Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Модель нанесення цифрових водяних знаків на JPEG-зображення

(тема)

Виконав:

студент II курсу, групи СПм-22-4

Скиба О. В.
(прізвище, ініціали)

Спеціальність 123 «Комп’ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма Системне програмування
(повна назва освітньої програми)

Керівник: доц. Мартовицький В.О.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ЕОМ _____ Коваленко А.А.
(підпис) (прізвище, ініціали)

2024 р.

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп’ютерна інженерія»
(код і повна назва)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма Системне програмування
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
“____” _____ 20___ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Скибі Олександру Володимировичу
(прізвище, ім’я, по батькові)

1. Тема роботи Модель нанесення цифрових водяних знаків на JPEG-зображення

затверджена наказом по університету від “ 01 ” квітня 2024 р. № 257 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 15 червня 2024 р.

3. Вхідні дані до роботи Набір зображень

4. Перелік питань, що потрібно опрацювати у роботі

1) Огляд предметної області
2) Огляд методів стеганографії
3) Розробка запропонованого методу
4) Проведення експеременту

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) 16 слайдів

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Аналіз сучасних досліджень в предметній	02.04.24-08.04.24	
	області		
2	Огляд підходів до ЦВЗ	09.04.24-16.04.24	
3	Розробка методу	17.04.24-22.04.24	
4	Проведення експерементів	23.04.24-06.05.24	
5	Оформлення матеріалів кваліфікаційної роботи	07.05.24-23.05.24	
6	Подання кваліфікаційної роботи керівникові та	24.05.24-03.06.24	
	її попередній захист		
7	Подання кваліфікаційної роботи на рецензу-	04.06.24-07.06.24	
	вання		

Дата видачі завдання 01 квітня 2024 р.

Студент _____
(підпис)

Керівник роботи _____ доц. Мартовицький В.О.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 53 с., 15 рис., 3 табл., 1 дод., 21 джерел.

ЗОБРАЖЕННЯ, ЦВЗ, СТЕГАНОГРАФІЯ, АВТЕНТИФІКАЦІЯ, ЦІЛІСНІСТЬ.

Метою кваліфікаційної роботи є розробка, дослідження та вдосконалення моделі нанесення цифрових водяних знаків на JPEG зображення. Основна увага приділяється забезпеченню високого рівня стійкості водяних знаків до різних видів атак, збереженню якості зображення та забезпеченню ефективності та надійності методу.

Завдання роботи:

- аналіз існуючих методів нанесення цифрових водяних знаків;
- вибір та обґрунтування методології;
- розробка моделі нанесення водяного знака;
- експериментальне дослідження;
- аналіз стійкості водяного знака.

ABSTRACT

Master’s thesis: 53 pages, 15 figures, 3 tables, 1 appendices, 21 sources.

IMAGE, DIGITAL WATERMARK, STEGANOGRAPHY, AUTHENTICATION, INTEGRITY.

The aim of the qualification work is to develop, research and improve a model for applying digital watermarks to JPEG images. The main focus is to ensure a high level of watermarking resistance to various types of attacks, preserve image quality, and ensure the efficiency and reliability of the method.

Objectives:

- analysis of existing methods of digital watermarking;
- selection and justification of the methodology;
- development of a watermarking model;
- experimental study;
- analysis of watermark durability.

*** Translated with www.DeepL.com/Translator (free version) ***

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

IWT – інтервальне хвильове перетворення (Interval Wavelet Transform)

PSNR – пік-сигнал-шум-відношення (Peak Signal-to-Noise Ratio)

DRM – управління цифровими правами (Digital Rights Management)

DMCA – закон про авторські права в цифровому столітті (Digital Millennium Copyright Act)

JPEG – група експертів з фотографічних зображень (Joint Photographic Experts Group)

PNG – портативна мережева графіка (Portable Network Graphics)

RSA – алгоритм шифрування з відкритим ключем (Rivest-Shamir-Adleman)

AES – розширений стандарт шифрування (Advanced Encryption Standard)

MD5 – повідомлення про хеш-код 5 (Message Digest Algorithm 5)

SHA – безпека адаптивного хешу (Secure Hash Algorithm)

SVD – перетворення сингулярних значень (Singular Value Decomposition)

GUI – графічний інтерфейс користувача (Graphical User Interface)

OCR – оптичне розпізнавання символів (Optical Character Recognition)

ВСТУП

У нинішню епоху інформаційних технологій і швидкого технологічного прогресу Інтернет відіграє все більшу роль у поширенні мультимедійних ресурсів через цифрові мережі. Це створює загрозу несанкціонованого володіння та використання цифрових матеріалів. Додатковою загрозою є незаконне втручання та модифікація цифрових матеріалів. Недоліком цифрових мультимедійних матеріалів є те, що вони легко піддаються незаконним методам копіювання, таким як піратство, підробка та шахрайство. Таким чином, виникає потреба в методах захисту авторського права на цифрові матеріали. Сучасні виклики та фактори, які необхідно враховувати при пошуку таких методів, полягають у захисті прав власності від незаконних дій таким чином, щоб право власності на цифровий матеріал не підлягало сумніву. Це особливо актуально для візуальних медіа, таких як матеріали у форматах JPEG і MPEG, оскільки це дві найпопулярніші форми візуальних цифрових матеріалів в Інтернеті.

Управління цифровими правами (DRM) спрямоване на захист цифрового контенту протягом усього його життя і в даний час набуває все більшого значення в захисті цифрових матеріалів, доступних в Інтернеті. Це стосується таких цифрових матеріалів, як комп'ютерні програми, музика і зображення в цифровому форматі, а також мультимедійні матеріали. У цих сферах управління цифровими правами включає такі аспекти, як захист авторських прав, перевірка прав власності, контроль за розповсюдженням і використанням, ідентифікація та перевірка законних користувачів, запобігання/виявлення незаконного копіювання тощо. Розробка безпечних систем доставки контенту, які включають управління цифровими правами, наразі викликає значний інтерес в індустрії. Основною технологією DRM, на якій зосереджено увагу в цій роботі, є технологія цифрового водяного маркування.

У багатьох випадках цифрові матеріали стискаються відповідно до стандарту Об'єднаної групи фотографічних експертів (JPEG). Основна проблема, яку вирішуємо, полягає в тому, щоб забезпечити цифрову технологію нанесення водяних знаків для зображень у форматі JPEG, засновану на методах кодування, як доповнення до спектральних методів нанесення водяних знаків, щоб не допустити спотворення зображення після нанесення водяного знаку.

1 ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Огляд цифрових водяних знаків

У час, коли інформаційні мережі розвиваються та змінюються такими швидкими темпами, захист інтелектуальних прав набуває все більшого значення. Це пов'язано з тим, що цифрові дані особливо легко копіювати та перепродавати без втрати якості [1]. Цифрове представлення та розповсюдження даних збільшило потенціал для зловживань та крадіжок, а отже, породило проблеми, пов'язані із захистом авторських прав та забезпеченням дотримання цих прав. У нещодавньому дослідженні загроз безпеці електронної комерції [2] було виявлено, що ще одним основним чинником, який сприяє виникненню вищезгаданої проблеми, є те, що люди не знають або не усвідомлюють обмежень авторського права, які захищають інтелектуальну власність.

Інтелектуальна власність - це право власності на ідеї та контроль над матеріальним або віртуальним представленням цих ідей. Порушення авторських прав так чи інакше завдає шкоди, як правило, грошової, власнику авторських прав. Забезпечення дотримання авторських прав в Інтернеті, наприклад, визначення того, коли цифрове зображення було запозичене, обрізане або незаконно використане на веб-сторінці, є надзвичайно складним завданням. Таким чином, проблема полягає в тому, щоб відображати і робити цифрові продукти доступними в Інтернеті, одночасно захищаючи ці роботи, захищені авторським правом.

Існує два основні технічні підходи до вирішення проблеми захисту інтелектуального авторського права, а саме: контроль використання та цифрові методи нанесення водяних знаків [1]. Найбільш перспективним виявився метод цифрового нанесення водяних знаків.

Основне завдання цифрових водяних знаків - захистити інтелектуальну

власність мультимедійного контенту. Оцифрування нашого світу розширило концепцію водяних знаків, щоб використовувати їх для підтвердження автентичності прав власності та захисту майнових інтересів. Цифрові водяні знаки можна застосовувати до різних цифрових продуктів, таких як зображення, аудіо, відео, текст, графіка і сертифікати. Тут ми зосередимося на застосуванні водяних знаків для захисту зображень у форматі JPEG. Таким чином, далі в цьому документі термін "водяні знаки" згадується в контексті цифрових зображень.

Цифровий водяний знак - це сигнал, який вбудовується в цифровий матеріал для того, щоб можна було встановити право власності, ідентифікувати покупця або надати певну інформацію про авторські права. Як обговорюється в [1], це може утримати людей від незаконного копіювання, дозволяючи визначити законного власника захищеного зображення і відповідні авторські права. Цифрові водяні знаки відіграють важливу роль у наданні доказів порушення авторських прав і, таким чином, дозволяють відстежити неправомірне використання захищених зображень.

Існує дві основні категорії водяних знаків: видимі та невидимі водяні знаки. Видимі водяні знаки призначені для сприйняття користувачем і зазвичай містять візуальне повідомлення або логотип компанії, який чітко вказує на право власності на зображення. Більшість досліджень наразі зосереджені на невидимих водяних знаках, які є непомітними за звичайних умов перегляду. Мета обох категорій водяних знаків - назавжди і безповоротно позначити зображення так, щоб авторство або право власності на нього не викликало сумнівів.

Видимі водяні знаки особливо корисні для передачі негайної заяви про право власності. Основна перевага видимих водяних знаків, принаймні в принципі, полягає в тому, що вони практично усувають комерційну цінність документа для "потенційного" крадія, не зменшуючи при цьому корисність документа для законних і дозволених цілей [3].

Невидимий водяний знак має бути непомітним, але за необхідності

його можна виявити та витягти за допомогою відповідного програмного забезпечення. Зображення, що містить невидимий водяний знак, має бути схожим на оригінальне немарковане зображення. Потрібно, щоб зображення з водяним знаком не зазнавало помітного погіршення якості порівняно з оригіналом. Ці водяні знаки також повинні бути такими, що не викликають заперечень, тобто будь-хто повинен мати можливість перевірити, що вони вбудовані і що вони означають. Цей тип водяних знаків корисний як засіб ідентифікації джерела, автора, творця, власника та уповноваженого споживача документа або зображення. У разі незаконного використання, водяний знак полегшить заяву про право власності, отримання доходів від авторських прав або успіх судового переслідування [3]. Невидимі водяні знаки відіграють роль скоріше у затриманні злодія, ніж у запобіганні крадіжкам.

Водяні знаки можна класифікувати як крихкі, напівкрихкі або стійкі. Крихкі водяні знаки пошкоджуються або спотворюються при будь-якій обробці зображення. Напівкрихкі водяні знаки пошкоджуються, якщо піддаються будь-яким змінам, що перевищують встановлений користувачем поріг. Таким чином, поріг, що дорівнює нулю, утворює крихкий водяний знак. Надійні водяні знаки витримують звичайні операції обробки зображень, такі як зміна масштабу, обрізання, стиснення тощо. Це означає, що водяний знак повинен залишатися цілим і неушкодженим, його можна виявити і відновити, незважаючи на атаки на обробку сигналу.

Конкретні вимоги кожного методу нанесення водяних знаків можуть відрізнятися залежно від застосування, і не існує універсального методу нанесення водяних знаків, який би задовольняв усім вимогам для всіх застосувань. Існує кілька методів вбудовування інформації (сигналу даних або малюнка), яку частіше називають водяним знаком, у цифрове зображення. Деякі з основних категорій методів, що використовуються для вирішення проблеми захисту авторських прав, розглядаються нижче.

Просторові водяні знаки створюються в просторовій області

зображення і вбудовуються безпосередньо в піксельні дані зображення. Спектральні або засновані на перетвореннях водяні знаки вбудовуються в коефіцієнти перетворення зображення (DCT, Wavelet). Сліпі методи нанесення водяних знаків виконують перевірку водяного знаку без використання оригінального зображення. Більшість інших методів потребують оригінального зображення для виявлення водяного знаку. Адаптивні до зображення методи нанесення водяних знаків, як правило, базуються на перетвореннях і є дуже стійкими. Вони були розроблені для стиснення зображень.

1.2 Основні цілі роботи

Ця робота зосереджується на цифровому матеріалі, який було стиснуто відповідно до стандарту JPEG, і важливим аспектом цього стандарту є те, що коефіцієнти стискаються за допомогою ентропійного кодування, такого як кодування Хаффмана або арифметичне кодування. У цих методах ентропійного кодування двійкові кодові слова призначаються відповідно до ймовірності появи окремих коефіцієнтів, що забезпечує стиснення даних. Це стосується деяких методів нанесення водяних знаків, які використовуються для забезпечення захисту авторських прав на цифрові зображення. Гомофонне кодування - це добре відомий метод криптографічного кодування, який використовує імовірнісні властивості джерела повідомлення [4]. Гомофонне кодування забезпечує стиснення даних і водночас вводить зовнішню випадкову інформацію в закодований потік повідомлень як частину властивого процесу кодування. Зовнішня інформація може бути використана для вбудовування власної інформації в потік повідомлень, використовуючи розподіл ймовірностей окремих символів джерела повідомлення.

Часто бажано отримати надійний метод цифрового водяного маркування, який не спотворює цифрове зображення, навіть якщо це означає,

що зображення дещо збільшується в розмірах. Таким чином, основною метою цієї роботи є розробка та реалізація алгоритму, який нанносить водяні знаки на зображення у форматі JPEG. Таким чином, це дослідження спрямоване на створення унікальної та надійної техніки нанесення водяних знаків.

2 МЕТОДИ НАНЕСЕННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ

2.1 Виникнення водяних знаків

Цифрове водяне маркування - це процес вбудовування цифрових даних, які називаються водяними знаками, в мультимедійний об'єкт таким чином, що водяний знак можна виявити або витягти пізніше, щоб зробити твердження про об'єкт [5]. Водяні знаки мають на меті вбудувати унікальний фрагмент даних в оригінальний твір.

Методи цифрового нанесення водяних знаків гарантують, що певна інформація, пов'язана з авторським правом, буде доступна кожному, хто зацікавлений у законному володінні об'єктом інтелектуальної власності. У цій дисертації ми розглядаємо інтелектуальну власність на зображення у форматі JPEG.

2.2 Характеристики цифрових водяних знаків

Водяні знаки призначені для постійного вбудовування в основні дані, в даному випадку в оригінальне зображення. У випадку, коли власник зображення знаходиться під питанням, інформація, витягнута з водяного знаку, повинна підтверджувати власника. Для того, щоб бути ефективним у захисті права власності на об'єкти інтелектуальної власності, водяний знак повинен відповідати певним вимогам. Ці вимоги наведені нижче [6]:

- непомітність. Водяний знак повинен бути невидимим для сприйняття, щоб не впливати на враження від перегляду зображення;

- стійкість. Водяний знак повинен витримувати модифікації зображення, характерні для типових програм обробки зображень, наприклад, масштабування, обрізання та стиснення зображень. Це означає, що водяний знак повинен бути відновлюваним навіть після застосування звичайних

операцій обробки сигналів, таких як геометричні операції з зображеннями та фільтрація шуму;

- невидаляємість. Водяний знак має бути складно видалити неавторизованому користувачеві без погіршення якості оригінального зображення;

- однозначність. Відновлення водяного знаку повинно безпомилково ідентифікувати власника зображення з водяним знаком.

2.3 Класифікація методів нанесення водяних знаків

Як згадувалося раніше, специфічні вимоги кожного методу нанесення водяних знаків можуть відрізнятися залежно від застосування, і не існує універсального методу нанесення водяних знаків, який би повністю задовольняв усім вимогам для всіх застосувань. Загалом, будь-який метод нанесення водяних знаків включає в себе процес вбудовування і процес виявлення. Огляд загального методу нанесення водяних знаків наведено на рисунку 2.1 нижче.

Процес вбудовування зазвичай складається з генерації водяного знаку, що зазвичай включає шифрування водяного знаку та вбудовування водяного знаку, що призводить до отримання зображення з водяним знаком. У процесі вбудовування водяного знаку, враховуючи оригінальне зображення I і водяний знак W, зображення I' з водяним знаком можна математично виразити наступним рівнянням.

$$I' = I + f(I, W) \tag{2.1}$$

Оригінальне зображення I та водяний знак W слугують входами системи, а необов'язковий відкритий або секретний ключ K може бути використаний у схемі нанесення водяного знаку [9].

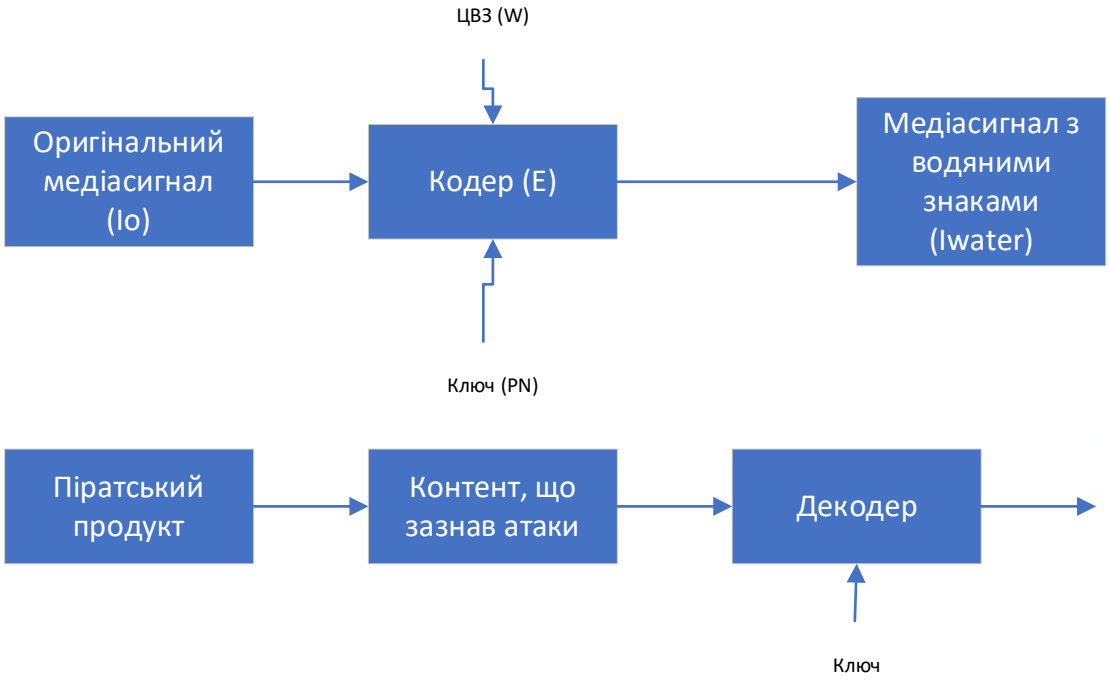

Рисунок 2.1 − Загальна система водяних знаків, включаючи вбудовування та виявлення

Результатом роботи системи є зображення I' з водяним знаком. Процес виявлення водяного знаку встановлює наявність водяного знаку в цифровому контенті.

Існує кілька методів вбудовування водяного знаку в цифрове зображення. Загалом, методи нанесення водяних знаків на зображення поділяються на дві основні категорії, а саме: підхід у просторовій області та підхід у частотній області [3].

Просторовий підхід передбачає використання просторових водяних знаків, які створюються в просторовій області зображення і вбудовуються безпосередньо в піксельні дані зображення. Методи частотної області або розширеного спектра передбачають спектральні або засновані на перетвореннях водяні знаки, які вбудовуються в коефіцієнти перетворення зображення за допомогою дискретного косинусного перетворення (ДКП), дискретного вейвлет-перетворення (DWT), дискретного перетворення Фур'є

(ДПФ) і швидкого перетворення Фур'є (ШПФ). Ці методи працюють за допомогою перетворень для аналізу даних і, таким чином, маніпулюють коефіцієнтами, отриманими в результаті перетворень, з метою вбудовування інформації в зображення [7]. Інші методи області перетворень включають перетворення Мелліна-Фур'є, фрактальне перетворення тощо. Огляд двох основних категорій методів нанесення водяних знаків зображено на рисунку 2.2 нижче.

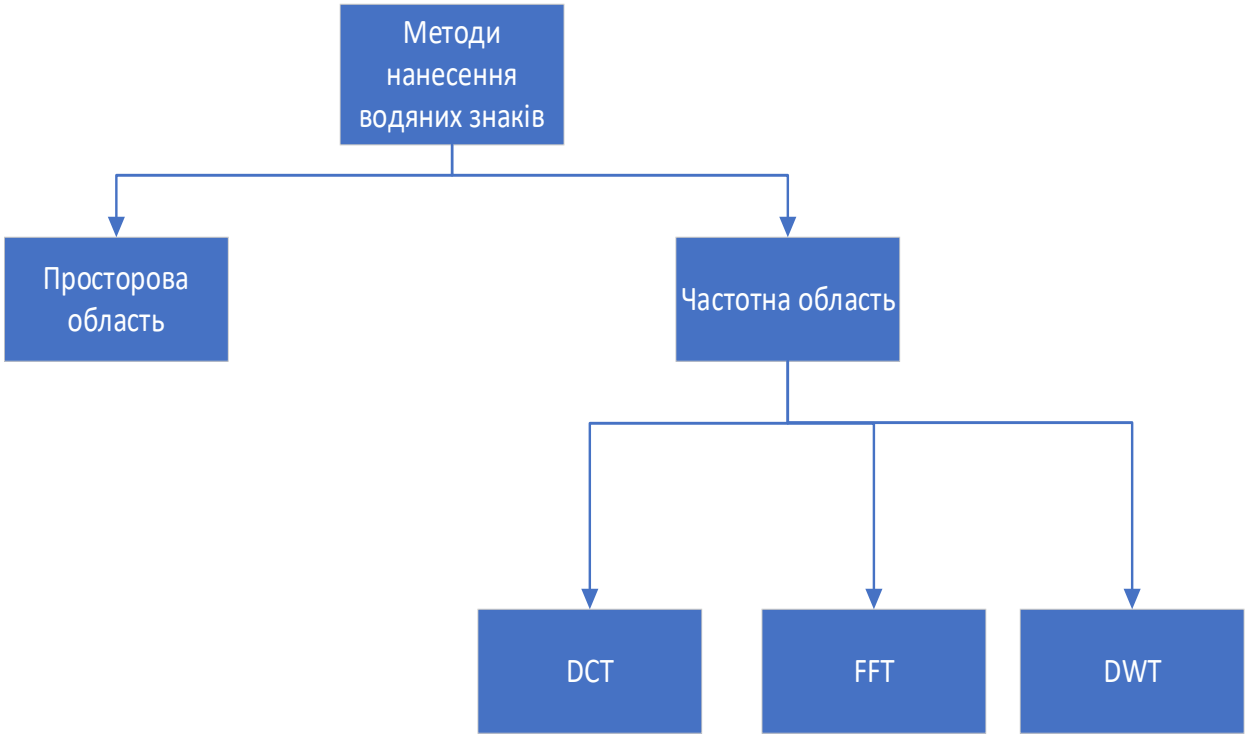

Рисунок 2.2 – Огляд методів нанесення водяних знаків

Інші важливі методи нанесення водяних знаків коротко описані тут. Сліпі методи нанесення водяних знаків виконують перевірку водяного знаку без використання оригінального зображення. Більшість інших методів потребують оригінального зображення для виявлення водяного знаку і, як правило, є більш надійними. Адаптивні до зображення методи нанесення водяних знаків зазвичай базуються на перетвореннях і є дуже стійкими. Адаптивні до зображення методи в основному були розроблені для

стиснення зображень.

Стеганографічні та нестеганографічні методи нанесення водяних знаків, де стеганографічні методи нанесення водяних знаків гарантують, що користувачі не знають про наявність водяного знаку, а в нестеганографічних методах нанесення водяних знаків користувачі знають, що водяний знак існує, і, таким чином, використовуються для запобігання піратству [6]. Існують також асиметричні та симетричні водяні знаки, де асиметричні водяні знаки - це техніка, в якій для вбудовування та виявлення використовуються два різні ключі. Симетричне водяне маркування передбачає використання одного ключа для вбудовування та виявлення водяного знаку.

Методи просторового нанесення водяних знаків розсіюють дані, що вбудовуються, щоб зробити їх малопомітними. Водяні знаки для зображень у просторовій області передбачають модифікацію пікселів для вбудовування інформації. Найпоширенішими методами нанесення просторових водяних знаків є метод найменш значущого біта (LSB) та алгоритм клаптикового шифрування [9].

Метод LSB дозволяє без особливих зусиль вбудовувати дані у фіксовану кількість LSB пікселів зображення. Цей метод базується на маскуванні, і водяний знак вбудовується шляхом вибору 1 та 0, що становлять дані водяного знаку, для LSB. Цей метод спочатку був розроблений для роботи із зображеннями у відтінках сірого, але його легко поширити на кольорові зображення, розглядаючи кожну кольорову площину як єдину площину, в яку вставляються дані в LSB [6]. Таким чином, водяний знак може бути вилучений або декодований, якщо відомі позиції LSB, що використовуються в процесі вбудовування. Основна перевага LSB-методу полягає в тому, що реалізація такого методу недорога в обчислювальному плані.

Клаптиковий алгоритм використовує секретний ключ для ініціалізації генератора псевдовипадкових чисел, який виводить розташування

обкладинки, на якій буде розміщено водяний знак. У процесі вбудовування n-піксельні пари випадковим чином вибираються відповідно до секретного ключа. Значення яскравості (ai, bi) n пар пікселів модифікуються шляхом додавання 1 до всіх значень ai і віднімання 1 від кожного значення bi. Це призводить до збільшення яскравості ai та зменшення яскравості bi. Для виявлення використовується статистичний підхід, де сума

$$S = \sum_{i=1}^{n} a_i - b_i \tag{2.2}$$

обчислюється, а a_i та b_i у наведеному вище рівнянні - це значення після того, як вони були змінені на 1. Якщо зображення містить водяний знак, то очікується, що сума дорівнюватиме 2n, в іншому випадку вона повинна бути приблизно рівною нулю. Це базується на припущенні, що випадково вибрані пари пікселів є незалежними та однаково розподіленими [10].

Слід пам'ятати, що будь-який підхід, який модифікує зображення за допомогою просторових методів, дуже чутливий до шуму і може бути легко зруйнований. Просторові методи також можуть призвести до погіршення якості зображення через вставку водяного знаку. Просторові методи стійкі до обрізання і перекладу, але слабкі до таких атак, як шум і стиснення [9].

Найпоширенішими методами перетворення даних у частотній області є DCT, DWT і DFT. У цих методах водяний знак, що вбудовується, розподіляється по всій області зображення обкладинки, і це досягається шляхом застосування перетворення до оригінального зображення.

Дискретне косинусне перетворення спочатку широко вивчалося спільнотою кодувальників в контексті JPEG і MPEG, а пізніше також розглядалося для вбудовування повідомлень у зображення і відео [10]. Згодом це переросло у використання ДКП для нанесення водяних знаків. Вважається, що ДКП є найпоширенішим методом перетворення в кодуванні зображень [11].

Зображення складається з багатьох пікселів, розташованих у масиві m x n. У схемі нанесення водяних знаків на основі ДКП вихідне зображення спочатку розбивається на блоки пікселів розміром 8x8. Розмір блоків було обрано як компроміс між складністю та якістю. Потім двовимірне ДКП виконується незалежно для кожного блоку, щоб отримати коефіцієнти ДКП для кожного блоку 8x8 пікселів. В результаті отримуємо 64 коефіцієнти ДКП для кожного блоку. Коефіцієнти середньочастотного діапазону вибираються з коефіцієнтів ДКП і модифікуються таким чином, щоб їх відносні значення кодували одиницю або нуль для вбудовування бітів водяного знаку. Коефіцієнти середньої частоти зазвичай вибирають через їхню властивість помірної дисперсії (тобто вони мають подібні величини). Це потрібно для того, щоб зміна коефіцієнтів ДКП не була помітною для сприйняття. Потім зображення з водяним знаком отримують шляхом виконання оберненого ДКП (IDCT) кожного блоку.

Основними перевагами ДКП є його високі властивості енергетичного ущільнення та наявність швидких алгоритмів для обчислення перетворення. Властивість енергетичного ущільнення ДКП призводить до того, що лише кілька коефіцієнтів перетворення мають значні значення [11], що робить його добре придатним для нанесення водяних знаків. Правила вбудовування в області DCT часто є більш стійкими до стиснення JPEG і MPEG, що дозволяє розробнику водяних знаків легше запобігати атакам JPEG/MPEG. Ще однією основною перевагою нанесення водяних знаків у DCT-домені є те, що він надає можливість безпосередньо реалізувати оператор вбудовування в стиснутому домені (тобто всередині JPEG або MPEG-кодера), щоб мінімізувати час обчислень [10].

Дискретне вейвлет-перетворення складається з багатомасштабного частотного розкладання зображення. У випадку DWT для двовимірного зображення, зображення спочатку розкладається на чотири частини високих, середніх і низьких частот (тобто LL_1, HL_1, LH_1, HH_1) шляхом субдискретизації горизонтальних і вертикальних каналів за допомогою

підсмугових фільтрів [12]. Ці підсмуги можуть бути розкладені далі для отримання наступних більш грубих масштабованих вейвлет-коефіцієнтів. На рисунку 2.3 показано концептуальний приклад декомпозиції зображення з трьома масштабними коефіцієнтами.

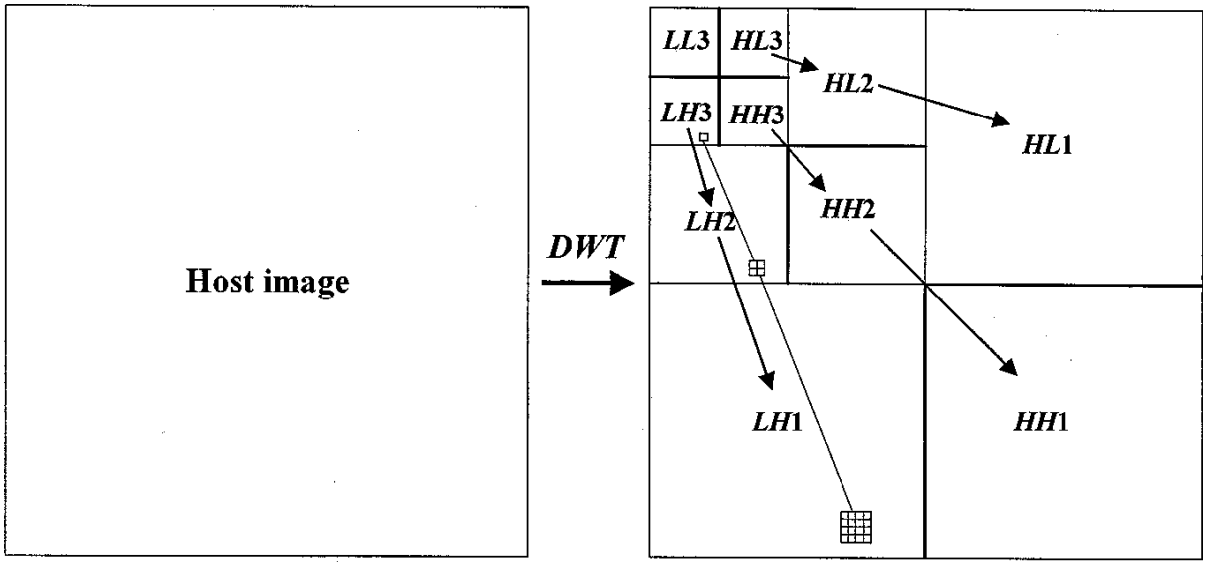

Рисунок 2.3 − Мультимасштабна декомпозиція зображення

Найнижча частотна смуга при найнижчому масштабному коефіцієнті, в даному випадку використовується масштабний коефіцієнт 3, знаходиться в лівому верхньому куті, тобто в блоці LL3. На тому ж рівні роздільної здатності блок HL3 містить інформацію про найвищу горизонтальну та найнижчу вертикальну смуги частот [10]. LH3 містить інформацію про найнижчу горизонтальну та найвищу вертикальну смуги частот, а HH3 містить інформацію про найвищу горизонтальну та найвищу вертикальну смуги частот при найнижчому масштабному коефіцієнті. Той самий процес повторюється для проміжного та найвищого рівнів роздільної здатності. Таке розкладання DWT продемонстровано на рисунку 2.4 на прикладі зображення Lena.

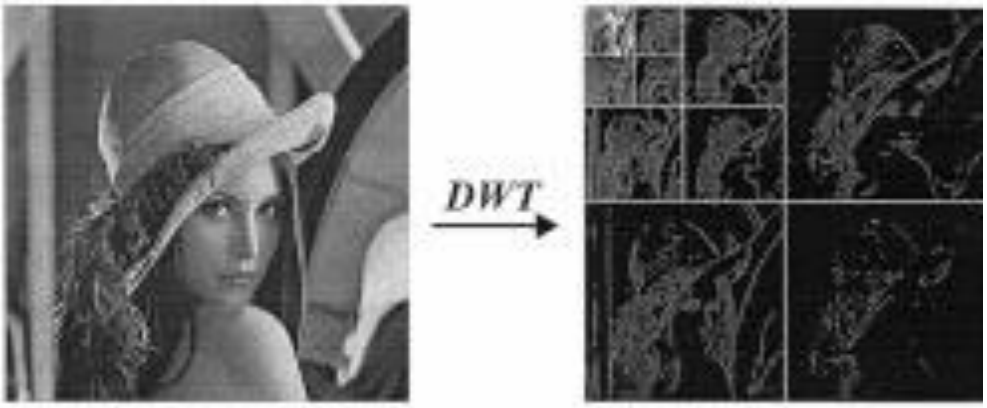

Рисунок 2.4 − Оригінальне зображення Lena розміром 512x512. DWT-розклад зображення Lena

Одним із способів вставки водяного знаку на цьому етапі є використання вейвлет-злиття, коли вейвлет-коефіцієнти водяного знаку та зображення додаються на різних рівнях роздільної здатності. Перед додаванням вейвлет-коефіцієнтів водяного знаку вони модулюються за допомогою обмеження візуальної моделі людини [10]. Після того, як вибрано позиції для заливки і водяний знак вбудовано в різні підсмуги, виконується зворотне дискретне вейвлет-перетворення (IDWT) для отримання зображення з водяним знаком. Цей процес вбудовування зображено на рисунку 2.5.

Нанесення водяних знаків у вейвлет-області забезпечує стійкість до стиснення JPEG, і було розроблено багато схем, які використовують DWT для нанесення водяних знаків.

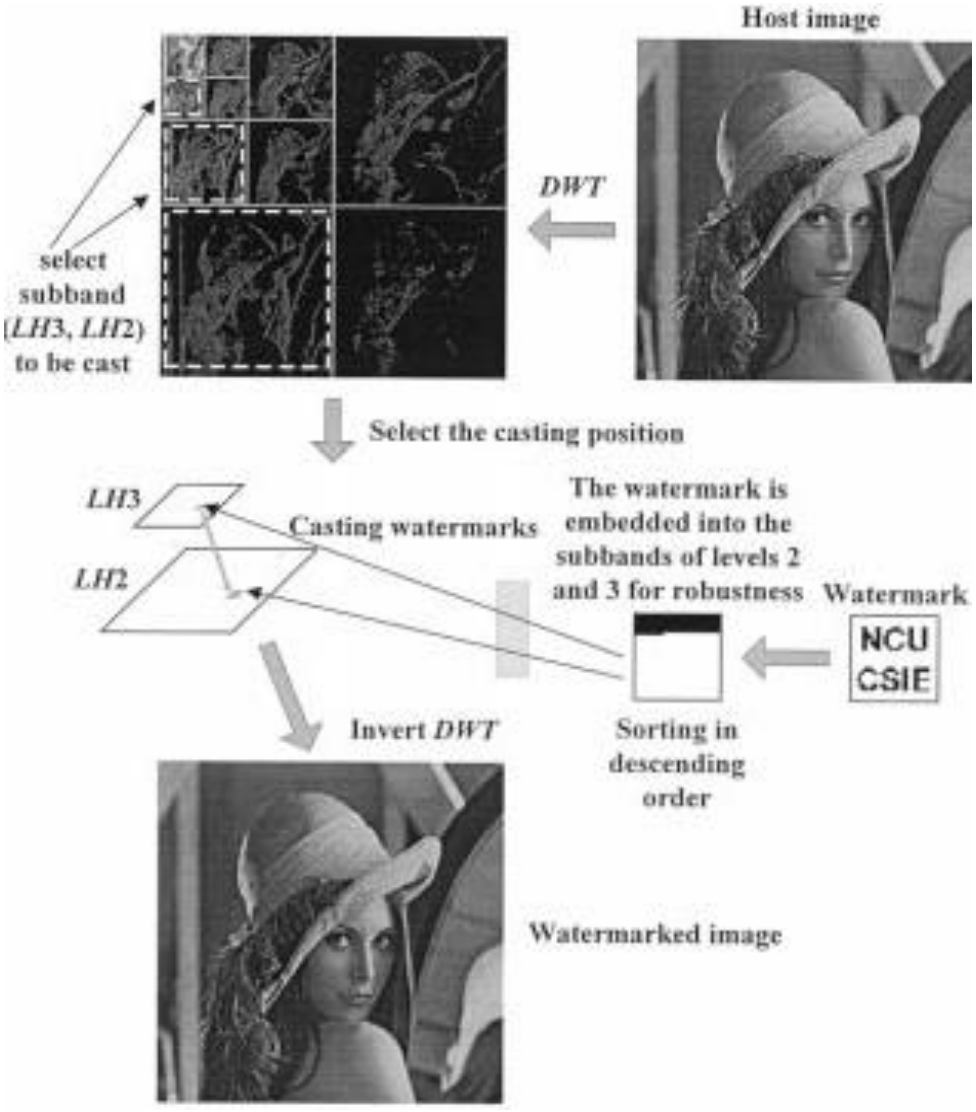

Рисунок 2.5 − Загальний процес вбудовування водяного знаку DWT [12].

Дискретне перетворення Фур'є широко вивчається в галузі обробки сигналів і було розглянуто в галузі нанесення водяних знаків для того, щоб представити можливість контролювати частоти основного сигналу. Часто буває корисно вибрати адекватні частини зображення для вбудовування водяного знаку, щоб отримати найкращий компроміс між видимістю і стійкістю [10].

Двовимірне ДПФ виконується в області дійсних чисел і, таким чином, ДПФ зображення призводить до амплітудного та фазового представлення зображення. Таким чином, було виявлено, що фазова модуляція може бути

використана для надійного нанесення водяних знаків [10]. Фазові компоненти ДПФ мають більший психо-візуальний вплив, ніж амплітудні компоненти. Таким чином, коли водяний знак вбудовується у фазові компоненти з високою надлишковістю, зловмисник може завдати неприйнятної шкоди якості зображення, намагаючись видалити водяний знак. Цей аспект коефіцієнта ДПФ гарантує, що атаки на водяний знак не призведуть до неприйнятної втрати якості зображення.

ДПФ виявляється корисним для нанесення водяних знаків, коли фазова модуляція виконується між водяним знаком і його покриттям, а також ДПФ використовується для розділення зображень на смуги сприйняття.

Як і будь-яка система захисту, водяні знаки піддаються певним атакам. Ці атаки можна розділити на чотири основні класи, а саме: атаки на видалення, геометричні атаки, криптографічні атаки та атаки на протокол. При вивченні різних атак важливо пам'ятати, що вимоги до стійкості кожної системи водяних знаків залежать від конкретного застосування і можуть не відповідати всім можливим атакам.

Атака на видалення, також відома як атака на стійкість, має на меті видалити присутність водяного знаку, не пошкоджуючи зображення, окрім того, щоб зробити його непридатним для використання. Ця атака передбачає видалення інформації про водяний знак з даних з водяним знаком без злому безпеки алгоритму водяного знаку, тобто без ключа, який використовується для вбудовування водяного знаку [13]. Це означає, що жодна обробка, якою б складною вона не була, не зможе відновити інформацію про водяні знаки з даних, що зазнали атаки.

Типові атаки на видалення включають знебарвлення, квантування (для стиснення з втратами), усереднення, фільтрацію, друк і сканування [13]. Хоча всі ці методи спрямовані на повне видалення водяних знаків, це не завжди вдається, але більшість методів завдають значної шкоди інформації про водяні знаки. У більш складних атаках на видалення використовуються статистичні моделі для оригінального зображення і водяного знаку з метою

оптимізації таких операцій, як згладжування або квантування, щоб знищити вбудований водяний знак, зберігаючи при цьому якість зображення.

Як правило, ефект атак на видалення призводить до зменшення ефективної пропускної здатності каналу в процесі видалення вбудованого водяного знаку.

Геометричні атаки, також відомі як атаки презентації, маніпулюють зображенням так, що детектор більше не може знайти водяний знак. Прикладами таких атак є масштабування, обрізання, поворот і тремтіння. На відміну від атак видалення, геометричні атаки фактично не видаляють водяний знак, а спотворюють його так, щоб погіршити виявлення. Таким чином, втрачається синхронізація детектора водяних знаків із вбудованою інформацією [13].

Найвідомішими інструментами для тестування водяних знаків зображень є Stirmark та Unzign. Обидва ці бенчмарки використовують різноманітні геометричні атаки. Unzign вводить локальне тремтіння пікселів і виявився ефективним в атаці на методи просторових доменних водяних знаків. Stirmark вносить глобальні та локальні геометричні спотворення. Більшість сучасних методів водяних знаків витримують ці атаки завдяки використанню спеціальних методів синхронізації. Хоча стійкість до випадкової атаки згинання, яку представляє Stirmark, все ще залишається проблемою для більшості комерційних інструментів водяних знаків [13]. Ця конкретна випадкова атака використовує той аспект, що людська зорова система (HVS) нечутлива до локальних зсувів, таких як пікселі, які зсуваються, масштабуються і обертаються, не вносячи значних візуальних спотворень.

Геометричні атаки іноді також можна назвати атаками з метою вимкнення виявлення або синхронізації, оскільки їхньою основною метою є спроба порушити кореляцію і зробити відновлення водяного знаку неможливим для детектора водяних знаків. Таким чином, в цьому типі атаки водяний знак все ще залишається в атакованих даних, але не може бути

виявлений. Винятком є випадки, коли детектор або декодер водяних знаків має підвищену інтелектуальність або складність.

Криптографічні атаки мають на меті зламати методи захисту в схемах нанесення водяних знаків і таким чином отримати спосіб видалити вбудований водяний знак або вбудувати оманливі водяні знаки. Прикладом криптографічної атаки є пошук ключа для вбудованої секретної інформації методом грубої сили. Іншою такою атакою є атака Oracle, яка може створити сигнал без водяного знаку, коли під рукою є пристрій для виявлення водяних знаків.

Метою криптографічних атак є видалення або знищення вбудованого водяного знаку, але застосування цих атак обмежене через їхню високу обчислювальну складність.

Атаки на протокол спрямовані на атаку всієї концепції застосування водяних знаків шляхом виявлення слабких місць на системному рівні, а потім демонстрації того, що даний метод нанесення водяних знаків не є безпечним.

Одним з видів атак на протокол є атака копіювання, метою якої є не знищення водяного знаку або погіршення його виявлення, а скоріше оцінка водяного знаку з даних з водяним знаком і копіювання його в інші дані, які зазвичай називаються цільовими даними [13]. Оцінений водяний знак адаптується до локальних особливостей цільових даних, щоб забезпечити його непомітність. Атаки копіювання застосовуються, коли дійсний водяний знак у цільових даних може бути створений без знання алгоритму накладання водяного знаку або ключа, який використовується для вбудовування водяного знаку.

Інша атака на протокол відома як інверсійна атака, коли зловмисник віднімає свій власний водяний знак від даних з водяними знаками і заявляє, що він є власником даних з водяними знаками. Це призводить до неоднозначності щодо того, хто є справжнім власником зображення. Для захисту авторських прав часто вимагається, щоб водяні знаки були неінвертованими. Це означає, що не повинно бути можливості витягти

водяний знак з документа без водяного знаку.

Інші атаки, які часто зустрічаються, - це атаки на основі оцінок та атаки на основі інтерпретації. Атаки на основі оцінок ґрунтуються на знанні технології нанесення водяних знаків і використовують статистику оригінального зображення та даних з водяними знаками. Атаки на інтерпретацію - це спроба ввести інший водяний знак у вже марковане водяним знаком зображення, тим самим створюючи тупикову ситуацію з правом власності.

Таким чином, можна побачити, що важливо враховувати атаки під час проектування системи водяних знаків.

2.4 Методи нанесення водяних знаків на зображення jpeg

У цьому розділі наведено короткий опис декількох сучасних методів нанесення водяних знаків, що використовуються для захисту зображень у форматі JPEG. Основна увага приділяється зображенням у форматі JPEG, оскільки метою цієї дисертаційної роботи є розробка алгоритму нанесення водяних знаків для зображень у форматі JPEG.

При нанесенні водяних знаків на зображення JPEG в JPEG (J2J) вхідним файлом є файл зображення JPEG, а зображення з водяним знаком стискається в JPEG таким чином, що вихідний файл також є файлом JPEG. Один з таких методів використовує зорову систему людини (HVS) для оцінки максимальної кількості бітів, які можуть бути вбудовані в JPEG-стиснене зображення. У цьому методі модель HVS Ватсона модифіковано для оцінки ледь помітної різниці (JND) для коефіцієнтів ДКП [14]. Кількість модифікацій, які можна виконати над коефіцієнтами ДКП, обмежується JND, щоб гарантувати невидимість водяного знаку.

Існує декілька схем J2J водяних знаків. Деякі схеми використовують міжблокову кореляцію вибраних коефіцієнтів ДКП для вбудовування бітів водяного знаку [15, 16]. Це досягається додаванням або відніманням зсуву до

середнього значення сусідніх коефіцієнтів ДКП. Інші запропоновані схеми приховують біти водяного знаку шляхом модифікації коефіцієнтів DC [17] і AC [18] в блоковій області ДКП. Існують також методи, які захищають зображення JPEG за допомогою модифікованого дискретного косинусного перетворення (MDCT). Було показано, що ці схеми дозволяють досягти високої якості зображення, а також стійкості до стиснення, фільтрації та геометричних перетворень.

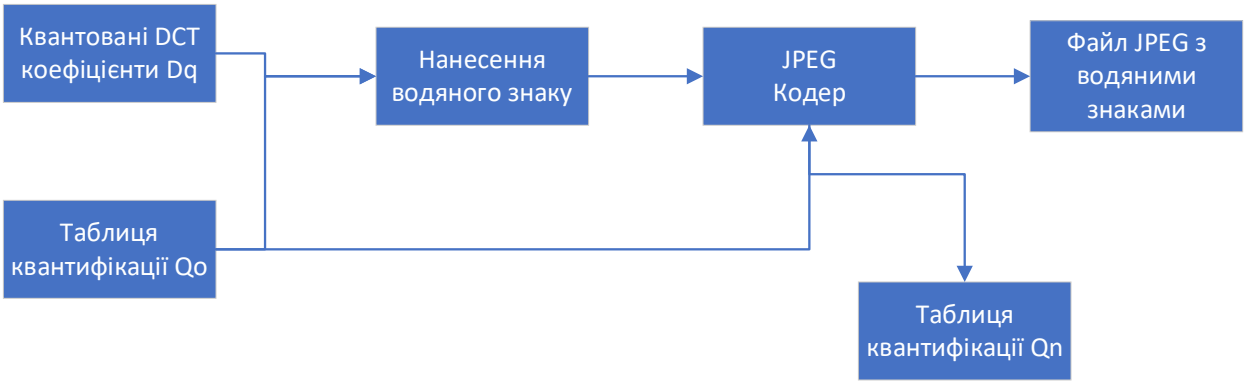

Рисунок 2.6 − Нанесення водяних знаків JPEG-JPEG (J2J)

Для вбудовування водяного знаку в зображення, стиснуті у форматі JPEG, файл JPEG повинен бути частково або повністю декодований. Рівень декодування залежить від області, в яку буде вбудовано водяний знак. Якщо водяний знак вбудовується в область бітового потоку, потрібне лише декодування змінної довжини. Якщо водяний знак вбудовується в область ДКП на основі блоків 8x8, то знадобиться зворотне зигзагоподібне сканування та зворотне квантування. У випадку, коли водяний знак вбудовано в просторову або будь-яку іншу частотну область, необхідно використовувати інверсне ДКП.

Узагальнену модель нанесення водяних знаків J2J зображено на рисунку 2.6. На цьому рисунку передбачається, що зображення з водяними знаками буде стиснуто у форматі JPEG з використанням або оригінальної

таблиці квантування, або нової таблиці квантування, визначеної користувачем. Також передбачається, що розміри зображень не змінюються в процесі вбудовування водяних знаків.

З наведених вище обговорень і сучасної літератури видно, що більшість схем водяних знаків у форматі JPEG, як правило, використовують для вбудовування водяного знака область перетворення або розширеного спектра. Також зазначається, що більшість схем намагаються зберегти розміри зображення незмінними, вносячи при цьому певний відсоток спотворення. Таким чином, у цій галузі існує можливість для нової схеми водяного маркування, яка вбудовує водяний знак, використовуючи методи кодування, а не спектральні методи. Це і є метою даної дисертаційної роботи, яка також спрямована на отримання зображення з водяним знаком, яке, можливо, дещо розширене, але не вносить жодних спотворень.

3 ЦИФРОВЕ НАНЕСЕННЯ ВОДЯНИХ ЗНАКІВ НА ЗОБРАЖЕННЯ З ВИКОРИСТАННЯМ ДИСКРЕТНОГО ЛІНІЙНОЇ МОДУЛЯЦІЇ НА ОСНОВІ КОСИНУСНОГО ПЕРЕТВОРЕННЯ

3.1 Опис роботи методу

Нехай H - вихідне сіре зображення розміром NxM, яке розбито на блоки розміром 8 X 8 пікселів, що не перетинаються. Оригінальне зображення подається наступним чином: H ={D(i,j), $0 \leq N$, $0 \leq j \leq M$}, де $D(i,j) \in \{0, 1, ..., 2^L -1\}$ - інтенсивність пікселя (i,j), а L - кількість бітів, використаних у кожному пікселі, 8-бітовий піксель має рівні від 0 до 255. Етапи підходу вбудовування проілюстровано нижче:

Крок 1: Дискретне косинусне перетворення (DCT)

Водяні знаки можна класифікувати на методи перетворення та просторові методи; де методи просторової області працюють зі значеннями пікселів, методи перетворення використовують DCT (математичні інструменти) для перетворення значень пікселів у значення частотних діапазонів (коефіцієнтів), а процес вбудовування водяного знаку здійснюється таким чином, щоб створити більш суттєвий вплив у межах зображення на область значень. У більшості робіт сигнал водяного знаку обережно вставляється в певні визначені блоки зображення. Одним із широко використовуваних перетворень у технології цифрової обробки сигналів є DCT. DCT розділяє зображення на ділянки або спектральні підсмуги різної значущості (з урахуванням якості перегляду зображення) , як показано на рисунку 3.1.

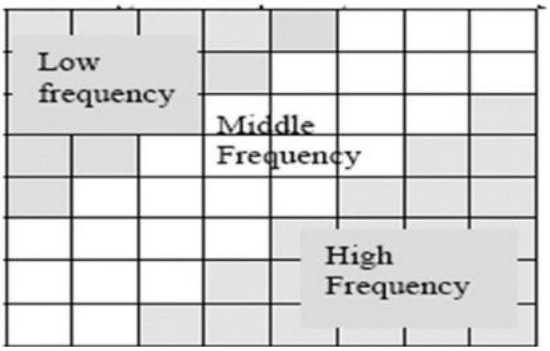

Рисунок 3.1 − Матриця коефіцієнтів DCT

Використовуючи DCT, область просторових даних може бути перетворена в дані частотної області, і вона може бути перетворена назад в область просторових даних за допомогою зворотного IDCT. Наведені нижче рівняння представляють формули DCT 3.1 і 3.2

$$D(i,j) = \frac{1}{\sqrt{2N}} C(i)C(j) \sum_{x=0}^{N-1}\sum_{y}^{N-1} f(x,y) \times \cos\left[\frac{(2x+1)}{2N}\right]\cos\left[\frac{(2y+1)i\pi}{2N}\right] \quad (3.1)$$

$$f(x,y) = \frac{1}{\sqrt{2N}} \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} C(i)C(j)D(i,j) \times \cos\left[\frac{(2x+1)i\pi}{2N}\right]\cos\left[\frac{(2y+1)i\pi}{2N}\right] \quad (3.2)$$

де

$$C(k) = \begin{cases} \frac{1}{\sqrt{2}} if\ k = 0 \\ 1 if\ k = 1,2,...,N-1 \end{cases} \quad (3.3)$$

f(x, y) в рівняннях 3.1 і 3.2 позначає інтенсивність значення пікселя в

позиції (x, y), значення коефіцієнту - D(i, j), де позиція в частотній області (i, j), а ширина вхідного зображення позначається через N. Коефіцієнт у верхньому лівому куті матриці частотної області відповідає значенню постійного струму в частотній області зображення. Значення змінного струму складають частину, що залишилася, причому абсолютне значення змінного струму в кожній точці позначає об'єм енергії. Основна операція перетворення зображення (N×N) у частотну область за допомогою ДКП виглядає так, як показано на рисунку 3.2.

```
1.   For i =0 to N-1;
2.     For j = 0 to N-1;
3.       Sum =0;
4.           For x= 0 to N-1;
5.             For y= 0 to N-1;
6.                 Sum = sum + f(x,y) * cos((2x + 1) * iπ)/2N) * cos((2y + 1) * iπ)/2N);
7.             Next y;
8.           Next x;
9.       F (i, j) =sum *1/√2N ;
10.    Next j;
11.  Next i;
```

Рисунок 3.2 − Псевдо код DC

Значення DTC у рядку k_1 та стовпчику k_2 матриці DTC - це f (x, y). Вихідне зображення N. D(i, j) позначається значенням інтенсивності пікселя в рядку I та стовпчику j. Низькі частоти, які відображаються у верхньому лівому куті DCT, складають основну частину енергії сигналу на більшості зображень (значення DC). Стиснення виконується тому, що нижній правий кут вказує на вищі частоти, які, як правило, досить скромні, щоб їх можна було ігнорувати з невеликим видимим спотворенням. Значення DTC є цілочисельною матрицею 8×8, що складається з рівня відтінків сірого пікселів, ці пікселі мають рівні від 0 до 255, а алгоритм DCT є одним з основних компонентів техніки стиснення JPEG.

Крок 2: Вбудовування водяного знаку за допомогою алгоритму лінійної модуляції.

Блоки водяного знаку вбудовуються в кожен індексований блок з

низькою частотою на основному зображенні. Відповідно до зигзагоподібного формату, коефіцієнти ДКП зберігаються [20], як показано на рис. 3, C (i,j) представляє місце вбудовування низької частоти. Коли починається фаза вбудовування водяного знаку, блок вбудовується шляхом заміни його на LSB коефіцієнтів DCT.

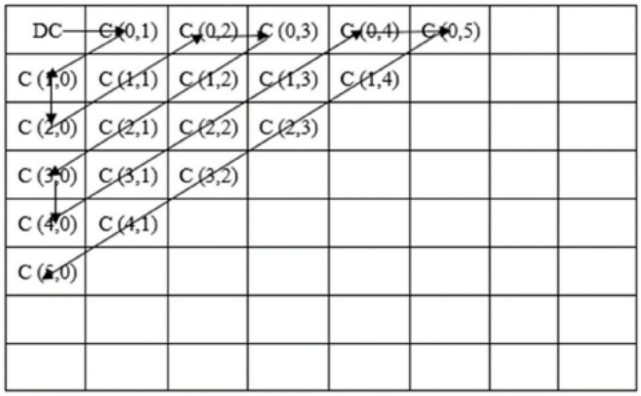

Рисунок 3.3 − Позиція вбудовування ZIG-ZAG в низькочастотному діапазоні

У цьому алгоритмі водяний знак, вбудований в область ДКП, використовується для підвищення стійкості методу водяного маркування до різних атак на зображення. У кожен n×n DCT-блок зображення вбудовуються біти водяного знаку. Для вбудовування бітів водяного знаку в блок n×n слід ретельно вибирати техніку вбудовування. Вбудовування бітів водяного знаку в низькочастотні компоненти блоку ДКП не є гарною ідеєю, оскільки це зробить вбудовані дані помітними. Крім того, біти водяного знаку не можна вбудовувати у високочастотні частини ДКП, оскільки всі ці коефіцієнти сильно квантуються під час стиснення даних. Як правило, краще вбудовувати водяний знак у середньочастотну область. Щоб пояснити процес вбудовування, припустимо, що на вході JPEG є зображення 640×480 RGB з роздільною здатністю 24 біт/піксель.

Процес вбудовування ілюструється наступним чином:

1 Оригінальне зображення слід перетворити з RGB в YCbCr за

допомогою рівнянь 3.4, 3.5 і 3.6 відповідно

$$Y = 0.299R + 0.587G + 0.114B \tag{3.4}$$

$$Cb = 0.5 + (B - Y)/2 \tag{3.5}$$

$$Cr = 0.5 + (R - Y)/1.6 \tag{3.6}$$

де Y позначає яскравість пікселя чорно-білого зображення, а Cb та Cr - кольоровість. Кожен з цих елементів матриці знаходиться в діапазоні [0, 255]. Матриця Cb і Cr містить чотири пікселі у вигляді квадратних блоків, щоб зменшити їх до 320×240. Щоб помістити 0 в середину діапазону, кожен елемент усіх трьох матриць віднімається від 128. Всі матриці розбито на блоки 8×8. Матриця Y має 4800 блоків, а дві інші - по 1200 блоків, як показано на рисунку 3.4.

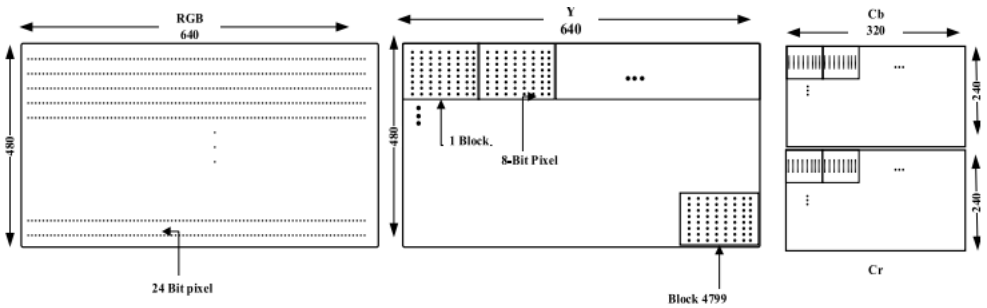

Рисунок 3.4 − Матриця коефіцієнтів DCT

2 Розбиваємо матрицю Y на блоки 8×8. Застосовуємо ДКП (дискретне косинусне перетворення) для перетворення блоку зображення у відповідну матрицю, коли ми застосовуємо ДКП до кожного з 7200 блоків окремо. Результатом всіх ДКП є матриця 8×8. Елемент ДКП (0, 0) є середнім значенням блоку

3 Коефіцієнти ДКП квантуються відповідно до таблиці квантування, як

показано на рисунку 3.5. Коефіцієнт квантування отримують діленням кожного елемента DCT на відповідний елемент таблиці квантування.

DCT Coefficients

150	80	40	14	4	2	1	0
92	75	36	10	6	1	0	0
52	38	26	8	7	4	0	0
12	8	6	4	2	1	0	0
4	3	2	0	0	0	0	0
2	2	1	1	0	0	0	0
1	1	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Quantization table

1	1	2	4	8	16	32	64
1	1	2	4	8	16	32	64
2	2	2	4	8	16	32	64
4	4	4	4	8	16	32	64
8	8	8	8	8	16	32	64
16	16	16	16	16	16	32	64
32	32	32	32	32	32	32	64
64	64	64	64	64	64	64	64

Quantized coefficients

150	80	20	4	1	0	0	0
92	75	18	3	1	0	0	0
26	19	13	2	1	0	0	0
3	2	2	1	0	0	0	0
1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Рисунок 3.5 − Обчислення квантованих коефіцієнтів ДКП

$$CQ(i, j) = DCTcoefficient / quantizationelement \quad (3.7)$$

Результатом цього кроку є коефіцієнт квантування CQ(i,j), а матриця залишків R(i,j) (похибка квантування може бути додатною або від'ємною) зберігається. Застосуємо рівняння (3.8) для знаходження C(i,j).

$$C(i, j) = CQ(i, j) + R(i, j) \quad (3.8)$$

де C (i, j) - новий коефіцієнт після квантування, CQ (i, j) - абсолютний квантований коефіцієнт, а R - матриця похибок. Залишок може бути додатним або від'ємним.

Коли всі ваги дорівнюють 1, перетворення нічого не дає. Однак, вищі просторові частоти швидко згладжуються, коли ваги різко зростають від джерела. Загалом, квантування означає обмеження можливих значень величини або кількості до чітко визначеного набору значень. Отже, це схоже на перехід від безперервних значень до дискретних. Квантування зменшує кількість можливих значень, зменшуючи кількість бітів, необхідних для їх представлення.

4 Водяний знак вбудовується за формулою вбудовування 3.9.

$$C'QM(i,j) = (1-\alpha)C(i,j) + \alpha W(i,j),\ \alpha = 0.5 \quad (3.9)$$

де W (i, j) - біт водяного знаку; C'QM (i, j) - модифікований коефіцієнт середніх частот (блок зображення з водяним знаком), а C (i, j) - блок з основного зображення. Це вбудовує біт водяного знаку в LSB середньочастотних коефіцієнтів. Алгоритм повторюється для побудови всього зображення з водяним знаком. Оскільки водяний знак вбудовується в LSB на середній частоті квантованого блоку, це обмежує довжину послідовності водяного знаку, яка не може бути більшою за кількість середньочастотних коефіцієнтів. Решта частотних компонент (що відповідають високим і низьким частотам) беруться як у рівнянні (3.10):

$$C'Q(i,j) = \begin{cases} C'QM(i,j) \in middlefrequency \\ CQ(i,j)\ forremaining \end{cases} \quad (3.10)$$

5 Залишок, який було збережено на кроці 3, додається до відповідних коефіцієнтів. Це робиться для того, щоб уникнути втрати даних через квантування.

$$C'(i,j) = C'Q(i,j) + R(i,j) \quad (3.11)$$

6. Матриця коефіцієнтів C` (i, j), отримана на кроці 5, застосовується до оберненого перетворення, щоб отримати фінальне зображення з водяними знаками рис. 3.6.

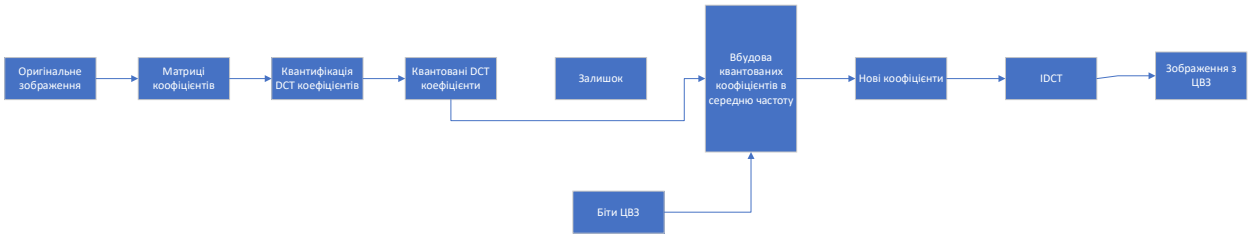

Рисунок 3.6 – Процес вбудовування водяного знаку

Процес вилучення можна проілюструвати наступним чином: для вилучення водяного знаку потрібне оригінальне зображення носія. Відновіть кожен блок оригінального блоку зображення водяного знаку, використовуючи рівняння (3.12):

$$W(i,j) = \left(C'QM(i,j) - \left((1-\alpha)C(i,j)\right)\right) / \alpha \text{ where } \alpha \text{ is } \alpha \text{ factor } = 0.5 \quad (3.12)$$

Процес вилучення водяного знаку є зворотним до вбудовування зображення водяного знаку, див. рис. 3.7. Короткий приклад процесу вбудовування та вилучення можна побачити на рис. 3.9. Крім того, короткий практичний приклад етапів вбудовування та вилучення водяних знаків показано нижче на рисунку 3.8.

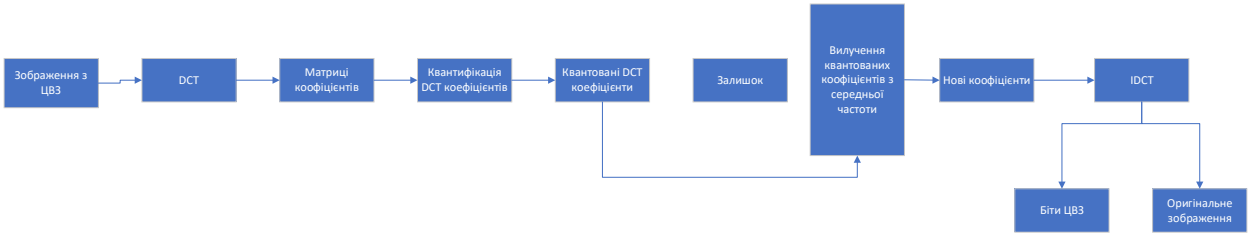

Рисунок 3.7 – Процес вилучення водяного знаку

Embedding an extraction process in detail:
E.g. let watermark bit =1, let DCT coefficient =12, let the quantization =8, i=2, j=2.
According to Eq.8:
$C(i,j) = CQ(i,j) + R(i,j)$ ... (8)
CQ (2,2) =round (DCT coefficient / quantization)
CQ (2,2) =round (12/8) =1.50 ~ 2

R (2, 2) = (exact CQ (2, 2) – round (exact))
R (2, 2) =1.50-2= -0.50 // save in error matrix
C (i, j) = 2+-0.5 = 1.5

- **Embedded** According to Eq.9:

$C'QM(i,j) = (1-\alpha)C(i,j) + \alpha W(i,j)$, $\alpha = 0.5$ ... (9)
= (1-0.5) (2+-0.5) +0.5(1)
= (0.5) (1.5) +(0.5)
=8

- **The extraction** algorithm of watermark requires running the algorithm backward according to equation (12):

$W(i,j) = \left(C'QM(i,j) - \left((1-\alpha)C(i,j)\right)\right)/\alpha$ ... (12)
= (8-((1-0.5) (1.5)))/0.5
= (8-7.5)/0.5
=1

Рисунок 3.8 – Практичний приклад вбудовування та вилучення водяних знаків

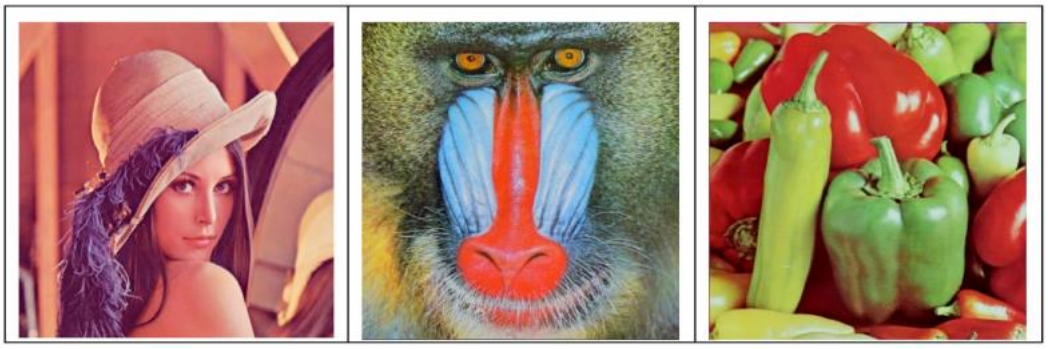

Рисунок 3.9 − Зображення для вставки розміром 640×480 пікселів. Lena, Mandrill (baboon), Peppers

3.2 Експерименти та результати

Методи цифрового нанесення водяних знаків оцінюються за непомітністю та стійкістю водяного знаку до будь-яких маніпуляцій. Непомітність вбудованого водяного знаку для людини та стійкість водяного знаку до будь-яких маніпуляцій із зображенням, на яке нанесено водяний знак, оцінюється як непомітність після вбудовування, так і стійкість до будь-яких маніпуляцій. У цьому розділі представлено оцінку як непомітності після процесу вбудовування, так і стійкості після процесу вилучення. Також показано оцінку алгоритмів лінійної модуляції

У цьому розділі представлено експериментальну конфігурацію запропонованого підходу. У цьому експерименті використано три кольорові зображення, як показано на рис. 3.9, розміром 640×480 пікселів (в основному використовується набір даних в області водяних знаків зображень), які використовуються для бенчмаркінгу запропонованого методу стеганографії. Водяний знак (стеганографічний текст), який використовується для оцінки, являє собою послідовність двійкових цифр [0, 1], що містить інформацію для автентифікації. Секретне повідомлення перетворюється з масиву символів (або байтів) в масив бітів як послідовність бітів. Розмір стего-тексту становить 50 символів, що повторюються десять разів, максимальна ємність

водяного знаку досягає 131 072 біт, а зображення хоста є 8-бітними зображеннями сірого рівня. Для вимірювання стійкості запропоновані алгоритми були оцінені під впливом різних типів атак, геометричних атак (обертання) та негеометричних атак (гаусівський шум, Salt & pepper та шум стиснення JPEG), список різних атак та їх опис наведено в таблиці 3. Всі експерименти проводилися на настільному комп'ютері з процесором Intel Core i3 з тактовою частотою 2,67 ГГц і 4 ГБ оперативної пам'яті,

Таблиця 3.1 демонструє значення PSNR та NC після вставки стего-тексту з використанням нашого підходу для зображень Лена, Бабуїн та перець, відповідно. При різній довжині стего-тексту, що досягала 50 символів, він повторювався десять разів, без жодної атаки.

Таблиця 3.1 −Значення PSNR та NC на різних зображеннях після вставки стего-тексту без атаки

Розмір стего-тексту (char) повторено 10 разів	Lena (640×480)		Baboon (640×480)		Peppers (640×480)	
	PSNR	NC	PSNR	NC	PSNR	NC
20	43.36 dB	1	42.64 dB	1	43.28 dB	1
30	43.33 dB	1	42.63 dB	1	43.26 dB	1
40	43.31 dB	1	42.63 dB	1	43.26 dB	1
50	43.30dB	1	42.62 dB	1	43.25 dB	1

Таблиця 3.2 демонструє стійкість вбудови до JPEG стиснення.

Запропонована схема досягла більш високого значення PSNR, що означає, що схема лінійної модуляції дає хороші результати по непомітності стеготексту при використанні її в якості алгоритму стеганографії і не

викликає ніяких підозр.

Таблиця 3.2 − Стеганографічне зображення Олени після стиснення JPEG та результат BER, NC витягнутого стего-тексту

Коефіцієнт стиснення	PSNR	Стего-текст BER	Стего-текст NC
Q=90	39.61 dB	1.57%	0.9872
Q=70	38.42 dB	1.69%	0.9867
Q=30	36.64 dB	3.47%	0.9681

BER(%) і NC розраховуються для оцінки надійності приховування і його стійкості до різних атак, запропонована схема алгоритму покращила надійність і помітність вилучення стего-тексту при атаках гаусівським шумом, сіллю і перцем, обертанням і стисненням JPEG у випадку приховування 1 біт/блок. основним обмеженням є те, що вона показує низьку надійність при приховуванні водяного знаку 2 біт/блок. Через застосування однакового розміру кроку квантування для всіх блоків на низьких частотах у просторовій області, де він може мати важливі характеристики.

ВИСНОВКИ

Ця робота була присвячена дослідженню методів вбудовування цифрових водяних знаків у частотній області з використанням дискретного косинусного перетворення (ДКП). Основною метою було дослідження ефективності та стійкості методу вбудовування водяного знака шляхом модифікації найменш значущого біта (НЗБ) частотних компонент з використанням лінійних модуляцій.

Запропонована схема досягла більш високого значення PSNR, що означає, що схема лінійної модуляції дає хороші результати по непомітності стеготексту при використанні її в якості алгоритму стеганографії і не викликає ніяких підозр. BER(%) і NC розраховуються для оцінки надійності приховування і його стійкості до різних атак, запропонована схема алгоритму покращила надійність і помітність вилучення стего-тексту при атаках гаусівським шумом, сіллю і перцем, обертанням і стисненням JPEG у випадку приховування 1 біт/блок. основним обмеженням є те, що вона показує низьку надійність при приховуванні водяного знаку 2 біт/блок. Через застосування однакового розміру кроку квантування для всіх блоків на низьких частотах у просторовій області, де він може мати важливі характеристики.

Метод вбудовування цифрових водяних знаків у частотній області з використанням ДКП та модифікації найменш значущого біта за допомогою лінійних модуляцій є ефективним та надійним. Він забезпечує високий рівень непомітності, стійкість до різних атак та точність вилучення водяного знака. Цей метод може бути рекомендований для використання в системах захисту авторських прав та аутентифікації цифрових зображень.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. R.Oppliger, “Security Technologies for the World Wide Web," in Intellectual Property Protection, 2nd ed Norwood, MA: Artech House, 2003, pp. 347-357

2. G.P.Schneider and J.T.Perry, Electronic Commerce, 2nd ed Canada: Course Technology Thomson Learning, 2001, p.198.

3. H. Berghel and L. O'Gorman, "Protecting Ownership Rights through Digital Watermarking," IEEE Computer, vol. 29, no.7, pp. 101-103, 1996.

4. W.T. Penzhorn and W.C. Els, “A universal Homophonic coding algorithm based on Arithmetic coding,” in Proc. IEEE South African Symposium on Communications and Signal Processing, pp. 52-59, 1994.

5. S.P.Mohanty, "Digital Watermarking: A Tutorial Review," Tampa: Department of Computer Science and Engineering, University of Florida, 1999.

6. A.Kejariwal, "Watermarking," IEEE Potentials, vol. 22, no. 4, pp. 37-40, 2003.

7. P.Wayner, Disappearing Cryptography-Information Hiding:Steganography & Watermarking, 2nd ed San Francisco: Morgan Kaufmann Publishers, 2002, p. 271.

8. M.A. Suhail and M.S. Obaidat, “Digital watermarking-based DCT and JPEG model,” IEEE Transactions on Instrumentation and Measurement, vol. 52, no. 5, pp. 1640-1647, 2003.

9. S. Lee and S. Jung, “A survey of watermarking techniques applied to multimedia,” in Proc. IEEE International Symposium on Industrial Electronics, vol.1, pp. 272- 277, 2001.

10. S. Katzenbeisser and F.A.P. Petitcolas, Information hiding techniques for steganography and digital watermarking, Norwood, MA: Artech House, 2002, pp. 121-132.

11. J.G. Proakis and M. Salehi, Communication Systems Engineering,

2nd ed, New Jersey: Prentice Hall, 2002, pp323-324.

12. M.S. Hsieh, D.C. Tseng and Y.H. Huang, “Hiding digital watermarks using multiresolution wavelet transform,” IEEE Transactions on Industrial Electronics, vol. 48, no. 5, pp. 875-882, 2001.

13. S. Voloshynovskiy et al, “Attacks on Digital Watermarks: Classification, Estimation-Based attacks and Benchmarks,” IEEE Communications, pp 118-126, 2001.

14. P.H.W. Wong and O.C. Au, “A capacity estimation technique for JPEG-to-JPEG image watermarking,” IEEE Transactions on Circuits and systems for video technology, vol. 13, no. 8, pp. 746-752, 2003.

15. Y. Choi and K. Aizawa, “Digital watermarking using inter-block correlation: extension to JPEG coded domain,” in Proc. IEEE Int. Conf. Information Technology: Coding and Computing, pp. 133–138, 2000.

16. W. Luo, G. L. Heileman, and C. E. Pizano, “Fast and robust watermarking of JPEG files,” in Proc. IEEE 5th Southwest Symp. Image Analysis and Interpretation, pp. 158–162, 2002.

17. P. H. W. Wong and O. C. Au, “Data hiding and watermarking in JPEG compressed domain by DC coefficient modification,” in Proc. SPIE Security and Watermarking of Multimedia Contents, vol. 3971, pp. 237–244, 2000.

18. P. H. W. Wong and O. C. Au, “Data hiding technique in JPEG compressed domain,” in Proc.SPIE Security and Watermarking of Multimedia Contents, vol. 4314, pp. 309–320, 2001.

19. G.K Wallace, “The JPEG still picture compression standard,” IEEE Transactions on Consumer Electronics, 1991.

20. DCube Software Technologies, “JPEG Baseline compression”, http://www.funducode.com/conferences.asp. Last accessed on June 2005.

21. О. О. Галицька, Н. М Бологова, Д. О. Кібірєв, О. В. Скиба " ОГЛЯД ПІДХОДІВ ДО ЗАХИСТУ ТРИВИМІРНИХ МОДЕЛЕЙ ВІД НЕСАНКЦІОНОВАНОГО РОЗПОВСЮДЖЕННЯ" Системи управління, навігації та зв'язку. 2024. No 3 104-108