Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет навчально-науковий центр заочної форми навчання
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Модель децентралізованої системи автентифікації зображень

(тема)

Виконав:

студент II курсу, групи СПзм-20-1

Лазарєв О. К.
(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)

2023 р.

Харківський національний університет радіоелектроніки

Факультет навчально-науковий центр заочної форми навчання

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 Лазарєву Олександру Костянтиновичу
(прізвище, ім'я, по батькові)

1. Тема роботи Модель децентралізованої системи автентифікації зображень

затверджена наказом по університету від " 25 " березня 2022 р. № 33 СТз

2. Термін подання студентом роботи до екзаменаційної комісії 18 травня 2022 р.

3. Вхідні дані до роботи Параметри роботи системи

4. Перелік питань, що потрібно опрацювати у роботі

Аналіз сучасних публікацій;

Аналіз стеганографічних систем;

Розробка моделі децентралізованої системи автентифікації зображень

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) 9 слайдів презентації

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

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

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Огляд основних публікацій	29.03.22-04.04.22	
2	Вибір та обгрунтування методики дослідження	05.04.22-12.04.22	
3	Огляд стеганосистем	13.04.22-19.04.22	
4	Розробка моделі	20.04.22-26.04.22	
5	Проведення експериментів	27.04.22-04.05.22	
6	Оформлення матеріалів кваліфікаційної роботи	05.05.22-10.05.22	
7	Подання кваліфікаційної роботи керівникові та	11.05.22-12.05.22	
	її попередній захист		
8	Подання кваліфікаційної роботи на рецензу-	13.05.22-17.05.22	
	вання		

Дата видачі завдання 28 березня 2022 р.

Студент _____
(підпис)

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

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 75 с., 22 рис., 2 табл., 1 дод., 26 джерел.

ДЕЦЕНТРАЛІЗАЦІЯ, ІНТЕРНЕТ, ЗОБРАЖЕННЯ, БЛОКЧЕЙН, СЕРВЕР.

Метою кваліфікаційної роботи є розробка моделей і алгоритмів захисного маркування растрових зображень, що зберігаються в базах даних, для визначення їх автентичності і цілісності за допомогою багаторазового вбудовування цифрових водяних знаків.

Для досягнення поставленої мети у роботі вирішуються такі задачі:

- аналіз існуючих методів та алгоритмів маркування цифрових зображень водяними знаками;
- розробка моделі захисту та алгоритму захисного маркування растрових зображень шляхом багаторазового вбудовування водяних знаків;
- розробка моделі та алгоритму перевірки растрових зображень на автентичність та цілісність;
- програмна реалізація розроблених алгоритмів;
- проведення експериментів з метою підтвердження працездатності та практичної застосовності запропонованих моделей та алгоритмів.

ABSTRACT

Master’s thesis: 75 pages, 22 figures, 2 tables, 1 appendices, 26 sources.

DECENTRALIZATION, INTERNET, IMAGE, BLOCKCHAIN, SERVER.

The major goal of this thesis is is to develop models and algorithms for the protective marking of bitmap images stored in databases to determine their authenticity and integrity using multiple embedding of digital watermarks.

To achieve the set goal, the following tasks are solved in the work:

- analysis of existing methods and algorithms for marking digital images with watermarks;

- development of a protection model and an algorithm for protective marking of raster images by multiple embedding of watermarks;

- development of a model and algorithm for checking raster images for authenticity and integrity;

- software implementation of developed algorithms;

- conducting experiments in order to confirm the efficiency and practical applicability of the proposed models and algorithms.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

PSNR –відношення рівня сигналу вихідного зображення до рівня шуму (англ. Additive white Gaussian noise)

АСОД – автоматизована система обробки даних

ДКД – дискретне косинусне перетворення

ЕП – електронний підписам

СЛЗ – система людського зору

ЦВЗ – цифровий водяний знак

ВСТУП

Останні десятиліття, які можна справедливо назвати часом цифрових та мережних технологій, відкрили великі можливості для фотографів, художників та інших фахівців, які працюють із растровими зображеннями.

Згодом у більшості дизайнерів, графіків і фотографів накопичується велика кількість створених ними зображень, які найзручніше зберігати в різних документарних системах. Постійний розвиток та вдосконалення інструментів графічних редакторів дозволяє не лише покращувати якість вихідних зображень, а й змінювати їх формат, геометричні параметри, а також інформаційний зміст. Повсюдне використання глобальних мереж, а також поширення електронних засобів масової інформації дають можливість графікам і фотохудожникам демонструвати свої роботи безлічі людей по всьому світу, а фотокореспондентам – оперативно розміщувати репортажі про події, що відбуваються.

Постійне вдосконалення інструментів обробки растрових зображень має свою негативну сторону, оскільки спрощує процес підробки зображень сторонніми особами. Проблема забезпечення автентичності та цілісності растрових зображень робить актуальним завдання розробки моделей та алгоритмів їхнього захисного маркування.

Завдання розробки таких моделей та алгоритмів не є тривіальним, оскільки необхідно не просто довести факт порушення авторського права на растровому зображенні, а визначити, яким чином було порушено його цілісність, тобто вказати, в яких саме фрагментах цього зображення було зроблено зміни.

При фальсифікації цифрове растрове зображення може бути піддане наступним впливам: кадруванню, видаленню, клонуванню або додаванню інформаційних фрагментів, застосуванню графічних фільтрів редакторів та інструментів для корекції зображень, а також зміні цифрового формату,

стиснення із втратами, поворотів на малі кути та масштабування. Деякі з цих впливів, такі як повороти та масштабування, не видаляючи захисне маркування, унеможливлюють його детектування без повернення промаркованого зображення у вихідний стан. Для спрощення вирішення цього завдання передбачається використання допоміжних засобів захисту зображень, таких як документарні системи.

Розроблена модель захисного маркування растрових зображень повинна вказувати на зміну їхньої цілісності, бути стійкою до наслідків впливів на ці зображення, а також враховувати особливості їх форматів. Основою для моделі захисного маркування послужили цифрові водяні знаки (ЦВЗ) – невидимі мітки, що вбудовуються в зображення для підтвердження авторського права на нього.

Об'єктом дослідження є документарні системи, куди входять бази цифрових зображень.

Предметом дослідження є існуючі методи та алгоритми вбудовування цифрових водяних знаків.

1 АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ЗАХИСНОГО МАРКУВАННЯРАСТРОВИХ ЗОБРАЖЕНЬ ЦИФРОВИМИ ВОДЯНИМИ ЗНАКАМИ

1.1 Основні растрові формати цифрових зображень

Під цифровим зображенням слід розуміти подання інформації у графічному вигляді, призначене для зорового сприйняття [1]. При цьому цифрове зображення може спочатку створюватися в цифровому вигляді за допомогою комп'ютерної програми або бути перетвореним з природного або аналогового видів на цифровий за допомогою пристроїв введення.

Спосіб запису та зберігання графічної інформації у файлі називається графічний формат. Формати графічних файлів досить сильно відрізняються один від одного в залежності від типу інформації, що зберігається в них [2].

Всі існуючі цифрові зображення за принципом їх формування, що залежить від інформації, що зберігається в них, можна розділити на чотири види: фрактальна, тривимірна, векторна і растрова графіка. На вигляд прив'язки до типу зображення графічні формати можна розбити на два види [3]: формати, що представляють спеціалізовані зображення з чіткою структурою, та формати, що не висувають жодних вимог до характеру зображень.

Графічні формати першого типу враховують особливості зображень, що зберігаються в них. У таких форматах зберігається фрактальна, тривимірна та векторна графіка.

Фрактальна графіка ґрунтується на математичному моделюванні зображень за допомогою програмних засобів. Тривимірна графіка широко використовується у комп'ютерних іграх, кінематографії та мультиплікації, а також тривимірному моделюванні різних процесів та об'єктів.

Векторна графіка ґрунтується на поданні зображень у вигляді

елементарних геометричних об'єктів, що описуються математичними функціями. Застосування векторної графіки обмежується складністю зображення багатьох реальних об'єктів, для побудови яких можливе знадобиться створення дуже великої кількості графічних примітивів, при цьому точність відображення не може бути гарантована. Також до форматів цього типу належать файли, у яких зберігаються шрифти.

Недоліком графічних форматів, що становлять зображення з чіткою структурою, є обмеженість класів цифрових зображень, що подаються тим чи іншим способом. Наслідком є велика кількість форматів файлів, багато з яких у вихідному вигляді можна переглянути тільки в спеціалізованих програмних засобах.

Графічні формати другого типу можуть представляти практично будь-які зображення, тобто даний спосіб зберігання графічної інформації має широке охоплення. Фактично в цих форматах зберігають інформацію про фізичний процес, що породжує зображення [3]. При цьому безперервний процес представляється у дискретному вигляді. Графічні формати другого типу зберігають у собі растрову графіку. Важливим плюсом растрової графіки є можливість створення будь-якого зображення, незалежно від його складності, тому цей вид графіки поширений досить широко. Надалі растрові зображення також називатимемо просто цифровими зображеннями, оскільки робота із зображеннями першого типу не входить у рамки даного дослідження.

Растрове зображення розглядається людським мозком як двовимірна матриця, основним елементом якої є точка або піксель, що характеризується кольором та координатами у горизонтальному та вертикальному рядах зображення. Для запису відповідного кожному пікселю оптичного сигналу використовують різні способи, найбільш поширеним у тому числі є розкладання сигналу з його спектральним складовим.

Засобами такого розкладання є колірні моделі, що описують сигнал як концептуально, а й кількісно. Існує три типи колірних моделей: перцепційні

(засновані на сприйнятті кольорів), субтрактивні (засновані на відніманні) та адитивні (засновані на додаванні). На практиці під час роботи з растровими зображеннями найчастіше користуються перцепційною моделлю YCbCr, субтрактивною моделлю CMYK та адитивною моделлю RGB. Всі ці колірні моделі зводяться одна до одноїлінійним перетворенням.

Абревіатура YCbCr розшифровується як «lumenocitY, Compensation of Blue, Compensation of Red» [3]. Зображення, збережені в цій колірній моделі, мають три колірні канали. Канал «lumenocity» – яскравості, він не несе в собі інформації про колір пікселів. Два інших канали засновані на кольоровості: «Compensation of Blue» (діапазон кольору від жовтого до синього) та «Compensation of Red» (діапазон кольору від пурпурового до зеленого). Колірна модель YCbCr використовується в деяких схемах стиснення зображення із втратами.

Субтрактивна модель CMYK (Cyan, Magenta, Yellow, blacK) широко застосовується у поліграфії. Кольори зображень, збережених у цій моделі, виходять внаслідок поглинання та відображення від запечатаного простору тих чи інших світлових хвиль. Діапазон цього колірного простору менше, ніж діапазон адитивного простору RGB і набагато менше, ніж діапазон YCbCr.

Адитивна модель RGB (Red, Green, Blue) фактично є рідною всім пристроїв введення (цифрових камер, сканерів, моніторів) [4]. Вона заснована на представленні кольору у вигляді підсумовування червоного, зеленого та синього світлових потоків. Оскільки охоплення кольорової моделі RGB більше, ніж охоплення колірного простору CMYK, цифрові зображення, отримані з пристроїв введення, особливо ті, що не призначені для подальшого використання в поліграфії, краще зберігати саме в цій моделі кольорів. На рисунку 1.1 представлено перетин кольорових просторів RGB і CMYK.

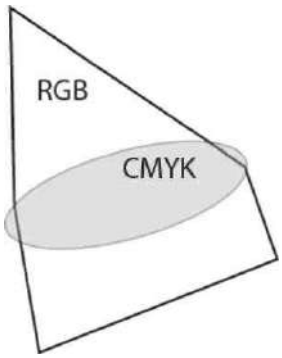

Рисунок 1.1 – Перетин кольорових просторів CMYK та RGB

З існуючих растрових форматів графічних файлів нині найбільш потрібні формати BMP, GIF, PNG, JPEG і TIFF [3], які підтримуються практично будь-якими засобами роботи з растрової графікою. Розглянемо їх особливості з урахуванням використовуваних у них колірних моделей,максимального числа кольорів, що відображаються, типу стиснення (без втрат і з втратами, що вносять спотворення у вихідну матрицю зображення при її зворотному перетворенні), а також суб'єктивної оцінки якості цифрового зображення.

Графічний формат BMP використовує колірну модель RGB і містить лише безпосередню інформацію про пікселі, тому його можна назвати одним з найпростіших форматів зображень. Діапазон значень кольори по кожному з колірних каналів лежить в інтервалі від 0 до 2^8, тобто збережене зображення фактично є повнокольоровим. Також можназберігати зображення у відтінках сірого кольору (колірна модель Grayscale, діапазон значень від 0 до 2^8). Зображення зберігається без втрат якості, оскільки базова версія формату не передбачає схеми стиснення, а розширена може використовувати малоефективне стиск за алгоритмом RLE (кодування серій, що повторюються). З урахуванням вищесказаного, цифрові зображення, збережені у форматі BMP, мають високі показники якості, але при цьомуЦей формат є низькоефективним.

Графічний формат GIF так само, як і формат BMP, використовує

колірну модель RGB, але, на відміну від BMP, колірна схема формату GIF неповнокольорова (256 кольорів). Також можна зберігати зображення у відтінках сірого кольору, при цьому загальна кількість відтінків дорівнюватиме 2^8 . Стиснення GIF-зображення здійснюється за алгоритмом LZW, ефективним і здійснює компресію без втрат якості. Цифрові фотографії, збережені у форматі GIF, мають об'єм менший, ніж у BMP-зображень, але через підтримку в палітрі лише 256 кольорів забезпечують дуже посередню якість зображення.

Графічний формат PNG поєднує плюси форматів BMP і GIF. Він використовує колірну модель RGB, але дає можливість зберігати зображення у відтінках сірого кольору. Перші версії цього формату підтримували 2^8 на кожен канал, але його сучасні розширення підтримують до 16 біт на колірний канал (до 2^{48} кольорів на зображення). Стиснення цифрового зображення, збереженого у цьому форматі, здійснюється за алгоритмом LZ77, що здійснює компресію без втрат якості. З урахуванням вищесказаного, растрові зображення, збережені у цьому форматі, мають високу якість.

Графічний формат TIFF може використовувати не лише колірну модель RGB, а й моделі Grayscale, YCbCr, CMYK, а також деякі інші колірні простори. Діапазон кольору на один канал може сягати 2^{64} як при цілочисельному значенні пікселя, так і при його значенні з плаваючою комою. Стиснення зображень, збережених у форматі TIFF, здійснюється за різними алгоритмами, що здійснюють як стиск без втрат (RLE, LZ77 та LZW), так і з втратами (наприклад, JPEG). Якість зображень, збережених у цьому форматі, висока. На відміну від зображень, збережених у форматах BMP, GIF та PNG, TIFF-зображення найкраще підходять для використання у поліграфії [4].

Графічний формат JPEG може використовувати колірні моделі Grayscale, CMYK та модель RGB. Дані зберігаються в повнокольоровому режимі, з діапазоном кольорів на канал від 0 до 2^8. Для JPEG-зображень можливе стиснення без втрат, але найчастіше такі зображення стискаються із

втратами. При стисканні зображення перетворюється на проміжну модель YCbCr, до нього застосовується квантування з дискретним косинусним перетворенням (ДКП). Формат добре підходить для збереження повнокольорових фотографій з метою їх подальшого використання у глобальних мережах або електронних виданнях, але не застосовується для стиснення зображень, що містять текстову інформацію, креслень, а також цифрових зображень (наприклад, медичних), у яких неприпустимі навіть найменші втрати даних [5]. Крім того, при багатоступінчастій обробціцифрових зображень при кожному проміжному збереженні коригованого файлу зображення будуть вноситись спотворення.

1.2 Огляд видів модифікації зображень, що захищаються

Незалежно від формату, цифрові зображення можуть піддаватися різним зовнішнім впливам (атакам), наприклад, під час їх редагування. Під час підготовки зображень до комерційного використання найімовірніші такі види впливів: кадрування, зміна кольорової моделі,зміна цифрового формату, стиснення, масштабування. При спробах фальсифікації [6] цифрове зображення також може зазнати клонування, видалення або додавання будь-яких інформаційних фрагментів [7]. Крім того, до цифрових фотографій можливе застосування інструментів тонової та кольорової корекції, різних кольорових фільтрів, посилення різкості, видалення шумів або їх додавання. Розглянемо докладніше ці дії.

Під кадруванням цифрового зображення мається на увазі його обрізання з метою його приведення до необхідного розміру або зміни композиції зображення.

Оскільки колірні моделі RGB та CMYK мають різне охоплення, між ними не існує взаємно-однозначної відповідності [4], відповідно, зміна колірної моделі може спричинити деякі зміни в кольорах зображення.

Також руйнівним для інформаційного змісту растрового зображення

може стати його збереження у форматі, який використовує алгоритм стиснення втрати. Під стисненням цифрового зображення слід розуміти зменшення необхідного його представлення числа біт [8]. Коефіцієнти стиснення можуть бути досить великими, якщо цей процес відбувається з урахуванням психовізуальної надмірності зображення. Цифрове зображення представляється як частотних смуг, та її близькі до нуля частотні коефіцієнти обнуляются, у своїй зі зростанням коефіцієнта стиснення посилюються спотворення вихідного зображення.

Під масштабуванням растрового зображення розуміють зміну його роздільної здатності, тобто кількості пікселів на одиницю площі, у бік збільшення чи зменшення. Фактично двовимірна матриця пікселів, що становлять зображення, зменшується або збільшується відповідно до розміру зображення та його роздільної здатності. Масштабування зазвичай спотворює деталі зображення, породжуючи ефекти сходів або, навпаки, небажаного згладжування контурів.

Клонування інформаційних фрагментів цифрових зображень є їх дублювання в межах зображення, що змінюється. При видаленні елементів растрового зображення відбувається їхнє заміщення іншими об'єктами, зокрема фрагментами інших цифрових зображень. Зміни такого роду часто використовують, наприклад, при створенні фото реалістичних колажів або для підробки зображень.

Застосування інструментів кольорової або тонової корекції, а також кольорових фільтрів, різкості та видалення шумів використовують для підвищення якості зображення в цілому або його фрагментів. Також кольорові фільтри або штучне зашумлення зображення можуть використовуватися для досягнення певного художнього ефекту або маскування деяких дефектів зображення

При розробці інструментів захисту інформаційного змісту цифрових зображень для доказу факту фальсифікації необхідно враховувати всі можливі атаки, які можуть піддатися.

1.3 Цифрові водяні знаки

При розробці моделі захисного маркування растрових зображень та їх перевірки на автентичність та стійкість було враховано два важливі моменти [9]:

- растрове зображення за рахунок своєї візуальної надмірності не вимагає особливої точності, тому може бути до певної міри змінено, при цьому не втрачаючи функціональності;

- система людського зору влаштована так, що не може надійно розрізняти незначні зміни у зображенні (наприклад, коригування яскравості, кольору, контрасту), і не всякий інструментарій здатний вирішувати це завдання.

У зв'язку з цим було прийнято рішення розробити модель, що базується на коригуванні даних растрового зображення із приховуванням у них захисної інформації.

В якості основи для розроблюваної моделі захисного маркування були обрані цифрові водяні знаки, що впроваджуються в захищувані зображення («digital watermarking», ЦВЗ). Назва «digital watermarking» була вперше використана у роботі С. Осборна [10]. На відміну від звичайних водяних знаків, ЦВЗ повинні бути непомітними (виявленими за допомогою спеціального декодера), але при цьому стійкими до впливу різних атак на захищене зображення. ЦВЗ може являти собою якийсь автентичний код або керуючу інформацію [8], графічний логотип, хеш-функцію, і т.д.

Вбудовування ЦВЗ є одним із напрямків стеганографії, науки про непомітне вбудовування послідовностей бітів у інших аналогових послідовностях [8]. Нині є багато розробок, присвячених захисту зображень з допомогою ЦВЗ.

Існує ряд термінів, що належать до цієї науки [3,8,9].

Впроваджуваний у зображення ЦВЗ є секретною інформацією, що приховується, називається повідомленням m. Саме захищуване цифрове

зображення називається контейнером b, причому до моменту впровадження ЦВЗ контейнер є пустим, а контейнер з впровадженим повідомленням b_m (захищене зображення) – модифікованим або заповненим. Ключ k – це деяка інформація, необхідна для впровадження повідомлення m в контейнер b. Ключ може бути секретним або загальнодоступним, при цьому для введення повідомлення в контейнер можна використовувати декілька ключів. Області зображення, в які можна проводити використання біт повідомлення, називаються простором приховування, а модифіковані в результаті впровадження ЦВЗ області – простором приховування, що використовується.

Над зображенням, ЦВЗ і ключем проводять порівняння заповненого контейнеру пряме стеганографічне перетворення. Зворотне стеганографічне перетворення проводиться над заповненим контейнером з використанням ключа, при цьому результатом такого перетворення є виявлення ЦВЗ, який може бути модифікованим внаслідок будь-яких впливів на захищене зображення.

Сукупність пустих та захищених контейнерів, повідомлень, ключів та прямих та зворотних стеганографічних перетворень називають стегосистемою. Узагальнена схема стегосистеми показано рисунку 1.2.

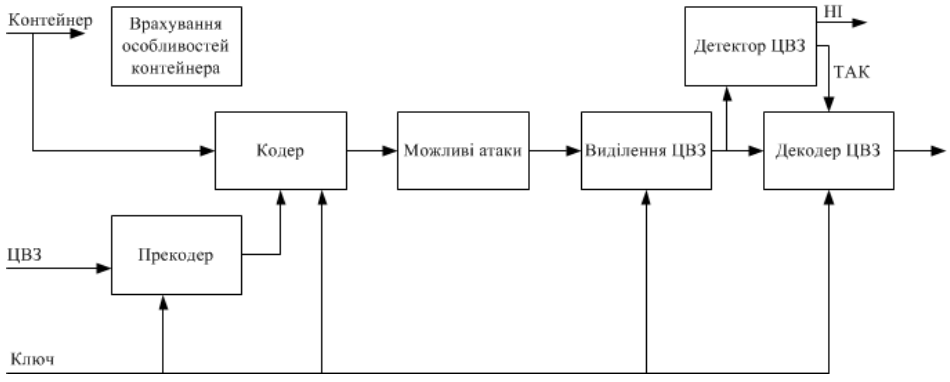

Рисунок 1.2 – Узагальнена структурна схема стегосистеми [8]

Пряме та зворотне стеганографічне перетворення відбуваються

наступним чином. У прекодер відбувається перетворення ЦВЗ m до виду, зручному для вбудовування. У кодері з використанням ключа відбувається впровадження біт перетвореного ЦВЗ зображення (контейнер), що знаходиться у вихідному вигляді або перетворене з урахуванням його особливостей. Результат прямого перетворення зберігається у вигляді заповненого контейнеру. Захищене зображення може зазнавати різних випадкових або навмисних атак, в результаті яких воно модифікується.

Змінене в результаті атак зображення-контейнер піддається зворотному стеганографічному перетворенню для виділення вбудованого повідомлення. Детектор ЦВЗ визначає наявність повідомлення у контейнері, а декодер ЦВЗ відновлює вбудоване повідомлення.

За характером інформації, необхідної виявлення вбудованих повідомлень, існуючі стегосистеми можна розділити на такі класи [3,8]:

- закриті стегосистеми першого та другого типів, що вимагають наявності вихідного пустого контейнеру. Системам першого типу також необхідний вихідний ЦВЗ, при цьому детектор виносить рішення про наявність або відсутність повідомлення в контейнері, що досліджується. Системам другого типу вихідне повідомлення не потрібне: за наявності відповіді детектора про наявність ЦВЗ декодер відновлює впроваджену інформацію;

- напівзакриті стегосистеми, що вимагають наявності вихідного ЦВЗ. Контейнер досліджується на наявність впровадженої інформації, яка порівнюється з наявним ЦВЗ, і при збігу значень детектор виносить рішення про наявність або відсутність секретного повідомлення;

- відкриті стегосистеми, що не вимагають наявності вихідного зображення та ЦВЗ. За наявності відповіді детектора про наявність ЦВЗ декодер відновлює впроваджену інформацію.

Для розробки моделі захисного маркування растрових зображень та перевірки їхньої автентичності та цілісності краще використовувати відкриті стегосистеми, оскільки, наприклад, при кадруванні захищеного зображення

його порівняння з вихідним контейнером викликає певні незручності.

Використовувані в стегосистемах ЦВЗ можуть бути стійкими (робастними), напівкрихкими та крихкими [3,8]. Робастні ЦВЗ стійкі до широкого спектру впливів, тому присвячено більшість розробок. Напівкрихкі водяні знаки розробляються таким чином, щоб бути стійким до одних впливів, але нестійким до інших. Крихкі ЦВЗ руйнуються при більшості впливів на заповнений контейнер, допускаючи лише зовсім незначну модифікацію, наприклад, стиснення зображення. При цьому крихкі водяні знаки можуть вказувати на розташування модифікації контейнеру.

Фактично, майже всі існуючі ЦВЗ можна віднести до категорії напівкрихкі, оскільки жодна з розроблених на сьогоднішній день стегосистем не є вільною від недоліків [11,12].

1.4 Організаційні засоби захисту зображень

Відсутність універсальних з погляду протидії всім можливим атакам стегосистем змушує шукати способи компенсації їх недоліків.

При вивченні вразливості стегосистем необхідно відрізняти стійкість впровадженого ЦВЗ до різних впливів можливості його вилучення зі зміненого зображення. Наприклад, при повороті зображення вбудоване повідомлення може зберегтися, але при цьому не виділятися декодером. У статті [13] розглядаються наслідки атак на зображення із впровадженими в них ЦВЗ. Автор доводить, що впроваджена інформація виявляється стійкою не тільки до наслідків впливу інструментів корекції зображень, але й до афінних перетворень (поворотів і масштабування), що часто унеможливлюють виявлення ЦВЗ. Якщо привести перетворене зображення до початкового вигляду, повернувши йому вихідний масштаб або повернувши на потрібний кут, водяні знаки можуть бути виявлені. Очевидно, що для коректності відновлення необхідно мати оригінал заповненого контейнеру, а також знати його точні розміри і вид вбудованого водяного

знаку.

Одним із способів компенсування недоліків стегосистем може стати використання організаційних способів захисту цифрових зображень.

До організаційних засобів захисту зображень також можна віднести використання різних інформаційних систем [14], баз даних або автоматизованих систем обробки даних (АСОД) [15]. Розглянемо захист цифрових зображень з прикладу АСОД.

Для захисту даних у цих системах використовується комплекс методів, заходів та засобів для системного забезпечення необхідної надійності збереженої та цифрової інформації, що обробляється в АСОД.

Однією з важливих цілей захисту цифрової інформації, що зберігається в АСОД, є попередження її випадкової або зловмисної модифікації. Надійність інформації у цих системах характеризується з погляду її фізичної цілісності і при цьому впевненості у її справжності та безпеці. Під фізичною цілісністю у разі розуміють наявність всіх фрагментів даних, і відсутність у них спотворень. Справжність інформації можлива за її фізичної цілісності та впевненості у відсутності її фальсифікації. Під безпекою інформації розуміють відсутність несанкціонованого доступу до неї.

В автоматизованих системах обробки даних існують поняття об'єктів та елементів захисту. Під елементами захисту мають на увазі фрагменти інформації, що захищаються, які виділяються за принципами локалізованості та однорідності (з точки зору впливу руйнівних факторів). Під об'єктом захисту мають на увазі структурний компонент системи, призначені для зберігання елементів захисту.

При використанні автоматизованих систем обробки даних як організаційні способи захисту зображень в об'єктах систем доцільно зберігати такі елементи:

- цифрові зображення, промарковані ЦВЗ та збережені у потрібному форматі;
- зразки впроваджених у зображення водяних знаків;

- ключі, відповідно до яких ЦВЗ впроваджуються у зображення;
- горизонтальний та вертикальний розміри збереженого зображення;
- різна супровідна інформація, до якої може належати назва зображення та його опис, дата зйомки та різні коментарі;
- вихідне, не промарковане цифрове зображення.

Таким чином, використання систем обробки даних дає додаткові можливості захисту цифрових зображень. Якщо детектор не виявив впровадженої інформації в досліджуваному зображенні, необхідно знайти в базі даних вихідне і привести до нього у відповідність зображення, що перевіряється.

1.5 Аналіз алгоритмів маркування зображень цифровими водяними знаками

При розробці алгоритмів вбудовування ЦВЗ у зображення необхідно враховувати особливості системи людського зору (СЛЗ), оскільки візуальна непомітність впроваджених повідомлень одна із головних вимог до будь-якої стегосистеми.

Властивості СЛЗ поділяються на фізіологічні (низькорівневі) та психофізіологічні (високорівневі) [8].

Оскільки впроваджену в зображення приховану інформацію фактично можна розглядати як доданий до нього сторонній шум, розробник стегосистем має враховувати такі фізіологічні властивості людського зору [16]:

- чутливість зору до зміни контрастності (яскравості) зображення;
- чутливість до частот;
- ефект маскування сигналу зображення.

У результаті експерименту, описаного Б. Гірод у [17], було встановлено усереднену чутливість людського зору до зміни яскравості. Було виявлено, що для середніх яскравих значень контраст приблизно постійний, а для

великих і малих значень поріг невиразності зростає. Пізніші дослідження [8] показали, що за малих значень яскравості поріг несприйнятливості яскравості не збільшується, а знижується, що свідчить про високу чутливість СЛЗ у діапазоні малих яскравостей. Графік залежності мінімального контрасту ΔI/I від яскравості I показано на рисунку 1.3.

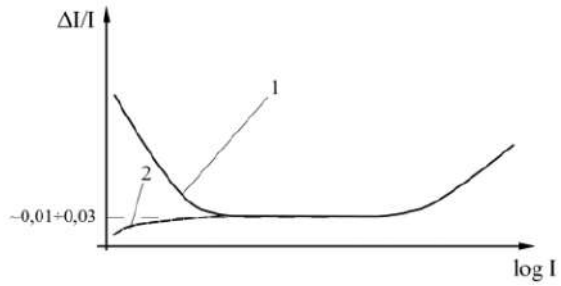

Рисунок 1.3 – Залежність мінімального контрасту від яскравості [9]
1– класична теорія, 2 – нові дослідження

Чутливість до частот зображення виявляється в тому, що для СЛЗ через особливості її амплітудно-частотної характеристики шум у низькочастотних областях більш помітний, ніж високочастотний.

Фоторецептори сітківки людського ока, що відповідають за кольоровий зір, так звані колбочки [18], поділяються на три види, кожен з яких чутливий до певних довжин світлових хвиль (коротких, середніх та довгих). Тому зорова інформація сприймається у вигляді трьох складових, які збуджують нервові закінчення в оці через певні підканали.

Кожна з таких складових відрізняється за частотними характеристиками, також має різну просторову орієнтацію. На рисунку 1.4 показані графіки поглинання світлових хвиль різними видами колб та паличок (Фоторецептори, відповідальні за сутінковий зір).

З рисунку 1.4 видно, що при розгляді зображень, збережених у моделі RGB, СЛЗ найменш сприйнятливий до інформації з синього кольорового каналу. У червоному каналі людське око сприймає сім біт із восьми, у

зеленому – вісім із восьми і лише у синьому каналі із восьми біт сприймається лише чотири біти.

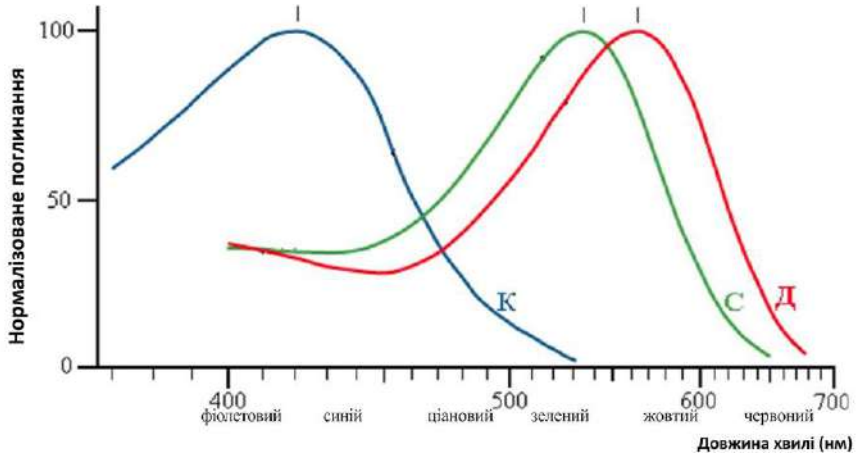

Рисунок 1.4 – Сприйняття різними типами колб світлових хвиль

При зоровому сприйнятті двох складових, що мають схожі характеристики, відбувається ефект маскування, тобто збільшення порога знаходження сигналу у присутності іншого сигналу зі схожими характеристиками. Ефект маскування також пояснює факт меншої помітності високочастотного шуму ніж низькочастотного, що спостерігається на однотонних ділянках зображень.

Психофізіологічні властивості людського зору виявляються після обробки первинної інформації, що надійшла від зорового аналізатору; вони спрямовані на «підлаштування» інформації під зображення [8]. СЛЗ чутлива до висококонтрастних ділянок цифрового зображення, до розмірів, форми, розташування та кольору інформаційних фрагментів. Увага в першу чергу привертають люди, що знаходяться на зображенні, а також об'єкти, розташовані на передньому плані.

При створенні стегосистем психофізіологічні властивості СЛЗ мало враховуються.

З моменту першої згадки терміна «digital watermarking» велика

кількість досліджень, пов'язаних із ЦВЗ, присвячена захисту растрових зображень. Це пов'язано як з актуальністю завдання захисту авторських прав, так і з особливостями цифрового представлення зображень, такими, як надмірність, наявність областей із шумовою структурою, а також розвитком методів цифрового оброблення растрових зображень [8].

Для вибору алгоритму вбудовування ЦВЗ, що відповідає більшості вимог, було проведено аналіз наявних методів і алгоритмів [13].

Методи вбудовування прихованих повідомлень можна класифікувати за різними критеріями, зокрема, за способом вилучення ЦВЗ, способом їх впровадження, а також за областю вбудовування (рисунок 1.5).

Рисунок 1.5 – Класифікація методів вбудовування прихованих повідомлень. Кольором позначено методи, які підходять для вирішення поставлених завдань

За способом отримання прихованої інформації з контейнеру алгоритми маркування зображень можна розділити на три групи:

- алгоритми, що виконують пошук секретного повідомлення без вихідного промаркованого зображення (так звана сліпа схема);
- алгоритми, що вимагають наявності промаркованого зображення;

- алгоритми, які виконують пошук повідомлень із використанням фрагмента оригіналу контейнера.

Алгоритми, що виконують пошук повідомлень з використанням фрагмента оригіналу контейнера, зручні у разі використання ЦВЗ, однакового для всього маркованого зображення. У разі впровадження в різні області зображення декількох видів водяних знаків, що захищаються, такі алгоритми можуть працювати некоректно.

Алгоритми, що виконують пошук ЦВЗ з використанням оригінального контейнера, погано застосовні в разі кадрування вихідного зображення, а також його перевірки на наявність запозичених фрагментів.

Алгоритми, що працюють за сліпою схемою, зручніші для вирішення поставлених у роботі завдань.

За способом застосування ЦВЗ існуючі методи можна розділити такі групи [8]:

- лінійні, що базуються на лінійній модифікації зображення;
- нелінійні, що використовують векторне або скалярне квантування;
- інші (зокрема використовують фрактальні перетворення).

Щодо області вбудовування прихованих даних існуючі методи можна розділити на дві групи:

- просторові, засновані на впровадженні біт ЦВЗ внаслідок змін яскравих чи кольорових складових зображення;

- спектральні, засновані на декомпозиції маркованих областей зображення.

2 ВИБІР МЕТОДУ МАРКУВАННЯ ЦИФРОВИХ ЗОБРАЖЕНЬ

У цьому розділі будуть розглянуті основні методи впровадження ЦВЗ в растрові зображення, що ґрунтуються на дискретному косинусному перетворенні, оскільки саме це перетворення входить до алгоритму стиснення JPEG. Спочатку необхідно розглянути механізм прямого і зворотного дискретного косинусного перетворення, а потім проаналізувати існуючі методи за такими критеріями, як види ЦВЗ, що вбудовуються, схема їх вилучення і можливість вилучення маркування, а не підтвердження факту її наявності.

На основі обраного методу в наступному розділі будуть побудовані моделі захисного маркування растрових зображень та перевірки промаркованих зображень на автентичність та цілісність.

2.1 Двовимірне дискретне косинусне перетворення

Вперше застосування ДКП для впровадження ЦВЗ у цифрове зображення було описано у роботі Коха і Жао [20] у 1995 році, при цьому перетворення застосовувалося до всієї матриці пікселів зображення. В даний час велике поширення набула поблочна декомпозиція, хоча зустрічаються алгоритми, що ґрунтуються на повній декомпозиції растрового зображення.

Розглянемо побічний метод декомпозиції зображення.

Растрове зображення розбивається на блоки розміром 8x8 пікселів. Кожен із блоків піддається двовимірному дискретному косинусному перетворенню, в результаті чого цілочисленні матриці пікселів перетворюються на частотні матриці коефіцієнтів ДКП розміром 8x8 пікселів

Двовимірне ДКП здійснюється за такою формулою:

$$DCT(uv) = \sqrt{\frac{2}{m}}a(v)\left(\sum_{j=0}^{m-1}\left(\sqrt{\frac{2}{n}}a(u)\sum_{i=0}^{n-1}Fi,\mathrm{j}\cos\left(\frac{\pi(2i+1)u}{2n}\right)\right)cos\left(\frac{\pi(2\mathrm{j}+1)v}{2m}\right)\right) \quad (2.1)$$

де: DCT(u,v) – значення елементів отриманої частотної матриці коефіцієнтів;

Fi,j – значення елементів вихідної цілої матриці пікселів;

n – кількість стовпців матриці пікселів;

m – кількість рядків матриці пікселів;

i, j – позиція поточного елемента матриці пікселів зображення;

u, v – позиція формованого елемента частотної матриці:

u ∈ [0,-l], v∈ [0,j-l];

при u =0 a(u) = 1⁄√ 2, при u>0 a(u)=1;

при v=0 a(v) = 1⁄√ 2, при v>0 a (v)=1.

Приблизне розташування частотних коефіцієнтів отриманої після двовимірного дискретного косинусного перетворення матриці зображено на рисунку 2.1.

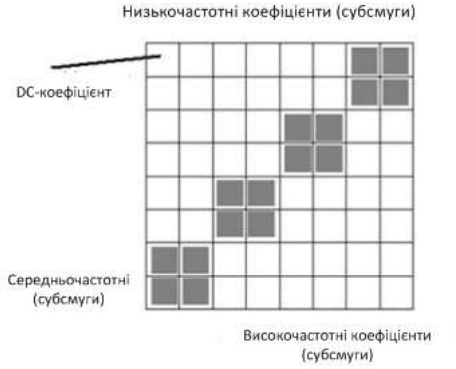

Рисунок 2.1 – Матриця частотних коефіцієнтів блоку8x8 пікселів [8]

Коефіцієнт, розташований у верхньому лівому куті отриманої частотної матриці, називається DC-коефіцієнтом; він містить інформацію про яскравість всього блоку пікселів. Інші коефіцієнти матриці називаються AC-

коефіцієнтами. АС-коефіцієнти можуть набувати позитивних, негативних і нульових значень.

Низькочастотні коефіцієнти, що містять основну частину енергії зображення, розташовуються ближче до верхнього лівого кута матриці, а вразливіші для атак, пов'язаних з обробкою зображення, високочастотні коефіцієнти згруповані в нижній правій частині. Автори більшості алгоритмів вважають придатними для впровадження біт водяних знаків тільки середньочастотні коефіцієнти: інформація прихована в областях, істотних для системи людського зору, і, водночас, не буде спотворюватися при малих значеннях стиснення з втратами [19].

Після впровадження в частотні матриці блоків зображення біт ЦВЗ виконують зворотне дискретне косинусне перетворення для переходу до цілочисельних матриць пікселів. При цьому спочатку виконується одновимірне ДКП за рядками, потім за стовпчиками матриці коефіцієнтів.

$$F(u,j) = \sqrt{\frac{2}{m}} \sum_{v=1}^{m-1} a(v)\, DCT(u,v) \cos\left[\frac{\pi(2j+1)v}{2m}\right] \tag{2.2}$$

$$F(i,j) = \sqrt{\frac{2}{n}} \sum_{u=1}^{n-1} a(uv)\, F(u,j) \cos\left[\frac{\pi(2i+1)u}{2n}\right] \tag{2.3}$$

2.2 Порівняння методів приховування даних у коефіцієнтах дискретного косинусного перетворення

Для вибору алгоритму, який можна використовувати для розробки моделей захисного маркування зображень та перевірки їх цілісності та автентичності, були розглянуті найбільш відомі методи маркування зображень за допомогою ДКП:

- метод Коха та Жао (Koch, 1995) [20];
- метод Бенхама (Benham, 1997) [21];

- метод Хсу та Ву (Hsu, 1999) [22];
- метод Барні (Barni, 1997) [23];
- метод Фрідріха (Fridrich, 1998) [24];
- метод Подільчака (Podilchuk, 1997) [3];
- метод Коксу (Cox, 1997) [25].

Алгоритми розглядалися з погляду їхньої відповідності наступним критеріям:

- тип дискретного косинусного перетворення зображення (поблокове або повне перетворення зображення);
- види використовуваних для вбудовування цифрових водяних знаків;
- схема виділення впровадженої інформації із досліджуваного зображення;
- наявність декодера, який отримує впроваджену інформацію.

Результати аналізу методів представлені у таблиці 2.1.

Таблиця 2.1– Аналіз методів вбудовування захисної інформації на основі ДКП

Метод	Тип ДКП	ЦВЗ	Схема вилучення	Детектор/декодер
Koch (1995) Кох і Жао	Поблокове, 1 біт у блок 8x8 пікселів	Bitmap зображення або послідовність {0,1}	Сліпа	Декодер ЦВЗ
Benham (97) Бенхам	Поблокове, вибираються лише «придатні» блоки 8x8	Bitmap зображення або послідовність {0,1}	Сліпа	Декодер ЦВЗ

Продовження таблиці 2.1

Метод	Тип ДКП	ЦВЗ	Схема вилучення	Детектор/декодер
Hsu (1999) Хсу та Ву	Поблоково	Bitmap зображення, ½ вихідного	Вихідне зображення	Декодер ЦВЗ
Barni (1998) Барні	ДКП всього зображення	Довільний рядок біт	Сліпа	Декодер ЦВЗ
Fridrich (1998) Фрідріх	Низькочастотні та середньочастотні коефіцієнти	Послідовність чисел {-1,1}	Сліпа	Декодер ЦВЗ
Podilchuk (1997) Подилчак	Поблоково	Випадковий процес	Вихідне зображення	Детектор ЦВЗ
Cox (1997) Кокс	ДКП всього зображення	Послідовність	Вихідне зображення	Детектор ЦВЗ

Коротко охарактеризуємо розглянуті методи захисного маркування растрових зображень.

В алгоритмі, розробленому Кохом і Жао [20], відбувається впровадження біт водяних знаків у блоки зображення розміром 8x8 пікселів, при цьому як ЦВЗ може використовуватися як монохромне зображення, так і певна послідовність {0,1}, що складається з довільної кількості чисел. Виявлення вбудованих у досліджуване зображення даних відбувається за сліпою схемою; при цьому відбувається вилучення впровадженої інформації.

Алгоритм, розроблений Бенхамом [21], вважається поліпшеною версією алгоритму Коха і Жао, оскільки впроваджені дані є стійкішими. Це досягається в результаті вибору негладких та багатоконтурних блоків для приховування біт ЦВЗ, а також використання для впровадження біт водяних знаків більшої кількості частотних коефіцієнтів усередині блоків 8x8

пікселів.

В алгоритмі Хсу і Ву [22] використання біт ЦВЗ також відбувається поблоково, крім того, при виявленні вбудованих даних у досліджуваному зображенні декодер дає на виході впроваджений ЦВЗ. Але розроблений метод передбачає використання монохромного зображення, розміром удвічі менше захищеного. Біти ЦВЗ піддаються випадковим перестановкам за допомогою ключа та впроваджуються середньочастотні характеристики блоку. Для виявлення вбудованого ЦВЗ потрібне використання промаркованого зображення. Даний метод нестійкий до стиснення з втратами, а також кадрування зображення.

Алгоритм Барні [23] використовує ДКП всього маркованого зображення, і є покращеною модифікацією методу Коксу [25], на відміну від якого використовує сліпу схему виявлення впроваджених даних та витягує впроваджену інформацію. Обидва алгоритми передбачають впровадження інформації в кілька АС-коефіцієнтів ДКП всього зображення, що захищається, тому цей метод буде нестійкий до кадрування.

Впровадження водяних знаків, що є послідовністю{-1,1}, відповідно до алгоритму Фрідріха [24] відбувається при попередньому ДКП всього зображення, що захищається, коефіцієнти якого піддаються подальшим перетворенням.

Алгоритм Подільчака [3] передбачає поблокове вбудовування даних, але при цьому не отримує впроваджену інформацію, а виявляє факт наявності маркування.

Після розгляду алгоритмів, що вбудовують водяні знаки в області ДКП, в якості основи для методики, що розробляється, був обраний алгоритм Коха і Жао, що має ряд переваг, придатних для вирішення поставлених задач. До них відносяться:

- поблокове дискретне косинусне перетворення растрового зображення;
- невибагливість до вибору блоків для вбудовування біт ЦВЗ;

- невибагливість до вибору виду водяних знаків (можна використовувати як двовимірне монохромне зображення, і числову послідовність);
- пошук біт впровадженої інформації за сліпою схемою;
- вилучення впровадженої інформації.

2.3. Метод Коха та Жао

Метод Коха і Жао і сьогодні є досить затребуваним [20]. Схема застосування даних з цього способу показано рисунку 2.2.

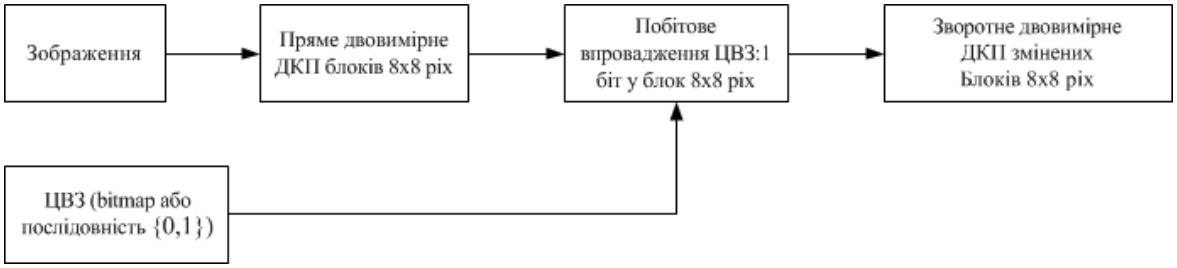

Рисунок 2.2 – Схема впровадження цифрових водяних знаків у зображення

Водяні знаки, призначені для захисного маркування зображень, можуть бути як монохромне (bitmap) зображення, так і числову послідовність {0,1} довільної довжини. Впровадження біт ЦВЗ за методом Коха і Жао здійснюється в блоки пікселів растрового зображення, яке може бути збережене у будь-якому з розглянутих у першому розділі графічних форматах, а також у будь-якій із розглянутих кольорових моделей.

Растрове зображення, що захищається, розбивається на N блоків (матриць) f_α розміром 8x8 пікселів, які піддаються двовимірному ДКП за формулою 2.1. При цьому кожна цілочисельна матриця пікселів зображення перетворюється на матрицю частотних коефіцієнтів. Перед початком маркування необхідно оцінити відповідність розмірів впроваджуваного ЦВЗ

кількості отриманих блоків зображення.

Далі отримані частотні матриці DCT_α здійснюють побітове вбудовування водяних знаків, при цьому кожен біт водяного знака впроваджується в блок 8x8 пікселів в результаті відносної заміни двох або трьох елементів матриці DCT_α. Надалі розглядатимемо алгоритм, заснований на модифікації двох коефіцієнтів частотної матриці.

Як було сказано в попередньому розділі, для людського зору більш суттєвими є області середніх частот, крім того, дані, вбудовані в такі частоти, будуть більш стійкими до JPEG-стиснення. Приклад вибору частотних коефіцієнтів застосування біт ЦВЗ показаний рисунку 2.3

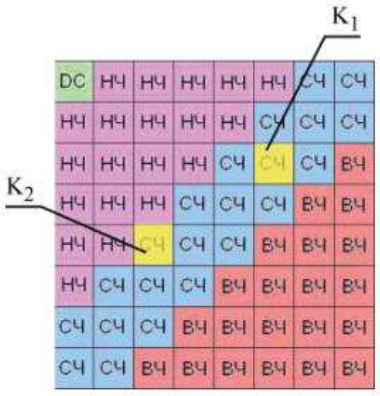

Рисунок 2.3 – Вибір коефіцієнтів K_1 та K_2

В одній з отриманих матриць растрового зображення, що захищається, з області середніх частот вибираються два коефіцієнти з координатами (u_1, ν_1). і (u_2,ν_2). Позначимо їх K_1 і K_2. Позиції (u_1, ν_1) та (u_2, ν_2) повинні бути однаковимидля всіх матриць DCT_α, що маркуються бітами ЦВЗ.

Захисне маркування растрового зображення водяними знаками починається з вибору блоків, призначених для впровадження біт ЦВЗ m_i. Залежно від співвідношення розмірів водяного знака і зображення, що захищається, а також від способу маркування, можлива зміна як всіх блоків зображення, так і їх частини.

Суть захисного маркування полягає у порівнянні модулів значень коефіцієнтів $К_1$ та $К_2$, і за необхідності, зміни значень одного з них залежно від значень вбудованого блок біта ЦВЗ.

Для маркування блоку бітом водяного знака, що має значення 0, необхідно виконання умови:

$$|K_1| - |K_2| > p \tag{2.4}$$

де ρ – цілочисельний параметр, що впливає на силу вбудовування біта, або коефіцієнт сили вбудовування [34].

Для вбудовування блок біта водяного знака, що має значення 1, добиваються виконання умови:

$$|K_1| - |K_2| > -p \tag{2.5}$$

Якщо умови 2.4 або 2.5 не виконуються, значення коефіцієнтів $К_1$ або $К_2$ коригують.

З нерівностей 2.4 і 2.5 видно, що чим більшу величину має коефіцієнт сили вбудовування ρ, тим більше змінюватимуться значення коефіцієнтів К [20].

Після впровадження в частотні матриці біт ЦВЗ здійснюється перехід до цілочисельних матриць шляхом зворотного дискретного косинусного перетворення за формулами 2.2 і 2.3.

Природним наслідком коригування значень коефіцієнтів К є деяке спотворення значень усіх пікселів промаркованих блоків. Вплив значення коефіцієнта сили вбудовування на растрове зображення і впроваджену інформацію полягає в такому: чим більша величина ρ, тим маркування стійкіше до стиснення з втратами, але водночас збільшення параметра сили вбудовування значно погіршує якість промаркованого зображення, за великих значень р можливе візуальне виявлення слідів маркування.

Для перевірки автентичності растрового зображення проводять виявлення захисного маркування. Схема виявлення біт впровадженої інформації показана на рисунку 2.4.

Рисунок 2.4 – Схема виявлення впровадженої інформації

Для перевірки наявності впровадженої інформації досліджуване растрове зображення розділяється на N`блоків-матриць $f`_{\alpha}$ розміром 8х8 пікселів, до яких також застосовується пряме двовимірне ДКП за формулою 2.1. В результаті цього перетворення матриці пікселів перетворюються в частотні матриці $DCT`_{\alpha}$.

Відповідно до схеми захисного маркування зображенняв отриманих частотних матрицях шукають значення біт водяних знаків. Для цього в частотних матрицях $DCT`_{\alpha}$ за відомими координатами $(u_1, \nu_1)$ та $(u_2, \nu_2)$) виділяються коефіцієнти $K`_1$ та $K`_2$. Ухвалення рішення про значення біт вбудованої інформації здійснюється відповідно до нерівностей

$$0 \text{ при} |K`_1| > |K`_2| \quad (2.6)$$

$$1 \text{ при} |K`_1| < |K`_2| \quad (2.7)$$

З виявлених значень біт формується вихідний водяний знак.

При використанні цього способу функція вилучення біт водяного знака

з растрового зображення обернена функції їх застосування. Тому за відсутності руйнівних впливів зображення чи, зокрема, на впроваджену інформацію, виявлений ЦВЗ має відповідати вихідному.

При розробці моделей захисного маркування та перевірки автентичності та цілісності захищених растрових зображень було вирішено впроваджувати біти ЦВЗ за методом Коха та Жао не на всі пікселі зображення. Передбачається попередній поділ зображення, що захищається на блоки і впровадження інформації в обрані за певною схемою частотні області, що у кожному їх. Таке поблочне вбудовування дозволить вирішити не лише проблему доказу автентичності растрових зображень, а й визначення їхньої цілісності після кадрування, або коригування окремихфрагментів.

У роботі [17] описано вплив методу Коха і Жао на спотворення растрового зображення, що захищається, які виникають при маркуванні. Для оцінки спотворює вплив автор використовував відношення рівня сигналу вихідного зображення до рівня шуму (PSNR), що визначається за формулою 2.8:

$$PSNR = \frac{N \times \max(F_x)^2}{\sum_{x=1}^{N}(F_x - F_x`)^2} \quad (2.8)$$

де N – число пікселів у зображенні;

$F`_x$ – значення пікселя вихідного растрового зображення;

F'_x – значення пікселя промаркованого зображення.

Значення $F`_x$ безпосередньо залежить від значення коефіцієнта сили вбудовування ρ, тому при великих значеннях ρ PSNR буде зменшуватися. На рисунку 2.5 [29] показаний приклад графіка залежності відношення рівнів сигналу та шуму відзначення коефіцієнта сили вбудовування ρ.

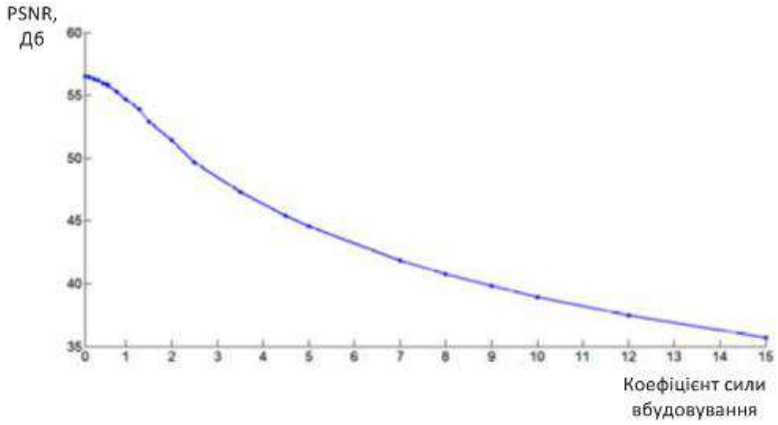

Рисунок 2.5 – Залежність PSNR від коефіцієнта сили вбудовування [29]

Як видно з графіка, при значеннях $\rho \leq 5$ промарковане растрове зображення незначно спотворюється, тому з точки зору підвищення скритності вбудованих ЦВЗ переважно вибирати невеликі значення коефіцієнта сили вбудовування.

3 РОЗРОБКА МОДЕЛЕЙ ЗАХИСТУ РАСТРОВИХ ЗОБРАЖЕНЬ

3.1 Моделі захисного маркування растрових зображень

Відповідно до моделі автентифікації цифрових зображень, яка детально представлена в роботі [26], пропонується наступна загальна схема інформаційної технології підтвердження права власності на цифрові зображення рис. 3.1.

Рисунок 3.1 – Загальна схема інформаційної технології підтвердження права власності на цифрові зображення

Процес підтвердження права власності на цифрове зображення пропонується проводити за етапами , які представлені на рис. 3.2.

З рис. 3.2 можемо виділити основні процеси, які забезпечують роботу технології підтвердження права власності на цифрове зображення:

1) реєстрація користувачів відповідними органами та компаніями, які відповідають за реєстрацію права власності. За результатами цього

користувач отримує права на внесення своїх зображень в систему та згідно з технологією блокчейн смарт-контракт, який буде його ідентифікатором в системі та дозволить здійснювати передачу авторських прав на зображення;

2) перевірка зображення на наявність цифрового водяного знаку та пошук дублікату зображення. Цей процес забезпечує захист від можливих повторних підписів захищених зображень та пошук дублікатів зображень для уникнення різного роду колізій;

3) генерація цифрового водяного знаку. Даний процес на основі даних користувача (смарт-контракт користувача), вхідного зображення створює смарт-контракт зображення та формування на його основі цифрового водяного знаку. Смарт-контракт зображення містить інформацію про зображення, про правовласника та час внесення в систему. За допомогою цього смарт-контракту відповідно до блокчейн технології відбуватиметься підтвердження права власності та можливість його передачі в комерційних цілях;

4) нанесення цифрового підпису на зображення. Даний процес на основі згенерованого ЦВЗ наносить підпис цифрового зображення та видає користувачеві захищену копію зображення. Також даний процес після підпису зображення забезпечує збереження оригінала зображення у розподіленій системі зберігання даних IPFS та внесення інформації про захищене зображення до блокчейн сховища;

5) перевірка автентичності зображення. Даний процес забезпечує локалізацію та вилучення цифрового водяного знаку з зображення, після чого перевіряє автентичність смарт-контракт зображення відповідно до технології блокчейн, цим самим забезпечуючи достовірність права власності на цифрове зображення;

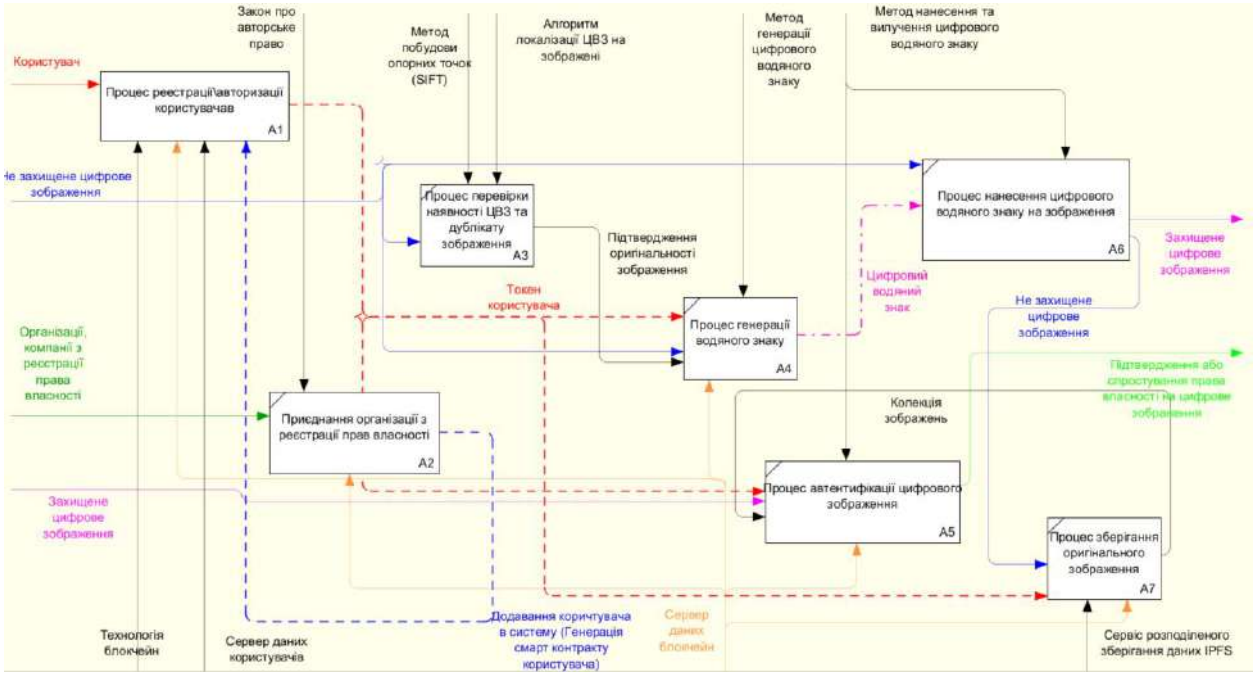

Рисунок 3.2 – Процес підтвердження права власності на цифрове зображення

Для реалізації даної технології була розроблена архітектура системи підтвердження права власності на цифрове зображення, яка представлена на рис. 3.3.

На рис. 3.3 показаний процес підтвердження автентичності цифрового зображення, який включає в себе обробку даних поза ланцюжком блокчейн і обробку даних в мережі блокчейн. Враховуючи різноманітність організацій, сервісів та систем, які можуть надавати послуги реєстрації авторського права, з точки зору структури збережених даних та функціональних можливостей доцільно запропонувати Rest API-рішення, як універсальну технологію для інтеграції таких систем та платформи обміну блокчейнами.

API-інтерфейс системи дозволяє всім зацікавленим особам та організаціям здійснювати основні операції з нею, такі як:

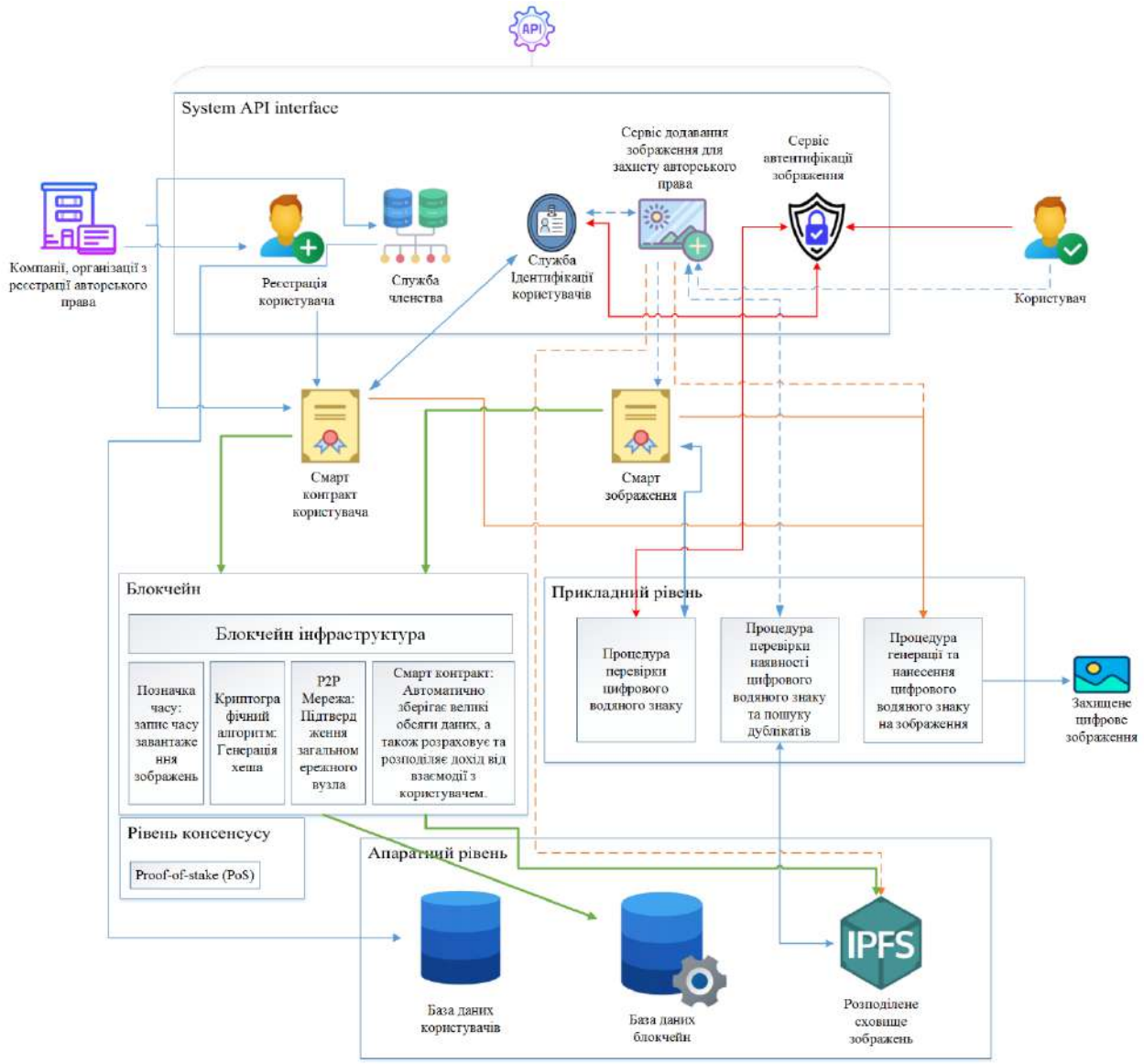

Рисунок 3.3 – Архітектура системи підтвердження права власності на цифрові зображення

- приєднання нової організації забезпечення права власності;
- створення відповідними організаціями користувачів системи (реєстрація користувача);
- додавання зображення для захисту права власності на нього;
- перевірка автентичності зображення. Весь процес перевірки поділяється на дві процедури, залежно від потреб організацій. Перша процедура – автентифікація власника захищеного зображення за допомогою смарт-контракту користувача. Друга процедура автентифікації – отримання детальної інформації про захищене цифрове зображення за допомогою

смарт-контракту зображення.

Прикладний рівень забезпечує реалізацію основних процесів захисту та автентифікації цифрових зображень. Він надає інтерфейс користувача, за допомогою якого здійснюється процедура нанесення цифрового підпису та автентифікації зображення. Також саме через цей рівень здійснюється процедура зберігання зображень, які підлягають захисту авторського права.

Рівень блокчейн. Цей процес починається зі створення «Початкового блока» для кожного зареєстрованого в системі користувача, який хоче забезпечити підтвердження авторства на свої цифрові зображення. Після чого всі транзакції записуються в блокчейн. Кожен блок містить унікальний заголовок, що ідентифікується по хешу заголовка блока. Блок складається з таких компонентів: хеш попереднього блока, інформація про правовласника, хеш-зображення, яке захищається, і мітка часу. Цей процес повторюється кожен раз коли користувач додає нове зображення в систему.

Рівень консенсусу. Оскільки система основується на блокчейн технології, то вона є децентралізованою і не контролюється жодною з організацій реєстрації авторського права. Тому потрібен спосіб перевірки транзакцій в системі. Одним з методів, який використовують багато систем, заснованих на блокчейн, є доказ частки (Proof of Stak). Цей метод є альтернативою методу доказу роботи (Proof of Work), першим механізмом консенсусу, розробленим для криптовалют. Оскільки доказ частки (Proof of Stak) набагато енергоефективніший, тому він пропонується для перевірки транзакцій в системі. Модель proof-of-stake дозволяє власникам робити ставки на активи системи та створювати свої власні вузли-валідатори. Стейкінг - це процес, коли учасник мережі блокчейн зобов'язуєтеся використовувати свої активи для перевірки транзакцій. Коли блок транзакцій буде готовий для обробки протокол підтвердження частки обирає вузол-валідатор для перевірки блоку. Валідатор перевіряє правильність транзакцій у блоці. Якщо це так, вони додають блок у ланцюжок блоків та отримують крипто-нагороди за свій внесок. Однак, якщо валідатор пропонує додати

блок з неточною інформацією, він втрачає частину своїх стейкінгових активів як штраф.

Апаратний рівень. Як показано на рис. 4 апаратний рівень складається з трьох основних компонентів:

- сховища авторизованих користувачів – централізованої база даних організації (державних органів, організацій забезпечення права власності), зареєстрованих як користувачі. Він використовує службу членства, яка має доступ до отримання даних за допомогою RestAPI.

- сховища блокчейн даних – блокчейн консорціуму, який функціонує під керівництвом групи організацій, що забезпечує спільну трансформацію бізнесу між організаціями. У даному випадку координатор призначає унікальний доступ для кожного користувача (державних органів, організацій забезпечення права власності).

- розподіленого сховища – децентралізованого сховища зображень, для яких система забезпечує можливість підтвердження автентичності.

3.2 Алгоритм множинного захисного маркування растрових зображень

Алгоритм множинного захисного маркування растрових зображень полягає в наступному [9, 14, 17].

Захищене растрове зображення зберігається в режимі RGB з 24-бітною глибиною представлення, відтворюючи в трьох колірних каналах по 256 кольорів кожен до шістнадцяти мільйонів кольорів.

Кожен піксель зображення представляється як кортежу pix=<r, g, b>, де $r \in [0;255]$ – значення інтенсивності кольору пікселя по червоному каналу, $g \in [0;255]$ – значення інтенсивності кольору пікселя по зеленому каналу, $b \in [0; 255]$ – значення інтенсивностей кольору пікселя по синьому каналу.

Растрове зображення можна у вигляді двовимірної матриці $Pict = |pix_{ij}|$, $i \in [l;h]$, $j \in [l;w]$, де w – кількість пікселів зображення по горизонталі, h – його

кількість пікселів по вертикалі.

У зв'язку з необхідністю визначення цілісності кожного з фрагментів растрового зображення двовимірна матриця Pict представляється у вигляді $h_\rho * w_\rho$ квадратних підматриц (блоків) $P_{k,l}$, $k \in [l;h_\rho]$, $l \in [l;w_\rho]$, де h_ρ – кількість квадратних блоків зображення за висотою w_ρ – кількість квадратних блоків зображення по ширині. Розмір кожного з отриманих блоків $P_{k,l}$ становить 64x64 пікселі. Якщо зображення, що захищається, не кратно 64 по горизонталі та/або вертикалі, що залишилися після розбиття неповні підматриці-блоки Pgn шириною [1;63] пікселя розміщуються по правому краю матриці Pict, а неповні підматриці-блоки Pvn висотою [1;63] пікселя розміщуються по її нижньому краю.

Кожна з отриманих підматриць $P_{k,l}$ є кортежем із матриць трьох колірних площин за кількістю каналів зображення, тобто.

P=<Red, Green,Blue>,

де Red = $|R_{ij}|$ – двовимірна матриця значень інтенсивностей кольору пікселя по червоному каналу зображення;

Green = $|G_{ij}|$ – двовимірна матриця значень інтенсивностей кольору пікселя по зелений канал зображення;

Blue = $|B_{ij}|$ – двовимірна матриця значень інтенсивностей кольору пікселя по синьому каналу зображення:

де $i \in [r,h_{fr}]$,$j \in [l;w_{fr}]$;

$pix_{ij} = <R_{ij}, G_{ij}, B_{ij}>$;

h_{fr} – кількість пікселів фрагментів за висотою;

w_{fr} – кількість пікселів фрагментів за шириною.

R_{ij}, G_{ij}, B_{ij} приймають значення з інтервалу [0; 255].

Аналогічно, отримані матриці Pgn і Pvn подаються у вигляді кортежів $Pgn = <Red_g, Green_g, Blue_g>$ та $Pvn = <Red_v, Green_v, Blue_v>$.

$Red_g = |Rg_{ij}|$ та $Red_v = |Rv_{ij}|$ – двовимірні матриці значень інтенсивностей кольору пікселя по червоному каналу зображення,

$Green_g = |Gg_{ij}|$ та $Green_v = |Gv_{ij}|$ – двовимірні матриці значень

інтенсивностей кольору пікселя по зеленому каналу зображення,

$Blue_g = |Bg_{ij}|$ та $Blue_v = |Bv_{ij}|$ – двовимірні матриці значень інтенсивностей кольору пікселя по синьому каналу зображення:

де $i \in [r, h_{fr}]$, $j \in [l; w_{fr}]$;

h_{fr} – кількість пікселів фрагментів за висотою;

w_{fr} – кількість пікселів фрагментів за шириною.

Rg_{ij}, Gg_{ij}, Bg_{ij}, Rv_{ij}, Gv_{ij}, Bvjjприймають значення з інтервалу [0; 255].

Оскільки, як було зазначено в першому розділі, СЛЗ добре сприйнятлива до спотворень у зеленому каналі зображення, біти захисного маркування двома видами ЦВЗ переважно впроваджуються в матрицю Blue (сприйнятливість 4 з 8 біт) і, меншою мірою, в матрицю Red (сприйнятливість 7 із 8 біт).

Монохромний логотип і електронні сигнатури, що впроваджуються в захищене зображення, готуються до впровадження наступним чином.

Монохромний логотип представляється у вигляді матриці $Logo = |Log_{f,h}|$, $Log_{f,h}$ [0; l], $f \in [l, h_{log}]$, $h \in [l, w_{log}]$:

де h_{log} – кількість біт логотипу за його висотою,

w_{log} – кількість біт за шириною.

Як було зазначено вище, електронні сигнатури являють собою 16-бітні розміри зображення в пікселях за висотою і шириною, а також 16-бітні контрольні суми (CRC) за різними характеристиками матриць блоків зображення, що захищається. ЕП впроваджуються в блоки зображення циклічно відповідно до заданого алгоритму формування видів сигнатур (наприклад, CRC по поточній матриці Red, CRC по поточній матриці Green, CRC по поточній матриці Blue, ширина растрового зображення в пікселях, висота растрового зображення в пікселях). Для матриць Blue CRC складаються без включення їх центральних областей $BC=|BC_{ij}|$, де $i \in [l;32]$, $j \in [l;32]$.

Для всіх матриць Red і Blue без зачіплення їх центральних областей

RC=|RC_{ij}| і BC=|BC_{ij}|, де і ∈ [1;32], j∈ [l;32], вибираються підматриці, що не перекриваються $RLog_d$=|RL_{ij}| і $BLog_d$=|BL_{ij}|, де d∈ [l;(h_{log}*w_{log})/2], I∈ [1;8],J ∈ [1;8].

Розташування складових підматриці $RLog_d$ і $BLog_d$ елементів однаково для всіх підматриць-блоків Red і Blue. До всіх вибраних підматриць застосовується двовимірне ДКП за формулою 2.1.

Нехай $DRLog_d$ та $DBLog_d$ – матриці, отримані в результаті двовимірного ДКП з матриць $RLog_d$ та $BLog_d$. Вбудовування елементів матриці Logo частотні матриці $DRLog_d$ і $DBLog_d$ проводиться в результаті перетворення обраних коефіцієнтів, однакових для всіх цих матриць, за формулами 2.4 і 2.5.

До всіх центральних областей матриць Blue BC=|BC_{ij}|, де і∈ [1;32], j∈ [l;32], також застосовується двовимірне ДКП за формулою 2.1. Далі проводиться формування значень електронних сигнатур відповідно до заданого алгоритму та їх впровадження в матриці Blue BC в результаті перетворення вибраних коефіцієнтів, однакових для всіх цих матриць, за формулами 2.4 та 2.5

Схематичне представлення застосування захисного маркування монохромним логотипом і електронними сигнатурами показано рисунку 3.4: а – використання біт логотипу в підматриці Blue, б – використання біт логотипу і ЕП в підматриці Red.

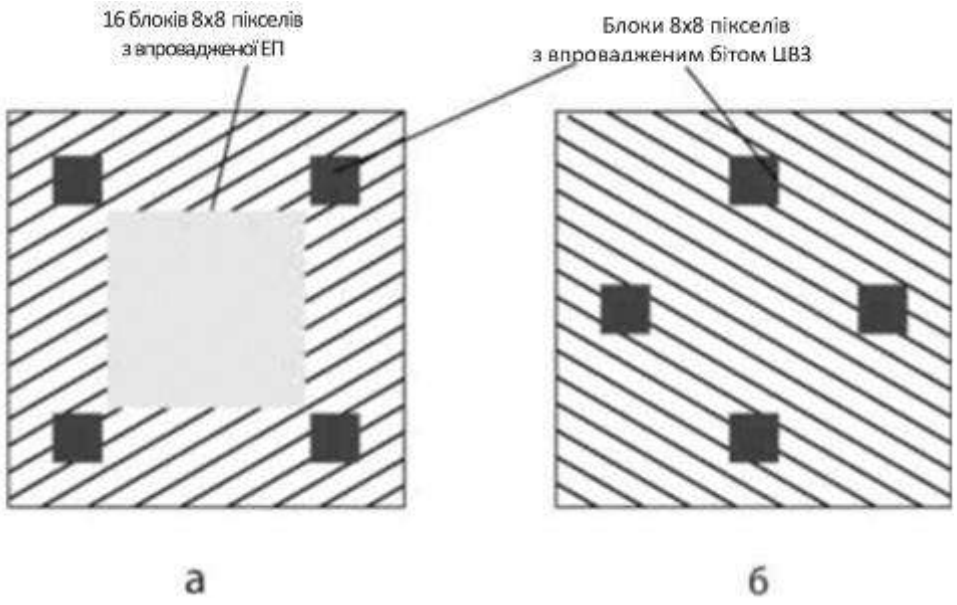

Рисунок 3.4 – Схематичне подання впровадження захисного маркування вблок зображення розміром 64 х 64 пікселя

Захисне маркування підматриць-блоків Pgn і Pvn відрізняється від маркування підматрицей P: такі блоки не маркуються електронними сигнатурами, в них вбудовуються лише біти монохромного логотипу.

Якщо блок Pgn або Pvn має розмір менше 64, але більше 12 пікселів з одного боку, вбудовування біт монохромного логотипу здійснюється через рівні інтервали вздовж його більшої сторони. У блоці, що знаходиться в нижньому правому куті зображення (кутовому блоці), біти монохромного логотипувбудовуються в матрицю синього каналу по вершинах прямокутника, який формує блок, а в матрицю червоного каналу - по серединах його сторін. При цьому розмір кутового блоку по обидва боки повинен бути не менше 32х32 пікселя. Приклад схематичного представлення застосування захисної маркування монохромним логотипом в неповні нижні і праві блоки, і навіть у кутовий блок показано риснку 3.5: а – використання біт логотипу в підматриці синього каналу, б – використання біт логотипу в підматриці червоного каналу.

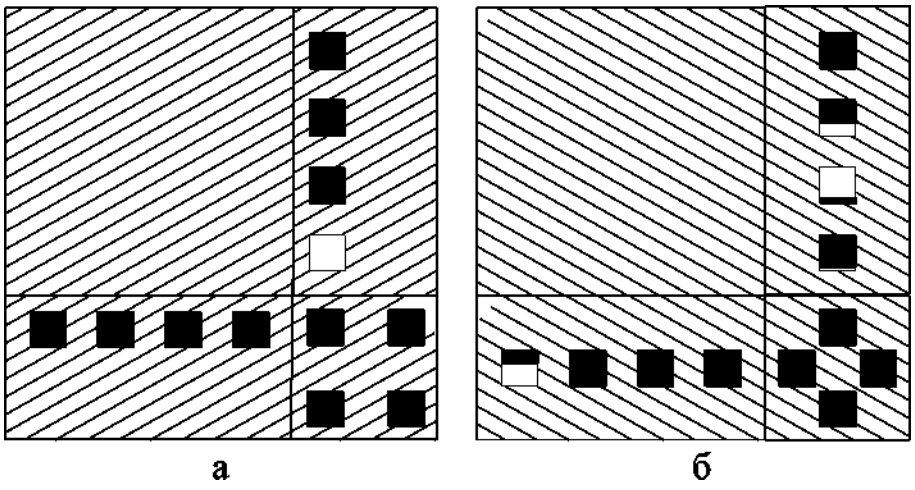

Рисунок 3.5 – Схематичне подання впровадження захисного маркування у неповні нижні та неповні праві блоки зображення, а також у неповний кутовий блок

Кутовий блок розміром трохи більше 9x9 пікселів не маркується.

Для всіх матриць Red_g і $Blue_g$, а також Red_v і $Blue_v$ вибираються підматриці, що не перекриваються $RgLog_d=|RgL_{ij}|$ і $BgLog_d=|BgLjj|$, а також $RvLogd=|RgL_{ij}|$ і $BvLog_d=|BgL_{ij}|$ відповідно, де

$d \in [l;(h_{log}*w_{log})/2]$,

$I \in [1;8], J \in [1;8]$.

Розташування складових підматриці $RgLog_d$ і $BgLog_d$ елементів однаково всім подматриц-блоков Redg і Blueg. Аналогічно розташування складових підматриці $RvLog_d$ і $BvLog_d$ елементів однаково всім підматриць-блоків Red_v і $Blue_v$.Ко всім обраним підматрицям застосовується двовимірне ДКП за формулою 2.1.

Нехай DRgLogd та DBgLogd – матриці, отримані в результаті двовимірного ДКП з матриць $RLog_d$ та $BLog_d$, $DRvLog_d$ та $DBvLog_d$ – матриці, отримані в результаті двовимірного ДКП з матриць $RvLog_d$ та $BvLog_d$. Вбудовування елементів матриці Logo отримані частотні матриці проводиться в результаті перетворення обраних коефіцієнтів, однакових для всіх цих матриць, за формулами 2.4 і 2.5.

Після маркування до частотних матриць всіх блоків зображення, що захищається застосовується зворотне ДКП за формулами 2.2 і 2.3. Отримане промарковане растрове зображення зберігається у новому файлі.

3.3 Алгоритм перевірки цілісності промаркованих растрових зображень

Для перевірки автентичності та цілісності промаркованого растрового зображення Pict` потрібно визначити розбиття зображення на квадратні блоки-підматриці (Pict`=| $P`_{k,l}$|),промарковані бітами монохромного логотипу, а потім перевірити коректність значень електронних сигнатур у кожному знайденому блоці.

Для визначення розбиття зображення на підматриці необхідно знати схему розташування біт монохромного логотипу. Схема розташування біт і вид логотипу стосовно кожного зображення вносяться до бази даних після впровадження захисного маркування разом із промаркованим зображенням.

У разі кадрування промаркованого зображення, його нарощування додатковими областями по краях, або додавання до нього сторонніх об'єктів, можливе зміщення координат підматриць-блоків розміром 64 х 64 пікселя. У зв'язку з цим для пошуку правильного розбиття захищеного растрового зображення підматриці доцільно використовувати наступний алгоритм.

Спочатку передбачається, що усунення підматриць-блоків (розміром 64 х 64 пікселя) по горизонталі та по вертикалі дорівнюють нулю.

В отриманих частотних підматрицях відбувається пошук бітів монохромного логотипу Logo' за формулами 2.6 і 2.7. У разі коректного знаходження всіх біт логотипу Logo, отримана матриця порівнюється з матрицею Logo. У разі ідентичності матриць дана матриця вважається знайденою коректно, тобто знайдено базовий блок.

В іншому випадку можливе зміщення поточної позиції по горизонталі наодин піксель (при цьому зсув проводиться в інтервалі [1; 64]), або на величину одного блоку (при цьому зсув проводиться в інтервалі [l; w'p]).

Якщо у першому чи другому випадку відбувається вихід межі інтервалу, поточному зміщенню по горизонталі присвоюється значення, рівне 0, і відбувається зміщення позицій по вертикалі однією піксель (в інтервалі [1; 64]), чи величину одного блоку (в інтервалі [l; h $'_P$]).

Якщо перевірені всі точки в заданому діапазоні, базовий блок вважається не знайдений. Після цього генерується наступне зміщення по вертикалі та горизонталі, і алгоритм повторюється до знаходження базового блоку.

Розташування біт монохромного логотипу в базовому блоці вказує на місцезнаходження центральної області з впровадженими бітами електронної сигнатури. Для перевірки коректності ЕП блоку необхідно обчислити її значення за формулами 2.6-2.7 та порівняти його з розрахованим згідно з логотипом розміщення. У разі збігу значень базовий блок вважається автентичним та цілісним. Якщо монохромний логотип, знайдений у блоці, є коректним, а виявлене значення електронної сигнатури не збігається з розрахунковим, цей блок вважається зміненим.

Після визначення базового блоку промарковане зображення ділиться на підматриці, починаючи з цього блоку, і перевірка автентичності і цілісності інших матриць цього зображення Фактично можливі три результати перевірки блоку растрового зображення:

- у першому випадку за відсутності біт монохромного логотипа в блоці, що перевіряється, вважається, що дана підматриця не містилася у вихідному зображенні(сторонній фрагмент), або зображення в підматриці було змінено;

- у другому випадку всі біти монохромного логотипу знайдені коректно, але виявлене значення електронної сигнатури не збігається з розрахунковим. В даному випадку можна припустити, що або зображення зазнавало змін, що не торкнулися області застосування біт логотипу, або в даному блоці міститься стороння інформація, що також не торкнулася області з впровадженими бітами логотипу;

- у третьому випадку у блоці коректно детектуються біти монохромного логотипу, а знайдене значення електронної сигнатури збігається з розрахунковим. В даному випадку можна стверджувати, що цей блок є автентичним та цілісним.

Аналогічно базовому блоку аналізується коректність всіх підматриць зображення. Блоки з коректно знайденим монохромним логотипом та модифіковані блоки можуть об'єднуватись у єдині області. За рахунок подібного перетворення можна зробити висновок про межі, в яких проводилася модифікація промаркованого растрового зображення.

У разі коли всі інші підматриці, крім знайденого базового блоку, не містять коректно знайдених біт монохромного логотипу, можливе збереження поточних значень зсуву по горизонталі і вертикалі з подальшим зміщенням і перевіркою підматриць до моменту знаходження нового базового блоку. Після визначення промарковане зображення ділиться на підматриці, починаючи з цього блоку, після чого проводиться їх перевірка на автентичність і цілісність. У разі коректного знаходження монохромного логотипу в більшості підматриць можна припустити, що спочатку знайдений блок зміщений щодо основного зображення

4 ПРАКТИЧНА РЕАЛІЗАЦІЯ РОЗРОБЛЕНИХ МОДЕЛЕЙ

4.1 Програмний модуль

Розроблені моделі та алгоритми були реалізовані у вигляді програмного модуля, написаного мовою програмування C# та призначеного для роботи в ОС Windows (версії XP та вище). При проектуванні програмного модуля було вирішено керуватися схемою архітектури програмного комплексу стеганографічного приховування інформації в графічних файлах, запропонованого в роботі [15]. Схема архітектури показано рисунку 4.1

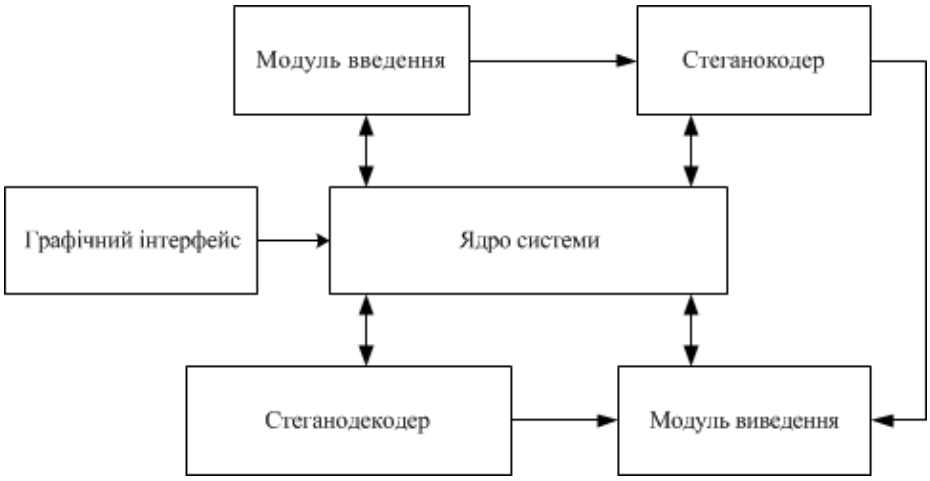

Рисунок 4.1 – Приклад архітектури програмного комплексу приховування інформації

Головне вікно розробленого програмного модуля показано рисунку 4.2.

Рисунок 4.2 – Основне вікно програмного модуля

Це вікно складається з наступних блоків:

- блок «Зображення», що відображає вихідне, промарковане або досліджуване растрове зображення, а також візуалізацію перевірки автентичності та цілісності зображення, що досліджується;

- блок «Вигляд та збереження», що дозволяє вибрати тип відображення растрового зображення (звичайний, R-G- або B-канали, а також візуалізація перевірки зображення). При натисканні на кнопку "Збереження" дозволяє зберегти поточне відображення растрового зображення в окремий файл;

- блок "Параметри". У цьому блоці користувач може задати власний монохромний логотип і вибрати необхідне значення коефіцієнта сили вбудовування ρ;

- блок "Відображення блоків", що показує області зображення, що мають розмір 64 x 64 пікселя (блоки);

- блок «Зсув», що дозволяє вибрати режим перерозподілу досліджуваного зображення на блоки для пошуку впроваджених даних;

- блок "Події". Даний блок дозволяє контролювати процес захисного маркування, процес її пошуку в досліджуваному зображенні, візуалізувати знайдений монохромний логотип і величину зміщення блоку, а також переривати перевірку наявності захисного маркування.

Для захисного маркування растрових зображень у розробленому програмному модулі передбачено два види ЦВЗ:

- 8-бітний монохромний логотип розміром 4x2 пікселів;

- 5типів електронних сигнатур, що циклічно вбудовуються зверху вниз в центральну область блоків зображення, що захищається: 16-ти бітна CRC по червоному каналу поточного блоку, 16-бітна CRC по зеленому каналу поточного блоку, 16-бітна CRC по синьому каналу поточного блоку (без розгляду області вбудовування ЕП), ширина зображення та його висота.

Розроблений програмний модуль надає користувачеві такі можливості:

- захисне маркування растрового зображення з можливістю створення власного монохромного логотипу та автоматично генерованими електронними сигнатурами;

- збереження промаркованого растрового зображення в окремому файлі PNG;

- пошук у досліджуваному растровому зображенні захисного маркування (монохромний логотип та електронні сигнатури);

- перевірка цілісності досліджуваного растрового зображення за допомогою дослідження всіх його блоків на наявність та збіг логотипу, а також за допомогою порівняння розрахункових та знайдених у блоках значень ЕП;

- графічна візуалізація результатів перевірки автентичності та цілісності виділенням кольором оригінальних та фальсифікованих блоків, а також коректних та некоректних електронних сигнатур;

- можливість збереження результату візуалізації в окремий файл формату PNG

Діаграма класів розробленого програмного модуля представлена на рисунку 4.3.

Рисунок 4.3 – Діаграма класів розробленого програмного модуля

Коротка характеристика показаним на діаграмі класів наведено в таблиці 4.1.

Таблиця 4.1 – Класи програмного модуля

Клас	**Призначення**
DKP	Двовимірне Дискретно-Косинусне Перетворення (ДКП)
BlockSepar	Розбиття зображення на блоки та їх перетворення
Клас	Призначення
CRC	Клас, який відповідає за роботу з електронною
CVZ	Клас, який відповідає за роботу з монохромним
CVZInterfa	Організація взаємодії функцій ЦВЗ
DataBlock	Інформація про координати для
GBox	Опис блоку 64 х 64
PictData	Дані про зображення
PictDrawin	Малювання
Recognitio	Розпізнавання
Main Form	Взаємодія з інтерфейсом програмного модуля

Розроблений програмний продукт дозволив провести серію експериментів щодо дослідження стійкості захисної інформації, впровадженої в комплект із п'ятдесяти тестових растрових зображень, взятих з особистого архіву дисертанта, до різних впливів на них.

4.2 Експериментальна оцінка безпеки інформації післяатак на зображення

У першому розділі роботи були описані види атак, яким може зазнати захищене растрове зображення. Після захисного маркування тестових зображень з використанням розробленого програмного продукту було проведено серію експериментів на п'ятдесяти тестових зображень з метою дослідження стійкості вкладеної інформації до різних атак на захищені зображення. Усі тестові зображення було взято з особистого фотоархіву дисертанта.

Додавання сторонніх фрагментів.

Цей вид спотворення захищених зображень можливий у разі фальшування з метою свідомого спотворення реальної інформації, а також у разі створення різних колажів та композицій.

Під час експериментів до відкритих у графічному редакторі промаркованих тестових растрових зображень додавалися сторонні фрагменти різних типів:

- растрові фрагменти не промаркованих зображень;
- фрагменти растрових зображень, промаркованих монохромним логотип, що відрізняється від логотипу, вбудованого в досліджуване зображення;
- фрагменти растрових зображень, промарковані тим же монохромним логотипом, що і вихідне зображення.

Після додавання стороннього фрагмента змінене промарковане зображення зберігалося під іншим ім'ям у графічному форматі PNG. Далі

збережене растрове зображення досліджувалося автентичність і цілісність за допомогою функції «Розпізнавання» розробленого програмного модуля. Проведена серія експериментів призвела до таких результатів.

При додаванні до промаркованого зображення чужорідних фрагментів монохромний логотип коректно детектувався у всі блоки, що піддавалися зміні, і не детектувався в блоках, повністю перекритих сторонніми фрагментами. У блоках, що містять сторонню та оригінальну інформацію, виявлення вбудованого логотипу залежало від геометрії та розташування пікселів чужорідних фрагментів. У разі коли блоки, що містять біти цього водяного знака, не перекривалися сторонньоїінформацією, логотип детектувався коректно.

Значення електронних сигнатур були коректними в блоках, які не зазнавали змін, а також у блоках, в яких значення ЕП відповідало геометричним параметрам вихідного зображення, а область вбудовування біт сигнатури не перекривалася пікселями чужорідних фрагментів. У блоках, що містять лише сторонні дані, значення електронної сигнатури були неправильними. У блоках, що містять оригінальну та чужорідну інформацію, значення сигнатури, що відповідає інформації про яскравість блоків, детектувалися як помилкові.

У разі додавання сторонніх фрагментів, промаркованих тим самим монохромним логотипом, що і вихідне растрове зображення, логотип коректно детектувався у всіх блоках, що не піддавалися зміні. У повністю перекритих сторонними фрагментами блоках виявлення логотипу було можливе лише у разі повного збігу меж промаркованих блоків чужорідних фрагментів та оригінального зображення. Значення електронних сигнатур були коректними в блоках, що не зазнавали змін, та в блоках з оригінальною областю ЕП, значення якої відповідало геометричним параметрам вихідного зображення. У блоках, що містять лише сторонні дані, значення електронної сигнатури булиневірні.

На риснку 4.4 показаний приклад знаходження сторонніх фрагментів у зображенні, отриманому в результаті перевірки промаркованого тестовогозображення за допомогою функції «Розпізнавання» розробленого

програмного модуля.

Область зображення, що містить сторонні фрагменти, виділена контрастним кольором, оскільки чужорідна інформація перекриває області вбудовування біт логотипу, внаслідок чого він не детектується. Темні діагональні мітки вказують на невідповідність фактичного та розрахункового значень ЕП. Світла діагональна мітка у правому нижньому блоці області з сторонніми фрагментами вказує на збіг фактичного та розрахункового значення ЕП, оскільки у значенні сигнатури цього блоку закодована ширинавихідного зображення.

Рисунок 4.4 – Растрове зображення з доданим стороннім фрагментом

Таким чином, серія проведених експериментів дозволила зробити такі висновки. Блоки, що містять сторонню інформацію, виявляються в результаті неправильного значення монохромного логотипу, або через некоректнезначення електронної сигнатури Помилкове ухвалення рішення про автентичність і цілісність блоку, що містить сторонні фрагменти, відбувається тільки в тих випадках, коли пікселі чужорідних вкладень не перекривають блоки з бітами водяних знаків, а значення сигнатури відповідає геометричним параметрам вихідного зображення .

Видалення фрагментів зображення.

При видаленні фрагментів промаркованих тестових зображень у їхній растрової структурі утворюються однорідно забарвлені області. Під це поняття також підпадають різні на зображення з метою його ретуші: наприклад, усунення дефектів чи зміна фрагментів з допомогою інструмента «пензель».

У ході експериментів у відкритих у графічному редакторі тестових зображеннях виділялися фрагменти різної форми. Виділені області видалялися за допомогою інструмента Cut, або зафарбовувалися однотонним кольором за допомогою інструментів заливка або кисть. Отримане після видалення фрагментів зображення зберігалося під іншим ім'ям у графічному форматі PNG і досліджувалося на автентичність та цілісність за допомогою функції «Розпізнавання» розробленого програмного модуля.

Проведена серія експериментів показала, що змінені блоки можуть детектуватися по-різному в залежності від значень впроваджених в них електронних сигнатур, а також форми та розташування віддалених фрагментів зображення щодо областей вбудовування біт водяних знаків.

Монохромний логотип детектувався коректно лише в тих випадках, коли віддалені фрагменти не включали областей вбудовування біт логотипу. Значення електронної сигнатури збігалися з розрахунковими у разі, коли віддалені фрагменти не включали областей вбудовування біт ЕП, а її значення відповідало геометричним параметрам вихідного зображення.

На рисунку 4.5 показаний приклад знаходження спотворених фрагментів у зображенні, отриманому в результаті перевірки промаркованого зображення за допомогою функції «Розпізнавання».

Блок зображення, який містить віддалені фрагменти, виділено контрастним кольором, оскільки логотип у цьому блоці не детектується. Фактичне та розрахункове значення ЕП збігаються, на що вказує світла діагональна мітка, оскільки у значенні сигнатури закодована ширина вихідного зображення.

Рисунок 4.5 – Растрове зображення з віддаленими фрагментами

Серія проведених експериментів дозволила зробити такі висновки. Блоки з віддаленими даними виявляються в результаті неправильного значення монохромного логотипу або через некоректне значення електронної сигнатури. Помилкове ухвалення рішення про автентичність і цілісність блоку з віддаленими даними відбувається тільки в тих випадках, коли пікселі чужорідних вкладень не перекривають блоки з бітами водяних знаків, а значення сигнатури відповідає геометричним параметрам вихідногозображення.

Клонування фрагментів зображення.

Під клонуванням фрагментів зображення в дисертації розуміється їхнє дублювання з подальшим зрушенням або переміщенням у межах вихідного зображення з метою створення необхідного ефекту. До цієї групи впливів відноситься як переміщення фрагментів зображення для фальсифікації або зміни його композиції, так і ретуш за допомогою різних інструментів, наприклад інструменту «латку», що часто використовується для усуненняплям, подряпин та інших дефектів зображення.

У ході експериментів у відкритих у графічному редакторі тестових зображеннях виділялися області різного розміру та форми. Виділені фрагменти дублювалися з подальшим їх зміщенням у межах зображення. Після клонування фрагментів отримане зображення зберігалося під іншим ім'ям у графічному форматі PNG і досліджувалося наавтентичність та цілісність за допомогою

функції «Розпізнавання» розробленого програмного модуля.

Проведена серія експериментів показала, що детектування логотипу в клонованих областях було можливим лише у разі повного збігу меж блоків клонованих фрагментів та оригінального зображення. При цьому значення електронних сигнатур вказували на зміну областей зображення через невідповідність типу ЕП заданому порядку їх розташування.

Також можливе детектування логотипу у разі, коли клоновані елементи малі та не перекривають області, що містять ЦВЗ. При цьому значення електронної сигнатури збігаються з розрахунковими у разі, коли в них було закодовано геометричні розміри вихідного зображення.

Рисунок 4.6 – Растрове зображення з клонованим фрагментом

На рисунку 4.6 показаний приклад знаходження зміненого фрагментазображенні, отриманому в результаті перевірки промаркованого зображення за допомогою функції «Розпізнавання». Область зображення, що містить клонований фрагмент, виділена контрастним кольором, що відповідає відсутності детектування логотипу. Темні діагональні мітки вказують на невідповідність фактичного та розрахункового значень ЕП Серія проведених експериментів дозволила зробити такі висновки. Клоновані фрагменти зображення виявляються в результаті неправильного значення монохромного логотипу та/або через некоректне значення електронної

сигнатури. Помилкове прийняття рішення про автентичність та цілісність блоку з віддаленими даними відбувається у випадках одночасного збігу меж клонованого та оригінальних блоків та відповідності типу електронної сигнатури порядку розташування ЕП, а також малих розмірів клонованих фрагментів при ЕП, що кодують геометричні параметри зображення.

JPEG-стиснення

Стиснення зображень, збережених у графічному форматі JPEG, відбувається за складним алгоритмом перетворення, що включає внутрішнє перетворення колірної моделі, двовимірне ДКП та квантування [32]. Суть квантування інформації полягає у відкиданні частини її обсягу відповідно до спеціальних таблиць або матриць цілих позитивних чисел, при цьому найбільш схильні до квантування високі частоти растрових зображень.

Експерименти дослідження стійкості захисного маркування до JPEG-стиснення проводилися наступним чином. Промарковані тестові зображення послідовно зберігалися у графічному форматі JPEG з коефіцієнтами якості від 12 до 8. Отримані зображення перевірялися на стійкість захисного маркування у розробленому програмному модулі здопомогою функції «Розпізнавання»

Проведені експерименти сприяли наступним результатам. У зображень, промаркованих з коефіцієнтом ρ=5..7 і збережених уформат JPEG з коефіцієнтом якості 12, монохромний логотип детектувався в більшості блоків. Блоки, у яких логотип був знайдено, розташовувалися випадковим чином. Значення електронних сигнатур також були коректними в більшості блоків, відмінні від розрахункових значення сигнатур знаходилися в блоках з логотипом, що коректно детектується. У 60% тестових зображень, промаркованих з коефіцієнтом ρ=5..7 та збережених з коефіцієнтом якості 11, захисне маркування монохромним логотипом не детектувалося, тобто доказ їхньої автентичності ставав неможливим.

При збереженні у графічному форматі з коефіцієнтом якості 11-12 JPEG тестових зображень, промаркованих з коефіцієнтом ρ=10..15, монохромний логотип детектується, більшість значень електронних сигнатур збігаються з

розрахунковими. У зображень, промаркованих зі значенням коефіцієнта ρ=40, монохромний логотип детектується при збереженні у форматі JPEG з коефіцієнтом якості 9, при цьому кількість блоків з помилковим значенням логотипу та електронних сигнатур збільшується.

На рисунку 4.17 показані приклади перевірки тестових зображень, збережених у форматі JPEG: а коефіцієнт якості JPEG 12, ρ=5; б -коефіцієнт якості JPEG 9, ρ = 40.

Серія проведених експериментів дозволила зробити такі висновки. JPEG-стиск є досить руйнівним впливом на захиснумаркування. При малих значеннях коефіцієнта сили вбудовування підтвердження автентичності зображення можливе лише за максимального значення коефіцієнта якості JPEG.

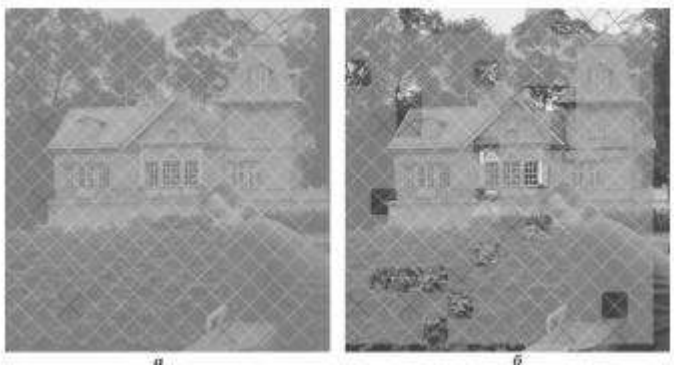

Рисунок 4.7 – Збереження маркування в растровому зображенні, збереженому вформаті JPEG з різними коефіцієнтами якості

На основі розроблених алгоритмів захисного маркування зображень та перевірки промаркованих зображень на автентичність та цілісність було створено програмний модуль, що показав стійку роботу розроблених моделей.

ВИСНОВКИ

У атестаційній роботі вирішена актуальна наукова задача з розробки методики захисту цифрових зображень на основі впровадження цифрових водяних знаків у частотні коефіцієнти зображення, що захищаються.

Було розроблено моделі захисного маркування растрових зображень та їх перевірки на автентичність та цілісність. Запропоноване рішення відрізняється від існуючих аналогів тим, що дозволяє розділяти модифіковані та незмінені фрагменти зображення.

Розроблено алгоритм захисного маркування фрагментів зображень, що дозволяє проводити використання біт водяних знаків з урахуванням системи людського зору і не залежить від наявності «відповідних» областей.

Розроблено алгоритм пошуку вбудованої інформації в зображеннях, що перевіряються за сліпою схемою, що дозволяє виділити наявність модифікованих фрагментів і види модифікації. На основі знайденого у зображенні маркування проводиться перевірка відсутності спотворень елементів.

Запропоновані теоретичні розробки реалізовані як програмного модуля мовою програмування C#.

Розроблена програмна реалізація дозволила підтвердити ефективність та практичну значущість розроблених моделей та алгоритмів.

Запропоновані алгоритми реалізовані як програмної системи мовою програмування C#.

Розроблені програмні засоби, на основі застосування яких були отримані практичні результати, підтвердили ефективність та практичну значущість розроблених моделей та алгоритмів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Maes M., Rongen P., van Overveld C. Digital image watermarking by salient point modification practical results // SPIE Conference on Security and Watermarking of Multimedia Contents. 1999. Vol. 3657. P. 273-282

2. Елементи інформатики [Текст] : довідник / В. С. Височанський, А. І. Кардаш, В. С. Костєв, В. В. Черняхівський. – К. : Наук. думка, 2003. – 192 с.

3. Podilchuk C., Zeng W. Perceptual watermarking of still images // Electronic Proceedings of the IEEE Workshop on Multimedia Signal Process-ing. 199

4. Tao B., Dickinson B. Adaptive watermarking in the DCT domain // Proceedings of the International Conference on Acoustics, Speech and Signal Processing. 1997

5. Nikolaidis N., Pitas I. Robust image watermarking in the spatial domain //Signal Processing, Special Issue on Copyright Protection and Control. 1998. Vol. 66.№ 3. P. 385-403

6. Білобокова Ю.А. Захист інформаційного змісту цифрових фотографій шляхом багаторазового маркування цифровими водяними знаками. / Ю.А. Білобокова, Е.С. Клишинський // М: «Системний адміністратор», 2014, № 4, квітень. – С. 70-73.

7. Білобокова Ю.А. Метод багаторазового маркування цифрових фотографій для захисту від фальшування / Ю.А. Білобокова, Є.В. Булатников// Известия Вищих навчальних закладів. Проблеми поліграфії та видавничої справи. – М.: «Московський державний університет друку», 2014. – № 2, березень-квітень. – С. 33-41.

8. Грибунін В.Г., ОковІ.М., ТуринцівІ.В. Цифрова стеганографія. Наука та навчання, 2002. – 288 с

9. Конахович Г.Ф., Пузиренко А.Ю. Комп'ютерна стеганографія.

Теорія та практика. МК-Прес. Київ, 2006. 288 с.

10. Osborne C., van Schyndel R., Tirkel A. A Digital Watermark // IEEE Intern. Conf. on Image Processing, 1994. P. 86-90

11. Волосатова Т.М., Чичварін Н.В. Специфіка інформаційної безпеки САПР. // Вісті ВНЗ. Сер. "Машинобудування". – 2012. – № Фундаментальні проблеми створення. – С. 89-94.

12. Горбачов В.М., Кайнарова О.М., Кулик О.М., Метелєв І.К. Методи цифрової стеганографії для захисту зображальної інформації. // М.: Проблеми поліграфії та видавничої справи. - 2011. - № 2. С. 32-49

13. Шарова М.Д. Вивчення властивостей електронного водяного знака, вбудованого в частотну область стегоконтейнера. // Системний аналіз у науці та освіті. – 2012. – Випуск №3. С.

14. Аграновський А.В., БалакінА.В., ХадіР.А. Навчальні системи стеганографії/О.В. Аграновський, А.В. Балакін, Р.А. Хаді// Донецьк: Штучний інтелект. -2002. -№4. З. 132-135.

15. Партика Т.Л., Попов І.І. Інформаційна безпека. М.: ФОРУМ, 2010. - 432 с

16. Кайнов П.А., Борисенко Б.Б. Впровадження цифрових водяних знаків з використанням сегментації зображення. // Вістн. КТУ. - 2013. - Т. 16, № 4. С. 286-291.

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

18. Гонсалес Р., Вудс Р. Цифрова обробка зображень. М.: Техносфера, 2005. - 1072 с.

19. Kutter M., Jordan F., Bossen F. Digital signature of color images using amplitude modulation // Journal of Electronics Imaging, Vol. 7. 1998. P. 326-332

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

21. Benham D., Memon N., Yeo B.-L., Yeung M. Fast watermarking of DCTbased compressed images // Proc. of the International Conference on Image Science, Systems and Technology. 1997. P. 243-252.

22. Hsu C.-T., Wu J.-L. Hidden digital watermarks in images // IEEE Transactions on Image Processing. 1999. Vol. 8. № 1. P. 58-68

23. Barni M., Bartolini R., Cappellini V., Piva A. A DCT-domain system for robust image watermarking // Signal Processing, Special Issue on Copyright Protection and Control. 1998. Vol. 66. № 3. P. 357-372

24. Fridrich J. Combining low-frequency and spread spectrum watermarking // Proceedings of the SPIE Conference on Mathematics of Data/Image Coding, Compression and Encryption. 1998. Vol. 3456. P. 2-12

25. Cox I., Kilian J., Leighton T., Shamoon T. Secure spread spectrum watermarking for multimedia // IEEE Transactions on Image Processing. 1997. Vol. 6. № 12. P. 1673-1687.

26. Ruban, I., Bolohova, N., Martovytskyi, V., & Koptsev, O. (2021). DIGITAL IMAGE AUTHENTICATION MODEL. Advanced Information Systems, 5(1), 113-117.