Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: "Дослідження стійкості стеганографічних методів в просторовій та частотній областях до перетворення графічних форматів"

Виконав: студент (ка) IV курсу, групи СБс-41

Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Рибак Владислав Юрійович
підпис (прізвище та ініціали)

Керівник Загородна Н.В.
підпис (прізвище та ініціали)

Нормоконтроль Дроздова Т.В.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2025

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Рибаку Владиславу Юрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження стійкості стеганографічних методів в просторовій та частотній областях до перетворення графічних форматів

Керівник роботи Загородна Наталія Володимирівна, к.т.н., доцент, асистент кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «02» 05 2025 року № 4/7-361

2. Термін подання студентом завершеної роботи 16.06.2025

3. Вихідні дані до роботи літературні джерела про предметну область
Приховування інформації

4. Зміст роботи (перелік питань, які потрібно розробити)
Теоретичні основи стеганографії
Основні формати графічних зображень
Математичні основи стеганографічних методів
Експериментальні дослідження
Безпека життєдіяльності, основи охорони праці
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	Мариненко С.Ю., доц. кафедри МТ		

7. Дата видачі завдання 20.01.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	20.01 – 23.01	Виконано
2.	Підбір джерел про стеганографічні методи перетворення інформації	25.01 – 05.02	Виконано
3.	Опрацювання джерел в галузі дослідження	06.02 – 20.02	Виконано
4.	Провести аналіз стеганографічних методів	22.02 – 12.03	Виконано
5.	Здійснення програмну реалізацію обраних методів	15.03-25.03	Виконано
6.	Провести експериментальні дослідження стосовно стійкості обраних методів до перетворень графічних форматів	25.02 – 10.04	Виконано
7.	Оформлення розділу «Теоретичні основи стеганографії та перетворень графічних форматів»	10.02 – 05.03	Виконано
8.	Оформлення розділу «Математичні основи стеганографічних методів»	26.03 – 04.05	Виконано
9.	Оформлення розділу «Експериментальні дослідження»	12.04-20.04	Виконано
10.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи охорони праці»	25.04 – 10.05	Виконано
11.	Оформлення кваліфікаційної роботи	23.05 – 08.06	Виконано
12.	Нормоконтроль	10.06 – 15.06	Виконано
13.	Перевірка на плагіат	20.06 – 22.06	Виконано
14.	Попередній захист кваліфікаційної роботи	14.06 – 15.06	Виконано
15.	Захист кваліфікаційної роботи	25.06.2025	

Студент _____ Рибак В.Ю.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Загородна Н.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Дослідження стійкості стеганографічних методів в просторовій та частотній областях до перетворення графічних форматів. // Кваліфікаційна робота ОР «Бакалавр» // Рибак Владислав Юрійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-41 // Тернопіль, 2025 // С. 65, рис. – __, табл. – - , кресл. – __, додат. – ___.

КЛЮЧОВІ СЛОВА: стеганографічні методи, графічні формати, просторова область, частотна область стійкість

У даній кваліфікаційній роботі було проведено огляд літературних джерел, проаналізовано принципи функціонування стеганографічних алгоритмів, відібрано ключові графічні формати. Після реалізації та застосування обраних методів до тестових зображень, було проведено серію експериментів із застосуванням перетворень форматів контейнерів. Отримана оцінка збереження прихованої інформації дозволила зіставити результати та зробити висновок про значно вищу стійкість методів частотної області порівняно з методами просторової області до типових перетворень, що підтверджує їхню більшу придатність для практичного використання в умовах реального цифрового середовища.

ABSTRACT

Study of the Resilience of Steganographic Methods in Spatial and Frequency Domains Against Graphic Format Transformations // Thesis of educational level "Bachelor"// Rybak Vladyslav // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБс-41 // Ternopil, 2025 // P. 65, fig. - ___, tab. - ___, drawing - ____, added. – ____.

Keywords: steganographic methods, graphic formats, spatial domain, frequency domain, resilience

In this qualification paper, a review of literature sources was conducted, the principles of functioning of steganographic algorithms were analyzed, and key graphic formats were selected. After the implementation and application of the chosen methods to test images, a series of experiments were conducted involving transformations of container formats. The obtained assessment of the hidden information's preservation allowed for a comparison of the results and a conclusion about the significantly higher resistance of frequency-domain methods compared to spatial-domain methods to typical transformations, which confirms their greater suitability for practical use in a real digital environment.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

BMP	Bitmap
DCT	Discrete Cosine Transform
IoT	Internet of Things
JPEG	Joint Photographic Experts Group
MSB	most significant bits
LSB	Least Significant Bit
PNG	Portable Network Graphics
ГПВЧ	Генератор псевдовипадкових чисел
ДКП	Дискретне косинусне перетворення
МКДБ	Метод Куттера-Джордана-Боссена

ЗМІСТ

ВСТУП

Актуальність теми. Інтенсивний розвиток інформаційних технологій та їх впровадження у всі сфери життя людини вивело на новий рівень питання інформаційної безпеки. Основними компонентами інформаційної безпеки є конфіденційність, цілісність, доступність інформації. Проте захист інформації вже далеко не обмежується даними задачами.

Історично, стеганографія бере свій початок з криптографії. Проте, на відміну від криптографічних методів захисту інформації, яка приховує вміст повідомлення, забезпечуючи конфіденційність інформації, стеганографія приховує сам факт передачі інформації. Стеганографічні методи прихованого передавання даних дають змогу непомітно вбудовувати секретну інформацію в цифрові об’єкти (зображення, відео чи аудіо) без очевидних ознак її присутності.

Інтерес до стеганографічних методів у сучасному світі зумовлений зростаючими викликами в галузі інформаційної безпеки, потребою у прихованій передачі даних, захисті приватності, обході цензури, а також необхідністю цифрового маркування авторських матеріалів. В умовах масового обміну мультимедійним контентом та активного контролю над інформаційними потоками, стеганографія забезпечує можливість непомітного вбудовування секретної інформації в цифрові об’єкти без викликання підозри, що робить її цінним інструментом як для особистого, так і для професійного використання.

Широке поширення цифрових медіа та платформ обміну контентом також посилило інтерес до стеганографічних методів у сферах журналістики, правозахисної діяльності та кібербезпеки. Таким чином, розвиток та вдосконалення методів цифрової стеганографії є актуальним завданням, спрямованим на зміцнення інформаційної безпеки у відкритому цифровому середовищі.

Одним із ключових викликів для практичного застосування стеганографії є стійкість методів до форматних перетворень, зокрема перекодування, зміни розміру, стиснення або конвертації зображень. Такі операції часто виконуються автоматично під час обміну файлами в Інтернеті або при завантаженні на онлайн-

платформи. Якщо вбудована інформація втрачається або спотворюється внаслідок таких змін, це суттєво обмежує надійність і застосовність методу. Тому дослідження стійкості стеганографічних алгоритмів до графічних перетворень є необхідним кроком для забезпечення їх ефективності в реальних умовах.

*Мета і задачі дослідження***.** Визначити та порівняти стійкість стеганографічних методів, реалізованих у просторовій та частотній областях, до типових перетворень графічних форматів з метою оцінки їхньої придатності до практичного використання в умовах реального цифрового середовища.

Досягнення поставленої мети передбачало виконання наступних задач.

1. Провести огляд літературних джерел, що стосуються стеганографічного приховування інформації.
2. Проаналізувати принципи функціонування стеганографічних методів у просторовій та частотній областях.
3. Відібрати типові графічні формати та визначити основні види перетворень, які вони здійснюють над зображенням.
4. Реалізувати або обрати відповідні стеганографічні алгоритми для кожної області вбудовування.
5. Застосувати обрані методи до зображень і виконати серію перетворень графічних форматів.
6. Провести оцінку збереження прихованої інформації після кожного типу перетворення.
7. Зіставити отримані результати та зробити висновки щодо стійкості кожного методу та його практичної ефективності.

*Об'єкт дослідження***.** Стеганографічні методи.

*Предмет дослідження***.** Стійкість стеганографічних методів.

*Практичне значення одержаних результатів***.** Отримані висновки дозволяють обґрунтовано обирати найбільш стійкі стеганографічні методи для захування інформації в зображеннях, які піддаються форматним перетворенням під час збереження, пересилання чи публікації в цифровому середовищі. Це особливо актуально для застосувань у сфері інформаційної безпеки, цифрового

водяного маркування, захисту авторських прав та прихованої комунікації, де важливо забезпечити збереження прихованого повідомлення навіть після автоматичного перекодування або стиснення зображень. Результати дослідження можуть бути використані як рекомендаційна база для розробників стеганографічних систем, а також при створенні надійних інструментів прихованого обміну даними.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ СТЕГАНОГРАФІЇ ТА ПЕРЕТВОРЕНЬ ГРАФІЧНИХ ФОРМАТІВ

1.1 Загальна характеристика стеганографії як методу інформаційного захисту

Зростаюча цифровізація всіх сфер життя – від особистого спілкування та фінансових операцій до державних секретів та інфраструктури – породжує безліч викликів, пов'язаних з забезпеченням конфіденційності, цілісності та доступності даних.

Постійний розвиток загроз є одним з головних викликів. Зловмисники невпинно вдосконалюють свої методи та інструменти атак. Це можуть бути нові віруси, програми-вимагачі, фішингові схеми, складні соціальні інженерні прийоми та кібершпигунство. Захисні системи повинні не тільки реагувати на існуючі загрози, а й передбачати потенційні. Крім того, зростаюча складність IT-інфраструктури, що включає хмарні технології, мобільні пристрої, Інтернет речей (IoT) та розподілені мережі, ускладнює завдання забезпечення уніфікованого та надійного захисту інформації. Кожен елемент системи може стати потенційною точкою входу для атаки.

Людський фактор також залишається однією з головних причин витоків даних та інцидентів безпеки. Попри технологічні рішення, людська помилка або недбалість, як-от недостатня обізнаність користувачів, недотримання політик безпеки або навіть навмисні дії інсайдерів, створюють значні ризики. Не варто забувати й про законодавчі та нормативні вимоги; захист інформації регулюється численними законами та стандартами, і їх дотримання є обов'язковим, проте часто вимагає значних ресурсів та постійного моніторингу. Економічний тиск також впливає на процес, адже забезпечення високого рівня безпеки потребує значних інвестицій у технології, персонал та навчання, і організації нерідко стикаються з дилемою між необхідністю захисту та обмеженими бюджетами. Нарешті, глобалізація та транскордонні потоки даних ускладнюють питання юрисдикції та застосування правових норм у разі інцидентів, оскільки інформація часто перетинає кордони.

Виходячи з цих викликів, завдання захисту інформації полягають у забезпеченні конфіденційності, що означає запобігання несанкціонованому доступу до інформації, а також цілісності, гарантуючи, що інформація не була змінена або знищена несанкціонованим способом. Важливим є й забезпечення доступності – доступу до інформації для авторизованих користувачів тоді, коли це необхідно. Додаткові завдання включають неспростовність (можливість підтвердити, що відправник дійсно відправив повідомлення, а одержувач його отримав), ідентифікацію та автентифікацію (перевірка особи користувача або системи, що намагається отримати доступ до ресурсів). Для ефективного захисту також необхідні аудит та моніторинг (постійний контроль за системою для виявлення потенційних загроз та інцидентів), розробка політик та процедур (створення чітких правил та інструкцій) та, безумовно, навчання та підвищення обізнаності персоналу щодо правил безпеки та методів реагування на загрози. механізмів, таких як автоматизовані системи для виявлення та блокування атакуючих, щоб забезпечити стійкість та надійність мережевого середовища призвести до значних проблем у доступності мережевих ресурсів та сервісів, що робить їх надзвичайно небезпечними. Захист від таких атак вимагає розробки та впровадження ефективних захисних.

Стеганографія – це мистецтво і наука приховування факту існування повідомлення. На відміну від криптографії, яка фокусується на приховуванні змісту повідомлення, роблячи його незрозумілим для сторонніх, стеганографія має на меті приховати сам факт передачі або існування повідомлення. Це означає, що для стороннього спостерігача повідомлення взагалі не існує [1].

Основні принципи стеганографії включають використання контейнера даних, який є каналом для приховування повідомлення. Це може бути цифровий файл, наприклад, зображення, аудіо, відео чи текстовий файл, або навіть фізичний об'єкт. Повідомлення інтегрується в цей контейнер таким чином, щоб зміни були непомітними для людського ока або слуху, або для автоматичних систем аналізу. Для підвищення безпеки може використовуватися секретний ключ, який дозволяє лише авторизованим користувачам витягувати приховане повідомлення. Головною метою стеганографії є збереження непомітності: якщо

контейнер виглядає підозріло або відрізняється від звичайних файлів, це може привернути увагу до прихованого повідомлення. Найпростіша модель стеганосистеми виглядає наступним чином [2]

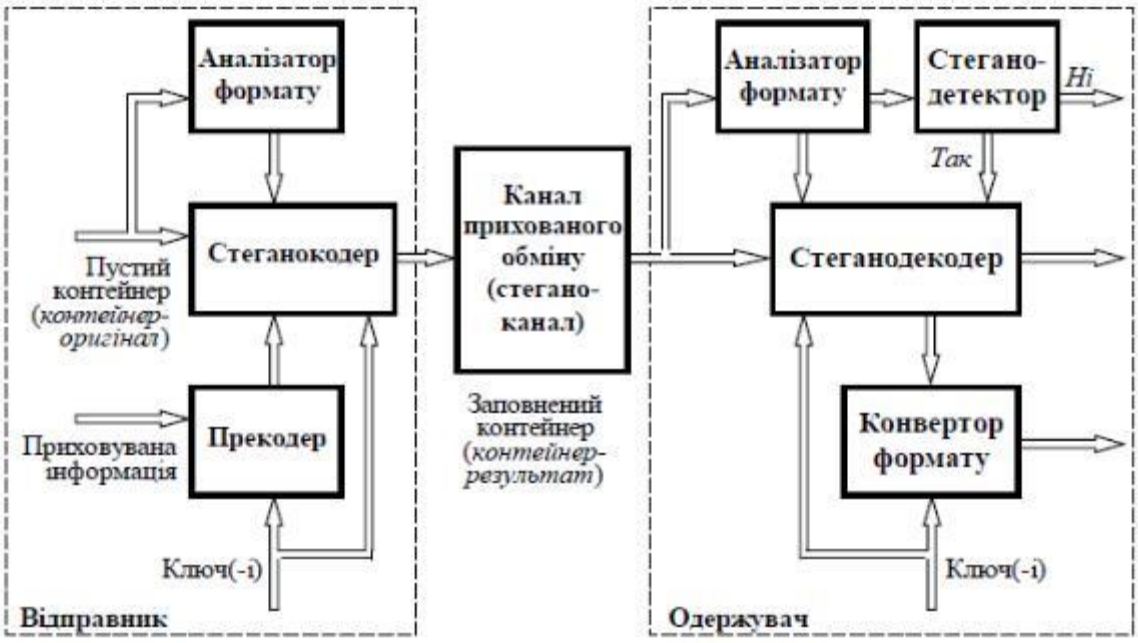


Рисунок 1.1 – Модель стеганосистеми

Розпишемо детальніше компоненти моделі, які, власне, дежать в основі стеганосистеми.

«Прекодер» – це блок відповідає за попередню обробку приховуваної інформації. Він може виконувати такі функції, як стиснення даних для зменшення їхнього обсягу, шифрування для підвищення конфіденційності (хоча стеганографія сама по собі є методом приховування, часто її комбінують з криптографією), додавання надмірності для корекції помилок, або перетворення формату інформації для кращої інтеграції в контейнер. «Прекодер» може використовувати Ключ(-і) для шифрування або інших операцій.

«Аналізатор формату» – це модуль аналізує структуру та особливості формату пустого контейнера. Він виявляє місця, де можна непомітно вбудовувати приховувану інформацію, визначає його характеристики (розмір, тип, бітові потоки тощо), які можуть бути використані «Стеганокодером».

«Стеганокодер» – це ключовий елемент системи Відправника. Він отримує попередньо оброблену приховувану інформацію від Прекодера та пустий контейнер разом з інформацією про його формат від Аналізатора формату. Завдання «Стеганокодера» – вбудувати приховувану інформацію в контейнер таким чином, щоб це було максимально непомітно. Цей процес може використовувати Ключ, який вказує, як саме відбувається вбудовування (наприклад, які біти змінювати, або яка послідовність дій). Результатом роботи «Стеганокодера» є «Заповнений контейнер»

«Стегано-детектор» – цей блок є необов'язковим, але дуже важливим елементом для виявлення факту приховування. Його завдання – визначити, чи містить Заповнений контейнер приховану інформацію. Він може використовувати різні методи стеганалізу. Його вихід може бути "Так" (інформація присутня) або "Ні" (інформації немає). Якщо «Стегано-детектор» визначив, що інформація присутня ("Так"), вона передається до Стеганодекодера, а якщо ні, то може бути виведений результат "Ні" (Ні).

«Стеганодекодер» – цей блок відповідає за вилучення прихованої інформації із Заповненого контейнера. Він використовує інформацію про формат від Аналізатора формату та, якщо потрібно, той самий Ключ(-і), який використовувався під час кодування, щоб правильно розпізнати та вилучити вбудовані дані. Результатом його роботи є витягнута приховувана інформація (можливо, ще в закодованому вигляді)

«Конвертор формату» – цей блок виконує зворотну функцію до «Прекодера». Він приймає витягнуту інформацію від «Стеганодекодера» і перетворює її до початкового, придатного для використання формату. Це може включати дешифрування (якщо інформація була зашифрована «Прекодером»), розпакування даних або корекцію помилок. Для дешифрування також може використовуватись Ключ(-і). Результатом є Приховувана інформація у її вихідному вигляді.

Переваги стеганографії як методу інформаційного захисту полягають у її здатності приховувати факт зв'язку. На відміну від криптографії, яка сигналізує про існування зашифрованого повідомлення, стеганографія прагне повністю

приховати комунікацію, що може бути корисно в ситуаціях, де сам факт спілкування є небажаним або небезпечним. Вона також може дозволити обійти цензуру та моніторинг, оскільки приховане повідомлення виглядає як звичайний, нешкідливий контент, і системи моніторингу, що шукають зашифрований трафік, можуть його не помітити.

Однак стеганографія має й свої недоліки та обмеження. Вона є досить крихкою: приховане повідомлення може бути легко знищено або пошкоджено при будь-якій модифікації контейнера, наприклад, при зміні розміру зображення або стисненні з втратами. Також існує обмежена ємність: кількість інформації, яку можна приховати в контейнері без помітних змін, зазвичай обмежена. Крім того, не варто забувати про детектування: існують методи та інструменти (стеганаліз), які можуть виявляти ознаки прихованої інформації в файлах, і постійно розробляються нові методи стеганалізу. Нарешті, існують легальні та етичні аспекти, оскільки стеганографія може бути використана для приховування незаконної або шкідливої інформації, що створює етичні та юридичні дилеми.

Застосування стеганографії, хоча й не є панацеєю для всіх проблем інформаційного захисту, знаходить своє місце в нішевих сферах. Це включає захист авторських прав, приховану комунікацію у випадках, де відкрите використання криптографії може викликати підозри, а також для цілісності даних, шляхом додавання прихованих контрольних сум або хешів для перевірки цілісності файлів. Підсумовуючи, стеганографія – це потужний інструмент, який доповнює інші методи інформаційного захисту, пропонуючи унікальний підхід до приховування факту існування інформації. Проте, її ефективність залежить від контексту застосування та постійного розвитку як методів приховування, так і методів детектування.

Застосування охоплює як легальні, так і потенційно зловмисні сфери [3].

Захист інформації:

- Конфіденційна передача даних.
- Військова і дипломатична комунікація.
- Збереження приватності для людей, які живуть в авторитарних режимах.

Захист авторських прав:

- Цифрове маркування зображень, відео та аудіо.
- Верифікація автентичності.

Безпека в інформаційних системах:

- Вбудовані механізми перевірки цілісності даних.
- Система прихованих міток у документах.

Зловмисне використання:

- Приховування шкідливого ПЗ або команд.
- Комунікація між зловмисниками.
- Обхід систем моніторингу трафіку (IDS/IPS).

Освіта та дослідження:

- Навчання безпечному обміну інформацією.
- Розробка нових методів захисту інформації.

Застосування в мобільних застосунках і соціальних мережах:

- Приховування особистої інформації у фото.
- Захист від цензури в соцмережах.

1.2 Класифікація стеганографічних методів

Історія стеганографії сягає глибокої давнини, задовго до появи цифрових технологій, демонструючи прагнення людства приховувати інформацію. У класичній, або аналоговій, стеганографії методи приховування повідомлень традиційно поділялися на дві основні категорії: хімічні та фізичні. Хімічні методи включали використання невидимих чорнил, які ставали видимими лише за певних умов, наприклад, під впливом тепла або спеціальних реагентів. Фізичні ж методи були більш різноманітними і охоплювали техніки від вишкрябування написів на воскових табличках під шаром воску до татуювань на голові раба, які приховувалися відрослим волоссям.

Загалом автори [4] виділяють класичну, цифрову, квантову та лінвістичну стеганографію. Короткий огляд класичної криптографії наведено дещо вище. Цифрова стеганографія полягає у приховуванні секретних даних у цифрових

носіях, таких як зображення, аудіо, відео, текст або мережеві пакети, шляхом внесення непомітних для людського сприйняття модифікацій у надлишкові біти носія. Квантова стеганографія використовує принципи квантової механіки, зокрема суперпозицію та заплутаність, для приховування інформації, забезпечуючи теоретично неможливість виявлення прихованого повідомлення без порушення його квантового стану. Лінгвістична стеганографія займається приховуванням інформації у текстових документах, використовуючи особливості мови – синтаксичні, семантичні або стилістичні зміни, що не змінюють видимого змісту тексту, але кодують приховане повідомлення.

Розвиток інформаційних технологій значно розширив можливості цифрової стеганографії, породивши безліч методів, які можна класифікувати за різними критеріями.

На рисунку 1.2 наведено множину критеріїв, за якими можна проводити класифікацію методів цифрової стеганографії [5-7].

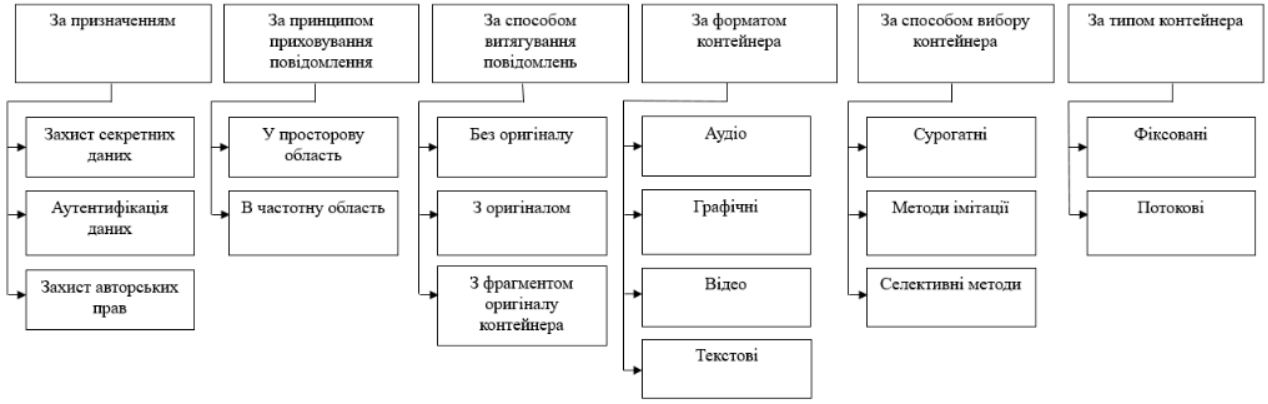


Рисунок 1.2 – Класифікація методів цифрової стеганографії

Одним з таких критеріїв є тип носія. Це найфундаментальніший критерій, який визначає природу файлу або потоку даних, що використовується для приховування секретної інформації. На рисунку 1.3 наведено класифікацію методів цифрової стеганографії за типом контейнера.

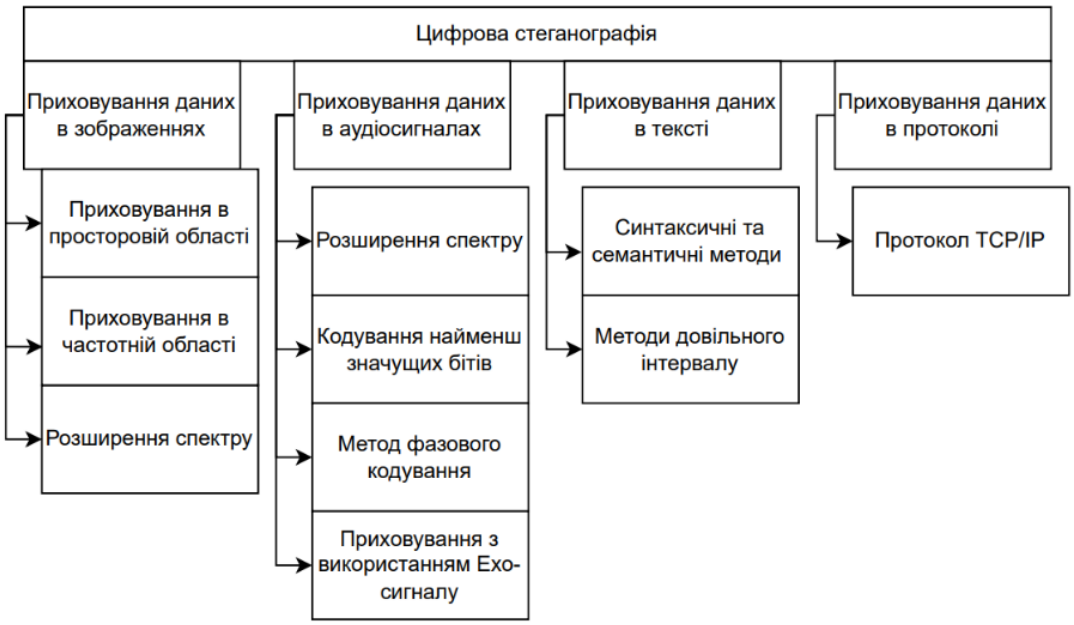


Рисунок 1.3 – Класифікація стеганографічних методів за типом контейнера

Згідно рисунку 1.3 стеганографічні техніки поділяються на чотири основні категорії залежно від типу носія, в якому приховуються дані: зображення, аудіосигнали, текст та протоколи. Кожна з цих категорій далі деталізується на конкретні методи, що використовуються для реалізації приховування.

Для приховування даних у зображеннях схема виділяє три основні підходи: приховування у просторовій області, що стосується маніпуляцій з пікселями зображення; приховування у частотній області, що передбачає використання перетворень, таких як дискретне косинусне перетворення, та розширення спектру. У випадку аудіосигналів, методи включають розширення спектру, кодування найменш значущих бітів (LSB), метод фазового кодування та приховування з використанням Exo-сигналу, що свідчить про різноманіття технік, які експлуатують особливості слухового сприйняття.

Приховування даних у тексті поділяється на синтаксичні та семантичні методи, що натякає на використання мовних особливостей для вбудовування інформації, а також методи довільного інтервалу. Нарешті, найпростіша категорія – приховування даних у протоколах – вказує на використання протоколу TCP/IP, що може включати маніпуляції з заголовками або полями пакетів для передачі прихованих даних. Загалом, схема ілюструє широке

розмаїття підходів до цифрової стеганографії, адаптованих під різні типи цифрових носіїв.

За способом застосування стеганографічні методи можна прокласифікувати наступним чином, зображеним на рисунку 1.4.

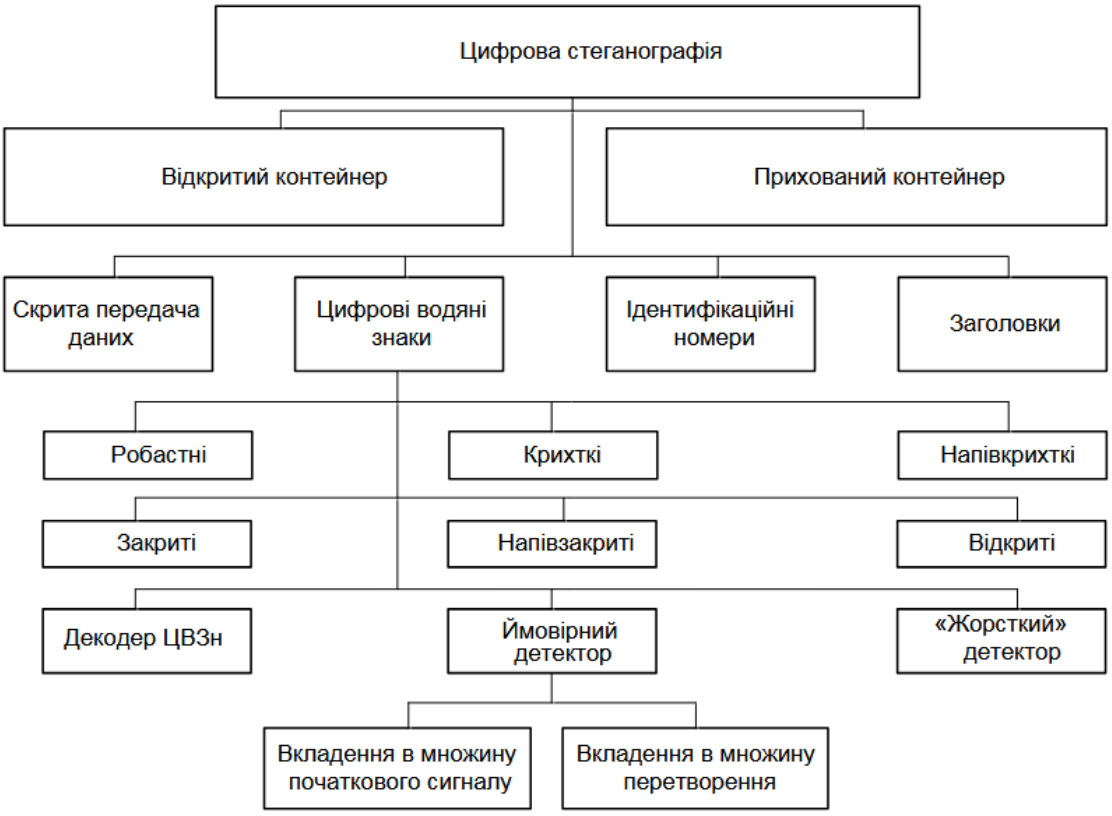


Рисунок 1.4 – Класифікація стеганографічних методів за способом застосування

Серед груп методів виділяється прихована передача даних, яка фокусується на приховуванні конфіденційної інформації для її таємної передачі, де ключова мета – забезпечити, щоб сам факт комунікації залишився непоміченим для стороннього спостерігача. Паралельно існують цифрові водяні знаки (ЦВЗ), спеціалізований метод, що застосовується для захисту авторських прав, аутентифікації та відстеження розповсюдження контенту [10]. ЦВЗ поділяються на робастні (стійкі до спотворень носія), крихкі (чутливі до будь-яких змін, що слугують для виявлення втручань) та напівкрихкі (проміжний варіант), а також можуть бути закритими (потребують оригіналу для вилучення) або відкритими (можуть бути вилучені без оригіналу).

Окрім цього, важливими елементами є приховування за допомогою ідентифікаційних номерів, що передбачає вбудовування унікальних ідентифікаторів у носій таким чином, щоб їхня присутність була непомітною, але вони могли бути використані для трасування чи інших цілей. Також застосовується приховування інформації у заголовках файлів або мережевих протоколів, використовуючи невикористані, зарезервовані або рідко використовувані поля для маскування секретного повідомлення серед звичайних службових даних.

1.3 Основні формати графічних зображень та особливості їх перетворення

Розуміння форматів графічних зображень та особливостей їх перетворення є критично важливим для ефективного застосування та аналізу стеганографічних технік. Різноманітність цих форматів обумовлена потребами у якості, розмірі файлу, прозорості та можливості редагування, і кожен з них має свої унікальні властивості, що впливають на вибір стеганографічного методу та його стійкість.

Основними форматами графічних зображень, з якими найчастіше мають справу у цифровій стеганографії, є растрові та векторні зображення, хоча більшість стеганографічних методів зосереджені на растрових форматах через їхню дискретну структуру пікселів. Серед растрових форматів особливо виділяються BMP, PNG та JPEG.

BMP є нестисненим або мінімально стисненим форматом, що зберігає інформацію про кожен піксель окремо. Його основна характеристика полягає в тому, що він зазвичай зберігає інформацію про кожен піксель зображення окремо, без застосування складних алгоритмів стиснення із втратами. Це означає, що кожен піксель у BMP-файлі відповідає певному кольору, і цей колір представлений у вигляді комбінації значень червоного, зеленого та синього (RGB) компонентів, або ж використовується палітра кольорів для індексованих зображень. Завдяки цій "прямій" відповідності між пікселями зображення та даними у файлі, BMP-файли відрізняються високою якістю зображення, оскільки не відбувається втрати деталей під час збереження.

Однак, простота структури BMP-файлу та відсутність значного стиснення призводять до того, що файли цього формату часто мають дуже великий розмір, особливо для зображень з високою роздільною здатністю та великою глибиною кольору. Це робить їх менш зручними для використання в інтернеті або для зберігання на пристроях з обмеженим обсягом пам'яті. З точки зору стеганографії, великий розмір і мінімальне стиснення роблять BMP ідеальним кандидатом для методів, що працюють у просторовій області, таких як кодування найменш значущих бітів (LSB), оскільки навіть значна кількість прихованих даних, розподілених по всьому зображенню, не викликає помітних візуальних спотворень. Проте, відсутність стиснення також означає, що приховані дані не захищені від подальшого стиснення або перетворення у менш "прості" формати.

На противагу BMP, формат PNG є значно досконалішим форматом для растрових зображень, оскільки він забезпечує стиснення без втрати якості. Це досягається за рахунок використання складних алгоритмів, таких як DEFLATE, які кодують повторювані послідовності пікселів та шаблони, що дозволяє значно зменшити розмір файлу без будь-яких втрат оригінальної інформації про зображення. Ця властивість робить PNG надзвичайно привабливим для використання в веб-графіці, для іконок, логотипів та будь-яких зображень, де важлива абсолютна чіткість і відсутність артефактів стиснення. Додатковою важливою особливістю PNG є підтримка альфа-каналу, що дозволяє реалізовувати різні рівні прозорості, інтегруючи зображення бездоганно в будь-яке фонове середовище.

З точки зору стеганографії, той факт, що PNG є форматом без втрат, створює сприятливі умови для приховування даних. Приховані дані, вбудовані, наприклад, методом LSB, мають високі шанси зберегтися, оскільки алгоритми стиснення PNG не відкидають інформацію, а лише ефективніше її кодують. Однак, незважаючи на це, агресивніші стеганографічні методи, які вносять суттєві або нетипові для природних зображень зміни у послідовності бітів, можуть бути виявлені. Алгоритми стиснення PNG, хоч і працюють без втрат, можуть виявити ці "аномалії" під час кодування, що потенційно може призвести до зміни розміру файлу, нехарактерного для чистого зображення, або до появи

певних статистичних відхилень, які можуть бути ідентифіковані методами стегоаналізу.

Найбільш поширеним для фотографій є JPEG, який використовує стиснення із втратами, базуючись на дискретному косинусному перетворенні (DCT). Саме через це JPEG-зображення є складнішим, але й цікавішим об'єктом для стеганографії.

На рисунку 1.5 представлено схему роботи JPEG-формату.

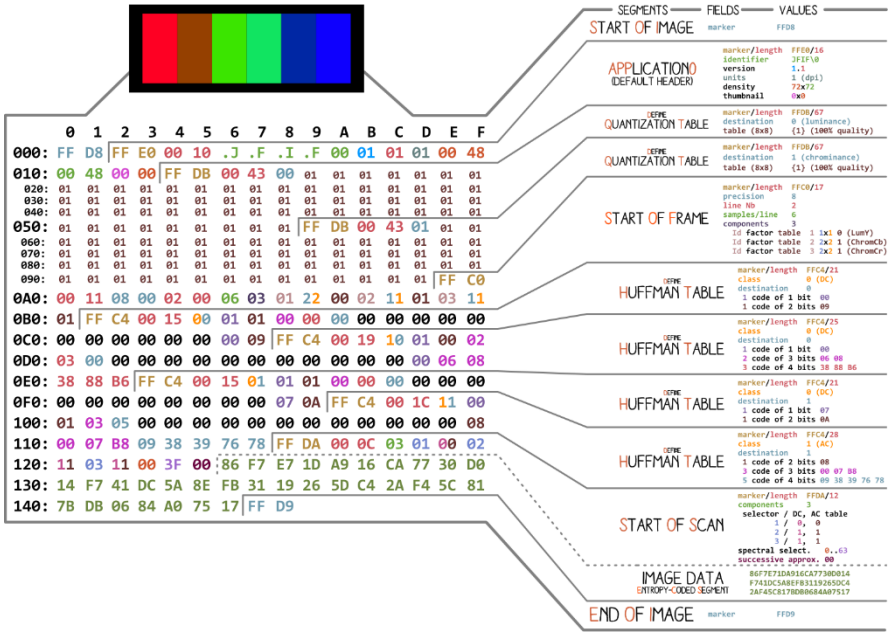


Рисунок 1.5 – Принцип роботи JPEG формату

Принцип роботи JPEG-файлу, як видно з рисунку, базується на сегментній організації даних та застосуванні трансформації дискретного косинусного перетворення (DCT) та квантування. Файл починається з маркера START OF IMAGE (FFD8), який вказує на початок JPEG-файлу. Далі йдуть різні сегменти, кожен з яких починається з унікального маркера та містить специфічну інформацію про зображення. Наприклад, сегмент APPLICATION (FFE0) може містити метадані про зображення, такі як його ідентифікатор, одиниці виміру, роздільна здатність, а також дані мініатюри.

Ключову роль у стисненні JPEG відіграють QUANTIZATION TABLE (FFDB) та HUFFMAN TABLE (FFC4). Квантуючі таблиці визначають ступінь втрати інформації, оскільки вони містять коефіцієнти, які використовуються для

значень DCT-коефіцієнтів, що призводить до відкидання менш значущих деталей і, як наслідок, до зменшення розміру файлу. Huffman-таблиці, у свою чергу, використовуються для ентропійного кодування (стиснення без втрат) квантованих DCT-коефіцієнтів. Рисунок показує наявність окремих таблиць для яскравості (Luminance) та кольорових компонентів (Chrominance), що підкреслює психовізуальну модель JPEG, яка експлуатує той факт, що людське око чутливіше до змін яскравості, ніж до змін кольору.

Після цих таблиць йде сегмент START OF FRAME (FFC0), що описує характеристики самого зображення, такі як розмір (кількість рядків/семплів, кількість компонентів) та фактори дискретизації для різних компонентів. Кульмінацією є сегмент START OF SCAN (FFDA), який сигналізує про початок закодованих даних зображення. Власне IMAGE DATA (Minimally-coded segment) є результатом застосування DCT, квантування та Huffman-кодування до піксельних даних. Вся ця послідовність завершується маркером END OF IMAGE (FFD9). Таким чином, JPEG працює шляхом перетворення просторових даних зображення у частотну область, їх квантування для досягнення стиснення із втратами, а потім ентропійного кодування отриманих коефіцієнтів для подальшого зменшення розміру файлу.

1.4 Критерії оцінки якості стеганографічних методів

Оцінка якості стеганографічних систем є багатогранним завданням, що вимагає врахування низки взаємопов'язаних критеріїв. Як це прекрасно ілюструє трикутник стеганографії (рисунок 1.6), що складається з ємності, непомітності та стійкості, ці характеристики часто перебувають у конфлікті одна з одною.

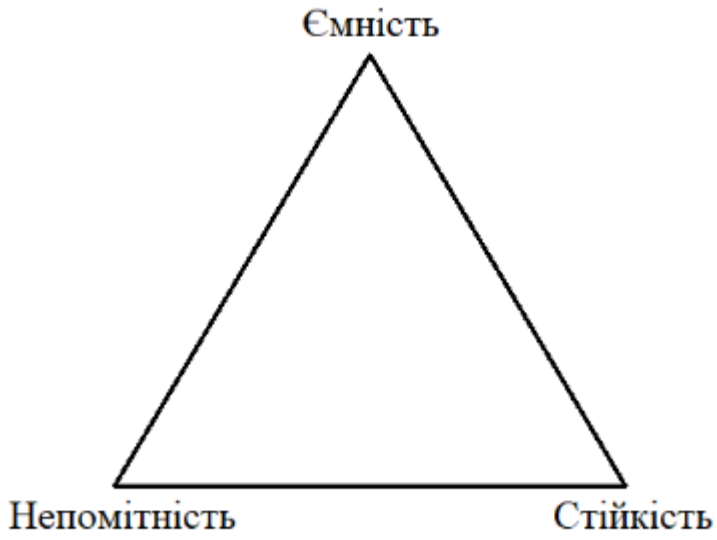


Рисунок 1.6 – Взаємозв’язок між критеріями якості стеганографічних систем

Досягнення оптимального балансу між ними визначає успішність та застосовність конкретного стеганографічного методу в реальних умовах. Кожен з цих критеріїв, а також додаткові аспекти, такі як безпека та час обробки, відіграють вирішальну роль у виборі та розробці стеганографічних рішень, які можуть бути застосовані до різноманітних носіїв, як це показано на схемі класифікації.

Ємність (Capacity), розташована на вершині трикутника, визначає максимальну кількість секретної інформації, яку можна приховати в заданому носії без суттєвого погіршення інших критеріїв. Це безпосередньо залежить від характеристик носія. Наприклад, зображення або аудіофайли, як видно зі схеми класифікації, зазвичай мають високу надмірність даних, що дозволяє приховувати значні обсяги інформації, особливо методами, що працюють у просторовій області або з використанням найменш значущих бітів (LSB). У таких випадках, як кодування LSB для зображень або аудіо, можна досягти значної ємності, оскільки кожен біт носія може бути потенційним місцем для прихованого біту. Однак, чим більша ємність, тим вищий ризик виявлення прихованих даних, оскільки вбудовування більшої кількості інформації може призвести до більш помітних статистичних або перцептивних змін у носії. Для

текстової стеганографії, як правило, характерна низька ємність через відносну відсутність надмірності у текстових даних, що обмежує кількість прихованої інформації, незалежно від використання синтаксичних, семантичних методів чи методів довільного інтервалу.

Непомітність (Imperceptibility), або прихований характер, є фундаментальним критерієм, що визначає, наскільки важко виявити присутність прихованого повідомлення. Це критично важливо, оскільки основна мета стеганографії – зробити сам факт передачі повідомлення непомітним. Якщо приховане повідомлення змінює носій таким чином, що це стає помітним для людського сприйняття (ока чи вуха) або для автоматизованих інструментів стегоаналізу, то стеганографічна система вважається неефективною. Методи, що працюють у частотній області, як це показано для зображень та аудіо ("Приховування у частотній області", "Метод фазового кодування", "Розширення спектру"), часто прагнуть максимізувати непомітність, оскільки зміни в частотних коефіцієнтах менш помітні, ніж прямі зміни пікселів або семплів. Для мережевої стеганографії ("Протокол TCP/IP") непомітність означає, що приховані дані повинні виглядати як звичайний мережевий трафік, не викликаючи підозр у моніторингових систем. Досягнення високої непомітності часто вимагає компромісу з ємністю, оскільки більша кількість прихованих даних може призвести до помітніших спотворень.

Стійкість (Robustness), третя вершина трикутника, характеризує здатність прихованого повідомлення витримувати різні операції над носієм без втрати інформації. Ці операції можуть включати навмисні атаки стегоаналізу, а також звичайні маніпуляції з даними, такі як стиснення (наприклад, перекодування JPEG), фільтрація, зміна розміру, обрізка, додавання шуму або конвертація формату. Робастність є особливо важливою для цифрових водяних знаків, де метою часто є захист авторських прав, і водяний знак повинен залишатися недоторканим навіть після спроб його видалення або спотворення. Методи розширення спектру, як це зазначено для зображень та аудіо, є одними з найбільш робастних, оскільки вони розподіляють приховану інформацію по широкому діапазону носія, що робить її стійкою до локальних пошкоджень.

Однак, методи, які надають перевагу високій ємності (наприклад, проста модифікація LSB), зазвичай є менш робастними, оскільки приховані дані легко руйнуються при незначних змінах носія. Оптимізація всіх трьох критеріїв є складним інженерним завданням, оскільки вони часто суперечать один одному, і для конкретного застосування необхідно знайти оптимальний баланс, що відповідає поставленим цілям.

Дослідження стійкості до перетворень графічних форматів є критично важливим у контексті стеганографії, оскільки цифрові зображення рідко залишаються у своєму початковому вигляді після вбудовування прихованої інформації. Зображення часто піддаються різноманітним операціям, таким як стиснення (наприклад, перетворення в JPEG з високим рівнем компресії), зміна розміру для публікації в мережі, обрізка, застосування фільтрів для покращення якості або просто конвертація в інший формат для сумісності. Кожне з цих перетворень може призвести до втрати або спотворення частини даних зображення, і, відповідно, до руйнування прихованого повідомлення. Якщо стеганографічна система не враховує ці типові трансформації, прихована інформація може бути легко втрачена, що робить її непридатною для практичного застосування.

Таким чином, розробка робастних стеганографічних методів, які можуть витримувати ці перетворення, є ключовим завданням. Це вимагає глибокого розуміння того, як різні формати зберігають і обробляють дані, а також як конкретні алгоритми стиснення та редагування впливають на біти, які використовуються для приховування інформації. Лише завдяки ретельному аналізу та тестуванню стійкості до таких маніпуляцій можна створити стеганографічні системи, які є не тільки непомітними та ємними, але й достатньо надійними для передачі конфіденційних даних у реальному світі, де зображення постійно піддаються різним модифікаціям.

РОЗДІЛ 2 МАТЕМАТИЧНІ ОСНОВИ СТЕГАНОГРАФІЧНИХ МЕТОДІВ

Для проведення досліджень розглянемо кейс, коли секретною інформацією є звичайне текстове повідомлення, а контейнером для приховування є зображення. На першому етапі необхідно спершу вибрати методи вбудовування інформації в контейнер. На рисунку 2.1 продемонстровано, що існує дві великі групи стеганографічних методів, що дозволяють приховувати інформацію в просторовій та частотній області.

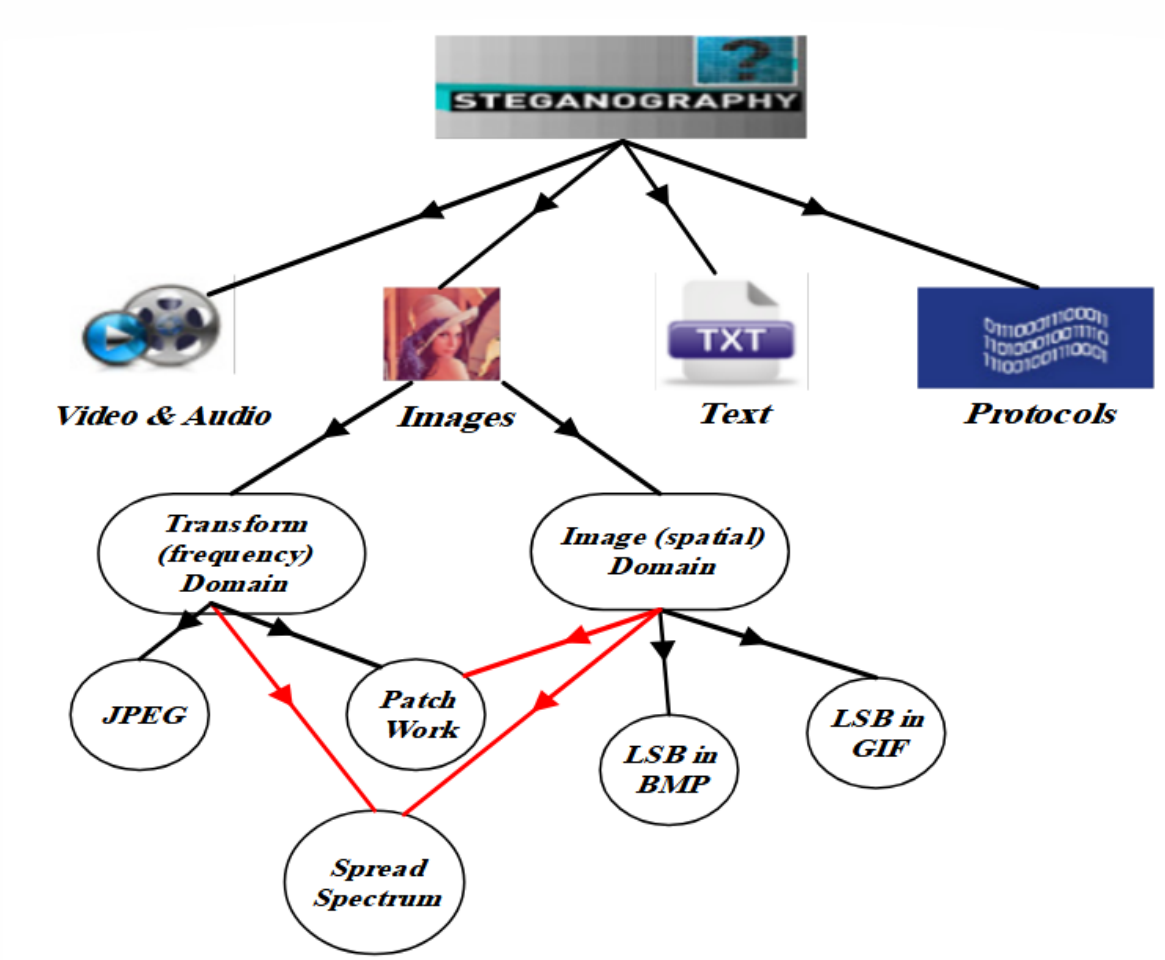


Рисунок 2.1 – Основні напрямки стеганографії для приховування інформації в зображеннях

Як бачимо просторові методи рекомендовано використовувати для форматів BMP та GIF, а разом з частотними методами приховування інформації рекомендовано використовувати jpeg. В наступних підрозділах розглянемо алгоритми кожної групи методів.

2.1 Вибір методу приховування інформації в просторовій області

2.1.1 Метод заміни наймолодшого біта

Метод заміни наймолодшого біта (англ. Least Significant Bit - LSB) є базовим стеганографічним підходом, що використовується для приховування інформації в цифрових зображеннях. Його основна ідея полягає у зміні найменш значущих бітів байтів, які зберігають колірну інформацію пікселів. Оскільки ці біти мають найменший вплив на загальне значення кольору, то значення пікселю фактично не змінюється. Завдяки малій зміні значення пікселя, візуально зображення майже не відрізняється від оригіналу, що дозволяє приховати інформацію без викликання підозри.

У цифрових зображеннях, представлених у форматі RGB, кожен піксель складається з трьох компонентів: червоного, зеленого та синього (рисунок 2.2).

Рисунок 2.2 – Формат RGB

Кожна з цих компонент зазвичай має значення від 0 до 255, яке записується у вигляді одного байта (8 бітів). Наприклад, якщо яскравість червоного каналу для певного пікселя дорівнює 150, то у двійковій системі це виглядає як 10010110.

Наймолодший біт – це останній (правий) біт у цьому записі. У нашому прикладі він дорівнює 0. Метод LSB полягає у тому, щоб змінити цей біт на значення, що відповідає бітові повідомлення, яке потрібно приховати. Це дозволяє сховати інформацію на побітовому рівні без суттєвих змін зображення. У випадку нашого прикладу зі значенням червоного пікселя 150, заміна наймолодшого біта або ж залишить значення пікселя без змін, або ж значення пікселю стане 151. Зрозуміло, що така незначна зміна колірної гами залишиться непоміченою для людського ока. Цей принцип працює для кожного каналу

окремо, тобто на один піксель можна закодувати до трьох біт повідомлення (по одному на кожен з каналів RGB)

Розглянемо детальніше алгоритм методу. На рисунку 2.3 наведено принцип роботи методу, описаний вище.

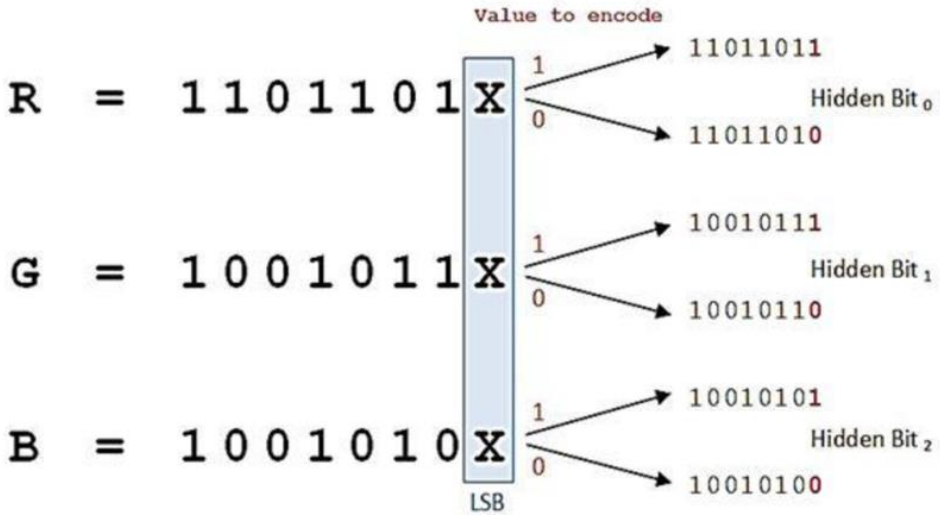


Рисунок 2.3 – Принцип роботи методу LSB [11]

З рисунку очевидно, що по-перше, приховування може відбуватися в кожній з трьох компонент RGB моделі, а по-друге, що немає жодного значення, який біт стояв на останньому місці, бо він просто замінюється на певний біт текстового повідомлення. Проте, слід зазначити, що дослідники експериментують з кількістю останніх біт для приховування і можуть використовувати від одного до трьох біт [12]. На рисунку 2.4 наведено приклад приховування інформації в двох останніх бітах

Піксель зображення до вбудовування

Red								Green								Blue							
0	1	1	0	0	1	**0**	**0**	0	1	1	0	1	1	**0**	**1**	1	0	1	1	0	1	**1**	**1**

Секретне повідомлення

0	**1**	**1**	**0**	**0**	**1**	0	0	0	1	1	0

Піксель зображення після вбудовування

Red								Green								Blue							
0	1	1	0	0	1	**0**	**1**	0	1	1	0	1	1	**1**	**0**	1	0	1	1	0	1	**0**	**1**

Рисунок 2.4 – Приховування інформації в двох останній бітах

Схожим чином приховування інформації можна виконувати і в трьох наймолодших бітах. Більшу кількість бітів не рекомендовано використовувати, оскільки це може привести до спотворення зображення.

Для практичної реалізації методу, необхідно виконати послідовність кроків:

- перетворити повідомлення у бітовий потік;
- додати мітки початку та кінця повідомлення;
- вбудувати біти у зображення-контейнер;
- зберегти нове зображення.

Для перетворення повідомлення в послідовність бітів, спочатку кожен символ тексту необхідно подати у вигляді коду ASCII або Unicode, що відображає його числове значення; далі це числове значення перетворюється у двійкову систему (бінарний код) з фіксованою довжиною, зазвичай 8 бітів для ASCII; отримані двійкові представлення символів об'єднуються в єдиний бітовий потік, який потім можна використовувати для приховування у цифровому носії.

До переваг методу відносять:

- простоту реалізації;
- високу непомітність;
- високу швидкість;
- високу місткість.

Попри простоту та ефективність методу заміни наймолодшого біта, його основним недоліком є низька стійкість до будь-яких модифікацій або перетворень зображення. Зокрема, такі операції як стиснення у формат JPEG, зміна розміру, фільтрація, корекція яскравості чи контрасту можуть пошкодити або повністю знищити приховані біти. Це пояснюється тим, що наймолодші біти містять дуже дрібні зміни, які легко губляться під час обробки, адже більшість графічних алгоритмів просто ігнорують або перезаписують ці незначущі для зображення дані.

Крім того, навіть автоматичне повторне збереження зображення у форматі, що застосовує втрати (наприклад, JPEG), може призвести до руйнування вбудованої інформації. Це суттєво обмежує використання LSB-методу для

передавання конфіденційних або важливих даних у відкритому середовищі, де зображення може бути оброблене або змінене користувачем чи системою.

Ще одним вагомим недоліком методу заміни наймолодшого біта є відсутність надійного захисту від зловмисників, оскільки сам підхід не передбачає шифрування або приховування місця зберігання даних. Якщо зловмисник підозрює, що у зображенні приховано інформацію методом LSB, він може просто зчитати останні біти кольорових каналів пікселів у прямому порядку. Завдяки простоті структури цього методу, навіть базові навички програмування дозволяють автоматично зчитати потенційний бітовий потік і спробувати перетворити його назад у текст або інші зрозумілі дані.

Більш того, існують спеціалізовані інструменти й програми, які дозволяють проводити аналіз зображень на предмет прихованих даних, автоматично скануючи наймолодші біти. Відсутність маскування або рандомізації розташування бітів робить повідомлення вразливим: навіть якщо зловмисник не знає, що саме заховано, він може експериментально отримати частину змісту або встановити сам факт стеганографії.

Щоб усунути вразливість методу LSB до легкого зчитування даних, однією з найпростіших і водночас ефективних модифікацій є використання псевдовипадкового розподілу бітів повідомлення по пікселях зображення. Замість того, щоб просто записувати інформацію у послідовні пікселі, можна використовувати генератор псевдовипадкових чисел з певним ключем, який визначатиме порядок обходу пікселів. Реалізується цей підхід за допомогою генератора псевдовипадкових чисел (ГПВЧ). Алгоритм працює так: задається початковий ключ, на його основі генератор створює послідовність чисел, які вказують індекси пікселів або кольорових каналів, у які треба вбудовувати біти повідомлення. Таким чином, навіть якщо зловмисник зчитує наймолодші біти у звичному порядку, він отримає беззмістовний потік, а не справжнє повідомлення. Відновити правильну послідовність бітів можна лише маючи ключ, який використовувався для генерації випадкового порядку.

В статті [13] запропонована інша модифікація методу. Секретний біт повідомлення S_i вбудовується в останній біт кольору зображення проте з

використанням деяких старших бітів. Наприклад, беремо два старші біти (most significant bits - MSB) – C_1 та C_2, після чого застосовуємо певну бінарну операцію до цих операндів. Кількість використаних старших бітів і їхні позиції в байті та порядковий номер цієї бінарної операції є частинами складного секретного ключа. Даний підхід проілюстровано на рисунку 2.5.

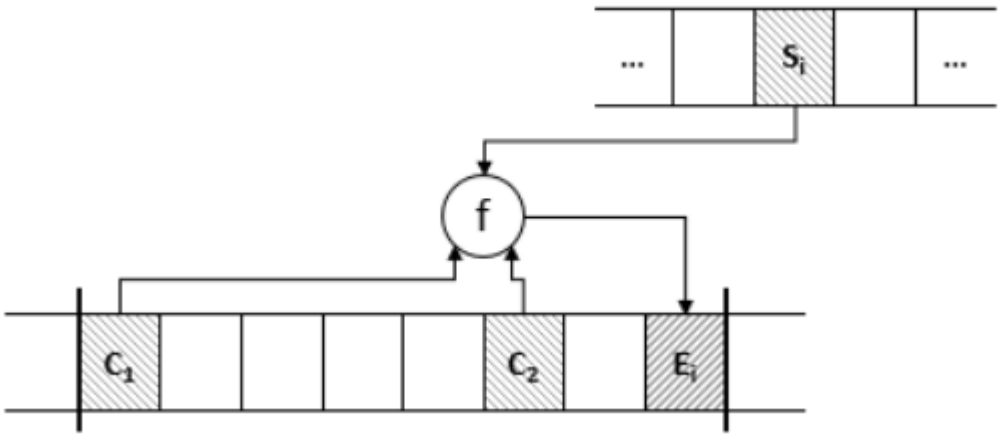


Рисунок 2.5 – Модифікація методу заміни наймолодшого біта

Метод LSB доцільно застосовувати в тих випадках, коли потрібно непомітно передати невеликий обсяг конфіденційної інформації в цифрових зображеннях, аудіо- чи відеофайлах без суттєвого впливу на їхню якість. Він особливо корисний у ситуаціях, коли не очікується активного аналізу або модифікації файлів, наприклад, для особистого використання чи в закритих системах зв'язку. Основні обмеження методу – низька стійкість до стиснення, переформатування або редагування файлу, а також вразливість до виявлення за допомогою стеганоаналітичних інструментів, що робить його непридатним для використання в умовах високої загрози чи ворожого середовища. Проте ми використаємо його в даній роботі для дослідження.

2.1.2 Метод Куттера-Джордана-Боссена

Ще одним із найпопулярніших та широко використовуваних підходів у стеганографії, який відноситься до класу методів приховання інформації на основі заміни найменш значущих бітів є метод Куттера-Джордана-Боссена

(МКДБ). Цей метод поєднує простоту реалізації з достатньою ефективністю та непомітністю, що робить його особливо привабливим для вбудовування секретних даних у цифрові зображення. Ідея МКДБ полягає у зміні лише тих бітів пікселів, які найменше впливають на якість візуального сприйняття зображення, що дозволяє зберегти зовнішній вигляд файлу практично без змін.

Метод Куттера-Джордана-Боссена (МКДБ) часто приховує інформацію саме в синьому кольорі зображення через особливості сприйняття людським оком. Зір людини значно менш чутливий до змін у синьому спектрі порівняно з червоним або зеленим, тому модифікації найменш значущих бітів у синьому каналі практично непомітні для спостерігача. Це дозволяє ефективніше вбудовувати приховані дані без видимих артефактів, зберігаючи високу якість і природний вигляд зображення. Такий вибір каналу підвищує непомітність стеганографічного вмісту і робить метод більш надійним у випадках, коли важлива маскувальна здатність.

У методі Куттера-Джордана-Боссена поняття чутливості до контрасту яскравості та порогу нечутливості відіграють важливу роль для забезпечення максимально непомітного вбудовування інформації в зображення. Контрастна чутливість визначається як обернене значення порогу контрасту та тісно пов’язана з законом Вебера (рис2.6), який має два ключові наслідки:

- Контрастна чутливість приблизно не залежить від яскравості фону.
- Важливими є відносні зміни яскравості.

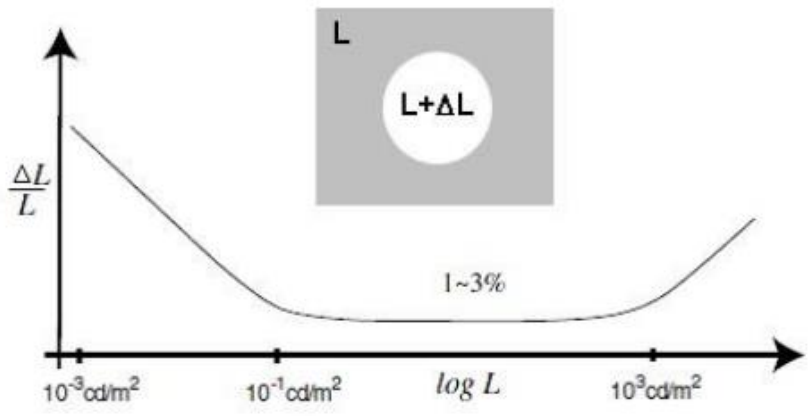


Рисунок 2.6 – Закон Вебера-Фехнера

Чутливість до контрасту яскравості означає, що людське око краще розпізнає зміни яскравості в однорідних або мало контрастних ділянках зображення, тоді як у зонах із високим контрастом і різноманітністю деталей ці зміни сприймаються набагато гірше. Метод МКДБ використовує цю особливість, вбудовуючи приховані біти переважно в області зображення, де контраст яскравості високий – наприклад, на текстурних або різнокольорових ділянках.

Суть МКДБ полягає у наступному : *i* - тий біт повідомлення *S* приховується у псевдовипадково обраному пікселі $p_{x,\,y}$ зображення *C*, представленого у системі кольорів RGB, шляхом модифікації яскравості $l_{x,\ y}$ цього пік-селя в каналі синього кольору $B_{x,\,y}$:

$$B^*_{x,y} = \begin{cases} B_{x,y} + \boldsymbol{\lambda} \mathrm{Y}_{x,y} & \text{при } m_i = 1 \\ B_{x,y} - \boldsymbol{\lambda} \mathrm{Y}_{x,y} & \text{при } m_i = 0 \end{cases} \tag{2.1}$$

де $\boldsymbol{\lambda}$ *=0.1,* $Y_{x,y} = 0{,}3R_{x,y} + 0{,}59\,G_{x,y} + 0{,}11B_{x,y}$, $R_{x,\,y}$ і $G_{x,\,y}$ – початкове значення яскравості обраного пікселю $p_{x,\ y}$ в каналі, відповідно, червоного та зеленого кольору; m_i - *i*-тий біт прихованого повідомлення; λ - константа, що визначає енергію біту, що вбудовується; $B_{x,\,y}$ і $B_{x,\,y}$ – початкове та модифіковане значення яскравості обраного пікселю $p_{x,\,y}$ в каналі синього кольору.

Для детектування прихованого біту m_i використовується передбачення початкового значення пікселя, ґрунтуючись на значеннях сусідніх пікселів.

$$\tilde{B}_{x,y} = \frac{\sum_{i=1}^{\sigma=2}(B_{x,y+i} + B_{x,y-i} + B_{x+i,y} + B_{x-i,y})}{4\sigma} \tag{2.2}$$

де **σ**=3.

Рішення приймається за наступним правилом:

$$m_i = \begin{cases} 1, & \text{якщо } B^*_{x,y} > \tilde{B}_{x,y} \\ 0, & \text{якщо } B^*_{x,y} < \tilde{B}_{x,y} \end{cases} \tag{2.3}$$

Розглянемо роботу методу на практичному прикладі. На рисунку 2.7 наведено принцип роботи методу для $\sigma = 2$.

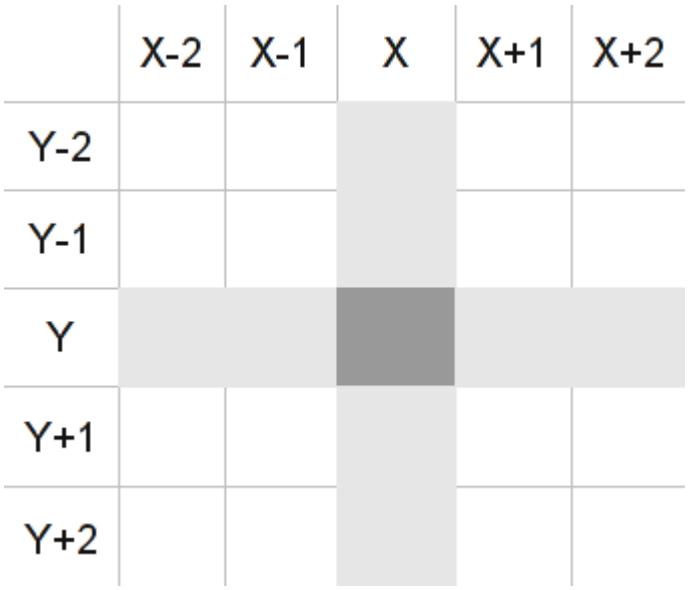


Рисунок 2.7 - Ілюстрація роботи методу МКДБ для $\sigma = 2$

На рисунку 2.7 піксель в центрі – яскравість синього кольору, яку ми хочемо спрогнозувати, опираючись на пікселі, позначені світлосірим кольором. Для конкретики приймемо наступні початкові дані:

- Приховуваний біт повідомлення: $m_i = 1$
- Початкові значення кольорових каналів пікселя *(X, Y)*: $R_{X,Y} = 100$, $G_{X,Y} = 150$, $B_{X,Y} = 200$
- Константа: λ=0.1

Для приховування біту обчислюємо спершу яскравість за NTSC:

$$Y_{x,y} = 0{,}3R_{x,y} + 0{,}59\,G_{x,y} + 0{,}11B_{x,y} = \quad (2.4)$$
$$= 0.3 \cdot 100 + 0.59 \cdot 150 + 0.11 \cdot 200 = 140.5$$

Далі модифікуємо значення синього каналу в пікселі (X, Y). З врахуванням того, що $m_i = 1$, за формулою (2.1) маємо:

$$B^*_{x,y} = B_{x,y} + \lambda Y_{x,y} = \tag{2.5}$$
$$= 200 + 0.1 \cdot 140.5 = 214.05 \approx 214$$

Отримувач для виявлення біту використовує формула (σ = 2):

$$B_{x,y} = \frac{1}{8}\sum_{i=1}^{\sigma=2}(B_{x,y+i} + B_{x,y-i} + B_{x+i,y} + B_{x-i,y}) \tag{2.6}$$

На рисунку 2.7 це пікселі по вертикалі та горизонталі на відстані 1 і 2, тобто:

- Вертикальні $B_{X,Y-2}$, $B_{X,Y-1}$, $B_{X,Y+1}$, $B_{X,Y+2}$.
- Горизонтальні $B_{X-2,Y}$, $B_{X-1,Y}$, $B_{X+1,Y}$, $B_{X+2,Y}$

Нехай ці значення дорівнюють: $B_{X,Y-2} = 198, B_{X,Y-1} = 202, B_{X,Y+1} = 201, B_{X,Y+2} = 199, \quad B_{X-2,Y} = 203, B_{X-1,Y} = 200, B_{X+1,Y} = 197, \; B_{X+2,Y} = 198.$ Тоді для цих визначених значень за формулою (2.6) маємо:

$$\tilde{B}_{x,y} = \frac{1}{8}(198 + 202 + 201 + 199 + 203 + 200 + 197 + 198) \approx 200 \tag{2.7}$$

Для отримання прихованого біта порівнюємо модифіковане значення пікселю $B^*_{x,y} = 214$ та обчислене значення $\tilde{B}_{x,y}$. Оскільки $B^*_{x,y} > \tilde{B}_{x,y}$, то за правилом з формули (2.3) маємо $m_i = 1$.

До переваг методу належать:

- Висока непомітність.
- Сліпа детекція.
- Простота реалізації.
- Локальність операцій.
- Стійкість до несанкціонованого ознайомлення.
- Стійкість до руйнування молодших біт контейнера.
- Стійкість до частотного детектування.

Недоліками методу є низька стійкість до компресії, невисока ємність і залежність від локальної структури.

Метод Кутерра–Джордана – це ефективний і простий підхід до невидимого водяного знакування або стеганографії, який використовує локальне передбачення пікселів для приховування та виявлення даних. Його основна цінність – це висока непомітність і відсутність потреби в оригіналі зображення, проте він менш стійкий до агресивних методів стиснення та обробки зображень.

В даній роботі ми, все-таки, вирішили сконцентруватись на методі заміни наймолодшого біта, щоб продемонструвати його вразливість до атак перетворення контейнера-зображення.

2.2 Вибір методу приховування інформації в частотній області

2.2.1 Частотне перетворення зображень

У цифровій обробці зображень кожне зображення зазвичай подається у просторовій області як матриця пікселів, де кожне значення описує яскравість або колірну складову в конкретній точці. Однак існує інша форма подання – частотна область, у якій зображення розглядається як сукупність хвильових компонент із різними просторовими частотами. Частотне перетворення зображень – це процес представлення зображення не в просторі пікселів (просторова область), а в термінах його частотних компонент. Це дозволяє аналізувати та обробляти зображення з погляду зміни яскравості та текстури, а не лише кольорів у точках. Існують кілька підходів до переходу в частотну область. Історично першим було перетворення Фур’є.

Основна ідея перетворення Фур'є полягає в тому, що будь-яке зображення можна розкласти на набір синусоїдальних компонент. Для зображення розміром M×N дискретне двовимірне перетворення Фур'є задається формулою:

$$F_{u,v} = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f_{x,y} e^{-i2\pi(\frac{ux}{M}+\frac{vy}{N})},\ u = \overline{0, M-1},\ v = \overline{0, N-1} \qquad (2.8)$$

Тут:

- $f_{x,y}$– значення яскравості пікселя у просторовій області;

- $F_{u,v}$– спектральне представлення в частотній області;
- u,v – індекси частот по горизонталі та вертикалі.

Зворотне перетворення дозволяє відновити зображення:

$$f\_inv_{x,y} = \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} F_{u,v} e^{i2\pi(\frac{ux}{M}+\frac{vy}{N})}, x = \overline{0, M-1}, y = \overline{0, N-1} \quad (2.9)$$

Ілюстрація представлення зображення в просторовій та частотній областях наведена на рисунку

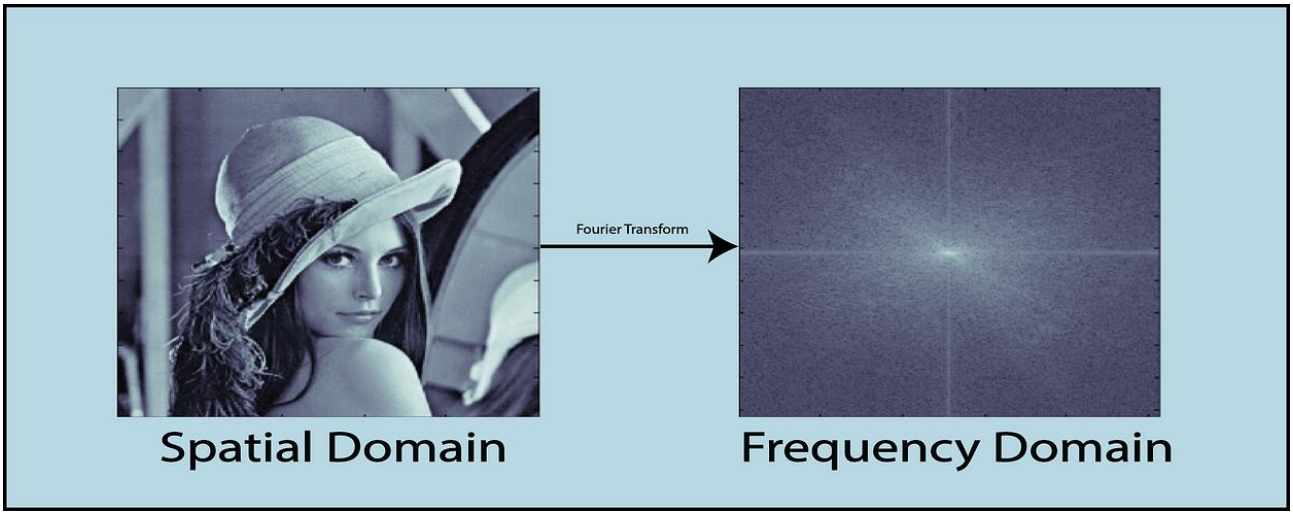


Рисунок 2.8 – Представлення зображення в просторовій та частотній областях

Високі частоти відповідають різким змінам – краям, шуму, текстурам. Низькі – плавним переходам, загальному тлу.

У JPEG-стисненні широко використовується дискретне косинусне перетворення (Discrete Cosine Tranform, DCT), що наближено розкладає зображення на сукупність косинусів різної частоти. Зображення розбивається на блоки 8×8, і до кожного застосовується DCT. Пряме косинусне перетворення має вигляд:

$$F_{u,v} = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} a_u a_v f_{x,y} cos\left(\frac{\pi u}{2M}(2x+1)\right) cos\left(\frac{\pi v}{2N}(2y+1)\right) \quad (2.10)$$

Тут:

$$a_i = \begin{cases} 1 & if\ \ i = 0 \\ \sqrt{2} & otherwise \end{cases}$$

У результаті ми отримаємо матрицю коефіцієнтів:

- Верхній лівий кут – низькі частоти.
- Нижній правий кут – високі частоти.

Після DCT більшість високочастотних коефіцієнтів зануляються (квантування), що значно зменшує обсяг даних.

Обернене перетворення DCT має вигляд:

$$\mathrm{f\_inv_{x,y}} = \frac{1}{\sqrt{\mathrm{MN}}} \sum_{\mathrm{u=0}}^{\mathrm{M-1}} \sum_{\mathrm{v=0}}^{\mathrm{N-1}} a_u a_v \mathrm{F_{u,v}} \cos\left(\frac{\pi u}{2M}(2x+1)\right) \cos\left(\frac{\pi v}{2N}(2y+1)\right) \quad (2.11)$$

Слід зазначити, що за умови збереження загальної кількості коєфіцієнтів, $\mathrm{f\_inv_{x,y}}$ ідентичне до початкового зображення $f_{x,y}$, для якого виконували перетворення. Це твердження є справедливим і для дискретного косинусного перетворення і для перетворення Фур'є.

Перетворення зображення у частотну область дозволяє подати його не як сукупність пікселів, а як набір частот, які описують його зміни, структуру та візуальні особливості. Це потужний інструмент для стиснення, аналізу та водяного маркування. При цьому DCT забезпечує ефективне кодування енергії, DFT – точне частотне представлення

2.2.2 Метод Коха-Жао

Метод Коха-Жао є одним із відомих стеганографічних алгоритмів у домені перетворень. Він базується на порівнянні величин коефіцієнтів дискретного косинусного перетворення (ДКП) певних блоків зображення. Замість того, щоб безпосередньо змінювати значення пікселів або коефіцієнтів, цей метод вбудовує біти прихованої інформації, модифікуючи співвідношення між

вибраними парами коефіцієнтів ДКП, що робить його досить стійким до певних атак, таких як стиснення JPEG.

В загальному, можна зазначити, що суть методу полягає в наступному: вихідне зображення розбивається на блоки (наприклад, 8x8 пікселів), до кожного з яких застосовується ДКП. На рисунку 2.9 наведено приклад такого перетворення.

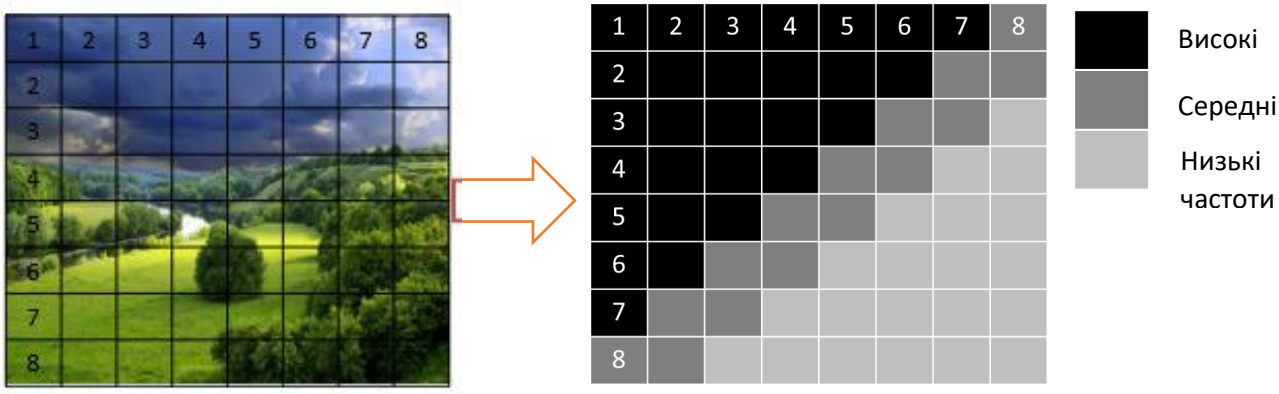


Рисунок 2.9 – Приклад косинусного перетворення

Потім, для вбудовування біта прихованої інформації (0 або 1), вибираються дві специфічні зони коефіцієнтів ДКП у кожному блоці. Якщо потрібно вбудувати "0", співвідношення величин коефіцієнтів у цих двох зонах коригується таким чином, щоб коефіцієнти однієї зони були більшими за коефіцієнти іншої. Якщо ж потрібно вбудувати "1", співвідношення змінюється на протилежне. Таким чином, інформація закодована не в абсолютних значеннях, а у відносних, що забезпечує більшу робастність прихованої інформації.

Розглянемо алгоритм приховування методом Коха-Жао детальніше:

1. Розбити зображення на блоки 8x8.
2. Для кожного блоку застосувати дискретне косинусне перетворення. Формула (2.10) матиме вигляд:

$$F_{u,v} = \frac{1}{4}\sum_{x=0}^{7}\sum_{y=0}^{7} a_u a_v f_{x,y} cos\left(\frac{\pi u}{16}(2x+1)\right) cos\left(\frac{\pi v}{16}(2y+1)\right) \qquad (2.12)$$

3. Вибрати пару DCT-коефіцієнтів (наприклад, $F1_{u,v}$ та $F2_{u,v}$), які не належать до найнижчих частот, щоби не впливати на якість, і не найвищих, які зникають при JPEG-стисненні. За звичай рекомендують використовувати центральні частоти (4, 5) і (5, 4).

4. Для кожного біта $m_i \in \{0,1\}$ мають виконуватись наступні правила:

- Якщо $m_i = 1$, зробити $F1_{u,v} > F2_{u,v}$.
- Якщо $m_i = 0$, зробити $F1_{u,v} < F2_{u,v}$.

Формально це можна виконати наступним чином:

$$\begin{cases} F1_{u,v} = F2_{u,v} + \Delta, \text{ якщо } m_i = 1 \text{ і } F1_{u,v} \leq F2_{u,v} \\ F2_{u,v} = F1_{u,v} + \Delta \text{ , якщо } m_i = 0 \text{ і } F1_{u,v} \geq F2_{u,v} \end{cases} \quad (2.13)$$

де Δ– контрольована величина зміни (наприклад, 10–20)

5. Виконати обернене косинусне перетворення блоку.

Для вилучення повідомлення потрібно виконати схожі дії. Спочатку розбити зображення на блоки 8x8. Потім до кожного блоку застосувати DCT. Висновок про прихований біт зробити на основі порівняння визначених пар:

$$\begin{cases} m_i = 1, \text{якщо } F1_{u,v} > F2_{u,v} \\ m_i = 0 \text{ , якщо } F1_{u,v} < F2_{u,v} \end{cases} \quad (2.14)$$

На рисунку 2.10 наведено приклад вбудовування інформації в зображення методом Коха-Жао. Результати були отримані авторами [14]. Як бачимо, візуальних змін між рисунками не помітно.

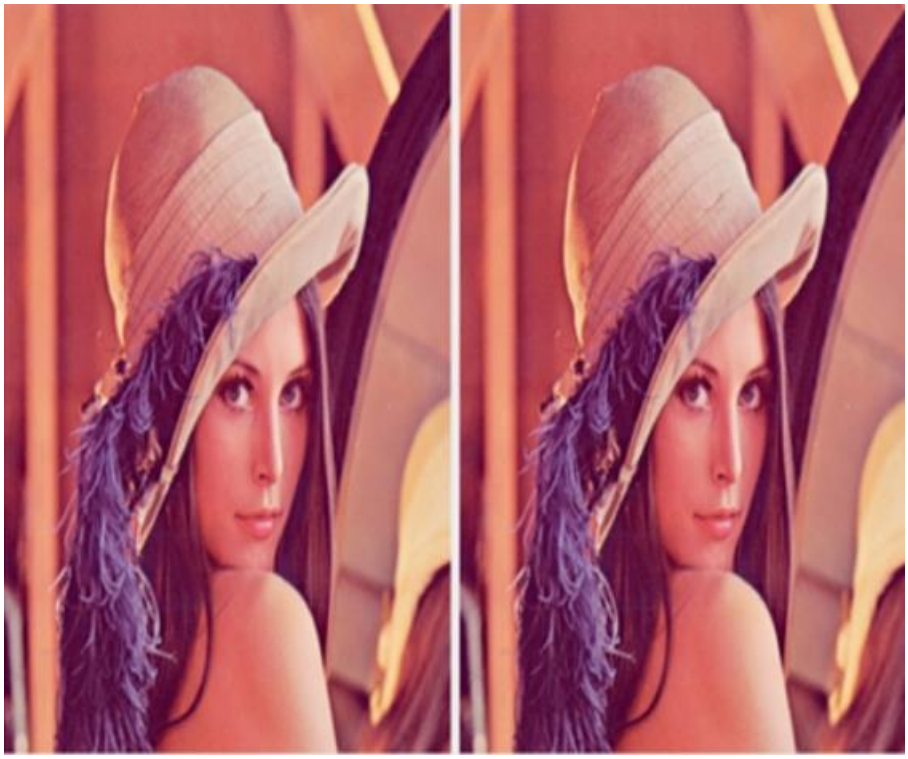


Рисунок 2.10 – Зображення контейнер до та після вбудовування секретної інформації методом Коха-Жао

Переваги методу Коха-Жао полягають у його відносній стійкості до поширених атак на стеганограму, зокрема до компресії з втратами, як-от JPEG. Це досягається завдяки тому, що інформація вбудовується шляхом маніпулювання співвідношеннями між коефіцієнтами ДКП, а не їхніми абсолютними значеннями. Такі зміни є менш помітними для ока і краще зберігаються при стисненні, оскільки компресія часто впливає на абсолютні значення коефіцієнтів, але зберігає їхні відносні величини. Крім того, цей метод дозволяє вбудовувати інформацію у важливі частотні компоненти зображення, що також сприяє його робастності.

Незважаючи на переваги, метод Коха-Жао має й певні недоліки. Одним із них є обмежена ємність для приховування інформації. Оскільки кожен біт кодується через зміну співвідношення між двома групами коефіцієнтів ДКП, кількість інформації, яку можна вбудувати в зображення, є відносно невеликою порівняно з деякими іншими стеганографічними методами. Інший недолік полягає в можливій втраті якості зображення при надмірному вбудовуванні. Хоча метод намагається бути непомітним, велика кількість модифікацій

коефіцієнтів ДКП, необхідних для приховування значного обсягу даних, може призвести до видимих артефактів або спотворень у зображенні, що порушить головний принцип стеганографії – непомітність.

РОЗДІЛ 3 ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ

3.1 Обґрунтування середовища розробки

Python є однією з найпопулярніших мов програмування у сучасному світі, яка знаходить широке застосування у багатьох галузях, включаючи обробку зображень, комп'ютерний зір та, звісно, стеганографію. Популярність Python у світі програмування постійно зростає. Згідно з індексом TIOBE Index [15], який оцінює популярність мов програмування, Python стабільно посідає одне з перших місць протягом останніх років, часто займаючи першу позицію. Наприклад, у червні 2024 року, Python є лідером за популярністю. Це свідчить про його широке поширення та активне використання в різних галузях промисловості та досліджень.

Дослідження Stack Overflow Developer Survey [16] також підтверджують домінування Python. У звітах за останні роки (наприклад, 2023 рік) Python постійно вказується як одна з найбажаніших та найпопулярніших мов серед розробників. Зокрема, у сфері аналізу даних, машинного навчання та штучного інтелекту, Python є фактичним стандартом, а ці галузі тісно перетинаються з обробкою зображень, що є основою стеганографії.

Більше того, кількість проектів з відкритим вихідним кодом на GitHub, що використовують Python, є однією з найбільших. Це створює сприятливе середовище для розробників стеганографії, оскільки вони можуть використовувати існуючі рішення, модифікувати їх та ділитися власними розробками зі спільнотою.

До переваг Python відносять:

- Велика кількість бібліотек. Python володіє величезною екосистемою бібліотек, які ідеально підходять для роботи зі стеганографією.
- Швидка прототипізація: Завдяки простоті синтаксису та великій кількості готових компонентів, Python дозволяє розробникам швидко створювати та тестувати різні стеганографічні підходи. Це значно скорочує час від ідеї до робочого прототипу.

- Кросплатформність: Python є кросплатформною мовою, що означає, що код, написаний на Python, може бути запущений на різних операційних системах (Windows, macOS, Linux) без значних модифікацій, що спрощує поширення та використання стеганографічних інструментів.

- Велика спільнота та ресурси: Python має величезну та активну спільноту розробників, що забезпечує постійну підтримку, оновлення бібліотек та велику кількість навчальних матеріалів, прикладів коду та форумів для вирішення проблем. Це спрощує вивчення та впровадження нових методів.

- Інтеграція з іншими технологіями: Python легко інтегрується з іншими мовами програмування (наприклад, C/C++ через Cython або Boost.Python) для оптимізації продуктивності критичних ділянок коду, що може бути важливо для ресурсоємних стеганографічних алгоритмів.

Одним із головних недоліків Python є його відносно нижча швидкість виконання порівняно з компільованими мовами, такими як C++ або Java. Для обробки великих обсягів зображень або відео в режимі реального часу це може бути критичним. Хоча NumPy та інші бібліотеки використовують оптимізовані C-реалізації, базовий інтерпретований код Python все ще може бути повільним. Python-додатки можуть споживати більше пам'яті порівняно з аналогічними програмами, написаними на більш низькорівневих мовах, що може бути проблемою при роботі з дуже великими зображеннями або складними алгоритмами.

Найбільш популярні бібліотеки Python, що можуть використовуватись під час реалізації стеганографічних методів:

- NumPy. Фундаментальна бібліотека для числових обчислень, що надає високоефективні засоби для роботи з багатовимірними масивами (зображеннями). Це дозволяє швидко виконувати матричні операції, необхідні для реалізації багатьох стеганографічних алгоритмів.

- OpenCV. Потужна бібліотека для комп'ютерного зору, яка пропонує широкий спектр функцій для читання/запису зображень, зміни розмірів, фільтрації, перетворень кольорового простору та багато іншого. Ці функції є

незамінними при підготовці зображення-контейнера та при вилученні прихованої інформації.

- Pillow. Бібліотека для обробки зображень, яка забезпечує зручні засоби для маніпуляцій з пікселями, зміни форматів, накладання фільтрів – операції, що часто використовуються в стеганографії на рівні пікселів.
- SciPy. Доповнює NumPy, надаючи модулі для наукових та технічних обчислень, включаючи обробку сигналів (signal processing), що корисно для реалізації складніших перетворень.
- Matplotlib/Seaborn. Бібліотеки для візуалізації даних, які дозволяють легко відображати зображення, гістограми, спектри частот, що є критично важливим для аналізу результатів стеганографічних вбудовувань та виявлення артефактів.

Однією з ключових переваг Python є його високий рівень абстракції та читабельний синтаксис, що значно прискорює процес розробки. Складні алгоритми, що лежать в основі стеганографії (наприклад, перетворення Фур'є, дискретне косинусне перетворення, вейвлет-перетворення), можуть бути реалізовані за допомогою компактного та зрозумілого коду, що робить його доступним навіть для розробників з обмеженим досвідом у галузі цифрової обробки сигналів. Це особливо важливо у сфері стеганографії, де часто доводиться працювати з математично інтенсивними операціями. Його популярність пояснюється поєднанням потужних можливостей, простоти синтаксису та великої кількості доступних бібліотек. Саме ці характеристики роблять Python надзвичайно привабливим вибором для розробки та реалізації стеганографічних методів, як класичних, так і сучасних.

3.2 Реалізація обраних методів стеганографічного перетворення інформації

Для кращої демонстрації впливу перетворень графічних форматів на стійкість стеганографічних методів приховування інформації було обрано два методи: заміни наймолодшого біта в просторовій області та метода Коха-Жао в частотній області.

Для реалізації методу заміни наймолодшого біта нам потрібно або просто замінити наймолодший біт пікселя на біт повідомлення або виконати інші математичні операції. В найпростішому випадку підхід може виглядати так, як зображено на рисунку 3.1

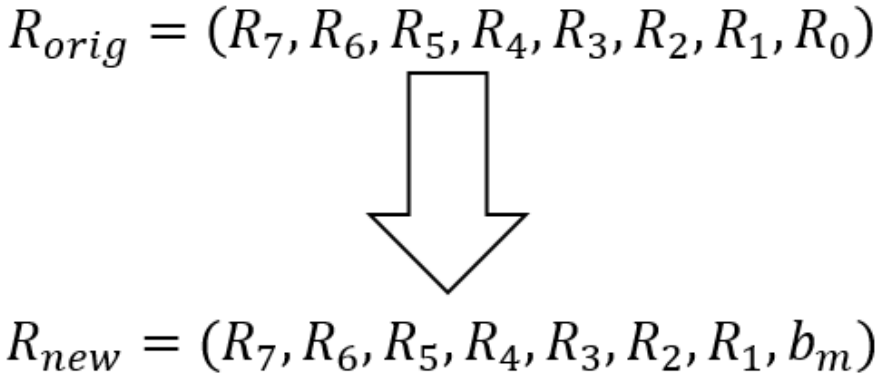


Рисунок 3.1 –Ілюстрація заміни наймолодшого кольору в компоненті червоного кольору

Для збільшення ємності методу було вирішено приховувати по 2 біти в компоненті червоного і зеленого кольорів і по 3 біти в компоненті синього кольору, оскільки зміни синього кольору найменш відчутні для людського ока. Для реалізації цього підходу спочатку ми визначені біти обнулили. В лістингу 3.1 наведено код, який дозволяє значення двох наймолодших біт червоної та зеленої компоненти, а також 3 наймолодших біти синьої компоненти присвоїти нулю

Лістинг 3.1 – Код, що встановлює значення визначених молодших бітів в нуль

```
def normalize_pixel(pixel):
    return (
        pixel[0] - pixel[0] % 4,# 2 LS bits
        pixel[1] - pixel[1] % 4,# 2 LS bits
        pixel[2] - pixel[2] % 8 # 3 LS bits
```

Під нормалізацією пікселів будемо розуміти процедуру встановлення значень визначених наймолодших пікселів в нуль. В лістингу 3.2 наведено обробка всіх пікселів зображення.

Лістинг 3.2 – Підготовка пікселів зображення до вбудовування бітів секретного повідомлення

```
for i in range(container.size[0]):
    for j in range(container.size[1]):
        offset = j * 7 + i * container.size[1]
        result_pixel = list(normalize_pixel(pixel_map[i,j]))
        if offset >= secret_len:
            result_pixels[i, j] = tuple(result_pixel)
            continue
```

Після нормалізації всіх пікселів зображення, вбудовування секретного повідомлення можна виконати простим додаванням до значення пікселю необхідної кількості біт повідомленння, що і відображено в лістингу 3.3

Лістинг 3.3 – Вбудовування повідомлення

```
for i in range(container.size[0]):
    for j in range(container.size[1]):
        offset = j * 7 + i * container.size[1]
        result_pixel = list(normalize_pixel(pixel_map[i,j]))
        if offset >= secret_len:
            result_pixels[i, j] = tuple(result_pixel)
            continue
```

Для отримання секретного повідомлення необхідно виконати код з лістингу 3.4. Щоб отримати біти повідомлення ми використовується функція отримання остачі. Щоб отримати 2 останні біти, шукаємо остачі від ділення на 4, щоб отримати 3 останні біти, шукаємо остачу від ділення на 8.

Лістинг 3.4 – Отримання секретного повідомлення

```
    def lpad(string, symbol, needed_len):
        while len(string) < needed_len:
            string = symbol + string
        return string
    secret_bytes = []
    for i in range(modified.size[0]):
        for j in range(modified.size[1]):
            pixel = pixels_modified[i, j]
            red = pixel[0] % 4
            green = pixel[1] % 4
            blue = pixel[2] % 8
            secret_bytes.append(
                lpad(bin((red << 5) + (green << 3) +
blue).replace('0b', ''), '0', 7)
            )
    modified.close()
    secret_bytes = ''.join(secret_bytes).split(BOUNDRY_TAG)[1]
    phrase = ''
    for char_offset in range(0, len(secret_bytes), 7):
        phrase += chr(int(secret_bytes[char_offset:char_offset +
7], 2))
print("The hidden secret message is:", phrase, sep="\n")
```

Для реалізації метода Коха-Жао використовується код з лістингу 3.5. Оскільки даний метод працює в частотній області, то для переходу в частотну область використовується дискретне косинусне перетворення. Скрипт починається з імпорту необхідних бібліотек: skimage.io для читання/запису зображень, користувацьких модулів str_to_bin для перетворення рядка у бінарний вигляд, DCT для керування DCT-перетворенням та SteganoEncoder – основний клас для вбудовування повідомлень. У головній частині користувача просять ввести секретне повідомлення, яке потім перетворюється на послідовність бітів. Зображення-контейнер завантажується, створюються об'єкти DCT та SteganoEncoder, після чого секретне повідомлення вбудовується у контейнер за допомогою методу embed_message(). Результат – зображення з

прихованим повідомленням – зберігається як filled.png, а потім обидва зображення (оригінальне та закодоване) відображаються поруч за допомогою matplotlib для візуального порівняння.

Лістинг 3.5 – Вбудовування методом Коха-Жао

```
from skimage import io
from lib.bin import str_to_bin
from lib.dct import DCT
from lib.stegano_encoder import SteganoEncoder
import matplotlib.pyplot as plt
if __name__ == '__main__':
    secret = input("Enter your secret, I won't tell it to anyone:
")
    secret_bytes = str_to_bin(secret)
    print("Message Length is - ", len(secret_bytes))
    container = io.imread('container.png')
    dct = DCT()
    stegano_encoder = SteganoEncoder(dct_manager=dct)
    encoded = stegano_encoder.embed_message(container,
secret_bytes)
    io.imsave('filled.png', encoded)
    f, axarr = plt.subplots(1, 2)
    axarr[0].imshow(container)
    axarr[1].imshow(encoded)
    plt.show()
```

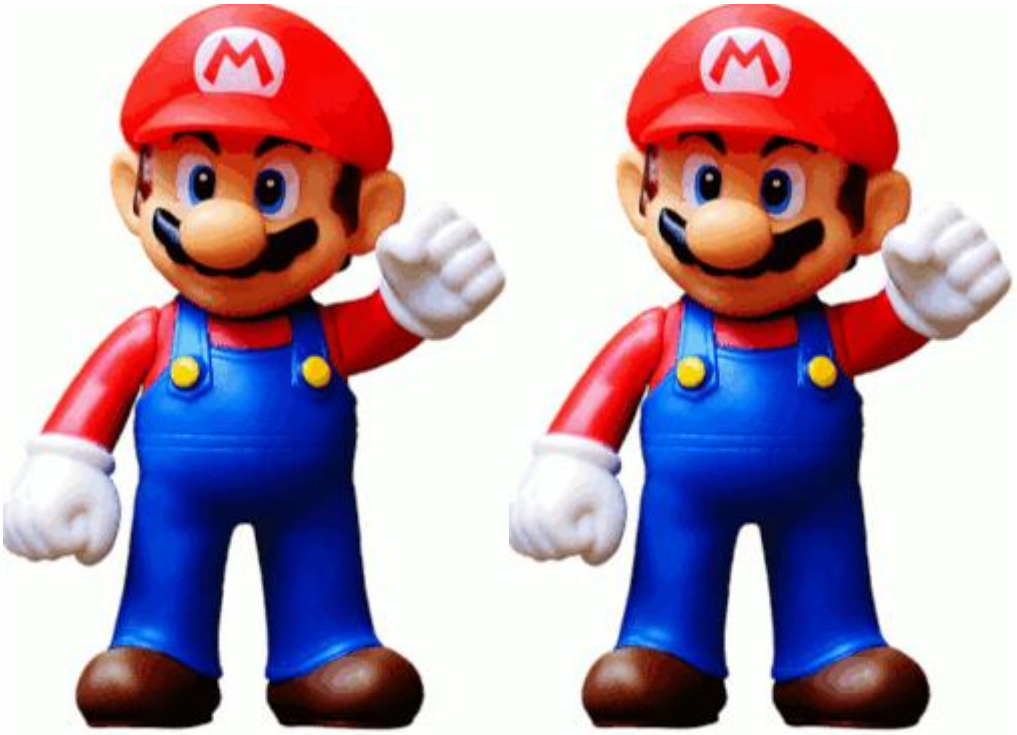
З використанням схожих функцій та бібліотек отримуємо секретне повідомлення із зображення.

3.3 Аналіз отриманих експериментальних результатів

Аналіз отриманих експериментальних результатів зосереджений на порівнянні ефективності двох поширених стеганографічних методів вбудовування: класичного методу заміни наймолодшого біта (LSB) та більш

складного метода Коха-Жао, заснованого на косинусному перетворенні. Метою дослідження було оцінити, як ці методи впливають на якість зображення-контейнера та стійкість прихованих до модифікації контейнера.

На рисунку 3.2 наведено результат приховування повідомлення «mamaTereza» в BMP форматі методом заміни наймолодшого біта. Бачимо, що попри те, що приховування інформації здійснювалось в двох компонентах в двох наймолодших бітах, а в одному компоненті в трьох бітах, жодних спотворень непомітно.



а б

Рисунок 3.2 – Порожній контейнер (а) та заповнений контейнер (б) методом заміни наймолодшого біта в форматі BMP

Проте відбулись мінімальні зміни в розмірі файлу, який змінився з 375 Кб до 450 Кб. З контейнера вдалося без проблем отримати приховане повідомлення «mamaTereza». При збереженні даного файлу в Jpeg форматі високої якості розмір зображення зменшився в більш ніж 5 разів до 115 Кб, приховане повідомлення було повністю зруйноване.

Схожі результати отримали і для зображення в форматі PNG (рисунок 3.3)

а б

Рисунок 3.3 – Порожній контейнер (а) та заповнений контейнер (б) методом заміни наймолодшого біта в форматі PNG

Як бачимо з рисунку 3.3 зміни не помітні, Розмір зображення при вбудовуванні повідомлення зменшився майже вдвічі з 236 Кб до 150 Кб. При конвертації зображення в JPEG формат як високої та і низької якості початкове повідомлення «mamaTereza» було втрачене.

Останнім ми тестували метод, який проводить вбудовування бітів в частотній області в форматі PNG. Результат вбудовування зображено на рисунку 3.4. Як бачимо візуальних спотворень не помітно.

а б

Рисунок 3.4 – Порожній контейнер (а) та заповнений контейнер (б) методом Коха-Жао в форматі PNG

Розмір зображення при вбудовуванні бітів теж зменшився. Початкове повідомлення вдалось відновити. При перетворенні PNG в JPEG формат з

високою якістю зображення початкове повідомлення було відновлено. Проте при збереженні в JPEG з низькою якістю початкове повідомлення було втрачене.

В таблиці 3.1 наведено основні результати роботи

Таблиця 3.1 – Порівняльний аналіз результатів стійкості до результатів перетворень графічних форматів

Тип формату контей-неру	Початко-вий розмір контей-неру	Стегано-графічний метод	Розмір запо-вненого контей-неру	Чи вдалось отримати початкове повідомлення	Новий формат контей-неру	Розмір контейнеру у новому форматі	Чи вдалось отримати початкове повідомлення
BMP	375	LSB	450	так	JPEG високої якості	115	ні
PNG	236	LSB	150	так	JPEG високої якості	86	ні
PNG	236	LSB	150	так	JPEG низької якості	51	ні
PNG	236	Коха-Жао	241		JPEG високої якості	86	так
PNG	236	Коха-Жао	241	так	JPEG низької якості	51	ні
JPEG високої якості	85	Коха-Жао	79	так	JPEG низької якості	49	ні

Надана таблиця ілюструє поведінку двох стеганографічних методів LSB та Коха-Жао при перетворенні зображень-контейнерів у формат JPEG з різними рівнями якості. Особливу увагу слід звернути на вплив перетворення та стиснення на можливість отримання прихованого повідомлення.

У всіх випадках застосування методу LSB приховане повідомлення не вдалося отримати після перетворення в JPEG, незалежно від початкового формату (BMP чи PNG) та якості JPEG (висока). Це є очікуваним результатом, оскільки LSB-метод вбудовує дані в найменш значущі біти пікселів, які є дуже

чутливими до будь-яких змін, викликаних стисненням із втратами, як у JPEG. Навіть "висока якість" JPEG все одно передбачає певне стиснення, яке призводить до втрати цих незначних змін.

Метод Коха-Жао демонструє помірну стійкість до стиснення у форматі JPEG, що значно відрізняє його від абсолютно нестійкого методу LSB. Зокрема, у випадку перетворення PNG-зображення у формат JPEG високої якості з помірним зменшенням розміру файлу, приховане повідомлення було успішно вилучено. Це свідчить про його потенційну ефективність у сценаріях, де застосовується відносно легке стиснення зображень, дозволяючи йому зберегти цілісність вбудованих даних, на відміну від LSB, який втрачає інформацію навіть при такому ж стисненні.

Однак, стійкість методу Коха-Жао має свої межі, що чітко видно з результатів при більш агресивному стисненні. Коли зображення перетворювалося у JPEG низької якості, або ж існуюче JPEG-зображення піддавалося подальшому сильному стисненню, приховане повідомлення не вдалося вилучити. Це означає, що попри кращу стійкість порівняно з LSB, метод Коха-Жао все ще чутливий до значних втрат, характерних для інтенсивного JPEG-стиснення.

У контексті сучасних месенджерів, які автоматично стискають зображення, часто до значно нижчої якості, застосування двох досліджуваних методів може бути неефективним.

LSB-метод повністю провалюється навіть при "високій якості" JPEG, використання його для передачі прихованої інформації через месенджери є марним. Автоматичне стиснення месенджерами гарантовано знищить будь-які дані, приховані цим методом.

Хоча метод Коха-Жао показав стійкість до JPEG високої якості, його "провал" при JPEG низької якості або повторному стисненні вказує на те, що він також не є панацеєю. Месенджери часто використовують досить агресивні алгоритми стиснення для досягнення максимальної економії даних. Якщо рівень стиснення, застосовуваний месенджером, відповідає "низькій якості" JPEG або є

ще більш агресивним, то навіть метод Коха-Жао не зможе забезпечити успішне вилучення прихованого повідомлення.

Для успішної стеганографії в умовах, коли зображення проходять через процеси стиснення JPEG (як це відбувається при пересилці через більшість месенджерів), необхідні значно більш надійні та стійкі методи, ніж LSB, і навіть стійкіші, ніж базовий Коха-Жао, який розглянуто. Ці методи повинні бути розроблені з урахуванням робастності до значних втрат інформації, що є невід'ємною частиною JPEG-стиснення. Це може включати використання методів, які вбудовують дані в більш значущі коефіцієнти дискретного перетворення (наприклад, DCT або DWT), застосування надлишкового кодування для виправлення помилок або використання адаптивних алгоритмів, які враховують особливості стиснення.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Охорона праці

В Україні діють закони, які визначають права і обов'язки її працівників, а також організаційну структуру органів влади і виробництва. Конституція України – основний закон держави, який декларує рівні права і свободи всім жителям держави на вільний вибір праці, що відповідає безпечним і здоровим умовам, на відпочинок, на соціальний захист у разі втрати працездатності та у старості. Всі закони і нормативні документи узгоджуються, базуються і відповідають статтям Конституції.

Згідно закону України "Про охорону праці", в останній редакції 2018 року, охорона праці – це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних, лікувально-профілактичних заходів та засобів, спрямованих на збереження здоров'я і працездатності людини в процесі трудової діяльності. Дія цього Закону поширюється на всіх юридичних та фізичних осіб, які відповідно до законодавства використовують найману працю, та на всіх працюючих.

Для управління охороною праці створюються відповідні служби і призначаються компетентними органами посадові особи, які забезпечують вирішення конкретних питань охорони праці. На підприємстві з кількістю працюючих 50 і більше осіб роботодавець створює службу охорони праці відповідно до типового положення, що затверджується спеціально уповноваженим центральним органом виконавчої влади з питань нагляду за охороною праці (стаття 15). На підприємстві з кількістю працюючих менше 50 осіб функції служби охорони праці можуть виконувати в порядку сумісництва особи, які мають відповідну підготовку. На підприємстві з кількістю працюючих менше 20 осіб для виконання функцій служби охорони праці можуть залучатися сторонні спеціалісти на договірних засадах, які мають відповідну підготовку.

За порушення законодавства про охорону праці, невиконання розпоряджень посадових осіб органів державного нагляду за охороною праці юридичні та фізичні особи, які відповідно до законодавства використовують найману працю, притягаються органами державного нагляду за охороною праці до сплати штрафу у порядку, встановленому законом.

Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями (затверджені наказом Міністерства соціальної політики України №207 від 14.02.2018) поширюються на всіх суб'єктів господарювання незалежно від форм власності, організаційно-правової форми і видів діяльності та встановлюють мінімальні вимоги безпеки та захисту здоров'я під час здійснення роботи, пов'язаної з використанням екранних пристроїв незалежно від їхнього типу та моделі. Під екранними пристроями розуміють електронні засоби для відтворення будь-якої графічної або алфавітно-цифрової інформації (на основі електронно-променевої трубки, рідкокристалічні, плазмові, проекційні, органічні світлодіодні монітори та інші новітні розробки у сфері інформаційних технологій)

Облаштування робочого місця працівника з екранними пристроями має відповідати вимогам Санітарних норм виробничого шуму, ультразвуку та інфразвуку ДСН 3.3.6.037-99, затверджених постановою Головного державного санітарного лікаря України від 01 грудня 1999 року № 37 та враховувати:

- належні умови освітлення приміщення і робочого місця, відсутність відблисків;
- оптимальні параметри мікроклімату;
- м'яке рентгенівське випромінювання;
- наявність шуму та вібрації;
- електромагнітне випромінювання;
- ультрафіолетове та інфрачервоне випромінювання;
- електростатичне поле між екраном і оператором.

Вимоги безпеки до робочих місць працівників з екранними пристроями передбачають:

- Робочі місця працівників з екранними пристроями мають бути спроектовані так і мати такі розміри, щоб працівники мали простір для зміни робочого положення та рухів.

- Для забезпечення безпеки та захисту здоров'я працівників усе випромінювання від екранних пристроїв має бути зведене до гранично допустимого рівня з погляду безпеки та охорони здоров'я працівників.

- Організація робочого місця працівника з екранними пристроями має забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним, антропологічним, психофізіологічним вимогам, а також характеру виконуваних робіт.

- Освітлення робочого місця працівника з екранними пристроями має створювати відповідний контраст між екраном і навколишнім середовищем (з урахуванням виду роботи) та відповідати вимогам ДСанПІН 3.3.2.007-98 [22].

- Мікроклімат виробничих приміщень з робочими місцями працівників з екранними пристроями має підтримуватись на постійному рівні та відповідати вимогам Санітарних норм мікроклімату виробничих приміщень ДСН 3.3.6.042-99, затверджених постановою Головного державного санітарного лікаря України від 01 грудня 1999 року № 42 (далі - ДСН 3.3.6.042-99).

- Робочий стіл або робоча поверхня повинні бути достатнього розміру та мати поверхню з низькою відбивною здатністю, допускати гнучкість під час розміщення екрана, клавіатури, документів і відповідного устаткування.

- Робоче крісло має бути стійким і дозволяти працівнику з екранними пристроями легко рухатися та займати зручне положення. Сидіння має регулюватися по висоті, спинка сидіння - як по висоті, так і по нахилу.

4.2 **Безпека життєдіяльності**

Повномасштабне вторгнення, яке розпочала росія 24 лютого 2022 року на території України, має неабиякий негативний вплив на психічне й фізичне здоров'я людини. Уже понад півтори роки українці живуть із відчуттям страху, що нагадує про себе з кожним сповіщенням про повітряну тривогу та звуком сирени. Щодня велика кількість новини про зруйновані будинки від обстрілів та

число загиблих морально пригнічують українці, а економічні труднощі спричиняють емоційні страждання. Ті, хто перебувають у виснаженому стані, а також ті, хто залишаються у форматі самомобілізації повинні усвідомити, що їхній стан – це наслідок психологічної травми. Відтак в умовах війни підвищення життєдіяльності людини є надзвичайно складним, але водночас важливим завданням для підтримки морального стану і збереження фізичних сил. Однак, навіть у таких реаліях, є кілька методів, які можуть сприяти збереженню працездатності людей.

Основні методи підвищення життєдіяльності можна умовно розділити на два типи: активні – ті, що напряму впливають на трудові можливості людини, та пасивні – мають лише дотичний вплив на продуктивність (рис. 4.1).

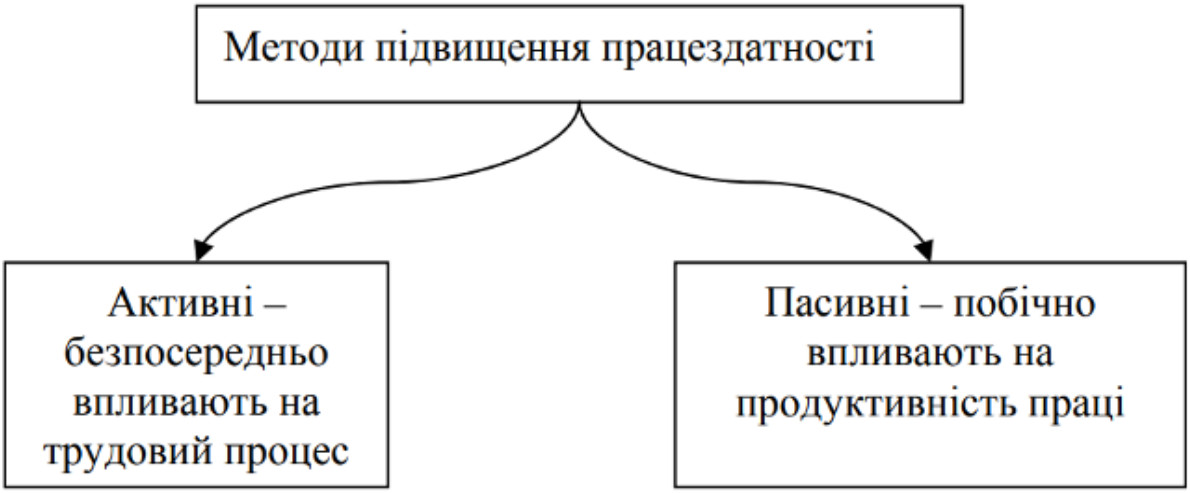


Рисунок 4.1 – Методи підвищення працездатності

До активних методів належать розподіл і кооперація праці; оптимізація ритму праці; раціональна організація робочого місця; удосконалення режиму праці й відпочинку; раціональне застосування засобів фізичної культури й спорту. [7] До кожного аспекту активного методу застосовують різні шляхи покращення працездатності:

- Делегування праці або командна робота – цей шлях базується на взаємодії між людьми з метою досягнення спільної мети. Розподіл завдань та кооперація покращують ефективність використання наявних ресурсів, зокрема людських, фінансових і матеріальних. Учасники команди мають виконувати ту

роботу, в якій можуть бути найбільш продуктивними, а їхня праця – результативною. Люди можуть навчатися один від одного, передавати знання та навички, що дозволяє кожному зростати як професіоналу, і разом сприяти подоланню спільних труднощів.

- Оптимізація темпу праці – такий спосіб передбачає ефективність робочих процесів та використання сучасних технологій. Автоматизація рутинних завдань та застосування програмного забезпечення можуть допомогти зменшити необхідний час для виконання певних робіт. Наприклад, використання спеціалізованого програмного забезпечення для обліку або автоматичного розсилання електронних листів може суттєво зекономити час працівнику. Також ефективне планування робочого дня, встановлення пріоритетів та використання технік управління часом (метод Pomodoro), допоможуть зосередитися на найважливіших завданнях і уникнути розсіяності;

- Організація робочого місця – це один із шляхів покращення життєдіяльності, що передбачає оптимізацію освітлення, простору, ергономіку меблів та обладнання, і, безпосередньо, зручність та безпеку. Робоче місце розташовують у найкраще природно освітлювальній частині кімнати. У разі нестачі природного світла використовують приємне та регульоване штучне освітлення, яке не спричиняє надмірного напруження очей. Належне розташування столу, стільця, монітора комп’ютера, клавіатури та миші допомагає уникнути перенапруження м'язів, що може спровокувати проблеми з поставою.

- Покращення режиму праці та відпочинку – цей спосіб передбачає баланс між роботою та вільним часом. Наприклад, складання розкладу чи графіку на кілька днів або тижнів, де буде запланований час для відпочинку та розваг. До того ж створення режиму задля якісного сну відновлює фізичну і психологічну енергію, покращує когнітивні функції і загальний стан здоров'я людини.

- Раціональне використання засобів фізичної культури й спорту – здоровий спосіб життя є ключовим аспектом підвищення життєдіяльності. Регулярні перерви, фізична активність, здоровий сон і налагоджені відносини в

робочому оточенні можуть позитивно вплинути на продуктивність і загальний стан працівника не лише в умовах війни, але й загалом.

До пасивних методів, що побічно впливають на працездатність і продуктивність праці, можна віднести оздоровлення умов зовнішнього середовища, тобто поліпшення метеорологічних умов, зниження шуму, вібрації, зменшення запиленості й загазованості повітря тощо [17].

Кліматичні умови можуть суттєво впливати на самопочуття та працездатність людини. Підтримка комфортної температури та вологості повітря сприяє зниженню фізичного напруження, покращує концентрацію та сприйняття інформації.

Щодо основних організаційних методів зниження шуму та відбрації, то до них належать: захист часом (обмеження часу перебування людини в умовах підвищеного шуму); захист відстанню (віддалення робочих місць від джерел шуму) []. Також для зниження рівня шуму і вібрації використовують індивідуальні засоби захисту, а саме: вушні вкладиші, навушники, шоломофони тощо. Під час їхнього застосування отримують зниження рівня звукового тиску на 10–15 дБ. Навушники знижують рівень звукового тиску на 7–35 дБ в середньому діапазоні частот. Шоломофони захищають вушну область і знижують рівень звукового тиску на 30–40 дБ у середньому діапазоні частот.

Повітря, яке містить багато шкідливих речовин, може мати негативний вплив на дихальну систему, спричиняти алергічні реакції та погіршувати загальний стан здоров'я. Застосування ефективної системи вентиляції, використання фільтрів повітря та забезпечення чистоти приміщень можуть допомогти зменшити запиленість та забезпечити свіжий і безпечний для дихання повітря.

Отже, всі проаналізовані шляхи щодо покращення життєдіяльності людини в умовах воєнного стану можуть бути застосовані і як загальні поради задля удосконалення. Сприятливі умови праці забезпечують комфорт та безпеку працівників, а також сприяють підвищенню їх продуктивності та загального самопочуття, що є надважливо станом на сьогодні.

ВИСНОВКИ

У рамках даної кваліфікаційної роботи була успішно досягнута поставлена мета – визначення та порівняння стійкості стеганографічних методів у просторовій та частотній областях до типових перетворень графічних форматів. Для цього були послідовно виконані всі визначені задачі:

1. Проведено огляд літературних джерел, а саме здійснено аналіз сучасних наукових робіт та публікацій у галузі стеганографічного приховування інформації, що дозволило сформувати теоретичну базу дослідження.

2. Проаналізовано принципи функціонування методів, зокрема детально вивчено та описано механізми роботи стеганографічних алгоритмів, що оперують у просторовій (LSB та Кутера-Джордана-Боссена) та частотній (Коха-Жао) областях, виявивши їхні фундаментальні відмінності у підході до вбудовування даних.

3. Визначено ключові формати зображень (BMP, PNG, JPEG) та їхні характерні перетворення (стиснення, зміна розміру, конвертація), які були використані для експериментального тестування стійкості стеганограм.

4. Реалізовано обрані стеганографічні алгоритми для кожної області вбудовування для проведення експериментів, що дозволило проводити порівняльний аналіз.

5. Обрані стеганографічні алгоритми були практично застосовані до тестових зображень, після чого над цими зображеннями була виконана серія заздалегідь визначених перетворень графічних форматів.

6. Проведено оцінку збереження прихованої інформації: після кожного етапу перетворення зображень-контейнерів здійснювалося спроба вилучення прихованого повідомлення, і результати фіксувалися для подальшого аналізу.

7. На основі отриманих експериментальних даних проведено порівняльний аналіз стійкості кожного стеганографічного методу до різних типів перетворень.

За результатами проведеного дослідження можна зробити висновок, що жоден з розглянутих стеганографічних методів не забезпечує абсолютної стійкості до всіх можливих перетворень графічних форматів в умовах реального

цифрового середовища. Однак, методи частотної області мають значну перевагу над методами просторової області з точки зору робастності.

Для практичного використання в умовах, де зображення можуть бути піддані типовим перетворенням, рекомендується надавати перевагу стеганографічним методам, що працюють у частотній області. Вони є більш придатними для сценаріїв, де необхідно забезпечити збереження прихованої інформації в умовах, близьких до реальних. Проте, при виборі конкретного алгоритму слід враховувати допустимий рівень спотворень зображення-контейнера, бажану ємність прихованої інформації та очікувані види та інтенсивність атак (перетворень).

Майбутні дослідження можуть бути спрямовані на розробку гібридних стеганографічних методів, які поєднують переваги обох областей, а також на впровадження адаптивних алгоритмів, що динамічно змінюють параметри вбудовування залежно від характеристик зображення-контейнера та передбачуваних перетворень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Коханович Г.Ф., Прогонов Д.О., Пузиренко О.Ю. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних. Центр навчальної літератури, 2018. 560с.
2. Стеганографія : навчальний посібник / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 232 с.
3. Srinivasan, Divyasree & Manojkumar, Khushi & Syed, Afreen & Nutakki, Harichandana. (2024). A Comprehensive Review on Advancements and Applications of Steganography. 10.13140/RG.2.2.13568.44807.
4. Стасюк, О.І & Gnatyuk, Sergiy & Довгич, Н.І & Літош, М.С. (2011). СУЧАСНІ СТЕГАНОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ. Ukrainian Information Security Research Journal. 13. 10.18372/2410-7840.13.1994
5. Currie, D.L. & Irvine, C.E., “Surmounting the effects of lossy compression on Steganography”, 19th National Information Systems Security Conference, 1996
6. Moerland, T., “Steganography and Steganalysis”, Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf
7. Artz, D., “Digital Steganography: Hiding Data within Data”, IEEE Internet Computing Journal, June 2001
8. Currie, D.L. & Irvine, C.E., “Surmounting the effects of lossy compression on Steganography”, 19th National Information Systems Security Conference, 1996
9. Moerland, T., “Steganography and Steganalysis”, Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf
10. Artz, D., “Digital Steganography: Hiding Data within Data”, IEEE Internet Computing Journal, June 2001
11. Balagyozyan, L.A. & Hakobyan, Robert. (2021). Steganography in Frames of Graphical Animation. E3S Web of Conferences. 266. 09006. 10.1051/e3sconf/202126609006.
12. Alsarayreh, Maher & Alia, Mohammad & A., Khulood. (2017). A novel image steganographic system based on exact matching algorithm and key-dependent

data technique. Journal of Theoretical and Applied Information Technology. 95. 1212-1224.

13. Sulema, Yevgeniya. (2016). Image protection method based on binary operations. 1-4. 10.1109/IWSSIP.2016.7502760.
14. Okkyung Choi, InBae Jeon, Seung-Wha Yoo, Seungbin Moon (2013) An Extended DCT Domain Watermarking for Robot Vision against Geometric Image Attacks. Journal of Applied Mathematics
15. TIOBE Index - TIOBE. TIOBE. URL: https://www.tiobe.com/tiobe-index/ (date of access: 21.06.2025).
16. Stack Overflow Developer Survey 2023. Stack Overflow. URL: https://survey.stackoverflow.co/2023/ (date of access: 21.06.2025).
17. Стиценко Т.Є., Пронюк Г.В., Сердюк Н.М., Хондак І.І. «Безпека життєдіяльності»: навч. посібник / Т.Є Стиценко, Г.В. Пронюк, Н.М. Сердюк, І.І. Хондак. – Харків: ХНУРЕ, 2018. – 336 с.
18. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N., Tymoshchuk, V., (2024). Detection and classification of DDoS flooding attacks by machine learning methods. CEUR Workshop Proceedings, 3842, pp. 184 - 195.
19. Lupenko, S. A., Orobchuk, O., & Kateryniuk, I. (2020, November). Mathematical Modeling of Diagnosis and Diagnostic Information Space of Chinese Image Medicine for their Unified Representation in Information Systems for Integrative Scientific Medicine. In IDDM (pp. 370-376).
20. Kuznetsov, A., Karpinski, M., Ziubina, R., Kandiy, S., Frontoni E., Veselska, O., & Kozak, R. (2023). Generation of nonlinear substitutions by simulated annealing algorithm. Information, 14(5), art. no. 259, 1-16. doi: 10.3390/info14050259.
21. Development of the Structure of the Ontooriented Database of Information System «Image Therapist» Lupenko, S., Orobchuk, O., Kateryniuk, I. CEUR Workshop ProceedingsThis link is disabled., 2023, 3373, pp. 261–270.
22. Secure information system for Chinese Image medicine knowledge consolidation; CEUR Workshop Proceedings. Vol. Vol-3896. 2024. S. Lupenko, O. Orobchuk, I. Kateryniuk, R. Kozak, H. Lypak. https://ceur-ws.org/Vol-3896/
24. Y. Boltov, I. Skarga-Bandurova and M. Derkach, "A Comparative Analysis of Deep Learning-Based Object Detectors for Embedded Systems," 2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Dortmund, Germany, 2023, pp. 1156-1160, doi: 10.1109/IDAACS58523.2023.10348642.
25. Деркач М. В., Остополець В. Ю., Дерев'янченко В. С. Розробка мобільного додатку для визначення автентичності медіа файлу. Вісник Східноукраїнського національного університету імені Володимира Даля. 2023. № 3 (279). С. 5-10.