**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ**
**ТА ЗАХИСТУ ІНФОРМАЦІЇ**
**КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ**

# КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Системи кіберзахисту передачі конфіденційних даних інформаційно - комунікаційних каналами на основі стеганографічних технологій»

на здобуття освітнього ступеня магістра
зі спеціальності __125 Кібербезпека та захист інформації»
*(код, найменування спеціальності)*
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

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

Виконав: здобувач вищої освіти групи СЗДМ 61
Дмитро ЖУКОВСЬКИЙ

Керівник: ТУРОВСЬКИЙ Олександр
*д.т.н., професор* (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2026

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**
**КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ**

Кафедра ___Технічних систем кіберзахисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___Кібербезпека та захист інформації_____
Освітньо-професійна програма _Технічні системи інформаційного та кібернетичного захисту

**ЗАТВЕРДЖУЮ**
Завідувач кафедри ТСКБ
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2025 р.

**ЗАВДАННЯ**
**НА КВАЛІФІКАЦІЙНУ РОБОТУ**

___Жуковському Дмитру Петровичу_____
*(прізвище, ім'я, по батькові здобувача)*

1. Тема кваліфікаційної роботи:
«Системи кіберзахисту передачі конфіденційних даних інформаційно - комунікаційних каналами на основі стеганографічних технологій»
керівник кваліфікаційної роботи __Олександр ТУРОВСЬКИЙ д.т.н., професор_____

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

2. Строк подання кваліфікаційної роботи 15.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи: графічні зображення, стеганографічні методи приховування інформації, структурна модель системи прихованої передачі інформації у зображенні, критерії оцінки системи передачі інформації у зображенні.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
4.1. Основи застосування методів приховування інформації у зображеннях
4.2. Оцінка методів приховування інформації у зображеннях
4.3. Оцінка стійкості методів приховування інформації у зображеннях до зовнішніх впливів

5. Перелік графічного матеріалу: ___Презентаційний матеріал на слайдах._____

6. Дата видачі завдання_____15.10.2025_____

# КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Підбір науково-технічної літератури | | |
| 2 | Написання першого розділу роботи | | |
| 3 | Написання другого розділу роботи | | |
| 4 | Написання третього розділу роботи | | |
| 5 | Написання висновків по роботі | | |
| 6 | Підготовка демонстраційних матеріалів | | |
| 7 | Підготовка доповіді | | |

Здобувач вищої освіти _____ Дмитро ЖУКОВСЬКИЙ
*(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Олександр ТУРОВСЬКИЙ
*(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

# РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, загальний обсяг роботи складає 72 сторінок, має 13 рисунків, 10 таблиць. Список використаних джерел містить 24 найменування і займає 3 сторінки.

**Метою кваліфікаційної роботи** є оцінка ефективності застосування стеганографічних методів приховування інформації у зображеннях.

В кваліфікаційній роботі: проведено огляд сфер застосування методів приховування інформації в зображені; визначено математичну модель стегосистем;, подано порядок застосування контейнера передачі інформації; подано критерії оцінки стегосистеми та критерії оцінки стеганографічних методів; із застосуванням вказаних критеріїв проведено порівняльний аналіз методів приховування інформації в зображеннях та оцінено їх ефективність; оцінено стійкість методів приховування інформації у зображеннях до зовнішніх впливів та збурень.

**Апробація:**

М.В. Онищенко, Д.П. Жуковський. Принципи побудови та основи функціонування системи кіберзахисту передачі конфіденційних даних мережевими каналами на основі стеганографічних технологій. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-комунікаційних систем*. м. Київ, 05 листопада 2025 року, Київ: РВЦ ДУІКТ. – 2025. С.41-42. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

**Ключові слова**: графічні зображення, СТЕГАНОГРАФІЧНІ МЕТОДИ, МЕТОДИ ПРИХОВУВАННЯ ІНФОРМАЦІЇ, КРИТЕРІЇ ОЦІНКИ СИСТЕМИ ПЕРЕДАЧІ ІНФОРМАЦІЇ У ЗОБРАЖЕННІ.

# ABSTRACT

The qualification work consists of an introduction, three sections, general conclusions, a list of sources used, the total volume of the work is 72 pages, has 13 figures, 10 tables. The list of sources used contains 24 names and takes up 3 pages.

The purpose of the qualification work is to assess the effectiveness of the use of steganographic methods of hiding information in images.

In the qualification work: an overview of the areas of application of methods of hiding information in images is conducted; a mathematical model of stegosystems is defined; the procedure for using the information transmission container is presented; criteria for evaluating the stegosystem and criteria for evaluating steganographic methods are presented; using the specified criteria, a comparative analysis of methods of hiding information in images is conducted and their effectiveness is assessed; the stability of methods of hiding information in images to external influences and disturbances is assessed.

**Approbation:**

M.V. Onyshchenko, D.P. Zhukovsky. Principles of construction and basics of functioning of the system of cyber protection of transmission of confidential data via network channels based on steganographic technologies. All-Ukrainian scientific and practical conference: Actual problems of security of information and communication systems. Kyiv, November 05, 2025, Kyiv: DUIKT Research and Development Center. – 2025. P.41-42. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

**Keywords:** graphic images, STEGANOGRAPHIC METHODS, INFORMATION HIDDEN METHODS, CRITERIA FOR EVALUATION OF INFORMATION TRANSMISSION SYSTEMS IN IMAGES.

# ЗМІСТ

# СПИСОК УМОВНИХ СКОРОЧЕНЬ

| | | |
|---|---|---|
| NAD | – | Нормована середня абсолютна різниця |
| IF | – | Якість зображення |
| ЦОС | – | Цифрова обробка сигналу |
| ЦВЗ | – | Цифровий водяний знак |
| ПСП | – | Псевдо випадкова послідовність |
| ЗСЛ | – | Зорова система людини |
| ДКП | – | Дискретне косинусне перетворення |
| ДПФ | – | Дискретне перетворення Фур'є |
| ДКЛП | – | Дискретне перетворення Карунена-Лоєва |
| НЗБ | – | Метод заміни найменш значущого біта |
| ДВП | – | Методи на основі дискретного вейвлет-перетворення |
| КВ | – | Коефіцієнт важливості |

# ВСТУП

Обмеження на використання інструментів шифрування різними країнами, а також виникнення питань щодо захисту прав інтелектуальної власності на інформацію, представлену в цифровому вигляді, стимулювали бурхливий розвиток досліджень у галузі стеганографії. Стеганографічні методи, які приховують та передають інформацію через зображення, можуть не лише таємно передавати дані (тобто так звана класична стеганографія), але й ефективно вирішувати такі проблеми, як перешкодостійка автентифікація, запобігання несанкціонованому копіюванню інформації, відстеження поширення інформації в мережах зв'язку та пошук інформації в мультимедійних базах даних.

**Метою кваліфікаційної роботи є** оцінка ефективності застосування стеганографічних методів приховування інформації у зображеннях.

У процесі підготовки кваліфікаційної роботи були поставлені наступні задачі:

– Проведено огляд сфери застосування та порядку використання методів приховування інформації в зображеннях.

– Проведено оцінку ефективності методів приховування інформації у зображеннях.

– Проведено оцінку стійкості методів приховування інформації у зображеннях до зовнішніх впливів та збурень.

**Об’єкт дослідження**. Процес приховування інформації у зображеннях.

**Предмет дослідження**. Методи приховування інформації у зображеннях.

# Розділ 1 ОСНОВИ ЗАСТОСУВАННЯ МЕТОДІВ ПРИХОВУВАННЯ ІНФОРМАЦІЇ У ЗОБРАЖЕННЯХ

## 1.1 Сфери застосування методів приховування інформації у зображеннях

З самого початку людської цивілізації проблема приховування та безпечної передачі даних існувала завжди. Навіть стародавні цивілізації використовували секретні письма та однолітерні коди заміни для захисту інформації. Відтоді ми відкрили багато геніальних та інноваційних рішень у галузі стеганографії та криптографії [1,2].

Поява та швидкий розвиток комп'ютерних технологій стимулювали розвиток суміжних галузей, таких як стеганографія та криптографія. Постійно з'являються нові напрямки в стеганографії та методи вбудовування інформації. Поява мобільних терміналів (смартфонів, комунікаторів, а пізніше планшетів) надала нові можливості для застосування стеганографії. Різноманітність контейнерів, диверсифікація методів передачі та широке використання мобільних платформ визначають важливість вищезазначених проблем сьогодні[4,7,8,11].

Стеганаліз – це наука, яка вивчає методи та техніки приховування конфіденційних даних. Його основним завданням є приховування існування секретних даних під час передачі, зберігання або обробки. Завдання вилучення інформації є вторинним і здебільшого вирішується стандартними криптографічними методами. Іншими словами, існування прихованої інформації означає не лише те, що наявність іншого (прихованого) повідомлення в перехопленій інформації не може бути виявлена, але й те, що не виникне жодних підозр, оскільки в останньому випадку проблеми інформаційної безпеки зводяться до стабільності криптографії. Тому стеганографія не замінює криптографію в забезпеченні безпеки, а радше доповнює її [1,2].

Стеганологічний аналіз можна реалізувати різними способами. Спільним для них є вбудовування прихованої інформації в непомітний об'єкт, а потім публічне надсилання цього об'єкта одержувачу.

Історично стеганографія спочатку була основним методом приховування інформації, але з часом її значною мірою витіснила криптографія. За останні два десятиліття інтерес до стеганографії відродився завдяки широкому використанню мультимедійних технологій. Не менш важливою є поява нових каналів передачі інформації, що, поряд з першим фактором, стимулювало розвиток та вдосконалення стеганографії, що призвело до появи нових методів стеганографії, заснованих на характеристиках представлення інформації комп'ютерних файлів, комп'ютерних мереж тощо. Це, у свою чергу, дозволяє обговорювати появу нового напрямку в галузі захисту інформації — комп'ютерної стеганографії [2,3].

Сьогодні стеганографія — це наука, що швидко розвивається, яка використовує методи та досягнення криптографії, цифрової обробки сигналів, зв'язку та теорії інформації. Методи стеганографії дозволяють не тільки таємно передавати дані (так звана класична стеганографія), але й успішно вирішувати проблему перешкодостійкої автентифікації. Захист інформації включає запобігання несанкціонованому копіюванню, відстеження поширення інформації в мережах зв'язку, пошук інформації в мультимедійних базах даних тощо. У рамках існуючих інформаційних потоків або інформаційних середовищ було розглянуто деякі важливі питання захисту інформації в цих областях застосування [1,2,3].

Комп'ютерна стеганографія має дві основні області застосування [2,4]:

– Застосування, поєднані з цифровою обробкою сигналів (ЦОС);

– Застосування, не поєднані з ЦОС.

У першому випадку секретна інформація вбудована в цифрові дані, які зазвичай мають аналогові характеристики (мовлення, зображення, аудіо- та відеозаписи) [4].

У другому випадку конфіденційна інформація розміщується в заголовку документа або пакета даних. Оскільки вилучення або знищення прихованої інформації є відносно простим, ця область не використовується широко [2,4].

Наразі більшість досліджень у галузі стеганографії пов'язані з ЦОС, тому ми можемо назвати її цифровою стеганографією. Зростання досліджень стеганографії зумовлене головним чином двома причинами: по-перше, обмеженнями на використання методів шифрування в різних країнах; і по-друге, зростаюча важливість питання захисту прав інтелектуальної власності на інформацію, представлену в цифровому вигляді. Перша причина спонукала до великої кількості досліджень, зосереджених на традиційній стеганографії (тобто приховуванні фактів передачі інформації), тоді як друга спонукала до більшої кількості досліджень так званих «водяних знаків». Цифрові водяні знаки (ЦВЗ) – це спеціальні теги, які непомітно додаються до зображень або інших сигналів, певним чином контролюючи їх використання [4,5].

Просто покладатися на незнання зловмисником методу приховування інформації наразі неефективно. Тому, навіть якщо зловмисник повністю розуміє структуру та алгоритми роботи системи безпеки, система безпеки все одно повинна виконувати свої функції [2,4].

Наразі стеганографія може використовуватися для прихованого зв'язку, захисту авторських прав на зображення (автентифікація), розпізнавання відбитків пальців (відстеження зрадників), додавання описового тексту до зображень, додавання субтитрів до відео, захисту цілісності зображення (виявлення підробок), контролю авторських прав при записі DVD та інтелектуальних браузерах, а також автоматичного надання інформації про авторські права [4,7,8,11].

Прикладом стеганографії є створення резервних каналів зв'язку, таких як зв'язок з дипломатичними місіями, розташованими за кордоном. У тоталітарних країнах із суворою інтернет-цензурою стеганографія також використовується для надсилання секретних повідомлень (рис. 1.1) [5].

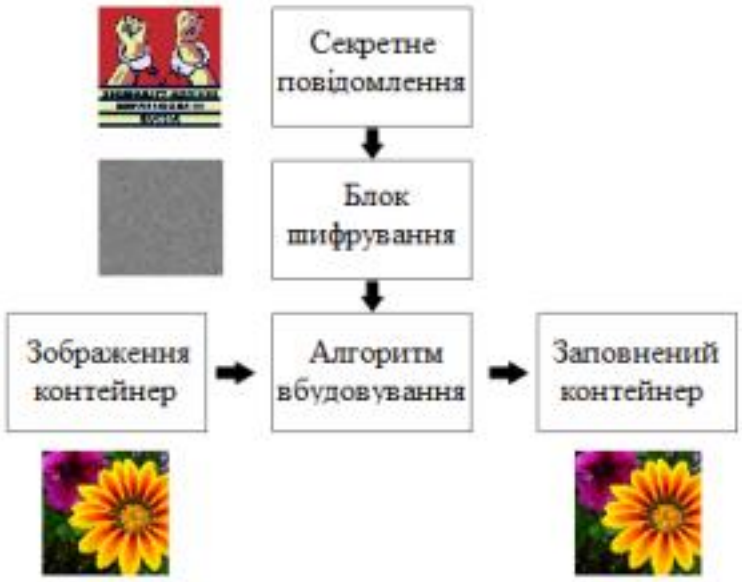



Рис. 1.1. Блок-схема процесу вбудовування повідомлення при прихованому зв’язку

У цьому випадку необхідно враховувати моніторинг локальних каналів зв'язку. Надсилання зашифрованих повідомлень неминуче викличе підозру та може призвести до обмеження доступу до комунікаційної інфраструктури. Тому відправник повинен максимально приховувати існування зв'язку. Цю ситуацію можна вирішити, використовуючи відповідні протоколи стеганографії [5,6].

Зі швидким розвитком мультимедійних технологій питання захисту авторських прав на зображення, а саме автентифікація (Рисунок 1.2) [5], стало особливо актуальним. Наприклад, фотографії, аудіо- та відеозаписи тощо. Переваги представлення та передачі інформації в цифровому вигляді можуть бути компенсовані її легкістю крадіжки або підробки. Наприклад, автор цифрового зображення може захотіти «підписати» зображення, щоб інші не могли ідентифікувати його як автора. Інформацію про автора не можна додати до файлу зображення або надрукувати на зображенні видимим чином, оскільки такі підписи легко видалити або замінити [4,7,8,11].

Зашифровані цифрові підписи можна використовувати лише для

перевірки каналів зв'язку, але вони не можуть захистити зображення на веб-сторінках. Найкращий спосіб захистити зображення - це вбудувати стабільний, безпечний та невидимий цифровий підпис у зображення. У цьому випадку автор повинен зберегти оригінальне зображення. Щоб довести своє авторство або ідентифікувати підроблене зображення, автору потрібно перевірити, чи є на зображенні вбудований цифровий підпис. Досвідчені злодії можуть спробувати видалити оригінальний водяний знак або вставити власний підпис у зображення. Але це не спрацює, оскільки зображення залишить сліди цифрового підпису, тоді як автор може надати оригінальний файл [5,6].

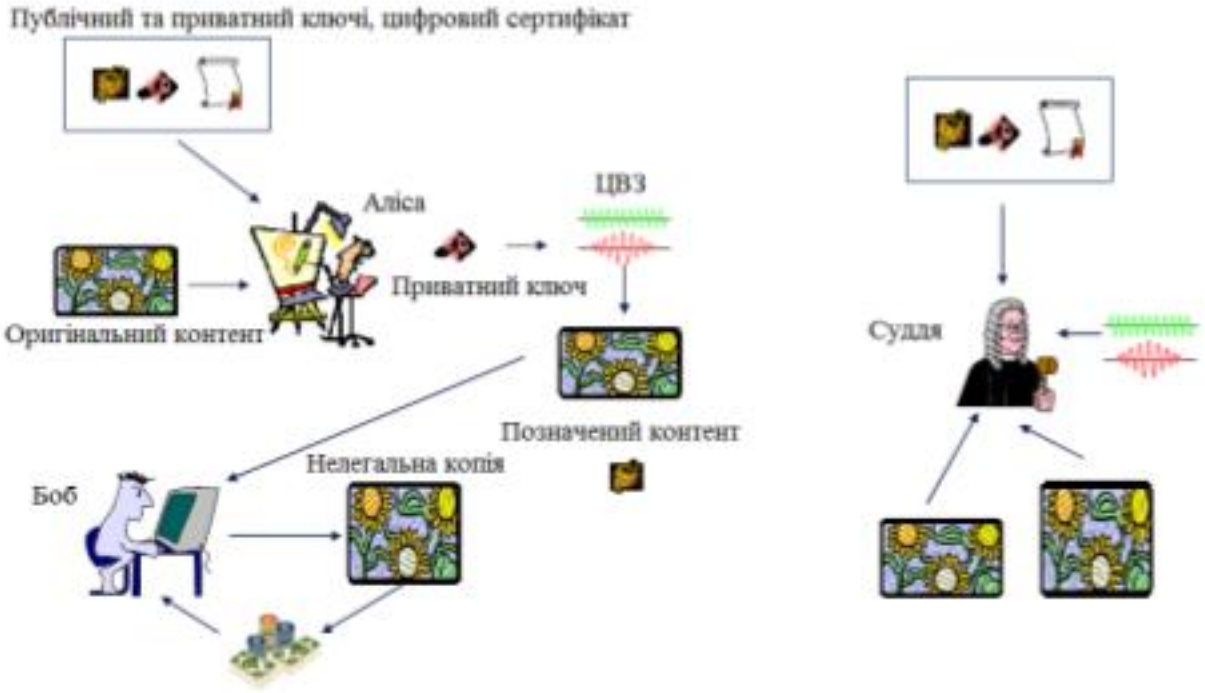



Рис. 1.2. Блок-схема процесу вбудовування ЦВЗ з метою захисту авторських прав

Технологія вбудовування ідентифікаційних кодів виробника має багато спільного з технологією CVE. Різниця полягає в тому, що кожна захищена копія має свій унікальний вбудований номер (звідси й назва – буквально означає «відбиток пальця»). Цей ідентифікаційний код дозволяє виробнику відстежувати подальший потік своєї продукції [5,7]. Типовим прикладом є

продаж справжніх компакт-дисків. Завдяки цьому унікальному номеру легко визначити, хто виготовив і розповсюдив ці незаконні копії (Рисунок 1.3) [5]. Іншим сценарієм є розповсюдження конфіденційної інформації (фотографій, відео) кільком представникам та відстеження того, хто є зрадником і через кого інформація просочилася ворогу. У цьому випадку неможливо використовувати видимий підпис, оскільки така позначка виглядатиме підозріло і її легко видалити. Ідентифікаційна позначка має бути візуально невидимою та присутньою на кожному розповсюдженому зображенні [4,7,8,11].

Крім того, вбудований ідентифікаційний код має бути достатньо надійним, щоб не вийти з ладу навіть після багаторазового копіювання та редагування.

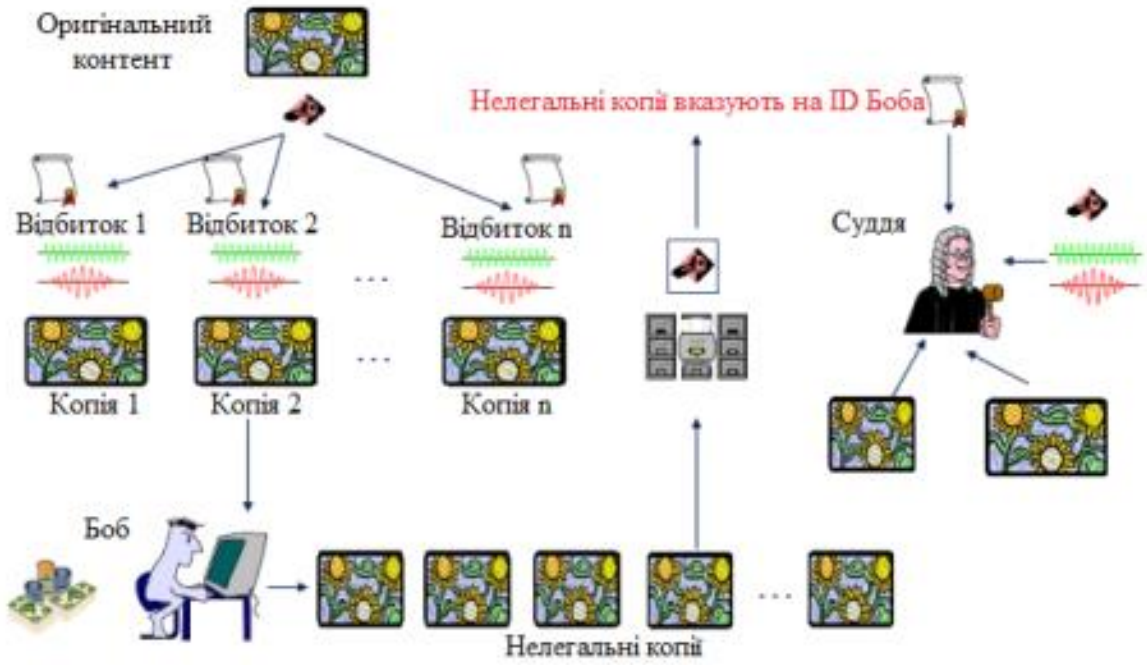



Рис. 1.3. Блок-схема процесу вбудовування ідентифікаційних номерів з метою відстеження порушника

Наприклад, вбудовані титри можуть використовуватися для додавання субтитрів до медичних зображень, додавання легенд до карт тощо. Мета полягає в тому, щоб зберігати інформацію, представлену в різних формах, в

межах однієї сутності. Це може бути єдиним застосуванням стеганографії, де немає очевидного потенційного порушника [5,6,7].

Типові приклади включають багатомовне дублювання фільмів, субтитри та відстеження використання даних (історичні файли). Наприклад, одну копію фільму можна розповсюджувати разом з багатомовними субтитрами. Відеомагнітофони, DVD-програвачі, телевізори та інші відеопристрої можуть отримувати доступ до додаткового тексту (субтитрів) для кожного кадру та декодувати його в режимі реального часу та відображати на екрані телевізора. Хоча цей процес можна досягти шляхом додавання інформації замість неявного вбудовування, вимоги до пропускної здатності та необхідність зміни формату іноді можуть перешкоджати цій практиці [5,7].

Однією з областей застосування стеганографії є захист цілісності зображення, що дозволяє виявляти шахрайство (рис. 1.4) [5]. На жаль, цифрові зображення наразі не є допустимими як судові докази через легкість підробки та складність виявлення фальсифікації зображення. Вбудовування водяних знаків у цифрові зображення для виявлення місця та ступеня модифікації зображення відіграватиме важливу роль у виявленні цифрового шахрайства та може служити судовим доказом. Переваги використання водяних знаків очевидні: водяні знаки не залежать від формату зображення, не збільшують пропускну здатність (на відміну від додавання інформації заголовка) та не можуть бути видалені для запобігання підробці [4,7,8,11].

Пристрої обробки зображень (такі як цифрові камери, відеокамери або сканери) позначають зображення унікальними, постійними та безпечними водяними знаками перед тим, як зберігати їх на електронних носіях або надсилати на інші пристрої (такі як комп'ютери) для відображення [5,7].

Поширеним застосуванням стеганографії є контроль копіювання під час запису DVD. Комерційно випущені фільми часто мають постійні, невидимі водяні знаки, які вказують на те, чи можна копіювати фільм [6].

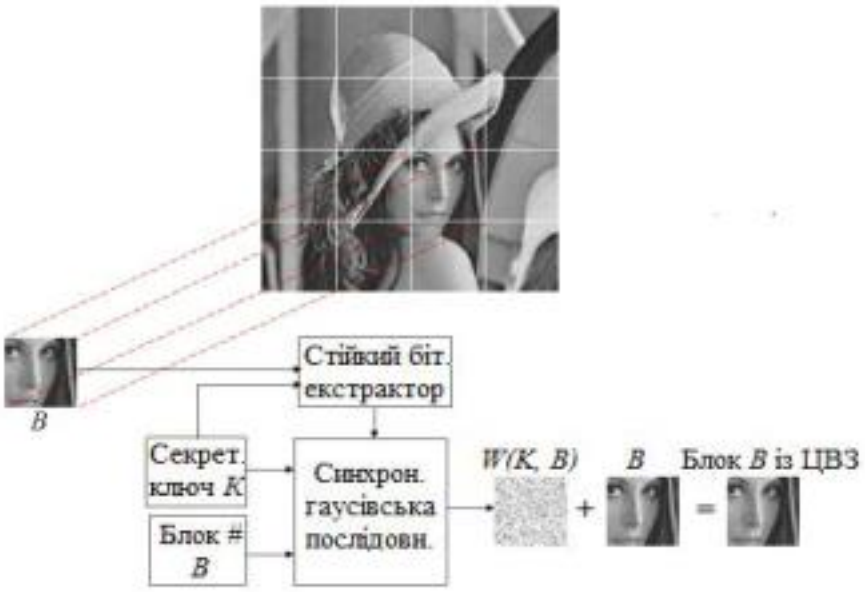



Рис. 1.4. Блок-схема процесу вбудовування ЦВЗ для захисту цілісності зображення

DVD-програвачі можуть отримати доступ до водяного знака та відмовитися копіювати фільм на інший диск (рис. 1.5) [5].

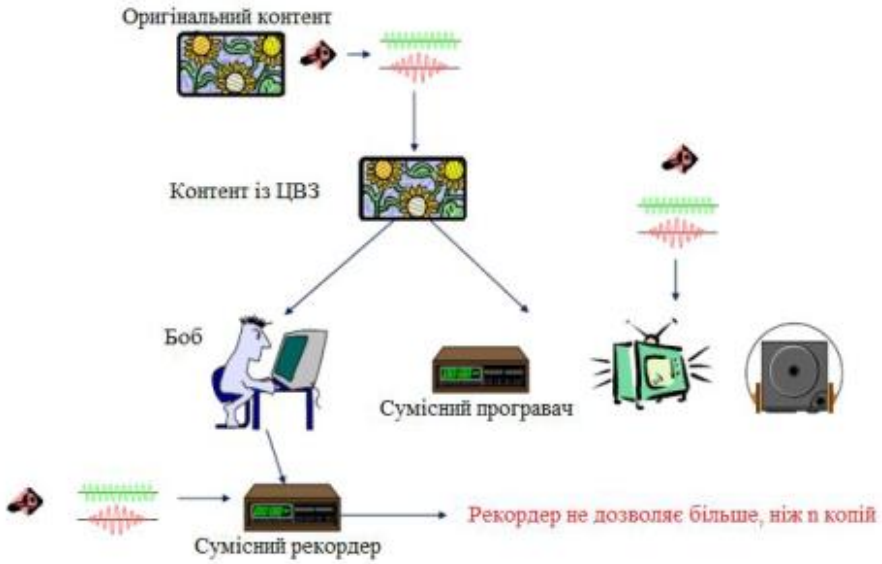



Рис. 1.5. Блок-схема процесу вбудовування ЦВЗ для управління копіюванням при записі DVD

Стеганографія також використовується в інтелектуальних браузерах та для автоматичного надання інформації про авторські права.

Після завантаження зображення воно перевіряється на наявність водяних знаків перед відображенням у браузері [5,6,7]. Якщо виявляються водяні знаки, зображення не відображається та автоматично видаляється з пам'яті комп'ютера. Ще одним застосуванням цієї технології є відображення інформації про авторські права для кожного зображення, наданого браузером, а також інформації про авторські права програмного забезпечення, яке обробило зображення (наприклад, Photoshop або PaintShop) [4].

## 1.2 Структурна модель системи передачі інформації у зображенні

На рисунку 1.6 показано загальну структурну схему стеганографічної системи як системи передачі інформації [5,7].

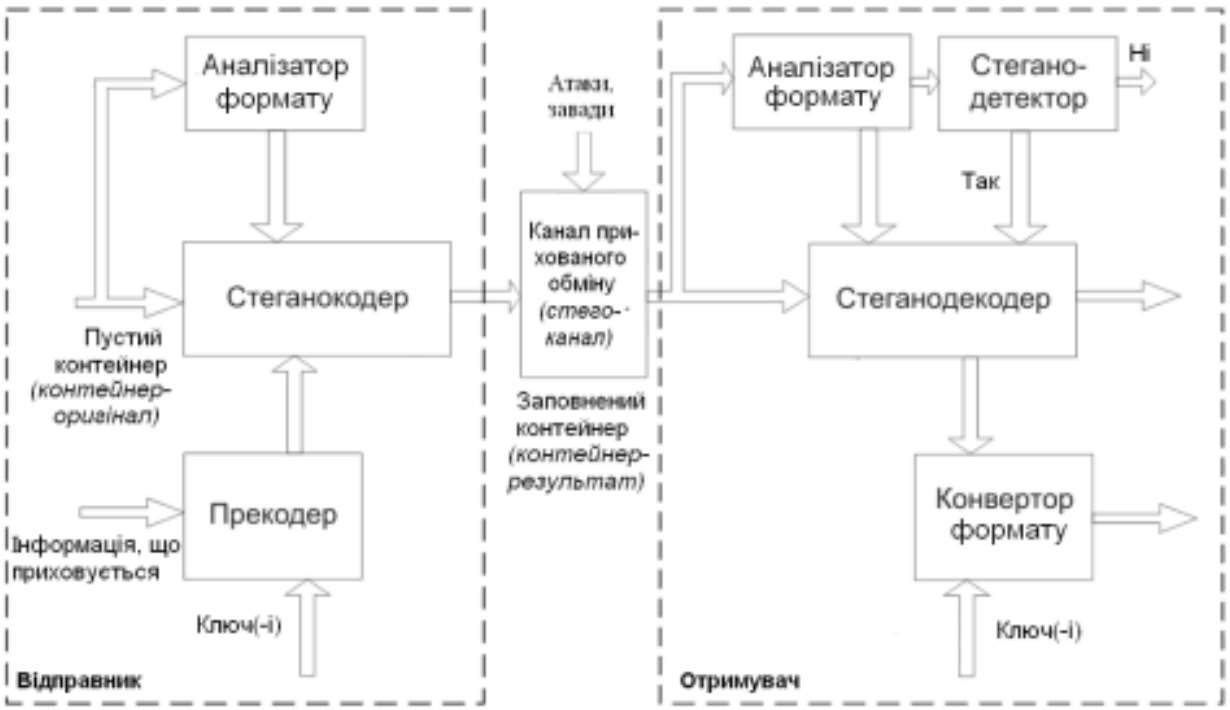



Рис. 1.6. Структурна схема стеганосистеми як системи передачі інформації

### 1.2.1 Математична модель стеганосистеми.

Процес тривіального стеганографічного перетворення описується залежностями [1,8 ]:

$$E: C \times M \rightarrow S; (2.1) \quad (1.1)$$

$$D: S \rightarrow M, (2.2) \quad (1.2)$$

де $S = \{(c1, m1), (c2, m2), ..., (cn, mn), ..., (cq, mq)\} = \{s1, s2, ..., sq\}$ – множина контейнерів-результатів (стеганограм).

Залежність (1.1) описує процес приховування інформації, а залежність (1.2) описує процес вилучення прихованої інформації. Необхідною умовою в цьому випадку є відсутність "перетину" [1,8], тобто, якщо $ma \neq mb$, і $ma, mb \in M$, і $(ca, ma), (cb, mb) \in S$, то $E(ca, ma) \cap E(cb, mb) = \emptyset$. Крім того, також має бути виконано вимогу до потужності множини $|C| \geq |M|$. У цьому випадку і відправник, і одержувач повинні знати алгоритми прямого (E) та зворотного (D) стеганографічного перетворення.

Отже, загалом, стеганографічна система складається з набору $\Sigma = (C, M, S, E, D)$ контейнерів (вихідної інформації та результату), повідомлень та перетворень, що їх з'єднують.

Для більшості стеганографічних систем вибір множини контейнерів C такий, що після стеганографічного перетворення (1.1) заповнений контейнер подібний до вихідного контейнера. Цю подібність можна формально оцінити за допомогою функції подібності [1,7].

Визначення 1.1. Нехай C — непорожня множина, тоді функція має вигляд:

$$sim(C) \rightarrow (-\infty, 1]$$

є функцією подібності на множині C.

Якщо для будь-яких $x, y \in C$ справедливо, що $sim(x, y) = 1$ у випадку $x = y$ і $sim(x, y) < 1$ при $x \neq y$.

Стеганографічну систему можна вважати надійною, якщо sim[c, E(c, m)] ≈ 1 для всіх m ∈ M та c ∈ C. Крім того, контейнер c слід вибрати таким, що раніше не використовувався.

Крім того, неавторизований персонал не повинен мати доступу до набору контейнерів, що використовуються для секретного зв'язку.

Вибір конкретного контейнера c з можливого набору контейнерів C може бути довільним (так званий метод проксі-вибору контейнера), або це може бути контейнер, який найменше змінюється під час стеганографічного перетворення (вибірковий метод). В останньому випадку вибір контейнера відбувається за правилом: c sim[x, E(x, m)] x∈C=max.

Слід також зазначити, що загалом функції стеганографічного перетворення вперед (E) та назад (D) можуть бути довільними (звичайно, вони відповідають одна одній), проте на практиці вимога стабільності прихованої інформації накладає певні обмеження на ці функції. Отже, у більшості випадків E(c, m) ≈ E(c + δ, m), або D[E(c, m)] ≈ D[E(c + δ, m)] = m, тобто незначна зміна контейнера (на значення δ) не призведе до зміни прихованої інформації в ньому [1,7,8].

### 1.2.2 Порядок формування та застосування контейнерів передачі інформації.

Процес передачі файлу від відправника до одержувача починається з обробки секретної інформації (тобто повідомлення), яку потрібно приховати. Початкову обробку виконує попередній кодувальник. Це має вирішальне значення для підвищення безпеки та стійкості стеганографічної системи до несанкціонованого доступу. У більшості випадків ключ використовується для визначення секретного алгоритму, який визначає порядок, у якому повідомлення потрапляють до контейнерів [5,6].

Контейнери – це несекретна інформація, яку можна використовувати для приховування повідомлень. Звичайні текстові файли та мультимедійні формати можуть використовуватися як як повідомлення, так і як контейнери [1,6].

Порожній контейнер (вихідний контейнер) – це контейнер, який не містить прихованої інформації.

Заповнений контейнер (результативний контейнер) – це контейнер, який вже містить приховану інформацію. Важливою вимогою є те, щоб результуючий контейнер візуально не відрізнявся від вихідного контейнера. Існує два основних типи контейнерів: потокові контейнери та фіксовані контейнери [4,7,8,11].

Потоковий контейнер – це постійно змінна послідовність бітів. Повідомлення вбудовується в нього в режимі реального часу, тому кодер не може заздалегідь знати, чи достатній розмір контейнера для передачі всього повідомлення. Основна проблема полягає у виконанні синхронізації, визначенні початкової та кінцевої точок послідовності. Якщо в заданій послідовності присутні біти синхронізації, заголовки пакетів тощо, прихована інформація може слідувати негайно. З точки зору забезпечення конфіденційності, складність організаційної синхронізації насправді є перевагою.

У фіксованому контейнері розмір та характеристики контейнера відомі заздалегідь. Це дозволяє вбудовувати дані найкращим чином. Тому фіксовані контейнери («контейнери») будуть розглянуті в основному нижче [1,6].

Контейнери можуть бути вибраними, випадковими або обов'язковими. Вибраний контейнер залежить від вбудованого повідомлення, а в крайніх випадках також від функції повідомлення. Цей тип контейнера найбільш характерний для стеганографії. Обов'язкові контейнери виникають, коли постачальник контейнера підозрює про можливість прихованого зв'язку та бажає запобігти йому. Однак на практиці вони найчастіше мають справу з випадковими контейнерами [4,7,8,11].

Прихована інформація часто є значною, що ставить високі вимоги до контейнера; Його розмір має бути щонайменше в кілька разів більшим за

розмір вбудованих даних. Очевидно, що для покращення конфіденційності зазначене співвідношення має бути трохи більшим.

Перед вбудовуванням повідомлення в контейнер його необхідно представити у вигляді, який легко зрозуміти. Крім того, для підвищення безпеки секретної інформації її можна зашифрувати за допомогою стабільних криптографічних кодів перед інкапсуляцією в контейнер. У багатьох випадках отримані стеганографічні повідомлення також повинні бути стійкими до втручання (включаючи зловмисне втручання) [1,2,6].

Під час передачі відео, зображень або будь-якої іншої інформації, що використовується як контейнер, можуть відбуватися різні перетворення (включаючи використання алгоритмів з втратами): наприклад, зміни обсягу, перетворення в інші формати тощо. Тому для збереження цілісності вбудованої інформації можуть знадобитися коди корекції помилок (шумостійкі коди).

Початкова обробка інформації, яку потрібно приховати, виконується попереднім кодером. Одним з найважливіших кроків попередньої обробки повідомлення (та його контейнера) є обчислення його узагальненого перетворення Фур'є. Це дозволяє вбудувати дані в спектральну область, значно покращуючи їх стійкість до спотворень. Для підвищення конфіденційності вбудовування попередня обробка зазвичай використовує ключ [4,6].

Упаковка повідомлення в порожній контейнер з урахуванням формату контейнера виконується за допомогою стегкодера. У більшості стегоаналітичних систем для упаковки та вилучення повідомлень використовується ключ; цей ключ визначає порядок, у якому повідомлення вставляються в контейнер, і визначає секретний алгоритм. Тип ключа визначає існування двох стеганалітичних систем [4,5,6]:

– Використання закритого ключа;

– Використання відкритого ключа.

Генератори псевдовипадкових послідовностей (PSS) можуть використовуватися як секретні алгоритми.

Прихована інформація вводиться в ці біти відповідно до ключа, і модифікації цих бітів не викликають суттєвого спотворення контейнера. Ці біти складають так званий стеганографічний канал.

Стеганографічний канал – це канал, який використовується для передачі результату контейнера. Однак у межах стеганографічного каналу контейнер, що містить приховану інформацію, може бути об'єктом навмисних атак або випадкових перешкод [5,6].

Стеганалітичні детектори виявляють наявність потенційно змінених прихованих даних у контейнері на основі формату даних контейнера. Ці модифікації можуть бути пов'язані з помилками в каналі зв'язку, операціями обробки сигналів або навмисними атаками зловмисників.

Деякі стеганографічні детектори призначені виключно для виявлення наявності вбудованих повідомлень; інші, такі як стегкодери, призначені для вилучення повідомлення з контейнера [4,5,6].

Таким чином, у стеганографічній системі два типи інформації поєднуються унікальним чином, що робить їх сприйнятими по-різному різними детекторами. Один детектор – це система вилучення прихованого повідомлення, а інший – той, що надсилає запит до системи передачі, що важко формально описати.

Для забезпечення надійної та високоякісної стеганографічної системи під час проектування необхідно виконати кілька вимог [4,5,6]:

– Заповнений контейнер повинен бути візуально невідрізним від порожнього контейнера. Щоб відповідати цій вимозі, приховане повідомлення має бути явно вбудоване у візуально непомітні області сигналу. Однак ці області також використовуються алгоритмами стиснення. Отже, якщо зображення додатково стиснути, прихована інформація може бути знищена.

Тому інформаційні біти повинні бути вбудовані у візуально важливі області, а їхня відносна невидимість має бути досягнута за допомогою спеціальних методів.

Система стеганографії CVS повинна мати низьку ймовірність хибного виявлення, тобто низьку ймовірність неправильного виявлення прихованої інформації в сигналі, який її не містить. У деяких застосуваннях такі хибні виявлення можуть мати серйозні наслідки. Необхідно забезпечити достатню пропускну здатність [4,7,8,11].

Обчислювальна складність реалізації системи стеганографії повинна бути в межах прийнятного діапазону. У цьому випадку в системі CVS може існувати асиметрія складності реалізації, тобто складний стегкодер проти простого стегкодеру.

### 1.3. Критерії оцінки стеганосистем

Наразі запропоновано велику кількість методів стеганографії, деякі з яких є універсальними, а інші призначені для різноманітних завдань. Для порівняння та оцінки якості інструментів стеганографії можна використовувати визнані метрики, які забезпечують як кількісні, так і якісні оцінки [5-8].

#### 1.3.1. Кількісні показники

Для порівняння та оцінки ефективності інструментів стеганографії зазвичай використовуються існуючі кількісні метрики, засновані на зображеннях на рівні пікселів. Однак, з відповідними коригуваннями, ці метрики також можна застосовувати до інших методів опису зображень та аудіоданих [4,5,6].

Під час аналізу ступеня спотворень, що вносяться в контейнер під час приховування інформації, найчастіше використовується метрика відношення сигнал/шум (SNR), яка походить з радіотехніки. Це безрозмірна величина, що дорівнює відношенню корисного сигналу до шуму. Чим більше це відношення, тим менше спотворень зображення спричинено шумом [5,6].

$$SNR = \frac{\sum_{x=1}^{rows(C)} \sum_{y=1}^{cols(C)} (C_{x,y})^2}{\sum_{x=1}^{rows(C)} \sum_{y=1}^{cols(C)} (C_{x,y} - S_{x,y})^2}, \quad (1.3.)$$

де $C_{x,y}$ – значення пікселя порожнього контейнера з координатами $(x,y)$,

$S_{x,y}$ – відповідне значення пікселя заповненого контейнера,

*rows (C)* – кількість рядків у масиві $C$,

*cols (C)* – кількість стовпців у масиві $C$.

Нормалізована середня абсолютна різниця (NAD) відображає ступінь різниці між оригінальним контейнером та контейнером із вбудованим секретним файлом і розраховується наступним чином [5,6]:

$$NAD = \frac{\sum_{x=1}^{rows(C)} \sum_{y=1}^{cols(C)} |C_{x,y} - S_{x,y}|}{\sum_{x=1}^{rows(C)} \sum_{y=1}^{cols(C)} |C_{x,y}|}. \quad (1.4)$$

Якість зображення (ЯЗ) є однією з основних оціночних характеристик методів стеганографії зображень. Це пояснюється тим, що візуальні атаки базуються на здатності зорової системи людини аналізувати зображення та виявляти суттєві відмінності в них. Вона характеризує ступінь відповідності між порожнім та повним контейнерами [5,6].

$$IF = 1 - \frac{\sum_{x=1}^{rows(C)} \sum_{y=1}^{cols(C)} (C_{x,y} - S_{x,y})^2}{\sum_{x=1}^{rows(C)} \sum_{y=1}^{cols(C)} (C_{x,y})^2}. \quad (1.5)$$

Середньоквадратична похибка (СКП) – це стандартне відхилення статистичного розподілу вибірки. Іншими словами, її можна використовувати

для оцінки точності середнього значення вибірки [5,6]:

$$MSE = \frac{1}{X \cdot Y} \sum_{x=1}^{rows(C)} \sum_{y=1}^{cols(C)} (C_{x,y} - S_{x,y})^2 . \quad (1.6)$$

Середня абсолютна різниця (AD) визначає середнє значення модулів різниці між пікселями в порожньому контейнері та пікселями в повному контейнері. Більше значення AD вказує на гіршу якість зображення [5,6]:

$$AD = \frac{1}{X \cdot Y} \sum_{x=1}^{rows(C)} \sum_{y=1}^{cols(C)} \left| C_{x,y} - S_{x,y} \right| . \quad (1.7)$$

### 1.3.2. Якісні показники

Найважливіші якісні характеристики стеганографічних систем, створених за допомогою різних методів, включають [5,6,7]:

Пропускна здатність — кількість бітів прихованої інформації, яку можна передати за допомогою цього методу на зображенні фіксованого розміру. Стеганографічні системи повинні забезпечувати необхідну пропускну здатність [8,9].

Стабільність — здатність витягувати приховану інформацію після звичайних операцій обробки зображень, таких як лінійна та нелінійна фільтрація (розмиття, підвищення різкості, медіанна фільтрація), стиснення з втратами, коригування контрастності, перефарбовування, передискретизація, масштабування, обертання, додавання шуму, обрізання, друк/копіювання/сканування, перестановка пікселів у малій околиці [7,8], квантування кольору тощо. Ми наголошуємо, що концепція стабільності не включає атаки на метод вбудовування, засновані на знанні алгоритму приховування або вилучення. Стабільність стосується здатності протистояти

«сліпим», ненаправленим модифікаціям або звичайним маніпуляціям із зображеннями [4,7,8,11].

Невидимість стосується властивості, що стегааналіз не може бути виявлений людським оком без використання спеціальних інструментів. Ця концепція повністю базується на характеристиках зорової системи людини (ЗСЛ). Прихована інформація вважається невидимою, якщо пересічна людина не може розрізнити носій, що містить приховану інформацію, від того, що її не містить. У психовізуальних експериментах часто використовується загальноприйнятий експериментальний протокол (так званий сліпий тест). Принцип полягає в тому, що суб'єктам випадковим чином демонструється велика кількість носіїв, що містять і не містять вбудованої інформації, і їх просять вибрати, які носії містять приховані дані [8,9].

Важливо зазначити, що концепцію невидимості також можна визначити по-іншому та пов'язати зі статистичною моделлю джерела зображення.

У цьому випадку прихована інформація вважається невидимою, якщо зображення заповненого контейнера узгоджується з моделлю оригінального джерела зображення та може бути обчислене об'єктивними методами (наприклад, за допомогою індексу IF).

Безпека — на основі відомих алгоритмів вбудовування та вилучення (за винятком ключа) та знання принаймні одного носія, що містить приховану інформацію, вбудовану інформацію неможливо видалити цілеспрямованою атакою. Концепція безпеки також включає процедурні атаки, такі як атака IBM [7,8], або атаки, засновані на знанні часткових модифікацій носія у вбудованій інформації [8,9].

Складність вбудовування та вилучення — кількість стандартних операцій, необхідних для вбудовування та виявлення прихованої інформації.

Системи стегаграфічної обробки повинні мати прийнятну обчислювальну складність. У цьому випадку для реалізації стеганографічної системи передачі інформації можна використовувати асиметричний підхід, а саме, використовуючи складний стегкодер та простий стегкодер.

Вищезазначені вимоги суперечать одна одній і не можуть бути оптимально досягнуті одночасно. Якщо на зображенні потрібно приховати довгу інформацію, не можна одночасно вимагати абсолютної невидимості та високої стабільності; необхідно знайти оптимальний компроміс. З іншого боку, якщо потрібна стійкість до значного спотворення зображення, довжина надійно прихованої інформації не може бути занадто великою. Рисунок 1.7 схематично ілюструє це явище. [5,9]

### 1.4. Огляд існуючих стеганографічних методів

Більшість існуючих методів приховування інформації використовують просторову область та область перетворення [1,2,4,5,9]. Методи, що використовують область перетворення, в основному базуються на дискретному косинусному перетворенні (DCT), дискретному перетворенні Фур'є (DFT), дискретному вейвлет-перетворенні (DWT), дискретному перетворенні Карунена-Лоева (DKLT) тощо. Ці перетворення можуть бути застосовані до різних частин зображення або до всього зображення [1,2,4,5,9].


Рис. 1.7. «Магічний трикутник» ключових характеристик стеганосистем

У цьому дослідженні було обрано найпоширеніший метод заміщення найменш значущих бітів (LSB), один з найкращих методів у просторовій області – метод Каттера-Джордана-Боссена, один з основних методів у частотній області – вдосконалений метод Коха-Чжао, метод Бенгама – удосконалення попереднього методу, метод на основі DVP та метод на основі спектрального розкиду [1,2,4,5,9].

### 1.4.1. Методи приховування у просторову область

Методи, що використовують просторові області зображення, вбудовують приховані дані в область вихідного зображення. Їхня перевага полягає в тому, що вбудовування можна виконувати без виконання обчислювально складних та трудомістких перетворень зображення.

Ми представимо кольорове зображення C за допомогою дискретної функції, яка визначає вектор кольору c(x, y) для кожного пікселя (x, y) на зображенні, де значення кольору задаються тривимірним вектором у колірному просторі.

Найпоширенішим методом перетворення кольорів є модель RGB, де основними кольорами є червоний, зелений та синій, а будь-який інший колір може бути представлений як зважена сума основних кольорів [1, 5, 9].

Вектор кольору c(x, y) у просторі RGB представляє інтенсивність основного кольору. Повідомлення можна вбудувати [1, 5, 9] шляхом маніпулювання колірними компонентами або безпосереднього маніпулювання яскравістю [4,7,8,11].

Основний принцип цих методів полягає в заміні надлишкових, неважливих частин зображення бітами секретного повідомлення. Щоб витягти повідомлення, необхідно знати алгоритм розміщення прихованої інформації в контейнері. Підстановка найменш значущим бітом (LSB) є найпоширенішим методом підстановки в просторовій області.

Найменш значущі біти зображення несуть найменшу кількість інформації. Як добре відомо, людське око в більшості випадків не може сприйняти зміни в цьому біті. Фактично, сам LSB є шумом, тому інформацію можна вбудувати, замінивши найменш значущий біт пікселя зображення бітами, що містять секретну інформацію. Для зображень у градаціях сірого (кожен піксель закодований одним байтом) обсяг вбудованих даних може досягати 1/8 від загальної ємності контейнера. Заміна двох LSB подвоює пропускну здатність [1,5,9].

Цей метод популярний завдяки своїй простоті та тому, що він дозволяє приховати значну кількість інформації у відносно невеликих файлах (пропускна здатність створеного прихованого каналу зв'язку коливається від 12,5% до 30%). Цей метод найчастіше використовується для растрових зображень, представлених у нестиснутих форматах, таких як GIF та BMP.

Цей метод вбудовує приховані дані в області вихідного зображення. Його перевага полягає в тому, що під час вбудовування не потрібні обчислювально складні та трудомісткі перетворення зображень (рис. 1.8) [1,5,9].


Рис. 1.8. Зміна кольору при заміні НЗБ

Основним недоліком методу NDB є його слабка стійкість до атак як пасивних, так і активних зловмисників, оскільки він дуже чутливий до невеликих змін у контейнері. Для зменшення цієї чутливості зазвичай додатково використовується шумостійке кодування [5,8].

Метод Каттера-Джордана-Боссена («метод перехресного розрізання») пропонує використовувати синій канал зображення, закодованого за допомогою RGB, для приховування інформації [5,8]. Це пояснюється тим, що

стеганографія нульового порядку (ZSL) найменш чутлива до змін яскравості синього кольору порівняно з червоним та зеленим.

Інформація вбудовується наступним чином: і-й біт mi повідомлення вбудовується у псевдовипадковий піксель у контейнері p = (x, y).

Ключ K0 визначає координати пікселя, де буде прихована інформація. Під час вбудовування яскравість червоного та зеленого кольорів залишається незмінною, тоді як яскравість синього змінюється за такою формулою [5,8]:

$$B^*_{x,y} = \begin{cases} B_{x,y} + \upsilon \cdot \lambda_{x,y}, при\ m_i = 0; \\ B_{x,y} - \upsilon \cdot \lambda_{x,y}, при\ m_i = 1. \end{cases}, \quad (1.8)$$

де $\lambda_{x,y} = 0.3 \cdot R_{x,y} + 0.59 \cdot G_{x,y} + 0.11 \cdot B_{x,y}$ – яскравість пікселя;

$\upsilon$ – коефіцієнт, що задає енергію біта даних, що вбудовуються

Оскільки приймач не має оригінального зображення, ми не можемо визначити, як змінилася яскравість синього кольору. Тому, щоб виділити синій, ми прогнозуємо початкове значення яскравості синього кольору на основі сусідніх кольорів [5,8]:

$$\overline{B_{x,y}} = \frac{\sum_{i=1}^{\sigma} (B_{x,y+i} + B_{x,y-i} + B_{x+i,y} + B_{x-i,y})}{4\sigma}, \quad (1.9)$$

де $\sigma = 1 \div 3$ – розмір області, по якій буде прогнозуватися яскравість.

Центральний піксель – це той, яскравість синього кольору якого ми повинні передбачити на основі пікселя, позначеного світло-сірим кольором (рис. 1.9). [5]

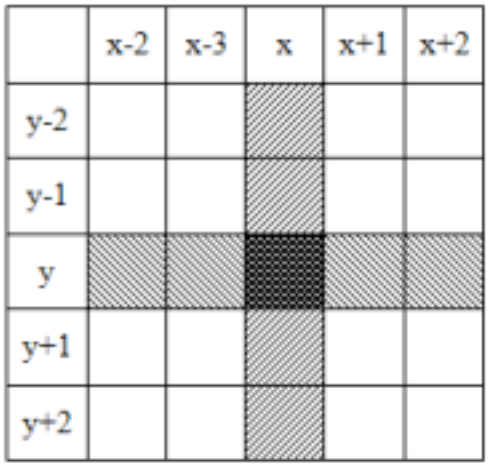



Рис. 1.9. Метод «хреста» при σ = 2

Перевагами цього методу є висока пропускна здатність та стійкість до несанкціонованого зчитування, виявлення частоти, пошкодження низьких біт контейнера та атаки стиснення.

Недоліком є те, що вилучення повідомлень є ймовірнісним [9,10]. Для зменшення ймовірності помилки використовується шумостійке кодування. Крім того, кожен біт може повторюватися кілька разів під час процесу вбудовування (багаторазове вбудовування).

### 1.4.2. Методи приховування в області перетворень

Більш надійний підхід полягає у використанні частотної області, а не просторової, для приховування даних [9,10].

Існує багато способів представлення зображень у частотній області.

У цьому випадку потрібне певне розкладання зображення, що використовується як контейнер. Наприклад, методи, засновані на дискретному косинусному перетворенні (DCT), дискретному перетворенні Фур'є (DFT), вейвлет-перетворенні, перетворенні Карунена-Лоева тощо. Ці перетворення можна застосовувати до окремих частин зображення або до всього зображення [5,8,11,12].

У стеганографії вейвлет-перетворення та DCT є найбільш широко використовуваними з усіх ортогональних перетворень, частково завдяки їх широкому використанню в стисканні зображень [5,12]. Крім того, для приховування даних найкраще використовувати перетворення, які відбуваються на зображенні з часом під час стиснення.

Ефективність використання вейвлет-перетворення та дискретного косинусного перетворення (DCT) для стиснення зображень полягає в їхній здатності добре імітувати обробку зображення в навчанні нульового простору (ZSL), відрізняючи важливі деталі від другорядних. Отже, ці перетворення більше підходять для ситуацій, пов'язаних з активним вторгненням, оскільки зміна критичних коефіцієнтів може призвести до неприйнятного спотворення зображення [11,12].

У цифровій обробці зображень зазвичай використовується двовимірне дискретне косинусне перетворення (ДКП).

Метод відносної заміни коефіцієнтів ДКП (метод Коха та Чжао).

Наразі одним з найпоширеніших методів приховування конфіденційної інформації в частотній області зображення є метод відносної заміни коефіцієнтів ДКП [5,8,10].

На початковому етапі вихідне зображення розділяється на блоки розміром 8x8 пікселів. DCP застосовується до кожного блоку (1.10), генеруючи матрицю коефіцієнтів DCP розміром 8×8, яку зазвичай позначають як Ωb(υ, ν), де b - номер блоку контейнера C, а (υ, ν) - положення коефіцієнта в цьому блоці. Кожен блок використовується для приховування одного біта даних.

Під час побудови секретного каналу користувач повинен попередньо узгодити два конкретні коефіцієнти DCP для приховування даних у кожному блоці. Ці коефіцієнти задаються координатами в масиві коефіцієнтів DCP: (υ1, ν1) та (υ2, ν2). Крім того, зазначені коефіцієнти повинні відповідати косинусоїдальним функціям середньої частоти. Це гарантує, що інформація буде прихована в області сигналу, критично важливою для приховування

нульового сигналу (ZSL), і що інформація не буде спотворена під час низькостиснення JPEG [5,8,11].

Процес приховування починається з випадкового вибору блоку зображення Cb для кодування b-го біта повідомлення.

Вбудовування інформації виконується наступним чином: для передачі біта "0" різниця абсолютних значень вибраних коефіцієнтів DCT повинна перевищувати певний поріг. Для заданого позитивного значення різниця менша відносно заданого негативного значення P при передачі біта "1".

Отже, якщо відносні значення коефіцієнтів DCT не відповідають прихованим бітам, зміна коефіцієнтів DCT спотворить оригінальне зображення. Чим більше значення P, тим стійкіша до стиснення система стеганографії, створена на основі цього методу, але якість зображення також значно знизиться. Після відповідної корекції значень коефіцієнтів, які повинні задовольняти нерівність, виконується обернене DCT [5,12,13].

Для вилучення даних у декодері виконується аналогічний процес вибору коефіцієнтів, а передані біти визначаються за певними правилами.

Метод Бенгама-Мемона-Ео-Янга є оптимізованою версією вищезгаданого методу [36]. Крім того, оптимізаційна робота виконується двома способами: по-перше, замість використання всіх блоків зображення для вбудовування використовуються лише найбільш підходящі блоки зображення; по-друге, у частотній області блоків зображення, що використовуються для вбудовування, замість двох вибираються три коефіцієнти DCT, що значно зменшує візуальне спотворення контейнера [5,8,11]. Наступні блоки зображення вважаються придатними для вбудовування інформації, якщо вони одночасно відповідають наступним двом умовам [5,11]:

– Блок зображення не повинен мати очевидних переходів яскравості.

– Блок зображення не повинен бути надмірно монотонним.

Блоки зображення, які не відповідають першій умові, характеризуються дуже великими низькочастотними коефіцієнтами DCP, з амплітудами, порівнянними з коефіцієнтами DC. Блоки зображення, які не відповідають

другій умові, характеризуються тим, що більшість високочастотних коефіцієнтів дорівнюють нулю. Ці характеристики є критеріями для відхилення непридатних блоків зображення.

Зазначені вимоги до відхилення розглядаються з використанням двох порогових коефіцієнтів: PL (для першої вимоги) та PH (для другої вимоги). Перевищення PL або недосягнення PH вказує на те, що блок непридатний для модифікації в частотній області.

Процес вбудовування бітів повідомлення в блоки виглядає наступним чином: з блоків у координатах середньочастотної області (υ1, ν1) та (υ2, ν2) вибираються три коефіцієнти DCP (для покращення стабільності стеганографічної системи використовується псевдовипадковий метод). Якщо потрібно вбудувати "0", ці коефіцієнти змінюються так, щоб третій коефіцієнт був меншим за будь-який з перших двох коефіцієнтів; якщо потрібно приховати "1", його роблять більшим відносно першого та другого коефіцієнтів [5,13].

Подібно до попередніх методів, щоб визначити, чи достатні задані коефіцієнти DCT для диференціації, значення порогу диференціації P підставляється в правила щодо переданих бітів.

Якщо така модифікація призводить до значного погіршення якості зображення, коефіцієнти залишаються незмінними, і блок не використовується як контейнер [8,11].

Використання трьох коефіцієнтів замість двох є критично важливим; що ще важливіше, якщо спотворення зображення неприйнятне, блок зображення відхиляється для модифікації. Зменшення помилок, внесених повідомленням. Отримувач завжди може ідентифікувати невбудовані блоки даних, повторюючи аналогічний аналіз, як і відправник [8,11].

Метод, заснований на дискретному вейвлет-перетворенні (DWT).

Вейвлет-перетворення – це метод локалізованого аналізу часового інтервалу, який використовує фіксований розмір вікна та форму перетворення для ефективного визначення деталей низькочастотного сигналу (фундаментальних гармонік) у частотній області та деталей високочастотного

сигналу у часовій області [5,8,12]. Основна ідея DWT в обробці зображень полягає в розкладанні зображення на частини зображення в різних просторових та частотних областях.

Після обробки DWT інформація аналізується в чотирьох частотних областях, одна з яких є низькочастотною областю (LL), а три – високочастотними областями (LH, HL, HH).

Як правило, високочастотні компоненти використовуються для приховування водяних знаків, оскільки людське око менш чутливе до змін у цих областях [12]. Однак область LL є відносно стабільнішою, оскільки вона містить більшу частину енергії зображення. Для отримання кращих показників стабільності в цю частину зображення вбудовані водяні знаки [8,11].

У дворівневому розкладі DVP спочатку виконується у вертикальному напрямку, а потім у горизонтальному для кожного рівня. Після розкладу першого рівня формуються чотири піддіапазони: LL1, LH1, HL1 та HH1.

Для кожного наступного рівня розкладу піддіапазон LL використовується як вихідне зображення. Тому для розкладу другого рівня DVP застосовується до діапазону LL1, перетворюючи його на чотири піддіапазони: LL2, LH2, HL2 та HH2.

Для розкладу третього рівня DVP застосовується до діапазону LL2, розкладаючи його на чотири піддіапазони: LL3, LH3, HL3 та HH3. Це призводить до розкладу одного компонента на 10 піддіапазонів. LH1, HL1 та HH1 містять компоненти з найвищими частотами на зображенні, тоді як LL3 містить компоненти з найнижчими частотами [8,11].

На рисунку 1.10 показано трирівневе розкладання DVP [5,13].

У дискретному вейвлет-аналізі використовуються різні бази вейвлетів, зокрема вейвлети Хаара, вейвлети Даубеха, вейвлети симлетів, вейвлети кофлетів та ортогональні вейвлети.

Відмінності між цими базами вейвлетів полягають у значеннях коефіцієнтів вейвлетів та способі формування спектра.

У реалізації цього методу використовуються вейвлети Даубеха. Альфа-

змішування використовується як метод вбудовування для CVD. Тобто, компоненти вейвлет-розкладання вихідного зображення та CVD множаться на коефіцієнт масштабування, а потім підсумовуються [5,8,12].

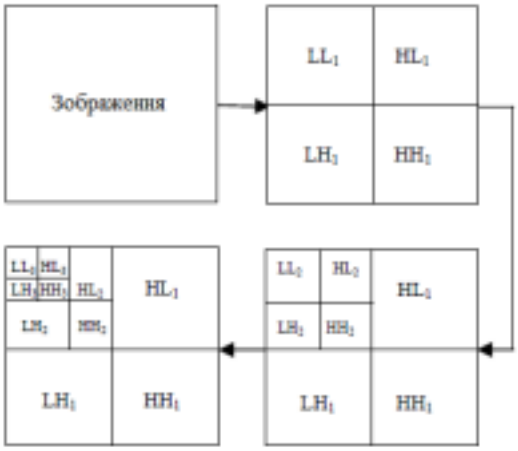



Рис. 1.10. 3-рівневе дискретне вейвлет розкладання

Після вбудовування DCS у зображення-контейнер, коефіцієнти отриманого зображення піддаються зворотному трирівневому перетворенню DVP для отримання кінцевого захищеного зображення DCS.

Методи розширеного спектру. У цьому дослідженні обрано два методи вбудовування водяних знаків шляхом модуляції коефіцієнтів DCS [5,12], оскільки вони мають найвищі показники стабільності серед методів розширеного спектру.

Перший метод, запропонований доктором Руні [5,14,15], базується на модуляції середньочастотної смуги кожного блоку зображення за допомогою випадкового гауссового сигналу.

Другий метод, запропонований Півою та ін. [5,15], також модулює коефіцієнти DCS, але використовує інший низькочастотний діапазон. Стабільність водяного знака додатково коригується за допомогою перцептивної маски.

Метод 1: Спочатку зображення розділяється на блоки 128×128. DCT-перетворення виконується на кожному блоці для отримання коефіцієнтів у пилкоподібному шаблоні, подібному до стиснення JPEG. Середні 30% коефіцієнтів, Dk, модулюються за допомогою гауссового сигналу Sk з нульовим середнім значенням; просте додавання двох сигналів дає результат.

Позначений блок DFT отримується шляхом виконання оберненого DCT з використанням модифікованих коефіцієнтів D'k. Вибирається певний діапазон частот для досягнення балансу між невидимістю та стійкістю DFT [8,11].

Піва та ін. [5,8,14,15] запропонували та дослідили Метод 2 у кількох статтях. Зовсім недавно DFT було розширено. Зображення трансформується за допомогою DCT, де коефіцієнти отримуються у зигзагоподібному візерунку. Перші M коефіцієнтів пропускаються (щоб уникнути видимих артефактів), а наступні L коефіцієнтів модифікуються за допомогою заздалегідь визначених правил.

Значення M та L залежать від розміру зображення та можуть бути скориговані для досягнення балансу між стійкістю та стійкістю DFT. Аналогічно, модифіковане зображення Im отримується шляхом обчислення оберненого DCT з використанням замінених коефіцієнтів DCT D'k. Далі зображення в CVD Iw обчислюється як опукла комбінація (попіксельне додавання) модифікованого зображення Im та вихідного зображення I [5,12,13].

## 1.5. Висновки по розділу

1. Рзглядається сфера застосування методів приховування інформації про зображення. Визначено основні терміни та поняття, пов'язані з процесами та методами приховування інформації про зображення, а також описано їх реалізацію.

2. Пропонується загальна структурна схема систем передачі інформації про зображення та на її основі створюється математична модель. Розкривається сутність обробки інформації, необхідної для досягнення прихованої передачі зображення.

3. Підсумовано критерії оцінки систем стеганографії та наведено кількісні та якісні показники.

4. Демонструються критерії вибору для приховано вбудованих зображень, окреслюються типи, моделі та формати цифрових зображень, що використовуються для прихованої передачі інформації, а також зазначаються їхні переваги та недоліки.

5. Розглядаються методи стеганографії, включаючи: заміщення найменш значущих бітів (LSB), метод Каттера-Джордана-Боссена, вдосконалений метод Коха-Чжао, метод Бенгама, методи, засновані на цифровій векторній проекції (DVP), та методи, засновані на спектральному розкиді. Будуть розкриті їх сутність, переваги та недоліки.

# РОЗДІЛ 2
# АНАЛІЗ МЕТОДІВ ПРИХОВУВАННЯ ІНФОРМАЦІЇ У ЗОБРАЖЕННЯХ

## 2.1. Вибір критерію для порівняння стеганографічних методів приховування інформації

Розглядається сфера застосування методів приховування інформації про зображення. Визначено основні терміни та поняття, пов'язані з процесами та методами приховування інформації про зображення, а також описано їх реалізацію. Пропонується загальна структурна схема систем передачі інформації про зображення та на її основі створюється математична модель. Розкривається сутність обробки інформації, необхідної для досягнення прихованої передачі зображення. Підсумовано критерії оцінки систем стеганографії та наведено кількісні та якісні показники [4,7,8,11].

Демонструються критерії вибору для приховано вбудованих зображень, окреслюються типи, моделі та формати цифрових зображень, що використовуються для прихованої передачі інформації, а також зазначаються їхні переваги та недоліки. Розглядаються методи стеганографії, включаючи: заміщення найменш значущих бітів (LSB), метод Каттера-Джордана-Боссена, вдосконалений метод Коха-Чжао, метод Бенгама, методи, засновані на цифровій векторній проекції (DVP), та методи, засновані на спектральному розкиді. Будуть розкриті їх сутність, переваги та недоліки [5,9,12,14].

### 2.1.1. Вимоги, що висуваються до стеганографічних методів

Найважливішою вимогою до методів стеганографії, що використовуються для створення систем прихованого зв'язку, є те, що вбудована інформація має бути невиявлюваною. Це означає, що незалежно від застосованих статистичних тестів, зображення з секретним вкладенням та без нього повинні виглядати абсолютно однаково. Розуміння статистичних властивостей джерела зображення-контейнера має вирішальне значення.

Наприклад, якщо стеганографічний контейнер є сканованим зображенням, його кореляція в горизонтальному напрямку буде сильнішою, ніж у вертикальному. Характеристики шуму можуть відрізнятися залежно від сканера, і ці фактори необхідно враховувати, якщо потрібна надійна та безпечна система стеганографії. З іншого боку, якщо зображення захоплено за допомогою цифрової CCD-камери, шум матиме специфічні властивості, спричинені елементами CCD та характеристиками зчитування даних. У будь-якому випадку, алгоритм приховування даних повинен відповідати всім відомим статистичним властивостям джерела зображення, а отримане зображення з секретною інформацією має бути невідрізним від зображення без будь-яких вкладень [8,11].

Ще однією важливою вимогою є пропускна здатність каналу зв'язку. Очевидно, що один біт інформації може бути вбудований у кожен кадр відеопослідовності без урахування шумового середовища. Однак, така система зв'язку призведе до низької ефективності використання пропускної здатності каналу. Тому необхідно вбудовувати якомога більше інформації, не порушуючи існуючі моделі шуму зображення [1,2,8,16]. Остання важлива вимога – це можливість вилучення прихованої інформації без використання оригінального зображення. Іноді це можна вирішити, використовуючи попередньо узгоджену базу даних зображень, де зображення використовуються як контейнери лише один раз. Однак це значно обмежує застосовність таких методів [1,2,8,16].

Вимоги до методів вбудовування цифрового підпису, що використовуються для захисту авторських прав та автентифікації, такі: надійність, безпека, невидимість та незворотність відносно оригінального зображення (для запобігання атакам IBM). Методи цифрового підпису можуть використовувати оригінальне зображення для вилучення цифрової мітки. Це спрощує виявлення зображення контейнера перед декодуванням. Ще однією характеристикою є відносно низька пропускна здатність (1-100 біт) [5,9,12,14].

Вбудовування ідентифікаційних номерів («відбитків пальців») вимагає алгоритму, здатного незворотно застосовувати стабільний, безпечний та

невидимий цифровий підпис до оригінального зображення. У цьому випадку метод цифрового підпису не повинен використовувати оригінальне зображення для вилучення мітки. Оскільки для публічного використання може бути поширена велика кількість документів з різними тегами, ці методи повинні бути стійкими до атак змови. Інші характеристики включають відносно низьку пропускну здатність [1,8].

Щоб зберегти якість контейнерів, що містять вбудовані заголовки або іншу додаткову інформацію, методи стеганографії повинні бути достатньо стійкими до стиснення з втратами та шуму, а водяний знак повинен залишатися невидимим навіть при великих обсягах даних. У цьому випадку оригінальне зображення (кадр) не може бути використане для вилучення повідомлень.

Оскільки прихована інформація корисна для користувача, безпека не є проблемою — користувач не видалятиме вбудовані дані. Потрібне високошвидкісне вилучення повідомлень, враховуючи, що водяний знак має бути відновлений у режимі реального часу. Однак вбудовування CVS може бути більш трудомістким [5,9,12,14].

Для програмного забезпечення, що використовується для захисту цілісності зображень, такого як Adobe Photoshop або PaintShop Pro, забезпечення стабільності, безпеки та невидимості вбудованого CVS є вирішальним. У цих застосуваннях детектор може працювати без оригінального зображення.

Для контролю поведінки копіювання під час запису DVD, стабільні, прозорі та захищені файли CWZ повинні бути вбудовані в кадр. Оригінальний кадр, як правило, непридатний для видалення тегів.

Для використання стеганографії в інтелектуальних браузерах та автоматичного надання інформації про авторські права необхідно забезпечити стабільність, прихованість та безпеку детекторів відкритих тегів, реалізованих у програмному забезпеченні. Наразі невідомо, чи існують безпечні детектори відкритих тегів у програмному забезпеченні [5,9,12,14].

У [1,8,9] дослідники провели детальне дослідження та використали

кольорову шкалу (рис. 2.1) для оцінки вимог до відповідних властивостей у кожній поширеній області застосування стеганографії.

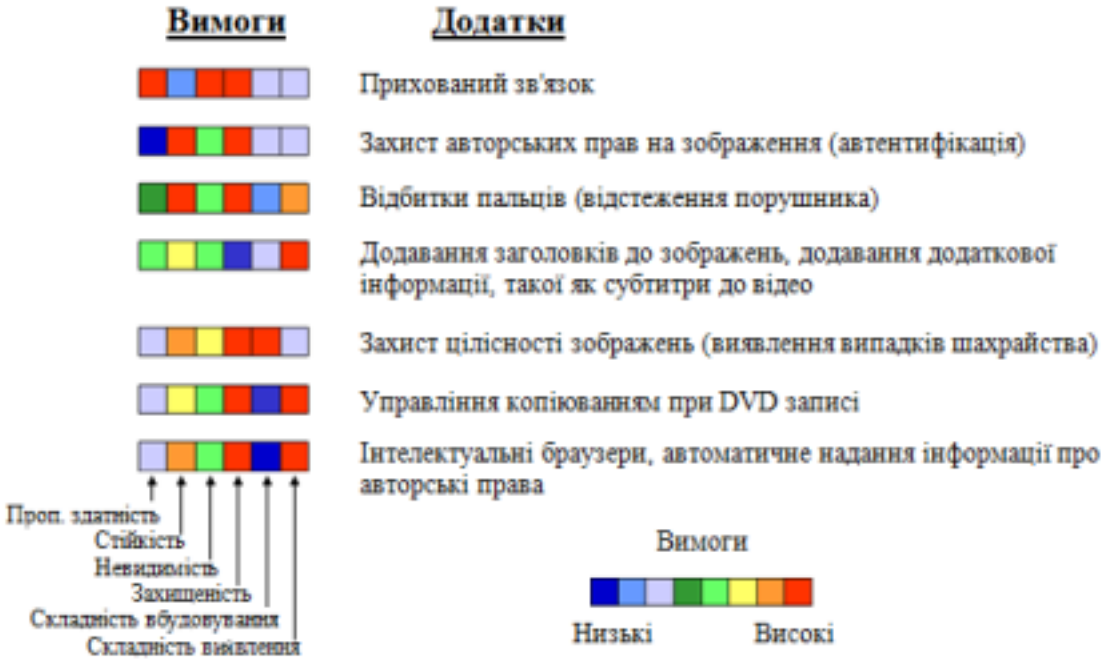



Рис. 2.1. Основні сфери використання та їх вимоги до характеристик

Використовуючи набір функцій, запропонований у розділі 1.3.2, рекомендується використовувати процес аналітичної ієрархії (AHP) для попарного порівняння метрик для кожного застосунку.

### 2.2.2. Розрахунок вагових характеристик

Представлення попарного порівняння [15,16,17] є оберненою симетричною матрицею (Таблиця 2.1), де елементи Wij є представленнями інтенсивності елементів ієрархії і відносно ієрархії j, з оцінками інтенсивності за шкалою інтенсивності від 1 до 9, а оцінки такі [15,16,17]:

1 – рівні значення;

3 – помірна перевага одного над іншим;

5 – істотна перевага одного над іншим;

7 – значна перевага одного над іншим;

9 – дуже сильна перевага одного над іншим;

2, 4, 6, 8 – відповідні проміжні значення.

Згодом було побудовано матрицю пріоритетів (таблиці 2.1 та 2.2), яка включає: пропускну здатність (a), стабільність (b), невидимість (c), безпеку (d), складність вбудовування (e) та складність вилучення (f) [15,16,17].

Таблиця 2.1

Матриця пріоритетів (для додатку прихованого зв'язку)

| *W* | *a* | *b* | *c* | *d* | *e* | *f* |
|---|---|---|---|---|---|---|
| *a* | | 7 | 1 | 1 | 6 | 6 |
| *b* | 1/7 | | 1/7 | 1/7 | 1/2 | 1/2 |
| *c* | 1 | 7 | | 1 | 6 | 6 |
| *d* | 1 | 7 | 1 | | 6 | 6 |
| *e* | 1/6 | 2 | 1/6 | 1/6 | | 1 |
| *f* | 1/6 | 2 | 1/6 | 1/6 | 1 | |

Таблиця 2.2

Матриця пріоритетів (для додатку орієнтованого на захист цілісності зображення)

| *W* | *a* | *b* | *c* | *d* | *e* | *f* |
|---|---|---|---|---|---|---|
| *a* | | 1/5 | 1/4 | 1/6 | 1/6 | 1 |
| *b* | 5 | | 2 | 1/2 | 1/2 | 5 |
| *c* | 4 | 1/2 | | 1/3 | 1/3 | 4 |
| *d* | 6 | 2 | 3 | | 1 | 6 |
| *e* | 6 | 2 | 3 | 1 | | 6 |
| *f* | 1 | 1/5 | 1/4 | 1/6 | 1/6 | |

Під час заповнення матриці пріоритетів дотримуйтесь цього правила: якщо порівняння елемента i та елемента j дає Wij = b, то Wij = 1/b.

Після побудови матриці пріоритетів визначте пріоритет кожного об'єкта в ієрархії, обчислюючи відповідні елементи нормалізованих головних власних векторів матриці V.

Точне визначення головних пріоритетів власних векторів матриці є досить складним. На практиці рекомендується один із наступних методів [15,16,17]:

1. Підсумуйте елементи кожного рядка, потім нормалізуйте суму, поділивши її на суму всіх елементів у матриці. Перший елемент результуючого вектора представлятиме пріоритет першого об'єкта, другий елемент - пріоритет другого об'єкта тощо.

2. Підсумуйте елементи кожного стовпця та знайдіть обернену величину цих сум.

Нормалізуйте кожне обернене значення, поділивши його на обернене значення суми, так щоб сума нормалізованих значень дорівнювала 1.

3. Поділіть елементи кожного стовпця на суму елементів у цьому стовпці (стовпець вже нормалізований), потім підсумуйте елементи кожного рядка та поділіть на кількість елементів у цьому рядку. 4. Обчисліть середнє геометричне кожного рядка та нормалізуйте результат.

5. Зведіть матрицю до як завгодно великого степеня, обчисліть суму елементів у кожному рядку та нормалізуйте результат.

У цій статті використовується метод, який зосереджений на обчисленні середнього геометричного кожного рядка (4). Згідно з цим методом, компоненти вектора пріоритетів обчислюються наступним чином [17,18]:

$$V_i = \frac{\sqrt[N]{\prod_{j=1}^{N} W_{ij}}}{\sum_{k=1}^{N} \sqrt[N]{\prod_{j=1}^{N} W_{kj}}}, \qquad (2.1)$$

де N – розмірність пріоритетів; Wij – елемент пріоритетів, що відображає

результат порівняння елементів і і j.

Усереднюючи результати по всіх застосуваннях (2.2), ми отримуємо ваги (важливості) кожної ознаки методу стеганографії (Таблиця 2.3). [16,17,18]:

$$R_i = \sum_{i=1}^{7} V_i / 7. \tag{2.2}$$

Таблиця 2.3

Загальні ваги характеристик

| Характеристика (*i*) | Вага (*R*) |
|---|---|
| Пропускна здатність | 0,084 |
| Стійкість | 0,203 |
| Невидимість | 0,128 |
| Захищеність | 0,299 |
| Складність вбудовування | 0,070 |
| Складність виявлення | 0,218 |

Отже, результати оцінювання показують, що найважливішими характеристиками методу стеганографії єбезпека (вага R = 0,299), складність виявлення (вага R = 0,218) та стійкість (вага R = 0,203) [16,17].

## 2.3. Порівняльний аналіз та оцінка методів за обраними критеріями

Отримані оцінки були використані для аналізу обраного методу стеганографії вбудовування інформації та вибору оптимального методу на основі кількох критеріїв. На основі інформації, наданої в посиланнях [1,8,15,16,17,18], та з використанням методу призначення коефіцієнтів факторів, була створена Таблиця 2.4, де:

*A1* – метод заміни найменш значущих біт (НЗБ) [6, 8,16,17];

*A2* – метод Куттера-Джордана-Боссена;

*A3* – метод Коха-Жао;

*A4* – метод Бенгама-Мемона-Ео-Юнга;

*A5* – метод із розширенням спектру;

*A6* – метод, заснований на 3-рівневому ДВП.

Таблиця 2.4

Порівняльний аналіз методів вбудовування

| | *a* | *b* | *c* | *d* | *e* | *f* |
|---|---|---|---|---|---|---|
| *A1* | 8 | 1 | 7 | 1 | 8 | 8 |
| *A2* | 6 | 4 | 7 | 4 | 7 | 7 |
| *A3* | 2 | 7 | 5 | 7 | 5 | 5 |
| *A4* | 1 | 6 | 6 | 7 | 4 | 4 |
| *A5* | 4 | 7 | 8 | 6 | 3 | 3 |
| *A6* | 3 | 8 | 8 | 8 | 1 | 1 |

Де: a – пропускна здатність; b – стійкість; c – невидимість; d – захищеність; e – складність вбудовування; f – складність виявлення.

У таблиці 2.9 «8» позначає найкраще значення для цієї ознаки, а «1» – найгірше. Для розуміння значень, описаних у таблиці 2.4, наведено метод розрахунку коефіцієнта пропускної здатності.

Для методу NBR пропускна здатність залежить від розміру зображення (h – висота, w – ширина) та розраховується за таким виразом:

$$C_1 = h \cdot w \cdot 3.$$

Зазвичай, прихована інформація використовує лише один колірний компонент, але також можливо вбудувати інформацію в усі три компоненти одночасно.

У методі Каттера один піксель може вбудувати один біт інформації, тому

пропускна здатність визначається як:

$$C_2 = h \cdot w.$$

Метод Коха-Чжао використовує блок коефіцієнтів DCT 8x8 для вбудовування одного біта інформації; тому пропускна здатність визначається такими факторами:

$$C_3 = (h \cdot w) / (8 \cdot 8)$$

У методі Бенгама блоки даних поділяються на три категорії, і кожну категорію можна вбудовувати лише за допомогою однієї з трьох категорій. Таким чином, у середньому:

$$C_4 = (h \cdot w) / (8 \cdot 8 \cdot 3).$$

Для методів розширеного спектру смуга пропускання визначається формулою Шеннона:

$$C_5 = B \cdot \log_2(1 + SNR),$$

Використання однорівневого методу перетворення DVP може забезпечити вищу пропускну здатність:

$$C_6 = (h \cdot w) / 4.$$

Після розрахунку середнього значення коефіцієнти пропускної здатності були визначені шляхом безпосереднього ранжування різних методів (перший стовпець у таблиці 2.4).

Щодо інших характеристик, стабільність оцінювалася за кількістю загальних операцій обробки зображень, які стеганографічна система, побудована за допомогою певного методу, могла виконати, не втрачаючи здатності виявляти вбудовану інформацію [16]. Стелс оцінювався за допомогою кількісного індексу якості зображення (IF). Безпека оцінювалася на основі

даних, наведених у посиланнях [1,16,17,18,19], з урахуванням стійкості методу до атак. Складність вбудовування та вилучення розраховувалась за кількістю стандартних операцій, необхідних для вбудовування та вилучення прихованої інформації. У цьому випадку контейнер стеганографії був заповнений лише на 10% від максимальної пропускної здатності. Тому комплексний порівняльний аналіз вибраних методів А1–А6 може бути проведений на основі даних таблиці 2.9. Для цього було використано метод попарного порівняння.

На основі детального аналізу кожної ознаки було проведено порівняльний аналіз різних методів, а результати наведено у матричній формі в таблицях 2.5 та 2.6 [16,17].

Таблиця 2.5

Матриця порівняння методів (за пропускною здатністю)

| | *A1* | *A2* | *A3* | *A4* | *A5* | *A6* |
|---|---|---|---|---|---|---|
| *A1* | | 3 | 7 | 8 | 5 | 6 |
| *A2* | 1/3 | | 5 | 6 | 3 | 4 |
| *A3* | 1/7 | 1/5 | | 2 | 1/3 | 1/2 |
| *A4* | 1/8 | 1/6 | 1/2 | | 1/4 | 1/3 |
| *A5* | 1/5 | 1/3 | 3 | 4 | | 2 |
| *A6* | 1/6 | 1/4 | 2 | 3 | 1/2 | |

Таблиця 2.6

Матриця порівняння методів (за захищеністю)

| | *A1* | *A2* | *A3* | *A4* | *A5* | *A6* |
|---|---|---|---|---|---|---|
| *A1* | | 1/4 | 1/7 | 1/7 | 1/6 | 1/8 |
| *A2* | 4 | | 1/4 | 1/4 | 1/3 | 1/5 |
| *A3* | 7 | 4 | | 1 | 2 | 1/2 |
| *A4* | 7 | 4 | 1 | | 2 | 1/2 |
| *A5* | 6 | 3 | 1/2 | 1/2 | | 1/3 |
| *A6* | 8 | 5 | 2 | 2 | 3 | |

Особливості методів A1–A6 оцінюються за формулою (2.1). Параметри для зваженої оцінки якості методу отримують шляхом підсумовування значень усіх параметрів (2.23) та їх нормалізації, як показано в таблиці 2.7 [16,17,18,19].

Таблиця 2.7

Порівняння методів, не враховуючи важливість (вагу) характеристик

| Метод (*a*) | Значення (*WW*) |
|---|---|
| *A1* | 0,266 |
| *A2* | 0,181 |
| *A3* | 0,126 |
| *A4* | 0,097 |
| *A5* | 0,137 |
| *A6* | 0,193 |

Як видно з таблиці 2.7, метод NZB (A1, WW = 0.266) має найвище значення. Однак, враховуючи оцінку важливості ознак, таблицю 2.7 можна модифікувати в таблицю 2.8, де значення параметрів отримані з виразу (2.3) [18,19]:

$$WW1_a = \frac{\sum_{i=1}^{k=6}(V_i \cdot R_i)}{\sum_{a=1}^{A=6}\sum_{i=1}^{k=6} V_{ia} \cdot R_i},$$

(2.3)

Отже, при порівнянні методів вбудовування інформації для стеганографічних застосувань, найкращі результати показав ансамблевий метод, заснований на DTT (A6, WW1 = 0,333) та дискретному косинусному перетворенні (DCT) (A3, WW1 = 0,184) [17,18,19].

Таблиця 2.8

Порівняння методів, враховуючи важливість (вагу) характеристик

| Метод (*a*) | Значення (*WW1*) |
|---|---|
| *A1* | 0,081 |
| *A2* | 0,086 |
| *A3* | 0,184 |
| *A4* | 0,146 |
| *A5* | 0,170 |
| *A6* | 0,333 |

## 2.4 Висновки по розділу

1. Було обрано та перевірено критерії оцінювання та коефіцієнти важливості для методів стеганографії. Запропоновані критерії оцінювання включають пропускну здатність, стабільність, невидимість, безпеку та складність вбудовування та вилучення інформації.

2. Було узагальнено вимоги до методів стеганографії приховування інформації. Зокрема, було визначено невиявлюваність вбудованої інформації, пропускну здатність каналу зв'язку та можливість вилучення прихованої інформації без вихідного зображення.

3. Було розраховано вагові ознаки для вибраних методів приховування інформації, а також побудовано матрицю пріоритетів на основі вимог до методів приховування інформації.

Результати оцінювання показують, що найважливішими ознаками методів стеганографії є безпека (вага R = 0,299), складність виявлення (вага R = 0,218) та стабільність (вага R = 0,203).

# РОЗДІЛ 3
# ОЦІНКА СТІЙКОСТІ МЕТОДІВ ПРИХОВУВАННЯ ІНФОРМАЦІЇ У ЗОБРАЖЕННЯХ ДО ЗОВНІШНІХ ВПЛИВІВ

## 3.1. Стійкість стеганографічних методів до спрямованих атак

Під час передачі через канал зв'язку зображення заповненого контейнера є дуже вразливим до атак або зовнішніх перешкод [1,7,8,21].

Перешкода стосується спотворення або викривлення корисних сигналів або поведінки, що переносить ключову інформацію всередині пристрою зв'язку. Вплив перешкод може призвести до значних помилок у стеганографічній системі [7,8].

Атака - це будь-яка спроба виявити, видалити або змінити приховану стеганографічну інформацію [8,21]. Деякі стеганографічні програми більш вразливі до перешкод каналу зв'язку, такі як стеганографічні системи, що використовуються для прихованого зв'язку, та системи захисту авторських прав на зображення. Інші програми часто піддаються атакам користувачів, особливо під час використання стеганографії для відстеження порушників або виявлення несанкціонованого копіювання та шахрайства.

Здатність стеганографічної системи протистояти атакам та перешкодам називається стабільністю або безпекою, залежно від умов та мети впливу [7,21].

Загальновідомо, що основним завданням стеганографії є приховування існування стеганографічного каналу. Однак, якщо зловмисник вживає зловмисних дій, він може припустити наявність прихованої інформації на зображенні та розпочати різні атаки для пошкодження або видалення вбудованих даних. Одночасно навіть абсолютно нічого не підозрюючі користувачі можуть несвідомо розпочати атаки на CVZ [5,9,12,14].

Найпростішою атакою є суб'єктивна (візуальна) атака, під час якої зловмисник ретельно вивчає зображення, намагаючись «на вигляд» визначити, чи існує прихована інформація. Ця атака ефективна лише проти повністю

незахищених стеганографічних систем. Тим не менш, вона залишається найпоширенішим методом атаки для виявлення початкових стадій стеганографічної системи. Під час оцінки методів вбудовування візуальна невидимість вбудованої інформації характеризується параметром невидимості [6,7,21].

### 3.1.1. Класифікація атак на стеганографічні системи

Атаки на стеганографічні системи можна класифікувати за багатьма критеріями, але загалом їх можна розділити на такі категорії [6,21]:

1. Атаки на вбудовані повідомлення — спрямовані на видалення або знищення стеганалітичного водяного знака (CVM) шляхом маніпулювання стеганалітичним контейнером. Ці атаки включають: стиснення зображення, додавання шуму, зміну контрастності, застосування лінійних та нелінійних фільтрів (розмиття, підвищення різкості, медіанна фільтрація).

2. Атаки на стеганалітичні детектори — спрямовані на ускладнення або неможливість належного функціонування детектора. У цьому випадку водяний знак залишається на зображенні, але його неможливо отримати. Ці атаки включають афінні перетворення (наприклад, масштабування, переміщення, обертання), обрізання зображень, перестановку пікселів, друк/копіювання/сканування, квантування кольорів тощо.

3. Атаки на протоколи вбудовування повідомлень, що в основному включають створення помилкових вбудовувань та CVD, інверсію водяного знака, додавання кількох CVD тощо.

4. Атаки на сам водяний знак, спрямовані на оцінку та вилучення CVD зі стеганографічної системи, в ідеалі без руйнування контейнера. Ці атаки включають атаки змови, статистичне усереднення, методи шумозаглушення сигналу, певні типи нелінійної фільтрації тощо.

### 3.1.2. Дослідження стійкості стеганографічних систем до атак

Для дослідження впливу атак на детектори стеганалізу (рис. 1.6) у цій статті розглядаються геометричні атаки, оскільки це найпоширеніший тип атак, що виконуються на зображеннях звичайними користувачами для особистих цілей. Геометричні атаки математично моделюються як афінні перетворення, невідомі детектору. Вони призводять до втрати синхронізації детектора; водяний знак на зображенні залишається, але ймовірність його правильного виявлення втрачається [6,7,21].

У таблиці 3.1 представлено результати впливу геометричних ефектів на здатність правильно виявляти CVD. Тут LSB відноситься до методу заміщення найменш значущих бітів, KGB - до методу Каттера-Джордана-Боссена, KZh - до методу Кох-Чжао, BMEYU - до методу Бенгама-Мемона-Ео-Юнга, а DVP - до методу на основі вейвлет-перетворення. Максимально допустима варіація виражена у відсотках у таблиці. Ці атаки були реалізовані за допомогою програмних засобів Adobe Photoshop та Microsoft Office Picture Manager [7,21].

Таблиця 3.1

Аналіз стійкості до атак проти стеганографічного детектора

| Вид геометричної атаки | в просторовій обл. | | в частотній обл. | | в обл. перетв. |
|---|---|---|---|---|---|
| | НЗБ | КДБ | КЖ | БМЕЮ | ДВП |
| 1. Масштабування | – | – | – | – | – |
| 2. Зміна пропорцій | – | 17% | 1% | – | – |
| 3. Повороти | – | – | – | – | + |
| 4. Відсічення | – | – | – | – | + |
| 6. Яскравість | – | 17% | 18% | 15% | 20% |
| 7. Контрастність | – | 52% | 55% | 5% | 60% |

Аналізуючи еталонні зображення, ми робимо висновок, що атаки стеганографічного детектора, засновані на масштабуванні зображення,

обертанні та обрізанні, призведуть до його збою. Усі досліджені методи не здатні захиститися від цих атак.

Найімовірнішою атакою проти вбудованих повідомлень є переформатування та стиснення зображень, вбудованих за допомогою CVZ (Таблиця 3.2).

Де представляє ступінь стиснення зображення (виражений у відсотках) під час переформатування зображення у формат JPG [7,21,22].

Таблиця 3.2

Аналіз стійкості до атак проти вбудованого повідомлення

| Переформатув. / стиснення | в простор. обл. | | в частотній обл. | | | | в обл. перет. |
|---|---|---|---|---|---|---|---|
| | НЗБ | КДБ | КЖ | | БМЕЮ | | ДВП |
| Розмір зображення: | 640× 640 | 640× 640 | 2048× 2048 | 640× 640 | 2048× 2048 | 640× 640 | 640× 640 |
| bmp-png | + | + | + | + | + | + | + |
| bmp-tiff | + | + | + | + | + | + | + |
| bmp-jpeg(rgb)/0% | – | – | + | + | + | + | + |
| bmp-jpeg(rgb)/25% | – | – | + | + | + | + | + |
| bmp-jpeg(rgb)/50% | – | – | + | + | + | + | + |
| bmp-jpeg (Ycbcr)/0% | – | – | + | – | + | – | + |
| bmp-jpeg (Ycbcr)/25% | – | – | + | – | – | – | + |
| bmp-jpeg (CMYK)/0% | – | + | + | + | + | + | + |
| bmp-jpeg (CMYK)/25% | – | – | + | + | + | + | + |

Отже, серед методів вбудовування просторових доменів, метод Каттера-Джордана-Боссена демонструє найвищу стійкість до стеганографічних атак та безпеку. Однак, навіть попри це, він все ще значно відстає від методів перетворення доменів при вивченні ефективності атак проти вбудованих повідомлень [7,21].

Дослідження показали, що вейвлет-перетворення є найефективнішим методом приховування даних. Вейвлет-перетворення рекомендується навіть за наявності активних порушників (наприклад, законних власників). Цей метод виявився найбільш стійким до геометричних атак, а також добре показує себе при стисканні зображень. Єдина вимога - правильний вибір діапазону частот вбудовування, який визначає стабільність стиснення зображення [12,20,21].

## 3.2 Аналіз методів підвищення стійкості стеганографічних методів до зовнішніх атак та впливів

### 3.2.1. Аналіз методів підвищення стійкості до атак

Найпоширенішою атакою на стеганографічні системи є геометрична атака. На відміну від атак видалення, геометричні атаки спрямовані на зміну CVD (даних кольорових векторів) шляхом введення просторових або часових спотворень. Геометричні атаки математично моделюються як афінні перетворення, параметри яких невідомі декодеру. Як правило, існує шість типів афінних перетворень: масштабування, зміна співвідношення сторін, обертання, переміщення та відсікання. Ці атаки можуть призвести до втрати синхронізації CVD-детектора, як локально, так і глобально (тобто застосованої до всього сигналу). У цьому випадку зловмисник може відсікати окремі пікселі або лінії, переставляти їх, застосовувати перетворення тощо. Подібні атаки реалізовані в програмах Unsign (локальна атака) та Stirmark (локальна та глобальна атака) [7,21].

Крім того, існують деякі більш «інтелектуальні» атаки, засновані на методах синхронізації CVD. Основна ідея цих атак полягає у визначенні методу

синхронізації та його зруйнуванні шляхом згладжування піків у амплітудному спектрі CVD. Ефективність цих атак залежить від того, чи використовується періодичний шаблон як механізм синхронізації. У цьому випадку для забезпечення синхронізації можна використовувати два методи [7,8,21]:

– Вбудовування піків у спектральну область;

– Періодичне введення CVD-послідовностей.

В обох випадках у спектрі формуються піки, які порушуються розглянутими атаками. Після порушення можна застосовувати інші геометричні атаки: синхронізація більше не присутня [21,23,24].

Розробка систем водяних знаків, стійких до геометричних спотворень та змін значень пікселів, має вирішальне значення. Стійкість водяних знаків до спотворень значень пікселів, спричинених стисненням та фільтрацією сигналу, високо цінується. Однак нещодавні дослідження показали, що навіть незначні геометричні перетворення можуть порушувати водяні знаки [21,24]. Ця проблема є найсерйознішою, коли оригінальне немічене зображення детектора недоступне. Якщо оригінальне зображення доступне на кінці детектора, майже завжди можна порівняти оригінальне зображення та заповнене CVD-зображення та інвертувати геометричні операції. Однак методи стеганографії зазвичай вимагають CVD-детектування без доступу до оригінального зображення. Тому зазвичай неможливо виконати зворотні геометричні перетворення шляхом порівняння оригінального та спотвореного зображень [5,9,12,14].

Одна зі стратегій виявлення CVD після геометричного спотворення полягає у спробі визначити, які перетворення були застосовані, та зворотно перетворити їх перед застосуванням стеганографічного детектора [21,24]. Цього можна досягти шляхом вбудовування шаблону реєстрації разом із CVD [21,23,24] (Рисунок 3.1). Єдина проблема полягає в тому, що цей метод вимагає двох CVD: одного для змін реєстрації та іншого для зберігання корисної інформації. Такий підхід може негативно вплинути на пропускну здатність та прихованість стеганографічної системи. Це потрібно розглядати окремо.

Недоліком цього підходу є те, що якщо алгоритм використовує один і той самий шаблон для всіх зображень контейнерів, це може знизити безпеку системи. Цей факт може бути вигідним для зловмисника, якщо він має кілька позначених тегами зображень [5,9,12,14].

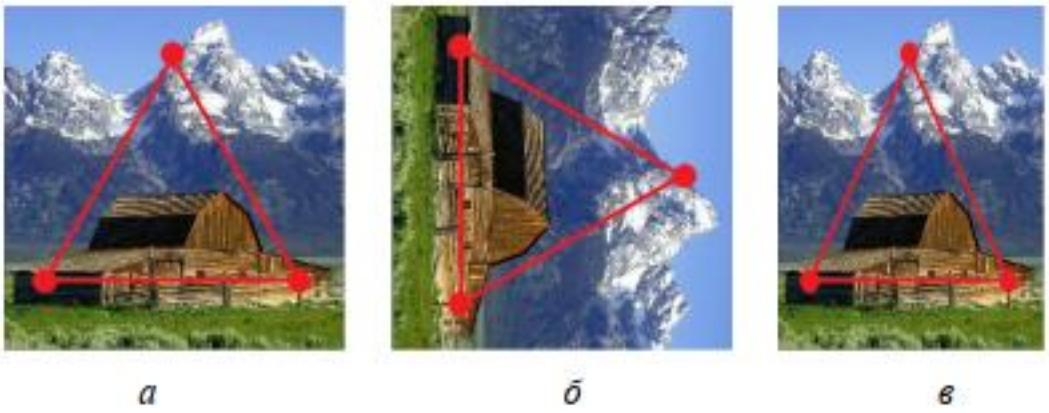



Рис. 3.1. Вбудовування реєстраційного шаблону (а – оригінальне зображення, б – зображення, повернуте на 90°, в – зображення зі зміною пропорцій)

У цьому випадку він може зареєструвати шаблон та видалити його з усіх захищених зображень, тим самим усуваючи можливість виконання зворотних геометричних перетворень [21,24,25].

Інший підхід до реалізації запропонованої стратегії полягає в тому, щоб надати CVD розпізнавану структуру (Рисунок 3.2). Наприклад, пропонується вбудовувати CVD кілька разів у різні просторові області [21,24].

Функція автокореляції заповненого зображення створить піковий шаблон, що відповідає місцю вбудовування. Варіації цього пікового шаблону можна використовувати для визначення будь-яких афінних спотворень, яких зазнає позначене зображення. Цей підхід має великий потенціал, але, як і описані вище методи, він також має деякі недоліки. Успішне вилучення прихованої інформації вимагає успішного вилучення ідентифікатора геометричного спотворення та вилучення самого CVD після зворотного перетворення [21,22]. Обидва вбудовування повинні бути надійними та стійкими до підробки. Крім того, через стиснення JPEG (яке може бути застосоване до зображення після

вбудовування CVS, але до процесу виявлення) можуть з'являтися помилкові піки автокореляції.

Очевидно, що методи, що створюють стеганографічні системи, стійкі до геометричних перетворень та спотворення значень пікселів зображення, що містять приховану інформацію, мають значні переваги в практичному застосуванні [14].

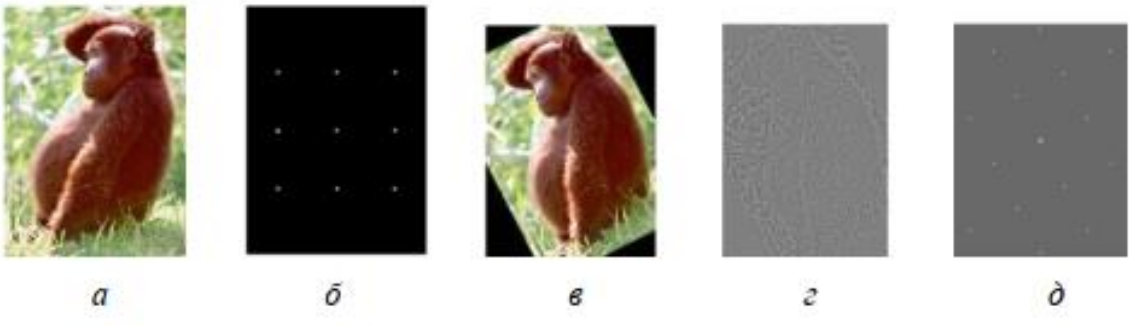



Рис. 3.2. а – оригінальне зображення із ЦВЗ, б – прогнозована автокореляційна функція, в – зображення із ЦВЗ, повернуте на 27° та зменшене до 91%, г – фільтрація зображення в нелінійним фільтром ВЧ, д – автокореляційна функція зображення із ЦВЗ

### 3.2.2. Аналіз методів підвищення пропускної здатності

Для забезпечення вищої стійкості до шуму необхідно збільшити пропускну здатність, оскільки як методи шумостійкого кодування, так і дублювання інформації вимагають передачі додаткових бітів.

Під час нашого дослідження ми визначили два методи збільшення пропускної здатності при використанні методів вбудовування в області перетворення. Перший метод базується на припущенні, що вбудовування коефіцієнтів ДКП середньої частоти забезпечує достатню стабільність зображення, оскільки ці коефіцієнти, як правило, не залежать від алгоритмів стиснення. Крім того, людське око не особливо чутливе до змін цих коефіцієнтів. Тому ми пропонуємо метод, який повністю використовує компоненти середньої частоти зображення (Рисунок 3.3) [21,24].

Другий метод покращення стабільності зображення використовує не лише синю матрицю зображення для вбудовування, як це зазвичай буває в інших методах, але й зелену матрицю зображення. Для цього методу рекомендується використовувати зображення переважно зеленого кольору без великих монотонних областей як контейнер [4,7,8,11].


Рис. 3.3. Використання 2-х діагоналей СЧ ДКП для вбудовування повідомлення

### 3.3. Висновки по розділу

1. Визначено поняття та зміст стійкості методів стеганографії до цілеспрямованих атак, а також класифіковано атаки на стеганографічні системи.

2. Досліджено можливості стеганографічних систем щодо стійкості до атак. Геометричні атаки визначено як основні атаки, та пояснено їхній вплив на різні стеганографічні системи. Визначено метод стеганографії з найвищою стійкістю та безпекою проти стеганографічних атак.

3. Проаналізовано методи підвищення стійкості методів стеганографії до зовнішніх атак та впливів. Дослідження показують, що методи побудови стеганографічних систем, які можуть протистояти геометричним перетворенням та спотворенню значень пікселів зображення, що містять приховану інформацію, мають значні переваги в практичному застосуванні.

# ВИСНОВКИ

Під час кваліфікаційного процесу було виконано такі завдання:

– Розглянуто сферу застосування та процедури методів приховування інформації про зображення.

– Оцінено ефективність методів приховування інформації про зображення.

– Оцінено стійкість методів приховування інформації про зображення до зовнішніх впливів та перешкод.

1. У першій частині кваліфікаційної роботи було розглянуто сферу застосування методів приховування інформації про зображення. Пояснено природу обробки інформації, необхідної для досягнення прихованої передачі зображення. Узагальнено критерії оцінки стеганографічних систем. Запропоновано кількісні та якісні показники для оцінки стеганографічних систем.

Було розглянуто методи стеганоаналізу, включаючи: методи заміщення найменш значущих бітів (LSB), методи Каттера-Жордана-Боссена, вдосконалені методи Коха-Чжао, методи Бенгама (вдосконалення першого), методи на основі DVP та методи на основі спектрального розкиду. Було розкрито їхню природу, переваги та недоліки.

2. У другій частині кваліфікаційної роботи було обрано та продемонстровано коефіцієнти важливості та критерії оцінки стеганографічних методів. Запропоновані критерії оцінювання включали пропускну здатність, стабільність, невидимість, безпеку та складність вбудовування та вилучення інформації. Узагальнено вимоги до методів стеганографії приховування інформації.

Розраховано вагові характеристики вибраних методів приховування інформації, а на основі вимог побудовано матрицю пріоритетів. Результати оцінювання показують, що найважливішими характеристиками методів стеганографії є безпека, складність виявлення та стабільність.

3. У третій частині оціночної роботи визначено концепцію та зміст

стійкості методів стеганографії до цілеспрямованих атак. Запропоновано класифікацію навмисних атак на стеганографічні системи. Досліджено стійкість стеганографічних систем до атак. Геометричні атаки визначено як основний тип атаки та пояснюється їхній вплив на різні стеганографічні системи. У цій статті визначено метод стеганографії з найвищою стійкістю та безпекою до стеганографічних атак та проаналізовано методи підвищення стійкості методів стеганографії до зовнішніх атак та впливів. Дослідження показують, що методи побудови стеганографічних систем, які можуть протистояти геометричним перетворенням та спотворенню значень пікселів зображення, що містять приховану інформацію, мають значні переваги в практичному застосуванні.

# ПЕРЕЛІК ПОСИЛАНЬ

1. Конахович Г.Ф. Комп’ютерна стеганографія. Теорія і практика / Г.Ф. Конахович, А. Ю. Пузиренко. - Київ: МК-Пресс, 2006. – 288с.

2. Кузнецов О. О. Стеганографія: навчальний посібник / О.О.Кузнецов, С. П. Євсеєв, О. Г. Король. - Х.: Вид. ХНЕУ, 2011. - 232с.

3. Рябко Б. Я., Фионов А. Н. Основы современной криптографии и стеганографии. 2-е изд. / Рябко Б. Я., Фионов А. Н. // М.: Горячая линия - Телеком, 2013. 232 с.

4. Кінзерявий О.М. Стеганографічні методи приховування даних увекторні зображення, стійкі до активних атак на основі афінних перетворень / О.М. Кінзерявий // Київ – 2015, 324 с.

5. Вовк О.О. Методи підвищення стійкості та пропускної здатності систем прихованої передачі інформації / Вовк О.О. – Харків, 2016 – 177с.

6. Грибунин В. Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: СОЛОН-Пресс, 2002. – 272 с.

7. Худьо В.Д., Моделювання стійкої стегофонічної системи із заданими характеристиками мережі / В.Д. Худьо // Тернопіль – 2017. – 98с.

8. Юдін О.К., Конахович Г.Ф., Корченко О.Г. Захист інформації в мережах передачі даних: Підручник. К.: Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009, 716 с.

9. Fidrich J. Steganography in Digital Media: Principles, Algorithms, and Applications / J. Fidrich. – Cambridge: Cambride University Press, 2009. – 438 p.

10. 34. Kutter M. A fair benchmark for image watermarking systems / M. Kutter, F. Petitcolas // Proc. of SPIE: Security and Watermarking of Multimedia Contents. − San Jose, France, 1999. – vol. 3657 − P. 226 – 239.

11. Кінзерявий О.М. Стеганографічні методи приховування даних у векторні зображення, стійкі до активних атак на основі афінних перетворень / О.М. Кінзерявий // Київ – 2015, 324 с.

12. Лагун А. Використання вейвлет-перетворення для приховування

інформації в нерухомих зображеннях / А. Лагун, І. Лагун // Захист інформації і безпека інформаційних систем. – Л., 2013. – С. 98 – 99.

13. Горніцька Д.А. Визначення коефіцієнтів важливості для експертного оцінювання у галузі інформаційної безпеки / Д.А. Горніцька, О.Г. Корченко, В.В. Волянська // Захист інформації. – 2012. – №1. – С. 108 – 121.

14. Ó Ruanaidh J. Rotation, scale and translation invariant digital image watermarking / J. Ó Ruanaidh, T. Pun // Proc. of the ICIP'97. – California, 1997. – vol. 1, P. 536–539.

15. Семенко К.О. Визначення коефіцієнтів важливості для експертного оцінювання стеганографічних методів / К.О. Семенко, наук. кер. О.О. Вовк // 20-й Міжнародний молодіжний форум «Радіоелектроніка і молодь у XXI столітті». – Х.: ХНУРЕ, 2016. – т.4. – С. 167 – 168.

16. Вовк О. О. Визначення коефіцієнтів важливості для експертного оцінювання стеганографічних методів / О. О. Вовк // Науковий журнал «Телекомунікаційні та інформаційні технології». – Київ, 2015. – №3. – С. 70 – 80.

17. Вовк О.О. Розроблення методики оцінювання важливості характеристик стеганографічних алгоритмів / О.О. Вовк, А.А. Астраханцев // Вісник національного університету «Львівська політехніка» «Інформаційні системи та мережі». – Львів, 2014. – № 805. – С. 52 – 60.

18. Вовк О.О. Синтез стеганографічного методу передачі даних, ефективного за критеріями надійності та захищеності / О.О. Вовк, А.А. Астраханцев // Електронне наукове фахове видання ХНУРЕ «Проблеми телекомунікацій». – Харків, 2015. – № 1 (16). – С. 103 – 115.

19. Vovk O. Synthesis of optimal steganographic method meeting given criteria / O. Vovk, A. Astrahantsev // Informatyka Automatyka Pomiary w Gospodarce i Ochronie Środowiska (technical and scientific journal). – Lublin, Poland, 2015. – P. 27-34

20. Сейеди С.А. Сравнение методов стеганографии в изображениях / С.А. Сейеди, Р.Х. Садыхов // Информатика. – БГУИР, 2013. – С. 66 – 75.

21. Вовк О.О. Анализ атак на цифровые водяные знаки в видеофайлах и изображениях / О.О. Вовк наук. кер. А.А. Астраханцев // V Міжнародна науково-практична конференція «Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій». – Запоріжжя, ЗНТУ, 2010. – С. 88 – 90.

22. Тігулев М. Стеганография в GIF [Электронный ресурс]. – Режим доступа: http://habrahabr.ru/post/128327.

23. Основи комп'ютерної графіки: навч. посіб. / В.С. Березовський, В.О. Потієнко, І.О. Завадський; за заг. ред. А.М. Гуржія. − К.: BHV, 2009. − 400 с.

24. Грачева Ю.А. Несколько слов о стеганографии – методе защиты графической информации от нарушения авторских прав / Ю.А. Грачева // Московский государственный университет печати. – С. 76 – 81.

25. Adnan M. Watermark re-synchronization using log-polar mapping of image autocorrelation / M. Adnan, J. Meyer // Digimarc Corporation. – P. 1 – 4.

# ДОДАТОК А

## Оформлення слайдів та роздаткового матеріалу

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ**

Кваліфікаційна робота здобувача освітнього ступеня «МАГІСТР»

# СИСТЕМИ КІБЕРЗАХИСТУ ПЕРЕДАЧІ КОНФІДЕНЦІЙНИХ ДАНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИМИ КАНАЛАМИ НА ОСНОВІ СТЕГАНОГРАФІЧНИХ ТЕХНОЛОГІЙ

Спеціальність: 125 - Кібербезпека та захист інформації

Виконав: Дмитро ЖУКОВСЬКИЙ

Керівник: д.т.н., проф. Олександр ТУРОВСЬКИЙ

**Київ - 2026**

## АКТУАЛЬНІСТЬ, МЕТА ТА ЗАВДАННЯ ДОСЛІДЖЕННЯ



- Актуальність теми обумовлена потребою прихованої та захищеної передачі конфіденційних даних у цифрових інформаційно-комунікаційних каналах.
- Мета роботи - оцінка ефективності застосування стеганографічних методів приховування інформації у зображеннях.
- Об’єкт дослідження - процес приховування інформації у зображеннях.
- Предмет дослідження - методи приховування інформації у зображеннях.
- Завдання: проаналізувати сфери застосування стеганографії, сформувати критерії оцінки, порівняти методи приховування та оцінити їх стійкість до зовнішніх впливів.

## ЗДОБУТІ РЕЗУЛЬТАТИ КВАЛІФІКАЦІЙНОЇ РОБОТИ



- У першому розділі розглянуто основи застосування методів приховування інформації у зображеннях та структурну модель стеганографічної системи.
- У другому розділі сформовано критерії оцінювання та проведено порівняльний аналіз стеганографічних методів.
- У третьому розділі досліджено стійкість методів приховування інформації до атак, спотворень і зовнішніх впливів.
- Практична цінність роботи полягає у виборі ефективних методів прихованої передачі даних з урахуванням пропускної здатності, непомітності та захищеності.

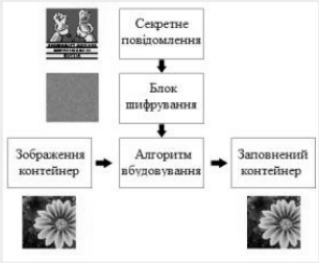
## СФЕРИ ЗАСТОСУВАННЯ СТЕГАНОГРАФІЧНИХ МЕТОДІВ

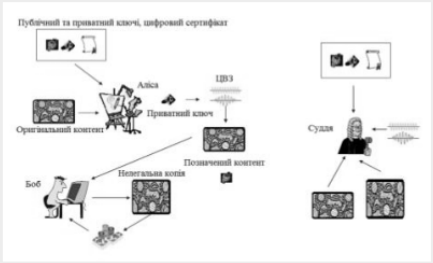


- Стеганографія доповнює криптографію: вона приховує сам факт передавання або наявності секретного повідомлення.
- Основні напрями застосування: прихований зв’язок, цифрові водяні знаки, автентифікація зображень, контроль копіювання та захист авторських прав.
- Для зображень ключовим є збереження візуальної якості контейнера після вбудовування даних.
- Особливе значення мають методи, що дозволяють виявляти підроблення, відстежувати джерело витоку та підтверджувати авторство цифрового контенту.

## ПРИХОВАНИЙ ЗВ’ЯЗОК ТА ЦИФРОВІ ВОДЯНІ ЗНАКИ



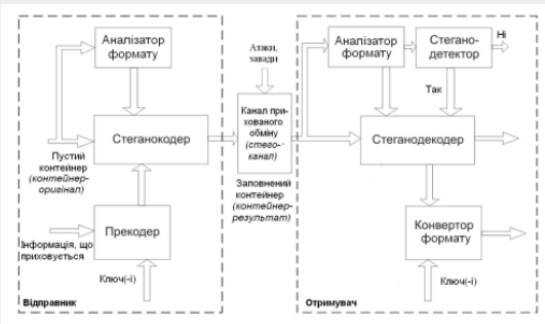



- При прихованому зв’язку секретне повідомлення попередньо обробляється, шифрується та вбудовується у зображення-контейнер.
- Цифровий водяний знак використовується для захисту авторських прав і повинен бути невидимим, стійким та придатним для подальшої перевірки.
- Перевага стеганографічного підходу полягає в тому, що контейнер після вбудовування не викликає підозри у стороннього спостерігача.

## СТРУКТУРНА МОДЕЛЬ СТЕГАНОГРАФІЧНОЇ СИСТЕМИ






- Система містить відправника, стеганокодер, контейнер, стегоканал, одержувача, стеганодетектор і стеганодекодер.
- На стороні відправника повідомлення вбудовується у порожній контейнер, у результаті чого формується заповнений контейнер.
- У каналі можливі атаки та завади, тому модель повинна враховувати не лише непомітність, а й стійкість прихованої інформації.
- На стороні одержувача виконується виявлення та вилучення повідомлення з контейнера.

## МАТЕМАТИЧНА МОДЕЛЬ СТЕГАНОСИСТЕМИ



- Стеганографічна система подається як сукупність контейнерів, повідомлень, стеганограм і перетворень, що забезпечують приховування та вилучення інформації.
- Функція E описує процес вбудовування повідомлення у контейнер, а функція D - процес вилучення повідомлення зі стеганограми.
- Надійність системи пов’язана з подібністю вихідного і заповненого контейнерів: після приховування візуальні відмінності мають бути мінімальними.
- Для підвищення захищеності можуть застосовуватися ключі, псевдовипадкові послідовності та попереднє криптографічне перетворення повідомлення.

## КРИТЕРІЇ ОЦІНКИ ЯКОСТІ СТЕГОСИСТЕМИ



$$SNR = \frac{\sum_{x=1}^{rows(C)} \sum_{y=1}^{cols(C)} (C_{x,y})^2}{\sum_{x=1}^{rows(C)} \sum_{y=1}^{cols(C)} (C_{x,y} - S_{x,y})^2},$$

$$NAD = \frac{\sum_{x=1}^{rows(C)} \sum_{y=1}^{cols(C)} \left| C_{x,y} - S_{x,y} \right|}{\sum_{x=1}^{rows(C)} \sum_{y=1}^{cols(C)} \left| C_{x,y} \right|}.$$

- Якість заповненого контейнера оцінюється кількісними показниками спотворення зображення.
- До ключових показників належать SNR, MSE, NAD, AD та інші метрики, які відображають відмінність між оригінальним і модифікованим зображенням.
- Для ефективного методу важливо забезпечити баланс між пропускною здатністю, непомітністю приховування та стійкістю до обробки зображення.

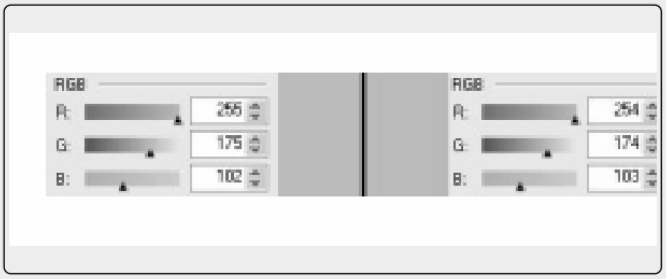
## ВИМОГИ ДО СТЕГАНОГРАФІЧНИХ МЕТОДІВ

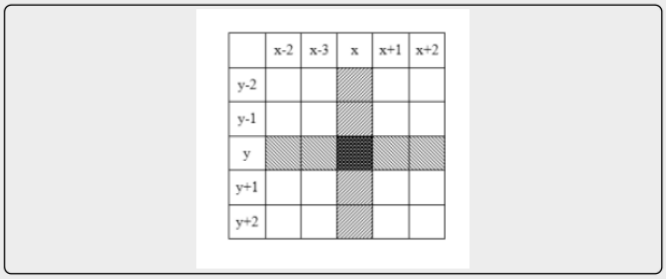


- До основних вимог належать непомітність, пропускна здатність, стійкість до збурень та захищеність від виявлення.
- Ці вимоги часто суперечать одна одній: збільшення обсягу прихованих даних може знижувати непомітність і стійкість.
- Оптимальний метод обирається залежно від прикладної задачі: прихований зв’язок, водяні знаки, контроль авторських прав або автентифікація.
- У роботі застосовано багатокритеріальний підхід до порівняння методів.


## МЕТОДИ ПРИХОВУВАННЯ У ПРОСТОРОВІЙ ОБЛАСТІ



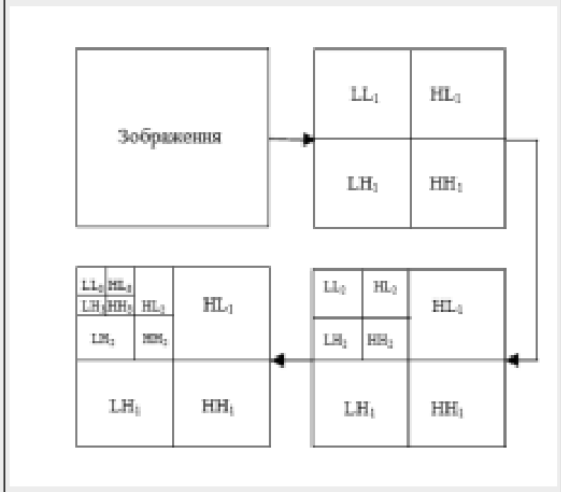



- Метод заміни найменш значущого біта (НЗБ/LSB) є простим і забезпечує високу пропускну здатність.
- Недоліком LSB є відносно низька стійкість до стискання, фільтрації, геометричних атак та статистичного стеганалізу.
- Методи псевдовипадкового вибору позицій і метод «хреста» підвищують складність несанкціонованого виявлення та вилучення повідомлення.

## МЕТОДИ ПРИХОВУВАННЯ В ОБЛАСТІ ПЕРЕТВОРЕНЬ

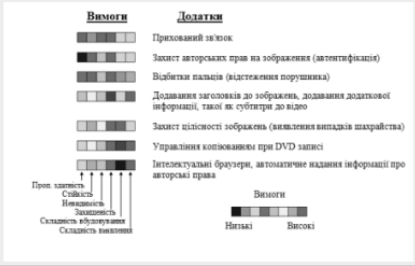





- Методи області перетворень використовують ДКП, ДПФ, ДВП та інші перетворення для розміщення даних у спектральних коефіцієнтах.
- Вбудовування у значущі коефіцієнти дозволяє підвищити стійкість прихованої інформації до стискання та обробки зображення.
- Методи на основі дискретного вейвлет-перетворення краще враховують багаторівневу структуру зображення.
- Порівняно з просторовими методами, такі підходи складніші, але забезпечують кращу стійкість.

## ВИБІР КРИТЕРІЇВ ТА РОЗРАХУНОК ВАГОВИХ ХАРАКТЕРИСТИК






| Характеристика ($i$) | Вага ($R$) |
|---|---|
| Пропускна здатність | 0,084 |
| Стійкість | 0,203 |
| Невидимість | 0,128 |
| Захищеність | 0,299 |
| Складність вбудовування | 0,070 |
| Складність виявлення | 0,218 |

- Для оцінювання методів використано систему критеріїв, що охоплює пропускну здатність, стійкість, непомітність, захищеність і складність вбудовування.
- Вагові характеристики визначають відносну важливість кожного критерію для конкретної області застосування.
- Застосування ваг дає змогу перейти від окремих показників до узагальненої інтегральної оцінки методу.

## ПОРІВНЯЛЬНИЙ АНАЛІЗ СТЕГАНОГРАФІЧНИХ МЕТОДІВ



| | *A1* | *A2* | *A3* | *A4* | *A5* | *A6* |
|---|---|---|---|---|---|---|
| *A1* | | 1/4 | 1/7 | 1/7 | 1/6 | 1/8 |
| *A2* | 4 | | 1/4 | 1/4 | 1/3 | 1/5 |
| *A3* | 7 | 4 | | 1 | 2 | 1/2 |
| *A4* | 7 | 4 | 1 | | 2 | 1/2 |
| *A5* | 6 | 3 | 1/2 | 1/2 | | 1/3 |
| *A6* | 8 | 5 | 2 | 2 | 3 | |

| Метод (*a*) | Значення (*WW1*) |
|---|---|
| *A1* | 0,081 |
| *A2* | 0,086 |
| *A3* | 0,184 |
| *A4* | 0,146 |
| *A5* | 0,170 |
| *A6* | 0,333 |

- У роботі порівнюються методи A1-A6: LSB, метод прямого розширення спектра, Коха-Жао, Бенгама-Мемона-Ео-Юнга, метод із розширенням спектру та методи на основі ДВП.
- Порівняльні матриці дозволяють оцінити методи за обраними критеріями та отримати узагальнену перевагу кожного підходу.
- Найкращий вибір залежить від того, що є пріоритетом: пропускна здатність, стійкість до атак або візуальна непомітність.

## СТІЙКІСТЬ СТЕГАНОГРАФІЧНИХ СИСТЕМ ДО АТАК



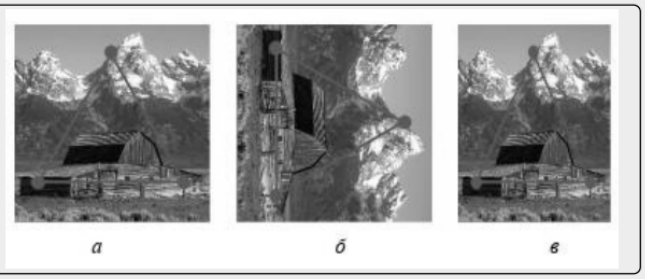
| Вид геометричної атаки | в просторовій обл. | | в частотній обл. | | в обл. перетв. |
|---|---|---|---|---|---|
| | НЗБ | КДБ | КЖ | БМЕЮ | ДВП |
| 1. Масштабування | – | – | – | – | – |
| 2. Зміна пропорцій | – | 17% | 1% | – | – |
| 3. Повороти | – | – | – | – | + |
| 4. Відсічення | – | – | – | – | + |
| 6. Яскравість | – | 17% | 18% | 15% | 20% |
| 7. Контрастність | – | 52% | 55% | 5% | 60% |

| Преформатув. / стиснення | в простор. обл. | | в частотній обл. | | | | в обл. перет. |
|---|---|---|---|---|---|---|---|
| | НЗБ | КДБ | КЖ | | БМЕЮ | | ДВП |
| Розмір зображення | 640× 640 | 640× 640 | 2048× 2048 | 640× 640 | 2048× 2048 | 640× 640 | 640× 640 |
| bmp-png | + | + | + | + | + | + | + |
| bmp-tiff | + | + | + | + | + | + | + |
| bmp-jpeg(gigh)/0% | – | – | + | + | + | + | + |
| bmp-jpeg(gigh)/25% | – | – | + | + | + | + | + |
| bmp-jpeg(gigh)/50% | – | – | + | + | + | + | + |
| bmp-jpeg (Ycbcr)/0% | – | – | + | – | + | – | + |
| bmp-jpeg (Ycbcr)/25% | – | – | + | – | – | – | + |
| bmp-jpeg (CMYK)/0% | – | + | + | + | + | + | + |
| bmp-jpeg (CMYK)/25% | – | – | + | + | + | + | + |

- Спрямовані атаки можуть бути орієнтовані на виявлення факту приховування, руйнування прихованого повідомлення або вилучення стеганографічного ключа.
- Найбільш небезпечними є геометричні перетворення, стискання з втратами, фільтрація, шумові впливи, обрізання та обертання.
- Для підвищення стійкості необхідно поєднувати стеганографічне вбудовування з криптографічним захистом і коригувальними кодами.

## МЕТОДИ ПІДВИЩЕННЯ СТІЙКОСТІ ТА ПРОПУСКНОЇ ЗДАТНОСТІ






| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 1 | 1603 | 203 | 11 | 45 | -30 | -14 | -14 | -7 |
| 2 | 108 | -93 | 10 | 49 | 27 | 6 | 8 | 2 |
| 3 | -42 | -20 | -6 | 16 | 17 | 9 | 3 | 2 |
| 4 | 56 | 69 | 7 | -25 | -10 | -5 | -2 | -2 |
| 5 | -33 | -21 | 17 | 8 | 3 | -4 | -5 | -3 |
| 6 | -16 | -14 | 8 | 2 | -4 | -2 | 1 | 1 |
| 7 | 0 | -5 | -6 | -1 | 2 | 3 | 0 | 1 |
| 8 | 9 | 5 | -6 | -9 | 0 | 3 | 3 | 1 |

- Підвищення стійкості досягається за рахунок вибору областей зображення, менш чутливих до типових операцій обробки.
- Для протидії атакам використовуються псевдовипадкове розміщення, повторне вбудовування, спектральне розширення та адаптивний вибір контейнерних фрагментів.
- Підвищення пропускної здатності повинно виконуватися без критичного зростання видимих спотворень і без суттєвого зниження стійкості.

## ВИСНОВКИ



- У роботі проаналізовано основні сфери застосування стеганографічних методів приховування інформації у зображеннях.
- Подано структурну та математичну модель стеганографічної системи як системи прихованої передачі інформації.
- Сформовано критерії оцінювання та виконано порівняльний аналіз методів приховування інформації у зображеннях.
- Встановлено, що вибір методу має здійснюватися з урахуванням компромісу між непомітністю, пропускною здатністю, захищеністю і стійкістю до зовнішніх впливів.
- Запропонований підхід може бути використаний для вибору стеганографічних технологій у системах кіберзахисту передачі конфіденційних даних.