**Міністерство освіти і науки України**
**Національний технічний університет**
**«Дніпровська політехніка»**

**Інститут електроенергетики**
**Факультет інформаційних технологій**
**Кафедра безпеки інформації та телекомунікацій**

# ПОЯСНЮВАЛЬНА ЗАПИСКА
## кваліфікаційної роботи ступеня магістра

**студента** *Воробйова Максима Володимировича*

**академічної групи** *125м-19-1*

**спеціальності** *125 Кібербезпека*

**спеціалізації**[1]

**за освітньо-професійною програмою** *Кібербезпека*

**на тему** *Стеганографічне вбудовування цифрових водяних знаків на основі алгоритму дискретного вейвлет перетворення*

| **Керівники** | **Прізвище, ініціали** | **Оцінка за шкалою** | | **Підпис** |
|---|---|---|---|---|
| | | **рейтинговою** | **інституційною** | |
| кваліфікаційної роботи | к.т.н., доц. Герасіна О.В. | | | |
| розділів: | | | | |
| спеціальний | к.т.н., доц. Герасіна О.В. | | | |
| економічний | к.е.н., доц. Пілова Д.П. | | | |
| **Рецензент** | | | | |
| **Нормоконтролер** | ст. викл. Мєшков В.І. | | | |

**Дніпро**
**2020**

**ЗАТВЕРДЖЕНО:**
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

# ЗАВДАННЯ
## на кваліфікаційну роботу
## ступеня магістра

**студенту** *Воробйову Максиму Володимировичу* **академічної групи** *125м-19-1*
(прізвище ім'я по-батькові) (шифр)

**спеціальності** *125 Кібербезпека*

**за освітньо-професійною програмою** *Кібербезпека*

**на тему** *Стеганографічне вбудовування цифрових водяних знаків на основі алгоритму дискретного вейвлет перетворення*

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

| Розділ | Зміст | Термін виконання |
|---|---|---|
| Розділ 1 | Аналіз основ побудови стеганографічних алгоритмів, а також стійкості ЦВЗ до зовнішніх впливів на зображення-контейнер. | 03.09.2020 – 10.10.2020 |
| Розділ 2 | Дослідження ланцюга кодування JPEG 2000, знаходження етапів, на яких відбувається основна втрата інформації при стисненні; розробка підходів і алгоритмів підвищення стійкості ЦВЗ до зовнішніх впливів на зображення-контейнер та оцінка їх ефективності. | 11.10.2020 – 24.11.2020 |
| Розділ 3 | Розрахунки капітальних витрат, витрат на вбудовування ЦВЗ та термін окупності інвестицій застосування запропонованих підходів. | 25.11.2020 – 04.12.2020 |

**Завдання видано** _____ Герасіна О.В.
(підпис керівника) (прізвище, ініціали)

**Дата видачі:** _____

**Дата подання до екзаменаційної комісії:** _____

**Прийнято до виконання** _____ Воробйов М.В.
(підпис студента) (прізвище, ініціали)

# РЕФЕРАТ

Пояснювальна записка: 106 с., 27 рис., 4 додатки, 37 джерел.

Об’єкт дослідження – стеганографічні підходи і алгоритми впровадження ЦВЗ в область дискретного вейвлет перетворення цифрових зображень.

Предмет дослідження – стійкість ЦВЗ до зовнішніх впливів на зображення-контейнер.

Мета кваліфікаційної роботи – розробка алгоритмів і підходів, що дозволяють вбудовувати цифрові водяні знаки підвищеної стійкості до зовнішніх впливів на зображення-контейнер в форматі JPEG 2000.

Наукова новизна результатів полягає у розробці підходів до підвищення стійкості ЦВЗ до зовнішніх впливів на зображення-контейнер шляхом вибору оптимального коефіцієнта сили вбудовування, фільтрів з найменшими спотвореннями при ДВП і глибини рівня вейвлет-розкладання.

У першому розділі проаналізовано основи побудови стегоалгоритмів, а також стійкість ЦВЗ до зовнішніх впливів.

У спеціальній частині роботи досліджено ланцюг кодування JPEG 2000 і знайдено етапи, на яких відбувається основна втрата інформації при стисненні; запропоновано підходи і алгоритми підвищення стійкості ЦВЗ до зовнішніх впливів на зображення-контейнер та оцінено їх ефективність. За наслідками досліджень зроблено висновки щодо рішення поставленої задачі.

У економічному розділі виконані розрахунки капітальних витрат, витрат на стеганографічне вбудовування ЦВЗ та термін окупності інвестицій застосування запропонованих підходів та алгоритмів.

ЦИФРОВИЙ ВОДЯНИЙ ЗНАК, СТЕГАНОГРАФІЯ, ДИСКРЕТНЕ ВЕЙВЛЕТ ПЕРЕТВОРЕННЯ, КОЕФІЦІЄНТ ПОМИЛКОВИХ БІТ, КВАНТУВАННЯ, ЗОБРАЖЕННЯ-КОНТЕЙНЕР, СТИСНЕННЯ ЗІ ВТРАТАМИ

# РЕФЕРАТ

Пояснительная записка 106 с., 27 рис., 4 приложения, 37 источников.

Объект исследования – стеганографические подходы и алгоритмы внедрения ЦВЗ в область дискретного вейвлет преобразования цифровых изображений.

Предмет исследования – устойчивость ЦВЗ к внешним воздействиям на изображение-контейнер.

Цель квалификационной работы – разработка алгоритмов и подходов, позволяющих встраивать цифровые водяные знаки повышенной устойчивости к внешним воздействиям на изображение-контейнер в формате JPEG 2000.

Научная новизна заключается в разработке подходов к повышению устойчивости ЦВЗ к внешним воздействиям на изображение-контейнер путем выбора оптимального коэффициента силы встраивания, фильтров с наименьшими искажениями при ДВП и глубины уровня вейвлет-разложения.

В первой главе проанализированы основы построения стегоалгоритмов, а также устойчивость ЦВЗ к внешним воздействиям.

В специальной части работы исследованы цепь кодирования JPEG 2000 и найдено этапы, на которых происходит основная потеря информации при сжатии; предложены подходы и алгоритмы повышения устойчивости ЦВЗ к внешним воздействиям на изображение-контейнер и оценена их эффективность. По результатам исследований сделаны выводы относительно решения поставленной задачи.

В экономическом разделе выполнены расчеты капитальных расходов, расходов на стеганографическое встраивания ЦВЗ и срок окупаемости инвестиций применения предложенных подходов и алгоритмов.

ЦИФРОВОЙ ВОДЯНОЙ ЗНАК, СТЕГАНОГРАФИЯ, ДИСКРЕТНОЕ ВЕЙВЛЕТ ПРЕОБРАЗОВАНИЕ, КОЭФФИЦИЕНТ ОШИБОЧНЫХ БИТ, КВАНТОВАНИЕ, ИЗОБРАЖЕНИЕ-КОНТЕЙНЕР, СЖАТИЕ С ПОТЕРЕЙ

# ABSTRACT

Explanatory note: p. 106, fig. 27, 4 additions, 37 sources.

The object of study is steganographic approaches and algorithms for implementing digital watermark in the field of discrete wavelet conversion of digital images.

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

The scientific novelty of the results is to develop approaches to increase the resistance of digital watermarks to external influences on the image-container by selecting the optimal embedding force factor, filters with discrete wavelet transform and the level of wavelet decomposition.

The first section analyzes the basics of constructing stegoalgorithms, as well as the resistance of digital watermarks to external influences.

In a special part of the work the JPEG 2000 coding chain is investigated and the stages at which the main loss of information during compression occurs are found; approaches and algorithms for increasing the resistance of digital watermarks to external influences on the image-container are proposed and their effectiveness is evaluated. Based on the results of research, conclusions were made regarding the solution of the problem.

In the economic section, calculations of capital costs, costs of steganographic embedding of digital watermarks and payback period of investments using the proposed approaches and algorithms.

DIGITAL WATERMARK, STEGANOGRAPHY, DISCRETE WAVELET TRANSFORMATION, ERROR BIT COEFFICIENT, QUANTIFICATION, IMAGE-CORRECTION

# СПИСОК УМОВНИХ СКОРОЧЕНЬ

ДВП – Дискретне вейвлет перетворення;

ДКП – Дискретне косинусне перетворення;

ДПФ – Дискретне перетворення Фур'є;

ПВП – Псевдовипадкова послідовність;

ПКЛ – Перетворення Карунена-Лоєва;

СЛЗ – Система людського зору;

ЦВЗ – Цифровий водяний знак;

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

BER – Bit Error Rate – Коефіцієнт помилкових біт;

EBCOT – Embedded Block Coding with Optimized Truncation – Вкладене блокове кодування з оптимізованим урізанням;

JPEG 2000 – Стандарт стиснення зі втратами для повнокольорових зображень на основі алгоритму дискретного вейвлет перетворення;

LSB – Least Significant Bit – Молодший значущий біт;

PSNR – Peak Signal to Noise Ratio – Пікове відношення сигналу до шуму;

ROI – Region Of Interest – Етап обробки регіонів, що виділяються, в якому проводиться довільний доступ до кодового потоку; цей етап може бути підключено в схемі кодування JPEG 2000;

SNR – Signal to Noise Ratio – Відношення сигнал / шум.

ЗМІСТ

с.

ВСТУП ... 10
1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ ... 12
1.1 Основи побудови стеганографічних алгоритмів ... 12
1.1.1 Введення в предметну область ... 12
1.1.2 Вимоги, що пред'являються до систем вбудовування ЦВЗ ... 14
1.1.3 Типи цифрових водяних знаків ... 16
1.1.4 Області застосування ЦВЗ ... 17
1.1.5 Типи стегоконтейнерів ... 18
1.1.6 Використання цифрових зображень як контейнера для вбудовування ... 20
1.1.7 Методи і алгоритми цифрової стеганографії. ... 23
1.1.8 Вбудовування ЦВЗ в зображення форматів стиснення зі втратами JPEG і JPEG 2000 ... 25
1.1.9 Огляд алгоритмів вбудовування ЦВЗ в область ДВП ... 29
1.2 Аналіз стійкості ЦВЗ до зовнішніх впливів ... 33
1.2.1 Вплив стиснення з втратами на зображення. ... 33
1.2.2 Інші зовнішні впливи на зображення ... 36
1.2.3 Параметри алгоритму, що впливають на стійкість до зовнішніх впливів ... 38
1.2.4 Оцінка скритності впровадження ... 39
1.2.5 Оцінка пропускної здатності зображення-контейнера ... 45
1.2.6 Оцінка стійкості вбудованої інформації до зовнішніх впливів ... 49
1.2.7 Результати аналізу стійкості ЦВЗ до зовнішніх впливів на зображення-контейнер ... 52
1.3 Висновок. Постановка задачі ... 56
2 СПЕЦІАЛЬНА ЧАСТИНА ... 59
2.1 Алгоритми підвищення стійкості ЦВЗ до зовнішніх впливів на зображення-контейнер ... 59
2.1.1 Дослідження ланцюга кодування JPEG 2000 для

можливості вбудовування ЦВЗ ..... 59
2.1.2 Втрата інформації при квантуванні для JPEG 2000 ..... 64
2.1.3 Алгоритм вбудовування ЦВЗ під час стадії квантування ..... 67
2.1.4 Алгоритм зчитування ЦВЗ з зображення ..... 74
2.1.5 Аналіз стійкості ЦВЗ до зовнішніх впливів
на зображення-контейнер ..... 75
2.2 Підходи до підвищення стійкості ЦВЗ до
зовнішніх впливів на зображення-контейнер ..... 81
2.2.1 Підвищення коефіцієнта сили вбудовування ..... 81
2.2.2 Вибір фільтрів при ДВП ..... 82
2.2.3 Вибір рівня вейвлет розкладу ..... 82
2.2.4 Застосування підходів до підвищення стійкості для
запропонованого алгоритму ..... 83
2.2.5 Аналіз стійкості ЦВЗ при використанні розроблених підходів ..... 84
2.3 Висновок ..... 88
3 ЕКОНОМІЧНИЙ РОЗДІЛ ..... 89
3.1 Розрахунок (фіксованих) капітальних витрат ..... 89
3.1.1 Визначення витрат на стеганографічне вбудовування ЦВЗ
на основі алгоритму дискретного вейвлет перетворення ..... 90
3.1.2 Розрахунок поточних витрат ..... 92
3.2 Оцінка можливого збитку ..... 94
3.2.1 Оцінка величини збитку ..... 94
3.2.2 Загальний ефект від застосування стеганографічного
вбудовування ЦВЗ на основі алгоритму
дискретного вейвлет перетворення ..... 95
3.3 Визначення та аналіз показників економічної ефективності
системи інформаційної безпеки ..... 95
3.4 Висновок ..... 96
ВИСНОВКИ ..... 97
ПЕРЕЛІК ПОСИЛАНЬ ..... 99

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи ..... 103
ДОДАТОК Б. Перелік документів на оптичному носії..... 104
ДОДАТОК В. Відгук керівника економічного розділу..... 105
ДОДАТОК Г. Відгук керівника кваліфікаційної роботи ..... 106

# ВСТУП

Наразі стеганографічні алгоритми широко використовуються для впровадження прихованої інформації в мультимедійні файли з метою захисту авторських прав на продукцію. Більшість великих Інтернет магазинів перед викладанням продукції автора накладають цифрові водяні знаки (ЦВЗ) на неї. У якості продукції виступають постановочні фотографії, панорами, обкладинки та вкладки музичних альбомів і відеофільмів тощо. ЦВЗ містять інформацію, яка однозначно підтверджує авторство або права на комерційне використання зображення, що захищається. Ця інформація може бути зчитана 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 початкових, але ступінь відмінності не є істотною з точки зору їх подальшого використання. Тому потрібно передбачити, щоб вбудована інформація була стійка до такого стиску.

У комп'ютерних мережах найбільш популярним форматом зображень є формат JPEG, в якому для зменшення обсягу інформації для зберігання точок використовуються залежності, кореляції між близько розташованими одна до одної областями зображення. Стандарт стиснення JPEG 2000 замість дискретного косинусного перетворення, що застосовується у популярному форматі JPEG, використовує технологію вейвлет-перетворення, що ґрунтується на поданні сигналу у вигляді суперпозиції базових функцій – хвильових пакетів. В результаті такої компресії зображення виходить більш гладким і чітким, а розмір файлу у порівнянні з JPEG при однаковій якості виявляється меншим.

Наразі формат JPEG 2000 є найбільш актуальним для стиснення зображень з метою поширення їх в електронних магазинах на продаж. Він

використовується в кодеках для створення 3D-анімації (візуалізації) і в кодуванні / декодуванні відео високої роздільної здатності (наприклад, Motion JPEG-2000). Вбудований водяний знак повинен бути стійкий до подібного стиску і різних зовнішніх впливів (обрізка, фрагментація, масштабування, зашумлення, фільтрація). Це й є одним з найважливіших вимог до стеганографічного алгоритму.

Таким чином, розробка підходів і алгоритмів, використання яких при побудові стеганографічних систем захисту авторських прав для зображень може гарантувати цілісність ЦВЗ, наразі є актуальною задачею.

Метою роботи є розробка алгоритмів і підходів, що дозволяють вбудовувати цифрові водяні знаки підвищеної стійкості до зовнішніх впливів на зображення-контейнер в форматі JPEG 2000.

Постановка задачі:

• запропонувати методику оцінки впливу зовнішніх впливів на вбудований ЦВЗ;

• провести порівняльний аналіз стійкості ЦВЗ, впроваджених різними алгоритмами в зображення JPEG 2000, при якому збережуться оптимальні рівні скритності впровадження та пропускної здатності;

• дослідити ланцюг кодування JPEG 2000 і знайти етапи, на яких відбувається основна втрата інформації при стисненні;

• розробити підходи і алгоритми підвищення стійкості ЦВЗ до зовнішніх впливів на зображення-контейнер;

• оцінити ефективність розроблених підходів і алгоритмів.

# 1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

## 1.1 Основи побудови стеганографічних алгоритмів

### 1.1.1 Введення в предметну область

Цифрова стеганографія – напрям класичної стеганографії, заснований на приховуванні або впровадженні додаткової інформації в цифрові об'єкти, викликаючи при цьому деякі спотворення цих об'єктів. Ці об'єкти є мультимедійними файлами (зображення, відео, аудіо, текст) і внесення спотворень, які знаходяться нижче порога чутливості середньостатистичної людини, не призводить до помітних змін цих об'єктів. Наразі стеганографія дозволяє не тільки успішно вирішувати основну задачу – приховано передавати інформацію, але й цілий ряд інших актуальних задач, в тому числі вбудовування прихованої інформації з метою захисту авторських прав на інтелектуальну власність, представлену у цифровому вигляді [1-11]. Ця прихована інформація є цифровим водяним знаком, який представляє собою спеціальну мітку, що містить інформацію, яка однозначно підтверджує авторство або права на комерційне використання об'єкта, що захищається. Вона непомітно впроваджується в зображення або 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 в цифровому вигляді. ЦВЗ активно використовуються при розміщенні унікальних фотографій, відео, аудіо в електронному вигляді в мережі Інтернет. Перші роботи по врахуванню водяних знаків були зроблені в 90-х рр. XX ст. У 1996 р. на конференції Information Hiding: First Information Workshop була прийнята єдина термінологія в області цифрової стеганографії:

1. Стеганографічна система (стегосистема) – об'єднання методів і засобів, що використовуються для створення прихованого каналу для передачі інформації. При цьому: невідомим для противника є ключ за допомогою якого можна дізнатися про факт існування і змісту таємного повідомлення; при виявленні противником наявності прихованого повідомлення він не повинен змогти отримати повідомлення до тих пір поки не буде володіти ключем; противник не має технічних та інших переваг.

2. Повідомлення – термін, який використовується для загальної назви переданої прихованої інформації (наприклад, цифровий файл).

3. Контейнер – будь-яка інформація, яка використовується для приховування таємного повідомлення. При цьому, порожній контейнер не містить секретного послання, заповнений контейнер (стегоконтейнер) – містить.

4. Стеганографічний канал (стегоканал) – канал передачі стегоконтейнера.

5. Ключ (стегоключ) – секретний ключ, потрібний для приховування стегоконтейнера. Ключі в стегосистемах бувають двох типів: приватні та публічні. Якщо стегосистема використовує секретний ключ, то він повинен бути створений або до початку обміну повідомленнями, або переданий по захищеному каналу. Стегосистема, що використовує відкритий ключ, повинна бути влаштована таким чином, щоб було неможливо отримати з нього закритий ключ. У такому випадку відкритий ключ можна передавати по незахищеному каналу [2, 11, 12].

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

• прекодер – пристрій, призначений для перетворення приховуваного повідомлення до вигляду, зручного для вбудовування в сигнал-контейнер;

• контейнер – інформаційна послідовність, в якій ховається повідомлення;

• стегокодер – пристрій, призначене для здійснення вкладення прихованого повідомлення в інші дані з урахуванням їх моделі;

• пристрій виділення вбудованого повідомлення;

• стегодетектор – пристрій, призначений для визначення наявності стегоповідомлення;

• декодер – пристрій, що відновлює приховане повідомлення. Цей вузол може бути відсутнім, якщо потрібно лише встановити факт наявності в об'єкті вбудованого до цього ЦВЗ.

### 1.1.2 Вимоги, що пред'являються до систем вбудовування ЦВЗ

Основні вимоги до стегосистеми вбудовування прихованої інформації:

• методи приховування повинні забезпечувати автентичність і цілісність файлу;

• передбачається, що противнику повністю відомі можливі стеганографічні методи;

• безпека методів ґрунтується на збереженні стеганографічним перетворенням основних властивостей відкрито переданого файлу при внесенні до нього секретного повідомлення і деякої невідомої противнику інформації – ключа;

• навіть якщо факт приховування повідомлення став відомий противнику, витяг самого секретного повідомлення є складною обчислювальною задачею;

• стегосистеми повинна мати низьку ймовірність помилкового виявлення прихованого повідомлення в сигналі, його що не містить (у деяких додатках таке виявлення може призвести до серйозних наслідків [11, 13]).

• заповнений контейнер повинен візуально не відрізнятися від незаповненого.

Для задоволення останньої вимоги потрібно, на перший погляд, впроваджувати приховане повідомлення в візуально незначущі області сигналу. Але ці ж області використовують і алгоритми стиснення. Тому, якщо зображення буде надалі піддаватися стиску, то приховане повідомлення може зруйнуватися. Отже, біти повинні вбудовуватися в візуально значущі області, а

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

Крім цього, можна додати, що до систем вбудовування ЦВЗ пред'являються ще й додаткові вимоги:

1. Стійкість до зовнішніх впливів. ЦВЗ не повинен пошкоджуватися в результаті маніпуляцій з контейнером, які можуть відбутись при його використанні, таким як фільтрація, нанесення шуму, стиснення із втратами, обрізка, масштабування, друк, сканування, перетворення в інший формат.

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

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

4. Повинна бути можливість використовувати вдосконалені версії тієї ж самої техніки впровадження, коли буде доступна більша потужність обчислювальної техніки.

5. Якщо доступний тільки фрагмент стегоконтейнера, отриманий в результаті обрізки або обертання, ЦВЗ повинен як і раніше детектуватися і читатися.

Усі перераховані вимоги не повинні обов'язково виконуватись в стегоалгоритмі у повному обсязі., тим більше, що деякі властивості знаходяться у суперечності одна з одною. Як правило, при розробці стегоалгоритму автори роблять акцент на певну властивість або групу властивостей, оскільки задовольнити усі вимоги відразу непросто. Покращуючи одну властивість стегоалгоритму можна погіршити його інша властивість. Саме тому існує безліч різних технологій, які мають місце застосування в різних ситуаціях. Тим більше з плином часу багато технологій застарівають і на їх місце з ростом потужності обчислювальної техніки з'являються більш нові поліпшені алгоритми впровадження ЦВЗ. Також існує безліч вбудованих модулів (plug-

in), які можуть бути підключені до популярних медіа редакторів (наприклад, Adobe Photoshop) і які об'єднують в собі різні алгоритми вбудовування ЦВЗ для різних ситуацій.

Наразі безліч технологій вбудовування ЦВЗ добре використовуються в мережі Інтернет, але не всі ці алгоритми мають хороші показники захисту від зовнішніх впливів на контейнер. Тому ця область постійно розвивається.

### 1.1.3 Типи цифрових водяних знаків

Як правило, розрізняють три різних типи ЦВЗ: робастні, тендітні і напівкрихкі. Під робастністю розуміється стійкість ЦВЗ до різного виду впливів на стегоконтейнер. Такі ЦВЗ застосовуються для захисту авторських прав на інтелектуальну власність, що виставляється в публічних комп'ютерних мережах. Тендітні ЦВЗ руйнуються при незначній модифікації заповненого контейнера, вони застосовуються для аутентифікації сигналів. Відмінність від засобів електронного цифрового підпису полягає у тому, що тендітні ЦВЗ все ж допускають деяку модифікацію контенту [11, 14-29]. Це важливо для захисту мультимедійної інформації, оскільки законний користувач може, наприклад, побажати стиснути зображення.

Напівкрихкі ЦВЗ стійкі по відношенню до одних впливів і нестійкі по відношенню до інших. Напівкрихкі ЦВЗ спеціально проектуються таким чином, щоб бути нестійкими по відношенню до певного роду операцій. Наприклад, вони можуть дозволяти виконувати стиснення зображення, але забороняти вирізку з нього або вставку в нього фрагмента.

ЦВЗ називають непомітним, якщо початковий і позначений сигнали по певним критеріям сприйняття відрізняються. Зазвичай легко зробити надійний або непомітний ЦВЗ, але, як правило, важко зробити ЦВЗ непомітним і надійним одночасно.

ЦВЗ можуть представлятися у вигляді бітової послідовності, зображення або послідовності з плаваючою точкою. Бітова послідовність є найбільш

популярним видом ЦВЗ і представляється у вигляді рядка ASCII символів або символів іншого кодування. У цифрове зображення або відеопослідовність може вбудовуватись і додаткове приховане зображення, наприклад з логотипом компанії. Використання ЦВЗ у вигляді зображення є не дуже практичним, оскільки ідентифікація різних логотипів є досить непростим завданням. Послідовність, з плаваючою точкою, як правило, має нормальний закон розподілу, що робить її схожою зі звичайним шумом. Такий ЦВЗ обчислювально складно зчитувати з контейнера, але при цьому він володіє хорошими показниками скритності і представляється з розподілених чисел з плаваючою точкою. Додаткову обчислювальну складність додає перетворення прихованого повідомлення з цієї послідовності чисел в вигляд, що читається.

### 1.1.4 Області застосування ЦВЗ

Вбудовування ЦВЗ в медіафайли може бути використано для таких цілей:

1. Вбудовування інформації з метою її прихованої передачі. Цей напрямок використовується з метою захисту конфіденційної інформації від несанкціонованого доступу і безпечної її передачі по комп'ютерних мережах.

2. Вбудовування ЦВЗ з метою 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 для підтвердження прав власності. Найбільші досягнення стеганографії були досягнуті саме в цій області, і наразі вона знаходиться в постійному розвитку.

3. Маркування ідентифікаційними номерами для відстеження шляхів поширення нелегальних копій продукту, використовуючи техніку унікального підпису для кожної легальної копії. В 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 і надав продукт для незаконного розповсюдження або копіювання.

4. Вбудовування з метою захисту від копіювання медіафайлу. Вбудований ЦВЗ може безпосередньо контролювати цифрові записуючі або друкуючі пристрої. Детектор ЦВЗ на записуючим пристрої визначає, чи може інформація, яка надана пристрою, бути скопійована.

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

6. Вбудовування з метою перевірки цілісності переданих даних. Впровадження ЦВЗ дозволяє перевірити дані на предмет зміни або пошкодження як навмисного, так і випадкового характеру. Також можливе визначення, в якій саме частині даних були зроблені зміни.

7. Вбудовування з метою індексації частин файлу. Якщо вбудувати ЦВЗ в відеопослідовність, то можна полегшити задачу пошуковому движку.

8. Вбудовування ЦВЗ для підпису медичних знімків або нанесення легенди на карту. Метою є зберігання різнорідно представленої інформації в єдине ціле. Впровадження інформації допоможе уникнути плутанини і забезпечить зручність зберігання інформації.

У даній кваліфікаційній роботі було розглянуто саме область застосування ЦВЗ з метою захисту авторських прав на комерційну інформацію, представлену в цифровому вигляді.

### 1.1.5 Типи стегоконтейнерів

У сучасній цифровій стеганографії як контейнери можуть виступати музичні файли (найбільш популярні формати WAV і MP3), зображення (формати JPEG і BMP), відео (формати AVI і MPEG) і текстові файли (формати DOC і PDF). Стегоконтейнер повинен візуально не відрізняється від порожнього контейнера. Розрізняють два основних типи контейнерів:

потоковий і фіксований. Істотний вплив на надійність і стійкість стегосистеми, а також можливість виявлення факту передачі прихованого повідомлення надає вибір контейнера. Найбільш досвідчені дизайнери зі сприйняттям кольорової гами більшої, ніж у звичайного користувача при впровадженні повідомлення в зображення можуть помітити даний контейнер. Тому з вибором типу контейнера доводиться бути обережним.

Потоковий контейнер являє собою безперервно наступну послідовність біт. Повідомлення вкладається в нього в реальному масштабі часу, так що в кодері невідомо заздалегідь, чи вистачить розмірів контейнера для передачі всього повідомлення. В один контейнер великого розміру може бути вбудовано й декілька повідомлень. Інтервали між вбудованими бітами визначаються генератором псевдовипадкової послідовності з рівномірним розподілом інтервалів між відліками. Основна складність полягає в здійсненні синхронізації, визначенні початку і кінця послідовності. Якщо в даних контейнера є біти синхронізації, заголовки пакетів тощо, то прихована інформація може йти відразу після них. Труднощі забезпечення синхронізації перетворюється на переваги з точки зору забезпечення скритності передачі. Крім того, потоковий контейнер має велике практичне значення: припустимо під прикриттям звичайного, незначущого телефонного дзвінка можна передавати інші дані, і не знаючи секретного ключа можна не тільки дізнатися зміст прихованої передачі, але й сам факт її існування [30].

У фіксованого контейнера розміри і характеристики заздалегідь відомі. Це дозволяє здійснювати вкладення даних оптимальним чином. Але контейнери фіксованої довжини мають обмежений обсяг, і іноді повідомлення, що вбудовується, може не поміститись в файл-контейнер. Інший недолік у тому, що відстані між приховуючими бітами рівномірно розподілені між найбільш короткою і найбільш довгою заданими відстанями, у той час як справжній випадковий шум буде мати експоненціальний розподіл довжин інтервалу [31]. Звичайно, можна використовувати псевдовипадкові експоненційно розподілені числа, але цей шлях зазвичай занадто

обчислювально складний. На практиці найчастіше використовуються саме контейнери фіксованої довжини, як найбільш поширені й доступні. Контейнер може бути обраним, випадковим або нав'язаним. Обраний контейнер залежить від вбудованого повідомлення, а в граничному випадку є його функцією. Цей тип контейнера більше характерний для стеганографії. Нав'язаний контейнер може з'явитися в сценарії, коли особа, яка надає контейнер, підозрює про можливе приховане листуванні і бажає запобігти йому. На практиці найчастіше стикаються із випадковим контейнером.

Для кожного типу контейнерів існує безліч алгоритмів впровадження ЦВЗ, специфічних для конкретного виду стегоконтейнера. Стегоконтейнери можуть бути представлені в різних форматах, що накладає певні обмеження на реалізацію стегоалгоритму.

### 1.1.6 Використання цифрових зображень як контейнера для вбудовування

Цифрові зображення можуть виступати відмінним контейнером для впровадження в них прихованої інформації. Це обумовлено деякою надмірністю візуальної інформації. Популярність використання цифрових зображень в якості стегоконтейнера обумовлена наступними причинами [32-37]:

• існуванням практично важливим завданням захисту фотографій, відео від незаконного тиражування і розповсюдження;

• відносно великим обсягом пропускної здатності зображень, що дозволяє впроваджувати ЦВЗ великого обсягу або підвищувати робастність впровадження;

• наявністю у більшості реальних зображень текстурних областей, що мають шумову структуру і підходять для вбудовування інформації;

• слабкою чутливістю людського ока до незначних змін кольорів зображення, його яскравості, контрастності, вмісту в ньому шуму, спотворень поблизу контурів.

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

Для впровадження прихованого повідомлення в зображення потрібно створити стегосистему, яка буде займатися шифруванням повідомлення, вбудовуванням його в контейнер, зчитуванням назад повідомлення і дешифруванням його. Схема системи представлена на рис. 1.1.

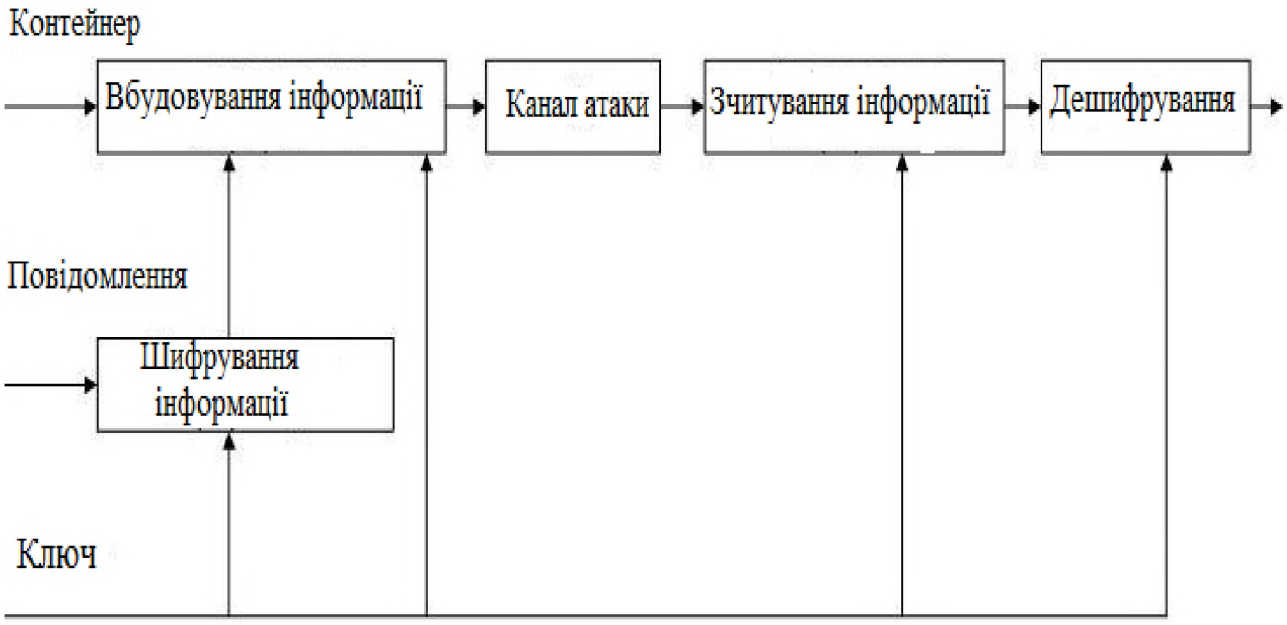



Рисунок 1.1 – Структура стегосистеми вбудовування та зчитування інформації

Перш, ніж здійснити вбудовування ЦВЗ у контейнер, ЦВЗ повинен бути перетворений до деякого відповідного вигляду. Так, якщо в якості контейнера виступає зображення, то й послідовність ЦВЗ часто представляється, як двовимірний масив біт. Для того щоб підвищити стійкість ЦВЗ до спотворень нерідко виконують його завадостійке кодування, або застосовують широкосмугові сигнали. Попередня обробка часто виконується із використанням ключа для підвищення секретності вбудовування. Ключ може

бути призначений для вузького кола осіб або ж бути загальнодоступним. Далі ЦВЗ вбудовується в контейнер. Прихована інформація впроваджується відповідно до ключа в ті відліки, спотворення яких не призводить до суттєвих перекручень контейнера. В залежності від програми, під істотним спотворенням можна розуміти спотворення, яке призводить як до неприйнятність для людини-адресата заповненого контейнера, так і до можливості виявлення факту наявності прихованого повідомлення після стегоаналізу. Області вбудовування можуть бути виключені виходячи з різних обмежень, які накладаються в рамках того чи іншого стегоалгоритму. У числі вимог, що впливають на відбір придатних областей вбудовування можуть бути: візуальна невідмінність зображення з ЦВЗ від оригіналу, складність несанкціонованого детектування ЦВЗ, стійкість ЦВЗ до різного роду перетворень зображення-контейнера [28].

Для того щоб захистити впроваджуваний ЦВЗ від похибок, як правило, здійснюється зменшення його обсягу за допомогою використання алгоритмів стиснення і використовується багаторазове повторення вбудовування ЦВЗ в зображення-контейнер.

При створенні системи вбудовування та зчитування ЦВЗ потрібно дуже уважно підходити до питання системи людського зору (СЛЗ). Зображення мають велику психовізуальну надмірність. Око людини подібне низькочастотному фільтру, якому непомітні спотворення в високочастотній області зображень. Стеганографія заснована на використанні наявної в зображеннях психовізуальної надмірності [11].

Алгоритм зчитування ЦВЗ повинен вірно реконструювати ЦВЗ навіть після того, як підписане зображення було піддано таким змінам як: поворот, урізання країв, стиснення без втрат тощо, не позначитись на якості зображення. Також детектор повинен володіти вкрай низькою ймовірністю помилкового детектування ЦВЗ (визначення є або немає ЦВЗ в зображенні). Детектор в якості вхідних даних може вимагати: оригінальне зображення, ЦВЗ, секретний ключ. Якщо оригінальне зображення не потрібне для детектування ЦВЗ, то

стегоалгоритм називають «сліпим». Існують детектори, які можуть визначати тільки можливість присутності ЦВЗ, інші здійснюють зчитування, отримуючи у результаті відновлений ЦВЗ.

### 1.1.7 Методи і алгоритми цифрової стеганографії

У 1989 р. був отриманий перший патент на спосіб прихованого вкладення інформації в зображення шляхом модифікації молодшого значущого біта (Least significant bit, LSB). У даному випадку детектор аналізує тільки значення цього біта для кожного пікселя, а око людини, навпаки, сприймає тільки старші 7 біт. Науково підтверджено факт, що система людського зору найменш чутлива до змін інтенсивності у синій області спектра. Таким чином, можна з великою впевненістю підміняти молодший біт байта, що відповідає за інтенсивність синього каналу, по обраній нами закономірності. Людському оку буде принципово важко відрізнити оригінальне чисте зображення від зображення із вбудованим прихованим повідомленням [2]. Даний метод є типовим представником методів вбудовування в просторову область зображення, при якому для вбудовування використовуються безпосередні зміни значень параметрів яскравості і кольоровості зображень. Існує багато модифікацій цього методу, але наразі багато з них застаріли.

Наразі існує безліч різних варіантів вибору області вбудовування ЦВЗ. Класифікація алгоритмів по області вбудовування наведена на рис. 1.2.

Методи приховування даних в просторовій області зображення є нестійкими до більшості з відомих видів спотворень, наприклад стиснення зі втратами. Вони розрізняються тільки вибором підмножини пік селів, яка модифікується, і стратегією зміни значень пікселів. Впровадження ЦВЗ відбувається в області початкового зображення. Перевагою таких алгоритмів є те, що для впровадження ЦВЗ немає необхідності виконувати обчислювально громіздкі лінійні перетворення зображень. ЦВЗ впроваджується за рахунок маніпуляцій яскравістю або колірними складовими.


Рисунок 1.2 – Класифікація алгоритмів вбудовування ЦВЗ по області, яка використовується в процесі впровадження

Найбільший інтерес в області цифрових зображень представляють методи вбудовування інформації в зображення, при використанні яких відбувається стиснення зі втратами (формати JPEG і JPEG 2000). Для таких форматів немає сенсу вбудовувати в просторову область, оскільки після певних перетворень дані будуть відрізнятися від початкових, і тому багато повідомлень, що впроваджуються, попросту неможливо витягти, й, отже, втрачається сенс системи. Для вбудовування інформації використовується область змінюваного дозволу або частотна область. Ці підходи з'явилися пізніше попереднього і продовжують розвиватися. Методи, які використовують для приховування даних частотну область, є більш стійкими до різних можливих зовнішніх

впливів на зображення-контейнер. У цій групі використовуються наступні 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 гарні характеристики робастності. Подібні перетворення можуть застосовуватись або до окремих частин зображення, або до зображення в цілому. Алгоритм ДКП є базовим в стандарті JPEG, а ДВП – в стандарті JPEG 2000. Тому для формату JPEG 2000 найбільш підходять технології вбудовування в коефіцієнти ДВП, а для формату JPEG – в коефіцієнти ДКП. При цих методах використовується скалярне або векторне квантування. Під квантуванням розуміється процес зіставлення великої (можливо й нескінченної) множини значень з деякою кінцевою множиною чисел. Квантування знаходить застосування в алгоритмах стиснення зі втратами JPEG і JPEG 2000. Розрізняють скалярне і векторне квантування. При векторному квантуванні відбувається відображення не окремо взятого відліку, а їх сукупності (вектора). Векторне квантування ефективніше скалярного за ступенем стиснення, при цьому є більш складним. Методи вбудовування в цифрові зображення стають основою для більш складних методів вбудовування інформації в відеопослідовності.

### 1.1.8 Вбудовування ЦВЗ в зображення форматів стиснення зі втратами JPEG і JPEG 2000

У комп'ютерних мережах зазвичай викладаються цифрові зображення в форматах, де відбувається стиснення з втратами. Це обумовлено великим розміром таких файлів. При використанні стиснення зі втратами розпаковані

після стиснення дані будуть відрізняються від початкових, але ступінь відмінності при цьому не буде суттєвою з точки зору їх подальшого використання. У таких кодеках фрейми зображень трансформуються в новий базисний простір, і проводиться квантування. А головне при використанні методів стиснення зі втратами зображення будуть задовольняти вимогам спотворення в допустимих межах чутливості людини [32]. При цьому файл може дуже сильно відрізнятися від оригіналу на рівні порівняння біт в біт, але практично не відрізнятися для людського ока.

При встановленні ЦВЗ в просторову область ми зможемо забезпечити стійкість впровадженої інформації тільки до дуже низьких ступенів стиснення JPEG або JPEG 2000, зате при цьому не потрібно робити обчислювально складні математичні операції. Якщо метою є вбудовування ЦВЗ для можливого захисту авторських прав, то такі алгоритми не потрібно використовувати. Набагато доцільніше вбудовувати в область перетворень, яка використовується в форматі стиснення зображення (для JPEG це область ДКП, а для JPEG 2000 – ДВП).

За останні роки було зроблено безліч нових і вдосконалено старих алгоритмів вбудовування ЦВЗ в коефіцієнти ДКП. Ці алгоритми дозволяють вбудованому ЦВЗ протистояти високим ступеням стиснення JPEG і 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, в результаті чого отримують матриці коефіцієнтів ДКП, також розміром 8x8. Коефіцієнти позначаються через $c_b(j, k)$, де $b$ – номер блоку, $(j, k)$ – позиція коефіцієнта всередині блоку. якщо блок сканується в зигзагоподібному порядку, то коефіцієнти позначаються через $c_{b,j}$. Коефіцієнт в лівому верхньому кутку $c_b(0, 0)$ зазвичай називається DC-коефіцієнтом. Він містить інформацію про яскравість всього блоку. Решта коефіцієнтів називаються AC-коефіцієнтами [23]. Псевдовипадково обираються декілька коефіцієнтів ДКП і вбудовування здійснюється з певної умови, в залежності від

алгоритму. Розділяють однокоефіцієнтні, двокоефіцієнтні і багатокоефіцієнтні алгоритми. З огляду на зростання обчислювальних потужностей і збільшення зростання Інтернет торгівлі алгоритми, що вбудовують ЦВЗ область ДКП, продовжують поліпшуватися, і з'являються нові роботи в цьому напрямі.

Наразі найбільш актуальним напрямком є вбудовування в область ДВП, при якому можливо протистояти стиску зі втратами при алгоритмі JPEG 2000. Вбудовування в область ДВП найбільш доцільно застосовувати в разі активного порушника.

Формат JPEG 2000 розроблявся ще давно з метою згодом повністю замінити JPEG, але на даний момент цього не сталося. Незважаючи на те, що популярність зображень в форматі JPEG в мережі набагато вище, формат JPEG 2000 знайшов найбільш широке застосування. Основні області застосування цього формату:

• зберігання стиснутих зображень високої якості при передачі по мережі;

• цифровий кінематограф;

• 3D-візуалізація;

• охоронні системи (для стиснення зображень, одержуваних з цифрових відеокамер);

• клієнт-серверні взаємодії (бази даних зображень);

• для зберігання фотографій власника в біометричних паспортах;

• зберігання оцифрованих версій географічних карт;

• зберігання медичних файлів.

Стандарт стиснення JPEG 2000 замість ДКП, що застосовується в популярному форматі JPEG, використовує технологію ДВП, що ґрунтується на поданні сигналу у вигляді суперпозиції базових функцій – хвильових пакетів. В результаті такої компресії зображення виходить більш гладким і чітким, а розмір файлу у порівнянні з JPEG при однаковій якості виявляється набагато меншим [27].

Основні переваги JPEG 2000 у порівнянні із JPEG:

1. JPEG 2000 на низьких і високих бітрейтах має ступінь стиснення більше, ніж у формату JPEG. Це досягається завдяки використанню ДВП і складнішого ентропійного кодування.

2. Масштабованість фрагментів зображень. JPEG 2000 забезпечує безшовне стиснення різних компонентів зображення. Завдяки розбиттю на блоки можна зберігати зображення різних дозволів в одному кодовому потоці.

3. Довільний доступ до кодовому потоку (ROI). У форматі забезпечується декілька механізмів для підтримки довільного доступу, також підтримується декілька ступенів розбиття на частини.

4. Гнучкий формат файлу: формати файлів JP2 і JPX забезпечують зберігання інформації про кольорні простори, метаданих та інформації для узгодженого доступу в мережевих додатках, взаємодіючих 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 дозвіл і якість. Найбільш цінною є можливість подання коефіцієнтів вейвлет перетворення в цілих числах, у той час як в ДКП алгоритмах робота здійснюється з коефіцієнтами, представленими у вигляді чисел з плаваючою точкою, що призводить до похибок округлення при проміжних перетвореннях, наприклад при масштабуванні. Таким чином, зміна дозволу зображення або ступеня його компресії всередині інтегрованої системи кодування, заснованої на ДВП, здійснюється без тих втрат, які були характерні для ДКП перетворень. Більш того, в 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 і якості. У випадку з ДКП асоційована фільтрова система була фіксована, а для її зміни потрібно повторне кодування. Практично все програмне забезпечення наразі, яке так чи інакше стосується роботи із зображеннями, функціонує з JPEG-2000 [24].

Зображення піддається послідовностям вертикальних і горизонтальних одновимірних вейвлет перетворень, ці послідовності чергуються. Спочатку перетворюються всі рядки, а потім всі стовпці. На наступному етапі ліва верхня чверть матриці, яка була отримана в результаті попереднього перетворення, знову перетвориться; і так далі. Кількість етапів відповідає кількості рівнів вейвлет-декомпозиції. В результаті перетворення отримують безліч частотних діапазонів, які містять інформацію про те, як поводиться початковий сигнал (зображення) при різному дозволі. Обробляючи спеціальним чином частотні піддіапазони ДВП в початкове зображення можна вбудувати ЦВЗ.

### 1.1.9 Огляд алгоритмів вбудовування ЦВЗ в область ДВП

У табл. 1.1 наведено популярні наразі стегоалгоритми вбудовування ЦВЗ в область ДВП. Ці алгоритми відрізняються один від одного піддіапазонами ДВП, в які проводиться вбудовування ЦВЗ і типом застосовуваного ЦВЗ.

Таблиця 1.1 – Огляд алгоритмів вбудовування ЦВЗ в область ДВП

| **Алгоритм** | **Область вбудовування** | **ЦВЗ** | **Особливості алгоритму** |
|---|---|---|---|
| Elbasi-Eskicioglu | Модифікація коефіцієнтів LL і HH піддіапазонів 2-х рівневого розкладання | Бітовий рядок | Стійкість до широкого спектру атак за рахунок використання різних частотних піддіапазонів. |
| Wang | Модифікація коефіцієнтів HH піддіапазонів | Бітовий рядок | Висока скритність впровадження |
| Y. Kim | Модифікація найбільших коефіцієнтів кожного піддіапазону трирівневої декомпозиції зображення крім | Послідовність псевдовипадкових дійсних чисел, розподілених за гаусівським законом | Для виявлення ЦВЗ не потрібно наявність початкового зображення |

| Алгоритм | Область вбудовування | ЦВЗ | Особливості алгоритму |
|---|---|---|---|
| | піддіапазонів найвищого рівня дозволу | | |
| Chirag-Ganesh | Модифікація трьох коефіцієнтів LL піддіапазону | Бітовий рядок | Хороша стійкість до стиснення зі втратами |
| J. Chae | Модифікація всіх коефіцієнтів однорівневої декомпозиції початкового зображення | Чорно-білий логотип, розміром до 25% від початкового зображення | Великий розмір приховуваного ЦВЗ, але для вилучення ЦВЗ необхідно мати початкове зображення |
| Hsu | Модифікація HL і LH областей дворівневого ДВП | Бінарне зображення, розміром в половину від початкового | Великий розмір приховуваного ЦВЗ, але для вилучення ЦВЗ необхідно мати початкове зображення |
| G. Nacchiotti | Модифікація всіх коефіцієнтів LL піддіапазону ДВП | Масив псевдовипадкових чисел, розподілених за законом Гауса | Для вилучення ЦВЗ необхідно мати початкове зображення |
| G. X'ie | Модифікація коефіцієнтів LL піддіапазону багаторівневого розкладання | Бітовий рядок | Стійкість до широкого спектру атак. Низька скритність впровадження ЦВЗ |
| M. Ali Akhaee | Модифікація коефіцієнтів LL піддіапазону | Бітовий рядок | Висока скритність ЦВЗ. Значна обчислювальна ємність, великий розмір секретного ключа |

| Алгоритм | Область вбудовування | ЦВЗ | Особливості алгоритму |
|---|---|---|---|
| Huo-Gao | Модифікація коефіцієнтів HL і LH піддіапазонів 3-х рівневої декомпозиції | Бітовий рядок | Для виявлення ЦВЗ не потрібно наявність початкового зображення |
| Meerwald | Вбудовування в коефіцієнти при квантуванні індексів модуляції (QIM) | Бітовий рядок | Висока стійкість до зовнішніх впливів, але при цьому низька скритність впровадження |
| Li & Zhang | Модифікуються коефіцієнти залежно від цільової швидкості бітового потоку | Бітовий рядок | Висока скритність впровадження |
| Fan & Tsao | Модифікація коефіцієнтів HL і LH піддіапазонів | Два види ЦВЗ, крихкий і надійний | Використання однієї подвійної пірамідальної схеми вбудовування ЦВЗ. Висока стійкість до зовнішніх впливів і запобігання вкладення помилкових ЦВЗ |
| Hsu-Wu | Модифікація найбільших коефіцієнтів детальних піддіапазонів трирівневої декомпозиції зображення | Послідовність псевдовипадкових дійсних чисел, розподілених за законом Гауса | Гарне візуальне маскування впроваджених даних. Для виявлення ЦВЗ не потрібно початкове зображення |
| P. Loo | Модифікація 1000 найбільших коефіцієнтів ДВП | Масив псевдовипадкових чисел | Для виявлення ЦВЗ не потрібно початкове зображення, але є обмеження за глибиною |

| Алгоритм | Область вбудовування | ЦВЗ | Особливості алгоритму |
|---|---|---|---|
| | | | перетворення і розмірами зображення |
| Schlauweg | Вбудовування в коефіцієнти декількох високочастотних піддіапазонів при розширеному скалярному квантування | Бітовий рядок | Погіршення характеристик зображення при встановленні ЦВЗ |
| Fan, Chiang & Shen | Вбудовування в область регіонів, що виділяються (ROI) | Бітовий рядок | ЦВЗ стійкий при обробці регіонів, що виділяються. Алгоритм працює тільки якщо ввімкнено кодування регіонів, що виділяються |
| Ouled-Zaid, Makhloufi & Olivier | Вбудовування в коефіцієнти LH і LL | Бітовий рядок | Висока стійкість до зовнішніх впливів |

З цих рішень найбільш цікаві ті, що впроваджують ЦВЗ, який має досить високу стійкість до зовнішніх впливів. Крім того алгоритм детектування ЦВЗ повинен бути сліпим, тобто при вилученні не потрібно початкове зображення з ЦВЗ для порівняння. Саме такі алгоритми підійдуть для впровадження ЦВЗ з метою захисту авторських прав. При цьому вбудовування має здійснюватись в псевдовипадкові області.

З усього різноманіття варто звертати увагу на алгоритми впровадження ЦВЗ у вигляді бітової рядка. Використовуючи бітовий рядок, на відміну від псевдовипадкової послідовності (ПВП) чисел або зображення, скорочується кількість обчислювально складних операцій і прискорюється процес впровадження і вилучення, що є не менш важливим при досягненні мети

кваліфікаційної роботи. При цьому ідентифікувати бітову послідовність буде набагато краще, ніж ЦВЗ у вигляді зображення.

Варто відзначити перевагу в часі вбудовування у алгоритмів, які інтегровані в ланцюг кодування JPEG 2000. Такими алгоритмами є Li & Zhang [35], Meerwald [34], Ouled-Zaid, Makhloufi & Olivier [7] і Fan, Chiang & Shen [8]. При аналізі алгоритмів з табл. 1.1 було помічено, що два підходи вбудовування водяних знаків широко використовуються в сучасності. Одним з них є вбудовування даних у вейвлет коефіцієнти до стадії квантування, як в алгоритмі Ouled-Zaid, Makhloufi & Olivier. Інший працює безпосередньо при квантуванні індексів модуляції після процесу квантування. Це такі алгоритми як Li & Zhang, Meerwald і Fan, Chiang & Shen. Найбільші показники стійкості до зовнішніх впливів спостерігаються у алгоритмів Wang, Ouled-Zaid, Makhloufi & Olivier, Chirag-Ganesh і Li & Zhang. Саме з цими алгоритмами надалі будуть проводитись дослідження в рамках цієї роботи.

## 1.2 Аналіз стійкості ЦВЗ до зовнішніх впливів

### 1.2.1 Вплив стиснення з втратами на зображення

Цифрові зображення з вбудованим ЦВЗ можуть бути піддані навмисним змінам або випадковим завадам. Як було зазначено в розділі 1.1, зазвичай зображення викладаються в комп'ютерних мережах в форматах стиснення зі втратами. Тому потрібно передбачити, щоб вбудований ЦВЗ був стійкий до подібного стиску. В результаті спотворень при вбудовуванні, впливу випадкових і навмисних завад передачі, а також похибок при добуванні відновлене одержувачем повідомлення буде відрізнятися від оригіналу, і отриманий контейнер буде відрізнятися від початкового. Також контейнер обов'язково буде спотворюватися при встановленні приховуваного повідомлення. При збереженні зображення у форматі JPEG або JPEG 2000 вказується параметр якості, що задається в деяких умовних одиницях,

наприклад, від 1 до 100 або від 1 до 10. Більше число зазвичай відповідає кращій якості, мале число відповідає більш сильному стиску. На рис. 1.3,*а* показане початкове растрове зображення великого розміру, яке стисле за алгоритмом JPEG 2000 (рис. 1.3,*б*) і за алгоритмом JPEG (рис. 1.3,*в*) з однаковим коефіцієнтом якості.

*а* *б* *в*

Рисунок 1.3 – Початкове растрове зображення (*а*), стисле за алгоритмом JPEG 2000 (*б*) і JPEG (*в*)

Перше зображення має обсягом в 3 МБ, на другому і третьому обсяг зменшено до 150 кБ. При цьому якщо уважніше подивитися на третього зображення у форматі JPEG, то можна побачити видимі артефакти у вигляді решіток 8х8. Зображення, яке стисле за алгоритмом JPEG 2000, більш якісне, такими артефактами не володіє і більш схоже на початкове зображення.

На рис. 1.4 можна побачити частину наведеного зображення (рис. 1.3,*а*) стисненого з коефіцієнтом якості 30 по алгоритму JPEG (рис. 1.4,*а*) з видимими артефактами і JPEG 2000 (рис. 1.4,*б*).

Після втрати частини інформації детектор може не виявити ЦВЗ, який представлений у вигляді бітової послідовності або може виявити лише частину повідомлення. Тому потрібно заздалегідь передбачити на яких коефіцієнтах якості ЦВЗ буде стабільно детектуватися. Потрібно використовувати техніку багаторазового дублювання ЦВЗ, що підвищить його стійкість до стиснення зі

втратами, але повної гарантії збереження ЦВЗ все одно добитись не вийде. Велику небезпеку для цілісності ЦВЗ представляє стиснення JPEG 2000 при малих значеннях коефіцієнта якості, що призводить до значної втрати інформації зображення після стиснення.

*а* *б*

Рисунок 1.4 – Зображення, стислий за алгоритмом JPEG (*а*) і JPEG 2000 (*б*) з однаковим коефіцієнтом якості

На рис. 1.5,*а* показано зображення з високим коефіцієнтом якості, а на рис. 1.5,*б* – з більш низьким. Зрозуміло, що при стисненні як на правому зображенні ЦВЗ буде найімовірніше втраченим для детектора. Але слід зауважити, що таке зображення є й маловживаним для продажу.

Зловмисник не зможе використовувати таке зображення з метою отримання прибутку і, в такому випадку, неважливо чи є в ньому ЦВЗ.

*а* *б*

Рисунок 1.5 – Зображення з високим коефіцієнтом якості JPEG 2000 (*а*) і вкрай низьким (*б*)

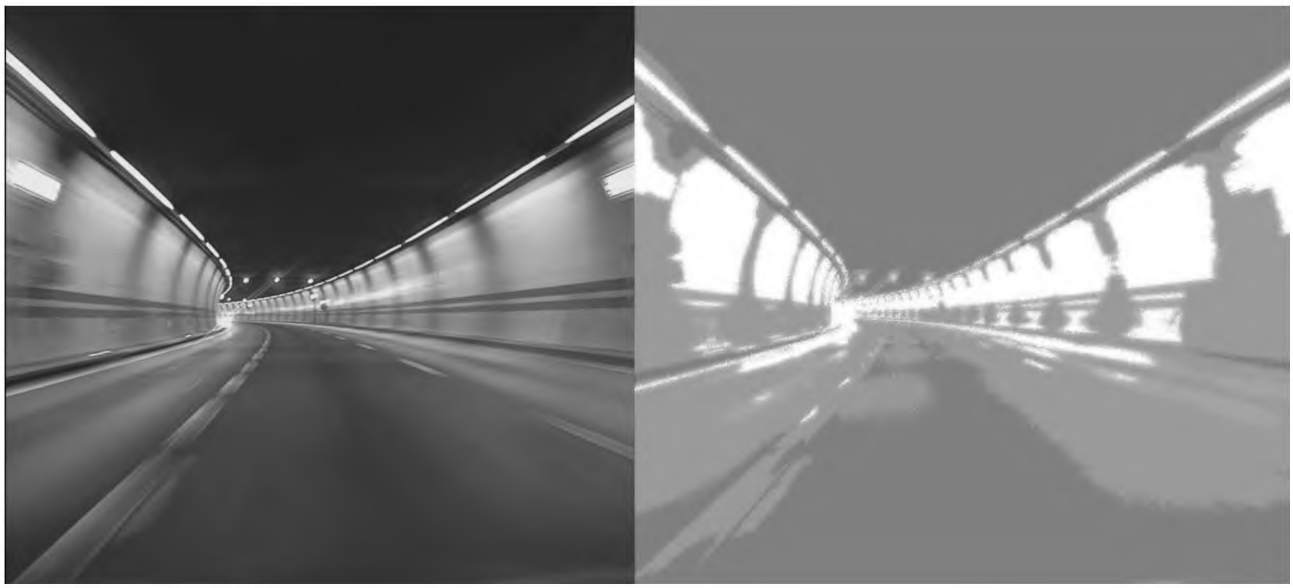
### 1.2.2 Інші зовнішні впливи на зображення

Крім стиснення зі втратами при роботі із зображеннями користувач може в редакторі (наприклад, Adobe Photoshop) додати колірні фільтри, шум, обрізати край, збільшити або зменшити зображення, перевернути або змінити формат. Наприклад, на рис. 1.6 для початкового зображення зліва було застосовано колірний фільтр і додано шум.

Така зміна не повинна призвести до знищення ЦВЗ, оскільки зображення зберегло комерційну цінність. ЦВЗ не буде і не повинен бути стійким до зовнішнього впливу на зображення-контейнер, при якому зображення буде зіпсовано остаточно. Якщо зробити високий колірний фільтр або вирізати більшу частину зображення, то ЦВЗ буде втрачено. Але при цьому і саме зображення втратить комерційний вигляд, і його буде неможливо виставляти на продаж в Інтернет магазині. Подібне зіпсоване зображення (велика кількість шуму і високий колірний фільтр) показано на рис. 1.7.

*а* *б*

Рисунок 1.6 – Початкове зображення (*а*) і змінене (*б*)



*а* *б*

Рисунок 1.7 – Початкове зображення (*а*) і зіпсоване (*б*)

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 і рівень скритності.

### 1.2.3 Параметри алгоритму, що впливають на стійкість до зовнішніх впливів

Здатність впровадженої в зображення інформації протистояти зовнішнім впливам на контейнер залежить від багатьох факторів, до основних з яких відносяться: алгоритм вбудовування, коефіцієнт сили вбудовування, кількість вбудовування одного й того ж біта інформації, вид і інтенсивність зовнішнього впливу. Зазвичай автор заздалегідь вибирає настройки, при яких будуть, на його думку, найбільш оптимальні показники при зовнішніх впливах. При цьому важливо не порушити скритність ЦВЗ і недооцінити пропускну здатність контейнера. Інакше ЦВЗ буде легко виявлений і буде порушено одне з важливих правил для стегоалгоритму – збереження скритності факту передачі вбудованого повідомлення. З огляду на ці моменти, може статися так, що ЦВЗ буде, припустимо, стійкий до фільтрації і зашумлення, але при цьому не стійкий до збільшення зображення (масштабованість). Тому потрібно заздалегідь визначити до яких зовнішніх впливів буде приділятися особлива увага при побудові системи. Одним з ключових параметрів алгоритму є коефіцієнт сили вбудовування. Його величина безпосередньо впливає як на стійкість впровадженої інформації, так і на скритність впровадження [3]. На рис. 1.8,*а* показано зображення з впровадженим ЦВЗ при низькому коефіцієнті вбудовування, а на рис. 1.8,*б* – вкрай високому, при якому видно артефакти від впровадження.

Чим вище значення коефіцієнта сили вбудовування, тим вище рівень спотворень, що вносяться в контейнер при самому вбудовуванні. Значення коефіцієнта сили вбудовування індивідуальне для кожного алгоритму. Іншим важливим параметром є розмір вбудованого ЦВЗ. При впровадження різних ЦВЗ необхідно переконатися, що рівень пропускної здатності зображення-контейнера достатній для впровадження повідомлення. Інакше може вийти так, що артефакти від впровадження також проявлять себе на контейнері.

*а* *б*

Рисунок 1.8 – Зображення з впровадженим ЦВЗ при низькому коефіцієнті вбудовування (*а*), поява артефактів при високому коефіцієнті (*б*)

### 1.2.4 Оцінка скритності впровадження

Вбудовування ЦВЗ має здійснюватись виходячи з умови забезпечення скритності впровадження. Як було зазначено вище, для вбудовування з метою захисту авторських прав не потрібно передбачати вкрай високий рівень скритності. Адже поліпшення скритності приведе до погіршення стійкості до зовнішніх впливів. Ці дві характеристики залежать одна від одної. Тому досить визначити рівень допустимих спотворень при вбудовуванні. Процес впровадження ЦВЗ повинен враховувати властивості системи сприйняття

людини. Властивості СЛЗ можна розділити на дві групи: низькорівневі (фізіологічні) і високорівневі (психофізіологічні). На поточний момент увагу варто приділяти обом групам властивостей. У минулому високорівневі властивості рідко розглядалися при побудові алгоритмів вбудовування [11]. У табл. 1.2 наведені основні властивості СЛЗ і обґрунтування впливу їх на сприйняття зображень людиною.

Таблиця 1.2 – Властивості СЛЗ і 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 більш чутлива до шуму в цьому діапазоні. |
| Частотна чутливість | СЛЗ набагато більш сприйнятлива до низькочастотного шуму, ніж до високочастотного. Це пов'язано з нерівномірністю амплітудно-частотної характеристики системи зору людини. |
| Ефект маскування | Полягає в збільшенні порога виявлення сигналу в присутності іншого сигналу, що володіє аналогічними характеристиками. Найбільш сильно ефект маскування проявляється, коли обидва сигнали мають однакову орієнтацію і місце розташування. |
| Високорівневі властивості СЛЗ | |
| Чутливість до контрасту | Висококонтрастні ділянки зображення і перепади яскравості звертають на себе більшу увагу. |
| Чутливість до розміру | Великі ділянки зображення помітніше менших розміром. Але існує поріг насичення, коли подальше збільшення розміру не істотно. |
| Чутливість до форми | Довгі і тонкі об'єкти звертають більшу увагу, ніж круглі однорідні. |
| Чутливість до кольору | Деякі кольори помітніше інших. Цей ефект посилюється, якщо фон заднього плану відрізняється від кольору фігур на ньому. |

| Властивість СЛЗ | Обґрунтування ефекту |
|---|---|
| Чутливість до місця розташування | Людина схильна в першу чергу розглядати центр зображення. |
| Підвищений увагу до зображень переднього плану | Люди уважніше до зображень переднього плану, ніж заднього. |
| Чутливість до зовнішніх подразників | Рух очей спостерігача залежить від конкретної обстановки, від отриманих ним перед переглядом або під час нього інструкцій, додаткової інформації. |

За допомогою побудови гістограм після впровадження ЦВЗ в зображення з різними коефіцієнтами сили вбудовування можна побачити зміни яскравості і 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 правильності експозиції, контрасті і кольоровому насиченні знімка, оцінити необхідну корекцію і при подальшій обробці. Зловмисник, який має при собі засоби для професійної роботи з зображеннями, може досить легко побачити невідповідності рівня яскравості в зображенні.

Для проведення оцінки потрібно вибрати алгоритм вбудовування та здійснювати запровадження ЦВЗ в зображення змінюючи силу вбудованого сигналу. На рис. 1.9,*а* приведено зображення без ЦВЗ, а на рис. 1.9,*б* – з вбудованим ЦВЗ за допомогою алгоритму Wang, де коефіцієнт сили вбудовування збільшений в півтора рази по відношенню до оптимального, який використовувався в алгоритмі. Як можна помітити, при збільшенні параметрів вбудовування гістограма дуже сильно відрізняється від початкової.

Використовуючи оптимальні параметри для алгоритму, було отримано гістограму, яка мало відрізняється від гістограми оригінального зображення.


*а* *б*

Рисунок 1.9 – Зображення без ЦВЗ (*а*) і з ЦВЗ при збільшеному коефіцієнті сили вбудовування (*б*)

Також для оцінки скритності впровадження можна використовувати метод експертної оцінки, але він суб'єктивний. Тому доцільно використовувати більш суворі математичні методи. Більшість показників спотворення відносяться до групи різницевих показників, які базуються на різниці між оригінальним контейнером і контейнером із вбудованим ЦВЗ [12]. Найбільш поширеним серед них є метод обчислення пікового відношення сигналу до шуму (Peak Signal to Noise Ratio, PSNR). Потрібно зробити розрахунок співвідношення між максимумом можливого значення сигналу і потужністю шуму, що спотворює значення сигналу. Як сигнал виступає зображення, а в якості шуму – ЦВЗ. При порівнянних потужностях приховуваного сигналу і шуму кваліфікованим зловмисником легко виявиться факт наявності ЦВЗ. Отже, в стегосистемах доводиться ховати приховуваний сигнал під більшим за величиною шумом прикриття. PSNR визначається таким чином:

$$PSNR = \frac{mn \cdot \max\limits_{i,j}\left(I_{i,j}\right)^2}{\sum\limits_{i,j}\left(I_{i,j} - K_{i,j}\right)^2}, \tag{1.1}$$

де m, n – розмір зображення; $I_{i,j}$ – значення пікселя зображення оригіналу; $K_{i,j}$ – значення пікселя зображення після додавання шуму.

Зазвичай відношення сигнал / шум (Signal to Noise Ratio, SNR) виражається в децибелах. Нормальними значеннями для зображень після стиснення є значення в межах від 25 до 50 дБ для різних груп зображень. Для темних оптимальним значенням є від 25 до 35 дБ, для середніх по яскравості цей діапазон буде від 30 до 40 дБ, а для світлих від 40 до 50 дБ. Досягти заданого рівня PSNR можна за допомогою зміни коефіцієнта сили вбудовування або розміру вбудованого повідомлення. При неможливості досягнення встановленої PSNR, шляхом зміни обраного параметра, необхідно визначити граничне значення параметра. Було проведено дослідження скритності впровадження для алгоритмів Wang, Ouled-Zaid, Makhloufi & Olivier, Chirag-Ganesh і Li & Zhang. Для різних груп зображень було виявлено, що при вбудовуванні однакових ЦВЗ при оптимальному зазначеному в алгоритмі коефіцієнті сили вбудовування їх SNR зі збільшенням стиснення буде збільшуватися. Результати показані в табл. 1.3.

Таблиця 1.3 – Оцінка скритності впровадження

| **Алгоритм** | **Група зображень** | **Коефіцієнт якості JPEG 2000,%** | **SNR, дБ** |
|---|---|---|---|
| Chirag-Ganesh | Світлі | 50 | 51.5 |
| | | 70 | 48.9 |
| | | 90 | 46.2 |
| | Середні за яскравістю | 50 | 40.3 |
| | | 70 | 37.3 |
| | | 90 | 35.1 |
| | Темні | 50 | 34.7 |
| | | 70 | 31.9 |
| | | 90 | 27.3 |
| Li & Zhang | Світлі | 50 | 49.2 |

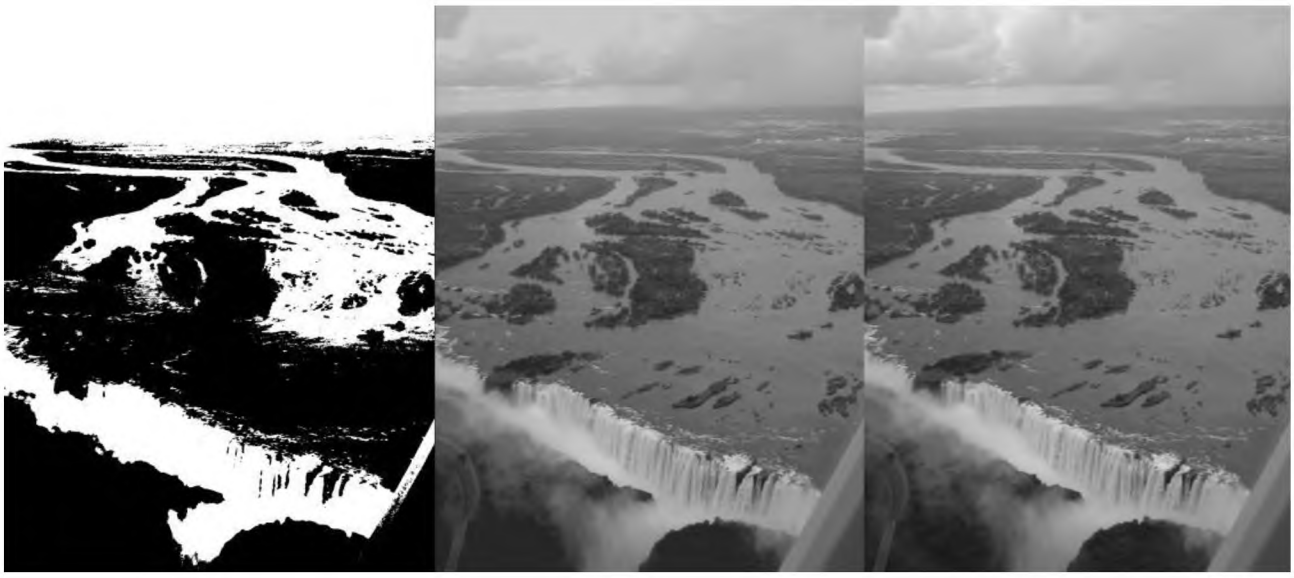
| Алгоритм | Група зображень | Коефіцієнт якості JPEG 2000,% | SNR, дБ |
|---|---|---|---|
| | | 70 | 47 |
| | | 90 | 45.5 |
| | Середні за яскравістю | 50 | 39.8 |
| | | 70 | 36.4 |
| | | 90 | 33.6 |
| | Темні | 50 | 34.1 |
| | | 70 | 31 |
| | | 90 | 27.6 |
| Wang | Світлі | 50 | 47.8 |
| | | 70 | 46.5 |
| | | 90 | 43 |
| | Середні за яскравістю | 50 | 38.4 |
| | | 70 | 35 |
| | | 90 | 32 |
| | Темні | 50 | 33.5 |
| | | 70 | 30.2 |
| | | 90 | 26.6 |
| Ouled-Zaid, Makhloufi & Olivier | Світлі | 50 | 52.2 |
| | | 70 | 49.4 |
| | | 90 | 46.7 |
| | Середні за яскравістю | 50 | 41.4 |
| | | 70 | 37.8 |
| | | 90 | 36.5 |
| | Темні | 50 | 36.4 |
| | | 70 | 32.9 |
| | | 90 | 28.2 |

Як можна побачити з табл. 1.3, впровадження ЦВЗ в зображення з більшим ступенем стиснення буде призводити до все більшої втрати скритності

впровадження і виявлення артефактів від вбудовування. При цьому оптимальний рекомендований коефіцієнт сили вбудовування у них різниться між собою.

### 1.2.5 Оцінка пропускної здатності зображення-контейнера

Зображення мають різний обсяг, тип і кількість областей, куди може бути впроваджено ЦВЗ, враховуючи умову забезпечення оптимального рівня скритності впровадження. Крім того, різні стегоалгоритми здійснюватимуть впровадження інформації в строго певні види зображень і області в них. Зображення можуть бути напівтоновими, бінарними, кольоровими тощо. На рис. 1.10 показані різні типи зображень.



*а* *б* *в*

Рисунок 1.10 – Бінарне (*а*), напівтонове (8-ми бітна шкала) (*б*) і кольорове (*в*) зображення

Розроблений для напівтонових зображень алгоритм може демонструвати погані показники стійкості або виявитися зовсім непридатним до використання з кольоровими зображеннями. Тому потрібно при оцінці заздалегідь визначитися з типом зображень і їх пропускною спроможністю. Для подальших

досліджень використовувались саме кольорові растрові зображення, оскільки саме вони частіше представляють комерційну цінність і виставляються на продаж. Під пропускною здатністю каналу передачі приховуваних повідомлень розуміють 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 приховуваних повідомлень, навмисного введення хибних повідомлень або руйнування вбудованої в контейнер інформації без втрати комерційного виду контейнера. Різні зображення-контейнери, можуть мати абсолютно різні характеристики. Для отримання адекватних результатів оцінки стійкості необхідно провести вибір відповідних зображень і аналіз пропускної здатності контейнера. Прихована пропускної здатність буде визначатися як:

$$C = 0.5 * \log_2\left(1 + \frac{\sigma_M^2}{\sigma_{\tilde{X}}^2 + \sigma_P^2}\right), \tag{1.2}$$

де $\sigma_M^2$ – потужність вбудованого сигналу; $\sigma_{\tilde{X}}^2$ – потужність контейнера; $\sigma_P^2$ – потужність шуму, який додається при стисненні.

Контейнер і шум стиснення мають нормальний розподіл. тоді обидва джерела шуму можна об'єднати в одне джерело $z$ з дисперсією $\sigma_Z^2 = \sigma_{\tilde{X}}^2 + \sigma_P^2$.

При здійсненні вкладення приховуваної інформації в контейнер допускається спотворення початкового зображення до величини пікового SNR, який був вирахуваний вище. Кількість біт / піксель для звичайного JPEG 2000 зображення становить 25. Амплітуди відліків рівномірно розподілені в діапазоні значень від 0 до 255 з дисперсією $\sigma_{\tilde{X}}^2$.

Для подальших розрахунків використовувалось програмне середовище Matlab, яке надає відмінні можливості по цифровій обробці зображень. За допомогою Matlab можна зробити розрахунки по потужності контейнера і шуму. Розподіл шуму стиснення проходить по гаусівському закону. Проведемо

оцінку пропускної здатності зображення JPEG 2000 з показником якості 50%. Для проведення оцінки буде використовуватись алгоритм вбудовування Chirag-Ganesh, при цьому коефіцієнт сили вбудовування буде використовуватися, як вказано в описі алгоритму. Тоді якщо взяти світле зображення з розмірами 1000x800 і розміром 900 кБ, використовуючи вбудовування ЦВЗ за алгоритмом Chirag-Ganesh, то можна розрахувати $\sigma^2_{\tilde{X}}$, яка буде дорівнювати 56. Тоді допустима потужність прихованого повідомлення дорівнює $\sigma_M^2$ =6.7. Підсумкова пропускна здатність становитиме C=2146 біт. Треба зауважити, що для систем вбудовування ЦВЗ висока ємність вбудовування менш важлива на відміну від систем прихованої передачі даних. Пропускна здатність для чотирьох обраних при огляді алгоритмів була розрахована для 5 різних розмірностей зображення при різних ступенях коефіцієнта якості JPEG 2000 і результати показані в табл. 1.4. Спотворення вихідного зображення при встановленні ЦВЗ і стисненні з втратами до величини пікового відношення сигнал / шум становитиме 46,8 дБ. Таке спотворення буде непомітно для ока людини, як було досліджено вище.

Таблиця 1.4 – Оцінка пропускної здатності

| **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 |
| | | 90 | 2870 |
| | 3400x2200 | 50 | 16010 |

| Алгоритм | Розміри зображення, пікселі | Коефіцієнт якості JPEG 2000,% | Загальна прихована пропускна здатність зображення, біт |
|---|---|---|---|
| | | 70 | 16950 |
| | | 90 | 18106 |
| Li & Zhang | 521x512 | 50 | 1 256 |
| | | 70 | 1420 |
| | | 90 | 1 650 |
| | 640x520 | 50 | 1465 |
| | | 70 | 1640 |
| | | 90 | 1870 |
| | 800x800 | 50 | 1 984 |
| | | 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 |
| Ouled-Zaid, Makhloufi & Olivier | 521x512 | 50 | 1430 |
| | | 70 | 1705 |
| | | 90 | 1900 |
| | 640x520 | 50 | 2430 |
| | | 70 | 2664 |
| | | 90 | 2807 |
| | 800x800 | 50 | 2510 |

| Алгоритм | Розміри зображення, пікселі | Коефіцієнт якості JPEG 2000,% | Загальна прихована пропускна здатність зображення, біт |
|---|---|---|---|
| | | 70 | 2730 |
| | | 90 | 3010 |
| | 1000x800 | 50 | 2950 |
| | | 70 | 3150 |
| | | 90 | 3550 |
| | 3400x2200 | 50 | 17220 |
| | | 70 | 18900 |
| | | 90 | 20406 |

Як можна побачити з табл. 1.4, при стисненні зображень з більш високим коефіцієнтом стиснення потужність шуму стиснення істотно зростає, і при цьому прихована пропускна здатність зменшується. При збільшенні шуму обробки при стисненні зображень величина прихованої пропускної здатності зменшується плавно.

### 1.2.6 Оцінка стійкості вбудованої інформації до зовнішніх впливів

Визначивши оптимальний рівень прихованої пропускної здатності і скритності впровадження можна переступити до оцінки стійкості до зовнішніх впливів, при яких ці рівні не порушуватимуться. Але для початку потрібно визначитися з тестовими даними, застосовуваними зовнішніми впливами і методикою проведення цієї оцінки. Існує безліч зовнішніх впливів, які можна застосувати до зображення. При проведенні аналізу важливо дотримуватись однакового діапазону інтенсивності впливу. Крім того, зовнішній дії повинно піддаватися все зображення-контейнер. Спочатку потрібно поставити мінімальне значення зовнішнього впливу і крок, з яким воно буде змінюватися. Вбудовування повинно проводитися з урахуванням збереження оптимальних параметрів скритності впровадження. Як було вже зазначено вище, для кожної групи зображень він буде відрізнятися при різних алгоритмах. При впровадженні буде використовуватися коефіцієнт сили вбудовування, при

якому буде збережено оптимальний рівень скритності для кожного алгоритму. Для проведення дослідження використовується програмне середовище MATLAB, як і в минулих пунктах розділу, оскільки воно надає значні засоби для цифрової обробки зображень і автоматизації завдання застосування зовнішніх впливів з певним кроком його зміни і побудови результуючого графіка.

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

1. ЦВЗ впроваджується в зображення-контейнер.

2. Контейнер піддається зовнішньому впливу.

3. ЦВЗ витягується з зображення-контейнера.

4. Витягнутий ЦВЗ порівнюється із оригінальним, і визначається ступінь їх відповідності.

Оцінка стійкості буде виконуватися за допомогою коефіцієнта помилкових біт (Bit Error Rate, BER). BER гарно підходить для оцінки спотворень в бітовій послідовності, якою у даному випадку й є ЦВЗ. Обчислюється даний коефіцієнт за формулою:

$$BER(S,S_1)=\frac{\sum p_i}{N};\ \ p_i=\begin{cases}1, & якщо\ \ \mathrm{S}\neq \mathrm{S}_1\\ 0, & якщо\ \ \mathrm{S}=\mathrm{S}_1\end{cases}, \tag{1.3}$$

де $S$ – $j$-й біт оригіналу вбудовуваного рядка; $S_1$ – біт витягнутого рядка; $N$ – загальна кількість біт.

При значенні коефіцієнта, що дорівнює 0, впроваджена і витягнута інформація повністю ідентичні. При значенні, рівному 1, кожен біт оригіналу не відповідає витягнутому. Для бітового рядку ACII символів значення BER>0.12 означає втрату більшої частини вбудованої інформації, тобто можна говорити про те, що ми не зможемо відновити початковий ЦВЗ. На рис. 1.11 показана блок-схема методики оцінки стійкості ЦВЗ до одного виду зовнішнього впливу на зображення-контейнер.

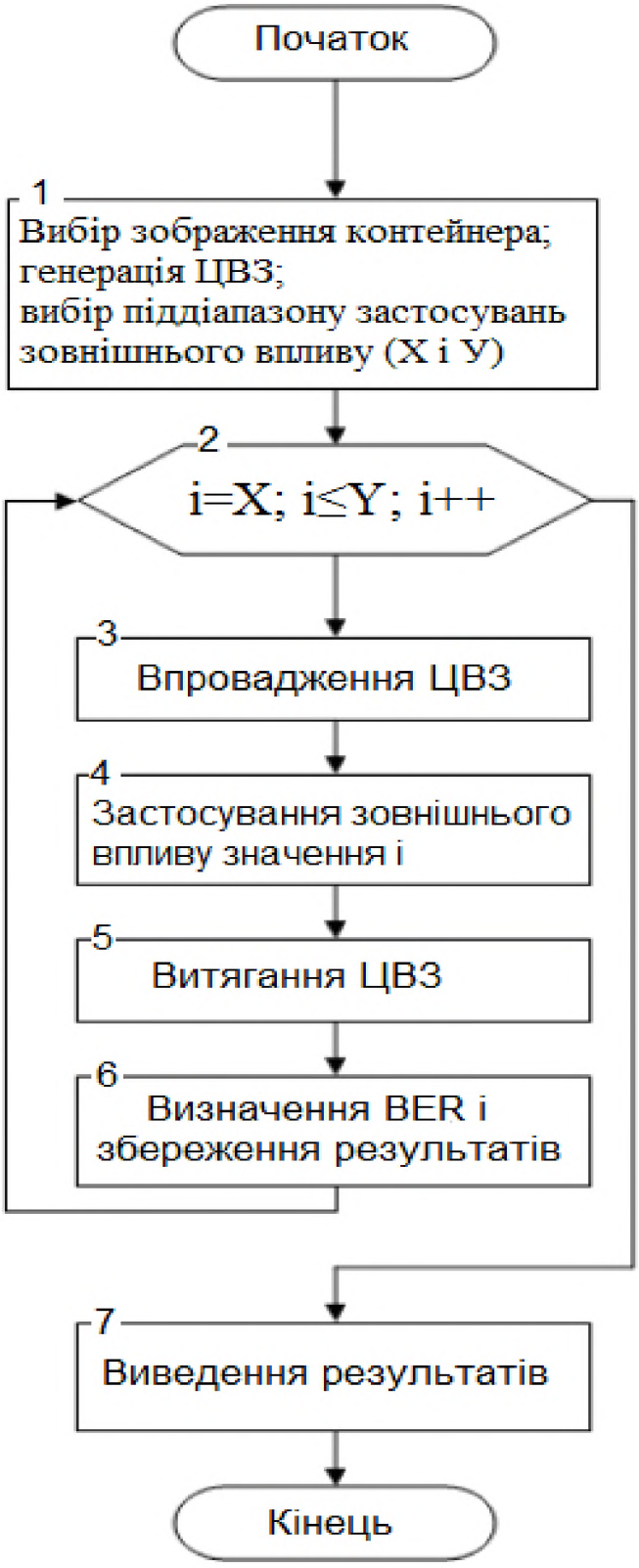



Рисунок 1.11 – Блок-схема методики оцінки стійкості ЦВЗ до зовнішніх впливів на зображення-контейнер

### 1.2.7 Результати аналізу стійкості ЦВЗ до зовнішніх впливів на зображення-контейнер

Дослідження проводилося для чотирьох алгоритмів вбудовування в область ДВП: Wang, Ouled-Zaid, Makhloufi & Olivier, Chirag-Ganesh та Li & Zhang. Для більш точної оцінки будемо здійснювати її на різних зображеннях, які будуть при цьому мати однаковий розмір. Було вибрано 4 світлих, 4 темних і 4 середніх по яскравості растрових зображень з розмірами 1000x800 пікселів. Як ЦВЗ краще використовувати псевдовипадкову інформацію однакового розміру, яка не перевищуватиме рівня максимальної прихованої пропускної здатності для зображення. Було вирішено використовувати ЦВЗ в 1024 біт. Такий ЦВЗ не перевищує рівень максимальної прихованої пропускної при зменшеному розмірі зображення для усіх чотирьох алгоритмів, що було обчислено в пункті 1.2.6.

В якості зовнішніх впливів використовувались найбільш популярні дії по зміни зображень: зашумлення зображення білим гаусівським шумом, масштабування, стиснення JPEG 2000 зі втратами, вирізання частини і фільтрація. Всі ці дії будуть сильно спотворювати зображення. Після проведення оцінки для одного типу зовнішнього впливу, дані, які отримані для різних зображень, будуть трохи відрізнятися, тому вони усереднювались для підсумкової оцінки.

Для перевірки стійкості до стиснення JPEG 2000 зображення із вбудованим ЦВЗ піддавалося стиску у всьому діапазоні значень коефіцієнта якості JPEG 2000 від 0 до 100. Глибина виконання ДВП для всіх алгоритмів була обрана трьохрівневою, а вбудовування здійснювалось в піддіапазоні максимальної глибини розкладання. Результати відношення BER від коефіцієнта якості JPEG 2000 показані на рис. 1.12. Для зручності на графіку горизонтальною пунктирною лінією показаний граничний рівень BER=0.12, при якому ми не зможемо відновити вбудовану інформацію.

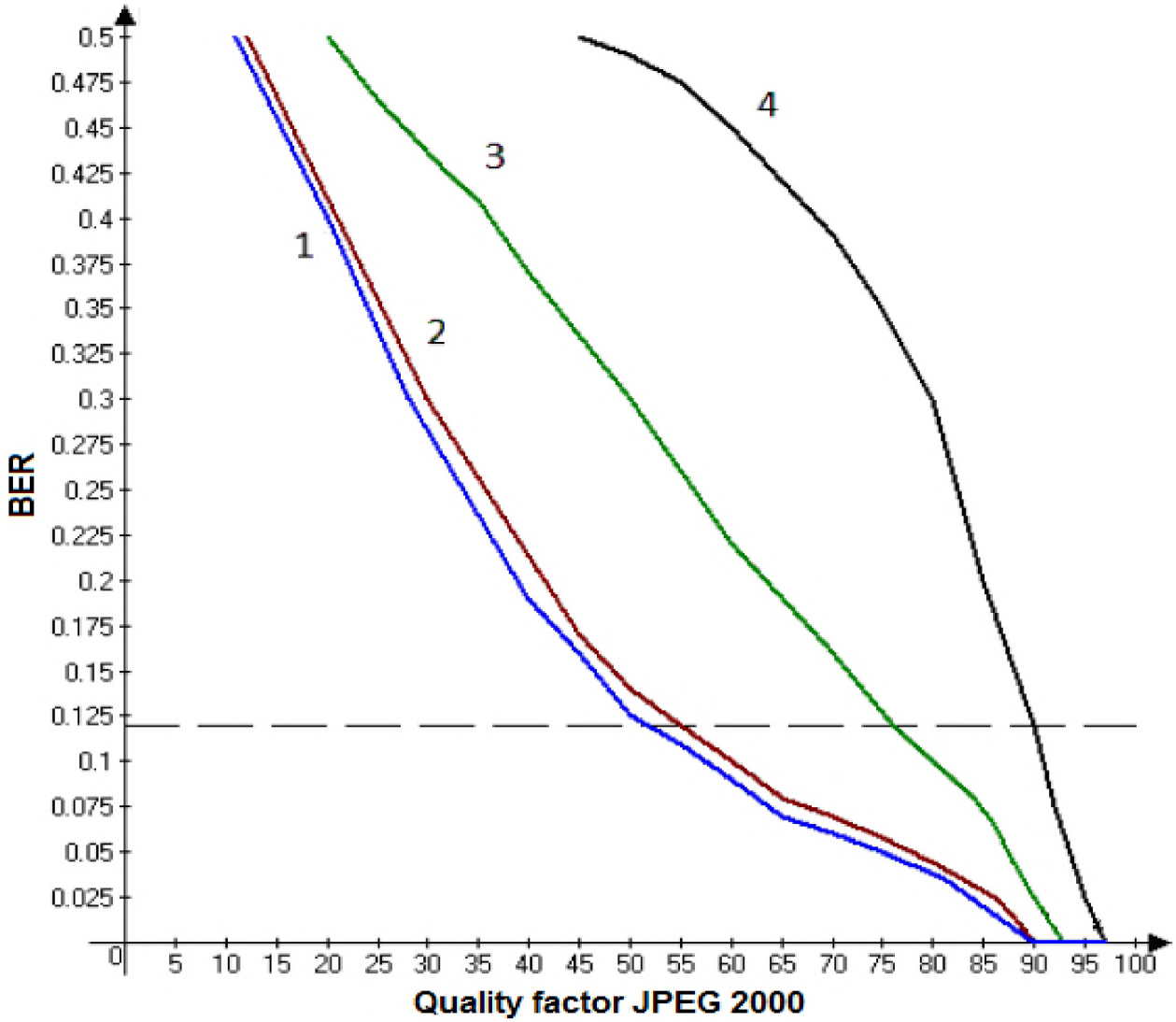



Рисунок 1.12 – Оцінка стійкості ЦВЗ до стиснення JPEG 2000 зі втратами: 1 – алгоритм Ouled-Zaid, Makhloufi & Olivier, 2 – алгоритм Chirag-Ganesh, 3 – алгоритм Li & Zhang, 4 – алгоритм Wang

Встановлено, що найкращі показники стійкості до ДВП мають алгоритми Chirag-Ganesh і Ouled-Zaid, Makhloufi & Olivier (рис. 1.12). Вбудовування ЦВЗ відбувається в низькочастотні LL і LH піддіапазони при цих алгоритмах. Алгоритм Wang, при якому відбувається вбудовування в високочастотний піддіапазон HH, показує найгірші результати стійкості до стиснення JPEG 2000, а алгоритм Li & Zhang, при якому модифікуються коефіцієнти в залежності від цільової швидкості бітового потоку, показує більш кращі результати. Тобто, при встановленні ЦВЗ в низькочастотні піддіапазони буде досягнутий більш високий показник стійкості до стиснення зі втратами JPEG 2000.

Для аналізу змін вейвлет коефіцієнтів при зашумленні зображення вносився гаусівський шум з нульовим середнім значенням і різними значеннями відхилення, що змінюються від 0 у бік зростання, поки деградація зображення не досягне неприйнятного рівня для використання. Результати показані на рис. 1.13. Найкращою стійкістю до цього виду впливу показав алгоритм Li & Zhang. Слід зазначити, що всі алгоритми демонструють приблизно однаково слабкі показники стійкості до цього виду зовнішньої дії.

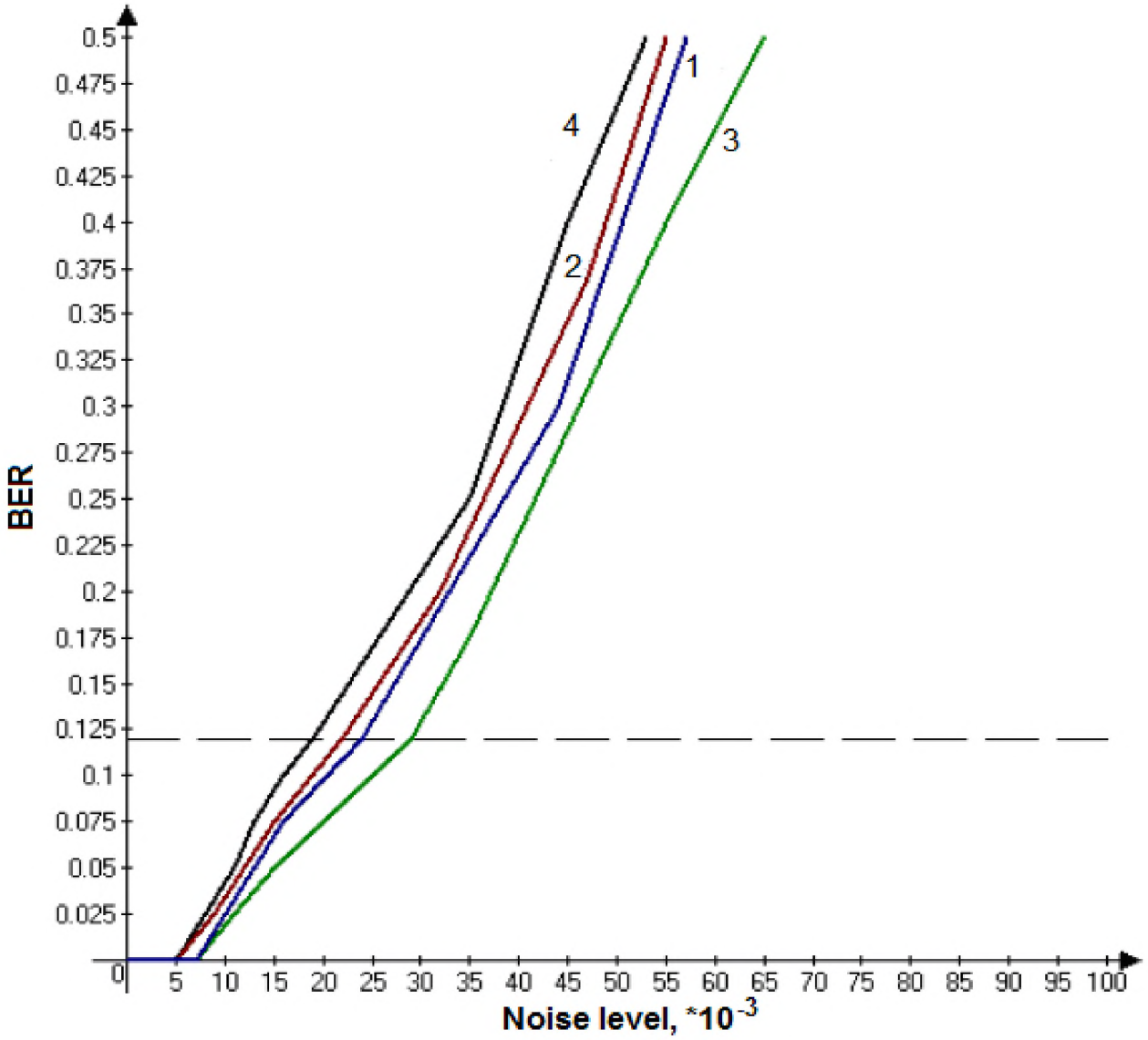



Рисунок 1.13 – Стійкість ЦВЗ до зашумлення: 1 – алгоритм Ouled-Zaid, Makhloufi & Olivier, 2 – алгоритм Chirag-Ganesh, 3 – алгоритм Li & Zhang, 4 – алгоритм Wang

В ході дослідження з масштабуванням зображення-контейнер стискалося до різних розмірів аж до 8 разів. Зчитувати повідомлення зі стисненого зображення неприйнятно, не зменшивши пропорційно розмір блоків, на які розбивається зображення. Зображення відновлювалось до початкового розміру, і тільки потім виконувалося зчитування ЦВЗ. Тільки при алгоритмі Quled-Zaid, Makhloufi & Olivier вдалося повністю відновити ЦВЗ при стисненні в 3 рази. Для інших алгоритмів граничним значенням, при якому BER менше 0.12, є стиснення в 2 рази. Всі ці алгоритми виявились не особливо стійкими до подібного виду впливу.

Для аналізу стійкості ЦВЗ при фільтрації з великого різноманіття фільтрів для цифрових зображень було обрано контрастний фільтр, що підвищує різкість зображення. У редакторах зображень діапазон зміни зазвичай представляється від -100 до 100, але для оцінки було проведено дослідження в діапазоні зміни від 0 до 100. Результати показані на рис. 1.14. Найкращі результати показав алгоритм Quled-Zaid, Makhloufi & Olivier.

Для аналізу стійкості до вирізання частини зображення був обраний діапазон зміни від 0 до 80% з кроком в 10%. Зрозуміло, що можна обрізати з усіх боків зображення, тільки з одного або зовсім взяти область в середині, і при цьому результати при оцінці будуть різні. Було вирішено проводити вирізку частини зображення зліва направо, 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 вирізання більше 20% виявилося фатальним. Алгоритми Chirag-Ganesh і Ouled-Zaid, Makhloufi & Olivier виявилися більш стійкими до подібного виду впливу, і відновити сполучення вдалося під час вирізання 30% зображення.

Підвівши підсумки, можна сказати що алгоритми, де вбудовування здійснюється в низькочастотні піддіапазони, мають кращі показники по стійкості до зовнішніх впливів. Однак вони ж мають менші показники по

скритності впровадження. Усі з досліджуваних алгоритмів виявилися погано стійкими до зашумлення і масштабування. Показники при стисненні JPEG 2000 виявилися несподівано невисокими.

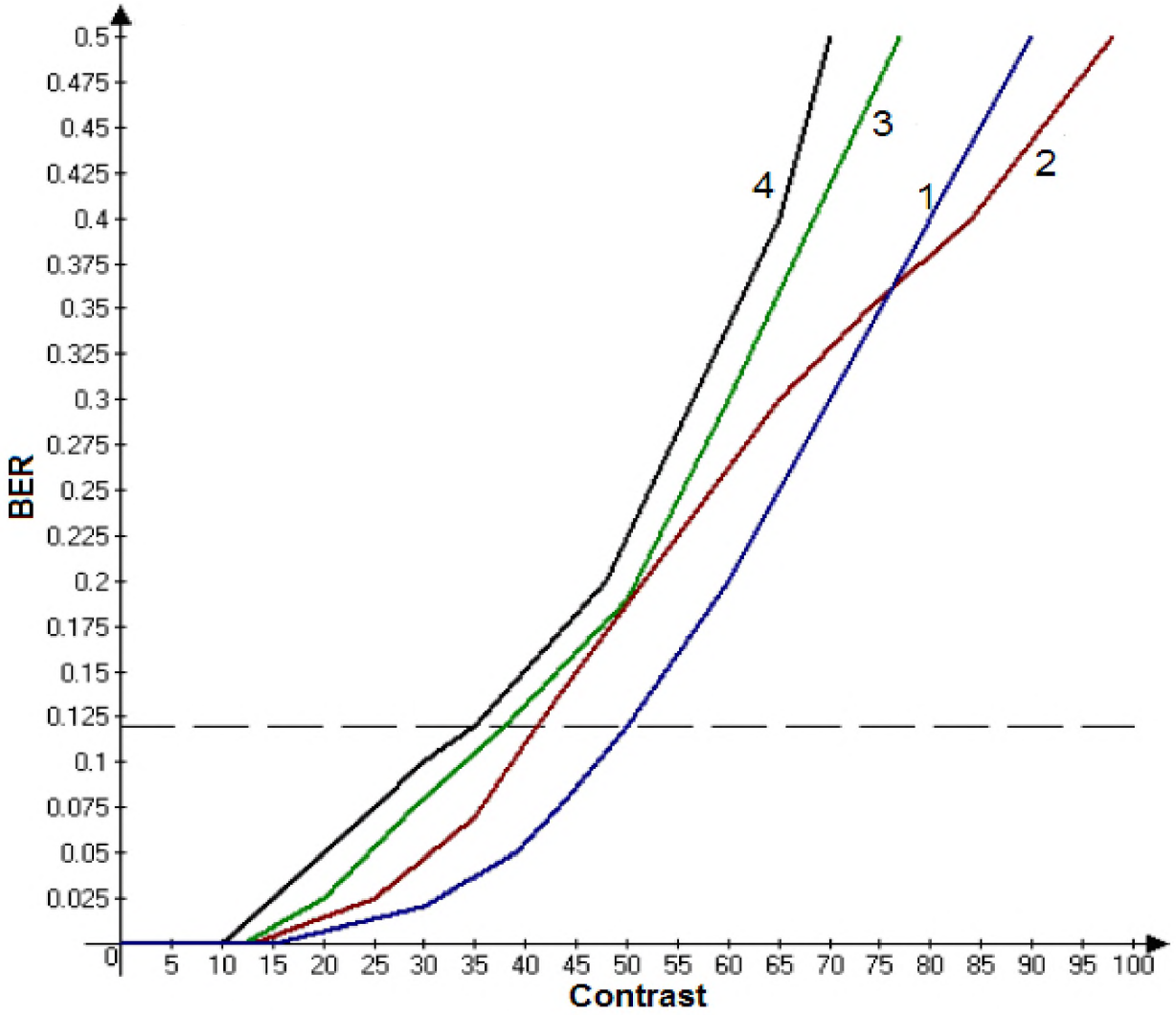



Рисунок 1.14 – Стійкість ЦВЗ до фільтрації:
1 – алгоритм Ouled-Zaid, Makhloufi & Olivier, 2 – алгоритм Chirag-Ganesh,
3 – алгоритм Li & Zhang, 4 – алгоритм Wang

## 1.3 Висновок. Постановка задачі

Розглянуто основні вимоги, що пред'являються до систем вбудовування та зчитування ЦВЗ і компоненти, які повинна включати в себе така система.

Для реалізації стегосистеми з метою захисту авторських прав треба найбільш уважно поставитися до питання стійкості ЦВЗ при зовнішніх впливах на зображення-контейнер. Наразі не всі існуючі алгоритми мають хороші показники стійкості до зовнішніх впливів.

Розглянуто основні області застосування ЦВЗ. Найбільш популярною областю є вбудовування з метою захисту авторських прав, і саме цій області присвячена кваліфікаційна робота.

Проаналізовано використовувані типи ЦВЗ і контейнерів для нього. Для подальшої роботи обрано фіксований контейнер у вигляді зображень у форматі стиснення зі втратами, які найбільш використовуються при передачі в комп'ютерних мережах. Використання ЦВЗ у вигляді бітової послідовності дозволить уникнути додаткових обчислювально складних операцій, дозволить приховати більший обсяг даних і буде набагато зручніше ідентифікуватися при детектуванні.

Розглянуто основні області вбудовування ЦВЗ. Найбільший інтерес викликає вбудовування в область ДВП. Саме ця область використовується при стисненні зі втратами у форматі JPEG 2000, який перевершує JPEG за якістю зображення і ступенями можливого стиснення.

Проведено аналіз існуючих популярних рішень вбудовування ЦВЗ в область ДВП. З усіх представлених алгоритмів обрано чотири найбільш стійких до зовнішніх впливів для подальших досліджень.

Розглянуто вплив параметрів вбудовування на стійкість до зовнішніх впливів і скритності впровадження. При збільшення обсягу ЦВЗ або сили вбудовування стійкість до зовнішніх впливів буде збільшуватися, а скритність падати.

Проведено оцінку скритності впровадження для чотирьох досліджуваних алгоритмів вбудовування. Знайдено оптимальні показники скритності.

Проведено оцінку максимальної прихованої пропускної здатності для досліджуваних алгоритмів вбудовування. Знайдено оптимальні показники.

Розроблено методику аналізу стійкості ЦВЗ до різних зовнішніх впливів на зображення-контейнер. Створено алгоритм для автоматизації процесу дослідження в програмному середовищі MatLab.

На основі методики порівняльного аналізу проведена оцінка стійкості до зовнішніх впливів для чотирьох досліджуваних алгоритмів, при якій не будуть порушені оптимальні показники скритності впровадження, знайдені раніше. В якості зовнішніх впливів були досліджені: зашумлення зображення білим гаусівським шумом, масштабування, стиснення JPEG 2000 зі втратами, вирізання частини і фільтрація.

За підсумками дослідження встановлено наступне. Алгоритми, де вбудовування здійснюється в низькочастотні піддіапазони, мають кращі показники по стійкості до зовнішніх впливів. Однак вони ж мають менші показники по скритності впровадження. Всі з досліджуваних алгоритмів виявились погано стійкими до зашумлення і масштабування. ЦВЗ, вбудований в найбільш стійкий алгоритм Ouled-Zaid, Makhloufi & Olivier буде втрачено при 50% стисненні зі втратами JPEG 2000, при цьому зображення збереже комерційну цінність. Знайдені показники виявилися несподівано невисокими і потребують поліпшення.

Отже, висновки, які отримані в цьому розділі, визначають подальші цілі і завдання, та підтверджують актуальність роботи.

Таким чином, для усунення недоліків існуючих алгоритмів необхідно:

• дослідити ланцюг кодування JPEG 2000 і знайти етапи, на яких відбувається основна втрата інформації при стисненні;

• розробити підходи і алгоритми підвищення стійкості ЦВЗ до зовнішніх впливів на зображення-контейнер;

• оцінити ефективність розроблених підходів і алгоритмів.

# 2 СПЕЦІАЛЬНА ЧАСТИНА

## 2.1 Алгоритми підвищення стійкості ЦВЗ до зовнішніх впливів на зображення-контейнер

### 2.1.1 Дослідження ланцюга кодування JPEG 2000 для можливості вбудовування ЦВЗ

Як зазначалося в огляді алгоритмів в розділі 1, наразі існують алгоритми вбудовування ЦВЗ, які інтегровані в ланцюг кодування JPEG 2000. Саме вони мають найбільший інтерес для подальших досліджень в цій області. Такі алгоритми мають перевагу перед іншими в швидкості впровадження ЦВЗ. З таких алгоритмів широко використовуються два підходи вбудовування прихованої інформації в цифрові зображення JPEG 2000. Одним з них є вбудовування даних у вейвлет коефіцієнти до стадії квантування. Стійкість до зовнішніх впливів при такому підході була досліджена на прикладі алгоритму Ouled-Zaid, Makhloufi & Olivier. Інший працює безпосередньо при квантуванні індексів після процесу квантування. Стійкість до зовнішніх впливів при такому підході була досліджена на прикладі алгоритму Li & Zhang.

Слід зазначити, що стандарт JPEG 2000 пропонує різні додаткові стадії, які можна включити в ланцюг, змінити або зовсім не використовувати. Є алгоритми, які будуть працювати, тільки якщо активовані ці додаткові стадії при кодуванні JPEG 2000, наприклад алгоритм Fan, Chiang & Shen, який працює тільки якщо ввімкнено кодування ROI.

Для розробки алгоритму підвищеної стійкості вбудованого ЦВЗ до зовнішніх впливів на зображення-контейнер було більш детально досліджено роботу кодера JPEG 2000. Спираючись на специфікацію формату і використовуючи програмне середовище MatLab, яке надає потужні можливості по цифровій обробці зображень, було проведено подальші дослідження і розрахунки для розробки алгоритму вбудовування ЦВЗ.

Стандарт стиснення JPEG 2000 ґрунтується на ДВП і забезпечує ряд важливих функцій, таких як варіатор дозволу і якості, більш краща стійкість до бітових похибок і виділеним регіонам кодування. Основні процедури кодування JPEG 2000 наведені на рис. 2.1.

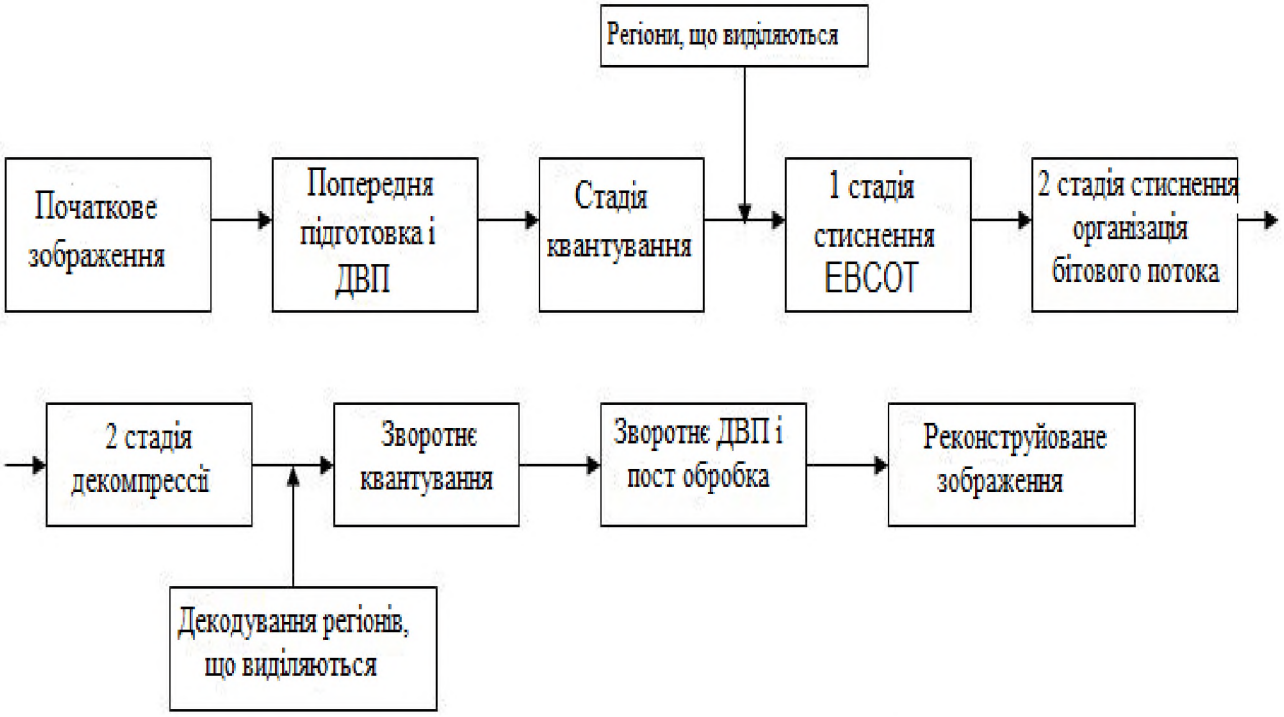



Рисунок 2.1 – Схема кодування JPEG 2000

По-перше, початкове зображення піддається деяким операціям попередньої обробки: зсув рівня і перетворення кольору. Зображення є набором невід'ємних цілих чисел. На етапі попередньої обробки з нього віднімають середнє. Крім того, якщо зображення великого розміру, то воно може бути розбите на частини. Тоді кожна частина стискається окремо. Далі відбувається перетворення зображення зі схеми RGB в схему YCrCb.

Далі зображення піддається послідовностям, що чергуються, вертикальних і горизонтальних одновимірних ДВП. Спочатку перетворюються всі рядки, а потім всі стовпці. На наступному етапі ліва верхня чверть матриці, яка вийшла в результаті попереднього перетворення знову перетворюється (спочатку всі рядки, потім все стовпці). Кількість етапів відповідає кількості

рівнів вейвлет-розкладання. Однорівневе ДВП сигналу $x$ отримують застосуванням набору певних фільтрів. Спочатку сигнал пропускається через низькочастотний фільтр з імпульсним відгуком $g$, і виходить згортка:

$$y[n] = (x * g)[n] = \sum_{k=-\infty}^{\infty} x[k]g[n-k] \quad . \tag{2.1}$$

Одночасно сигнал $x$ розкладається за допомогою високочастотного фільтра $h$. В результаті отримують деталізуючи коефіцієнти (після високочастотного фільтра) і коефіцієнти апроксимації (після фільтра низьких частот). Ці фільтри пов'язані між собою і називаються квадратурними дзеркальними фільтрами. Далі відліки сигналів можна прорідити в 2 рази:

$$y_{\text{low}}[n] = \sum_{k=-\infty}^{\infty} x[k]g[2n-k] \quad , \tag{2.2}$$

$$y_{\text{high}}[n] = \sum_{k=-\infty}^{\infty} x[k]h[2n-k] \quad . \tag{2.3}$$

Таке розкладання вдвічі зменшує дозвіл за часом в силу проріджування сигналу. Однак кожен з отриманих сигналів є половиною частотної смуги початкового сигналу, так що частотний дозвіл подвоюється. За допомогою оператора проріджування вищезгадані суми можна записати у вигляді:

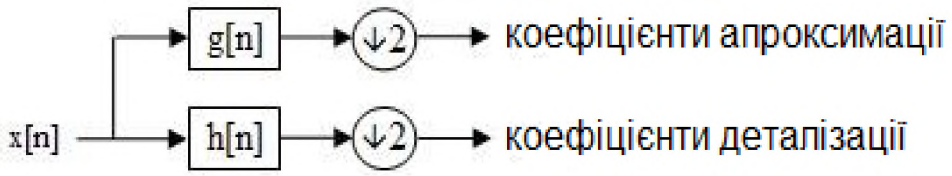
$$y_{\text{low}} = (x * g) \downarrow 2, \tag{2.4}$$

$$y_{\text{high}} = (x * h) \downarrow 2. \tag{2.5}$$

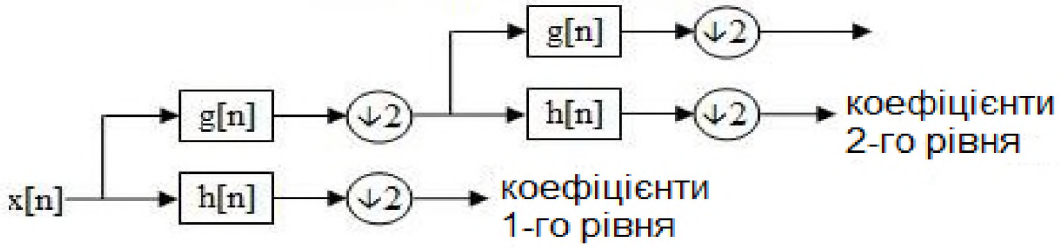
Розкладання можна повторити декілька раз для подальшого збільшення частотного дозволу з подальшим проріджуванням коефіцієнтів [15]. На рис. 2.2 показані приклади одновимірного і двовимірного розкладання.

В результаті перетворення зображення розбивається на прямокутники однакового розміру. Кожен з них стискається незалежно, використовуючи свій власний набір зазначених параметрів стиснення. Вони називаються частотними піддіапазонами, оскільки містять інформацію про те, як поводиться початковий двомірний сигнал при різному дозволі (тобто набір коефіцієнтів при різній частоті). З них розрізняються горизонтальний і вертикальний низькочастотний піддіапазон LL, горизонтальний високочастотний і вертикальний

низькочастотний піддіапазон HL, горизонтальний низькочастотний і вертикальний високочастотний піддіапазон LH і горизонтальний високочастотний і вертикальний високочастотний піддіапазон HH, які можуть бути організовані на підвищення рівня дозволу.




*а*




*б*

Рисунок 2.2 – Одномірне (*а*) і двовимірне (*б*) вейвлет-розкладання

Після цього вейвлет коефіцієнти квантуються. Саме на етапі квантування виникають основні інформаційні втрати, і саме за рахунок квантування можливе істотне зменшення обсягу представлення зображення. Після квантування можуть бути застосовані регіони кодування, які виділяються, але було вирішено не досліджувати цю можливість, оскільки вона мало використовувана на практиці. Далі квантовані вейвлет коефіцієнти для кожного піддіапазону розбиваються на невеликі прямокутні блоки, які називаються блоками коефіцієнтів, що підлягають кодуванню. Кожен кодовий блок кодується незалежно протягом першого рівня стадії кодування за допомогою кодувальника бітових площин. Це називається вкладеним блоковим кодуванням з оптимізованим урізанням (Embedded Block Coding with Optimized Truncation, EBCOT). Таким чином, кожен блок кодування має самостійний

потік бітів. Ці бітові потоки об'єднані в один потік і використовуються на другому рівні кодування, який ґрунтується на результаті етапу контролю швидкості генерації коду.

Ефективне співвідношення швидкості передачі і рівня спотворень алгоритму надає можливість усічення точок бітових потоків оптимальним способом, зводячи до мінімуму спотворення відповідно до будь-якої цільової швидкістю бітового потоку. Кодовані дані виводяться в кодовому потоці в пакети і файловий потік JPEG 2000 остаточно формується.

Наступні кроки забезпечать декомпресію стислих зображень. Після другого рівня декодування зображення потік бітів декодується EBCOT декодером. Далі вейвлет коефіцієнти відновлюються під час етапу зворотного квантування. Після зворотного ДВП і операцій кінцевої обробки виконується відновлення зображення.

Слід зазначити, що наразі реалізовано багато кодеків JPEG 2000, в яких підключені різні етапи кодування. Може бути присутнім етап виділення регіонів кодування, або можуть відрізнятися фільтри при застосування ДВП, алгоритм квантування і т.д. Можна самім задати параметри для більш оптимального вбудовування ЦВЗ, при якому стійкість ЦВЗ до зовнішніх впливів виявиться вище. Найбільший інтерес викликала можливість використання різних методів квантування коефіцієнтів і використання різних фільтрів при вейвлет-розкладанні. Саме застосування фільтрів і квантування впливає на незворотну втрату інформації при стисненні. Можуть бути використані дві групи фільтрів – оборотні та необоротні. Для досліджень, виконаних в рамках цієї роботи інтерес представляють саме незворотні фільтри, при яких відбудеться втрата інформації після стиснення. Треба зауважити, що рівень втрат при цьому буде вкрай низьким. Основна втрата інформації відбувається саме на стадії квантування, яка і буде далі розглянута більш докладно.

### 2.1.2 Втрата інформації при квантуванні для JPEG 2000

Квантувач відображає числовий сигнал з областю значень X в квантований сигнал області зі зменшеним числом значень. Це дає можливість представити квантовані величини з меншим числом біт у порівнянні з початковими неквантованими величинами. У кодері JPEG 2000 квантування може бути рівномірним скалярним або векторним з сітчастою геометрією. Скалярний квантувач відображає один вхідний семпл в одне квантоване значення на виході, а векторний квантувач відображає групу семплів на вході в групу квантованих величин. При цьому алгоритм JPEG 2000 дозволяє використовувати режим стиснення без втрат, при якому стадія квантування буде відключена.

Рівень втрат задається коефіцієнтом якості JPEG 2000, який має діапазон зміни від 0 до 100. Чим менше значення коефіцієнта, тим більше стиснення зображення і рівень втрат. Формула прямого перетворення при квантуванні має вигляд:

$$Q'_{(i,j)} = \left[ Q_{(i,j)} \frac{|Q_{(i,j)}|}{\Delta} \right] \operatorname{sgn}(Q_{(i,j)}), \tag{2.6}$$

де $Q'_{(i,j)}$ – квантоване значення коефіцієнта піддіапазона ДВП з координатами ($i$, $j$); $Q_{(i,j)}$ – оригінальне значення коефіцієнта піддіапазона ДВП з координатами ($i$, $j$); $\Delta$ – крок квантування; [] – знак округлення до найменшого цілого.

Інтервал можливих значень для квантованого і потім відновленого коефіцієнта піддіапазона ДВП представлений в формулі:

$$0{,}67 * Q_{(i,j)} < \Delta \leq 2 * Q_{(i,j)}. \tag{2.7}$$

Якщо величина змін коефіцієнтів піддіапазона ДВП, в результаті стиснення, починає перевищувати величину їх змін вироблених в процесі вбудовування ЦВЗ, то існує загроза втрати інформації вбудованого ЦВЗ. Квантування коефіцієнтів ДВП здійснюється з обраним кроком квантування,

що має єдине значення для цілого піддіапазона коефіцієнтів, при цьому найбільші втрати інформації зображення-контейнера будуть спостерігатися для високочастотних піддіапазонів нижніх рівнів розкладання.

Стандарт дозволяє використовувати квантування з сітчастою геометрією як заміну скалярному квантуванню. Квантування з сітчастою геометрією є конкретним видом векторного квантування. Варіант квантування з сітчастою геометрією, який використовується у другій частині стандарту JPEG 2000 є кодуванням ентропії квантування з сітчастою геометрією [17]. Єдиний квантувач з розміром кроку $\Delta$ розбивається на чотири підмножини – $D_0$, $D_1$, $D_2$ і $D_3$, які використовуються для позначення міток решітки. Два квантувача, пов'язані з кожним станом в решітці об'єднуються в союз квантувачів $A_0=D_0\cup D_2$, $A_1=D_1\cup D_3$. Кодова книга об'єднується з розміром кроку $\Delta$ і нульове кодове слово з'являється в двох підмножинах $D_0$ і $D_1$. У кожному стані в решітці, ми можемо вибрати один з двох квантувачів, що належать до об'єднаного квантувача і почати квантування вхідної послідовності $X$. Схема такого векторного квантування показана на рис. 2.3.

Процес квантування відбувається за допомогою алгоритму Вітербі для визначення шляху, щоб в решітці зводилося до мінімуму середньоквадратична похибка між вхідною послідовністю і вихідними кодовими словами. При квантуванні послідовно обробляється кадр за кадром, рухаючись по решітці, яка аналогічна тій, що використовується кодером. У кожен момент часу квантувач не знає, в якому вузлі знаходиться кодер. Він за прийнятою послідовність визначає найбільш правдоподібний шлях до кожного вузла і визначає відстань між кожним таким шляхом і прийнятою послідовністю.

Алгоритм Вітербі видає дві послідовності: перша є бінарною послідовністю, яка визначає мінімальний шлях спотворення; друга є послідовністю відповідних індексів квантування. Треба звертати увагу на побудову решітки, де найменш значущі біти кожного індексу $q(A_j)$ союзу квантувачів відповідають шляху, так як існує два можливих кодових слова для кожного індексу ($D_0$, $D_1$, $D_2$ і $D_3$).

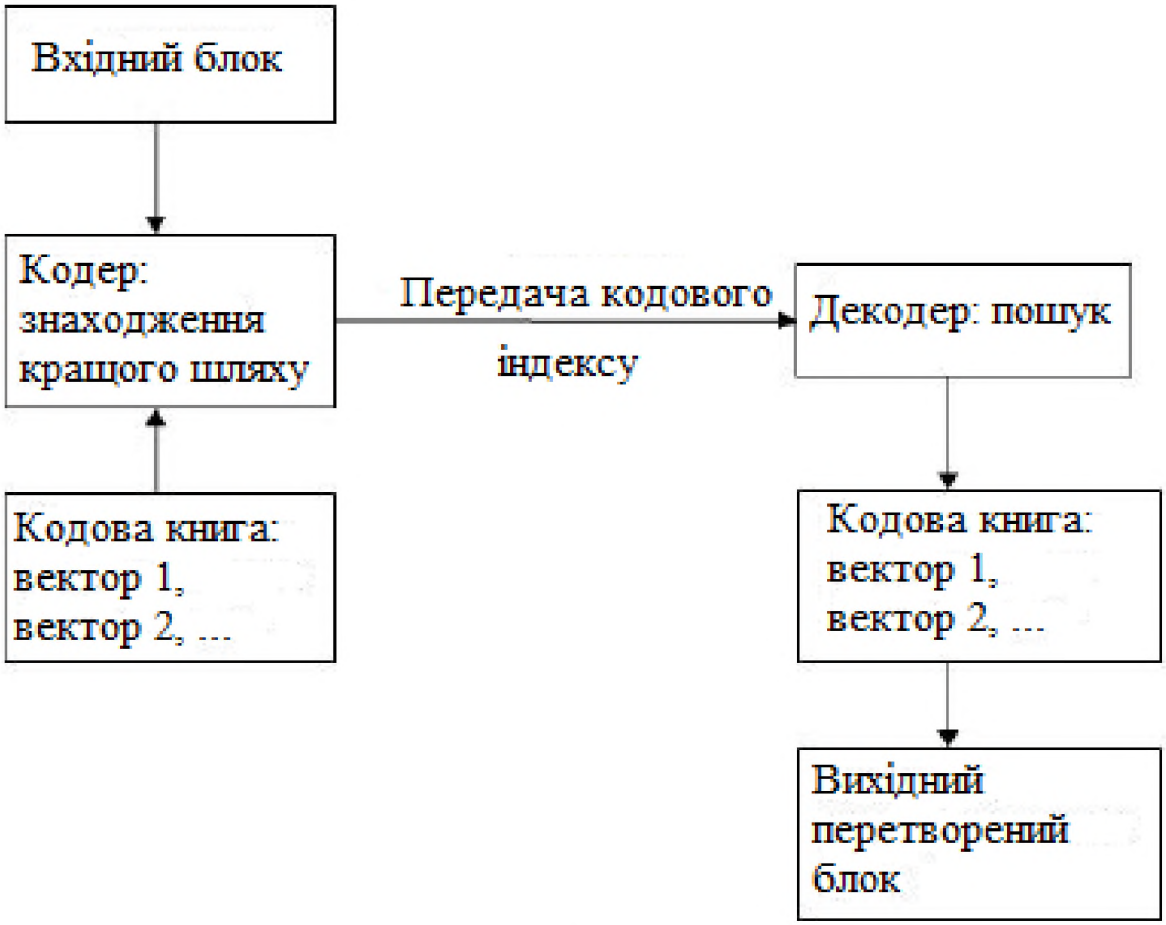



Рисунок 2.3 – Схема векторного квантування

Найменш значущі біти визначають шлях по решітці. З урахуванням початкового стану, а також конструкції решітки, індекси квантування з сітчастою геометрією об'єднаних квантувачів $A_0$ і $A_1$ надають всю інформацію, необхідну для реконструкції вейвлет коефіцієнтів. При дослідженні векторного квантування знайшлась можливість впроваджувати ЦВЗ під час цієї стадії. При використанні такого квантування підвищується швидкість роботи алгоритму стиснення зі втратами JPEG 2000 на відміну від скалярного квантування. Якщо провести вбудовування при такому квантуванні, то можна відразу підвищити скритність впровадження і стійкість до стиснення зі втратами за рахунок можливості знаходження вірних шляхів в решітці квантування.

### 2.1.3 Алгоритм вбудовування ЦВЗ під час стадії квантування

При детальному дослідженні векторного квантування була знайдена можливість заміни класичних компонентів квантування з сітчастою геометрією в JPEG 2000 кодері і декодері на гібридний модуль, який зможе виконувати одночасно квантування і впровадження водяного знака. Така техніка буде не залежати від шляхів в решітці і дозволить одночасно квантувати вейвлет коефіцієнти і вбудовувати ЦВЗ без інтеграції додаткових стадій для впровадження ЦВЗ в ланцюзі кодування / декодування JPEG 2000. Схема спільної схеми вбудовування водяних знаків під час кодування JPEG 2000 показана на рис. 2.4.

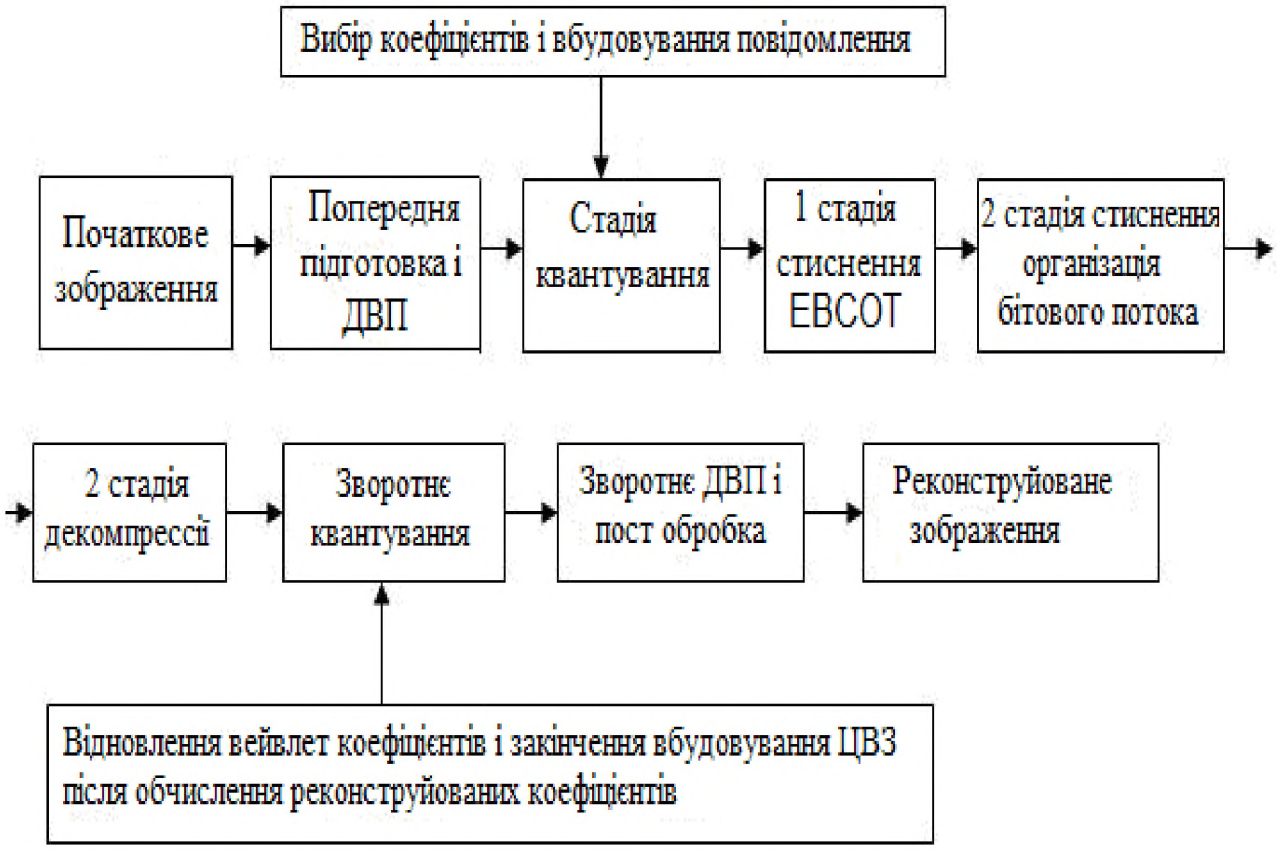



Рисунок 2.4 – Поєднана з квантуванням схема вбудовування ЦВЗ

Одним з найважливіших параметрів для розгляду є вибір вейвлет-коефіцієнтів, які повинні бути включені в процес впровадження ЦВЗ.

Специфікація алгоритму JPEG 2000 визначає, що коефіцієнти низькочастотних піддіапазонів ДВП піддаються меншим змінам, ніж коефіцієнти високочастотних піддіапазонів рівного рівня розкладання. З іншого боку, зміна коефіцієнтів високочастотних піддіапазонів менше впливає на якість зображення. Після вейвлет розкладу, LL піддіапазони з низькими частотами є найбільш значущими даними в перетвореному зображенні. Для того щоб уникнути значного погіршення якості в реконструйованому зображенні, вирішено не використовувати вейвлет коефіцієнти цього піддіапазону для процесу вбудовування ЦВЗ. Було вирішено впроваджувати ЦВЗ в HL, LH та HH детальні піддіапазони двох найвищих обраних рівнів розкладання. Незважаючи на те, що ці піддіапазони піддаються великим змінам при квантуванні, зі збільшенням рівня вейвлет-розкладання вийде досягти баланс в скритності впровадження за рахунок невикористання LL піддіапазонів, і стійкості до зовнішніх впливів. Корисне навантаження ЦВЗ визначається числом детальних піддіапазонів, які включені в процес нанесення водяного знаку. Корисне навантаження збільшується, коли ми додаємо більше детальних піддіапазонів з новим вибором рівня дозволу. Передбачається використання трьохрівневого вейвлет-розкладання при проведенні початкового ДВП. Вбудовування бітів ЦВЗ повинне проводитися в безліч коефіцієнтів різних піддіапазонів, щоб ЦВЗ був стійкий при обраному процесі квантування і міг бути відновлений.

Для впровадження ЦВЗ потрібно замінити єдині квантувачі, які використовуються в другій стадії кодування JPEG 2000, зсуваючи квантувачі з розміром кроку $\Delta$, як і для оригінальних квантувачів. Також можна використовувати більш високий розмір кроку шляхом множення оригінального на константу. Ці квантувачі відрізняються від попередніх квантувачів введенням зсуву $d$, який псевдовипадково виходить при рівномірному розподілі на $[-\Delta/2, \Delta/2]$.

Здійснення вбудовування біта ЦВЗ відбувається згідно формули:

$$D'=\begin{Bmatrix} D_j^0(d_0),\ якщо\ m_i=0 \\ D_j^1(d_1,|d_0-d_1|=\frac{\Delta}{2}),якщо\ m_i=1 \end{Bmatrix}, \quad (2.8)$$

де $D'$ – обраний квантувач; $d_0$, $d_1$ – зсуви; $\Delta$ – розмір кроку квантування; $m_i$ – біт вбудованого повідомлення.

Тобто якщо біт вбудовування дорівнює нулю, то використовується квантувач $D_j^0$ ($j$=0, 1, 2, 3) зі зсувом $d_0$. Якщо біт вбудовування дорівнює одиниці, то використовується квантувач $D_j^1$ із зсувом $d_1$ і задовольняється умова $|d_0- d_1|=\Delta/2$.

Для кожного переходу в решітці побудовані два зсуви $d_0[i]$ і $d_1[i]$ і чотири об'єднаних квантувачі $A_{0,i}^0 = D_{0,i}^0 \cup D_{2,i}^0$, $A_{1,i}^0 = D_{1,i}^0 \cup D_{3,i}^0$, $A_{0,i}^1 = D_{0,i}^1 \cup D_{2,i}^1$, $A_{1,i}^1 = D_{1,i}^1 \cup D_{3,i}^1$. Таким чином, є дві групи об'єднаних квантувачів для сітчастої структури, які використовуються в запропонованому підході: група 0, яка складається з усіх зсунутих об'єднаних квантувачів використовуваних для вбудовування біта 0 водяного знака і група 1, яка включає в себе зсунуті об'єднані квантувачі для вбудовування біта 1.

Будуємо два згладжуючих вектори $d_0$ і $d_1$: група 0 пов'язана з $d_0$ і група 1 пов'язана з $d_1$. Структура решітки, яка використовується в запропонованому підході, має чотири гілки, що проходять по кожному її стану. Для кожного стану, два об'єднаних квантувачі замість одного пов'язані з декількома вихідними гілками цього стану. Коефіцієнтом сили вбудовування при такому алгоритмі буде виступати саме крок квантувача. При його збільшенні стійкість до зовнішніх впливів буде рости, а скритність падати. На рис. 2.5 показана подібна одноступенева структура решітки, яка використовується для вбудовування ЦВЗ під час стадії квантування.

Функція вбудовування $F(x, m)$ впроваджує ЦВЗ $m$ в зображення $x$, після якого виходить зображення з ЦВЗ $x'$:

$$F(x[i],m[i]) = \left(\left[\frac{x[i]-d_{m[i]}}{\Delta}\right]\right)\Delta + d_{m[i]}, \quad (2.9)$$

де $d_{m[i]}$ – зсув обраного квантувача на розмір кроку Δ; $m[i]$ – вбудований біт при переході $i$.

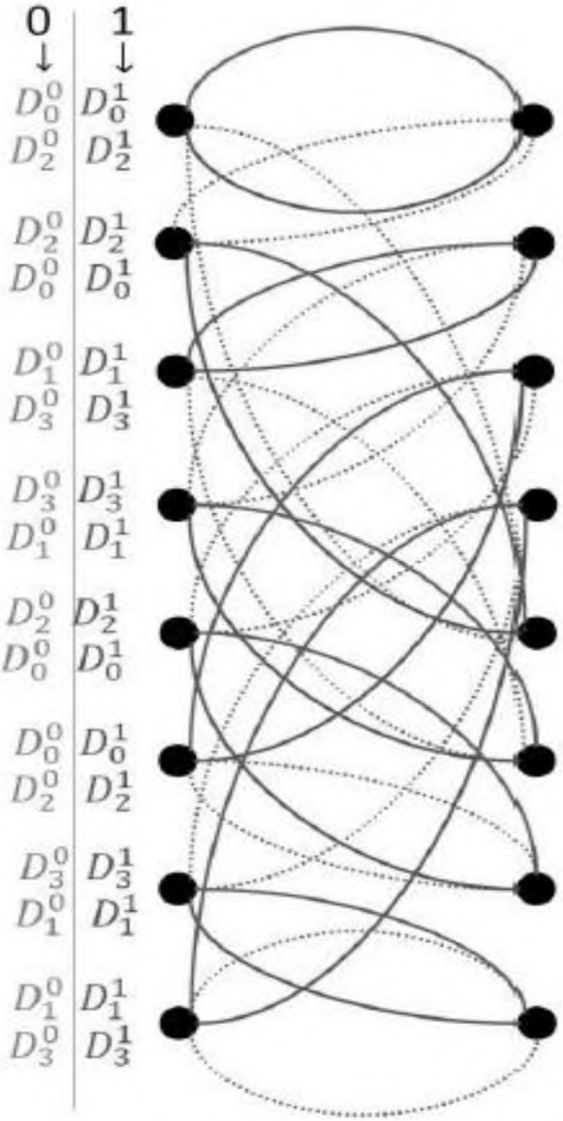



Рисунок 2.5 – Одноступінчата решітка з групами 0 і 1 об'єднаних квантувачів

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

пов'язані з гілками модифікованої решітки. Індекс квантування $q[i]$ буде розрахований за формулою:

$$q[i] = sign(x[i] - d_{m[i]}[i]) \left[ \frac{|x[i] - d_{m[i]}[i]|}{\Delta} \right], \tag{2.10}$$

де $d_{m[i]}[i]$ – додаткове зміщення вже зміщеного квантувача $D_{j,i}^{m[i]}$.

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

$$x'[i] = sign(q[i])(|q[i]| + \delta)\Delta + d_{m[i]}[i], \tag{2.11}$$

де $b$ – параметром, який обирається користувачем в межах $0<b<1$ (зазвичай він дорівнює 0.5).

Вбудовування ЦВЗ здійснюється в різні частини шляхів. ЦВЗ вбудовується оптимально, застосовуючи процедуру ітерацій з обмеженням мінімізації сприйняття відстані і підтримки постійної надійності. Кодове слово визначається за допомогою кореляції, а не квантування. Таким чином, ЦВЗ матиме підвищену стійкість до стиснення зі втратами, і при цьому буде зберігати високу скритність застосування.

Блок-схема запропонованого алгоритму вбудовування ЦВЗ під час стадії квантування приведена на рис. 2.6.

Процес впровадження водяного знака здійснюється незалежно для кожного блоку коефіцієнтів, які підлягають кодуванню. Для того щоб додати більше надійності повідомленням, його можна кодувати завадостійким кодом. Після цього перемішуються псевдовипадково біти в закодоване повідомлення із секретним ключем.

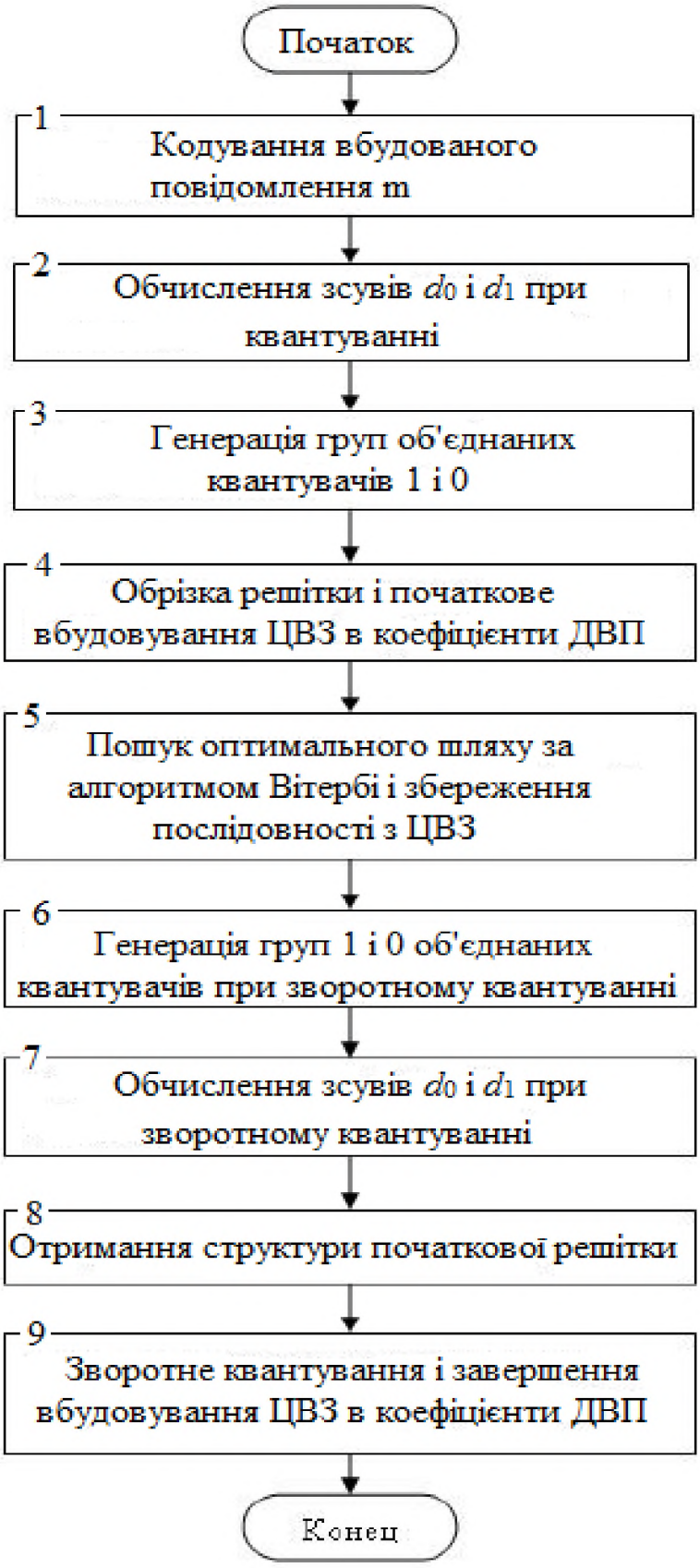



Рисунок 2.6 – Блок-схема запропонованого алгоритму вбудовування ЦВЗ під час стадії квантування

Для кожного кодового блоку процедура квантування і вбудовування ЦВЗ здійснюється наступним чином:

1. Обчислення зсувів $d_0$ і $d_1$: використовують псевдовипадковий генератор для ініціалізації секретного ключа $k$ і обчислення зсувів.

2. Генерація груп 0 і 1 об'єднаних квантувачів: для кожного переходу $i$ проводиться зсув квантувачів. При цьому помічаються гілки решітки для цих квантувачів.

3. Обрізка решітки: решітка спрощується настільки, що всі гілки, що йдуть через решітку, і всі пов'язані з об'єднаними квантувачами, кодують повідомлення $m$. Для кожного переходу, зберігають посилання на кількість збережених гілок. В результаті отримують послідовність $J$.

4. Пошук оптимального шляху: початковий стан даної структури решітки встановлено в 0. Алгоритм Вітербі застосовується для того, щоб знайти мінімальні спотворення траєкторії. Обчислюються індекси квантування. Послідовності $J$ об'єднані в послідовність $J_1$. Отримана послідовність далі кодується і зберігається в файлі, який передається в спільний декодер як стороння інформація.

Вбудовування водяного знака завершується протягом зворотного квантування на стадії декомпресії JPEG 2000. Бітовий потік зображення декодується EBCOT декодером, щоб отримати послідовність декодованих індексів квантування. Для кожного кодового блоку виконуються наступні кроки зворотного квантування:

1. Обчислення зсувів $d_0$ і $d_1$.

2. Генерація груп 0 і 1 об'єднаних квантувачів.

3. Отримання структури решітки використовуваної на етапі квантування: генерується структура решітки з чотирма гілками, що проходять через кожний стан. Кожна гілка решітки має після помічені зсуви квантувачів і посилання. Послідовність $J$ дозволяє отримати обрізані решітки, які використовувалися на стадії квантування. Для кожного переходу $i$ в решітці, обрізка визначається

шляхом видалення гілок, які мають посилання, що не дорівнюють послідовності.

4. Зворотне квантування: обрізана решітка використовується для відновлення вейвлет коефіцієнтів. З огляду на квантовані індекси, закінчується вбудовування водяного знака в ході обчислень реконструйованих вейвлет коефіцієнтів.

З огляду на, що проводиться вбудовування, інтегроване в ланцюг кодування JPEG 2000, буде збільшена швидкість впровадження у 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 зі втратами. Якщо включити режим без стиснення зі втратами при перетворенні зображення, то режим квантування буде отключено і вбудовування не буде здійснено.

### 2.1.4 Алгоритм зчитування ЦВЗ із зображення

Для зчитування повідомлення потрібно застосувати дискретне вейвлет перетворення на зображення. Кожен піддіапазон, який має вбудоване повідомлення розбити на блоки такого ж розміру, як і при кодуванні. Коефіцієнти, що належать поточному блоку, будуть зберігатися у векторі. Для кожного оброблюваного блоку потрібно витягти за допомогою секретного ключа зсуви $d_0$ і $d_1$ і виконати квантування на всю решітку. Це допоможе ідентифікувати шлях, по якому даються мінімальні спотворення квантування між вектором і вихідними кодовими словами. Закодоване повідомлення відновлюється, після цього перемішуються назад біти і застосовується розшифровки для отримання початкового повідомлення. Алгоритм зчитування бітів є зворотним алгоритму вбудовування. При цьому сама схема не потребує наявності оригінального зображення для знаходження коефіцієнтів, в які відбулося вбудовування (сліпа). Блок-схема запропонованого алгоритму зчитування ЦВЗ показана на рис. 2.7.

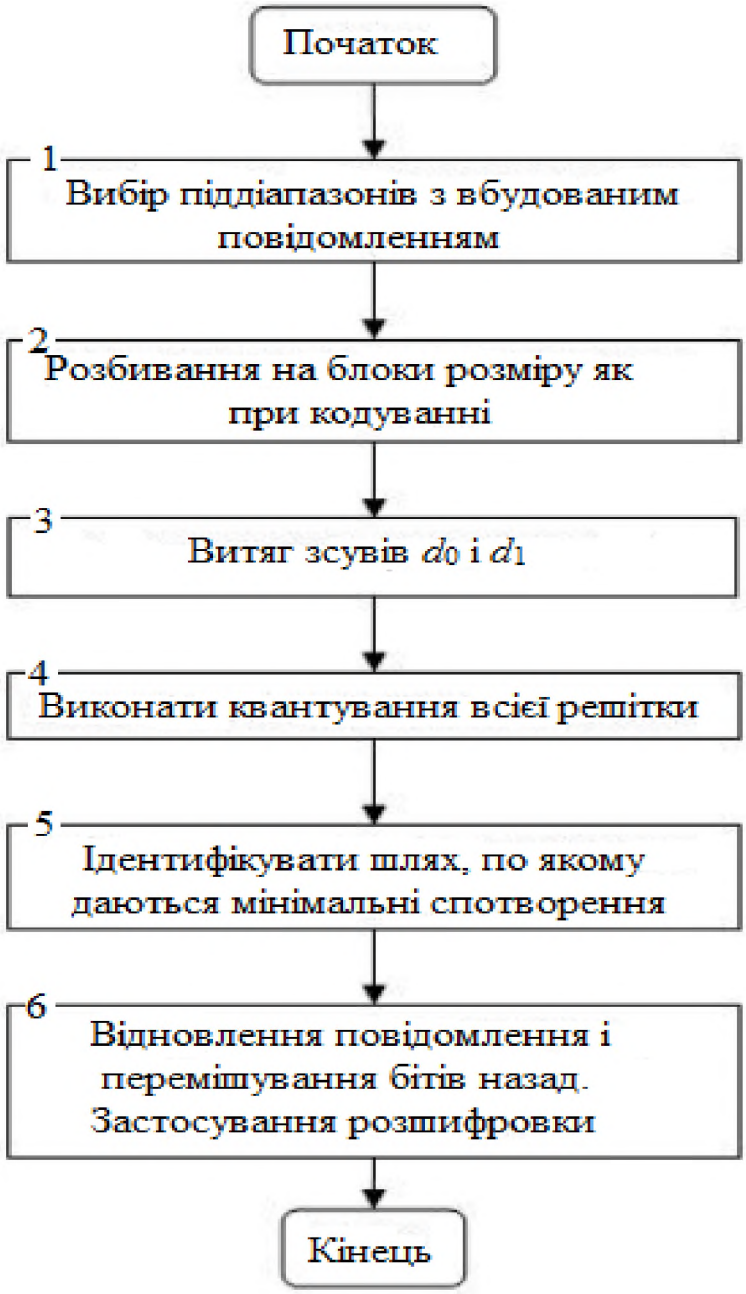



Рисунок 2.7 – Блок-схема запропонованого алгоритму зчитування ЦВЗ

2.1.5 Аналіз стійкості ЦВЗ до зовнішніх впливів на зображення-контейнер

Для оцінки стійкості запропонованого алгоритму була використана методика з розділу 1.2. Значення за різними зображеннями усереднювались.

Для початку треба розібратися зі значеннями скритності впровадження та оцінкою пропускної здатності. Результати оцінки скритності впровадження показані в табл. 2.1.

Таблиця 2.1 – Оцінка скритності впровадження при встановленні ЦВЗ і стисненні

| **Група зображень** | **Коефіцієнт якості JPEG 2000, %** | **SNR, дБ** |
|---|---|---|
| Світлі | 50 | 48.4 |
| | 70 | 46.9 |
| | 90 | 43.5 |
| Середні за яскравістю | 50 | 38.7 |
| | 70 | 35.3 |
| | 90 | 32.3 |
| Темні | 50 | 33.3 |
| | 70 | 31.2 |
| | 90 | 26.9 |

Результати оцінки запропонованого алгоритму виявилися трохи гіршими, ніж у алгоритму Wang, при якому забезпечується найбільш оптимальний рівень скритності впровадження. Але вони краще, ніж у інших 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 дБ, а для світлих від 40 до 50 дБ). Результати оцінки пропускної здатності представлені в табл. 2.2.

Таблиця 2.2 – Оцінка пропускної здатності 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 |

| Розміри зображення, пікселі | Коефіцієнт якості JPEG 2000, % | Загальна прихована пропускна здатність зображення, біт |
|---|---|---|
| 800x800 | 50<br>70<br>90 | 2640<br>2866<br>3150 |
| 1000x800 | 50<br>70<br>90 | 2854<br>3256<br>3630 |
| 3400x2200 | 50<br>70<br>90 | 17990<br>19400<br>20900 |

Встановлено (табл. 2.2), що запропонований алгоритм показав найвищі показники прихованої пропускної здатності, у порівнянні з чотирма існуючими алгоритмами, які досліджувались в розділі 1.2. Для аналізу стійкості до зовнішніх впливів були використані ті ж зображення що й для досліджуваних алгоритмів з розділу 1.2. Було вибрано 4 світлих, 4 темних і 4 середніх по яскравості растрових зображень з розмірами 1000x800 пікселів. ЦВЗ – псевдовипадковий бітовий рядок в 1024 біт. Як досліджувані зовнішні впливи використовувались зашумлення зображення білим гаусівським шумом, масштабування, стиснення JPEG 2000 зі втратами, вирізання частини і фільтрація. Треба зазначити, що зміна формату зображення на інший із стисненням зі втратами за алгоритмом, що відрізняється від JPEG 2000, в рамки дослідження не входить.

На рис. 2.8 показана оцінка стійкості ЦВЗ до стиснення зі втратами для запропонованого алгоритму і існуючих алгоритмів, які були досліджені у розділі 1.2.

Як можна помітити з рис. 2.8, запропонований алгоритм вбудовування під час стадії квантування поступається по стійкості до стиснення зі втратами тим існуючим алгоритмам, де вбудовування здійснюється в низькочастотні піддіапазони.

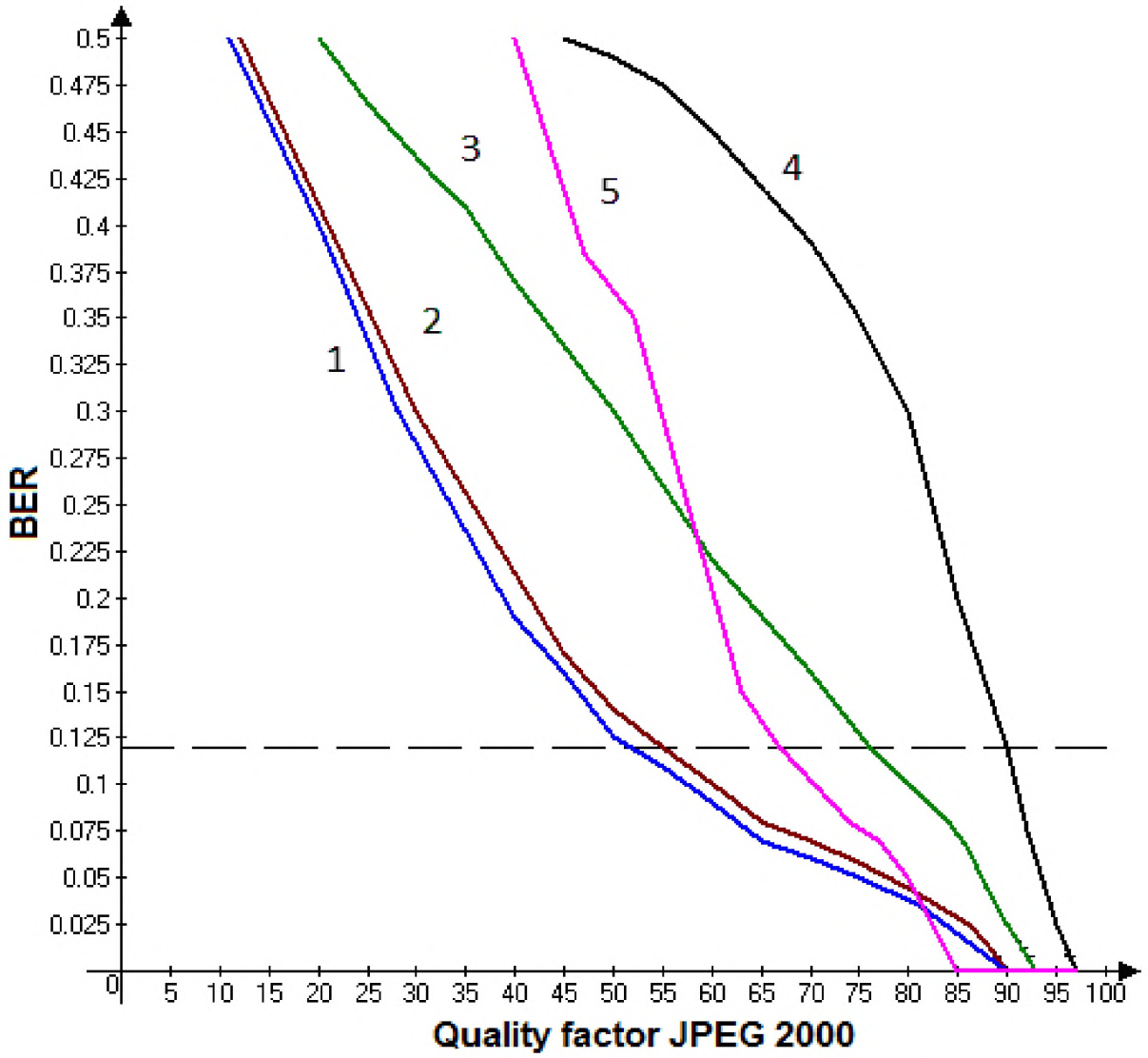



Рисунок 2.8 – Оцінка стійкості ЦВЗ до стиснення JPEG 2000 з втратами: 1 – алгоритм Ouled-Zaid, Makhloufi & Olivier, 2– алгоритм Chirag-Ganesh, 3 – алгоритм Li & Zhang, 4 – алгоритм Wang, 5 – запропонований алгоритм вбудовування під час стадії квантування

На рис. 2.9 показані результати стійкості ЦВЗ до гаусівського зашумлення зображення. Результати запропонованого алгоритму виявилися кращими, ніж у існуючих алгоритмів, які були досліджені у розділі 1.2.

В ході моделювання з масштабуванням зображення-контейнер стискалося до різних розмірів аж до 8 разів. ЦВЗ вдалося витягти при стисканні в 4 разів. Цей показник виявився вищим, ніж у існуючих алгоритмів, які були досліджені у розділі 1.2. Тоді тільки при алгоритмі Quled-Zaid, Makhloufi & Olivier вдалося

повністю відновлювати ЦВЗ при стисненні в 3 рази. Для інших алгоритмів граничним значенням, при якому BER менше 0.12, було стиснення в 2 рази.

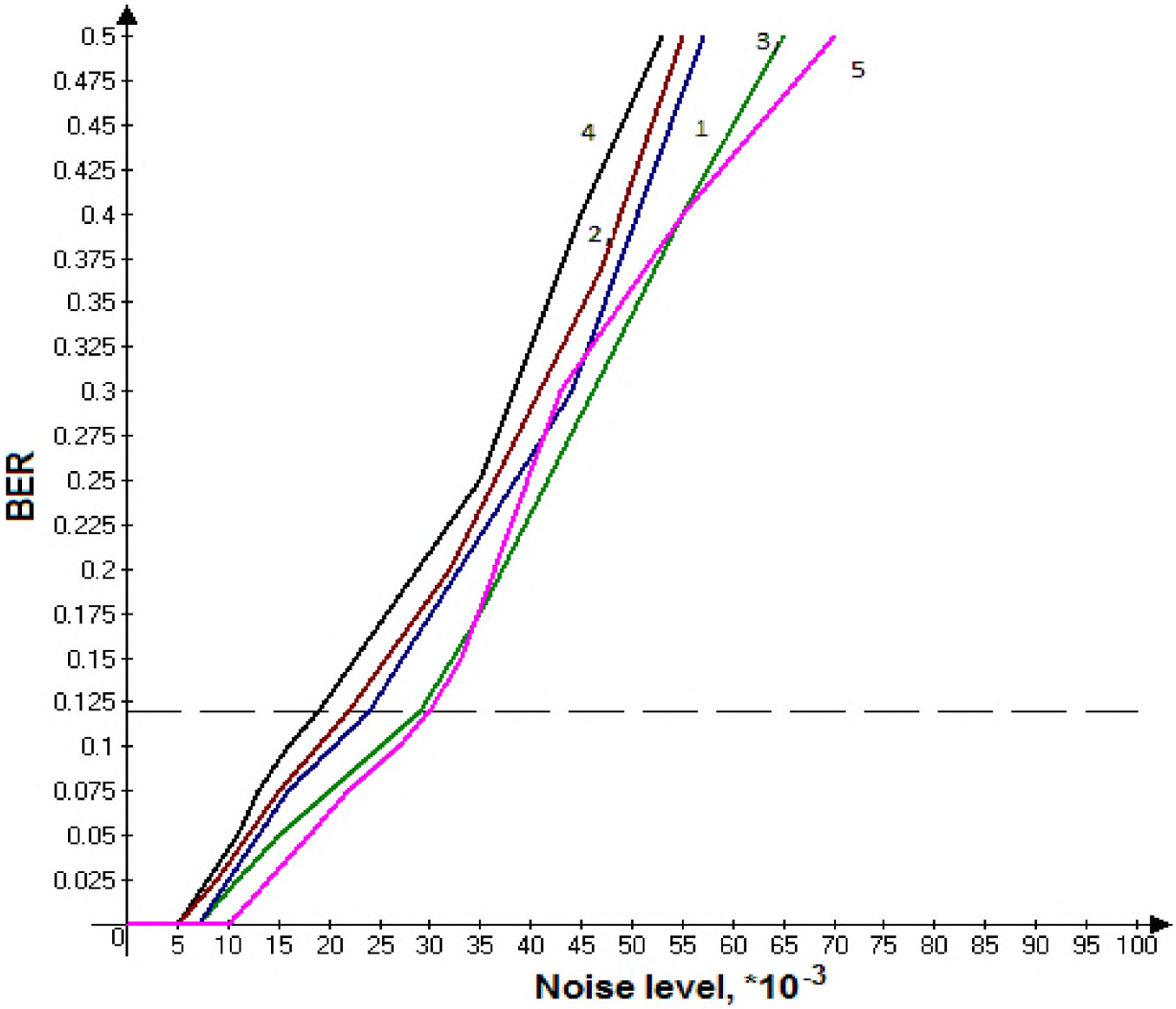



Рисунок 2.9 – Стійкість ЦВЗ до зашумлення:
1 – алгоритм Ouled-Zaid, Makhloufi & Olivier, 2 – алгоритм Chirag-Ganesh, 3 – алгоритм Li & Zhang, 4 – алгоритм Wang, 5 – запропонований алгоритм вбудовування під час стадії квантування

На рис. 2.10 показані результати стійкості ЦВЗ до фільтрації при використання контрастного фільтра.

Стійкість до цього виду зовнішньої дії у запропонованого алгоритму також виявилася кращою, ніж у всіх існуючих алгоритмів, які були досліджені у розділі 1.2.

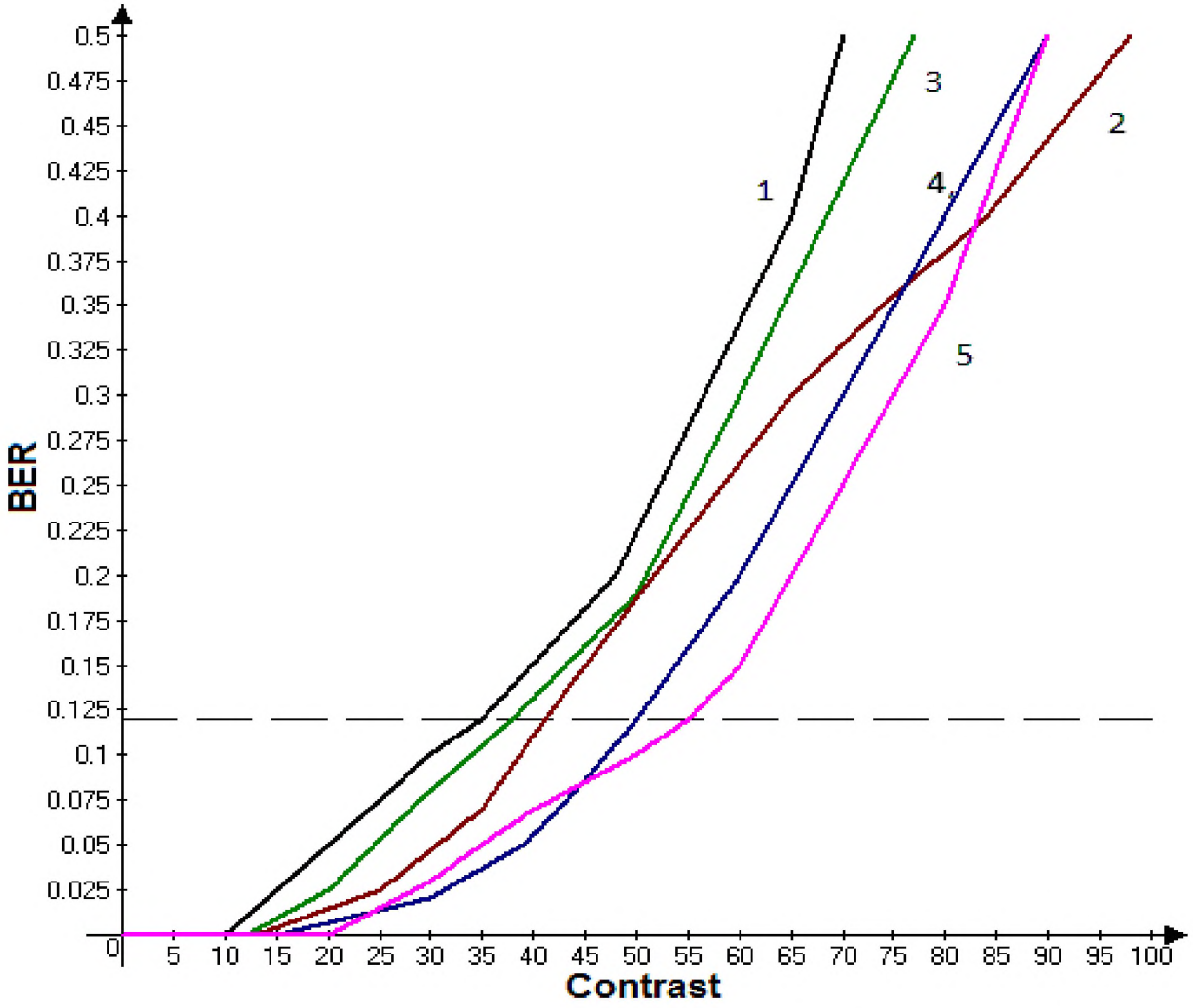



Рисунок 2.10 – Стійкість ЦВЗ до фільтрації: 1 – алгоритм Ouled-Zaid, Makhloufi & Olivier, 2 – алгоритм Chirag-Ganesh, 3 – алгоритм Li & Zhang, 4 – алгоритм Wang, 5 – запропонований алгоритм вбудовування під час стадії квантування

Для аналізу стійкості до вирізання частини зображення був обраний діапазон зміни від 0 до 80% з кроком в 10%. Проводилась вирізка частини зображення зліва направо, ділячи вертикально нову область для відсікання. Запропонований алгоритм виявився найстійкішим з досліджуваних при цьому виді впливу. Відновити ЦВЗ вдалося під час вирізання 40% зображення.

## 2.2 Підходи до підвищення стійкості ЦВЗ до зовнішніх впливів на зображення-контейнер

Як можна побачити з результатів моделювання, розроблений багатокоефіцієнтний алгоритм вбудовування ЦВЗ під час стадії квантування має високі показники стійкості до досліджуваних зовнішніх впливів на зображення-контейнер. Показник скритності впровадження та пропускної здатності при цьому залишився також на оптимальному рівні. Однак показник стійкості при стисканні зі втратами JPEG 2000 виявився не таким високим, як очікувалось, а перевага за іншими виявилось незначним у порівнянні з поточними популярними рішеннями. Було вирішено досліджувати можливість підвищення стійкості шляхом підбору оптимальних параметрів при встановленні. Стійкість можна підвищити, розібравшись з такими параметрами як коефіцієнт сили вбудовування, рівень вейвлет-розкладання і використовувані фільтри при ДВП.

### 2.2.1 Підвищення коефіцієнта сили вбудовування

У розробленому алгоритмі за коефіцієнт сили вбудовування відповідає такий параметр як крок квантувача $\Delta$. Чим він вищий, тим в більшу кількість коефіцієнтів буде проводитися вбудовування сторонньої інформації. Це буде призводити до погіршення якості зображення і тому важливо стежити за рівнем скритності впровадження при збільшенні цього параметра. У розробленому алгоритмі застосовується подвоєний оригінальний крок квантування $2\Delta$. Провівши дослідження щодо збільшення кроку квантувача було знайдено оптимальний розмір $3\Delta$, при якому не помітно погіршення якості. Далі збільшуючи крок до $4\Delta$, з'являється незначне падіння рівня скритності впровадження. Відчутний рівень падіння скритності впровадження і появи артефактів від вбудовування з'являється при збільшенні кроку у п'ять раз.

### 2.2.2 Вибір фільтрів при ДВП

Другим фактором, який дозволяє збільшити стійкість до зовнішніх впливів є вибір фільтрів при ДВП. Для дослідження впливу фільтрів на стійкість ЦВЗ були обрані кілька різних фільтрів: біортогональний фільтр Добеші 9/7 і ортогональні фільтри Хаара, Добеші 8, Добеші 2. Зазвичай в алгоритмах вбудовування ЦВЗ використовуються фільтри Хаара, які складаються всього з двох коефіцієнтів. Фільтр Хаара є найпростішим двохкоефіцієнтним фільтром. Але такий вибір дуже погано вплине на скритність застосування. В залежності від довжини фільтрів, що застосовуються при ДВП і наступному відновленні отримують різну кількість пікселів відновленого зображення. Правильно підібрані фільтри дозволять уникнути втрати якості зображення. Для дослідження можливості підвищення стійкості до зовнішніх впливів шляхом зміни фільтра при ДВП всі умови вбудовування ЦВЗ при розробленому алгоритмі залишалися стандартними, крім фільтрів, що використовуються при ДВП.

Провівши дослідження, виявилося, що фільтр Хаара не сприяє підвищенню стійкості ЦВЗ до зовнішніх впливів. З використанням фільтрів Добеші 9/7 ситуація змінилась в бік підвищення стійкості. Але найбільш кращі результати були отримані при використанні фільтра Добеші 2. При застосування цього фільтра, без внесень додаткових змін вдалося значно підвищити стійкість ЦВЗ до зовнішніх впливів, при цьому уникнувши значних погіршень в скритності впровадження.

### 2.2.3 Вибір рівня вейвлет розкладу

Важливим параметром є вибір рівня вейвлет розкладу. З ростом рівня відбувається зменшення кількості коефіцієнтів, які можуть бути використані для вбудовування біта ЦВЗ. Спотворення від модифікації одиничного коефіцієнта проектуються на більшу кількість пікселів зображення, що може

призвести до порушення скритності вбудовування ЦВЗ. Але для збільшення надійності ЦВЗ при достатній пропускній спроможності зображення слід використовувати якомога більшу глибину розкладання.

Зі збільшенням глибини розкладання зменшується значення кроку квантування, і піддіапазони глибшого рівня вейвлет розкладу піддаються меншим змінам при стисненні зі втратами. Вбудовування в LL піддіапазон дасть більший рівень надійності ЦВЗ, але може призвести до погіршення якості при певних високих обсягах інформації для вбудовування. Саме тому було вирішено не змінювати піддіапазони для вбудовування прихованої інформації. Для представленого алгоритму було встановлено, що 4-х рівневе вейвлет розкладання дозволяє збільшити рівень стійкості до зовнішніх впливів і при цьому задовольняє умові збереження скритності впровадження. Збільшення глибини розкладання супроводжується при цьому зниженням пропускної здатності. Однак для вбудовування ЦВЗ, який зберігає в собі малий обсяг інформації про автора і об'єкті викладання зменшення пропускної здатності не буде критичним.

### 2.2.4 Застосування підходів до підвищення стійкості для запропонованого алгоритму

Модифікувавши коефіцієнти сили вбудовування для запропонованого алгоритму вбудовування під час стадії квантування, збільшивши рівень вейвлет-розкладання до чотирьох і змінивши фільтри при ДВП на Добеші 2 в ланцюзі кодера JPEG 2000 вдалося отримати вдосконалений алгоритм, при якому значно підвищилася стійкість до зовнішніх впливів без значних втрат в скритності впровадження. При цьому відкрилась ще краща можливість підвищення стійкості. Збільшивши крок квантувача до $4\Delta$, і залишивши інші знайдені параметри, вдалось уникнути значного падіння скритності через використання фільтрів Добеші 2.

### 2.2.5 Аналіз стійкості ЦВЗ при використанні розроблених підходів

Для оцінки стійкості використовувалися все ті ж тестові дані, що й для запропонованого алгоритму. Було вибрано 4 світлих, 4 темних і 4 середніх по яскравості растрових зображень з розмірами 1000x800 пікселів. ЦВЗ являло собою псевдовипадковий бітовий рядок в 1024 біт. При використанні потроєного кроку квантувача, фільтрів Добеші 2 і чотирьохрівневого вейвлет-розкладання значення по скритності впровадження впало на 6%, а пропускної здатності на 7.7%. При використанні кроку квантувача 4Δ значення по скритності впало на 8.6%, а пропускної здатності на 9.5%. Спотворення від вбудовування лежать в межах оптимальних показників для груп зображень і будуть непомітні для людини навіть при високому ступені стиснення. З огляду на те, що розроблений алгоритм показав найбільші значення по пропускній здатності з усіх існуючих, падіння її нижче 10 відсотків буде не суттєвим.

В ході моделювання з масштабуванням ЦВЗ вдалось витягти при стисканні в 6 разів для алгоритму з використанням кроку квантувача 4Δ. При використанні кроку квантувача 3Δ BER вище 0.12 спостерігається у зображень стислих в 4 рази (що ідентично при використанні початкових параметрів).

На рис. 2.11 показана оцінка стійкості ЦВЗ до стиснення зі втратами для оригінального створеного алгоритму і алгоритмів з урахуванням підходів до підвищення стійкості. Як можна побачити, при застосуванні методів підвищення стійкості стійкість ЦВЗ до стиснення значно збільшується і перевершує досліджувані до цього існуючі алгоритми вбудовування. BER=0.12 при запропонованому алгоритмі досягається при коефіцієнті якості JPEG 2000 рівним 67, при використання кроку квантувача 3Δ граничний коефіцієнт якості JPEG 2000 дорівнює 44, а при використанні кроку квантувача 4Δ граничний коефіцієнт якості JPEG 2000 дорівнює 28. Це досить високий показник, і якщо зображення буде стиснено вище цього рівня, то воно буде сильно спотворено і втратить комерційну цінність.

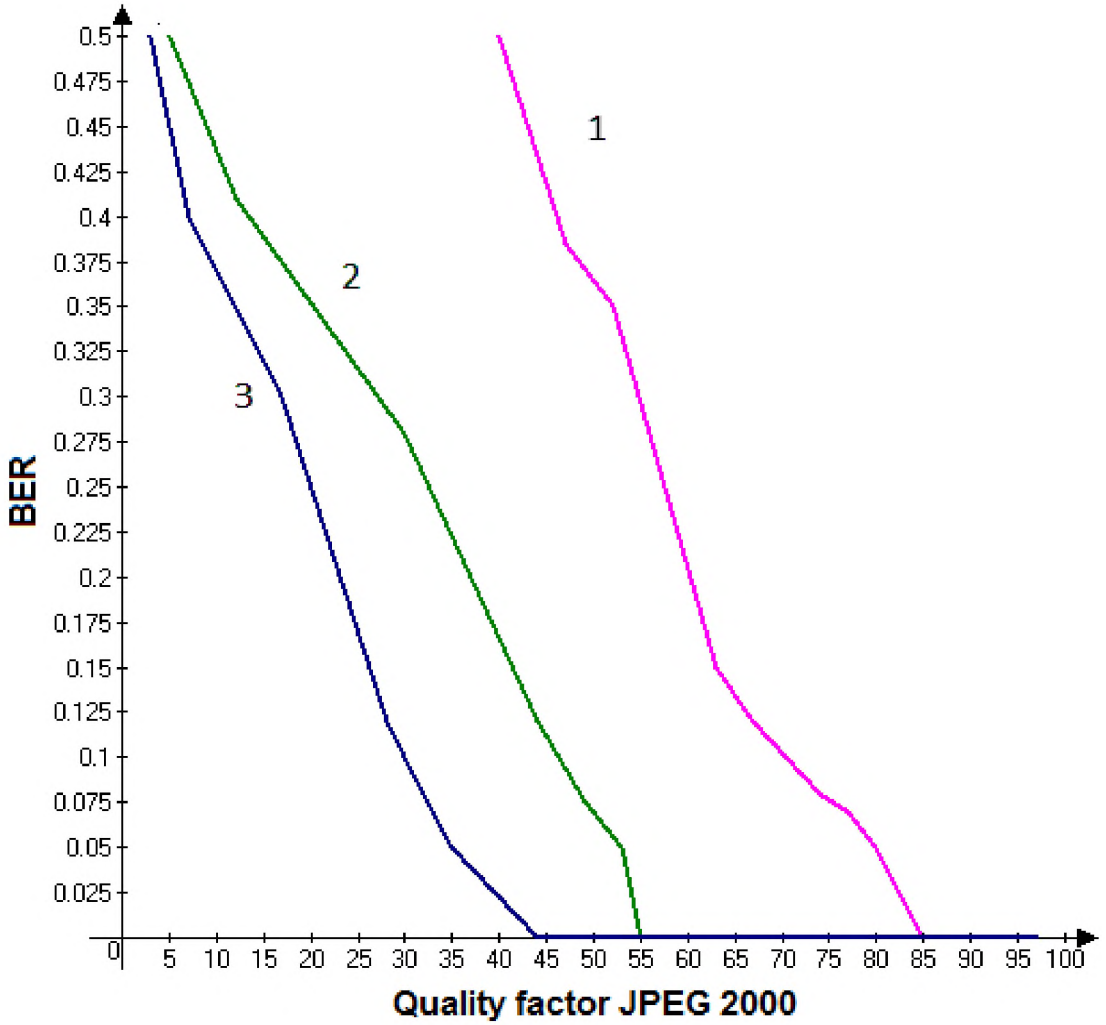



Рисунок 2.11 – Оцінка стійкості ЦВЗ до стиснення JPEG 2000 з втратами: 1 – оригінальний алгоритм, 2 – алгоритм з використанням кроку квантувача 3Δ, фільтрів Добеші 2 і чотирьохрівневого вейвлет-розкладання, 3 – алгоритм з використанням кроку квантувача 4Δ, фільтрів Добеші 2 і чотирьохрівневого вейвлет-розкладання

При використанні алгоритму з кроком квантувача 4Δ вдалося збільшити стійкість до вирізання частини зображення до 50%. Використання алгоритму з потроєним кроком квантування поліпшень в цьому виді впливів не принесло.

На рис. 2.12 показані результати стійкості ЦВЗ до гаусівського зашумлення зображення. Результати при використанні методів підвищення стійкості значно перевершують результат для початкового алгоритму. BER=0.12 при оригінальному алгоритмі досягається при відхиленні в 30 пунктів, при використанні кроку квантувача 3Δ граничне відхилення склало 43

пункти, а при використанні кроку квантувача 4Δ граничне відхилення підвищилося до значення в 71 пункт. Якщо зображення буде зашумлено вище цього рівня, то воно буде сильно спотворено і втратить комерційну цінність.

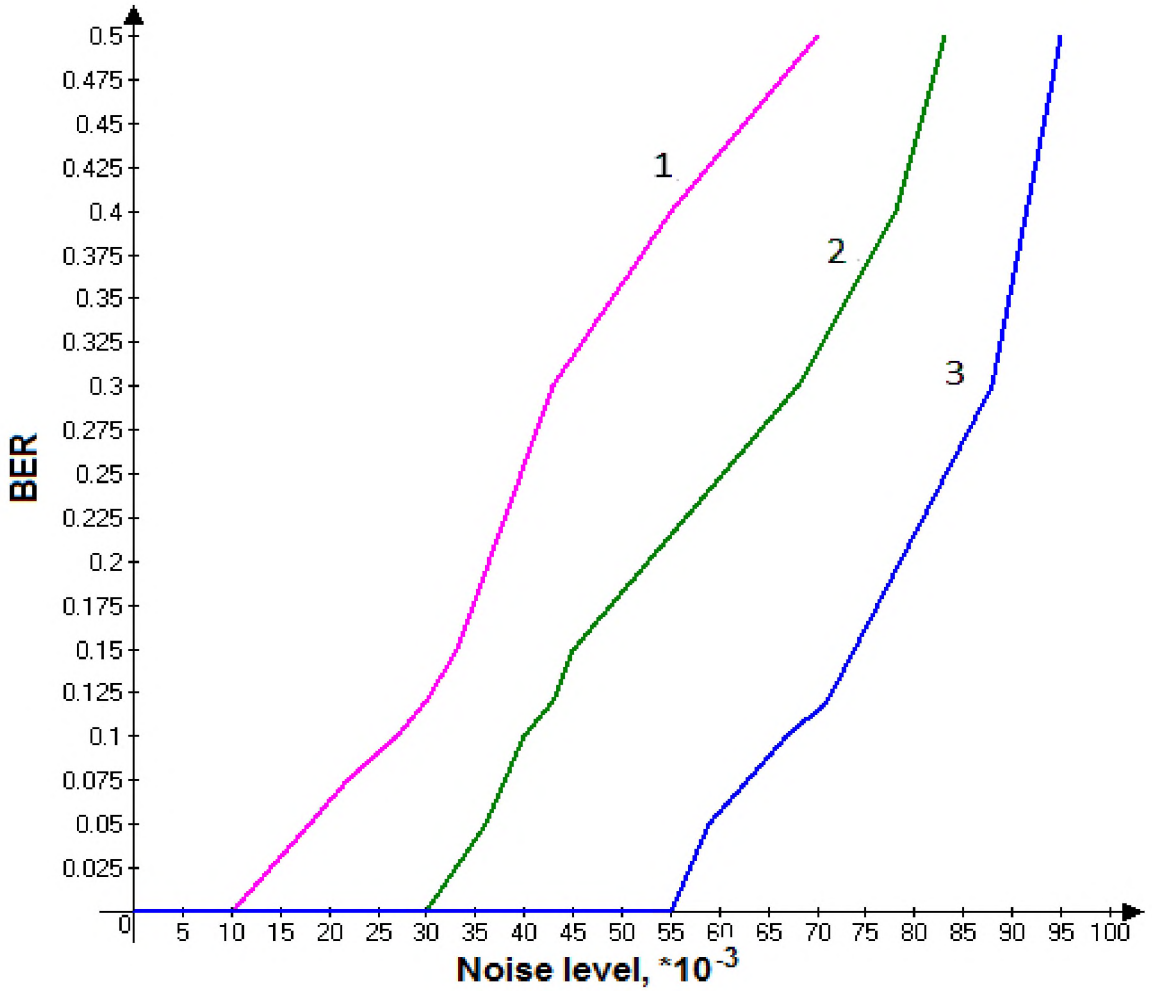



Рисунок 2.12 – Оцінка стійкості ЦВЗ при зашумленні:
1 – оригінальний алгоритм, 2 – алгоритм з використанням кроку квантувача 3Δ, фільтрів Добеші 2 і чотирьохрівневого вейвлет-розкладання, 3 – алгоритм з використанням кроку квантувача 4Δ, фільтрів Добеші 2 і чотирьохрівневого вейвлет-розкладання

На рис. 2.13 показані результати стійкості ЦВЗ до фільтрації при використанні контрастного фільтра. Стійкість до цього виду зовнішньої дії також збільшилася при використанні розроблених методів вбудовування. BER=0.12 при оригінальному алгоритмі досягається при відхиленні в 55

пунктів, при використанні кроку квантувача 3Δ граничне відхилення склало 77 пунктів, а при використанні кроку квантувача 4Δ граничне відхилення підвищилося до значення в 83 пункту. При більш високому значенні фільтра зображення буде не реалістичним і втратить комерційну цінність.

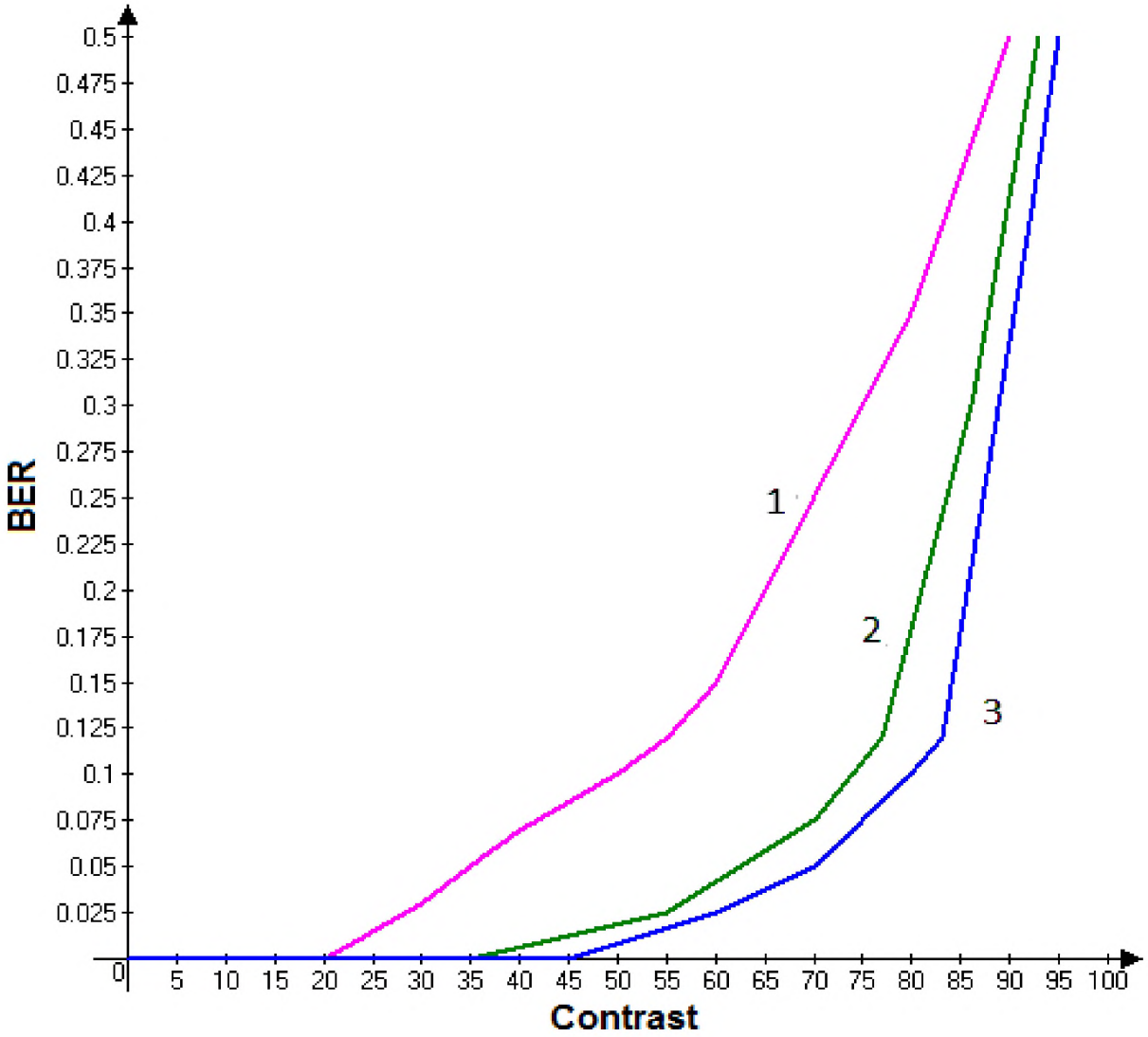



Рисунок 2.13 – Оцінка стійкості ЦВЗ до фільтрації:

1 – оригінальний алгоритм, 2 – алгоритм з використанням кроку квантувача 3Δ, фільтрів Добеші 2 і чотирьохрівневого вейвлет-розкладання, 3 – алгоритм з використанням кроку квантувача 4Δ, фільтрів Добеші 2 і чотирьохрівневого вейвлет-розкладання

## 2.3 Висновки

Досліджено ланцюг кодування JPEG 2000 для можливості вбудовування ЦВЗ. Встановлено, що основні втрати інформації відбуваються при використанні фільтрів при ДВП і на стадії квантування.

Побудовано математичну модель втрат ЦВЗ на стадії квантування. Знайдена можливість використання векторного квантування замість скалярного. При використанні такого квантування знайдена можливість підвищення скритності впровадження та стійкості до стиснення зі втратами за рахунок можливості знаходження вірних шляхів в решітці квантування.

Розроблено багатокоефіцієнтний алгоритм вбудовування ЦВЗ під час стадії квантування, інтегрований в ланцюг кодування JPEG 2000.

Розроблено алгоритм зчитування ЦВЗ, який є зворотним вбудовуванню і не вимагає наявності початкового зображення з ЦВЗ.

Проведено аналіз стійкості ЦВЗ до зовнішніх впливів на зображення-контейнер при використанні запропонованого алгоритму.

Розроблено підходи до підвищення стійкості ЦВЗ до зовнішніх впливів на зображення-контейнер шляхом вибору оптимального коефіцієнта сили вбудовування, фільтрів з найменшими спотвореннями при ДВП і глибини рівня вейвлет-розкладання.

Доопрацьовано алгоритм вбудовування ЦВЗ, при якому вдалося підвищити стійкість ЦВЗ до зовнішніх впливів, не втративши належного рівня скритності впровадження.

Знайдена можливість підвищити рівень скритності, і проведена доробка алгоритму вбудовування ЦВЗ, при якому значно підвищується стійкість ЦВЗ, при цьому рівень падіння скритності впровадження є не суттєвим.

Наведено результати оцінки стійкості ЦВЗ при використанні запропонованих підходів, де показана висока стійкість до досліджуваних видів зовнішніх впливів.

# 3 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою розділу є обґрунтування економічної доцільності стеганографічного вбудовування цифрових водяних знаків на основі алгоритму дискретного вейвлет перетворення. Для цього необхідно здійснити розрахунок капітальних витрат; експлуатаційних витрат, які визначають величину витрат на обслуговування системи на рік; величину можливого збитку; величину економічного ефекту; показники економічної ефективності.

Використання стеганографічних алгоритмів розповсюджено для впровадження прихованої інформації в мультимедійні файли з метою захисту авторських прав на продукцію. Більшість великих Інтернет магазинів перед викладанням продукції автора накладають ЦВЗ на неї. У якості продукції виступають постановочні фотографії, панорами, обкладинки та вкладки музичних альбомів і відеофільмів тощо. ЦВЗ містять інформацію, яка однозначно підтверджує авторство або права на комерційне використання зображення, що захищається. Відповідно до цієї інформації можуть бути вирішені спірні правові ситуації щодо порушення прав інтелектуальної власності та відшкодування збитків.

## 3.1 Розрахунок (фіксованих) капітальних витрат

Капітальні (фіксовані) витрати представляють суму витрат з створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н}$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

3.1.1 Визначення витрат на стеганографічне вбудовування ЦВЗ на основі алгоритму дискретного вейвлет перетворення

3.1.1.1. Визначення трудомісткості стеганографічного вбудовування цифрових водяних знаків на основі алгоритму дискретного вейвлет перетворення.

Трудомісткість розробки визначається тривалістю кожної робочої операції:

$$t = t_{тз} + t_{в} + t_{а} + t_{р} + t_{д},\ \text{годин},$$

де $t_{тз}$ – тривалість складання технічного завдання на стеганографічного вбудовування цифрових водяних знаків на основі алгоритму дискретного вейвлет перетворення, $t_{тз}=40$;

$t_{в}$ – тривалість аналізу існуючої інформації, вивчення ТЗ, літературних джерел за темою тощо, $t_{в}=20$;

$t_{а}$ – тривалість визначення стійкості ЦВЗ до зовнішніх впливів на зображення-контейнер (тривалість впровадження ЦВЗ в зображення-контейнер; аналізу зовнішнього впливу на контейнер; витягнення ЦВЗ з зображення-контейнера; порівняння витягнутого ЦВЗ із оригінальним, і визначення ступеню їх відповідності), $t_{а}=120$;

$t_р$ – вбудовування цифрових водяних знаків на основі алгоритму дискретного вейвлет перетворення, $t_м$=*96*;

$t_д$ – тривалість підготовки технічної документації, $t_д$=*20*.

Отже,

$$t = 40+20+120+96+20 = 296 \text{ годин.}$$

3.1.1.2. Розрахунок витрат на стеганографічне вбудовування цифрових водяних знаків на основі алгоритму дискретного вейвлет перетворення.

Витрати на розробку заходів безпеки Кпз складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки *Ззп* і вартості витрат машинного часу *Змч*:

$$К_{пз} = З_{зп} + З_{мч} = 96200 + 3216{,}63 = 99416{,}63 \text{ грн.}$$

$$З_{зп} = t\, З_{пр} = 296*325 = 96200 \text{ грн.}$$

де $t$ – загальна тривалість операцій, годин;

*Зпр* – средньогодинна заробітна плата спеціаліста с інформаційної безпеки з нарахуваннями, грн./годину.

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{мч} = t \cdot С_{мч} = 296 \cdot 10{,}87 = 3216{,}63 \text{ грн.}$$

де $t$ – трудомісткість операцій із побудови ефективної системи доступу персоналу, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = 0{,}8 \cdot 5 \cdot 1{,}55 + \frac{9200 \cdot 0{,}6}{1920} + \frac{8600 \cdot 0{,}4}{1920} = 10{,}87 \text{ грн.}$$

Стеганографічне вбудовування цифрових водяних знаків на основі алгоритму дискретного вейвлет перетворення планується здійснювати за допомогою Matlab, яке дозволяє зробити розрахунки по потужності контейнера і шуму, а також надає значні засоби для цифрової обробки зображень і

автоматизації завдання застосування зовнішніх впливів з певним кроком його зміни і побудови результуючого графіка. Вартість Matlab складає 38565,71 грн.

Для здійснення стеганографічного вбудовування цифрових водяних знаків на основі алгоритму дискретного вейвлет перетворення необхідно здійснити навчання відповідних спеціалістів вартістю 12000 грн. ($К_н$=12000 грн.).

Таким чином, капітальні (фіксовані) витрати на стеганографічне вбудовування цифрових водяних знаків на основі алгоритму дискретного вейвлет перетворення складуть:

$$К = 105160,6 + 38565,71 + 12000 = 155726,3 \text{ грн.}$$

### 3.1.2 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, \text{ грн.}$$

де $С_в$ – вартість відновлення й модернізації системи;

$С_к$ – витрати на керування системою в цілому;

$С_{ак}$ – витрати, викликані активністю користувачів системи інформаційної безпеки).

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн.}$$

Річний фонд амортизаційних відрахувань ($С_а$) визначається прямолінійним методом, виходячи з вартості активів та строку їх корисного використання. Matlab складає 38565,71 грн. Строк корисного використання – 5 роки. Таким чином,

$$С_а=38565,71/5=7713,14 \text{ грн.}$$

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.}$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 18000 грн. Додаткова заробітна плата – 8% від основної заробітної плати. Отже,

$$С_з = 18000*12 + 18000*12*0,08= 233280 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.09.2020 р. складає 22%.

$$С_{св} = 233280*0,22 = 51321,6 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.},$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=8,4 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,55 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 8,4*1920*1,55 = 24998,4 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1% (Стос = 155726,3*0,01=1557,3 грн.).

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються:

$$С_к = 7713,14 +233280+51321,6 +24998,4 + 1557,3 = 318870,4 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = 318870,4 \text{ грн.}$$

## 3.2 Оцінка можливого збитку

### 3.2.1 Оцінка величини збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки.

При порушенні прав інтелектуальної власності на зображення Інтернет магазинів величина можливого збитку може бути визначена відповідно до розміру відшкодування завданих збитків, що визначається правом інтелектуальної власності, зокрема Цивільним кодексом України, Кримінальним кодексом України, ВСУ від 31.03.95 р. №4 «Про судову практику у справах про відшкодування морального (немайнового) збитку» тощо. У разі встановлення величини компенсації за завдану шкоду підприємству, яка виникла внаслідок недостатнього рівня захищеності його об'єктів інтелектуальної власності, а саме, зображень за допомогою ЦВЗ, величину можливого збитку можна встновити наступним чином:

$$B = n * R * F$$

де n – кількість зображень, що потребує захисту;

R – середнє значення можливості реалізації ризику порушень прав інтелектуальної власності;

F – середнє значення можливого штрафу за законодавством України (ВСУ від 31.03.95 р. № 4 «Про судову практику у справах про відшкодування морального (немайнового) збитку»).

При кількості зображень Інтернет магазину 100 одиниць, вірогідності реалізації ризику, яка дорівнює 30% (R=0,3) та величині штрафу за порушення прав інтелектуальної власності, який дорівнюватиме 22000 грн., величина можливого збитку складе:

$$B=100*0,3*22000=66000 \text{ грн.}$$

### 3.2.2 Загальний ефект від застосування стеганографічного вбудовування ЦВЗ на основі алгоритму дискретного вейвлет перетворення

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C \text{ грн.},$$

де $B$ – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці;

С – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

$$E = 660000 - 318870{,}4 = 341129{,}6 \text{ грн.}$$

### 3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,}$$

де $E$ – загальний ефект від впровадження системи інформаційної безпеки грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{341129{,}6}{155726{,}3} = 2{,}19, \quad \text{частки одиниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} – N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (5,5 %);

$N_{інф}$ – річний рівень інфляції, (5%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$2,19 > (5,5 – 5)/100 = 2,19 > 0,005.$$

Термін окупності капітальних інвестицій $T_o$ показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки. Відповідно термін окупності розробки підходів до стеганографічного вбудовування цифрових водяних знаків на основі алгоритму дискретного вейвлет перетворення:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{2,19} = 0,46, \quad \text{років (5,5 місяців).}$$

## 3.4 Висновок

Згідно з наведеними розрахунками можна дійти висновку, що здійснення стеганографічного вбудовування цифрових водяних знаків на основі алгоритму дискретного вейвлет перетворення, є економічно доцільним, оскільки дозволяє попередити можливі збитку у наслідок порушення щодо прав інтелектуальної власності на зображення. Коефіцієнту повернення інвестицій ROSI, який складає 2,19 (ROSI=2,19). Отже, на 1 гривню капітальних витрат приходиметься 2,19 грн. економічного ефекту. Період окупності при цьому складе 0,46 років або 5,5 місяців. Капітальні інвестиції передбачені на рівні 155726,3 грн., а експлуатаційні витрати на рівні 318870,4 грн. на рік.

# ВИСНОВКИ

Основні результати кваліфікаційної роботи полягають у наступному:

1. Запропоновано методику оцінки впливу зовнішніх впливів на вбудований ЦВЗ, що дозволяє провести порівняльний аналіз стійкості ЦВЗ, вбудованих різними алгоритмами в зображення JPEG 2000.

2. Проведено аналіз стійкості ЦВЗ до зовнішніх впливів на зображення-контейнер при збереженні оптимального рівня скритності впровадження та пропускної здатності для чотирьох популярних існуючих алгоритмів. На основі аналізу сучасних існуючих алгоритмів вбудовування ЦВЗ в зображення формату JPEG 2000 показана доцільність розробки підходів і алгоритмів підвищення стійкості ЦВЗ до зовнішніх впливів на зображення-контейнер.

3. Досліджено ланцюг кодування JPEG 2000 і знайдені етапи, на яких відбувається втрата інформації при стисненні.

4. Розроблено багатокоефіцієнтний алгоритм вбудовування ЦВЗ під час стадії квантування, при якому вдалося підвищити значення стійкості ЦВЗ при зовнішніх впливах, не втративши оптимального рівня скритності впровадження. Розроблено алгоритм зчитування ЦВЗ, який є зворотним вбудовуванню і не вимагає наявності початкового зображення з ЦВЗ. Розроблено підходи до підвищення стійкості ЦВЗ до зовнішніх впливів на зображення-контейнер шляхом вибору оптимального коефіцієнта сили вбудовування, фільтрів з найменшими спотвореннями при ДВП і глибини рівня вейвлет-розкладання. Застосовуючи розроблені підходи, доопрацьовано алгоритм вбудовування ЦВЗ, при якому вдалося підвищити стійкість ЦВЗ до зовнішніх впливів, не втративши належного рівня скритності впровадження.

5. В результаті оцінки стійкості ЦВЗ при використанні запропонованих підходів і алгоритмів, показана висока стійкість до досліджуваних видів зовнішніх впливів.

Підвівши підсумки, можна сказати, що мета роботи, сформульована у вступі, в ході роботи є досягнутою. Впровадження розроблених підходів

дозволить окремим авторам і Інтернет магазинам вбудовувати ЦВЗ високого рівня стійкості до зовнішніх впливів на зображення для захисту авторських прав на свою продукцію.

# ПЕРЕЛІК ПОСИЛАНЬ

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

2. Хорошко В.О., Азаров О.Д., Шелест М.Э., Основы компьютерной стеганографии: Учебное пособие для студентов и аспирантов. – Винница: ВДТУ, 2003.-143 с.

3. Anusudha K., Ayeswarya S. A Robust Digital Watermarking of Satellite Image at Third Level DWT Decomposition // Proceedings of the International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007) – 2007. – Volume 4. – P. 78-82.

4. Li Fan, Tiegang Gao A Novel Blind Robust Watermarking Scheme Based on Statistic Characteristic of Wavelet Domain Coefficients // Proceedings of the 2009 International Conference on Signal Processing Systems – 2009 – P. 121-125.

5. Li Zhiyong An Improved Algorithm of Digital Watermarking Based on Wavelet Transform // Proceedings of the 2009 WRI World Congress on Computer Science and Information Engineering – 2009. – Volume 7. – P. 280-284.

6. T. Bianchi, A. Piva, and M. Barni Composite signal representation for fast and storage-efficient processing of encrypted signals // IEEETrans. Inf. Forensics Security – Mar. 2010. – vol. 5, no. 1 – P. 180–187.

7. Ouled-Zaid A., Makhlou A., Olivier C. Improved QIM-Based Watermarking Integrated to JPEG2000 Coding Scheme // Springer journal of Signal, Image and Video Processing – 2009. – Vol. 3, P. 197-207.

8. 4. Fan Y., Chiang A., Shen J. ROI-based watermarking scheme for JPEG 2000 // Springer journal of Circuits, Systems, and Signal Processing 27(5) – 2008. – P. 763-774.

9. Perez-Freire L., Perez-Gonzalez F. Security of lattice-based data hiding against the watermarked-only attack. // IEEE Transactions on Information Forensics and Security – Vol. 3(4) – 2008 – P. 593-610. 89

10. Braci S., Boyer R., Delpha C. Security evaluation of informed watermarking schemes // In: 16th IEEE International Conference on Image Processing (ICIP), Cairo, Egypt, Proc. ICIP 2009 – November 2009 – P. 117-120.

11. Конахович, Г.Ф. Компьютерная стеганография: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – Киев : МК-Пресс, 2006. – 288 с.

12. Chuang Lin , Jeng-Shyang Pan , Chia-An Huang, A Subsampling-Based Digital Image Watermarking Scheme Resistant to Permutation Attack // IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences – March 2008. – v.E91-A n.3 – P.911-915.

13. Husrev T. Sencar, Mahalinggam Pamkumar, Data Hiding Fundamentals And Applications. Content Security In Digital Multimedia / ELSEVIER science and technology books – 2004. – P. 364.

14. Satish K., Singh Shishir, Kumar A Wavelet Based Robust Digital Watermarking Technique Using Reverse Additive Algorithm (RAA) // Proceedings of the 2009 Third UKSim European Symposium on Computer Modeling and Simulation – 2009. – P. 241-244.

15. Su Xin Digital Watermarking Based on Fast Independent Component Analysis and Discrete Wavelet Transform // Proceedings of the 2009 International Conference on Computational Intelligence and Security – 2009 – Volume 2, P. 341-343.

16. Fu Yu, Wu Xiaoping, Chen Zemao, Ye Qing A Wavelet Digital Watermarking Algorithm Based on Chaotic Mapping // Proceedings of the 2008 International Symposium on Electronic Commerce and Security – 2008 – P. 886-889.

17. A. Sarkar, K. Solanki, and B. Manjunath Obtaining higher rates for steganographic schemes while maintaining the same detectability. // Information Hiding, 12th International Workshop – Calgary, Canada, June 28–30 2010. – volume 6387 of Lecture Notes in Computer Science. – P. 178–192.

18. T. Pevný, P. Bas, and J. Fridrich. Steganalysis by subtractive pixel adjacency matrix. // Proceedings of the 11th ACM Multimedia & Security Workshop – Princeton, NJ, September 7-8, 2009. – P. 75–84.

19. Q. Liu, A. H. Sung, M. Qiao, Z. Chen, and B. Ribeiro. An improved approach to steganalysis of JPEG images // Information Sciences – 2010. – vol. 180(9) – P. 1643–1655.

20. Q. Liu. Steganalysis of DCT-embedding based adaptive steganography and YASS. // Proceedings of the 13th ACM Multimedia & Security Workshop – Niagara Falls, NY, September 29–30, 2011. – P. 77-86.

21. J. Kodovský, T. Pevný, and J. Fridrich. Modern steganalysis can detect YASS. // Proceedings SPIE, Electronic Imaging, Security and Forensics of Multimedia XII – San Jose, CA, January 17–21 2010. – volume 7541. – P. 02–11.

22. C. Chen and Y. Q. Shi. JPEG image steganalysis utilizing both intrablock and interblock correlations // In Circuits and Systems, ISCAS 2008. IEEE International Symposium on – May 2008. – P. 3029–3032.

23. S. P. Mohanty A Secure Digital Camera Architecture for Integrated Real-Time Digital Rights Management // Elsevier Journal of Systems Architecture (JSA) – October-December 2009 – Volume 55, Issues 10-12. – P. 468-480. 91

24. J. Chen, T. S. Chen, C. N. Lin, and C. Y. Cheng. A bitrate controlled data hiding scheme for JPEG2000 // International Journal of Computers and Applications – 2010 – vol. 32(2). – P. 238–241.

25. Kutter M. Digital image watermarking: hiding information in images. PhD Thesis. University of Lausanne, EPFL, 1999.

26. Hartung F., Kutter M. Multimedia Watermarking Techniques // Proceedings IEEE, Special Issue on Identification and Protection of Multimedia Information. – 1999. – Vol. 87. №. 7. – P. 1079-1107.

27. Ivar Austvoll, Filter banks, wavelets, and frames with applications in computer vision and image processing (a review) // Proceedings of the 13th Scandinavian conference on Image analysis, June 29-July 02, 2003, Halmstad, Sweden.

28. Petitcolas F., Anderson R.J., Kuhn M.G. Information Hiding - A Survey // Proceedings IEEE, Special Issue on Identification and Protection of Multimedia Information. – 1999. – Vol. 87. №. 7. – P. 1069-1078.

29. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. New York // John Wiley and Sons, 1996.

30. Шеннон К. Работы по теории информации и кибернетики / Пер. с англ. –М.: Иностранная литература, 1963. – 829с.

31. Чиссар И., Кернер Я. Теория информации: Теоремы кодирования для дискретных систем без памяти / Перевод с англ. - М.: Мир, 1985, –400 с.

32. Marvel L. Image Steganography for Hidden Communication. PhD Thesis. University of Delavare, 1999. 115p.

33. Swanson M.D., Kobayahi M., Tewfik A.H. Multimedia Data-Embedding and Watermarking Strategies // Proceeding of IEEE. 1998. Vol. 86. №. 6. P. 1064-1087.

34. Meerwald P. Quantization watermarking in the JPEG2000 coding pipeline. // In: 5th joint working Conference on Communications and Multimedia Security, Communications and Multimedia Security Issues of the new century – Darmstadt, Germany, may 2001, Proc. IFIP TC6/TC11. – P. 69-79. 92

35. Li K., Zhang X.P. Reliable adaptive watermarking scheme integrated with JPEG2000 // In: International Symposium on Image and Signal Processing and Analysis (ISPA) – Rome, Italy, September 2003 – vol. 1. - P. 117-122.

36. Wang X., Zhang X.P. Generalized trellis coded quantization for data hiding // In: IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) – Honolulu, Hawaii, USA, April 2007 – vol. 2 – P. 269-272.

37. Fan Y.C., Tsao H. A dual pyramid watermarking for JPEG2000 // International Journal of High Performance Computing and Networking 5 – 2007 – P. 84-96.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

| № | **Формат** | **Найменування** | **Кількість листів** | **Примітки** |
|---|---|---|---|---|
| *Документація* | | | | |
| 1 | А4 | Реферат | 3 | |
| 2 | А4 | Список умовних скорочень | 1 | |
| 3 | А4 | Зміст | 3 | |
| 4 | А4 | Вступ | 2 | |
| 5 | А4 | Стан питання. Постановка задачі | 47 | |
| 6 | А4 | Спеціальна частина | 30 | |
| 7 | А4 | Економічний розділ | 8 | |
| 8 | А4 | Висновки | 2 | |
| 9 | А4 | Перелік посилань | 4 | |
| 10 | А4 | Додаток А | 1 | |
| 11 | А4 | Додаток Б | 1 | |
| 12 | А4 | Додаток В | 1 | |
| 13 | А4 | Додаток Г | 1 | |

# ДОДАТОК Б. Перелік документів на оптичному носії

1 Презентація Воробйов.ppt

2 Диплом Воробйов.doc

ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу _____ Пілова Д.П.

(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

**В І Д Г У К**

**на кваліфікаційну роботу студента групи 125м-19-1 Воробйова М.В. на тему: «Стеганографічне вбудовування цифрових водяних знаків на основі алгоритму дискретного вейвлет перетворення»**

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 106 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на розробку алгоритмів і підходів, що дозволяють вбудовувати цифрові водяні знаки підвищеної стійкості до зовнішніх впливів на зображення-контейнер в форматі JPEG 2000.

При виконанні роботи автор продемонстрував відмінний рівень теоретичних знань і практичних навичок. На основі аналізу побудови стегоалгоритмів, а також стійкості ЦВЗ до зовнішніх впливів в ній сформульовані задачі, вирішенню яких присвячений спеціальний розділ. У ньому було знайдено етапи, на яких відбувається основна втрата інформації при стисненні; запропоновано підходи і алгоритми підвищення стійкості ЦВЗ до зовнішніх впливів на зображення-контейнер та оцінено їх ефективність.

Практична цінність роботи полягає в тому, що впровадження розроблених підходів дозволить окремим авторам і Інтернет магазинам вбудовувати ЦВЗ високого рівня стійкості до зовнішніх впливів на зображення для захисту авторських прав на свою продукцію.

Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Воробйов М.В. заслуговує на оцінку «  » та присвоєння кваліфікації «Магістр з кібербезпеки» за спеціальністю 125 Кібербезпека.

**Керівник роботи,**
**к.т.н., доцент** **О.В. Герасіна**