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)

Метод нанесення цифрових водяних знаків на цифрове зображення за допомогою пірамідального перетворення
(тема)

Виконав:

студент II курсу, групи СПм-22-6

Зубко І.С.
(прізвище, ініціали)

Спеціальність

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

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

Освітня програма

Системне програмування
(повна назва освітньої програми)

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

Допускається до захисту

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

2024 р.

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

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

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

Освітня програма Системне програмування
(повна назва)

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

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Зубку Івану Сергійовичу
(прізвище, ім’я, по батькові)

1. Тема роботи Метод нанесення цифрових водяних знаків на цифрове зображення за допомогою пірамідального перетворення

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

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

3. Вхідні дані до роботи база даних зображень USC-SIPI

4. Перелік питань, що потрібно опрацювати у роботі

1) Аналіз сучасних досліджень в предметній області
2) Огляд пірамідальних перетворень
3) Розробка методу
4) Проведення експерементів

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) 15 слайдів

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

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

КАЛЕНДАРНИЙ ПЛАН

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

Дата видачі завдання 01 квітня 2024 р.

Студент _____
(підпис)

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

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 57 с., 9 рис., 3 табл., 1 дод., 21 джерело.

ЗОБРАЖЕННЯ, ЦВЗ, СТЕГАНОГРАФІЯ, АВТЕНТИФІКАЦІЯ, ЦІЛІСНІСТЬ.

Метою кваліфікаційної роботи є розробка та дослідження метод нанесення цифрових водяних знаків на цифрове зображення за допомогою пірамідального перетворення, що забезпечить високу стійкість водяних знаків до різних видів атак та мінімальну видимість для людського ока, зберігаючи при цьому високу якість зображення.

Завдання роботи:

- проаналізувати існуючі методи нанесення цифрових водяних знаків;
- дослідити методику пірамідального перетворення;
- розробити методики нанесення водяних знаків;
- реалізувати запропонований метод нанесення цифрових водяних знаків.

ABSTRACT

Master’s thesis: 57 pages, 9 figures, 3 tables, 1 appendices, 21 sources.

IMAGE, CVS, STEGANOGRAPHY, AUTHENTICATION, INTEGRITY.

The major goal of this thesis is to develop and study a method of applying digital watermarks to a digital image using a pyramidal transformation, which will ensure high resistance of watermarks to various types of attacks and minimal visibility to the human eye, while maintaining high image quality.

Objectives:

- analyse existing methods of digital watermarking;
- to investigate the pyramidal transformation technique;
- to develop methods of watermarking;
- to implement the proposed method of digital watermarking.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

AES – розширений стандарт шифрування (англ., Advanced Encryption Standard)

DRM – управління цифровими правами (англ., Digital Rights Management)

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

GUI – графічний інтерфейс користувача (англ., Graphical User Interface)

IWT – інтервальне хвильове перетворення (англ., Interval Wavelet Transform)

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

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

OCR – оптичне розпізнавання символів (англ., Optical Character Recognition)

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

PNG – портативна мережева графіка (англ., Portable Network Graphics)

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

SHA – безпека адаптивного хешу (англ., Secure Hash Algorithm)

SVD – перетворення сингулярних значень (англ., Singular Value Decomposition)

ВСТУП

Метод вбудови цифрового водяного знака в зображення дає змогу розв'язати проблему права власності, тому дослідження в області стеганографії має ширший спектр застосування, наприклад, захист авторських прав, автентифікація контенту, ідентифікація власника тощо. Яремчук та інші [1], Рубан та інші [2], A Ray та інші [3] представили огляд сучасних методів вбудови цифрових водяних знаків в зображеня, які застосовують у різних галузях. У цій статті представлено мотивацію подальших досліджень, області застосування, вимоги та питання проектування, класифікацію атак і методів вбудови цифрового водяного знака. Крім того, визначено деякі проблеми в галузі цифрових водяних знаків для зображень.

У наш час спостерігається зростання кількості різноманітних електронних пристроїв, призначених для зберігання та обробки мультимедійних даних, такі як:

- смартфони;
- планшетні комп'ютери;
- вбудовані мультимедійні програвачі;
- фотоапарати з підтримкою Wi-Fi або Bluetooth;
- портативні жорсткі диски та флеш-накопичувачі;
- електронні книги з можливістю відтворення аудіо та відеофайлів;
- портативні геймінгові консолі;
- умовно-портативні компактні комп'ютери, такі як ноутбуки та нетбуки.

Разом з появою портативних пристроїв також з’являються ефективні методи стиснення мультимедійних даних. Це в сукупності з високошвидкісним інтернет-з'єднання, сприяло поширенню різноманітних програм та сервісів, що базуються на використанні цифрового контенту.

Незважаючи на те, що цифрові дані мають багато переваг порівняно з аналоговою версією, їх справжність або право власності на них є найбільшою проблемою. Цифрові мультимедійні дані можна легко дублювати та/або маніпулювати ними, що створює реальну загрозу неправомірного використання мультимедійних даних для власника контенту. Щоб вирішити проблему неправомірного використання мультимедійних даних в мережі Інтернет треба забезпечити надійність і оригінальність переданих мультимедійних даних. У світлі цих негативних факторів, в сучасній ері цифрових технологій стає важливим забезпечити захист мультимедійних даних від незаконного використання.

Сьогодні власники мультимедійного контенту шукають технології, здатні захистити їхні права та убезпечити контент від піратства, несанкціонованого використання, а також ті технології, що дають змогу відстежувати й засуджувати медіапіратів. За останні десятиліття дослідники запропонували різні рішення для захисту мультимедійних даних від несанкціонованого використання. Одним із рішень цієї проблеми є вбудова невидимих ідентифікаторів у вихідні мультимедійні дані для доказу їхньої приналежності. Цей тип методів називається приховуванням інформації, яке можна розділити на різні підкласи, такі як криптографія, стеганографія та водяні знаки [5, 6].

Криптографія – найпоширеніший метод захисту цифрових мультимедійних даних, де мультимедійний контент шифрують перед виданням, а ключ для розшифрування надають тим, хто придбав справжні або легальні копії [7, 8]. Однак криптографія не може допомогти контент-провайдерам контролювати вміст після процесу розшифрування; зловмисник може легко викрасти справжню або легальну копію, а потім перепродати її або розповсюдити безплатно в загальнодоступній мережі.

Стеганографія – це запобігання виявленню зашифрованих даних, які були захищені криптографічними алгоритмами. Однак повідомлення, приховане за допомогою стеганографії, не є надійним. До водяних знаків

порівняно з алгоритмами стеганографії висуваються додаткові вимоги щодо стійкості до різних атак, пов'язаних з обробкою сигналу та геометричними перетворенями. Тому вкрай важливо знайти спосіб захисту цифрового мультимедійного контенту за допомогою більш точного методу, який дав би змогу власникам контенту бути впевненими в розміщенні та поширенні своїх матеріалів в Інтернеті. Таким засобом може стати водяний знак.

1 ЗАГАЛЬНІ ВІДОМОСТІ СТЕГАНОГРАФІЇ ТА АНАЛІЗ СТАНУ СУЧАСНИХ ДОСЛІДЖЕНЬ В СФЕРІ СТЕГАНОГРАФІЇ

1.1 Сфери застосування водяних знаків

Методи вбудови цифрових водяних знаків мають багато застосувань, а саме:

- захист авторських прав: одним з причин розробки методів нанесення водяних знаків є захист авторських прав. У цьому випадку дані/інформація про авторське право вбудовуються в основний об'єкт без втрати якості [9]. Вбудовані дані перешкоджають іншим сторонам претендувати на право власності на ці дані. Крім того, водяний знак повинен бути відомий лише автору і повинен бути стійким до різних атак;

- прихована комунікація: методи нанесення водяних знаків також можуть використовуватися для прихованої передачі інформації, оскільки різні відомства або уряди встановлюють обмеження на використання шифрування. У цьому випадку люди можуть надсилати свої секретні повідомлення, використовуючи методи вбудови цифрових водяних знаків [10];

- контроль копіювання: ця функція обмежує незаконне копіювання матеріалів, захищених авторським правом, шляхом вбудови цифрового водяного знаку, який не можна копіювати, або обмеження кількості разів копіювання [11]. Наприклад, сьогодні в Інтернеті доступно багато документів, які не можна зберегти та роздрукувати, щоб контролювати незаконне копіювання;

- автентифікація вмісту: крихкий водяний знак може бути вбудований у зображення хоста для перевірки автентичності даних. Крихкий водяний знак вказує на те, чи були дані змінені, а також надає інформацію про те, де

ці дані були змінені [12]. Тому ця задача не вимагає надійного водяного знаку, оскільки нам потрібно лише виявити зміни;

- зчитування цифрового відбитка: метод зчитування цифрового відбитка, застосовується власником для того, щоб відстежити джерело нелегальних копій. Для цього власник може вбудовувати різні водяні знаки в кожну копію, яка розповсюджується серед різних клієнтів [13]. Наприклад, унікальні серійні номери присвоюються покупцям і використовуються для ідентифікації покупця;

- моніторинг трансляції: власники захищених авторським правом телепрограм повинні знати про нелегальну трансляцію або рекламу, що транслюється телеканалами в певний час і в певному місці відповідно до умов контракту. Водяні знаки можуть бути вбудовані в будь-який тип даних для трансляції в мережі автоматизованими системами, які здатні контролювати канали розповсюдження, щоб відстежувати контент у потрібний час і в потрібному місці [14];

- медична безпека: останнім часом телемедицина полегшує медичну діагностику, надсилаючи медичні дані/звіт пацієнта через загальнодоступну мережу для подальшого аналізу там, де доступне сучасне медичне обладнання. Це обладнання виробляє велику кількість даних щодня. Отже, необхідно захистити ці важливі дані. Нанесення водяних знаків на медичні зображення є підходящим методом для підвищення безпеки та автентифікації медичних даних, які використовуються для подальшої діагностики та довідок [15]. Вбудовані дата та ім'я пацієнта в медичні зображення можуть бути корисними заходами безпеки;

- індексування: Одним з відомих застосувань цифрових водяних знаків є індексування мультимедійного контенту, такого як фільми, новини, відеопошта, зображення тощо [16]. При цьому коментарі або будь-який тег/жанр вбудовуються у вміст таким чином, щоб ці коментарі або теги використовувалися будь-якою пошуковою системою для пошуку цього вмісту в Інтернеті.

1.2 Вимоги та особливості проектування методів вбудови цифрових водяних знаків

Існують різні аспекти проектування та вимоги, пов'язані з будь-яким методом нанесення водяних знаків, такі як прозорість, надійність, пропускна здатність, безпека тощо. Завданням дослідників у галузі нанесення водяних знаків є максимізація всіх цих параметрів для конкретного методу. Крім того, ці параметри взаємозалежні один від одного, як показано на рисунку 1.1.

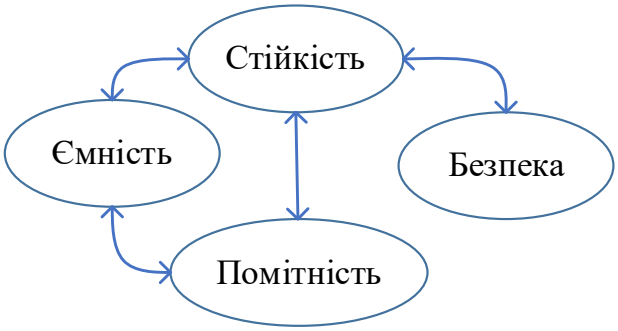

Рисунок 1.1 – Взаємна залежність між параметрами проектування

Три параметри, а саме: прозорість, стійкість та ємність обернено пропорційно пов'язані між собою, тобто, якщо прозорість методу водяних знаків зростає, то його стійкість погіршується, і навпаки. Цей взаємозв'язок зображено на рисунку 1.2.

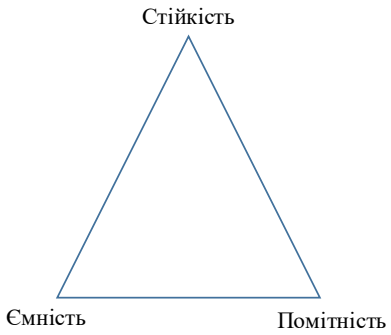

Рисунок 1.2 – Три основні суперечливі аспекти використання водяних знаків

Отже, відносна важливість цих параметрів залежить від конкретного застосування, як зазначено в попередньому розділі. Крім того, деякі програми вимагають більшої надійності у порівнянні з непомітністю. Таким чином, процес розробки методу нанесення водяних знаків включає в себе компроміс між суперечливими параметрами.

1.3 Систематизація атак на цифрові водяні знаки

Будь-яку процедуру, яка може знизити результативність методу нанесення водяних знаків, можна назвати атакою. Тестування стійкості та безпеки методу нанесення водяних знаків до атак є настільки ж важливим, як і процес розробки. Атаки не завжди видаляють або знищують водяний знак, але також унеможливлюють його виявлення. Спотворення, спричинені будь-якими атаками, погіршують функціонування методу нанесення водяних знаків.

Загалом, атаки на цифрові водяні знаки можна розділити на два класи, а саме: ненавмисні та навмисні атаки. Щоб досягти високої надійності виявлення цифрових водяних знаків, процес виявлення повинен бути стійким до змін у даних, спричинених як ненавмисними, так і навмисними атаками. Ненавмисні атаки відбуваються за допомогою операцій обробки сигналів над даними з цифровими водяними знаками, а саме: стиснення, друк, сканування, фільтрація, зашумлення, геометричні перетворення, обрізання тощо. Наприклад, мультимедійні дані зазвичай зберігаються у стислому форматі з втратами для того, щоб використовувати менше пам'яті. Ці алгоритми стиснення відкидають неважливі частини даних. Таке спотворення може призвести до пошкодження даних із вставленими водяними знаками. Це означає, що проста атака полягає в стисненні мультимедійних даних з втратами. Крім того, обертання або масштабування може змінити значення пікселів і знищити дані водяного знаку. Операції обробки сигналу, такі як квантування, декомпресія, повторна вибірка і зменшення кольору, можуть

зіпсувати водяний знак. У випадку навмисних атак, людина може цілеспрямовано атакувати вставлені дані цифрового водяного знаку, щоб скопіювати мультимедійні дані. В обох випадках будь-який метод нанесення цифрових водяних знаків повинен бути здатним виявити і витягти водяний знак після атаки. Таксономія різних навмисних і ненавмисних атак на методи нанесення водяних знаків наведена в таблиці 1.1.

Таблиця 1.1 – Систематизація атак на водяні знаки.

Атака	**Короткий опис**
Шум	Будь-який випадковий небажаний сигнал із заданим розподілом, а саме: гауссіан, «сіль і перець», Пуассона.
Фільтрація	Атаки типу фільтрації – це лінійна фільтрація, а саме: фільтрація нижніх/середніх частот, гауссова фільтрація, фільтрація з підвищенням різкості тощо.
Стиснення	Якщо цифровий водяний знак повинен протистояти різним рівням стиснення, зазвичай рекомендується виконувати вбудовування водяного знаку в той самий домен, де відбувається стиснення.
Множинні водяні знаки	Одним з рішень такого типу проблем є включення інформації про час нанесення ЦВЗ сертифікаційним центром
Геометричні атаки	Геометричні атаки спотворюють цифровий водяний знак шляхом просторових змін зображення. Найпоширенішими геометричними атаками є обертання, масштабування тощо.
Обрізання	Це дуже поширена атака, яка обрізає потрібну область від зображення з цифровим водяним знаком.

Продовження таблиці 1.1

Атаки на видалення водяних знаків і перешкоди	Мета таких атак – визначити або підмінити водяний знак.
Статистичне узагальнення	Метою таких атак є відновлення основного зображення та/або даних водяного знаку шляхом статистичного дослідження декількох наборів даних з водяними знаками.

Зазначимо, що з розвитком технологій захисту й аналізу цифрових даних, з'являються нові методи захисту від цих атак, а також нові способи їх виявлення та протидії.

1.4 Огляд підходів нанесення водяних знаків на зображення

Цифрове зображення може бути представлене/зберігатися або в просторово-часовій області, або в області перетворень. Зображення в просторово-часовій області характеризується пікселями, тоді як зображення в області перетворення описується в термінах його коефіцієнтів перетворення. Іншими словами, представлення зображення в області перетворення розділяє коефіцієнти перетворення на декілька частотних діапазонів. Для перетворення зображення в область перетворення можна використовувати різні доступні методи зворотнього перетворення, а саме: дискретне перетворення Фур'є (DFT), дискретне косинусне перетворення (DCT), дискретне вейвлет-перетворення (DWT), кероване пірамідальне перетворення (SPT) та інші. Кожен з цих методів перетворення має свої специфічні характеристики та представлення зображення.

Нанесення водяних знаків на цифрові зображення – це процес непомітного вбудовування водяного знаку (у вигляді підпису, випадкової послідовності або якогось зображення) в зображення (носій або обкладинку), який може бути використаний для перевірки автентичності його власника. Отримане в результаті цього процесу зображення називається зображенням з водяним знаком. Методи нанесення водяних знаків можуть виконуватися як у просторовій області, так і в області перетворень. У просторовому методі водяні знаки можуть бути вбудовані в зображення шляхом зміни значень пікселів або значень найменш значущих бітів (LSB). У той час як у методі на основі домену перетворення водяний знак може бути вбудований шляхом модифікації коефіцієнтів домену перетворення. Однак, більш стійкий водяний знак може бути вбудований в область перетворення зображень шляхом модифікації коефіцієнтів області перетворення порівняно з методом водяного маркування зображень на основі просторової області

Метод нанесення водяних знаків на основі просторового доменного підходу, приховує дані водяного знаку дані водяного знаку в значеннях пікселів основного зображення. Цей клас методів вносить незначні незначні зміни в інтенсивності пікселів основного зображення.

Одним з найпоширеніших прикладів такого методу є вбудовування водяного знаку в LSB пікселів зображення. Іншими словами, значна частина низькочастотних компонентів зображення повинна бути модифікована для того, щоб вставити дані водяного знаку надійним і стійким способом. Інший приклад: зображення розбивається на однакові за розміром блоки, і до підблоків додаються певні дані водяного знаку. Непомітність даних водяного знаку досягається на основі постулату, що біти LSB є візуально незначущими. Хоча метод просторових доменних водяних знаків може бути легко реалізований і дуже швидкий, він має багато недоліків. Ці методи дуже чутливі до звичайних операцій обробки сигналів і можуть бути легко порушені та послаблені. Наприклад, стиснення з втратами може повністю знищити дані водяного знаку. Таким чином, просторовий метод нанесення

водяних знаків дуже легко зруйнувати за допомогою деяких атак, таких як низькочастотна фільтрація, адитивний шум тощо. Іншими словами, методи просторового доменного водяного маркування зображень не є стійкими до звичайних операцій обробки сигналу на основному зображенні.

Області перетворення зображення – це просто інша форма представлення. Воно не змінює вміст, присутній у зображенні. Методи водяного маркування зображень на основі трансформованих доменів мають багато переваг над методами на основі просторових доменів . Як зазначено в літературі, методи водяного маркування зображень на основі трансформованих доменів є більш стійкими до різних атак на водяні знаки та операцій обробки сигналів, оскільки домен перетворення не використовує вихідне зображення для нанесення даних водяного знаку. Крім того, водяні знаки на основі домену перетворення розподіляють дані водяного знаку по всій частині основного зображення. Крім того, методи на основі перетворення доменів здатні вбудовувати більше бітів водяного знаку в основне зображення і є більш стійкими до атак.

1.5 Проблеми у сфері нанесення водяних знаків на зображення

Незважаючи на те, що було запропоновано багато різноманітних методів вбудови цифрових водяних знаків на зображення, але все ще існують певні проблеми, які потребують вирішення. Однією з головних проблем застосування водяних знаків є досягнення кращого компромісу між надійністю, прозорістю, пропускною здатністю та безпекою. Для того, щоб вирішити вищезгадану проблему (тобто знайти компроміс) для досягнення кращої продуктивності, багато дослідників представили її рішення для цієї проблеми в своїх роботах. Однак для того, щоб виправдати очікування індустрії, потрібні вдосконалення. Розглянемо деякі з найважливіших проблем, пов'язаних з нанесенням водяних знаків на зображення.

Більшість робіт у цій галузі за останнє десятиліття було присвячено захисту кольорових зображень або зображень у відтінках сірого (хост-зображень) шляхом вбудовування водяних знаків у відтінках сірого або бінарних зображень. Для вбудовування бінарного зображення або зображення у відтінках сірого потрібно перетворити його з кольорового, оскільки в мультимедіа використовується кольорові зображення. Однак, існує дуже мало методів, які вбудовують кольорові водяні знаки для захисту зображень [17-19]. З цієї точки зору, існує ще багато можливостей для вдосконалення в галузі водяних знаків зображень для вбудовування кольорового водяного знаку в кольорове основне зображення.

2. ОГЛЯД ВЕЙВЛЕТ ПЕРЕТВОРЕННЯ

2.1 Поняття про вейвлет

Вейвлет (wavelet – маленька хвиля) – це, у широкому сенсі слова, математична функція, що має вигляд хвильових пакетів тієї чи іншої форми, локалізованих по осі незалежної змінної і здатних до зсуву по ній і масштабування. Ця особливість виділяє вейвлети від базисних функцій перетворення Фур'є, які добре локалізовані у частотній області але не локалізовані зовсім у часовій, оскільки визначені на усій часовій області ( ). Одна з основних ідей вейвлет-представлення сигналів полягає в розбивці сигналу на дві складові – грубу (апроксимуючу) і деталізуючу – з подальшим їх дробленням з метою зміни рівня декомпозиції сигналу.

У вузькому сенсі вейвлети являють собою сукупність функцій, що утворюються за рахунок масштабування та зсувів основної, материнської функції (материнського вейвлету). Ці функції локалізовані по осі аргументів, інваріантні по відношенню до зсувів та лінійні до операцій масштабування. Саме за рахунок зміни масштабу вейвлети спроможні виявити ті чи інші особливості сигналу, а за рахунок зсувів проаналізувати сигнал в усіх точках, тобто провести частотно-часовий аналіз з виявленням локальних особливостей.

Вейвлети характеризуються чотирма принципово важливими властивостями:

- мають вигляд хвильових пакетів з нульовим значенням інтеграла тієї чи іншої форми, локалізованих у часі/просторі;
- мають можливість зсуву за часом;
- здатні до масштабування;
- мають обмежений частотний спектр.

Пряме вейвлет перетворення означає розкладання довільного вхідного сигналу на принципово новий базис у вигляді сукупності хвильових пакетів вейвлетів

2.2 Неперервне і дискретне вейвлет перетворення

При обробці даних на ПК може виконуватися дискретна версія вейвлет перетворення із заданими дискретними значеннями параметрів (a, b) вейвлетів з довільним кроком Δa і Δb. В результаті отримується надмірна кількість коефіцієнтів, що перевищую число відліків вихідного сигналу, яке не потрібно для реконструкції сигналів.

Дискретне вейвлет перетворення забезпечує достатньо інформації, як для аналізу сигналу, так і для його синтезу, будучи разом з тим економним по числу операцій і необхідного об'єму пам'яті.

Розглянемо простір 2LR( ) функцій x (t), визначених на усій дійсній осі $R \subset -\infty +\infty$ (;), та таких, які мають кінцеву по величині норму:

$$E_{f(t)} = \int_{-\infty}^{+\infty} |x(t)|^2 dt < \infty . \qquad (2.1)$$

Нехай базис функціонального простору $L^2(R)$ складається з системи зсувів та частотних перетворень (не обов'язково неперервних), деякої функції $\psi(t)$. Зміни незалежної частотної складової в спектральному представленні сигналу відображаються в часовому представленні у вигляді розтягнення або звуження функції за допомогою функції ψ (e) $\Rightarrow \psi$ (a^mt). Так само локальність функції забезпечується деякою незалежною змінною, що передбачає систему послідовних перекритів уздовж усієї дійсної осі, що виконується функцією виду $\psi(e) \Rightarrow \psi(t+k)$. Враховуючі ці умови, отримується наступна структура базисної функції:

$$\psi(a^m \cdot t + k). \tag{2.2}$$

Параметри m та k для зручності приймають цілими. При приведенні функції (2.2) до одиничної норми (2.3), отримаємо вираз базисної функції:

$$\|p(t)\| = \langle p(t), p(t) \rangle^{1/2}; \tag{2.3}$$

$$\psi_{mk}(t) = a^{m/2} \cdot \psi(a^m \cdot t + k). \tag{2.4}$$

Враховуючи вираз (2.11), вейвлет буде ортогональним, якщо сукупність функцій $\{\psi_{mk}(t)\}$ представляє собою ортонормований базис функціонального гільбертового простору $L^2(R)$, тобто:

$$\begin{cases} \int_{-\infty}^{+\infty} \psi_k(t) \cdot \overline{\psi_l(t)} dt = \delta_{kl} = 0, \ k \neq l \\ \int_{-\infty}^{+\infty} \left\{ |\psi_k(t)| \right\}^2 dt = \delta_{kl} = 1, \ k = l \end{cases}, \tag{2.5}$$

де δ_{kl} – дельта-функція Кронекера, що визначається так:

$$\delta_{kl} \begin{cases} 0, & якщо\ k \neq l \\ 1, & якщо\ k = l \end{cases}. \tag{2.6}$$

З виразу (2.7) слідує, що будь-яка функція гільбертового простору може бути представлена у вигляді ряду, тобто розкладена по базису:

$$x(t) = \sum_{m,k=-\infty}^{+\infty} C_{mk} \cdot \psi_{mk}(t) x(t) = \sum_{m,k=-\infty}^{+\infty} C_{mk} \cdot \psi_{mk}(t), \tag{2.7}$$

де C_{mk} – коефіцієнти представлення сигналу, тобто проекції сигналу на новий ортогональний базис функцій, що визначаються згідно виразу (2.8).

$$C_{mk} = \langle x(t), \psi_{mk}(t) \rangle = \int_{-\infty}^{+\infty} s(t) \cdot \psi_{mk} dt \,. \tag{2.8}$$

При цьому ряд (2.9) рівнобіжно сходиться, тобто:

$$\lim_{M,K \to \infty} \left\| x(t) - \sum_{m=-M}^{M} \sum_{k=-K}^{K} C_{mk} \cdot \psi_{mk}(t) \right\| = 0 \,. \tag{2.9}$$

Найпростішим прикладом ортогональної системи функцій є функції Хаара:

$$\psi(t) = \begin{cases} 1, \ t \in [0;0,5) \\ -1, \ t \in [0,5;1) \\ 0, \ t \notin [0;1) \end{cases} \,. \tag{2.10}$$

Під неперервним вейвлет-перетворенням (continuous wavelet transform – CWT) деякого сигналу x (t) $\in L^2$ (R) розуміють скалярний добуток цього сигналу та базисної функції

$$CWT_x^{\psi}(a,b) = \frac{1}{\sqrt{a}} \int_{-\infty}^{+\infty} f(t) \cdot \psi\left(\frac{t-b}{a}\right) dt \,, \tag{2.11}$$

параметри a та b визначають відповідно масштаб сигналу та розміщення у часі (зсув вейвлета). Причому велике значення параметра a >1 відповідає низьким частотам, розтягуючи вейвлет, а мале значення параметра a <1 – високим частотам, звужуючи вейвлет. Тому можна зробити висновок, що при фіксованому значенні параметра a значення (,) CWT є значенням згортки сигналу з розтягнутим або звуженим в a раз вейвлетом.

2.3 Перетворення Хаара

Вейвлет Хаара є одним з перших відомих ортогональних вейвлетів. Материнський вейвлет у нього має вигляд прямокутних імпульсів меандру. Його скейлінг функція має значення 1 в інтервалі [0,1] і 0 за межами цього

інтервалу. Вейвлети Хаара добре локалізовані в просторі, але не дуже добре локалізовані в частотній області, оскільки меандр має широкий спектр частот (рисунок 2.1).

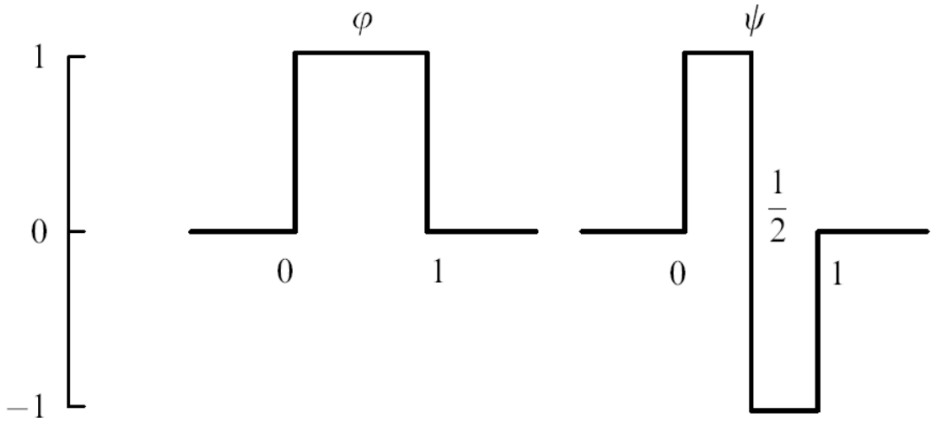

Рисунок 2.1 – Скейлінг та вейвлет функції вейвлета Хаара

Перетворення Хаара в загальному вигляді для одновимірного сигналу виглядає наступним чином. Нехай є одновимірний дискретний сигнал S. Кожній парі елементів з індексами j 2k , і j 2k +1 , j k, ∈ Ж , поставимо у відповідність два значення:

$$a_{j,k} = \frac{s_{j,2k} + s_{j,2k+1}}{2}, \quad d_{j,k} = \frac{s_{j,2k} - s_{j,2k+1}}{2}, \tag{2.12}$$

де aj і dj – вейвлет коефіцієнти сигналу s.

2.4 Перетворення Добеші

Вейвлети Добеші – сімейство ортогональних вейвлетів з компактним носієм, який обчислюється ітераційним шляхом. Вони були названі в честь математика з США, яка перша побудувала дане сімейство, Інгрід Добеши.

На рисунку 2.2. наведено скейлінг та вейвлет функції вейвлета Добеші.

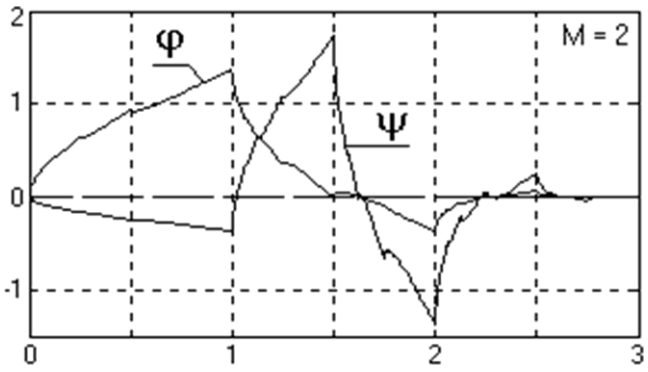

Рисунок 2.2 – Скейлінг та вейвлет функції вейвлета Хаара

Для побудови вейвлетів використовуються скейлінг функція та функція вейвлету:

$$\phi(t) = \sqrt{2}\sum_k h_k \phi(2t-k)$$
$$\psi(t) = \sqrt{2}\sum g_k \phi(2t-k) \quad . \qquad (2.13)$$

Компактність носія функцій і ψ може бути досягнута, якщо буде вибрано кінцеве число hn ≠ 0 таким чином, щоб була досягнута ортогональность і гладкість вейвлета, або щоб виконувалася умова моментів. Для області Фур'є умова ортогональності і гладкості виглядає наступним чином:

$$\left|m_0(\omega)\right|^2 + \left|m_0(\omega+\pi)\right|^2 = 1 \qquad (2.14)$$

Вейвлети Добеші відносяться до класу квадратурних зеркальних фільтрів. Особливістю цього класу є те, що фільтр високих частот отримується з відповідного фільтру низьких частот методом перестановки його коефіцієнтів у зворотному порядку і зміною знаку половини з них (парних чи непарних). Таким чином вейвлет являє собою ФВЧ а відповідний ФНЧ описується масштабною функцією

Нехай, наприклад, фільтр має носій довжиною 4 (тобто описується чотирма коефіцієнтами в дискретному випадку). Уявімо сигнал у вигляді вектора довжиною N, де N – кількість відліків. Тоді процес перетворення сигналу можна записати в матричному вигляді.

Вейвлети Добеші мають наступну властивість: як згладжені уявлення сигналу, так і його локальні особливості мають надмірність в два рази, тобто для вейвлета довжиною 2N результат перетворення сигналу в кожній точці є деякий "усереднення" сигналу і набір "деталей", що відрізняють вихідний сигнал від усередненого – причому усереднений сигнал є в 2 рази "більш гладким", ніж вихідний. Таким чином, кожен парний або кожен непарний відлік перетворення може бути виключений з розгляду, і в результаті перетворення виходять два вектора 42 вдвічі меншої довжини, один з яких містить згладжену версію сигналу, а інший – набір локальних особливостей. З урахуванням сказаного, можна виконувати перетворення сигналу не в кожній його точці, а тільки в тих, які будуть брати участь у подальшому розгляді, тобто тільки в парних або тільки в непарних. Тобто згортка обчислюється в половині точок, але в обчисленні беруть участь всі M послідовних точок, де M – довжина фільтра. Тоді матриця перетворення матиме розмірність (N / 2) × N (N- парне).

3 ІНСТРУМЕНТИ МОДЕЛЮВАННЯ НА PYTHON

3.1 Середовище розробки

Код на python може бути поміщений у файл із розширенням .py та надісланий інтерпретатору для виконання, це класичний підхід, який зазвичай розбавляється використанням середовища розробки, наприклад pyCharm. Однак, для python (і не тільки) існує інший спосіб взаємодії з інтерпретатором – інтерактивні блокноти jupyter, які зберігають проміжний стан програми між виконанням різних блоків коду, що можуть бути виконані в довільному порядку. Цей спосіб взаємодії запозичений у блокнотів Mathematica, пізніше аналог з'явився і в MATLAB (Live script).

Jupyter – це проєкт і спільнота, метою якої є «розробка програмного забезпечення з відкритим кодом, відкритих стандартів та служб для інтерактивних обчислень на десятках мов програмування». Його виділили з IPython у 2014 році Фернандо Перес та Браян Грейнджер. Назва Project Jupyter є посиланням на три основні мови програмування, які підтримує Jupyter, а саме: Julia, Python і R. Це також данина пам'яті записникам Галілея, в яких записані відкриття супутників Юпітера. Проєкт Jupyter розробив і підтримує інтерактивні обчислювальні продукти Jupyter Notebook, JupyterHub і JupyterLab. Jupyter фінансується NumFOCUS.

Jupyter Notebook може підключатися до багатьох ядер, щоб дозволити програмування різними мовами. Ядро Jupyter – це програма, відповідальна за обробку різних типів запитів (виконання коду, автодоповнення коду, перевірка) та надання відповіді. Ядра спілкуються з іншими компонентами Jupyter за допомогою ZeroMQ і, таким чином, можуть бути на тих самих або віддалених машинах. На відміну від багатьох інших інтерфейсів, подібних до ноутбуків, у Jupyter ядра не знають, що вони прикріплені до певного документа, і можуть бути підключені до багатьох клієнтів одночасно.

Зазвичай ядра дозволяють писати лише на одній мові, але є кілька винятків. За замовчуванням Jupyter Notebook постачається з ядром IPython. Станом на випуск 2.3 (жовтень 2014 р.) існує 49 ядер, сумісних з Jupyter, для багатьох мов програмування, включаючи Python, R, Julia та Haskell.

Блокнот Jupyter можна конвертувати в ряд відкритих стандартних вихідних форматів (HTML, презентаційні слайди[en], LaTeX, PDF, ReStructuredText, Markdown, Python) за допомогою «Download as» у веб-інтерфейсі та бібліотеки nbconvert[17] або інтерфейсу командного рядка «jupyter» nbconvert. Щоб спростити візуалізацію документів блокнота Jupyter в Інтернеті, бібліотека nbconvert[18] надається як послуга через NbViewer[19], яка може отримати URL-адресу будь-якого загальнодоступного документа блокнота, одразу ж перетворюючи його в HTML, та відобразити на користувача.

Інтерфейс блокнота був доданий до IPython у випуску 0.12 (грудень 2011 р.), перейменований на блокнот Jupyter у 2015 р. (IPython 4.0 – це Jupyter 1.0). Jupyter Notebook схожий на notebook-інтерфейси інших програм, таких як Maple, Mathematica і SageMath, стиль обчислювального інтерфейсу, який виник з Mathematica у 1980-х роках. Інтерес Jupyter наздогнав популярність інтерфейсу Mathematica notebook на початку 2018 року.

JupyterLab – це новіший інтерфейс користувача для Project Jupyter. Він пропонує будівельні блоки класичного блокнота Jupyter (ноутбук, термінал, текстовий редактор, браузер файлів, розширені вихідні дані тощо) у гнучкому інтерфейсі користувача. Перший стабільний випуск було оголошено 20 лютого 2018 року.

3.2 Візуалізація даних

Бібліотека аналізу даних Python також може бути використана для візуалізації даних . Вона дозволяє створювати прості графіки, такі як

діаграми розсіювання та лінійні діаграми, забезпечуючи значну гнучкість у налаштуванні. Python Pandas – популярна бібліотека з відкритим вихідним кодом для аналізу та маніпулювання даними. Вона надає ефективні та потужні інструменти для роботи зі структурованими даними, включаючи очищення, попередню обробку та перетворення даних. Python Pandas допомагає в дослідженнях у кількох напрямках, включаючи аналіз даних: Python Pandas дозволяє дослідникам легко аналізувати великі обсяги даних, включаючи фільтрацію, агрегування та узагальнення даних. Це особливо корисно у фінансах, охороні здоров'я та соціальних науках, де великі масиви даних часто аналізуються для виявлення закономірностей, тенденцій та взаємозв'язків. Візуалізація даних: Python Pandas надає інструменти для створення візуалізацій даних, включаючи графіки, діаграми та діаграми. Ці візуалізації допомагають дослідникам краще зрозуміти свої дані та донести свої висновки до інших. Аналіз часових рядів: Python Pandas має потужний набір інструментів для роботи з даними часових рядів, включаючи індексування на основі часу, повторну вибірку та операції з рухомим вікном. Це робить його цінним інструментом для дослідників у таких галузях, як фінанси та економіка . Очищення та попередня обробка даних: Python Pandas надає широкий спектр функцій для очищення та попередньої обробки даних, включаючи роботу з відсутніми даними, видалення дублікатів та перетворення даних.

Це допомагає дослідникам підготувати свої дані до аналізу та забезпечити їхню точність і якість. Інтеграція з іншими бібліотеками: Python Pandas добре інтегрується з популярними бібліотеками для аналізу даних та машинного навчання, такими як NumPy, Scikit-learn та Matplotlib. Це дозволяє дослідникам легко використовувати Python Pandas у більш широкому дослідницькому конвеєрі. Python Pandas допомагає дослідникам, надаючи ефективні та потужні інструменти для аналізу, візуалізації та маніпулювання даними. Його універсальність і простота використання роблять його цінним інструментом для дослідників у різних галузях .

Базовий пакет для наукових обчислень Python підтримує великі багатовимірні масиви та матриці, а також набір високорівневих математичних функцій для швидкого виконання цих функцій . Python NumPy (Numerical Python) – популярна бібліотека для наукових обчислень мовою Python. Вона надає потужний об'єкт N-вимірного масиву та інструменти для роботи з масивами. NumPy широко використовується в дослідженнях для різних застосувань, включаючи аналіз даних, обробку зображень, машинне навчання тощо. Ось кілька прикладів того, як NumPy допомогла в дослідженнях: Аналіз даних: Масиви NumPy забезпечують швидкий та ефективний спосіб виконання операцій над великими наборами даних. Дослідники можуть використовувати NumPy для маніпулювання, фільтрації та аналізу даних, що робить його важливим інструментом для аналізу даних у фінансах, економіці та біології. Обробка зображень: Масиви NumPy також використовуються для представлення та маніпулювання зображеннями. Дослідники можуть використовувати NumPy для застосування фільтрів, перетворень та інших операцій над зображеннями, що робить його цінним інструментом в астрономії, медичній візуалізації та комп'ютерному зорі.

Машинне навчання: Масиви NumPy є основою багатьох бібліотек машинного навчання на Python. Дослідники можуть використовувати NumPy для представлення та маніпулювання наборами даних, а також для виконання обчислень над цими наборами, що робить його важливим інструментом для досліджень у галузі машинного навчання.

Математичне моделювання: NumPy надає широкий спектр математичних функцій та інструментів для чисельної оптимізації, що робить його цінним інструментом для математичного моделювання. Дослідники можуть використовувати NumPy для моделювання складних систем та аналізу їхньої поведінки, що робить його важливим інструментом у фізиці, інженерії та хімії. Python NumPy є цінним інструментом для дослідників у різних галузях. Його здатність виконувати швидкі та ефективні операції над великими масивами даних, маніпулювати зображеннями, підтримувати

машинне навчання та надавати інструменти математичного моделювання зробила його важливою бібліотекою для наукових обчислень на Python.

Модуль Python для машинного навчання, який побудований на основі SciPy і поширюється за ліцензією 3-Clause BSD. Він широко використовується для створення предиктивних моделей на Python і надає інструменти для попередньої обробки даних, вибору моделі та оцінки моделі. Python Scikit-learn - популярна бібліотека машинного навчання з відкритим вихідним кодом, яка надає різні інструменти для інтелектуального аналізу даних. Вона широко використовується в дослідженнях для вирішення складних завдань, від класифікації зображень і текстів до регресії та кластеризації. Ось кілька способів, якими Python Scikit-learn допоміг у дослідженнях: Спрощена попередня обробка даних: Scikit-learn надає кілька інструментів для попередньої обробки даних, таких як імпутація даних, масштабування ознак та вилучення ознак. Це дозволяє дослідникам ефективно очищати і готувати дані для аналізу, який часто займає багато часу і є складним. Потужні алгоритми машинного навчання: Scikit-learn включає багато алгоритмів машинного навчання, таких як дерева рішень, випадкові ліси, машини опорних векторів і нейронні мережі.

Дослідники можуть використовувати ці алгоритми для побудови прогностичних моделей, які можуть бути використані для вирішення різноманітних дослідницьких завдань. Перехресна перевірка та вибір моделі: Scikit-learn надає інструменти для вибору моделі та перехресної перевірки, що дозволяє дослідникам оцінити ефективність своїх моделей і вибрати найкращу для конкретного завдання. Ефективне розгортання моделі: Scikit-learn надає інструменти для серіалізації та розгортання, що дозволяє дослідникам легко розгортати свої моделі у виробничих середовищах. Python Scikit-learn полегшив дослідження в різних галузях, таких як біологія, фінанси, соціальні науки та багато інших, надавши широкий спектр ефективних і простих у використанні інструментів машинного навчання.

Найвідомішою бібліотекою для візуалізації даних є Python. Це низькорівнева бібліотека, яка надає широкий спектр настроюваних 2D і 3D графіків, включаючи діаграми розсіювання, лінійні графіки, гістограми тощо. Matplotlib побудована на масивах NumPy і має високу сумісність з іншими бібліотеками Python, такими як Pandas, NumPy та sci-kit-learn. Вона також має інтерактивне середовище, яке можна використовувати на різних платформах. Matplotlib широко використовується в дослідженнях як потужний інструмент візуалізації даних, що дозволяє дослідникам ефективно представляти свої результати. Деякі способи, якими Matplotlib допоміг у дослідженнях, включають Візуалізація складних даних: Matplotlib надає широкий спектр варіантів візуалізації, включаючи лінійні діаграми, діаграми розсіювання, гістограми, теплові карти тощо. Це дозволяє дослідникам створювати візуалізації, які легко передають складні дані і тенденції. Інтерактивність: Matplotlib дозволяє створювати інтерактивні візуалізації, якими можна маніпулювати в режимі реального часу, що дає змогу дослідникам вивчати дані та виявляти закономірності і тенденції. Відтворюваність: Matplotlib надає можливість створювати візуалізації публікаційної якості, які можна легко відтворювати в наукових роботах, презентаціях та інших матеріалах. Інтеграція з Python: Matplotlib – це бібліотека Python, яку можна легко інтегрувати з іншими інструментами та пакетами Python, такими як NumPy, Pandas та SciPy. Matplotlib відіграє значну роль у допомозі дослідникам аналізувати та повідомляти про свої результати за допомогою ефективної візуалізації даних.

4 НАНЕСЕННЯ ВОДЯНИХ ЗНАКІВ НА ЦИФРОВІ ЗОБРАЖЕННЯ ЗА ДОПОМОГОЮ КЕРОВАНОГО ПІРАМІДАЛЬНОГО ПЕРЕТВОРЕННЯ НА ЗОБРАЖЕННЯ З ВОДЯНИМИ ЗНАКАМИ В ГРАДАЦІЯХ СІРОГО

4.1 Кероване пірамідальне перетворення (SPT)

Найпершою успішною мультимасштабною, мультиорієнтаційною декомпозицією зображення є SPT, запропонована Фріменом та Адельсоном . SPT – це вейвлетоподібна ілюстрація, функції якої є масштабованими і поверненими редакціями одного спрямованого вейвлету. Керованість – це властивість, при якій фундаментальні вейвлети можуть бути повернуті в будь-яку орієнтацію шляхом появи відповідних лінійних груп з первинного набору рівнокутних спрямованих вейвлет-компонентів. Ця властивість використовується в SPT для знаходження напрямку базисної функції зображення. SPT розкладає вхідне зображення на набір підсмуг різної орієнтації. На рисунку 4.1 зображено блок-схему декомпозиції вхідного зображення, що складається з трьох типів фільтрів: низькочастотного (L0), високочастотного (H0) та банку смугових фільтрів (B_0, ..., B_k). Тут k – порядок базисних функцій керованої піраміди, а k+1 – орієнтації. Вхідне зображення поділяється на підсмуги високих і низьких частот за допомогою фільтрів високих і низьких частот відповідно. Кожна підсмуга низьких частот знову поділяється на k+1 орієнтованих підсмуг і підсмугу низьких частот. Нарешті, субдискрети створюються з коефіцієнтом 2, а потім виконується подальша декомпозиція.

4.2 Запропонований метод

Запропонований метод використовує некорельований колірний простір для покращення якості та стійкості методів нанесення водяних знаків. Цей

метод вбудовує зображення сірої шкали водяного знаку в кольорове основне зображення шляхом модифікації розкладених SPT-коефіцієнтів основного зображення. Водяний знак додається до кожного кольорового каналу основного зображення, що підвищує надійність процесу вилучення та захист від поширених атак на обробку сигналів. Запропонований метод складається з п'яти етапів, а саме: попередня обробка основного зображення та водяного знаку, вбудовування водяного знаку, постобробка зображення, вилучення водяного знаку та покращення продуктивності за допомогою ГА. На рисунку 4.2 показано базову структурну схему запропонованого методу. Деталі кожного етапу запропонованого методу описано в наступних розділах.

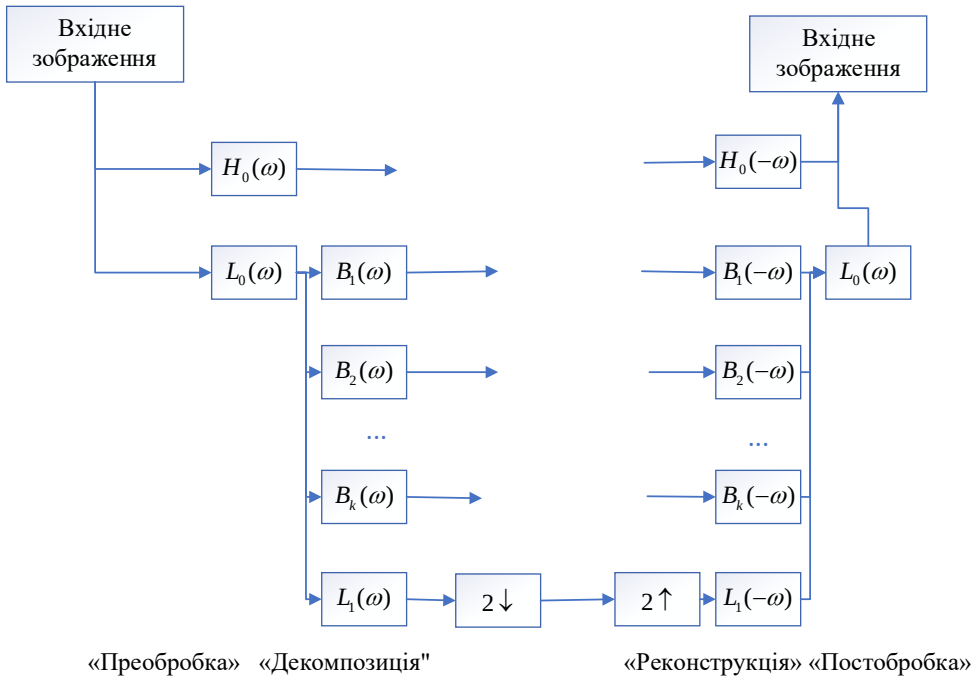

Рисунок 4.1 – Блок-схема для керованої пірамідальної декомпозиції зображення

4.2.1 Попередня обробка зображень

Попередня обробка зображення змінює кольорове RGB зображення (H) на кольорове зображення UCS , використовуючи рівняння (4.1), і генерує три незалежні компоненти зображення, а саме: H_U, H_C та H_S.

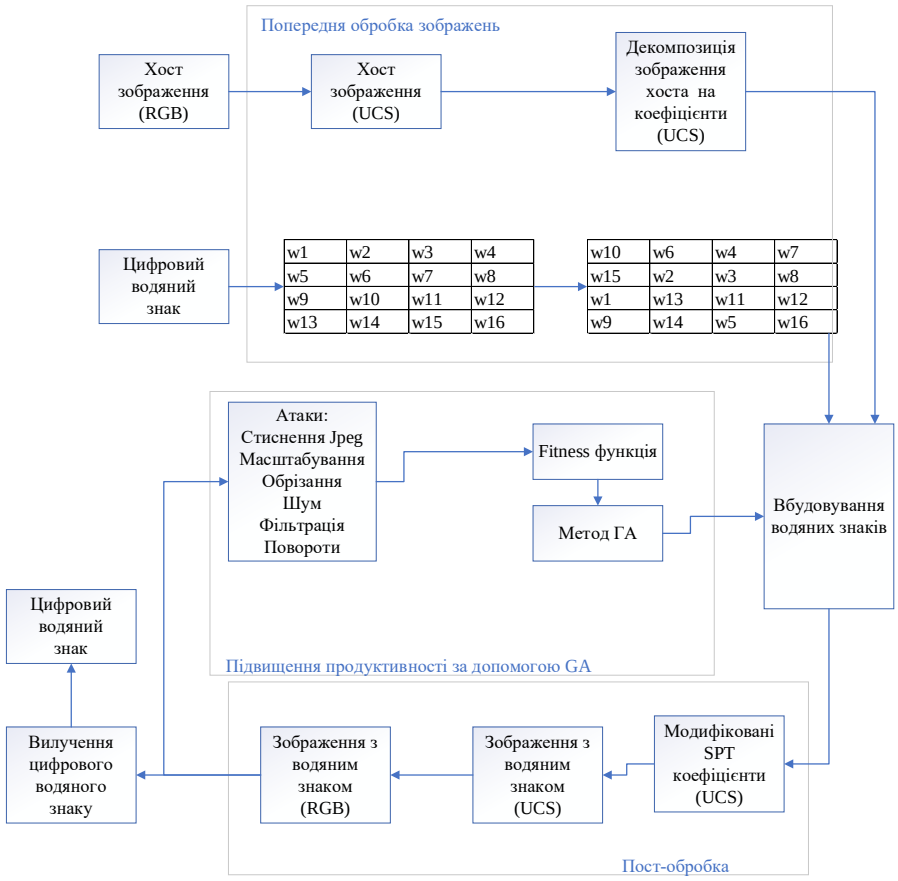

Рисунок 4.2 – Структурна схема запропонованого методу

$$\begin{bmatrix} H_u(x,y) \\ H_c(x,y) \\ H_x(x,y) \end{bmatrix} = W_u \begin{bmatrix} H_r(x,y) \\ H_g(x,y) \\ H_b(x,y) \end{bmatrix}, \tag{4.1}$$

де W_U обчислюється шляхом факторизації коваріаційної матриці C за допомогою аналізу головних компонент (PCA) у наступному вигляді:

$$C = W_u^t \Lambda W_u, \tag{4.2}$$

де W_u^t та Λ – ортогональна матриця власних векторів та діагональна матриця власних значень з діагональними елементами в порядку спадання, відповідно. Далі з водяного знаку генеруються 16 підобластей, що не перетинаються, як показано на рисунку 4.2. Ці підобласті водяного знаку потім переставляються або зашифровуються за допомогою певної

попередньо визначеної послідовності або ключа. Це підвищує рівень безпеки і змушує користувача використовувати ключ для вилучення зображення з водяним знаком. Далі, третій рівень декомпозиції застосовується до кожного компонента зображення хоста. Отримані в результаті коефіцієнти SPT третього рівня, H_{k3}, вибираються для процесу вбудовування, k = {1, 2, 3, ..., 16}.

4.2.2 Вбудова цифрових водяних знаків

Після етапу попередньої обробки зашифрований водяний знак вбудовується в SPT-коефіцієнти основного зображення (H_{k3}). Для того, щоб підвищити надійність та стійкість запропонованого методу до зловмисних атак, бажано приховати зображення водяного знаку у всіх колірних компонентах коефіцієнтів хоста. Тому низькочастотні деталі коефіцієнтів третього рівня розбиваються на 16 областей, що не перекриваються. Тепер зашифрований водяний знак вбудовується в низькочастотні деталі розкладених коефіцієнтів третього рівня основного зображення у всіх його колірних каналах за допомогою рівняння (4.3).

$$H_{w_{k3}}(x,y) = H_{k3}(x,y) = \alpha(r) W_p(x,y), \quad k, p, r = \{1,2,3,...,16\} \tag{4.3}$$

де, k представляє підобласті основного зображення, p – цільовий блок водяного знаку, а α позначає силу модифікації, зробленої в коефіцієнтах основного зображення.

4.2.3 Постобробка та вилучення цифрових водяних знаків

Після вбудовування зображення водяного знаку у відповідні коефіцієнти основного зображення SPT, для коефіцієнтів основного

зображення з водяним знаком застосовується обернене SPT (ISPT), яке повертає зображення з водяним знаком у колірному просторі UCS. Нарешті, зображення з водяними знаками UCS перетворюється в колірний простір RGB.

Процес вилучення водяного знаку потребує зображення з водяним знаком і заздалегідь визначеного ключа для вилучення водяного знаку. Зображення з водяним знаком RGB перетворюється в колірний простір UCS, а потім застосовується SPT-розкладання по кожному каналу. Для отримання зображення з водяним знаком застосовується зворотний процес вбудовування, як показано на рисунку 4.2, і витягується водяний знак за допомогою рівняння (4.4). Нарешті, зашифрований водяний знак переставляється у вихідну послідовність, використовуючи попередньо визначений ключ.

$$\hat{W}_p(x,y) = \frac{H_{k3}(x,y) - H_{W_{k3}}(x,y)}{\alpha(r)} \qquad (4.4)$$
$$k, p, r = \{1,2,3,...,16\}$$

4.2.4 Підвищення продуктивності за допомогою ГА

Зображення H_{Wk3} з водяними знаками піддається різним атакам, які погіршують ефективність методів нанесення водяних знаків. Існує два параметри, а саме: якість і стійкість, які повинні бути максимізовані для методу водяних знаків, але ці параметри обернено пропорційні один одному, тобто, якщо якість зростає, стійкість страждає, і навпаки. У цьому методі оптимальні значення цих параметрів залежать від відповідних значень коефіцієнта стійкості (α). Тому в цьому методі використовується метод ГА-оптимізації для вибору значень α, які оптимізують якість і надійність з точки зору фітнес-функції. У цьому методі використовується 16 коефіцієнтів

міцності, оптимізовані значення яких обчислюються шляхом мінімізації наступної функції пристосованості за допомогою ГА.

$$Fitness = \frac{100}{CPSNR} = 2 \times \sum_{Q=60\%}^{90\%} [1 - NC_{jpg(Q)}] + \sum_{Q=10\%}^{50\%} [1 - NC_{jpg(Q)}] + \sum_{i=1}^{3} [1 - NC_{filter(i)}] + \sum_{i=1}^{3} [1 - NC_{scale(i)}] + \sum_{i=1}^{3} [1 - NC_{noise(i)}] \sum_{i=1}^{4} [1 - NC_{crop(i)}] + [1 - NC_{rotation}] , \quad (2.5)$$

де, CPSNR – композитне пікове відношення сигнал/шум, а NC – нормалізована кореляція. Ці величини обчислюються шляхом застосування згаданих атак до маркованого зображення. Метод ГА виконується протягом 200 ітерацій для обчислення оптимальних значень коефіцієнтів підсилення (α).

4.3 Результати експерименту

Для порівняння ефективності запропонованого та розглянутого методів нанесення водяних знаків на зображення два популярних 24-бітних кольорових RGB-зображення, а саме lena та mandrill розміром 512 × 512 кожне, а також два зображення у відтінках сірого, а саме: логотип NURE та зображення літака розміром 64 × 64, логотип NURE та зображення літака розміром 64 × 64 використовуються як зображення водяних знаків для вбудовування їх в основні зображення, як показано на рисунку 4.3. Всі розглянуті зображення були взяті з бази даних зображень USC-SIPI [112], за винятком логотипу NURE який взято з сайту Харківського національного університету радіоелектроніки.

Рисунок 4.3 – Зображення хосту у форматі RGB lena, mandrill та зображення водяних знаків у сірій шкалі Nure, aeroplen

Ефективність запропонованого методу порівнюється з класичним методом DWT та ГА використовуються для підвищення якості та робастності методу нанесення водяних знаків на зображення. Для порівняння об'єктивного тесту та для оцінки якості отриманих зображень з водяними знаками за допомогою запропонованого методу було розраховано параметри ефективності CPSNR, які наведено в таблиці 4.1.

Таблиця 4.1 – Порівняння значень CPSNR

	Використаний водяний знак	Зображення з водяними знаками	Метод на основі DWT	Запропонований метод на основі SPT
1	Nure	Lena	35.92	37.23
2	Nure	Mandrill	35.67	36.87
3	Aeroplane	Lena	35.61	37.11
4	Aeroplane	Mandrill	35.59	36.08

З таблиці 4.1 видно, що всі методи підтримують якість зображення з водяними знаками з точки зору CPSNR (> 35 дБ). Однак, запропонований метод показує кращі результати з точки зору CPSNR порівняно з методом на основі DWT.

Стійкість запропонованих методів було перевірено шляхом застосування різних атак на зображення з водяними знаками. А саме з атак на

фільтрацію (середнє значення, медіана), шум (гауссівський, пуассонівський, сіль та перець), стиснення JPEG, обертання, масштабування та обрізання. Атаки застосовано до всіх чотирьох зображень з водяними знаками, які містять логотип Nure атак та зображенням літака наведено в таблиці 4.2.

Таблиця 4.2 – Порівняння стійкості за значеннями (NC), отриманими після застосування атак на зображення з водяними знаками

Атаки		NURE				Aeroplane			
		lena		Mandrill		lena		Mandrill	
		Метод на основі DWT	Запропонований метод на основі SPT	Метод на основі DWT	Запропонований метод на основі SPT	Метод на основі DWT	Запропонований метод на основі SPT	Метод на основі DWT	Запропонований метод на основі SPT
1	Медіанна фільтрація (3 × 3)	0.76	0.79	0.75	0.80	0.75	0.78	0.74	0.74
2	Фільтрація у вигляді сітчастого фільтра (3 × 3)	0.92	0.93	0.90	0.90	0.91	0.92	0.89	0.91
3	Середня фільтрація (3 × 3)	0.99	0.98	0.97	0.98	0.98	0.98	0.96	0.97
4	Гауссівський шум (0.006)	0.87	0.91	0.85	0.86	0.86	0.87	0.84	0.87
5	Пуассонівський шум	0.88	0.94	0.86	0.90	0.87	0.88	0.85	0.90
6	Шум солі та перцю	0.96	0.97	0.94	0.96	0.95	0.96	0.93	0.94
7	Стиснення JPEG (10%)	0.71	0.72	0.70	0.71	0.70	0.71	0.69	0.70
8	Стиснення JPEG (90%)	0.88	0.88	0.86	0.88	0.87	0.90	0.85	0.86
9	Поворот (1 градус)	0.96	0.97	0.95	0.96	0.95	0.97	0.93	0.94
10	Масштабування (0.6)	0.98	0.98	0.96	0.98	0.97	0.98	0.95	0.96
11	Масштабування (0.9)	0.98	0.98	0.97	0.98	0.98	0.98	0.96	0.97
12	Масштабування (1.2)	0.99	0.98	0.97	0.98	0.98	0.98	0.96	0.97
13	Обрізання (10%)	0.96	0.97	0.94	0.95	0.95	0.96	0.93	0.94
14	Обрізання (20%)	0.84	0.90	0.83	0.89	0.84	0.86	0.82	0.83
15	Обрізання (30%)	0.74	0.79	0.73	0.73	0.73	0.73	0.72	0.73
16	Обрізання (40%)	0.62	0.63	0.61	0.62	0.61	0.62	0.61	0.62

З таблиці 4.2 видно, що стійкість зображень з водяними знаками, вбудованими в логотип NURE, має більш високі значення NC порівняно із зображенням літака, що пов'язано з більшою грубістю зображення літака порівняно з логотипом NURE. Крім того, це можна зробити висновок з рисунків 4.4 та 4.5, на яких зображено витягнуті запропонованим методом водяні знаки логотипу NURE та зображення літака відповідно для всіх розглянутих атак. Таким чином, результати підтверджують, що запропонований метод з використанням SPT дає високоякісні та більш стійкі зображення з водяними знаками і може бути використаний для автентифікації контенту з метою захисту зображень, захищених авторським правом. Порівняльні результати показують, що запропонований метод перевершує інші методи для всіх розглянутих атак.

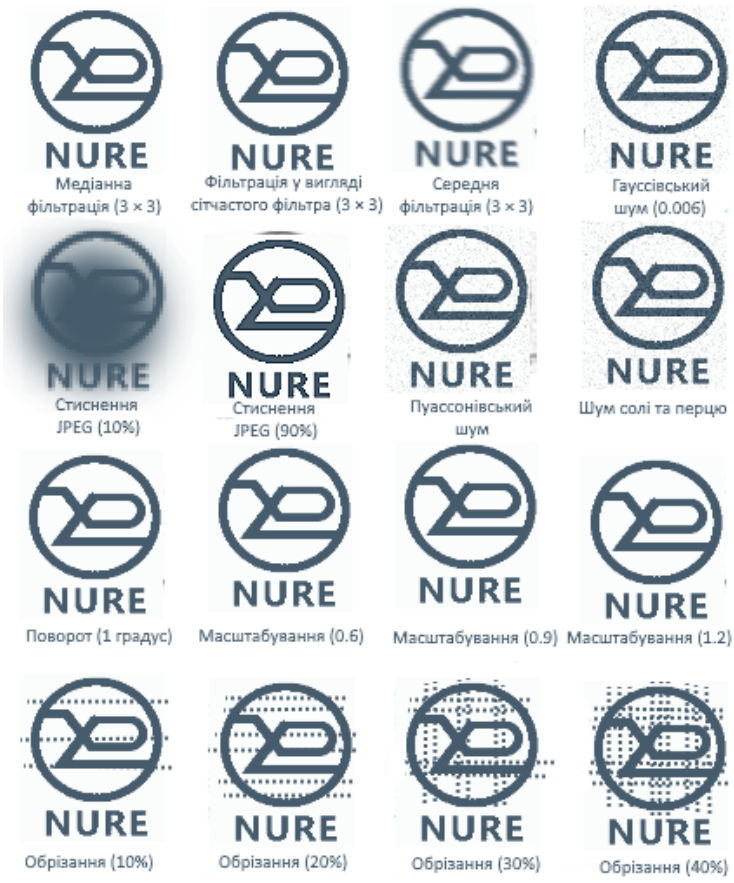

Рисунок 4.4 – Витягнуті водяні знаки логотипу NURE запропонованим методом після застосування розглянутих атак

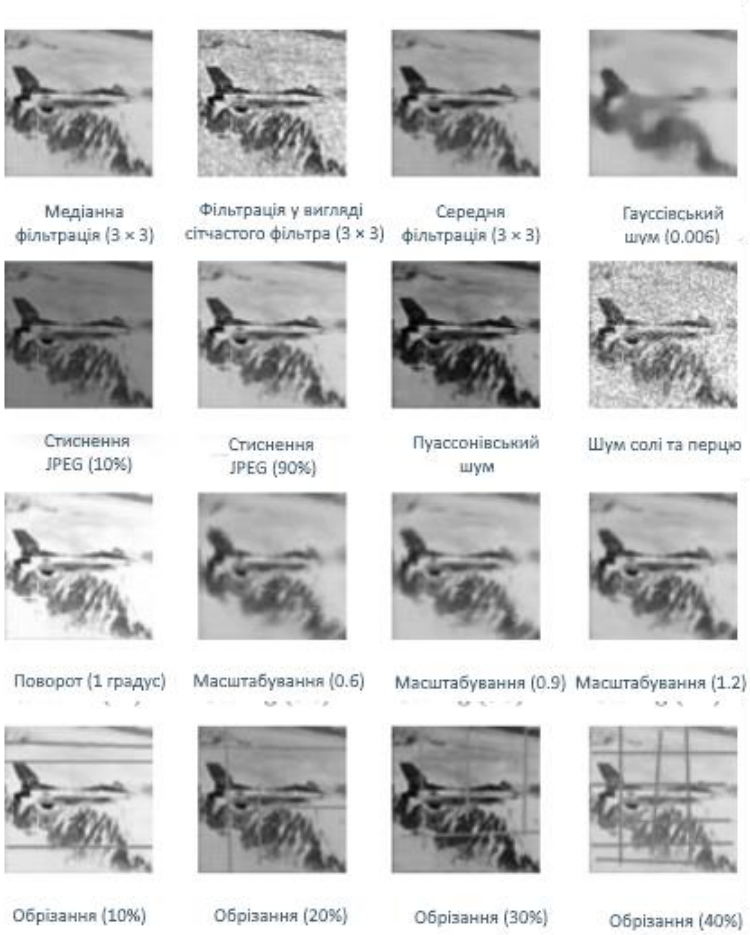

Рисунок 4.5 – Вилучені водяні знаки зображень літаків запропонованим методом після застосування розглянутих атак

В роботі представлено метод водяного маркування зображень на основі SPT з використанням UCS та ГА. Некорельований колірний простір збільшує ефективне використання всіх колірних каналів зображення порівняно з корельованими колірними просторами, в той час як ГА оптимізує коефіцієнти надійності та покращує якість і стійкість запропонованого методу. Результати підтверджують, що запропонований метод з використанням SPT та UCS є кращим за існуючі методи, які базуються на DWT, за всіма розглянутими параметрами продуктивності. Таким чином, зроблено висновок, що метод на основі SPT з використанням UCS є кращим порівняно з DWT.

ВИСНОВКИ

У цій роботі зроблено спробу визначити проблеми, пов'язані з нанесенням водяних знаків на кольорові зображення для їх захисту. У цій кваліфікаційній роботі було досліджено метод нанесення цифрових водяних знаків на цифрові зображення за допомогою пірамідального перетворення. Проведений аналіз та експериментальні дослідження дозволили зробити наступні висновки:

- пірамідальне перетворення є потужним інструментом для багатошарового представлення зображень, що дозволяє ефективно приховувати інформацію у високочастотних компонентах зображення;

- використання цього перетворення сприяє підвищенню стійкості цифрових водяних знаків до різноманітних атак, таких як масштабування, поворот, додавання шуму та інші обробки зображень;

- проведені експерименти показали, що метод нанесення водяних знаків за допомогою пірамідального перетворення дозволяє зберегти високу якість зображення. Спотворення зображення, спричинені вбудовуванням водяного знака, є майже непомітними для людського ока;

- аналіз за допомогою метрик якості зображення, таких як PSNR (пікове відношення сигнал/шум), підтвердив високу якість збережених зображень;

- запропонований метод демонструє високу стійкість до різних типів атак, включаючи фільтрацію, стиснення JPEG, додавання шуму та геометричні перетворення;

- цифрові водяні знаки, нанесені за допомогою пірамідального перетворення, залишаються розпізнаваними навіть після значних обробок зображень;

- реалізований алгоритм нанесення цифрових водяних знаків є ефективним та може бути застосований у реальних умовах для захисту авторських прав на зображення;

- запропонована методика може бути легко інтегрована у існуючі системи обробки зображень та мультимедійні платформи.

Можливості для подальших досліджень:

- подальші дослідження можуть бути спрямовані на оптимізацію алгоритму з точки зору швидкості його виконання;

- також доцільно вивчити можливість застосування методу до інших типів мультимедійних даних, таких як відео та аудіо.

Отже, метод нанесення цифрових водяних знаків на цифрові зображення за допомогою пірамідального перетворення є перспективним напрямком для захисту мультимедійної інформації. Він забезпечує високу якість зображень, стійкість до атак та практичну застосовність, що робить його важливим інструментом у сучасних системах захисту інформації.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Ю. Є. Яремчук, В. В. Карпінець, І. С. Зоря, і Д. О. . Козак, «ПІДВИЩЕННЯ СТІЙКОСТІ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ У ПОТОКОВИХ ВІДЕОЗАПИСАХ НА ОСНОВІ ДИФЕРЕНЦІАЛЬНОГО ВБУДОВУВАННЯ ЕНЕРГІЇ (DEW)», Вісник ВПІ, вип. 1, с. 55–64, Лют. 2023.

2. Рубан І. В. Інформаційна технологія підтвердження права власності на цифрові зображення / І. В. Рубан, Н. М. Бологова, В. О. Мартовицький // Сучасні інформаційні системи = Advanced Information Systems. – 2022. – Т. 6, № 1. – С. 118-123.

3. Ray, A., Roy, S. Recent trends in image watermarking techniques for copyright protection: a survey. Int J Multimed Info Retr 9, 249–270 (2020). https://doi.org/10.1007/s13735-020-00197-9

4. Guerriero M., Michele G. Adoption, support, and challenges of infrastructure-as-code: Insights from industry. In: 2019 IEEE international conference on software maintenance and evolution (ICSME). IEEE, 2019. p. 580-589.

5. Sahu, A.K., Umachandran, K., Biradar, V.D. et al. A Study on Content Tampering in Multimedia Watermarking. SN COMPUT. SCI. 4, 222 (2023). https://doi.org/10.1007/s42979-022-01657-1

6. Griffin, J., Noussia, K., Nedeva, S., Zervoudakis, S., Lux, J., & McNamara, J. (2023). Artificial Intelligence (AI) and Watermarking to Transform Copyright Arbitration and Dispute Resolution for Three-Dimensional (3D) printing: An Empirical Analysis. Europan Journal of Law and Technology.

7. Бодня, М., ЄсінаМ., & Пономар, В. (2024). Дослідження можливостей застосування стеганографічних та криптографічних алгоритмів для приховування інформації. Комп’ютерні науки та кібербезпека, (2), 43-57

8. Тарасенко. АВТОРСЬКЕ ПРАВО У ЦИФРОВУ ЕПОХУ: ОСНОВНІ

ТЕНДЕНЦІЇ І ЗМІНИ. Вісник Львівського університету. Серія юридична. 2022. Випуск 75. С. 61–72.

9. Martovytskyi, Vitalii and Ruban, Igor and Bolohova, Nataliia and Sievierinov, Oleksandr and Zhurylo, Oleg and Permiakov, Oleksandr and Nosyk, Andrii and Nepokrytov, Dmytro and Krylenko, Ivan, Development of Methods for Generation of Digital Watermarks Resistant to Distortion (December 29, 2021). Eastern-European Journal of Enterprise Technologies, 6 (2 (114)), 103–116. doi: https://doi.org/10.15587/1729-4061.2021.246641

10. Рубан И. В. Модель обработки TCP-соединений для стеганографической передачи данных в информационно-телекоммуникационных сетях / И. В. Рубан, А. А. Смирнов // Сучасні інформаційні технології у сфері безпеки та оборони. - 2015. - № 3. - С. 108-112

11. Tarhouni, N., Charfeddine, M. & Ben Amar, C. Novel and Robust Image Watermarking for Copyright Protection and Integrity Control. Circuits Syst Signal Process 39, 5059–5103 (2020). https://doi.org/10.1007/s00034-020-01401-1

12. Kozina, G. L., Savchenko, I., Voskoboynik, V., & Karpukov, L. (2023). STEGANOGRAPHIC PHOTO PROTECTION SYSTEM USING FRAGILE WATERMARKS. Systems and Technologies, 64(2), 75-81. https://doi.org/10.32782/2521-6643-2022.2-64.10

13. F. Regazzoni, P. Palmieri, F. Smailbegovic, R. Cammarota and I. Polian, “Protecting artificial intelligence IPs: A survey of watermarking and fingerprinting for machine learning,” CAAI Transactions on Intelligence Technology, vol. 6, no. 2, pp. 180–191, 2021.

14. Megías, D.; Mazurczyk, W.; Kuribayashi, M. Data Hiding and Its Applications: Digital Watermarking and Steganography. Appl. Sci. 2021, 11, 10928. https://doi.org/10.3390/app112210928

15. Anand, A., Singh, A.K. Watermarking techniques for medical data authentication: a survey. Multimed Tools Appl 80, 30165–30197 (2021). https://doi.org/10.1007/s11042-020-08801-0

16. Fernandez, Pierre, et al. "Active image indexing." arXiv preprint arXiv:2210.10620 (2022).URL: https://arxiv.org/abs/2210.10620 (date accessed: 07/01/2024)

17. Wang H, Yuan Z, Chen S, Su Q. Embedding color watermark image to color host image based on 2D-DCT. Optik (stuttg) 2023;274:170585. https://doi.org/10.1016/j.ijleo.2023.170585.

18. Su, Q., Zhang, X. & Wang, G. An improved watermarking algorithm for color image using Schur decomposition. Soft Comput 24, 445–460 (2020). https://doi.org/10.1007/s00500-019-03924-5

19. Hu, F., Cao, H., Chen, S. et al. A robust and secure blind color image watermarking scheme based on contourlet transform and Schur decomposition. Vis Comput 39, 4573–4592 (2023). https://doi.org/10.1007/s00371-022-02610-2

20. The USC-SIPI Image Database URL: https://sipi.usc.edu/database (date accessed: 07/01/2024)

21. І.С. Зубко, В.О. Мартовицький, А.В. Пунченко, Д.Д. Карачевцев «ОГЛЯД МЕТОДІВ НАНЕСЕННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ ДЛЯ ЗАХИСТУ ЗОБРАЖЕНЬ», Системи управляння, навігації ти зв’язку, 2024, №3, с. 95-99.