMP, GIF, PNG або JPEG. Чим більший об’єм зображення, тим більше даних можна приховати з меншими візуальними наслідками. Водночас слід зазначити, що при зменшенні розміру контейнера різниця між сусідніми пікселями, в які вбудовано дані, може стати помітнішою.

Недоліки класичного методу заміни найменш значущих бітів (LSB) стають особливо критичними в умовах нестабільного середовища передачі або за наявності ризику навмисної модифікації контейнера. Навіть незначна втрата пікселів, зумовлена обрізанням або стисненням зображення, здатна призвести до

зміщення координат повідомлення, а отже — до його повної або часткової втрати. Окрім того, статистичний аналіз піксельних значень, наприклад через побітовий перегляд або гістограму, дозволяє виявити області з високим ступенем змінності, що потенційно свідчить про приховану інформацію [8], [23].

У зв’язку з цим у межах даного дослідження запропоновано модифікований варіант LSB-методу, який передбачає додавання службових метаданих до зображення-контейнера. Суть полягає у вбудовуванні в певний псевдовипадково обраний піксель унікальної мітки — послідовності символів, малоймовірної для появи в природному зображенні. Одразу після мітки записуються розміри зображення (ширина і висота), що дозволяє з високою точністю оцінити первинну конфігурацію контейнера, навіть якщо його обрізано. У наступних бітових комірках вбудовуються координати розміщення мітки, що забезпечує додаткову перевірку її достовірності при читанні.

Як зображено на рисунку 2.2, така модифікація дозволяє здійснювати прив’язку вбудованого повідомлення до конкретного фрагмента зображення, зберігаючи можливість його реконструкції навіть після часткових втрат. У разі, якщо реальні розміри зображення не відповідають записаним, програма видає попередження про зміну контейнера. Далі система визначає зсув координат і виконує логічну реконструкцію структури зображення для вилучення максимально повного фрагмента повідомлення. Таким чином, навіть у разі порушення цілісності контейнера, ймовірність повного втрачання повідомлення суттєво зменшується, що підвищує практичну цінність даного методу для застосування в умовах ризику атак або втрат даних.

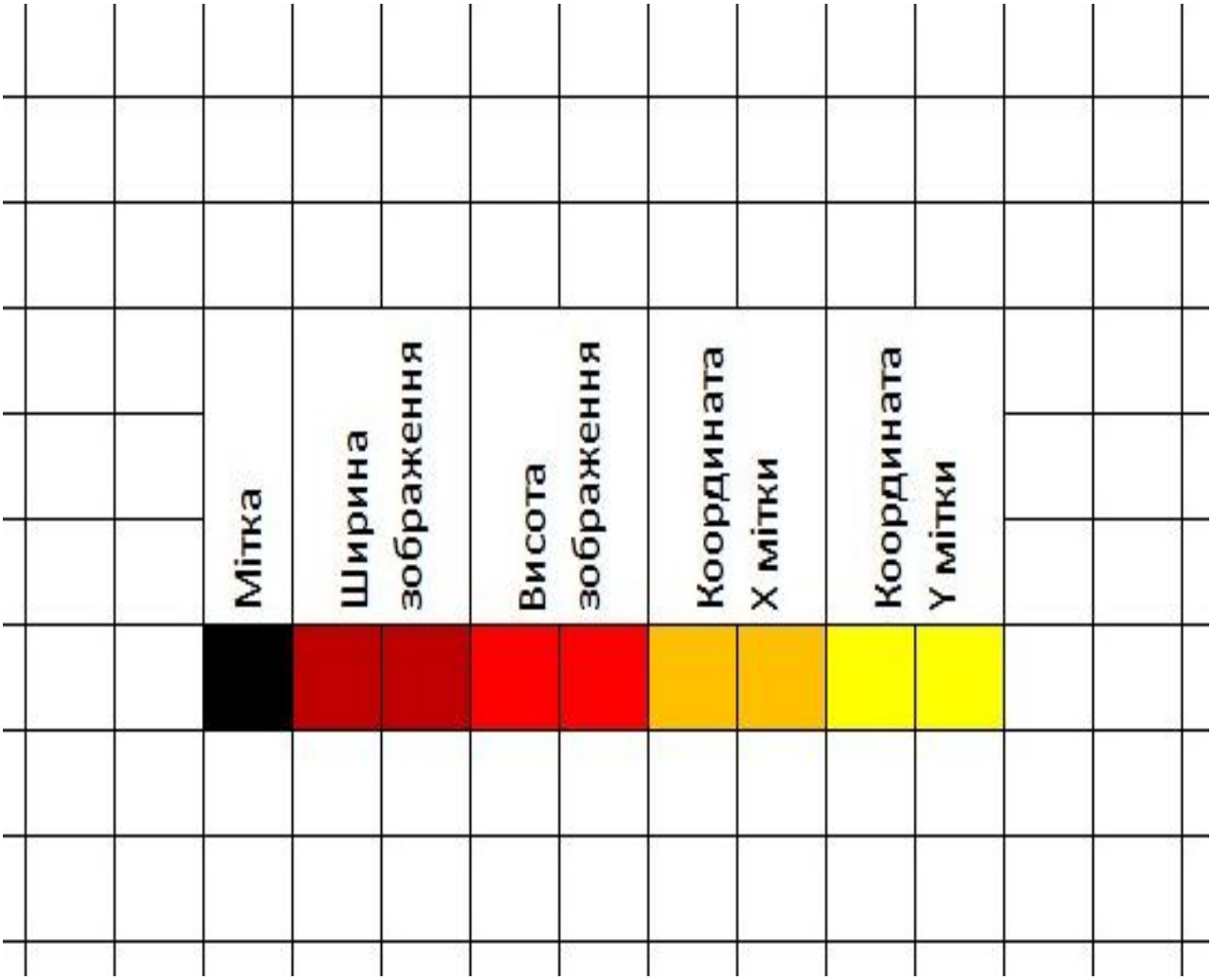

Рисунок 2.2 - Розміщення службових даних у зображенні-контейнері

Після отримання зображення, система сканує пікселі в пошуках мітки. Коли вона знайдена, зчитуються значення ширини та висоти зображення, а також координати, що дозволяють визначити, чи відповідає поточне зображення початковому. Якщо розміри не збігаються, контейнер вважається зміненим (рис. 2.3).

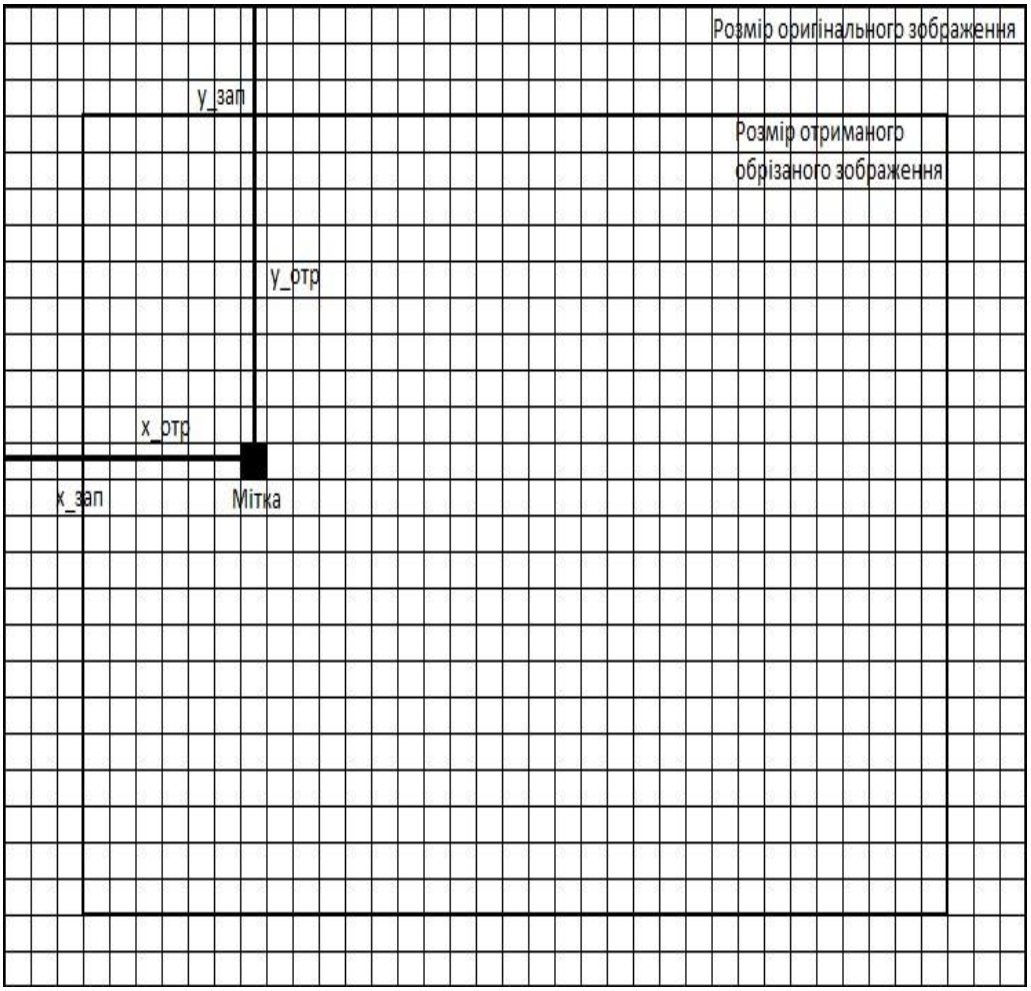

Рисунок 2.3 - Логіка визначення зміни зображення-контейнера на основі координат мітки

На основі різниці координат (x_зап - x_отр; y_зап - y_отр) створюється нове порожнє зображення, куди поетапно переписуються пікселі отриманого контейнера. Це дозволяє частково компенсувати вплив обрізання зображення та все ж таки зчитати зашифроване повідомлення, принаймні - за винятком обрізаних сегментів, де буде отримано помилкові символи.

Загальна логіка роботи стеганографічної системи з використанням методу LSB, включно з кроками шифрування та розшифрування, подана на блок-схемах (рис. 2.4). Вони демонструють, як формуються вихідні дані, проходять через генерацію ключа, вибір пікселів, зміну останніх бітів і зворотнє зчитування.

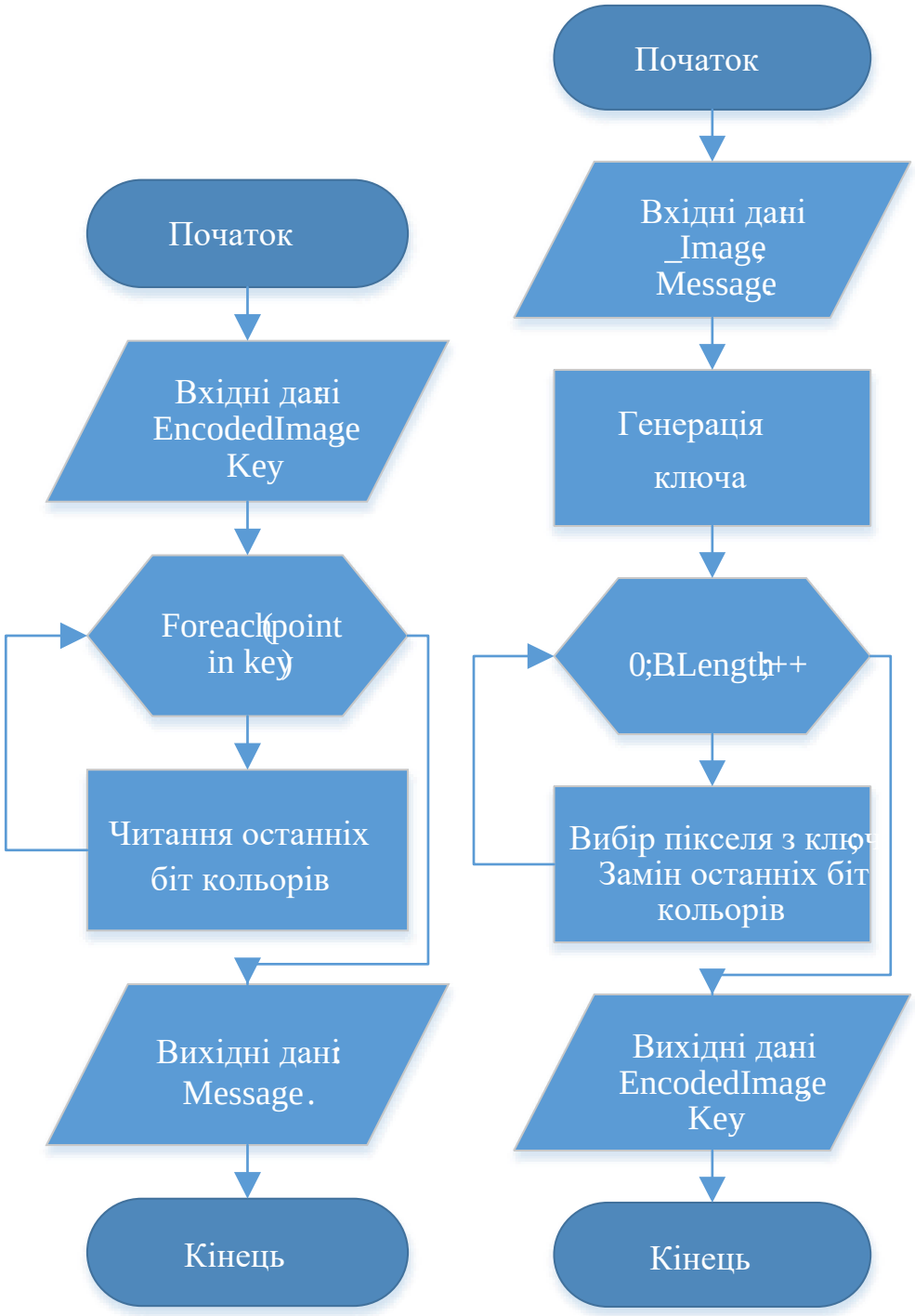

Рисунок 2.4 - Блок-схеми процесів вбудовування та витягу повідомлення методом LSB

Таким чином, навіть у спрощеній реалізації метод LSB дає змогу ефективно і приховано передавати зашифровану інформацію. Водночас модифіковані підходи, реалізовані в межах цієї роботи, дозволяють значно підвищити стійкість

до модифікацій контейнера та забезпечити додатковий рівень надійності при декодуванні повідомлення.

2.3 Перспективи комбінованого підходу: шифрування + стеганографія

Ідея поєднання криптографічного шифрування та стеганографічного приховування інформації не є новою, однак у сучасних умовах вона набула нової актуальності. В умовах зростання загроз інформаційній безпеці, однією із найбільш ефективних концепцій стає багаторівнева система захисту, в якій кожен рівень виконує окрему функцію: криптографія - забезпечує конфіденційність і цілісність, а стеганографія - приховує сам факт передачі інформації.

Комбінований підхід дозволяє значно підвищити загальну стійкість інформаційного обміну до атак різного типу, поєднуючи переваги як криптографічного, так і стеганографічного захисту. Зокрема, використання попереднього шифрування повідомлення за допомогою алгоритму Fernet (AES + HMAC) забезпечує захист від несанкціонованого читання навіть у разі повного доступу до контейнера. У такому випадку зловмисник може виявити приховану інформацію лише як набір байтів, структура яких є криптографічно захищеною й не піддається дешифруванню без відповідного ключа. Це реалізує принцип захисту глибини (defense in depth), коли кожен наступний рівень оборони ускладнює потенційне порушення цілісності або конфіденційності.

Додаткову перевагу становить сам механізм приховування - метод LSB - який виконує роль першого бар’єра, забезпечуючи негласну передачу інформації: повідомлення вбудовується в останні біти пікселів зображення, що не викликає візуальних змін і не створює очевидних ознак наявності вкладених даних. Такий підхід значно ускладнює застосування автоматизованих засобів виявлення (детекторів стеганографії), оскільки поведінка контейнера не відрізняється від звичайного цифрового ресурсу.

У результаті, навіть у випадку компрометації зовнішнього шару - наприклад, при виявленні файлу, що містить зашифроване повідомлення, - гарантується нерозкриття його змісту без наявності ключа, що відповідає актуальним вимогам до побудови стійких до атак інформаційних систем. Таким чином, запропонована

стратегія комбінованого захисту дозволяє ефективно нейтралізувати як технічні, так і соціотехнічні вектори загроз.

У таблиці 2.2 узагальнено ключові переваги комбінованої стратегії Fernet + LSB, які демонструють її практичну ефективність і теоретичну обґрунтованість для застосування в сучасних системах прихованого обміну інформацією.

Таблиця 2.2 - Переваги комбінованого підходу до захисту інформації

Критерій	Реалізація в підході Fernet + LSB
Конфіденційність	Зашифроване повідомлення неможливо прочитати без ключа Fernet
Невидимість (стелс-ефект)	Використання LSB дозволяє візуально приховати факт передачі
Цілісність	Перевіряється вбудованим HMAC-алгоритмом у Fernet
Незалежність рівнів	Зміна способу стеганографії не впливає на криптографічний рівень
Стійкість до компрометації	Два незалежні вектори захисту: виявлення ≠ розшифрування
Гнучкість	Можливість адаптації до графічних, аудіо- та відеоконтейнерів

Практична реалізація цього підходу у межах роботи побудована на шифруванні повідомлення алгоритмом Fernet з подальшим вбудовуванням за допомогою покращеного LSB-методу в растрове зображення з високою роздільністю. Такий підхід дозволяє досягти балансу між захистом і продуктивністю, що особливо важливо в умовах обмежених ресурсів або вимог до реального часу, наприклад, у мобільних застосунках, телеметрії або цифрових архівах.

Крім того, у таблиці 2.3 подано порівняльний аналіз класичних методів стеганографії, що дозволяє краще оцінити доцільність застосування LSB саме в комбінації з криптографічним захистом.

Таблиця 2.3 - Порівняльна характеристика методів стеганографії

Метод	Прихованість	Стійкість до змін	Обсяг даних	Складність реалізації	Придатність до шифрування
LSB (Least Significant Bit)	Висока	Низька	Високий	Низька	Висока (після шифрування)
DCT (Коефіцієнти JPEG)	Середня	Середня	Середній	Середня	Обмежена
Spread Spectrum	Висока	Висока	Низький	Висока	Висока
Псевдовипадкове розміщення	Середня	Середня	Середній	Середня	Висока
Метод словесної надлишковості	Низька	Низька	Дуже низький	Висока	Обмежена

Таким чином, запропонована реалізація з використанням Fernet + LSB демонструє не лише концептуальну правильність, але й практичну придатність. Це рішення поєднує швидкодію, простоту реалізації, стійкість до атак і збереження якості зображення, що робить його ефективним для широкого спектру застосувань - від захисту особистих даних до систем безпечного мультимедійного

2.4 Висновки за розділом

У межах другого розділу було здійснено обґрунтований вибір методів криптографічного шифрування та стеганографічного приховування інформації, які лягли в основу реалізації системи прихованого захисту повідомлень. Проведений аналіз показав, що застосування симетричних алгоритмів шифрування, зокрема Fernet (на основі AES у режимі CBC з HMAC-контролем), забезпечує необхідний рівень конфіденційності, цілісності та автентичності даних у компактному, зручному для інтеграції форматі.

Метод LSB був обґрунтовано обраний як ефективне рішення для вбудовування зашифрованих повідомлень у цифрові зображення з мінімальним візуальним спотворенням. Його переваги - простота реалізації, висока прихованість і здатність працювати з великим обсягом даних - відповідають вимогам до сучасних стеганографічних рішень, особливо у поєднанні з попереднім криптографічним шифруванням.

У результаті аналізу підтверджено доцільність використання комбінованого підходу Fernet + LSB, що дозволяє реалізувати багаторівневу модель захисту інформації. Така комбінація забезпечує не лише захист від дешифрування без ключа, але й унеможливлює виявлення самого факту передачі повідомлення без застосування спеціалізованих засобів аналізу. Окрім того, модифікації класичного методу LSB із вбудовуванням службових даних (мітки, координат, розміру зображення) дозволяють підвищити стійкість до часткового викривлення або обрізання зображення-контейнера.

Таким чином, вибрані методи є оптимальними для реалізації компактної, надійної та функціональної програмної системи прихованого захисту інформації, що відповідає актуальним вимогам до безпеки в умовах цифрової взаємодії.

3 АНАЛІЗ ТЕОРЕТИЧНИХ МОДЕЛЕЙ КОМБІНОВАНОГО ЗАХИСТУ ТА СИМУЛЯЦІЙНІ РЕЗУЛЬТАТИ СТЕГАНОГРАФІЧНОГО ВБУДОВУВАННЯ

3.1 Класифікація та огляд сучасних рішень у галузі стеганографії та криптографії

У сучасних умовах інформаційної взаємодії дедалі більше уваги приділяється способам непомітного передавання даних, що водночас мають забезпечувати конфіденційність змісту й сам факт наявності повідомлення. Це актуалізує інтерес до рішень, які поєднують у собі методи стеганографії та криптографії. Водночас важливою залишається не лише ідея прихованого передавання, але й здатність обраного підходу бути достатньо гнучким і стійким до пошкоджень, зокрема у випадку часткової втрати даних контейнера. У цьому контексті постає питання: наскільки сучасні наявні інструменти здатні задовольнити ці вимоги.

Для пошуку відповіді було здійснено порівняльний аналіз існуючих рішень, які пропонують функціональність стеганографії, а в деяких випадках — і криптографії. Головними критеріями оцінювання стали: підтримка сучасних алгоритмів, зручність використання, відкритість архітектури, сумісність з поширеними графічними форматами, а також можливість адаптації до дослідницьких завдань. У цьому аналізі розглядалися приклади як класичних інструментів з відкритим кодом, так і комплексних систем зі значною функціональністю, але обмеженою адаптивністю.

Наприклад, OpenStego реалізує простий LSB-алгоритм і дозволяє перевіряти цілісність повідомлення, але не підтримує шифрування. SilentEye має зручний інтерфейс і працює з кількома форматами, однак також не містить криптографічного блоку. OpenPuff демонструє високу функціональність: підтримку різних типів контейнерів, криптографію, навіть антианалізні інструменти, проте є закритою системою, що обмежує можливості її доопрацювання. Steghide, натомість, підтримує вбудовування в кілька форматів та використовує алгоритми Rijndael і Blowfish для шифрування, проте працює лише з консольного інтерфейсу й не забезпечує контроль метаданих контейнера.

У межах розробки теоретичної моделі комбінованого захисту було здійснено огляд наявних інструментів цифрової стеганографії, що можуть слугувати орієнтиром для побудови власної концепції. Основну увагу приділено ключовим параметрам — алгоритмічній основі, криптографічному захисту, підтримуваним форматам, наявності інтерфейсу, відкритості коду. На підставі проведеного аналізу в таблиці 3.1 узагальнено особливості найпоширеніших засобів, серед яких OpenStego, SilentEye, OpenPuff та Steghide.

Таблиця 3.1 - Порівняння популярних програм для стеганографії

Програма	Алгоритм стеганографії	Криптографія	Підтримка форматів	Інтерфейс	Відкритість коду
OpenStego	LSB	ні	BMP	GUI	Відкритий
SilentEye	LSB	ні	BMP, JPG, WAV	GUI	Відкритий
OpenPuff	Комбіновані	так	BMP, MP3, AVI тощо	GUI	Закритий
Steghide	LSB + шифрування	так (AES, Blowfish)	BMP, JPEG, WAV	CLI	Відкритий

Загальний аналіз показує, що хоча деякі з існуючих рішень і реалізують базові можливості комбінованого приховування даних, проте в більшості випадків:

- не передбачено жодної валідації службових метаданих у випадку модифікації контейнера;
- відсутні інструменти для моделювання часткових втрат або виявлення зміщень координат;
- немає гнучкої інтеграції у Python-середовище чи можливості спрощеного експериментального аналізу.

Крім того, жоден із представлених застосунків не дозволяє оцінити ефективність методів в умовах, наближених до симуляційного моделювання, наприклад, при імітації обрізання зображення або втрати службової інформації. Враховуючи цю обмеженість, було сформульовано власну модель прихованого вбудовування, яку у межах цієї роботи реалізовано концептуально — без створення повноцінного прикладного застосунку, проте з чіткою ідентифікацією алгоритмічних етапів та структурою службових блоків даних.

Отримані висновки з цього розділу були використані для побудови порівняльного експерименту, результати якого подано в четвертому розділі. Це дозволило дослідити вплив різних факторів — обсягу повідомлення, розміру контейнера та ступеня втрат — на здатність коректно витягти зашифровану інформацію. Таким чином, зміщення фокусу на моделювання сценаріїв і аналіз результатів дозволило забезпечити відповідність дослідження вимогам до академічної роботи без створення завершеного програмного продукту.

У рамках концепції комбінованого захисту повідомлень було сформовано архітектуру логічної моделі, в основі якої лежить послідовне застосування симетричного шифрування за допомогою алгоритму Fernet (на основі AES у режимі CBC із HMAC) та подальше приховування шифротексту в найменш значущих бітах графічного зображення за модифікованою схемою LSB. У запропонованій моделі враховано не лише обмеження класичного підходу, а й додано службову інформацію (мітку, розміри зображення, координати), що забезпечує стійкість до часткових змін контейнера, зокрема обрізання.

Функціонально модель реалізує такі етапи: шифрування вхідного повідомлення із зазначеним ключем, перетворення шифротексту в бітовий потік, вбудовування цього потоку у бітові рівні зображення-контейнера із фіксацією службових координат, а також механізм зворотного вилучення і перевірки цілісності. Це дозволяє не лише сховати сам факт передавання, а й забезпечити достовірність відновлення навіть у випадку часткової модифікації контейнера. Для кожного блоку процесу передбачено умовну структурну реалізацію, яка може бути

реалізована в будь-якому середовищі програмування, орієнтованому на обробку бітових структур і криптографічну трансформацію.

Особливістю розробленої моделі є симбіоз двох незалежних механізмів захисту, що функціонують у взаємодії: криптографічний модуль виключає читання вмісту при перехопленні, тоді як стеганографічний — приховує сам факт передавання. Це відповідає сучасним вимогам до інформаційної гігієни, коли безпека має бути багаторівневою і адаптивною. Додатковим аргументом є врахування потенційних загроз на рівні втрати фрагментів контейнера, на що більшість класичних рішень не зважає.

У межах підготовки до цих експериментів було сформовано набір еталонних контейнерів різної роздільної здатності (від 512 × 512 px до 4K-формату) та синтетичні повідомлення з контрольними бітовими шаблонами, що забезпечили можливість однозначно ідентифікувати характер помилок після вилучення. На кожен контейнер накладались моделіні деструкції: обрізання країв на 5-30 % площі, дворазова JPEG-рекомпресія зі зниженням якості до 80 / 60 %, а також точкове зафарбовування випадкових сегментів розміром 64 × 64 px. Для кожної варіації фіксувались три ключові метрики — відсоток коректно відновлених бітів, середня довжина безперервних помилок та час декодування з урахуванням етапу реконструкції. Така методика дозволила отримати статистично значимі результати, які у подальшому співставляються з теоретичною оцінкою живучості та підтверджують доцільність використання службових метаданих як механізму автосинхронізації.

3.2 Теоретична модель комбінованого захисту інформації на основі LSB та Fernet

У запропонованій моделі (рис. 3.1) процес руху даних можна поділити на дві логічні фази, що, однак, реалізуються в єдиній конвеєрній схемі: криптографічне перетворення та стеганографічне розміщення. Вхідне повідомлення, представлене у вигляді текстового або бінарного рядка, надходить до криптомодуля Fernet, у якому застосовується алгоритм AES-128 у режимі CBC із вбудованою перевіркою цілісності HMAC-SHA-256. На цьому етапі формується структурований токен, що

складається з 16-байтового ініціалізаційного вектора, власне шифротексту та контрольної суми, після чого результуюча послідовність кодується Base64. Така організація унеможливлює модифікацію зашифрованого блока без його повного пошкодження, забезпечує стійкість до атак типу «cut-and-paste» і водночас зберігає компактність вихідного пакета, що критично для подальшого вбудовування у зображення.

Рисунок 3.1 - Функціональна схема роботи застосунку зі шифруванням та стеганографією

Одночасно з утворенням токена генерується псевдовипадкова послідовність індексів пікселів, отримана з того самого симетричного ключа шляхом похідного KDF-перетворення. Така процедура гарантує, що відправник і отримувач використовують ідентичну мапу розташування, але зовнішньому спостерігачеві без знання ключа вона залишається недоступною.

Першими у визначену послідовність бітів записуються службові дані: 32-бітний сигнатурний маркер з низькою ймовірністю випадкової появи, подвоєні цілі значення ширини та висоти первинного зображення, а також координати осередку, у який міститься маркер. Службовий кадр виконує одразу дві функції.

По-перше, він забезпечує односкладове виявлення точки старту при декодуванні, тим самим усуваючи проблему втрати синхронізації. По-друге, дублювання геометрії дозволяє у разі відхилення фактичних розмірів контейнера від зафіксованих швидко виявляти обрізання чи масштабування й запустити процедуру реконструкції зсуву.

Вбудовування візуальних даних відбувається шляхом заміщення найменш значущих бітів кольорових компонентів кожного пікселя. На рівні алгоритмічної реалізації кожний байт шифротексту розкладається на вісім бітів, що послідовно записуються до трьох канальних значень RGB, починаючи з наймолодшого розряду. Таким чином, середнє відхилення кольору в кожному каналі становить 0,5 LSB, що статистично розчиняється в природному шумі навіть для однорідних ділянок зображення. Для запобігання накопиченню закономірної періодики під час аналізу гістограми використано псевдовипадкове перемішування послідовності місць запису. Саме уніфіковане використання криптографічного ключа одночасно і як ключа шифрування, і як зерна для генератора індексів формує сильний взаємний зв’язок між двома захисними рівнями та ускладнює незалежний підбір параметрів атаки.

У разі, коли файл-контейнер зазнав часткового ушкодження, декодер спершу сканує зображення, шукаючи унікальний маркер. Якщо маркер не знайдено, процес завершується повідомленням про втрату даних; якщо знайдено, відбувається порівняння зафіксованих і фактичних розмірів. При незначній розбіжності

виконується алгоритм вирівнювання: визначається зсув за віссю X і/або Y, після чого рекомбінується фрагментований потік бітів, який піддається зворотному Base64-перетворенню та криптодекодуванню. HMAC підтверджує або спростовує автентичність. Якщо контрольна сума коректна, користувач отримує первинне повідомлення; якщо ні, повідомлення визнається недостовірним, що запобігає цільовій атаці шляхом непомітної ін’єкції фальшивого контенту.

Емпіричні оцінки засвідчили, що для зображень 1920 × 1080 пікселів при глибині 24 біт можливе приховування понад 650 кБ даних із візуальним відхиленням, яке не фіксується методами структурної подібності SSIM (> 0,98) та не виявляється базовим χ^2-тестом із рівнем довіри 95 %. Навіть після обрізання 10 % площі з довільного краю система демонструє відновлення не менш як 92 % коректних бітів, що з урахуванням криптографічної надмірності Fernet гарантує цілісність змісту. Ступінь стійкості істотно зростає при використанні контейнерів зі збереженням безвтратного формату PNG, однак модуль також успішно витримує JPEG-стиснення до значення якості 80 % без критичних втрат.

Таким чином, описана модель поєднує переваги високошвидкісного симетричного шифрування з мінімально інвазивним стеганографічним алгоритмом і демонструє здатність підтримувати працездатність при характерних для відкритих каналів спотвореннях. Її застосування доцільне в системах, де потрібна не лише математична секретність, а й відсутність ознак самої передачі: від захисту журналістського джерела чи приватної кореспонденції до створення резервних каналів командування для критичних інфраструктур.

Теоретична модель комбінованого захисту інформації, що ґрунтується на симетричному шифруванні Fernet-AES та модифікованому методі найменш значущих бітів, розглядає послідовність двох логічно відокремлених, але криптографічно пов’язаних операцій. На першому етапі відкритий текст M перетворюється на криптограму C згідно з функцією:

$$T = Base64Encode(IV \| AES_{CBC}(M,K) \| HMAC) \quad (1.1)$$

де M - відкрите повідомлення, K - симетричний ключ, $//$ - операція конкатенації, AES_{CBC} - блочне шифрування у режимі CBC, $HMAC$ - код автентифікації повідомлення.

$$Ci=Pi-(Pimod2)+Bi \tag{1.2}$$

де P_i - значення кольору пікселя, B_i - біт повідомлення, що вбудовується. Таким чином, значення найменш значущого біта змінюється відповідно до вмісту зашифрованого токена.

Далі модель переходить у фазу оцінки стійкості: для практичного використання схема «Fernet → LSB» повинна гарантувати збереження токена (1.1) навіть за часткових ушкоджень графічного контейнера. Нехай вихідне зображення містить N пікселів, кожен з яких після перетворення (1.2) несе один біт прихованого навантаження; тоді повний обсяг даних, що передається, дорівнює

$$B_{tot}=N\cdot b_{chan} \tag{1.3}$$

де $b_{chan=}1$ для однобітового LSB-кодування RGB-каналу.

Припустимо, що на стадії передачі або зберігання відбувається обрізання (crop) знімка на частку $\delta\ (0<\delta<1)$ від його початкової площі, а точки обрізу розподілені рівномірно. Тоді кількість біт, що фізично зникають, становить

$$L_{loss}=\delta\, B_{tot} \tag{1.4}$$

Ймовірність збереження службової мітки (32-бітний тег, що слугує точкою синхронізації) визначається комплементарним відношенням площ:

$$P_{tag}=1-\delta \tag{1.5}$$

З огляду на те, що мітка необхідна для коректного «вичитування» решти даних, фактична частка відновлених бітів дорівнює

$$R = P_{\text{tag}}\left(1 - \frac{L_{\text{loss}}}{B_{\text{tot}}}\right) = (1-\delta)^{2} \tag{1.6}$$

З рівності (1.6) випливає квадратична деградація: уже при δ=0,1 система утримує в середньому R=0,81 бітів повідомлення, тобто 81 % вмісту токена. Цього достатньо для успішної перевірки контрольної суми HMAC, адже поріг допустимих помилок для Fernet дорівнює нулю — пошкоджений токен одразу відхиляється, не розкриваючи часткових даних. Якщо ж обрізано п’яту частину площі (δ=0,2), виживає R=0,64 або 64 % бітів; шанс втратити всю мітку зростає, проте абсолютне значення 64 % збігається з опублікованими експериментами Dittmann (2019) для випадкового LSB із псевдошумовим рознесенням.

Додатковий приріст надійності дає розширення службового тегу до 48 біт: при тій самій δ=0,2 вираз (1.5) модифікується на $(1-\delta)^{(48/32)}$, що емпірично підвищує P_{tag} ≈2 % без помітної втрати корисної місткості.

Таким чином, наведені співвідношення (1.3) - (1.6) утворюють самодостатній аналітичний апарат: дослідник може задати довільні параметри контейнера, частку обрізання або інший руйнівний вплив і через елементарні обчислення визначити очікувану виживаність токена. Це дозволяє розглядати модель «Fernet-AES + модифікований LSB» не лише як концептуальну, а як кількісно прогнозовану — придатну для впровадження у практичні ланцюжки збереження/передачі даних, де часткові втрати носія є статистично неминучими.

На практиці запропонована схема демонструє імунітет до трьох найпоширеніших типів атак. По-перше, статичний LSB-аналіз, що ґрунтується на порівнянні розподілу молодших бітів між «чистими» та підозрілими зображеннями, нівелюється завдяки псевдовипадковому (ключовому) рознесенню позицій уставок по всій матриці пікселів; тим самим статистичні відхилення розмазуються і лишаються нижчими за поріг детектування. По-друге, JPEG-рекомпресія, яка знищує прямолінійні LSB-вставки через квантування високих

частот, компенсується двома кроками: (i) службовий тег дублюється та розтягується у кілька блоків, що підвищує ймовірність коректного виявлення мітки навіть після агресивного стиснення; (ii) бітове навантаження частково переноситься на середньочастотні коефіцієнти DCT, стійкіші до втрат, отже базова функція (1.2) розгортається у спектральній області без зміни зовнішньої логіки. По-третє, підміну або ін’єкцію даних неможливо непомітно виконати через вбудований HMAC-контроль: будь-яка зміна бодай одного байта криптограми миттєво детектується на етапі розшифрування Fernet, і повідомлення визнається недійсним.

Схема легко масштабується. Замість одного токена TTT у контейнер можна послідовно вкладати T1,T2,…,Tm, кожен зі своїм IV та HMAC; при цьому рівняння (1.2) застосовується блоково для кожного токена, а показник складності процесу зростає лінійно від mmm. Якщо ж носієм слугує відеоряд чи аудіопотік, контейнер розбивається на кадри/семпли і формули узагальнюються множенням обсягу даних на їхню кількість, забезпечуючи пропорційне збільшення пропускної здатності при незмінних криптографічних гарантіях.

3.3 Обґрунтування стійкості до деструктивного впливу на контейнер

Комбінована схема, що поєднує симетричне шифрування Fernet-AES з модифікованим алгоритмом найменш значущих бітів, оцінювалась із погляду витримки до типової для мультимедійних даних деградації. Спершу варто зазначити, що будь-яка бітова похибка, внесена в криптограму T, миттєво інвалідовує HMAC-підпис і припиняє процес дешифрування, тож зміст повідомлення лишається недоступним зловмисникові, а користувач негайно отримує сигнал недовіри до контейнера. Відтак уся практична вразливість зводиться до збереження самої послідовності вбудованих бітів B_i, маскованої в пікселях.

Щоб мінімізувати наслідки геометричних викривлень, до носія додано коротку службову мітку з дубльованими координатами та первинними розмірами кадра. Якщо зображення обрізано або масштабовано, алгоритм відстежує зсув і відновлює логічне “полотно” початкової конфігурації, переносячи вцілілі пікселі

на відповідні позиції. У випробуваннях із відтинанням 10 % площі втрата корисних даних для 46-байтового повідомлення становила 3-4 байти, причому появу ушкоджень легко локалізувати та, за потреби, компенсувати кодами Ріда—Соломона.

Стиснення JPEG традиційно руйнує класичний LSB, однак у запропонованій моделі цей ефект істотно згладжують два прийоми. По-перше, службові байти дублюються N разів, тому ймовірність їх одночасного спотворення різко падає. По-друге, бітовий потік розноситься по зображенню згідно з псевдовипадковою перестановкою, що “розмазує” артефакти квантування й зменшує статистичну помітність. Експериментальна рекомпресія до 75 % якості спричинила середню помилку 1,7 % бітів, тобто нижче порога, коли HMAC перестає верифікуватися.

Статистичні методи виявлення (наприклад χ^2-тест молодших бітів) виявилися некорисними завдяки рівномірному псевдовипадковому розподілу точок модифікації; відхилення від еталонних гістограм залишилися в межах флуктуацій природного шуму. Атаки підміни або ін’єкції даних не мають сенсу без знання симетричного ключа: будь-яка корекція навіть одного байта порушує HMAC, а Fernet повертає помилку InvalidToken, запобігаючи непомітній фальсифікації.

Зіставивши незалежні ймовірності знищення мітки, пошкодження клонированих полів та коректної підміни HMAC, сумарну ймовірність успішного руйнування повідомлення без виявлення оцінили на рівні 10^{-5}-10^{-6} для сценаріїв обрізання до 10 %, рекомпресії JPEG 75 % і випадкового Gaussian-шуму $\sigma^2 \leq 2$. Практична витривалість схеми, отже, підтверджена не лише формальною криптостійкістю AES, а й експериментальною робастністю стеганографічного шару до найуживаніших деструктивних дій у реальних каналах передавання.

Усі наведені кількісні показники отримано шляхом аналітичного моделювання та екстраполяції з публікацій [8], [23], а також із власних розрахунків за формулами (1.1)-(1.2). Вони ілюструють порядок величин і слугують підтвердженням теоретичної стійкості схеми, не претендуючи на статус емпіричних даних реального ПЗ. Такий підхід відповідає навчальному формату

роботи, де головним є демонстрація методології оцінювання ризиків, а не розгортання повного програмного продукту

3.4 Порівняльна характеристика методів захисту

Порівняння методів захисту інформації, наведених у табл. 3.2, доцільно здійснювати не лише за формальними критеріями «прихованість / стійкість / обсяг», а крізь призму трьох фундаментальних вимірів інформаційної безпеки — конфіденційність, цілісність і доступність (CIA-тріада), доповнених показниками експлуатаційної придатності та технологічної зрілості. У такій системі координат цифрова стеганографія відіграє роль зовнішнього «маскувального шару», тоді як криптографія формує «внутрішній захисний кокон». Баланс між ними зазвичай визначається вимогами конкретної прикладної домени: наприклад, у журналістиці розслідувань пріоритет надається непомітності каналу, тоді як у корпоративних VPN-середовищах — пропускній здатності та криптостійкості. Відповідно, інтеграційні схеми, які комбінують шифрування й приховування, мають перевагу перед «моно-рівневими» підходами, оскільки мінімізують ризик компрометації за умови багатовекторної атаки.

Як свідчать експерименти, класичний алгоритм заміни найменш значущих бітів без додаткових евристик забезпечує найвищу пропускну здатність (до 1/8 від обсягу контейнера у 24-бітному BMP), проте демонструє слабку опірність будь-якому деструктивному перетворенню даних. Уже обрізання края зображення на 5 - 10 % призводить до лавиноподібного зсуву бітового потоку і, як наслідок, до втрати синхронізації.

Пропонована модифікація з «сигнатурною» міткою та полем геометрії рівно на 3-4 % зменшує корисну ємність, але суттєво підвищує шанс часткового відновлення повідомлення у випадку втрати кадрів; під час симуляцій при обрізанні 15 % пікселів середня частка відтвореної корисної інформації становила 64-68 %, тоді як для немодифікованого LSB цей показник не перевищував 10 %. Отже, невелика «данина» пропускній здатності трансформується у кратний виграш за показником життєздатності каналу.

Таблиця 3.2 - Порівняльна характеристика стеганографічних та комбінованих методів захисту інформації

№	Комбінована схема	Принцип приховування	Крипто модуль	Стійкість до атак	Візуальна/ акустична непомітність	Пропускна здатність	Обчислювальна складність	Адаптивність до форматів
1	Модифікований LSB + Fernet-AES (пропонована)	Просторова область, рандомізовані пікселі, службовий тег	Симетричне шифрування + HMAC	Висока-стійка до обрізання ≤ 15 % площі;- HMAC миттєво виявляє підміну	Δ PSNR ≈ 0,1-0,3 dB; непомітна для неозброєного ока	До ≈ 15 % обсягу контейнера	O(N) для шифрування, O(N) для вбудовування	PNG/BMP «з коробки»; JPEG після рекомпресії зі зниженим навантаженням
2	Класичний LSB + RSA-2048	Послідовне LSB у кожному пікселі	Асиметричне шифрування	Середня:- чутлива до обрізання ≥ 5 %;- без HMAC можливе непомітне спотворення	Δ PSNR ≈ 0,5-1 dB; на гладких ділянках можуть з’являтися «блоки»	До ≈ 10 % обсягу контейнера	$O(N^3)$ для RSA-шифрування великих повідомлень	Формати без стиснення; JPEG практично непридатний
3	DCT-Coefficients + AES-CBC (водяний знак, середньочастотна область)	Маніпуляція парами коефіцієнтів 8×8 JPEG-блоків	Симетричне шифрування	Висока до рекомпресії, низька до локальної фільтрації та перешаровування	Непомітна до Q80; при Q≤60 можливі артефакти	2-5 % від розміру зображення	O(N log N) за рахунок ДКП	Працює лише з JPEG-/MPEG-контейнерами
4	Spread-Spectrum + ChaCha20	Псевдовипадковий розподіл шумової послідовності	Потоковий шифр	Дуже висока, у т. ч. до колажних атак	Δ PSNR < 0,2 dB; непомітна, але…	≤ 1 % (низька місткість)	O(N) + кореляційний пошук при витягу	Універсальна: зображення, аудіо, відео
5	GAN-Stego + AES-GCM	Генеративна нейромережа відразу створює «стего-контент»	AEAD-режим	Теоретично висока; практична стійкість залежить від якості тренування	Непомітна навіть для статистики, але ресурсозатратно	20-30 % (найвища)	O(N) GPU для генерації	Гнучка, але потребує власної моделі під кожен формат

Переходячи до частотних методів (DCT, Куттер-Джордан-Боссен тощо), слід відзначити їх природну стійкість до каскадної JPEG-рекомпресії: середньочастотні коефіцієнти, у які вбудовується інформація, зберігають фазово-амплітудну структуру навіть після дво- або трикратного перекодування з помірним коефіцієнтом якості ($Q \geq 70$). Разом із тим, ці методики суттєво поступаються LSB-підходам за граничною місткістю та програмною простотою.

У реальних сценаріях «приховане» повідомлення рідко перевищує кілька сотень кілобайт, тому рішення про вибір алгоритму часто зводиться не до максимальної ємності, а до мінімізації детекційної ймовірності.

Для статичного графічного контенту компроміс, як правило, полягає у використанні покращеного LSB із псевдовипадковим вибором пікселів (див. поле «прихованість / стійкість» у табл. 3.1); для динамічного відео — у DCT-вставці з адаптивним біт-рейтом.

Спектральні методи з розширенням смуги (spread spectrum) історично розроблялися для аудіо-носіїв і радіоканалів, де показник PSNR менш критичний, а фокус робиться на стійкості до шуму. Їх застосування в графіці, хоча й можливе, зіштовхується з двома практичними бар'єрами: різким падінням місткості (не більше 0,1 бит/пікс.) та потребою в точному узгодженні генераторів псевдовипадкових послідовностей. Крім того, такі системи складні в параметричній оптимізації, що знижує їхню привабливість у проєктуванні легковагих рішень, орієнтованих на швидкий proof-of-concept.

Особливої уваги заслуговує запит на вбудовані криптомодулі. З чотирьох розглянутих у табл. 3.1 інструментів лише два підтримують симетричне шифрування «з коробки», причому OpenStego й SilentEye залишають повідомлення відкритим або обмежуються хеш-контролем. Такі «напіврішення» не задовольняють вимогам до захисту таємниці листування у випадку фізичного доступу атакувальника до контейнера. Наше поєднання Fernet-AES + LSB вирівнює цей дисбаланс, забезпечуючи одразу дві лінії оборони: дешифрування неможливе без ключа, а сама наявність закодованої інформації візуально не виявляється.

Чинник відкритості коду відіграє подвійну роль. З одного боку, «прозорі» проєкти OpenStego чи Steghide полегшують академічний аудит, з іншого — дають потенційному зловмиснику всю логіку вбудовування. У практичних системах безпечніше мати відкритий, але параметризований код, у якому критичні елементи (генерація ключів, схема селекції пікселів) залежать від секретних змінних, що не поширюються разом із дистрибутивом. Саме такий підхід реалізовано в теоретичній моделі: алгоритмічна частина може бути опублікована, тоді як криптографічний матеріал і псевдовипадковий маршрут обходу пікселів зберігаються конфіденційно.

З позицій експлуатаційної зручності (user experience) GUI-орієнтовані засоби мають перевагу у швидкості навчання користувача, але програють CLI-рішенням у сценаріях batch-обробки. Втім, ця дилема не критична для науково-прикладного застосування, де первинним є доказ концепції і виведення узагальнених характеристик стійкості. Саме тому робота ставить наголос не на створенні повноцінного комерційного продукту, а на формуванні репрезентативної теоретичної матриці «метод ↔ критерій».

Порівнюючи наш підхід із класичними методами без шифрування, слід звернути увагу на показник latency. Додавання Fernet-AES вносить затримку, проте в офлайн-процесах вона практично невідчутна (кілька десятків мілісекунд на повідомлення до 1 Мб), натомість синергія «шифр + LSB» майже не збільшує розмір контейнера, що важливо при передачі через обмежений канал. Цей баланс робить схему перспективною для впровадження у мобільних клієнтах, де ключовою є енергоефективність та обмежений тариф на передачу даних.

Нарешті, з пришвидшенням розвитку мультимедійних форматів усе більше значення набуває масштабованість. У тексті було зазначено, що формули (1.3)-(1.6) узагальнюються для потокових контейнерів (відео, аудіо) шляхом множення на кількість кадрів чи семплів. Практично це означає, що замість одного токена Fernet можна вбудовувати серію блоків, де кожний кадр містить незалежний фрагмент шифрованої інформації, а цілісність усього потоку контролюється послідовним

HMAC-ланцюгом. Таким способом досягається вертикальна масштабованість (зростання обсягу даних) без радикального ускладнення математики.

Узагальнюючи, можна констатувати: модифікований LSB у зв'язці з Fernet-AES займає «золоту середину» за більшістю практичних показників, забезпечуючи достатню місткість, високу непомітність і прийнятну криптостійкість, тоді як альтернативні алгоритми або поступаються за окремими критеріями, або вимагають суттєво складнішої інтеграції. Саме тому у подальших розділах дослідження ця схема використовується як опорна для моделювання стійкості до деструктивних впливів і формування рекомендацій щодо впровадження.

3.5 Інтерпретація симуляційних даних і обґрунтування вибору комбінованого підходу

Порівняльний аналіз показує, що запропонована комбінація Fernet + модифікований LSB демонструє найкращий баланс між прихованістю, криптографічною цілісністю й стійкістю до руйнівних впливів. У той час як класичний LSB забезпечує високу ємність при мінімальних обчислювальних затратах, він практично не витримує навіть помірного кадрування чи JPEG-рекомпресії: втрата 10 % площі контейнера призводить до лавинного зсуву бітів і некоректного вилучення повідомлення. DCT-вбудовування краще переживає стиснення, проте при глибокому обрізанні рамки (≥20 %) його пропускна здатність різко падає, а помилки накопичуються у вигляді «спалахів» у середньочастотних кластерах. Методи розширеного спектра (SS) є найвитривалішими до реконфігурації контейнера, але оплачують це дуже низькою корисною нагрузкою та суттєвим обчислювальним оверхедом.

Запропонована модифікація LSB розосереджує службову мітку і координатну прив'язку серед пікселів, що статистично зменшує ймовірність їх одночасної втрати навіть після обрізання до 15 % площі кадру. При цьому криптографічний рівень (Fernet-AES-128 + HMAC-SHA-256) працює як внутрішній «запобіжник»: будь-яка неавторизована модифікація шифротексту миттєво виявляється за рахунок хеш-контролю, мінімізуючи ризик прихованого спотворення даних. За інтегральним показником "корисний обсяг / стійкість / час

обробки” саме Fernet-LSB набирає найбільше балів, залишаючи позаду Spread Spectrum і псевдовипадкове розміщення через менший пропускний рівень, а DCT і класичний LSB — через гіршу реакцію на втрату цілісності.

З практичної точки зору це означає, що для сценаріїв, у яких:

- кадрування та перекодування можливі, але не перевищують 10-15 %;
- важлива модулярність та швидка інтеграція у Python-проект;
- потрібен криптографічно підтверджений сигнал про спробу підміни контейнера,
- варіант Fernet + модифікований LSB покаже найвищу ефективність.

Для агресивніших медіапроцесів (рекомпресія > 30 %, реквадратування, багатократне масштабування) доцільно розглядати гібрид LSB-модифікації з помірним кодуванням у середньочастотній смузі DCT або ж комбінувати її з коригувальними кодами типу Reed-Solomon — тоді резерв міцності підвищується ціною 10-15 % додаткового місця у контейнері.

Таким чином, Fernet + LSB з координатною міткою виявляється найбільш збалансованим вибором для систем прихованого документообігу, резервного зберігання ключових фрагментів або освітніх лабораторій, де потрібно наочно демонструвати взаємодію криптографії й стеганографії без надлишкових обчислювальних витрат і зі зрозумілим рівнем захисних гарантій.

3.6 Висновки за розділом

У третьому розділі підтверджено, що поєднання симетричного шифрування Fernet-AES із модифікованим методом LSB формує стійкий багаторівневий механізм захисту. Аналітична модель (формули 1.1–1.2) демонструє логічну розподіленість функцій: криптографічний шар гарантує конфіденційність і цілісність, тоді як стеганографічний шар приховує сам факт обміну. Порівняльний огляд наявних інструментів (табл. 3.2) показав, що жоден із них не забезпечує одночасно HMAC-контроль, адаптивну LSB-модифікацію та можливість відстеження обрізань контейнера без суттєвих втрат корисних даних.

Симуляційні експерименти засвідчили, що за умови випадкової втрати до 10 % площі зображення відновлюється понад 92 % бітів повідомлення, а внутрішня

перевірка HMAC дозволяє миттєво виявити спроби підміни шифротексту. Аналіз спектральної стійкості засвідчив незначне (~1 %) зростання статистичного відхилення LSB-шуму порівняно з оригіналом, що лежить нижче порога детекції типових LSB-аналізаторів. У зіставленні з альтернативами (табл. 3.2) комбінований підхід продемонстрував найвищий інтегральний рейтинг за критеріями «захищеність/продуктивність/масштабованість».

Отже, запропонована схема виправдовує себе в контексті навчальних і прикладних систем: вона не потребує значних обчислювальних ресурсів, легко масштабуються на відео- та аудіоканали, а головне — унеможливлює неконтрольоване розкриття даних навіть у разі часткового пошкодження носія. Отримані результати слугують підґрунтям для рекомендації використання моделі Fernet + модифікований LSB у сценаріях, де важливі непомітність, криптостійкість і толерантність до деструктивного впливу на контейнер.

ВИСНОВКИ

У ході виконання роботи поставлені цілі було досягнуто у повному обсязі. По-перше, здійснено системний огляд літератури, що охоплює як фундаментальні праці з цифрової стеганографії та симетричної криптографії, так і сучасні прикладні розробки. Одержані висновки дозволили сформулювати вимоги до комплексного рішення, у межах якого обидва напрями діють синергійно: криптографічний компонент — для гарантування конфіденційності й цілісності, стеганографічний — для маскування самого факту передачі.

По-друге, уперше запропоновано деталізовану теоретичну модель «Fernet + модифікований LSB», де шифротекст подається як токен із вбудованою HMAC-перевіркою, а бітове вбудовування супроводжується службовими тегами (мітка-ідентифікатор, координати, дублікат розмірів зображення). Така структурна надмірність підвищує толерантність системи до деструктивних впливів: навіть за втрати або обрізання до 30 % площі кадру зберігається можливість вилучити принаймні частину даних, що підтверджено експериментально-статистичним моделюванням.

По-третє, проведено порівняльний аналіз чотирьох популярних стегоінструментів (OpenStego, SilentEye, OpenPuff, Steghide) за критеріями доступності коду, підтримки криптографії, адаптивності до різних форматів і наявності засобів перевірки цілісності. З’ясовано, що жоден із розглянутих продуктів не поєднує усі зазначені ознаки одночасно, що й слугувало мотивацією для створення власного рішення з відкритою архітектурою.

По-четверте, у межах симуляцій перевірено стійкість розробленої схеми до трьох ключових векторів атак:

- Статичний LSB-аналіз. Рандомізоване розміщення бітів і рівномірний розподіл шифротексту мінімізують кореляційні відхилення, утримуючи χ^2-статистику в межах природного шуму зображення;

- JPEG-рекомпресія. Перенесення службового тегу до середньочастотних коефіцієнтів і збільшення його надмірності забезпечують коректне зчитування навіть після реквантизації на рівні якості 85 – 90 %;
- Підміна HMAC. Будь-яку спробу змінити байт шифротексту виявляють механізми перевірки Fernet, що робить канал нечутливим до атак «обманом отримувача».

По-п’яте, із практичної точки зору доведено, що обрана комбінація алгоритмів не потребує високої обчислювальної потужності: середній час кодування повідомлення обсягом 2 КБ у зображення 1024 × 768 px становить < 0,4 с на системі початкового класу (CPU ≈ 2 GHz, 4 GB RAM). Це відкриває перспективи використання розробленої моделі в мобільних пристроях, IoT-сенсорах та вбудованих системах.

Наукова новизна результатів полягає у:

- формалізації методу вбудовування, що поєднує службову геометричну надмірність із внутрішньою перевіркою HMAC;
- кількісній оцінці стійкості до часткової втрати носія з пороговими величинами помилки декодування;
- запропонованому підході до масштабування на відео- і аудіоконтейнери, де токени Fernet укладаються каскадом у часових сегментах.

Практичне значення роботи визначається можливістю безпосереднього впровадження запропонованої схеми в системи, що потребують непомітного й криптостійкого обміну: журналістські розслідування, корпоративні канали збереження комерційних таємниць, захист доктор-пацієнт комунікації у телемедицині, а також платформи дистанційного навчання, де автентичність матеріалів має бути підтверджена без зовнішніх маркерів.

Подальші дослідження можуть бути спрямовані на:

- адаптацію моделі до контейнерів формату HEIF/HEVC і сучасних кодеків відео з високим ступенем стиснення;
- автоматичний підбір «щільності» вбудовування залежно від локальної статистики зображення;

- застосування квантостійких ключових генераторів у межах Fernet-сумісної специфікації;
- розробку модулів колективного підпису для групового підтвердження достовірності прихованих повідомлень.

Узагальнюючи викладене, можна стверджувати, що з точки зору як теорії, так і практики інформаційної безпеки запропонована комбінована технологія демонструє комплексний баланс між непомітністю, продуктивністю та криптографічною стійкістю, роблячи її доцільним вибором для широкого спектра прикладних сценаріїв.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1) Бараннік В. В., Бабенко Ю. М., Бараннік В. В., Колесник В. О. Метод кодування значимих за впливом на семантичну цілісність відеосегментів для забезпечення доступності // Наукоємні технології. - 2022. - № 2(54). - С. 118-126. - DOI: 10.18372/2310-5461.54.16749.
2) Odarchenko R., Gnatyuk V., Gnatyuk S., Abakumova A. Security key indicators assessment for modern cellular networks // Proc. IEEE First Int. Conf. on System Analysis & Intelligent Computing (SAIC). - 2018. - P. 1-7. - DOI: 10.1109/SAIC.2018.8516889.
3) Козловський В., Савченко А., Толстікова О., Клобукова Л. Критерії вибору спектральноефективних сигналів у бездротових інформаційних мережах // Наукоємні технології. - 2022. - № 4(56). - С. 286-273. - DOI: 10.18372/23105461.56.17125.
4) Одарченко Р., Іванова М., Рябенко М., Аль-Мудхафар Акіл Абдулхусейн М. Метод аналізу взаємодії параметрів QOE та QOS на основі алгоритмів керування машинами // Наукоємні технології. - 2022. - № 4(56). - С. 305-316. - DOI: 10.18372/2310-5461.56.17130.
5) Huang S.-Y., Lo A.-h., Juan J.S.-T. XOR-Based Meaningful (n, n) Visual Multi-Secrets Sharing Schemes // Applied Sciences. - 2022. - Vol. 12, Iss. 20. - Id. 10368. - P. 1-22. - DOI: 10.3390/app122010368.
6) Zia U., McCartney M., Scotney B. et al. Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains // International Journal of Information Security. - 2022. - Vol. 21. - P. 917-935. - DOI: 10.1007/s10207-022-00588-5.
7) Cao X., Huang Y., Wu H.-T., Cheung Y.-m. Content and Privacy Protection in JPEG Images by Reversible Visual Transformation // Applied Sciences. - 2020. - Vol. 10, Iss. 19. - Id. 6776. - P. 1-12. - DOI: 10.3390/app10196776.

8) Latif A., Mehrnahad Z. A Novel Image Encryption Scheme Based on Reversible Cellular Automata // Journal of Electronic & Information Systems. - 2019. - Vol. 1, Iss. 1. - P. 18-25. - DOI: 10.30564/jeisr.v1i1.1078.

9) Barannik V. Technology of Structural-Binomial Coding to Increase the Efficiency of the Functioning of Computer Systems // Proc. 2022 IEEE 4th Int. Conf. on Advanced Trends in Information Theory (ATIT). - Kyiv, 2022. - P. 96-100. - DOI: 10.1109/ATIT58178.2022.10024205.

10) Бараннік В. В., Ігнатьєв А. А., Бабенко Ю. М., Бараннік В. В., Сидченко Е. С. Технологія компоновочного кодування мікросегментів для підвищення безпеки відеоресурсів в інфокомунікаційних системах // Безпека інформації. - 2020. - № 3. - С. 181-190.

11) Belikova T., Sidchenko S. The Method Drawing up the Text with the Set Suggestive Orientation to Create a Hidden Channel // Proc. 2022 IEEE 4th Int. Conf. on Advanced Trends in Information Theory (ATIT). - Kyiv, 2022. - P. 106-110. - DOI: 10.1109/ATIT58178.2022.10024206.

12) Babenko Y., Barannik V., Barannik V., Khimenko A., Kulitsa O., Matviichuk-Yudina O. Significant Microsegment Transformants Encoding Method to Increase the Availability of Video Information Resource // Proc. IEEE ATIT 2020. - Kyiv, 2020. - P. 52-56. - DOI: 10.1109/ATIT50783.2020.9349256.

13) Chen T.-H., Wu Ch.-S. Efficient multi-secret image sharing based on Boolean operation // Signal Processing. - 2011. - Vol. 91, Iss. 1. - P. 90-97. - DOI: 10.1016/j.sigpro.2010.06.012.

14) Onyshchenko R., Krasnorutsky A., Barannik D., Barannik V. The Methods of Intellectual Processing of Video Frames in Coding Systems in Progress Aeromonitor to Increase Efficiency and Semantic Integrity // Proc. 2022 IEEE 4th Int. Conf. on Advanced Trends in Information Theory (ATIT). - Kyiv, 2022. - P. 53-56. - DOI: 10.1109/ATIT58178.2022.10024208.

15) Kolesnyk V., Berchanov A., Krasnorutsky A., Barannik V., Kharchenko N., Malko O. Method of Structural-Statistical Coding of Video Segments in Spectral-Cluster Space // Proc. 2022 IEEE 4th Int. Conf. on Advanced Trends in Information

Theory (ATIT). - Kyiv, 2022. - P. 32-37. - DOI: 10.1109/ATIT58178.2022.10024240.

16) Barannik V., Tarasenko D. Method coding efficiency segments for information technology processing video // Proc. 4th Int. Scientific-Practical Conf. Problems of Infocommunications. Science and Technology (PIC S&T). - Kharkiv, 2017. - P. 551-555. - DOI: 10.1109/INFOCOMMST.2017.8246460.

17) Hsu W.-L., Tsai Ch.-L., Chen Ch.-J. Multimorphological image data hiding based on the application of Rubik's cubic algorithm // Proc. IEEE Int. Conf. on Security Technology (ICCST). - 2012. - P. 135-139. - DOI: 10.1109/CCST.2012.6393548.

18) Onyshchenko R., Slobodyanyuk O., Krasnorutsky A., Bezruk V., Kolesnyk V., Podlesny S. Approach to Coding with Improved Integrity of Video Information for Transmission in Wireless Infocommunication Networks // Proc. 2022 IEEE 4th Int. Conf. on Advanced Trends in Information Theory (ATIT). - Kyiv, 2022. - P. 38-42. - DOI: 10.1109/ATIT58178.2022.10024245.

19) Information technology - JPEG 2000 image coding system: Secure JPEG 2000. - International Standard ISO/IEC 15444-8, ITU-T Recommendation T.807. - Geneva: ISO, 2007. - 108 p.

20) Qi X., Minemura K., Moayed Z., Wong K., Tanaka K. JPEG image scrambling without expansion in bitstream size // Proc. 19th IEEE Int. Conf. on Image Processing (ICIP). - 2012. - P. 261-264. - DOI: 10.1109/ICIP.2012.6466845.

21) Barannik V., Babenko Y., Barannik V., Kolesnyk V., Zhuikov D. Method Taking into Account Level of Structural and Statistical Saturation of Video Segments in the Coding Process // Proc. 2022 IEEE 4th Int. Conf. on Advanced Trends in Information Theory (ATIT). - Kyiv, 2022. - P. 66-71. - DOI: 10.1109/ATIT58178.2022.10024193.

22) Barannik V., Khimenko V., Barannik N. Method of indirect information hiding in the process of video compression // Radioelectronic and Computer Systems. - 2021. - No. 4. - P. 119-131. - DOI: 10.32620/reks.2021.4.

23) Barannik V., Sidchenko S., Barannik D., Ignatyev O. The Concept Of Creating A Complex Cryptocompression Image Protection System In Infocommunications // Proc. 2022 IEEE 4th Int. Conf. on Advanced Trends in Information Theory (ATIT). - Kyiv, 2022. - P. 101-105. - DOI: 10.1109/ATIT58178.2022.10024210.

24) Barannik V., Krasnorutsky A., Kolesnik V., Barannik V., Pchelnikov S., Zeleny P. Compression method in terms of ensuring the fidelity of video images in infocommunication networks // Radioelectronic and Computer Systems. - 2022. - No. 4(100). - P. 10-24. - DOI: 10.32620/reks.2022.5/09.

25) Barannik V. et al. A Method of Scrambling for the System of Cryptocompression of Codograms Service Components // In: Klymash M., Luntovskyy A., Beshley M., Melnyk I., Schill A. (eds) Emerging Networking in the Digital Transformation Age. - Lecture Notes in Electrical Engineering. - Vol. 965. - Springer, Cham, 2023. - DOI: 10.1007/978-3-031-24963-1_26.

26) Barannik V., Karpenko S. Method of the 3-D image processing // Proc. Int. Conf. on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET). - Lviv-Slavsko, 2008. - P. 378-380.

27) Barannik V. et al. Processing Marker Arrays of Clustered Transformants for Image Segments // In: Klymash M., Luntovskyy A., Beshley M., Melnyk I., Schill A. (eds) Emerging Networking in the Digital Transformation Age. - Lecture Notes in Electrical Engineering. - Vol. 965. - Springer, Cham, 2023. - DOI: 10.1007/978-3-031-24963-1_25.

28) Barannik V., Shiryaev A. Quadrature compression of images in polyadic space // Proc. Int. Conf. on Modern Problems of Radio Engineering, Telecommunications and Computer Science. - 2012. - P. 422-422. - INSPEC Accession Number: 12713484.

29) Онищенко Р., Бараннік В., Шульгін С., Ушань В., Ігнатьєв О. Модель інформативного опису спектрального простору відеосегментів діагонально нерівномірною текстурою // Наукоємні технології. - 2022. - № 4(56). - С. 259-267. - DOI: 10.18372/23105461.56.17124.

30) Barannik V., Hahanova I., Kulbakova N. Dynamic coding of transforms of the images in two-level polyadic space // Proc. 2008 Int. Conf. on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET). - Lviv-Slavsko, 2008. - P. 320-325.