Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *Інформаційних радіотехнологій і технічного захисту інформації*

Кафедра *Комп'ютерної інженерії та систем технічного захисту інформації*

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти *другий (магістерський)*

Порівняльний аналіз алгоритмів генерування та вбудовування цифрових водяних знаків у 2D зображення

Виконав:
студент *2* курсу, групи *СТЗІАм-22-1*
Мосолов Владислав Вадимович

Спеціальність *125 «Кібербезпека»*

Тип програми *освітньо-професійна*

Освітня програма *«Системи технічного захисту інформації, автоматизація її обробки»*

Керівник *асист. Василенко Т.О.*

Допускається до захисту
Зав. кафедри _____ *проф. Антіпов І.Є.*
(підпис)

2024 р.

Харківський національний університет радіоелектроніки

Факультет *Інформаційних радіотехнологій і технічного захисту інформації*
Кафедра *Комп'ютерної інженерії та систем технічного захисту інформації*
Рівень вищої освіти *другий (магістерський)*
Спеціальність *125 «Кібербезпека»*
Тип програми *освітньо-професійна*
Освітня програма *«Системи технічного захисту інформації, автоматизація її обробки»*

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«___» _____ 20 _____ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові *Мосолову Владиславу Вадимовичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Порівняльний аналіз алгоритмів генерування та вбудовування цифрових водяних знаків у 2D зображення*

затверджена наказом по університету від « 03 » 11 2023 р. № 1281 Ст

2. Термін подання студентом роботи до екзаменаційної комісії *10 січня 2024 р.*

3. Вихідні дані до роботи

Алгоритми, засновані на вбудовуванні цифрових водяних знаків у коефіцієнти дискретного косинусного та дискретного вейвлет перетворення зображення
Критерії порівняння ефективності дослідних алгоритмів:
1) візуальна непомітність вбудовування ЦВЗ;
2) прихована пропускна здатність;
3) стійкості до атак проти стегодекодеру.

4. Перелік питань, що потрібно опрацювати в роботі

Провести порівняльний аналіз алгоритмів вбудовування ЦВЗ у статичні 2D зображення, заснованих на дискретному косинусному та дискретному вейвлет перетвореннях. Для досягнення поставленої мети необхідно розв'язати наступні задачі: 1) провести аналітичний огляд сучасних рішень і технік застосування комп'ютерної стеганографії до створення ЦВЗ; 2) провести аналітичний огляд основних алгоритмів вбудовування ЦВЗ в файли-зображення. Обрати декілька з них для подальших досліджень; 3) провести експериментальні дослідження обраних алгоритмів вбудовування ЦВЗ за критеріями візуальної непомітності вбудовування ЦВЗ, прихованої пропускної здатності та стійкості до атак проти стегодекодеру.

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

1. Мета та задачі кваліфікаційної роботи. А4. Ел.ф.

2. Порівняльний аналіз алгоритмів генерування та вбудовування цифрових водяних знаків у статичні 2D зображення А4. Ел.ф.

3. Сучасні алгоритми створення ЦВЗ для файлів-зображень. А4. Ел.ф.

4. Дискретне косинусне перетворення зображення. А4. Ел.ф.

5. Дискретне вейвлет-перетворення зображення. А4. Ел.ф.

6. Алгоритми та зображення-контейнери, що використовувалися в експериментальних дослідженнях. А4. Ел.ф.

7. Результати оцінки візуальних спотворень зображень, що виникають під час використання дослідних алгоритмів. А4. Ел.ф.

8. Результати оцінки стійкості дослідних алгоритмів до атак. А4. Ел.ф.

9. Результати оцінки пропускної здатності дослідних алгоритмів. А4. Ел.ф.

10. Висновки

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	*Огляд засобів та технік застосування комп'ютерної стеганографії для створення цифрових водяних знаків*	*01.09.23 – 20.09.23*	
2	*Огляд алгоритмів вбудовування цифрових водяних знаків у 2D зображення*	*21.09.23 – 31.10.23*	
3	*Проведення експериментальних досліджень*	*01.11.23 – 31.12.23*	
4	*Перевірка роботи на антиплагіат*	*03.01.24 – 05.01.24*	
5	*Представлення кваліфікаційної роботи на кафедрі*	*10.01.2024*	

Дата видачі завдання *02 вересня 2023 р.*

Студент _____
(підпис)

Керівник роботи _____ _____
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 104 с., 27 рис., 18 табл., 43 джерела, 1 додаток.

СТЕГАНОГРАФІЯ, ЦИФРОВИЙ ВОДЯНИЙ ЗНАК, ДИСКРЕТНЕ КОСИНУСНЕ ПЕРЕТВОРЕННЯ, ДИСКРЕТНЕ ВЕЙВЛЕТ-ПЕРЕТВОРЕННЯ.

В роботі розглянуто основні алгоритми створення цифрових водяних знаків (ЦВЗ) для файлів-зображень. Зазначено, що основною проблемою при реалізації технологій створення ЦВЗ є збереження якості маркованих при вбудовуванні ЦВЗ файлів при їх використанні за основним призначенням у поєднанні з достовірністю подальшого відновлення ЦВЗ.

Проведено експериментальні дослідження чотирьох алгоритмів вбудовування ЦВЗ, що базуються на дискретних перетвореннях. В якості критерії при порівнянні було обрано: візуальну непомітність вбудовування, приховану пропускна здатність, стійкість до спотворень.

ABSTRACT

Master thesis: 104 p., 18 tables, 27 fig., 43 sources, 1 annex.

STEGANOGRAPHY, DIGITAL WATERMARK, DISCRETE COSINE TRANSFORM, DISCRETE WAVELET TRANSFORM.

The paper considers the several algorithms for creating digital watermarks (DWM) for image-files. It is noted that the main problem in the implementation of the technologies for creating the DWM is the preservation of the quality of the files marked during the embedding of the DWM when they are used for their main purpose in combination with the reliability of the subsequent restoration of the DWM.

Experimental studies of four algorithms for embedding DWM, which are based on discrete transformations, have been carried out. The following criteria were chosen for the comparison: visual inconspicuousness of embedding, hidden bandwidth, resistance to distortions.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА ТЕРМІНІВ

SVD – Singular Value Decomposition – сингулярне розкладання матриці;

ВЧ – високочастотний;

ДВП – дискретне вейвлет-перетворення;

ДЗВ – джерело зовнішнього впливу;

ДКП – дискретне косинус не перетворення;

ДПФ – дискретне перетворення Фур’є;

ЕК – незаповнений (порожній) контейнер;

ЕЦП – електронно-цифровий підпис;

ЗСЛ – зорова система людини;

КС – комп'ютерна стеганографія;

НЧ – низькочастотний;

ОЦК – об'єкт цифрового (електронного) контенту;

ПЗ – програмне забезпечення;

ППЗ – прихована пропускна здатність;

PCA – Principal Component Analysis – метод головних компонент;

СПІ – стеганографічне приховування інформації;

СС – стеганографічна система;

СЧ – середньо частотний;

ЦВЗ – цифровий водяний знак.

ВСТУП

Останніми роками як у державних, так і комерційних організаціях все ширше використовується електронний документообіг, у зв'язку з чим проблема захисту електронних документів є дуже актуальною. Очевидно, що в залежності від змісту електронні документи мають різний ступінь конфіденційності. Існує також проблема справжності документів, що передаються в мережі, наприклад, документ, отриманий електронною поштою, не можна засвідчити печаткою або підписати звичайним способом. Тому електронний документообіг необхідно супроводжувати різними організаційними та технічними заходами та засобами для захисту електронних документів від несанкціонованого доступу чи модифікації.

Загрози для електронних документів є типовими для інформації в електронному вигляді – це загроза цілісності, конфіденційності та доступності. Для протидії типовим загрозам при використанні електронного документообігу повинно також забезпечуватися збереження документів від втрати та пошкодження та мати можливість їх швидкого відновлення.

Безпечний доступ до даних усередині системи електронного документообігу забезпечується аутентифікацією та розмежуванням прав користувача. Найбільш поширені два методи аутентифікації – парольний та майновий. На парольний метод сильно впливає людський фактор – пароль часто виявляється відомим порушнику. Майновий метод більшу міру захисту оскільки для аутентифікації необхідні різні USB-ключі, смарт-картки тощо. Даний метод теж не захищений від людського фактору, проте, крім паролю, необхідно мати і пристрій для доступу. У будь-якій системі обов'язково має бути передбачене розмежування прав користувача, і чим гнучкіше і детальніше, то краще.

Конфіденційність найчастіше забезпечується криптографічними методами. За допомогою них конфіденційність зберігається навіть при попаданні документа до рук зловмисників. Використання криптографічних засобів ви-

магає звертання уваги і на організаційну складову захисту інформації. Незалежно від криптографічних методів, зловмисник може отримати доступ до документа за допомогою комп'ютера з відкритим документом. Розшифровка інформації також не становить труднощів, якщо не здійснюється контроль ключів у користувачів.

Електронно-цифровий підпис (ЕЦП) є основним засобом забезпечення аутентичності документу, отриманого в електронному вигляді. ЕЦП служить для захисту документа від спотворення, підміни авторства, відмовлення від авторства. Електронно-цифровий підпис по суті є цифровим друком, тому що, на відміну від фізичного підпису, він є спільним для підприємства, відділу або комп'ютера. Виходить, що будь-яка людина, яка має доступ до ресурсів, які відповідають за створення та інші дії з ЕЦП, може вчинити такі протиправні дії:

1) змінити вихідний документ, після чого згенерувати нову ЕЦП;

2) змінити авторство документа, в результаті привласнити собі чужий документ, або відправити свій документ під чужим ім'ям;

3) знищити вихідний документ, надіслати інший документ замість вихідного.

Таким чином, через подібні зловмисні дії під загрозою виявляється не лише цілісність документа, а й авторство. Для захисту документа від таких впливів рекомендується використовувати крім ЕЦП ще і інші засоби, фактично поєднуючи криптографічні та стеганографічні методи захисту.

Одним із таких засобів може бути цифровий водяний знак (ЦВЗ) – спеціальна мітка, що вбудовується в контейнер з метою захисту авторських прав та підтвердження цілісності контенту. ЦВЗ застосовуються для захисту від несанкціонованого використання, зміни та копіювання документів.

Метою роботи є підвищення інформаційної безпеки систем електронного документообігу.

Для досягнення поставленої мети необхідно розв’язати наступні задачі:

1) провести аналітичний огляд сучасних рішень і технік застосування

комп'ютерної стеганографії до створення ЦВЗ;

2) провести аналітичний огляд основних алгоритмів вбудовування ЦВЗ в файли-зображення;

3) провести експериментальні дослідження алгоритмів вбудовування ЦВЗ, що базуються на дискретних перетвореннях за критеріями візуальної непомітності вбудовування, прихованої пропускної здатності, стійкості до спотворень.

1 АНАЛІЗ ВІДОМИХ МЕТОДІВ ТА АЛГОРИТМІВ СТВОРЕННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ

В наш час у зв'язку з інтенсивним розвитком та поширенням технологій, які дозволяють за допомогою комп'ютера інтегрувати, обробляти та синхронно відтворювати різні типи даних та інформації (мультимедійні технології), питання ідентифікації та підтвердження авторського права стосовно об'єктів цифрового (електронного) контенту (ОЦК), є надзвичайно актуальним [1].

Для того щоб комп'ютерний файл, що є об'єктом авторського права, містив всю необхідну інформацію про його автора та історію його створення, застосовуються спеціальні мітки або, так звані, цифрові водяні знаки (ЦВЗ). Застосування ЦВЗ дозволяє не лише ускладнити порушення авторських прав, але й проконтролювати його використання авторизованими користувачами та іншими особами. Поряд з інформацією, поданою у формі цифрових зображень (фотографіями, малюнками, відсканованими паперовими документами тощо), ЦВЗ також широко використовуються для маркування відео- та аудіоданих.

Отримання доступу до інформації у зв'язку з появою та розповсюдженням глобальних комп'ютерних мереж є досить простою процедурою. Водночас легкість і швидкість такого доступу передбачають активне використання ЦВЗ при розміщенні унікальних фотографій, відео, аудіотреків в електронному вигляді у глобальній мережі Інтернет [1].

Базовим підходом, використовуваним для реалізації технологій ЦВЗ, є застосування методів комп'ютерної стеганографії. Тому метою цього розділу є аналіз понять та методів комп'ютерної стеганографії, що необхідно для подальшого викладу матеріалів кваліфікаційної роботи.

1.1. Методи комп'ютерної стеганографії

Комп'ютерна стеганографія (КС) є порівняно молодим напрямом інформатики. На міжнародній конференції Information Hiding: First Information Workshop у 1996 році було запропоновано використовувати єдину термінологію та основні поняття КС [2], які наведено нижче.

Стеганографія – наука про передачу інформації в прихованій формі, причому сам факт передачі може бути невідомий зовнішньому спостерігачеві.

Розрізняють два види стеганографії:

1) приховування інформації від пасивного спостерігача. У цьому випадку основна мета – не допустити виявлення вбудованої в ОЦК інформації;

2) приховування інформації від активного спостерігача, коли факт наявності вбудованої в ОЦК інформації відомий, але отримання цієї інформації має бути суттєво ускладнене.

Повідомлення – інформація (дані), яку необхідно вбудувати в ОЦК, а потім відновити для передачі споживачеві. Далі в тексті кваліфікаційної роботи повідомлення буде позначатись як вектор $d \in R^m$. В якості такого повідомлення в даній роботі розглядаються ЦВЗ.

Контейнер або носій – будь-який файл або потік даних, структура та розмір якого дозволяють вбудувати (приховати) необхідні дані. Далі в тексті кваліфікаційної роботи контейнер буде позначатись як вектор $z \in R^n, n \gg m.$

Як правило, обсяг інформації, що стеганографічно вбудовується в контейнер, безпосередньо залежить від об’єму цього контейнера. Чим більший об’єм контейнера, тим більше інформації можна вбудувати. До найбільш часто використовуваних у якості контейнерів цифрових носіїв відносяться: статичні зображення, текстові, аудіо- та відеофайли, а також виконувані файли і деякі протоколи (наприклад, протокол транспортного рівня TCP) [3, 4].

Незаповнений (порожній) контейнер (НК) – контейнер, який не містить вбудованого повідомлення, але є потенційно придатним для приховування інформації.

Заповнений контейнер (ЗК) – контейнер, що містить вбудовану інформацію. Як правило, висувається вимога, щоб заповнений ЗК був «зовні» не відмінний від незаповненого контейнера або щоб вбудована інформація не заважала сприймати основну зовнішню інформацію.

Стеганографічний ключ (стегоключ) – закритий або відкритий ключ, необхідний для приховування місцезнаходження даних у контейнері. Далі в тексті кваліфікаційної роботи стеганографічний ключ буде позначатись як вектор $k \in K < R^r, n \gg r$.

Найчастіше в якості стегоключа використовують спеціально сформовані дані, а також певні послідовності дій або алгоритми, що задають послідовність операцій при вбудовуванні / відновленні даних в елементи природних контейнерів. За необхідності вбудовані дані можуть бути зашифровані додатково звичайними методами. Стегоключі можуть бути як відкритими, так і закритими, все залежить від особливостей аналізованого способу стеганографічного приховування інформації (СПІ) та його застосування. При цьому може використовуватись один або кілька ключів. У деяких випадках ключ може бути відсутнім взагалі. Знаючи ключ користувач зможе відновити приховане повідомлення.

Стеганографічним перетворенням даних називається наступна пара перетворень:

$$F_1 : Z \times D \times K \to \tilde{Z}, \;\; F_2 : \tilde{Z} \times K \to \tilde{D}, \tag{1.1}$$

де Z – множина всіх контейнерів; D – множина усіх повідомлень; K – множина ключів; $\tilde{Z}$ – множина заповнених контейнерів; оператор F_1 (прямий оператор) реалізує вбудовування інформації, а оператор F_2 (зворотний оператор) – її відновлення. При виконанні відповідних перетворень для елементів зазначених множин повинні виконуватись такі вимоги:

$$\begin{gathered} \tilde{z} = F_1(z, d, k), \;\; z \in Z, \;\; d \in D, \;\; k \in K, \;\; \tilde{d} = F_2(\tilde{z}, k), \;\; \tilde{d} \in \tilde{D}, \\ \|z - \tilde{z}\| \to \min, \quad \left\|d - \tilde{d}\right\| \to \min, \end{gathered} \tag{1.2}$$

тобто при виконанні стеганографічних перетворень властивості контейнера і повідомлення, що відновлюється, повинні спотворюватися в міні-

мальній мірі.

Стеганографічною системою (стегосистемою) називається $\{Z, D, K, F_1, F_2\}$ – сукупність контейнерів, повідомлень, ключів та пов'язуючих їх перетворень. Іншими словами, стеганографічна система (СС) – це сукупність засобів і методів для формування прихованого каналу передачі інформації (стегоканалу).

Джерело зовнішнього впливу (ДЗВ) – потенційний чи реальний суб'єкт (зловмисник, сторонній користувач тощо), який здійснює навмисний (атаку) або ненавмисний вплив на стегоситему з метою виявлення стегоканалу, відновлення інформації, що передається в ньому, або її спотворення та / або знищення. При цьому виявлення стегоканалу є найбільш трудомісткою задачею.

Прихована пропускна здатність (ППЗ) стегоканалу – максимальна кількість інформації, яка може бути вбудована в один елемент (піксель, відлік) контейнера. Обов'язковою умовою при цьому є безпомилковість передачі даних одержувачу,а також їх захищеність від таких атак зловмисника як спроба виявлення факту наявності стегоканалу, отримання змісту прихованих повідомлень, навмисне введення сфальшованих даних або руйнування вбудованої в контейнер інформації.

Стеганографічна стійкість – здатність стегосистеми приховувати від кваліфікованого зловмисника факт передачі повідомлень, а також здатність протистояти спробам зловмисника зруйнувати, спотворити, видалити повідомлення, що потайно передаються, а також здатність підтвердити або спростувати справжність приховуваної інформації. Вважають, якщо порушник має можливість виявити факт наявності прихованого каналу передачі повідомлень, то СС, як правило, вже є нестійкою.

Стегоаналіз – процедура виявлення факту СПІ та, якщо можливо, визначення стеганографічного ключа та (або) відновлення раніше прихованої інформації.

Основними положеннями сучасної комп'ютерної стеганографії є [5]:

- методи приховування повинні забезпечувати автентичність та цілісність файлу контейнера;
- передбачається, що джерелам зовнішнього впливу повністю або частково відомі можливі стеганографічні методи;
- безпека інформаційних технологій ґрунтується на збереженні стеганографічним перетворенням основних властивостей файлу, що відкрито передається, при внесенні в нього повідомлення та деякої невідомої інформації – ключа;
- навіть якщо факт приховування повідомлення став відомий ДЗВ, відновлення самого повідомлення є складною обчислювальною задачею.

Переважна більшість методів КС базується на двох ключових принципах [2]:

- файли, які не вимагають абсолютної точності представлення та відтворення даних (наприклад, файли-зображення, аудіо-файли тощо), можуть бути видозмінені (до певної міри) без втрати своєї функціональності;
- органи чуття людини нездатні надійно розрізняти незначні зміни у модифікованих таким чином файлах та / або відсутній спеціальний інструментарій, який міг би виконувати дану задачу.

В основі базових підходів до реалізації методів КС у рамках того чи іншого інформаційного середовища лежить виділення малозначних фрагментів цього середовища та заміна наявної в них інформації іншою інформацією, яку необхідно приховати. Оскільки в КС розглядаються середовища, що підтримуються засобами обчислювальної техніки та комп'ютерними мережами, то все інформаційне середовище в результаті може бути представлене у цифровому вигляді.

Таким чином, незначні для кадру інформаційного середовища фрагменти відносно до того чи іншого алгоритму або методики аналізу замінюються фрагментами з інформацією, що приховується. Під кадром інформаційного середовища у даному випадку розуміють певну його частину, виділену за характерними ознаками. Наприклад, як такий кадр може розглядатися якесь

окреме зображення, звуковий файл, Web-сторінка тощо.

Для існуючих методів комп'ютерної стеганографії використовують наступну класифікацію (рис. 1.1) [1].

За способом вибору контейнера розрізняють сурогатні, селективні та конструюючі методи стеганографії.

В сурогатних (безальтернативних) методах стеганографії повністю відсутня можливість вибору контейнера, і для приховування повідомлення обирається випадковий контейнер – ерзац-контейнер, який в більшості випадків не оптимальний для приховування повідомлення заданого формату.

У селективних методах КС вважається, що приховане повідомлення має відтворювати спеціальні статистичні характеристики шуму контейнера. Для цього генерують велику кількість альтернативних контейнерів з наступним вибором оптимального з них для конкретного повідомлення. Особливим випадком такого підходу є обчислення певної хеш-функції кожного контейнера. При цьому для приховування повідомлення вибирається той контейнер, хеш-функція якого збігається зі значенням хеш-функції повідомлення (тобто стеганограмою є обраний контейнер).

У конструюючих методах стеганографії контейнер генерується стеганосистемою. При цьому існує декілька варіантів реалізації. Так, наприклад, шум контейнера може імітуватися прихованим повідомленням. Це реалізується за допомогою процедур, які не тільки кодують повідомлення, що приховується під шум, але і зберігають модель початкового шуму. У граничному випадку за моделлю шуму може будуватися ціле повідомлення.

За способом доступу до інформації, що приховується, розрізняють методи для потокових (безперервних) контейнерів і методи для фіксованих (обмеженої довжини) контейнерів.

За способом організації контейнери, подібно до завадодостійких кодів, можуть бути систематичними та несистематичними.

В перших можна вказати конкретні місця стеганограми, де знаходяться інформаційні біти контейнера, а де – шумові біти, призначені для приховання

інформації (як, наприклад, у широко поширеному методі найменш значущого біта).

У випадку несистематичної організації контейнера такий поділ неможливий – для виділення прихованої інформації необхідно обробляти вміст усієї стеганограми.

Рисунок 1.1 – Класифікація методів комп'ютерної стеганографії

За принципом приховування інформації методів комп'ютерної стеганографії поділяються на два основні класи: методи безпосередньої заміни та спектральні методи. Якщо перші, використовуючи надлишок інформаційного середовища в просторовій (для зображення) або часовій (для аудіо) області, полягають у заміні малозначної частини контейнера бітами секретного повідомлення, то другий клас для приховування даних використовує спектральні подання елементів середовища, в яке вбудовуються приховувані дані (наприклад, дискретно-косинусне перетворення, перетворення Фур'є, Карунена-Лоєва, Адамара, Хаара і т.д.).

Основним напрямом комп'ютерної стеганографії є використання саме властивостей надмірності контейнера-оригіналу, але при цьому слід мати на увазі, що в результаті приховування інформації відбувається спотворення деяких статистичних властивостей контейнера або порушення його структури. Це необхідно враховувати зменшення демаскирующих ознак [1].

В особливу групу можна виділити методи, які використовують спеціальні властивості форматів представлення файлів:

- зарезервовані для розширення поля файлів, які часто заповнюються нулями та не використовуються;
- спеціальне форматування даних (зсув слів, речень, абзаців або вибір певних позицій символів);
- використання незадіяних ділянок на магнітних та оптичних носіях;
- видалення файлових заголовків-ідентифікаторів тощо.

В основному для таких методів характерні низька ступінь скритності, низька пропускна здатність та слабка продуктивність.

За призначенням розрізняють методи для прихованої передачі (або прихованого зберігання) даних та методи приховування даних у цифрових об'єктах з метою підтвердження авторських прав на них.

За типом контейнера виділяють методи з контейнерами у вигляді тексту, аудіо-файли, файли-зображення та відео-файли. В наш час методи ком-

п'ютерної стеганографії розвиваються за двома основними напрямками [6]:

- методи, засновані на використанні спеціальних властивостей форматів файлів;
- методи, засновані на надмірності аудіо- та візуальної інформації.

Порівняльні характеристики існуючих стеганографічних методів наведено в табл. 1.1. Як видно, лише перший клас методів ґрунтується на використанні спеціальних властивостей комп'ютерних форматів подання даних, а не надмірності самих даних. Таким чином, можна зробити висновок, що основним напрямком комп'ютерної стеганографії є використання надмірності аудіо- та візуальної інформації.

Області практичного застосування методів сучасної комп'ютерної стеганографії досить широкі. З погляду авторів [2, 6, 8] основні сфери використання комп'ютерної стеганографії:

- потайлива передача інформації;
- камуфлювання програмного забезпечення;
- створення цифрових водяних знаків для різних програм.

Зупинимося докладніше кожної з перелічених задач [6].

Прихована передача інформації. Ця сфера використання КС є найбільш ефективною. Так, наприклад, лише одна секунда оцифрованого звуку з частотою дискретизації 44100 Гц та 256 рівнями квантування (8 біт) у стерео режимі дозволяє приховати за рахунок заміни найменш значущих молодших розрядів аудіо-файлу близько 10 Кбайт інформації. При цьому зміна значень відліків становить менше 1%.

Камуфлювання програмного забезпечення (ПЗ). Іншою важливою задачею стеганографії є камуфлювання ПЗ.У тих випадках, коли використання ПЗ незареєстрованими користувачами є небажаним, воно може бути закамуфльовано під стандартні універсальні програмні продукти (наприклад, текстові редактори) або приховано у мультимедійних файлах (наприклад, у звуковому супроводі комп'ютерних ігор).

Таблиця1.1 – Порівняльні характеристики стеганографічних методів

<table>
<tr><th colspan="2">Стеганографічні методи</th><th>Коротка характеристика та особливості методів</th><th>Недоліки</th><th>Переваги</th></tr>
<tr><td colspan="5">Методи використання спеціальних властивостей комп'ютерних форматів даних</td></tr>
<tr><td colspan="2">Методи використання зарезервованих для розширення полів комп'ютерних форматів даних</td><td>Поля розширення є у багатьох мультимедійних форматах, ці поля заповнюються нульовою інформацією та не враховуються основною програмою</td><td>Низький ступінь скритності, передача невеликих обмежених обсягів інформації</td><td>Простота використання</td></tr>
<tr><td rowspan="3">Методи спеціального форматування текстових фай-лів</td><td>Методи використання відомого усунення слів, речень, абзаців</td><td>Методи засновані на зміні положення рядків та розміщення слів у реченні, що забезпечується вставкою додаткових пробілів між словами</td><td>Слабка продуктивність методу, передача невеликих обсягів інформації низький ступінь скритності</td><td>Простота використання. Наявне опубліковане програмне забезпечення реалізації даного методу</td></tr>
<tr><td>Методи вибору певних позицій літер (нульовий шифр)</td><td colspan="3">Акровірш – окремий випадок цього методу (наприклад, початкові літери кожного рядка утворюють повідомлення)</td></tr>
<tr><td>Методи використання спеціальних властивостей полів форматів, що не відображаються на екрані</td><td colspan="3">Методи засновані на використанні спеціальних "невидимих", прихованих полів для організації виносок та посилань (наприклад, використання чорного шрифту на чорному тлі)</td></tr>
<tr><td colspan="2">Методи приховування в місцях гнучких дисків, що не використовуються.</td><td>Інформація записується у місцях, що зазвичай не використовуються, ГМД (наприклад, у нульовій доріжці)</td><td>Слабка Продуктивність методу, передача невеликих обсягів інформації Низький ступінь скритності</td><td>Простота використання. Наявне опубліковане програмне забезпечення реалізації даного методу</td></tr>
<tr><td colspan="2">Методи використання імітючих функцій (mimic-function)</td><td>Методи засновані на генерації текстів і є узагальненням акровірша. Для таємного повідомлення генерується осмислений текст, який приховує саме повідомлення</td><td>Слабка продуктивність методу, передача невеликих обсягів інформації Низький ступінь скритності</td><td>Результуючий текст не є підозрілим для систем моніторингу мережі</td></tr>
</table>

Продовження таблиці 1.1

Стеганографічні методи	Коротка характеристика та особливості методів	Недоліки	Переваги
Методи видалення ідентифікаційного заголовка файлу	Приховане повідомлення шифрується і у результату видаляється ідентифікуючий заголовок, залишаючи тільки шифровані дані. Одержувач заздалегідь знає про передачу повідомлення і має брак заголовка	Проблема приховування вирішується лише частково. Необхідно заздалегідь передати частину інформації одержувачу	Простота реалізації. Багато засобів (White Noise Storm, S-Tools) забезпечують реалізацію цього методу з PGP шифром
Методи використання надмірності аудіо- та візуальної інформації			
Методи безпосередньої модифікації елементів аудіо- та відео-файлів (просторові методи)	Молодші розряди цифрових відліків містять дуже мало корисної інформації. Їх заповнення додатковою інформацією практично не впливає на якість сприйняття, що дає можливість приховувати конфіденційну інформацію	За рахунок вбудовування додаткової інформації спотворюються статистичні характеристики цифрових потоків. Для зниження компрометуючих ознак потрібна корекція статистичних характеристик	Можливість прихованої передачі великого обсягу інформації. Можливість підтвердження авторського права, прихованого зображення товарної марки, реєстраційних номерів тощо
Методи безпосередньої модифікації спектральних подань аудіо- та відео-файлів (спектральні методи)	У реальних алгоритмах стиску здійснюють обнулення не пікселів зображення, а спектральних коефіцієнтів. Перевага такого підходу полягає в тому, що близькі до нуля спектральні коефіцієнти мають тенденцію розташовуватися в заздалегідь передбачених областях, що призводить до появи довгих серій двійкових нулів, а отже до підвищення ефективності методу	Те саме	Те саме

Створення цифрових водяних знаків. У загальному випадку цифрові водяні знаки використовуються у таких додатках:

- приховане або видиме маркування об'єктів цифрового контенту, представлених у вигляді графічних, відео- та аудіо-файлів для їх ідентифікації, представлення історії створення, а також внесення будь-якої інформації, що цікавить користувача, без істотних спотворень, що заважають використовувати ОЦК за основним призначенням;
- підтвердження авторських прав на об'єкти цифрового контенту, а також справжності копій об'єктів, що використовуються;
- створення RFID-міток підвищеної скритності та стійкості.

Слід також відзначити низку принципових відмінностей постановки задачі створення ЦВЗ при реалізації стеганографічного методу та протидії негативним впливам ДЗВ:

- як правило, сам факт наявності ЦВЗ у файлі-контейнері може бути відомий потенційному ДЗВ з високим ступенем достовірності;
- при здійсненні зовнішнього впливу ДЗВ цікавить не стільки зміст вбудованого повідомлення, а, більшою мірою, його знищення та модифікація;
- файл-контейнер ОЦК з внесеним до нього ЦВЗ може піддаватися трансформаціям і різним перетворенням формату представлення даних, що дозволяє при цьому використовувати об'єкт за основним призначенням, хоча і з гіршою якістю.

Вказані обставини висувають підвищені вимоги до скритності самого способу створення ЦВЗ (прихованості стегоключа), складності відтворення або повторення алгоритму вбудовування ЦВЗ зловмисником або стороннім користувачем, стійкості ЦВЗ до різноманітних трансформацій і перетворень формату файлу-контейнеру.

1.2. Застосування комп'ютерної стеганографії для створення цифрових водяних знаків

Аналіз цілого ряду публікацій [2, 4, 5, 6] за існуючими алгоритмами та технологіями створення цифрових водяних знаків (ЦВЗ), дозволяє зробити висновок, що використання ЦВЗ в наш час набувають все більшої популярності.

ЦВЗ діляться над ва типи – видимі та невидимі. Видимі ЦВЗ досить просто видалити або замінити. Для цього можуть бути використані графічні чи текстові редактори. Невидимі ЦВЗ є вбудовуваними в файли вставками, що не видимі людським очам. Зазвичай для технологій створення ЦВЗ висувають такі вимоги:

- непомітність ЦВЗ для користувачів;
- індивідуальність алгоритму вбудовування (досягається за допомогою алгоритму стеганографічного з використанням ключа);
- можливість для автора виявити неприпустиме використання файлу;
- неможливість видалення неуповноваженими особами;
- стійкість до змін носія-контейнера (до зміни його формату та розмірів, до масштабування, стиснення, повороту, фільтрації, введення спецефектів, монтажу, аналогових та цифрових перетворень).

В роботі [5] розглядаються основні типи ЦВЗ. Основі їх особливості наведено в табл. 1.2.

Задачі вбудовування та відновлення повідомлень з іншої інформації виконує стегосистема (див. на рис. 1.2), що складається з наступних основних елементів:

- прекодер – пристрій, призначений для перетворення повідомлення, що приховується, до виду, зручного для вбудовування в сигнал-контейнер;
- стегокодер – пристрій, призначений для здійснення вбудовування прихованого повідомлення в інші дані з урахуванням їх моделі;

- пристрій відновлдення вбудованого повідомлення;
- стегодетектор – пристрій, призначений визначення наявності стеганоповідомлення;
- декодер – пристрій, який відновлює приховане повідомлення. Цей вузол може бути відсутнім.

Таблиця1.2 – Основні особливості технологій цифрових водяних знаків

Технологія ЦВЗ	Особливості ЦВЗ	Примітка
Робасні (РЦВЗ)	Мають високу стійкість до зовнішніх впливів	Аналіз літератури показує, що РЦВЗ присвячено найбільшу кількість робіт
Крихкі (КЦВЗ)	Руйнуються за незначної модифікації заповненого контейнера. Використовуються для автентифікації сигналів / документів	Містять інформацію не тільки про факт модифікації контейнера, але також і про вид та місцезнаходження цієї зміни
Напівкрихкі (НКЦВЗ)	Стійкі по відношенню до одних впливів і не стійкі до інших	Дозволяють виконувати стиснення зображення, але забороняють вирізку з нього або вставку в нього фрагмента

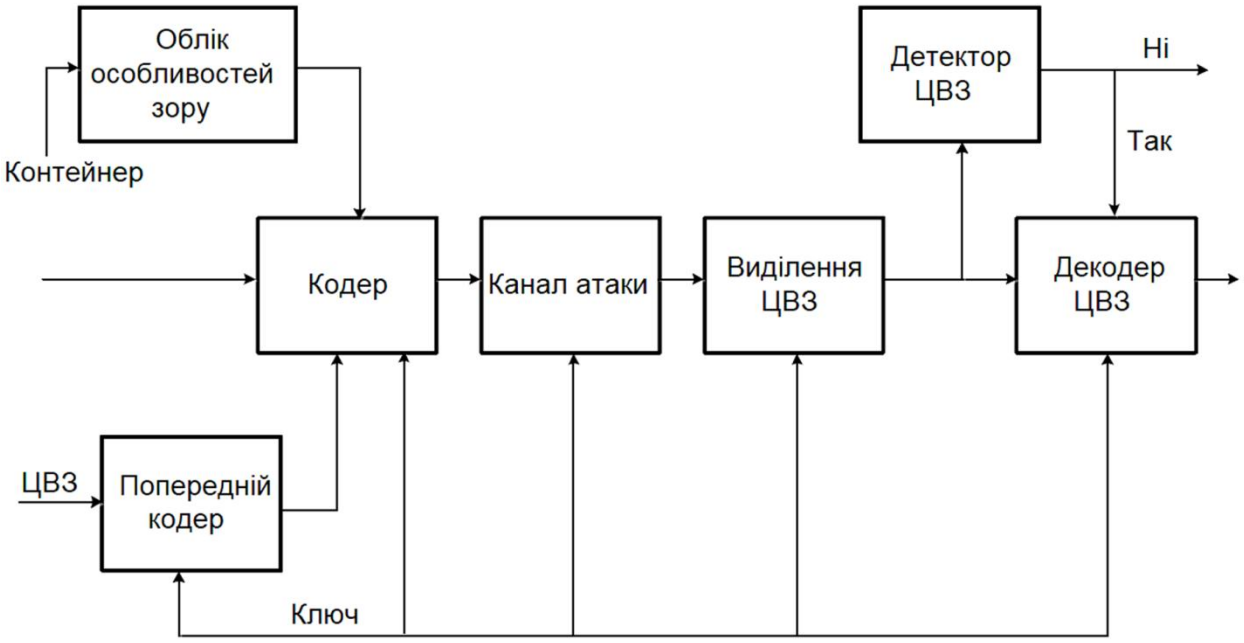


Рисунок 1.2 – Структурна схема типової стегосистеми ЦВЗ

У роботі [6] авторами наведено класифікацію та результати аналізу сучасних алгоритмів вбудовування ЦВЗ у файли-зображення. При цьому виділяються клас адитивних алгоритмів та клас алгоритмів на основі квантування.

Алгоритми адитивного вбудовування ЦВЗ використовують лінійну модифікацію первинного файлу графічного формату, а відновлення в декодері виконується на основі кореляційних методів. При цьому ЦВЗ зазвичай накладається на контейнер, чи «вплавляється» (fusion) у нього.

Відповідно, адитивні алгоритми поділяються на алгоритми на основі лінійного вбудовування даних та алгоритми на основі злиття ЦВЗ та контейнера. В алгоритмах на основі лінійного вбудовування даних ЦВЗ є послідовністю чисел довжини N, яка вбудовується в обрану підмножину відліків файлу-контейнера. Якщо замість послідовності псевдовипадкових чисел в зображення вбудовується інше зображення (наприклад, логотип фірми), то відповідні алгоритми впровадження називаються алгоритмами злиття. Розмір повідомлення, що вбудовується, набагато менше розміру первинного зображення. Перед вбудовуванням воно може бути зашифроване або перетворене якимось іншим чином.

Під квантуванням розуміється процес зіставлення великої (нескінченної) множини значень з деякою скінченною множиною чисел. Звісно, що відбувається зменшення об’єму інформації в наслідок її спотворення. Квантування знаходить застосування у алгоритмах стискання з втратами.

Алгоритми на основі квантування поділяються на алгоритми вбудовування ЦВЗ з використанням скалярного квантування (на вхід квантувача подаються скалярні значення) та алгоритми вбудовування ЦВЗ з використанням векторного квантування (на вхід квантувача подаються послідовності або блоки відліків).

Фрактальне кодування може розглядатися як різновид векторного квантування, причому у якості кодової книги виступають різні перетворення (поворот, зсув, масштабування), що дозволяють апроксимувати блоки зобра-

ження малого розміру (рангові) блоками більшого розміру (доменами). Ця послідовність перетворень передається декодеру.

Розглянемо докладніше відомі алгоритми створення ЦВЗ для контейнерів-зображень. В роботі [9] розглядаються наступний перелік базових алгоритмів створення ЦВЗ, заснованих на модифікації файлів у первинному поданні (просторово-часовий підхід). Їх перевагою є те, що з вбудовуванням ЦВЗ немає необхідності виконувати обчислювально громіздкі лінійні перетворення зображень, а ЦВЗ вбудовуються за допомогою маніпуляцій яскравістю чи з кольоровими складовими. До цих методів відносять: алгоритм Катеру (Kutter), алгоритм Брундокса (Bruyndonckx), алгоритм Ленгелаара (Langelaar), алгоритм Пітаса (Pitas), алгоритм Роджена(Rongen), алгоритм PatchWork, алгоритм Бендера (Bender).

Існуючі на даний момент алгоритми вбудовування ЦВЗ в цифрові зображення мають загальний недолік – більшість з них здійснює вбудовування в частотній області [10, 11], тобто необхідними етапами вбудовування ЦВЗ зображення є пряме і зворотне ДПФ всього зображення-контейнера. Даний підхід, забезпечуючи стійкість вбудованого ЦВЗ до повороту, масштабування та кадрування зображення-контейнера (так званий RST-invariant watermarking), водночас значно підвищує обчислювальну складність процедури вбудовування та унеможливлює поблочне вбудовування ЦВЗ [12].

В роботі [12] основну увагу приділено алгоритмам створення стійких ЦВЗ для цифрових зображень та наводиться наступна класифікація:

1) алгоритми, що базуються на вбудовуванні ЦВЗ в області перетворення, інваріантного до заданих типів спотворень (transform domain);

2) алгоритми вбудовування ЦВЗ, що використовують так звані стійкі до спотворень «мітки синхронізації» (локальні екстремуми в заданих областях енергетичного спектру зображення) для оцінки та компенсації спотворень зображення-контейнера [13, 14].

Основними недоліками першого типу алгоритмів є обчислювальна складність та значне спотворення зображення-контейнера в процесі вбудову-

вання при обчисленні прямого та зворотного перетворення Фур'є-Мелліна. Крім того, більшість алгоритмів даного класу використовують так званий «закритий» детектор [12] і не дозволяють вбудовувати в яксоті ЦВЗ довільну, не відому одержувачу послідовність біт. Основним недоліком другого типу алгоритмів є їх нестійкість до атаки «watermark template attack» [12].

Крім того,у роботі [12] запропоновано новий алгоритм вбудовування цифрових водяних знаків у файли графічного формату, що забезпечує стійкість ЦВЗ до широкого набору перетворень зображення-контейнера та має ряд переваг у порівнянні з існуючими алгоритмами вбудовування стійких ЦВЗ. Даний алгоритм дозволяє вбудовувати ЦВЗ у файли графічного формату за допомогою поблочної обробки первинного контейнера і не вимагає виконання спектральних перетворень при вбудовуванні ЦВЗ. Даний алгоритм, як і алгоритми, засновані на спектральних перетвореннях місту контейнера, забезпечує стійкість ЦВЗ до повороту, масштабування, кадрування зображення-контейнера, а також до інших поширених перетворень (стиснення з втратами, адитивне зашумлення, лінійна фільтрація тощо).

Основним недоліком відомих алгоритмів є те, що у більшості перерахованих алгоритмів для створення ЦВЗ використовуються процедури, що реалізують суворо певні послідовності операцій перетворення даних, в кінцевому рахунку, утворюючи скінченну множину варіантів, які можуть бути ідентифіковані та розкриті. До недоліків багатьох алгоритмів вбудовування ЦВЗ також можна віднести жорстку залежність від формату файлу, трудомісткість обчислення цифрових водяних знаків, порівняно низьку стійкість щодо операцій перетворення сигналів, можливе помітне погіршення якості маркованого файлу (наприклад, зображення) при вбудовуванні мітки, і, крім того, у ряді алгоритмів для отримання цифрового водяного знака необхідно мати вихідний (немаркований) файл.

Певною мірою подолати недоліки можна з використанням можливостей штучних нейронних мереж [15, 16], що використовуються для створення універсальних функціональних моделей перетворення даних.

У роботі [17] запропоновано використати новий алгоритм створення цифрових водяних знаків на основі нейронних мереж. ЦВЗ непомітно вбудовується в кольорове зображення за аналогією до методу Катера (вбудовування виконується в канал синього кольору RGB зображення, тому що до синього кольору людський зір є найменш чутливим). Потім з використанням нейронних мереж вибірково розпізнаються характеристики вбудованих бітів ЦВЗ на основі відмінностей між безпосередньо вбудованих пікселів і цих пікселів в симетричному хрестоподібному вікні. Крім того, представлені результати проведених експериментів, що ілюструють стійкість алгоритму проти різних типів атак.

У роботі [18] розглядається можливість застосування нейронних мереж при вбудовуванні та відновленні ЦВЗ. Запропонована методика ґрунтується на об'єднанні двох підходів [19, 20]. Спочатку первиннний ЦВЗ поділяється на блоки, для кожного з яких розраховується дискретно-косинусное перетворення у частотній області. Перед вбудовуванням ЦВЗ випадковим чином розсіюється, що робить виявлення ЦВЗ досить трудомістким, у своїй коефіцієнти ДКП також неупорядковані. Потім коефіцієнти ДКП групуються в різні підмножини і кодуються в шестирозрядні двійкові послідовності. Після чого відбувається безпосередньо вбудовування ЦВЗ у первинний файл графічного формату. Для відновлення ЦВЗ використовується спеціально навчена нейронна мережа, на виході їх якої отримують шестирозрядні послідовності біт, які перетворюються назад у десяткове подання. Результати проведених експериментів (різний рівень розмитості, різкості, JPEG стиск із втратами) показали, що відновлений ЦВЗ має деякі незначні артефакти, що дещо впливає на надійність та непомітність запропонованого методу вбудовування ЦВЗ.

Таблиця1.3 – Сучасні алгоритми створення ЦВЗ для файлів-зображень

Характеристика ЦВЗ	Принцип роботи	Переваги	Недоліки
Адитивні алгоритми створення ЦВЗ			
Алгоритми на основі лінійного вбудовування ЦВЗ			
Послідовність псевдовипадкових чисел, розподілених за законом Гауса, довжиною 1000 чисел	Модифікація 1000 найбільших коефіці-єнтів дискретного косинусного перетворення (ДКП)	Робастність (нечутливість) ЦВЗ до стискання та інших видів обробки сигналу	Трудомісткість обчислення двовимірного ДКП
Послідовність бінарних псевдовипадкових чисел $\{-1,1\}$, довжина якої визначається розмірами первинного зображення	Модифікація всіх коефіцієнтів детальних піддіапазонів першого підрівня розкладання при виконанні чотирирівневого вейвлет перетворення	Можливість виявлення ЦВЗ без первинного зображення. Візуальна непоміт-ність ЦВЗ	Для відновлення ЦВЗ необхідно мати первинне зображення
Масив псевдовипадкових чисел, розподілених згідно із законом Гауса, розміром 1024 числа	Модифікація всіх коефіцієнтів LL піддіапазону вейвлет перетворення зображення	Можливість модифікації алгоритму для використання секретного ключа	Для відновлення ЦВЗ необхідно мати первинне зображення
Послідовність псевдовипадкових дійсних чисел, розподілених за законом Гауса	Модифікація найбільших коефіцієнтів детальних піддіапазонів трирівневої декомпозиції зображення	Добре візуальне маскування вбудованих даних. Для виявлення ЦВЗ не потрібна наявність первинного зображення	
Послідовність псевдовипадкових дійсних чисел, розподілених за законом Гауса, довжиною 1000 чисел	Модифікація перцептуально значущих коефіцієнтів трирівневої декомпозиції зображення з використанням біортогональних вейвлет-фільтрів	Робастність ЦВЗ до багатьох видів атак. Для виявлення ЦВЗ не потрібна наявність первинного зображення	
Послідовність псевдовипадкових дійсних чисел, розподілених за гауссівським законом	Модифікація найбільших коефіцієнтів кожного піддіапазону трирівневої декомпозиції зображення	Для виявлення ЦВЗ не потрібна наявність первинного зображення	

Продовження таблиці 1.3

Характеристика ЦВЗ	Принцип роботи	Переваги	Недоліки
Масив біполярних псевдовипадкових чисел	Модифікація1000 найбільших коефіцієнтів комплексного вейвлет-перетворення (ЦВЗ також піддається перетворенню)	Для виявлення ЦВЗ не потрібна наявність первинного зображення	
Послідовність псевдовипадкових дійсних чисел, розподілених за гауссівським законом	Модифікація найбільших коефіцієнтів тирівневого вейвлет-перетворення (коефіцієнти відбираються відповідно до задано-го порогу)	Робастність ЦВЗ до деяких видів атак	Для відновлення ЦВЗ необхідно мати первинне зображення
Послідовність псевдовипадкових дійсних чисел, довжина якої залежить від пропускної здатності зображення, що обчислюється на основі моделі людського зору	Модифікація коефіцієнтів чотирирівневого вейвлет-перетворення, відібраних з урахуванням заданого порога	Висока робастність вбудованого ЦВЗ	Для відновлення ЦВЗ необхідно мати первинне зображення
Послідовність псевдовипадкових дійсних чисел, розподілених за гауссівським законом	Модифікація найбільших коефіцієнтів з високочастотного та середньо частотного діапазонів перетворення Хаара	Висока робастність до атак із зміною масштабу.	Для відновлення ЦВЗ необхідно мати первинне зображення
Послідовність псевдовипадкових дійсних чисел, розподілених за гауссівським аконом (довжина відповідає кількості модифікованих коефіцієнтів)	Модифікація значимих коефіцієнтів всіх піддіапазонів п'ятирівневого вейвлет-перетворення	Можливість модифікації алгоритму для використання стегоключа	Для відновлення ЦВЗ необхідно мати первинне зображення
Послідовність псевдовипадкових дійсних чисел, розподілених за гауссівським законом (довжина відповідає кількості модифікованих коефіцієнтів)	Алгоритм є модифікованим варіантом попереднього алгоритму, зі сліпим відновленням ЦВЗ	Для виявлення ЦВЗ не потрібна наявність первинного зображення	Сильно знижена Завадостійкість в порівнянні з попереднім алгоритмом

Продовження таблиці 1.3

Характеристика ЦВЗ	Принцип роботи	Переваги	Недоліки
Алгоритми на основі злиття ЦВЗ та контейнера			
Чорно-білий логотип розміром до 25% від первинного зображення	Модифікація всіх коефіцієнтів однорівневої декомпозиції первинного зображення	Великий розмір ЦВЗ, що приховується (до чверті розміру первинного зображення)	Для відновлення ЦВЗ необхідно мати первинне зображення
Чорно-білий логотип	Модифікація всіх коефіцієнтів детальних піддіапазонів вейвлет перетворення первинного зображення	Для виявлення ЦВЗ не потрібна наявність первинного зображення	
Алгоритми створення ЦВЗ на основі квантування			
Алгоритми з використанням скалярного квантування			
Послідовність ±1	Модифікація високочастотних коефіцієнтів зображення після цілого вейвлет-перетворення	Для виявлення ЦВЗ не потрібна наявність первинного зображення	
Бінарне зображення розміром 1/2 від первинного зображення	Модифікація ВЧ-НЧ та НЧ-ВЧ областей дворівневого вейвлет-перетворення первинного зображення	Великий розмір ЦВЗ, що приховується	Для вилучення ЦВЗ необхідно мати первинне зображення; низька стійкість алгоритму по відношенню до операцій обробки сигналу
Алгоритми з використанням векторного квантування			
Послідовність символів, отримана з логотипу розміром 25% від первинного зображення	Модифікація n мірного вектора коефіцієнтів дискретного вейвлет-перетворення первинного зображення	Великий розмір ЦВЗ, що приховується Можливо контролювати робастність, рівень спотворень і якість вбудованого зображення	Для відновлення ЦВЗ необхідно мати первинне зображення

Продовження таблиці 1.3

Характеристика ЦВЗ	Принцип роботи	Переваги	Недоліки
Алгоритми створення ЦВЗ, що використовують фрактальне перетворення			
Формується з первинного зображення (до 15 різних ЦВЗ)	Модифікація декількох «особливих» точок з використанням методу фрактального кодування Харріса. Для кожної особливої точки виконують зміну доменного блоку тієї ж позиції так, щоб він був більш схожий на ранговий блок	Для виявлення ЦВЗ не потрібна наявність первинного зображення	
Рядок бітів	Модифікація обраного відповідно до ключа рангового блоку в доменному пулі. Якщо треба вбудувати «1», пошук виконується в одній частині пулу, якщо «0» в іншій частині	Наявність секретного ключа; стійкість до стиснення JPEG	
Рядок бітів	Модифікація вручну вибраних двох квадратних областей на зображенні, що не перекриваються (так звані рангова та доменна області)	Наявність секретного ключа	Можливе помітне погіршення якості зображення при вбудовуванні ЦВЗ

1.3. Висновки.

1. Розглянуто способи застосування комп'ютерної стеганографії до створення ЦВЗ. Зазначено, що використання ЦВЗ для підтвердження авторських прав в наш час набувають все більшої популярності. Коротко розглянуто та проаналізовано основні особливості технологій цифрових водяних знаків та вимоги до цих технологій. Розглянуто схему стегосистеми, призначену для вбудовування ЦВЗ в цифрові зображення. Наводиться докладна

класифікація та результати аналізу сучасних алгоритмів вбудовування ЦВЗ у файли-зображення при цьому виділяються клас адитивних алгоритмів, клас алгоритмів, на основі злиття ЦВЗ та контейнера, та клас алгоритмів на основі квантування.

2. Докладно розглядаються основні алгоритми створення ЦВЗ для файлів-зображень, що ґрунтуються на модифікації файлів у первинному поданні. Зазначено, що основною проблемою при реалізації технологій створення ЦВЗ є збереження якості маркованих при впровадженні ЦВЗ файлів при їх використанні за основним призначенням у поєднанні з достовірністю подальшого відновлення ЦВЗ. Основним недоліком відомих рішень є те, що в більшості перерахованих алгоритмів створення ЦВЗ використовуються процедури, що реалізують суворо певні послідовності операцій перетворення даних, в кінцевому рахунку, що утворюють скінченну множину варіантів, які можуть бути ідентифіковані і розкриті.

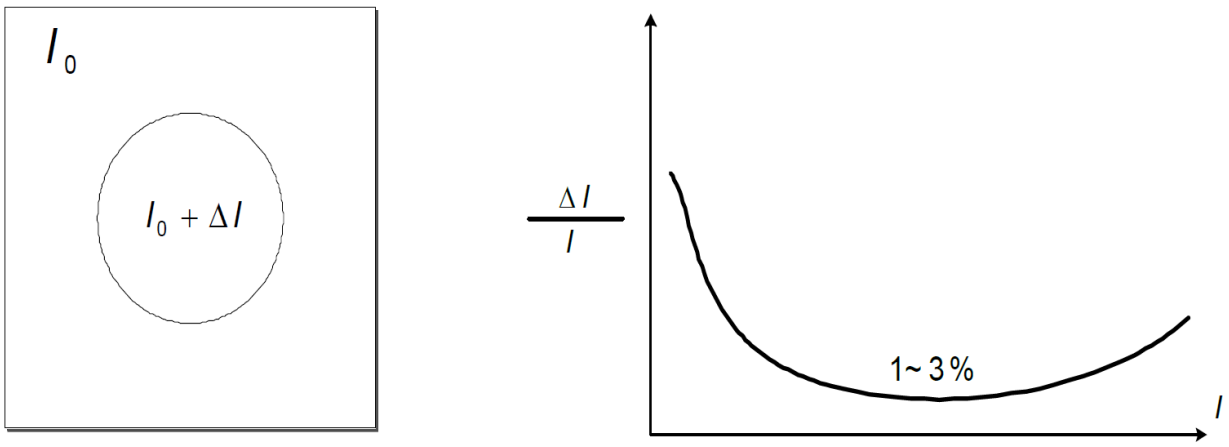
2 АЛГОРИТМИ ВБУДОВУВАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ У 2D ЗОБРАЖЕННЯ

2.1. Основні властивості зорової системи людини, що використовуються при приховуванні даних у зображеннях

Властивості зорової системи людини (ЗСЛ) можна розділити на дві групи: низькорівневі ("фізіологічні") і високорівневі ("психофізіологічні"). До середини 1990-х років дослідники брали до уваги, головним чином, низькорівневі властивості зору. В останні роки намітилася тенденція побудови стеганоалгоритмів з врахуванням і високорівневих характеристик ЗСЛ.

Можна виділити три найбільш важливі низькорівневі властивості, що впливають на помітність стороннього шуму в зображенні: чутливість до зміни яскравості зображення, частотна чутливість і ефект маскування.

Чутливість до зміни яскравості визначається в такий спосіб [21]. Випробуваному показують деяку однотонну картинку (рис. 2.1, а). Після того, як око адаптувалося до її освітленості I, "настроїлося на неї", поступово змінюють яскравість навколо центральної плями. Зміну освітленості ΔI продовжують доти, поки вона не буде виявлена. На рис. 2.1, б наведено залежність мінімального контрасту $\Delta I / I$ від яскравості I.



а б

Рисунок 2.1 – Властивості зорової системи людини

Як видно з рис. 2.1, для середнього діапазону зміни яскравості контраст приблизно постійний, тоді як для малих і більших яскравостей значення порогу нерозрізненості зростає. Було встановлено, що $\Delta I \approx (0.01 - 0.03)I$ для середніх значень яскравості.

Результати новітніх досліджень суперечать "класичній" точці зору і показують, що при малих значеннях яскравості ЗСЛ поріг нерозрізненості зменшується, тобто ЗСЛ більш чутлива до шуму в цьому діапазоні.

Частотна чутливість ЗСЛ проявляється в тому, що людина набагато більш сприйнятлива до низькочастотного (НЧ), ніж до високочастотного (ВЧ) шуму. Це пов’язане з нерівномірністю амплітудно-частотної характеристики системи зору людини. Експериментально її можна визначити за допомогою того ж експерименту, що і при чутливості до яскравості. Але цього разу в центральному квадраті змінюються просторові частоти доти, поки зміни не стануть помітними.

Елементи ЗСЛ розділяють відеосигнал, що надходить, на окремі компоненти. Кожна складова збуджує нервові закінчення ока через ряд підканалів. Вирізнювані оком компоненти мають різні просторові й частотні характеристики, а також різну орієнтацію (горизонтальну, вертикальну, діагональну) [22]. У випадку одночасного впливу на око двох компонентів з подібними характеристиками збуджуються ті самі підканали. Це приводить до ефекту маскування, що полягає в збільшенні порога виявлення відеосигналу в присутності іншого сигналу, що володіє аналогічними характеристиками. Тому адитивний шум набагато помітніше на гладких ділянках зображення, ніж на високочастотних, тобто в останньому випадку спостерігається маскування. Найбільш сильно ефект маскування проявляється, коли обидва сигнали мають однакову орієнтацію й місце розташування.

Частотна чутливість тісно пов’язана з яскравісною. Наразі розроблено формули для визначення порогу маскування на основі відомої яскравісної чутливості, що дозволяє знайти метрику спотворення зображення, що враховує властивості ЗСЛ. Такого типу математичні моделі добре розроблені для

випадку квантування коефіцієнтів дискретного косинусного перетворення зображення, тому що саме воно застосовується в стандарті JPEG.

Ефект маскування в просторовій множині може бути пояснений шляхом побудови стохастичних моделей зображення. При цьому зображення представляється у вигляді марківського випадкового поля, розподіл імовірностей якого підкоряється, наприклад, узагальненому гауссівському закону.

Таким чином, можна запропонувати таку узагальнену схему вбудовування даних у зображення:

1. Виконати фільтрацію зображення за допомогою смугових фільтрів. При цьому можна отримати розподіл енергії по частотно-просторових компонентах.

2. Обчислити поріг маскування на основі знання локальної величини енергії.

3. Масштабувати значення енергії вбудовуваного ЦВЗ у кожному компоненті так, щоб воно було менше порога маскування.

Високорівневі властивості ЗСЛ поки рідко враховуються при побудові стеганоалгоритмів. Їх відмінністю від низькорівневих є те, що ці властивості проявляються "вдруге", обробивши первинну інформацію від ЗСЛ, мозок видає команди на її "підстроювання" під зображення. До основних високорівневих властивостей відносять:

1. Чутливість до контрасту. Висококонтрастні ділянки зображення, перепади яскравості привертають до себе значну увагу.

2. Чутливість до розміру. Більші ділянки зображення "помітніші" менших за розміром. Причому існує поріг насичення, коли подальше збільшення розміру не істотне.

3. Чутливість до форми. Довгі й тонкі об’єкти привертають більшу увагу, ніж круглі однорідні.

4. Чутливість до кольору. Деякі кольори (наприклад, червоний) "помітніші" інших. Цей ефект підсилюється, якщо фон заднього плану відрізняється від кольору фігур на ньому.

5. Чутливість до місця розташування. Людина схильна у першу чергу розглядати центр зображення.

6. зазвичай людина більш уважно розглядає зображення на передньому плані ніж на задньому.

7. Якщо на зображенні є люди, у першу чергу людина зверне свою увагу на них. На фотографії людина звертає першочергову увагу на обличчя, очі, рот, руки.

8. Чутливість до зовнішніх подразників. Рух очей спостерігача залежить від конкретної обстановки, від отриманих їм перед переглядом або під час його інструкцій, додаткової інформації.

2.2 Цифрові формати 2D зображень

Формат BMP [23]. Абревіатура BMP означає BitMap («бітова карта»). Як і випливає з назви, BMP відноситься до тих форматів, де дані представлені «як є», без будь-яких перетворень та стиснення. З цієї причини розмір файлів BMP досить великий, проте формат файлу досить простий, що робить його дуже популярним для застосування як стегоконтейнер.

Існують два способи зберігання стиснених графічних даних.

1. Індексований. Використовує так звану палітру – спеціальний масив даних з описом всіх кольорів, що зустрічаються в зображенні. Матриця зображення містить лише індекси палітри. Зі всього зображення для включення даних може використовуватися лише палітра, інакше виникнуть серйозні спотворення, дуже помітні для людини.

Палітра має постійний розмір 1 Кб, тому дозволяє зберігати лише 128 байт даних незалежно від роздільної здатності та розміру самого зображення. Існують також способи включення даних у все індексоване зображення, проте для цього виконуються перетворення, що призводять до серйозної втрати якості зображення. З цих причин індексовані зображення рідко використовуються стеганографічним програмним забезпеченням.

2. Неіндексований. Цей спосіб представлення даних в основному призначений для повнокольорової графіки та широко поширений. Яскравим представником неіндексованих форматів є 24-бітний BMP. Він найбільш популярний серед різних стеганографіческіх програм.

На рис. 2.2 представлено формат 24-бітового BMP-файлу. На самому початку файлу розташовуються два заголовки з необхідними службовими полями, за ними слідує поле даних, де кожна точка зображення кодується трьома кольоровими компонентами: синім, зеленим і червоним (R, G і B). Під кожну компоненту відводиться по одному байту, отже, один піксель зображення займає 3 байти або 24 біти. При вбудовуванні прихованої інформації в кожен молодший біт максимальна ємність контейнера складе приблизно 12.5 % від його розміру.

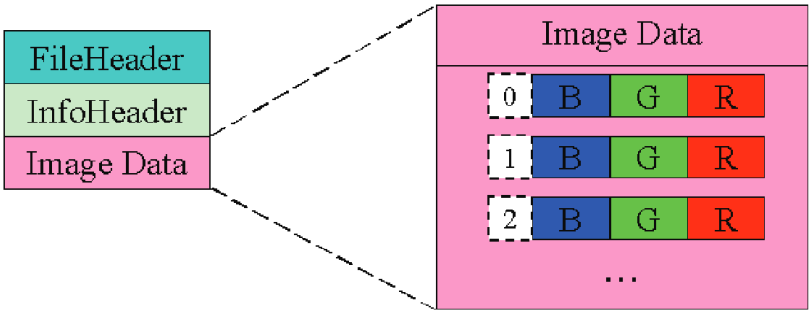


Рисунок 2.2 – Структура 24-бітного BMP-файлу

Формат JPEG [24] розроблений у середині 1980-х Об'єднаною групою експертів з фотографії (Joint Photographic Expert Group) і звідси бере свою назву. Метою групи було створення ефективного алгоритму стиснення повнокольорових зображень. Цей алгоритм досить складний, тому прийнято розрізняти:

• формат JPEG-файлу – спосіб подання даних JPEG у файлі.

• «алгоритм стиснення JPEG» – набір перетворень, які переводять стиснуту графічну інформацію в стислі дані JPEG.

Формат JPEG файлу на відміну від алгоритму стиснення не був стандартизований. В наш час загальноприйнятим стандартом вважається версія формату, що отримала назву JFIF. Зважаючи на певну заплутаність формату

файлу та наявність у ньому всіляких «фірмових» розширень (наприклад, від Adobe), лише невелика частина програм реалізує обробку JPEG-файлу самостійно. Прийнятою практикою є використання бібліотек підтримки форматів, наприклад IJD JPEG Library для формату JPEG. Усі операції з обробки файлу та виконання алгоритму JPEG покладаються на бібліотеку.

На рис. 2.3 наведено основні етапи алгоритму JPEG.

1. Перетворення на колірний простір YCbCr. Вихідні дані можуть бути в будь-якому колірному просторі, наприклад RGB, CMYK та інше, але алгоритм JPEG працює з даними в просторі YCbCr (Y – яскравість, Cb та Cr – хроматичний синій та хроматичний червоний відповідно). Зміна компоненти Y набагато помітніше для людини, ніж зміна Cb і Cr. Тому відразу після 1-го етапу з матриць Cb і Cr, як правило, відкидається кожен другий рядок і кожен другий стовпець.

2. Дискретне косинусне перетворення (ДКП). Являє собою двовимірне перетворення Фур'є. Його основний сенс – переведення даних із просторового подання до частотного.

3. Квантування. Зміна високочастотних складових зображення набагато менш помітна для очей, ніж зміна низькочастотних. Це дозволяє замінити всі високочастотні коефіцієнти ДКП на нульові байти. Квантування є розподіл коефіцієнтів ДКП на елементи спеціальної матриці квантування з наступним округленням. Це призводить до обнулення більшості високочастотних коефіцієнтів.

4. Стиснення без втрат (ентропійне кодування). Отримані після третього етапу дані містять багато нульових байтів, що повторюються, тому ефективно стискаються за допомогою алгоритму кодування довжин повторів (RLE) і потім – алгоритмом Хаффмана.

Структура файлу. Зображення JPEG представляється як послідовність сегментів, де кожен сегмент починається з маркера. Кожен маркер починається з байта 0xFF, за яким слідує прапор маркера, що представляє тип маркера. Корисне навантаження, за яким слідує маркер, залежить від типу мар-

кера. Поширені типи маркерів JPEG перераховані в табл. 2.1.

В ентропійно-кодованих даних після будь-якого байта 0xFF кодер вставляє байт 0x00 перед наступним байтом, щоб не було маркера там, де він не призначений, запобігаючи помилкам кадрування. Декодери повинні пропускати цей байт 0x00. Ця техніка, яка називається байтове наповнення, застосовується лише до ентропійно-кодованих даних, а не до даних корисного навантаження маркера.

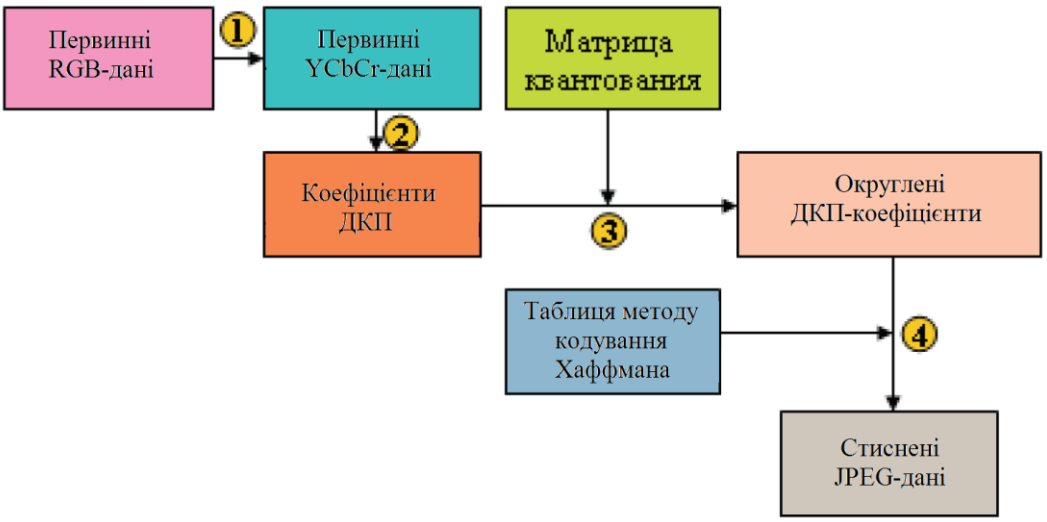


Рисунок 2.3 – Алгоритм стискання JPEG

Таблиця 2.1 – Поширені типи маркерів JPEG

Коротка назва	Байт	Корисне навантаження	Ім’я
SOI	0xFF, 0xD8	немає	Початок зображення
S0F0	0xFF, 0xC0	розмір змінної	Початок кадру
S0F2	0xFF, 0xC2	розмір змінної	Початок кадру
DHT	0xFF, 0xC4	розмір змінної	Визначення таблиці Хаффмана
DQT	0xFF, 0xDB	розмір змінної	Визначення таблиці квантування
DRI	0xFF, 0xDD	4 байти	Визначення інтервалу перезапуску
SOS	0xFF, 0xDA	розмір змінної	Початок сканування
RSTn	0xFF, 0xD//n//(/uk//n//#0..7)	немає	Перезапуск
APPn	0xFF, 0xE//n//	розмір змінної	специфічної програми
COM	0xFF, 0xFE	розмір змінної	Коментар
EOI	0xFF, 0xD9	немає	Кінець зображення

Формат GIF [25] (англ. Graphics Interchange Format) – формат зберігання графічних зображень, здатний зберігати стислі дані без втрати якості у форматі до 256 кольорів. Цей формат був розроблений у 1987 році (GIF87a) фірмою CompuServe для передачі растрових зображень мережами. У 1989-му формат був модифікований (GIF89a), було додано підтримку прозорості та анімації.

Файли формату GIF мають блокову структуру. Дані блоки завжди мають фіксовану довжину, так що помилитися в тому, де який блок знаходиться, практично неможливо. Структура найпростішого неанімованого GIF-зображення формату GIF89a наведена на рис. 2.4.

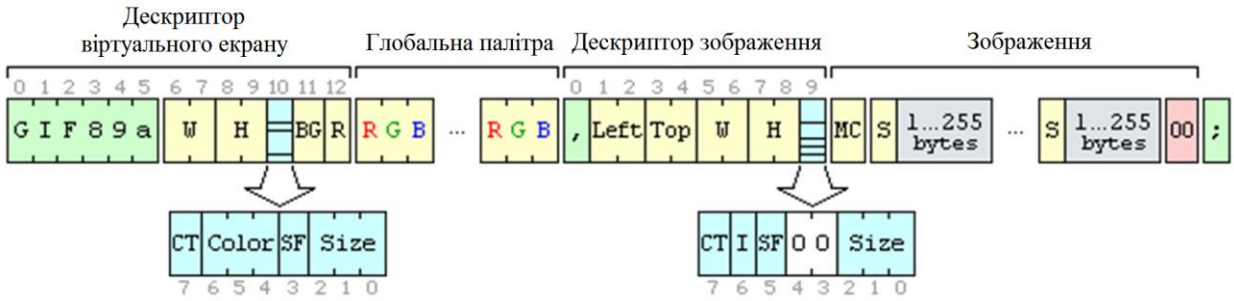


Рисунок 2.4 – Структуру GIF файлу

З усіх блоків для задач стеганографії найчастіше використовують блок глобальної палітри та параметри, які відповідають за палітру:

CT – наявність глобальної палітри. Якщо цей прапор встановлений, відразу після дескриптора логічного екрану повинна починатися глобальна палітра;

Size – розмір палітри та кількість кольорів зображення: від значення $size = 0$ і розміру палітри 6 байт (кількість кольорів – 2) до значення $size = 7$ і розміру палітри 768 байт (кількість кольорів – 256).

Також слід відмітити, що стеганографічний метод розширення палітри працює лише зі структурою GIF. Він буде найбільш ефективним у зображеннях з палітрою невеликих розмірів. Суть методу полягає в тому, що він збільшує розмір палітри, додаючи додатковий простір для запису необхідних байт на місця байтів кольорів. Якщо врахувати що мінімальний розмір палі-

ри становить 2 кольори (6 байт), то максимальний розмір повідомлення може бути $256 \times 3 - 6 = 762$ байти. Недолік – низька криптозахищеність, прочитати вбудоване повідомлення можна за допомогою будь-якого текстового редактора, якщо повідомлення не піддавалося додатковому шифруванню.

Формат PNG [26] призначений для збереження і передачі растрових зображень. Він дає змогу зберігати зображення, бітова глибина яких досягає 16 (у шкалі сірого кольору) або 48 (у truecolor-зображеннях) біт/піксель, а також 16 біт для шару прозорості зображення (альфа-канал).

Кожен PNG файл (див. рис. 2.5) починається з восьми стандартних байт підпису – [89 50 4e 47 0d 0a 1a 0a]. Ця послідовність, яка називається заголовком, буде однаковою для будь-якого PNG-файлу.

Остання частина PNG-файлу складається з блоків байтів, що повторюються та відповідають такому патерну: SIZE (4 байти), TYPE (4 байти), DATA (будь-яка кількість байтів) і CRC (4 байти).

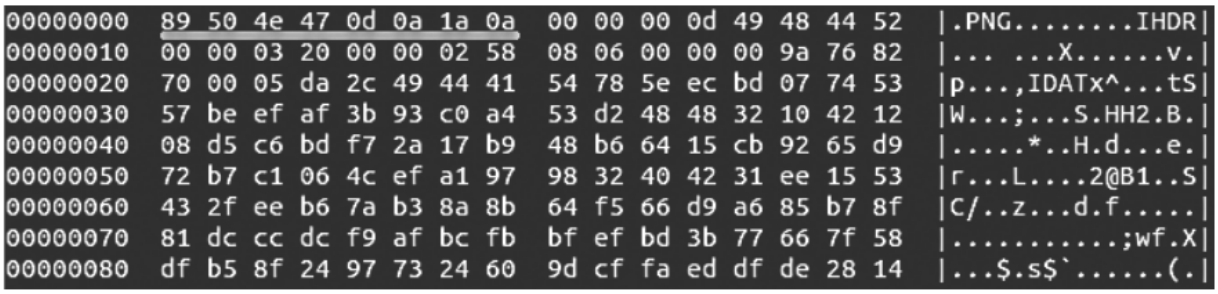


Рисунок 2.5 – Структура PNG файлу у 16-розрядному форматі

На рис. 2.5 можна побачити, що перший блок SIZE складається з байтів [0x00 0x00 0x00 0x0d]. Він визначає довжину блоку DATA. Шістнадцятирозрядне перетворення в десяти-розрядне дає 13, отже, блок DATA складатиметься з 13 байт. Байти блоку TYPE – [0x49 0x48 0x44 0x52] – в наведеному прикладі перетворюються на значення IHDR. Специфікація PNG визначає різні типи. Деякі з них, такі як IHDR, використовуються для визначення метаданих зображення або оповіщення про завершення потоку даних. Інші типи, зокрема IDAT, містять байти самого зображення.

Далі слідує блок DATA, довжина якого визначається блоком SIZE. За-

вершує сегмент блок CRC. Він складається з контрольної суми CRC – 32 байтів TYPE та DATA. Саме цей блок CRC представлений байтами [0x9a 0x76 0x82 0x70] на рис. 2.5. В такому форматі блоки повторюються протягом всього файлу зображення, доки не буде досягнуто стану End of File (EOF), що позначається блоком типу IEND.

Отже, в специфікації формату PNG визначаються основні та допоміжні сегменти блоків. Основні блоки необхідні для обробки зображення декодером, а допоміжні є необов'язковими і надають різні елементи метаданих, не критичні для кодування або декодування, наприклад часові мітки і текст. Таким чином, допоміжний тип блоку це ідеальне місце для перезапису існуючого блоку або впровадження нового.

Специфікація TIFF була розроблена Aldus Corporation у 1986 р. і представила даний формат як стандартний метод збереження чорно-білих зображень, створених сканерами і програмними пакетами верстки. Широкого поширення набула розроблена в квітні 1987 р. модифікація формату 4.0, що змогла підтримувати обробку нестиснених кольорових RGB-зображень. TIFF модифікації 5.0 (що з'явився у серпні 1988 р.) давав змогу зберігати кольорові зображення з палітрою і підтримувати алгоритм стиснення LZW.

Розроблений у червні 1992 р. TIFF 6.0 розширив свої функціональні можливості підтримкою кольорових зображень моделей CMYK і YCbCr, а також використанням методу стиснення JPEG.

Файли TIFF складаються з трьох розділів (див. рис. 2.6): заголовка файлу зображення (Image File Header – IFH), директорії файлу зображень (Image File Directory – IFD) і растрових даних (Тег). З них необхідними є тільки IFH і IFD. Отже, допускається можливість існування файлу TIFF, що не містить растрових даних. Файл TIFF, що містить декілька зображень, буде включати стільки ж директорій файлу і розділів растрових даних (по одному для кожного зображення).

Кожен тег є 12-байтним записом, що містить інформацію про растрові дані. Тег може зберігати дані будь-якого типу, бо специфікація TIFF визначає

понад 70 тегів, що використовуються для представлення заданої інформації. Теги кожної директорії поєднуються в неперервні групи.

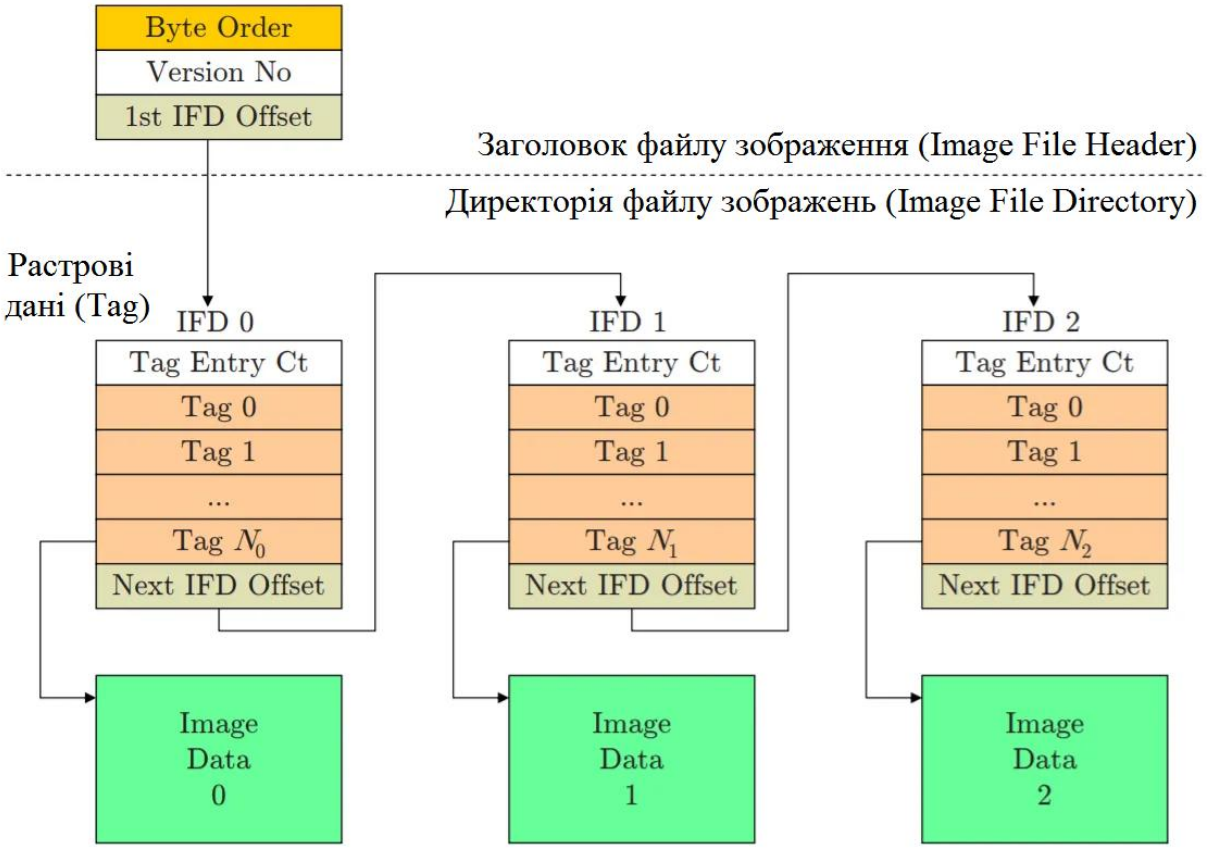


Рисунок 2.6 – Структура TIFF файлу

Файл TIFF може містити будь-яку кількість зображень (включаючи нульову). Кожне зображення розглядається як окремий растровий субфайл, дані якого описуються інформацією IFD. Кожен субфайл TIFF може бути записаний у вигляді окремого файлу або разом з іншими субфайлами об’єднаний в один файл TIFF. Кожен растровий субфайл має свою директорію файлу зображення і може розташовуватися в будь-якому місці (після заголовка). Кожному зображенню може відповідати тільки одна директорія.

Отже, TIFF файли забезпечують більше свободу у виборі місця вбудовування повідомлення.

2.3. Алгоритми, засновані на вбудовуванні ЦВЗ у коефіцієнти дискретного косинусного перетворення зображення

Як було зазначено у першій главі кваліфікаційної роботи, увагою розробників алгоритмів генерування та вбудовування робастних цифрових водяних знаків користуються методи вбудовування у коефіцієнти швидких перетворень. Найвідомішими і придатними для цього завдання є дискретне косинусне перетворення (ДКП) та дискретне вейвлетне перетворення (ДВП).

2.3.1. Дискретне косинусне перетворення.

Дискретне косинусне перетворення – ортогональне перетворення, варіант косинусного перетворення для вектора дійсних чисел. В ДКП зображення сприймається як сукупність просторових хвиль, для яких вісі X і Y проводяться паралельно поздовжній і поперечній вісям зображення, а по вісі Z відкладається значення кольору відповідного пікселя зображення [28].

Найбільш поширений двовимірний варіант перетворення для матриць $N \times N$. Таким чином, спочатку первинне зображення розбивається на блоки розмірністю $N \times N$ пікселів, а потім ДКП застосовується до кожного блоку.

Двовимірні пряме та обернене дискретне косинусне перетворення для блоку з індексом b розраховуються за формулами:

$$\Omega_b(\upsilon,\nu) = \frac{\zeta(\upsilon)\cdot\gamma(\nu)}{\sqrt{2N}} \times \\ \times \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} C_b(x,y)\cos\left[\frac{\pi\cdot\upsilon\cdot(2x+1)}{2N}\right]\cos\left[\frac{\pi\cdot\nu\cdot(2y+1)}{2N}\right]', \tag{2.1}$$

$$C_b(x,y) = \frac{1}{\sqrt{2N}}\sum_{\upsilon=0}^{N-1}\sum_{\nu=0}^{N-1}\left[\begin{array}{c}\zeta(\upsilon)\gamma(\nu)\cdot\Omega_b(\upsilon,\nu)\times \\ \times\cos\left[\frac{\pi\upsilon\cdot(2x+1)}{2N}\right]\cos\left[\frac{\pi\nu\cdot(2y+1)}{2N}\right]\end{array}\right], \tag{2.2}$$

$$\zeta(\upsilon) = \begin{cases}\frac{1}{\sqrt{N}}, \upsilon = 0, \\ \sqrt{\frac{2}{N}}, 0 < \upsilon < N-1.\end{cases}, \quad \gamma(\nu) = \begin{cases}\frac{1}{\sqrt{N}}, \nu = 0, \\ \sqrt{\frac{2}{N}}, 0 < \nu < N-1.\end{cases},$$

де $C_b(x, y)$ – значення пікселя блоку b в позиції (x, y); (υ, ν) – позиція коефіцієнту ДКП в блоці b.

В результат і перетворення (2.1) можна отримати матрицю розміром $N \times N$ коефіцієнтів ДКП, які позначаються $\Omega_b(\upsilon, \nu)$.

Коефіцієнт у лівому верхньому куті матриці Ω_b (тобто $\Omega_b(1,1)$) містить інформацію про яскравість всього блоку (його зазвичай називають DC-коефіцієнтом). Інші коефіцієнти називаються AC-коефіцієнтами. Причому, коефіцієнти НЧ компонентів розташовані ближче до лівого верхнього кута, а ВЧ компонентів – ближче до правого нижнього кута (рис. 2.7).

	1	2	3	4	5	6	7	8
1	–603	203	11	45	–30	–14	–14	–7
2	–108	–93	10	49	27	6	8	2
3	–42	–20	–6	16	17	9	3	3
4	56	69	7	–25	–10	–5	–2	–2
5	–33	–21	17	8	3	–4	–5	–3
6	–16	–14	8	2	–4	–2	1	1
7	0	–5	–6	–1	2	3	1	1
8	9	5	–6	–9	0	3	3	2

– НЧ компоненти;
– СЧ компоненти;
– ВЧ компоненти.

Рисунок 2.7 – Приклад матриці $\Omega_b(\upsilon, \nu)$ коефіцієнтів ДКП

Як було зазначено в розділі 2.1, НЧ компоненти містять переважну частину енергії зображення і, отже, носять шумовий характер. ВЧ компоненти більше піддаються впливові з боку різних алгоритмів обробки. Таким чином, для вбудовування повідомлення більш оптимальними є середньочастотні компоненти спектру зображення.

Розглянемо приклад обчислення пари двовимірних дискретних косинусних перетворень у блоках із розмірами 8x8 елементів первинного зображення. Далі при реконструкції зображення буде враховано лише 10 коефіцієнтів з кожного блоку, решту прирівняємо до нуля.

На рис. 2.8 представлено два зображення – первинне та реконструйова-

не. При реконструкції зображення використовувалося лише 15 % коефіцієнтів дискретного косинусного перетворення. Однак, слід зазначити, що якість реконструйованого зображення є досить прийнятною.

Як висновок можна відзначити переваги та недоліки даного методу. До переваг можна віднести простоту реалізації. Цей метод не вимагає великих апаратних ресурсів. Але у зв'язку з цим виникає очевидний недолік методу. Під час перетворення зображення необхідно розбивати на блоки (зазвичай 8x8 елементів) і обробляти їх окремо. У результаті відновлення вихідного зображення буде помітна блокова структура.

Рисунок 2.8 – Приклад стиснення зображення
на основі дискретного косинусного перетворення

2.3.2 Метод Коха-Жао (Koch-Zhao)

Під час організації секретного каналу одержувачу має бути відомо про два конкретні обрані коефіцієнти ДКП з кожного блоку 8x8, які будуть використовуватися для приховування даних [29]. Ці коефіцієнти задаються їх координатами в масивах коефіцієнтів ДКП: (v_1, ν_1) і (v_2, ν_2). Крім цього, зазначені коефіцієнти повинні відповідати косинус-функціям із середніми частотами, що забезпечить приховування інформації у несуттєвих для ЗСЛ областях сигналу. Також з огляду на високорівневі особливості ЗСЛ, секретне по-

відомлення вбудовується у канал синього кольору зображення

Сам процес приховання починається з випадкового вибору блоку C_b зображення, призначеного для кодування біта повідомлення з індексом b. Вбудовування інформації здійснюється таким чином: для передачі біта зі значенням «0» різницю абсолютних значень коефіцієнтів ДКП штучно роблять більшою за деяку додатну величину, а для передачі біта зі значенням «1» ця різниця робиться меншою порівняно з деякою від'ємною величиною:

$$\begin{aligned} &|\Omega_b(v_1, \nu_1)| - |\Omega_b(v_2, \nu_2)| > P, \ \ при \ \ w_b = 0; \\ &|\Omega_b(v_1, \nu_1)| - |\Omega_b(v_2, \nu_2)| < -P, \ \ при \ \ w_b = 1. \end{aligned} \tag{2.3}$$

Ці зміни вносяться в коефіцієнти ДКП, якщо їх різниця не відповідає біту, що приховується. Чим більше значення P, тим стеганосистема, що використовує даний алгоритм, є більш стійкою до стиснення JPEG, при цьому якість зображення погіршується. Після внесення змін до значень коефіцієнтів, які повинні задовольняти умовам у формулі (2.3), проводиться зворотне ДКП.

Для отримання даних одержувач виконує аналогічну процедуру вибору коефіцієнтів на основі отриманих від відправника відомостей про вбудовування ЦВЗ (індекси блоків, в які велося вбудовування; індекси коефіцієнтів всередині блоку і значення параметра різниці P), а рішення про переданий біт приймається відповідно до наступного правила:

$$\begin{aligned} &w_b^* = 0, \ \ \text{при} \ \ |\Omega_b^*(v_1, \nu_1)| > |\Omega_b^*(v_2, \nu_2)|, \\ &w_b^* = 1, \ \ \text{при} \ \ |\Omega_b^*(v_1, \nu_1)| < |\Omega_b^*(v_2, \nu_2)|. \end{aligned} \tag{2.4}$$

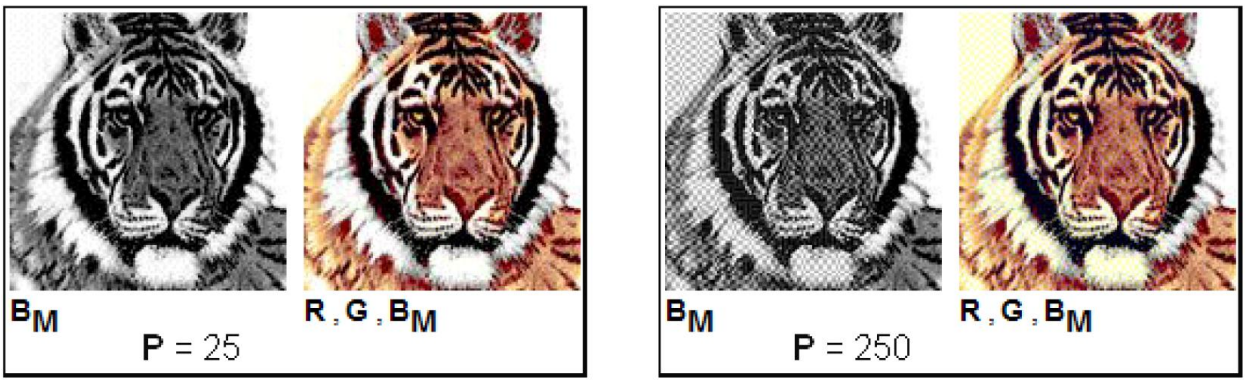


Рисунок 2.9 – Результати вбудовування секретного повідомлення методом Коха-Жао при різних значеннях порогу P

Приклад вбудовування секретного повідомлення M до контейнера шляхом модифікації коефіцієнтів ДКП сегментів в канал синього кольору і контейнер-результат при різних значеннях порогу P при незмінних координатах (υ_1, ν_1) та υ_2, ν_2 наведено на рис. 2.9. Як можна бачити, збільшення порогу P призводить до збільшення спотворень зображення файлу-контейнера.

Метод є досить стійким до спотворення зображення, навіть до його суттєвої зміни, але для приховування великих обсягів даних не застосовується, бо кожен блок 8x8 придатний для запису лише одного біта інформації.

2.3.3 Метод Бенгама-Мемона-Ео-Юнг (Benham-Memon-Yeo-Yeung)

Цей метод використовує ідеї попереднього. Істотним нововведенням є вибір найбільш підходящих для вбудовування блоків та відносна зміна значень трьох (замість двох) середньочастотних коефіцієнтів всередині блоку, що обумовлено зменшенням спотворень при вбудовуванні [30].

Розглянемо зазначені удосконалення більш докладно.

Придатними для вбудовування інформації вважаються блоки зображення, які одночасно задовольняють наступним двом вимогам: 1) блоки не повинні мати різких переходів яскравості; 2) не повинні бути занадто монотонними. Блоки, що не відповідають першій вимозі, характеризуються наявністю декількох занадто великих значень низькочастотних коефіцієнтів ДКП, порівнянних за своєю величиною з DC-коефіцієнтом. Для блоків, що не задовольняють другій вимозі, є характерною рівність нулеві більшості високочастотних коефіцієнтів. Вказані особливості являються критерієм відбраковування непридатних блоків.

Зазначені вимоги відбраковування враховуються використанням двох порогових коефіцієнтів: P_L (для першої вимоги) і P_H (для другої вимоги), перевищення (P_L) або недосягнення (P_H) яких вказуватиме, що блок не придатний для модифікацій у частотній області.

Вбудовування біту повідомлення до блоку здійснюється наступним чи-

ном. Обираються (для більшої стійкості стеганосистеми – псевдовипадково) три коефіцієнти ДКП блоку з середньочастотної області з координатами (υ_1, ν_1), (υ_2, ν_2) та (υ_3, ν_3). Якщо необхідно провести вбудовування «0» $(w_b = 0)$, ці коефіцієнти змінюються таким чином, щоб третій коефіцієнт став менше кожного з перших двох; якщо потрібно приховати «1» $(w_b = 1)$, він робиться більшим за інші:

$$\begin{cases} |\Omega_b(\upsilon_3, \nu_3)| < |\Omega_b(\upsilon_1, \nu_1)| \\ |\Omega_b(\upsilon_3, \nu_3)| < |\Omega_b(\upsilon_2, \nu_2)| \end{cases} \text{при} \quad w_b = 0, \\ \begin{cases} |\Omega_b(\upsilon_3, \nu_3)| > |\Omega_b(\upsilon_1, \nu_1)| \\ |\Omega_b(\upsilon_3, \nu_3)| > |\Omega_b(\upsilon_1, \nu_1)| \end{cases} \text{при} \quad w_b = 1. \tag{2.5}$$

Як і у попередньому методі, для встановлення достатності розрізнення зазначених коефіцієнтів ДКП, введемо до виразу (2.5) вводиться значення порогу розрізнення P:

$$\begin{cases} |\Omega_b(\upsilon_3, \nu_3)| < \min(|\Omega_b(\upsilon_1, \nu_1)|, |\Omega_b(\upsilon_2, \nu_2)|) - P, & \text{при} \quad w_b = 0, \\ |\Omega_b(\upsilon_3, \nu_3)| > \max(|\Omega_b(\upsilon_1, \nu_1)|, |\Omega_b(\upsilon_2, \nu_2)|) - P, & \text{при} \quad w_b = 1. \end{cases} \tag{2.6}$$

У випадку, якщо така модифікація призводить до занадто великої деградації зображення, коефіцієнти не змінюють, тобто блок не використовується в якості контейнера.

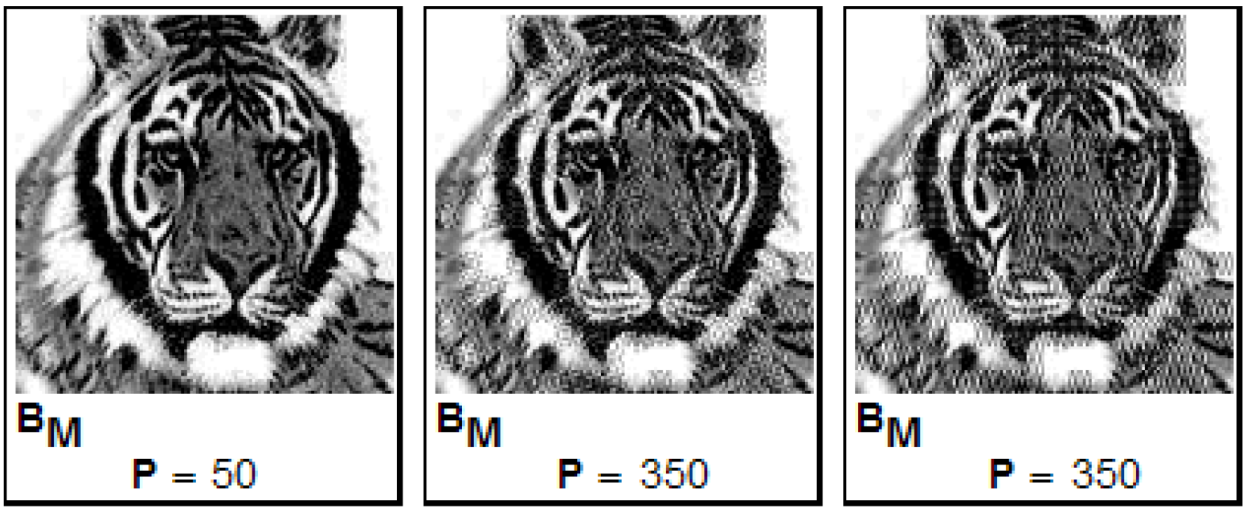


Рисунок 2.10 – Результати вбудовування секретного повідомлення методом Бенгама-Мемона-Ео-Юнг в канал синього кольору при різних значеннях порогу P

Використання трьох коефіцієнтів замість двох і, що найголовніше, відмова від модифікації у випадку неприйнятних спотворювань зображення зменшує похибки, що вносяться повідомленням. Одержувач завжди може визначити блоки, до яких не проводилося вбудовування, повторивши аналіз, аналогічний виконаному на передавальній стороні.

Приклад вбудовування секретного повідомлення M до контейнера методом Бенгама-Мемона-Ео-Юнг в канал синього кольору при різних значеннях порогу P при незмінних початкових даних наведено на рис. 2.10. Як можна бачити з рис. 2.9 та рис. 2.10, метод Бенгама-Мемона-Ео-Юнг має перевагу над методом Коха і Жао, оскільки перший дозволяє ефективно відібрати саме ті блоки зображення, вбудовування до яких буде якнайменш помітним.

2.3.4 Метод Хсу-Ву (Hsu-Wu)

У цьому методі для відновлення повідомлення одержувачу потрібно знати первинне зображення-контейнер [31].

Нехай C – первинне напівтонове зображення розміром $X \times Y$, а ЦВЗ (W) – двійкове зображення розміром $A \times Z$. Оскільки пікселі мають ЦВЗ приймати лише значення 0 та 1, тобто інтенсивність будь-якого пікселю дорівнює 0 чи 1, що відповідає чорному кольору, то спочатку у чорно-білому зображення ЦВЗ замінюється інтенсивність білих пікселів (255) на 1. Відповідно при відновленні треба матрицю яскравості ЦВЗ помножити на 255.

Метод передбачає, що кожен блок ЦВЗ вбудовується до коефіцієнтів ДКП кожного блоку контейнера шляхом використання блочного перетворення замість перетворення всього контейнера. Тому, замість загального контейнера, кожен блок ЦВЗ буде розсіяний лише по відповідному блоку першого. Очевидно, що за відсутності належного регулювання просторових зв’язків ЦВЗ, звичайне масштабування контейнера може зруйнувати ЦВЗ.

Для забезпечення стійкості до масштабування авторами було запропоновано псевдовипадкову перестановку пікселів в блоці ЦВЗ.

Для збільшення рівня прихованості, повинні бути враховані характеристики контейнера (наприклад, відомо, що модифікація високих частот або ділянок з більшою яскравістю є менш помітною). Подібні, залежні від контейнера властивості можуть бути використані для перестановки псевдовипадково змішаного ЦВЗ для одержання більшої відповідності чутливості ЗСЛ. Автори пропонують впорядкувати блоки контейнера за зміною дисперсій інтенсивностей пікселів (наприклад, по їх зменшенню). У свою чергу, блоки ЦВЗ сортуються за кількістю інформації (тобто кількістю значущих (одиничних) пікселів). Вид сортування блоків ЦВЗ (за зростанням / за убуванням) повинен відповідати аналогічній операції над блоками контейнера. Таким чином, кожному блоку контейнера відповідає свій блок ЦВЗ. На рис. 2.11 наведено приклад сортування і перестановки блоків.

Індекс блоку контейнера	*Значення дисперсії*
7	67.1
2	61.2
3	53.0
6	41.9
1	32.3
5	14.5
4	7.4

Індекс блоку ЦВЗ	*Кількість одиниць*
4	15
1	13
3	10
2	9
6	8
7	6
5	3

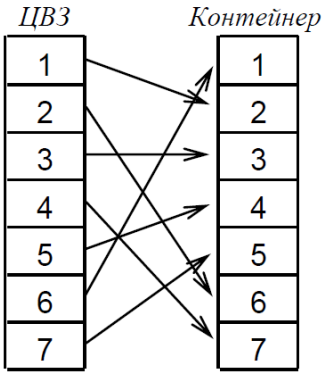


Рисунок 2.11 – Приклад перестановки блоків ЦВЗ
в залежності від характеристик блоків контейнера

Для того, щоб вбудований ЦВЗ був візуально непомітним і залишався стійким до компресії даних із втратами, очевидним компромісом є його вбудовування до діапазону середніх частот контейнера. При цьому, для кожного блоку 8×8 контейнера з наявних 64-х відбираються $64 \times A \times Z/(X \times Y)$ коефіцієнти ДКП, розміщені вздовж другої діагоналі матриці ДКП. Відібрані коефіцієнти для зручності подальших дій згортаються до зменшеної матриці розмірністю $\left(\frac{8A}{X}\right) \times \left(\frac{8Z}{Y}\right)$.

Зокрема, якщо $A = X/2$ та $Z = Y/2$, під час вбудовування ЦВЗ обробляються лише 16 коефіцієнтів ДКП, а інші 48 залишаються незміненими. Викладений вище процес формування масиву СЧ-коефіцієнтів ДКП проілюстровано на рис. 2.12.

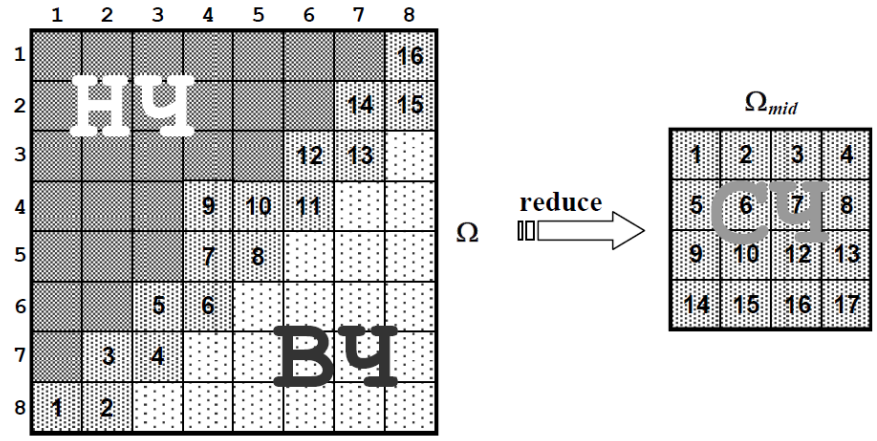


Рисунок 2.12 – Конфігурація матриці коефіцієнтів ДКП
і приклад зведення СЧ-коефіцієнтів до окремої матриці

В результаті попередніх дій можна отримати: переставлений у псевдовипадковому порядку і поставлений у відповідність до блоку контейнера блок ЦВЗ, а також призведене частотне відображення контейнеру (яке містить лише СЧ-компоненти первинного зображення), обидва розмірністю $\left(\frac{8A}{X}\right) \times \left(\frac{8Z}{Y}\right)$.

На думку авторів алгоритму, ефективним засобом досягнення непомітності ЦВЗ і стійкості стеганосистеми при низьких коефіцієнтах JPEG-компресії є вбудовування кожного пікселя ЦВЗ шляхом модифікації полярності між відповідними пікселями сусідніх блоків.

Для підрахунку полярності обраних СЧ-коефіцієнтів сусідніх блоків використовується так звана “залишкова” маска – матриця 3×3, причому центральній позиції відповідає поточне відображення ДКП. В такому разі полярність становитиме собою двійковий образ – масив нулів та одиниць, який характеризуватиме, що коефіцієнт ДКП поточної позиції даного блоку відображення коефіцієнтів ДКП є більшим (полярність дорівнює 1) або меншим

(полярність дорівнює 0) за коефіцієнт на відповідній позиції попереднього блоку.

Після одержання відображень полярності P для всіх блоків контейнера, проводиться виявлення коефіцієнтів ДКП, які потребують модифікації для приховання окремого пікселі переставленого ЦВЗ. Пошук проводиться у відповідності до залишкової маски шляхом зміни поточної полярності.

Далі, на основі масивів полярності $\tilde{P}$ для кожного блоку контейнера формують матрицю модифікованих СЧ-коефіцієнтів ДКП за умови, щоб різниця між первинною матрицею СЧ-коефіцієнтів та отриманою матрицею була зведена до мінімуму або була меншою за встановлений поріг.

Для того, щоб зменшити деградацію зображення (як наслідок вбудовування ЦВЗ), автори методу пропонують обчислювати полярність для абсолютних значень коефіцієнтів ДКП, що дозволить гарантовано зберегти знак (плюс або мінус) модифікованого коефіцієнта.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

а

8	6	5	8	12	20	26	31
6	6	7	10	13	29	30	28
7	7	8	12	20	29	35	28
7	9	11	15	26	44	40	31
9	11	19	28	34	55	52	39
12	18	28	32	41	52	57	46
25	32	39	44	52	61	60	51
36	47	48	49	56	50	52	50

б

Рисунок 2.13 – Приклади таблиць квантування яскравості:
стандартна JPEG (а) та Image Alchemy, Handmade Software Inc. (б)

Крім того, для підвищення стійкості стеганосистеми до JPEG-компресії із втратами, повинен бути врахований ефект квантування, що використовується у технології JPEG. На рис. 2.13, а наведено таблицю квантування яскравості, пропоновану стандартом JPEG, яка, зазвичай, викликає помітні спотворення (так звані «артефакти») зображення. На рис. 2.13, б зображено іншу

таблицю квантування, використовувану у більшості програм, які працюють з JPEG. Видно, що значення при цьому є майже вдвічі меншими за відповідні у попередній таблиці.

Заснована на таблиці квантування полярність являє собою результат обчислення різниці між квантованими і згодом деквантованими коефіцієнтами ДКП відповідних блоків.

Показники візуального спотворення для розглянутого методу є більшими, ніж для двох попередніх методів, проте тут слід взяти до уваги те, що до контейнера вбудовується інформація, об'єм (у пікселях) якої всього у 4 рази менший за об'єм контейнера. Тобто за критерію об'єм / кількість спотворень цей метод є найкращим.

2.4 Алгоритми, засновані на вбудовуванні ЦВЗ в коефіцієнти дискретного вейвлет-перетворення зображення

Використання ВП в стеганографії зображень полягає в ієрархічному розкладанні вхідного сигналу на послідовності так званих базових компонент з послідовно зменшуваним розрідженням і пов'язаних з ними компонентів деталей (дозволяє добре локалізувати низькочастотні деталі сигналу в частотній області, а високочастотні – в часовій). На кожному рівні розкладання базова компонента і компонента деталей містять інформацію, необхідну для відновлення базового сигналу на наступному рівні більш з високою роздільною здатністю.

2.4.1 Перетворення Хаара

Перетворення Хаара (ПХ) є одним з найпростіших базисних вейвлет-перетворень. Нехай задано одновимірний дискретний сигнал $f = (f_1, f_2, \ldots, f_N)$. ПХ розкладає цей сигнал на два компоненти, один із яких називається «середнім», а інший відомий як «різниця» [28]. Перше середнє значення підсигналу $a^1 = (a_1, a_2, \ldots, a_{N/2})$ на першому рівні для одного сиг-

налу довжиною N ($f = (f_1, f_2, \ldots, f_N)$) обчислюється за формулою:

$$a_n = \frac{f_{2n-1} + f_{2n}}{\sqrt{2}}, \quad n = 1, 2, \ldots \frac{N}{2} \tag{2.7}$$

і перший різницевий (або деталізуючий) підсигнал $d^1 = (d_1, d_2, \ldots, d_{N/2})$ на цьому ж рівні розраховується наступним чином:

$$d_n = \frac{f_{2n-1} - f_{2n}}{\sqrt{2}}, \qquad n = 1, 2, \ldots \frac{N}{2}. \tag{2.8}$$

Ці значення формують два нових сигнали: $a = \{a_n\}$ та $d = \{d_n\}$, один з яких є огрубленою версією вихідного сигналу (кожній парі елементів f відповідає їх середнє арифметичне), а інший містить інформацію (деталізуючу), потрібну для відновлення первинного сигналу:

$$f_{2n-1} = a_n + d_n, \qquad f_{2n} = a_n - d_n. \tag{2.9}$$

До сигналу a можна застосувати аналогічну операцію і також отримати два сигнали, один з яких є огрубленою версією a, а інший містить деталізуючу інформацію, необхідну для відновлення a.

Наступний приклад ілюструє принцип роботи вейвлет-перетворення. Нехай

$$I = \begin{vmatrix} 1 & 2 & 3 & 4 \\ 4 & 5 & 6 & 7 \\ 8 & 9 & 1 & 2 \\ 3 & 4 & 5 & 6 \end{vmatrix}$$

У разі застосування одновимірного ПХ уздовж першого рядка коефіцієнти апроксимації наступні: $(1+2)/\sqrt{2}$, $(3+4)/\sqrt{2}$, коефіцієнти відмінності: $(1-2)/\sqrt{2}$, $(3-4)/\sqrt{2}$. Теж саме перетворення застосовується до інших рядків матриці I. Маючи коефіцієнти апроксимації кожного рядка в перших двох стовпцях і відповідні коефіцієнти відмінності в останніх двох стовпцях, можна отримати (коефіцієнти апроксимації та коефіцієнти відмінності в кожному рядку відокремлені точками):

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 4 & 5 & 6 & 7 \\ 8 & 9 & 1 & 2 \\ 3 & 4 & 5 & 6 \end{vmatrix} \rightarrow \frac{1}{\sqrt{2}} \left|\begin{array}{cc:cc} 3 & 7 & -1 & -1 \\ 9 & 13 & -1 & -1 \\ 17 & 3 & -1 & -1 \\ 7 & 11 & -1 & -1 \end{array}\right|.$$

Застосовуючи на наступному етапі одновимірне ПХ до стовпця результуючої матриці, можна отримати результуючу матрицю на першому рівні:

$$\frac{1}{\sqrt{2}}\begin{vmatrix} 3 & 7 & \vdots & -1 & -1 \\ 9 & 13 & \vdots & -1 & -1 \\ 17 & 3 & \vdots & -1 & -1 \\ 7 & 11 & \vdots & -1 & -1 \end{vmatrix} \rightarrow \frac{1}{\sqrt{2}}\begin{vmatrix} 12 & 20 & \vdots & -2 & -2 \\ 24 & 14 & \vdots & -2 & -2 \\ \cdots & \cdots & \vdots & \cdots & \cdots \\ -6 & -6 & \vdots & 0 & 0 \\ 10 & -8 & \vdots & 0 & 0 \end{vmatrix}.$$

Таким чином:

$$A = \begin{vmatrix} 12 & 20 \\ 24 & 14 \end{vmatrix}, \qquad H = \begin{vmatrix} -2 & -2 \\ -2 & -2 \end{vmatrix}, \; V = \begin{vmatrix} -6 & -6 \\ 10 & -8 \end{vmatrix}, \; D = \begin{vmatrix} 0 & 0 \\ 0 & 0 \end{vmatrix}.$$

Як можна бачити, кожна частина одновимірного ПХ дослідного прикладу має розмірність 2×2. Область A (область наближення) містить інформацію про глобальні властивості зображення. Видалення спектральних коефіцієнтів з цієї області призводить до найбільшого спотворення первинного зображення. Область H (горизонтальна область) містить інформацію про вертикальні рядки зображення. Видалення спектральних коефіцієнтів з цієї області видаляє горизонтальні деталі з первинного зображення. Область V (вертикальна область) містить інформацію про горизонтальні рядки зображення. Видалення спектральних коефіцієнтів з цієї області призводить до видалення вертикальних деталей з первинного зображення. Область D (діагональна область) містить інформацію про діагональні деталі зображення. Видалення спектральних коефіцієнтів з цієї області призводить до мінімального спотворення первинного зображення.

Двовимірне вейвлет-перетворення є почерговими одновимірними вейвлет-перетвореннями рядків і стовпців матриці яскравості зображення. Спочатку виконуються одновимірні вейвлет-перетворення кожного рядка, після чого перетворений рядок записується на колишнє місце. Далі вейвлет-перетворення застосовуються до всіх стовпців. В результаті зображення розбивається на чотири рівні частини (рис. 2.14): LL, LH, HL, HH. Квадрант LL відповідає низькочастотним вейвлет-коефіцієнтам, високочастотним HH [28].

Під N-кратним двовимірним вейвлет-перетворенням розуміють застосування N раз двовимірного вейвлет-перетворення, причому чергове двови-

мірне вейвлет-перетворення застосовується до молодшої чверті матриці (квадрант LL на рис. 2.15). Отримане N-кратне перетворення наведено на рис. 2.15 ($N = 3$).

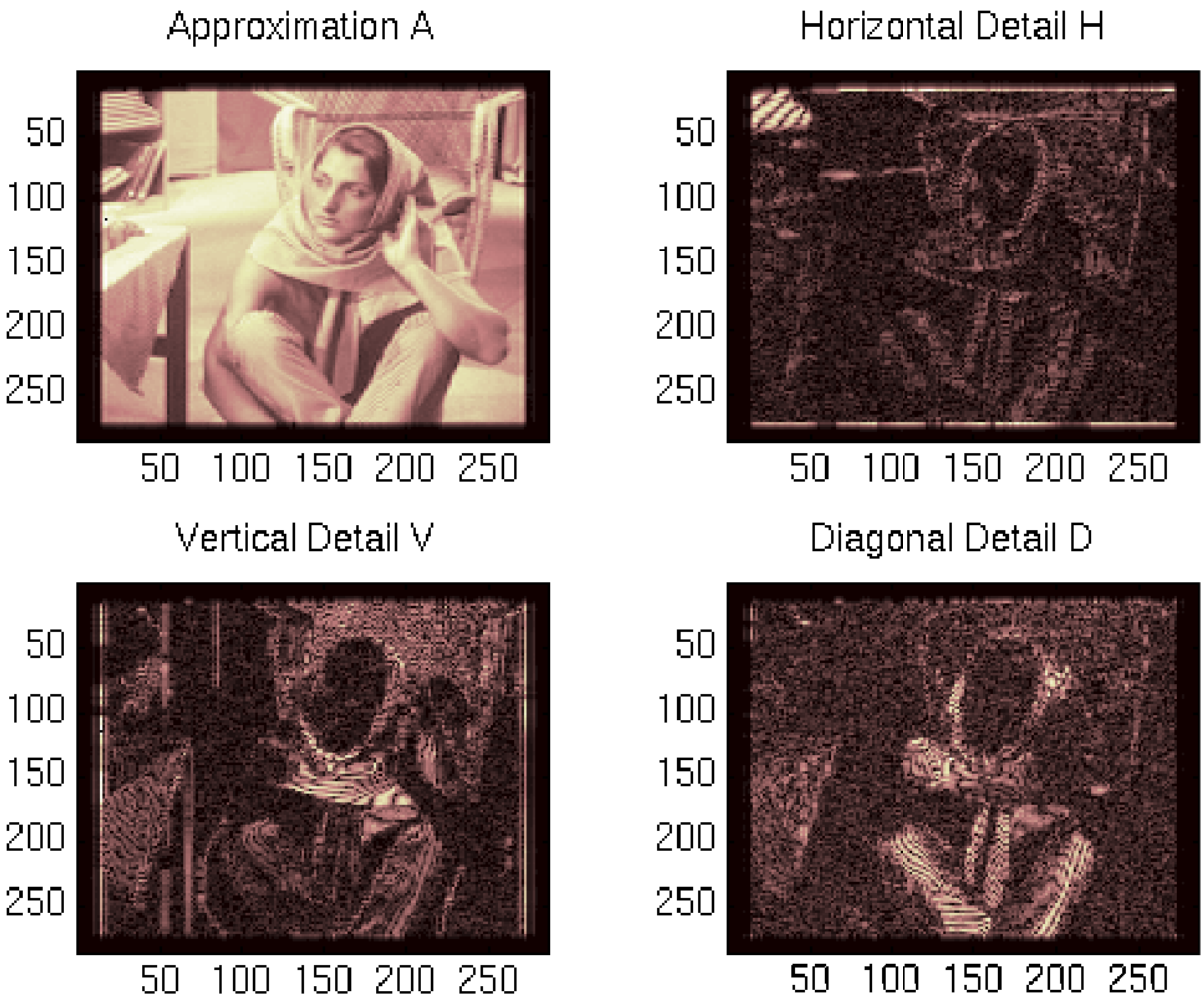


Рисунок 2.14 – Пояснення до матриць $A,\ H,\ V,\ D$
одновимірного вейвлет-перетворення

Зворотне двовимірне вейвлет-перетворення рекурсивно відновлює молодший квадрант. У разі прикладу з на рис. 2.16 для отримання (відновлення) нового квадранту LL2 використовуються квадранти LL3, LH3, HL3 і HH3. Далі, для відновлення квадранта LL1 використовуються квадранти LL2, LH2, HL2, HH2 і т.д.. Аналогічно виконується N-кратное зворотне вейвлет-перетворення.

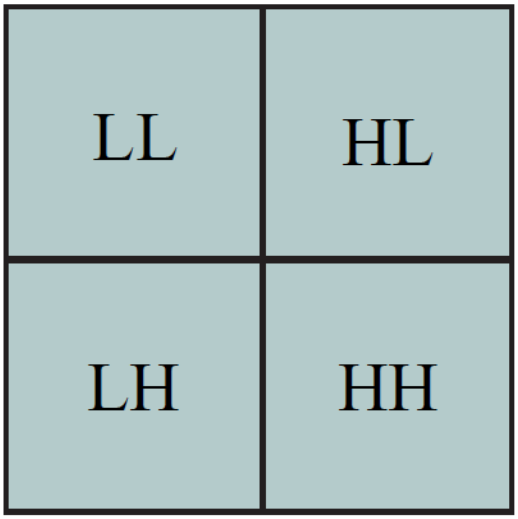


Рисунок 2.15 – Однорівневе двовимірне вейвлет-перетворення квадратного зображення

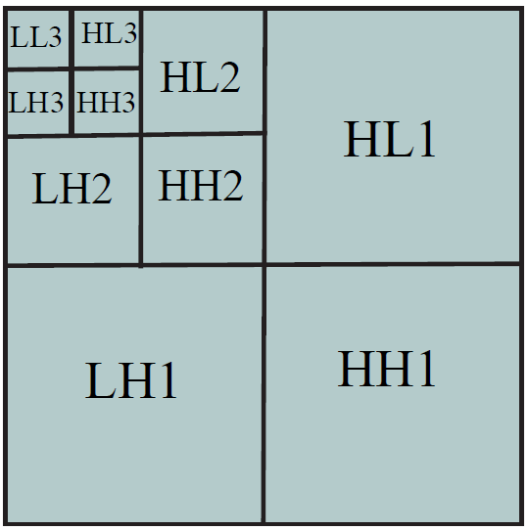


Рисунок 2.16 – Трирівневе двовимірне вейвлет-перетворення квадратного зображення

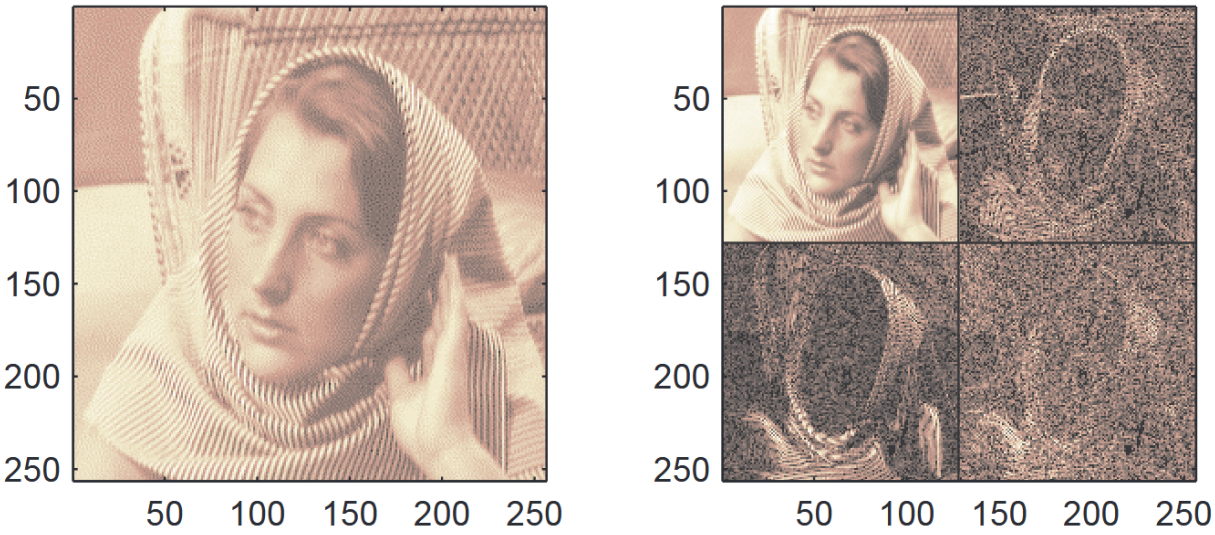


Рисунок 2.17 – Застосування $(N-1)$-кратного зворотного вейвлет-перетворення до зображення, отриманого N-кратним вейвлет-перетворенням

Перетворення Хаара є ієрархічним, тобто якщо при використанні зворотного вейвлет-перетворення обчислюються не всі рівні, а менша їх кількість, то в квадранті LL утворюється зменшена копія первинного зображення (рис. 2.17). Якщо зворотне вейвлет-перетворення не використовується, молодший квадрант також є зменшеною копією зображення. Внаслідок цієї властивості зворотне вейвлет-перетворення дозволяє вирізати фрагменти зобра-

жень різного масштабу. Однак, по-перше, доступні масштаби визначаються кількістю рівнів вейвлет-перетворення, і, по-друге, масштаби не довільні, а збільшені вдвічі.

2.4.2 Алгоритм Сангхаві (Sanghavi)

Алгоритм заснований на вбудовуванні ЦВЗ в зображення шляхом зміни розташування коефіцієнтів ДВП і може застосовуватися як для статичних зображень, так і для відео-файлів [32].

В алгоритмі використовується 4-рівневе вейвлет-перетворення Хаара. Цифровий водяний знак являє собою чорно-біле зображення. Вбудовування бітів ЦВЗ у коефіцієнти ДВП відбувається шляхом зміни їх позицій в такий спосіб:

$$\begin{matrix} якщо\ \ w_j = 1,\ \ то\ \ N(q_i) = N\big(max(q_i, q_{i+1}, q_{i+2}, q_{i+3}, q_{i+4})\big), \\ якщо\ \ w_j = 0,\ \ то\ \ N(q_i) = N(min(q_i, q_{i+1}, q_{i+2}, q_{i+3}, q_{i+4}), \end{matrix} \quad (2.10)$$

де w_j – біт ЦВЗ, q_i – коефіцієнт ДВП, N – індекс коефіцієнта ДВП.

При цьому в процесі вбудовування беруть участь лише середньочастотні (HL та LH) коефіцієнти всіх рівнів розкладання.

Для відновлення цифрового водяного знака не потрібне первинне зображення-контйнер. Перед відновленням до зображення використовується 4-рівневе вейвлет-перетворення. Значення біта ЦВЗ визначається наступним чином:

$$\begin{matrix} якщо\ \ q_i^{'} > median\big(q_i^{'}, q_{i+1}^{'}, q_{i+2}^{'}, q_{i+3}^{'}, q_{i+4}^{'}\big),\ \ то\ \ w_j^{'} = 1, \\ якщо\ \ q_i^{'} < median\big(q_i^{'}, q_{i+1}^{'}, q_{i+2}^{'}, q_{i+3}^{'}, q_{i+4}^{'}\big),\ \ то\ \ w_j^{'} = 0, \end{matrix} \quad (2.11)$$

де $w_j^{'}$ – біт відновлюваного ЦВЗ, $q_i^{'}$ – коефіцієнт ДВП.

Автор алгоритму вказує на стійкість запропонованої схеми до шумів та втрати частини контейнера. У той же час метод нестійкий до застосування афінних перетворень та медіанних фільтрів.

Ще однією серйозною проблемою є необхідність проводити 4-рівневе пряме та зворотне ДВП, як при вбудовуванні ЦВЗ, так і при його відновленні.

2.4.3 Алгоритм Сінха (Sinha)

В [33] запропоновано алгоритм, заснований на застосуванні дискретного вейвлет-перетворення та методу головних компонентів (PCA), що застосовується для статичних зображень та відео-файлів.

Відомо, що після декомпозиції спостерігається кореляція між сусідніми коефіцієнтами ДВП, що спрощує аналіз контейнера та пошук ЦВЗ.

Ортогональне перетворення PCA – це математична процедура, яка на вході має набір корелюваних значень, а на виході видає набір некорельованих значень. Отже, задача відновлення ЦВЗ зловмисником ускладнюється.

Процес вбудовування ЦВЗ за алгоритмом Сінха:

1) цифровий водяний знак, що представляє собою чорно-біле зображення, перетворюється на вектор бітів;

2) зображення-контейнер конвертується у колірну схему YUV (яскравість, синя компонента, червона компонента);

3) до компоненту яскравості кожного кадру застосовується 1-рівневе вейвлет-перетворення;

4) блок низькочастотних (LL) коефіцієнтів розбивається на кількість підблоків, що дорівнює розміру ЦВЗ;

5) над усіма отриманими підблоками проводиться ортогональне перетворення PCA, в результаті отримують набір некорельованих значень (кожне значення відповідає одному підблоку);

6) вбудовування відбувається шляхом зміни значень, отриманих на попередньому кроці за формулою:

$$S_i^{'} = S_i + \alpha w_i, \tag{2.12}$$

де S_i – значення до вбудовування, $S_i^{'}$ – значення після вбудовування, w_i – значення біта ЦВЗ, α – ваговий коефіцієнт;

7) застосовується зворотне перетворення PCA до низькочастотних коефіцієнтів ДВП;

8) здійснюється зворотне ДВП і відбувається перехід до колірної схеми RGB.

Після вбудовування та відправлення каналом зв'язку, одержувач здійснює відновлення ЦВЗ за алгоритмом:

1) здійснюється перехід зображення до колірної схеми YUV;

2) проводиться 1-рівневе вейвлет-перетворення компонентів яскравості кожного кадру;

3) блок низькочастотних коефіцієнтів розбивається на підблоки;

4) до кожного підблоку застосовується PCA;

5) значення біта ЦВЗ визначається за формулою:

$$w_i^{'} = \frac{S_i^{'} - S_i}{\alpha}, \tag{2.13}$$

де $w_i^{'}$ – відновлене значення біта ЦВЗ.

Автор відмічає задовільну стійкість алгоритму до шумів та геометричних перетворень. Метод використовує 1-рівневе вейвлет-перетворення, що значно збільшує швидкість його роботи порівняно з алгоритмом Санхаві.

До недоліків алгоритму можна віднести візуальну помітність вбудовування в низькочастотну компоненту, необхідність наявності первинного зображення в декодері.

2.4.3 Алгоритм Хонга (Hong)

Алгоритм [34] здійснює генерування ЦВЗ на основі значень вейвлет-коефіцієнтів первинного зображення та їх вбудовування шляхом зміни значень середньочастотних коефіцієнтів другого рівня вейвлет-розкладання. Метод має один параметр – ваговий коефіцієнт водяного знаку α.

Процедура вбудовування ЦВЗ складається з 4 етапів:

1) дворівневе вейвлет-розкладання зображення-контейнера;

2) для визначення коефіцієнтів, в які проводитиметься вбудовування, генерується псевдовипадкова послідовність неповторних індексів;

3) для деякої околиці кожного обраного коефіцієнта обчислюється середнє значення:

$$m_{i,j} = mean\left(q_{i,j-1}, q_{i-1,j}, q_{i+1,j}, q_{i,j+1}\right); \tag{2.14}$$

4) генерування та вбудовування ЦВЗ відбувається виходячи із середніх значень, отриманих на попередньому етапі:

$$\begin{aligned} &\text{якщо } \mathrm{q}_{i,j} > m_{i,j}, \text{ то } \mathrm{q}'_{i,j} = \mathrm{q}_{i,j} \cdot (1+\alpha), \ w_k = 1, \\ &\text{якщо } \mathrm{q}_{i,j} < \mathrm{m}_{i,j}, \text{ то } \mathrm{q}'_{i,j} = \mathrm{q}_{i,j} \cdot (1-\alpha), \ w_k = 0; \end{aligned} \tag{2.15}$$

5) проводиться зворотне ДВП.

Процес відновлення ЦВЗ практично збігається з вбудовуванням: також проводиться 2-рівневе ДВП, обчислюються середні значення і на їх основі визначаються значення бітів ЦВЗ.

В даному алгоритмі значення бітів ЦВЗ залежить від статистики контейнера, що робить його схожим з алгоритмами цифрового підпису зображень з урахуванням обчислення хеш-функций. У той же час, на відміну від цифрового підпису, вбудовування ЦВЗ призводить до невеликої зміни контейнера, що робить цей алгоритм більш стійким до атак.

2.4.4 Алгоритм Пунам-Арора (Poonam-Arora)

Алгоритм Пунам-Арора [35] заснований на використанні комбінації ДВП та дуже популярного в останній час методу сингулярного розкладання матриці (Singular Value Decomposition, SVD).

По-перше, метод SVD [36] є одним з найбільш ефективних методів стиснення зображень.

Матриця зображення $A(m \times n)$ розкладається на три матриці $A = U \times S \times V^T$, де S – сингулярна матриця, тобто діагональна матриця, на головній діагоналі якої розташовані корені з власних значень матриці A^T. Матриці U та V є ортогональними. В матриці Σ виділяються перші r рядків і стовпців, а ті, що залишилися, замінюються нулями. Перші r сингулярних чисел називають головними компонентами. Використовуючи r головних компонент можна реконструювати первинну матрицю з використанням меншого обсягу вхідної інформації:

$$A(m \times n) = U(m \times r)S(r \times r)V^T(r \times n).$$

По-друге, сингулярні числа мають високу стабільність щодо незначних спотворень зображення.

В роботі [35] запропоновано наступний метод вбудовування ЦВЗ.

1. Зображення-контейнер та зображення-ЦВЗ піддаються 4-рівневому та 3-рівневому ДВП відповідно.

2. Для зображення-контейнеру та зображення-ЦВЗ виділяються області низькочастотних вейвлет-коефіцієнтів ДВП (див. рис. 2.16):

$$host\ image\ \rightarrow DWT(LL3) = [LL4, LH4, HL4, HH4], \tag{2.16}$$

$$watermark\ image \rightarrow DWT(LL2) = [LL3, LH3, HL3, HH3]. \tag{2.17}$$

3. Застосовується метод сингулярного розкладання:

$$host\ image\ \rightarrow \begin{cases} SVD(LL4) = U_{h1} \times\ S_{h1} \times V_{h1}^T \\ SVD(S_{h1}) = U_{h2} \times\ S_{h2} \times V_{h2}^T \end{cases}, \tag{2.18}$$

$$host\ image\ \rightarrow \begin{cases} SVD(HH4) = U_{h3} \times\ S_{h3} \times V_{h3}^T \\ SVD(S_{h3}) = U_{h4} \times S_{h4} \times V_{h4}^T \end{cases}, \tag{2.19}$$

$$watermark\ image\ \rightarrow \begin{cases} SVD(LL3) = U_{w1} \times S_{w1} \times V_{w1}^T \\ SVD(S_{w1}) = U_{w2} \times\ S_{w2} \times V_{w2}^T \end{cases}, \tag{2.20}$$

$$watermark\ image\ \rightarrow \begin{cases} SVD(HH3) = U_{w3} \times\ S_{w3} \times V_{w3}^T \\ SVD(S_{w3}) = U_{w4} \times\ S_{w4} \times V_{w4}^T \end{cases}. \tag{2.21}$$

4. Формування нових векторів сингулярних чисел:

$$host\ image\ \rightarrow \begin{cases} S_h^{LL4} = S_{h1} + S_{h2} \\ S_h^{HH4} = S_{h3} + S_{h4} \end{cases}, \tag{2.22}$$

$$watermark\ image\ \rightarrow \begin{cases} S_w^{LL3} = S_{w1} + S_{w2} \\ S_w^{HH3} = S_{w3} + S_{w4} \end{cases}. \tag{2.23}$$

5. Вбудовування ЦВЗ до зображення-контейнеру:

$$S_{hw}^{LL4} = S_h^{LL4} + \alpha S_w^{LL3}, \tag{2.24}$$

$$S_{hw}^{HH4} = S_h^{HH4} + \alpha S_w^{HH3}, \tag{2.25}$$

де α – ваговий коефіцієнт.

6. Застосування оберненого сингулярного розкладання:

$$MI^{LL4} = U_{h1} \times S_{hw}^{LL4} \times V_{h1}^T, \tag{2.26}$$

$$MI^{HH4} = U_{h3} \times S_{hw}^{HH4} \times V_{h3}^T. \tag{2.27}$$

7. Застосування обернених ДВП для формування зображення з вбудованим ЦВЗ.

Процес відновлення ЦВЗ.

1. Зображення-контейнер та стегозображення піддаються 4-рівневому ДВП, в результаті чого виділяються області низькочастотних вейвлет-коефіцієнтів.

2. Застосовується метод сингулярного розкладання:

$$marked\ image\ \rightarrow \begin{cases} SVD(LL4) = U_{MI1} \times\ S_{MI1} \times V_{MI1}^{T} \\ SVD(S_{MI1}) = U_{MI2} \times\ S_{MI2} \times V_{MI2}^{T} \end{cases}, \tag{2.28}$$

$$marked\ image\ \rightarrow \begin{cases} SVD(HH4) = U_{MI3} \times\ S_{MI3} \times V_{MI3}^{T} \\ SVD(S_{h3}) = U_{MI4} \times S_{MI4} \times V_{MI4}^{T} \end{cases}, \tag{2.29}$$

$$host\ image\ \rightarrow \begin{cases} SVD(LL4) = U_{h1} \times S_{h1} \times V_{h1}^{T} \\ SVD(S_{h1}) = U_{h2} \times\ S_{h2} \times V_{h2}^{T} \end{cases}, \tag{2.30}$$

$$host\ image\ \rightarrow \begin{cases} SVD(HH4) = U_{h3} \times\ S_{h3} \times V_{h3}^{T} \\ SVD(S_{w3}) = U_{h4} \times\ S_{h4} \times V_{h4}^{T} \end{cases}. \tag{2.31}$$

3. Формування нових векторів сингулярних чисел:

$$marked\ \ image\ \rightarrow \begin{cases} S_{MI}^{LL4} = S_{MI1} + S_{MI2} \\ S_{MI}^{HH4} = S_{MI3} + S_{MI4} \end{cases}, \tag{2.32}$$

$$host\ image\ \rightarrow \begin{cases} S_{h}^{LL4} = S_{h1} + S_{h2} \\ S_{h}^{HH4} = S_{h3} + S_{h4} \end{cases}. \tag{2.33}$$

4. Відновлення векторів сингулярних чисел ЦВЗ зі стегозображення:

$$S_{w}^{LL3} = \frac{(S_{MI}^{LL4} - S_{h}^{LL4})}{\alpha}, \tag{2.34}$$

$$S_{w}^{HH3} = \frac{(S_{MI}^{HH4} - S_{h}^{HH4})}{\alpha}, \tag{2.35}$$

$$S_{w1} = S_{w}^{LL3} - S_{w2}, \tag{2.36}$$

$$S_{w3} = S_{w}^{HH3} - S_{w4}, \tag{2.37}$$

$$SVD(LL3) = U_{w1} \times S_{w1} \times V_{w1}^{T}, \tag{2.38}$$

$$SVD(HH3) = U_{w3} \times S_{w3} \times V_{w3}^{T}. \tag{2.39}$$

5. Застосування обернених ДВП для відновлення ЦВЗ.

2.4.5 Алгоритм Патідара (Patidar)

Розглянуті вище методи вбудовування ЦВЗ або мають велику ємність, але вузькоспрямовану стійкість тільки до одного класу спотворень, або є стійкими до багатьох видів спотворень, але не дозволяють вбудувати достатній обсяг даних.

Серед основних видів спотворень, крім JPEG-стиснення (див. розділ 2.2), також виділяють зміну яскравості та контрастності. Останні можуть використовуватися для покращення візуального сприйняття змісту зображення без порушення його цілісності. Популярним прикладом є системи електронного документообігу, де користувач може коригувати від скановане зображення перед його відправкою.

Під зміною яскравості зображення розуміють наступну лінійну операцію:

$$\hat{X} = x(1 + b),$$

де $\hat{X}$ – матриця значень яскравості пікселів після зміни яскравості зображення; b – параметр зміни яскравості.

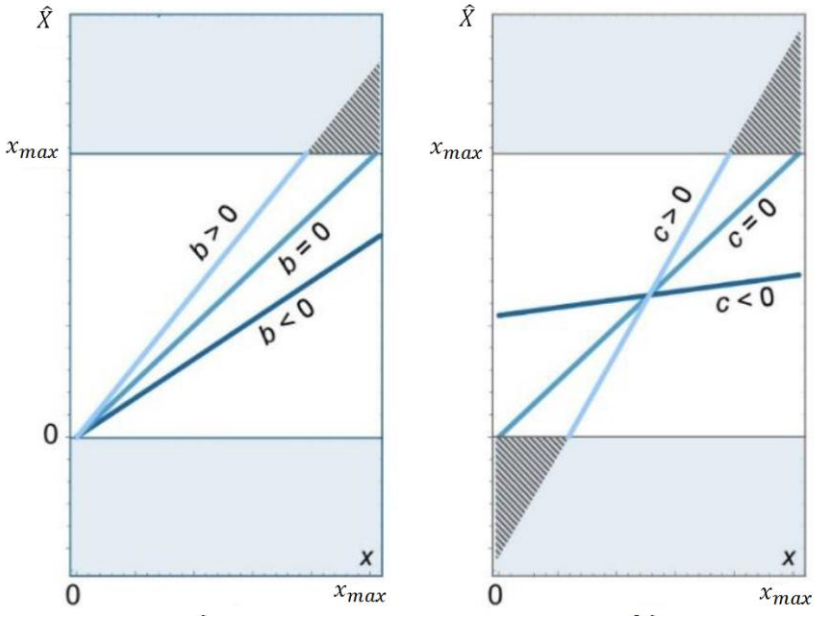
В реальних зображеннях існують обмеження на мінімальне та максимальне можливе значення яскравості одного пікселю. Для 8-бітного цифрового зображення вони дорівнюють $x_{min} = 0$ і $x_{max} = 255$ відповідно. Тому, незважаючи на те, що операція зміни яскравості є лінійною операцією, після її застосування можливе обрізання гістограми зображення ліворуч або праворуч. На рис. 2.18, а) заштрихованими областями показано ділянки гістограми зображення після застосування операції зміни яскравості параметром b, що виходять за межі динамічного діапазону зображення.

Мета зміни контрастності, на відміну зміни яскравості, у тому, щоб зробити світлі ділянки зображення більш-менш відмінними від темних. Тому така операція може мати різноспрямований ефект на значення яскравості пікселів:

$$\hat{X} = (1 + c)\left(x - \frac{x_{max}}{2}\right) + \frac{x_{max}}{2},$$

де $\hat{X}$ – матриця значень яскравості пікселів після зміни контрастності зображення; c – параметр зміни контрастності. На рис. 2.18, б) заштрихованими областями показано ділянки гістограми зображення після застосування операції зміни контрастності з параметром c, що виходять за межі динамічного діапазону зображення.

У випадку, якщо відбулося обрізання гістограми ліворуч або праворуч, то частина даних ЦВЗ, вкладена в ці ділянки, може бути безповоротно втрачена. Тому неможливо створити метод вкладення, який був би стійкий до операцій зміни яскравості або контрастності для будь-яких значень параметрів b і c – тільки для деякого невеликого діапазону. Дане обмеження існує і для стиснення JPEG. Успішне відновлення ЦВЗ можливе лише при невеликих спотвореннях, які виникають за деяких допустимих межах параметра стиснення.



а б

Рисунок 2.18 – Результат застосування операцій зміни яскравості (а) та контрастності (b) на вихідні значення пікселів $\hat{X}$ за вхідними значеннями x

В роботі [37] запропоновано наступний метод вбудовування ЦВЗ.

1. Кожен біт m_i даних ЦВЗ вбудовується в коефіцієнт s_i області LH3 (див. рис. 2.16) 3-рівневого ДВП за правилом:

$$\hat{s}_i = \begin{cases} \gamma\left(\left[\frac{s_i}{\gamma}\right] + \frac{1}{4}\right), & \text{якщо } \ m_i = 1, \\ \gamma\left(\left[\frac{s_i}{\gamma}\right] - \frac{1}{4}\right), & \text{якщо } \ m_i = 0, \end{cases} \tag{2.40}$$

де $\hat{s}_i$ – коефіцієнт ДВП після вбудовування біта m_i; γ – параметр «глибини вбудовування», $[x]$ – найближче ціле значення числа x.

Використання ДВП, як і ДКП, дозволяє досягти значної стійкості ЦВЗ до стиску JPEG.

2. Зображення з вбудованим ЦВЗ піддається процедурі вирівнювання гістограми. Мета – покращення якості зображень шляхом приведення гістограму зображення до рівномірного розподілу. Приклад результату застосування операції вирівнювання гістограми наведено на рис. 2.19.

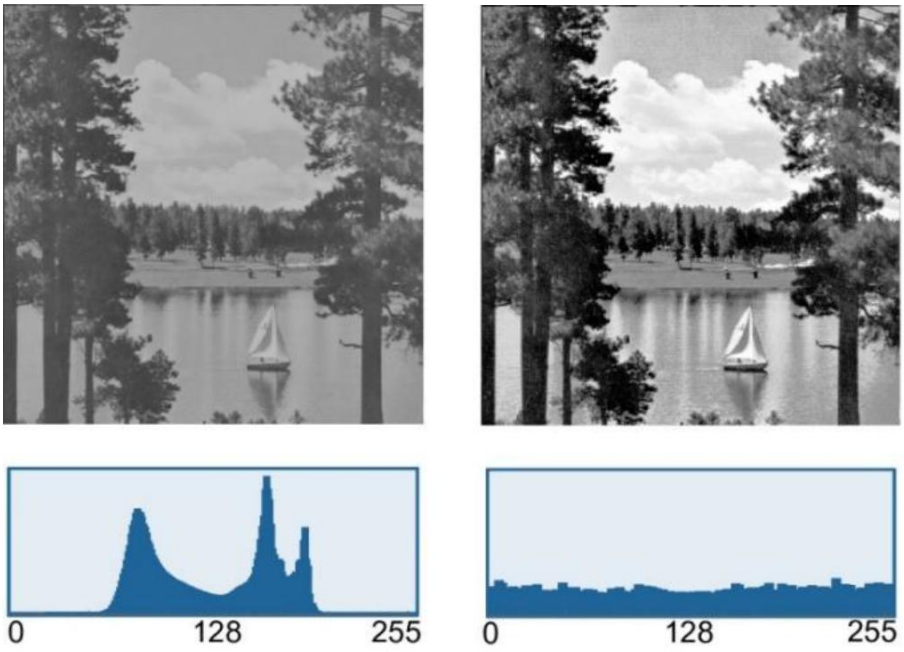


Рисунок 2.19 – Зображення та гістограма до (ліворуч) та після (праворуч) застосування операції вирівнювання гістограми зображення

3. Виконується вторинне вбудовування бітів ЦВЗ за формулою (2.40). При цьому вбудовуються ті ж самі біти ЦВЗ, що і на першому кроці, але в область HL3 (див. рис. 2.16) 3-рівневого ДВП. Отримане зображення з ЦВЗ піддається процедурі відновлення гістограми до її первинної форми до вбудовування.

Таким чином, за рахунок додавання другого етапу досягається стійкість до змін яскравості та контрастності.

Процес відновлення ЦВЗ виконується у зворотному порядку відносно алгоритму вбудовування. Спочатку отримане зображення з можливими спотвореннями копіюється. Після чого одна копія розкладається в області ДВП коефіцієнтів одразу, а друга – після виконання процедури попереднього вирівнювання гістограми. Кожен коефіцієнт з областей LH3 та HL3 3-рівневого ДВП надходить на декодер ЦВЗ, який приймає рішення за наступним алгоритмом:

$$\widehat{m}_i = \begin{cases} 1, \ \text{якщо} \ \ \hat{s}_i - \gamma \left[\frac{\hat{s}_i}{\gamma}\right] \geq 0, \\ 1, \ \text{якщо} \ \ \hat{s}_i - \gamma \left[\frac{\hat{s}_i}{\gamma}\right] < 0, \end{cases} \tag{2.41}$$

де $\widehat{m}_i$ – біт, відновлений з коефіцієнту $\hat{s}_i$.

Після відновлення з областей LH3 та HL3 виконується процедура порівняння отриманих ЦВЗ в завадостійкому декодері та виправлення помилок.

3 ПОРІВНЯЛЬНИЙ АНАЛІЗ АЛГОРИТМІВ ГЕНЕРУВАННЯ ТА ВБУДОВУВАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ У СТАТИЧНІ ЗОБРАЖЕННЯ

3.1. Початкові умови експериментального дослідження.

В якості зображень-контейнерів було обрано зображення 4 поширених форматів представлення графічних даних: JPEG, BMP, PNG та TIFF – див. рис. 3.1 – рис. 3.6. В якості цифрового водяного знаку використовувався набір біт, отриманий з текстового рядка в кодуванні ASCII "Test Watermark Algorithm Message". Довжина рядка – 32 символи, розмір повідомлення – 256 біт. В експериментальному досліджені брали участь 4 розглянутих у попередньому розділі алгоритми вбудовування ЦВЗ у зображення: алгоритм Коха-Жао, алгоритм Сангхаві, алгоритм Пунам-Арора та алгоритм Патідара.

Для алгоритму Коха-Жао параметр вбудовування P дорівнював 16. Для алгоритму Пунам-Арора ваговий коефіцієнт α дорівнював 0.03. Для алгоритму Патідара параметр вбудовування γ дорівнював 0.11. Крок завадостійкого кодування пропускався. Але на етапі відновлення копії ЦВЗ порівнювались між собою і факт неспівпадіння враховувався як додаткова перевага, бо знайдено помилку в ЦВЗ і її можна виправити. Моделювання алгоритму Коха-Жао відбувалось в пакеті Mathcad 15 на основі лістингів програм з підручника [9]. Моделювання алгоритму Сангхаві відбувалось в програмному середовищі Matlab 2021 на основі лістингів програм, наданих автором алгоритму [38]. Моделювання алгоритму Пунам-Арора відбувалось в програмному середовищі Matlab 2021 на основі лістингів програм, наданих автором алгоритму [39]. Моделювання алгоритму Патідара відбувалось в програмному середовищі Matlab 2021 на основі лістингів програм, наданих автором алгоритму [40].

Рисунок 3.1 – Файл Castle.jpg

Рисунок 3.2 – Файл Lemur.jpg

Рисунок 3.3 – Файл Snap.jpg

Рисунок 3.4 – Файл Tiffany.bmp

Рисунок 3.5 – Файл Lego.png

Рисунок 3.7 – Файл Universe.tiff

3.2 Дослідження візуальних спотворень, що виникають під час використання алгоритмів

Створення надійної стеганосистеми потребує наявності інструментів оцінки її стійкості до зовнішніх впливів. Оцінка візуальної стійкості стеганографічної системи є досить складною задачею.

Досить ефективним є метод оцінки рівня схованості виходячи з аналізу статистичних характеристик стегозображення. Статистика дає кількісні критерії ймовірності, які дозволяють створювати детектори, що виявляють статистичні розбіжності між оригінальним контейнером та стегозображенням. Для оцінки якості стеганографічних засобів також використовуються показники, що оперують зображеннями лише на рівні пікселів чи окремих колірних компонент пікселів. Найбільш поширеними показниками при аналізі рівня спотворень, які вносяться у зображення під час приховування в ньому інформації, є співвідношення «сигнал/шум», що обчислюється в децибелах та якість зображення, що вимірюється у відсотках. Серед інших показників можна виділити середню абсолютну різницю значень пікселів, нормовану середню абсолютну різницю значень пікселів та максимальне відношення «сигнал-шум» [41] – табл. 3.1.

Таблиця 3.1 – Найпоширеніші показники візуального спотворення стегозображення S, засновані на аналіз піксельної структури контейнера C

Показник спотворення	Формула для розрахунку
Середня абсолютна різниця (Average Absolute Difference – AD)	$AD = \frac{1}{XY}\sum_{x,y} \lvert C_{x,y} - S_{x,y} \rvert$
Нормована середня абсолютна різниця (Normalized Average Absolute Difference – NAD)	$NAD = \frac{\sum_{x,y} \lvert C_{x,y} - S_{x,y} \rvert}{\sum_{x,y} \lvert C_{x,y} \rvert}$
Відношення сигнал/шум (Signal to Noise Ratio – SNR)	$SNR = \frac{\sum_{x,y}(C_{x,y})^2}{\sum_{x,y}(C_{x,y} - S_{x,y})^2}$
Максимальне значення відношення сигнал/шум (Peak Signal to Noise Ratio – PSNR)	$PSNR = XY\frac{\max\limits_{x,y}(C_{x,y})^2}{\sum_{x,y}(C_{x,y} - S_{x,y})^2}$
Якість зображення (Image Fidelity – IF)	$IF = 1 - \frac{\sum_{x,y}(C_{x,y} - S_{x,y})^2}{\sum_{x,y}(\mathrm{C}_{x,y})^2}$

Таблиця 3.2–Значення параметрів візуального спотворення для зображення Castle.jpeg

Алгоритм/Міра	AD	NAD	SNR	PSNR	IF
Коха-Жао	0.403295	0.004097	43400	148680	99.9977%
Сангхаві	0.615485	0.006252	1663	5696	99.9399%
Пунам-Арора	0.007187	0.000073	860114	2946540	99.9999%
Патідара	0.251603	0.002556	49882	170882	99.998%

Таблиця 3.3 – Показники візуального спотворення зображення Koala.jpeg

Алгоритм/Міра	AD	NAD	SNR	PSNR	IF
Коха-Жао	0.992101	0.009729	13915	64914	99.9928%
Сангхаві	1.42665	0.013991	495.5	2312	99.7982%
Пунам-Арора	0.10544	0.00103	91392	426347	99.9989%
Патідара	0.249512	0.002447	37021	172704	99.9973%

Таблиця 3.4 – Показники візуального спотворення зображення Snap.jpeg

Алгоритм/Міра	AD	NAD	SNR	PSNR	IF
Коха-Жао	1.8437	0.018934	2307.63	10862	99.9567%
Сангхаві	0.291491	0.002993	6633.71	31224.8	99.9849%
Пунам-Арора	0.024596	0.000252	51286.1	241403	99.9981%
Патідара	0.241043	0.002466	36293.8	170835	99.9972%

Таблиця 3.5 – Показники візуального спотворення при вбудовуванні зображення Tiffany.bmp

Алгоритм/Міра	AD	NAD	SNR	PSNR	IF
Коха-Жао	18.204	0.172697	35.89	148.1	97.2138%
Сангхаві	0.472923	0.004486	1743	7190	99.9426%
Пунам-Арора	0.244946	0.002324	33886	139797	99.997%
Патідара	0.29617	0.00281	32371	133549	99.9969%

Таблиця 3.6 – Показники візуального спотворення для зображення Lego.png

Алгоритм/Міра	AD	NAD	SNR	PSNR	IF
Коха-Жао	27.031	0.282674	12.4877	50.7181	91.9921%
Сангхаві	0.960529	0.010045	941.223	3822.74	99.8938%
Пунам-Арора	0.013367	0.00014	119835	486704	99.9992%
Патідара	0.24809	0.002594	25945.3	105376	99.9961%

Таблиця 3.7 – Показники візуального спотворення для зображення Universe.tiff

Алгоритм/Міра	AD	NAD	SNR	PSNR	IF
Коха-Жао	2.00351	0.033614	114.05	991.257	99.1232%
Сангхаві	0.394585	0.00662	1371.43	11919.6	99.9271%
Пунам-Арора	0.22379	0.00375	27215.2	236539	99.9963%
Патідара	0.24749	0.004152	20003.2	173856	99.995%

Узагальнені результати проведеного дослідження візуальних спотворень, що виникають під час використання алгоритмів Коха-Жао, Сангхаві, Пунам-Арора та Патідара наведено в табл. 3.8. Кращий показник з табл. 3.2 – табл. 3.7 оцінювався в 4 бали, другий результат –3 бали, третій –2 бали, четвертий – 1 бал. Якщо алгоритм вносив занадто серйозні спотворення або декодер був не здатний коректно відновити ЦВЗ – 0 балів.

Таблиця 3.8 – Результати дослідження стійкості до візуальних спотворень

Зображення / Алгоритм	Коха-Жао	Сангхаві	Пунам-Арора	Патідара
Castle	2	1	3	4
Lemur	2	1	3	4
Snap	1	2	3	4
Tiffany	1	2	4	3
Lego	1	2	3	4
Milky Way	0	0	3	4
Підсумок	7	8	22	27

Алгоритм Патідара за рахунок використання двох ДВП дозволив звести спотворення при вбудовуванні ЦВЗ до мінімуму та уникнути виникнення артефактів у всіх випадках. Якість зображення для всіх стегосистем близько 100%. Дуже близькі оцінки отримав алгорим Пунам-Арора. Особливо помітна перевага використання цього алгоритму при порівнянні його результатів з результатами алгоритмів Сангхаві та Коха-Жао. Використання даного алгоритму рекомендовано за необхідності приховати факту вбудовування ЦВЗ, що вкрай важливо для систем цифрових водяних знаків.

Використання алгоритму Сангхаві у більшості випадків призвело до виникнення артефактів, а в деяких випадках і до невірної детекції ЦВЗ. Певною мірою це пов'язані з перестановками коефіцієнтів ДВП, що знаходяться на краях зображення. Відмова від зміни позицій таких коефіцієнтів може призвести до збереження прийнятної якості зображення.

Алгоритм Коха-Жао показав прийнятні показники у експериментах з контейнерами формату JPEG, але викликав серйозні спотворення при вбудовуванні ЦВЗ у зображення інших форматів. Ця обставина пов'язана з використанням у ньому ДКП, яке застосовується лише при стисканні JPEG.

3.3 Дослідження стійкості алгоритмів до різних видів атак

Атаки на системи вбудовування ЦВЗ можуть бути поділені на чотири групи [42].

1. Атаки проти вбудованого повідомлення – спрямовані на видалення або псування ЦВЗ шляхом маніпулювання стегозображенням. Методи атак, що входять до цієї категорії, не намагаються оцінити і виділити водяний знак. Прикладами таких атак можуть бути лінійна фільтрація, стиснення зображень, додавання шуму, вирівнювання гістограми, зміна контрастності тощо.

2. Атаки проти стегодетектора спрямовані на те, щоб ускладнити або унеможливити правильну роботу детектора. При цьому водяний знак в зо-

браженні залишається, але втрачається можливість його відновлення.

3. Атаки проти протоколу використання ЦВЗ переважно пов'язані зі створенням помилкових ЦВЗ, хибних стегозображень, інверсією ЦВЗ, додаванням кількох ЦВЗ.

4. Атаки проти ЦВЗ спрямовані на оцінювання і відновлення ЦВЗ зі стегозображення, бажано без спотворення контейнеру. До цієї групи входять такі атаки, як атаки змови, статистичного усереднення, методи очищення сигналів від шумів, деякі види нелінійної фільтрації та інші.

В експериментальних дослідженнях використовувались наступні типи атак: поворот контейнера-зображення на 90 градусів (поворот камери часто зустрічається при фотозйомці), стиснення в 2 рази (адресату не відомий первинний розмір зображення), збільшення контрастності, збільшення та зменшення яскравості, обрізання зображення, стиснення JPEG з різними показниками якості.

Таблиця 3.9 – Стійкість стегосистеми з контейнером Lemur.jpg

Атака / Алгоритм	Коха-Жао	Сангхаві	Пунам-Арора	Патідара
Масштабування	-	-	-	-
Поворот	+	-	-	-
Контрастність	+	-	-	+
Підвищення яскравості	+	-	+	+
Зниження яскравості	+	-	-	+
Видалення частини зображення	+	+	+	+
Стиснення JPEG з коефіцієнтом якості 0.7	+	-	-	+
Стиснення JPEG з коефіцієнтом якості 0.5	+	-	-	-

Таблиця 3.10 – Стійкість стегосистеми з контейнером Snap.jpg

Атака / Алгоритм	Коха-Жао	Сангхаві	Пунам-Арора	Патідара
Масштабування	-	-	-	-
Поворот	+	-	-	-
Контрастність	+	-	+	+
Підвищення яскравості	+	-	+	+
Зниження яскравості	+	-	+	+
Видалення частини зображення	+	+	+	+
Стиснення JPEG з коефіцієнтом якості 0.7	+	-	-	+
Стиснення JPEG з коефіцієнтом якості 0.5	+	-	-	-

Таблиця 3.11 – Стійкість стегосистеми з контейнером Tiffany.bmp

Атака / Алгоритм	Коха-Жао	Сангхаві	Пунам-Арора	Патідара
Масштабування	-	-	-	-
Поворот	+	-	-	-
Контрастність	+	-	-	+
Підвищення яскравості	+	-	-	+
Зниження яскравості	+	-	-	+
Видалення частини зображення	+	-	+	+
Стиснення JPEG з коефіцієнтом якості 0.7	+	-	-	+
Стиснення JPEG з коефіцієнтом якості 0.5	+	-	-	-

Таблиця 3.12 – Стійкість стегосистеми з контейнером Lego.png

Атака / Алгоритм	Коха-Жао	Сангхаві	Пунам-Арора	Патідара
Масштабування	-	-	-	-
Поворот	+	-	-	-
Контрастність	+	-	+	+
Підвищення яскравості	+	-	+	+
Зниження яскравості	+	-	-	+
Видалення частини зображення	+	+	+	+
Стиснення JPEG з коефіцієнтом якості 0.7	+	-	-	+
Стиснення JPEG з коефіцієнтом якості 0.5	+	-	-	-

Таблиця 3.13 – Стійкість стегосистеми з контейнером Universe.tiff

Атака / Алгоритм	Коха-Жао	Сангхаві	Пунам-Арора	Патідара
Масштабування	-	-	-	-
Поворот	+	-	-	-
Контрастність	+	+	+	+
Підвищення яскравості	+	-	+	+
Зниження яскравості	+	-	+	+
Видалення частини зображення	+	+	+	+
Стиснення JPEG з коефіцієнтом якості 0.7	+	-	-	+
Стиснення JPEG з коефіцієнтом якості 0.5	+	-	-	-

Проведені експерименти показали, що використання дискретного косинусного перетворення дозволяє створювати стійкі алгоритми генерування і вбудовування цифрових водяних знаків у зображення. Алгоритм Коха-Жао, що використовує вбудовування в коефіцієнти ДКП, виявився стійким до всіх розглянутих атак, крім масштабування. Це пов’язано з широким використанням ДКП в технологіях обробки зображень. Однак візуальні спотворення, що виникають, і помилки в декодуванні ЦВЗ серйозно ускладнюють використання таких стеганосистем і не дозволяють їм бути універсальним засобом для використання в системах ЦВЗ.

Алгоритми, що використовують дискретне вейвлет-перетворення, не забезпечують високої стійкості до атак (особливо геометричних та стиснення JPEG).

Як видно з результатів експериментів, алгоритм Сангхаві є най нестійкішим. При непарній розмірності зображення виникають спотворення ЦВЗ та помилки у роботі декодера. Показники стійкості значно варіюються для різних зображень. Максимального показника було досягнуто при вбудовуванні ЦВЗ у зображення Universe – ЦВЗ виявився стійким до зміни яскравості (як освітлення, так і затемнення) і контрастності (при цьому в зображенні виникли артефакти і неправильно спрацював декодер).

Стійкість ЦВЗ, вбудованого за допомогою алгоритму Пунам-Арора, не

залежить від властивостей зображення. При цьому ЦВЗ стійкий до половини з дослідних атак.

Алгоритм Патідара також не залежить від формату та властивостей зображення, як і алгоритм Пунам-Арора. Але на відміну від останнього даний алгоритм також стійкий до збільшення яскравості (засвічування зображення) і накладання контрастних фільтрів. Подібні завади також поширені в каналах передачі мережі. Пропонований алгоритм може успішно зарекомендувати себе при побудові систем із напівкрихткими ЦВЗ в мережі, де виникають спотворення значень пікселів контейнера.

За результатами експериментів встановлено, що найскладнішою атакою для дослідних алгоритмів вбудовування ЦВЗ є атака масштабування. Вирішенням цієї проблеми може бути перевірка розмірності зображення. Для цього можна рекомендувати супроводжувати зображення даними про його розміри.

3.4 Дослідження пропускної здатності алгоритмів

До найважливіших якісних характеристик стеганографічних систем відносять пропускну здатність – кількість бітів прихованого повідомлення, що можуть бути передані за допомогою вказаного алгоритму в зображенні розміру $M \times N$ [43].

Під прихованою пропускною здатністю розуміють максимальну кількість інформації, яка може бути вбудована в контейнер, при цьому повідомлення, що приховуються, повинні бути безпомилково передані адресату і захищені від атак зловмисника.

В результаті експериментальних досліджень було отримано оцінки нормованої прихованої пропускної здатності дослідних алгоритмів, як максимальної кількості бітів, яку можна вбудувати в зображення-контейнер без суттєвих втрат в якості зображення (візуальної непомітності) при збереженні стійкості алгоритму до атак.

В якості тестових контейнерів було обрано зображення Castle.jpg, Tiffany.bmp, Lego.png та Universe.tiff.

Таблиця 3.14 – Прихована пропускна здатність дослідних алгоритмів вбудовування ЦВЗ

Алгоритм	Контейнер Castle.jpg	Контейнер Tiffany.bmp	Контейнер Lego.png	Контейнер Universe.tiff
Коха-Жао	0.446	1	1	0.563
Сангхаві	0.203	0.212	0.323	0.117
Пунам-Арора	0.308	0.287	0.395	1
Патідара	1	1	1	0.401

В результаті випробувань добре зарекомендував себе метод Патідара. Для всіх зображень (крім Universe) стегосистеми можна вбудувати стійкий до застосування яскравого та контрастного фільтрів ЦВЗ досить великого обсягу. Прихована пропускна здатність для трьох з чотирьох тестових зображень виявилася вищою, ніж у алгоритмів Коха-Жао та Пунам-Арора, і у всіх випадках значно перевищувала аналогічні показники алгоритму Сангхаві.

Метод Коха-Жао у двох з чотирьох випадків показав результати, тотожні результатам алгоритму Патідара. Серйозним обмежуючим фактором його застосування є спотворення, що вносяться при вбудовуванні ЦВЗ (для зображень не стиснутих в JPEG). У випадку наявності у зловмисника незаповненого контейнеру та засобів аналізу зображень (графічні редактори) від застосування даного алгоритму рекомендовано відмовитись. За відсутності зловмисних дій та грамотного обмеження доступу до зображення-контейнеру, цей алгоритм може застосовуватись у стегосистемах.

Алгоритм Пунам-Арора дозволяє непомітно вбудовувати стійкі ЦВЗ невеликого розміру. Даний алгоритм є оптимальним для вбудовування ЦВЗ у зображення з однотонним тлом та наявністю безлічі яскравих об'єктів. Зокрема, стегосистема з контейнером Universe і ЦВЗ, вбудованим за допомогою даного методу, показала приховану пропускну спроможність, що у кілька ра-

зів перевищує аналогічний показник при застосуванні інших алгоритмів.

Алгоритм Сангхаві на практиці продемонстрував низькі показники прихованої пропускної здатності. Вбудовування бітів ЦВЗ у коефіцієнти першого рівня вейвлет-розкладання неефективне через відсутність стійкості до застосування фільтрів. Вбудовування бітів повідомлення в коефіцієнти четвертого рівня також неможливе внаслідок низької кількості коефіцієнтів областей (див. рис. 2.16) даного рівня розкладання і виникненням артефактів. Вбудовування у коефіцієнти другого та третього рівня найбільш доцільно. Але й у цьому випадку вибір рівня та області вбудовування (див. рис. 2.16) індивідуальний для кожного зображення, а успішний результат не гарантований.

ВИСНОВКИ

1. Розглянуто способи застосування комп'ютерної стеганографії до створення ЦВЗ. Зазначено, що використання ЦВЗ для підтвердження автентичності цифрових документів в наш час набувають все більшої популярності.

2. Докладно розглянуто основні алгоритми створення ЦВЗ для файлів-зображень. Зазначено, що основною проблемою при реалізації технологій створення ЦВЗ є збереження якості маркованих при вбудовуванні ЦВЗ файлів при їх використанні за основним призначенням у поєднанні з достовірністю подальшого відновлення ЦВЗ.

3. Проведено експериментальні дослідження чотирьох алгоритмів вбудовування ЦВЗ, що базуються на дискретних перетвореннях. В якості критерії при порівнянні було обрано: візуальну непомітність вбудовування, приховану пропускна здатність, стійкість до спотворень.

Результати експериментів показали, що алгоритми, засновані на дискретному косинусному перетворенні (зокрема, найпопулярніший у цій групі алгоритм Коха-Жао), мають дуже високу стійкість до атак, але візуальна непомітність роботи алгоритму недостатня. Крім того, даний алгоритм показав низькі результати за обраними критеріями у випадку вбудовування в нестиснуті зображення.

Більш кращі показники мали алгоритми, побудовані на застосуванні дискретного вейвлет-перетворення. Загальним недоліком цієї групи методів є порівняно низька стійкість до атак (алгоритм Сангхаві). Головною ж перевагою є висока прихована пропускна здатність та непомітність вбудованого ЦВЗ.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

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

2. Вовк О.О. Методи підвищення стійкості та пропускної здатності систем прихованої передачі інформації: дис. канд. техн. наук: 05.12.02 / Вовк Олеся Олегівна; Харків. нац. ун-т радіоелектроніки. – Харків, 2016. –177 с.

3. Ахмаметьєва Г.В. Підвищення ефективності стеганоаналізу для цифрових зображень і відео: дис. канд. техн. наук: 05.13.21 / Ахмаметьєва Ганна Валеріївна; Одеський національний політехнічний університет. – Одеса, 2017. –162 с.

4. Браіловський М.М. Технології захисту інформації: підручник / М.М. Браіловський, С.В. Зибін, І.В. Пискун, В.О. Хорошко, Ю.Є. Хохлачова. – К.: ЦК “Компринт”, 2021. – 296 с.

5. Золотар О.О. Інформаційна безпека людини: теорія і практика: монографія / О.О. Золотар; Науково-дослідний ін-т інформатики і права Нац. академії правових наук України. – Київ : АртЕк, 2018. – 446 с.

6. Проєктування комплексних систем захисту інформації: підручник / [В.О. Хорошко, І.М. Павлов, Ю.Я. Бобало та ін.]; М-во освіти і науки України, Нац. ун-т «Львів. політехніка». – Львів : Вид-во Львів. політехніки, 2020. – 320 с.: іл.

7. Запоточний В.Й. Технології захисту цінних паперів: навч. посіб. / В.Й. Запоточний; М-во освіти і науки України, Нац. ун-т «Львів. політехніка». – 2-ге вид., допов. – Львів : Вид-во Львів. політехніки, 2013. – 152 с.: іл.

8. Забезпечення інформаційної безпеки держави: навч. посіб. / В.Б. Дудикевич, І.Р. Опірський, П.І. Гаранюк та ін.; М-во освіти і науки України, Нац. ун-т «Львів. політехніка». – Львів : Вид-во Львів. політехніки, 2017. – 204 с.: іл., табл.

9. Г.Ф. Конахович. Комп’ютерна стеганографічна обробка і аналіз му-

льтимедійних даних: підручник. К.: «Центр учбової літератури», 2018. 558 с.

10. O'Ruanaidh, J.K. Rotation, scale, and translation invariant digital image watermarking / J.K. O'Ruanaidh, T. Pun // Proceedings of ICIP. –1997. – Vol. 1. – P. 536-539.

11. O'Ruanaidh, J.K. Rotation, scale, and translation invariant spread spectrum digital image watermarking / J.K. O'Ruanaidh, T. Pun // Signal Processing. –1998. – Vol. 66. – P. 303-317.

12. Mohammad, A.M.F. and N.M. Asad, 2006. An optimization approach for selecting blocks of embedding process in robust watermarking system. J. Comput. Sci., 2: 114-117.

13. Pereira, S. Robust template matching for affine resistant image watermarks / S. Pereira, T. Pun // IEEE Trans. on Image Processing. – 2000. – Vol. 9. – P. 1123-1129.

14. Pereira, S. Template based recovery of Fourier-based watermarks using log-polar and log-log map / S. Pereira, J.K. O'Ruanaidh, F. Deguillaume, G. Csurka, T. Pun //Proceedings of ICMCS. – 1999. – P. 870-874.

15. S.S. Sharma and V. Chandrasekaran, "A robust hybrid digital watermarking technique against a powerful CNN-based adversarial attack," Multimedia Tools Appl., vol. 79, nos. 43–44, pp. 32769–32790, Nov. 2020.

16. Kandi, H.; Mishra, D.; Gorthi, S.R.S. Exploring the learning capabilities of convolutional neural networks for robust image watermarking. Comput. Secur. 2017, 65, 247–268

17. Pao-Ta, Yu Digital watermarking based on neural networks for color images / Pao-Ta Yu, Hung-Hsu Tsai, Jyh-Shyan Lin // Signal Processing. – 2001. – Vol. 81. – Issue 3. – P. 663-671.

18. Chen, J. Digital Watermarking Based on Neural Network Technology for Grayscale Images / J. Chen, Tung-Shou Chen, Keh-Jian Ma, Pin-Hsin Wang // Encyclopedia of Multimedia Technology and Networking . – 2005. – Vol. 29. - P. 204-212.

19. Chang, C.C. A technique for computing watermarks from digital images.

/ C.-C. Chang, C.-S. Tsai // Informatica. – 2000. – Vol. 24. – P. 391-396.

20. Hwang, M.S. A time-stamping protocol for digital watermarking / M.S. Hwang, K.F. Hwang, C.C. Chang // Applied Mathematics and Computation. – 2005. – Vol. 169. – Issue 2. – P. 1276-1284.

21. Girod B. The information theoretical significance of spatial and temporal masking in video signals / B. Girod // Proc. of the SPIE Symposium on Electronic Imaging. – 1989. – Vol. 1077. – P. 178–187.

22. Watson A. The cortex transform: rapid computation of simulated neural images / A. Watson // Computer Vision, Graphics, and Image Processing. – 1987. – Vol. 39. – № 3. – P. 311–327.

23. BMP file format. URL: https://en.wikipedia.org/wiki/BMP_file_format (дата звернення: 20.10.2023).

24. JPEG file format. URL: https://en.wikipedia.org/wiki/JPEG (дата звернення: 20.10.2023).

25. GIF file format. URL: https://en.wikipedia.org/wiki/GIF (дата звернення: 20.10.2023).

26. PNG file format. URL: https://en.wikipedia.org/wiki/PNG (дата звернення: 20.10.2023).

27. TIFF file format. URL: https://en.wikipedia.org/wiki/TIFF (дата звернення: 20.10.2023).

28. Спектральні методи обробки зображень. URL: http://pzs.dstu.dp.ua/ComputerGraphics/spectrum/index.html (дата звернення: 20.10.2023).

29. Zhao, J. Towards Robust and Hidden Image Copyright Labeling / J. Zhao, E. Koch // IEEE Workshop on Nonlinear Signal and Image Processing. – Greece, 1995. – P. 123–132.

30. D. Benham, N. Memon, B.-L. Yeo, M. Yeung, "Fast Watermarking of DCT-based Compressed Images" Proc. Of the International Conference on Image Science, Systems and Technology. Las Vegas, Nevada, vol. 1, pp. 243-252, June 30 - July 3, 1997.

31. Hsu, C. T., Wu, J. L. (1999) Hidden Digital Watermarks in Images. IEEE Transactions on Image Processing, 8(1), 58–68.

32. Sanghavi, M.R., Dr. Archana, M., Dr. Mathur, R., Kotecha, K.S. A robust scheme for Digital Video Watermarking based on Scrambling of Watermark. Interna-tional Journal of Computer Applications. Vol. 35(2): Pp. 31-38, December 2011.

33. Sinha, S., Bardhan, P., Pramanick, S., Jagatramka, A., Dipak, K. Digital Vid-eo Watermarking using Discrete Wavelet Transform and Principal Component Anal-ysis, International Journal of Wisdom Based Computing, Vol. 1 (2), August 2011. Pp 7-12.

34. Ikpyo Hong, Intaek Kim, Seung-Soo Han. A blind watermarking technique using wavelet transform // Industrial Electronics Proceedings, Pusan, Korea. 2001. Vol.3. Pp. 1946-1950.

35. Poonam and Arora, S.M., (2018). A DWT-SVD based Robust Digital Watermarking for Digital Images. Procedia Computer Science, 132, 1441-1448

36. Singular Value Decomposition (SVD) tutorial. URL: https://web.mit.edu/be.400/www/SVD/Singular_Value_Decomposition.htm (дата звернення: 20.10.2023).

37. Sunil K. Patidar,Saima Khan and Shivendra Vikram Singh 2019,Security for Digital Image and Text Message with Steganography and Watermarking Technique,International Conference on Smart Systems and Inventive Technology (ICSSIT),1106-10.

38. Image watermarking and extraction. URL: https://www.mathworks.com/matlabcentral/fileexchange/85498-image-watermarking-and-extraction?s_tid=FX_rc2_behav (дата звернення: 20.10.2023).

39. DWT-SVD robust and secure watermarking scheme. URL: https://www.mathworks.com/matlabcentral/fileexchange/41686-dwt-svd-robust-and-secure-watermarking-scheme?s_tid=srchtitle (дата звернення: 20.10.2023).

40. Watermarking GUI using DWT. URL: https://www.mathworks.com/matlabcentral/fileexchange/41815-watermarking-gui-

using-dwt (дата звернення: 20.10.2023).

41. Garg, P.; Kishore, R. Performance comparison of various watermarking techniques. Multimed. Tools Appl. 2020, 79, 25921–25967.

42. Tanha, Maryam, Seyed Dawood Sajjadi Torshizi, Mohd Taufik Abdullah, and Fazirulhisyam Hashim (2012) “An overview of attacks against digital watermarking and their respective countermeasures.” In: International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), IEEE, Kuala Lumpur, Malaysia, pp. 265-270.

43. N. Chandrakar and J. Baggaa,”Performance Comparison of Digital Image Watermarking Techniques: A Survey,” International Journal of computer Application Technology and Research, vol. 2, no. 2, pp. 126-130, 2013. DOI: https://doi.org/10.7753/ijcatr0202.1008.