Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління
(повна назва)

Кафедра безпеки інформаційних технологій
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Метод нанесення водяних знаків на зображення на основі DWT і SVD

(тема)

Виконав:

студент II курсу, групи БІКСзм-20-1

Костенков П.Ю.
(прізвище, ініціали)

Спеціальність

125 «Кібербезпека»
(код і повна назва спеціальності)

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

Освітня програма

Безпека інформаційних і комунікаційних систем
(повна назва освітньої програми)

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

Допускається до захисту

Зав. кафедри БІТ _____ Халімов Г.З.
(підпис) (прізвище, ініціали)

2021 р.

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління

Кафедра безпеки інформаційних технологій

Рівень вищої освіти другий (магістерський)

Спеціальність 125 «Кібербезпека»
(код і повна назва)

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

Освітня програма Безпека інформаційних і комунікаційних систем
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
"____" _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Костенкову Павлу Юрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Метод нанесення водяних знаків на зображення на основі DWT і SVD

затверджена наказом по університету від " 25 " жовтня 2021 р. № 166 Стз

2. Термін подання студентом роботи до екзаменаційної комісії 13 грудня 2021 р.

3. Вхідні дані до роботи Алгоритми вбудови ЦВЗ та набір зображень

4. Перелік питань, що потрібно опрацювати у роботі

1) Запропонувати методику оцінки впливу зовнішніх впливів на вбудований ЦВЗ

2) Знайти оптимальні показники непомітності застосування та пропускної спроможності спроможності зображення-контейнера

3) Провести порівняльний аналіз стійкості ЦВЗ, впроваджених різними алгоритмами

4) Розробити алгоритм вбудови ЦВЗ на основі DWT і SVD

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

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 сфер застосування цифрових водяних	09.11.21-12.11.21	
2	Аналіз форматів представлення зображень	13.11.21-18.11.21	
3	Огляд сучасних методів нанесення ЦВЗ	19.11.21-22.11.21	
4	Розробка програмного комплексу	23.11.21-29.11.21	
5	Проведення експериментів	30.11.21-03.12.21	
6	Оформлення матеріалів кваліфікаційної роботи	04.12.21-07.12.21	
7	Подання кваліфікаційної роботи керівникові та	08.12.21-09.12.21	
	її попередній захист		
8	Подання кваліфікаційної роботи на	10.12.21-11.12.21	

Дата видачі завдання 25 жовтня 2021 р.

Студент _____
(підпис)

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

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: XX с., 17 рис., 5 табл., 1 дод., 7 джерел.

ЗОБРАЖЕННЯ, ЦИФРОВИЙ ВОДЯНИЙ ЗНАК, СТЕГАНОГРАФІЯ, АВТОРСЬКІ ПРАВА.

Метою кваліфікаційної роботи є розробка алгоритму, що дозволяє вбудовувати ЦВЗ підвищеної стійкості до зовнішніх впливів на зображення-контейнер у форматі JPEG 2000.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1. Запропонувати методику оцінки впливу зовнішніх впливів на вбудований ЦВЗ.
2. Знайти оптимальні показники непомітності застосування та пропускної спроможності зображення-контейнера при вбудовуванні ЦВЗ.
3. Провести порівняльний аналіз стійкості ЦВЗ, впроваджених різними алгоритмами зображення JPEG 2000, при якому зберігаються оптимальні рівні скритності впровадження і пропускної спроможності.

Предметом дослідження є стійкість ЦВЗ до зовнішніх впливів на зображення-контейнер.

Об'єктом дослідження є стеганографічні методи та алгоритми впровадження ЦВЗ у область ДВП цифрових зображень.

ABSTRACT

Master’s thesis: XX pages, 17 figures, 5 tables, 1 appendices, 7 sources.

IMAGE, DIGITAL WATERMARK, STEGANOGRAPHY, COPYRIGHT.

The major goal of this thesis is to develop an algorithm that allows you to embed the WM of high resistance to external influences on the image-container in JPEG 2000 format.

To achieve this goal it is necessary to solve the following tasks:

1. To propose a method of assessing the impact of external influences on the built-in WM.

2. To find the optimal indicators of invisibility of application and bandwidth of the image-container at embedding of WM.

3. Carry out a comparative analysis of the stability of WM implemented by different image algorithms JPEG 2000, which maintains the optimal levels of secrecy of implementation and bandwidth.

The subject of the study is the resistance of the WM to external influences on the image-container.

The object of research is steganographic methods and algorithms for the implementation of WM in the field of fiberboard digital images.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ДКП – дискретне косинусне перетворення

ДВП – дискретне вейвлет перетворення

ПФ – перетворення Фур'є

ЦВЗ – цифровий водяний знак

СЛЗ – Система людського зору

ASCII – American Standard Code for Information Interchange – стандартний американський код для обміну інформацією

JPEG 2000 – стандарт стиснення із втратами для повнокольорових зображень на основі алгоритму дискретного вейвлету перетворення

ROI – Етап обробки регіонів, де виділяється довільний доступ до кодового потоку. Цей етап може бути підключений до схеми кодування JPEG 2000

EBCOT – Етап вкладеного блокового кодування з оптимізованим усіченням ланцюга кодування JPEG 2000

RGB – основна палітра, що використовується в програмуванні та комп'ютерній графіці (абревіатура англійських слів Red, Green, Blue – червоний, зелений, синій)

ВСТУП

На даний момент стеганографічні алгоритми широко використовуються для впровадження прихованої інформації в мультимедіа файли з метою захисту авторських прав на продукцію. Більшість великих інтернет-магазинів перед викладанням продукції автора накладають цифрові водяні знаки на неї (ЦВЗ). Як продукція виступають постановочні фотографії, панорами, обкладинки та вкладки музичних альбомів та відеофільмів. ЦВЗ містять інформацію, що однозначно підтверджує авторство або права на комерційне використання зображення, що захищається, яка може бути рахована для вирішення спірних правових ситуацій. Для маркування комерційної продукції цифровими водяними знаками потрібно передбачити такий момент, що в мережах зазвичай викладаються цифрові зображення, які проходять стиснення за певним алгоритмом з метою зменшення обсягу. Зазвичай застосовується стиснення з втратами, при використанні якого розпаковані дані відрізняються від вихідних, але відмінність не є істотною з точки зору їх подальшого використання. Тому потрібно передбачити, щоб інформація, що вбудовується, була стійка до такого стиску.

У комп'ютерних мережах найпопулярнішим форматом зображень є JPEG – формат, у якому зменшення обсягу інформації для зберігання точок використовуються залежності, кореляції між близько розташованими друг до друга областями зображення. Стандарт стиснення JPEG 2000 замість дискретного косинусного перетворення, що використовується в популярному форматі JPEG, використовує технологію вейвлет-перетворення, що базується на поданні сигналу у вигляді суперпозиції базових функцій хвильових пакетів.

В результаті такої компресії зображення виходить гладкішим і чіткішим, а розмір файлу в порівнянні з JPEG при однаковій якості

виявляється меншим. Цей формат є найбільш актуальним для стиснення зображень з метою розповсюдження їх у електронних магазинах на продаж [1]. Він використовується в кодеках для створення 3D-анімації (візуалізації) і кодування/декодування відео високої роздільної здатності (наприклад Motion JPEG-2000). Вбудований водяний знак повинен бути стійким до подібного стиснення та різних зовнішніх впливів (обрізання, фрагментація, масштабування, зашумлення, фільтрація). Це одна з найважливіших вимог до стегоалгоритмам. Тому завдання створення методів і алгоритмів, використання яких при побудові стеганографічних систем захисту авторських прав для зображень може гарантувати цілісність ЦВЗ є актуальною.

Метою роботи є розробка алгоритмів та методів, що дозволяють вбудовувати ЦВЗ підвищеної стійкості до зовнішніх впливів на зображення-контейнер у форматі JPEG 2000.

Для досягнення поставленої мети необхідно вирішити такі завдання:

4. Запропонувати методику оцінки впливу зовнішніх впливів на вбудований ЦВЗ.

5. Знайти оптимальні показники непомітності застосування та пропускної спроможності зображення-контейнера при вбудовуванні ЦВЗ.

6. Провести порівняльний аналіз стійкості ЦВЗ, впроваджених різними алгоритмами зображення JPEG 2000, при якому зберігаються оптимальні рівні скритності впровадження і пропускної спроможності.

Предметом дослідження є стійкість ЦВЗ до зовнішніх впливів на зображення-контейнер.

Об'єктом дослідження є стеганографічні методи та алгоритми впровадження ЦВЗ у область ДВП цифрових зображень.

У методах дослідження використовувалися: методи теоретичного та емпіричного дослідження, апарати обчислювальної математики, методи проектування та програмування.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Основи стеганографії

Цифрова стеганографія - напрямок класичної стеганографії, заснований на приховуванні або впровадженні додаткової інформації в цифрові об'єкти, викликаючи деякі спотворення цих об'єктів. Дані об'єкти є мультимедіа файлами (зображення, відео, аудіо, текст) та внесення спотворень, що знаходяться нижче за поріг чутливості середньостатистичної людини, не призводить до помітних змін цих об'єктів. Сьогодні стеганографія дозволяє не лише успішно вирішувати основне завдання – потай передавати інформацію, а й цілу низку інших актуальних завдань, у тому числі вбудова прихованої інформації з метою захисту авторських прав на інтелектуальну власність, представлену в цифровому вигляді [1]. Ця інформація, що приховується, називається цифровим водяним знаком (ЦВЗ), який являє собою спеціальну мітку, що містить інформацію, однозначно підтверджує авторство або права на комерційне використання об'єкта, що захищається. Вона непомітно впроваджується у зображення чи інший сигнал з метою тим чи іншим чином контролювати його використання.

В останні роки у зв'язку з інтенсивним розвитком мультимедійних технологій дуже гостро постало питання захисту авторських прав та інтелектуальної власності, представленої у цифровому вигляді. ЦВЗ активно використовуються при розміщенні унікальних фотографій, відео, аудіо в електронному вигляді в Інтернеті. Перші роботи з вбудовування водяних знаків було зроблено у 90-х роках 20 століття. А в 1996 році на конференції Information Hiding: First Information Workshop було прийнято єдину термінологію в галузі цифрової стеганографії, яка буде використана надалі в роботі:

Стеганографічна система (стегосистема) - об'єднання методів і засобів,

що використовуються для створення прихованого каналу для передачі інформації. При побудові такої системи домовилися, що: 1) ворог знає роботу стеганографічної системи. Невідомим для противника є ключ, за допомогою якого можна дізнатися про факт існування та змісту таємного повідомлення. 2) При виявленні противником наявності прихованого повідомлення він повинен змогти витягти повідомлення до того часу поки він володіє ключем. 3) Противник не має технічних та інших переваг.

Повідомлення – це термін, що використовується для загальної назви прихованої інформації, що передається, будь то лист або цифровий файл.

Контейнер – так називається будь-яка інформація, яка використовується для приховування таємного повідомлення. Порожній контейнер – контейнер, який не містить секретного послання. Заповнений контейнер (стегоконтейнер) – контейнер, що містить таємне послання.

Стеганографічний канал (стегоканал) – канал передачі стегоконтейнера.

Ключ (стегоключ) – секретний ключ, необхідний для приховування стегоконтейнера. Ключі в стегосистемах бувають двох типів: секретні та відкриті. Якщо стегосистема використовує секретний ключ, то він має бути створений або до початку обміну повідомленнями, або переданий захищеним каналом. Стегосистема, що використовує відкритий ключ, повинна бути влаштована таким чином, щоб неможливо було отримати з нього закритий ключ. У цьому випадку відкритий ключ ми можемо передавати незахищеним каналом [2].

Завдання вбудовування та виділення повідомлень з іншої інформації виконує стегосистема. Стегосистема складається з наступних основних елементів:

Прекодер – пристрій, призначений для перетворення прихованого повідомлення до вигляду, зручного для вбудови на сигнал-контейнер.

Контейнер – інформаційна послідовність, в якій ховається повідомлення.

Стегокодер – пристрій, призначене для здійснення вкладення прихованого повідомлення в інші дані з урахуванням їхньої моделі.

Пристрій виділення вбудованого повідомлення

Стегодетектор – пристрій, призначений для визначення наявності стегоповідомлення.

Декодер – пристрій, який відновлює приховане повідомлення. Цей вузол може бути відсутнім, якщо нам потрібно лише встановити факт наявності в об'єкті вбудованого раніше нами ЦВЗ.

1.2 Вимоги до систем вбудови цифрового водяного знаку

Основними вимогами до стегосистем вбудовування прихованої інформації, що згадуються в літературі, є наступні вимоги перелічені далі.

Методи приховування повинні забезпечувати автентичність та цілісність файлу.

Передбачається, що противнику повністю відомі можливі методи стеганографії.

Безпека методів ґрунтується на збереженні стеганографічним перетворенням основних властивостей файлу, що відкрито передається при внесенні в нього секретного повідомлення і деякої невідомої противнику інформації - ключа.

Навіть якщо факт приховування повідомлення став відомий супротивнику через спільника, вилучення таємного повідомлення представляє складне обчислювальне завдання.

Заповнений контейнер повинен бути візуально не відмінним від незаповненого. Для задоволення цієї вимоги треба, здавалося б, впроваджувати приховане повідомлення візуально незначущі області сигналу. Однак ці області використовують і алгоритми стиснення. Тому, якщо зображення буде надалі стискатися, то приховане повідомлення може зруйнуватися. Отже, біти повинні вбудовуватися у візуально

значущі області, а відносна непомітність може бути досягнута за рахунок використання спеціальних методів, наприклад, модуляції з розширенням спектра.

Стегосистема повинна мати низьку ймовірність помилкового виявлення прихованого повідомлення в сигналі, що його не містить. У деяких програмах таке виявлення може призвести до серйозних наслідків [3].

Крім цього можна додати, що до систем вбудовування ЦВЗ висуваються ще додаткові вимоги:

1. Стійкість до зовнішніх дій. ЦВЗ не повинен ушкоджуватися в результаті маніпуляцій з контейнером, які можуть статися при його використанні, таким як фільтрація, нанесення шуму, стиснення з втратами, обрізка, масштабування, роздруківка та сканування, перетворення в інший формат.

2. ЦВЗ повинен протистояти спробам видалення його зі стегоконтейнера або це має супроводжуватися неприйнятним рівнем пошкодження зображення самого стегоконтейнера.

3. Має бути можливість багаторазового застосування ЦВЗ. Це необхідно для випадків, коли продукт виготовлений декількома виробниками, і кожен з них має власний стандарт ЦВЗ.

4. Повинна бути можливість використовувати покращені версії тієї ж техніки застосування, коли буде доступна велика потужність обчислювальної техніки.

5. Якщо доступний лише фрагмент стегоконтейнера, отриманий в результаті обрізки або обертання, ЦВЗ має детектуватися і читатися.

Усі перелічені вимоги не повинні обов'язково виконуватись у стегоалгоритмах у повному обсязі. Тим більше, деякі властивості перебувають у суперечності один з одним. Як правило, при розробці стегоалгоритму автори наголошують на певну властивість або групу властивостей. Це відбувається тому, що задовольнити всім вимогам відразу

непросто. Покращуючи одну властивість стегоалгоритму, можна погіршити його іншу властивість. Саме тому існує безліч різних конкуруючих технологій, які представлені на ринку та мають місце застосування клієнтами у різних ситуаціях. Тим більше з часом багато технологій старіють і на їх місце зі зростанням потужності обчислювальної техніки з'являються нові покращені алгоритми впровадження ЦВЗ. Також існує безліч вбудованих модулів (plug-in), які можуть бути підключені до популярних медіаредакторів (наприклад найбільш популярний редактор цифрових зображень Adobe Photoshop) і поєднують у собі різні алгоритми вбудовування ЦВЗ для різних ситуацій.

На даний момент безліч технологій вбудовування ЦВЗ добре використовуються в мережі інтернет, але не багато алгоритмів мають хороші показники захисту від зовнішніх впливів на контейнер. Тому ця область перебуває у постійному розвитку.

1.3 Сфери застосування цифрових водяних знакі

Вбудовування ЦВЗ у медіафайли може бути використане для таких цілей:

Вбудова інформації і її прихованої передачі. Цей напрямок використовується з метою захисту конфіденційної інформації від несанкціонованого доступу та безпечної її передачі через комп'ютерні мережі. Також подібний напрямок є привабливим, коли уряд країни накладає серйозні обмеження на використання засобів шифрування.

Вбудова ЦВЗ для захисту авторських прав на інтелектуальну власність, представлену в цифровому форматі. Правовласник або видавець може впровадити ЦВЗ, що містить інформацію про авторство в продукт, що захищається. Впроваджений ЦВЗ може бути використаний на підтвердження прав власності. Найбільші досягнення стеганографії були досягнуті саме в цій галузі, і вона перебуває у постійному розвитку на даний момент.

Маркування ідентифікаційними номерами для відстеження шляхів розповсюдження нелегальних копій продукту за допомогою техніки унікального підпису для кожної легальної копії. У цьому випадку власник може впроваджувати різні ЦВЗ для різних замовників. ЦВЗ може містити інформацію про серійний номер, що однозначно ідентифікує покупця, який порушив ліцензійну угоду та надав продукт для незаконного розповсюдження або копіювання.

Вбудова для захисту від копіювання медіафайлу. Впроваджений ЦВЗ може безпосередньо контролювати цифрові записуючі або друкувальні пристрої. Детектор ЦВЗ на записувальному пристрої визначає, чи може інформація надана пристрою бути скопійована.

Моніторинг широкомовних каналів. Таким чином, можна перевірити за допомогою автоматизованої системи, чи виконується контракт на трансляцію комерційної інформації з впровадженим ЦВЗ.

Вбудова для перевірки цілісності переданих даних. Впровадження ЦВЗ дозволяє перевірити дані щодо зміни чи пошкодження як навмисного, і випадкового характеру. Також можливе визначення, в якій саме частині даних було здійснено зміни.

Вбудова для індексації частин файлу. Допустимо якщо вбудувати ЦВЗ у відеопослідовність, то можна полегшити завдання пошуковому движку.

Вбудова ЦВЗ для підпису медичних знімків або нанесення легенди на карту. Метою є зберігання різнорідно поданої інформації у цілому. Впровадження інформації допоможе уникнути плутанини та забезпечить зручність зберігання інформації.

1.4 Різновиди контейнерів в стеганографії

Далі розглянемо докладніше поняття контейнера. У сучасній цифровій стеганографії як контейнери можуть виступати музичні файли (найпопулярніші формати WAV і MP3), зображення (формати JPEG та

BMP), відео (формати AVI та MPEG) та текстові файли (формати DOC та PDF). Стегоконтейнер повинен бути візуально відмінним від порожнього контейнера. Розрізняють два основних типи контейнерів: потоковий та фіксований. Істотний вплив на надійність та стійкість стегосистеми, а також можливість виявлення факту передачі прихованого повідомлення надає вибір контейнера. Найбільш досвідчені дизайнери з сприйняттям колірної гами більшої, ніж у звичайного користувача при введенні повідомлення зображення можуть помітити даний контейнер. Тому із вибором типу контейнера доводиться бути обережним.

Потоковий контейнер є безперервно наступною бітовою послідовністю. Повідомлення вкладається в нього в реальному масштабі часу, так що кодер невідомо заздалегідь, чи вистачить розмірів контейнера для передачі всього повідомлення. В один контейнер великого розміру може бути вбудовано кілька повідомлень. Інтервали між вбудовуваними бітами визначаються генератором псевдовипадкової послідовності з рівномірним розподілом інтервалів між відліками. Основна труднощі полягає у здійсненні синхронізації, визначенні початку та кінця послідовності. Якщо даних контейнера є біти синхронізації, заголовки пакетів і т.д., то приховується інформація може йти відразу після них. Трудність забезпечення синхронізації перетворюється на гідність з погляду забезпечення скритності передачі. Крім того, у фіксованого контейнера розміри та характеристики заздалегідь відомі. Це дозволяє здійснювати вкладення даних оптимальним чином. Але контейнери фіксованої довжини мають обмежений об'єм, і інколи вбудоване повідомлення може не помістится у файл-контейнер. Інший недолік у тому, що відстані між бітами, що приховують, рівномірно розподілені між найбільш коротким і найбільш довгим заданими відстанями, в той час як істинний випадковий шум буде мати експоненціальний розподіл довжин інтервалу [4]. Звичайно, можна породити псевдовипадкові експонентно розподілені числа, але цей шлях зазвичай занадто обчислювально складний. Насправді найчастіше

використовуються саме контейнери фіксованої довжини, як найпоширеніші і доступні. Контейнер може бути вибраним, випадковим чи нав'язаним. Вибраний контейнер залежить від вбудованого повідомлення, а в граничному випадку є його функцією. Цей тип контейнера більше уражає стеганографії. Нав'язаний контейнер може з'явитися в сценарії, коли особа, яка надає контейнер, підозрює про можливе приховане листування і бажає запобігти його. Насправді найчастіше стикаються з випадковим контейнером.

До кожного типу контейнерів існує безліч алгоритмів застосування ЦВЗ, специфічних конкретного виду стегоконтейнера. Стегоконтейнери можуть бути представлені в різних форматах, що накладає певні обмеження на реалізацію стегоалгоритму. У моїй дисертації я працюю з фіксованими контейнерами, які є цифровими зображеннями.

1.5 Використання зображень в якості стегоконтейнер

Цифрові зображення можуть бути гарним контейнером для впровадження в них прихованої інформації. Це пов'язано з фактом деякої надмірності візуальної інформації. Популярність використання цифрових зображень як стегоконтейнери обумовлена такими причинами:

- існуванням практично значущим завданням захисту фотографій, відео від незаконного тиражування та розповсюдження;
- великим обсягом пропускної спроможності зображень, що дозволяє впроваджувати ЦВЗ великого обсягу чи підвищувати робастність використання;
- наявністю у більшості реальних зображень текстурних областей, що мають шумову структуру та підходять для вбудовування інформації;
- слабкою чутливістю людського ока до незначних змін кольорів зображення, його яскравості, контрастності, змісту шуму, спотворень поблизу контурів .

Зображення з вбудованою секретною інформацією можна розмістити в певному місці в комп'ютерній мережі, яке буде відоме одержувачу. Знаючи ключ, він може розшифрувати повідомлення. Таким чином можна налагодити прихований канал передачі даних. Або можна перед розміщенням у відкриті джерела вбудувати свої зображення ЦВЗ, який точно ідентифікує автора файлу і використовуватиметься з метою захисту його авторських прав [5].

Для впровадження прихованого повідомлення у зображення потрібно створити стеганографічну систему, яка займатиметься шифруванням повідомлення, вбудовуванням його в контейнер, зчитуванням повідомлення та дешифруванням його. Схема системи представлена рис. 1.1.

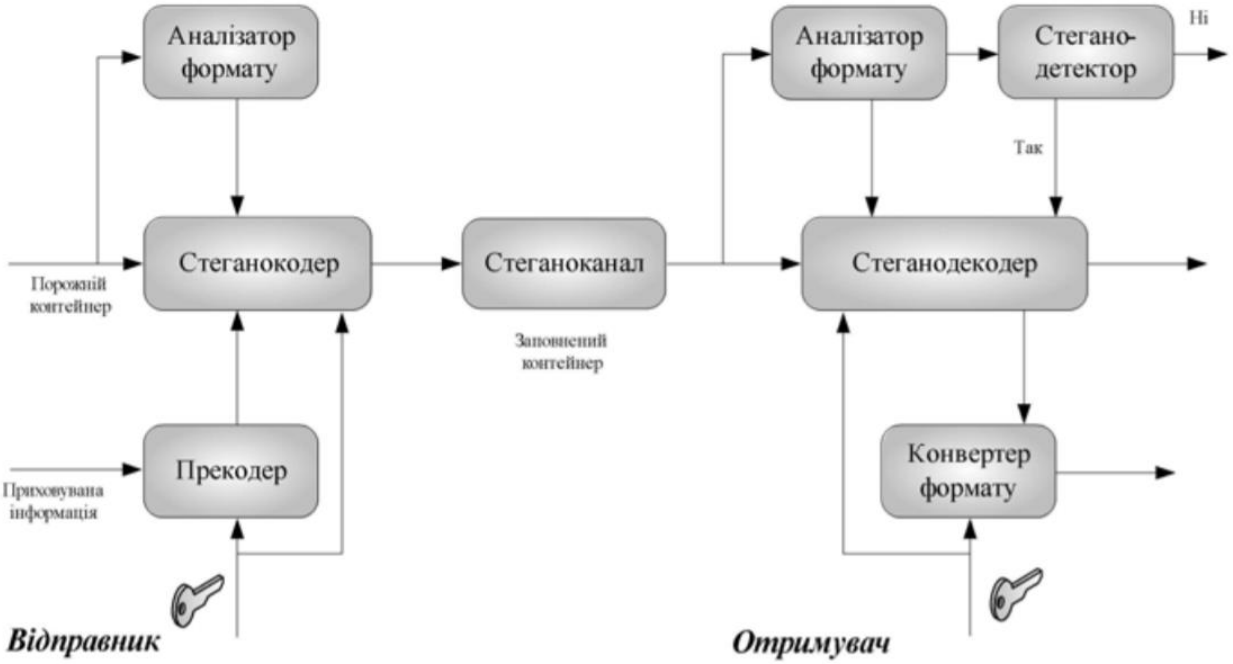

Рисунок 1.1 – Схема стегосистеми

Перш, ніж здійснити вбудовування ЦВЗ в контейнер, ЦВЗ має бути перетворений в деякий відповідний вид. Наприклад, якщо в якості контейнера виступає зображення, то й послідовність ЦВЗ найчастіше представляється як двовимірний масив біт. Для того щоб підвищити стійкість

ЦВЗ до спотворень нерідко виконують його стійкість до перешкод, або застосовують широкосмугові сигнали. Попередня обробка часто виконується з використанням ключа підвищення секретності вбудовування. Ключ може бути призначений для вузького кола осіб або бути загальнодоступним. Далі ЦВЗ вбудовується у контейнер. Прихована інформація впроваджується відповідно до ключа у ті відліки, спотворення яких не призводить до суттєвих спотворень контейнера. Залежно від додатка, під суттєвим спотворенням можна розуміти спотворення, що призводить як до неприйнятності для людини-адресата заповненого контейнера, так і до можливості виявлення прихованого повідомлення після стегоаналізу. Області вбудовування можуть бути виключені виходячи з різних обмежень, які накладаються в рамках того чи іншого стегоалгоритму. Серед вимог, що впливають на відбір придатних областей вбудовування можуть бути: візуальна невідмінність зображення з ЦВЗ від оригіналу зображення, складність несанкціонованого детектування ЦВЗ, стійкість ЦВЗ до різноманітних перетворень зображення-контейнера [6].

Для того щоб захистити впроваджуваний ЦВЗ від помилок, як правило, здійснюється зменшення його об'єму за допомогою використання алгоритмів стиснення і використовується багаторазове повторення вбудовування ЦВЗ у зображення-контейнер.

створенні системи вбудовування і зчитування ЦВЗ потрібно дуже уважно підходити до питання системи людського зору (СЛЗ). Зображення мають велику психовізуальну надмірність. Око людини подібне до низькочастотного фільтра, якому непомітні спотворення у високочастотній області зображень. Стеганографія заснована на використанні наявної у зображеннях психовізуальної надмірності [7].

Алгоритм зчитування ЦВЗ повинен правильно реконструювати ЦВЗ навіть після того, як підписане зображення було піддано таким змінам як: поворот, урізання країв, стиснення без втрат і т.д., які не позначилися на якості зображення. Також детектор повинен мати вкрай низьку ймовірність

помилкового детектування ЦВЗ (визначення є чи ні ЦВЗ у зображенні). Детектор як вхідні дані може вимагати: оригінальне зображення, ЦВЗ, секретний ключ. Якщо оригінальне зображення не потрібно для детектування ЦВЗ, то стегоалгоритм називають сліпим. Існують детектори, які можуть визначати лише можливість присутності ЦВЗ, інші здійснюють зчитування, отримуючи в результаті відновлений ЦВЗ.

2 МЕТОДИ ТА АЛГОРИТМИ ЦИФРОВОЇ СТЕГАНОГРАФІЇ

У 1989 був отриманий перший патент на спосіб прихованого вкладення інформації в зображення шляхом модифікації молодшого біта (LSB). У разі детектор аналізує лише значення цього біта кожному за пікселя, а око людини, навпаки, приймає лише старші 7 біт. Науково підтверджено факт, що система людського зору найменш чутлива до змін інтенсивності в синій області спектра. Таким чином, можна з великою впевненістю заміняти молодший біт байта, який відповідає за інтенсивність синього каналу, за обраною нами закономірністю. Людському оку буде важко відрізнити оригінальне чисте зображення від зображення з вбудованим прихованим повідомленням [2]. Даний метод є типовим представником методів вбудовування у просторову область зображення, при якому для вбудовування використовуються безпосередні зміни значень параметрів яскравості та кольоровості зображень. Існує багато модифікацій цього методу, але на даний момент багато з них застаріли.

2.1 Класифікація методів стеганографії

На даний момент існує безліч різних варіантів вибору області вбудовування ЦВЗ. Класифікація алгоритмів за способами вбудови наведено рис 2.1.

Рисунок 2.1 – Класифікація алгоритмів вбудови ЦВЗ

Методи приховування даних у просторовій області зображення є нестійкими до більшості відомих видів спотворень, наприклад стиснення з втратами. Вони відрізняються лише вибором підмножини пікселів, що модифікується, і стратегією зміни значень пікселів. Використання ЦВЗ відбувається у області вихідного зображення. Перевагою таких алгоритмів і те, що з впровадження ЦВЗ немає необхідності виконувати обчислювально громіздкі лінійні перетворення зображень. ЦВЗ впроваджується за рахунок маніпуляцій яскравістю або колірними складовими.

Найбільший інтерес у галузі цифрових зображень представляють методи вбудови інформації у зображення, де відбувається стискання із втратами (такі популярні формати як JPEG та JPEG 2000). Для таких форматів немає сенсу вбудовувати в просторову область, тому що після певних перетворень дані будуть відрізнятися від вихідних, і тому багато повідомлень просто неможливо витягти і таким чином втрачається сенс системи. Для вбудови інформації використовується область роздільної здатності або частотна область. Ці підходи з'явилися пізніше за попередній і продовжують розвиватися. Методи, що використовують для приховування даних частотну область, є стійкішими до різних можливих зовнішніх впливів на зображення-контейнер. У цій групі використовуються досить різноманітні трансформації:

- дискретне косинус-перетворення (ДКП)
- вейвлет-перетворення (ДВП)
- дискретне перетворення Фур'є (ДПФ)
- перетворення Карунена-Лоєва (ПКЛ)
- сингулярне розкладання.

Ці методи використовують переваги, якими володіє представлення зображення кінцевим набором коефіцієнтів. Такі методи мають добрі характеристики робастності. Подібні перетворення можуть застосовуватися або до окремих частин зображення або до зображення в цілому. Для приховування даних доцільно застосовувати саме таке перетворення зображення. Алгоритм ДКП є базовим у стандарті JPEG, а ДВП – у стандарті JPEG-2000. Тому для формату JPEG 2000 найбільш підходять технології вбудови коефіцієнти дискретного вейвлет перетворення, а формату JPEG коефіцієнти ДКП. При цих способах використовується скалярне або векторне квантування. Під квантуванням розуміється процес зіставлення великої (можливо і нескінченної) множини значень з деяким кінцевим безліччю чисел. Квантування знаходить застосування в алгоритмах стиснення із втратами JPEG та JPEG 2000. Розрізняють скалярне та векторне квантування. При векторному квантуванні, на відміну скалярного, відбувається відображення не окремо взятого відліку, які сукупності (вектора). Векторне квантування ефективніше скалярного за ступенем стиснення, маючи більшу складність. Методи вбудовування цифрові зображення стають основою для складніших методів вбудовування інформації у видеопоследовательности.

2.2 Методи вбудови цифрового водяного знаку в формати JPEG та JPEG 2000

2.2.1 Зображення у форматі зі стисненням з втратами

У комп'ютерних мережах зазвичай використовуються цифрові зображення форматах, де відбувається стиск із втратами. Це пов'язано з

великим розміром таких файлів. При використанні стиснення з втратами розпаковані після стиснення дані будуть відрізнятися від вихідних, але ступінь відмінності при цьому не буде суттєвим з точки зору їх подальшого використання. У таких кодеках кадри зображень трансформуються в новий базовий простір, і виконується квантування. А головне при використанні методів стиснення із втратами зображення задовольнятимуть вимоги спотворення у допустимих межах чутливості людських органів. При цьому файл може дуже відрізнятися від оригіналу на рівні порівняння біт в біт, але практично не відрізняється для людського ока. При цьому зображення будуть записані у форматі JPEG або JPEG 2000,

При вбудові ЦВЗ у просторову область зможемо забезпечити стійкість впровадженої інформації тільки до дуже низьких ступенів стиснення JPEG або JPEG 2000, зате нам не потрібно буде робити обчислювально складних математичних операцій. Якщо нашою метою є вбудова ЦВЗ для можливого захисту авторських прав, такі алгоритми не потрібно використовувати. Набагато доцільніше, як було зазначено раніше, вбудовувати в область перетворень, яка використовується у форматі стиснення зображення. Для JPEG це область ДКП, а для JPEG 2000 область ДВП.

2.2.2 Вбудова цифрового водяного знаку в область дискретного косинусного перетворення при форматі JPEG

За останні роки було зроблено безліч нових та вдосконалено старих алгоритмів вбудови ЦВЗ у коефіцієнти ДКП. Ці алгоритми дозволяють вбудоваувати ЦВЗ, протистояти високим ступеням стиснення JPEG та іншим зовнішнім впливам, таким як масштабування, зміна на формат стиснення без втрат, фільтрація, зашумлення. У найбільш класичній ситуації зображення спочатку розбивається на блоки розміром 8x8 пікселів. ДКП застосовується до кожного блоку, у результаті виходять матриці коефіцієнтів ДКП, і навіть розміром 8x8. Коефіцієнти позначаються через $c_b(j,k)$, де b – номер блоку, (j, k) – позиція коефіцієнта усередині блоку. Якщо блок сканується в зигзагоподібному порядку, то коефіцієнти позначаються через $c_{b,k}$

Коефіцієнт в лівому верхньому кутку $c_b(0,0)$ зазвичай називається DC-коефіцієнтом. Він містить інформацію про яскравість всього блоку. Інші коефіцієнти називаються AC-коефіцієнтами. Псевдовипадково вибираються кілька коефіцієнтів ДКП і вбудовування здійснюється з певної умови залежно від алгоритму. Поділяють однокоефіцієнтні, двокоефіцієнтні та багатокоефіцієнтні алгоритми. Враховуючи зростання обчислювальних потужностей та збільшення зростання інтернет торгівлі алгоритми, що вбудовують ЦВЗ в область ДКП, продовжують покращуватися, і з'являються нові роботи в цьому напрямі.

2.2.3 Вбудова цифрового водяного знаку в область дискретного вейвлет перетворення при форматі JPEG 2000

Найбільш актуальним напрямком на даний момент є вбудовування в область ДВП, при якому можна протистояти стиску з втратами при алгоритмі JPEG 2000. Вбудовування в область ДВП найбільше доцільно застосовувати у разі активного порушника.

Формат JPEG 2000 розроблявся ще давно з метою повністю замінити JPEG, але на даний момент цього не сталося. Незважаючи на те, що популярність зображень у форматі JPEG у мережі набагато вища, формат JPEG 2000 знайшов набагато ширше застосування.

Основні сфери застосування цього формату:

- зберігання стислих зображень високої якості під час передачі через мережу;
- цифровий кінематограф;
- 3D-візуалізація;
- охоронні системи (для стиснення зображень, одержуваних із цифрових відеокамер);
- клієнт-серверні взаємодії (бази даних зображень);
- для зберігання фотографій власника у біометричних паспортах;
- зберігання оцифрованих версій географічних карт;
- Зберігання медичних файлів.

Стандарт стиснення JPEG 2000 замість дискретного косинусного перетворення, що використовується в популярному форматі JPEG, використовує технологію ДВП, що базується на поданні сигналу у вигляді суперпозиції базових функцій хвильових пакетів. В результаті такої компресії зображення виходить гладкішим і чіткішим, а розмір файлу в порівнянні з JPEG при однаковій якості виявляється набагато меншим [5].

Виділимо головні переваги JPEG 2000 у порівнянні з JPEG:

- JPEG 2000 на низьких та високих бітрейтах має ступінь стиснення більший, ніж у формату JPEG. Це досягається завдяки використанню ДВП та складнішому ентропійному кодуванню.

- масштабованість фрагментів зображень. JPEG 2000 забезпечує безшовне стискування різних компонентів зображення. Завдяки розбиттю на блоки можна зберігати зображення різних дозволів в одному кодовому потоці.

- довільний доступ до кодового потоку (ROI). У форматі забезпечується кілька механізмів підтримки довільного доступу, також підтримується кілька ступенів розбиття на частини.

- гнучкий формат файлу: формати файлів JP2 і JPX забезпечують зберігання інформації про колірні простори, метадані та інформації для узгодженого доступу в мережевих програмах, що взаємодіють за допомогою протоколу JPEG Part 9 JPIP.

ДВП пропонує велику гнучкість при поданні зображення завдяки можливості вибору коефіцієнтів перетворення для зміни різних характеристик, таких як роздільна здатність та якість. Найбільш цінною є можливість представлення коефіцієнтів вейвлет-перетворення у цілих числах, у той час як у ДКП алгоритмах робота здійснюється з коефіцієнтами, представленими у вигляді чисел з плаваючою точкою, що призводить до помилок округлення при проміжних перетвореннях, наприклад, при масштабуванні. Таким чином, зміна роздільної здатності зображення або ступеня його компресії всередині інтегрованої системи кодування, заснованої

на ДВП, здійснюється без втрат, які були характерні для ДКП-перетворень. Більше того, ДВП є набір парних цифрових фільтрів, які можуть використовуватися для представлення зображення. За рахунок цього забезпечується можливість вибору фільтрових пар, що залежать від необхідної характеристики зображення – розміру та якості. У випадку з ДКП асоційована фільтрова система була фіксована, а для її зміни потрібно повторне кодування. Практично все програмне забезпечення на даний момент так чи інакше стосується роботи із зображеннями, функціонує з JPEG-2000.

Зображення піддається послідовностям вертикальних і горизонтальних одновимірних вейвлет перетворень, що чергуються. Спочатку перетворюються всі рядки, а потім усі стовпці. На наступному етапі ліва верхня чверть матриці, що вийшла в результаті попереднього перетворення, знову перетворюється. І так далі. Кількість етапів відповідає кількості рівнів вейвлет-декомпозиції. В результаті перетворення ми отримуємо безліч частотних діапазонів, які містять інформацію про те, як поводиться вихідний сигнал (зображення) при різній роздільній здатності. Обробляючи спеціальним чином частотні піддіапазони ДВП у вихідне зображення, можна вбудувати ЦВЗ.

3 АНАЛІЗ СТІЙКОСТІ ЦВЗ ДО ЗОВНІШНІХ ВПЛИВ

3.1 Вплив стиснення із втратами на зображення

Цифрові зображення з вбудованим ЦВЗ можуть бути схильні до навмисних змін або випадкових перешкод. Як було зазначено в попередньому розділі, зазвичай зображення викладаються в комп'ютерних мережах у форматах стиснення із втратами. Тому потрібно передбачити, щоб вбудований ЦВЗ був стійкий до подібного стиску. В результаті спотворень при вбудовуванні, впливу випадкових і навмисних перешкод передачі, а також похибок при вилученні відновлене одержувачем повідомлення відрізнятиметься від оригіналу, отриманий контейнер буде відрізнятися від вихідного. Також контейнер обов'язково буде спотворюватися при вбудовуванні повідомлення, що приховується. При збереженні зображення у форматі JPEG або JPEG 2000 вказується параметр якості, який визначається в деяких умовних одиницях, наприклад, від 1 до 100 або від 1 до 10. Більша кількість зазвичай відповідає кращій якості. Мале число відповідає більш сильному стиску. На рис. 3.1 показано вихідне растрове зображення великого розміру, далі стиснуте за алгоритмом JPEG 2000 та алгоритмом JPEG з однаковим коефіцієнтом якості.

Рисунок 3.1 – Початкове растрове зображення, стиснуте за JPEG 2000 та JPEG

Перше зображення має об'єм 226 кб, на другому і третьому об'єм зменшений до 16 кб. При цьому якщо уважніше подивитися на третє зображення у форматі JPEG, то можна побачити видимі неозброєним оком артефакти у вигляді ґрат 8x8. Третє зображення, стиснуте за алгоритмом JPEG 2000, якісніше, такими артефактами не має і більше схоже з вихідним зображенням. На рис. 3.2 можна побачити частину наведеного зображення стисненого з коефіцієнтом якості 30 за алгоритмом JPEG (ліворуч) з видимими артефактами та JPEG 2000 (праворуч).

Рисунок 3.2 – зображення, стиснуте за алгоритмом JPEG (ліворуч) та JPEG 2000 (праворуч) з однаковим коефіцієнтом якості

Після втрати частини інформації детектор може не виявити ЦВЗ, який представлений у вигляді бітової послідовності або може виявитись лише частина повідомлення. Тому потрібно заздалегідь передбачити, на яких коефіцієнтах якості ЦВЗ стабільно детектуватиметься. Потрібно використовувати техніку багаторазового дублювання ЦВЗ, що підвищить його стійкість до стиску з втратами, але повної гарантії безпеки ЦВЗ все одно домогтися не вдасться. Велику небезпеку для цілісності ЦВЗ становить стиснення JPEG 2000 за малих значень коефіцієнта якості, що призводить до значної втрати інформації зображення після стиснення. На рси 3.3 показані зображення з високим коефіцієнтом якості та з найнижчим. Зрозуміло, що

при стисканні як на правому зображення ЦВЗ буде найімовірніше втраченим для детектора.

Рисунок 3.3 – Зображення з високим коефіцієнтом якості JPEG 2000 та вкрай низьким

Зловмисник не зможе використовувати таке зображення з метою отримання прибутку і, у такому разі, чи не має в ньому нашого ЦВЗ.

3.2 Зовнішні впливи на зображення

Крім стиснення із втратами під час роботи із зображеннями користувач може в редакторі (наприклад, Adobe Photoshop) додати колірні фільтри, шум, обрізати краї, збільшити або зменшити зображення, перевернути або змінити формат. Наприклад, на рис. 3.4 для вихідного зображення зліва був застосований колірний фільтр і доданий шум.

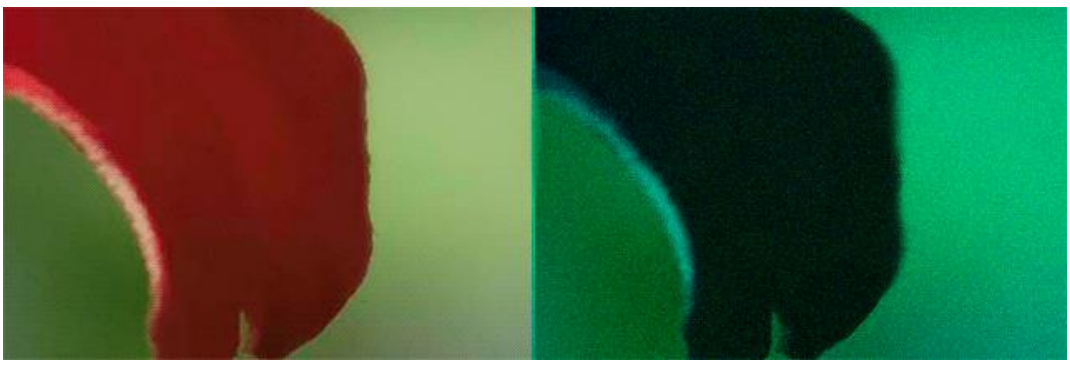

Рисунок 3.4 – Вихідне зображення та змінене

Подібна зміна не повинна призвести до знищення ЦВЗ, оскільки зображення зберегло комерційну цінність. ЦВЗ нічого очікувати і має бути стійкий до зовнішнього впливу на зображення-контейнер, у якому зображення буде зіпсовано остаточно. Якщо зробити високий колірний фільтр або вирізати більшу частину зображення, ЦВЗ буде втрачено. Але при цьому і саме зображення втратить комерційний вигляд, і його неможливо буде виставляти на продаж в інтернет-магазині. Подібне зіпсоване зображення показане рис. 3.5.

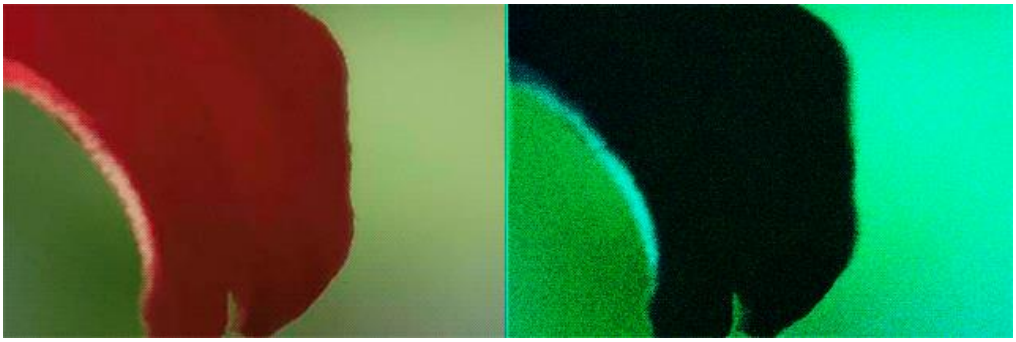

Рисунок 3.5 – Вихідне зображення та зіпсоване (велика кількість шуму та високий колірний фільтр)

Не завжди алгоритм вбудовування ЦВЗ буде стійкий до будь-яких із зазначених раніше зовнішніх впливів. Для подальшого аналізу необхідно визначитися з параметрами, які безпосередньо впливають на стійкість до зовнішніх впливів та рівень скритності.

3.3 Оцінка непомітності вбудови цифрового водяного знаку

Вбудовування ЦВЗ має здійснюватися з умови забезпечення скритності застосування. Як було зазначено вище, для вбудовування для захисту авторських прав не потрібно передбачати вкрай високий рівень скритності. Адже покращення скритності призведе до погіршення стійкості

до зовнішніх впливів. Ці дві характеристики залежить один від одного. Тому достатньо визначити рівень допустимих спотворень під час вбудовування. Процес застосування ЦВЗ має враховувати властивості системи сприйняття людини. Властивості СЛЗ можна розділити на дві групи: низькорівневі (фізіологічні) та високорівневі (психофізіологічні). На даний момент увагу варто приділяти обом групам властивостей.. У таблиці 3.1 представлені властивості СЧЗ та вплив їх на сприйняття зображень людиною

Таблиця 2.1 – Властивості СЛЗ та вплив їх на сприйняття зображень людиною

Властивість СЛЗ	Обґрунтування ефекту
Низькорівневі властивості СЛЗ	
Чутливість до зміни яскравості зображення	При малих значеннях яскравості СЛЗ поріг нерозрізненості зменшується, СЛЗ більше чутлива до шуму у цьому діапазоні.
Частотна чутливість	СЛЗ набагато сприйнятливіша до низькочастотного шуму, ніж до високочастотного. Це пов'язано з нерівномірністю амплітудно-частотної характеристики системи зору людини
Ефект маскування	Полягає у збільшенні порога виявлення сигналу в присутності іншого сигналу, що володіє аналогічними характеристиками. Найбільш сильно ефект маскування проявляється, коли обидва сигнали мають однакову орієнтацію та місцезнаходження.

Продовження таблиці 3.1

Високорівневі властивості СЧЗ	
Чутливість до контрасту	Висококонтрастні ділянки зображення і перепади яскравості звертають на себе більшу увагу.
Чутливість до розміру	Великі ділянки зображення помітніші за менші розміри. Але існує поріг насичення, коли подальше збільшення розміру не суттєво.
Чутливість до форми	Довгі та тонкі об'єкти звертають більше увага, чим кругліоднорідні.
Чутливість до кольору	Деякі кольори помітніші за інші. Цей ефект посилюється, якщо задній фон план відрізняється від кольору фігур на ньому.
Чутливість до розташування	Людина схильний в першу черга розглянути центр зображення.
Підвищене увага до зображення переднього плану	Люди уважніше до зображенням переднього плану, ніж заднього.
Чутливість до зовнішнім подразникам	Рух очей спостерігача залежить від конкретної обстановки, від отриманих перед переглядом або під час нього інструкцій, додатковоюінформації.

За допомогою побудови гістограм після впровадження ЦВЗ зображення з різними коефіцієнтами сили вбудовування можна побачити зміни яскравості та частотних характеристик. Гістограма є графіком статистичного розподілу елементів цифрового зображення з різною яскравістю, в якому по горизонтальній осі представлена яскравість, а по вертикалі відносне число пікселів з конкретним значенням яскравості. Вивчивши гістограму, можна

отримати загальне уявлення про правильність експозиції, контрасті та колірному насиченні знімка, оцінити необхідну корекцію та при подальшій обробці. Зловмисник, що має при собі засоби для професійної роботи із зображеннями, може досить легко побачити невідповідність рівня яскравості зображення.

Для проведення оцінки необхідно вибрати алгоритм вбудовування і здійснювати використання ЦВЗ у зображення змінюючи силу вбудованого сигналу. На рис. 3.7 наведено зображення без ЦВЗ і з вбудованим ЦВЗ за допомогою алгоритму Wang, де коефіцієнт сили вбудовування збільшений у півтора рази по відношенню до оптимального алгоритму. Як можна помітити, зі збільшенням параметрів вбудовування гістограма дуже відрізняється від вихідної.

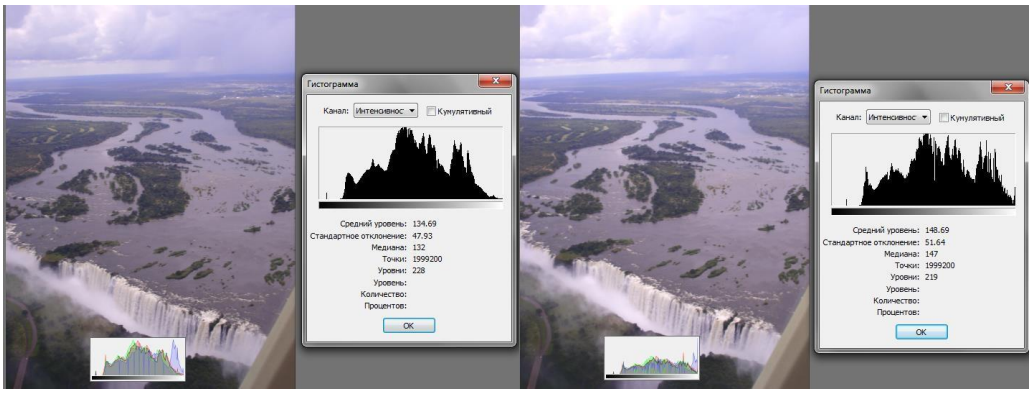

Рисунок 3.7 – Зображення без ЦВЗ та з ЦВЗ при збільшеному коефіцієнті сили вбудови

Використовуючи оптимальні параметри алгоритму, ми отримаємо гістограму, яка мало відрізняється від гістограми оригінального зображення.

Також для оцінки скритності застосування можна використовувати спосіб експертної оцінки, але він суб'єктивний. Тому у всьому світі використовуються суворіші математичні методи. Більшість показників спотворення відносяться до групи різницевих показників спотворення. Ці показники базуються на відмінності між оригінальним контейнером та контейнером із вбудованим ЦВЗ. Найбільш поширеним серед них є метод

обчислення пікового відношення сигналу до шуму, або peak signal to noise ratio (PSNR). Потрібно зробити розрахунок співвідношення між максимумом можливого значеннясигналу та потужністю шуму, спотворює значення сигналу. Як сигнал виступає зображення, а як шум – ЦВЗ. При порівнянні потужностях приховуваного сигналу і шуму кваліфікованим зловмисником легко виявиться факт наявності ЦВЗ. Отже, в стегосистемах доводиться ховати сигнал, що приховується, під великим за величиною шумом прикриття. PSNR визначається так:

$$PSNR = \frac{mn \cdot \max_{i,j}(I_{i,j})^2}{\sum_{i,j}(I_{i,j} - K_{i,j})^2} \qquad (3.1)$$

де m, n – розмір зображення;

$I_{i,j}$ – рначення пікселя зображення оригіналу;

$K_{i,j}$ – значення пікселя зображення після додавання шуму.

Зазвичай відношення сигнал/шум виявляється у децибелах. Нормальними значеннями для зображень після стиснення є значення від 25 до 50 дБ для різних груп зображень. Для темних оптимальним значенням є від 25 до 35 дБ, для середніх яскравостей цей діапазон буде від 30 до 40, а для світлих від 40 до 50 дБ. Досягти заданого рівня PSNR можна за допомогою зміни коефіцієнта сили вбудовування або розміру повідомлення, що вбудовується. При неможливості досягнення заданої величини PSNR шляхом зміни вибраного параметра необхідно визначити граничне значення параметра. Було проведено дослідження скритності застосування для алгоритмів Wang, Ouled-Zaid, Makhloufi & Olivier, Chirag-Ganesh та Li & Zhang. Для різних груп зображень було виявлено, що при вбудовуванні однакових ЦВЗ при оптимальному вказаному в алгоритмі коефіцієнті сили вбудовування їхнє відношення сигналу і шуму зі збільшенням стиснення

буде збільшуватися. Результати показані у таблиці 3.2.

Таблиця 3.2 - Оцінка скритності застосування

Алгоритм	Група зображень	Коефіцієнт якості JPEG 2000, %	Співвідношення сигнал/шум, дБ
Chirag-Ganesh	Світлі	50 70 90	51.5 48.9 46.2
	Середні по яскравості	50 70 90	40.3 37.3 35.1
	Темні	50 70 90	34.7 31.9 27.3
Li & Zhang	Світлі	50 70 90	49.2 47 45.5
	Середні по яскравості	50 70 90	39.8 36.4 33.6
	Темні	50 70 90	34.1 31 27.6
Wang	Світлі	50 70 90	47.8 46.5 43
	Середні по яскравості	50 70 90	38.4 35 32
	Темні	50 70 90	33.5 30.2 26.6
Ouled-Zaid, Makhloufi & Olivier	Світлі	50 70 90	52.2 49.4 46.7
	Середні по яскравості	50 70 90	41.4 37.8 36.5
	Темні	50 70 90	36.4 32.9 28.2

Як можна побачити з таблиці, впровадження ЦВЗ у зображення з більшим ступенем стиснення призводитиме до все більшої втрати скритності впровадження та виявлення артефактів від вбудови. У цьому оптимальний рекомендований коефіцієнт сили вбудовування вони різниться друг з одним.

3.4 Оцінка пропускної здатності зображення-контейнера.

Зображення мають різний об'єм, тип і кількість областей, куди може бути впроваджено ЦВЗ, враховуючи умову забезпечення оптимального рівня скритності впровадження. Крім того, різні стегоалгоритми будуть здійснювати впровадження інформації в певні види зображень і області в них. Зображення можуть бути напівтоновими, бінарними, повнокольоровими тощо. На рис 3.8 показані різні типи зображень.

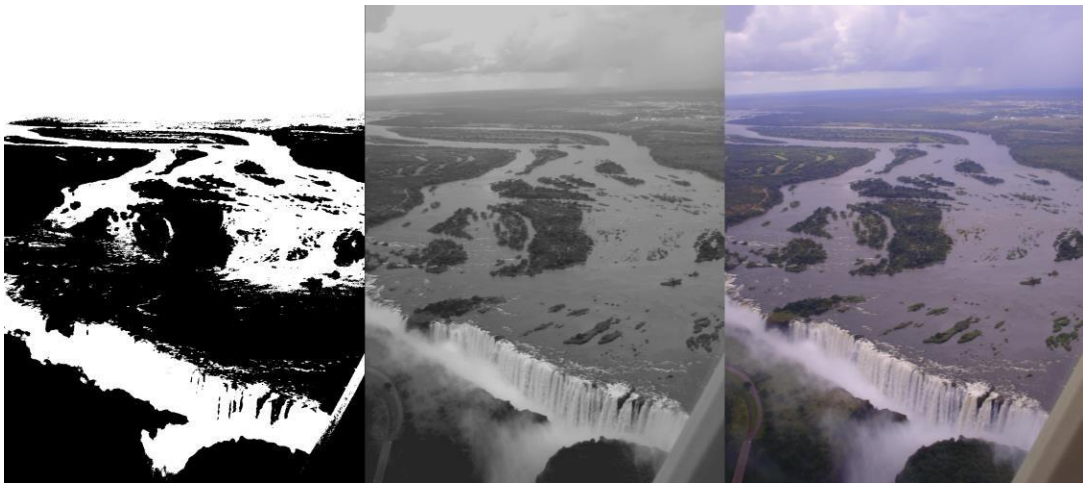

Рисунок 3.8 – Бінарне, напівтонове та кольорове зображення

Розроблений для напівтонових зображень алгоритм може демонструвати погані показники стійкості або виявитися непридатним для використання з кольоровими зображеннями. Тому необхідно оцінити заздалегідь визначитися з типом зображень та його пропускної спроможністю. Для подальших досліджень я використовуватиму саме

кольорові растрові зображення, тому що саме вони найчастіше представляють комерційну цінність і виставляються на продаж. Під пропускною здатністю каналу передачі повідомлень, що приховуються, будемо розуміти максимальну кількість інформації, яка може бути вкладена в один елемент контейнера виходячи з умови збереження знайденого оптимального рівня скритності, стійкості до зовнішніх впливів і безпомилковості детектування. При цьому ЦВЗ повинен бути захищений від атак порушника, таких як спроби читання повідомлень, що приховуються, навмисного введення помилкових повідомлень або руйнування вбудованої в контейнер інформації без втрати комерційного вигляду контейнера. Різні зображення-контейнери можуть мати абсолютно різні характеристики. Для отримання адекватних результатів оцінки стійкості необхідно провести вибір відповідних зображень та провести аналіз пропускної спроможності контейнера. Прихована пропускна здатність визначатиметься як:

$$C = 0.5 * \log_2(1 + \frac{\sigma_M^2}{\sigma_{\tilde{X}}^2 + \sigma_P^2}) \qquad (3.2)$$

де σ_M^2 – потужність вбудованого сигналу;

$\sigma_{\tilde{X}}^2$ – потужність контейнера;

σ_P^2 – потужність шуму при стисненні;

При здійсненні вкладення інформації, що приховується в контейнер допускається спотворення вихідного зображення до величини пікового відношення сигнал/шум, який був вирахований до цього вище. Кількість біт/піксель для звичайного JPEG 2000 зображення становить 25.

Для подальших розрахунків буде використовуватися комплекс Matlab, який надає чудові можливості цифрової обробки зображень. За допомогою комплексу Matlab можна зробити розрахунки за потужністю контейнера та шуму. Розподіл шуму стиснення відбувається за гаусівським законом.

Проведемо оцінку пропускної спроможності зображення JPEG 2000 з показником якості 50%. Для проведення оцінки використовуватиметься алгоритм вбудовування Chirag-Ganesh. Коефіцієнт сили вбудови будуть використовуватися, як зазначено в описі алгоритму. Тоді якщо взяти світле зображення з розмірами 1000x800 та розміром 900 кб, використовуючи вбудовуи ЦВЗ за алгоритмом Chirag-Ganesh, можна розрахувати $\sigma_{\tilde{X}}^2$, яка буде дорівнювати 56. Тоді допустима потужність прихованого повідомлення дорівнює σ_M^2=7, а σ_P^2=6.7.

Підсумкова пропускна здатність становитиме C=2146 біт. Треба сказати, що для систем вбудовування ЦВЗ висока ємність вбудовування менш важлива на відміну від систем прихованої передачі даних. Пропускна здатність для чотирьох вибраних під час огляду алгоритмів була вирахована для 5 різних розмірностей зображення за різних ступенів коефіцієнта якості JPEG 2000 і результати показані в таблиці 3.3. Спотворення вихідного зображення при вбудовуванні ЦВЗ і стиснення з втратами до величини пікового відношення сигнал/шум становитиме 46,8 дБ. Таке спотворення буде непомітно на око, як було досліджено вище.

Таблиця 3.3 – Оцінка пропускної спроможності

Алгоритм	Розміри зображення, пікселі	Коефіцієнт якості JPEG 2000, %	Загальна прихована пропускна здатність зображення, біт
Chirag-Ganesh	521x512	50	936
		70	1205
		90	1491
	640x520	50	1336
		70	1588
		90	1687
	800x800	50	1660
		70	1966
		90	2175
	1000x800	50	2246
		70	2544

Продовження таблиці 3.3

		90	2870
	3400x2200	50	16010
		70	16950
		90	18106
Li & Zhang	521x512	50	1256
		70	1420
		90	1650
	640x520	50	1465
		70	1640
		90	1870
	800x800	50	1984
		70	2110
		90	2400
	1000x800	50	2594
		70	2830
		90	3050
	3400x2200	50	16330
		70	18030
		90	19800
Wang	521x512	50	940
		70	1020
		90	1250
	640x520	50	1020
		70	1210
		90	1480
	800x800	50	1680
		70	1930
		90	2220
	1000x800	50	2030
		70	2205
		90	2440
	3400x2200	50	11970
		70	13650
		90	14340

Як можна побачити з таблиці, при стисненні зображень з більш високим коефіцієнтом стиснення потужність шуму стиснення суттєво зростає, і при цьому прихована пропускна здатність зменшується. При збільшенні шуму обробки при стисненні зображень величина прихованої

пропускної здатності зменшується плавно

3.5 Оцінка стійкості вбудованої інформації до зовнішніх впливів

Визначивши оптимальний рівень прихованої пропускної спроможності та скритності застосування можна переступити до оцінки стійкості до зовнішніх впливів, у яких ці рівні нічого очікувати порушуватися. Але для початку потрібно визначитися з тестовими даними, що застосовуються зовнішніми впливами та методикою проведення цієї оцінки. Існує безліч зовнішніх впливів, які ми можемо застосувати до зображення, як було сказано на початку глави. При проведенні аналізу важливо дотримуватися однакового діапазону інтенсивності впливу. Крім того, зовнішньому впливу має бути піддано все зображення-контейнер. Спочатку потрібно задати мінімальне значення зовнішнього впливу та крок, з яким воно змінюватиметься. Вбудовування має проводитися з урахуванням збереження оптимальних параметрів скритності застосування. Як було вже визначено вище, для кожної групи зображень він відрізнятиметься за різних алгоритмів. При впровадженні використовуватиметься коефіцієнт сили вбудовування, при якому буде збережено оптимальний рівень скритності для кожного алгоритму. Для проведення дослідження використовується комплекс MATLab, як і в попередніх пунктах глави. Він надає хороші засоби для цифрової обробки зображень та автоматизування завдання застосування зовнішніх впливів з певним кроком його зміни та побудови результуючого графіка.

Визначення стійкості ЦВЗ до зовнішніх впливів на зображення-контейнер складається з наступних кроків:

1. ЦВЗ впроваджується у зображення-контейнер.
2. Контейнер зазнає зовнішнього впливу.
3. ЦВЗ витягується із зображення-контейнера.

4. Вилучений ЦВЗ порівнюється з оригінальним, і визначається ступінь їхньої відповідності.

Оцінка стійкості виконуватиметься за допомогою коефіцієнта помилкових біт (Bit Error Rate). Коефіцієнт помилкових біт чудово підходить для оцінки спотворень у бітовій послідовності, яку в даному випадку і є ЦВЗ. Обчислюється цей коефіцієнт за формулою:

$$BER(S, S1) = \frac{\sum p_i}{N}, p_i = \begin{Bmatrix} 1, S \neq S1 \\ 0, S = S1 \end{Bmatrix} \quad (3.3)$$

де S - j-й біт оригіналу рядка, що вбудовується;

S1 - біт витягнутого рядка;

N - загальна кількість біт.

При значенні коефіцієнта, що дорівнює 0, впроваджена та вилучена інформація повністю ідентичні. При значенні, що дорівнює 1, кожен біт оригіналу не відповідає вилученому. Для бітового рядка ACII символів значення BER більше 0.12 означає втрату більшу частину вбудованої інформації, тобто можна говорити, що ми зможемо відновити вихідний ЦВЗ.

3.6 Результати аналізу стійкості ЦВЗ до зовнішніх впливів на зображення-контейнер

Дослідження проводилося для чотирьох алгоритмів вбудовування в область ДВП, які були обрані під час практичних досліджень. Це алгоритми Wang, Ouled-Zaid, Makhloufi & Olivier, Chirag-Ganesh та Li & Zhang. Для більш точної оцінки вироблятимемо її на різних зображеннях, які будуть мати однаковий розмір. Було вибрано 4 світлі, 4 темні та 4 середні за яскравістю растрові зображення з розмірами 1000x800 пікселів. Як ЦВЗ краще використовувати псевдовипадкову інформацію однакового розміру, яка не перевищуватиме рівня максимальної прихованої пропускної здатності

для зображення. Вирішили використовувати ЦВЗ в 1024 біт.

Як зовнішні впливи було вирішено використовувати найбільш популярні дії щодо зміни зображень: зашумлення зображення білим гауссівським шумом, масштабування, стиснення JPEG 2000 з втратами, вирізування частини та фільтрація. Всі ці дії сильно спотворюватимуть зображення. Після проведення оцінки для одного типу зовнішнього впливу дані отримані для різних зображень трохи відрізнятимуться, тому вони будуть усереднюватися для підсумкової оцінки.

Для перевірки стійкості до стиснення JPEG 2000 зображення з вбудованим ЦВЗ піддавалося стиску у всьому діапазоні значень коефіцієнта якості JPEG 2000 від 0 до 100. Глибина виконання ДВП для всіх алгоритмів була обрана трирівневою, а вбудовування здійснювалося в піддіапазони максимально. Результати показані рис. 3.10. По вертикальній осі відкладаються значення коефіцієнта BER, а горизонтальної значення коефіцієнта якості JPEG 2000. Для зручності на графіку горизонтальною пунктирною лінією показаний граничний рівень BER=0.12, у якому ми зможемо відновити вбудовану інформацію. Найкращі показники стійкості до ДВП мають алгоритми Chirag-Ganesh та Ouled-Zaid, Makhloufi & Olivier. Вбудовування ЦВЗ відбувається в низькочастотні LL та LH піддіапазони при цих алгоритмах. Алгоритм Wang, бітового потоку, показує кращі результати. Тобто можна сказати, що при вбудовуванні ЦВЗ в низькочастотні піддіапазони буде досягнуто більшого показника стійкості до стиснення з втратами JPEG 2000.

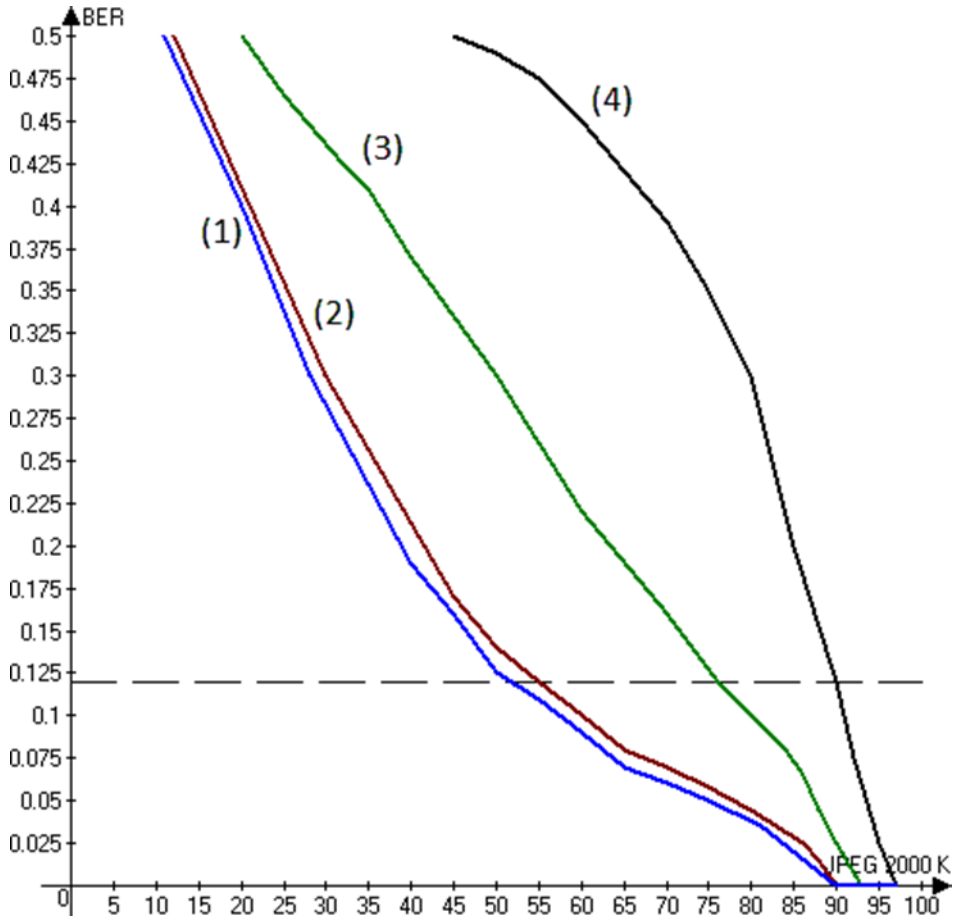

Рисунок 3.10 – Оцінка стійкості ЦВЗ до стиснення JPEG 2000 із втратами ((1) – алгоритм Ouled-Zaid, Makhloufi & Olivier, (2) – алгоритм Chirag-Ganesh, (3) – алгоритм Li & Zhang, (4) –алгоритм Wang).

Для аналізу змін вейвлет коефіцієнтів при зашумленні зображення вносився гаусівський шум з нульовим середнім значенням та різними значеннями відхилення, що змінюються від 0 у бік зростання, доки деградація зображення не досягла неприйнятного рівня для використання. Результати показані рис. 3.11. Найкращою стійкістю до цього виду впливу показав алгоритм Li&Zhang. Треба сказати, що ці алгоритми демонструють приблизно однаково слабкі показники стійкості до цього виду зовнішнього впливу.

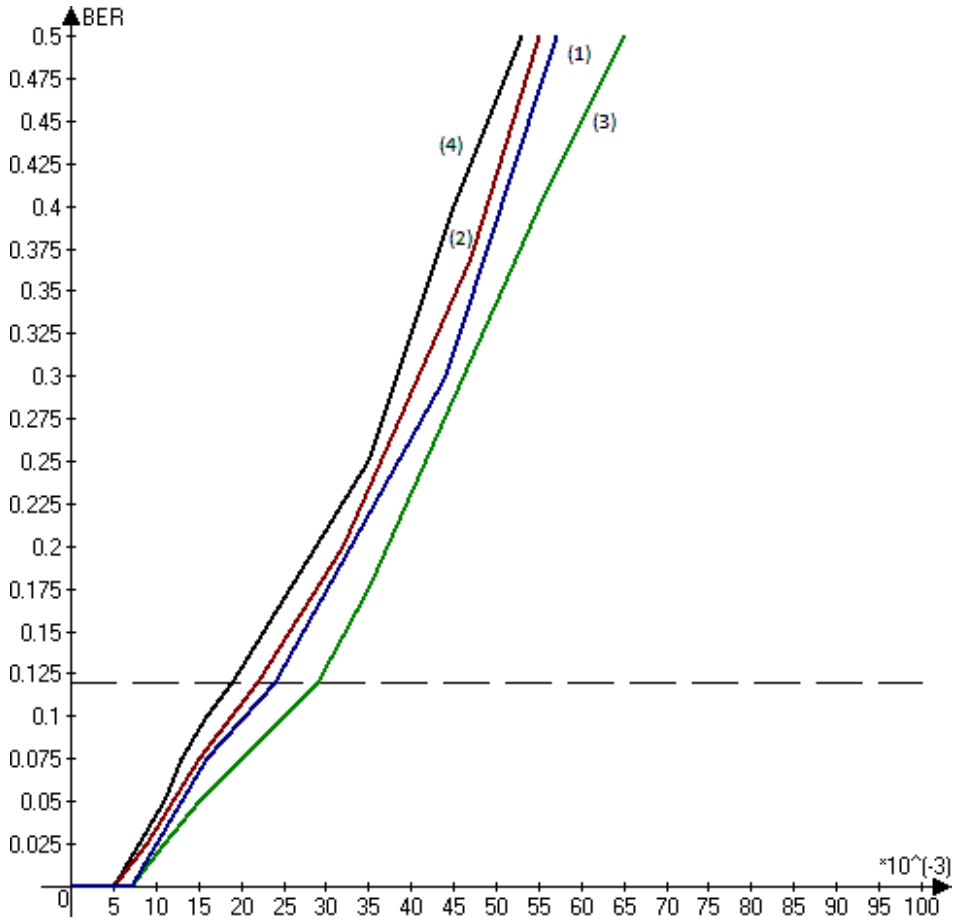

Рисунок 3.11 – Стійкість ЦВЗ до зашумлення ((1) – алгоритм Ouled-Zaid, Makhloufi & Olivier, (2) – алгоритм Chirag-Ganesh, (3) – алгоритм Li & Zhang, (4) – алгоритм Wang)

У результаті експерименту з масштабуванням зображення-контейнер стискалося до різних розмірів до 8 раз. Зчитувати повідомлення зі стисненого зображення неприйнятно, не зменшивши розмір блоків, на які розбивається зображення. Зображення відновлювалося до вихідного розміру, і лише потім виконувалося зчитування ЦВЗ. Тільки за алгоритму Quled-Zaid, Makhloufi & Olivier вдалося повністю відновлювати ЦВЗ при стисканні в 3 рази. Для інших алгоритмів граничним значенням, у якому BER менше 0.12, є стиск у 2 разу. Всі ці алгоритми виявилися не особливо стійкими до такого виду дії.

Для аналізу стійкості ЦВЗ при фільтрації з великої різноманітності фільтрів для цифрових зображень було обрано контрастний фільтр, що підвищує різкість зображення. У редакторах зображень діапазон зміни зазвичай представляється від -100 до 100, але оцінки було проведено

дослідження у діапазоні зміни від 0 до 100. Результати показані рис. 3.12. Найкращі результати показав алгоритм Quled-Zaid, Makhloufi & Olivier.

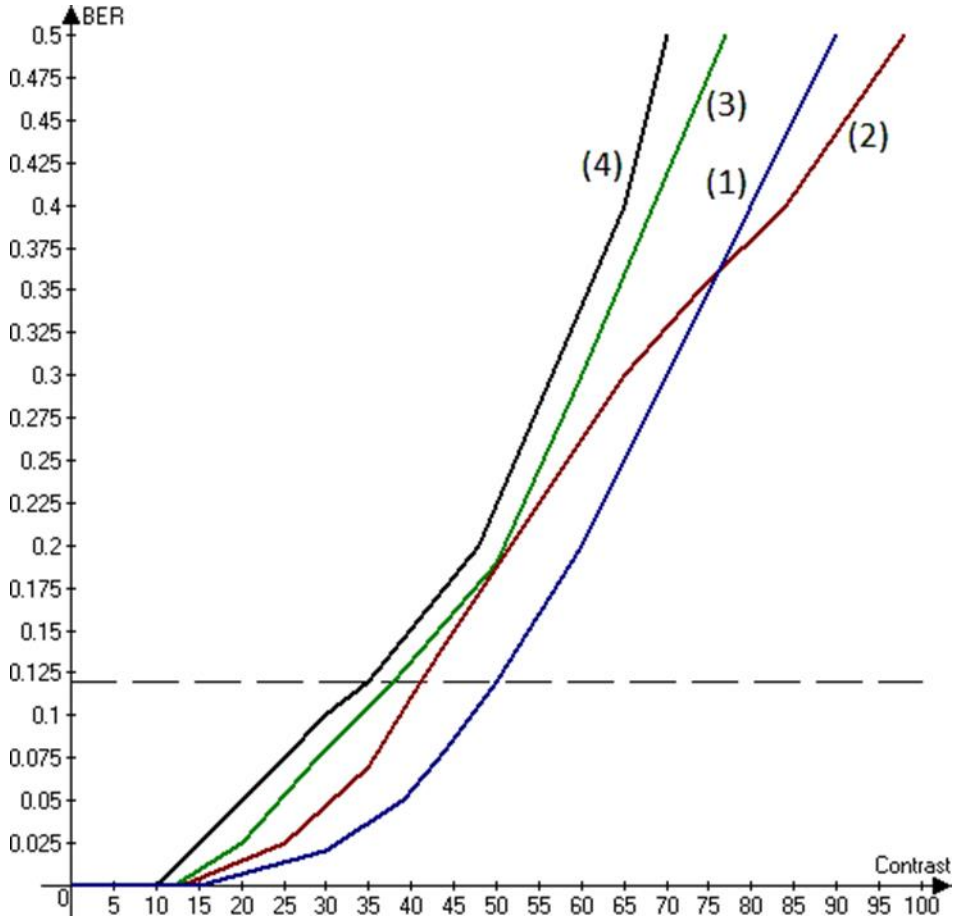

Рисунок 2.12 – Стійкість ЦВЗ до фільтрації ((1) – алгоритм Ouled-Zaid, Makhloufi & Olivier, (2) – алгоритм Chirag-Ganesh, (3) – алгоритм Li & Zhang, (4) – алгоритм Wang)

Для аналізу стійкості до вирізування частини зображення було обрано діапазон зміни від 0 до 80% з кроком 10%. Зрозуміло, що можна обрізати з усіх боків зображення, тільки з однієї або взяти область в середині, і при цьому ми найімовірніше отримаємо різні результати при оцінці. Було вирішено робити вирізку частини зображення ліворуч, ділячи вертикально нову область для відсікання. Алгоритм Wang виявився погано стійким до подібного впливу. Вирізання більше 10% зображення призвело до втрати ЦВЗ. Вбудовування при алгоритмі Li & Zhang показало різні результати для різних зображень, але у всіх випадках вирізування понад 20% виявилося

фатальним. Алгоритми Chirag-Ganesh та Ouled-Zaid, Makhloufi & Olivier виявилися більше стійкими до подібного виду впливу, і відновити повідомлення вдалося при вирізанні 30% зображення.

Підбивши підсумки, можна сказати, що алгоритми, де вбудовування здійснюється в низькочастотні піддіапазони, мають кращі показники стійкості до зовнішніх впливів. Проте вони мають менші показники по скритності впровадження. Усі з досліджуваних алгоритмів виявилися погано стійкі до зашумлення та масштабування. Показники при стиску JPEG 2000 виявилися несподівано невисокими.

4 АЛГОРИТМ ПІДВИЩЕННЯ СТІЙКОСТІ ЦВЗ ДО ЗОВНІШНИХ ВПЛИВ НА ЗОБРАЖЕННЯ-КОНТЕЙНЕР

4.1 Алгоритм вбудовування ЦВЗ під час стадії квантування

При докладному дослідженні векторного квантування було знайдено можливість заміни класичних компонентів квантування із сітчастою геометрією в JPEG 2000 кодері та декодері на гібридний модуль, який зможе виконувати одночасно квантування та впровадження водяного знаку. Така техніка не залежатиме від шляхів у решітці і дозволить одночасно квантувати вейвлет коефіцієнти та вбудовувати ЦВЗ без інтеграції додаткових стадій для впровадження ЦВЗ у ланцюзі кодування/декодування JPEG 2000. Схема спільної схеми вбудови водяних знаків під час кодування JPEG 2000 показано рис. 4.1.

Рисунок 4.1 – Сполучена з квантуванням схема вбудовування ЦВЗ

Одним із найважливіших параметрів для розгляду є вибір вейвлет-

коефіцієнтів, які мають бути включені до процесу впровадження ЦВЗ. Специфікація алгоритму JPEG 2000 визначає, що коефіцієнти низькочастотних піддіапазонів ДВП зазнають менших змін, ніж коефіцієнти високочастотних піддіапазонів рівного рівня розкладання. З іншого боку, зміна коефіцієнтів високочастотних піддіапазонів менше впливає якість зображення. Після вейвлет розкладання, LL піддіапазони з низькими частотами є найбільш значущими даними в перетвореному зображенні. Щоб уникнути значного погіршення якості у реконструйованому зображенні, вирішено не використовувати вейвлет коефіцієнти цього поддиапазона процесу вбудовування ЦВЗ. Було вирішено впроваджувати ЦВЗ у HL, LH та HH детальні піддіапазони двох найвищих вибраних рівнів розкладання. Незважаючи на те, що ці піддіапазони зазнають великих змін при квантуванні, зі збільшенням рівня вейвлет-розкладання вдасться досягти балансу в скритності застосування за рахунок не використання LL піддіапазонів, і стійкості до зовнішніх впливів. Корисне навантаження ЦВЗ визначається кількістю детальних піддіапазонів, які включені в процес нанесення водяного знака. Корисне навантаження збільшується, коли ми додаємо більше детальних піддіапазонів з новим вибором рівня Корисне навантаження ЦВЗ визначається кількістю детальних піддіапазонів, які включені в процес нанесення водяного знака. Корисне навантаження збільшується, коли ми додаємо більше детальних піддіапазонів з новим вибором рівня Корисне навантаження ЦВЗ визначається кількістю детальних піддіапазонів, які включені в процес нанесення водяного знака. Корисне навантаження збільшується, коли ми додаємо більше детальних піддіапазонів з новим вибором рівня дозволу. Передбачається використання трирівневого вейвлет-розкладання під час проведення початкового ДВП. Вбудовування бітів ЦВЗ має проводитися в безліч коефіцієнтів різних піддіапазонів, щоб ЦВЗ був стійкий при вибраному процесі квантування і міг бути відновлений.

Для застосування ЦВЗ необхідно замінити єдині квантувачі, що використовуються в другій стадії кодування JPEG 2000, зсуваючи квантувачі

з розміром кроку Δ, як і для оригінальних квантувальників. Також можемо використовувати вищий розмір кроку шляхом множення оригінального на константу. Ці квантувачі відрізняються від попередніх квантувачів запровадженням зсуву d, який псевдовипадково виходить при рівномірному розподілі на [-Δ/2, Δ/2].

Формула здійснення вбудови біта ЦВЗ буде такою:

$$D' = \begin{cases} D_j^0(d_0), m_i = 0 \\ D_j^1(d_1, |d_0 - d_1| = \frac{\Delta}{2}), m_i = 1 \end{cases} \quad (4.1)$$

де D' – вибраний квантувач;

d_0, d_1 – зсув;

Δ – розмір кроку квантування;

m_i – біт повідомлення, що вбудовується

Тобто якщо біт вбудови дорівнює нулю, то використовується квантувач D_j^0 (j=0, 1, 2, 3) зі зсувом d_0. Якщо біт дорівнює 1, то використовуємо квантувач D_j^1 зсувом d_1 і задовольняє умову $|d_0 - d_1| = \frac{\Delta}{2}$.

Для кожного переходу в решітці побудовано два зсуви $d_0[i]$ і $d_1[i]$ і чотири об’єднаних квантователя. Таким чином, є дві групи об'єднаних квантувальників для сітчастої структури, які використовуються в нашому підході: групи 0, яка складається з усіх зрушених об'єднаних квантувальників, що використовуються для вбудовування біта 0 водяного знака і групу 1, яка включає зрушені об'єднані квантувачі для вбудовування біта 1.

Структура решітки, що використовується в запропонованому способі, має чотири гілки, що проходять по кожному її стану. Для кожного стану, два об'єднані квантувачі замість одного пов'язані з декількома вихідними гілками цього стану. Коефіцієнтом сили вбудовування за такого алгоритму

виступатиме саме крок квантувача. При його збільшенні стійкість до зовнішніх впливів зростатиме, а скритність падатиме. На рис. 4.2 показана подібна одноступінчаста структура решітки, яка використовується для вбудови ЦВЗ під час стадії квантування.

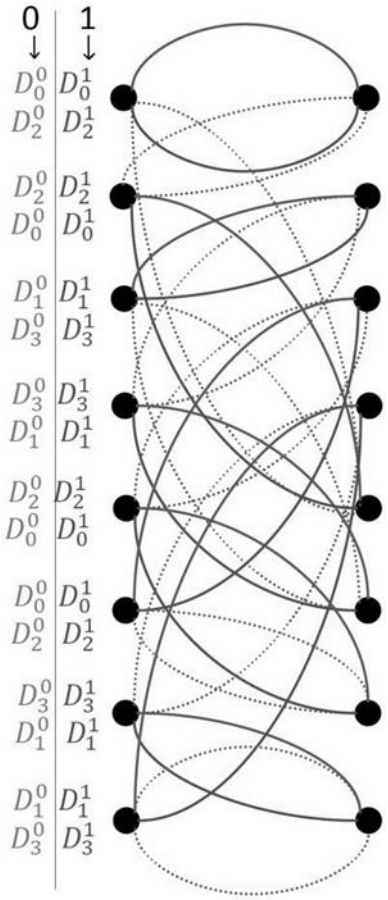

Рисунок 4.2 – Одноступінчасті грати з групами 0 та 1 об'єднаних квантувальників.

Функція вбудовування F(x, m) впроваджує ЦВЗ m зображення x, після якого виходить зображення з ЦВЗ x'. Функція виражена такою формулою:

$$F(x[i], m[i]) = \left(\left[\frac{x[i] - d_{m[i]}}{\square} \right] \right) \square + d_{m[i]} \qquad (4.2)$$

де dm[i] – зсув обраного квантувача на розмір кроку □;

m[i] – вбудований біт під час переходу i.

Процес впровадження ЦВЗ і двох кроків до виконання вбудовування в JPEG 2000. Перший крок виконується протягом стадії квантування процесу стиснення JPEG 2000. Для кожного переходу і у решітці, об'єднані квантувачі обрані відповідно до значення m[i]. Решітка, таким чином, модифікується для того, щоб видалити всі гілки, які не позначені об'єднаними квантувачами, які кодують повідомлення. Підмножини $D_{i,j}^{m[i]}$ (j=0, 1, 2, 3) пов'язані з гілками модифікованої решітки. Індекс квантування q[i] буде розрахований за формулою:

$$q[i] = \text{sing}(\text{x[i]-d}_{\text{m[i]}}\text{[i]})\left\lfloor \frac{\text{x[i]-d}_{\text{m[i]}}\text{[i]}}{\square} \right\rfloor \qquad (4.3)$$

де $\text{d}_{\text{m[i]}}\text{[i]}$ – додаткове змішення вже зміщеного квантувача.

На другому етапі здійснюється етап зворотного квантування при процесі декомпресії JPEG 2000. Ґрати повинні бути скорочені для того, щоб отримати ті ж ґрати, що використовуються при першому кроці процесу вбудовування водяних знаків. Відновлення значень зображення із вбудованим ЦВЗ x' проводиться наступним чином:

$$x' = \sin g(q[i])(|q[i]| + \delta)\Delta + d_{m[i]}[i] \qquad (4.4)$$

де b є параметром, що вибирається користувачем у межах 0<b<1 (зазвичай він дорівнює 0.5).

Вбудова ЦВЗ здійснюється у різні частини шляхів. ЦВЗ вбудовується оптимально, застосовуючи процедуру ітерацій з обмеженням мінімізації сприйняття відстані та підтримання постійної надійності. Кодове слово визначається за допомогою кореляції чи квантування. Таким чином, ЦВЗ матиме підвищену стійкість до стисненню з втратами, і при цьому зберігатиме високу скритність впровадження. Блок-схема алгоритму

вбудовування наведено рис. 4.3.

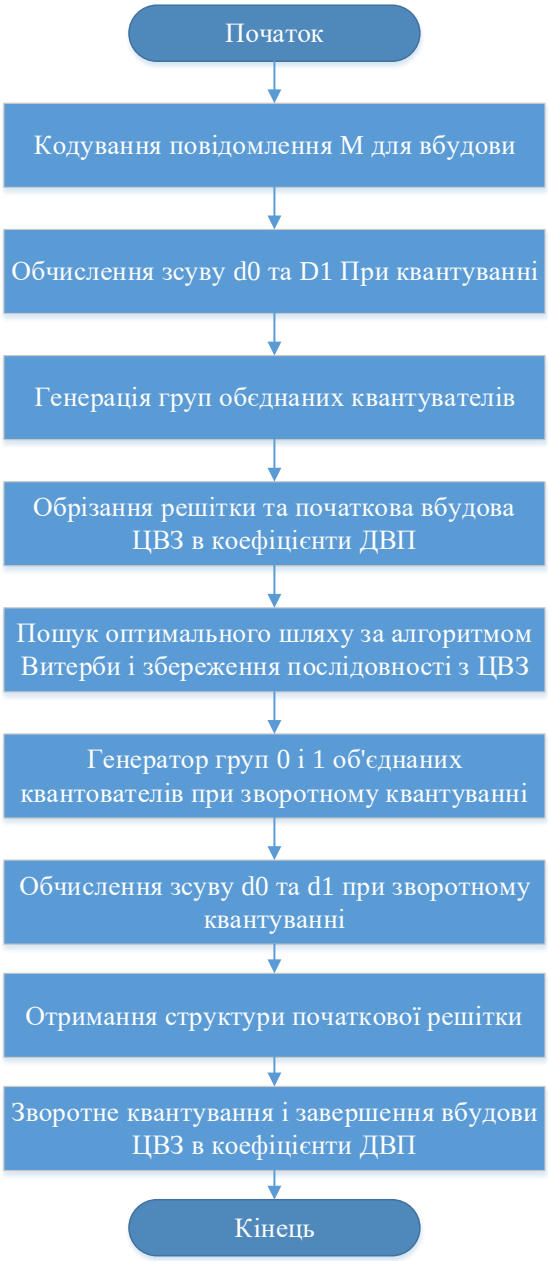

Рисунок 4.3 – Блок-схема алгоритму вбудовування ЦВЗ під час стадії квантування

Процес застосування водяного знака здійснюється незалежно кожного блоку коефіцієнтів підлягають кодування. Щоб додати більше надійності повідомленню, його можна кодувати завадовим кодом. Після цього перемішуються псевдовипадково біті в закодован повідомлення із секретним

ключем. Для кожного кодового блоку процедура квантування та вбудовування ЦВЗ здійснюється наступним чином:

Обчислення зсувів d0 та d1: ми використовуємо псевдовипадковий генератор для ініціалізації секретного ключа k та обчислення зрушень.

Генерація груп 0 і 1 об'єднаних квантувальників: для кожного переходу ми зрушуємо квантувачі. Ми помічаємо гілки ґрат для цих квантувальників.

Обрізка ґрат: решітка спрощується настільки, що всі гілки, що йдуть через ґрати, і всі пов'язані з об'єднаними квантувачами, кодують повідомлення m. Для кожного переходу, ми зберігаємо посилання на кількість гілок, що збереглися. Ми отримаємо послідовність J.

Пошук оптимального шляху: початковий стан цієї структури решітки встановлено 0. Алгоритм Вітербі застосовується у тому, щоб знайти мінімальні спотворення траєкторії. Обчислюються індекси квантування. Послідовності J об'єднані у послідовність J1. Отримана послідовність після кодується та зберігається у файлі, який передається у спільний декодер як стороння інформація.

Вбудовування водяного знака завершується протягом зворотного квантування стадії декомпресії JPEG2000. Бітовий потік зображення декодується EBCOT декодером, щоб отримати послідовність декодованих індексів квантування. Для кожного кодового блоку виконуються такі кроки зворотного квантування:

Обчислення зсувів d0 та d1.

Генерація груп 0 та 1 об'єднаних квантувальників.

Отримання структури решітки, що використовується на етапі квантування: генерується структура решітки з чотирма гілками, що проходять через кожен стан. Кожна гілка грат має після помічені зрушення квантувачів і посилання. Послідовність J дозволяє отримати обрізані ґрати, які використовувалися на стадії квантування. Для кожного переходу і у решітці, обрізка визначається шляхом видалення гілок, які мають посилання на нерівну послідовність.

Зворотне квантування: решітки, що обрізають, використовується для відновлення вейвлет коефіцієнтів. З огляду на квантовані індекси, закінчується вбудовування водяного знака під час обчислень реконструйованих вейвлет коефіцієнтів.

Враховуючи, що ми виробляємо вбудовування, інтегроване в ланцюг кодування JPEG 2000, буде збільшена швидкість впровадження в порівнянні з алгоритмами, які не інтегровані в схему JPEG 2000. Але мінусом подібного вбудовування є те, що його можна використовувати тільки при початковому стисненні зображення з втратами. Якщо увімкнути режим без стиснення з втратами під час перетворення зображення, то режим квантування буде вимкнений і вбудовування не буде здійснено.

Для зчитування повідомлення потрібно застосувати дискретне вейвлет-перетворення зображення. Кожен піддіапазон, який має вбудоване повідомлення, розбити на блоки такого ж розміру, як і при кодуванні. Коефіцієнти, що належать поточному блоку, зберігатимуться у векторі. Для кожного оброблюваного блоку потрібно витягти за допомогою секретного ключа зрушення d0 і d1 і виконати квантування на всю решітку. Це допоможе ідентифікувати шлях, яким даються мінімальні спотворення квантування між вектором і вихідними кодовими словами. Закодоване повідомлення відновлюється, після чого ми перемішуємо назад біти та використовуємо розшифровку для отримання вихідного повідомлення. Алгоритм зчитування бітів є зворотним алгоритмом вбудовування. При цьому сама схема не вимагає наявності оригінального зображення для знаходження коефіцієнтів, у які відбулося вбудовування (сліпа). Блок-схема алгоритму зчитування ЦВЗ показано рис. 4.4.

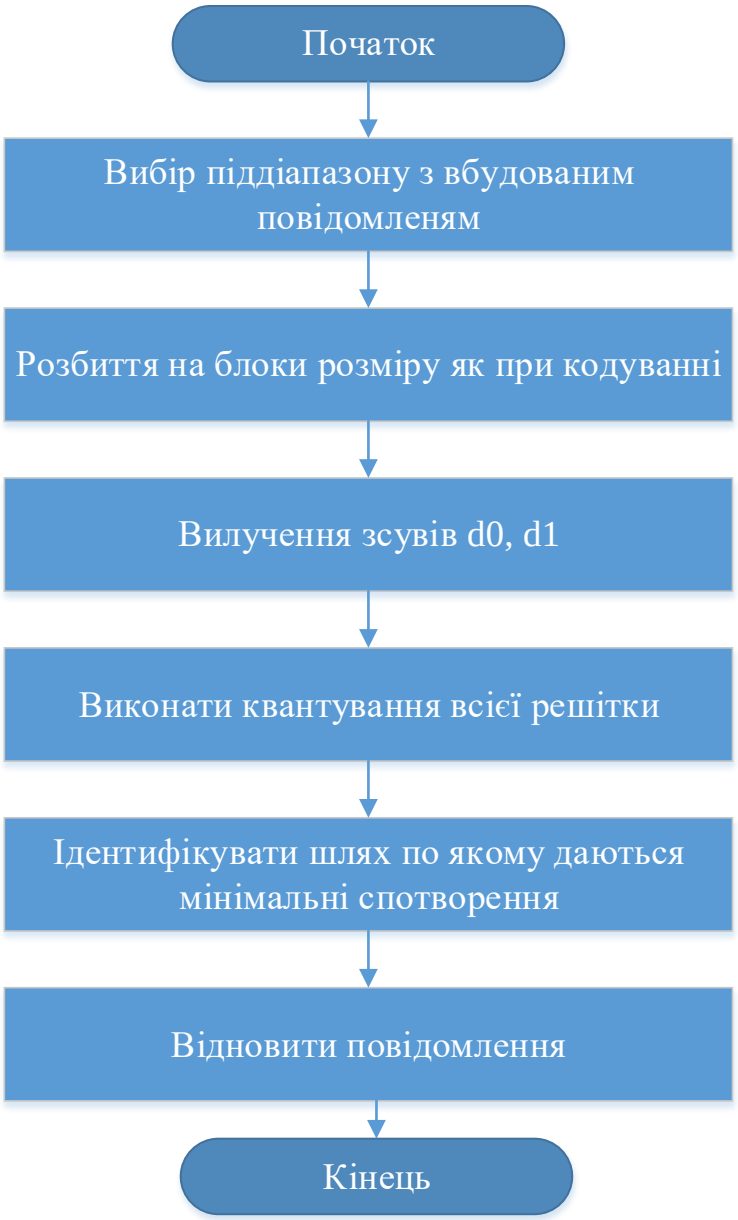

Рисунок 4.4 – Алгоритм зчитування ЦВЗ

4.2 Аналіз стійкості ЦВЗ до зовнішніх впливів на зображення-контейнер

Для оцінки стійкості створеного алгоритму буде використано методику з другого розділу. Значення за різними зображеннями будуть усереднюватися. Для початку треба розібратися зі значеннями скритності застосування та оцінкою пропускної спроможності. Результати з оцінки скритності застосування показані у таблиці 4.1.

Таблиця 3.1 - Оцінка непомітності при вбудові ЦВЗ

Група зображень	Коефіцієнт якості JPEG 2000,%	Співвідношення сигнал/шум, дБ
Світлі	50	48.4
	70	46.9
	90	43.5
Середні по яскравості	50	38.7
	70	35.3
	90	32.3
Темні	50	33.3
	70	31.2
	90	26.9

Ці результати виявилися трохи гіршими, ніж у алгоритму Wang, при якому забезпечується найкращий рівень скритності впровадження. Але вони краще, ніж у решти трьох алгоритмів. Головне, що вони вписуються в оптимальні показники для досліджуваних груп зображень (для темних від 25 до 35 дБ, для середніх по яскравості від 30 до 40, а для світлих від 40 до 50 дБ). Результати оцінки пропускної спроможності представлені у таблиці 4.2.

Таблиця 4.2 – Оцінка пропускної спроможності зображень-контейнерів

Розміри зображення, пікселі	Коефіцієнт якості JPEG 2000 %	Загальна прихована пропускна здатність зображення, біт
521x512	50	1520
	70	1815
	90	1996
640x520	50	2734
	70	2769
	90	2907
800x800	50	2640
	70	2866
	90	3150
1000x800	50	2854
	70	3256
	90	3630

Алгоритм показав найвищі показники прихованої пропускної спроможності, порівняно з чотирма досліджуваними алгоритмами другого розділу. Для аналізу стійкості до зовнішніх впливів будуть використані ті ж зображення що й досліджуваних алгоритмів з другого розділу. Було вибрано 4 світлі, 4 темні та 4 середні за яскравістю растрові зображення з розмірами 1000x800 пікселів. ЦВЗ являтиме собою псевдовипадковий бітовий рядок в 1024 біт. Як досліджувані зовнішні впливи було вирішено використовувати зашумлення зображення білим гаусівським шумом, масштабування, стиснення JPEG 2000 з втратами, вирізування частини та фільтрація. Треба сказати відразу, що зміна формату зображення на інший зі стиском з втратами за алгоритмом, що відрізняється від JPEG 2000, до рамок дослідження не входить. На малюнку 3.8 показано оцінку стійкості ЦВЗ до стиску з втратами для створеного алгоритму та алгоритмів, досліджених у третьому розділі.

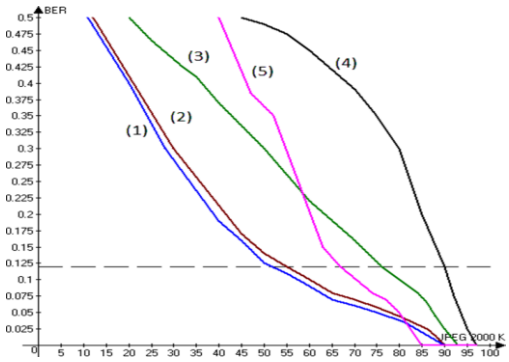

Рисунок 4.5 – Оцінка стійкості ЦВЗ до стиснення JPEG 2000 із втратами ((1) – алгоритм Ouled-Zaid, Makhloufi & Olivier, (2) – алгоритм Chirag-Ganesh, (3) – алгоритм Li & Zhang, (4) –алгоритм Wang (5) – створений алгоритм вбудовування під час стадії квантування).

Як можна помітити, алгоритм поступається за стійкістю до стиснення з втратами алгоритмів, де вбудовування здійснюється низькочастотними піддіапазонами.

ВИСНОВКИ

В кваліфікаційній роботі було проведено аналіз стійкості ЦВЗ до зовнішніх впливів на зображення-контейнер при збереженні оптимального рівня скритності впровадження та пропускної спроможності для чотирьох популярних алгоритмів, що використовуються

На основі аналізу сучасних алгоритмів вбудовування ЦВЗ зображення формату JPEG 2000 показана доцільність розробки методів і алгоритмів підвищення стійкості ЦВЗ до зовнішніх впливів на зображення-контейнер.

Розроблено багатокоефіцієнтний алгоритм вбудовування ЦВЗ під час стадії квантування, у якому вдалося підвищити значення стійкості ЦВЗ при зовнішніх впливах, не втративши оптимального рівня скритності впровадження.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Яремчук, Ю. Є., and В. В. Карпінець. "Аналіз стійкості стеганографічного перетворення до вбудовування цифрових водяних знаків у зображення." Інформаційні технології та компютерна інженерія.№ 1: 212-217. (2007).

2. Абазина, Евгения Сергеевна, and Анатолий Александрович Ерунов. "Цифровая стеганография: состояние и перспективы." Системы управления, связи и безопасности 2 (2016).

3. Navrotskyi, D. O. (2007). Методи комп’ютерної стеганографії. Visnyk NTUU KPI Seriia-Radiotekhnika Radioaparatobuduvannia, (35), 105-108..

4. Ахмаметьєва, Г. В., Г. А. Баранюк, and А. І. Казаков. "Модифікація стеганографічного методу вбудови цифрового водяного знаку в зображення на основі вейвлет-перетворення." Інформатика та математичні методи в моделюванні 9,№ 1-2 (2019): 38-48.

5. ЯЮ, Яремчук. "Підвищення стійкості цифрових водяних знаків до геометричних перетворень шляхом визначення особливих точок зображення." Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.–Випуск 2 (36), 2019.–С. 27–36. (2018).

6. Павленко, Б. В., et al. "Підвищення стійкості методу захисту забезпечення автентичності растрових зображень доказової бази від несанкціонованого доступу." *Реєстрація, зберігання і обробка даних* (2018).

7. Наріманова, О. В., and Д. М. Семенченко. "Метод захисту QR-коду з використанням цифрового водяного знаку." Інформатика та математичні методи в моделюванні 3,№ 4 (2013): 361-368.