Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Методи нанесення цифрових водяних знаків на цифрові зображення для захисту авторських прав та автентифікації
(тема)

Виконав:

студент II курсу, групи СПм-22-1

Єфімов А. Ю.
(прізвище, ініціали)

Спеціальність

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

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

Освітня програма

Системне програмування
(повна назва освітньої програми)

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

Допускається до захисту

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

2024 р.

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

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

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

Освітня програма Системне програмування
(повна назва)

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

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Єфімову Антону Юрійовичу
(прізвище, ім’я, по батькові)

1. Тема роботи Методи нанесення цифрових водяних знаків на цифрові зображення для захисту авторських прав та автентифікації

затверджена наказом по університету від “ 06 ” листопада 2023 р. № 1299Ст

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

3. Вхідні дані до роботи Набір зображень

4. Перелік питань, що потрібно опрацювати у роботі

Аналіз методів автентифікації

Аналіз методів стеганографії

Розробка методу захисту авторських прав та автентифікації

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) 19 слайдів

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

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

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Огляд автентифікації	06.11.23 – 08.11.23	
2	Огляд механізмів захисту цілісності	09.11.23 – 12.11.23	
	цифрових зображень		
3	Огляд методів хешування	13.11.23 – 19.11.23	
4	Розробка комбінованого підходу до	20.11.23 – 03.12.23	
	захисту цілісності та автентифікації		
5	Проведення експериментів	04.12.23 – 10.12.23	
6	Оформлення матеріалів кваліфікаційної роботи	11.12.23 – 29.12.23	
7	Подання кваліфікаційної роботи керівникові та	30.12.23 – 04.01.24	
	її попередній захист		
8	Подання кваліфікаційної роботи на	05.01.24 – 12.01.24	

Дата видачі завдання 06 листопада 2023 р.

Студент _____
(підпис)

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

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 70 с., 17 рис., 4 табл., 1 дод., 23 джерел.

ЗОБРАЖЕННЯ, ЦВЗ, СТЕГАНОГРАФІЯ, АВТЕНТИФІКАЦІЯ, ЦІЛІСНІСТЬ,

Метою кваліфікаційної роботи є розробка метода нанесення цифрових водяних знаків на цифрові зображення для захисту авторських прав та автентифікації

У ході виконання кваліфікаційної роботи було виканоно наступні завдання:

- проаналізовано методи автентифікації;
- проаналізовано методи стеганографії;
- розроблено метод захисту авторських прав та автентифікації.

ABSTRACT

Master’s thesis: 70 pages, 17 figures, 4 tables, 1 appendices, 23 sources.

IMAGE, CVS, STEGANOGRAPHY, AUTHENTICATION, INTEGRITY,

The major goal of this thesis is development of a method for applying digital watermarks to digital images for copyright protection and authentication

In the course of the qualification work, the following tasks were completed:

- analysed authentication methods;
- analysed the methods of steganography;
- develop a method of copyright protection and authentication.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

IWT – інтервальне хвильове перетворення (Interval Wavelet Transform)

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

DRM – управління цифровими правами (Digital Rights Management)

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

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

PNG – портативна мережева графіка (Portable Network Graphics)

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

AES – розширений стандарт шифрування (Advanced Encryption Standard)

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

SHA – безпека адаптивного хешу (Secure Hash Algorithm)

SVD – перетворення сингулярних значень (Singular Value Decomposition)

GUI – графічний інтерфейс користувача (Graphical User Interface)

OCR – оптичне розпізнавання символів (Optical Character Recognition)

ВСТУП

Зображення є основним компонентом мультимедійного вмісту. Прикладами зображень є цифрове мистецтво, ілюстративні діаграми, картини культурної спадщини в оцифрованій формі та цифрові фотографії. Розвиток комп'ютерного обладнання, програмного забезпечення та мереж створив загрози захисту авторських прав і цілісності вмісту. Наприклад, зображення можна легко копіювати, змінювати та поширювати. Цифровий водяний знак є потенційно хорошим інструментом для забезпечення захисту вмісту. Шифрування забезпечує конфіденційність і цілісність захисту вмісту, а розшифрований вміст можна додатково захистити за допомогою цифрових водяних знаків. Процес нанесення водяних знаків вбудовує сигнал у зображення без значного погіршення його візуальної якості. Потім стегозображення можна оприлюднити або надіслати кінцевому користувачеві. Далі виявлений водяний знак можна використовувати для захисту авторських прав і аутентифікації вмісту.

Надійність водяних знаків є однією з основних характеристик, які впливають на продуктивність і застосування водяних знаків в цифрових зображенях. Надійність у цьому контексті означає здатність водяного знака протистояти звичайній обробці зображень. Залежно від міцності водяні знаки можна розділити на три основні групи: надійні, крихкі та напівкрихкі. Надійні водяні знаки мають бути успішно виявлені на зображеннях, які зазнали маніпулятивних спотворень. З іншого боку, крихкі водяні знаки дуже чутливі й легко знищуються під час модифікації зображення. Посередині обох крайніх кінців знаходяться напівкрихкі водяні знаки. Вони можуть протистояти законним змінам, водночас чутливі до серйозного втручання.

Захист авторських прав стосується позитивної ідентифікації права власності на вміст з метою захисту прав власника. Надійні водяні знаки можна використовувати для захисту авторських прав, оскільки вони постійно

пов’язані із зображенням. Спроби видалити водяний знак мають призвести до серйозного погіршення візуальної якості зображення. Виявлення водяного знака на зображенні може використовуватися для ідентифікації власника авторських прав. З іншого боку, автентифікація вмісту - це перевірка цілісності вмісту. Це нова сфера, яка не вимагає точної перевірки числових значень даних. Крихкі водяні знаки хороші при строгому рівні перевірки цілісності. Напівкрихкі водяні знаки добре підходять для автентифікації вмісту. У цьому випадку виявлений водяний знак порівнюється з його оригінальним вмістом, щоб визначити його цілісність. Крім того, для автентифікації вмісту можна застосовувати напівкрихкі водяні знаки. На відміну від міцного водяного знака, успішне виявлення напівкрихкого водяного знака вказує на те, що вміст не було підроблено. Таким чином, вміст можна перевірити як автентичний.

У цій дипломній роботі досліджуємо методи водяних знаків для захисту авторських прав і автентифікації вмісту. Крім того, також розробляємо можливість «самовідновлення» в методі напівкрихких водяних знаків. Ця можливість дозволяє відновити оригінальний вміст зміненого зображення. Незважаючи на його потенційне застосування в медіа-криміналістиці, його рідко можна знайти в існуючих методах водяних знаків. Щоб забезпечити комплексне рішення для захисту авторських прав і автентифікації вмісту, об’єднуємо два методи водяних знаків у гібридний метод.

1 КОНЦЕПЦІЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ

Список нижче містить значення стандартних термінів, які використовуються в цій дипломній роботі:

- зображення обгортка - це оригінальне зображення, яке використовується для водяних знаків;
- стегозображення - це зображення обгортка після вставлення водяного знака;
- тестове зображення - це можливо модифіковане стегозображення, з якого буде вилучено водяний знак;
- еталонне зображення - це зображення, яке використовується для виявлення водяних знаків. Це може бути зображення обкладинки, стего-зображення або тестове зображення. Зазвичай воно використовується при реєстрації зображень, коли інформація про водяні знаки синхронізується для забезпечення точності вилучення водяних знаків. Процес реєстрації зображень зіставляє розташування кожного об'єкта на спотвореному зображенні з відповідним розташуванням об'єкта на еталонному зображенні, таким чином синхронізуючи числове представлення зображень;
- водяний знак - може бути простим сигналом, що складається з псевдовипадкової двійкової послідовності, або багатобітовим повідомленням, закодованим у домені перетворення;
- вбудовування водяного знака - це процес кодування сигналу водяного знака (тобто водяного знака) у зображення;
- виявлення водяних знаків - це процес виявлення водяного знака, прихованого в зображенні. Цей процес зазвичай складається з кількох кроків, тобто вилучення водяного знака, декодування вилученого повідомлення та перевірка розшифрованої інформації;
- сліпе виявлення водяних знаків - це виявлення водяних знаків, для якого не потрібне контрольне зображення;

- схема водяного знака включає в себе методи вбудови та виявлення;
- спотворення - це зміни, внесені до стегозображення для оцінки його надійності. Ці зміни можуть бути стисненням зображення з втратами, геометричними операціями та звичайною обробкою зображень. Хоча спотворення іноді називають атаками, вони не стосуються зловмисних намірів з метою оцінки аспектів безпеки водяного знака.

Щоб зрозуміти методи водяних знаків і визначити їх застосування, потрібно знати властивості цифрових водяних знаків. Нижче наведено деякі основні властивості водяних знаків:

- міцність водяного знака означає його здатність протистояти незловмисним спотворенням. Наприклад, надійний водяний знак має бути виявлений після стандартних операцій обробки зображень [1, 2];
- корисне навантаження даних - це розмір закодованого повідомлення водяного знака на зображенні. Найпростіша форма водяного знака не містить корисних даних. Він лише дає відповідь «Так/Ні» під час виявлення водяного знака, щоб вказати наявність водяного знака на зображенні. З іншого боку, багатобітові водяні знаки можуть нести текстову або графічну інформацію [3];
- ємність - це кількість інформації про водяний знак на зображенні. Якщо в зображення вбудовано кілька водяних знаків, то здатність водяних знаків зображення є сумою корисних даних усіх окремих водяних знаків [3] ;
- непомітність - це характеристика приховування водяного знака, щоб він не погіршував візуальну якість зображення. Близько пов’язаний термін – вірність;
- точність - це візуальна схожість між стего-зображенням і його обгорткою;
- безпека водяного знака - це здатність водяного знака протистояти зловмисним атакам. Ці атаки включають навмисні операції вставки, модифікації, видалення та оцінки водяних знаків, які мають на меті

перешкодити меті водяних знаків [1, 2] ;

- обчислювальна вартість - це міра обчислювальних ресурсів, необхідних для виконання процесів вбудовування або виявлення водяних знаків. Його можна виміряти за допомогою часу обробки для даної конфігурації комп’ютера.

Існує кілька способів класифікації методів водяних знаків. Одна з найпоширеніших класифікацій базується на надійності водяних знаків. За цією класифікацією водяні знаки можна згрупувати в 3 типи:

- міцні водяні знаки – це водяні знаки, які можуть протистояти незловмисним спотворенням;
- крихкі водяні знаки легко знищуються будь-якими спотвореннями зображення;
- напівкрихківодяні знаки можуть бути знищені певними типами спотворень, одночасно протистоя іншим незначним змінам.

Окрім стійкості, водяні знаки можна також класифікувати на видимі та невидимі. Видимі водяні знаки сприймаються глядачем. Приклад такого водяного знаку зображено на рисунку 1.1. З іншого боку, невидимі водяні знаки є невідчутними і не змінюють візуальний вигляд зображень. У цій роботі нас цікавлять саме невидимі водяні знаки, оскільки вони мають ширший спектр застосування порівняно з видимими водяними знаками. Наприклад, невидимі водяні знаки не впливають на естетичну цінність зображення, а порушення приватності є менш імовірним з огляду на їх затушовування.

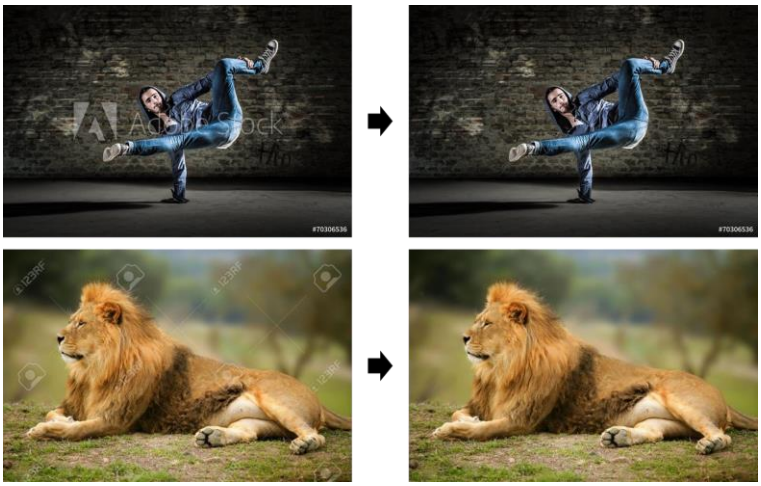


Рисунок 1.1 – Приклад зображення з видимим текстовим водяним знаком

З точки зору застосування, надійні водяні знаки підходять для захисту авторських прав, оскільки вони можуть протистояти звичайним операціям обробки зображень. З іншого боку, крихкі водяні знаки можна використовувати для виявлення підробки та автентифікації зображень, оскільки вони чутливі до змін. Напівкрихкі водяні знаки зазвичай застосовують у деяких особливих випадках автентифікації та виявлення несанкціонованого доступу. У цих випадках стиснення зображення з втратами може розглядатися як легітимні зміни, а геометричні спотворення - як навмисні атаки.

Слід зазначити, що водяні знаки можна вбудовувати і виявляти в різних типах доменів. Найбільш прямим підходом є нанесення водяних знаків у просторовій області, де значення пікселів модифікуються для кодування сигналу водяного знаку. Крім того, частотні області, такі як дискретне косинусне перетворення (ДКП) і дискретне перетворення Фур'є (ДПФ), широко використовуються для нанесення водяних знаків на зображення. Інші області включають дискретне вейвлет-перетворення (DWT), перетворення Радона, перетворення фракталів, чирп-Z-перетворення, перетворення Хадамара, розкладання за сингулярним значенням (SVD) і перетворення Фур'є-Мелліна (FM).

2 НАНЕСЕННЯ ВОДЯНИХ ЗНАКІВ НА ЦИФРОВІ ЗОБРАЖЕННЯ

2.1 Цифровий водяний знак

Між приховуванням інформації, стеганографією та водяними знаками є багато спільного. Приховування інформації передбачає приховування інформації так, щоб спостерігач не знав про її існування. Стеганографія зазвичай означає "зашифроване письмо", коли комунікації здійснюються таємно. Водяні знаки - це вбудовування інформації, залежної від вмісту. Можна скласти ієрархічну таксономію для зв'язку цих областей, тобто приховування інформації охоплює як стеганографію, так і водяні знаки. Ця теза стосується водяного маркування зображень, тобто вбудовування невидимих водяних знаків у зображення.

Аналогом цифрового водяного знаку є паперовий водяний знак. Паперові водяні знаки на грошових купюрах і корпоративних бланках використовуються для підтвердження їхньої автентичності. Аналогічно, цифрові водяні знаки вбудовуються в цифрові носії для підтвердження їхнього вмісту. Хоча криптографічні методи вже давно застосовуються для захисту цифрового контенту, розшифрований контент потребує додаткового захисту. Наприклад, твір мистецтва може бути отриманий законним шляхом, але незаконно розповсюджений серед інших через пірингові мережі. Цифрові водяні знаки можуть забезпечити додатковий захист розшифрованого контенту, оскільки вони вбудовуються в нього.

Технології цифрового водяного маркування почали стрімко розвиватися в останні десятиліття. Про це свідчить експоненціальне зростання кількості наукових публікацій про цифрові водяні знаки протягом багатьох років. Деякі з цих статей були опубліковані в журналах з високим рейтингом. Наприклад, станом на жовтень 2022 року в IEEE Transactions on Signal Processing та IEEE Transactions on Image Processing було опубліковано понад

100 статей про водяні знаки. Дослідницька діяльність у галузі цифрового водяного маркування досягла такого рівня, що з'явилися нові конференції [4-8]. Тематика цих публікацій охоплює багато аспектів цифрового водяного маркування. Вони варіюються від теоретичних дискусій до реальних застосувань. Крім того, теми досліджень стають все більш спеціалізованими, наприклад, надійні водяні знаки, відбитки пальців, бенчмаркінг, стеганоаналіз і безпека. Крім того, технології водяних знаків були комерціалізовані. Наприклад, водяний знак Digimarc [9] було додано до Adobe Photoshop [10], щоб уможливити вбудовування та виявлення водяних знаків на цифрових зображеннях. Компанії Epson [11] та Kodak [12] випустили фотоапарати з можливістю нанесення водяних знаків на зображення. Дослідження в галузі цифрових водяних знаків охоплюють майже всі форми медіа. Приклади включають аудіо, відео, зображення, текст, 3D-моделі та програмні коди. Цифрові водяні знаки - це сигнали, які непомітно вбудовуються в носій і можуть бути виявлені за певних умов. Ця теза зосереджується на водяних знаках для цифрових зображень у відтінках сірого.

Відтінки сірого - це результат простої дискретизації, де кожному пікселю присвоюється певне значення. Типові напівтонові зображення, що використовуються для експериментів у дослідницькій спільноті, мають 8 біт на піксель, отже, кожен піксель має $2^8 = 256$ рівнів сірого. Невелика кількість дослідників працює з іншими форматами зображень, такими як напівтонові та кольорові зображення. Напівтонові зображення підходять для друкованих видань завдяки своєму бінарному вигляду. Кольорові зображення зазвичай складаються з трьох колірних каналів, наприклад, червоного, зеленого та синього. Кожен канал концептуально схожий на відтінки сірого.

Схему нанесення водяних знаків на цифрове зображення можна змоделювати як процес комунікації за участю вбудовувача та детектора, як показано на рисунку 2.1.

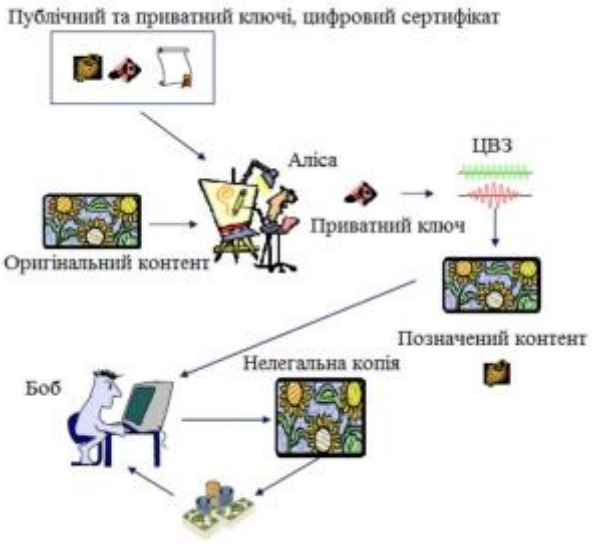


Рисунок 2.1 – Загальна система водяних знаків

По-перше, сигнал водяного знаку непомітно вбудовується в зображення обкладинки для створення стегозображення. Для зберігання сигналу не потрібно додаткового місця. Стегозображення потім передається споживачеві. Під час цього процесу можуть виникати спотворення через ненавмисну модифікацію, зловмисні атаки та стиснення даних. Нарешті, застосовується детектор водяних знаків, щоб визначити, чи існує водяний знак у можливо спотвореному зображенні.

Щоб зрозуміти системи водяних знаків і визначити їх застосування, необхідно знати властивості цифрових водяних знаків.

2.2 Властивості цифрових водяних знаків

Існує кілька важливих властивостей, пов'язаних із системами водяних знаків для цифрових зображень, і вони обговорюються тут.

Стійкість водяного знаку - це його здатність протистояти нешкідливим спотворенням. До таких спотворень зазвичай відносять звичайну обробку зображень, геометричні перетворення та стиснення зображень. Наприклад,

вважається, що водяний знак стійкий до стиснення JPEG, якщо його можна виявити після стиснення зображення. Поширені операції обробки зображень включають вставку шуму, регулювання контрастності, згладжування та обрізання. Геометричні перетворення включають обертання, масштабування та переведення. Хоча бажано, щоб водяні знаки були стійкими до всіх можливих спотворень, реальні програми можуть вимагати лише часткової стійкості. Наприклад, зображення можуть зберігатися в базах даних у стислому форматі. Для цього потрібні водяні знаки, стійкі до високоякісного стиснення зображень. Однак низькоякісне стиснення, яке значно погіршує їхній візуальний вигляд, не є релевантним. Іншими словами, стійкі водяні знаки зазвичай не повинні витримувати екстремальні умови. За таких умов сильні спотворення якості зображення знижують його цінність.

Серед багатьох згаданих типів спотворень, геометричні спотворення залишаються основною проблемою для надійного захисту водяних знаків. Геометричні спотворення можна легко вносити за допомогою готового програмного забезпечення для обробки зображень, і вони суперечать призначенню водяних знаків, роблячи їх невизначуваними. Вони можуть завдати серйозної шкоди інформації водяного знаку через ефекти десинхронізації. Більшість геометричних спотворень можна змоделювати як комбінації трьох основних перетворень: обертання, масштабування і трансляції (RST). Тому багато досліджень у галузі стійкого захисту водяних знаків зосереджені на геометричній стійкості, зокрема на стійкості до RST-перетворень.

Водяні знаки можна класифікувати як стійкі, крихкі або напівкрихкі залежно від їхньої здатності протистояти спотворенням. Стійкі водяні знаки зазвичай призначені для того, щоб витримувати ненавмисні зміни, спричинені звичайною обробкою зображень. Наприклад, ненавмисні зміни можуть включати згладжування зображення. Ранні цифрові методи нанесення водяних знаків вбудовували водяний знак у просторову область або область перетворення зображення без урахування особливостей, важливих для сприйняття. Нові покоління методів нанесення водяних знаків враховують вміст зо-

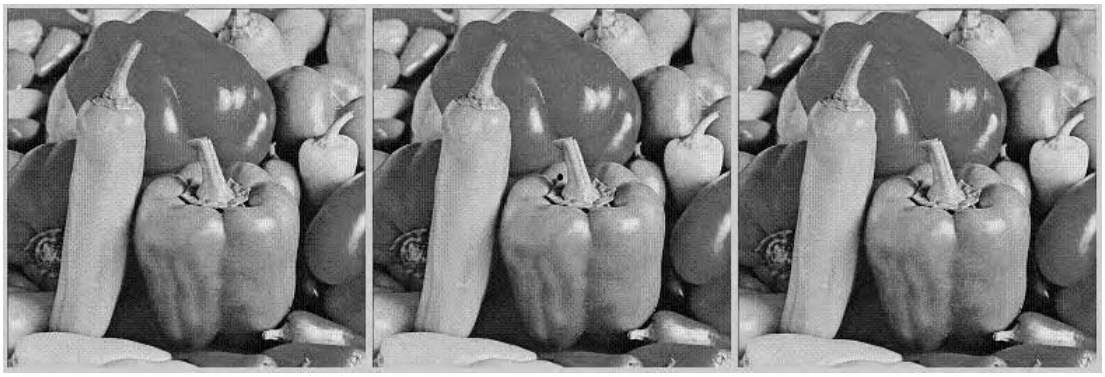
браження та його візуальні особливості [13]. Таке вдосконалення дозволяє підвищити стійкість до геометричних маніпуляцій. З іншого боку, крихкі водяні знаки легко руйнуються від незначних спотворень. Відсутність крихкого водяного знаку вказує на те, що до зображення, в яке він був вбудований, були внесені зміни. Напівкрихкі водяні знаки знаходяться в сірій зоні між двома крайнощами між стійкими і нестійкими водяними знаками. Напівкрихкі водяні знаки мають часткові характеристики надійних і крихких водяних знаків. Наприклад, напівкрихкі водяні знаки можуть бути знищені при зменшенні розміру зображення, але при цьому виявляються після стиснення зображення.

Кількість бітів водяного знаку, закодованих у повідомленні, є корисним навантаженням даних [14], а максимальне повторення корисного навантаження даних у зображенні є ємністю водяного знаку. Найпростішою формою водяних знаків є однобітний водяний знак. (Деякі дослідники вважають за краще називати його нульовим водяним знаком [14]). У цьому випадку детектор водяних знаків матиме 2 можливих виходи: "водяний знак виявлено" і "водяний знак не виявлено", які можна порівняти з простою відповіддю "Так/Ні". Залежно від застосування, деякі методи нанесення водяних знаків вимагають, щоб обсяг даних перевищував 10 000 біт. Водяний знак може мати високу ємність, але низьке корисне навантаження даних. Наприклад, однобітовий водяний знак може бути вбудований багато разів у зображення. Визначення верхньої межі ємності водяних знаків привернуло увагу деяких дослідників. Це могло б стати окремим напрямком дослідження водяних знаків, зважаючи на збільшення кількості публікацій у цій галузі [15]. Однак інтерес цієї роботи полягає у стійкості водяних знаків та комплексному захисті контенту.

Зазвичай бажано, щоб стего зображення були візуально схожими на зображення обкладинки. В іншому випадку, спотворення стего зображення, спричинені вбудовуванням водяного знаку, знизять його естетичну цінність. Крім того, вони можуть викликати підозри і поставити під загрозу безпеку

водяного знака. Ця властивість називається непомітністю водяного знаку [2]. Іноді її називають вірністю або прозорістю сприйняття. Моделі людської зорової системи (HVS) можуть бути застосовані під час вбудовування водяних знаків для підвищення непомітності та стійкості водяних знаків. Модель визначає, що зорова система людських очей має певні характеристики. Очі менш чутливі до змін, що відбуваються у високотекстурованих областях, порівняно з пласкими областями. Текстуровані області мають складні візерунки, тоді як плоскі області є монотонними. Використовуючи модель HVS, можна використовувати більшу вагу водяних знаків при адитивному вбудовуванні для областей зображення зі складною текстурою порівняно з областями з простою текстурою. Результатом збільшення ваги вбудовування буде підвищена стійкість водяного знаку.

Щоб оцінити непомітність серед методів нанесення водяних знаків, необхідно протестувати велику кількість зображень. Через величезні зусилля, тривалий час і високу вартість оцінювання за допомогою людини, зазвичай використовують автоматизоване вимірювання непомітності. Для цього зазвичай використовують пікове відношення сигнал/шум (PSNR) для для порівняння показників непомітності, хоча це не ідеальний показник. Чим більше схожість між стего-зображенням і зображенням на обкладинці, тим вищим є PSNR. Однак стего-зображення може мати високий PSNR, незважаючи на очевидні спотворення сприйняття. Також можлива і протилежна ситуація. Рисунок 2.2 ілюструє ці випадки на прикладі зображення Pepper отриманого з бази даних зображень Університету Південної Каліфорнії за адресою http://sipi.usc.edu/database/. Порівнюючи зображення на рисунку 2.2 (б) із зображенням на рисунку 2.2 (а), очевидна чорна крапка біля центру зображення не дуже зменшує значення PSNR, оскільки артефакт невеликий порівняно з усім зображенням. Зображення на рисунку 2.2 (в) має низьке значення PSNR, оскільки зміни відбулися у всіх областях.



а) б) в)

Рисунок 2.2 – Приклади неточності PSNR для оцінки непомітності водяних знаків. (а) Зображення обкладинки, (б) Тестове зображення з високим PSNR (39,59 дБ), незважаючи на очевидну крапку біля центру зображення, (в) Тестове зображення з низьким PSNR (21,37 дБ) після кругового зсуву рядків

Це означає, що PSNR не дуже точно моделює перцептивну схожість. На жаль, краща перцептивна модель для вимірювання непомітності ще не з'явилася в літературі. ще не з'явилася в літературі. У спільноті фахівців з водяних знаків прийнято вважати, що мінімальний PSNR 38 дБ є прийнятним. Якщо припустити, що зображення має 8-бітну шкалу сірого, то PSNR [19] стего-зображення у порівнянні із зображенням j,ujhnrj. становить

$$PSNR = 20\log_{10}(\frac{I_{\max}}{RMSE}) \tag{2.1}$$

де I_{MAX} - це максимальний рівень сірого у зображенні. У цьому випадку I_{MAX} може мати максимальне значення 255. RMSE - це середньоквадратична похибка, яка визначається за формулою

$$RMSE = \sqrt{\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[(\tilde{f}(m,n) - f(m,n))\right]^2} \tag{2.2}$$

де $\tilde{f}(m,n)$ - стего-зображення, а $f(m,n)$ - зображення обгортка. Альтернативне

обчислення PSNR виглядає наступним чином

$$PSNR = 10\log_{10}(\frac{I_{\max}^{\ 2}}{MSE}) \tag{2.3}$$

де MSE - середньоквадратична похибка, визначена за формулою

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[\tilde{f}(m,n) - f(m,n)\right]^2 \tag{2.4}$$

Зважений PSNR (WPSNR) було запропоновано для підвищення точності вимірювання схожості між зображеннями [19, 20]. Однак він не набув широкого поширення у спільноті фахівців з водяних знаків. Використовуючи ті ж позначення, що і вище, обчислення WPSNR подано за допомогою:

$$WPSNR = 10\log_{10}\frac{I_{\max}^{\ 2}}{\left\|NVF()\,\tilde{f}(m,n) - f(m,n)\right\|^2} \tag{2.5}$$

де NVF - функція шумоподібної видимості (Noise Visibility Function, NVF). NVF [21] для кожного пікселя (n_1, n_2) обчислюється з використанням підсмуг DWT $x_{k,l}$:

$$NVF_{k,l}(n_1,\ n_2) = \frac{x_{k,l}(n_1,\ n_2)}{_{k,l}(n_1,\ n_2) + \sigma^2_{x_{k,l}}} \tag{2.6}$$

де $\sigma^2_{x_{k,l}}$ - глобальна дисперсія вейвлет-коефіцієнтів у підсмузі (k,l).

Захищений метод нанесення водяних знаків може протистояти багатьом ворожим атакам, які намагаються звести нанівець призначення

водяного знаку [14]. Такими атаками можуть бути несанкціоновані операції з видалення, вбудовування, модифікації та виявлення (оцінювання) водяних знаків. Однак деякі програми можуть потребувати лише низького рівня захисту. Наприклад, навряд чи можна атакувати водяний знак, який забезпечує локалізацію підробки та відновлення вмісту. У цьому випадку розширена функція відновлення пошкоджених ділянок зображення має додаткову цінність для користувача. Тому користувач не має стимулу знищувати водяний знак. Інформація водяного знаку може бути використана для виправлення бітів помилок в зображеннях, що виникають через подряпини на поверхні CDROM, де зберігаються зображення. Локалізація несанкціонованого доступу до зображення - це ідентифікація модифікованих ділянок зображення. Відновлення вмісту - це відновлення оригінального вмісту зображення на пошкодженому зображенні.

Найбільш прямим підходом до захисту інформації про водяні знаки є застосування принципу Керкгоффа, як у криптографії. Принцип полягає в тому, що безпека системи повинна покладатися на ключ, а не на приховування алгоритму нанесення водяних знаків. Іншими словами, алгоритм може бути відомий всім, включаючи зловмисника. Однак тільки авторизований користувач, який має ключ, може розкрити захищений водяний знак. Зловмиснику має бути дуже важко "розблокувати" захищений водяний знак, не знаючи правильного ключа. У цьому підході водяний знак генерується з використанням деякої контекстної інформації, такої як розмір зображення і дайджест вмісту. Потім він шифрується секретним ключем. Захищений водяний знак вбудовується в зображення і надсилається одержувачу. Одержувач повинен витягти водяний знак і розшифрувати його за допомогою правильного ключа, щоб отримати інформацію про водяний знак. Цей підхід добре бореться з несанкціонованим виявленням і модифікацією водяних знаків, оскільки зловмисник не може прочитати зашифровану інформацію про водяний знак без використання правильного ключа розшифрування. Однак цей підхід не запобігає несанкціонованому

вбудовуванню та видаленню водяних знаків. Наприклад, зловмиснику не потрібно знати інформацію про водяний знак при виконанні атаки змови для видалення водяного знаку. В атаці змови використовується декілька копій стего-зображення з різними секретними ключами для усереднення інформації про водяний знак.

Слід зазначити, що безпека - це не те саме, що стійкість водяних знаків. Надійний водяний знак може витримати звичайну обробку зображень, але може бути не захищеним від зловмисного підробки. Ця теза фокусується на надійності, а не на безпеці. З огляду на це, іноді буває незрозуміло, що термін "атаки" в літературі може використовуватися як взаємозамінний у контекстах стійкості та безпеки водяних знаків.

Методи нанесення водяних знаків з дуже складними алгоритмами вимагають більших обчислювальних витрат порівняно з методами з низькою складністю. Хоча швидкість обробки даних і обсяг пам'яті споживчого обладнання зростали протягом багатьох років, складність алгоритмів зробила програми більш вимогливими до ресурсів.

Простота обчислень все ще надається перевагу в середовищах з обмеженими ресурсами, таких як мобільні пристрої. Наразі програми на мобільних пристроях повинні знаходити баланс між споживанням енергії акумулятора, використанням пропускної здатності, розподілом пам'яті та багатьма іншими факторами. Поширення водяних знаків зображень на водяні знаки відеокадрів також може потребувати алгоритмів низької складності. Етапи виявлення водяних знаків, які виконуються досить швидко, забезпечать плавний перехід від одного кадру до іншого в реальному часі. Якщо виявлення водяних знаків занадто складне, то це вплине на практичну цінність водяних знаків для відеокадрів.

Оцінити обчислювальні витрати можна, вимірявши час виконання етапів вбудовування та виявлення водяних знаків за допомогою мінімально сконфігурованих систем.

Для моделювання надійного водяного знаку в сценарії захисту

авторських прав можемо використовувати водяний знак, який складається з псевдовипадкової двійкової послідовності, що представляє ідентифікатор власника авторських прав. Значення кореляції між ідентифікацією та правильно виявленим водяним знаком зазвичай дуже високе порівняно зі значенням кореляції між ідентифікацією та випадково вибраним водяним знаком. У цьому випадку графік значень кореляції, побудований проти водяних знаків, має значний пік на правильно виявленому водяному знаку, який відповідає особі власника авторських прав.

Ситуація, описана вище, є простим результатом виявлення водяних знаків. Повніший розгляд включатиме хибнопозитивний, хибнонегативний, істиннопозитивний, істиннонегативний та робочі характеристики приймача (ROC).

Для зображення із вбудованим водяним знаком існує 2 можливих результати виявлення водяного знаку:

- успішне виявлення водяного знаку називається істинним позитивним результатом;
- невдале виявлення водяного знаку називається хибнонегативним.

Аналогічно, для заданого зображення обкладинки (або тестового зображення без водяного знаку) існує 2 можливих результати виявлення водяного знаку:

- відсутність водяного знаку називається істинно негативним;
- неправильно виявлений водяний знак спричиняє хибне спрацьовування (так звану помилкову тривогу).

Ймовірність хибнопозитивного спрацьовування (P_f) - це ймовірність того, що відбудеться хибнопозитивне спрацьовування, і вона часто використовується для визначення ефективності методу нанесення водяних знаків. Залежно від застосування, надійний водяний знак зазвичай вимагає P_f між 10^{-6} і 10^{-12} [14].

Існує певний компроміс між частотою хибнопозитивних і хибнонегативних спрацьовувань, оскільки вони взаємопов'язані. Наприклад,

зменшення частоти хибнонегативних спрацьовувань може призвести до збільшення частоти хибнопозитивних спрацьовувань. ROC-крива може бути використана, щоб показати взаємозв'язок між ймовірністю хибнопозитивного результату та ймовірністю достовірно позитивного результату. Для того, щоб побудувати ROC-криву, нам потрібно мати розподіл зображень обкладинки та стегозображень. Змінюючи поріг виявлення, можна обчислити відповідну частоту хибнопозитивних і хибнонегативних спрацьовувань. Рисунок 2.3 ілюструє розподіл значень виявлення водяних знаків для зображень обкладинки та стего. Світло заштрихована область - це ймовірність хибнопозитивного результату. Сума слабо заштрихованих і сильно заштрихованих ділянок - це ймовірність істинно позитивного результату. Після цього за даними точок хибнопозитивних і хибнонегативних результатів будується ROC-крива.

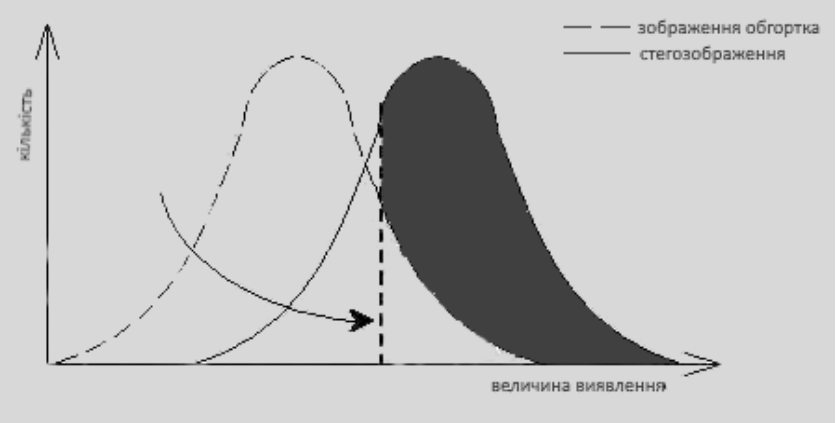


Рисунок 2.3 – Розподіл значень виявлення водяних знаків для зображень обгортки та стего

Сліпе виявлення - це виявлення водяного знаку без еталонного зображення. Еталонним зображенням може бути зображення обкладинки, зображення стего з іншим водяним знаком або неспотворене зображення стего. Щоб стати більш практичним, метод нанесення водяних знаків не повинен покладатися на наявність еталонного зображення. Він має

забезпечувати сліпе виявлення водяних знаків, використовуючи лише зображення, що тестується. Іншими словами, ми можемо виявити водяний знак, використовуючи лише тестове зображення при сліпому виявленні водяних знаків. Виявлення водяних знаків буде приймати тестове зображення як вхідні дані, виконувати алгоритм для виявлення і виводити виявлений водяний знак. З іншого боку, несліпе виявлення водяних знаків схоже на сліпе виявлення водяних знаків, за винятком того, що воно вимагає еталонного зображення. Проблема полягає в тому, що еталонне зображення може бути недоступним.

Інформоване виявлення протистоїть сліпому виявленню. При інформованому виявленні водяних знаків детектор повинен мати доступ до зображення обкладинки. Ця вимога обмежує застосування інформованого виявлення водяних знаків.

Основний принцип нанесення водяних знаків полягає у використанні надмірності зображень для вбудовування інформації про водяний знак. Враховуючи той факт, що багато з існуючих алгоритмів стиснення зображень не є досконалими, водяні знаки стають можливими завдяки вбудовуванню додаткової інформації в надлишкові частини. Крім того, підвищення стійкості водяного знаку зазвичай вимагає більших спотворень зображення і збільшення надмірності. Це призводить до меншої непомітності та більшої ймовірності видалення під час зловмисних атак.

Багато з описаних вище властивостей водяних знаків мають суперечливі характеристики. Наприклад, збільшення стійкості водяного знака зазвичай знижує його непомітність через більшу енергію водяного знака, що накладається на зображення обкладинки. Крім того, більша ємність ставить під загрозу його непомітність, оскільки для вбудовування водяного знака потрібно більше модифікацій зображення обкладинки. Тому розробка методу нанесення водяних знаків зазвичай вимагає пошуку балансу між цими суперечливими факторами.

3 НАНЕСЕННЯ НАПІВКРИХКИХ ВОДЯНИХ ЗНАКІВ НА ЗОБРАЖЕННЯ ДЛЯ АВТЕНТИФІКАЦІЇ

Ранні методи нанесення водяних знаків зосереджені на точній автентифікації (так звана жорстка автентифікація, повна автентифікація) з використанням крихких водяних знаків. У такому випадку зміна одного біта в зображенні буде класифікована як неавтентична. Зображення може бути автентифіковане за допомогою криптографічного хешу або цифрового підпису в якості крихкого водяного знаку. Існує кілька переваг використання водяних знаків над криптографічними методами для цієї мети. По-перше, крихкий водяний знак, вбудований у зображення, не потребує додаткового зберігання. По-друге, він також несприйнятливий до перетворення формату, оскільки залишається цілим із зображенням і зазнає тих самих перетворень, що й зображення. Нарешті, на додаток до перевірки цілісності всього зображення, водяний знак може також визначати, яка частина зображення є неавтентичною. Це називається локалізацією несанкціонованого доступу, і буде розглянуто пізніше. Хоча надійні водяні знаки можна використовувати для автентифікації, простота крихких водяних знаків робить їх кращим варіантом [16].

Щоб гарантувати, що крихкий водяний знак не втручається в автентифікаційну інформацію зображення, простір вбудовування можна розділити на підпростір генерації водяного знаку та підпростір вбудовування водяного знаку. Простір вбудовування тут може бути просторовим або частотним. Наприклад, водяний знак можна вбудувати в площину найменш значущих бітів (LSB) після того, як він згенерований з іншої бітової площини вищого порядку. Окрім розбиття зображення на підпростори для генерації та вбудовування водяних знаків, іншим підходом є створення оборотних водяних знаків, які можна "стерти", щоб розкрити оригінальний вміст зображення. Цей підхід використовує виявлену інформацію про водяний знак для інвертування змін, зроблених під час вбудовування водяного знаку.

Для автентифікації контенту можна використовувати як стійкі, так і нестійкі водяні знаки. Однак вони є жорсткішими порівняно з напівкрихкими водяними знаками. Напівкрихкі водяні знаки можуть бути спроектовані так, щоб витримувати законні зміни, водночас виділяючи навмисні спотворення. Ця характеристика робить напівкрихкі водяні знаки придатними для широкого спектру застосувань. Наприклад, ми можемо дозволити стиснення зображень для економії місця на диску. Іншими застосуваннями напівкрихких водяних знаків є автентифікація вмісту, локалізація несанкціонованого доступу та відновлення вмісту. Вони будуть розглянуті у наступних підрозділах.

3.1 Перевірка автентичності вмісту зображення

Нові сфери застосування цифрових водяних знаків вимагають здатності відрізняти законні зміни від незаконних модифікацій. Наприклад, високоякісне стиснення, яке не впливає на візуальну якість зображення, має бути допустимим, а заміна області, яка змінює зміст зображення, має бути виділена. Тому для автентифікації контенту були створені напівкрихкі водяні знаки. Автентифікацію контенту в цьому контексті також називають м'якою автентифікацією або вибірковою автентифікацією. Для цього напівкрихкий водяний знак повинен легко руйнуватися під час звичайної обробки зображення, але при цьому бути стійким до законних змін. Перевірка цілісності зображення ґрунтується на його змісті, а не на числовому представленні. Ступінь напівкрихкості визначається сценарієм застосування. Прикладом застосування, яке віддає перевагу напівкрихким водяним знакам перед крихкими, є зменшення обсягу пам'яті за допомогою високоякісного стиснення зображень. Інша ситуація, яка підходить для напівкрихких водяних знаків, - це толерантність до бітових помилок при передачі та зберіганні даних.

Не існує загальноприйнятого стандарту щодо допустимого рівня деградації зображення. Нижче наведені деякі з видів легкої обробки, які можуть бути класифіковані як легітимні зміни:

- стиснення JPEG з коефіцієнтом якості вище 80%. Чим вищим є коефіцієнт якості зображення, стисненого JPEG, тим кращою є його візуальна якість. Зазвичай згадується, що коефіцієнт якості нижче 10% є неприйнятним через видимі блокові артефакти, хоча стиснення значно зменшує обсяг пам'яті [17] ;
- вставка шуму солі та перцю з максимальною інтенсивністю 1%. Це може імітувати концепцію бітових помилок через "подряпини" на оптичних носіях інформації, або підчас потокової передачі відео контенту;
- випадкова бітова помилка у вихідних даних з максимальною ймовірністю 0.001. За своєю концепцією це схоже на описаний вище шум солі та перцю.

Залежно від ситуації, наступні операції можуть вважатися або не вважатися дозволеними змінами. Наприклад, можна стверджувати, що заміна області зображення є підробкою і має бути виявлена як підроблена область. Однак, якщо замінена область візуально не відрізняється від оригіналу, то така модифікація може бути дозволена в деяких комерційних рекламах. Очевидно, що медичні зображення вимагають більш високого рівня доброчесності порівняно з творами образотворчого мистецтва.

- адитивний білий гаусівський шум (AWGN), що дає мінімальне відношення сигнал/шум (SNR) 36 дБ;
- згладжування зображення за допомогою ядра 3×3 із середньою вагою;
- вирівнювання гістограми з рівномірним розподілом;
- заміна області зображення, при якій зберігається візуальний вигляд;
- регіональне геометричне перетворення, яке не впливає на якість сприйняття;
- глобальний поворот менше ніж на 1 градус;
- глобальний круговий зсув на 1 рядок або 1 стовпець;
- обрізання вздовж кордонів зображення, що не перевищує 1%

площі зображення;

- перетворення формату файлу.

Зазвичай існує два способи автентифікації вмісту зображення. Один спосіб полягає у використанні важливих особливостей вмісту як водяного знаку для самоавтентифікації. Цей спосіб має перевагу у відновленні вмісту. Інший спосіб полягає у використанні цифрових підписів, які не залежать від вмісту. Для автентифікації вмісту зображень рішення часто приймається на основі порогових значень. Наприклад, можна використовувати заздалегідь визначене порогове значення для підрахунку кількості бітів помилки або значення кореляції автентифікації. Якщо розраховане значення перевищує порогове, то зображення класифікується як автентичне.

2.2 Локалізація несанкціонованого втручання

На ранній стадії розвитку крихких і напівкрихких водяних знаків результат виявлення водяного знаку - це лише проста відповідь про те, автентичний він чи не автентичний. Нові методи можуть ідентифікувати підроблені області на неавтентичному зображенні. Це можливість локалізації несанкціонованого доступу. Результати локалізації можуть бути корисними в медіакриміналістиці. Наприклад, можна визначити тип втручання, що стоїть за зміною певної ділянки зображення.

Більшість сучасних схем напівкрихких водяних знаків використовують блокову обробку для локалізації несанкціонованого доступу. Цей підхід розділяє зображення на блоки, що не перекриваються, і обробляє кожен з них окремо. Наприклад, середнє значення блоків розміром 8×8 пікселів можна вбудувати в зображення обкладинки. Пізніше його можна витягти зі стегозображення і порівняти з обчисленим середнім значенням блоку в тому ж місці, щоб виявити фальсифікацію. На рисунку 3.1 показано приклад локалізації на основі блоків. Зображення Lena (також відоме як Lenna) розбито на 16 блоків однакового розміру. Вбудовування та виявлення водяних знаків вико-

нується для кожного блоку окремо. Такий підхід, безумовно, передбачає великий обсяг обчислень. Вищої точності локалізації несанкціонованого доступу можна досягти, використовуючи менші блоки. Однак і вартість обчислень буде вищою. Перевага цього підходу полягає в тому, що для кожного блоку можна використовувати різну інформацію про водяні знаки, що робить його більш гнучким.

Рисунок 3.1 – Локалізація на основі блоків

Альтернативою блоковій локалізації є локалізація на основі зразків. У цьому підході двійковий логотип невеликого розміру вбудовується в плитковий візерунок на зображенні. Порушені ділянки підсвічуються, якщо виявлений шаблон водяного знака не відповідає плитковому шаблону. Приклад з використанням логотипу торгова марка показано на рисунку 3.2. Область, обмежена зразком у рядку 2 стовпчика 2, вказує на те, що відбулося підроблення, оскільки виявлений шаблон водяного знаку пошкоджено. Незважаючи на простоту реалізації та низьку складність, цей підхід є жорсткішим порівняно з попереднім підходом.

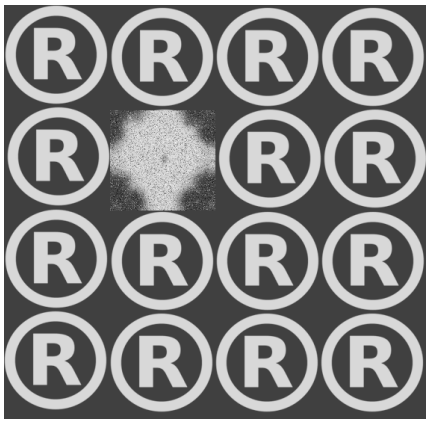


Рисунок 3.2 – Локалізація на основі зразка

Локалізація на основі вейвлетів, можливо, є більш елегантним та ефективним підходом порівняно з двома описаними вище підходами. Вейвлет-перетворення, таке як DWT розкладає зображення на низькочастотну підсмугу і три високочастотні підсмуги. Просторово-часова інформація у вейвлет-коефіцієнтах може бути легко використана для для локалізації несанкціонованого доступу. Це позбавляє від необхідності включати інформацію про місцезнаходження блоку у водяний знак. Переваги цього підходу також включають помірний обсяг обчислень і гнучкість нанесення водяних знаків. Наприклад, кращу точність локалізації можна досягти за рахунок нанесення водяних знаків на першому рівні вейвлет-розкладання, а також більшої надійності (меншої крихкості) можна досягти, накладаючи водяні знаки на вищому рівні вейвлет-розкладання. На рисунку 3.3 зображено 4-рівневий DWT, а коефіцієнт на рівні 2 відповідає 4 коефіцієнтам на рівні 1 в тій самій області. Крім того, маскування HVS можна легко застосувати, використовуючи енергетичну картину в низькочастотній підсмузі вейвлет-розкладу. Це можливо тому, що підсмуга низьких частот являє собою зменшену версію зображення, а HVS моделює сприйняття зображення людським оком.

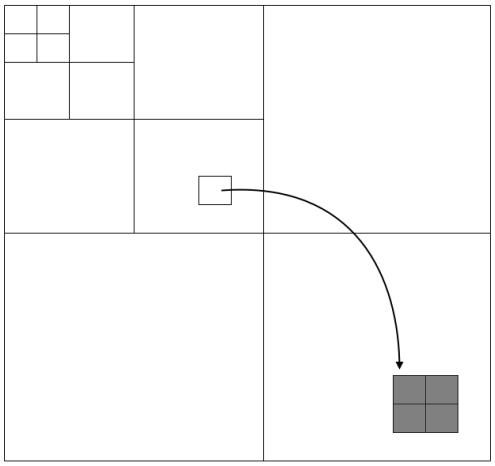


Рисунок 3.3 – Локалізація на основі вейвлетів

3.2 Відновлення вмісту зображення

Відновлення вмісту є відносно новою проблемою в галузі водяних знаків. Після ідентифікації пошкоджених ділянок з локалізацією хочеться виправити пошкодження і виявити оригінальний вміст. Порівнюючи відновлений вміст із підробленим зображенням, можна полегшити роботу судового експерта-криміналіста. Хоча повне відновлення контенту теоретично неможливе, його приблизне відновлення цілком досяжне. Повне відновлення вмісту практично неможливе, оскільки водяні знаки вносять спотворення і займають підпростір зображення.

Щоб забезпечити відновлення вмісту, стислий набір інформації про зображення може бути вбудований як водяний знак. Потім виявлений водяний знак можна використати для відновлення пошкодженої області. Цей процес іноді називають само-вбудовуванням, само-автентифікацією та самовідновленням. Конденсована інформація про зображення може бути зменшеною версією зображення, стисненим набором важливих характеристик зображення, коротким описом областей зображення або будь-якою іншою абстракцією зображення. Характеристиками зображення можуть бути краї, яскравість, текстура тощо. Вибір інформації про зображення для нанесення водяного знаку є дуже важливим, оскільки він безпосередньо визначає потужність водяного

знаку та якість відновленого контенту. Слід зазначити, що надійні хеші, візуальні хеші та цифрові підписи не підходять для відновлення контенту, оскільки вони мають занадто мало інформації для опису вмісту зображення. Крім того, важливо уникати вбудовування водяного знаку в ту саму область, щоб протистояти атакам обрізання. В іншому випадку, водяний знак буде втрачено разом з обрізаною областю, і відновлення вмісту буде неможливим.

На сьогоднішній день існує дуже мало напівкрихких водяних знаків з можливістю відновлення вмісту [18] Це спостереження можна пояснити природою напівкрихких водяних знаків. В ідеалі, водяний знак повинен бути стійким, а не напівкрихким, щоб витримувати якомога більше спотворень, щоб оригінальний вміст, закодований у водяному знаку, можна було використовувати при відновленні вмісту. Крихкі водяні знаки також можуть певною мірою сприяти відновленню контенту [19].

3.3 Гібридні методи у нанесенні водяних знаків на зображення

Окремі методи нанесення водяних знаків, стійкі або напівстійкі, можуть слугувати лише для обмеженої кількості цілей. Вони обмежені своєю стійкістю або напівкрихкістю. Наприклад, напівкрихкі водяні знаки не підходять для захисту авторських прав, оскільки вони можуть бути знищені зловмисником. Для подолання цих обмежень хорошим вибором є гібридний метод нанесення водяних знаків, оскільки він поєднує в собі надійний і напівкрихкий водяні знаки. Доповнюючи слабкі сторони кожного окремого водяного знака, гібридний метод водяного маркування має високий потенціал у практичному використанні. Хоча існують деякі ранні гібридні методи водяних знаків, які поєднують стійкі та крихкі водяні знаки, ми особливо зацікавлені в комбінації стійких та напівкрихких водяних знаків. Напівкрихкі водяні знаки мають явну перевагу порівняно з крихкими водяними знаками, оскільки вони можуть відрізнити законні зміни від недозволених модифікацій.

Гібридні методи водяних знаків можуть бути широко реалізовані двома

способами. Перший спосіб полягає в тому, що під час вбудовування надійний і напівкрихкий водяні знаки накладаються один на одного, і кожен з них виявляється окремо. Надійний водяний знак вбудовується першим, а потім напівкрихкий водяний знак. Це зроблено на основі того, що стійкий водяний знак повинен бути здатним протистояти спотворенням, введеним напівкрихким водяним знаком. Ці міркування обговорювали Фрідріх [20] та Мінцер-Браудевей [21]. Інший спосіб гібридного накладання водяних знаків полягає в тому, щоб переконатися, що стійкі та напівкрихкі водяні знаки не перекриваються під час вбудовування водяного знаку. Це можна зробити, розбивши зображення на блоки для незалежної обробки. Виявлення водяних знаків виконується окремо для стійких і напівкрихких водяних знаків. Таке ортогональне розташування може бути досягнуто шляхом вбудовування водяних знаків у різні набори коефіцієнтів в області перетворення. Така реалізація зменшить інтерференцію між двома водяними знаками, що забезпечить кращі результати виявлення водяних знаків порівняно з першою реалізацією. Однак практичний гібридний метод нанесення водяних знаків повинен знайти баланс між кількома важливими факторами, наприклад, непомітністю водяних знаків, стійкістю або напівкрихкістю кожного водяного знаку, точністю локалізації несанкціонованого доступу, ефективністю відновлення контенту та загальними обчислювальними витратами. Наприклад, непомітність водяних знаків може бути гіршою в методі накладання через вищий рівень спотворень.

У літературі не так багато гібридних методів нанесення водяних знаків, порівняно з методами нанесення одного водяного знаку. Це може бути пов'язано зі складністю розробки гібридного методу. Однак, підвищені функції захисту в гібридному методі, можливо, спонукали до публікації деяких дослідницьких робіт. Більшість гібридних методів нанесення водяних знаків використовують надійний водяний знак для захисту авторських прав і крихкий водяний знак для виявлення несанкціонованого доступу. Вони коротко розглянуті нижче.

Найперший гібридний метод, ймовірно, був запропонований Фрідріхом у 1999 році [19]. Він складається з блочного стійкого водяного знаку та крихкого водяного знаку. Зображення розбивається на блоки однакового розміру, що не перекриваються, і обробляється окремо. Розмір блоку повинен бути компромісом між стійкістю стійкого водяного знаку і точністю локалізації тампера. Наприклад, великий розмір блоку має кращу стійкість, але менш точний при локалізації підробки. Стійкий водяний знак вбудовується в середньочастотні коефіцієнти домену ДКП за допомогою методу розширеного спектра і захищається секретним ключем. Виявлення стійкого водяного знаку обчислюється за допомогою кореляції в області DCT. Крихкий водяний знак має можливість локалізації підробки, але він не може відрізнити значні модифікації від невинної обробки зображення. Однак, використовуючи результати виявлення як стійких, так і крихких водяних знаків, можна визначити значні модифікації та невинну обробку зображень. Наприклад, успішне виявлення стійкого водяного знаку і відсутність крихкого водяного знаку без локалізованого підробки вказує на те, що зображення могло бути піддано звичайній обробці.

Гібридний метод, описаний в роботі Фан-Цао [22], розроблено спеціально для формату JPEG2000. Надійний водяний знак вбудовується з використанням скалярного квантування на декількох масштабах в області DWT. Його стего-зображення мають низьку візуальну якість, оскільки стійкий водяний знак було вбудовано в низькочастотні підсмуги, де він спричиняє багато спотворень. Крихкий водяний знак аналогічно вбудований у підсмуги високих частот на різних масштабах. Виявлення стійких і нестійких водяних знаків виконується на різних масштабах в області DWT з використанням однакового скалярного квантування у відповідних підсмугах. Стійкість до звичайної обробки зображень та геометричних атак не повідомляється.

4 ГІБРИДНИЙ МЕТОД НАНЕСЕННЯ ВОДЯНИХ ЗНАКІВ

Надійні водяні знаки зазвичай використовуються для захисту авторських прав, оскільки їх важко видалити з відповідного зображення. З іншого боку, крихкі водяні знаки підходять для автентифікації, оскільки вони чутливі до змін, зроблених на зображенні. Між цими двома типами водяних знаків знаходиться напівкрихкий водяний знак. Напівкрихкі водяні знаки зазвичай застосовуються для автентифікації контенту, оскільки вони дозволяють вносити законні зміни і можуть виявити зловмисне втручання.

Гібридні методи нанесення водяних знаків поєднують стійкі та крихкі водяні знаки, щоб забезпечити захист авторських прав та автентифікацію в інтегрованому рішенні. Крім того, гібридні методи водяного маркування можуть також поєднувати стійкі та напіввразливі водяні знаки для надання дедуктивної інформації в криміналістиці цифрових медіа.

Було досліджено гібридні методи нанесення водяних знаків у 3 етапи. На першому етапі було проведено пілотне дослідження поєднання стійкого та крихкого водяних знаків у гібридному методі нанесення водяних знаків. Основна мета цього дослідження - оцінити непомітність водяного знаку на стегозображеннях. Крім того, також вивчаємо можливість анотування з використанням стійкого водяного знаку та практичність виявлення несанкціонованого доступу з використанням крихкого водяного знаку.

4.1 Сліпе виявлення водяних знаків у вейвлет-області

Найпоширенішими стратегіями вбудовування водяних знаків є адитивна, мультиплікативна та квантування. Адитивне вбудовування є простим і швидким. Зазвичай воно має вигляд $I' = I + \alpha m$, де I' - стего-зображення, I - зображення-обкладинка, α - сила вбудовування, а m - сигнал водяного знаку. Використовуючи той самий набір позначень, що наведено

вище, мультиплікативне вбудовування реалізується за допомогою I' = I × αm. Квантоване вбудовування може бути реалізоване за допомогою методу квантування. Наприклад, коефіцієнти DWT можна розділити на 2 набори, подібно до концепції парних/непарних чисел. Один набір коефіцієнтів представляє біт "0", тоді як інший набір коефіцієнтів представляє біт "1". Цей метод вбудовування є більш складним порівняно з адитивним та мультиплікативним вбудовуванням. Наприклад, розмір кроку, який визначає проміжок між 2 наборами коефіцієнтів, повинен бути ретельно обраний шляхом аналізу діапазону значень коефіцієнтів. Великий розмір кроку погіршить непомітність водяного знаку, в той час як малий розмір кроку вплине на стійкість водяного знаку. У цьому дослідженні будемо використовувати адитивне вбудовування для низьких обчислювальних витрат.

Етапи вбудовування водяних знаків для трьох досліджуваних методів схожі. Він починається з декомпозиції зображення за допомогою DWT, за яким слідує обчислення міцності вбудовування за допомогою відповідних методів, і завершується оберненим DWT (IDWT), який реконструює стего-зображення. На рисунку 4.1 зображено ці процеси.

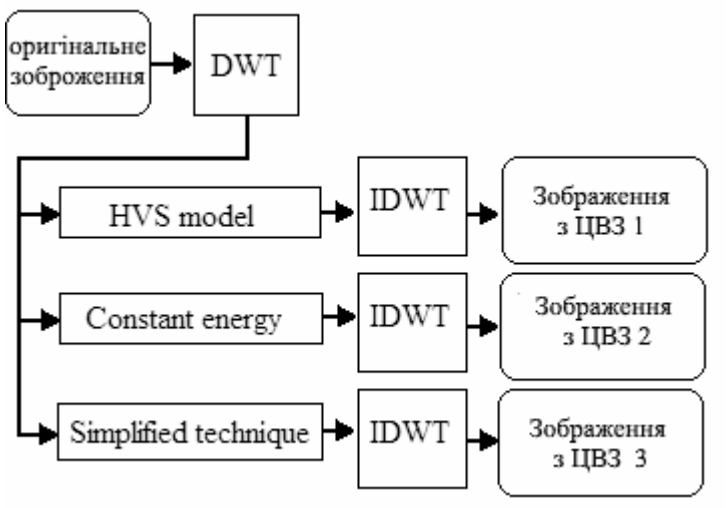


Рисунок 4.1 – Вбудовування водяних знаків трьома методами

Надійний метод нанесення водяних знаків на основі DWT [23] вбудовує інформацію про водяний знак у домен DWT. Він також включає ваговий коефіцієнт вбудовування, який використовує характеристики HVS. Це дозволяє адаптувати силу вбудовування відповідно до змін текстури зображення, відстані між краями, чутливості до шуму та локальної яскравості. Таким чином, метод отримав надійність і непомітність одночасно. Спочатку зображення розкладається на підсмуги високих і низьких частот за допомогою DWT з фільтром Daubechies-6.

Кожен l-й рівень декомпозиції складається з трьох спрямованих смуг високих частот і смуги низьких частот. Щоб уникнути аналітичних атак, водяний знак зазвичай вбудовується у всі смуги високих частот, а не в деякі з підсмуг.

Детально метод нанесення водяних знаків на основі HVS описано в [20], а тут наведено загальний опис. Водяний знак вбудовується в три смуги високих частот на рівні 0 за допомогою наступного рівняння.

$$I_0'^{\theta}(i,j) = I_0^{\theta}(i,j) + \alpha w^{\theta}(i,j) x^{\theta}(i,j) \tag{4.1}$$

le $\theta \in \{0,1,2\}$ - значення підсмуги високих частот,

$I_0^{\theta}(i,j)$ - вихідні коефіцієнти підсмуги,

$I_0'^{\theta}(i,j)$ - стего-підсмуга $I_0^{\theta}(i,j)$,

α - глобальний енергетичний параметр, який визначає міцність вбудовування водяного знаку,

$w^{\theta}(i,j)$ - вагова функція, отримана з локальної чутливості до шуму, яка забезпечує маскувальні характеристики HVS,

$x^{\theta}(i,j)$ - псевдовипадкова двійкова послідовність, $m_h \in \{+1, -1\}$, закодована у двовимірному масиві за допомогою рівняння (4.2).

$$x^{\theta}(i,j) = m_{(\theta MN+iN+j)} \tag{4.2}$$

де θ ∈{0,1,2} - вибір підсмуги високих частот, а 2M×2N - розмір зображення обкладинки. Вагова функція w є адаптацією квантування коефіцієнта DWT, що використовується для стиснення зображень.

З рівняння (4.1) видно, що обчислена вагова функція w на кожному пікселі дозволяє досягти високого рівня непомітності та стійкості водяних знаків на основі HVS. Нарешті, IDWT виконується після вбудовування водяного знаку для створення стегозображення.

Метод вбудовування постійної енергії реалізується аналогічним методом, але з опущеною ваговою функцією w.

$$I_0'^{\theta}(i,j) = I_0^{\theta}(i,j) + \alpha x^{\theta}(i,j) \tag{4.3}$$

Значення α у рівнянні (4.3) має бути більшим, ніж у рівнянні (4.1), щоб гарантувати високу енергію вбудовування та успішне виявлення водяних знаків. Очевидно, що цей метод вбудовування вимагає найменшої кількості обчислень порівняно з HVS та спрощеними методами. Метод вбудовування з постійною енергією обрано як базовий у цьому порівняльному дослідженні.

Щоб досягти балансу між двома крайнощами методів HVS і постійної енергії, створили спрощений метод вбудовування. Спрощений метод вбудовування значно скорочує час вбудовування, зберігаючи при цьому характеристики непомітності та стійкості. Метод швидкого вбудовування використовує неявні особливості піддіапазонів DWT. Коефіцієнти DWT у низькочастотному діапазоні забезпечують хороше наближення інформації про яскравість зображення. Крім того, коефіцієнти DWT у смугах високих частот дають оцінку інформації про краї зображення. Посилаючись на рівняння (4.1), Спрощений метод вбудовування використовує іншу вагову функцію s.

$$I_0'^{\theta}(i,j) = I_0^{\theta}(i,j) + \alpha s^{\theta}(i,j) x^{\theta}(i,j) \tag{4.4}$$

де $s^{\theta}(i, j)$ позначає яскравість та інформацію про край на зображенні; інші члени такі ж, як і в рівнянні (4.1).

Вагова функція s обчислюється за допомогою рівнянь (4.5) та (4.6) нижче.

$$s^{\theta}(i, j) = \frac{q_0''^{\theta}(i, j)}{2} \tag{4.5}$$

$$q_0''^{\theta}(i, j) = \Theta(l, \theta)\Lambda''(i, j)\Xi_0''^{\theta}(i, j)^2 \tag{4.6}$$

де $\Theta(l, \theta)$ враховує чутливість до шуму,

$\Lambda''(i, j)$ враховує яскравість для рівнів сірого в підсмузі низьких частот з рівняння (4.7). Має сенс взяти частину апроксимаційних значень з низькочастотного діапазону, оскільки ці значення містять інформацію про zcrhfdscnm. Наші експериментальні результати показують, що β = 0.01 дає хороші результати,

$$\Lambda''(i, j) = I_3^3(i, j) \times \beta \tag{4.7}$$

$\Xi_0''^{\theta}(i, j)$ враховує інформацію про краї за допомогою рівняння (4.8). На відміну від розрахунку вагів чутливості людського ока до шуму представлених в роботі [23], у (4.8) ця величина підноситься до квадрату, щоб забезпечити швидке зменшення значення при врахуванні інформації про краї в кожному з піддіапазонів. Наші експерименти показують, що δ = 0.005 дає хороші результати.

$$\Xi_0''^{\theta}(i, j) = I_0^{\theta}(i, j) \times \delta \tag{4.8}$$

По суті зменшили інформативність про текстуру у (4.8) та збільшили швидкість обчислень.

Незалежно від використоного методу вбудовування, при сліпому виявленні водяних знаків застосовується метод крос-кореляції. Це забезпечує справедливе порівняння між трьома методами вбудовування щодо стійкості до різних атак. Щоб виявити наявність сигналу водяного знаку x, ми починаємо з операції DWT над стего-зображенням, подібно до процесу вбудовування. Потім за допомогою рівняння (4.9) обчислюється значення крос-кореляції між коефіцієнтами підсмуги стего I' і шаблоном водяного знаку x.

$$\rho = \frac{1}{3MN}\sum_{\theta=0}^{2}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} I_0'^{\theta}(i,j)x^{\theta}(i,j) \tag{4.9}$$

Варто зазначити, що адаптивне порогове значення T_p обчислюється динамічно, що дозволяє уникнути вимоги до коефіцієнта надійності вбудовування α. Якщо $\rho > T_p$, то водяний знак x присутній, в іншому випадку - відсутній. Для того, щоб ймовірність помилкового спрацьовування не перевищувала 10^{-8}, поріг T_p обирається наступним чином:

$$T_p = 3.97\sqrt{2\sigma_{\rho\beta}^2} \tag{4.10}$$

$$\sigma_{\rho\beta}^2 = \frac{1}{3MN}\sum_{\theta=0}^{2}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(I_0^{\theta}(i,j))^2 \tag{4.11}$$

Розрахунок цього порогового значення адаптовано на основі критерію Неймана-Пірсона. Значення 3,97 у рівнянні (4.10) базується на результатах масових випробувань [23].

Для оцінки якості непомітності стегозображень вимірюється WPSNR

кожного стегозображення. WPSNR обрано через його вищу точність порівняно з PSNR.

Тести на стійкість були проведені з шістьма типами звичайних атак, переліченими в Таблиці 4.1.

Застосовуючи кроки вбудовування, показані на рисунку 4.1, бінарний шаблон водяного знаку, показаний на рисунку 4.2 нижче, вбудовується у три смуги високих частот (тобто темні квадранти) Lena.

а) б)

Рисунок 4.2 – Підсмуги водяного знаку та DWT (а) Шаблон водяного знаку x, (б) підсмуги DWT рівня 0 для Lena

Таблиця 4.1 – Атаки, що використовуються в тестах на стійкість

No	Тип атаки	Опис
1	Стиснення JPEG	Рівень якості 85%, 70%, 55%, 40% і 25%
2	Вставка гауссового шуму	Нульове середнє, дисперсія 0.0002, 0.0004, 0.0006, 0.0008 та 0.0010
3	Обрізання	8×8, 16×16, 32×32, 64×64, та 128×128 квадратів у центрі зображення обрізано.
4	Регулювання контрастності	Гамма 0.8
5	Медіанна фільтрація	2D медіанна фільтрація з використанням околиці 3×3
6	Глобальне геомет-ричне спотворення	Поворот на 3 градуси по центру зобра-ження, випадкове згинання.

Експерименти показали, що спрощений метод вбудовування займає стільки ж часу, як і метод вбудовування з постійною енергією. З іншого боку, метод вбудовування HVS вимагає більш ніж у 55 разів більшої тривалості обробки. У таблиці 4.2 наведено час вбудовування для оброблених зображень. Виявлення водяних знаків до атаки було зроблено для кожного з вбудованих зображень. У всіх випадках водяні знаки було виявлено успішно.

Таблиця 4.2 – Час вбудовування для трьох методів вбудовування

Зображення	Час вбудовування (секунди)		
	HVS	Simplified	Constant
Бабуїн	62.370	1.222	1.111
Оператор	61.398	1.172	1.071
Лєна	61.209	1.182	1.072
Перець	61.089	1.182	1.072
Рибальський човен	61.209	1.182	1.072

Для стегозображень, отриманих кожним з методів вбудовування, вимірюється значення WPSNR. На рисунках 4.3-4.7 зображено стего-зображення та їхні значення WPSNR. Для цих тестів використовували розширену версію спрощеного методу вбудовування, оскільки вплив крайової інформації дуже малий на загальну міцність вбудовування $\alpha s\theta(i,j)$. Значення α, вибрані для методів HVS, постійної енергії та спрощеного вбудовування, становлять 4.5, 1.5 та 2.2 відповідно. Крім того, у спрощеному методі використовується $\beta = 0{,}01$. Такі умови є необхідними, оскільки основний інтерес полягає у порівнянні коефіцієнтів ефективності. Хоча значення α методів вбудовування відрізняються, ефективна сила вбудовування після множення на відповідні вагові функції не сильно відрізняється.

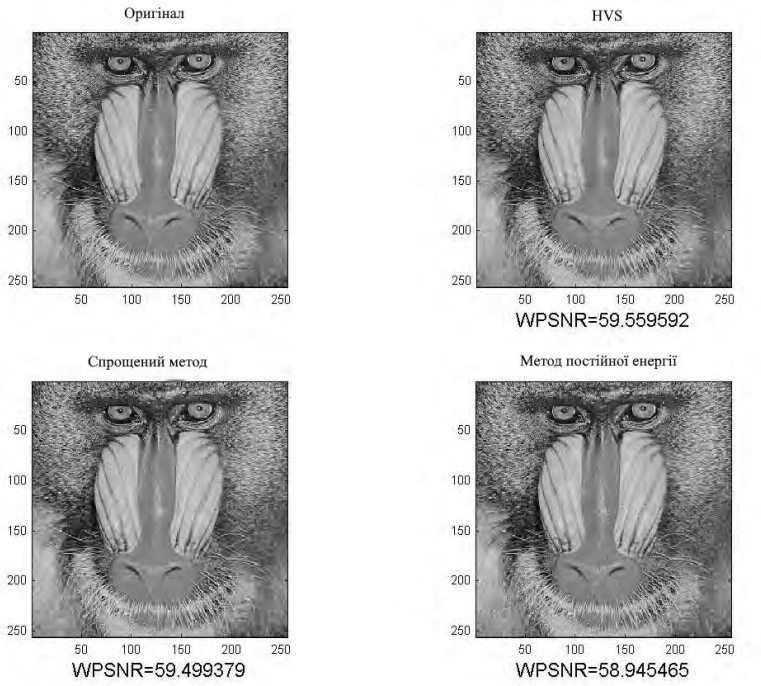


Рисунок 4.3 – Набір результатів вбудовування Baboon з відповідним WPSNR

Рисунок 4.4 – Набір результатів вбудовування Cameraman з відповідним WPSNR

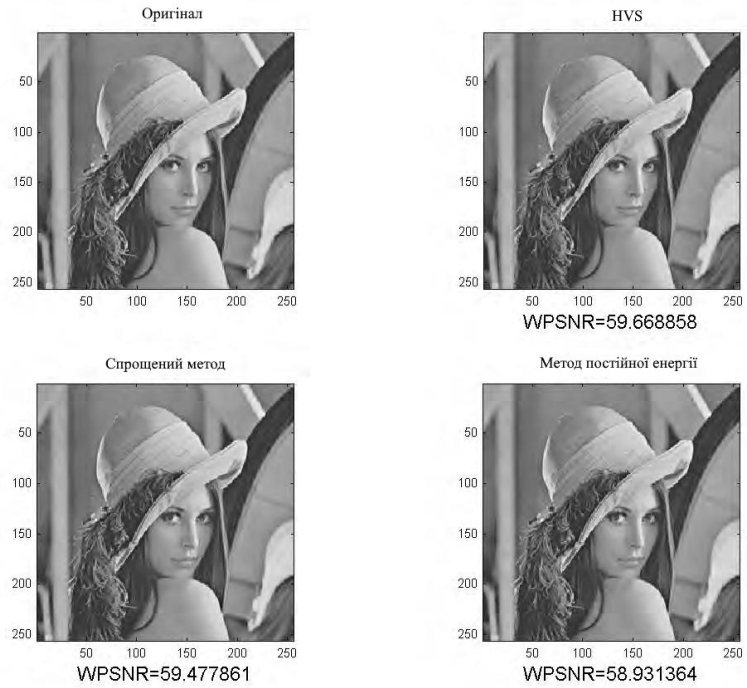


Рисунок 4.5 – Набір результатів вбудовування Lena з відповідним WPSNR

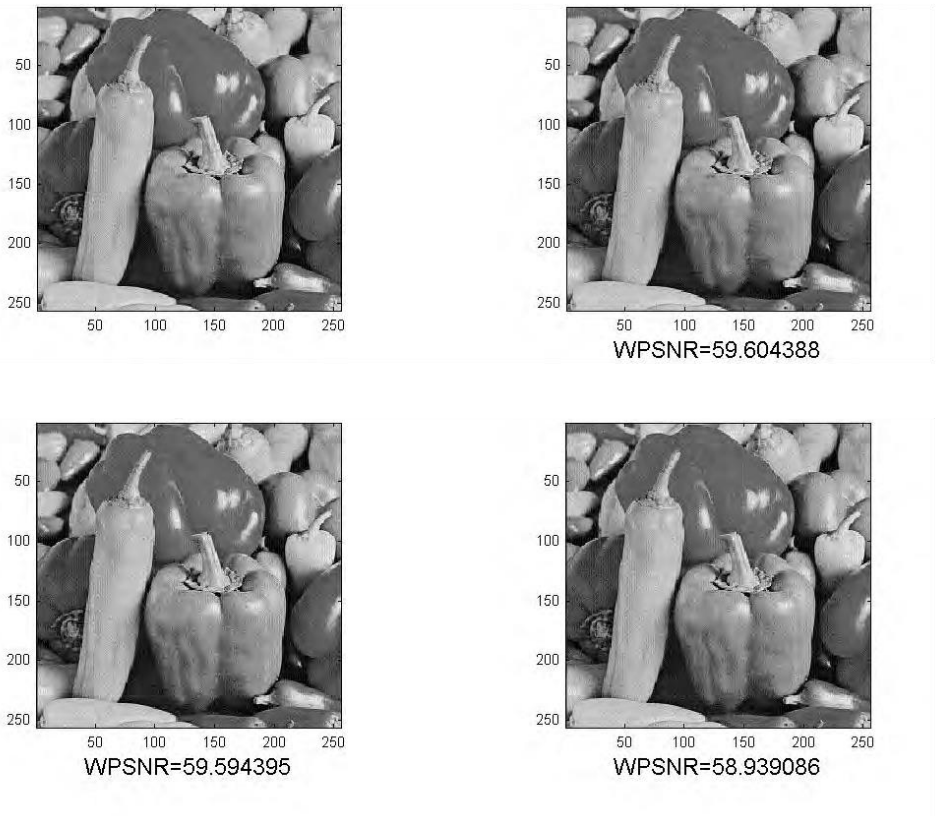


Рисунок 4.6 – Набір результатів вбудовування Pepper з відповідним WPSNR

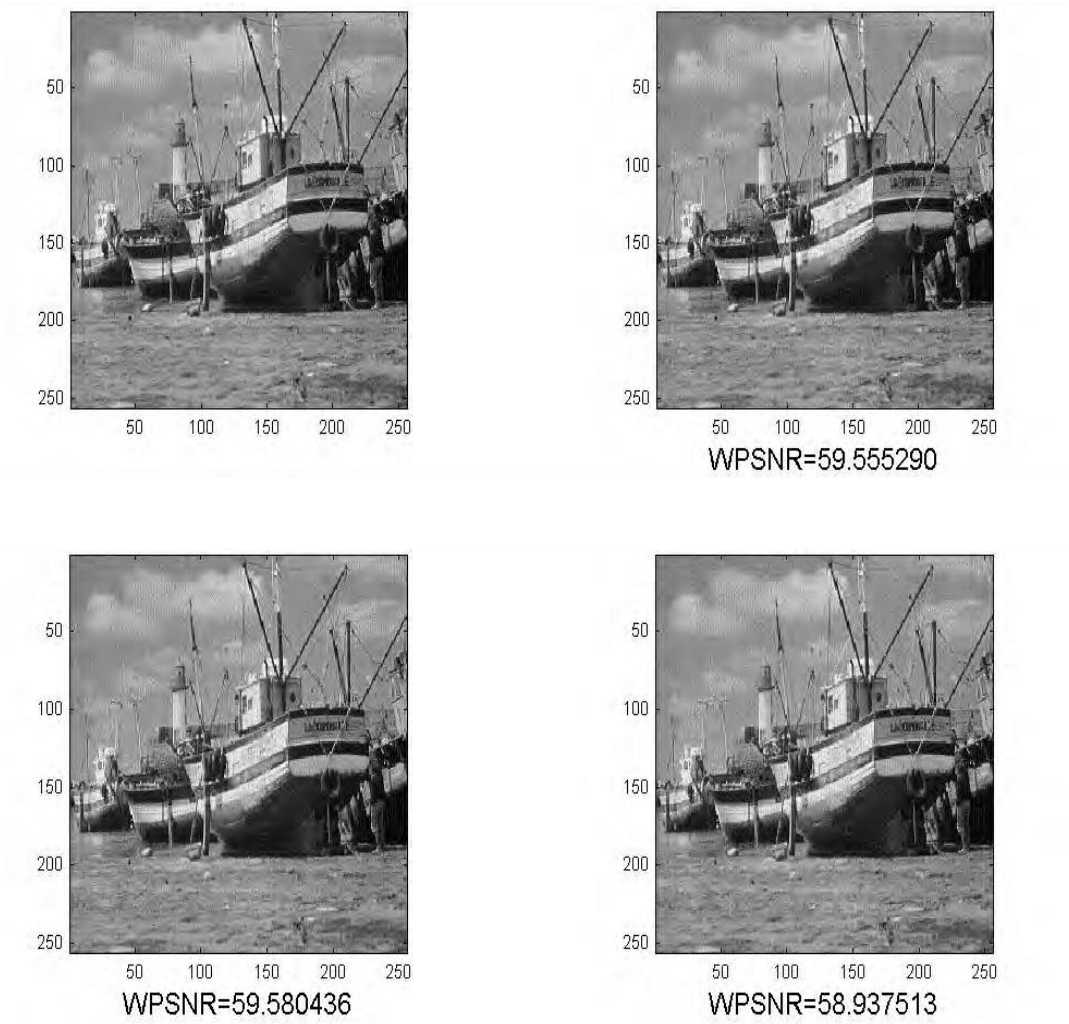


Рисунок 4.7 – Набір результатів вбудовування рибальських суден з відповідними WPSNR

Наочне порівняння непомітності у графічному вигляді представлено на рисунку 4.8. Метод вбудовування з постійною енергією має найнижчу візуальну якість в цілому, а метод вбудовування HVS досягає найвищої візуальної якості в цілому. Також помічено, що метод спрощеного вбудовування має дещо нижчу візуальну якість, ніж метод вбудовування HVS.

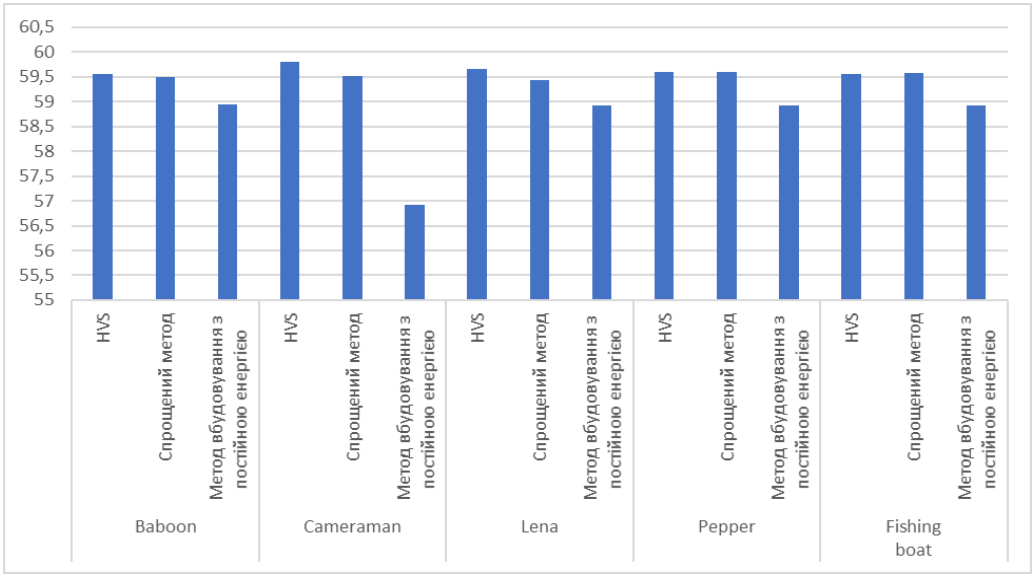


Рисунок 4.8 – WPSNR стегозображень при різних методах вбудовування

Всі вбудовані зображення були атаковані шістьма операціями, переліченими в таблиці 4.1. Для перших 3 типів атак було виконано п'ять рівнів атаки, описаних у таблиці. Приклади різних атакованих зображень наведено на рисунку 4.10. Оригінальне зображення Олени показано на 4.9 (а). Стиснення JPEG з коефіцієнтом якості 25% для вбудованого зображення HVS показано на 4.9 (б). Гаусівський шум з дисперсією 0.001 додано до спрощеного вбудованого зображення і показано на 4.9 (в), а 4.9 (г) показує область 32×32 пікселів, обрізану на вбудованому зображенні з постійною енергією. На 4.9 (д) показано регулювання контрасту з гамою 0,8 на вбудованому зображенні HVS. На рисунку 4.9 (е) показано двовимірне зображення з медіанною фільтрацією на вбудованому зображенні з постійною енергією Lena, в якому використано ядро околиці 3×3. Нарешті, глобальне обертання на 3 градуси навколо центру зображення проти годинникової стрілки на спрощеному вкладеному зображенні показано на 4.9 (є).

Результати експериментів для всіх п'яти зображень при всіх умовах атаки, перелічених у таблиці 4.1, зібрано в таблиці 4.1. Результати тестів на

стійкість зведено до таблиці 4.3. Для кожної з атак стиснення JPEG, вставки гаусівського шуму та обрізання кожен метод виявлення тестується на 25 стего-зображеннях. До кожного зображення застосовується 5 рівнів атаки. Таким чином, для кожного методу вбудовування є 25 (5×5=25) тестових зображень. Для кожної з трьох атак, що залишилися в таблиці, кожен метод виявлення тестується на 5 стего-зображеннях. До кожного зображення застосовується 1 рівень атаки. Таким чином, для кожного методу вбудовування є 5 (1×5=5) тестових зображень. Для атак на стиснення JPEG вбудовування з постійною енергією показало відмінні результати, оскільки обрана енергія є достатньо сильною в компромісі з візуальною якістю. Однак методи HVS та спрощеного вбудовування не можуть протистояти високому рівню стиснення з втратами.

Рисунок 4.9 – Зразки атакованих зображень а) оригінал Lena, б) стиснення у форматі JPEG, в) Гауссів шум, г) обрізання, д) регулювання контрасту, е) медіанна фільтрація, є) обертання

Таблиця 4.3 – Зведені результати виявлення водяних знаків для всіх рівнів атак

№	Тип атаки	Кількість виявлених водяних знаків		
		HVS	Constant	Simplified
1	Стиснення JPEG	21	25	21
2	Вставка гауссового шуму	25	25	25
3	Обрізання	25	25	25
4	Регулювання контрастності	5	5	5
5	Медіанна фільтрація	1	1	1
6	Глобальне геометричне спотворення	0	0	0

Використовуємо значення $C = (\rho - T_p)$ для вимірювання "компетентності" виявлення водяних знаків. Додатне значення C означає, що водяний знак виявлено, а від'ємне - ні. Вище значення C означає вищу "силу" успішного виявлення водяних знаків. З таблиці 4.4 видно, що метод вбудовування HVS не призводить до виявлення водяного знаку в Cameraman під час атаки стиснення JPEG з коефіцієнтом якості 55%.

Таблиця 4.4 – Порівняння компетентності трьох методів вбудовування при атаці стиснення JPEG з коефіцієнтом якості 55%

Зображення	Цінність компетенції		
	HVS	Simplified	Constant
Baboon	1.1961	1.3458	2.2954
Cameraman	– 0.0016	0.1142	0.4805
Lena	0.1740	0.1830	0.4464
Pepper	0.6264	0.6225	1.1627
Fishing boat	0.4942	0.5867	1.2233

Водяний знак також не виявляється у вбудованому HVS Cameraman

для нижчих коефіцієнтів якості 40% і 25%. В експериментах не було виявлено водяних знаків для зображень Cameraman, створених методом спрощеного вбудовування, коли коефіцієнт якості атаки стиснення JPEG встановлено на рівні 40% або 25%. Ці спостереження можна пояснити великими площами пласких ділянок у зображенні Cameraman. При використанні методів HVS і Спрощеного вбудовування надійність вбудовування водяних знаків на пласких ділянках є нижчою порівняно з високотекстурованими ділянками. Тому міцність вбудовування водяних знаків занадто слабка, щоб протистояти сильному стисненню JPEG. Всі методи вбудовування дали позитивні результати при трьох наступних типах атак: Вставка гауссівського шуму, регіональне обрізання та регулювання контрастності. Деякі позитивні значення компетентності, C, були отримані при медіанній фільтрації для всіх методів вбудовування. Фактично, всі виявлення в Лені були успішними під час атак для HVS, постійної енергії та спрощеного методу вбудовування. Однак, жоден з методів вбудовування не забезпечив виявлення стего-зображень при медіанній фільтрації [23].

4.2 Експериментальне дослідження гібридного методу нанесення водяних знаків

Було створено гібридний метод створення водяних знаків, як показано на рисунку 4.1 нижче. Водяний знак з додатковою інформацією та крихкий водяний знак вбудовуються окремо в різні області зображення.

Щоб забезпечити безпеку даних і конфіденційність пацієнта, інформація про пацієнта може бути зашифрована і супроводжуватися водяним знаком анотації. Крім того, особистість лікаря, який бере участь у процесі візуалізації, може бути підписана цифровим підписом, який також супроводжується водяним знаком анотації для автентифікації.

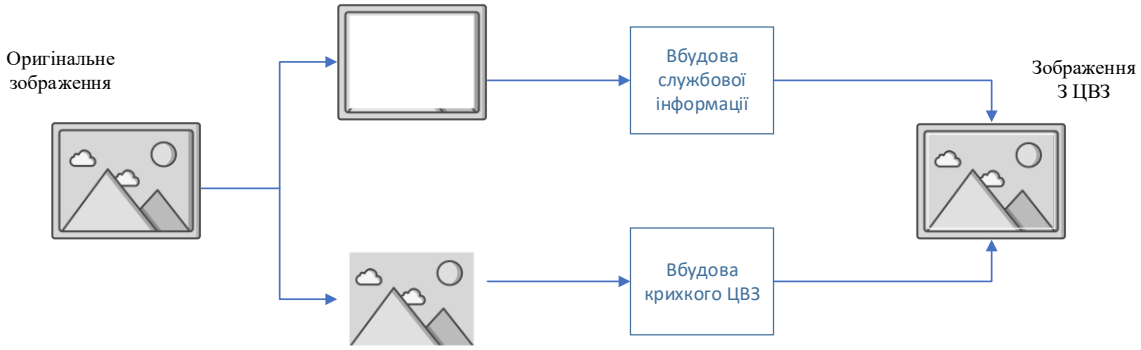


Рисунок 4.10 – Вбудова гібридних водяних знаків

Вдосконалена версія методу спрощеного вбудовування повністю опускає інформацію про края, вилучаючи Ξ для прискорення обчислень. Наші експерименти показують, що продуктивність подібна до оригінальної версії, оскільки малі значення інформації про края в рівнянні представлених в роботі [24] мало впливають на вагову функцію s. Ємність водяного знаку в усіх вищезгаданих методах вбудовування однакова. Це пов'язано з однаковим розміром шаблону водяного знаку x, що застосовується.

Використовуючи процедури вбудовування та виявлення водяних знаків, було протестовано набір з п'яти поширених зображень.

Всі вони є зображеннями у відтінках сірого зі стандартним розміром 256×256 пікселів. Зображення ідентифіковані за назвами: "Бабуїн", "Оператор", "Лена", "Перець" та "Рибальський човен".

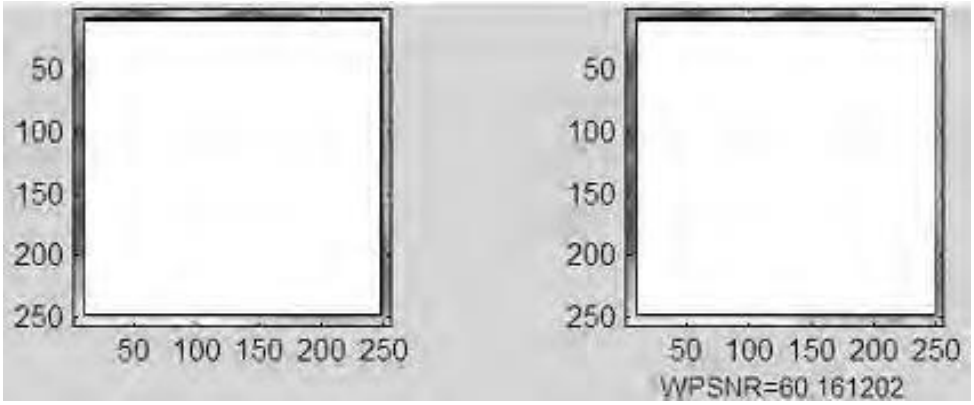
Обчислювальні витрати порівнюються шляхом вимірювання часу вбудовування, який займає кожен з методів вбудовування. Інтуїтивно зрозуміло, що модель HVS має найбільший обсяг обчислень, оскільки обчислення вагової функції включає багато операцій підсумовування/згортання. Навпаки, метод вбудовування постійної енергії має бути найшвидшим, оскільки вагова функція не обчислюється.

Щоб забезпечити безпеку даних і конфіденційність пацієнта, інформація про пацієнта може бути зашифрована і супроводжуватися водяним зна-

ком анотації. Крім того, особистість лікаря, який бере участь у процесі візуалізації, може бути підписана цифровим підписом, який також супроводжується водяним знаком анотації для автентифікації.

Сигнал водяного знаку розміщується у шаблоні кадру, як показано на рисунку 4.11. Потім він вбудовується за допомогою лінійного адитивного методу в три смуги високих частот DWT границь зображення обкладинки. Це здійснюється на першому рівні підсмуг DWT. Обернене DWT виконується над відміченими коефіцієнтами для отримання відміченої межі зображення. Це показано на рисунку 4.12. Хоча на ілюстрації використовуються межі фіксованого розміру для квадратного зображення, цей метод можна легко адаптувати до прямокутних зображень будь-яких розмірів.

Рисунок 4.11 – Розташування водяних знаків анотацій у шаблоні кадру



а) б)

Рисунок 4.12 –Рамки зображень для нанесення водяних знаків анотації а) Рамки зображення обкладинки, що використовуються для вбудовування водяних знаків анотації. б) Межі зображення стего

Цілісність медичного зображення можна перевірити за допомогою крихкого водяного знаку. Фальсифікацію зображення можна виявити, вивчаючи шаблони крихких водяних знаків, що нанесені плиткою.

Крихкий водяний знак вбудовується в центральну область зображення обкладинки за допомогою методу LSB. Таким чином, ми можемо гарантувати, що спотворення не буде надто сильним для більшості частин ROI на зображенні. Як результат, зображення стего має хороший рівень непомітності водяних знаків. Межа зображення зарезервована для вбудовування водяного знаку анотаціївбудовування. Двійковий шаблон водяного знаку накладається плиткою на все зображення, а його двійкові значення пікселів використовуються для перезапису відповідних LSB пікселів зображення-обкладинки. На рисунку 4.13 наведено приклад цього процесу на прикладі рентгенівського знімка грудної клітки.

Після вбудовування водяного знаку анотації та крихкого водяного знаку обидві частини об'єднуються, щоб сформувати повне гібридне стего-зображення. На рисунку 4.14 показано гібридне зображення з водяними знаками.

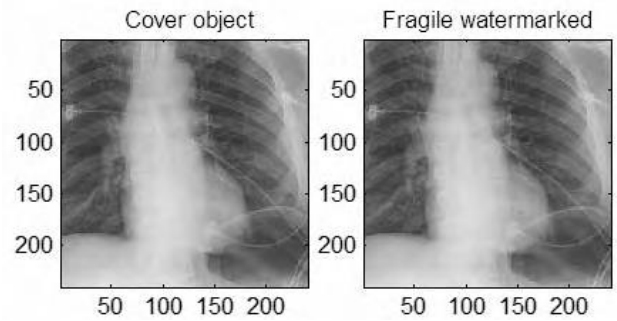


Рисунок 4.13 – Вбудовування крихких водяних знаків (а) Зображення обкладинки, (б) Крихкий водяний знак, вбудований у центральну частину рентгенівського знімка грудної клітки

Рисунок 4.14 – Гібридне зображення стего

ВИСНОВКИ

Метою кваліфікаційної роботи була розробка метода нанесення цифрових водяних знаків на цифрові зображення для захисту авторських прав та автентифікації.

У ході виконання кваліфікаційної роботи було виканоно наступні завдання:

- проаналізовано методи автентифікації;
- проаналізовано методи стеганографії;
- розроблено метод захисту авторських прав та автентифікації.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. ECRYPT, First Summary Report on Forensic Tracking. 2015, European Network of Excellence in Cryptology.

2. ECRYPT, First Summary Report on Fundamentals. 2015, European Network of Excellence in Cryptology.

3. Lin, E.T., Video and Image Watermark Synchronization, in Center for Education and Research in Information Assurance and Security. PhD thesis, Purdue University: West Lafayette.2015.

4. The 8th Information Hiding Conference, 2023. [Електроний ресурс]. – Режим доступу: http://ih2006.jjtc.com/.

5. International Workshop on Digital Watermarking, 2023. [Електроний ресурс]. – Режим доступу: http://www.iwdw.org/.

6. LNCS Transactions on Data Hiding and Multimedia Security, 2023. [Електроний ресурс]. – Режим доступу: http://web.njit.edu/~shi/TDHM.html.

7. IEEE Transactions on Information Forensics and Security, 2023. [Електроний ресурс]. – Режим доступу: http://www.ieee.org/organizations/society/sp/tifs.html.

8. EURASIP Journal on Information Security, 2023. [Електроний ресурс]. – Режим доступу: http://www.hindawi.com/GetJournal.aspx?journal=.

9. Digimarc Corporation, 2023 . [Електроний ресурс]. – Режим доступу: http://www.digimarc.com/.

10. Adobe Systems Inc., 2023. [Електроний ресурс]. – Режим доступу: http://www.adobe.com/.

11. Seiko EpsonCorporation,2006. [Електроний ресурс]. – Режим доступу: http://www.epson.com/america_north.html.

12. Kodak Australia, 2006. [Електроний ресурс]. – Режим доступу: http://wwwau.kodak.com/AU/en/consumer/consumer.jhtml

13. Kutter, M.,S.K. Bhattacharjee, and T. Ebrahimi. Towards second

generation watermarking schemes. in International Conference on Image Processing 1999. P.320 – 323.

14. Cox, I., M.L. Miller, and J.A. Bloom, Digital watermarking. 2001, San Francisco, CA, USA.: Morgan Kaufmann Publishers Inc. 539P.

15. Jiang, D., X. Weixin, and Y. Jianping. Study on capacity of information hiding for still images. in Signal Processing Proceedings, 2000. WCCC-ICSP 2000. 5th International Conference on. 2000. Vol.2. P.1010-1013

16. Wong, P.W. A public key watermark for image verification and authentication. in Image Processing. Proceedings. 2008 International Conference on. 2008. Voll.1. P.455-459.

17. JPEG ImageCompression, 2006. [Електроний ресурс]. – Режим доступу: http://www.vectorsite.net/ttdcmp2.html

18. Lin, C.-Y. and S.-F. Chang. SARI: Self-Authentication-and-Recovery Image Watermarking System. in ACM Multimedia 2011. Ottawa, Canada: ACM Press.2011. P628-629.

19. Fridrich, J. and M. Goljan. Images with self-correcting capabilities. in International Conference on Image Processing 1999 (ICIP 99). Kobe, Japan: IEEE. 1999. P.792-796

20. Fridrich, J. A Hybrid Watermark for Tamper Detection in Digital Images. in Proceedings of the Fifth International Symposium on Signal Processing and Its Applications 1999. Brisbane, Australia. 1999 Vol.1. P.301-304.

21. Mintzer, F. and G.W. Braudaway. If One Watermark is Good, Are More Better? in IEEE International Conference on Acoustics, Speech, and Signal Processing 1999 (ICASSP '99). Phoenix, AZ, USA. 1999. Vol.4 P. 2067-2069.

22. Fan, Y.-C. and H.-W. Tsao. A Dual Pyramid Watermarking for JPEG-2000. in 19th International Conference on Advanced Information Networking and Applications. 2015. Vol.2. P.239-242 .

23. Barni, M., F. Bartolini, and A. Piva, Improved wavelet-based watermarking through pixel-wise masking. Image Processing, IEEE Transactions. 2010. Vol.10. № 5.P. 783-791.

24. Єфімов А. Ю.., et al. " Методи нанесення цифрових водяних знаків на цифрові зображення для захисту авторських прав та автентифікації." InterConf (2023): С. 44-52.

.