МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ПРИРОДОКОРИСТУВАННЯ
ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ
ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

перший (бакалаврський) рівень вищої освіти

на тему:

«Розробка системи нанесення видимих цифрових водяних знаків на відео та графічний контент для захисту авторських прав»

Виконала: студентка
групи ІТ-41
спеціальності 126 «Інформаційні системи та технології»
Гординяк М.М.
(прізвище та ініціали)

Керівник: **Станько В.Ю.**
(прізвище та ініціали)

ДУБЛЯНИ 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ПРИРОДОКОРИСТУВАННЯ
ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ
ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Перший (бакалаврський) рівень вищої освіти
Спеціальність 126 «Інформаційні системи та технології»

"ЗАТВЕРДЖУЮ"
Завідувач кафедри

_____
(підпис)

д.т.н., професор, Тригуба А.М.
"____"_____ 202_ р.

ЗАВДАННЯ
на кваліфікаційну роботу
Гординяк Марії Михайлівни

1. Тема роботи: *«Розробка системи нанесення видимих цифрових водяних знаків на відео та графічний контент для захисту авторських прав»*
Керівник роботи *к.е.н. Станько В.Ю.*
Затверджені наказом по університету *від 27.11.2023 року № 641/к-с*

2. Строк подання студентом роботи *10.06.2024 р.*

3. Вихідні дані до роботи: *характеристика сучасних інформаційних систем, вимоги до побудови інформаційних систем, науково-технічна і довідкова література, засоби створення та мови програмування, методика нанесення ЦВЗ на графічний контент.*

4. Зміст розрахунково-пояснювальної записки: (перелік питань, які потрібно розробити) *Вступ*
1. Аналіз предметної області
2. Постановка задачі
3. Проектування методів дослідження системи нанесення ЦВЗ для захисту авторських прав
4. Охорона праці та безпека в надзвичайних ситуаціях
Висновки та пропозиції
Бібліографічний список
Додатки

5. Перелік графічного матеріалу: *Графічний матеріал подається у вигляді презентації*

6. Консультанти з розділів:

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1, 2, 3	*Станько В.Ю., в.о. доцента кафедри інформаційних систем та технологій*		
5	*Городецький І.М., доцент кафедри фізики, інженерної механіки та безпеки виробництва*		

7. Дата видачі завдання *30.11.2023 р.*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту	Строк виконання етапів роботи	Відмітка про виконання
1.	*Написання першого розділу та означення головних завдань роботи*	*30.11.2023 – 03.01.2024*	
2.	*Виконання другого розділу та формування головних алгоритмів*	*04.01.2024 – 28.02.2024*	
3.	*Виконання третього розділу, розрахунків та розробка проектної частини*	*01.03.2024 – 30.03.2024*	
4.	*Написання розділу: «Охорона праці та безпека в надзвичайних ситуаціях»*	*01.04.2024 – 30.04.2024*	
5.	*Завершення оформлення розрахунково-пояснювальної записки та презентаційного матеріалу*	*01.05.2024 – 30.05.2024*	
6.	*Завершення роботи в цілому. Підготовка до захисту кваліфікаційної роботи*	*01.06.2024 – 10.06.2024*	

Здобувач _____ Гординяк М.М.
(підпис)

Керівник роботи _____ Станько В.Ю.
(підпис)

УДК 004.056:347.77(477.83)

Кваліфікаційна робота: 57 сторінок текстової частини, 15 рисунків, 24 джерел літератури, 3 додатки.

«Розробка системи нанесення видимих цифрових водяних знаків на відео та графічний контент для захисту авторських прав»

Гординяк М.М. – Кваліфікаційна робота. Кафедра інформаційних технологій. Дубляни, Львівський національний університет природокористування.

Показано алгоритми та діаграму послідовності нанесення ЦВЗ на графічний контент, а саме на окремі види фото та відео різних форматів. Було проведено аналіз та принцип розробки алгоритмів, визначено характеристики та функціональні вимоги.

Реалізовані алгоритми нанесення цифрових водяних знаків на графічний контент, складено діаграму нанесення цифрових водяних знаків на графічний контент, досліджено методи використання систем нанесення цифрових водяних знаків з метою захисту авторських прав. Детально описані та розглянуті поняття графічного фото та відео контенту, авторських прав і цифрових водяних знаків, обґрунтовано їх подальше використання з метою покращення методів нанесення цифрових водяних знаків.

Ключові слова: ЦВЗ, відео та фото формат, алгоритми, діаграма, авторські права, інформаційні технології

Keywords: video and photo format, algorithms, diagram, copyright, information technology

Зміст

ВСТУП

У сучасному цифровому світі, де швидкість поширення інформації постійно зростає, захист авторських прав стає надзвичайно важливим завданням. Особливо це стосується відео та графічного контенту, які легко копіюються, модифікуються та поширюються без дозволу власника. У цьому контексті виникає потреба в удосконаленні методів захисту авторських прав, а одним з ефективних інструментів захисту є використання системи нанесення видимих цифрових водяних знаків.

Проблема порушення авторських прав на відео та графічний контент є серйозною в сучасному інформаційному суспільстві. Цифрові технології дозволяють легко копіювати та поширювати контент без дозволу власника, що призводить до значних втрат для авторів та правовласників. У зв'язку з цим виникає необхідність у розробці та вдосконаленні методів захисту цього контенту.

Актуальність розробки методу використання системи нанесення видимих цифрових водяних знаків на відео та графічний контент для захисту авторських прав обумовлена зростанням обсягу цифрового контенту, який потребує захисту. Відповідно, розвиток ефективних технологій захисту є важливим завданням для забезпечення прав авторів і власників контенту.

Розробка методу використання системи нанесення видимих цифрових водяних знаків має на меті визначити ефективні та надійні підходи до захисту відео та графічного контенту від незаконного використання. Це дослідження є важливим для розробки імовірності автоматизованого процесу нанесення водяних знаків з мінімальним втручанням користувача та максимальною ефективністю захисту.

Метою даної роботи є дослідження та аналіз методів використання системи нанесення видимих цифрових водяних знаків на відео та графічний контент для захисту авторських прав. Завдання включають вивчення існуючих підходів, розробку алгоритмів та програмного забезпечення для реалізації системи нанесення видимих цифрових водяних знаків, оцінку ефективності цих методів і визначення можливих обмежень та викликів у їх застосуванні.

Очікується, що результати дослідження дадуть уявлення про ефективність методів нанесення видимих цифрових водяних знаків на відео та графічний контент. Будуть розроблені алгоритми та програмне забезпечення для застосування цих методів у практичній сфері. Також будуть виявлені можливі обмеження та виклики, які можуть виникнути під час застосування цих методів у реальних умовах.

Для досягнення поставленої мети були використані наступні методи дослідження:

– проведено огляд літератури, аналіз наукових статей, публікацій і технічних документів, що стосуються методів нанесення ЦВЗ знаків на відео та графічний контент;

– досліджено існуючі методи нанесення ЦВЗ, включаючи методи, які базуються на перетворенні простору кольорів та інших підходах.

– розроблені алгоритми для нанесення видимих ЦВЗ на відео та графічний контент. Враховуватимуться фактори, такі як розміщення ЦВЗ, прозорість та стійкість до обробки.

– розроблено програмне забезпечення для застосування розроблених алгоритмів на практиці. Програма дозволить користувачам наносити ЦВЗ на їх власний контент.

– проведені експерименти, під час яких застосовані розроблені методи нанесення ЦВЗ на відео та графічний контент. Ефективність методів буде оцінена за допомогою метрик, таких як розпізнаваність водяних знаків та стійкість до обробки.

РОЗДІЛ 1
АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Огляд видів комп'ютерної графіки

Сучасні апаратні та програмні рішення великою мірою розширюють можливості комп'ютерної графіки, надаючи зручні інструменти для роботи з графічними зображеннями, що стають доступними не лише для професіоналів, а й для звичайних користувачів, огляд видів засобів можна також побачити на рисунку 1.1.

Рисунок 1.1 – Види засобів ПК графіки

Розрізняють 3 види комп'ютерної графіки: растрова, векторна і фрактальна, які зображені на рисунку 1.2. Вони відрізняються між собою принципами формування зображення при відображенні на екрані монітора чи друку на папері [7].

Рисунок 1.2 – Види комп'ютерної графіки

В даній роботі, ми розглянемо види комп'ютерної графіки, які класифікуються за способом побудови та кодування.

Розглянемо кожен із видів детальніше, розпочнемо із растрової графіки.

Растрова графіка являє собою графічні об'єкти у вигляді комбінації точок, що володіють власним кольором і яскравістю. 1. Одна точка в такому зображенні називається пікселем (pixel від англійського "image element" – елемент малюнка). Представлення зображення у вигляді набору пікселів, розташованих у рядках і стовпцях, називається растром [18].

Приклад растрового зображення можна розглянути на рисунку 1.3.

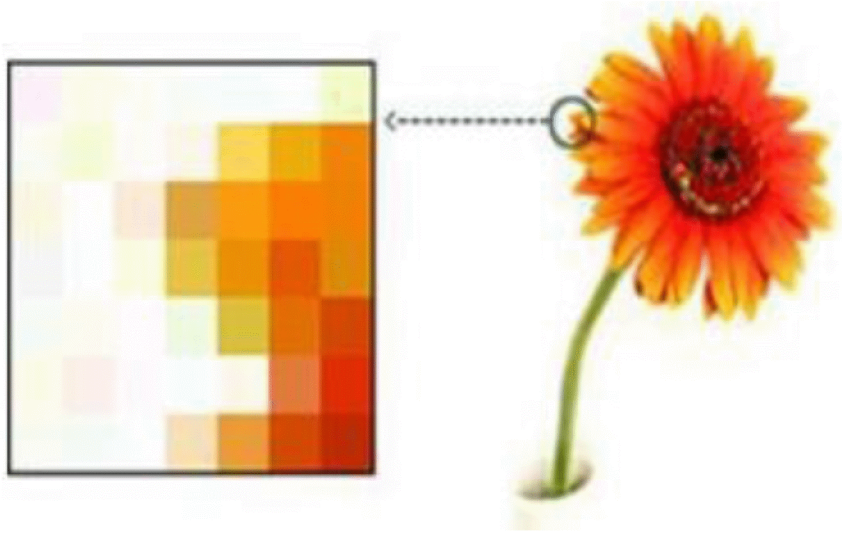


Рисунок 1.3 – Растрове зображення

Властивості растрового зображення:

1. Розмір-це ширина і висота. Він вимірюється в пікселях, сантиметрах і дюймах.

2. Роздільна здатність-це кількість пікселів на одиницю довжини. Воно вимірюється в пікселях на 1 дюйм (dpi) або пікселях на 1 см.чим вище дозвіл, тим чіткіше зображення, але тим більше Розмір файлу.

3. Глибина кольору-це кількість бітів, що використовуються для кодування одного пікселя в певний колір. Воно вимірюється за допомогою кількості біт на піксель (bpp). 8 біт можуть містити 256 кольорів, 16 біт можуть містити 65536 кольорів, 24 біта можуть перевищувати 1600 мільйонів, а 32 біта можуть перевищувати 40 мільярдів.

Формати растрових файлів включають BMP, які можна зберігати без стиснення, та розширення імен файлів bmp, які мають досить великий розмір. Формат файлу paint.

• JPEG – це спосіб стиснення даних з втратою якості шляхом розширення імен файлів у форматі JPEG або JPEG. для зберігання зображень.

• GIF дозволяє стискати дані без втрати даних. підтримує прозорість і анімацію. 256 різних відтінків. Тип розширення: gif. для малюнків і анімації.

• PNG дозволяє стискати файли без втрати даних. забезпечує прозорість. Більше 16 мільйонів різних відтінків Тип розширення: png.

• TIFF дозволяє зберігати дані без втрат. Розширення файлів tiff або tif. Збереження фотографій для друку або сканування

Векторна графіка заснована на використанні базових геометричних об'єктів (графічних примітивів), в комп'ютерній графіці об'єктами у векторній графіці основними елементами є лінії, що описуються математичними формулами [18].

Сьогодні векторна графіка відіграє велику роль. Її технологія широко використовується як в друкованому дизайні, так і в веб-дизайні. Векторні зображення використовуються для створення графічних об'єктів, де важливо зберегти чіткі контури (малюнки, схеми, логотипи, карти, діаграми і т.д.). Навіть при зміні розміру. Приклад векторної графіки показаний на рисунку 1.4.

Рисунок 1.4 – Зображення векторної графіки

Основні властивості векторних зображень:

- Тип і кількість графічних примітивів, з яких створено зображення;
- Кількість використовуваних квітів.

- Формат файлу векторного зображення:
- Файли AI з програми Adobe Illustrator. Розширення-ai.
- CDR-файли програми CorelDRAW. Розширення-cdr.
- SVG - також зберігає анімацію. Використовується для інженерної графіки та розробки веб-сайтів. Розширення-svg.
- WMF-універсальний формат для програм, що працюють в ОС Windows. Розширення-wmf, emf [20].

Отже, дослідивши види комп'ютерної графіки, ми розглянемо також недоліки та переваги деяких типів і порівняємо їх, а саме векторних та растрових зображень, які є зображені на рисунку 1.5.

Переваги та недоліки растрових і векторних зображень

ВИД ГРАФІЧНОГО ЗОБРАЖЕННЯ	ПЕРЕВАГИ	НЕДОЛІКИ
РАСТРОВЕ	• Реалістичність зображень. • Природність кольорів. • Можливість отримання зображень з використанням спеціальних пристроїв	• Великі за розміром файли зображень. • Пікселізація зображення після збільшення. • Складність редагування окремих елементів зображення
ВЕКТОРНЕ	• Невеликі за розміром файли зображень. • Збереження якості після масштабування. • Простота редагування окремих елементів зображення	• Складність реалістичного відтворення об'єктів навколишнього середовища. • Відсутність пристроїв для автоматизованого створення зображення

Рисунок 1.5 – Порівняння недоліків та переваг між векторними та растровими зображеннями

Фрактальна графіка – це технологія, яка дозволяє створювати зображення на основі фракталів. Фрактальна геометрія є основою фрактальної графіки. Рисунок 1.6 показує приклад зображення даного виду графіки.

Фрактальне зображення, яке складається з елементів, які мають схожі характеристики. Автоматична генерація зображень відповідно до формул завершує побудову.

Фрактал – це об’єкт, окремі компоненти якого успадковують характеристики своїх батьківських структур.

Рисунок 1.6 – Приклад зображення фрактальної графіки

Фрактальна графіка обчислюється як векторна, однак на відміну від традиційної векторної графіки, в ній не зберігаються жодні об'єкти в пам'яті комп'ютера. Натомість, зображення будується за певною математичною формулою або системою рівнянь, тому для його відтворення потрібно лише зберігати саму формулу, а не цілі об'єкти. Це дозволяє досягти дуже малих обсягів даних, а також простоти модифікації зображень, оскільки достатньо змінити коефіцієнти у формулі, щоб отримати зовсім нову картину [21].

Фрактальні об'єкти, такі як фрактальний трикутник, характеризуються властивістю самоподібності - складаються з елементів, подібних до цілого. Ця

властивість дозволяє моделювати багато природних об'єктів, від снігових кристалів до рослин та кристалів. Завдяки цьому, фрактальні алгоритми широко використовуються для автоматичної генерації незвичних ілюстрацій.

Хоча фрактальна графіка має переваги у вигляді малих обсягів даних, простоти модифікації та можливості деталізації зображень, вона також має певні недоліки. Зокрема, фрактальні зображення можуть мати абстрактний характер, а їх створення вимагає застосування складних математичних понять і формул.

Формат файлів фрактальної графіки fr4.

Готові фрактальні зображення зберігаються у форматі *.frs і можуть бути експортовані в один з растрових графічних форматів jpg, bmp, png і gif, у той час як фрактальні анімації зберігаються як AVI-файли.

Тривимірна графіка, або 3D-графіка – розділ комп'ютерної графіки, сукупність прийомів та інструментів (як програмних, так і апаратних), призначених для зображення об'ємних об'єктів, один з яких є зображений на рисунку 1.7.

Тривимірна графіка зазвичай оперує віртуальним, уявним тривимірним простором, який відображається на плоскій, двовимірній поверхні дисплея або аркуша паперу [17].

Рисунок 1.7 – Приклад зображення 3D-графіки

До основних переваг 3D-моделювання можна віднести:

1. Підвищена інформативність окремих ділянок екрана або зображення в складних об'єктах. Складні геометричні об'єкти можна розглянути з усіх боків, що дає можливість детальніше їх вивчити та зрозуміти. Це перетворює складні об'єкти на більш прості для сприйняття.

2. Можливість обертати об'єкти, що дозволяє побачити всі їхні частини повністю.

3. Отримання нових можливостей та перспектив. 3D-графіка дозволяє бачити реальні пропорції об'єктів, навіть якщо вони розташовані хаотично та на різній відстані один від одного.

4. Створення діаграм нових форм. З'являється можливість додавати нові змінні під час створення діаграм, що підвищує їхню інформативність.

5. Застосування технологій віртуальної реальності. Завдяки 3D-зображенням стає можливим повністю занурити людину в іншу реальність.

Щодо недоліків 3D-графіки:

1. Вимоги до характеристик комп'ютера, на якому створюється 3D-графіка, є високими.

2. Створення однієї 3D-моделі потребує багато часу, адже її необхідно опрацювати з усіх боків.

3. 3D-графіка надає менше свободи своєму творцю порівняно з 2D, оскільки складно спотворювати об'єкти, їхні реальні пропорції та перспективи.

4. Потрібно постійно стежити за взаємодією між об'єктами, щоб запобігти їхньому проникненню один в одного.

До найпоширеніших типів файлів належать OBJ, FBX, STL, AMF, IGES та інші.

1.2 Формати файлів відео-контенту

Один із найпопулярніших форматів мультимедійних файлів у наш час – відеофайли. Кожен формат відеофайлу має свої переваги та недоліки, далі розглянемо найбільш поширені формати.

Одним із найбільш поширених форматів відеофайлів є MP4. Його було створено за стандартом MPEG-4, який містить багато різних кодеків, які гарантують високу якість відео та звуку. Формат MP4 універсальний і може бути відтворений на більшості пристроїв, таких як планшети, комп'ютери, мобільні телефони та телевізори [19].

Формат відеофайлів AVI (Audio Video Interleave).

AVI – один із найпопулярніших форматів відеофайлів, розроблений Microsoft у 1992 році. Він забезпечує високу якість відео та звуку, зберігаючи аудіо та відео в окремих потоках. Тим не менш, AVI має деякі обмеження, наприклад великий розмір файлу та те, що він не працює на деяких пристроях.

У 1992 році Microsoft представила AVI з метою надання більш надійного та сучасного формату аудіо- та відеофайлів. Завдяки поширенню Інтернету формат швидко став популярним, оскільки він дозволяє людям безпосередньо чи опосередковано обмінюватись відеофайлами через хмарне сховище мультимедіа.

Обмеження формату:

- Інформація про співвідношення сторін не може бути закодована в оригінальній специфікації AVI, але пізніша специфікація OpenDML (AVI2. 0) забезпечує стандартизований метод
- Файли AVI широко використовуються при обробці фільмів і телешоу, але різні підходи до додавання до них тимчасових кодів конкурують один з одним і можуть призвести до помилок форматування.
- Відеофайли, закодовані у форматі AVI, не можуть використовувати методи стиснення, які вимагають даних про майбутні кадри за межами закодованого кадру (B-кадр).

- Використання файлів AVI зі змінною швидкістю передачі даних (VBR) є проблематичним (наприклад, аудіо MP3 із частотою дискретизації менше 3 кГц).
- Як правило, при стандартному кодуванні художніх фільмів у форматі AVI накладні витрати становлять близько 5 МБ на годину, залежно від того, як використовується файл.
- Якщо ваш AVI-файл не може містити вкладень, таких як шрифти або субтитри, ви можете жорстко закодувати субтитри в відеопотік або помістити їх в окремий файл.

Формат WMV (Windows Media Video).

WMV – формат відеофайлів, розроблений Microsoft у 1999 році. Ви можете отримати високу якість відео та звуку при мінімальному розмірі файлу. У форматі WMV часто відтворюються відео на комп'ютерах з операційною системою Windows.

За допомогою власних кодеків корпорації Майкрософт у 1999 році було розроблено новий формат стисненого відео, відомий як WMV7, який базувався на MPEG-4, частина 2. Удосконалення були додані в наступні дві версії, тобто WMV8 і 9. Корпорація Майкрософт представила 9-ту версію від WMV до SMPTE для стандартизації в 2003 році, який зрештою був стандартизований у 2006 році як SMPTE 421M, також відомий як VC-1. Ідея, що лежить в основі WMV, полягала в тому, щоб розробити медіаформат, який міг би підтримуватися всім апаратним і програмним забезпеченням, що підтримується Microsoft. Крім того, ще однією важливою метою була передача відеопотоків через Інтернет за оптимальним сценарієм. Після стандартизації від SMPTE WMV також став відеоформатом для дисків Blu-ray.

Хоча в серії Windows Media Video 9 доступні різні аудіо- та відеокодеки для створення та відтворення цифрових медіа, кодек WMV-9 є найновішим і найкращим відеокодеком, оскільки він може досягти оптимального стиснення з дуже низьких бітрейтів, тобто 160 x Від 120 зі швидкістю 10 Кбіт/с до 1920 x 1080 зі швидкістю 4–8 Мбіт/с для різних HD-відео.

Формат MOV (QuickTime).

Відеофайл формату MOV розроблено компанією Apple. Він забезпечує високу якість відео та звуку та зберігає аудіо та відео в окремих потоках. Формат MOV є стандартним для відтворення відео на пристроях Apple, таких як iPhone, iPad та Mac.

На основі специфікації QuickTime File Format (QTFF) 2001 року був розроблений формат файлу MPEG-4. Формат був схвалений Міжнародною організацією стандартизації, а системні специфікації MPEG-4 Part 1 були опубліковані в 1999 році. У 2001 році було опубліковано файл перегляду у форматі MP4.

Перша версія mp4була переведена в 2003mpeg mpeg-4, частина 14 (iso/iec14496-14:2003). Він був випущений в 2004 році.

В даний момент вин використовується як інформація для читачів, так і для журналістів.

- відеоплеєр VLC eltima elmedia player
- Mpeg-4-MP4
- Відео webm-вебм
- Розширений системний формат-asf
- Ogg Vorbis Audio -OGG
- MP3 аудіо-MP3
- Wave аудіо-WAV

Adobe створила формат відеофайлів FLV. Він може зберігати відео та аудіо в окремих потоках, що дозволяє зберігати відео та аудіо високої якості при мінімальному розмірі файлу. Стандартним форматом відео, який використовується на вебсайтах та відеохостингах, таких як YouTube, є формат FLV. Бітові відеопотоки Sorenson Spark є власним варіантом відеостандарту H.263, який міститься у файлах FLV. Для Flash Player 6 і 7 необхідний формат стиснення.

Таким чином, Flash Player версії 8 підтримує наступні аудіо - та відеоформати:

- Video. On2TrueMotion VP6. Цей формат стиснення рекомендується для Flash Player8 і пізніших версій.

- Аудіо. Nellymoser Asao, Speex (з відкритим кодом), MP3, нестиснене аудіо, ADPCM та формати AAC (HE-AAC/AAC SBR, AAC Main Profile, AAC-LC).

Файли FLV (Flash Video) складаються із заголовків та пакетів. Заголовок містить наступні поля:

- Підпис. Значення "FLV" Значення за замовчуванням дорівнює 1, і допускається лише 0x01

- Прапорець 0x04 для аудіо, 0x01 для відео, 0x05 для аудіо та відео

- Розмір заголовка за замовчуванням 9, використовується для пропуску нових розширених заголовків.

За заголовком слідує пакет, кожен з яких містить 15-байтовий заголовок. Ці пакети можуть містити аудіо, відео, сценарії, зашифровану інформацію та корисні метадані. Ключові області пакету:

- Зарезервовано має бути 0

- Фільтр 0 для незашифрованих файлів, 1 для зашифрованих файлів

- Тип пакету 8 для аудіо, 9 для відео, 18 для даних скрипта

- Розмір даних довжина повідомлення

- Нижня мітка часу мітка часу першого пакета(у мілісекундах) – NULL

- Верхня мітка часу розширене значення uint32_be

- Ідентифікатор потоку NULL для першого потоку

- Дані корисного навантаження: дані на основі типу пакета

Формат відеофайлів MKV є відкритим для розробників. Він може зберігати відео та аудіо в окремих потоках, що дозволяє зберігати відео та аудіо високої якості при мінімальному розмірі файлу. Формат MKV є універсальним і може бути відтворений більшістю пристроїв.

Лассе Керккайнен був головним розробником, працюючи зі Стівом Ломме, засновником Matroska, та командою програмістів. MKV є відкритим вихідним кодом і може вільно використовуватися, оскільки розробляється як проект з

відкритим стандартом. Формат був розроблений і став основою мультимедійного формату WebM у 2010 році.

Документ Matroska повинен складатися щонайменше з 1 документа EBML, що використовує тип документа Matroska. Кожен документ EBML починається з заголовка EBML, що містить кореневий елемент EBML, визначений як сегмент. EBML використовує систему елементів для створення документів EBML.

Формат відеофайлів WebM походить від відкритого безкоштовного формату файлу WebM. Він був створений для обміну відео в Інтернеті та описує структуру контейнера файлів, яка охоплює формати відео та аудіо. WebM є повністю безкоштовним і працює на високій якості на основі відкритих технологій, таких як HTML, HTTP та TCP/IP, які доступні для всіх.

WebM був розроблений, щоб працювати з відео в Інтернеті, тому він підходить для потокового передавання з низьким обчислювальним слідом. Це дозволяє відтворювати відео на будь-яких пристроях, особливо на невеликих нетбуках, планшетах і ноутбуках.

Високоефективні технології стиснення VP8 або VP9 стискають відеопотоки, які містяться в файлі WebM. Так само кодеки Vorbis або Opus, розроблені Xiph Foundation, використовуються для стиснення аудіопотоків у файлі WebM. Зведені специфікації формату файлу WebM наведено нижче на рисунку 1.8.

Поле	Опис
типу MIME	video/webm
Тип MIME лише аудіо	audio/webm
Уніфікований ідентифікатор типу	org.webmproject.webm
Назва відеокодеку	VP8 або VP9
Назва аудіокодека	Vorbis або Opus

Рисунок 1.8 – Специфікації для формату файлу WebM

Через велику кількість файлів у папці DVD Movie важко визначити, які файли запускати для відкриття фільму. Однак, якщо ви знаєте, чим відрізняються файли з різними розширеннями, орієнтуватися в цьому типі буде простіше. База об'єктів з версіями (VOB) - це розширення контейнера, що містить відео (або деякі з них) MPEG-2, аудіо, субтитри до фільмів та меню. Це основні файли, що містять фільм на DVD.

Інформація про фільми, порядок відтворення файлів VOB та меню включена у файли з розширенням IFO. Тобто службовий файл створюється під час запису фільму на DVD.

Окрім стандартних файлів .m2v та .m2p, які використовуються для створення VOB-файлів та запису фільмів на DVD, існують й інші популярні формати оптичних дисків:

DVD - Найпоширеніший формат, що витіснив VHS. Відео стиснуте в стандарті MPEG-2 з бітрейтом 2000-9800 Кб/с та роздільністю 720x576 (PAL) або 720x480 (NTSC).

HDDVD - Диски великої ємності для запису відео високої чіткості. Використовують аналогічні стандарти стиснення, як і Blu-Ray.

Blu-Ray - Оптичний носій нового покоління з підвищеною ємністю для зберігання відео, включаючи високу чіткість. Став популярним в 2006 році, витіснив HDDVD в 2008.

Кожен формат має свої переваги та недоліки, тому вибір залежить від потреб користувача та пристрою відтворення. Незалежно від формату, важливо забезпечити високу якість відео та звуку для максимального комфорту перегляду.

Відео-контент став невід'ємною частиною ведення бізнесу. Його широко використовують у рекламних кампаніях, адже дослідження Hubspot показують, що відеоролики про товари чи послуги є ключовим фактором при ухваленні рішення про покупку. Це пояснюється тим, що більшість людей краще сприймають візуальну інформацію. Наочна 10-секундна демонстрація переваг продукту може бути ефективнішою, інформативнішою та переконливішою за звичайну текстову рекламу [14].

Відеоконтент також характеризується високим рівнем рентабельності інвестицій, що робить його незамінним елементом будь-якого маркетингового просування. Популярність відео продовжує зростати, адже такі платформи, як YouTube, Facebook, Instagram та TikTok, активно інвестують у розвиток відеосегмента. За даними Hubspot, понад 80% інтернет-трафіку припадає на відеоконтент, тому використання відеореклами наразі необхідно для всіх видів бізнесу.

Навіть невеликий рекламний ролик може донести набагато більше інформації про продукт чи послугу, ніж довгий текст, тож потенційному клієнту не треба витрачати багато часу на вивчення пропозиції.

Відеоконтент можна використовувати не лише для реклами товарів та послуг, а й для підвищення впізнаваності бренду, а також для інших цілей, таких як інформування, розваги чи організація конкурсів. Відеоконтент та інші динамічні рекламні інструменти привертають набагато більше уваги, ніж статична текстова реклама, що в підсумку дає вищу конверсію. Візуальна демонстрація переваг товару чи послуги викликає більше довіри, ніж простий список вигід, мотивуючи споживача зробити покупку. Відеоконтент легше розповсюджувати, що забезпечує ширше охоплення аудиторії, а також збільшує ймовірність того, що ролик стане вірусним. Відеоконтент підвищує час перебування на сайті, що покращує позиції ресурсу в пошукових системах. Хоча створення відеороликів дорожче, ніж текстової реклами, у довгостроковій перспективі вона окупається за рахунок вищої ефективності[16].

Сайти з відеоконтентом демонструють на 34% вищу конверсію та на 27% більше кліків порівняно з іншими ресурсами. Відеохостинги можуть стати джерелом значного трафіку на сайт або посадкову сторінку за умови розміщення необхідних посилань. Використання відеоконтенту виправдовує очікування аудиторії, а майданчики для його публікації створюють комфортні умови для його поширення.

1.3 Огляд та аналіз видів цифрових водяних знаків (ЦВЗ)

Водяні знаки вперше з'явилися в Болоньї (Італія) в 1282 або 1283 році. Виробники паперу використовували їх тоді і пізніше для ідентифікації своєї продукції, а також на поштових марках, банкнотах та інших державних документах для захисту від підробки.

У 1866 році французький філателіст Жак Амабль Легран написав основну роботу про водяні знаки на поштових марках [6].

Водяні знаки – це ідентифікаційні позначки, які наносилися на папір у процесі його виготовлення. На мокрому папері штампували певний символ або малюнок, і ця ділянка ставала тоншою за навколишній папір. Після висихання паперу цей "водяний знак" ставав видимим при піднесенні до світла. Цей процес використовувався для перевірки автентичності офіційних документів, грошей, марок тощо.

Цифрові водяні знаки – це сучасна форма водяних знаків. Вони використовуються для ідентифікації власника/автора та аутентифікації цифрових носіїв інформації, таких як зображення, аудіо та відео, аналогічно фізичним водяним знакам на папері [9].

Як зробити водяний знак? Для фотографій і відео це зазвичай означає застосування видимого тексту або графіки .png (логотипу). Зазвичай це можна зробити в растровому редакторі, наприклад PhotoShop. Або додаток, спеціалізований для нанесення водяного знака. Plum Amazing створює програми для водяних знаків для iOS, Mac, Android і Windows, усі вони називаються iWatermark. iWatermark спрощує створення водяних знаків на фотографіях і відео. iWatermark не просто накладає текст або зображення на фото чи відео.

Коли фотографії чи відео швидко поширюються в Інтернеті, інформація про їх автора часто втрачається. Це може призвести до конфліктів з інтелектуальною власністю, дорогих судових процесів та звинувачень у плагіаті.

Цифровий водяний знак вирішує цю проблему, адже він вбудовується в цифровий контент для захисту авторських прав та підтвердження його цілісності.

Якщо файл змінюється, змінюється і водяний знак. Цифрові водяні знаки можуть бути видимими чи невидимими.

Зазвичай системи цифрових водяних знаків мають два основні блоки: для вбудовування та для виявлення/вилучення водяного знака (рис.1.9). Це допомагає захистити авторство в епоху швидкого поширення контенту в соціальних медіа [10].

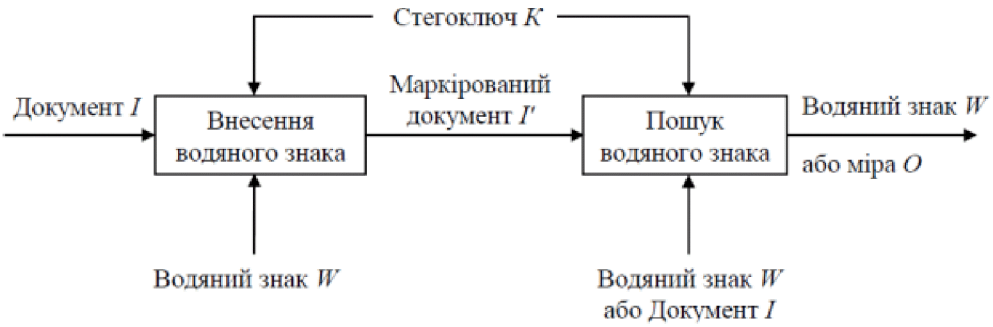


Рисунок 1.9 – Схема внесення водяного знака і схема пошуку/витягання.

Для вбудовування водяного знака в цифровий об'єкт I потрібні такі вхідні дані: сам водяний знак W та необов'язковий стегоключ K. Вихідним результатом є цифровий об'єкт з вбудованим водяним знаком.

Для пошуку або вилучення водяного знака з об'єкту $\bar{I}'$ потрібні такі вхідні дані: об'єкт з водяним знаком $\bar{I}'$, стегоключ K, а іноді й оригінальні дані I або W. Вихідним результатом є витягнений водяний знак W або оцінка O ймовірності його наявності.

Ця структура характерна для електронних систем водяних знаків з різними типами даних, такими як аудіо, зображення, відео, відформатований текст та 3D-моделі.

Відповідність водяним знакам можна встановити наступним чином.

1. Невидимість користувача, індивідуальність алгоритму програми, здатність автора ідентифікувати несанкціоноване використання файлу, неможливість його видалення неавторизованими особами, стійкість до різних змін контейнерного середовища.

2. Перешкодозахищеність водяних знаків від випадкового пошкодження і навмисних атак є найбільш важливою характеристикою, від якої залежать споживчі характеристики системи.

3. Обов'язкове використання стьобаних ключів для забезпечення захисту водяного знаку від навмисного скручування і видалення.

4. Оптимальний поріг "видимості" водяного знака – це параметр, що характеризує допустимий рівень спотворень.

5. Відносний обсяг введеної інформації – це параметр, який залежить від характеру конфіденційних даних і характеру цифрового об'єкта.

6. Коли наноситься велика кількість водяних знаків, це знижує завадостійкість до атак.

7. Алгоритми створення та видалення водяних знаків не повинні бути секретними, а доступ до водяних знаків повинен бути обмежений.

8. Місце розташування водяного знака залежить від стегоключа і впливає на видимі перекручування в зображенні [10].

Цифрові водяні знаки - це додаткова інформація, закодована в цифровому контенті, такому як зображення, звук чи відео, для ідентифікації та захисту авторських прав.

Існує два основні типи цифрових водяних знаків:

- Видимі водяні знаки - це відкрита позначка, нанесена на контент, яка може бути текстом, логотипом, QR-кодом тощо.

- Невидимі водяні знаки - це прихована інформація, вбудована у контент, яка не впливає на його візуальне сприйняття.

За стійкістю до змін цифрові водяні знаки поділяються на:

- Крихкі - виявляють будь-які зміни в контенті.

- Напівкрихкі - стійкі до деяких змін, наприклад, стискання.

- Міцні - стійкі до різних атак та змін контенту.

Програма iWatermark дозволяє додавати різноманітні види видимих водяних знаків на цифрові зображення, відео та графіку.

Невидимий водяний знак - це спосіб приховування інформації всередині зображення. Існує два основні види невидимих водяних знаків: стегомарки та метадані [13].

Стегомарки були розроблені компанією Plum Amazing для приховування невеликої кількості тексту, такого як слова, речення, електронна пошта чи URL-адреса, всередині фотографій. Вони являють собою цифри, зашифровані певним алгоритмом у зображення. Стегомарки можуть бути захищені паролем або ні. На відміну від звичайних водяних знаків, стегомарки складніше видалити з фотографії та можуть витримувати повторне стиснення JPEG. На даний момент стегомарки застосовуються лише для файлів у форматі JPEG і є частиною програми iWatermark [**Помилка! Джерело посилання не знайдено.**].

Кожен тег - це змінна, яка представляє певну метаінформацію, що зчитується з кожного зображення та застосовується як видимий водяний знак до цього зображення. Це унікальна особливість iWatermark.

Існує 3 основні категорії метаданих:

1. Ідентифікатор-інформація про візуальний вміст, такий як заголовки, заголовки, ключові слова, зображені люди, місця, підприємства та об'єкти мистецтва. Ця інформація може бути введена у вигляді довільного тексту або коду з контрольованого словникового запасу.

2. Права-інформація про ідентифікацію авторів, авторські права, кредити, модельні права та права власності, а також умови використання та ліцензії.

3. Адміністратор-дата і місце створення, інструкції користувача, ідентифікатор завдання та інші відомості.

Будь-які з цих метаданих можна використовувати як текстовий водяний знак, накладений на фотографію.

Електронний водяний знак-це процес вбудовування інформації в медіафайл для перевірки її автентичності та автора.

Водяний знак-це видимий та / або невидимий цифровий маркер, який ідентифікує власника цифрового вмісту.

Видимі водяні знаки-це текстова інформація або інформація про логотип, що відображається на зображенні, що ідентифікує власника фотографії.

Невидимі водяні знаки-це конфіденційна інформація, вбудована в фотографічні зображення, тому вони невидимі для людського ока. Стеганографія використовує подібну техніку, але для різних цілей [**Помилка! Джерело п осилання не знайдено.**].

Метадані – це описова інформація, вбудована в будь-який тип файлу. Елементи EXIF, XMP та IPTC - це різні типи метаданих, які додаються до фотографій. Метадані змінюють лише Жовтневу додаткову інформацію у файлі, а не фактичні дані зображення. Деякі Інтернет-сервіси, такі як Facebook та Flickr, видаляють ці метадані.

EXIF - це тип метаданих, який зберігається майже у всіх цифрових камерах. Він містить інформацію про налаштування камери, дату/час, мініатюри, GPS дані та авторські права. Ця інформація не може бути змінена, але може бути видалена.

IPTC - це стандарт метаданих, розроблений Міжнародною радою з питань телекомунікацій для обміну новинами між газетами та інформаційними агенціями.

XMP - це розширювана мова розмітки, що використовується для зберігання метаданих у цифрових фотографіях. Вона сумісна зі стандартом IPTC і була представлена Adobe в 2001 році [24].

Тег - це окремий фрагмент метаданих у межах EXIF, IPTC або XMP.

Використання фото з ЦВЗ, піратство чи крадіжка має два випадки:

1. Фото піратство - коли люди в соціальних мережах без вашого дозволу використовують ваші фотографії, але для некомерційних цілей. Це зазвичай сприймається як менш серйозне порушення.

2. Фото крадіжка - коли компанія використовує ваші фотографії в комерційних цілях без вашого дозволу. Це вважається серйознішим порушенням авторських прав, і в такому випадку ви маєте підстави подати на них до суду.

Додавання водяних знаків на фотографії може мати кілька важливих переваг:

1. Захист авторських прав: Водяний знак є візуальним підтвердженням ваших прав на зображення. Це допомагає запобігти використанню ваших фотографій без

вашого дозволу і може слугувати доказом вашого права власності, якщо хтось використовує ваше зображення незаконно.

2. Визнання вашої роботи: Водяний знак може бути способом позначити ваше авторство, якщо хтось ділиться вашим зображенням у соціальних мережах чи на веб-сайтах. Це гарантує, що ваша робота буде належним чином атрибутована.

3. Запобігання неналежному використанню: Водяні знаки можуть допомогти запобігти використанню ваших зображень у спосіб, який суперечить вашим цінностям або бренду, наприклад, якщо ви фотограф.

4. Захист від крадіжки зображень: Крадіжка зображень є поширеною проблемою в Інтернеті, але водяні знаки ускладнюють цей процес і вказують на справжнього автора [8].

Отже, водяні знаки є простим і ефективним способом захистити ваші фотографії, незалежно від того, чи ви професіонал чи аматор. Вони допомагають забезпечити визнання вашої роботи та запобігти несанкціонованому використанню ваших зображень.

РОЗДІЛ 2
ПОСТАНОВКА ЗАДАЧІ

2.1 Обґрунтування вибору та актуальність теми

У сучасному світі стрімкого технологічного розвитку інтелектуальна власність стає все більш вразливою до зловживань, крадіжок та піратства. Спеціалізовані програми та алгоритми постійно вдосконалюються, ускладнюючи захист авторських прав на контент, відео та графічні матеріали.

Поява нових цифрових платформ і сервісів, таких як стрімінгові платформи, соціальні медіа тощо, зумовлює зростання потреби в ефективних методах захисту інтелектуальної власності. Технології цифрового маркування, як-от водяні знаки, можуть стати ключовим інструментом протидії цим викликам.

У медіаіндустрії, де контент постійно публікується та поширюється онлайн, захист авторських прав критично важливий для забезпечення справедливої винагороди правовласникам. Попри наявність різних методів цифрового маркування, все ще існують проблеми з їхньою ефективністю та непомітністю. Дослідження нових підходів може сприяти вдосконаленню захисту авторських прав.

Результати такого дослідження можуть мати практичну цінність для компаній медіагалузі та інших суб'єктів, зацікавлених у захисті свого контенту від незаконного використання. Робота над цією темою дасть студенту можливість розвинути навички у сфері цифрових технологій, обробки медіаданих та охорони інтелектуальної власності.

Таким чином, обрана тема диплома є актуальною, має важливе практичне значення для медіаіндустрії.

2.2 Вибір методів нанесення ЦВЗ

Розвиток генеративного ШІ відкрив нову еру створення цифрового контенту, але були висловлені побоювання з приводу дезінформації, шахрайства та потенційного обману та шкоди за допомогою цифрових засобів масової інформації, створених ШІ, особливо при виявленні та моніторингу контенту, створеного ШІ. штучний інтелект.

Нещодавні розробки в генеративних моделях ШІ призвели до необхідності декомунізації між реальними та штучними матеріалами, щоб запобігти зловживанню вмістом, створеним ШІ.

1. Один із способів вирішити цю проблему-застосувати водяний знак. Цей метод дозволяє відрізнити фотографії ШІ від інших джерел.

Дослідники з кафедри комп'ютерних наук Університету Меріленда вивчали стабільність водяних знаків та детекторів підробок на основі класифікаторів. На рисунку 2.1 показаний приклад атаки на метод лікування ССЗ [12].

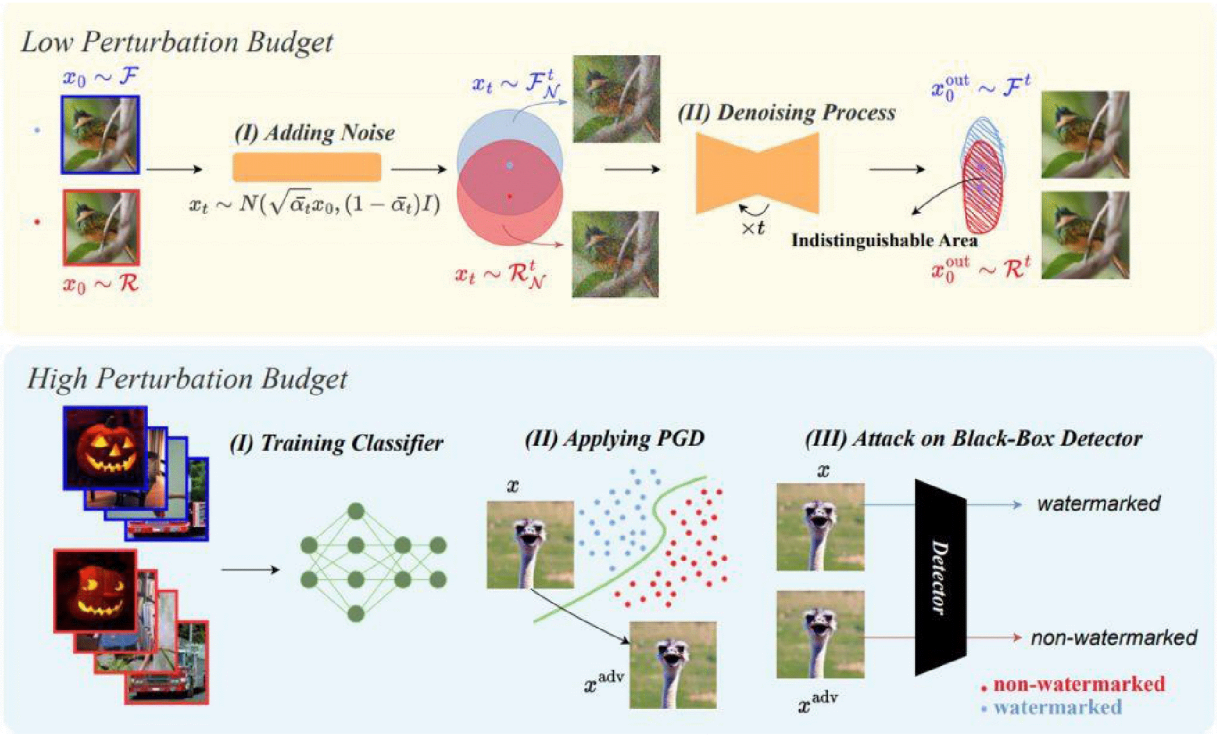


Рисунок 2.1 – Ілюстрація атаки на методи ЦВЗ зображень

Верхня частина демонструє атаку дифузійного очищення для низькобюджетних збурень водяних знаків. Вона створює нерозрізнену область, створюючи гаусівський шум, що призводить до сертифікованої нижньої межі похибки детекторів водяних знаків. Дифузійні моделі використовуються для деноізування зашумлених зображень.

Внизу показана резервна схема атаки для бюджетних водяних знаків з високим рівнем перешкод. Метод передбачає навчання резервного класифікатора та виконання атак PGD (модуляція посилення сприйняття та демодуляційні атаки). Цей тип атаки спрямований на знищення цілісності вмісту водяних знаків та зменшення впливу водяних знаків на якість медіа, використовуючи ці маніпульовані зображення для обману детекторів водяних знаків "чорної скриньки".

Їх дослідження виявило значний компроміс між частотою помилок ухилення та частотою помилок декомунізації при використанні методів водяних знаків, які вносять невеликі збурення в зображення. Частота помилок уникнення показує, скільки разів зображення водяного знака було змішано з зображенням без водяного знака, а частота помилок підробки показує, скільки разів воно було змішано з зображенням водяного знака при атаці дифузійної очищення.

Це дослідження емпірично доводить, що атаки з розсіяним очищенням можуть ефективно видаляти водяні знаки з зображень з невеликими збуреннями. Зображення, трохи змінені за допомогою технології водяних знаків, є більш вразливими до цієї атаки. Але для методів нанесення водяних знаків, які значно змінюють зображення, атаки дифузійного очищення не дуже успішні. Навпаки, дослідження пропонує іншу атаку, яка називається атакою перемикання шаблонів. Атаці вдалося усунути водяні знаки за допомогою сильно порушених методів маркування води, і вважалося, що модель захисту водяних знаків видаляє вміст водяних знаків.

У цьому дослідженні ми виявили вразливість технології водяних знаків для контрафактних атак. Зловмисник може завдати шкоди репутації автора, створивши

галасливе зображення, що імітує присутність водяного знака, і прикріпивши його до реальної фотографії.

Вирішення завдань кваліфікаційної роботи передбачає дослідження проблем та вразливостей детекторів зображень на основі штучного інтелекту, особливо технології водяних знаків, перед обличчям шкідливих атак та розповсюдження вмісту, створеного штучним інтелектом. Для ефективного вирішення цих проблем підкреслюється важливість постійного вдосконалення та вдосконалення методів виявлення в епоху продуктивного штучного інтелекту.

2.3 Використання методу аналізу стійкості

Використання методів проектування та об'єктно-орієнтованого програмування (ООП) є основою цього підходу для створення програми, яка може автоматично тестувати алгоритми цифрового маркування.

Зазвичай використовується загальний метод під час аналізу попередніх робіт щодо перевірки стійкості алгоритму цифрового маркування до різних типів атак. Перед його застосуванням необхідно визначити набір параметрів, які впливають на результати тестування безпосередньо або опосередковано. Ці параметри будуть розглянуті в наступних розділах. Схема перевірки стійкості алгоритму ЦВЗ до шкідливих впливів представлена на рисунку 2.2.

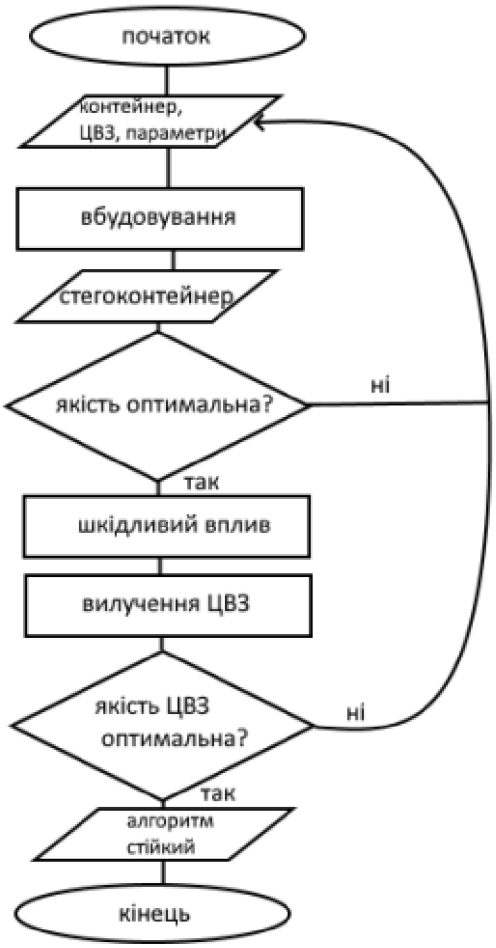


Рисунок 2.2 – Загальна схема перевірки стійкості алгоритму цифрового маркування до шкідливих впливів

Три основні етапи складають цей метод: використання ЦВЗ, атака на стеганоконтейнер і виявлення водяного знака. Після етапів маркування зображення використовується ряд метрик для порівняння зображення, захищеного від спотворення, з оригіналом. Якщо якість стеганоконтейнера досягається до максимального можливого рівня, його можуть атакувати кілька людей. Інакше параметри вбудовування змінюються. Витягування ЦВЗ також здійснюється так само. Висновок про стійкість алгоритму ґрунтується на якості водяного знаку, який було отримано [**Помилка! Джерело посилання не знайдено.**].

Непомітність ЦВЗ оцінюється за ступенем видимості спотворень оригінального зображення.

2.4 Дослідження систем еталонного тестування

В даний час розробляється багато еталонних тестових систем. Кожна система має свою архітектуру, інтерфейс та набір атак.

Компанія Stirmark була створена в 1997 році і стала еталоном для тестування алгоритмів цифрового маркування. Це набір класів, що використовуються в мовах програмування C та C ++.

Його незручно використовувати, оскільки він не має графічного інтерфейсу користувача. Тому вам потрібно уважно прочитати інструкцію.

Система складається з серії простих атак (найпоширеніші операції обробки зображень), атак, які стирають цифрові зображення, або атак, які відключають виявлення декодерів.

Параметри шкідливого впливу визначаються функціональністю класу системи. Отже, щоб їх змінити, вам доведеться працювати безпосередньо з програмним кодом.

Рисунок 2.3 – Демонстрація роботи алгоритмів Stirmark

Щоб протестувати алгоритм, вам потрібно перетворити алгоритм у бібліотеку програмного забезпечення. Якість зображення оцінюється за допомогою таких параметрів, як кореляція та PSNR. Інші недоліки Stirmark включають високу складність, нездатність автоматизувати виконання декількох елементів керування

алгоритмом цифрового маркування, відсутність оцінки ймовірності неправильного декодера та відсутність оцінки складності алгоритму ДЕК-стеганографії.

Таким чином, у Штірмарка є значна можливість для тестування стабільності. Однак через вищевказаних недоліків ця система незручна у використанні. Однак варто відзначити, що творці цієї системи пізніше розробили клієнт-серверну версію і усунули деякі її недоліки.

Іншим поколінням систем еталонного тестування є Checkmark. Matlab – це мова програмування, яка використовується для розробки системи. Немає інтерфейсу користувача 29. Використовується зображення формату JPEG як контейнер. Ця система не підтримує інші графічні формати. Порівняно зі Stirmark, Checkmark має більшу кількість шкідливих впливів. Так, наприклад, було додано стискання JPEG2000, яке було надзвичайно важливим через його високу продуктивність і, отже, значну руйнівну силу порівняно з JPEG.

Тим не менш, атака неоднозначності відсутня, як і у Stirmark. У порівнянні з попередньою системою Checkmark містить метрики оцінки якості зображення, включаючи виважений PSNR і метод Уотсона.

Optimark – система еталонного тестування з графічним інтерфейсом користувача, яка безсумнівно є перевагою порівняно зі Stirmark і Checkmark. Загальні операції з обробки зображень, атаки відключення ЦВЗ детектором і атаки невизначеності – це приклади шкідливих дій. Для тестування алгоритму Optimark від користувача необхідно створити дві консольні програми, які відповідають за впровадження та вилучення водяного знака. Щоб імпортувати тестовані алгоритми, Stirmark і Optimark використовують програмну бібліотеку.

Основними недоліками Optimark є застосування простих метрик сприйняття якості зображення, обмежена кількість атак і відсутність можливості додати додаткові шкідливі впливи. Наприклад, зараз у системі немає атак на компресію JPEG2000, що унеможливлює використання Optimark у цій роботі.

RK Benchmark – система тестування, яка використовує графічний програмний інтерфейс, розроблений на мові програмування Matlab. Було розроблено, щоб зробити аналіз стійкості вбудованих водяних знаків простішим,

оскільки, як стверджує автор, інші системи складні та складні для розуміння. З точки зору наявних типів шкідливих впливів Stirmark, Checkmark і Optimark перевершують їх.

Він не має достатньо часу для оцінки алгоритму. Було встановлено, що коли користувач працює з програмним кодом, написаним мовою Matlab, він не може змінювати параметри алгоритму, який був розроблений. Це було зроблено на основі того, як виглядає програмний інтерфейс даної системи. Це може викликати деякі проблеми під час роботи з цією системою. Іншим недоліком є те, що видів шкідливих впливів дуже мало, а метрики аналізу якості зображення обмежені нормалізованою кореляцією та PSNR.

РОЗДІЛ 3
ПРОЕКТУВАННЯ МЕТОДІВ ДОСЛІДЖЕННЯ СИСТЕМИ НАНЕСЕННЯ ЦВЗ ДЛЯ ЗАХИСТУ АВТОРСЬКИХ ПРАВ

3.1 Практичне використання технологій нанесення ЦВЗ на графічний контент

Загалом, iWatermark є потужним інструментом для управління метаданими та захисту авторських прав фотографів [22].

iWatermark пропонує інструменти для маркування води, які недоступні в Lightroom. До прикладу, текстовий водяний знак у Lightroom має певний розмір пікселів, тому його розмір змінюється залежно від роздільної здатності фотографій. З іншого боку, текстові водяні знаки iWatermark не завжди масштабуються пропорційно залежно від роздільної здатності або портрета/ландшафту.

На відміну від Lightroom, яке використовує пікселі для розміщення водяних знаків, iWatermark підходить до цього пропорційно, зберігаючи однаковий вигляд водяного знаку навіть на фотографіях різної роздільної здатності та орієнтації. Крім того, iWatermark здатний не масштабувати водяний знак.

Ще одна ключова перевага iWatermark - це можливість використовувати метадані фотографій для автоматичного додавання водяних знаків. Наприклад, інформація про камеру, об'єктив, дату і час, GPS-координати тощо може бути перетворена у видимий водяний знак на фотографії. Це дозволяє швидко і ефективно додавати такі знаки до великої кількості фотографій без необхідності ручних налаштувань.Наступне питання: чи може iWatermark написати метадані до фотографії?

Отже, резюмуючи, програма iWatermark дозволяє додавати, змінювати та читати метадані фотографій. Це особливо корисно для професійних фотографів, які працюють, наприклад, у Reuters чи The New York Times, адже вони можуть легко додавати своє ім'я, авторські права, місцезнаходження тощо до знімків. Після

створення таких наборів метаданих, їх можна легко застосовувати до багатьох фотографій одним кліком. Це дуже зручно та ефективно.

Крім того, програма пропонує водяні знаки для фотографій, які можуть бути корисними, коли зображення публікуються у соціальних мережах, оскільки там часто видаляється інформація про автора. Водяні знаки гарантують, що власник фото буде чітко ідентифікований, навіть якщо зображення розповсюджуватиметься далі.

3.2 Моделювання діаграми послідовності нанесення цифрових водяних знаків

Діаграма послідовності (див. Додаток Б) відображає процес додавання цифрових водяних знаків до контенту покроково. Загальний опис такої діаграми:

1. Користувач обирає вміст для захисту, визначивши фотографію або відео, на яке потрібно додати цифровий водяний знак.

2. Користувач вибирає тип цифрового водяного знака, який він хоче застосувати: текстовий, графічний або комбінацію обох.

3. Користувач налаштовує параметри водяного знака, такі як розмір, прозорість, розташування тощо.

4. Система генерує цифровий водяний знак відповідно до обраних параметрів.

5. Система накладає згенерований водяний знак на вибраний користувачем контент згідно з вказаними налаштуваннями.

6. Користувач може попередньо переглянути результат і внести необхідні коригування для досягнення бажаного ефекту.

7. Після додавання водяного знака користувач може зберегти модифікований контент для подальшого використання або публікації.

8. Змінений контент із цифровим водяним знаком може бути опублікований або використаний відповідно до вимог авторського права [23].

Перелічені вимоги конкуруючі взаємно і не можуть оптимальними бути одночасно. При необхідності приховувати великі повідомлення всередині зображень, унеможливлює абсолютну невидимість і високу стійкість. дане спостереження зображено схематично на рис. 3.1.

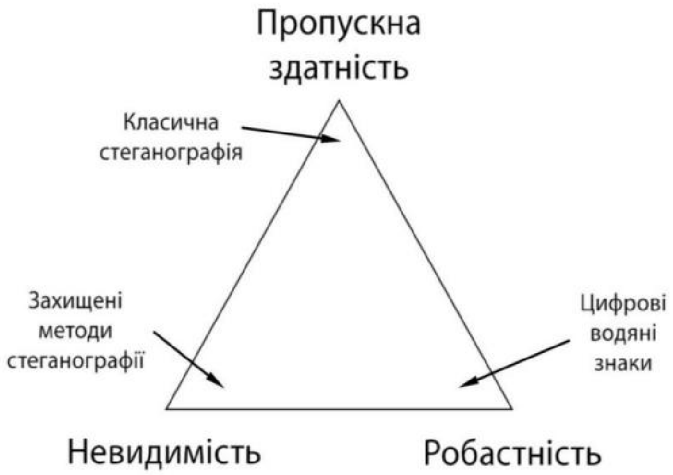


Рисунок 3.1 – Трикутник моделювання ЦВЗ з характеристикою стеганосистеми

Як бачимо з рисунка 3.1. завжди потрібно шукати компроміс. Або ж, якщо потрібна стійкість до спотворення зображення, тоді наше повідомлення має мати належний сховок і не бути дуже великим.

Майже всі відомі алгоритми можна класифікувати за типом області, у яку вбудовується чи з якої вилучається ЦВЗ, пропускною здатністю яку вони мають, продуктивністю в режимі реального часу, а також стійкістю до певних типів атак. В залежності від місця вбудовування ЦВЗ, сучасні алгоритми які їх вбудовують у відеофайли можна умовно поділити на такі основні групи:

- алгоритми вбудовування в просторовій області;
- в області перетворень
- алгоритми вбудовування у відеофайли, стиснені за стандартом MPEG (рисунок 3.2).

Рисунок 3.2 – Класифікація алгоритмів побудови ЦВЗ

У вітчизняній та закордонній літературі описано багато різних методів і алгоритмів для додавання цифрового водяного знаку до медіафайлів. За стандартом MPEG ці методи поділяються на просторові, частотні та стиснені (рисунок 3.3). Наприклад, просторовий метод LSB. До частотних – ЦВЗ додається шляхом розширення спектру.

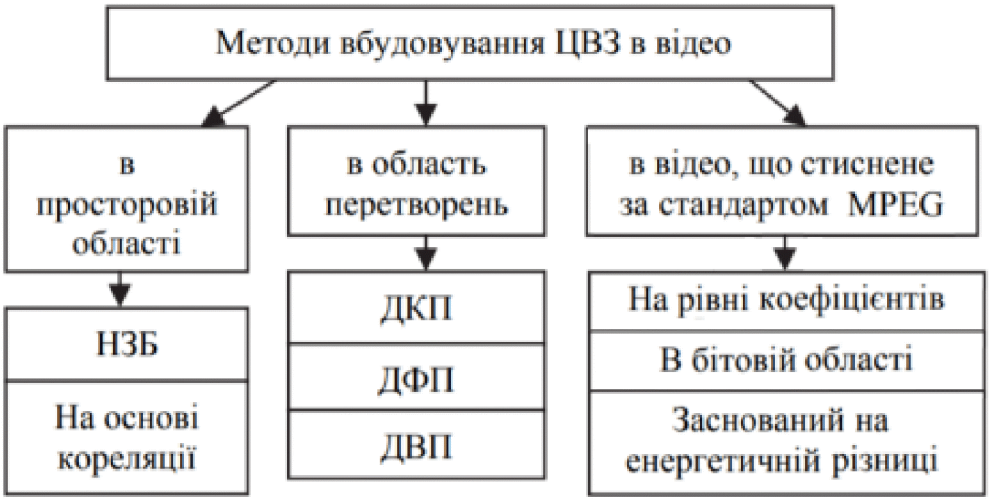


Рисунок 3.3 – Огляд методів вбудовування ЦВЗ з відео

Розглянемо алгоритми вбудовування ЦВЗ у відео (див. Додаток А), які зараз використовуються: адитивні, на основі злиття ЦВЗ і контейнера, фрактальні перетворення та інші. В адитивних методах впровадження ЦВЗ послідовність чисел

wi довжини N впроваджується в вибрану підмножину відліків вихідного зображення f.

Для підвищення стійкості цифрових водяних знаків (ЦВЗ) до видалення, в багатьох алгоритмах використовуються широкосмугові сигнали. Це включає багаторазове повторення інформаційних бітів, кодування із застосуванням корегуючих кодів або інших перетворень, після чого вони модулюються псевдовипадковою гаусівською послідовністю. Така послідовність моделює шум, присутній у реальних зображеннях. На відміну від цього, синтетичні зображення зазвичай не містять шумів, тому впровадження ЦВЗ у них є складнішим. Тому замість псевдовипадкової послідовності, часто легше використовувати рівномірно розподілену послідовність, яку потім перетворюють у гаусову [1].

Крім того, замість використання псевдовипадкових чисел, в зображення може вбудовуватися інше зображення, наприклад логотип. Такі алгоритми називаються алгоритмами злиття. Розмір впроваджуваного повідомлення значно менший за розмір вихідного файлу, і воно може бути зашифровано або перетворено іншим чином. Перевагою таких алгоритмів є те, що вони використовують складні моделі людського сприйняття і навіть при спотворенні прихованого повідомлення, наявність впровадженого логотипу є переконливим доказом авторських прав.

Особливість методу стеганографічного вбудовування інформації у стегоконтейнер із використанням фрактальних перетворень полягає в застосуванні двовимірного фрактального зображення як ключа. Наприклад, можна використовувати фрактальне зображення множини Жюліа як секретний ключ. Це унеможливлює згенерування ідентичного фрактального зображення без знання певного комплексного числа [**Помилка! Джерело посилання не знайдено.**].

Існуючі методи, такі як шифрування посилок, не можуть захистити авторські права, права інтелектуальної власності та конфіденційні дані від несанкціонованого доступу. Перевагою методу є те, що використання фракталів дозволяє практично не втрачати ЦВЗ, при цьому стегоконтейнер візуально не відрізняється від контейнера з конфіденційною інформацією.

Оскільки в Україні питання ефективного захисту авторського права в Інтернеті ще не вирішене, необхідні дослідження та узагальнення міжнародного досвіду для відповідного правового регулювання [**Помилка! Джерело посилання не знайдено.**].

Дослідження технологій нанесення ЦВЗ на графічний контент.

Стеганографічні алгоритми за способом вбудовування цифрових водяних знаків (ЦВЗ) поділяються на адитивні та нелінійні. В адитивних алгоритмах вихідне зображення лінійно модифікується для вбудовування інформації, а при вилученні використовуються кореляційні методи. При цьому ЦВЗ або є частиною зображення-контейнера, або вплавлений в нього. Нелінійні методи в основному ґрунтуються на скалярному та векторному квантуванні (див.Додаток В).

Серед лінійних алгоритмів можна виокремити методи приховування даних у просторовій області та в області перетворення. Нелінійні методи можна поділити на алгоритми розширення спектра, скалярного та векторного квантування, а також методи, що базуються на фрактальному кодуванні [12].

Метод заміни найменш значущого біта (LSB – Least Significant Bit) є найпопулярнішим серед методів заміни у просторовій області. Найменший значущий біт зображення майже не містить інформації, тому людина зазвичай не помічає змін у ньому. Фактично LSB є шумом, тому його можна використовувати для вбудовування інформації шляхом заміни менш значущих бітів пікселів зображення бітами секретного повідомлення. Для зображень у відтінках сірого (кожен піксель кодується одним байтом) обсяг вбудованих даних може становити 1/8 від загального обсягу контейнера. Популярність цього методу зумовлена його простотою та високою пропускною здатністю.

3.3 Безпосередній захист авторських прав після нанесення ЦВЗ на графічний контент

Захист фотографій від незаконного тиражування та поширення стає особливо місцем у сучасному світі, надалі розвиваються глобальні мережі. Багато досліджень вивчали стеганографію як засіб захисту графічних даних.

Згідно з чинним законодавством, автор має право на будь-який твір, такий як фотографія чи інше зображення. Однак підтвердження авторства може бути складним у деяких випадках.

Один із загальноприйнятих методів захисту авторських прав - вбудовування знака копірайту у захищений контейнер. Проте, недоліком цього методу є можливість видалення знака при обрізанні зображення.

Щоб уникнути цієї проблеми, можна використовувати невидимі та невіддільні від контейнера цифрові водяні знаки. Ці знаки не впливають на якість зображення і не помітні для ока, але дозволяють ідентифікувати власника.

Компанія Digimarc розробила систему для розпізнавання цифрових водяних знаків, інтегровану в популярний графічний редактор Adobe Photoshop. Ця система звертається до онлайн-бази даних, використовуючи водяний знак як ключ, і знаходить інформацію про автора роботи, навіть після внесених змін [22].

При створенні таких стегосистем застосовуються методи цифрової стеганографії, які враховують вимоги робастності (стійкості до спотворень), прозорості (відсутності відмінностей між початковим і зміненим зображеннями) та стійкості до атак (спроб видалення або спотворення вбудованого повідомлення).

Перед приховуванням текстового файлу в контейнері його можна захистити за допомогою криптографічного кодування, наприклад, шифру Віженера. Для чіткого визначення початку та кінця прихованого повідомлення при розпакуванні контейнера доцільно використовувати секретні мітки, які обмежують це повідомлення. Ці мітки повинні бути достатньо довгими, щоб випадкові символи не сприймалися як мітки.

Графічні контейнери поділяються на "чисті" та "зашумлені". У "чистих" контейнерах можна виявити зв'язки між молодшими та іншими бітами колірних компонентів, а також залежності між молодшими бітами [15].

Вбудовування повідомлення в "чисте" зображення порушує ці існуючі залежності, що може бути легко виявлено. Якщо зображення спочатку є "зашумленим" (наприклад, відскановане або цифрове фото), виявлення прихованого повідомлення стає складнішим, хоча й можливим за допомогою теорії ймовірностей і математичної статистики.

РОЗДІЛ 4
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Обґрунтування організаційно-технічних рекомендацій з охорони праці

Ці рекомендації базуються на наукових дослідженнях, законодавстві та нормах, а також на практичних досвіду охорони праці. Організаційні рекомендації з охорони праці включають такі аспекти:

1. Розробка політики безпеки та здоров'я: Рекомендується визначити чітку політику охорони праці, яка забезпечує впровадження найкращих практик у сфері безпеки праці. Це включає зобов'язання керівництва компанії створити безпечне робоче середовище та забезпечити необхідні ресурси для виконання цієї політики.

2. Організація навчання та підвищення кваліфікації: Рекомендується проводити регулярні навчальні програми з охорони праці для всіх працівників. Це допоможе забезпечити, що всі працівники мають необхідні знання та навички для безпечного виконання своїх обов'язків. Також слід сприяти підвищенню кваліфікації працівників в галузі охорони праці.

3. Встановлення процедур безпеки: Рекомендується розробити та впровадити процедури безпеки для всіх робочих процесів і ділянок. Це може включати в себе правила використання особистого захисного спорядження, правила безпеки під час роботи з небезпечними речовинами або машинами, а також процедури евакуації та пожежної безпеки.

4. Забезпечення відповідного обладнання та інструментів: Рекомендується забезпечити працівників необхідним безпечним обладнанням та інструментами для виконання їх роботи. Це може включати застосування захисних установок на машинах, систем вентиляції, ергономічне обладнання для зниження ризику виникнення травм.

5. Регулярний контроль та оцінка ризиків: Рекомендується проводити регулярні перевірки робочих місць з метою ідентифікації потенційних ризиків та оцінки їх впливу на здоров'я працівників. На основі цих оцінок можна 48 розробити та впровадити відповідні заходи з мінімізації ризиків та забезпечити безпеку праці.

Технічні рекомендації з охорони праці можуть включати такі аспекти:

1. Використання технологічних інновацій: Рекомендується використовувати технологічні рішення, які допомагають зменшити ризики для працівників. Наприклад, використання автоматизованих систем контролю безпеки, систем виявлення пожежі або систем моніторингу здоров'я працівників.

2. Ергономічне проектування робочих місць: Рекомендується враховувати принципи ергономіки при проектуванні робочих місць. Це допоможе забезпечити комфортні умови праці, запобігти травмам внаслідок неправильної позиції тіла або надмірного фізичного зусилля.

3. Розміщення заходів безпеки: Рекомендується розміщувати сигналізаційні таблички, інструкції з безпеки, екстрені виходи та засоби пожежогасіння у відповідних місцях для швидкого доступу працівників до них.

4. Постійне вдосконалення системи охорони праці:

Рекомендується постійно оновлювати та вдосконалювати систему охорони праці на основі нових вимог, технологій та рекомендацій.

Це допоможе забезпечити високий рівень безпеки та здоров'я працівників. Враховуючи ці організаційно-технічні рекомендації з охорони праці, компанії зможуть створити безпечне та здорове робоче середовище, знизити ризик виникнення нещасних випадків та захворювань серед працівників, а також забезпечити високу продуктивність та задоволення від роботи.

4.2 Огляд травмонебезпечних ситуацій під час виконання робіт

При аналізі травмонебезпечних ситуацій під час виконання робіт для розробки вебсайту кав’ярні, можна переглянути наступні аспекти:

1. Оцінка ризиків: проводиться детальний аналіз, потенційних травмонебезпечних ситуацій, які можуть статись в процесі розробки. Сюди можна включити такі пункти, як робота з апаратним забезпеченням, підключення до мережі, робота з електрикою і тому подібне.

2. Виявлення потенційних небезпек: встановлення можливих ризиків травматичних ситуацій або загроз, пов'язаних з різними етапами розробки вебсайту. Для прикладу: ризики пов'язані з програмним забезпеченням.

3. Застосування запобіжних заходів: розробка стратегій та методів з метою попередження можливих ризиків травмування. Сюди входить навчання персоналу, правильне розташування мережевих та електричних кабелів і звісно використання безпечних методів роботи які значно знижують ризик травмонебезпечних ситуацій.

4. Розробка безпечних вказівок. Цей аспект стосується визначення чітких правил безпеки, яких слід дотримуватись під час розробки вебсайту. Сюди входять регулярні перерви для відпочинку, контроль робочого місця на наявність небезпек, а також дотримання правил безпеки при роботі з технікою. 5. Документування та звітність. Цей пункт стосується формулювання записів щодо будь-яких травмонебезпечних ситуацій, які виникають під час розробки.

Це допомагає виявити тенденції, та прийняти відповідні заходи для запобіганню подібним ситуаціям у майбутньому.

4.3 Структурно-функціональний аналіз дотримання охорони праці при роботі з комп'ютером

Основною метою цього аналізу є забезпечення безпеки працівників та запобігання можливим травмам, фізичному та моральному здоров'ю. Структурно-функціональний аналіз дотримання охорони праці допомагає розпізнати, оцінити та вжити заходи безпеки для комфорту і здоров'я працівників. Структурна частина аналізу включає наступні елементи:

1. Організаційна структура: вивчення структури організації щодо визначення відповідальних осіб за безпеку праці та їх обов'язків.

2. Політика безпеки: оцінка наявності та ефективності політики безпеки, яка охоплює правила, процедури та норми, що регулюють безпеку праці при роботі з

комп'ютером. Це включає наявність письмових інструкцій, тренінгів та інших заходів для дотримання правил безпеки.

3. Оцінка ризиків: аналіз потенційних ризиків пов'язаних з роботою за комп'ютером, таких як погана ергономіка робочого місця, неправильна постановка монітора, незручна клавіатура і тому подібне. Функціональна частина аналізу охорони праці включає наступні аспекти:

1. Забезпечення необхідних ресурсів: переконання що працівники мають необхідне обладнання та інфраструктуру, які дозволяють їм працювати з комп'ютером в безпечних умовах. Сюди входять належна налаштовані робочі столи, зручні крісла, антиблікові фільтри на моніторах і т.д.

2. Навчання та освіта: забезпечення навчання та освіти працівників з питань безпеки праці при роботі з комп'ютером. Це включає навчання правильній постановці рук, використанню пауз та вправ для очей, що сприяють здоров'ю та безпеці працівників.

3. Моніторинг та оцінка: здійснення постійного моніторингу та оцінки дотримання правил безпеки при роботі з технікою, виявлення можливих проблем та розробка відповідних заходів для їх вирішення.

ВИСНОВКИ

В ході виконання даної кваліфікаційної роботи бакалаврського рівня, було проаналізовано, оглянуто та детально досліджено методи нанесення цифрових водяних знаків на зображення та відео-контент для забезпечення захисту авторських прав та для запобігання крадіжки даних, витоку даних, піратства, зламу чи іншої незаконної діяльності.

Отож, в даній роботі була вивчена та проаналізована предметна область, яка є пов'язана із захистом авторських прав на відео та графічний контент за допомогою нанесення цифрових водяних знаків (ЦВЗ).

У першому розділі детально розглянута, а також проаналізована предметна область, а саме: основні види комп'ютерної графіки та її формати, розглянуто та порівняно відносні переваги та недоліки між основними видами графічних об'єктів; основні види відео-контенту, а також їх формати, підвиди відеофайлів та особливості їхнього використання і звісно ж було описано основні характеристики цифрових водяних знаків; було розглянуто та описано визначення авторських прав та види злочинної діяльності у мережі.

Безумовно, початком цієї роботи у вступній частині було висвітлено та обґрунтовано актуальність теми дослідження, оскільки захист авторських прав у сучасному цифровому середовищі це надзвичайно важлива проблема. Під час розгляду актуальності теми роботи, було виявлено потребу у вдосконаленні методів нанесення ЦВЗ та аналізу їхньої стійкості алгоритмів та методики нанесення.

У результатах дослідження, безпосередньо, були виявлені переваги та недоліки використання ЦВЗ для захисту авторських прав на відео та графічний контент. Дослідження показали, що нанесення ЦВЗ у програмі iWatermark дозволяє додавати, змінювати та читати метадані фотографій. Це особливо корисно для професійних фотографів. Після створення таких наборів метаданих, їх можна легко застосовувати до багатьох фотографій одним кліком.

Також були розроблені алгоритми та наведені діаграми послідовності для застосування цих методів у практичній сфері.

А також, для забезпечення подальшої безпеки та дисципліни під час виконання кваліфікаційної роботи були запропоновані організаційно-технічні рекомендації з охорони праці (ОП) та безпеки в надзвичайних ситуаціях під час виконання робіт з комп'ютерною графікою та обробки відео-контенту.

Підсумовуючи вище зазначене та проведене дослідження, хочеться зазначити, що дана робота є досить важливим внеском у розвиток методів захисту авторських прав у цифровому середовищі та може слугувати основою для подальших досліджень у даній області.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Alan Siper Roger Farley and Craig Lombardo. The Rise of Steganography. Seidenberg School of CSIS Homepage. URL: https://csis.pace.edu/~ctappert/srd2005/d1.pdf (дата звернення: 12.01.2024).

2. Jeong J., Chun M. Y., Choo H. Integrated OTP-Based User Authentication Scheme Using Smart Cards in Home Networks. URL: https://www.researchgate.net/publication/221179773_Integrated_OTPBased_User_Authentication_Scheme_Using_Smart_Cards_in_Home_Networks (дата звернення: 13.02.2024).

3. Koptyra, K.; Ogiela, M.R. Steganography in IoT: Information Hiding with Joystick and Touch Sensors. 2023. 3288. URL: https://doi.org/10.3390/s23063288 (дата звернення: 29.12.2023).

4. Least Significant Bit. Science Direct. URL: https://www.sciencedirect.com/topics/computer-science/least-significant-bit (date of access: 10.02.2024).

5. Niels Provos. Abstract Defending Against Statistical Steganalysis. URL: https://www.researchgate.net/publication/2538327_Abstract_Defending_Against_Statistical_Steganalysis (дата звернення:13.02.2024).

6. Q&A про цифрові знаки. URL: https://plumamazing.com/uk/watermark-faq/ (дата звернення:17.03.2024).

7. Види комп'ютерної графіки. URL: https://www.miyklas.com.ua/p/informatica/6-klas/komp-iuterna-grafika-327916/poniattia-komp-iuternoyi-grafiki-326242/re-3ba2d73c-278d-4c0a-94e9-7b7812a7505f (дата звернення:01.04.2024).

8. Використання ЦВЗ. URL: https://internera.com/uk/blog/vodjanoj-znak-dlja-foto-votermark- (дата звернення:10.02.2024).

9. Водяні знаки. URL: https://dalistrategies.com/ua/vodyani-znaki/ (дата звернення:10.02.2024).

10. Застосування водяних знаків. URL: https://radiant.zapisi.cx.ua/ukraincyam/navishho-zastosovuyutsya-vodyani-znaki-osnovni-prichini-ta-metodi-vikoristannya.html (дата звернення:10.02.2024).

11. Захист відео онлайн сервісів. JOOMLA центр: веб-сайт. URL: https://joomla.center/blog-kurteev/kak-zashchitit-onlajnvideo (дата звернення:14.02.2024).

12. Інструменти ЦВЗ. URL: https://www.datanumen.com/uk/%D0%B1%D0%BB%D0%BE%D0%B3%D0%B8/11-%D0%BD%D0%B0%D0%B9%D0%BA%D1%80%D0%B0%D1%89%D0%B8%D1%85-%D0%B1%D0%B5%D0%B7%D0%BA%D0%BE%D1%88%D1%82%D0%BE%D0%B2%D0%BD%D0%B8%D1%85-%D1%96%D0%BD%D1%81%D1%82%D1%80%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D1%96%D0%B2-%D0%B4%D0%BB%D1%8F-%D0%BC%D0%B0%D0%BB%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F-%D0%B2%D0%BE%D0%B4%D1%8F%D0%BD%D0%B8%D1%85-%D0%B7%D0%BD%D0%B0%D0%BA%D1%96%D0%B2/ (дата звернення:12.03.2024).

13. Конахович Г. Ф., Прогонов Д. О., Пузиренко О. Ю. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних [підручник]. – К. : «Центр навчальної літератури», 2018. – 558 с.

14. Лісковський І.О., Кулик М.В. Реалізація стеганографічної системи для відео з використанням сингулярного розкладання. // Дванадцята міжнародна науково-технічна конференція «Проблеми телекомунікацій»; Десята міжнародна науково-технічна конференція студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем»: Матеріали конференції. К.: НТУУ "КПІ", 2018. – с. 288-290.

15. Нанесення ЦВЗ ШІ. URL: https://thetransmitted.com/ai/chi-mozhemo-mi-doviriti-shi-nanesennya-vodyanih-znakiv/ (дата звернення:12.03.2024).

16. Переваги відеоконтенту. URL: https://alpina-production.com/uk/news/10-preimushchestv-videokontenta/ (дата звернення:12.03.2024).

17. Переваги та недоліки 3-D графіки. URL: https://mukachevo.net/news/perevahy-ta-nedoliky-3d-hrafiky_1714877.html (дата звернення: 25.02.2024).

18. Растрові та векторні зображення. URL: https://informatik.pp.ua/uroky/6-klas/konspekty-uchnia/urok-2-rastrovi-ta-vektorni-zobrazhennia-formaty-failiv/ (дата звернення:15.01.2024).

19. Формати відео та їх характеристика. URL: https://ipkey.com.ua/uk/faq/550-video-formats.html (дата звернення:15.04.2024).

20. Формати графічних зображень. URL: https://uk.wikipedia.org/wiki/%D0%93%D1%80%D0%B0%D1%84%D1%96%D1%87%D0%BD%D1%96_%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8 (дата звернення:15.01.2024).

21. Фрактальна графіка. URL: https://elib.lntu.edu.ua/sites/default/files/elib_upload/%D1%84%D0%B5%D0%B4%D1%96%D0%BA%202/page12.html (дата звернення:13.01.2024).

22. ЦВЗ. URL: https://uk.wikipedia.org/wiki/%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B8%D0%B9_%D0%B2%D0%BE%D0%B4%D1%8F%D0%BD%D0%B8%D0%B9_%D0%B7%D0%BD%D0%B0%D0%BA (дата звернення:18.01.2024).

23. Як додати ЦВЗ? URL: https://netpeak.net/uk/blog/shcho-take-vodyaniy-znak-ta-yak-yogo-vikoristovuyut/ (дата звернення:18.01.2024).

24. Портал відкритих даних. URL: https://data.gov.ua./ (дата звернення:18.01.2024).

ДОДАТКИ

Додаток А

Код алгоритму для вставки ЦВЗ:

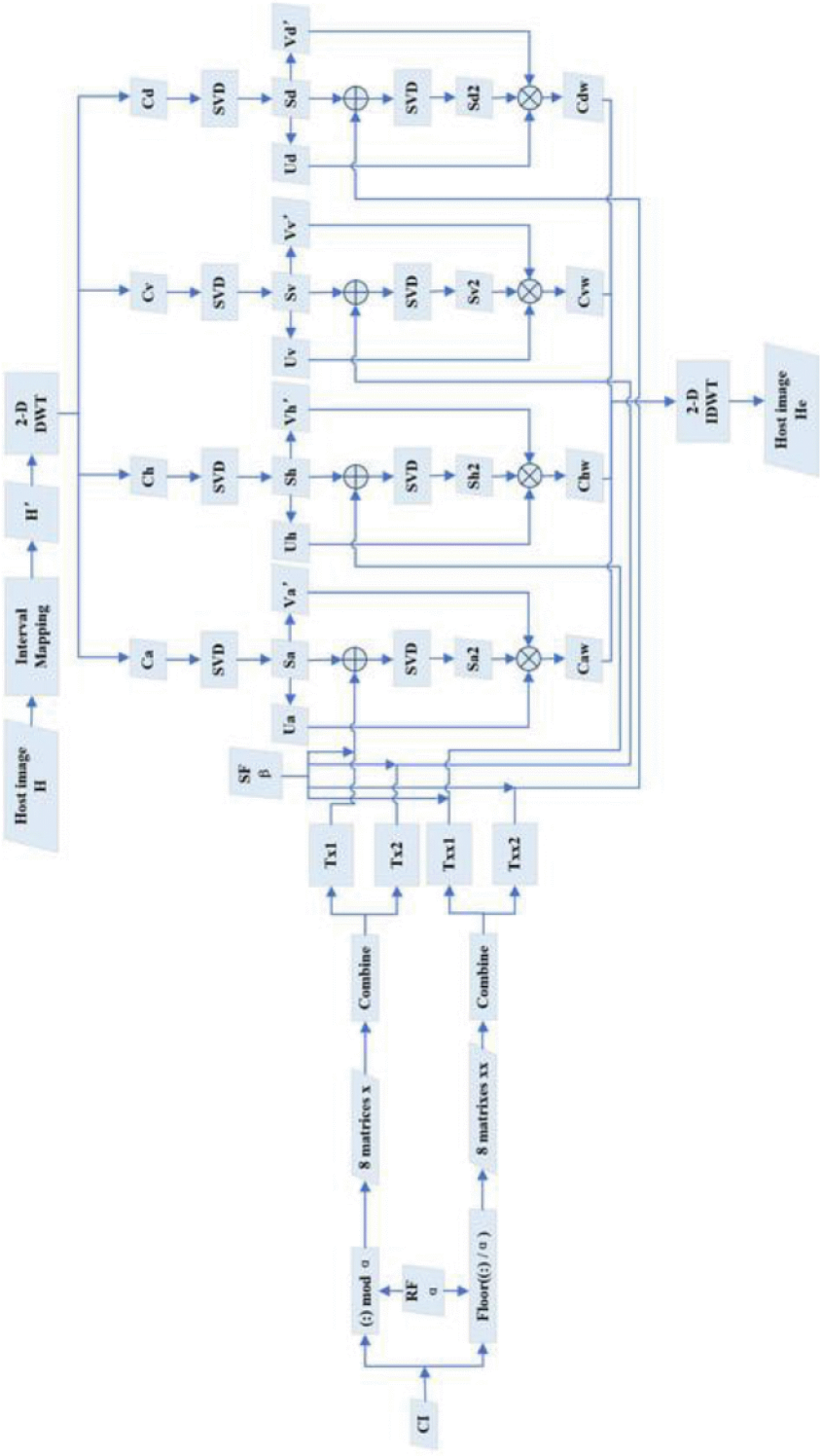
```
# Scramble the data

scrambled_data = scramble(data, secret)
mesh = pymesh.load_mesh(filename_in)
if partitions == -1:
 partitions = mesh.num_vertices/500

# Partition the mesh into patches
patches, mapping =
partitioning.mesh_partitioning(filename_in,
mesh, partitions)
```

Додаток Б

Рисунок діаграми послідовності:



Додаток В

Функція для підрахунку власних векторів:

```
def compute_eigenvectors (num_vertices, patch):
 laplacian = np.zeros((num_vertices, num_vertices))

 # Get the list of neighbors and the valence of each vertice
 star, d = utils.get_neighbors_and_valence(num_vertices,
patch)

 # Compute the Laplacian
 for i in range(num_vertices):
 laplacian[i][i] = 1
 for j in star[i]:
 laplacian[i][int(j)] = -1.0/d[i]

 # Get the eigenvectors and eigenvalues of the laplacian
 eigenValues, eigenVectors = np.linalg.eig(laplacian)

 # Sort the eigenvectors regarding to their eigenvalues
 idx = eigenValues.argsort()
 eigenValues = eigenValues[idx]
 eigenVectors = eigenVectors[:,idx]
 return np.transpose(eigenVectors)
```