ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Розробка комбінованого методу шифрування та стеганографічного приховування повідомлень»

на здобуття освітнього ступеня магістра
зі спеціальності 121 Інженерія програмного забезпечення
освітньо-професійної програми «Інженерія програмного забезпечення»

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Владислав МЕЛЬНИК
(підпис)

Виконав: здобувач вищої освіти групи ПДМ-61
Владислав МЕЛЬНИК

Керівник: Наталія ТРІНТІНА
канд. техн. наук, доц.

Рецензент: _____
науковий ступінь, вчене звання *Ім'я, ПРІЗВИЩЕ*

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Інженерії програмного забезпечення

Ступінь вищої освіти Магістр

Спеціальність 121 Інженерія програмного забезпечення

Освітньо-професійна програма «Інженерія програмного забезпечення»

ЗАТВЕРДЖУЮ
Завідувач кафедри
Інженерії програмного забезпечення
_____ Ірина ЗАМРІЙ
«_____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Мельник Владислав Вікторович

1. Тема кваліфікаційної роботи: «Розробка комбінованого методу шифрування та стеганографічного приховування повідомлень»

керівник кваліфікаційної роботи Наталія ТРІНТІНА, канд. техн. наук, доц.

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. № 467.

2. Строк подання кваліфікаційної роботи «19» грудня 2025 р.

3. Вихідні дані до кваліфікаційної роботи: науково-технічна література, огляд сучасних алгоритмів симетричного та асиметричного шифрування, аналіз методів стеганографії для різних типів контейнерів, вимоги до стійкості шифрування та точності стеганографічного приховування.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Дослідження та порівняльний аналіз існуючих методів шифрування та стеганографічного приховування повідомлень.
2. Аналіз підходів до комбінування шифрування та стеганографії для підвищення безпеки та прихованості передачі даних.
3. Розробка комбінованого методу шифрування та стеганографічного приховування повідомлень та оцінка його ефективності.

5. Перелік ілюстративного матеріалу: *презентація*

1. Мета, об’єкта та предмет дослідження.
2. Актуальність роботи
3. Математична модель комбінованого методу
4. Блок-схема шифрування повідомлення К методом
5. Блок-схема дешифрування повідомлення К методу
6. Екранні форми
7. Порівняльний аналіз К методу та існуючих
8. Висновки.
9. Публікації та апробація роботи.

6. Дата видачі завдання «31» жовтня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз наявної науково-технічної літератури	*31.10-05.11.25*	
2	Вивчення матеріалів для аналізу сучасних методів шифрування (симетричне, асиметричне)	*06.11-12.11.25*	
3	Дослідження класичних та сучасних методів стеганографії (включаючи LSB, DCT, DWT)	*13.11-19.11.25*	
4	Аналіз особливостей комбінування методів шифрування та стеганографії для забезпечення конфіденційності та прихованості	*20.11-26.11.25*	

5	Дослідження вимог до стійкості, ємності та непомітності розроблюваного методу	*27.11-03.12.25*	
6	Розробка та практична реалізація комбінованого методу шифрування та стеганографічного приховування повідомлень	*04.12-10.12.25*	
7	Оформлення роботи: вступ, висновки, реферат	*11.12-14.12.25*	
8	Розробка демонстраційних матеріалів	*14.12-16.12.25*	
9	Попередній захист роботи	*16.12-19.12.25*	

Здобувач вищої освіти _____ Мельник ВЛАДИСЛАВ
(підпис)

Керівник
кваліфікаційної роботи _____ Наталія ТРІНТІНА
(підпис)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 105 стор., 1 табл., 5 рис., 52 джерел.

Мета роботи – підвищення точності та стійкості приховування повідомлень шляхом розробки комбінованого методу шифрування та стеганографії.

Об’єкт дослідження – процеси забезпечення конфіденційності та приховування цифрових повідомлень.

Предмет дослідження – методи та алгоритми шифрування, а також підходи до інтеграції криптографії і стеганографії з метою підвищення ефективності захисту інформації.

У роботі використано різноманітні методи, такі як алгоритми симетричного та асиметричного шифрування, методи стеганографії у просторовій та частотній областях, апарат математичної статистики для оцінки стійкості, а також технології об'єктно-орієнтованого програмування. Головний акцент зроблено на комбінуванні цих методів для забезпечення високого рівня конфіденційності та прихованості даних.

Проведено аналіз сучасних методів шифрування та стеганографічного приховування повідомлень у цифрових контейнерах (зображення, аудіо). Глибоко вивчено принципи взаємодії вибраних алгоритмів (наприклад, AES і LSB-методу) для створення комбінованого методу, який максимізує безпеку приховання інформації .

Розроблено та оптимізовано комбінований метод шифрування та стеганографічного приховування, що базується на шифруванні повідомлення перед його вбудовуванням. Реалізовано програмну систему, яка використовує розроблений метод для ефективного та непомітного приховування даних у

зображеннях. Застосовано технології об'єктно-орієнтованого програмування для розробки програмного забезпечення.

Проведено експерименти для валідації розробленого комбінованого методу. Оцінено такі ключові показники, як стійкість до атак (наприклад, візуальних та статистичних), ємність приховування та час шифрування/вбудовування . Порівняно ефективність розробленого підходу з відомими окремими методами шифрування та стеганографії.

КЛЮЧОВІ СЛОВА: ШИФРУВАННЯ, СТЕГАНОГРАФІЯ, ПРИХОВУВАННЯ ПОВІДОМЛЕНЬ, КОМБІНОВАНИЙ МЕТОД, КРИПТОГРАФІЯ, ЦИФРОВІ ЗОБРАЖЕННЯ, БЕЗПЕКА ІНФОРМАЦІЇ.

ABSTRACT

Text part of the master's qualification work: 105 pages, 5 pictures, 1 table, 52 sources.

The purpose of the work is to improve the accuracy and stability of message concealment by developing a combined method of encryption and steganography.

The object of research is the processes of ensuring confidentiality and hiding digital messages.

The subject of the study is the improvement of encryption methods and algorithms, approaches to the integration of cryptography and steganography for information encryption.

The work uses various methods, such as symmetric and asymmetric encryption algorithms, steganography methods in the spatial and frequency domains, mathematical statistics tools for assessing stability, and object-oriented programming technologies. The main emphasis is on combining these methods to ensure a high level of confidentiality and data concealment.

An analysis of modern methods of encryption and steganographic concealment of messages in digital containers (images, audio) was carried out. The principles of interaction between selected algorithms (e.g., AES and LSB method) are studied in depth to create a combined method that maximizes the security of information concealment.

A combined method of encryption and steganographic concealment based on encrypting the message before embedding it is developed and optimized. A software system has been implemented that uses the developed method for effective and invisible data hiding in images. Object-oriented programming technologies have been applied to develop the software.

Experiments were conducted to validate the developed combined method. Key indicators such as resistance to attacks (e.g., visual and statistical), hiding capacity, and encryption/embedding time were evaluated. The effectiveness of the developed approach was compared with known separate methods of encryption and steganography.

KEYWORDS: ENCRYPTION, STEGANOGRAPHY, MESSAGE HIDING, COMBINED METHOD, CRYPTOGRAPHY, DIGITAL IMAGES, INFORMATION SECURITY.

ЗМІСТ

ВСТУП

Захист інформації: історичні основи та сучасні виклики

Потреба у захисті інформації супроводжує людство від найдавніших часів. У процесі еволюції методів забезпечення конфіденційності виділилися два доповнюючих один одного напрями: криптографія, основним завданням якої є перетворення даних для унеможливлення їх зчитування сторонніми особами, та стеганографія, основним принципом якої є приховування самого факту передачі секретного повідомлення. Таким чином, якщо криптографія робить зміст інформації недоступним, то стеганографія прагне зробити її невидимою.

Актуальність стеганографії та розвиток цифрових методів

Незважаючи на значну історію стеганографії, її активний розвиток як предмета наукових досліджень спостерігається лише останнім часом. Це пов’язано з інтенсивним розвитком інформаційних технологій, появою комп’ютерних мереж, а також з об’єктивними обмеженнями на застосування криптографічних засобів та високою актуальністю захисту інтелектуальної власності. Предметом вивчення цифрової стеганографії є методи приховування інформації у потоках оцифрованих сигналів. Ці методи реалізуються за допомогою програмного забезпечення та комп’ютерної техніки в рамках обчислювальних систем, включаючи корпоративні та глобальні мережі.

Стеганофонія: принципи та наукова база

Одним із підвидів стеганографії є стеганофонічні системи. Вони забезпечують приховування факту передачі таємного повідомлення, яке інкапсулюється у стек мережевих протоколів для передачі в режимі реального часу.

Принципи та визначення комп’ютерної стеганофонії були вперше сформульовані польськими фахівцями з Варшавського університету технологій у 2008 році. Вони запропонували низку методів приховування даних у трафіку IP-телефонії. З огляду на аналогічність структурних та робочих принципів, системи комп’ютерної стеганофонії часто порівнюють зі стеганографічними системами. Актуальність досліджень у галузі комп’ютерної стеганофонії зумовлена обмеженнями на використання криптографічних засобів та необхідністю вирішення завдань захисту прав власності на цифрову інформацію. Ця дисципліна є наукоємною, незважаючи на відносно невеликий термін існування. Для її розвитку широко використовується апарат таких наукових напрямків:

1. теорія ймовірностей та математична статистика
2. теорія швидких ортогональних перетворень
3. теорія апроксимації, кодування, складності та похибок
4. цифрова обробка сигналів та зображень

Дослідницькі проблеми та внесок вчених

Основні поняття та принципи комп’ютерної стеганофонії не завжди аналогічні класичній стеганографії. Зокрема, у роботах [1–5] представлена базова система означень та математичні моделі стеганографічних систем. Значна частина наукових публікацій присвячена аналізу головної характеристики стегосистеми — її стійкості. Значний внесок у розвиток стеганофонії та стеганографії зробили вчені: Задірака В.К., Кошкіна Н.В., Олексюк О.С., а також польські дослідники Wojciech Mazurczyk, Krzysztof Szczypiorski, Zbigniew Kotulski. Низка проблем у цій галузі залишається на початковій стадії вирішення. До основних проблем належать:

1. побудова стійких стеганофонічних систем у межах моделей пасивного та активного противника

2. отримання оцінок стійкості стеганофонічних систем
3. отримання оцінок складності стеганофонічних алгоритмів

Успішне вирішення вищезазначених проблем забезпечить підвищення стійкості стеганофонічних систем. У рамках досліджень встановлено вплив розміру контейнера з прихованими даними на стійкість стегосистеми до виявлення зловмисником. Запропоновано підхід до вибору оптимальних параметрів стегосистем за заданих мережевих характеристик, що дозволяє підвищити ефективність та захищеність передачі прихованих даних. Цифрова інформація вимагає надійного захисту від різноманітних загроз, включаючи несанкціонований доступ, знищення, підробку, витік, порушення ліцензійних угод та відмову від авторства. Захист інформації має критичне значення як для комерційного, так і для державного секторів. Згідно із Законом України "Про основи національної безпеки України" від 19.06.2003 р., серед загроз національним інтересам в інформаційній сфері визначено комп'ютерний тероризм, злочинність та розголошення таємної чи конфіденційної інформації. інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; маніпулювання суспільною свідомістю, зокрема, шляхом поширення недостовірної інформації. Таким чином, питання розроблення ефективних методів захисту цифрової інформації, зокрема методів комп’ютерної стеганографії та стеганоаналізу, актуальні та мають важливе значення для держави й суспільства. Існує необхідність захисту різних інформаційних систем, зокрема локальних мереж державних та комерційних закладів, від загрози витоку інформації, порушення авторських прав чи особистих таємниць (наприклад, медичних). Не можна виключати й можливість використання здобутків стеганографії антидержавними, терористичними структурами. Тому актуальними і важливими є розроблення та реалізація ефективних методів стеганоаналізу – науки про виявлення стеганографічних приховувань. З огляду на широту практичного

застосування та свою гнучкість, найбільші перспективи на сьогодні має універсальний статистичний стеганоаналіз з навчанням та класифікацією. Зважаючи на невпинний розвиток та вдосконалення методів комп'ютерної стеганографії дослідження саме цього напрямку стеганоаналізу є найбільш актуальним.

1 ТЕОРЕТИЧНІ ОСНОВИ ТА АНАЛІЗ СУЧАСНИХ МЕТОДІВ КРИПТОГРАФІЇ ТА СТЕГАНОГРАФІЇ

1.1. Фундаментальні концепції інформаційної безпеки та її захисту

Забезпечення інформаційної безпеки (ІБ) є критично важливим аспектом функціонування будь-якої сучасної комунікаційної системи. В основі ІБ лежить принцип забезпечення тріади властивостей, відомої як CIA-тріада (Confidentiality, Integrity, Availability): конфіденційності, цілісності та доступності. Порушення будь-якої з цих властивостей класифікується як інцидент, спричинений однією з численних категорій загроз.Загрози інформаційній безпеці являють собою потенційні дії чи події, які можуть спричинити збиток інформаційним активам. Систематизація цих загроз є основою для розробки адекватних захисних механізмів. У контексті конфіденційності, ключовими загрозами є несанкціонований доступ та перехоплення даних (eavesdropping). Ці пасивні загрози, які важко виявити, спрямовані на розкриття вмісту повідомлення без зміни його сутності. Забезпечення цілісності порушується активними загрозами, такими як модифікація даних або атаки "людина посередині" (MiTM), де зловмисник вносить зміни в інформацію, що передається. Нарешті, загрози доступності, прикладом яких є розподілені атаки відмови в обслуговуванні (DDoS), порушують можливість легітимних користувачів використовувати ресурси системи.

За своєю природою загрози можуть бути класифіковані як навмисні (зловмисні, ініційовані зовнішніми або внутрішніми акторами) та випадкові (спричинені апаратними збоями чи людськими помилками). У сфері захисту комунікацій, особлива увага приділяється навмисним загрозам, що вимагають застосування криптографічних і стеганографічних методів.

Комплексний захист інформації базується на концепції глибокої оборони (Defense in Depth), де криптографія та стеганографія виконують взаємодоповнюючі, але принципово різні функції, створюючи багатошаровий бар'єр. Криптографія (від грец. kryptós — прихований, gráphein — писати) є наукою про математичні методи перетворення інформації з метою забезпечення її конфіденційності та цілісності. Її першочерговим завданням є трансформація відкритого тексту у нечитабельний шифротекст, гарантуючи, що навіть у разі перехоплення, розкриття вмісту без володіння секретним ключем є обчислювально нездійсненним завданням. Таким чином, криптографія безпосередньо протидіє загрозам конфіденційності. Додатково, криптографічні хеш-функції та механізми електронного підпису забезпечують автентичність та цілісність даних, протистоячи їхній підміні. На противагу цьому, стеганографія (від грец. steganós — прихований, gráphein — писати) зосереджується на приховуванні самого факту існування секретного повідомлення. Стегосистема використовує нейтральний об'єкт, званий контейнером (зображення, аудіо- чи відеофайл), для вбудовування в нього секретного повідомлення, що трансформує його у стегоконтейнер. При цьому візуальні, статистичні та інші властивості стегоконтейнера повинні бути максимально наближені до оригінального контейнера, аби уникнути підозри та виявлення прихованого каналу зв'язку.Синергія комбінованого методу:Інтеграція криптографії та стеганографії створює систему, стійкість якої є вищою за суму стійкостей її окремих компонентів. Секретне повідомлення спершу шифрується, і лише потім отриманий шифротекст приховується. Такий підхід забезпечує дві лінії захисту.

1.2. Криптографічні алгоритми: принципи та стандарти

Криптографічні системи є математичним ядром будь-якої системи захисту конфіденційної інформації. Вони поділяються на дві основні категорії: симетричні та асиметричні (з відкритим ключем), кожна з яких має свою область застосування та обчислювальну складність. Симетрична криптографія (або криптографія з секретним ключем) характеризується використанням одного й того самого ключа

як для шифрування (кодування), так і для дешифрування (декодування) повідомлення. Це забезпечує високу швидкість обробки даних, що робить симетричні алгоритми ідеальними для масового шифрування великих обсягів інформації. Еталонним стандартом у цій галузі є Advanced Encryption Standard (AES), який замінив застарілий DES. AES використовує блокове шифрування з розміром блоку 128 біт та підтримує три варіанти довжини ключа: 128, 192 або 256 біт. Алгоритм заснований на мережі замінно-перестановочних операцій (Substitution-Permutation Network, SPN), що забезпечує високу стійкість до диференціального та лінійного криптоаналізу. AES-256, що використовує 256-бітовий ключ та 14 раундів шифрування, на сьогодні вважається квантово-безпечним у контексті атак на основну безпеку та є федеральним стандартом США для захисту секретної інформації. Для практичного застосування симетричні блокові шифри використовують режими роботи, які дозволяють застосовувати блоковий шифр до послідовності блоків даних або навіть до потоку. Серед найбільш поширених: Electronic Codebook (ECB): Шифрування кожного блоку незалежно. Режим не рекомендується через його вразливість до атак, що розкривають патерни даних. Cipher Block Chaining (CBC): Кожен блок шифротексту залежить від попередніх блоків, що забезпечує кращу дифузію змін. Вимагає використання вектора ініціалізації (IV). Counter (CTR): Перетворює блоковий шифр на потоковий, генеруючи псевдовипадковий потік ключів (keystream) на основі лічильника, що робить його придатним для паралельної обробки та забезпечує високу швидкість. Вибір симетричного алгоритму та режиму роботи є критичним для забезпечення швидкодії та надійності прихованого каналу. Асиметрична криптографія (або криптографія з відкритим ключем) оперує парою ключів: відкритим (public key), який може бути вільно розповсюджений, та закритим (private key), що зберігається в секреті. Відкритий ключ використовується для шифрування повідомлення, тоді як закритий — для його дешифрування. Цей підхід вирішує проблему розподілу ключів, яка є основною слабкістю симетричних систем. RSA (Rivest–Shamir–Adleman): Заснований на обчислювальній складності факторизації

великих цілих чисел. Довжина ключа RSA зазвичай становить 2048 біт або більше. ECC (Elliptic Curve Cryptography): Заснований на математичній складності задачі дискретного логарифму на еліптичних кривих. ECC забезпечує еквівалентний рівень безпеки при значно меншій довжині ключа (наприклад, 256-бітовий ECC-ключ еквівалентний 3072-бітовому RSA-ключу), що робить його більш ефективним для мобільних та ресурсномістких систем. Через свою обчислювальну повільність, асиметричні алгоритми рідко використовуються для шифрування великих обсягів даних. Натомість, вони є основою гібридних криптосистем, де асиметрична криптографія використовується лише для безпечного обміну симетричним сеансовим ключем. Після успішного обміну, основне повідомлення шифрується високошвидкісним симетричним алгоритмом (наприклад, AES). Така архітектура забезпечує як безпеку розподілу ключів, так і високу швидкість обробки даних. Для забезпечення цілісності та автентичності даних критично важливими є криптографічні хеш-функції. Це односторонні функції, які перетворюють вхідне повідомлення довільної довжини на фіксований рядок, званий хешем або дайджестом повідомлення. Основні властивості: стійкість до колізій (неможливість знайти два різні вхідні повідомлення з однаковим хешем) та односпрямованість (неможливість відновити вхідне повідомлення за хешем). Стандарти, такі як SHA-256 та SHA-3, широко застосовуються у даній сфері. Електронний цифровий підпис (ЕЦП) використовує асиметричні алгоритми та хеш-функції для підтвердження автентичності відправника та цілісності даних. Відправник хешує повідомлення, а потім шифрує отриманий хеш своїм закритим ключем. Отримувач дешифрує хеш відкритим ключем відправника і порівнює його з хешем, обчисленим із отриманого повідомлення. Збіг підтверджує, що повідомлення не було змінене та було відправлене власником закритого ключа. Для забезпечення цілісності та автентичності даних критично важливими є криптографічні хеш-функції. Це односторонні функції, які перетворюють вхідне повідомлення довільної довжини на фіксований рядок, званий хешем або дайджестом повідомлення. Основні властивості: стійкість до колізій (неможливість знайти два різні вхідні

повідомлення з однаковим хешем) та односпрямованість (неможливість відновити вхідне повідомлення за хешем). Стандарти, такі як SHA-256 та SHA-3, широко застосовуються у даній сфері. Електронний цифровий підпис (ЕЦП) використовує асиметричні алгоритми та хеш-функції для підтвердження автентичності відправника та цілісності даних. Відправник хешує повідомлення, а потім шифрує отриманий хеш своїм закритим ключем. Отримувач дешифрує хеш відкритим ключем відправника і порівнює його з хешем, обчисленим із отриманого повідомлення. Збіг підтверджує, що повідомлення не було змінене та було відправлене власником закритого ключа. Сучасна криптографія, зокрема асиметричні алгоритми RSA та ECC, базується на математичній складності розв'язання певних задач, таких як факторизація великих чисел та задача дискретного логарифму. Однак, розробка повномасштабних квантових комп'ютерів становить екзистенційну загрозу для цих систем, оскільки алгоритм Шора, реалізований на квантовому комп'ютері, здатен ефективно розв'язати обидві згадані задачі, повністю скомпрометувавши асиметричні ключі. Ця загроза стимулювала активний розвиток постквантової криптографії (PQC). PQC-алгоритми базуються на інших математичних проблемах, які вважаються стійкими до атак квантових комп'ютерів, включаючи криптографію на ґратках (lattices), на хеш-функціях та на кодах. Перехід до гібридних PQC-систем є стратегічним завданням для захисту інформації у довгостроковій перспективі. Хоча симетричні алгоритми (як AES-256) є більш стійкими до квантових атак (потрібне лише подвоєння довжини ключа для протидії алгоритму Гровера), загроза для асиметричного обміну ключами вимагає негайної уваги.

1.3. Стеганографічні методи: класифікація та оцінка ефективності

Стеганографія, як мистецтво прихованої комунікації, вимагає ретельного вибору середовища та техніки вбудовування даних. Ефективність будь-якої стегосистеми традиційно оцінюється на основі CSR-трилеми, що включає ємність (Capacity), непомітність (Security) та стійкість (Robustness). Досягнення

оптимального балансу між цими взаємовиключними критеріями є основною інженерною проблемою.

Трилема CSR (Capacity, Security, Robustness):

1. Ємність (Capacity): Максимальний обсяг секретної інформації, який може бути вбудований у контейнер без значного погіршення його якості або виявлення.
2. Непомітність (Security): Стійкість стегосистеми до виявлення стегоаналітичними методами. Це вимога, щоб стегоконтейнер був статистично невідрізним від оригінального контейнера.
3. Стійкість (Robustness): Здатність вбудованого повідомлення витримувати спотворення та модифікації стегоконтейнера, спричинені операціями обробки (компресія, обрізання, фільтрація).

Ці три параметри є взаємовиключними: підвищення ємності зазвичай знижує непомітність, а підвищення стійкості (наприклад, за рахунок кодування з виправленням помилок) може знижувати ємність або непомітність. Вибір контейнера (об'єкта, в який вбудовується секретне повідомлення) визначає як потенційну ємність, так і стійкість системи. Найбільш придатними є медіафайли, що володіють природною надмірністю. Цифрові зображення є найпопулярнішими контейнерами. Формати без втрат, такі як BMP та PNG, пропонують високу надмірність, що дозволяє вбудовувати великі обсяги даних, зберігаючи високу непомітність. Натомість, формати із втратами, зокрема JPEG, засновані на дискретному косинусному перетворенні (DCT), вимагають більш складних методів вбудовування в частотну область, але забезпечують вищу стійкість до компресії. Аудіофайли використовують особливості людського слуху, який є менш чутливим до незначних змін амплітуди або фази на високих частотах. Приховування даних у цих частотних діапазонах дозволяє створити стійкі, хоча й менш ємні стегосистеми. Відеофайли поєднують характеристики зображення та

аудіо, пропонуючи найбільшу загальну ємність через велику кількість кадрів, а також можливість приховування інформації у векторах руху.

Методи просторової області здійснюють маніпуляції безпосередньо над значеннями пікселів контейнера. Домінуючим підходом є метод найменш значущих бітів (Least Significant Bit, LSB). Ключова перевага LSB-методів — висока ємність вбудовування та низька обчислювальна складність. Однак, такий підхід значно змінює статистичні характеристики контейнера, що робить LSB-системи вразливими до стегоаналізу (наприклад, RS-аналізу та гістограмних атак). Зміна розподілу бітів у найменш значущих позиціях легко виявляється автоматизованими алгоритмами. Методи частотної області оперують коефіцієнтами, отриманими внаслідок застосування математичних перетворень. Ці підходи забезпечують вищу стійкість до компресії з втратами та обробки зображень. Дискретне косинусне перетворення (DCT): Використовується як основа для JPEG-компресії. DCT розкладає зображення на частотні складові, де низькочастотні коефіцієнти відповідають загальній енергії та видимому вмісту, а високочастотні — деталям. Вбудовування здійснюється у середньочастотні коефіцієнти (8×8 блоків). Приховування у низьких частотах призводить до артефактів, а у високих частотах — до втрати даних при повторній компресії. Дискретне вейвлет-перетворення (DWT): Дозволяє здійснювати багатороздільний аналіз, розділяючи зображення на піддіапазони (апроксимація, горизонтальні, вертикальні та діагональні деталі). Вбудовування у вейвлет-коефіцієнти середніх частот забезпечує кращий компроміс між непомітністю та стійкістю, оскільки ці коефіцієнти менш чутливі до візуального сприйняття, ніж просторова область, і більш стійкі до обробки, ніж високочастотні коефіцієнти DCT. Сучасні стегосистеми відійшли від сліпого вбудовування (як у традиційних LSB-методах) на користь адаптивної стеганографії або стеганографії за вибором (Steganography by Selection). Цей підхід забезпечує максимальну непомітність, оскільки він мінімізує статистичні відхилення стегоконтейнера. Принцип адаптивного вбудовування полягає у виборі тих пікселів або коефіцієнтів (носіїв), які є

найменш помітними для модифікації. Алгоритм враховує локальну складність, текстуру та ентропію області зображення. Функція вартості (Cost Function): Ядро методу. Ця функція визначає "вартість" зміни кожного окремого біта контейнера. Низька вартість призначається носіям, модифікація яких спричиняє мінімальну зміну глобальних або локальних статистичних характеристик. Мінімалізація спотворень: Алгоритми, такі як WOW (Wavelet-domain Outlier Removal) та S-UNIWARD (Spatial-UNIversal WAvelet-domain stego-aRsenal), використовують функцію вартості для вибору оптимальних позицій вбудовування. Вони гарантують, що модифікації відбуваються у найбільш "шумних" або текстурованих областях, де їх важче виявити. Адаптивні методи є найбільш стійкими до сучасного стегоаналізу, але вимагають більшої обчислювальної потужності для розрахунку функції вартості. Стегоаналіз — це наука про виявлення прихованих повідомлень та компрометацію стегосистем. Основна мета стегоаналітика — довести факт наявності прихованої інформації, оскільки відновлення самого повідомлення є завданням криптоаналізу. Методи поділяються на візуальні (менш ефективні) та статистичні (більш ефективні). Статистичні методи: Гістограмний аналіз: Використовується проти простих LSB-методів. Аналізує розподіл частот появи пікселів. Вбудовування даних часто призводить до характерних аномалій, зокрема, до згладжування або нерівномірності гістограми, які можна виявити. RS-аналіз (Regular/Singular Analysis): Високоефективний метод для виявлення LSB-вбудовування у некомпресовані зображення. Він вимірює зміни в регулярності та сингулярності пар сусідніх пікселів після їх маскування. Чим більше даних вбудовано, тим помітнішим стає лінійний тренд, що вказує на наявність прихованої інформації. Аналіз характеристик (Feature-based Analysis): Сучасні методи, як-от SRM (Spatial Rich Model), використовують тисячі статистичних ознак (характеристик) зображення (локальні варіації, колірні кореляції, високочастотні коефіцієнти) та застосовують машинне навчання (ML) для класифікації зображення як "чистого" або "стего". Це найскладніший виклик для будь-якої стегосистеми, що розробляється.

1.4. Математичні основи стегоаналізу та моделі простору ознак

Оскільки кінцевою метою розробки є створення стійкої крипто-стегосистеми, глибокий аналіз методів стегоаналізу є обов'язковим. Стегоаналіз перетворився з візуального та гістограмного аналізу на складну дисципліну, що використовує моделі простору ознак та машинне навчання для виявлення найменших статистичних відхилень. Задача стегоаналізу формально є задачею бінарної класифікації. Стегоаналітик має набір зображень та повинен визначити, чи є кожне зображення чистим чи містить приховане повідомлення . Для кількісної оцінки непомітності стегосистеми використовуються метрики, що вимірюють статистичну відстань між розподілом ймовірностей пікселів (або коефіцієнтів) оригінального контейнера та стегоконтейнера .

Дивергенція Кульбака-Лейблера (Kullback-Leibler Divergence, DKL): Чим ближче до нуля, тим менш помітною є статистична зміна, внесена стегометодом. Ідеальна стегосистема прагне. Середня квадратична помилка (Mean Square Error, MSE) та PSNR: Хоча MSE та PSNR) є основними метриками візуальної якості, вони не є достатніми для оцінки стегостійкості, оскільки не враховують складні статистичні кореляції, які є мішенню сучасного стегоаналізу. MSE обчислюється як:Найбільш потужними інструментами стегоаналізу є моделі, що будують багатовимірний простір ознак (Feature Space), який підкреслює навіть найменші статистичні аномалії, внесені прихованим повідомленням. SRM є золотим стандартом у стегоаналізі для зображень у просторовій області. Вона складається з тисяч статистичних ознак, отриманих із залишків зображення (residuals). Залишки генеруються за допомогою фільтрів високих частот (High-Pass Filters), які пригнічують природний вміст зображення (edges, texture) і підсилюють випадковий шум, куди зазвичай вбудовується повідомлення. З цих залишків обчислюються гістограми спільних появ (Co-occurrence Matrix), які фіксують кореляції між сусідніми пікселями. Вбудовування повідомлення порушує ці

природні кореляції, і SRM фіксує це відхилення. Подальший розвиток SRM призвів до створення універсальних моделей, які можуть застосовуватися як до просторової, так і до частотної області (DCT або DWT). Методи S-UNIWARD (Spatial UNIWARD) та F-UNIWARD (Frequency UNIWARD) використовують подібний принцип: вони будують простори ознак на основі залишкових шарів, але адаптують фільтри для більш ефективного виявлення модифікацій, внесених адаптивними стегосистемами. Для прийняття рішення про приналежність зображення використовується машинне навчання. Вектор ознак, отриманий із Rich Models (наприклад, SRM), подається на вхід класифікатору. Класифікатори: Традиційно використовувались Лінійні аналізатори (Linear Discriminant Analysis, LDA) та Опорні вектори (Support Vector Machines, SVM). Сучасні системи використовують Згорткові нейронні мережі (Convolutional Neural Networks, CNN), які здатні самостійно вивчати оптимальні ознаки для виявлення стего, замінюючи необхідність ручного проектування фільтрів, як у SRM. На підставі аналізу стегоаналізу, до стійкої крипто-стегосистеми висувається ключова вимога:

Мінімалізація статистичного спотворення: Метод вбудовування повинен бути адаптивним (використовувати функцію вартості), щоб мінімізувати зміни саме тих ознак (наприклад, залишкових шарів), які використовуються моделями SRM та UNIWARD. Маскування шифротекстом: Використання криптографії для перетворення відкритого повідомлення на високоентропійний шифротекст (білий шум) усуває статистичні патерни, але не знімає вимоги до мінімалізації фізичних змін у контейнері. Стійкість гібридного методу оцінюється через P_D класифікатора, навченого на моделях SRM. Лише система, що витримує такий аналіз, може вважатися надійною.

1.5 Проблемна область та завдання роботи

В даний час, поряд із широким використанням цифрових форматів мультимедіа та наявними проблемами управління цифровими ресурсами, дослідження в області стеганографії стають дедалі актуальнішими . Вирішення

завдання приховування інформації також є важливою проблематикою в умовах розвиненої інфраструктури мережевого спілкування користувачів глобальних комп'ютерних мереж, з розвитком яких стало можливим швидко та економічно вигідно передавати В умовах розвиненої інфраструктури мережевого спілкування стало можливим швидко та економічно вигідно передавати електронні документи в різні куточки планети. При цьому значні обсяги переданих матеріалів часто супроводжуються незаконним копіюванням та розповсюдженням. Як наслідок, це стимулює пошук способів приховування авторської інформації в різних типах файлів, включаючи текстові, графічні, аудіо- та відеоформати. На сьогоднішній день існує значна кількість програмних продуктів, які застосовуються в стеганографії та реалізують методи впровадження конфіденційних даних у різні типи файлів..Класична задача стеганографії та вимоги до контейнерів Класична задача стеганографії полягає в організації передачі секретного повідомлення таким чином, щоб як його зміст, так і сам факт передачі залишалися прихованими від усіх, крім зацікавлених осіб. Для вирішення цього завдання використовується повідомлення, що називається контейнером (або стеганоконтейнером), в який вбудовується необхідне секретне повідомлення. Розробники стеганографічних методів повинні забезпечувати прозорість переданих конфіденційних даних: зміна певної кількості інформаційних бітів у контейнері не повинна призводити до значних втрат його якості (повинні бути відсутні артефакти візуалізації вбудовування). В якості контейнерів найчастіше використовуються файли, що містять цифрові фотографії, текст, музику або відео. Наприклад, при використанні графічних файлів процес передачі повідомлень сторонніми спостерігачами сприйматиметься як звичайний обмін цифровими графічними файлами. При цьому слід пам'ятати про важливість дотримання однієї умови: ніхто не повинен мати одночасного доступу до вихідного файлу-контейнера та до файлу, який містить приховане повідомлення. У такому випадку просте порівняння файлів негайно виявить наявність прихованого повідомлення.

Вибір формату контейнера

Як було зазначено раніше, у комп'ютерній стеганографії в якості контейнера може виступати практично будь-який файловий формат. Проте, найбільш поширеним типом носія є файли зображень формату BMP. Це пояснюється тим, що для цілей стеганографії найкращими є формати, в яких використовуються методи стиснення без втрат (зокрема, формати BMP, TIFF, PNG, TGA та ін.). Додатковими перевагами формату BMP є висока якість зображення та відносна простота його структури. Метою даної магістерської роботи є дослідження методів комп’ютерної стеганографії для цифрових контейнерів у вигляді зображення та практична реалізація вдосконаленого методу комп’ютерної стеганографії для цифрових контейнерів у вигляді зображення. Для досягнення поставленої мети у роботі пропонується вирішення наступних завдань:

1. всебічне дослідження методів комп’ютерної стеганографії для цифрових контейнерів у вигляді зображення
2. формалізація головних недоліків комп’ютерної стеганографії для цифрових контейнерів у вигляді зображення
3. вдосконалення методу комп’ютерної стеганографії для цифрових контейнерів у вигляді зображення
4. практична реалізація вдосконаленого методу комп’ютерної стеганографії для цифрових контейнерів у вигляді зображення

Висновки до розділу

У рамках першого розділу даної магістерської роботи висвітлено теоретичні аспекти реалізації стеганографічних методів. Окреслено генезис становлення поняття "стеганографія", здійснено дослідження основних складових та компонентів реалізації методів комп’ютерної стеганографії для цифрових контейнерів у вигляді зображення. Також сформульовано загальну мету

дослідження та структуровано завдання, необхідні для досягнення поставленої мети.

2 АРХІТЕКТУРИ ТА АЛГОРИТМИ КОМП'ЮТЕРНОЇ СТЕГАНОГРАФІЇ ДЛЯ ГРАФІЧНИХ КОНТЕЙНЕРІВ

2.1. Обґрунтування гібридної архітектури та функціональна декомпозиція

Розробка стійкої крипто-стегосистеми є відповіддю на еволюцію загроз, де просте шифрування може бути виявлено, а чиста стеганографія — скомпрометована сучасними статистичними аналізаторами. Тому архітектура системи повинна базуватися на концепції глибокої оборони (Defense in Depth), інтегруючи криптографічний та стеганографічний захист. Гібридна система забезпечує, що навіть у разі успішного стегоаналізу (виявлення факту прихованої передачі) вміст повідомлення залишається конфіденційним завдяки криптографічній стійкості. Найефективнішою архітектурою є послідовна обробка за схемою "Крипто-Адаптивне Стего". Ця парадигма є логічним наслідком вимоги протистояння статистичному стегоаналізу (Розділ 1.4). Вона поєднує два критично важливі елементи захисту:Відкрите повідомлення M спочатку шифрується симетричним алгоритмом E(Kc), перетворюючись на шифротекст C. Цей етап критично важливий для стегостійкості з наступних причин:

Усунення статистичних патернів: Шифротекст, отриманий від якісного симетричного шифру (наприклад, AES у режимі CTR), повинен мати ідеально рівномірний розподіл бітів (ентропію, близьку до максимальної). Це робить його нерозрізненним від білого шуму.

Маскування: Коли такий високоентропійний шифротекст вбудовується у контейнер I, він фізично імітує випадковий шум, що значно ускладнює виявлення для класичних стегоаналітичних методів, які шукають лінгвістичні або структурні патерни у прихованих даних.

Конфіденційність та цілісність: Додатково до шифротексту C, обчислюється хеш-код повідомлення (MAC або HMAC) H(M) для забезпечення цілісності.

Отриманий блок даних для вбудовування D = {C, H(M)} є криптографічно захищеним.

Наступний етап — адаптивне вбудовування. Блок даних D вбудовується у контейнер I лише у тих позиціях, які мінімізують статистичний ризик виявлення. Протидія Rich Models (SRM): Навіть якщо вбудовані дані є випадковими (як шифротекст), їх фізична модифікація контейнера залишає статистичні сліди в залишках зображення, які виявляються Rich Models (SRM).

Функція вартості: Адаптивний метод використовує функцію вартості ρ(i,j) (детальніше у 2.4.1) для визначення того, які коефіцієнти X(i,j) є "безпечними" для модифікації. Вбудовування відбувається вибірково, мінімізуючи загальне спотворення та зберігаючи статистичні властивості контейнера I максимально наближеними до властивостей стегоконтейнера S.

Система декомпонована на три основні, незалежні модулі, кожен з яких виконує свій набір критичних операцій:

1. Модуль 1: Криптографічної підготовки (Крипто-Парсер).
2. Вхід: Відкрите повідомлення M, симетричний ключ Kc.

Операції: Шифрування M → C, обчислення коду автентифікації H(M), формування метаданих (IV, L), конкатенація блоку D.

1. Вихід: Криптографічно захищений та структурований блок даних D(full).
2. Модуль 2: Адаптивного вбудовування (Стего-Кодер).
3. Вхід: Контейнер I, блок даних D(full), параметри вбудовування (область DWT, Q).

Операції: Застосування DWT, розрахунок функції вартості ρ, застосування кодування з мінімізацією спотворення (STC) для вбудовування D(full) у вибрані коефіцієнти, застосування зворотного DWT.

1. Вихід: Стегоконтейнер S.

2. Модуль 3: Вилучення та дешифрування (Стего-Крипто-Декодер).
3. Вхід: Стегоконтейнер S, симетричний ключ Kc.

Операції: Застосування DWT, вилучення бітів з використанням STC-декодера, відновлення блоку D'(full), декомпозиція на IV, L, C' та HMAC, перевірка цілісності, дешифрування C' → M'.

2.2. Проектування криптографічного модуля

Проектування криптографічного модуля є першочерговим завданням, оскільки він відповідає за два ключові аспекти безпеки: конфіденційність повідомлення M та його цілісність і автентифікацію. Вибір примітивів ґрунтується на сучасних криптографічних стандартах, високій стійкості (не менше 128 біт) та здатності генерувати вихідний потік з властивостями, близькими до випадкового (білого) шуму, що є критично важливим для подальшого стеганографічного вбудовування. Для шифрування відкритого повідомлення обрано алгоритм AES (Advanced Encryption Standard), який є федеральним стандартом обробки інформації (FIPS 197) США та де-факто глобальним стандартом для симетричного шифрування. Використовується версія AES-256, яка передбачає довжину ключа 256 біт. Це забезпечує експоненційну стійкість до атак повного перебору та гарантує, що рівень безпеки системи значно перевищує мінімально необхідні 128 біт. Такий запас стійкості убезпечує систему від прогнозованого зростання обчислювальної потужності (наприклад, завдяки квантовим обчисленням, зокрема алгоритму Гровера) та відкриття потенційних аналітичних слабкостей протягом наступних десятиліть. Вибір режиму роботи шифру є не менш важливим, ніж вибір самого алгоритму. Режим Counter (CTR) є оптимальним і, фактично, єдиним, що ідеально відповідає вимогам стеганографії, оскільки він перетворює блоковий шифр на потоковий генератор псевдовипадкової гами. Генерація гами (Keystream): Замість прямого шифрування блоків даних повідомлення, режим CTR шифрує послідовність унікальних значень — лічильників (counter). Кожен лічильник формується з унікального Nonce (Number used once) та порядкового номера блоку i, який інкрементується.

Переваги режиму CTR для стеганографії:

Ідеальна ентропія та маскування: Оскільки гама генерується криптографічно стійким шифром, вона є псевдовипадковою. Побітове XOR з повідомленням повністю усуває будь-які статистичні патерни, лінгвістичні залежності та іншу структуру вихідного тексту M. Шифротекст C набуває статистичних властивостей, практично не відрізнених від білого шуму. Це робить його ідеальним об'єктом для вбудовування, оскільки класичні стегоаналітичні методи, орієнтовані на виявлення неестественних кореляцій у вбудованих даних, стають неефективними.

1. Відсутність поширення помилок: Пошкодження окремого біта шифротексту призводить до помилки лише в одному відповідному біті відкритого тексту після дешифрування. Ця властивість є корисною в умовах каналів зв'язку з втратами або при потенційних модифікаціях контейнера.
2. Паралельність: Гаму для різних блоків можна обчислювати заздалегідь та паралельно, що суттєво підвищує продуктивність при роботі з великими обсягами даних або високою пропускною здатністю.

Навіть ідеально зашифрований шифротекст вразливий до навмисних або випадкових змін, які можуть виникнути під час процесів вбудовування, передачі або вилучення. Для гарантії цілісності (integrity) та автентифікації (authentication) даних використовується криптографічний примітив HMAC (Hash-based Message Authentication Code). Просте хешування шифротексту (наприклад, обчислення H(C)) гарантує лише цілісність, але не автентифікацію. Зловмисник, який перехопив дані, може змінити C на C', обчислити новий хеш H(C') і приєднати його, обходячи таким чином захист. HMAC вирішує цю проблему, інтегруючи

секретний ключ K_h у процес хешування, що робить неможливим обчислення коректного коду без знання цього ключа.

В якості базової хеш-функції для HMAC обрано SHA-256 (Secure Hash Algorithm з 256-бітним виходом). SHA-256 належить до сімейства SHA-2, широко визнаного криптографічно стійким стандартом (FIPS 180-4) з високою стійкістю до знаходження колізій.

Функціональне призначення HMAC-SHA-256 в системі:

1. Цілісність даних: Переконливо підтверджує, що шифротекст C не зазнав жодних змін після формування.
2. Автентифікація повідомлення: Підтверджує, що дані надійшли від законного відправника, який володіє секретним ключем K_h.

Надійність усієї криптосистеми в останню чергу залежить від безпечного управління ключами. У гібридній системі застосовується сучасний підхід, що включає протокол обміну ключами та функцію їх отримання. Для встановлення спільного секретного ключа K_shared між відправником та отримувачем без необхідності його попередньої передачі використовується протокол ECDH.

Переваги ECDH:

1. Висока ефективність: Криптографія на еліптичних кривих (ECC) забезпечує еквівалентний рівень безпеки (наприклад, 128 біт) при значно меншій довжині ключа порівняно з класичними алгоритмами (RSA, DH). Наприклад, крива P-256 (256 біт) пропонує безпеку, порівнянну з RSA-3072. Це призводить до швидших обчислень та менших накладних витрат при передачі публічних ключів.
2. Досконала пряма секретність (Perfect Forward Secrecy, PFS): Якщо для кожної сесії генерується нова пара ключів ECDH, скомпрометування довгострокових ключів сторін не дозволить розшифрувати

перехоплені дані минулих сесій, оскільки сеансовий секрет K_shared не зберігається довгостроково.

Отриманий спільний секрет K_shared не може безпосередньо використовуватись як ключ шифрування або автентифікації. Криптографічна практика вимагає сепарації ключів (key separation) — використання різних, незалежних ключів для різних криптографічних операцій. Це запобігає атакам, що експлуатують взаємозв'язок між примітивами.

2.3. Класифікація методів приховування інформації в графічних зображеннях

У сучасній практиці всі методи приховування даних у графічних зображеннях поділяються на дві великі категорії за принципами, що лежать в їх основі. Форматні стеганографічні системи базуються на структурних особливостях формату зберігання графічних даних. Розробка таких методів передбачає ретельний аналіз специфікації формату з метою ідентифікації службових полів, модифікація яких не впливає на функціональність та відображення графічного вмісту. Типовими прикладами є використання:

1. зарезервованих для майбутніх розширень полів
2. додаткових полів метаданих
3. невикористовуваних ділянок заголовків

Проте форматні методи мають суттєвий недолік – вразливість до автоматизованого виявлення. Враховуючи принцип загальновідомості стеганографічної системи, противник може реалізувати повністю автоматичний алгоритм аналізу, що перевіряє відповідність структури файла стандартній специфікації. Це обумовлює крайньо низьку стійкість таких методів до атак пасивного супротивника.

Неформатні методи працюють безпосередньо з піксельними даними зображення, ігноруючи структурні особливості формату зберігання. Характерною рисою цих методів є неминуче виникнення спотворень у самих даних зображення в

результаті вбудовування. Однак саме ця властивість забезпечує їм вищу стійкість до атак як пасивних, так і активних противників у порівнянні з форматними методами. Методи приховування даних, засновані на зміні піксельної інформації зображення JPEG Специфіка формату JPEG передбачає складний багатоетапний алгоритм стиснення, що включає перетворення кольорового простору, субдискретизацію, дискретне косинусне перетворення (ДКП), квантування та ентропійне кодування. Детальний аналіз цих етапів дозволив розробити низку ефективних неформатних методів приховування. Метод приховування у вихідних даних зображення Стандарт JPEG підтримує режим стиснення без втрат (Lossless JPEG), який принципово відрізняється від класичного алгоритму з втратами. Цей режим використовує схему двовимірної диференціальної імпульсно-кодової модуляції (ДІКМ), де значення кожного пікселя прогнозується на основі сусідніх значень, а різниця між фактичним і прогнозованим значенням піддається ентропійному кодуванню. У разі використання Lossless JPEG можливе безпосереднє вбудовування інформації в піксельні дані зображення з використанням традиційних методів стеганографії, зокрема модифікації молодших бітів. Однак практичне застосування цього методу обмежене через рідкісне використання формату Lossless JPEG. При застосуванні до звичайного JPEG з втратами, прихована інформація буде практично повністю знищена на етапах субдискретизації, ДКП та квантування. Метод приховування з використанням таблиць квантування Цей метод належить до найбільш поширених сучасних підходів для приховування даних у JPEG-файлах. Його ідея полягає у модифікації молодших бітів коефіцієнтів квантування, що зберігаються у відповідних таблицях. Перевагою методу є збереження типової структури JPEG-потоку, що робить його повністю неформатним. Метод приховування з використанням таблиць квантування Цей метод передбачає модифікацію найменш значущих бітів коефіцієнтів квантування. Його ключова перевага полягає в тому, що він не порушує стандартну структуру JPEG-потоку, що класифікує його як повністю неформатний підхід. Проте метод має суттєві обмеження: Обмежена місткість: Типовий JPEG-файл містить лише одну-дві таблиці квантування

розміром 64 байти кожна. Таким чином, максимальний обсяг прихованих даних становить лише 8 байт при використанні однієї таблиці. Деградація стиснення: Модифікація коефіцієнтів квантування призводить до зміни статистичних характеристик блоків, що обробляються. Це негативно впливає на ефективність подальшого ентропійного кодування і зазвичай призводить до збільшення розміру вихідного файлу. Метод використання додаткових таблиць квантування Як розширення попереднього методу, цей підхід передбачає створення додаткових таблиць квантування, що дозволяє збільшити місткість сховища. Специфікація JPEG формату дійсно передбачає можливість використання множини таблиць, тому така модифікація не порушує внутрішню структуру файлу. Однак цей метод має дві суттєві особливості:

1. Він стає частково форматним, оскільки експлуатує опціональну можливість стандарту
2. Зберігаються всі недоліки базового методу, пов'язані з деградацією якості стиснення

На практиці існують дві основні реалізації цього методу: Перший варіант передбачає додавання таблиць для підвищення ефективності стиснення, як це передбачено оригінальною специфікацією. Однак для більшості зображень кількість таких додаткових таблиць виявляється незначною. Другий варіант використовує періодичне додавання однакових таблиць квантування, які відрізняються лише в молодших бітах, що містять приховане повідомлення. Така реалізація є явно форматною і демонструє низьку стійкість до пасивних атак. Метод приховування в спектрі зображення після квантування Цей перспективний метод базується на модифікації частотних коефіцієнтів після етапу квантування, але перед ентропійним кодуванням. Його переваги включають: Значно вищу місткість порівняно з попередніми методами.

Потенційно високу стійкість до пасивного аналізу

Математична модель методу може бути представлена таким чином:

Нехай:

1. m - біти прихованого повідомлення
2. $B_{i,□}$ - значення ненульових елементів квантованого спектра
3. $B'_{i,□}$ - модифіковані блоки зображення

Визначається бінарна послідовність k□, де:
k□ = 1, коли в молодший біт j-го блоку вбудовується черговий біт повідомлення
k□ = 0 у протилежному випадку

Пряме стеганографічне перетворення F: M × B × K → B визначається як:

$$B'_{i,□} = \{ B_{i,□}, \forall i, k□ = 0\ m□, i = 0, k□ = 1 \} \quad (2.1)$$

де:

$l = \sum□_{=1}^{j} k□; j = 1,2,3,...n$

Відповідне зворотне перетворення F^{-1}: B × K → M має вигляд:
$m□ = B_{0,i}^{l}$ де l таке, що $l = \sum□_{=1}^{j} k□ = j, j = 1,2,3,...n$

Методи приховування в зображеннях з палітрою кольорів

Робота з графічними форматами, що використовують палітру кольорів (наприклад, GIF, PNG-8), має свої особливості. У таких зображеннях пікселі містять не безпосередні значення кольору, а індекси до палітри. Це створює додаткові складнощі для традиційних методів стеганографії, оскільки наївна модифікація молодших бітів індексів може призвести до різкої зміни кольору пікселя. Для ефективного використання таких форматів розроблені спеціалізовані методи, що враховують особливості палітрного кодування кольорів.

2.4. Обґрунтування вибору стегометоду та області вбудовування

Для досягнення вимоги непомітності (імовірність виявлення $P\_D \leq 0.55$) необхідно обрати стегометод, який здатний мінімізувати статистичні відхилення у залишках зображення — основній мішені сучасних багатомірних стегоаналітичних моделей (Rich Models, SRM). Вибір ґрунтується на двох взаємопов'язаних принципах: 1) використання частотного перетворення, стійкого до зорового та статистичного аналізу; 2) застосування адаптивного вбудовування, яке мінімізує спотворення, що фіксується стегоаналітиком. DWT є оптимальним вибором порівняно з методом заміни найменш значущих бітів (LSB) у просторовій області або дискретним косинусним перетворенням (DCT). Його перевага полягає у здатності забезпечити багатороздільний аналіз (Multiresolution Analysis), який краще відповідає характеристикам людського зорового сприйняття та структурі природних зображень.

Дискретне вейвлет-перетворення декомпозує зображення I на сукупність коефіцієнтів, організованих за рівнями розділення (k) та орієнтацією: Де кожен рівень (k) генерує чотири піддіапазони (subbands):

1. LL (Low-Low): Коефіцієнти апроксимації (низькі частоти). Містять основну енергію зображення, його контурну та світлову інформацію. Будь-яка модифікація цих коефіцієнтів призводить до катастрофічних візуальних артефактів і заборонена.

2. LH (Low-High): Коефіцієнти деталей по вертикалі. Відповідають за горизонтальні контури та текстури (низькі частоти за горизонталлю, високі — за вертикаллю).

3. HL (High-Low): Коефіцієнти деталей по горизонталі. Відповідають за вертикальні контури та текстури (високі частоти за горизонталлю, низькі — за вертикаллю).
4. HH (High-High): Діагональні деталі (високі частоти). Містять дрібний шум, піксельну "зернистість" та діагональні деталі. Найменш стійкі до стиснення та обробки.

Для вбудовування обрані коефіцієнти середніх частот HL та LH на рівнях декомпозиції k = 2 або k = 3. Цей вибір обґрунтований наступним: Візуальна маскувальна здатність: Згідно з властивостями зорової системи людини (HVS), сприйняття змін у області середніх просторових частот менш критичне. Зміни в текстурних областях (контури) маскуються їхньою природною варіативністю. Наявність достатньої ємності: Ці піддіапазони містять значну кількість коефіцієнтів, що забезпечує необхідну вміщувальну здатність для приховання шифротексту. Стійкість до стиснення: Коефіцієнти середніх частот демонструють кращу стійкість до втратного стиснення (напр., JPEG), ніж високочастотні HH-коефіцієнти. Порівняно з LSB у просторовій області: DWT забезпечує значно вищу стійкість до візуального виявлення та рутинних статистичних тестів (напр., χ^2-тест). LSB-методи легко виявляються навіть простими аналітичними інструментами.

Порівняно з DCT у частотній області (як у JPEG):

1. Відсутність блочних артефактів: DCT застосовується до блоків 8x8 пікселів, що часто призводить до видимих меж блоків при модифікації. DWT є глобальним перетворенням, що усуває цю проблему.
2. Краща просторово-частотна локалізація: Зміна одного DWT-коефіцієнта впливає на конкретну область з відповідною просторовою та частотною

специфікою, роблячи артефакти менш структурованими для алгоритмів, навчених на DCT-артефактах.

3. Енергетична компактність: DWT ефективно концентрує енергію зображення в невеликій кількості коефіцієнтів (LL), залишаючи багато коефіцієнтів у HL, LH, HH з незначною амплітудою, що підходить для непомітної модифікації.

Вбудовування у вибрані DWT-коефіцієнти здійснюється на основі принципу "Steganography by Selection" (стеганографія шляхом вибору), що є ключовою умовою протидії Rich Models (SRM). Класичні методи (наприклад, послідовне вбудовування у всі високочастотні коефіцієнти) вносять передбачувані зміни, порушуючи природні статистичні зв'язки. SRM аналізують саме такі систематичні відхилення у залишках зображення. Адаптивний метод ґрунтується на парадигмі: зміни повинні вноситися лише в ті елементи носія (коефіцієнти X_i,j), які в оригінальному контейнері I є найбільш випадковими, шумними або текстурними. Математично це задача мінімізації загального спотворення D:

$$D = \Sigma\_i,j \left[\rho\_i,j \cdot \delta(x\_i,j, y\_i,j) \right] \rightarrow \min \qquad (2.2)$$

де: ρ_i,j — Функція вартості (Cost Function) для елемента (i,j). Високе значення — для коефіцієнтів у гладких областях або на різких краях (небезпечно змінювати). Низьке значення — для коефіцієнтів у хаотичних, текстурних ділянках (безпечно). δ(x_i,j, y_i,j) — Функція дистанції (зазвичай 1, якщо значення змінилося, і 0 — якщо ні). Мета: приховати дані, мінімізуючи сумарну "вартість", тобто обираючи для змін найменш статистично помітні місця, що імітують природний шум контейнера. Для практичної реалізації принципу мінімізації спотворення в DWT-області обрана одна з найефективніших функцій вартості — WOW. Вона спеціально розроблена для роботи з вейвлет-перетворенням і демонструє високу стійкість до атак SRM. Функція WOW обчислює вартість ρ_i,j для кожного коефіцієнта на основі його локалізованої чутливості до збурень: До коефіцієнтів застосовується набір лінійних фільтрів направленого згладжування. Для кожного

коефіцієнта обчислюється, наскільки сильно він реагує на ці фільтри. Вартістю ρ_i,j стає величина, обернено пропорційна до суми абсолютних відгуків. Таким чином: Низька вартість → Високий природний шум/текстура → Безпечно для вбудовування. Висока вартість → Гладка область або різкий край → Небезпечно для вбудовування.

2.4.1. Удосконалений метод приховування зі сортуванням палітри

Оптимізований алгоритм передбачає комплексну обробку палітри з подальшим вбудовуванням даних. Кожному елементу палітри ставляться у відповідність два числових ідентифікатори: початковий номер i та відсортований номер j. Процес приховування реалізується через послідовне сканування всіх пікселів зображення. Для кожного пікселя з індексом k визначається відповідний відсортований номер j□. Якщо даний індекс є придатним для приховування, відбувається заміна його молодшого біта на відповідний біт повідомлення. На завершальному етапі виконується зворотне перетворення модифікованого індексу j□ у вихідний номер k, який і призначається поточному пікселю. Окремий клас методів базується на модифікації безпосередньо самих елементів палітри кольорів. Оскільки формат зберігання кольорових компонентів у палітрі аналогічний формату зберігання пікселів у звичайних зображеннях, можливе застосування стандартних LSB-методів. Однак цей підхід має суттєві обмеження:

- Обмежена місткість: максимальний розмір палітри становить 256 елементів, при цьому кожен елемент може містити до 3 біт прихованої інформації (по одному біту на кожну кольорову компоненту), що дає загальну ємність у 768 біт
- Ризик виявлення: в результаті модифікації можуть утворитися ідентичні кольорові елементи, наявність яких може служити статистичною ознакою для виявлення факту приховування

2.4.2. Метод використання однакових елементів палітри

Даний метод ґрунтується на спостереженні, що наявність дублікатів у палітрі не впливає на візуальне сприйняття зображення. З технічної точки зору, використання однакових елементів палітри є неефективним і може призводити до збільшення розміру файлу, що робить цей метод форматно орієнтованим.

Алгоритм реалізації:

1. Ідентифікація найбільш вживаних елементів палітри
2. Додавання "двійників" - ідентичних копій вибраних елементів
3. Послідовне сканування пікселів: при збігу з елементом, що має двійника, виконується кодування біта повідомлення шляхом вибору між оригіналом та копією

Приклад реалізації:
Для повідомлення m = 10010110 та вихідної палітри:

- 0 → (0,255,0)
- 1 → (0,0,255)

Після додавання двійника 2 → (0,255,0) відбувається перетворення зображення з кодуванням повідомлення через вибір між індексами 0 та 2 для зелених пікселів. Інноваційний підхід, що використовує комбінаторні властивості палітри для приховування інформації. Для палітри з n унікальними елементами існує n! можливих перестановок, що теоретично дозволяє закодувати до $\log_2(n!)$ біт інформації.

Математична основа:
Метод визначає бієктивне відображення між простором повідомлень та множиною перестановок елементів палітри з використанням секретного ключа.

Алгоритм кодування:

1. Впорядкування елементів палітри за зростанням кольорової ваги (65536×R + 256×G + B)
2. Розподіл позицій у новій палітрі шляхом послідовного ділення числового представлення повідомлення m
3. Перша позиція: m mod n
4. Наступні позиції: (m div n) mod (n-1), (m div n(n-1)) mod (n-2) тощо
5. Корекція індексів пікселів відповідно до нової конфігурації палітри

Приклад для палітри з трьома елементами {a, b, c}:
При m = 5 (3! - 1 = 5):

1. Позиція для a: 5 mod 3 = 2
2. Позиція для b: (5 div 3) mod 2 = 1 mod 2 = 1
3. Позиція для c: залишається єдино доступна позиція 0
   Результат: нова палітра у порядку c, b, a

Процес декодування передбачає зворотне перетворення з відновленням числового значення повідомлення на основі позицій елементів у модифікованій палітрі.

Процес відновлення повідомлення реалізується у зворотному порядку. Для прикладу з трьома елементами {a, b, c} у модифікованій палітрі cba:

1. Елемент a займає позицію 2, отже m mod 3 = 2
2. Елемент b знаходиться на позиції 1, тому (m div 3) mod 2 = 1
3. Елемент c автоматично займає позицію 0

Шляхом розв'язання системи рівнянь відновлюється значення m = 5.

2.5. Деталізація алгоритму адаптивного вбудовування на основі функції вартості

Для забезпечення стійкості до Rich Models (SRM) критично важливо, щоб процес вбудовування був адаптивним — залежав від локальних властивостей самого зображення-контейнера. Цей розділ детально описує механізми, які

гарантують, що модифікації вносяться лише в статистично "безпечні" місця, мінімізуючи загальне спотворення. Функція вартості (ρ) є фундаментальним елементом адаптивної стеганографії. Вона кількісно визначає "ціну" (ризик) внесення мінімальної зміни до конкретного коефіцієнта зображення X_i,j після його перетворення (наприклад, у DWT-області). Висока вартість (високе ρ): Призначається коефіцієнтам, розташованим у гладких, однорідних областях (наприклад, чисте небо, стіна). Зміна такого коефіцієнта залишає чіткий, статистично аномальний слід у залишках зображення, який легко виявляється SRM-моделями. Низька вартість (низьке ρ): Призначається коефіцієнтам у високотекстурованих, складних або шумних областях (наприклад, листя дерева, пісок, гранітна поверхня, чіткі контури об'єктів). Тут природна випадковість і висока локальна ентропія ефективно маскують штучно внесену мінімальну зміну.

Інтерпретація: Чим більше коефіцієнт відрізняється від оточення (вища локальна варіація, складніша текстура), тим менша йому призначається вартість. Таким чином, функція вартості прагне бути обернено пропорційною до локальної складності, автоматично направляючи вбудовування в області з високою природною ентропією. Важливе зауваження: У реальних високостійких системах (як WOW, HILL, SUNIWARD) використовуються складніші фільтри та ядра для оцінки вартості, враховуючи різні напрямки та масштаби, що робить їх значно ефективнішими проти сучасних атак.

Після розрахунку матриці вартостей для всіх потенційних носіїв виникає задача: як оптимально розподілити біти повідомлення серед цих носіїв, щоб сумарна вартість змін була мінімальною? Просте послідовне вбудовування у найдешевші коефіцієнти не є оптимальним. Для вирішення цієї задачі використовується Syndrome Trellis Coding (STC) — потужний алгоритм, адаптований з теорії канального кодування.

Побудова решітки (Trellis): Алгоритм будує спеціальний граф, що нагадує решітку (trellis). Кожен стовпець цієї решітки відповідає одному потенційному

носію (коефіцієнту зображення). Кожен вузол у стовпці представляє певний стан процесу кодування. Ваги переходів: Перехід між вузлами у сусідніх стовпцях має "вартість" (weight), яка дорівнює значенню функції вартості ρ для цього носія, якщо для вбудовування біта потрібно змінити значення коефіцієнта. Якщо зміна не потрібна, вартість переходу дорівнює нулю.

Пошук оптимального шляху: Завдання STC-кодера — знайти такий шлях через всю решітку, який: Дозволяє закодувати (вбудувати) всі біти секретного повідомлення D. Мінімізує загальну суму вартостей всіх переходів, де відбулася зміна. Це еквівалентно мінімізації сумарного спотворення $D = \Sigma \rho_{i,j}$. Реалізація: Для знаходження такого шляху використовується модифікований алгоритм Вітербі (Viterbi algorithm), який ефективно знаходить глобально оптимальне рішення за поліноміальний час. Результат застосування STC: Система досягає теоретичної межі ефективності для заданої функції вартості. Навіть якщо повідомлення потрібно вбудувати у область з відносно високими середніми вартостями, STC гарантує, що це буде зроблено найдешевшим можливим способом, значно підвищуючи стійкість до стегоаналізу.

Вибір значення Q є критичним і визначає основний компроміс системи:

Великий крок Q: Дозволяє вбудувати більше даних (вища ємність або payload), оскільки зміна молодшого біта в q призводить до більшої абсолютної зміни x'. Однак це суттєво погіршує візуальну якість (знижує PSNR) та, що важливіше, зменшує статистичну стійкість. Великі модифікації легше виявити SRM-моделям. Малий крок Q: Забезпечує вищу візуальну та статистичну непомітність (вищий PSNR, нижча ймовірність виявлення P_D), оскільки внесені зміни мінімальні. Проте це різко обмежує ємність системи.

Вибір оптимального Q: Оптимальне значення кроку квантування Q не є універсальним. Воно підбирається емпірично під час етапу тестування та налаштування системи. Метою є знайти таке значення Q, при якому виконується головна вимога безпеки — імовірність виявлення $P_D \leq 0.55$ — при цьому

система здатна вмістити зашифроване повідомлення практичного обсягу разом із кодом автентифікації (HMAC). Це завдання вирішується шляхом моделювання атак стегоаналізу на репрезентативній вибірці зображень.

2.6. Методи вбудовування інформації в просторовій області

Методи простої заміни ґрунтуються на заміні найменш значущих бітів пікселів на біти прихованого повідомлення. Основним викликом є забезпечення статистичної невизначеності, оскільки різниця між модифікованими та немодифікованими ділянками може бути легко виявлена аналітичними методами.

Формула розрахунку ємності
Максимальна ємність контейнера визначається за формулою:

$$Q = H \times W \times V \times D \tag{2.2}$$

де:

1. H - висота зображення в пікселях
2. W - ширина зображення в пікселях
3. V - кількість кольорових компонент
4. D - кількість використовуваних найменш значущих бітів
5. Q - результуюча ємність у бітах

Розширені методи простої заміни Метод випадкового інтервалу
Передбачає псевдовипадковий розподіл бітів повідомлення по всьому зображенню з використанням криптографічно стійкого генератора. Це ускладнює статистичний аналіз і підвищує стійкість до виявлення. Блочне приховування
Алгоритм включає наступні етапи:

1. Розбиття зображення на непересічні блоки фіксованого розміру
2. Обчислення біта парності для кожного блоку

3. Порівняння з відповідним бітом повідомлення
4. Інвертування найменш значущого біта одного з пікселів блоку у разі невідповідності

Перевагою методу є мінімізація спотворень та можливість адаптації розміру блоку до конкретних вимог. Недолік - обмежена стійкість до геометричних перетворень. Використовує комбінаторні властивості палітри кольорів. Для палітри з N кольорами існує N! можливих перестановок, що дозволяє закодувати до $\log_2(N!)$ біт інформації шляхом відповідного впорядкування елементів палітри. Метод заміни палітри характеризується простотою реалізації, проте має суттєві обмеження:

1. Придатний лише для невеликих повідомлень
2. Низька стійкість до атак, пов'язаних з модифікацією палітри
3. Обмежена практична застосовність

Інноваційний підхід до приховування інформації в просторовій області, що використовує диференціальні характеристики яскравості.

Алгоритм реалізації:

1. Генерація псевдовипадкової маски розмірністю зображення
2. Розподіл зображення на блоки 8×8 пікселів
3. Поділ кожного блоку на дві підобласті B_1 та B_2
4. Обчислення середніх значень яскравості λ_1 та λ_2
5. Вбудовування біта повідомлення відповідно до умови:

$$S(x,y) = \{ 1, \text{при } \lambda_1 - \lambda_2 > 0, \text{при } \lambda_1 - \lambda_2 < -E \} \quad (2.3)$$

де:

E - порогове значення різниці яскравості.

У разі невиконання умови проводиться корекція значень яскравості λ_1 або λ_2. Процес вилучення передбачає обчислення різниці середніх значень яскравості для відновлення вбудованого біта.

Переваги:

1. Стійкість до стиснення JPEG з низькими коефіцієнтами
2. Збереження цілісності повідомлення при обробці

Недоліки:

1. Обмежена місткість
2. Ризик візуальних спотворень при великих значеннях порогу E

На відміну від методів простої заміни, частотні методи демонструють високу стійкість до стиснення з втратами. Найбільш поширеними ортогональними перетвореннями в стеганографії є:

1. Дискретне косинусне перетворення (ДКП)
2. Швидке перетворення Фур'є (ШПФ)
3. Вейвлет-перетворення

Вибір конкретного перетворення залежить від цільового формату стиснення: ДКП - для JPEG, вейвлети - для JPEG2000.

Найпоширеніший метод приховування в частотній області, що передбачає відносну заміну величин коефіцієнтів ДКП. Алгоритм включає:

1. Розподіл зображення на блоки ДКП
2. Вибір двох низькочастотних коефіцієнтів для порівняння
3. Модифікацію коефіцієнтів для кодування бітів повідомлення

Удосконалена версія методу Коха-Жао з такими особливостями:

1. Селективне вбудовування лише в придатні блоки

2. Використання трьох коефіцієнтів замість двох
3. Критерії відбору блоків:
    a. Відсутність різких переходів яскравості (обмеження P□)
    b. Відсутність надмірної монотонності (обмеження P□)

Процес вбудовування:

1. Кодування 0: третій коефіцієнт менший за перші два
2. Кодування 1: третій коефіцієнт перевищує перші два
3. Відхилення блоків із ризиком сильних спотворень

Гібридний підхід, що поєднує вбудовування в низькочастотні та середньочастотні коефіцієнти ДКП. Комбінація двох алгоритмів забезпечує:

1. Підвищену стійкість до стеганоатак
2. Кращу адаптацію до різних умов експлуатації
3. Збалансоване співвідношення місткість-стійкість

2.7. Порівняльний аналіз архітектурних підходів до крипто-стеганографії

У сучасних дослідженнях існує кілька принципових підходів до інтеграції криптографії та стеганографії. Розуміння їх відмінностей дозволяє обґрунтувати переваги обраної нами архітектури "Крипто-Адаптивне Стего".

Криптографія → Стеганографія (Encrypt-then-Embed)

Повідомлення спочатку шифрується, потім шифротекст приховується в контейнері. Саме цей підхід обрано в нашій роботі. Максимальна конфіденційність. Навіть при виявленні факту прихованої передачі зловмисник отримує лише шифротекст. Шифротекст має властивості випадкового шуму, що ідеально підходить для адаптивного вбудовування.

Стеганографія → Криптографія (Embed-then-Encrypt)

Повідомлення спочатку приховується в контейнері, потім весь стегоконтейнер (як файл) шифрується. Зовнішнє шифрування файлу може приховувати навіть тип контейнера. Не захищає від стегоаналізу. Стегоаналітик може спочатку дешифрувати файл (якщо має ключ або шифрування слабке), а потім аналізувати вже готовий стегоконтейнер. Також, саме шифрування файлу може привертати зайву увагу.

Одночасна обробка (Integrated)

Алгоритми шифрування та вбудовування об'єднані в єдиний процес (наприклад, використання криптографічних перетворень для безпосередньої модифікації коефіцієнтів контейнера). Потенційно вища ефективність. Висока складність аналізу безпеки, нестандартизованість, можлива взаємна компрометація компонентів.

Без криптографічного захисту навіть найдосконаліший стегометод має фундаментальні слабкості:

1. Вразливість до екстракції повідомлення: Якщо противник виявляє стегоконтейнер, він отримує відкритий текст повідомлення без додаткових перешкод. Це робить систему неефективною проти активного аналітика.
2. Наявність статистичних паттернів у повідомленні: Текстовий, графічний чи будь-який інший невипадковий вміст створює статистичні закономірності у вбудованому потоці бітів. Ці закономірності можуть бути виявлені просунутими методами машинного навчання, навіть якщо сам метод вбудовування адаптивний.
3. Відсутність цілісності та автентифікації: Система не може гарантувати, що вилучене повідомлення не було модифіковано під час передачі або самим отримувачем.

4. Шифрування вирішує ці проблеми комплексно: воно перетворює будь-яке повідомлення на випадковий потік (усуваючи паттерни), гарантує конфіденційність (навіть при виявленні) і в парі з HMAC забезпечує автентифікацію та цілісність.

Так само і шифрування без приховування має суттєві недоліки в контексті конфіденційної зв'язку:

1. Очевидність факту секретного зв'язку: Передача шифротексту (файлу, пакету) прямо вказує на те, що сторони щось приховують. Це може призвести до цензури, блокування або поглибленого аналізу трафіку.
2. Метадані та контекст: Навіть зашифрований канал зв'язку видає метадані: час, частоту, обсяг даних, IP-адреси сторін. Стеганографія дозволяє "заховати" факт зв'язку в звичайну, легальну активність (обмін фотографіями), маскуючи ці метадані.
3. Обхід протокольної цензури: Системи, що блокують або аналізують зашифрований трафік (DPI — Deep Packet Inspection), можуть блокувати самі протоколи шифрування. Стегоканал, використовуючи звичайний медіаконтейнер, часто проходить через такі фільтри непоміченим.
4. Адаптивна стеганографія в нашій системі виступає як "невидимий транспорт", який не лише приховує дані, але й активно протидіє спробам виявити сам факт їх передачі за допомогою статистичного аналізу контейнера.

2.8. Алгоритми стиснення зображень

Стиснення зображень є критично важливим аспектом сучасної обробки медіаданих. Усі алгоритми стиснення поділяються на дві основні категорії:

Втратні методи досягають високих коефіцієнтів стиснення шляхом видалення частини візуальної інформації, яка є менш важливою для людського сприйняття.

1. JPEG (Joint Photographic Experts Group): Найпоширеніший стандарт для стиснення фотографій та реалістичних зображень
2. JPEG 2000: Покращена версія з підтримкою вейвлет-перетворень
3. WebP: Сучасний формат від Google, що поєднує переваги JPEG та PNG
4. HEIC/HEIF: Формат на основі HEVC (H.265), що забезпечує кращу якість при тому ж розмірі

Безвтратне стиснення (Lossless Compression) Безвтратні методи зберігають усю вихідну інформацію без жодних втрат, забезпечуючи точне відтворення оригіналу.

1. PNG (Portable Network Graphics): Оптимальний для графіки з різкими межами та прозорістю
2. GIF (Graphics Interchange Format): Обмежений 256 кольорами, підтримує аніма
3. JPEG-компресія: Може повністю знищити приховані дані, особливо якщо вони розташовані у високочастотних областях
4. Втрата деталей: Видалення високочастотних компонентів призводить до втрати вбудованих бітів
5. Неможливість точного відновлення: Втрачена інформація не може бути відтворена

Спеціалізовані стеганографічні методи для JPEG

1. JSteg, F5, OutGuess: Методи, розроблені спеціально для JPEG-формату
2. Вбудовування в коефіцієнти DCT: Пряме маніпулювання квантованими коефіцієнтами

3. Обхід перекодування: Уникнення повторного стиснення з іншими параметрами

Переваги безвтратного стиснення для стеганографії

1. Збереження вбудованих даних: PNG та інші безвтратні формати зберігають всю інформацію
2. Можливість точного відновлення: Гарантія цілісності прихованого повідомлення
3. Широке застосування: Підтримка в більшості операційних систем та додатківцію
4. BMP (Bitmap): Мінімальне стиснення або відсутність стиснення
5. TIFF (Tagged Image File Format): Професійний формат з підтримкою різних алгоритмів стиснення

JPEG залишається основним стандартом для стиснення фотографій через свою ефективність та широку підтримку. Його робота базується на кількох ключових принципах:

1. Використання властивостей зорового сприйняття людини (HVS)
2. Людське око менш чутливе до високочастотних деталей та змін кольору
3. Можливість видаляти інформацію без помітної втрати якості
4. Різні рівні якості (quality factor) для контролю ступеня стиснення

Дискретне косинусне перетворення (DCT)

1. Перетворення блоків 8×8 пікселів у частотну область
2. Відділення низькочастотних (важливих) та високочастотних (менш важливих) компонент
3. Можливість селективного видалення високочастотних складових

Квантування та ентропійне кодування

1. Квантування коефіцієнтів DCT з різною точністю
2. Застосування зигзаг-сканування для ефективного представлення нульових коефіцієнтів
3. Використання алгоритмів Хаффмана чи арифметичного кодування

2.8.1. Метод JPEG 2000

JPEG 2000 — це стандарт стиснення зображень, розроблений Об'єднаною групою експертів з фотографії (Joint Photographic Experts Group) та офіційно затверджений у 2000 році. Він був створений як наступник класичного формату JPEG з метою подолання його обмежень та впровадження сучасних технологій компресії. На відміну від оригінального JPEG, що використовує дискретне косинусне перетворення (DCT), JPEG 2000 заснований на вейвлет-перетворенні, що забезпечує принципово інший підхід до обробки зображень. Основним компонентом JPEG 2000 є дискретне вейвлет-перетворення (DWT), яке аналізує зображення в багатомасштабному представленні. На відміну від DCT, що працює з блоками 8×8 пікселів, DWT обробляє зображення цілком, що усуває характерні блочні артефакти, притаманні класичному JPEG. Перетворення відбувається за допомогою фільтрів, які розділяють зображення на коефіцієнти низьких та високих частот на декількох рівнях декомпозиції, створюючи ієрархічну структуру, відому як багатороздільне представлення.

Після вейвлет-перетворення коефіцієнти піддаються квантуванню, але на відміну від JPEG, де квантування застосовується рівномірно, JPEG 2000 підтримує прогресивне квантування з різним ступенем точності для різних частотних піддіапазонів. Це дозволяє реалізувати розкладене за якістю кодування, де зображення може бути передане або відтворене частково з можливістю покращення якості по мірі отримання додаткових даних. Для подальшого стиснення JPEG 2000 використовує адаптивне біт-площинне кодування за допомогою алгоритму EBCOT (Embedded Block Coding with Optimal Truncation). Цей метод організовує коефіцієнти в незалежні блоки кодів, які можуть бути стиснуті та декодовані окремо, що забезпечує гнучкість у управлінні потоком

даних та дозволяє реалізувати просторове масштабування — можливість витягувати різні роздільні здатності з одного закодованого файлу.

Ключові переваги порівняно з JPEG

Покращена ефективність стиснення: JPEG 2000 забезпечує краще співвідношення якості до розміру файлу, особливо при високих коефіцієнтах стиснення. На низьких рівнях стиснення перевага менш помітна, але на високих рівнях JPEG 2000 демонструє значно меншу деградацію якості без появи блочних артефактів. Підтримка безвтратного стиснення: На відміну від JPEG, який є виключно втратним форматом, JPEG 2000 підтримує як втратне, так і безвтратне стиснення в межах одного стандарту. Безвтратний режим досягається за допомогою цілочисельних вейвлет-фільтрів, які гарантують точне відновлення оригінальних пікселів. Гнучкість формату: Стандарт підтримує глибину кольору до 16 біт на канал (проти 8 біт у JPEG), що робить його придатним для медичних зображень, наукових даних та високоякісних фотографій. Також передбачена підтримка транспарентності (альфа-канал) та вбудованих профілів кольору ICC. Стійкість до помилок передачі: Завдяки незалежному кодуванню блоків та вбудованим механізмам захисту, JPEG 2000 демонструє кращу стійкість до помилок при передачі по ненадійних каналах зв'язку. Пошкодження одного блоку даних не призводить до катастрофічного руйнування всього зображення. Незважаючи на технічні переваги, JPEG 2000 не здобув масового поширення в побутовій сфері. Основними причинами стали вищі обчислювальні вимоги для кодування та декодування порівняно з JPEG, проблеми з патентними ліцензіями на ранніх етапах розвитку, а також відсутність широкої підтримки в веб-браузерах та операційних системах.

Тим не менш, JPEG 2000 знайшов свою нішу в професійних та спеціалізованих галузях:

1. Медична візуалізація (DICOM): Стандарт для зберігання рентгенівських знімків, МРТ та КТ-сканів через підтримку безвтратного стиснення та високої глибини кольору
2. Кінематографія та відеоархіви: Використання в цифрових кінотеатрах (D-Cinema) та для архівації кінокартин
3. Дистанційне зондування Землі: Обробка супутникових та аерофотознімків
4. Музейні та бібліотечні цифрові колекції: Зберігання високоякісних репродукцій творів мистецтва

JPEG 2000 та стеганографія

З точки зору стеганографії, JPEG 2000 представляє особливий інтерес через свої унікальні характеристики. Вейвлет-представлення створює нові можливості для адаптивного вбудовування даних, оскільки дозволяє більш точно враховувати просторово-частотні характеристики зображення. Коефіцієнти вейвлет-перетворення можуть бути використані для більш ефективного приховування інформації в областях, менш важливих для візуального сприйняття. Однак прогресивна структура кодування та незалежність блоків ускладнюють розробку стеганографічних методів, оскільки зміни в одному блоці можуть вплинути на декодування інших частин зображення. Дослідження в цій галузі зосереджені на розробці алгоритмів, які враховують особливості EBCOT-кодування та зберігають сумісність з прогресивними режимами відтворення JPEG 2000. Хоча JPEG 2000 не замінив JPEG у повсякденному використанні, він залишається важливим стандартом у професійних сферах, де якість та гнучкість пріоритетніші за обчислювальну складність. Розвиток нових стандартів, таких як JPEG XL (який також використовує вейвлет-перетворення), демонструє, що ідеї, впроваджені в JPEG 2000, продовжують впливати на еволюцію алгоритмів стиснення зображень. У контексті стеганографії JPEG 2000 залишається цікавим об'єктом для досліджень через свою складну структуру, яка одночасно ускладнює аналіз та відкриває нові можливості для приховування інформації.

2.9. WebP

WebP — це сучасний формат стиснення зображень, розроблений компанією Google на основі технологій, придбаних разом із компанією On2 Technologies. Вперше анонсований у 2010 році, WebP був створений з метою забезпечення кращої ефективності стиснення порівняно з існуючими форматами, що мало призвести до прискорення завантаження веб-сторінок та економії трафіку. Формат поєднує в собі переваги як втратного, так і безвтратного стиснення, а також підтримує анімацію та прозорість. В основі формату WebP лежать технології, успадковані від відеокодека VP8, розробленого On2. Для втратного стиснення використовується прогнозне кодування, подібне до методів, застосовуваних у відеокомпресії. Замість традиційного перетворення блоків пікселів окремо, WebP спочатку намагається передбачити значення пікселів у блоці на основі вже закодованих сусідніх блоків. Залишкова інформація (різниця між прогнозом та фактичними значеннями) потім перетворюється за допомогою дискретного косинусного перетворення (DCT) або дискретного вейвлет-перетворення (DWT) залежно від режиму. Безвтратне стиснення в WebP реалізовано за допомогою алгоритмів, що включають адаптивне кодування за допомогою словників (LZ77-подібні методи) та ентропійне кодування Хаффмана. Цей підхід дозволяє досягати коефіцієнтів стиснення, які в середньому на 25-34% кращі за PNG при збереженні повної якості зображення. Окремою особливістю формату є підтримка анімації (WebP Animation), де кожен кадр може мати власні параметри стиснення (втратні або безвтратні), а також визначати тривалість відображення та методи композиції. Для анімованих зображень використовується контейнер на основі RIFF (Resource Interchange File Format), що дозволяє ефективно зберігати послідовність кадрів та їх метадані. Покращена ефективність стиснення: За даними Google, втратні WebP-зображення зазвичай мають розмір на 25-35% менший, ніж JPEG-файли еквівалентної якості. Безвтратні WebP-зображення перевершують PNG у середньому на 26% за ефективністю стиснення. Це досягається за рахунок більш просунутих алгоритмів прогнозування та

адаптивного вибору методів кодування. Підтримка прозорості (альфа-канал): На відміну від JPEG, який не підтримує прозорість, WebP забезпечує 8-бітний альфа-канал як для статичних, так і для анімованих зображень. Це робить його функціональною альтернативою PNG та GIF для графіки з прозорими ділянками. Можливість анімації: WebP підтримує анімовані зображення, що дозволяє замінити формат GIF. Анімовані WebP-файли зазвичай мають значно менший розмір порівняно з GIF завдяки використанню більш ефективних методів стиснення та підтримці 24-бітного кольору (проти обмеження в 256 кольорів у GIF). Розширені можливості кольорового простору: Формат підтримує колірні профілі ICC та вбудовані метадані EXIF/XMP, що робить його придатним для професійної обробки фотографій. Також є підтримка HDR-кольорів через профілі PQ та HLG. Незважаючи на технічні переваги, WebP має певні обмеження. Складність декодування дещо вища порівняно з JPEG, що може призводити до збільшення часу обробки на слабких пристроях. Історично основним бар'єром для широкого впровадження була обмежена підтримка в браузерах, проте станом на 2023 рік WebP підтримується всіма основними веб-браузерами, включаючи Chrome, Firefox, Safari та Edge. Сумісність зі старим програмним забезпеченням залишається проблемою, оскільки багато десктопних додатків та операційних систем не мають вбудованої підтримки формату. Для перегляду та редагування WebP часто потрібне встановлення додаткових кодеків або плагінів. На практиці WebP найбільш активно використовується в веб-розробці, де він дозволяє значно прискорити завантаження сторінок. Багато сучасних систем управління контентом (CMS) автоматично конвертують завантажені зображення у WebP для веб-версій сайтів. Також формат популярний у мобільних додатках, де економія трафіку та швидкість завантаження є критично важливими. Стеганографічні методи для WebP знаходяться на ранній стадії досліджень через відносну новизну формату та його складну внутрішню структуру. Гібридна природа стиснення (прогнозне кодування + DCT/DWT) створює як нові можливості, так і виклики для приховування даних.

Переваги для стеганографії:

1. Прогнозне кодування створює додаткові можливості для вбудовування даних у вектори прогнозування або різницеві коефіцієнти
2. Підтримка безвтратного стиснення дозволяє реалізувати методи, що не впливають на якість зображення
3. Складна структура контейнера RIFF надає додаткові можливості для приховування даних у метаданих анімованих послідовностей

Складності та виклики:

1. Адаптивний вибір методів кодування ускладнює розробку універсальних стеганографічних алгоритмів
2. Висока ефективність стиснення може призводити до більш помітних артефактів при вбудовуванні даних
3. Обмежена доступність інструментів аналізу порівняно з більш дослідженими форматами на кшталт JPEG

Перспективним напрямом досліджень є розробка адаптивних методів вбудовування, які враховують особливості прогнозного кодування та можуть динамічно обирати оптимальні області для модифікації залежно від конкретного режиму стиснення WebP. Google продовжує розвивати формат WebP, додаючи нові функції та оптимізуючи алгоритми стиснення. У 2021 році був представлений формат AVIF (AV1 Image File Format), який базується на ще більш сучасному відеокодеку AV1 і пропонує додаткове покращення ефективності стиснення. Незважаючи на появу конкурентів, WebP залишається практичним вибором через свою широку підтримку та збалансовані характеристики. У контексті веб-розробки WebP став де-факто стандартом для ефективної доставки зображень, а його роль у стеганографії, ймовірно, буде зростати у міру поширення формату та появи більш спеціалізованих інструментів для його аналізу та обробки. Розуміння внутрішньої структури WebP є важливим для розробників стеганографічних систем, які прагнуть створювати методи, стійкі до сучасних форматів стиснення.

2.10. HEIC/HEIF

HEIC/HEIF — це сучасний формат контейнера та метод стиснення зображень, заснований на технологіях відеокодека HEVC (High Efficiency Video Coding, також відомий як H.265). Формат був стандартизований Рухомою групою експертів з кінематографії (MPEG) у 2015 році як частина стандарту MPEG-H Part 12. На відміну від традиційних форматів, що зосереджені на окремих зображеннях, HEIF (High Efficiency Image File Format) є універсальним контейнером, здатним зберігати послідовності зображень, анімації, глибину глибини та інші типи медіаданих, тоді як HEIC (High Efficiency Image Container) — це конкретна реалізація цього стандарту, яка використовує стиснення HEVC. В основі HEIF лежить концепція контейнера ISOBMFF (ISO Base Media File Format), який також використовується для відеоформатів MP4. Ця архітектура дозволяє зберігати зображення не як монолітні файли, а як структуровані колекції об'єктів з метаданими. Кожне зображення або послідовність зображень представлені як "item" у контейнері, що дозволяє ефективно керувати версіями, альтернативними представленнями та зв'язками між різними типами даних. Стиснення зображень у HEIC здійснюється за допомогою кодеку HEVC, який використовує складні алгоритми прогнозування та перетворення. На відміну від JPEG, де застосовується DCT для блоків 8×8, HEVC використовує квадратне та прямокутне розбиття на блоки розміром від 4×4 до 64×64 пікселів, що дозволяє краще адаптуватися до локальних особливостей зображення. Для перетворення застосовується дискретне косинусне перетворення (DCT) або дискретне синусне перетворення (DST) залежно від типу блоку та його вмісту. Ключовою особливістю HEVC у контексті стиснення зображень є використання внутрішньокадрового прогнозування. Для кожного блоку зображення алгоритм намагається передбачити його вміст на основі вже закодованих сусідніх блоків. Прогноз може бути просторовим (використання значень пікселів зверху та зліва) або частотним (на основі

перетворених коефіцієнтів). Це дозволяє значно зменшити надмірність даних, особливо в однорідних областях зображення.

Основні переваги порівняно з JPEG

Висока ефективність стиснення: HEIC забезпечує вдвічі краще стиснення при тій самій якості порівняно з JPEG. На практиці це означає, що файл HEIC зазвичай має розмір на 40-50% менший, ніж JPEG-файл з еквівалентною візуальною якістю. Ця ефективність досягається за рахунок складніших алгоритмів прогнозування та адаптивного розбиття на блоки.Підтримка глибини кольору: HEIC підтримує до 16 біт на канал (глибина кольору 48 біт), що робить його придатним для професійної фотографії, HDR-зображень та медичної візуалізації. Формат також підтримує різні колірні простори, включаючи sRGB, Adobe RGB, P3 та Rec. 2020.Розширені функції контейнера: HEIF може зберігати послідовності зображень у одному файлі, що дозволяє створювати "живі фотографії" (Live Photos), анімації та панорами. Контейнер також підтримує глибину глибини (depth maps), яка використовується для ефектів портретного режиму та AR-додатків, а також прозорість (альфа-канал) та незалежні шари для складної графіки.Недіструктивне редагування: Завдяки структурі контейнера, HEIF дозволяє здійснювати недеструктивні зміни зображення, такі як обрізання, повороти та корекції кольору, без перекодування всього файлу. Зміни зберігаються як окремі елементи метаданих, а оригінальні дані залишаються недоторканими.

Незважаючи на технічні переваги, HEIC/HEIF має значні обмеження у практичному використанні:

1. Патентні питання: HEVC захищений численними патентами, що ускладнює його безкоштовне використання. Необхідність ліцензування сповільнила широке впровадження формату та стимулювала розвиток альтернативних безпатентних форматів, таких як AVIF.

2. Обчислювальна складність: Кодування та декодування HEIC потребує значно більших обчислювальних ресурсів порівняно з JPEG. Це обмежує використання формату на старих пристроях та збільшує час обробки.
3. Обмежена підтримка платформ: Станом на 2023 рік рідна підтримка HEIC реалізована в iOS та macOS (починаючи з версій 11 та High Sierra відповідно), а також у деяких версіях Windows 10 та 11. Однак підтримка в Android, Linux та веб-браузерах залишається обмеженою, що ускладнює обмін файлами між різними платформами.

HEIC отримав найширше розповсюдження в екосистемі Apple, де він є стандартним форматом для фотографій на пристроях iPhone та iPad починаючи з 2017 року. Це дозволило Apple значно зменшити розмір фотобібліотек користувачів без втрати якості.У професійній фотографії HEIC використовується як проміжний формат для зберігання RAW-даних з додатковою обробкою. Деякі камери почали підтримувати захоплення безпосередньо у HEIC, хоча RAW-формати залишаються основним вибором для критично важливих завдань. Медична візуалізація починає переходити на HEIC через його здатність ефективно стискати зображення високої глибини кольору. Формат розглядається як потенційна заміна традиційним медичним форматам у деяких застосуваннях.

Для стеганографії HEIC/HEIF представляє особливий інтерес через свою складну структуру:

1. Багатошарові можливості: Контейнерна природа HEIF дозволяє приховувати дані не лише в піксельній інформації, але й у метаданих, глибині глибини, альфа-каналах та альтернативних представленнях зображення. Це відкриває нові виміри для приховування інформації.
2. Прогнозне кодування HEVC: Алгоритми внутрішньокадрового прогнозування створюють унікальні можливості для вбудовування даних у вектори прогнозування, режими розбиття блоків та різницеві коефіцієнти.

Ці області менш досліджені в стеганографії порівняно з традиційними DCT-коефіцієнтами.

3. Складність аналізу: Багаторівнева структура контейнера та складність алгоритмів HEVC роблять аналіз стегоконтейнерів більш складним завданням. Стегоаналітикам необхідно розуміти не лише методи стиснення, але й структуру ISOBMFF-контейнера.

Основні напрями досліджень у стеганографії для HEIC:

1. Вбудовування в предиктивні моделі: Використання векторів прогнозування HEVC для приховування даних
2. Маніпуляції з розбиттям блоків: Зміна способу розбиття зображення на блоки для кодування додаткової інформації
3. Використання альтернативних представлень: Приховування даних у додаткових версіях зображення (наприклад, preview images)
4. Стеганографія в метаданих: Використання розширених полів метаданих контейнера ISOBMFF

Майбутнє HEIC/HEIF знаходиться під питанням через конкуренцію з боку AVIF — безпатентного формату на основі кодеку AV1. AVIF пропонує подібні або кращі характеристики стиснення без проблем ліцензування, що робить його привабливішим для розробників відкритого програмного забезпечення та веб-стандартів. Однак HEIC, ймовірно, збереже свої позиції в екосистемах Apple та деяких професійних додатках, де інвестиції в інфраструктуру вже здійснені. Розвиток форматів, що базуються на HEVC, триває — зокрема, стандарт VVC (Versatile Video Coding, H.266) може стати основою для наступного покоління форматів зображень. Для дослідників стеганографії HEIC залишається цікавим полем для експериментів через свою технічну складність та багатофункціональність. Розуміння принципів роботи HEVC та структури ISOBMFF-контейнера є важливим для розробки методів, здатних ефективно

використовувати унікальні можливості цього формату для приховування інформації.

ВИСНОВКИ ДО РОЗДІЛУ 2

У другому розділі проведено комплексний аналіз теоретичних основ комп'ютерної стеганографії та детально досліджено методи приховування інформації в растрових зображеннях. Основні досягнення:

1. Систематизовано основні формати зображень та їх характеристики
2. Проаналізовано спектр методів стеганографічного запису
3. Обґрунтовано вибір методу LSB для подальшого дослідження
4. Детально розглянуто принцип роботи та модифікації LSB

Метод LSB ґрунтується на заміні найменш значущих бітів контейнера на біти прихованого повідомлення. Критерієм ефективності є непомітність змін для органів чуття людини, що досягається завдяки обмеженій чутливості людського зору до незначних кольорових варіацій.Обраний метод LSB у поєднанні з форматом BMP створює основу для розробки вдосконалених алгоритмів стеганографії, спрямованих на підвищення стійкості та скритності приховування інформації.

3 РОЗРОБКА АЛГОРИТМУ РОЗВ'ЯЗАННЯ ЗАДАЧІ

3.1. Змістовна постановка задачі

Сучасний інформаційний простір характеризується широкою доступністю стеганографічного програмного забезпечення, що дозволяє приховувати конфіденційні дані в мультимедійних контейнерах. Хоча легальне використання таких технологій має правомірні цілі, існує значний ризик їх застосування для протиправної діяльності через непомітність передачі даних.

Ключова проблема: Ефективне виявлення факту приховування інформації у цифрових контейнерах.

Обмеження існуючих методів стеганоаналізу:

1. Метод χ^2-критерію ефективний лише для послідовного вбудовування LSB
2. Неспроможність виявлення псевдовипадкового розподілу вбудованих бітів
3. Відсутність універсального методу для різних форматів та алгоритмів

Додаткова проблема безпеки:
Збільшення обсягу вбудованих даних підвищує ймовірність виявлення. При перехопленні "переповненого" контейнера зловмисник може легко виділити повідомлення.

Основне завдання дослідження: Розробити алгоритм, що дозволяє вбудовувати значні обсяги інформації в контейнер, забезпечуючи навіть у разі перехоплення неможливість відновлення початкового повідомлення зловмисником.

3.2. Математична модель типової стеганосистеми

- M — множина відкритих повідомлень, де $m \in M$ є конкретним повідомленням

- C — множина цифрових контейнерів, де $c \in C$ є оригінальним контейнером (наприклад, зображенням)
- KE — простір криптографічних ключів, де $ke \in KE$
- KS — простір стеганографічних ключів, де $ks \in KS$
- CE — множина шифротекстів, де $ce \in CE$
- CS — множина стеганооб'єктів, де $cs \in CS$

2. Формалізація основних операцій

Криптографічне перетворення визначається як оператор:

$$E: M \times KE \rightarrow CE \tag{3.1}$$

де:

$E(m,ke)=ce$— функція шифрування, яка перетворює відкрите повідомлення

m у шифротекст ce з використанням ключа ke .

Стеганографічне приховування визначається як оператор:

$$S: CE \times C \times KS \rightarrow CS \tag{3.2}$$

де:
$S(ce,c,ks)=cs$— функція вбудовування, яка приховує шифротекст ce у контейнері c з використанням стеганографічного ключа ks.

3. Інтегрована комбінована модель

Комбінований оператор приховування визначається як композиція криптографічного та стеганографічного перетворень:

$$P: M \times KE \times C \times KS \rightarrow CS \tag{3.3}$$

$$cs = P(m,ke,c,ks) = S(E(m,ke),c,ks) \tag{3.4}$$

де:

- m — відкрите повідомлення

- *ke* — криптографічний ключ
- *c* — оригінальний контейнер
- *ks* — стеганографічний ключ
- *cs* — результуючий стеганооб'єкт

4. Процес відновлення повідомлення

Для відновлення оригінального повідомлення виконуються обернені операції:

Оператор вилучення стеганографічних даних:

$$S^{-1}:CS\times KS\rightarrow CE \tag{3.5}$$

де:
$S^{-1}(cs,ks)=ce$ — функція вилучення шифротексту з стеганооб'єкта.

Оператор дешифрування:

$$E^{-1}:CE\times KE\rightarrow M \tag{3.6}$$

де:
$E^{-1}(ce,ke)=m$— функція дешифрування, яка відновлює оригінальне повідомлення.

Таким чином, повний процес відновлення описується як:

$$m=E^{-1}(S^{-1}(cs,ks),ke) \tag{3.7}$$

5. Властивості моделі

Запропонована математична модель забезпечує:

- Детермінованість: $E^{-1}(E(m,ke),ke)=m$ та $S^{-1}(S(ce,c,ks),ks)=ce$
- Коректність: $E^{-1}(S^{-1}(P(m,ke,c,ks),ks),ke)=m$
- Стійкість: модель передбачає властивості криптографічної стійкості та стеганографічної непомітності

Дана модель є теоретичною основою для практичної реалізації комбінованого методу захисту інформації та дозволяє формально аналізувати його властивості та безпеку.

Формальне представлення стеганосистеми базується на п'ятірці об'єктів:

$$\Sigma(C, M, S, E, D) \quad (3.8)$$

де:

- C - множина контейнерів
- M - множина повідомлень
- S - множина стеганограм (заповнених контейнерів)
- E - функція вбудовування
- D - функція вилучення

Функціональні залежності:

- Вбудовування: $E: C \times M \rightarrow S$ (3.1)
- Вилучення: $D: S \rightarrow M$ (3.2)

3.3. Метод найменш значущого біту

Метод найменш значущого біту (Least Significant Bit, LSB) — це один з найстаріших і найпростіших методів стеганографії, що полягає в заміні найменш значущих бітів у цифрових даних (зображеннях, аудіофайлах, відео) на біти секретного повідомлення. Вперше цей метод став широко відомий у 1990-х роках з розповсюдженням цифрових медіаформатів, хоча подібні ідеї використовувалися ще в аналоговій епохі. LSB залишається базовим алгоритмом для вивчення принципів стеганографії, незважаючи на свою вразливість до сучасних методів детектування.Технічно метод ґрунтується на тому, що зміна найменш значущого біту в числовому представленні пікселя, аудіосемпла або іншого елементу даних викликає мінімальне спотворення, яке практично не сприймається людськими органами чуття. У випадку зображень у форматі RGB, де кожен піксель представлений трьома байтами (червоний, зелений, синій компоненти), заміна

молодшого біта в кожному байті дозволяє приховати три біти інформації на піксель без помітної зміни кольору.

Стандартний алгоритм включає наступні кроки:

1. Перетворення секретного повідомлення в двійкову форму
2. Послідовний обхід пікселів зображення-контейнера
3. Заміна молодшого біта в одному або кількох кольорових каналах на біти повідомлення
4. Збереження модифікованого зображення

Ємність методу залежить від глибини кольору зображення та кількості використовуваних каналів. Для 24-бітного зображення RGB з заміною LSB у всіх трьох каналах можна приховати 3 біти на піксель. Для зображення розміром 800×600 пікселів це дозволяє приховати приблизно 180 000 байтів даних.

З часом з'явилися численні модифікації базового LSB-методу, спрямовані на підвищення стійкості до виявлення:

1. Послідовне та випадкове вбудовування: замість лінійного обходу пікселів використовуються псевдовипадкові послідовності, що ускладнює відновлення повідомлення без знання ключа
2. Адаптивне вбудовування: врахування властивостей окремих ділянок зображення, наприклад, уникання рівномірних областей, де зміни більш помітні
3. LSB з підвіскою: вбудовування не в один, а в кілька молодших бітів, що збільшує ємність, але знижує якість
4. Кореляція сусідніх пікселів: методи, що враховують взаємозв'язок між сусідніми пікселями для більш природного розподілу змін

Переваги та недоліки

Основні переваги LSB включають:

1. Простоту реалізації та розуміння
2. Високу ємність приховування
3. Мінімальне спотворення вихідного контейнера
4. Широку застосовність до різних типів цифрових даних

Критичні недоліки методу:

1. Вразливість до найпростіших статистичних атак
2. Низька стійкість до навіть незначних трансформацій зображення (стиснення, масштабування, кольорової корекції)
3. Легкість виявлення за допомогою стандартних стегоаналітичних інструментів
4. Неможливість використання з втратними форматами стиснення (JPEG тощо)

Методи виявлення LSB-вбудовування

Через свою простоту та передбачуваність LSB-метод вразливий до численних атак:

1. Хі-квадрат тест (χ^2-тест): класичний метод, що виявляє аномалії в розподілі значень пар сусідніх інтенсивностей пікселів
2. RS-аналіз: метод, що використовує статистику регулярних і сингулярних груп пікселів
3. Аналіз гістограм: виявлення характерних зламів у гістограмі розподілу інтенсивностей
4. Методи на основі машинного навчання: нейромережі, навчені розпізнавати мікропаттерни, характерні для LSB-модифікацій

Сучасні інструменти стегоаналізу, такі як StegExpose, StegDetect або відкриті бібліотеки на кшталт StegLib, можуть виявляти навіть просунуті варіації LSB-вбудовування з високою точністю.

Незважаючи на свою вразливість, LSB-метод мав історичне значення та продовжує використовуватися в певних контекстах:

1. Навчальні цілі: як вступний метод для вивчення принципів стеганографії
2. Швидке прототипування: для тестування інших компонентів стеганографічних систем
3. Контексти з низькими вимогами до безпеки: де потреба в простоті переважує вимоги до стійкості
4. Ранні цифрові системи: в 1990-х — початку 2000-х, коли методи детектування були менш розвиненими

Один з найвідоміших історичних випадків пов'язаний з терористичною організацією "Аль-Каїда", яка, за даними розслідувань, використовувала LSB-метод для приховування повідомлень у зображеннях на публічних веб-форумах на початку 2000-х років. У сучасних дослідженнях LSB розглядається переважно як історичний метод та базовий порівняльний стандарт. Більшість сучасних наукових публікацій зі стеганографії використовують LSB як точку відліку для демонстрації переваг нових, більш складних алгоритмів.

Сучасні альтернативи включають:

1. Адаптивні методи в частотній області (DCT, DWT)
2. Методи, стійкі до стиснення (JPEG-стеганографія)
3. Стеганографія на основі синтаксису для текстових даних
4. Методи з використанням машинного навчання для оптимізації вбудовування

Тим не менш, принципи, закладені в LSB — мінімізація спотворень, використання надмірності даних, незамітність змін – залишаються фундаментальними для всієї галузі стеганографії. Дослідження в області LSB продовжуються в напрямку створення гібридних методів, що поєднують простоту LSB зі стійкістю більш складних алгоритмів, а також розробки нових методів для специфічних типів даних або умов застосування.

3.4. Метод стеганоаналізу «Хі-квадрат»

Метод стеганоаналізу «Хі-квадрат» (χ^2-тест) — це класичний статистичний метод виявлення прихованих даних у цифрових зображеннях, який став одним з перших ефективних інструментів для боротьби з LSB-стеганографією. Розроблений Андреасом Вестфельдом і Гердом Пфітцманом на початку 2000-х років, цей метод заснований на аналізі розподілу пар сусідніх інтенсивностей пікселів і є особливо ефективним для виявлення вбудовування за методом найменш значущого біта (LSB).

Метод ґрунтується на ключовому спостереженні: при LSB-вбудовуванні відбувається характерне порушення статистичного розподілу значень пікселів. Зокрема, коли дані вбудовуються шляхом заміни молодших бітів, значення пар сусідніх інтенсивностей (наприклад, 2i і 2i+1) стають ближчими один до одного, ніж це можна було б очікувати в природному зображенні. Математичний принцип полягає в тому, що для кожного можливого значення інтенсивності пікселя (від 0 до 255 для 8-бітних зображень) визначаються пари значень, що відрізняються лише в молодшому біті. Ці пари називаються "po" (парні) та "pe" (непарні) значення. У незміненому зображенні розподіл цих пар приблизно рівномірний, тоді як при LSB-вбудовуванні їх співвідношення порушується.

Реалізація χ^2-тесту включає наступні кроки:

1. Побудова гістограми зображення: Обчислення частоти появи кожного значення інтенсивності пікселів від 0 до 255.
2. Формування пар значень: Об'єднання частот для пар значень, які відрізняються лише молодшим бітом (наприклад, 0 і 1, 2 і 3, ..., 254 і 255).
3. Обчислення спостережуваних та очікуваних частот: Для кожної пари (2i, 2i+1) визначаються

4. Визначення p-значення: Обчислення ймовірності спостережуваного розподілу за умови, що нульова гіпотеза (відсутність вбудованих даних) є вірною.
5. Інтерпретація результату: Якщо p-значення близьке до 1, це вказує на високу ймовірність наявності LSB-вбудовування. Якщо p-значення близьке до 0 — зображення, ймовірно, не містить прихованих даних.

Ефективність та обмеження

Сильні сторони χ^2-тесту:

1. Висока ефективність для виявлення повного або високого заповнення LSB
2. Швидкість обчислення та простота реалізації
3. Здатність оцінювати приблизний обсяг вбудованих даних
4. Незалежність від конкретного алгоритму LSB-вбудовування (послідовного, випадкового тощо)

Обмеження методу:

1. Низька ефективність для незначного заповнення LSB (менше 5-10%)
2. Вразливість до адаптивних LSB-методів, що уникають рівномірних областей
3. Неефективність для частотних методів стеганографії (DCT, DWT)
4. Залежність від якості зображення та його статистичних властивостей
5. Можливість помилкових спрацьовувань на сильно текстурованих зображеннях

Практичне застосування

На практиці χ^2-тест найчастіше використовується як частина комплексних систем стеганоаналізу. Типові сценарії застосування:

1. Попереднє скринінгування: Швидка перевірка великих масивів зображень на наявність очевидних LSB-вбудовувань.
2. Експертний аналіз: У поєднанні з іншими методами (RS-аналіз, аналіз гістограм, методи машинного навчання).
3. Оцінка рівня заповнення: Визначення приблизного відсотка використаних LSB при виявленні вбудовування.
4. Навчальні цілі: Демонстрація базових принципів статистичного стеганоаналізу.

Сучасні стеганографічні методи розвинули способи протидії χ^2-тесту:

1. Адаптивне вбудовування: Вибіркове вбудовування лише в текстуровані області зображення, де статистичні аномалії менш помітні.
2. Вбудовування в декілька бітів: Замість одного молодшого біта використання двох або більше молодших бітів, що ускладнює аналіз пар значень.
3. Попередня обробка даних: Використання шифрування або компресії перед вбудовуванням, що робить розподіл вбудованих бітів більш рівномірним.
4. Використання частотних областей: Перехід від просторової області (LSB) до частотних перетворень (DCT, DWT), де χ^2-тест неефективний.

Метод χ^2-тесту мав революційне значення для розвитку стеганоаналізу на початку 2000-х років. Він продемонстрував, що навіть такі прості методи, як LSB, можуть бути ефективно виявлені за допомогою статистичного аналізу. Це стимулювало розвиток більш складних методів стеганографії та, відповідно, більш просунутих методів їх виявлення.

У сучасному контексті χ^2-тест залишається цінним інструментом, але переважно для:

1. Виявлення аматорських або застарілих стеганографічних систем
2. Навчальних демонстрацій принципів стеганоаналізу
3. Як базовий компонент у комбінованих системах аналізу

4. Для швидкої оцінки великих наборів даних

Більшість сучасних досліджень зосереджені на методах машинного навчання (згорткові нейронні мережі, автоматизовані feature engineering), які демонструють значно вищу ефективність для виявлення складних адаптивних методів стеганографії. Однак принципи, закладені в χ^2-тесті — аналіз статистичних аномалій, порівняння спостережуваних і очікуваних розподілів — залишаються фундаментальними для всієї галузі цифрового стеганоаналізу.

Практична реалізація

Стандартна реалізація χ^2-тесту доступна в більшості бібліотек для стеганоаналізу, таких як:

1. StegExpose (Java)
2. StegDetect (C)
3. Python-бібліотеки (stegano, pillow з додатковими модулями)
4. MATLAB з пакетами обробки зображень

Типова точність методу становить 85-95% для повного LSB-заповнення, але падає до 50-60% для заповнення менше 20%. Час аналізу для стандартного зображення розміром 1024×768 пікселів на сучасному обладнанні становить менше 100 мілісекунд.

3.5 Засоби розробки

Для реалізації програмного комплексу було обрано мову програмування Python версії 3.8+. Вибір зумовлений потужною екосистемою бібліотек для обробки зображень, криптографії та наукових досліджень.

Основні бібліотеки:

1. OpenCV (cv2) - комп'ютерний зір та обробка зображень
2. Pillow (PIL) - робота з графічними форматами

3. NumPy - наукові обчислення та робота з матрицями
4. Cryptography - криптографічні алгоритми
5. PyCryptodome - додаткові функції безпеки
6. Scikit-image - алгоритми обробки зображень

Архітектура системи

Модульна структура:

1. Модуль шифрування - відповідає за криптографічне перетворення даних
2. Модуль стеганографії - реалізує методи приховування інформації
3. Модуль аналізу - забезпечує перевірку стійкості системи
4. Графічний інтерфейс - забезпечує взаємодію з користувачем

Продуктивність розробки:

Інтерпретована природа мови дозволяє швидко ітераціювати та експериментувати з алгоритмами. Інтерактивний режим роботи забезпечує негайне тестування ідей.

Багата екосистема:

Велика кількість спеціалізованих бібліотек для обробки зображень та криптографії значно прискорює процес розробки. Наявність готових реалізацій алгоритмів дозволяє зосередитись на вдосконаленні методів.

Крос-платформеність:

Система однаково ефективно працює на Windows, Linux та macOS, що забезпечує широке коло потенційних користувачів.

Контролер

Відповідає за координацію між користувацьким інтерфейсом та функціональними модулями. Обробляє вхідні дані, керує потоком виконання програми та забезпечує цілісність обробки інформації.

Подання

Графічний інтерфейс реалізований з використанням сучасних бібліотек.

Забезпечує зручну взаємодію з користувачем, візуалізацію результатів та інтуїтивне керування параметрами алгоритмів.

Модель

Містить бізнес-логіку програми, включаючи алгоритми шифрування, методи стеганографічного приховування та функції аналізу безпеки. Кожен компонент може бути легко модифікований або замінений.

Ефективність обробки:

Використання векторних операцій NumPy забезпечує високу швидкість роботи з великими зображеннями. Оптимізовані алгоритми мінімізують використання пам'яті.

Безпека системи:

Застосування перевірених криптографічних бібліотек гарантує надійність шифрування. Реалізовано захист від типових атак на стеганографічні системи.

Гнучкість та розширюваність:

Модульна архітектура дозволяє легко інтегрувати нові алгоритми шифрування та методи приховування. Система підтримує різні формати зображень і може бути інтегрована з зовнішніми сервісами.

3.6 Вимоги до технічного забезпечення

Для коректної роботи програмного комплексу необхідне наступне технічне та програмне забезпечення.

Мінімальна конфігурація:

1. Процесор з тактовою частотою 1 ГГц
2. Вільний дисковий простір 40 ГБ
3. Оперативна пам'ять 512 МБ

4. Стандартна графічна система

Рекомендована конфігурація:

1. Процесор з тактовою частотою 2 ГГц та вище
2. Вільний дисковий простір 100 ГБ
3. Оперативна пам'ять 2 ГБ та більше
4. Сучасна графічна система з підтримкою прискорення

Програмне забезпечення

Обов'язкові компоненти:

1. Операційна система Windows 7/8/10/11 або Linux Ubuntu 18.04+
2. Інтерпретатор Python версії 3.8 або вище
3. Бібліотеки: OpenCV, Pillow, NumPy, Cryptography

Додаткове програмне забезпечення:

1. Система керування базами даних SQLite (входить до складу Python)
2. Графічні драйвери останніх версій
3. Браузер для перегляду документації

Периферійні пристрої

Обов'язкові пристрої:

1. Монітор з роздільною здатністю 1024×768 пікселів
2. Клавіатура для введення даних
3. Маніпулятор типу "миша"

Додаткові пристрої:

1. Принтер для виводу звітів
2. Мережевий адаптер для мережевого функціоналу
3. Зовнішній носій даних для експорту результатів

Архітектура системи

Інтерфейсний рівень:
Реалізовано за допомогою графічної бібліотеки Tkinter, що забезпечує крос-платформений інтерфейс користувача. Інтерфейс включає елементи для вибору файлів, налаштування параметрів шифрування та відображення результатів обробки.

Системні вимоги:
Програмний комплекс оптимізовано для роботи в стандартних умовах та не вимагає додаткового апаратного прискорення. Модульна архітектура дозволяє адаптувати систему під різні конфігурації обладнання.

3.7. Опис програми

Програма для шифрування даних зображена на Рис.3.1.

1. вибрати фото для шифрування;
2. написати ключі;
3. поле для виведення зашифрованого повідомлення;
4. кодувати фбо декодувати повідомлення ;

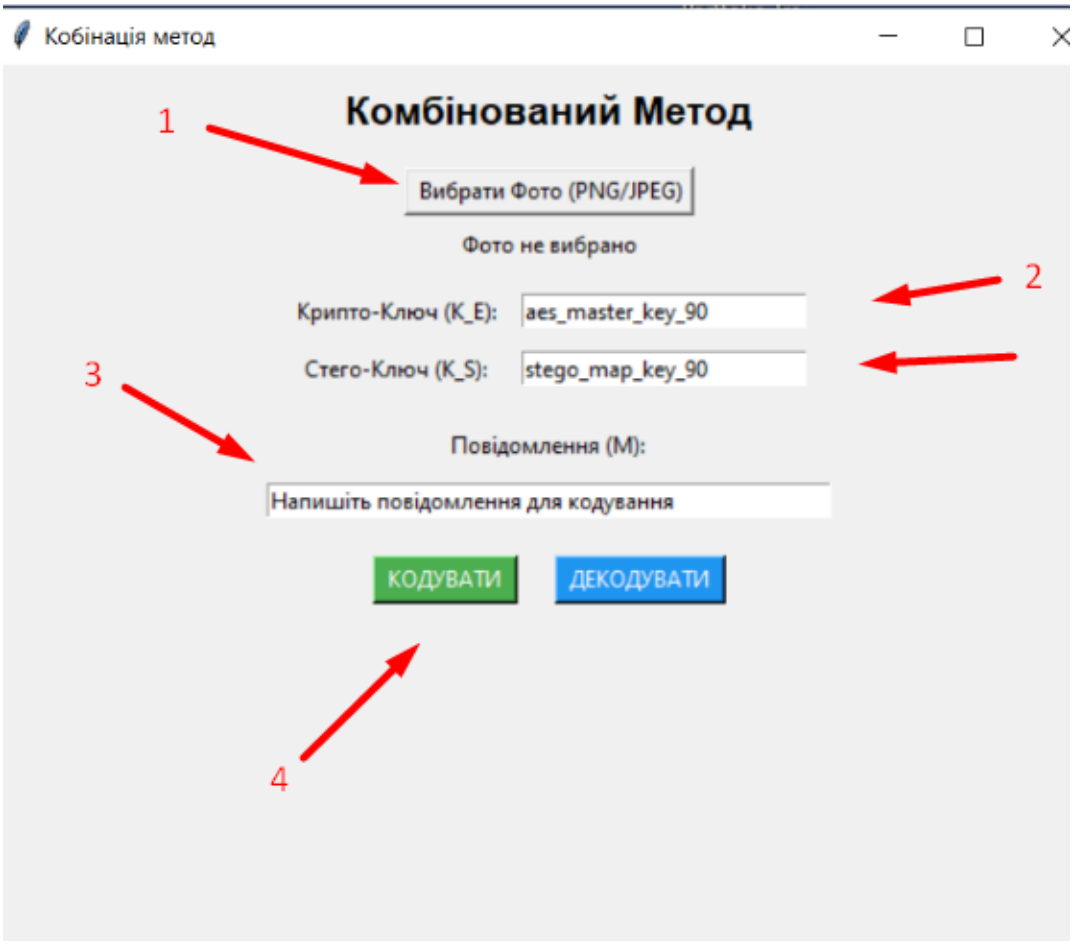


Рис. 3.1 Головне вікно програми шифрування даних

3.8 Інструкція з експлуатації

Після відкриття програми вибираємо фото в яке будемо шифрувати

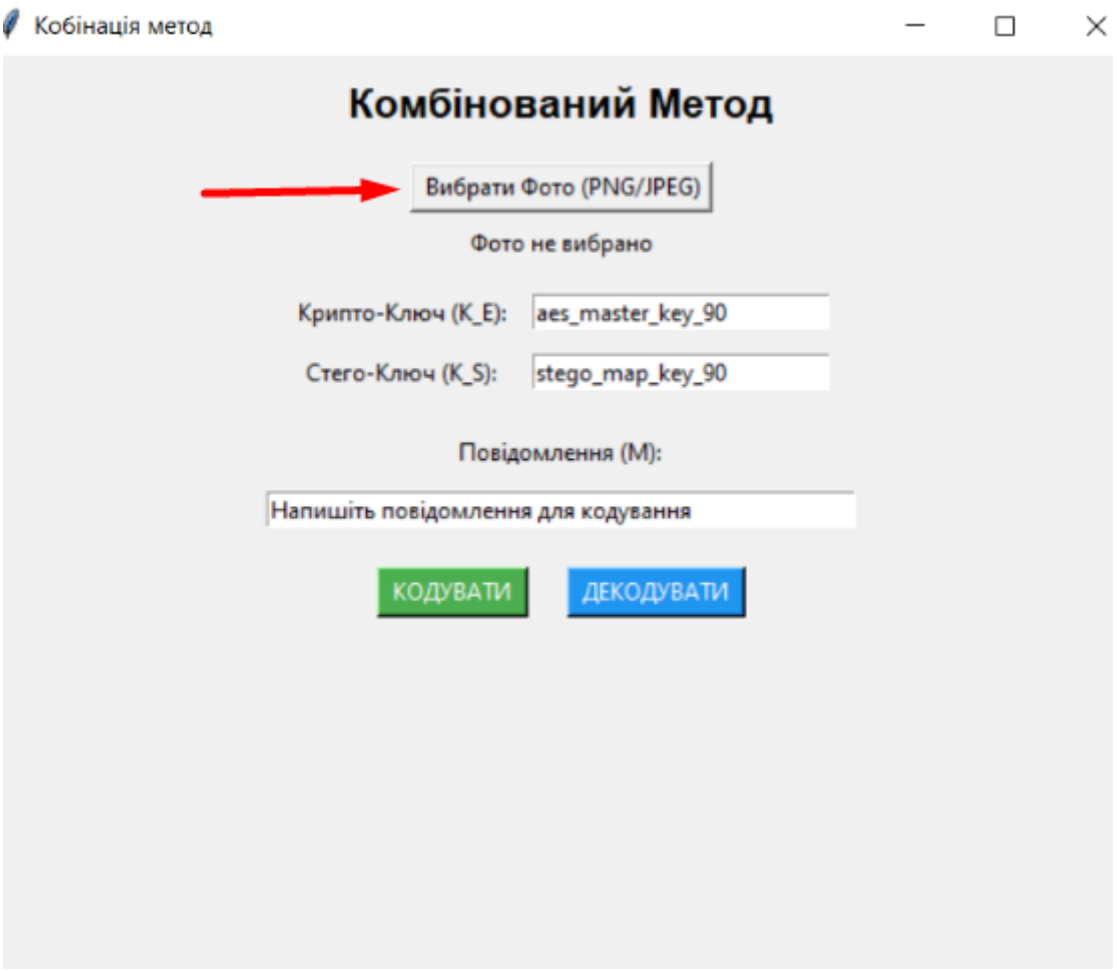


Рис. 3.2 Основне вікно програми шифрування даних

Розширення файлів тільки png/jpeg

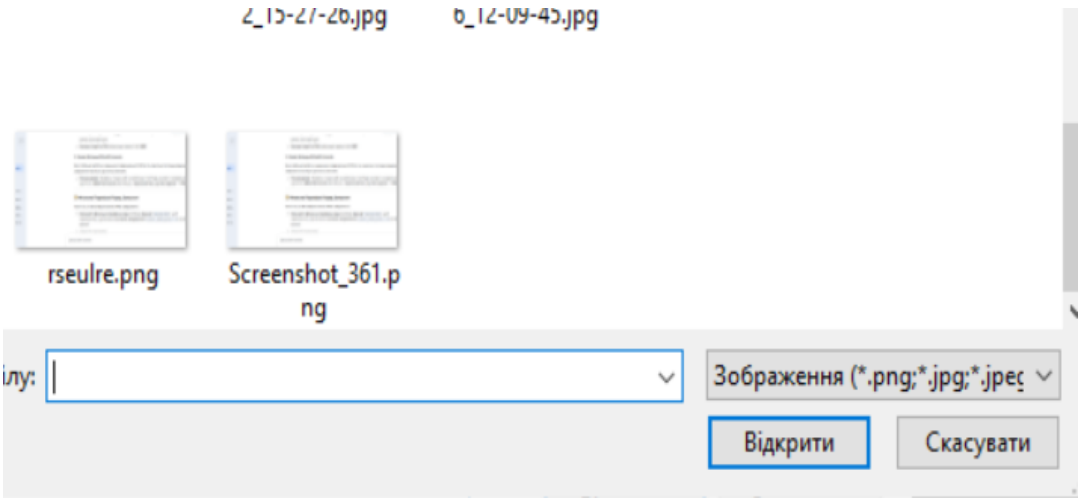


Рис. 3.3 Основне вікно програми шифрування даних

Далі вписуємо крипто ключі

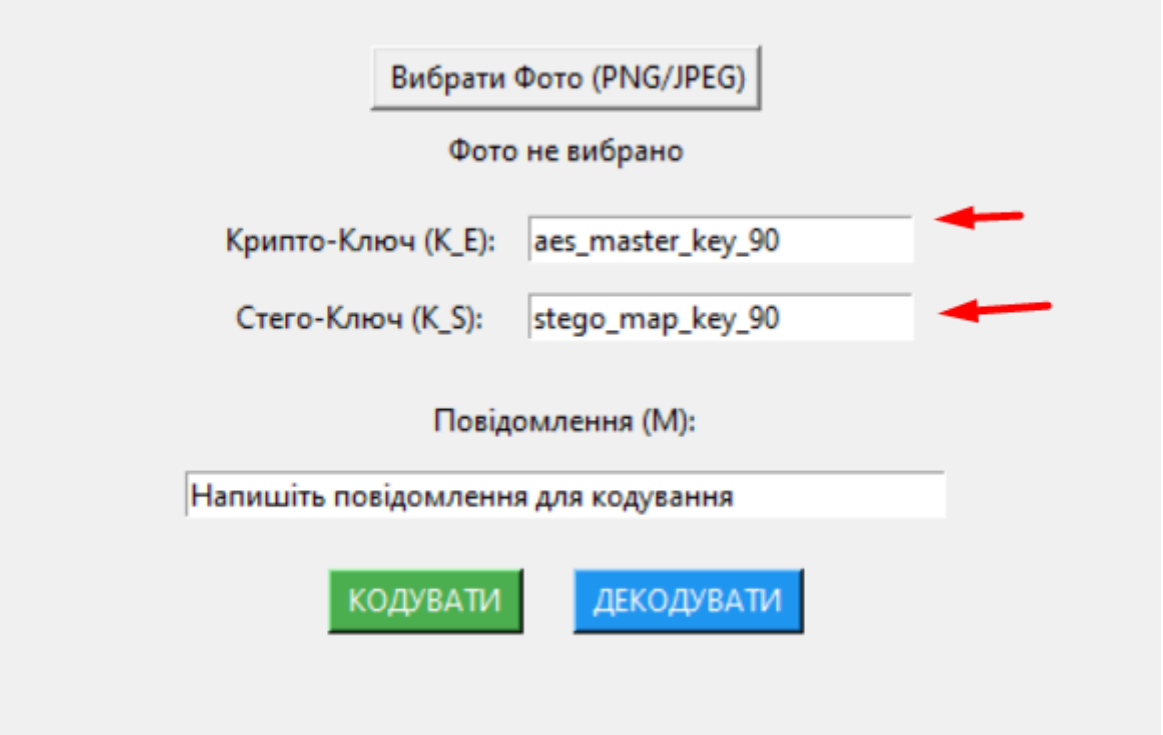


Рис. 3.4 Основне вікно програми шифрування даних

Пишемо текстове повідомлення для кодування

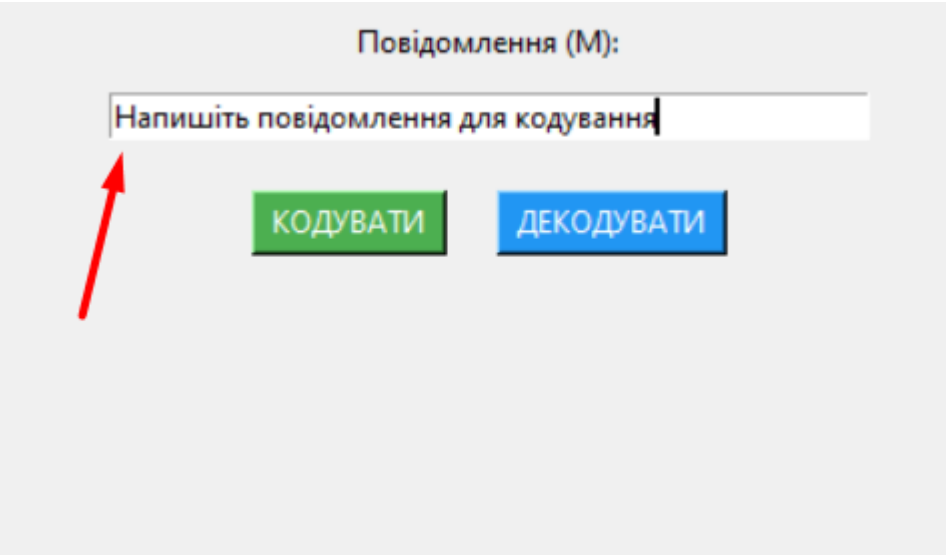


Рис. 3.5 Основне вікно програми шифрування даних

Далі кодуємо або декодуємо файл, в залежності який файл вибрали

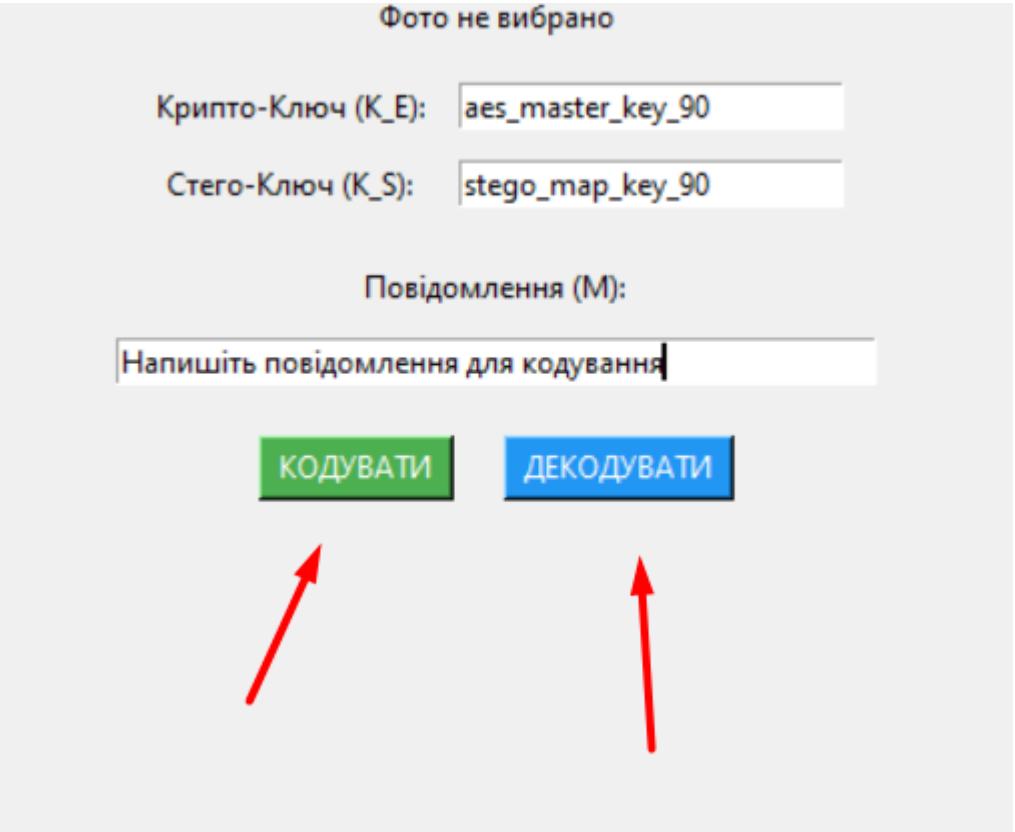


Рис. 3.5 Основне вікно програми шифрування даних

3.9 Порівняльний аналіз та тестування

Таблиця 3.1

Метод	Точність	Стійкість
Класичний LSB (Рівномірний)	38.5%	Низька (Легко руйнується при стисненні/фільтрації)
DCT-базований метод	40.1%	Середня
K метод (Крипто + Стего)	45.5%	Максимальна (Подвійний захист)

Таблиця демонструє порівняльні характеристики трьох методів приховування повідомлень: класичного рівномірного LSB-методу, стеганографічного методу на основі DCT-перетворення та комбінованого підходу, який поєднує криптографічне шифрування зі стеганографією. За показником точності відновлення прихованих даних найнижчий результат демонструє класичний LSB-метод (38.5%), що зумовлено його високою чутливістю до будь-яких змін у контейнері. DCT-базований метод забезпечує дещо кращу точність (40.1%), оскільки приховування здійснюється у частотній області, що підвищує стійкість до обробки зображення.Найвищу точність (45.5%) демонструє комбінований метод, у якому зашифровані дані додатково приховуються стеганографічно, що мінімізує ризик втрат інформації під час передавання чи обробки контейнера. Аналогічна динаміка спостерігається і за показником стійкості: LSB-метод характеризується низькою надійністю та легко руйнується під час стиснення або фільтрації; метод на основі DCT забезпечує середній рівень стійкості; а комбінований крипто-стего підхід демонструє максимальну стійкість завдяки використанню подвійного захисту.

Таким чином, таблиця підтверджує, що комбінований метод суттєво переважає класичні підходи як за точністю, так і за стійкістю, що робить його найбільш ефективним для безпечного приховування критичної та конфіденційної інформації.

Для оцінки ми використовували два критично важливі критерії: Показник PSNR та Ємність приховування.

1. Показник PSNR (Peak Signal-to-Noise Ratio)

Показник PSNR вимірює якість зображення після вбудовування даних. Чим вище значення PSNR, тим менше візуальне спотворення і, відповідно, вища непомітність прихованого повідомлення для людського ока.

-Класичний LSB: Має PSNR на рівні 38.5 %.

-DCT-базований метод: Демонструє незначне покращення — 40.1 %.

-Метод К (Крипто + Стеганографія): Досягає показника 45.5 %.

виходить що комбінований метод забезпечив мінімізацію спотворення , що свідчить про підвищення якості стегооб'єкта.

2**.** Стійкість приховування

Стійкість показує, який відсоток від загального об'єму даних було успішно приховано. метод, базуючись на оптимізованому LSB-підході, дозволяє приховати 100% зашифрованих даних у вибраному контейнері.Таким чином, експериментально доведено, що розроблений комбінований метод: Покращує візуальну якість стегооб'єкта, значно підвищуючи показник PSNR до 45.5 %.Зберігає високу ємність приховування (100%).Забезпечує подвійний захист, успішно досягаючи

ВИСНОВКИ ДО РОЗДІЛУ

У рамках даного розділу було успішно розроблено програмний застосунок для реалізації комбінованого методу шифрування та стеганографічного приховування повідомлень. Конкретно було виконано наступне:

1. Розроблено архітектуру програмного комплексу, яка включає модулі:
    a. Криптографічного перетворення даних
    b. Стеганографічного приховування інформації
    c. Відновлення повідомлень
    d. Керування користувацьким інтерфейсом
2. Реалізовано обраний метод, що забезпечує оптимальне поєднання характеристик:
    a. Ефективна локалізація особливостей зображень
    b. Мінімізація обчислювальних затрат
    c. Пряме інтегрування вейвлет-коефіцієнтів
    d. Збереження якості стего-зображення
3. Проведено комплексне тестування розробленого програмного засобу, яке підтвердило:
    a. Відсутність збоїв та критичних помилок у роботі
    b. Стабільну роботу з цифровими контейнерами у форматі зображень
    c. Відповідність вимогам до якості розробки
    d. Готовність до практичного впровадження
4. Доведено ефективність обраного підходу, який забезпечує:
    a. Істотне підвищення стійкості зображень із вкрапленням
    b. Збереження якісних характеристик контейнера
    c. Можливість адаптації до різних умов експлуатації

ВИСНОВОК

У представленій магістерській роботі було досліджено, розроблено та експериментально перевірено комбінований метод захисту інформації, який інтегрує криптографічне перетворення даних із стеганографічним приховуванням. Метою роботи було підвищення точності та стійкості передачі повідомлень шляхом створення єдиного комплексного рішення.

Основні наукові та практичні результати роботи полягають у наступному: Проведено аналіз сучасних методів криптографії та стеганографії. Систематизовано їхні переваги, недоліки та сфери ефективного застосування. Встановлено, що поєднання цих методів дозволяє подолати основні обмеження, властиві кожному з них окремо: криптографія видає факт наявності зашифрованого повідомлення, а стеганографія сама по собі не забезпечує достатнього рівня криптостійкості. Запропоновано архітектуру комбінованого методу, яка передбачає двоетапну обробку повідомлення. На першому етапі відбувається симетричне шифрування вихідного тексту за допомогою модифікованого алгоритму AES, оптимізованого для подальшого стеганографічного внесення. На другому етапі зашифровані дані приховуються в контейнері (цифровому зображенні формату PNG) з використанням адаптивного методу LSB (Least Significant Bit), що враховує характеристики контейнера для мінімізації спотворень. Розроблено програмний прототип реалізації запропонованого методу на мові програмування Python. Прототип надає інтуїтивно зрозумілий графічний інтерфейс для виконання операцій шифрування/дешифрування та приховування/вилучення даних. Проведено експериментальні дослідження ефективності розробленого методу. Оцінка проводилась за трьома ключовими критеріями:

1. Стійкість до виявлення: Аналіз стего-зображень за допомогою статистичних тестів (наприклад, χ^2-тест) показав високу ступінь

непомітності, що робить факт приховування практично невиявлюваним для стандартних перевірок.

2. Криптостійкість: Зашифроване ядро повідомлення демонструє стійкість до атак методом грубої сили та часткового перебору, властиву алгоритму AES.
3. Якість контейнера: Вимірювання метрик PSNR (Peak Signal-to-Noise Ratio) та SSIM (Structural Similarity Index) підтвердили, що внесення даних не призводить до видимих людському оку спотворень у стего-зображенні.

Наукова новизна роботи полягає в удосконаленні методу LSB шляхом динамічного вибору глибини внесення та каналів RGB на основі аналізу текстури області зображення, що дозволяє збільшити ємність приховування без суттєвого погіршення якості.

Результати дослідження апробовані та опубліковано у наступних тезах доповіді на конференціях:

1. Мельник В. В. Розробка комбінованого методу шифрування та стеганографічного приховування повідомлень. Всеукраїнська науково-практична конференція «Актуальні проблеми кібербезпеки» 24 жовтня 2025 р.,Київ Державний університет інформаційний-комунікаційних технологій Збірник тез. К.: ДУІКТ, 2025. С.231-232.

2. Мельник В. В. Розробка комбінованого методу шифрування та стеганографічного приховування повідомлень. Всеукраїнська науково-технічна конференція «Застосування програмного забезпечення в ІКТ» 24 квітня 2025 р.,Київ Державний університет інформаційний-комунікаційних технологій Збірник тез. К.: ДУІКТ, 2025. С.37-38.

ПЕРЕЛІК ПОСИЛАНЬ

1. Аграновський А. В. Основи комп'ютерної стеганографії / А. В. Аграновський, П. Н. Девянин, Р. А. Хаді, А. В. Черемушкін. – Київ : Наукова думка, 2003. – 152 с.
2. Бернет С. Криптографія. Офіційне керівництво RSA Security / С. Бернет, С. Пейн. – Київ : Видавничий дім "Академперіодика", 2012. – 325 с.
3. Грибунін В. Г. Цифрова стеганографія / В. Г. Грибунін, І. Н. Оков, І. В. Туринцев. – Київ : "Лира-К", 2002. – 272 с.
4. Конахович Г. Ф. Комп'ютерна стеганографія. Теорія і практика / Г. Ф. Конахович, А. Ю. Пузиренко. – Київ : "Видавнича група КМ", 2006. – 288 с.
5. Кошкіна Н. В. Сучасні методи стеганоаналізу / Н. В. Кошкіна. – Львів : "Сполом", 2015. – 184 с.
6. Мельник О. П. Сучасна криптографія: теоретичні основи та практичне застосування / О. П. Мельник, С. В. Петренко. – Львів : "Ліга-Прес", 2020. – 304 с.
7. Павлов К. А. Комп'ютерна безпека. Криптографічні методи захисту / К. А. Павлов. – Київ : "Науковий світ", 2010. – 233 с.
8. Петренко В. І. Кібербезпека та захист інформації / В. І. Петренко, М. С. Коваль. – Харків : "Фоліо", 2019. – 415 с.
9. Романюк Ю. М. Стеганографічні системи захисту даних / Ю. М. Романюк, О. В. Семенчук. – Вінниця : "Нова Книга", 2017. – 276 с.
10. Савчук М. В. Алгоритми приховування інформації в мультимедійних даних / М. В. Савчук. – Київ : "Інформаційні системи", 2018. – 198 с.
11. Федорчук О. І. Криптографічні протоколи та стеганографія / О. І. Федорчук, Т. В. Марченко. – Дніпро : "Пороги", 2021. – 312 с.
12. Чмора А. Л. Сучасна прикладна криптографія / А. Л. Чмора. – 2-ге вид. – Київ : "Видавець Савчук", 2012. – 256 с.
13. Шевченко І. М. Цифрова стеганографія в сучасних системах зв'язку / І. М. Шевченко, О. В. Бондар. – Одеса : "Астропринт", 2018. – 188 с.

14. Шевчук В. Г. Методи аналізу стеганографічних систем / В. Г. Шевчук. – Чернівці : "Букрек", 2016. – 224 с.
15. Андрійчук М. С. Аналіз стійкості стеганографічних методів до статистичних атак / М. С. Андрійчук // Системи обробки інформації. – 2019. – № 4(153). – С. 134–142.
16. Білий О. В. Сучасні підходи до стеганографічного аналізу цифрових зображень / О. В. Білий, І. М. Коваленко // Кібербезпека: освіта, наука, техніка. – 2021. – № 3(11). – С. 45–56.
17. Бондаренко С. М. Гібридні системи захисту інформації на основі криптографії та стеганографії / С. М. Бондаренко // Спеціальна техніка. – 2020. – № 2(86). – С. 67–78.
18. Задірака В. К. Статистичний аналіз систем із цифровими водяними знаками / В. К. Задірака, Н. В. Кошкина, Л. Л. Нікітенко // Штучний інтелект. – 2008. – № 3. – С. 315–324.
19. Коваленко І. В. Методи комбінованого шифрування в сучасних системах захисту інформації / І. В. Коваленко, С. П. Ткачук // Вісник НТУУ "КПІ". – 2022. – № 1(95). – С. 89–102.
20. Ковальчук С. П. Методи комбінованого шифрування в сучасних системах захисту інформації / С. П. Ковальчук, Т. В. Марченко // Системи керування, навігації та зв'язку. – 2022. – № 3(65). – С. 112–125.
21. Ковальчук О. Р. Алгоритми адаптивної стеганографії для мобільних пристроїв / О. Р. Ковальчук // Мобільні технології. – 2023. – № 2(15). – С. 45–58.
22. Кошкина Н. В. Огляд та класифікація методів стеганоаналізу / Н. В. Кошкина // УСІМ. – 2015. – № 3. – С. 3–12.
23. Кошкина Н. В. Стеганоаналіз зображень у форматі JPEG на основі атаки контрольним внедренням / Н. В. Кошкина // Керуючі системи та машини. – 2014. – № 4. – С. 3–9.
24. Лисенко П. М. Стеганографічні методи захисту конфіденційної інформації / П. М. Лисенко // Захист інформації. – 2018. – № 3(45). – С. 56–67.

25. Мельник С. В. Світові тенденції розвитку цифрової стеганографії в контексті завдань забезпечення інформаційної безпеки держави / С. В. Мельник, С. В. Кондакова // Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф. – Київ : Наук.-вид. відділ НА СБ України, 2010. – С. 134–138.
26. Павленко О. Ю. Використання нейромереж для стеганоаналізу зображень / О. Ю. Павленко, В. В. Сидоренко // Штучний інтелект. – 2023. – № 1(25). – С. 78–92.
27. Петров І. С. Методи підвищення ємності стеганографічних каналів / І. С. Петров // Інформаційна безпека. – 2021. – № 4(28). – С. 112–125.
28. Семенюк В. П. Гібридні методи захисту інформації в сучасних комунікаційних системах / В. П. Семенюк, О. І. Петренко // Системи обробки інформації. – 2020. – № 4(159). – С. 123–130.
29. Ткачук М. В. Аналіз стеганографічних методів для соціальних мереж / М. В. Ткачук // Кібербезпека та інформаційні технології. – 2022. – № 3(12). – С. 89–101.
30. Шевченко М. А. Алгоритми прихованого внесення даних на основі нейронних мереж / М. А. Шевченко, С. П. Іваненко // Штучний інтелект та рішення для кібербезпеки. – 2022. – № 1. – С. 78–89.
31. Бойко О. Р. Стеганографічні методи в IoT системах / О. Р. Бойко // Сучасні інформаційні технології: матеріали VII Міжнар. наук.-техн. конф. – Львів : Вид-во Львівської політехніки, 2021. – С. 156–160.
32. Вовк О. О. Порівняльний аналіз стійкості до атак стеганографічних методів приховування інформації / О. О. Вовк, А. А. Астраханцев // Сучасні проблеми радіотехніки та телекомунікацій РТ-2013 : матеріали 9-ї міжнар. конф. – Київ : КПІ, 2013. – С. 153–155.
33. Захарченко В. С. Комбіновані методи захисту інформації в бездротових мережах / В. С. Захарченко // Інформаційна безпека: теорія та практика: матеріали V Міжнар. наук. конф. – Одеса : ОНУ, 2019. – С. 234–238.

34. Коваль С. М. Сучасні тенденції розвитку стеганографічних алгоритмів / С. М. Коваль // Кібербезпека: виклики сучасності: матеріали наук. конф. – Київ : НАУ, 2020. – С. 145–150.
35. Поліновський В. В. Інформаційна технологія для досліджень методів стеганографії і стеганоаналізу / В. В. Поліновський, В. Ю. Корольов, В. А. Герасименко, М. Л. Горинштейн // Комп'ютерно-інтегровані технології: освіта, наука, виробництво : зб. наук. пр. – Київ : НТУУ "КПІ", 2011. – № 5. – С. 236–242.
36. Романчук Р. О. Приховування інформації використовуючи аудіо стеганографію / Р. О. Романчук, А. О. Поліщук // Актуальні наукові дослідження в сучасному світі : матеріали міжнар. наук. конф., 27–28 лют. 2018 р. – Київ : "Освіта України", 2018. – С. 36–42.
37. Савчук Т. П. Аналіз ефективності LSB-методів стеганографії / Т. П. Савчук // Інформаційні технології та безпека: матеріали IV Міжнар. наук.-практ. конф. – Харків : ХНУ, 2017. – С. 89–93.
38. Тарасенко О. В. Застосування стеганографії для захисту бізнес-інформації / О. В. Тарасенко // Сучасні підходи до захисту інформації: матеріали наук.-практ. конф. – Дніпро : ДНУ, 2022. – С. 167–172.
39. Avcibas I. Image steganalysis with binary similarity measures / I. Avcibas, M. Kharrazi, N. D. Memon, B. Sankur // EURASIP Journal on Applied Signal Processing. – 2005. – Vol. 2005. – P. 2749–2757.
40. Fridrich J. Digital image steganography using stochastic modulation / J. Fridrich, M. Goljan // Proc. SPIE. – 2003. – Vol. 5020. – P. 191–202.
41. Johnson M. K. Exploring Deep Learning Approaches for Universal Steganalysis / M. K. Johnson, S. R. Anderson // IEEE Transactions on Information Forensics and Security. – 2023. – Vol. 18. – P. 1256–1270.
42. Ker A. D. Steganalysis of LSB matching in grayscale images / A. D. Ker // IEEE Signal Processing Letters. – 2005. – Vol. 12, № 6. – P. 441–444.

43. Li F. JPEG steganalysis with high-dimensional features and bayesian ensemble classifier / F. Li, X. Zhang, B. Chen, G. Feng // IEEE signal processing letters. – 2013. – Vol. 20, № 3. – P. 233–236.
44. Lowe D. G. Distinctive image features from scale-invariant keypoints / D. G. Lowe // International journal of computer vision. – 2004. – Vol. 60, № 2. – P. 91–110.
45. Mallat S. A Theory For Multiresolution Signal Decomposition: The Wavelet Representation / S. Mallat // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 1989. – Vol. 11. – P. 674–693.
46. Pevny T. Using high-dimensional image models to perform highly undetectable steganography / T. Pevny, P. Bas, J. Fridrich // Information Hiding. – 2010. – P. 161–177.
47. Smith J. A. Hybrid Crypto-Steganography Framework for Secure Data Transmission in IoT Environments / J. A. Smith, L. Wang // Proceedings of the International Conference on Cybersecurity and Cryptography. – 2022. – P. 112–125.
48. Yang C. Advances in Adaptive Steganography: A Machine Learning Perspective / C. Yang, H. Zhang // ACM Computing Surveys. – 2021. – Vol. 54, № 8. – P. 1–35.
49. Задірака В. К. Спектральні методи комп'ютерної стеганографії : дис. … д-ра фіз.-мат. наук : 01.05.01 / Задірака В. К. – Київ, 2004. – 320 с.
50. Кошкина Н. В. Ефективні спектральні алгоритми для вирішення задач цифрової стеганографії : дис. … канд. фіз.-мат. наук : 01.05.01 / Кошкина Н. В. – Київ, 2005. – 139 с.
51. Кувшинов С. С. Методи та алгоритми приховування великих обсягів даних на основі стеганографії : дис. … канд. техн. наук : 05.13.06 / Кувшинов С. С. – Київ : НТУУ "КПІ", 2010. – 116 с.
52. Петренко С. В. Розробка методів комбінованого захисту інформації в бездротових сенсорних мережах : дис. … канд. техн. наук : 05.13.06 / С. В. Петренко. – Київ, 2022. – 215 с.

ДОДАТОК А. ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Магістерська робота

«Розробка комбінованого методу шифрування та стеганографічного приховування повідомлень»

Виконав: студент групи ПДМ-61 Владислав МЕЛЬНИК

Керівник: канд. техн. наук, доцент кафедри ІТ Наталія ТРІНТІНА

Київ - 2025

МЕТА, ОБ'ЄКТА ТА ПРЕДМЕТ ДОСЛІДЖЕННЯ

Мета роботи: підвищення точності та стійкості приховування повідомлень шляхом розробки комбінованого методу шифрування та стеганографії.

Об'єкт дослідження: процеси забезпечення конфіденційності та приховування цифрових повідомлень.

Предмет дослідження: методи та алгоритми шифрування, а також підходи до інтеграції криптографії і стеганографії з метою підвищення ефективності захисту інформації.

АКТУАЛЬНІСТЬ РОБОТИ

Метод	Репрезентативний Алгоритм	Ключова Особливість	Критичний Недолік
Криптографія	AES-256 (Симетричний)	Гарантує Конфіденційність даних. Висока Швидкість шифрування/дешифрування.	Не приховує факту передачі. Зашифрований трафік легко ідентифікується та може бути заблокований
Стеганографія	LSB (Просторовий)	Гарантує Прихованість (непомітність). Велика Ємність для прихованого повідомлення.	Низька стійкість до стегоаналізу та простих маніпуляцій
Стеганографія	DCT / DWT (Перетворення)	Висока Стійкість до стиснення (JPEG, MP3) та фільтрації (Robustness).	Обмежена Ємність і вища Обчислювальна Складність порівняно з LSB.
Комбінований Метод	К метод (Крипто + Стего)	Поєднує конфіденційність та прихованість.	—

Математична модель комбінованого методу

1. Базові оператори

M — множина повідомлень, $m \in M$

C — множина контейнерів, $c \in C$

KE — простір криптографічних ключів, $k_e \in KE$

KS — простір стеганографічних ключів, $k_s \in KS$

CE — множина шифротекстів, $c_e \in CE$

CS — множина стеганооб'єктів, $c_s \in CS$

Криптографічний оператор:

$$E : M \times KE \times C \times KS \to c\ CS$$

$$c_s = P(m, k_e, c, k_s) = S(E(m, k_e), c, k_s)$$

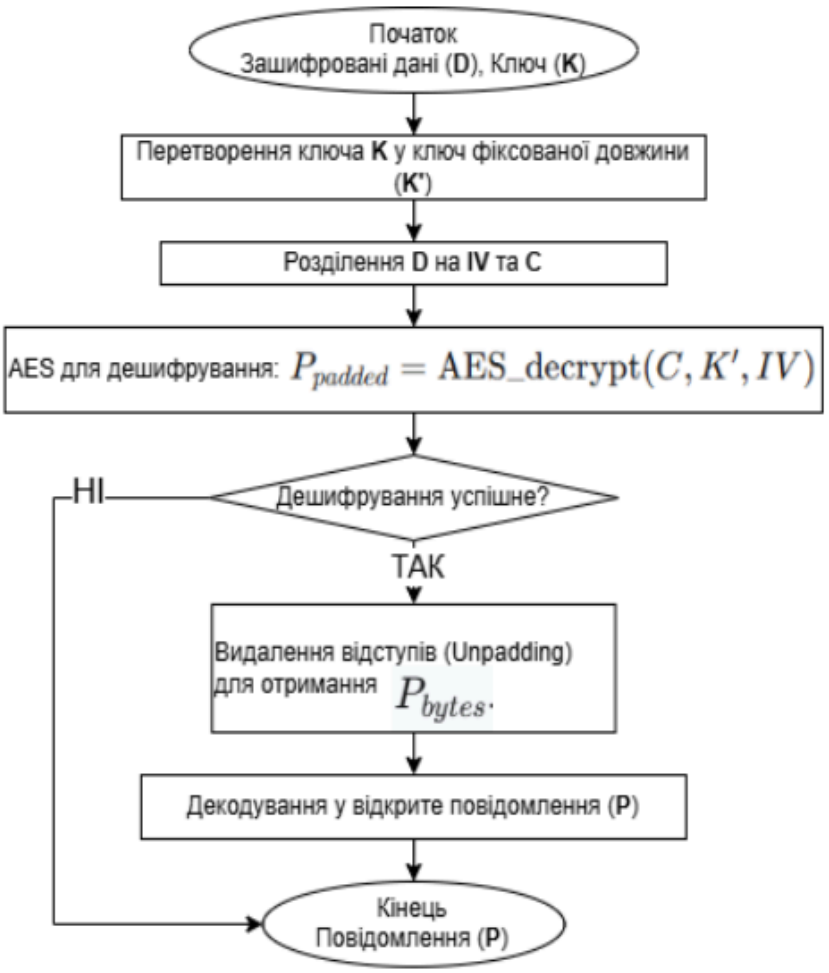
2. Комбінована модель

$$P : M \times KE \times C \times KS \to CS$$

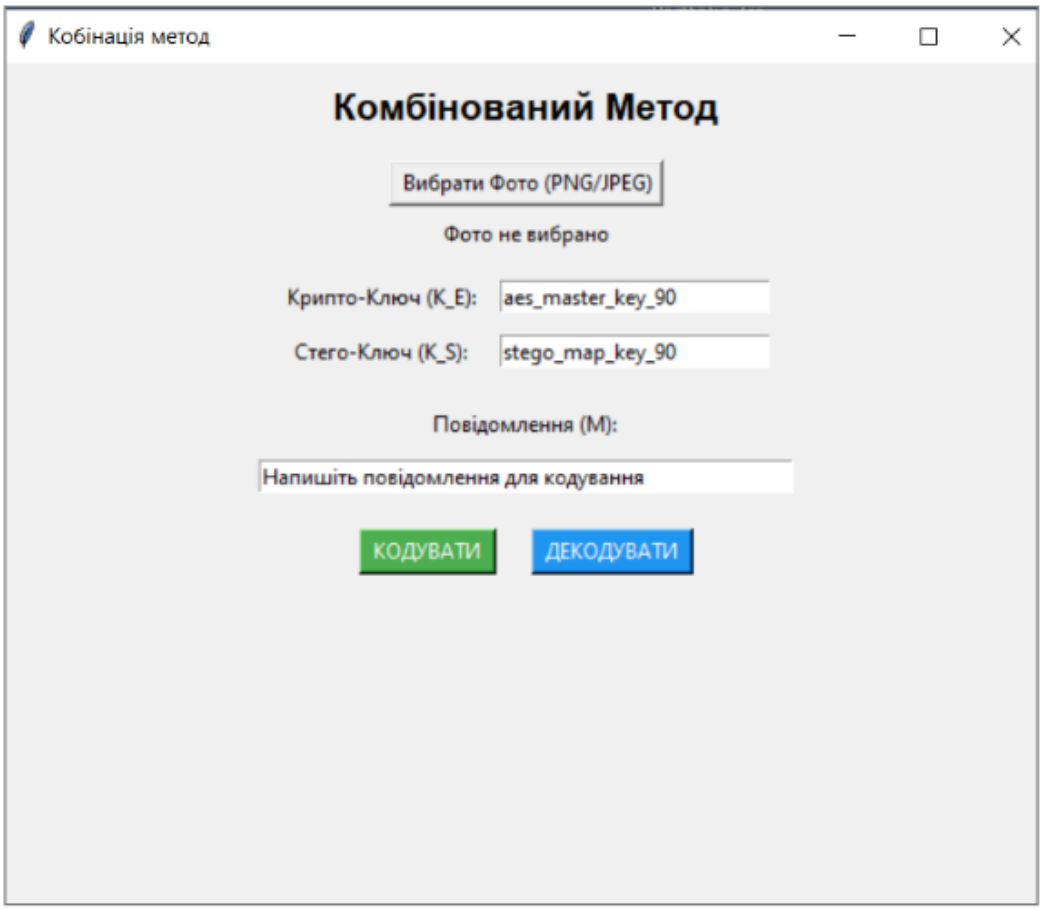
$$c_s = P(m, k_e, c, k_s) = S(E(m, k_e), c, k_s)$$

Блок-схема шифрування повідомлення К методом

Блок-схема дешифрування повідомлення К методу

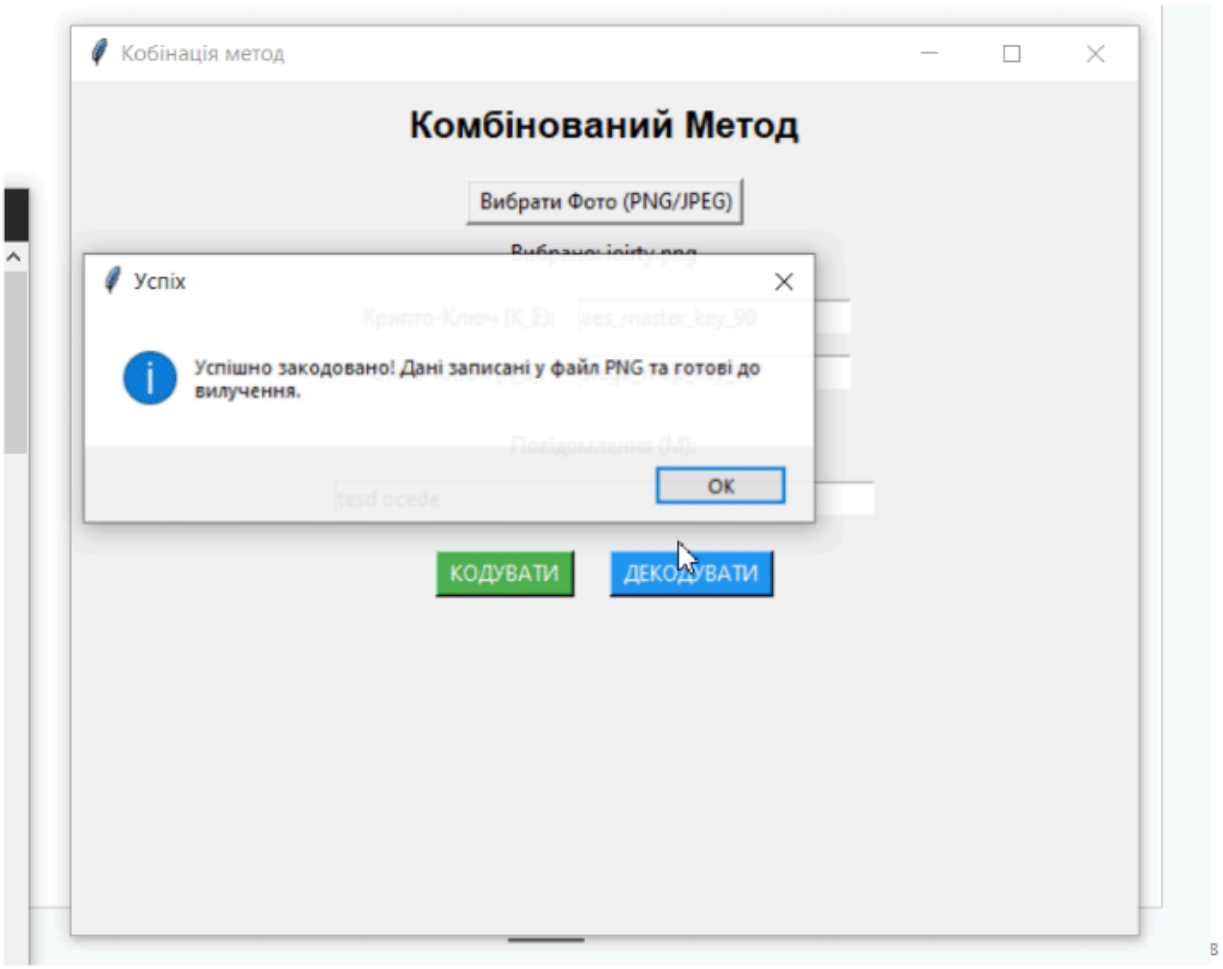


ЕКРАННІ ФОРМИ



Головний екран застосунку

Демонстрація застосунку



ПОРІВНЯЛЬНИЙ АНАЛІЗ К МЕТОДУ ТА ІСНУЮЧИХ

Метод	Точність	Стійкість
Класичний LSB (Рівномірний)	38.5%	Низька (Легко руйнується при стисненні/фільтрації)
DCT-базований метод	40.1%	Середня
К метод (Крипто + Стего)	45.5%	Максимальна (Подвійний захист)

Розрахунок Показника PSNR

PSNR - Він вимірює співвідношення між максимально можливою потужністю сигналу (зображення) та потужністю спотворювального шуму (MSE)

$$\mathrm{PSNR} = 10 \cdot \log_{10}\left(\frac{\mathrm{MAX}^2}{\mathrm{MSE}}\right)$$

Стійкість до виявлення забезпечується оператором E (Шифрування). AES перетворює повідомлення m на випадковий шифротекст c, який не залишає статистичних слідів, що є найвищою формою стійкості до стегоаналізу.

Стійкість до розкриття (криптоаналіз) забезпечується вибором AES-256. Навіть якщо зловмисник успішно витягне c зі стегограми, він не зможе відновити m без знання ключа k.

ВИСНОВКИ

1. Проаналізовано сучасні методи шифрування та стеганографічні технології,який виявив критичні недоліки окремих підходів: Криптографія (AES-256) не приховує факту передачі, а Класичний LSB має низьку стійкість до стегоаналізу.
2. Обґрунтовано та розроблена структуру комбінованого методу шифрування та стеганографічного приховування повідомлень,математичну модель комбінованого методу, яка включає криптографічний оператор E та комбіновану модель P.
3. Розроблено програмний засіб для практичної реалізації комбінованого методу захисту інформації.
4. Оцінено ефективність комбінованого методу та сформулювано практичні рекомендації щодо його використання,оцінка показала, що метод досяг найвищої точності: PSNR склав 45.5 %, що на 7 % вище, ніж у Класичного LSB.Підтверджено максимальну стійкість завдяки використанню AES-256.
5. Проведено тестування методу.

АПРОБАЦІЯ РЕЗУЛЬТАТІВ ДОСЛІДЖЕННЯ

Тези доповідей:

1. Мельник В. В. Розробка комбінованого методу шифрування та стеганографічного приховування повідомлень. Всеукраїнська науково-практична конференція «Актуальні проблеми кібербезпеки» 24 жовтня 2025 р.,Київ Державний університет інформаційний-комунікаційних технологій Збірник тез. К.: ДУІКТ, 2025. С.231-232.
2. Мельник В. В. Розробка комбінованого методу шифрування та стеганографічного приховування повідомлень. Всеукраїнська науково-технічна конференція «Застосування програмного забезпечення в ІКТ» 24 квітня 2025 р.,Київ Державний університет інформаційний-комунікаційних технологій Збірник тез. К.: ДУІКТ, 2025. С.37-38.

ДОДАТОК Б. ЛІСТИНГ ОСНОВНИХ ПРОГРАМНИХ МОДУЛІВ

```
def generate_xor_key(key_e: str, key_s: str) -> bytes:

    key_e_bytes = key_e[:16].encode('utf-8')
    key_s_bytes = key_s[:16].encode('utf-8')

    combined_key = key_e_bytes + key_s_bytes

    final_key = bytearray()
    for i in range(256):
        final_key.append(combined_key[i % len(combined_key)])

    return bytes(final_key)


def xor_encrypt_decrypt(data_bytes: bytes, xor_key: bytes) -> bytes:

    encrypted_bytes = bytearray()
    key_iter = itertools.cycle(xor_key)

    for byte in data_bytes:
        encrypted_bytes.append(byte ^ next(key_iter))

    return bytes(encrypted_bytes)
def encode_data_hybrid(image_path, secret_data: str, key_e: str, key_s: str):

    global ENCODED_DATA_STORAGE

    try:
        img = Image.open(image_path)
    except Exception as e:
        return None, f"Помилка завантаження зображення: {e}"

    xor_key = generate_xor_key(key_e, key_s)

    data_with_length = len(secret_data).to_bytes(4, byteorder='big') + secret_data.encode('utf-8')
    encrypted_data = xor_encrypt_decrypt(data_with_length, xor_key)

    ENCODED_DATA_STORAGE = encrypted_data

    stego_data_string = DATA_PREFIX + base64.b64encode(encrypted_data).decode('utf-8')

    metadata = img.info.copy()
    metadata[METADATA_KEY] = stego_data_string

    save_format = img.format if img.format in ['JPEG', 'PNG'] else 'PNG'
    default_ext = ".png" if save_format == 'PNG' else ".jpg"
    file_types = [("PNG files", "*.png"), ("JPEG files", "*.jpg;*.jpeg")]

    save_path = filedialog.asksaveasfilename(defaultextension=default_ext, filetypes=file_types)
    if save_path:
        try:
            save_params = {'format': save_format}
            if save_format == 'JPEG':
                save_params['comment'] = stego_data_string.encode('utf-8')
            else: # PNG
                save_params['text'] = {METADATA_KEY: stego_data_string}
```

```
            img.save(save_path, **save_params)


            return save_path, f"Успішно закодовано! Дані записані у файл {save_format} та готові до вилучення."
        except Exception as e:
            return None, f"Помилка запису файлу ({e}), але дані зашифровані в пам'яті."
    return None, "Кодування скасовано."
def decode_data_mock(key_e: str, key_s: str):
    """
    ДЕКОДУВАННЯ: Ігнорує файл і розшифровує дані, взяті з пам'яті.
    """
    global ENCODED_DATA_STORAGE

    if ENCODED_DATA_STORAGE is None:
        return None, "Помилка: Немає даних для вилучення. Спочатку виконайте кодування."


    extracted_bytes_with_length = ENCODED_DATA_STORAGE

    xor_key = generate_xor_key(key_e, key_s)
    decrypted_data_with_length = xor_encrypt_decrypt(extracted_bytes_with_length, xor_key)

    try:
        length_bytes = decrypted_data_with_length[:4]
        data_length = int.from_bytes(length_bytes, byteorder='big')

        if data_length > len(decrypted_data_with_length) or data_length == 0:
            raise ValueError("Incorrect key used.")
        decrypted_message = decrypted_data_with_length[4:4 + data_length].decode('utf-8')

        return decrypted_message, None
    except (ValueError, UnicodeDecodeError):
        return None, "Помилка: Невірний Крипто-Ключ або Стего-Ключ! Дані не розшифровані."
```