

Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

Підвищення стійкості вбудовуваного цифрового водяного знаку у потоковий відеозапис на основі вдосконаленого диференціального вбудовування енергії (DEW)

Виконав: ст. 2-го курсу, групи УБ-21м
спеціальності 125– Кібербезпека
Освітня програма – Управління
інформаційною безпекою

Козак Д.О. *Д. Козак*

Керівник: к.т.н., доц., доцент каф. МБІС
Карпінєць В.В. *В. Карпінєць*

« 15 » чрудня 2022 р.

Опонент: к.т.н., доц., доцент каф. ОТ

Савицька Л.А. *Л. Савицька*

« 15 » чрудня 2022 р.

Допущено до захисту

Голова секції УБ кафедри МБІС

Юрій Яремчук
Юрій ЯРЕМЧУК

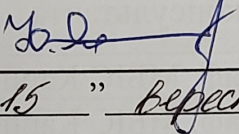
« 15 » чрудня 2022 р.

Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

Рівень вищої освіти II-й (магістерський)
Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітньо-професійна програма – Управління інформаційною безпекою

ЗАТВЕРДЖУЮ

Голова секції УБ, кафедра МБІС

 **Юрій ЯРЕМЧУК**
“ 15 ” вересня 2022 р.

ЗАВДАННЯ

на магістерську кваліфікаційну роботу студенту

Козак Діані Олегівні

1. Тема роботи «Підвищення стійкості вбудовуваного цифрового водяного знаку у потоковий відеозапис на основі вдосконаленого диференціального вбудовування енергії (DEW)»

Керівник роботи Карпинець В.В. к.т.н., доцент затверджені наказом вищого навчального закладу від «14» вересня 2022 року № 203

2. Строк подання студентом роботи за тиждень до захисту

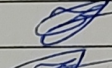

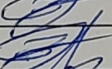

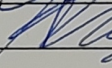

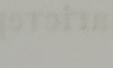

3. Вихідні дані до роботи: нормативно-правова база, монографії та сучасні наукові статті по темі, Інтернет-ресурси, стандарти, існуюче ПЗ.

4. Зміст текстової частини: в першому розділі проаналізувати методи вбудовування цифрових водяних знаків у відео; в другому розділі здійснити вдосконалення методу, провести проектування розробки, розробити алгоритми програмної частини; в третьому розділі здійснити програмну реалізацію розробки та аналіз результатів; в четвертому розділі проаналізувати економічну ефективність розробленого програмного забезпечення.

5. Перелік ілюстративного матеріалу (з точним зазначенням обов'язкових креслень):

- у першому розділі наведено 8 рис., 1 табл.;
- у другому розділі наведено 8 рис.;
- у третьому розділі наведено 20 рис., 4 табл.;
- у четвертому розділі наведено 1 рис. та 6 табл.

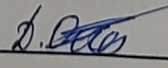
6. Консультанти розділів магістерської кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	к.т.н., доц. каф. МБІС Карпинець В.В.		
2	к.т.н., доц. каф. МБІС Карпинець В.В.		
3	к.т.н., доц. каф. МБІС Карпинець В.В.		
4	зав. каф. ЕПВМ, к.т.н. Лесько О.Й.		

7. Дата видачі завдання 15 вересня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів МКР	Строк виконання етапів МКР	Примітка
1.	Визначення напрямку МКР, формулювання теми	15.09.2022	30.09.2022
2.	Аналіз предметної області обраної теми	01.10.2022	15.10.2022
3.	Розробка алгоритму роботи	16.10.2022	31.10.2022
4.	Написання МКР на основі розробленої теми	01.11.2022	15.11.2022
5.	Розробка економічної частини	15.11.2022	23.11.2022
6.	Попередній захист МКР	24.11.2022	25.11.2022
7.	Виправлення, уточнення, коригування роботи	26.11.2022	15.12.2022
8.	Захист МКР	19.12.2022	21.12.2022

Студент  Козак Д.О.

Керівник МКР  Карпинець В.В.

АНОТАЦІЯ

УДК: 621.391.7

Козак О.Д. Підвищення стійкості вбудовуваного цифрового водяного знаку у потоковий відеозапис на основі вдосконаленого диференціального вбудовування енергії (DEW). Магістерська кваліфікаційна робота зі спеціальності 125 – «Кібербезпека», освітня програма «Управління інформаційною безпекою». Вінниця: ВНТУ, 2022. 108 с.

На укр. мові. Бібліогр.: 46 назв; рис.: 36; табл. 12.

У магістерській кваліфікаційній роботі представлено підвищення стійкості вбудовуваного цифрового водяного знаку у потоковий відеозапис на основі вдосконаленого диференціального вбудовування енергії із подальшою реалізацією даного вдосконаленого методу у розробленому онлайн-сервісі.

В першому розділі роботи здійснено аналіз теоретичного матеріалу обраної галузі: досліджено цифровий водяний знак, як засіб захисту авторського права, проведено аналіз алгоритмів вбудовування ЦВЗ та можливі атаки на них.

У другому розділі роботи описано вдосконалення методу за рахунок вбудовування ЦВЗ лише у низькочастотні коефіцієнти дискретно-косинусного перетворення та застосування методу сегментації Канні, який використовує багаторівневий обчислювальний підхід виявлення меж сегментів на зображенні та сприяє зменшенню візуальних змін контейнера.

У третьому розділі роботи здійснено практичну реалізацію онлайн-сервісу із використанням вдосконаленого алгоритму та дослідження результатів роботи, за підсумками яких зроблено висновок, що в загальному застосування вдосконаленого методу дозволяє підвищити показники орієнтовно на 12%.

У четвертому розділі роботи здійснено аналіз економічної доцільності розробки, який свідчить про її високий комерційний потенціал та доцільність подальшого впровадження.

Ключові слова: цифровий водяний знак, Differential Energy Watermarking, метод Канні, стійкість ЦВЗ, онлайн-сервіс, потокове відео.

ABSTRACT

Diana Kozak. Improving the robustness of embedded digital watermarking in video streaming based on improved differential energy embedding (DEW). Master's thesis in specialty 125 – «Cyber Security», Education Program «Information Security Management». Vinnitsa: VNTU, 2022. – 108 p.

In Ukrainian language. Bibliographer: 46 titles; fig.: 36; tabl. 12.

The master's thesis presents the improvement of the stability of the embedded digital watermark in the streaming video based on the improved differential energy embedding with the further implementation of this improved method in the developed online service.

In the first section of the work, an analysis of the theoretical material of the selected field was carried out: the digital watermark as a means of copyright protection was investigated, the algorithms of embedding of watermark and possible attacks on them were analyzed.

The second section of the work describes the improvement of the method by embedding the watermark only in the low-frequency coefficients of the discrete-cosine transformation and the application of the Canni segmentation method, which uses a multi-level computational approach to detect the boundaries of segments in the image and helps to reduce the visual changes of the container.

In the third section of the work, the practical implementation of the online service was carried out using the improved algorithm and the study of the results of the work, based on the results of which it was concluded that the general application of the improved method allows to increase the indicators by approximately 12%.

In the fourth chapter of the work, an analysis of the economic feasibility of the development was carried out, which testifies to its high commercial potential and the feasibility of further implementation.

Key words: digital watermark, Differential Energy Watermarking, Canni's method, watermark persistence, online service, streaming video.

ЗМІСТ

ВСТУП.....	7
1 ЗАГАЛЬНИЙ АНАЛІЗ ГАЛУЗІ СТЕГANOГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ.....	9
1.1 Актуальність дослідження обраної галузі.....	9
1.2 Аналіз особливостей цифрового водяного знаку	12
1.3 Аналіз алгоритмів генерування та вбудовування ЦВЗ	17
1.4 Аналіз атак на стегосистеми із ЦВЗ.....	21
1.5 Висновки та постановка задач.....	24
2 ПІДВИЩЕННЯ СТІЙКОСТІ ВБУДОВУВАНОВОГО ЦИФРОВОГО ВОДЯНОГО ЗНАКУ У ПОТОКОВИЙ ВІДЕОЗАПИС	25
2.1 Розробка алгоритму роботи методу для вбудовування ЦВЗ.....	25
2.2 Вдосконалення алгоритму вбудовування ЦВЗ у відео	28
2.3 Розробка алгоритму роботи програмного додатку	31
2.4 Обґрунтування вибору засобів програмування	36
2.5 Висновки до розділу	40
3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ВДОСКОНАЛЕНОВОГО МЕТОДУ ВБУДОВУВАННЯ ЦВЗ НА ПРИКЛАДІ ОНЛАЙН-СЕРВІСУ.....	41
3.1 Розробка графічного інтерфейсу програмної розробки.....	41
3.2 Програмна реалізація вдосконаленого алгоритму	45
3.3 Інструкція користувача для роботи з онлайн-сервісом	50
3.4 Аналіз результатів та тестування вдосконаленого методу.....	56
3.5 Висновки до розділу	63
4 ЕКОНОМІЧНА ЧАСТИНА.....	64
4.1 Оцінювання комерційного потенціалу розробки програмного забезпечення 64	
4.2 Прогнозування витрат на виконання наукової роботи та впровадження її результатів	70
4.3 Прогнозування комерційних ефектів від реалізації результатів розробки	74

4.4 Розрахунок ефективності вкладених інвестицій та періоду їх окупності	76
4.5 Висновки до розділу	79
ВИСНОВОК.....	81
ПЕРЕЛІК ПОСИЛАНЬ	83
ДОДАТКИ.....	88
Додаток А. Технічне завдання	89
Додаток Б. Лістинг HTML-сторінки	93
Додаток В. Лістинг фрагментів frontend-частини.....	95
Додаток Г. Інтерфейс онлайн-сервісу	98
Додаток Д. Ілюстративний матеріал	100
Додаток Е. Протокол перевірки на антиплагіат.....	108

ВСТУП

Актуальність. Завдання захисту інтелектуальної власності на сьогодні не тільки не втрачає своєї актуальності, але стає ще більш затребуваним через безперервне зростання обсягів цифрової інформації та ширше використання Інтернету. Поширення впровадження цифрових водяних знаків (ЦВЗ) у цифрові контейнери для захисту прав власності призводить до необхідності розробки методів, більш стійких до активних атак та природних спотворень у каналі обробки та передачі [1].

На даний момент одним із затребуваних підходів у цій галузі є застосування технологій, що базуються на використанні методів комп'ютерної стеганографії [2] та дозволяють потай вбудовувати необхідні дані в будь-які інформаційні масиви та об'єкти цифрового контенту (файли аудіо та відео, файли текстових форматів, нерухомі зображення тощо).

Технології цифрових водяних знаків (ЦВЗ) успішно використовуються для вирішення завдань підтвердження авторського права по відношенню до цифрових файлів, контролю їх використання авторизованими користувачами та іншими особами, підтвердження справжності та надійності копій програмних засобів та мультимедіа об'єктів, що використовуються [3 – 4].

Проте, із швидкими темпами розвитку технологій, зростає також потреба у постійному вдосконаленні методів вбудовування ЦВЗ, з метою уникнення зниження стійкості ЦВЗ до атак. Таким чином, дослідження у галузі підвищення стійкості методів ЦВЗ залишається наразі актуальним.

В роботі для дослідження обраний алгоритм вбудовування цифрового водяного знаку, що базується на ідеї диференціального енергетичного водяного знаку, та є методом вбудовування ЦВЗ, що заснований на вибіркового відкиданні частини високочастотних коефіцієнтів ДКП стислих зображень і відеозображень.

Для вдосконалення методу в роботі були внесені зміни до математичного апарату алгоритму DEW та застосовано оператор Канні з метою усунення

недоліку суттєвої помітності візуальних змін контейнера. Практичне тестування вдосконаленого методу, показало підвищення стійкості ЦВЗ на основі вдосконаленого методу орієнтовно на 12%, порівняно з базовим алгоритмом.

Мета і задачі дослідження. Метою роботи є підвищення стійкості вбудовуваного цифрового водяного знаку у потоковий відеозапис на основі вдосконаленого диференціального вбудовування енергії та програмна розробка онлайн-сервісу для практичної реалізації алгоритму.

Задачами дослідження є:

- аналіз існуючих методів захисту авторського права засобами стенографії та особливості застосування ЦВЗ у відео файлах;
- здійснення вдосконалення обраного алгоритму задля підвищення стійкості вбудовуваного цифрового водяного знаку у потоковий відеозапис;
- розробка алгоритму роботи програмного засобу на основі вдосконаленого методу;
- проектування та розробка інтерфейсу користувача та реалізація програмного засобу у вигляді онлайн сервісу;
- тестування розробки та аналіз отриманих результатів;
- економічне обґрунтування доцільності впровадження здійсненої розробки на основі вдосконаленого методу вбудовування ЦВЗ.

Об'єкт дослідження – цифровий водяний знак для захисту авторського права на відеофайли.

Предмет дослідження – процес підвищення стійкості вбудовуваного цифрового водяного знаку у потоковий відеозапис.

Наукова новизна: вдосконалення методу вбудовування ЦВЗ на основі алгоритму DEW.

Практична цінність: розроблено програмний продукт який реалізує вдосконалений метод вбудовування ЦВЗ у потокове відео з метою захисту авторського права.

Апробація: тези доповідей у даній галузі представленні на науково-технічних конференціях ВНТУ [5].

1 ЗАГАЛЬНИЙ АНАЛІЗ ГАЛУЗІ СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

На сьогодні проблема захисту інформації займає одне із провідних місць та є актуальною для сучасних досліджень. Тому розвиток інформаційних систем та технологій, глобальних комп'ютерних мереж та засобів мультимедіа стимулює розробку нових методів аналізу, зберігання, відтворення та передачі даних каналами інформаційних комунікацій. До них належать методи і засоби забезпечення високонадійної обробки даних в інформаційних структурах та системах, методи підвищення надійності та безпеки використання інформаційних технологій.

Зокрема, завдання захисту інтелектуальної власності на сьогодні не тільки не втрачає своєї актуальності, але стає ще більш затребуваною через безперервне зростання обсягів цифрової інформації та ширше використання Інтернету. Поширення впровадження цифрових водяних знаків (ЦВЗ) у цифрові контейнери для захисту прав власності призводить до необхідності розробки методів, більш стійких до активних атак та природних спотворень у каналі обробки та передачі [6].

В даному розділі здійснимо огляд теоретичного матеріалу та дослідження у галузі стенографічного захисту інформації, її актуальності, визначимо характеристики та структуру цифрових водяних знаків як засобу захисту інформації, здійснимо аналіз алгоритмів їх генерування та вбудовування, а також дослідимо атаки на системи ЦВЗ, що зумовлюють актуальність вдосконалення методів вбудовування ЦВЗ у інформаційні дані у вигляді відео.

1.1 Актуальність дослідження обраної галузі

Бурхливий розвиток інформаційних технологій, що спостерігається останніми роками, призвів до того, що сьогодні величезна кількість інформації, що становить інтелектуальну власність, зберігається та обробляється в комп'ютерних мережах та/або поширюється у цифровій формі.

Зокрема, розвиток засобів обчислювальної техніки дало поштовх у розвиток комп'ютерної стеганографії. Мова, відео, аудіозаписи та зображення – це цифрові дані, які мають аналогову природу. Саме в них на сьогоднішній день вбудовують повідомлення, що приховуються. Іноді інформація зашифровується в текстових файлах та виконуваних файлах програм [7].

Найбільш поширеними порушеннями прав інтелектуальної власності сьогодні є піратство, плагіат, підробка інформації, зміна інформації, недобросовісна конкуренція (промисловий шпигунство тощо) [7].

При цьому найбільша увага приділяється захисту прав інтелектуальної власності мультимедійної інформації, що розповсюджується на цифрових носіях та мережі Інтернет.

Серед завдань, розв'язуваних у межах систем захисту, особливе місце посідає завдання спеціального кодування інформації як даних, призначених для прихованої передачі [8].

Побудова стеганографічних методів привертає увагу багатьох фахівців, зайнятих розробкою нових технологій (наприклад, технологій аналізу та фільтрації інформації, що передається в мережі), спрямованих на забезпечення високої надійності інформаційних систем. Загалом завдання стеганографії та протилежне їй завдання стегааналізу є одними з базових проблем у теорії надійності та безпеки інформаційних технологій. На відміну від криптографії, що обмежує доступ до інформації, що міститься в повідомленні та передається, за допомогою деякого секретного ключа, завдання стеганографії полягає в тому, щоб приховати сам факт передачі будь-якого повідомлення від третіх осіб. Зазвичай, таке завдання вирішується шляхом впровадження секретного повідомлення, що передається, у нешкідливий на вигляд об'єкт даних, так званий контейнер. Сам контейнер підбирається таким чином, щоб факти існування або передачі не викликали ніякої підозри [9].

Основними характеристиками методів стеганографії слід вважати обсяг впроваджуваного повідомлення та стійкість до аналізу (виявлення факту наявності впровадження) [9].

У цифровій стеганографії [10] в якості контейнера використовується цифровий об'єкт – комп'ютерний файл. Сучасні методи вбудовування дозволяють впроваджувати приховану інформацію до файлів аудіо, відео, тексту, виконуваних програм тощо. В даний час існує велика кількість програмних пакетів стеганографії як комерційних, так і безкоштовних, з графічним інтерфейсом і у вигляді консольних додатків.

Основні сфери використання технології цифрового водяного знаку можна об'єднати в чотири групи: захист від копіювання (використання), прихована анотація документів, доказ автентичності інформації та прихований зв'язок (рис.1.1).

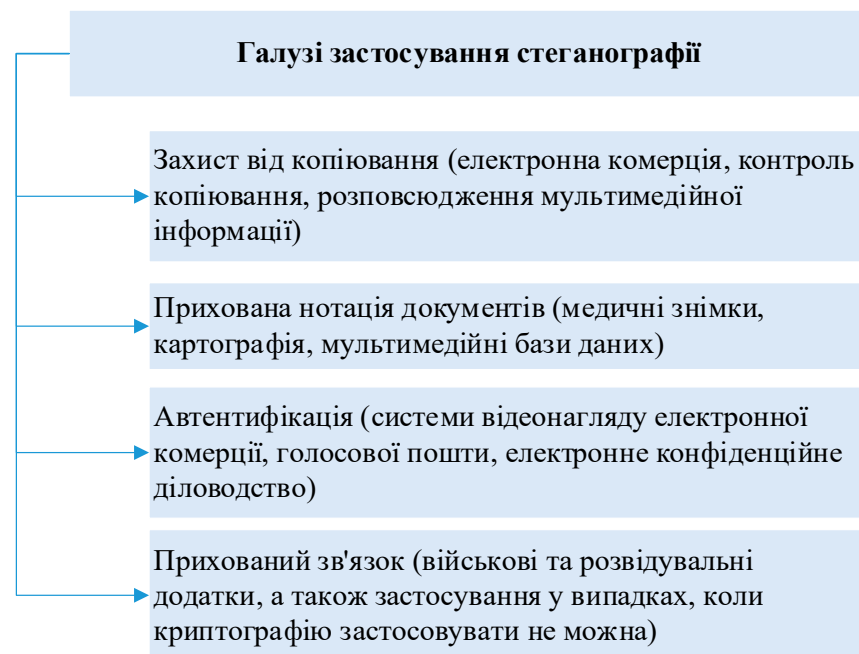


Рисунок 1.1 – Сфери застосування ЦВЗ [10]

Цифрова стеганографія набула широкого застосування у сфері захисту авторських прав. В об'єкт авторського права може бути впроваджена спеціальна мітка – відбиток пальця (fingerprint), що ідентифікує законного отримувача. Наприклад, у кожену копію програми, що продається, може бути впроваджена мітка, що ідентифікує ліцензійного покупця. У разі виявлення піратської копії програми за допомогою вбудованої мітки легко може бути відстежений користувач, який порушив ліцензійну угоду.

Ще однією вбудовуваною міткою може бути цифровий водяний знак (ЦВЗ,

watermark) [11], що ідентифікує автора. Припустимо, у фотографію впроваджується спеціальна мітка, яка містить паспортні дані автора. Потім виявляється стороння особа, яка видає цю фотографію як свою власну. Під час судового розгляду за допомогою видобутого водяного знаку може бути встановлений справжній автор фотографії.

Отже, популярність досліджень у цій галузі має причини. З них виділяються дві основні: у деяких країнах запроваджено обмеження на використання криптографічних засобів захисту інформації, а також необхідність враховувати права власності на оцифровану інформацію. Це в свою чергу стало причиною безлічі досліджень в області стеганографії, що стосується приховання самого факту наявності повідомлення і досліджень в області цифрових водяних знаків.

Таким чином, враховуючи суттєві переваги та особливості застосування стеганографічного методу захисту інформації, подальше його дослідження в роботі потребує більш детального розгляду та є актуальним.

1.2 Аналіз особливостей цифрового водяного знаку

В даному підрозділі детальніше розглянемо особливості цифрових водяних знаків, зокрема їх основні характеристики та структуру.

Цифровий водяний знак (ЦВЗ) – спеціальна мітка, що непомітно впроваджується у зображення або інший сигнал з метою тим чи іншим чином контролювати його використання [12].

Цифрові водяні знаки застосовуються як засіб захисту від несанкціонованого копіювання та використання. У зв'язку з бурхливим розвитком мультимедіа-технологій постало питання захисту авторських прав та інтелектуальної власності, представлені в цифровому вигляді. Прикладами такої власності є різного роду зображення (у тому числі і фотографії), аудіозаписи та відеозаписи тощо. і на сучасному рівні технологій не можна уникнути). Тому на додаток до існуючих заходів захисту інформації організаційного та технічного характеру постійно розробляються нові, покликані

захистити інтереси правовласників. Цифровий водяний знак – один із найефективніших технічних засобів захисту мультимедійної інформації. Він полягає в тому, що в об'єкт, що захищається, впроваджується інша інформація, яка грає роль невидимих міток. Ці невидимі мітки і є цифровими водяними знаками.

ЦВЗ може бути видимим і (зазвичай) невидимим. Рішення про коректність невидимих цифрових водяних знаків виносить спеціальний декодер, який проводить їх аналіз. Водяний знак може містити будь-яку інформацію, що дозволяє визначити власника об'єкта, що захищається. За допомогою водяних знаків можна захищати різну інформацію, але найбільше для цього підходять нерухомі зображення, аудіофайли та відеофайли [12].

ЦВЗ, що використовуються для захисту авторських прав, повинні задовольняти наступним вимогам (рис. 1.2) [12]:

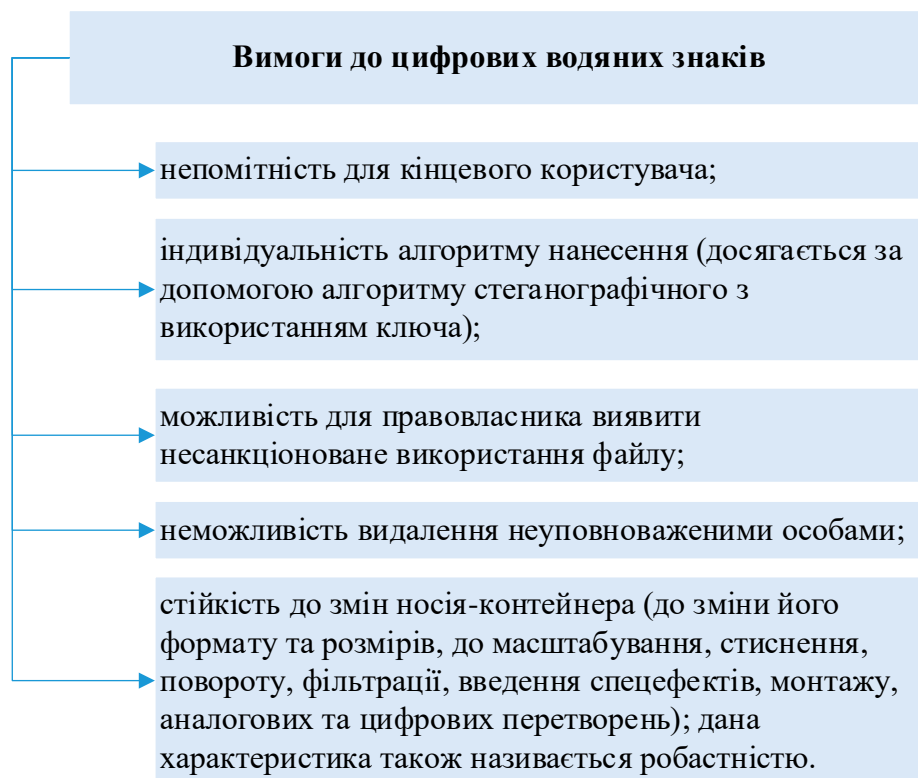


Рисунок 1.2 – Вимоги до ЦВЗ, що призначені для захист авторського права

Залежно від цілей застосування ЦВЗ робастність може змінюватись. Це дозволяє виділити три різновиди цифрових водяних знаків [12]:

– робасні (стійкі);

- крихкі;
- напівкрихкі.

Робастні водяні знаки є стійкими до будь-яких впливів і використовуються для захисту авторських прав – такі цифрові водяні знаки не можна спотворити чи видалити, і вони завжди вказують на правовласника.

Крихкі знаки руйнуються від незначних модифікацій контейнера. Вони поряд з електронним цифровим підписом служать для перевірки цілісності електронних документів. Алгоритми вбудовування крихких ЦВЗ відрізняються від інших особливою чутливістю до будь-яких спотворень та ефективні при вирішенні задачі контролю цілісності та захисту від фальсифікації.

Напівкрихкі водяні знаки можуть бути стійкі до одних видів впливу та нестійкі по відношенню до інших. Наприклад, такі ЦВЗ стійкі до стиснення, але вирізати фрагмент зображення-контейнера або усунути голос виконавця в аудіотреку-контейнері вже не можна.

Завдання вбудовування та виділення повідомлень з іншої інформації виконує стегосистема, структура стегосистеми наведена на рис. 1.3.

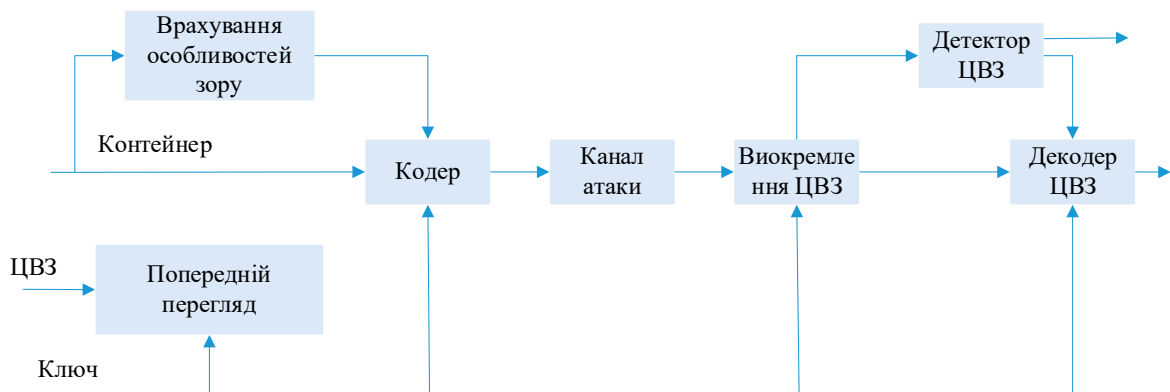


Рисунок 1.3 – Структура типової стегосистеми [13]

Стегосистема складається з наступних основних елементів [13]:

– прекодер (попередній кодер) – пристрій, який призначений для перетворення повідомлення, що приховується, до вигляду, який зручний для подальшого вбудовування цього повідомлення в сигнал-контейнер (інформаційну послідовність, в якій ховається повідомлення);

– стегакодер – пристрій, який призначений для впровадження прихованого повідомлення в інші дані з урахуванням їхньої моделі; розпізнавання (виділення) впровадженого повідомлення;

– стегадетектор – пристрій, який слугує для визначення наявності стегаповідомлення;

– декодер – пристрій, який займається відновленням повідомлення, що приховується (цей елемент може і відсутній).

У стегосистемі відбувається об'єднання двох типів інформації, щоб вони могли бути помітні двома принципово різними детекторами. Як один з детекторів виступає система виділення ЦВЗ, як інший – людина [13].

Спочатку водяний знак перетворюється на потрібний вид. Якщо в якості контейнера виступає зображення, то і послідовність ЦВЗ часто представляється як двовимірний масив біт. Для підвищення стійкості цифрового водяного знака часто виконують його стійкість до перешкод, або використовують широкосмугові сигнали.

Початкову обробку прихованого повідомлення виконує так званий прекодер (попередній кодер). Попередня обробка ЦВЗ та контейнера, в який буде розміщуватись інформація, полягає у обчисленні їх узагальненого перетворення Фур'є. Це дозволить впровадити ЦВЗ в спектральну область і суттєво підвищити стійкість водяного знака до різноманітних спотворень [13].

Попередня обробка нерідко здійснюється з використанням ключа K підвищення секретності вбудовування. Потім водяний знак вбудовується в контейнер, наприклад, шляхом модифікації значущих біт коефіцієнтів. Це можливо через особливості системи сприйняття людини.

Будь-які зображення мають значну психовізуальну надмірність. Людський зір нагадує низькочастотний фільтр – упускає безліч деталей. У високочастотних областях зображення спотворення можуть бути непомітні. Ця риса людського зору враховується, наприклад, при створенні алгоритмів для стиснення відео та зображень [13].

Стеготектор перевіряє захищене зображення, яке могло бути скомпрометовано, і виявляє вбудований водяний знак.

Стегодетектори прийнято ділити на два види: ті, що призначені для виявлення водяного знака в контейнері та ті, які призначені для виділення цього водяного знака (останні також відомі як стегакодері). Детектори першого виду у свою чергу діляться на дві категорії: з жорсткими рішеннями (тільки так чи ні) і з м'якими рішеннями [14].

Щоб зрозуміти, чи був застосований водяний знак, застосовують такі способи: обчислення відстані по Хеммінгу, розрахунок взаємної кореляцією між сигналом i (якщо ϵ) оригіналом [14]. У разі відсутності вихідного сигналу використовуються статистичні методи, що ґрунтуються на побудові моделей досліджуваного класу сигналів.

Існує два основних типи контейнерів [14]:

- потоковий;
- фіксований.

Потоковий контейнер є безперервно наступною послідовністю біт. Прихована інформація впроваджується в нього в реальному часі, і кодеру заздалегідь невідомо, чи буде достатнім розмір контейнера для передачі всієї інформації. У контейнер із великим розміром може бути впроваджено кілька повідомлень. Інтервали між бітами, що впроваджуються, встановлюються генератором псевдовипадкової послідовності з рівномірним розподілом інтервалів між відліками.

Складність полягає у необхідності вирішення трьох завдань [14]:

- синхронізації;
- визначенні початку послідовності;
- визначенні кінця послідовності.

Приховане повідомлення може йти відразу після бітів синхронізації, заголовків пакетів і так далі (якщо, звичайно, вони присутні в даних контейнера). Оскільки синхронізацію важко забезпечити, це призводить до покращення у плані таємності передачі.

Характеристики та розміри фіксованого контейнера відомі заздалегідь. Завдяки цьому можна впровадити інформацію, що приховується, найбільш оптимальним чином.

Враховуючи усі наведені особливості та обрану тему роботи, далі буде здійснено дослідження у сфері застосування цифрового водяного знаку у потоковому контейнері.

1.3 Аналіз алгоритмів генерування та вбудовування ЦВЗ

Оскільки в даній роботі увага надається вдосконаленню алгоритму для вбудовування ЦВЗ, в підрозділі розглянемо методи вбудовування цифрового водяного знаку у потоковий контейнер (рис.1.4). Найбільш популярними стандартами кодування відео є MPEG-2 [15] та MPEG-4 [15].



Рисунок 1.4 – Класифікація методів вбудовування ЦВЗ у відео [16]

Стеганографічні методи, що застосовуються для вбудовування інформації у відео, стиснуте за стандартом MPEG-2 (далі MPEG), повинні працювати в реальному часі. Способи вбудовування ЦВЗ, що працюють у реальному часі, повинні відповідати кільком вимогам і, в першу чергу, вони повинні бути сліпими і мати малу обчислювальну складність.

Таким чином, допустимими до використання є методи, що вбудовують

дані безпосередньо в потік стислих даних, щоб уникнути зайвих обчислень (рис. 1.5).

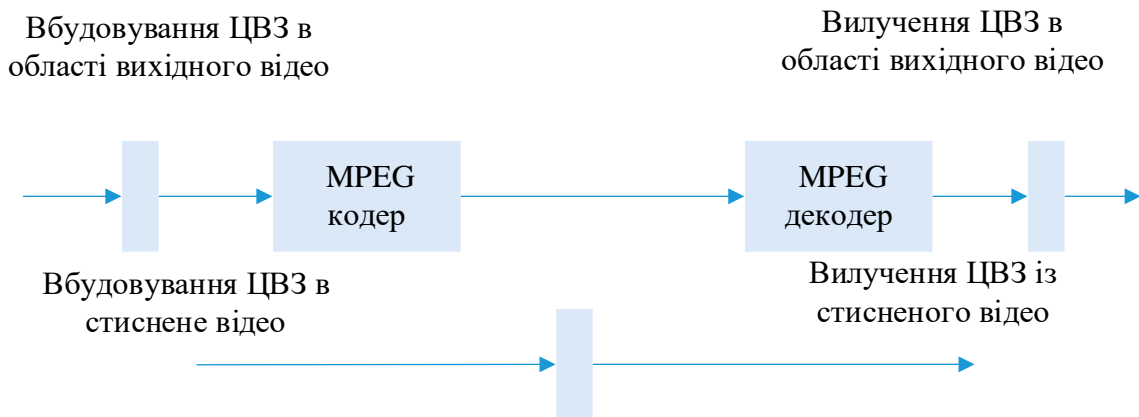


Рисунок 1.5 – Вбудовування/вилучення ЦВЗ у розгорнуті дані та здійснення цієї операції зі стислими даними [17]

Крім того, операція із впровадження ЦВЗ не повинна збільшувати розмір стислих відео даних. Якщо розмір даних збільшується, то можуть виникнути проблеми при передачі потоку відео даних каналом фіксованої швидкості.

Переходячи до аналізу методів вбудовування ЦВЗ, розглянемо більш детально стандарт стиснення даних MPEG [18].

Ключова суть стиснення MPEG полягає в тому, що з усього потоку даних повністю передаються тільки деякі кадри, а для решти передається їх відмінність від інших кадрів.

Потік відео в MPEG має ієрархічну синтаксичну структуру. Кожен рівень містить один або більше підлеглих рівнів [18].

В свою чергу, послідовність відеоданих поділяється на безліч груп кадрів, які представлені великою кількістю відеокадрів, що безпосередньо приходять один за одним у порядку показу. Далі, кадри поділяються на шари та макроблоки. Нижчий рівень, блоковий, складається з блоків яскравості та кольоровості макроблоку.

Алгоритм стиснення MPEG ґрунтується на гібридній схемі кодування. Ця схема поєднує міжкадрове та внутрішньокадрове кодування послідовності відеоданих.

У межах групи кадрів тимчасова надмірність серед відеокадрів зменшується за рахунок застосування руху з тимчасовим прогнозуванням. Це означає, що одні кадри передбачаються за іншими. Потім результуюча помилка передбачення кодується. У стандарті MPEG використовуються три типи кадрів (рис. 1.6).

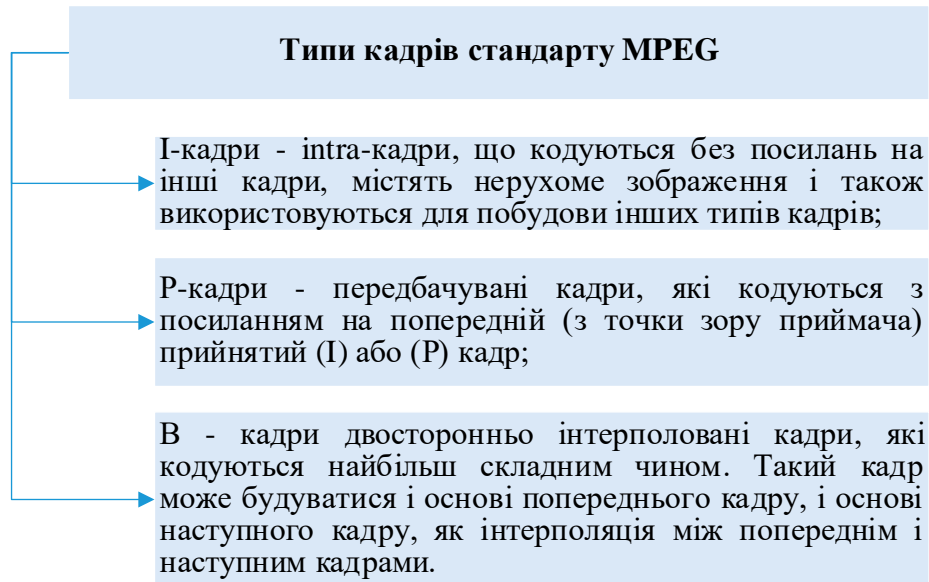


Рисунок 1.6 – Типи кадрів стандарту MPEG [19]

Закодована група кадрів завжди починається з I-кадра для забезпечення доступу до потоку відео з будь-якої випадкової точки. Група кадрів складається із 12 кадрів. Звідси слідує, що при частоті 25 кадрів в секунду, I-кадр приходить не рідше, аніж один раз за 0,48 секунди. А також разом з ним здійснюється відновлення в тій чи іншій мірі ідентичності зображення. P-кадри (B-кадри кодуються аналогічним чином) також розбиваються на блоки 8*8 пікселів та порівнюються з деяким опорним кадром. Потім можливі 3 випадки (рис. 1.7).

ДКП концентрує енергію в області низьких частот, а, так як людське око менш чутливе до високочастотних коливань, то компоненти ВЧ можуть бути оцифровані більш грубо. Коефіцієнт ДКП з індексом (0,0) називається DC-коефіцієнтом (постійного струму), і він становить середнє значення блоку пікселів. Інші коефіцієнти ДКП називаються AC-коефіцієнтами (змінного струму) [20].

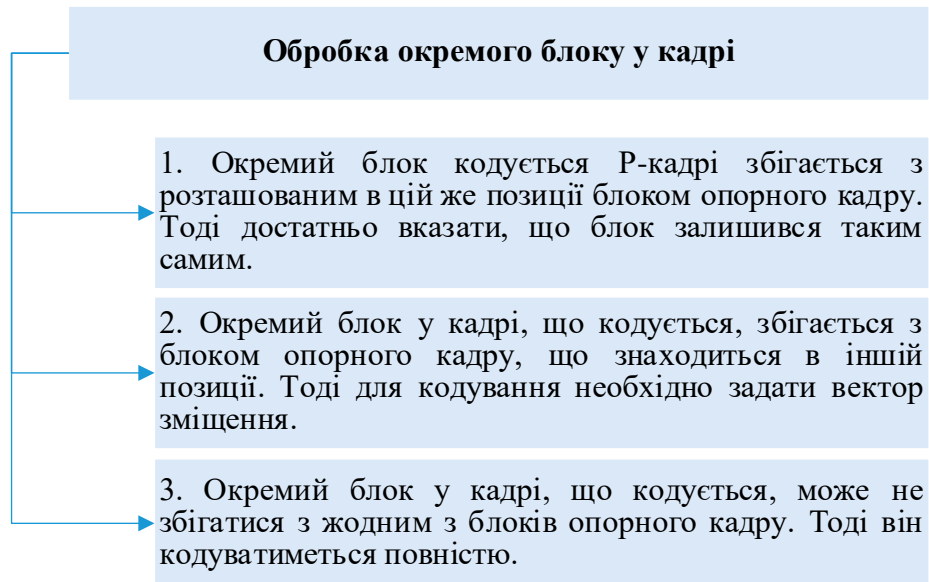


Рисунок 1.7 – Обробка блоків у кадрі [19]

Найбільш обчислювально простим буде алгоритм впровадження даних на блоковому рівні. Також невисоку складність має алгоритм вбудовування ЦВЗ лише на рівні коефіцієнтів, що вимагає лише здійснення кодування Хаффмана, кодування довжин серій і квантування [21].

Алгоритм вбудовування ЦВЗ, що працює в бітовій області, вимагає здійснення додаткового кодування Хаффмана. З цього випливає, що вся процедура вбудовування може складатися з декодування Хаффмана, спеціальної модифікації та кодування Хаффмана.

Отже, далі розглянемо та порівняємо алгоритми, що можливі до застосування у стандарті MPEG.

Алгоритм Wu відноситься до алгоритмів, що вбудовують інформацію на рівні коефіцієнтів дискретного косинусного перетворення (ДКП) і використовується в даних, стислих за стандартами MPEG з високою роздільною здатністю. При впровадженні здійснюється додавання псевдовипадкового масиву коефіцієнтів ДКП з індексом (0;0). Цей алгоритм відносно простий у реалізації, але при вбудовуванні можливе погіршення якості відео. Алгоритм Wu є застарілим, хоча може використовуватися і у відео високої якості за рахунок збільшення потоку відео [22].

Подальшим удосконаленням цього алгоритму є стегосистема Hartung [23], яка залучає більшу кількість коефіцієнтів ДКП, є робастною до фільтрування, зашумлення та дискретизації, виправляє проблему з видимістю ЦВЗ та її можливо використовувати для всіх видів кадрів. Але при цьому вона має високу обчислювальну складність. Hartung використовується в даних, стислих за стандартом MPEG-2 .

Алгоритм Langelaar-1 [24] вбудовує інформацію лише на рівні бітової площини, замінюючи незначні біти. До його переваг відносяться висока пропускна здатність і низька обчислювальна складність, але при цьому можливі незначні спотворення. Цей алгоритм, як і Hartung, використовується в даних, стислих за стандартом MPEG-2.

Алгоритм Langelaar-2 використовує вбудовування інформації на рівні енергетичної різниці коефіцієнтів ДКП, внаслідок чого його обчислювальна складність як мінімум удвічі менша, ніж у інших алгоритмів цієї групи, він вносить менше спотворень, ніж попередні алгоритми і є робастним для видалення ЦВЗ. До його недоліків можна віднести те, що зі збільшенням різниці енергій можлива поява видимих спотворень. Цей алгоритм застосовується у відео, кодованих на високих швидкостях [25].

Таким чином, можна зробити висновок, що подальше дослідження методу вбудовування цифрового водяного знаку на основі диференціального вбудовування енергії має сенс та буде обрано для вдосконалення в роботі.

1.4 Аналіз атак на стегосистеми із ЦВЗ

Маркування ЦВЗ є важливим заходом забезпечення безпеки захисту авторського права. Обсяги інформації, що створюється і захищається постійно зростають, водночас розвиваються і методи атак з боку зловмисників. Тому дослідження у цій галузі будуть актуальні ще тривалий час.

Кількісні методи оцінки стенографічного методу можна поділити на суб'єктивні та об'єктивні.

Суб'єктивні метрики ґрунтуються на перцептивній оцінці людиною-

спостерігачем, у той час як об'єктивні метрики ґрунтуються на обчислювальних моделях, які намагаються оцінити якість зображення. Суб'єктивні метрики часто є більш точними з точки зору сприйняття, проте не всі зручні: деякі з них трудомісткі або дороги для обчислення. Також результати оцінок суб'єктивним та об'єктивним способами часто можуть не збігатися. З цієї причини для аналізу результатів переважно використовувати метрики з обох категорій.

Далі розглянемо види атак на цифрові водяні знаки. Успішна атака повинна пошкодити або знищити цифровий водяний знак за умови збереження якості зображення. Для знищення слідів присутності цифрових водяних знаків можуть бути використані певні види атак окремо, так і їх сукупність.

Виділяються такі категорії специфічних атак проти систем ЦВЗ (рис. 1.8).

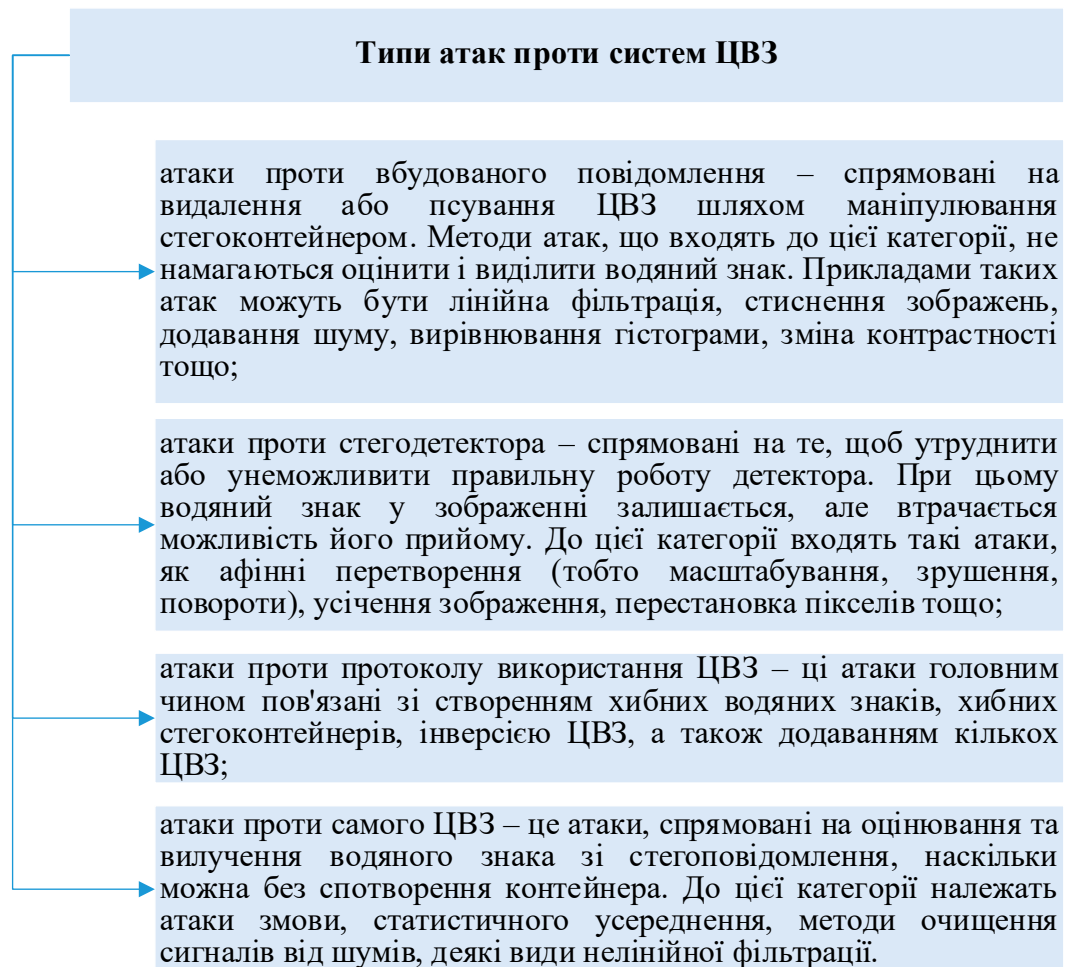


Рисунок 1.8 – Типи специфічних атак проти систем ЦВЗ [26 – 27]

Дотримуючись цієї класифікації, всі атаки на системи впровадження водяних знаків можна розділити на чотири групи:

- атаки, спрямовані на видалення ЦВЗ;
- геометричні атаки, спрямовані на спотворення контейнера;
- криптографічні атаки;
- атаки проти протоколу вбудовування та перевірки ЦВЗ, що використовується.

Проте, якщо проаналізувати існуючі методи захисту від атак на системи цифрових водяних знаків, то слід зазначити, що у найпростіших стегосистемах цифрових водяних знаків при впровадженні застосовується псевдовипадкова послідовність, яка є реалізацією білого гаусівського шуму [28]. Вона не враховує властивості контейнерів.

Подібні системи нестійкі до багатьох атак, що були розглянуті попередньо. Щоб підвищити робастність системи, необхідно застосувати низку покращень.

У стійкій стегосистемі потрібно правильно підібрати параметри псевдовипадкової послідовності.

До таких атак, як стиснення, додавання шуму та деяким іншим досить стійкими можуть бути системи з розширенням спектра.

Причиною нестійкості систем ЦВЗ з розширенням спектра до атак «змови» пояснюється тим, що послідовність, що використовується для вкладення, зазвичай має нульове середнє. Після усереднення за досить велику кількість реалізацій ЦВЗ видаляється.

Відомий спеціальний метод побудови водяного знака, спрямований проти такої атаки. При цьому коди розробляються таким чином, щоб за будь-якого усереднення завжди залишалася не рівна нулю частина послідовності (статична компонента). Проте, у ній можливе відновлення решти послідовності (динамічна компонента) [29].

Недоліком запропонованих кодів є те, що їхня довжина збільшується експоненційно зі зростанням числа захищених копій, що розповсюджуються. Можливим виходом із цього положення є застосування ієрархічного кодування, тобто призначення кодів для групи користувачів.

Таким чином, підвищення стійкості вбудовуваного цифрового водяного знаку у потоковий відеозапис на основі вдосконаленого методу є актуальним завданням для роботи та буде здійснено та описано надалі із урахуванням проаналізованого теоретичного матеріалу.

1.5 Висновки та постановка задач

Отже, в даному розділі було проведено теоретичний огляд галузі, в якій проводиться розробка. У розділі проаналізовано основні поняття стеганографічних систем та ЦВЗ як засіб захисту авторського права, здійснено аналіз застосування ЦВЗ для захисту файлів відео-формату на онлайн сервісі.

В результаті проведеного аналізу теоретичного матеріалу та виходячи з мети і актуальності теми, були поставлені наступні задачі подальшої роботи:

- здійснити вдосконалення обраного алгоритму задля підвищення стійкості вбудовуваного цифрового водяного знаку у потоковий відеозапис та розробити алгоритм роботи програмного засобу;
- спроектувати та розробити інтерфейс користувача додатку та програмний засіб для реалізації розробки онлайн сервісу захисту авторського права відео;
- здійснити тестування програмної розробки та вдосконаленого методу;
- економічно обґрунтувати розроблювальний вдосконалений метод вбудовування ЦВЗ.

В результаті виконання поставлених завдань, планується досягти основної мети роботи, а саме підвищити стійкість вбудовуваного цифрового водяного знаку у потоковий відеозапис на основі вдосконаленого методу DEW.

2 ПІДВИЩЕННЯ СТІЙКОСТІ ВБУДОВУВАНОВОГО ЦИФРОВОГО ВОДЯНОГО ЗНАКУ У ПОТОКОВИЙ ВІДЕОЗАПИС

В даному розділі здійснимо вдосконалення стенографічного методу на основі алгоритму диференціального вбудовування енергії та застосуємо його для розробки відповідного програмного засобу.

В ході виконання роботи опишемо алгоритм DEW [30] та проаналізуємо його переваги та недоліки. На основі отриманих результатів буде здійснено вдосконалення обраного методу за рахунок внесення змін до його математичного апарату, а також додаткового застосування методу Канні [31], що використовує багаторівневий обчислювальний підхід виявлення меж сегментів на зображенні.

Внесені зміни дозволять усунути виявлені недоліки, здійснити програмну розробку засобу для вбудовування цифрового водяного знаку у потоковий відеозапис та в подальшому здійснити тестування отриманих результатів роботи вдосконаленого алгоритму.

2.1 Розробка алгоритму роботи методу для вбудовування ЦВЗ

Опишемо алгоритм вбудовування цифрового водяного знаку, що базується на ідеї диференціального енергетичного водяного знаку та є методом вбудовування ЦВЗ, котрий заснований на вибіркового відкиданні частини високочастотних коефіцієнтів ДКП стислих зображень і відеозображень.

В основі даного методу лежить диференціальне вбудовування енергії (DEW – Differential Energy Watermarking), під енергією розуміється значення коефіцієнтів ДКП аналізованої області зображення.

За методом DEW здійснюється впровадження ЦВЗ, яке складається з біт $b_j (j = 0, 1, 2, \dots, l - 1)$. Кожен біт ЦВЗ вбудовується в обрану область, що складається з блоків n по 8×8 коефіцієнтів ДКП каналу яскравості зображення кожен. Розмір обраної області визначає швидкість вбудовування – що вище n , то нижча швидкість.

Кожен біт ЦВЗ впроваджується в обрану область модифікацією різниці

енергій між високочастотними коефіцієнтами ДКП верхньої частини цієї області (субобласть А) та її нижньої частини (субобласть В). Підмножина високочастотних коефіцієнтів позначається $S(c)$.

Енергія субобласті А обчислюється [32]:

$$E_A(c, n, Q) = \sum_{d=0}^{\frac{n}{2}-1} \sum_{i \in S(c)} ([\theta_{i,d}]_Q)^2,$$

де i, d – коефіцієнт ДКП з індексом i з d – го блоку коефіцієнтів ДКП субобласті А;

$[]_Q$ – означає, що енергія обчислюється у квантованих коефіцієнтів.

Енергія субобласті обчислюється аналогічно:

$$E_B(c, n, Q) = \sum_{d=0}^{\frac{n}{2}-1} \sum_{i \in S(c)} ([\theta_{i,d}]_Q)^2,$$

Підмножина $S(c)$ визначається на основі обраного порога:

$$S(c) = \{h \in \{1,63\} | (h \geq c)\}.$$

Вибором відповідного значення порога визначається стійкість ЦВЗ до видалення та її помітність на зображенні. Коли ж поріг кожної lc – області визначений, різниця енергій визначається як:

$$D(c, v, Q) = E_A(c, v, Q) - E_B(c, v, Q).$$

Значення біта, що впроваджується, визначає знак енергетичної різниці. Якщо значення біта «0», то $D > 0$, інакше $D < 0$.

Отже, процедура вбудовування інформації модифікує енергії E_A чи E_B , щоб вбудувати інформацію різниця енергій D .

Центральну роль, як у процесі вбудовування, і у процесі вилучення вбудованої інформації грають енергії субобластей А і В, величина яких визначається чотирма чинниками:

- характером субобластей А та В;
- кількістю блоків n на одну обрану область;
- кроком квантувача;
- розміром підмножини $S(c)$.

Алгоритм описаного методу наведемо на рис. 2.1.

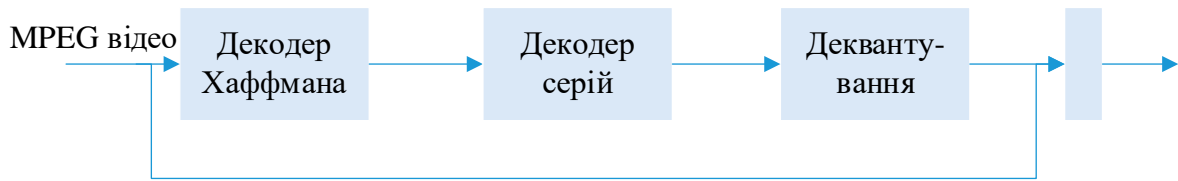


Рисунок 2.1 – Алгоритм вбудовування ЦВЗ на основі DEW [32]

Якщо обрана область однорідна, її енергія утримуватися в коефіцієнті ДКП. Енергія високочастотних коефіцієнтів дорівнює нулю.

У разі наявності контурів або текстур значення високочастотних коефіцієнтів будуть більшими. Чим більше блоків n береться на одну вибрану область, тим більше значення енергії, що міститься в ній. Крок квантувача визначає стійкість ЦВЗ до атаки перекодуванням. Розмір підмножини $S(c)$ визначається порогом c (рис. 2.2).

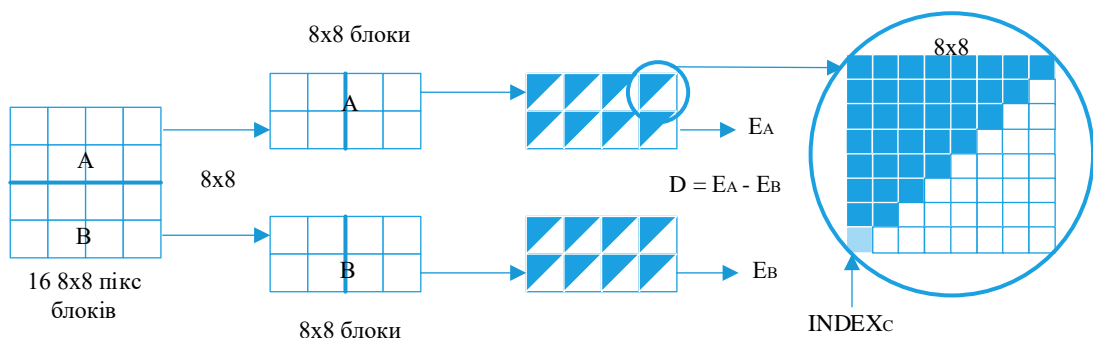


Рисунок 2.2 – Візуалізація вбудовування алгоритму DEW [32]

Для збільшення різниці енергій необхідно, щоб у процесі вбудовування інформації брало участь якнайбільше коефіцієнтів ДКП. Але надмірне збільшення розміру підмножини $S(c)$ призведе до помітних візуальних спотворень. Це означає, що для кожної обраної області необхідно знайти таке мінімальне за розмірами підмножина, для якої можна досягти необхідної різниці енергій.

Таким чином, описавши та проаналізувавши математичний апарат вбудовування цифрового водяного знаку на основі методу диференційного

обраховування енергії, основними його недоліками можна вважати:

– вразливість високочастотних коефіцієнтів контейнера до певних видів атак (оскільки, застосовувані у алгоритмі DEW високочастотні коефіцієнти ДКП легко відкидаються фільтрами)\$

– можливість суттєвих візуальних змін (оскільки, алгоритм DEW не враховує, який вплив на вихідне зображення має відкидання коефіцієнтів ДКП).

Разом з тим, алгоритм DEW має високу стійкість до видалення цифрового водяного знаку, а також захищений від значної кількості атак. Саме тому, доцільним у подальшій роботі є проведення удосконалення направлено на усунення виявлених недоліків, задля реалізації стійкого алгоритму вбудовування ЦВЗ на основі DEW.

В наступному підрозділі роботи розглянемо шляхи усунення вказаних недоліків та розробимо удосконалений метод вбудовування цифрового водяного знаку у потокове відео.

2.2 Вдосконалення алгоритму вбудовування ЦВЗ у відео

Проаналізувавши обраний базовий алгоритм DEW для вбудовування цифрового водяного знаку, здійснимо його удосконалення для усунення виокремлених недоліків.

Враховуючи, що однією із проблем стійкості алгоритму до атак є вразливість високочастотних коефіцієнтів контейнера, в модифікованому варіанті алгоритму в даній роботі врахуємо лише низькочастотні коефіцієнти дискретно-косинусного перетворення.

Для усунення недоліку суттєвої помітності візуальних змін контейнера застосуємо метод сегментації Канні, який використовує багаторівневий обчислювальний підхід виявлення меж сегментів на зображенні.

У більшості випадків, особливо при аналізі зашумлених зображень, цей метод має певні переваги перед іншими.

Регульованим параметром методу Канні є поріг чутливості: двоелементний вектор, у якому перший елемент нижній поріг, а другий елемент

верхній поріг.

Оскільки, низькочастотні коефіцієнти ДКП модифікувати небажано, так як це може погіршити візуальну якість зображення, поріг повинен бути не менше за певне значення c_{min} .

Для визначення відповідного c використаємо формулу:

$$c(n, Q, c_{min}) = \max \{c_{min}, \max \left\{ g \in \{1,63\} \mid \begin{array}{l} E_A(g, n, Q) > D \\ \cap (E_B(g, n, Q) > D) \end{array} \right\} \}$$

Для отримання вбудованого біта одержувачу знову необхідно знайти поріг c . Але тепер береться вже максимум за всіма порогами для субобластей А і В.

Робота методу перевіряється на моделях зображень із різними дефектами.

Результати зображення є бінарними, де одиницею відображається наявність кордонів, а нулем її відсутність.

Сегментація методом Кані проводиться наступним чином [33]:

Крок 1. Зображення згладжується фільтром Гауса [34] із заданим стандартним відхиленням для скорочення адитивного шуму.

Крок 2. У кожній точці обчислюється модуль вектора градієнта

$$g(x, y) = \sqrt{G_x^2 + G_y^2}$$

та напрямок вектору градієнта

$$\theta = \arctan \left(\frac{G_y}{G_x} \right)$$

Напрямок контуру в заданій точці перпендикулярно до напрямку вектора градієнта. При обчисленні G_x і G_y пропонується використовувати фільтри Собеля або Лапласа.

Таким чином, виділяються перепади інтенсивності зображення. Точки перепаду визначаються як точки локального максимуму градієнта.

Крок 3. Точки перепаду, визначені під час кроку 2, зумовлюють зростання гребенів на зображенні модуля градієнта. Після цього обчислюється вершини цих гребенів і надається нульове значення точкам, які лежать на гребені. В результаті на виході будується тонка лінія, а весь цей процес називається «немаксимальним придушенням».

Потім пікселі гребеня піддаються порогової обробки з використанням двох порогів T_1 і T_2 , причому $T_1 < T_2$. Значення порога знаходиться від 0 до 1 і регулює поріг яскравості між суміжними пікселями.

Крок 4. Об'єднання груп пікселів різних рівнів, розбитих з використанням порогів.

Таким чином, формується контур області, що виділяється шляхом приєднання пікселів одного рівня до пікселів іншого, за умови наявності хоча б одного сусіднього пікселя з восьми, що оточують заданий.

Інакше кажучи, до точок, значення інтенсивності у яких перевищує верхній поріг, приєднуються лише сусідні із ними точки, значення інтенсивності у яких перевищує нижній поріг.

Алгоритм можна представити наступним чином (рис. 2.3).

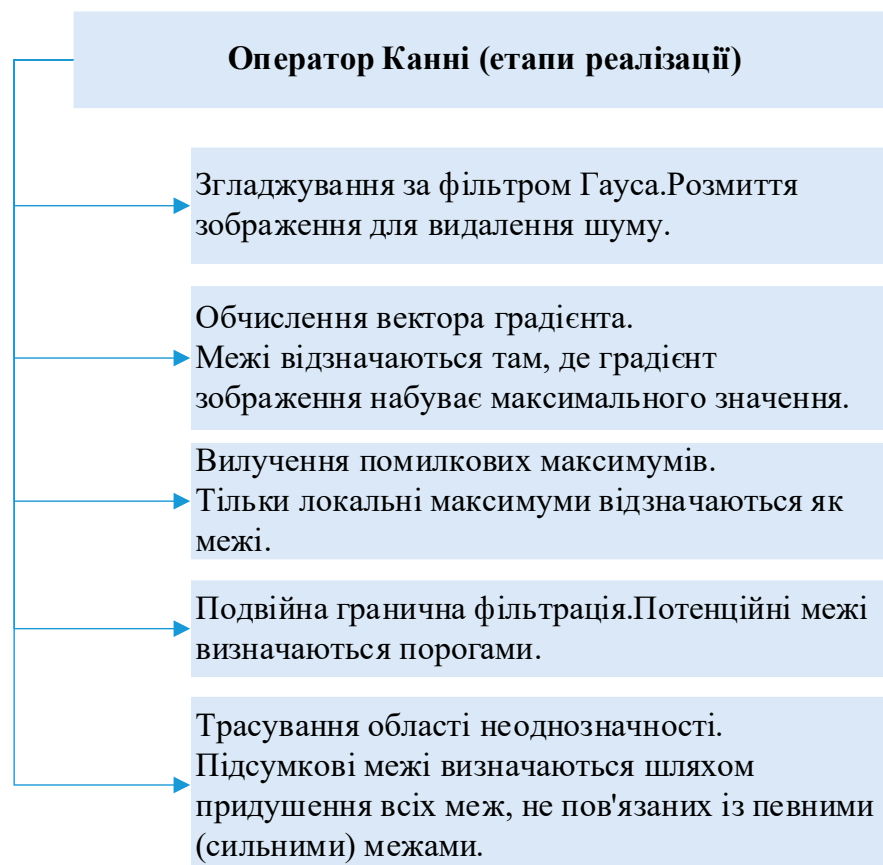


Рисунок 2.3 – Етапи реалізації алгоритму оператора Канні [35]

Перевагою методу Канні контурної сегментації зображень є використання морфологічної операції нарощування точок контуру в результаті вирішуються

такі завдання, як деталізація зображення та яскравість/колірність сегментації.

Отже, за рахунок реалізації описаного вдосконалення, водяний знак не надаватиме помітного впливу на зорове сприйняття, тим самим покращуючи прозорість сприйняття водяного знаку.

А враховування лише низькочастотних коефіцієнтів при вбудовуванні цифрового водяного знаку у контейнер підвищить стійкість алгоритму до фільтрації.

Таким чином, змінивши параметри в алгоритмі DEW (за рахунок зміни врахування коефіцієнтів ДКП та візуальної моделі Канні), відбувається відмова від вбудовування водяного знаку в область зі складними текстурями, щоб зменшити вплив на візуальну якість та підвищити стійкість алгоритму.

2.3 Розробка алгоритму роботи програмного додатку

Застосуємо вдосконалений алгоритм вбудовування цифрового водяного знаку у реалізації програмного засобу, що являє собою онлайн-сервіс для публікації відео.

Для практичної реалізації програмного засобу розробимо алгоритм його роботи.

Оскільки, роботою передбачено, що вдосконалений метод буде застосовуватись для вбудовування у потоковий відеозапис, мультимедійний файл, що слугуватиме стенографічним контейнером, будемо розглядати як послідовність кадрів (фреймів), де кожен з них обробляється як незалежне зображення і ЦВЗ вбудовується у кожний фрейм окремо.

В роботі досліджуватимуться формати відео .mp4 та .avi [36].

Роботою передбачається розробка онлайн-сервісу доступ до роботи з яким мають лише авторизовані користувачі. Авторизувавшись на сервісі, користувач має можливість переглядати та додавати відео захищені цифровим водяним знаком, ставити відповідні реакції на відео, залишати коментарі.

Схематично даний алгоритм представимо на рис. 2.4.

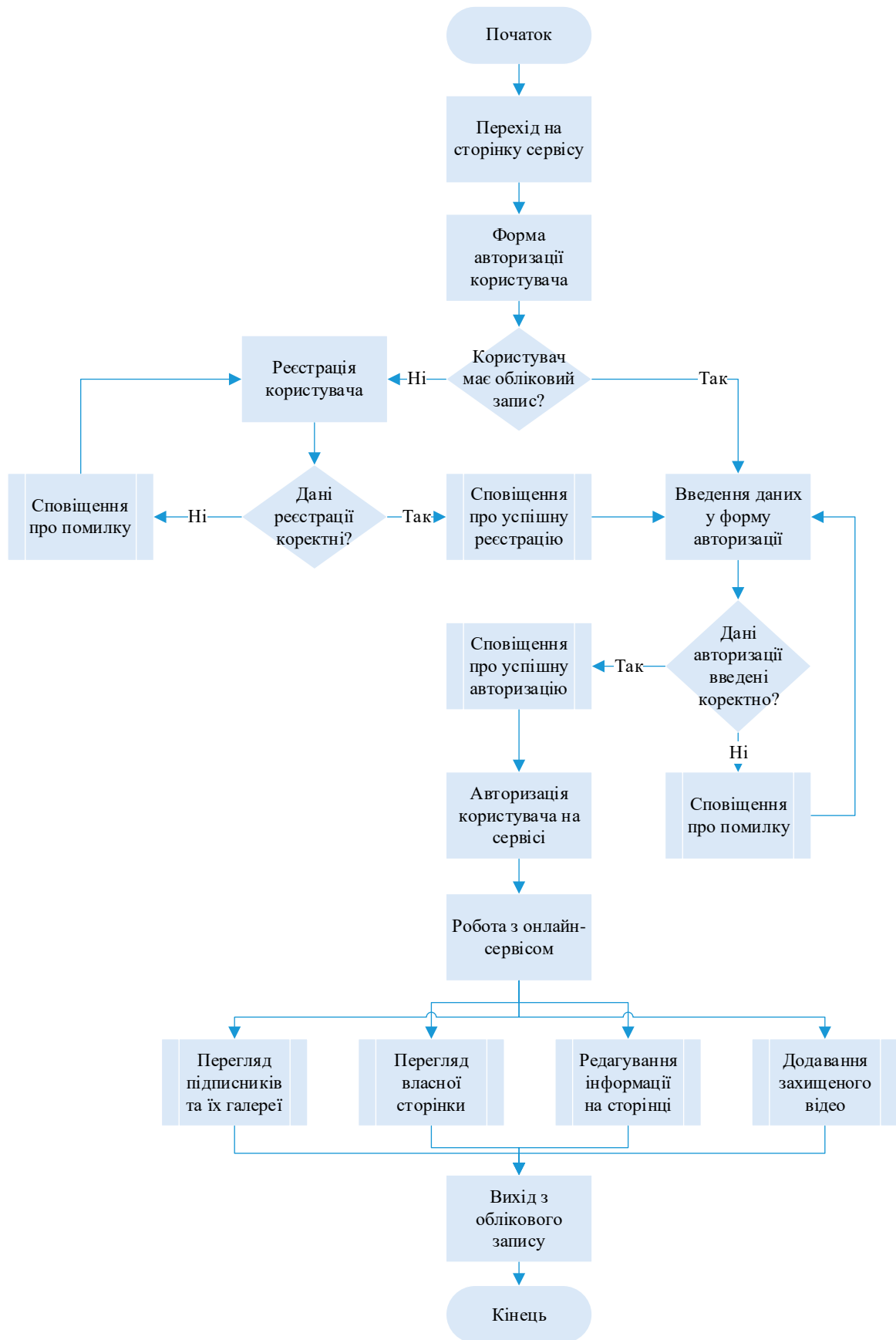


Рисунок 2.4 – Алгоритм роботи користувача з онлайн-сервісом

Далі опишемо покроково алгоритм роботи із розробленим сервісом.

Крок 1. Перехід за посиланням (адресою онлайн-сервісу).

Крок 2. Авторизація користувача.

2.1 Якщо користувач має обліковий запис на сервісі – перехід до кроку 4.

2.2 Якщо користувач відвідав сервіс вперше – необхідне здійснення реєстрації. Перехід до кроку 3.

Крок 3. Реєстрація користувача на сервісі. Перевірка введених даних реєстрації, підтвердження електронної адреси.

3.1 Якщо реєстрація успішна – перехід до кроку 4.

3.2 Якщо виявлені помилки при реєстрації – повторне здійснення кроку 3.

Крок 4. Заповнення форми авторизації користувача.

4.1 Якщо форма авторизації заповнена коректними даними – користувач отримує доступ до свого облікового запису на сервісі.

Крок 4.2 Якщо дані форми авторизації заповнені некоректно – виведення сповіщення про помилку, повторне виконання кроку 4.

Крок 5. Робота з онлайн-сервісом.

5.1 Перегляд підписників, їх відео, додавання реакцій та коментарів на переглянуті відео.

5.2 Перегляд власних відео, редагування назви, фільтрування коментарів, ознайомлення з даними про перегляди.

5.3 Редагування інформації про свій обліковий запис (ім'я, нік, пошта, аватар, відео галерея)

5.4 Додавання відео захищеного цифровим водяним знаком до відео галереї.

Крок 6. Завершення роботи з сервісом, вихід з облікового запису через відповідну функціональну кнопку.

Далі більш детально опишемо процес додавання відео із цифровим водяним знаком.

Схематично даний алгоритм представимо на рис. 2.5.

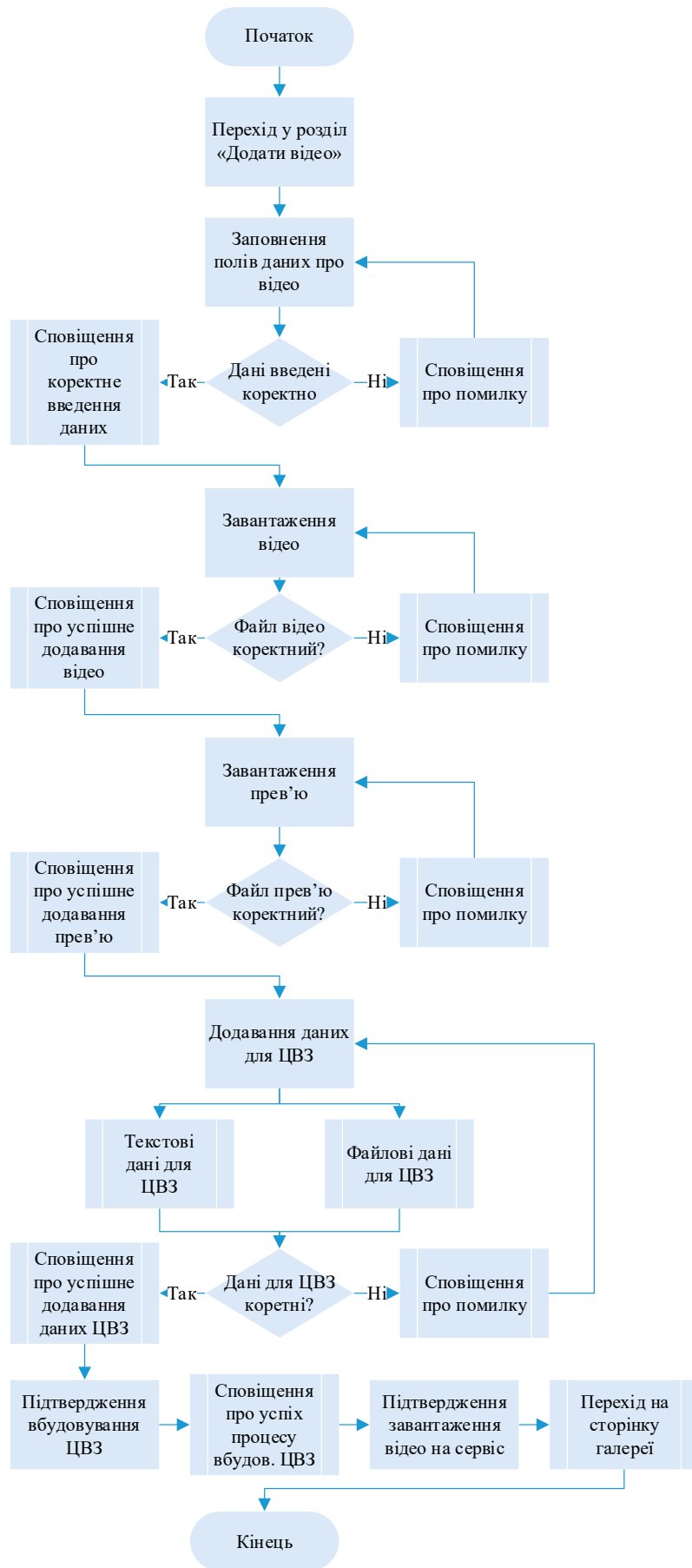


Рисунок 2.5 – Алгоритм додавання ЦВЗ у відео на онлайн-сервісі

Крок 1. Перехід у розділ «Додати відео».

Крок 2. Заповнення полів із даними про відео (назва, опис).

Крок 3. Перевірка коректності заповнених полів та вивід відповідного сповіщення.

Крок 4. Завантаження файлу відео (формат mp4, avi).

Крок 5. Перевірка відповідності вимогам завантаженого відео та вивід відповідного сповіщення.

Крок 6. Завантаження файлу прев'ю до відео (формат jpg, bmp).

Крок 7. Перевірка відповідності вимогам завантаженого зображення та вивід відповідного сповіщення.

Крок 8. Введення тексту для цифрового водяного знаку та / або додавання файлу для ЦВЗ.

Крок 9. Перевірка відповідності вимогам введених даних та вивід відповідного сповіщення.

Крок 10. Підтвердження вбудовування цифрового водяного знаку натисненням відповідної функціональної кнопки.

Крок 11. Сповіщення про результат вбудовування цифрового водяного знаку.

Крок 12. Підтвердження завантаження захищеного відео на сервіс натисненням відповідної функціональної кнопки.

Крок 13. Сповіщення про результат завантаження відео, автоматичний перехід на сторінку галереї користувача.

Таким чином, на основі розроблених алгоритмів роботи онлайн – сервісу, далі в роботі буде здійснено програмну реалізацію на основі вдосконаленого алгоритму вбудовування цифрового водяного знаку у потоковий відеозапис за рахунок використання методу диференціального вбудовування енергії, зміни враховуваних коефіцієнтів ДКП та застосування методу Канні.

Розробка даного засобу дозволить на практичному прикладі переконатись у доцільності здійсненого вдосконалення.

2.4 Обґрунтування вибору засобів програмування

Виходячи із поставлених задач роботи для практичної реалізації програмного додатку на основі вдосконаленого алгоритму диференціального вбудовування енергії (DEW) для підвищення стійкості вбудовуваного цифрового водяного знаку у потоковий відеозапис заплановано здійснити розробку за рахунок використання наступних програмних засобів:

- платформи ASP.NET Core 3.1 [37] та мови програмування C# [38] (backend);

- фреймворку Angular [39] та мови програмування Java Script [40] (frontend).

Розглянемо особливості наведених засобів програмування, що зумовили їх вибір для застосування у даній роботі.

Оскільки, роботою передбачено реалізацію саме веб-додатку, для його розробки доцільно застосувати платформу, що має достатній функціонал для вирішення даної задачі. Однією із таких платформ є ASP.NET – платформа, яка служить для створення веб-сайтів та веб-додатків. Дана платформа дозволяє здійснювати написання програмного продукту, зокрема на вивченій раніше автором мові C#, яка входить до комплекту .NET Framework [41]. На основі цієї технології можна створювати сайти різної складності та тематики.

ASP.NET набагато швидше, ніж звичайні скриптові мови. Він виконується швидше, тому що весь програмний код спочатку компілюється при першому запиті користувача і потім кешується в пам'яті.

Таким чином, усі подальші рази код просто виконується з пам'яті і не потребує повторного завантаження із сервера. Це скорочує час на парсинг, завантаження та оптимізацію файлів.

Також ASP.NET використовує схему MVC (Модель-Вид-Контролер) [42]. Кожна частина відповідає за певні дії. Наприклад, користувач щось робить на сайті та надсилає запит на сервер. Контролер інтерпретує дії користувача, сповіщаючи модель необхідність змін. У свою чергу модель надає дані та реагує

на команди контролера, змінюючи свій стан. І, нарешті, вигляд відповідає за відображення даних моделі користувачеві, реагуючи зміни моделі.

Схематично жаний процес наведено на рис. 2.6.

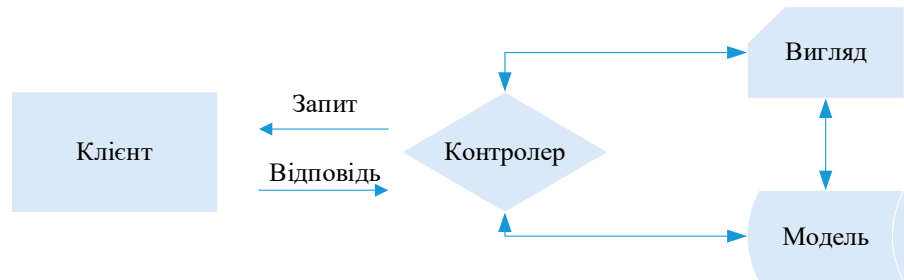


Рисунок 2.6 – Схема обробки запиту користувача на платформі ASP.NET [37]

Таким чином, посилаючи запит на сервер, контролер приймає цей запит, модель реагує на зміни та видає весь необхідний функціонал для відображення сторінки, а вигляд відповідає лише за зовнішній вигляд самої сторінки, тобто є просто HTML шаблоном сайту.

Для написання програмного коду на обраній платформі заплановано застосування вивчену раніше мову об'єктно-орієнтованого програмування C#. Дана мова програмування має ряд переваг, що зумовлюють її вибір для роботи. Дані переваги наведено на рис. 2.7.

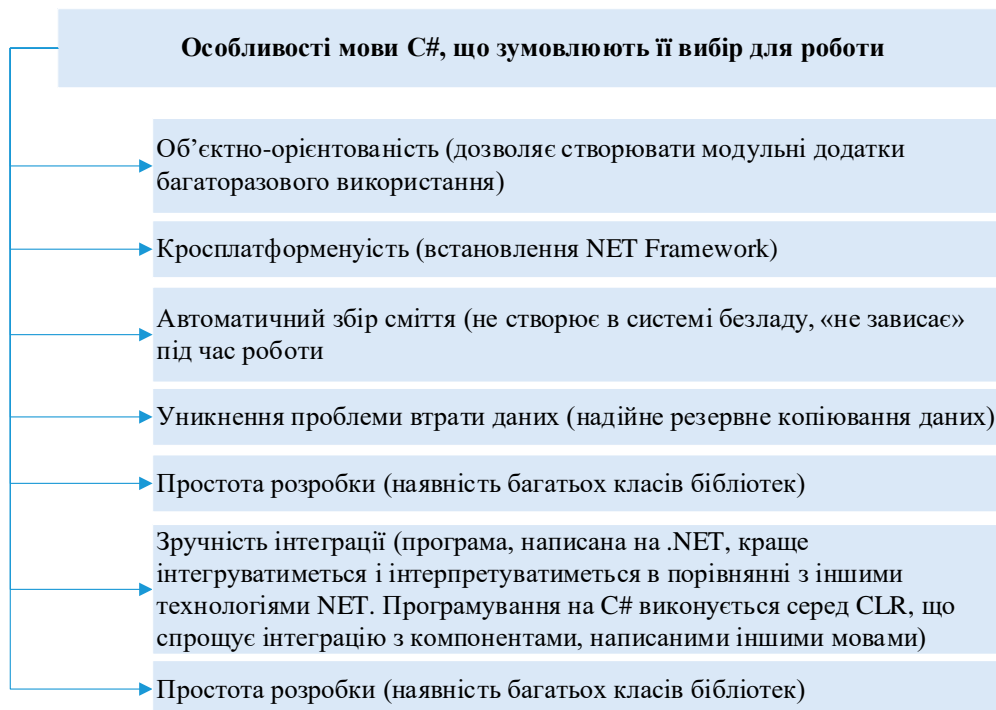


Рисунок 2.7 – Особливості мови C#, що зумовлюють її вибір для розробки

Окрім того, мова C# має потужну базу підтримки, є найбільш розвинутою мовою для .NET Framework, пристосована до постійних оновлень та має звичний синтаксис при практичній роботі з нею.

Для розробки презентаційної частини роботи застосуємо фреймворк Angular від компанії Google для створення просунутих безшовних (односторінкових) веб-додатків – SPA (Single Page Applications), зокрема на мові Java Script.

Вибір даного фреймворку зумовлений особливостями його засобів, зокрема, компонентів, модулів, форм, сервісів та директив. Розглянемо їх більш детально.

Компоненти – складові програми, які не залежать один від одного. Наприклад, один компонент – це стрічка новин, інший – шапка сайту. Додаток будується з них, як із блоків. В роботі передбачається збереження компонентів за допомогою CSS-стилів, що будуть в тому ж файлі, що і компонент. Таким чином, буде створюватись готовий блок інтерфейсу зі структурою, стилями та певною логікою поведінки.

Модулі – це також складові частини програми, що керуватимуть даними компонентами. Якщо компонент – це область програми, модуль відповідає за керування нею. Точка входу в програму, код для анімації або навігації – це всі модулі.

Головний модуль є у кожному проекті. Додаткові додаються в міру потреби та виконують конкретні завдання. Вони потрібні, щоб не перевантажувати основний модуль зайвою функціональністю та не робити його надто громіздким.

Як і більшість програмних додатків, розроблюваний в роботі програмний засіб є form-based, тобто заснований на формах. Форма – це структура, в яку користувач вводить якісь дані, а потім відправляє їх на сервер. Блок для написання коментаря чи зворотний зв'язок – це форма. Angular робить роботу з формами простішим: їх не доводиться писати з нуля. Для них вже створені шаблони, які потрібно адаптувати до нового завдання.

Наступним вагомим засобом платформи є сервіси, які схожі на компоненти, але більш вузькоспеціалізовані. Вони можуть визначатися як на рівні модуля, так і на рівні компонента або програми. У сервісах реалізується спеціальна логіка. Вони підключаються до програми як звичайний клас і використовуються для зберігання глобального стану програми. Також використовуються як постачальник даних.

Ще один окремий засіб, що активно застосовуватиметься при розробці – директиви, це складові програми, які змінюють структуру або поведінку сторінки. Компоненти також належать до директив. Але крім них існують ще два види: структурні директиви та директиви, що змінюють зовнішній вигляд чи поведінку елементів. Вони потрібні, щоб застосувати одну дію до всіх екземплярів одного компонента, наприклад, зміна валюти у всіх картках товару.

Разом із фреймворком Angular використаємо мову Java Script. Вибір даної мови зумовлений певними її перевагами, порівняно з іншими мовами, що застосовуються на даній платформі, деякі з них наведено на рис. 2.8.

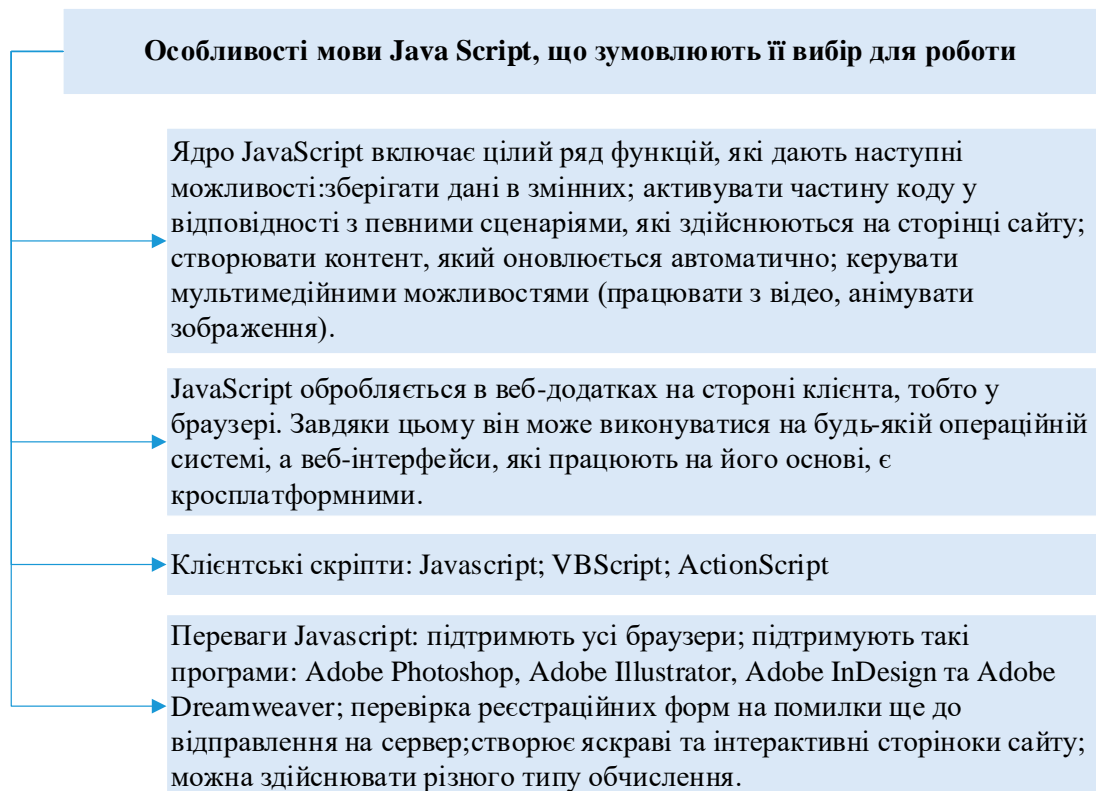


Рисунок 2.8 – Особливості мови Java Script, що зумовлюють її вибір для розробки

Окрім того, мова програмування JavaScript повністю інтегрована з HTML, здатна як завгодно змінювати веб-сторінку, дозволяє створити найрізноманітніший дизайн сторінки, прописати усі особливості структури сайту, що зумовлює її вибір при здійсненні розробки.

Таким чином, на основі використання обраних засобів програмування, далі в роботі здійснимо програмну реалізацію веб-додатку на основі вдосконаленого алгоритму для вбудовування цифрового водяного знаку у відео.

2.5 Висновки до розділу

Отже, в даному розділі було здійснено вдосконалення обраного алгоритму вбудовування цифрового водяного знаку задля підвищення стійкості вбудовуваного ЦВЗ у потоковий відеозапис та розроблено алгоритм роботи програмного засобу. Обраний алгоритм вбудовування цифрового водяного знаку, що базується на ідеї диференціального енергетичного водяного знаку, та є методом вбудовування ЦВЗ, заснований на вибірковому відкиданні частини високочастотних коефіцієнтів ДКП стислих зображень і відеозображень.

Основними проблемами алгоритму DEW є: високочастотні коефіцієнти ДКП, що легко відкидаються фільтрами, у зв'язку з чим алгоритм DEW, який використовує для впровадження ЦВЗ високочастотні коефіцієнти, буде вразливим до цієї дії на контейнер та те, що алгоритм DEW не враховує, який вплив на вихідне зображення має відкидання коефіцієнтів ДКП.

Для усунення недоліків методу DEW та, відповідно, підвищення стійкості вбудовуваного цифрового водяного знаку у потоковий відеозапис, застосуємо метод Канні та зміни у математичному апараті методу DEW. а саме вибір коефіцієнтів для вбудовування. Перевагами обраного методу є складність видалення ЦВЗ, стійкість до більшості видів атак, можливість знизити вплив на візуальну якість.

Для практичної реалізації програмного додатку заплановано застосувати платформу ASP.NET Core 3.1 та мову програмування C# (backend) та фреймворк Angular та мову програмування Java Script (frontend).

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ВДОСКОНАЛЕНОГО МЕТОДУ ВБУДОВУВАННЯ ЦВЗ НА ПРИКЛАДІ ОНЛАЙН-СЕРВІСУ

Враховуючи поставлені задачі роботи та розроблені алгоритми програмного засобу, в даному розділі опишемо практичну реалізацію програмного додатку на основі вдосконаленого алгоритму диференціального вбудовування енергії для підвищення стійкості вбудовуваного цифрового водяного знаку у потоковий відеозапис.

В роботі опишемо проектування користувацького інтерфейсу розробки, його програмну реалізацію, інструкцію користувача для роботи із розробленим онлайн-сервісом та проведемо тестування вдосконаленого алгоритму.

Програмну розробку заплановано здійснити за рахунок використання наступних програмних засобів: платформи ASP.NET Core 3.1 та мови програмування C# (backend) та фреймворку Angular та мови програмування Java Script (frontend).

3.1 Розробка графічного інтерфейсу програмної розробки

При розробці програмного додатку одним із важливих етапів роботи є розробка користувацького інтерфейсу. Здійснюючи планування сторінок веб-сервісу доцільно звернути увагу на такі вимоги до GUI:

- кожна сторінка сервісу повинна мати чітку візуальну ієрархію елементів;
- навігація по сторінках не повинна викликати сумнівів, запитань, та бути очевидною;
- фрагменти тексту мають розташовуватись на екрані таким чином, щоб погляд користувача автоматично переміщався в необхідному напрямку;
- вміст полів не повинен «притискатися» до контурів екрану, а розташовуватися біля горизонтальних або вертикальних осей.

Враховуючи поставлені задачі роботи та вимоги до інтерфейсу, спроектуємо вигляд деяких основних сторінок веб-сервісу.

Першою сторінкою, на яку потрапляє користувач при переході за посиланням є сторінка авторизації. В ній розміщені поля із назвою сторінки, поле для заповнення електронної пошти та паролю. Нижче розташуємо функціональні кнопки «Увійти» та «Зареєструватися», у випадку якщо користувач ще не має облікового запису (рис. 3.1).

The image shows a browser window with the following elements:

- Browser title: Вкладка сервісу
- Address bar: Посилання
- Page title: Авторизація
- Form fields:
 - Електронна пошта (Email)
 - Пароль (Password)
- Buttons:
 - Увійти (Login)
 - Зареєструватися (Register)

Рисунок 3.1 – Проектування сторінки авторизації

Наступна сторінка – це розділ «Відео», де розміщена галерея із відео користувача. На даній сторінці у верхній частині розмістимо функціональні кнопки для переходу по розділам сервісу «Підписки», «Відео», «Користувач». Окремо передбачається розробка стрічки пошуку відео по сервісу через стрічку «Пошук», що буде розміщена під кнопками з розділами.

У верхньому правому кутку розміщена функціональна кнопка «Вихід», якщо користувачеві необхідно вийти із свого облікового запису.

В основній частині вікна передбачається розміщення галереї.

Відео будуть розташовані на сторінці у форматі «плитки», наступним чином: для відображення відео використовується його прев'ю, яке користувачеві необхідно завантажити при додаванні відео. Під відео планується розмістити надписи із його назвою, зазначенням автора, а також відображати реакції на відгуки (like та dislike), фіксуючи їх кількість.

Спроектований вигляд даної сторінки веб-сервісу наведено на рис. 3.2.

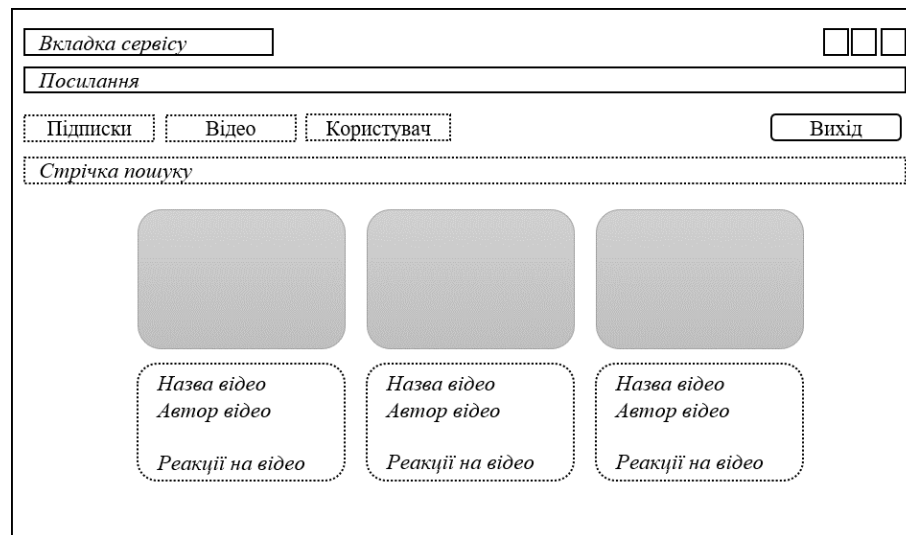


Рисунок 3.2 – Проектування сторінки із галереєю відео

Наступним кроком розглянемо сторінку на яку здійснюється перехід через вкладку «Користувач» – «Додати відео», яка призначена для завантаження відео на сервіс користувачем із вбудовуванням цифрового водяного знаку.

На даній сторінці аналогічним чином у верхній частині розміщені функціональні кнопки розділів та виходу із сервісу.

Нижче розташовано поле, в якому відображається аватар користувача, його нік, та функціональні кнопки підписки. Нижче під даним полем розташовані кнопки «Відео користувача», «Вподобані відео», «Невподобані відео» та «Додати відео», власне зміст останньої далі розглядатимемо.

У першому блоці розміщені поля для додавання інформації про відео, користувачеві слід ввести назву відео, за бажанням написати опис до нього, обов'язково завантажити відео та прев'ю до нього. При заповненні полів їх контури будуть підсвічуватись (зеленим – кольором, якщо поле заповнене та відповідає вимога, червоним – якщо дані вимоги не виконанні), при завантаженні файлу відео та прев'ю буде перевірятись відповідність їх формату.

У другому блоці розміщені поля для додавання даних цифрового водяного знаку, користувачеві слід завантажити файл ЦВЗ та / або додати відповідний текст.

Нижче розміщуватимуться функціональні кнопки «Вбудувати ЦВЗ» та «Додати відео» для збереження введених змін.

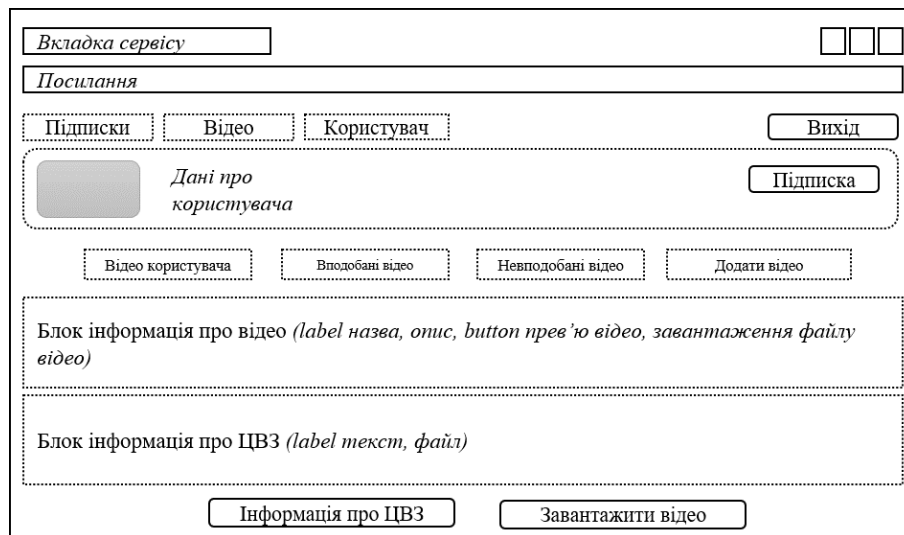


Рисунок 3.3 – Проектування сторінки «Додати відео»

Далі розглянемо сторінку відео, на яку переходитиме користувач після натиснення на відео для його перегляду. У основній частині вікна розташовуватиметься власне відео для його показу. Під відео планується розмістити надписи із його назвою, зазначенням автора, реакції на відгуки (like та dislike), фіксуючи їх кількість. Нижче заплановано розташувати поле «Коментарі» та відповідну функціональну кнопку для їх надсилання. У правій частині вікна у формі плитки можливе розташування інших відео з галереї.

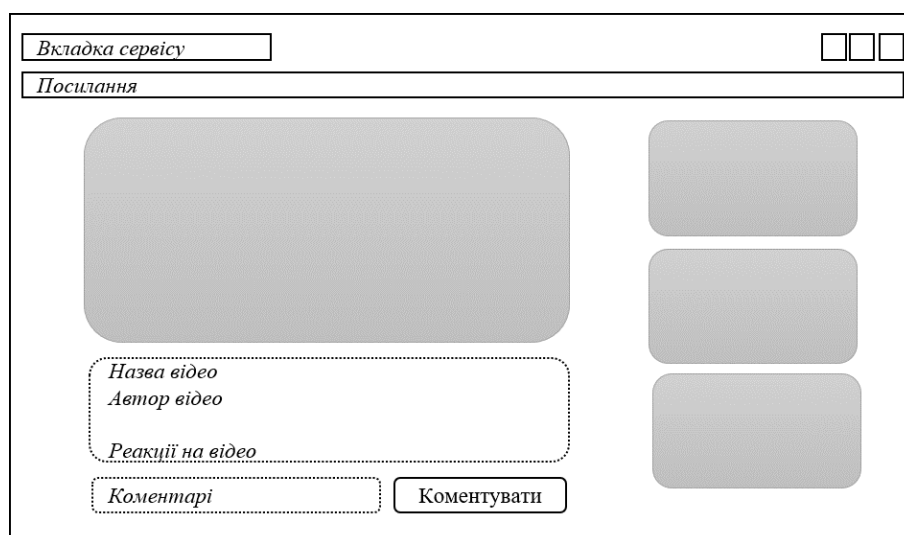


Рисунок 3.4 – Проектування сторінки перегляду відео

Таким чином, на основі спроектованого інтерфейсу далі в роботі буде здійснена програмна розробка сервісу для вбудовування ЦВЗ у відео на основі вдосконаленого методу.

3.2 Програмна реалізація вдосконаленого алгоритму

В даному розділі опишемо основні програмні частини, що були написані для практичної реалізації програмного веб-додатку, що призначений для практичного застосування алгоритму підвищення стійкості вбудовуваного цифрового водяного знаку у потоковий відеозапис на основі вдосконаленого диференціального вбудовування енергії.

Backend-частина розробки містить у собі такі ключові особливості як авторизація користувача, додавання відео, вбудовування цифрового водяного знаку, додавання користувачів, реакції на відео, коментарі і т.д., тобто функціонал веб-сервісу.

Для реалізації функції авторизації користувача описано клас `Authenticate`, що містить компоненти логін та пароль:

```
public async Task<ClaimsIdentity> Authenticate(string email, string password)
{
    User user = await _unitOfWork.UserManager.FindByEmailAsync(email);
    if (await _unitOfWork.UserManager.CheckPasswordAsync(user, password) == false)
    {
        return null;
    }
    var claims = new List<Claim>();
    var roles = await _unitOfWork.UserManager.GetRolesAsync(user);
    claims.Add(new Claim(ClaimsIdentity.DefaultNameClaimType, user.Id.ToString()));
    foreach (var role in roles)
    {
        claims.Add(new Claim(ClaimsIdentity.DefaultRoleClaimType, role));
    }
    ClaimsIdentity claimsIdentity =
        new ClaimsIdentity(claims, "Token", ClaimsIdentity.DefaultNameClaimType,
            ClaimsIdentity.DefaultRoleClaimType);
    return claimsIdentity;
}
```

Для додавання нового користувача реалізовано клас `AddUser` та описано його роль:

```
public async Task AddUser(UserDto userDto, UserLoginDto userLoginDto)
{
    User user = _mapper.Map<User>(userDto);
    await _unitOfWork.UserManager.CreateAsync(user, userLoginDto.Password);
    await _unitOfWork.UserManager.AddToRoleAsync(user, "User");
}
```

```

        await _unitOfWork.SaveAsync();
    }

```

Типовою функцією для онлайн-сервісу є також додавання коментарів під відео. Дану функцію реалізовано через клас `AddCommentary`, кожного коментаря додано властивості, зокрема `User` та `DateTime.Now` для того, щоб можна було бачити хто та коли залишив коментар:

```

public async Task AddCommentary(CommentaryDto commentaryDto)
{
    Commentary commentary = new Commentary
    {
        Id = Guid.NewGuid(),
        Content = commentaryDto.Content,
        User = await _unit.UserRepository.GetUserById(commentaryDto.UserId),
        Video = await _unit.VideoRepository.GetVideoById(commentaryDto.VideoId),
        DayOfCreation = DateTime.Now
    };
    _unit.CommentaryRepository.AddCommentary(commentary);
    await _unit.SaveAsync();
}

```

Окремо реалізовано можливість здійснювати підписку на інших користувачів. Створено клас `Subscribe` в якому прописано можливість підписатись та відписатись від того чи іншого користувача:

```

public async Task<bool> Subscribe(string subscriberId, string subscriptionId)
{
    User subscriber = await _unitOfWork.UserRepository.GetUserById(subscriberId);
    User subscription = await _unitOfWork.UserRepository.GetUserById(subscriptionId);
    bool isSubscriber = false;
    if (subscriber.Subscriptions.FirstOrDefault(x => x.SubscriberId == subscriptionId) ==
null)
    { isSubscriber = true;
      subscriber.Subscribe(subscription); }
    else
    { subscriber.Unsubscribe(subscription);
    }
    await _unitOfWork.SaveAsync();
    return isSubscriber;
}

```

Наступна можливість реалізована на сервісі – це залишати реакції на відео («лайк» або «дизлайк»). Реалізацію позитивної реакції описати через `public async Task PutLike`:

```
public async Task PutLike(Guid videoid, string userId)
{
    User user = await _unit.UserRepository.GetUserById(userId);
    Video video = await _unit.VideoRepository.GetVideoById(videoid);
    if (video == null)
    { throw new InvalidDataException("This video do not exist"); }
    user.AddLike(video);
    await _unit.SaveAsync();
}
```

Реалізацію негативної реакції на відео описано через public async Task PutDislike:

```
public async Task PutDislike(Guid videoid, string userId)
{
    User user = await _unit.UserRepository.GetUserById(userId);
    Video video = await _unit.VideoRepository.GetVideoById(videoid);
    if (video == null)
    { throw new InvalidDataException("This video do not exist"); }
    user.AddDislike(video);
    await _unit.SaveAsync();
}
```

Далі розглянемо практичну реалізацію frontend-частини.

Підключення до сервісу:

```
export const environment = {
  production: false,
  url: "https://apiv1.it-brain.tk/api",
  defaultError: "Error",
  token: "Token",
  id: "UserId",
  adminRole: "Admin"
};
```

Реалізація форми авторизації користувача після входу на сервіс, описана через login():

```
login(): void {
  this.loginService.authenticate(this.loginModel)
    .pipe(catchError(ErrorHandler.handleErrorFromObservable))
    .subscribe((ok) => {
      localStorage.setItem(environment.token, ok['access_token'])
      localStorage.setItem(environment.id, ok['id'])
      this.navigator.navigate(['/main']);
    },
    (error: HttpResponse) => {
      if (error.error != null && error.error != "") {
        this.toastr.error(error.error);
      }
    });
}
```



```

    } else {
      this.toastr.error(error.message);
    }
  });

```

Для створення сторінки, що містить інформацію про користувача з можливістю вносити в них зміни описано наступну кодову послідовність:

```

updateInfo() {
  this.userService.updateUserInfo(this.user)
    .pipe(concatMap(resp => {
      return this.userService.getUserInfo(localStorage.getItem(environment.id));
    })),
    catchError(ErrorHandler.handleErrorFromObservable)
  ) .subscribe(ok => {
    this.user = <UserModel>ok;
    this.toastr.success('Інформацію оновлено.');
```

```

  }, (error: HttpResponse) => {
    this.toastr.error(error.message);
  });

```

На сервісі також реалізована функція пошуку відео за певним запитом користувача, реалізована наступним чином:

```

find(name: string) {
  if (name == "") {
    this.getSubscriptionVideos();
  } else {
    this.$videos = this.videoSelectionService.getVideosByName(name).pipe(
      catchError((error: HttpResponse) => {
        this.toastr.error(error.message ?? error.error);
        return throwError(error);
      });
    );
  }
}

```

Компоненти для додавання відео:

```

@Component({
  selector: 'app-video-add',
  templateUrl: './video-add.component.html',
  styleUrls: ['./video-add.component.less']
})

```

В ході виконання процесу додавання відео на веб-ресурс, користувач також завантажує прев'ю на відео, яке буде відображатись в галереї, реалізовано через loadPhoto(event):

```

loadPhoto(event) {
  let photo = event.target.files[0];
  if (photo.type.match('png') || photo.type.match('jpeg')) {
    this.toastr.success('Фото завантажено.');
```

```

    this.photo = photo;
  } else {
    this.toastr.error('Фото повинно бути у форматі png або jpeg!!!');
  }

```

Важливим етапом при завантаженні відео користувачем, є перевірка наявності завантаженого відео та відповідності його формату. У випадку, якщо користувач натиснув кнопку «Додати відео», але файл не буде обрано, він отримає про це відповідне повідомлення, аналогічно користувач отримає сповіщення якщо завантажуваний формат відео не відповідає вимогам сервісу, реалізовано наступним чином:

```

videos: string = 'Не вибрано';
onFileSelectedVideos(event) {
  if (event.target.files.length > 0) {
    let video = event.target.files[0];
    this.videos = video.name
    if (video.type.match('mp4')) {
      this.toastr.success('Відео завантажено. ');
      this.video = video;
    } else {
      this.toastr.error('Відео має бути у форматі mp4!!!');
    }
  }
}
load1() {

```

Наступним кроком користувач завантажує файл та/або додає текст, що буде використано у якості ЦВЗ, після виконання процесу вбудовування ЦВЗ, користувач отримує відповідне повідомлення:

```

}
addEnc() {
  alert("ЦВЗ успішно додано")
}

```

Кодова послідовність html-сторінки, що була розроблена для сторінки сервісу, яка слугує для додавання відео наведена в додатку Б.

Лістинг фрагментів frontend-частини наведений у додатку В.

Таким чином, на основі розробленого програмного проекту було здійснено програмну реалізацію онлайн-сервісу, який надає користувачеві можливість завантажувати відео, захищаючи авторське право за рахунок ЦВЗ.

3.3 Інструкція користувача для роботи з онлайн-сервісом

В даному підрозділі роботи опишемо інструкцію користувача для роботи з онлайн-сервісом, що надаватиме можливість завантажувати відео та захищати авторське право на нього за рахунок використання цифрового водяного знаку.

Отже, для початку роботи з сервісом, користувачеві слід перейти за посиланням <https://webv1.it-brain.tk/>. На даній сторінці відобразиться вікно авторизації користувача (рис. 3.5), що надає можливість:

- увійти в систему зареєстрованому користувачеві;
- створити новий акаунт.

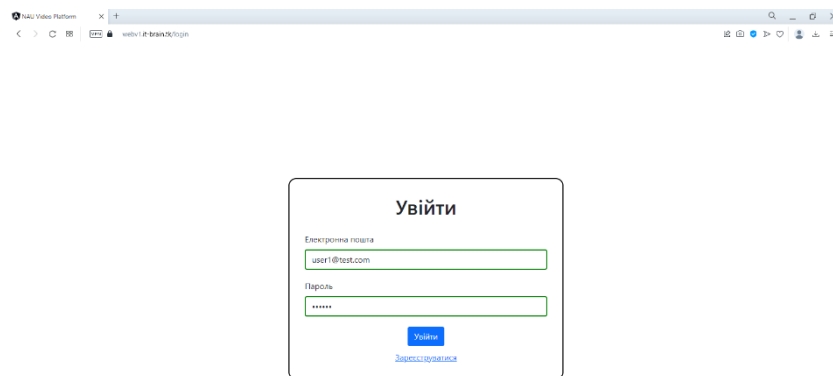


Рисунок 3.5 – Сторінка авторизації користувача

У випадку, якщо користувач вже зареєстрований на сервісі, йому необхідно у відповідні поля ввести логін та пароль для його ідентифікації системою.

Під час введення логіну та паролю перевіряється їх коректність. Якщо користувач ввів дані вірно (синтаксис електронної адреси відповідає заданому, а поле пароля заповнене) – дані поля підсвічені зеленим кольором.

У випадку, якщо користувач ввів некоректні дані, відповідні поля підсвічені червоним кольором та повідомляють користувачеві про необхідність редагування даних авторизації (рис. 3.6).

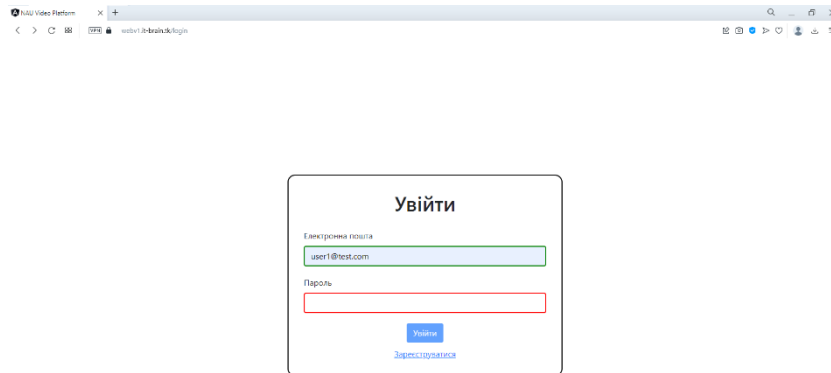


Рисунок 3.6 – Вигляд форми авторизації, що заповнена невірно

Якщо користувач вводить невірні дані авторизації, на сторінці з’являється відповідне повідомлення.

Користувачеві слід вводити коректні дані повторно.

Якщо у користувача ще не створено облікового запису на даному сервісі, йому необхідно скористатись кнопкою реєстрації та ввести у відповідну форму власні дані.

Для здійснення реєстрації користувачеві слід заповнити поля «Ім’я», «Прізвище», «Електронна пошта» та «Пароль» (рис 3.7).

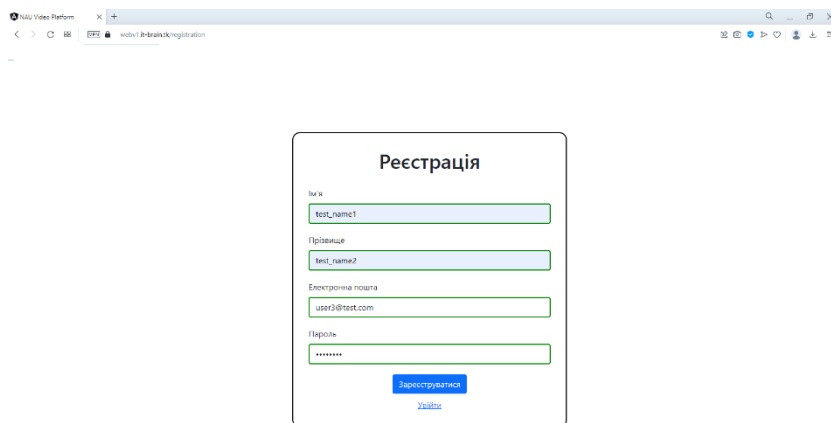


Рисунок 3.7 – Вигляд сторінки реєстрації користувача

Для завершення процесу реєстрації, на вказану електронну пошту користувачеві приходять повідомлення із проханням підтвердити електронний

адрес пошти.

Якщо вказані користувачем дані при реєстрації вже існують в системі (вже зареєстрована вказана пошта) або пароль не відповідає вимогам, на сторінці з'являється відповідне повідомлення про необхідність редагування даних.

Наступним етапом є отримання доступу користувачем до свого акаунту на сервісі. Зайшовши у власний обліковий запис, на головній сторінці користувач може переглянути основні розділи («Підписки», «Відео», «Користувач»), скористатись полем пошуку відео на сервісі.

В основній частині вікна у вигляді галереї розміщені відео, що належать до відео галереї даного користувача, у правому верхньому куті розташована кнопка виходу із акаунту (рис. 3.8).

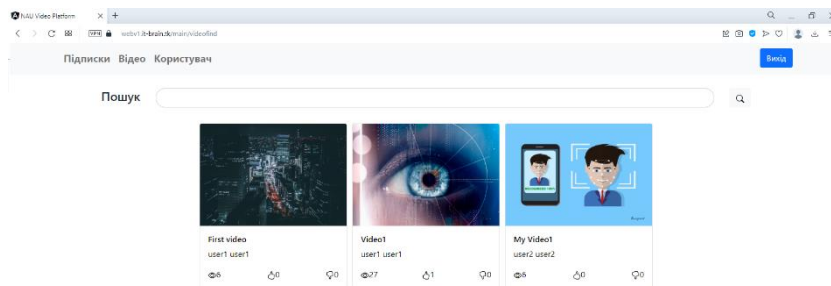


Рисунок 3.8 – Вигляд головної сторінки авторизованого користувача

Розглянемо наведені розділи детальніше. У розділі «Підписки» користувач може переглянути підписників свого акаунту, їх відео доступні для його перегляду. У розділі «Відео» наводиться відео галерея сервісу. У розділі «Користувач» (рис. 3.9) надається можливість редагувати інформацію (рис. 3.10), а також переглядати розділи з відео («Відео користувача», «Вподобані відео», «Не вподобані відео», «Додати відео»). Зупинимось більш детальніше на вкладці «Додати відео». На даній сторінці реалізована можливість додавати захищене відео, що ґрунтується на методі вбудовування ЦВЗ вдосконаленому у даній роботі (рис.3.11).

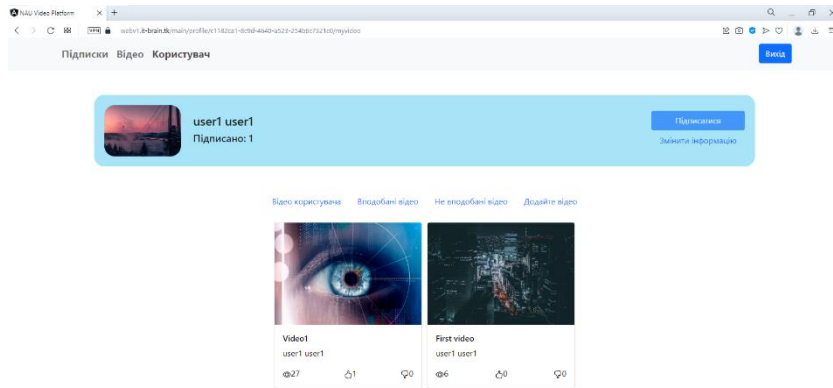


Рисунок 3.9 – Вигляд розділу сторінки «Користувач»

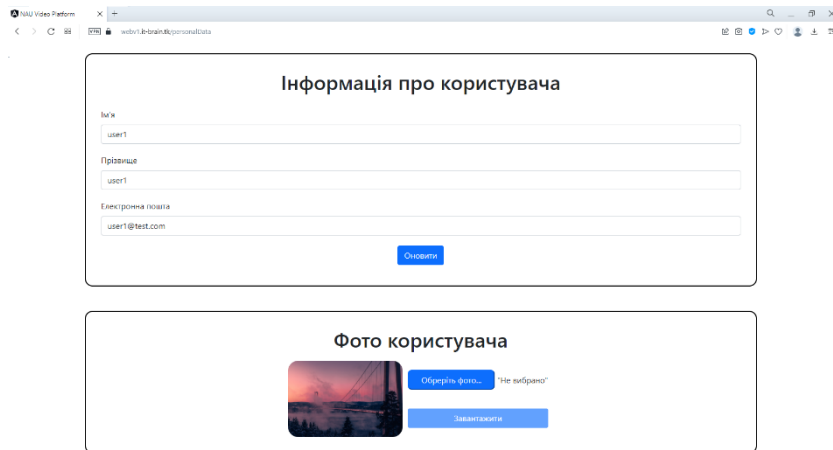


Рисунок 3.10 – Вигляд сторінки «Редагувати дані»

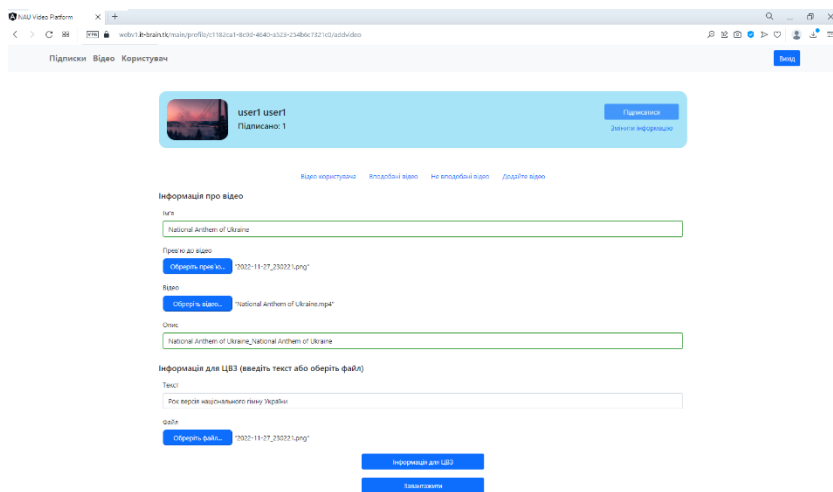


Рисунок 3.11 – Вигляд сторінки «Додати відео»

На сторінці додавання відео користувачеві необхідно заповнити поля «Інформація про відео» (назва, прев'ю та завантаження файлу відео) та «Інформація про ЦВЗ» (вказати текст ЦВЗ та / або додати файл ЦВЗ).

Після успішного завантаження файлів, користувач отримує відповідні сповіщення (рис. 3.12)

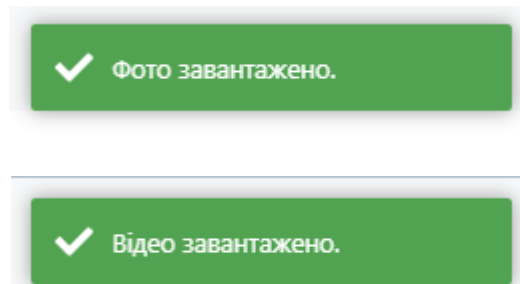


Рисунок 3.12 – Сповіщення про успішне завантаження файлів

Після введення вказаних даних користувач повинен натиснути кнопку «Інформація для ЦВЗ» у нижній частині сторінці. Дана кнопка запускає перевірку вказаних даних ЦВЗ та формує власне цифровий знак.

У випадку, якщо певні поля не будуть заповнені або будуть заповнені некоректно – вони будуть підсвічені червоним кольором, у випадку коректності введення усіх даних – поля підсвічуються зеленим кольором.

Після успішного завантаження ЦВЗ, на сторінці з'являється відповідне повідомлення (рис. 3.13).

Підтвердіть дію на сторінці webv1.it-brain.tk
ЦВЗ успішно додано



Рисунок 3.13 – Повідомлення про успішне додавання ЦВЗ

Після здійсненої перевірки, користувачеві слід натиснути кнопку «Завантажити», завантажене користувачем відео захищене цифровим водяним знаком за вдосконаленим алгоритмом додається на сервіс (рис. 3.14).

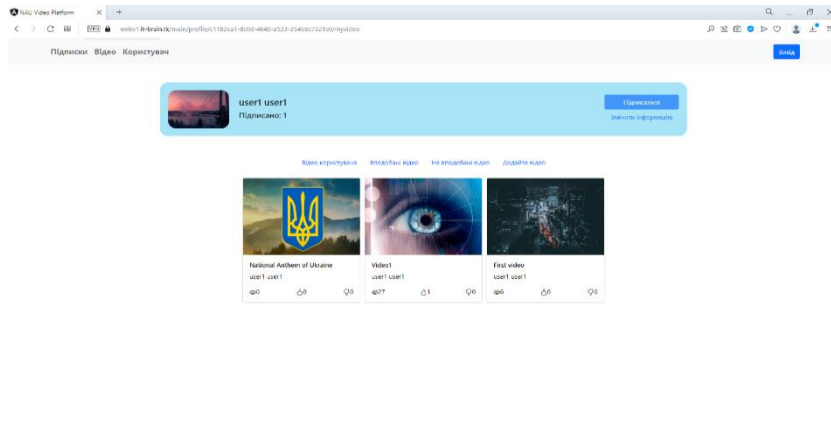


Рисунок 3.14 – Вигляд сторінки із завантаженим відео

Після завантаження відео, користувач може натиснути на прев'ю відео у відеогалереї та потрапити на сторінку з відео (рис.3.15).

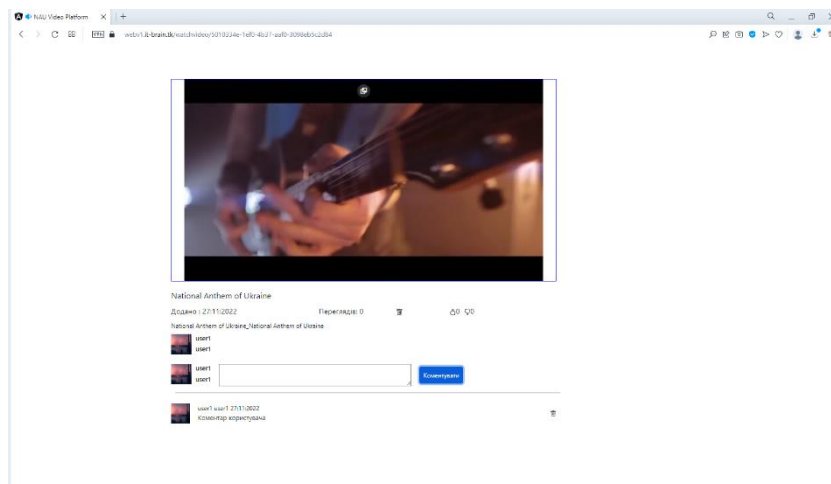


Рисунок 3.15 – Вигляд сторінки для перегляду відео

На даній сторінці надається можливість переглянути назву відео, дані про час та дату додавання, кількість переглядів, поставити вподобайку відео або навпаки. Крім того, реалізований розділ для додавання коментарів. Користувач має можливість залишити свій коментар під відео, видалити його, підтвердивши дану дію (рис. 3.16) та прочитати коментарі інших користувачів, що переглядали дане відео. Також власник відео має можливість його видалити, підтвердивши дану дію у відповідному повідомленні на сторінці (рис. 3.17).

Підтвердіть дію на сторінці webv1.it-brain.tk
 Ви бажаєте видалити цей коментар?



Рисунок 3.16 – Сповіщення про видалення коментаря

Підтвердіть дію на сторінці webv1.it-brain.tk
 Ви хочете видалити це відео?



Рисунок 3.17 – Сповіщення про видалення відео

Таким чином, в даному підрозділі було описано інструкцію користувача для роботи із розробленим онлайн сервісом, що передбачений для розміщення та перегляду відео, що захищається цифровим водяним знаком на основі вдосконаленого у роботі алгоритму.

3.4 Аналіз результатів та тестування вдосконаленого методу

Виходячи із поставленої мети роботи, було проведено вдосконалення методу вбудовування цифрового водяного знаку на основі DEW.

В даному розділі здійснимо тестування вдосконаленого алгоритму для визначення його стійкості до різного роду атак.

У даному підрозділі розглянемо такі метрики, що найчастіше використовуються, а саме: пікове відношення сигналу до шуму, структурна подібність, абсолютна різність, якість картинки.

В таблиці 3.1 опишемо основні досліджувані показники для здійснення тестування вдосконаленого алгоритму.

Таблиця 3.1 – Досліджуванні показники тестування алгоритму [43]

Показник	Розрахунок
Структурна подібність	$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$
Співвідношення сигнал / шум	$SNR = \frac{\sum_{x,y} (C_{x,y})^2}{\sum_{x,y} (C_{x,y} - S_{x,y})^2}$
Максимальне співвідношення сигнал / шум	$PSNR = XY \cdot \frac{\max_{x,y} (C_{x,y})^2}{\sum_{x,y} (C_{x,y} - S_{x,y})^2}$
Середня абсолютна відмінність	$AD = \frac{1}{XY} \sum_{x,y} C_{x,y} - S_{x,y} $
Нормована середня абсолютна відмінність	$NAD = \frac{\sum_{x,y} C_{x,y} - S_{x,y} }{\sum_{x,y} C_{x,y} }$
Якість картинки	$IF = 1 - \frac{\sum_{x,y} (C_{x,y} - S_{x,y})^2}{\sum_{x,y} (C_{x,y})^2}$

Дані показники обчислюються на основі різниці контейнера-оригіналу (неспотвореного сигналу) та стегоконтейнера (спотвореного сигналу).

У представлених співвідношеннях через $C_{x,y}$ позначається компонента пікселя порожнього контейнера з координатами (x, y) , в яку здійснюється вбудовування, а через $S_{x,y}$ – відповідна компонента пікселя заповненого контейнера.

Для тестування програмного забезпечення на основі вдосконаленого методу було обрано десять відео із вбудованим цифровим водяним знаком, що являє собою тестове повідомлення «Дане відео захищене авторським правом» (повідомлення представлене у вигляді стрічки ASCII, кількість символів 37, кожен символ по 8 біт, розмір повідомлення 296 біт).

Аналогічне тестування було проведено для дослідження відео в якому для вбудовування використовуються методи DEW, LSB [44] (метод найменш значущого біту) та Кутера (метод Кутера-Джордана-Босена) [45].

Результати, отримані у процесі тестування, були проаналізовані та узагальнені.

Для прикладу наведемо результати дослідження трьох стежоконтейнерів.

У першому дослідженні кадр має яскраві на насичені кольори, переходи між пікселями плавні, кольорові компоненти розподілені майже однаково, більш виражені червона та зелена.

Результат дослідження наведений у таблиці 3.2.

Таблиця 3.2 – Показники зміни контейнера у досліді 1

	<i>SSIM</i>	<i>SNR</i>	<i>PSNR</i>	<i>AD</i>	<i>NAD</i>	<i>IF</i>
DEW	0,723	85362	103681	0,9114	0,0181	99,8%
DEW удоск.	0,812	92548	126458	0,8754	0,0089	99,9%
LSB	0,652	65746	98535	0,4712	0,0082	99,8%
Кутера	0,689	36241	26854	0,6251	0,0095	98,7%

У даному дослідженні найбільш високі результати має алгоритму DEW вдосконалений та наступний за ним DEW початковий. Дані показники пов'язані із стійкістю алгоритмів до спотворення та більшості атак, в зв'язку із необхідністю проведення більш складних математичних операцій для спотворення ЦВЗ, на відміну від методів LSB та Кутера.

У другому дослідженні кадр має не насичені кольори, роздільна здатність низька, переходи між пікселями нечіткі, кольорові компоненти розподілені нерівномірно, найбільш виражена. Результат дослідження наведений у таблиці 3.3.

Таблиця 3.3 – Показники зміни контейнера у досліді 2

	<i>SSIM</i>	<i>SNR</i>	<i>PSNR</i>	<i>AD</i>	<i>NAD</i>	<i>IF</i>
DEW	0,693	18204,3	127271	0,652	0,0068	99,99%
DEW вдоск.	0,931	24526,8	131185	0,855	0,009	99,99%
LSB	0,762	21852,6	118897	0,785	0,008	99,98%
Кутера	0,625	17233,6	100197	0,568	0,005	99,85%

Із даних наведених у таблиці можемо побачити, що найбільш оптимальні показники мають алгоритми LSB та вдосконалений DEW. Найменш стійким є алгоритм Кутера. Основною проблемою якого виявилась слабкість його декодера, відповідно завданням розпізнання ЦВЗ було важким.

У третьому дослідженні кадр має насичені кольори, високу контрастність, роздільна здатність висока, переходи між пікселями нечіткі, кольорові компоненти рівномірно. Результат дослідження наведений у таблиці 3.4.

Таблиця 3.4 – Показники зміни контейнера у досліді 3

	<i>SSIM</i>	<i>SNR</i>	<i>PSNR</i>	<i>AD</i>	<i>NAD</i>	<i>IF</i>
DEW	0,893	856427	144825	0,894	0,007	99,98%
DEW вдоск.	0,925	945632	236587	0,987	0,008	99,99%
LSB	0,862	876325	128964	0,793	0,006	99,96%
Кутера	0,747	154369	5865	0,642	0,054	96,92%

В даному дослідженні найбільш високий показник має вдосконалений алгоритм DEW за усіма параметрами, оскільки показує найбільш високу здатність захисту від атак та візуальних змін.

Дещо нижчі показники мають початковий алгоритм DEW та LSB (що пов'язано із вразливістю до певних видів атак та змін за рахунок особливостей вбудовування ЦВЗ).

Найнижчий показник має алгоритм Кутера під підрахунку якості картинки. Даний результат пов'язаний із тим, що кадр має високу роздільну здатність та контрастність, а внесені зміни за рахунок ЦВЗ є найбільш помітними порівняно з іншими методами.

Для підведення підсумків за наведеним тестуванням скористаємось експертними оцінками (за результатами тестування кожного зразку оцінимо найкращий показник оцінкою 4, найнижчий – оцінкою 1).

Отримані результати наведено на графіку 3.18.

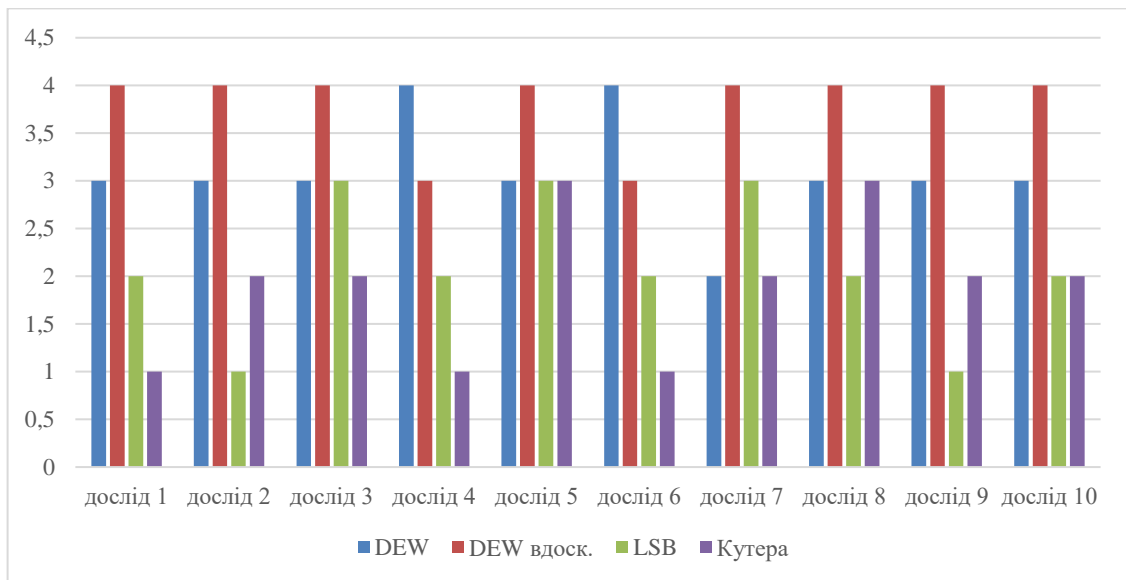


Рисунок 3.18 – Результати тестування

Далі розглянемо результати тестування, в якому проводилось дослідження робастності стежоконтейнера до певних видів змін (поворот контейнера на 90 градусів, стиснення в 2 рази, згладжування за допомогою функції Гауса, збільшення контрастності, збільшення та зменшення яскравості, ерозія зображення, обрізання 15% з різних сторін, стиснення з різними показниками якості). Для представлення результатів тестування також було застосовано метод оцінок (у випадку переважної стійкості алгоритму до змін – надається значення 2, якщо алгоритм уразливий до певних змін – значення 1).

Отримані результати наведено на графіку 3.19.

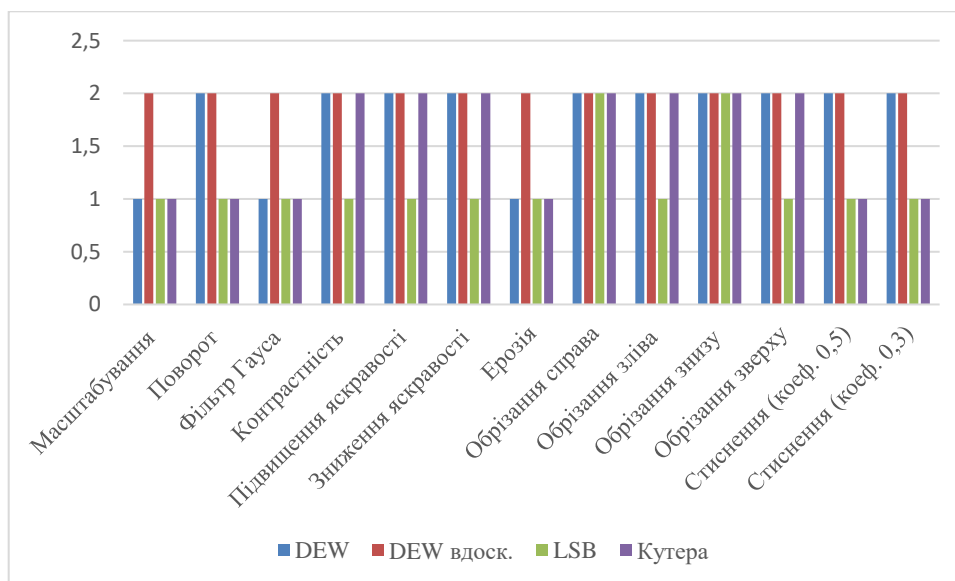


Рисунок 3.19 – Результати тестування

Враховуючи отримані результати проведеного дослідження, можна вважати, що вдосконалений метод DEW є стійким до багатьох видів впливів на контейнер, а стежоконтейнер із вбудованим ЦВЗ за даним методом зазнає найменш помітних змін.

Дані результати досягнуто за рахунок здійсненого удосконалення, а саме внесення змін до математичного апарату алгоритму DEW та застосуванню методу Канні для того, аби запобігти значних візуальних змін при вбудовуванні ЦВЗ.

Для визначення стійкості вбудованого цифрового водяного знаку за вдосконаленим методом проаналізуємо результати атак, що можуть здійснюватися на ЦВЗ внаслідок перекодування та стиснення файлу.

У процесі перекодування відеофайлу застосовуються різні методи перетворення і збереження відеофайлу на носіях інформації, що може мати безпосередній вплив на ЦВЗ.

При стисненні відеофайлу застосовується технологія цифрової компресії сигналу, що дозволяє скоротити кількість даних, що використовують для відеопотоку, а тому може безпосередньо вплинути на ЦВЗ.

Здійснимо дослідження при вказаних атаках.



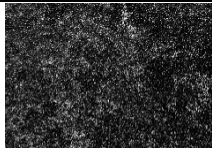



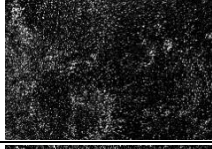



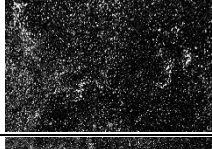



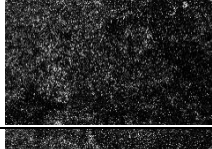



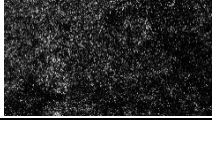

У випадку перекодування застосуємо кодеки бібліотеки `ffmpeg`: `mpeg1`, `mpeg2`, `mpeg3`, `flv` та `h264`.

При стисненні файлів введемо параметр q , що характеризує ступінь стиснення відеофайлу. Для параметра q задамо значення 5 та 10, для дослідження оберемо файл формату `.mp4`.



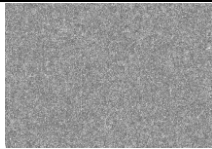



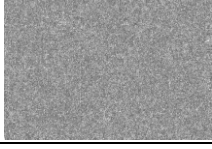

Досліджуваними методами є метод LSB, Кутера, DEW та вдосконалений в роботі алгоритм.

Результати дослідження наведено у табл. 3.5 (для перекодування) та у табл. 3.6 (для стиснення відеофайлів).

Таблиця 3.5 – Результати вилучення ЦВЗ після перекодування

	DEW	DEW (вдос.)	LSB	Кутера
mpeg1				
mpeg2				
mpeg3				
Flv				
h.264				

Таблиця 3.6 – Результати вилучення ЦВЗ після стиснення

	DEW	DEW (вдос.)	LSB	Кутера
$q = 5$				
$q = 10$				

Проаналізувавши подані результати, можемо відмітити, що метод LSB є не стійким до наведених атак, тому його не рекомендовано застосовувати для вбудовування цифрового водяного знаку у відео.

Метод Кутера, враховуючи його особливість вбудовування в просторову область, відносно стійкий до стиснення при низькому значенні параметра q , оскільки передбачений для даних з глибиною кольору в 24 біта.

Оригінальний метод DEW відносно стійкий до перекодування, проте має нестійкий до стиснення при більших значеннях параметра q .

Вдосконалений алгоритм на основі методу DEW показав якісні результати, незначні зміни спостерігаються при перекодування flv та стисненні при більших значеннях параметра q , проте суттєво не змінюють зміст ЦВЗ.

Таким чином, проаналізувавши результати наведеного тестування за показниками візуального впливу та стійкості до атак, можемо зробити висновок, що в загальному застосування вдосконаленого методу дозволяє підвищити показники орієнтовно на 12%, зокрема усуває недолік візуальної помітності змін у відео та має підвищену стійкість до атак перекодування та стиснення. Цифровий водяний знак, що вбудовується у файл не здійснює на нього суттєвого впливу, а вбудовування даних у низькочастотні коефіцієнти дозволяє підвищити стійкість до атак.

3.5 Висновки до розділу

Отже, в даному розділі було здійснено реалізацію програмного засобу для практичної можливості підвищення стійкості вбудовуваного цифрового водяного знаку у потоковий відеозапис на основі вдосконаленого диференціального вбудовування енергії (DEW). Виходячи із поставлених задач роботи розробку здійснено за рахунок використання платформи ASP.NET Core 3.1 та мови програмування C# (backend); фреймворку Angular та мови програмування Java Script (frontend). Також в розділі описано проектування інтерфейсу користувача, особливості програмної реалізації та інструкцію користувача для роботи з додатком. Здійснено тестування розробки, яке показало, що в загальному застосування вдосконаленого методу дозволяє підвищити показники орієнтовно на 12%.

4 ЕКОНОМІЧНА ЧАСТИНА

В даному розділі проведемо дослідження економічного потенціалу розробки, а саме: оцінювання комерційного потенціалу; прогнозування витрат на виконання наукової роботи та впровадження її результатів; прогнозування комерційних ефектів від реалізації результатів розробки та розрахунок ефективності вкладених інвестицій та періоду їх окупності.

Внаслідок даного дослідження буде прийнято рішення про економічну доцільність розробки програмного засобу для вбудовування цифрового водяного знаку у потокове відео на основі вдосконаленого методу.

4.1 Оцінювання комерційного потенціалу розробки програмного забезпечення

Метою проведення технологічного аудиту є оцінювання комерційного потенціалу розробки, створеної в результаті науково-технічної діяльності [46].

Результатом магістерської кваліфікаційної роботи є розробка програмного засобу на основі алгоритму для підвищення стійкості вбудовуваного цифрового водяного знаку у поточковий відеозапис на основі вдосконаленого диференціального вбудовування енергії, що практично реалізований у вигляді веб-сервісу.

Для проведення технологічного аудиту залучено трьох незалежних експертів.

У межах даної роботи такими експертами є викладачі кафедри МБІС:

- Карпінець В. В. (к.т.н., доцент каф. МБІС ВНТУ),
- Салієва О.В. (д.ф., викл. каф. МБІС ВНТУ)
- Грицак А. В. (доц., викл. каф. МБІС ВНТУ).

Оцінювання комерційного потенціалу здійснимо за критеріями, що наведені в таблиці 4.1

Таблиця 4.1 – Критерії оцінювання комерційного потенціалу розробки
бальна оцінка

Критерії оцінювання та бали (за 5-ти бальною шкалою)					
Кри-терій	0	1	2	3	4
Технічна здійсненність концепції:					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено роботоздатність продукту в реальних умовах
Ринкові переваги (недоліки):					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
Критерії оцінювання та бали (за 5-ти бальною шкалою)					
Кри-тер.	0	1	2	3	4
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експл. витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає

Продовження таблиці 4.1

Практична здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витратити значні кошти та час на навч. наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово-промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві
11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої к-ті дозвільних документів на вир-во та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь-які регламентні обмеження на виробництво та реалізацію продукту

Результати оцінювання комерційного потенціалу експертами розробки зведено в таблицю 4.2.

Таблиця 4.2 – Результати оцінювання комерційного потенціалу розробки

Критерії	Прізвище, ініціали, посада експерта		
	1 – Карпінєць В.В.	2 – Салієва О.В.	3 – Грицак А.В.
1	4	4	4
Ринкові переваги (недоліки):			
2	3	3	4
3	4	4	4
4	4	3	3
5	3	4	3
Ринкові перспективи			
6	4	3	3
7	3	4	3
Практична здійсненність			
8	4	4	4
9	4	3	4
10	3	4	3
11	4	4	4
12	3	4	4
Сума балів	СБ ₁ = 43	СБ ₁ = 44	СБ ₁ = 43
Середньоарифметична сума балів $\overline{СБ}$	$\overline{СБ} = 43,3$		

За даними таблиці 4.2 можна зробити висновок, щодо рівня комерційного потенціалу розробки. Зважимо на результат й порівняємо його з рівнями комерційного потенціалу розробки, що представлено в таблиці 4.3.

Таблиця 4.3 – Рівні комерційного потенціалу розробки

Середньоарифметична сума балів $\overline{СБ}$, розрахована на основі висновків експертів	Рівень комерційного потенціалу розробки
0 – 10	Низький
11 – 20	Нижче середнього
21 – 30	Середній
31 – 40	Вище середнього
41 – 48	Високий

Рівень комерційного потенціалу розробки, становить 43,3 балів, що відповідає рівню «високий».

Проаналізуємо суть технічної проблеми та розглянемо аналоги. Наукова новизна розробки полягає в підвищенні стійкості вбудовуваного цифрового водяного знаку у потоковий відеозапис на основі вдосконаленого

диференціального вбудовування енергії.

Розробка програмного засобу має на меті практичну реалізацію удосконаленого стенографічного методу вбудовування цифрового водяного знаку у відео на основі алгоритму диференціального вбудовування енергії.

Розроблюваний програмний продукт у вигляді онлайн-сервісу надаватиме можливість користувачам завантажувати відео та захищати авторське право на нього за рахунок використання цифрового водяного знаку.

Враховуючи отримані результати дослідження розробленого онлайн-сервісу на основі вдосконаленого методу, можна вважати, що він є стійким до багатьох видів впливів на контейнер, а стежоконтейнер із вбудованим ЦВЗ за даним методом зазнає найменш помітних змін.

Дані результати досягнуто за рахунок здійсненого удосконалення, а саме внесення змін до математичного апарату алгоритму DEW та застосуванню методу Канні для того, аби запобігти значних візуальних змін при вбудовуванні ЦВЗ.

Враховуючи такі переваги розробленого методу, можемо порівняти його з аналогами (табл. 1.2).

У таблиці 4.4 наведені основні технічні показники аналога і нового програмного продукту.

Таблиця 4.4 – Основні технічні показники аналога і нового програмного продукту

Показники, %	Аналог	Нова розробка	Відношення параметрів нової розробки до параметрів аналога
Функціональність	75	100	1,3
Надійність	80	100	1,25
Сумісність	90	100	1,1
Супровід	85	100	1,18
Економія ресурсів і часу	80	100	1,25
Простота використання	85	100	1,18

Бурхливий розвиток інформаційних технологій, що спостерігається останніми роками, призвів до того, що сьогодні величезна кількість інформації, що становить інтелектуальну власність, зберігається та обробляється в комп'ютерних мережах та/або поширюється у цифровій формі.

Зокрема, розвиток засобів обчислювальної техніки дало поштовх у розвиток комп'ютерної стеганографії.

Найбільш поширеними порушеннями прав інтелектуальної власності сьогодні є піратство, плагіат, підробка інформації, зміна інформації, недобросовісна конкуренція (промисловий шпигунство тощо).

При цьому найбільша увага приділяється захисту прав інтелектуальної власності мультимедійної інформації, що розповсюджується на цифрових носіях та мережі Інтернет.

Розроблений програмний додаток, порівняно з аналогами, має ряд переваг, зокрема: дозволяє вбудовувати цифрові водяні знаки у потокові відео; удосконалений алгоритм вбудовування цифрового водяного знаку, стійкість якого перевірена на практиці.

Обраний алгоритм вбудовування цифрового водяного знаку, що базується на ідеї диференціального енергетичного водяного знаку, та є методом вбудовування ЦВЗ, заснований на вибіркового відкиданні частини високочастотних коефіцієнтів ДКП стислих зображень і відеозображень.

Для усунення недоліків методу DEW та, відповідно, підвищення стійкості вбудовуваного цифрового водяного знаку у потоковий відеозапис, застосуємо метод Канні та зміни у математичному апараті методу DEW. а саме вибір коефіцієнтів для вбудовування.

Перевагами обраного методу є складність видалення ЦВЗ, стійкість до більшості видів атак, можливість знизити вплив на візуальну якість.

Враховуючи наведені вище матеріали, можна вважати, що нове технічне рішення, яке пропонується для розробки, матиме високі показники, порівняно з аналогами та більшою мірою задовольнить потреби споживачів. Тому його розробка та впровадження є актуальним та доцільним.

Програмна розробка на основі обраного та вдосконаленого алгоритму сьогодні є актуальною для використання як для звичайних так і корпоративних користувачів.

Для розповсюдження розробки можуть бути використанні торгові та рекламні майданчики інтернет-магазинів з продажу програмного забезпечення та/або офіційний сайт додатку із встановленою середньою ціною на продукт.

Оскільки, на сьогодні питання захисту інформації є актуальним, а технології ЦВЗ успішно використовуються для вирішення завдань підтвердження авторського права по відношенню до цифрових файлів, контролю їх використання авторизованими користувачами та іншими особами, підтвердження справжності та надійності копій програмних засобів та мультимедіа об'єктів, що використовуються – цілком ймовірний високий попит на запропонований програмний продукт.

4.2 Прогнозування витрат на виконання наукової роботи та впровадження її результатів

Прогнозування витрат на виконання науково-дослідної, дослідно-конструкторської та конструкторсько-технологічної роботи складається з таких етапів:

1-й етап: розрахунок витрат, які безпосередньо стосуються виконавців даного розділу роботи;

2-й етап: розрахунок загальних витрат на виконання даної роботи;

3-й етап: прогнозування загальних витрат на виконання та впровадження результатів даної роботи.

Виконаємо розрахунок витрат, які безпосередньо стосуються виконавців даного розділу роботи, за такими статтями та формулами, приймаючи до уваги те, що для розробки інформаційної технології було залучено одного розробника програмного забезпечення.

1. Основна заробітна Z_o :

$$Z_o = \frac{M}{T_p} \cdot t, \text{ грн.} \quad (4.1)$$

де M – місячний посадовий оклад – 22 000 грн.;

T_p – число робочих днів в місяці; приблизно $T_p = 22$ дні;

t – число робочих днів роботи – 44 дні.

Таким чином:

$$Z_o = \frac{22\,000}{22} \cdot 44 = 44\,000 \text{ (грн.)}$$

Таблиця 4.5 – Витрати по заробітній платі

Найменування посади	Місячний посадовий оклад, грн.	Оплата за робочий день, грн.	Число днів роботи	Витрати на заробітну плату
Розробник	22 000	1 000	44	44 000
Всього				44 000

2. Додаткова заробітна плата Z_d працівників розраховується як 12% від основної заробітної плати:

$$Z_d = 0,12 \cdot 44\,000 = 5\,280 \text{ (грн.)} - \text{для розробника}$$

3. Нарахування на заробітну плату $H_{зп}$ розробника становить:

$$H_{зп} = (Z_o + Z_d) \cdot \frac{\beta}{100} \quad (4.2)$$

де Z_o – основна заробітна плата розробника;

Z_d – додаткова заробітна плата розробника;

β – ставка єдиного внеску на загальнообов'язкове державне соціальне страхування – 22%.

$$H_{зп} = (44\,000 + 5\,280) \cdot 0,22 = 10\,842 \text{ (грн.)}$$

4. Амортизація обладнання, комп'ютерів та приміщень, які використовувались під час виконання даного етапу роботи розраховуємо за формулою:

$$A = \frac{Ц \cdot Т}{12 \cdot Т_B} \quad (4.3)$$

де Ц – загальна балансова вартість обладнання, приміщення тощо, грн.;

Т – фактична тривалість використання, міс.;

Т_В – термін використання обладнання, приміщень тощо, роки.

Розробка програмного забезпечення ведеться орієнтовно 2 місяці.

Для офісного приміщення $A = \frac{100\,000 \cdot 2}{12 \cdot 7} = 2\,703$ грн.; для комп'ютера $A = \frac{16\,000 \cdot 2}{12 \cdot 3} = 889$ грн.; для монітора $A = \frac{7\,500 \cdot 2}{12 \cdot 2} = 625$ грн.

Розрахунки зведено до таблиці 4.6:

Таблиця 4.6 – Амортизаційні відрахування

Найменування	Балансова вартість (грн.)	Термін використання (років)	Фактична тривалість в-ня, (міс.)	Величина ам.. відрахувань, (грн.)
Офісне приміщення	100 000	7	2	2 703
Комп'ютер	16 000	3	2	889
Монітор	7 500	2	2	625
Всього				4 217

5. Витрати на комплектуючі К, що були використані під час виконання даного етапу роботи, розраховуються за формулою:

$$K = \sum_1^n N_i \cdot Ц_i \cdot K_i \text{ (грн.)} \quad (4.4)$$

де N_i – кількість комплектуючих i-го виду, шт.;

Ц_i – ціна комплектуючих i-го виду, грн.;

K_i – коефіцієнт транспортних витрат, K_i = (1,1...1,15);

n – кількість видів комплектуючих.

Таблиця 4.7 – Витрати на комплектуючі

Найменування комплектувальних	Кількість	Ціна за штуку, грн.	Сума, грн.	Примітка
Клавіатура	1	500 грн.	500 грн.	
Комп'ютерна мишка	1	300 грн.	300 грн.	
Колонки	2	400 грн.	400 грн.	
Всього:			$K_i = 1,2,3$	1 200 грн.

6. Витрати на силову електроенергію V_e розраховуються за формулою:

$$V_e = V \cdot П \cdot \Phi \cdot K_{\Pi} \text{ (грн.)} \quad (4.5)$$

де V – вартість 1 кВт-год. (на сьогодні для підприємців вартість 3,45грн./кВт-год);

Π – установлена потужність обладнання – 0,8 кВт;

Φ – фактична кількість годин роботи обладнання – 440 годин,

K_{Π} – коефіцієнт використання потужності.

$$V_e = 6,4 \cdot 0,8 \cdot 440 \cdot 0,14 = 315,4 \text{ (грн.)}$$

7. Інші витрати $V_{ін}$ охоплюють:

- витрати на управління організацією;
- оплату службових відряджень;
- витрати на утримання, ремонт та експлуатацію основних засобів;
- витрати на опалення, освітлення, водопостачання, охорону праці тощо.

Інші витрати $V_{ін}$ можна прийняти як 100% від суми основної заробітної плати розробника:

$$V_{ін} = 44\,000 \cdot 1 = 44\,000 \text{ (грн)}$$

Послуги Інтернету – 300 грн., канцтовари – 200 грн. Загальна вартість становить:

$$300 + 200 = 500 \text{ (грн.)}$$

8. Сума всіх попередніх статей витрат дає витрати на виконання даної частини роботи – В.

$$V = 44\,000 + 5\,280 + 10\,842 + 4\,217 + 1200 + 315,4 + 44\,000 + 500 \\ = 110\,357,4 \text{ (грн.)}$$

9. Проведемо прогнозування загальних витрат ЗВ на виконання та впровадження результатів виконаної наукової роботи. Прогнозування здійснюється за формулою:

$$ЗВ = \frac{V_{\text{заг}}}{\beta}, \text{ грн.} \quad (4.6)$$

де β – коефіцієнт, який характеризує етап (стадію) виконання даної роботи.

Так, якщо розробка знаходиться:

- на стадії науково-дослідних робіт, то $\beta \approx 0,1$;
- на стадії технічного проектування, то $\beta \approx 0,2$;
- на стадії розробки конструкторської документації, то $\beta \approx 0,3$;
- на стадії розробки технологій, то $\beta \approx 0,4$;
- на стадії розробки дослідного зразка, то $\beta \approx 0,5$;
- на стадії розробки промислового зразка, $\beta \approx 0,7$;
- на стадії впровадження, то $\beta \approx 0,9$.

$V_{\text{заг}}$ – загальна вартість всієї наукової роботи.

$$V = 110\,357,4 \text{ (грн.)} \\ ЗВ = \frac{110\,357,4}{0,7} = 157\,653,4 \text{ (грн.)}$$

Отже, прогноз загальних витрат ЗВ на виконання та впровадження результатів виконаної наукової роботи складає 157 653,4 (грн.)

4.3 Прогнозування комерційних ефектів від реалізації результатів розробки

У даному підрозділі проведемо кількісне прогнозування, яку вигоду, зиск можна отримати у майбутньому від впровадження результатів виконаної

наукової роботи.

В умовах ринку узагальнюючим позитивним результатом, що його отримує підприємство від впровадження результатів тієї чи іншої розробки, є збільшення чистого прибутку підприємства. Зростання чистого прибутку можна оцінити у теперішній вартості грошей.

Зростання чистого прибутку забезпечить інвестору надходження додаткових коштів, які дозволять покращити фінансові результати діяльності.

Виконання даної наукової роботи та впровадження її результатів складає приблизно 1 рік. Позитивні результати від впровадження розробки очікуються вже в перші місяці після впровадження.

Проведемо детальне прогнозування позитивних результатів та кількісне їх оцінювання по роках.

Обчислимо збільшення чистого прибутку підприємства $\Delta\Pi_i$ для кожного із років, протягом яких очікується отримання позитивних результатів від впровадження розробки, розраховується за формулою:

$$\Delta\Pi_i = \sum_1^n (\Delta\Pi_{\text{я}} \cdot N + \Pi_{\text{я}} \cdot \Delta N)_i \quad (4.7)$$

де $\Delta\Pi_{\text{я}}$ – покращення основного якісного показника від впровадження результатів розробки у даному році;

N – основний кількісний показник, який визначає діяльність підприємства у даному році до впровадження результатів наукової розробки;

ΔN – покращення основного кількісного показника діяльності підприємства від впровадження результатів розробки;

$\Pi_{\text{я}}$ – основний якісний показник, який визначає діяльність підприємства у даному році після впровадження результатів наукової розробки;

n – кількість років, протягом яких очікується отримання позитивних результатів від впровадження розробки.

Припустимо, що внаслідок впровадження результатів наукової розробки чистий прибуток підприємства збільшиться на 100 грн., а кількість одиниць (наданих прав на користування сервісом) реалізованої послуги збільшиться:

- протягом першого року – на 750 од.,
- протягом другого року – ще на 850 од.,
- протягом третього року – ще на 950 од.

Орієнтовно: реалізація продукції до впровадження результатів наукової розробки складала 1 шт., а прибуток, що його отримувало підприємство на одиницю продукції до впровадження результатів наукової розробки – 150 грн.

Потрібно спрогнозувати збільшення чистого прибутку підприємства від впровадження результатів наукової розробки у кожному році відносно базового.

Збільшення чистого прибутку підприємства $\Delta\Pi_1$ протягом першого року складе:

$$\Delta\Pi_1 = 150 \cdot 1 + (150 + 120) \cdot 750 = 170\,590,9 \text{ (грн.)}$$

Обчислимо збільшення чистого прибутку підприємства $\Delta\Pi_2$ протягом другого року:

$$\Delta\Pi_2 = 150 \cdot 1 + (150 + 100) \cdot (750 + 850) = 330\,702,5 \text{ (грн.)}$$

Збільшення чистого прибутку підприємства $\Delta\Pi_3$ протягом третього року становитиме:

$$\Delta\Pi_3 = 150 \cdot 1 + (150 + 100) \cdot (750 + 850 + 950) = 479\,075,9 \text{ (грн.)}$$

Отже, розрахунки показують, що відповідно прогнозуванню комерційний ефект від впровадження розробки виражається у значному збільшенні чистого прибутку підприємства.

4.4 Розрахунок ефективності вкладених інвестицій та періоду їх окупності

Основними показниками, які визначають доцільність фінансування наукової розробки певним інвестором, є абсолютна і відносна ефективність вкладених інвестицій та термін їх окупності.

Розрахунок ефективності вкладених інвестицій передбачає:

1-й крок. Розрахунок теперішньої вартості інвестицій PV , що вкладаються в наукову розробку.

Такою вартістю ми можемо вважати прогнозовану величину загальних витрат ZB на виконання та впровадження результатів НДДКР, тобто $ZB = PV = 157\,449,3$ (грн.)

2-й крок. Розрахуємо очікуване збільшення прибутку $\Delta\Pi_1$, що його отримає підприємство (організація) від впровадження результатів наукової розробки, для кожного із років, починаючи з першого року впровадження.

Таке збільшення прибутку також було розраховане нами раніше та становить:

$$\Delta\Pi_1 = 170\,590,9 \text{ (грн),}$$

$$\Delta\Pi_2 = 330\,702,5 \text{ (грн),}$$

$$\Delta\Pi_3 = 479\,075,9 \text{ (грн).}$$

3-й крок. Будуємо вісь часу, на якій відображаємо всі платежі (інвестиції та прибутки), що мають місце під час виконання науково-дослідної роботи та впровадження її результатів.

Рисунок 4.1 характеризує рух платежів (інвестицій та додаткових прибутків).

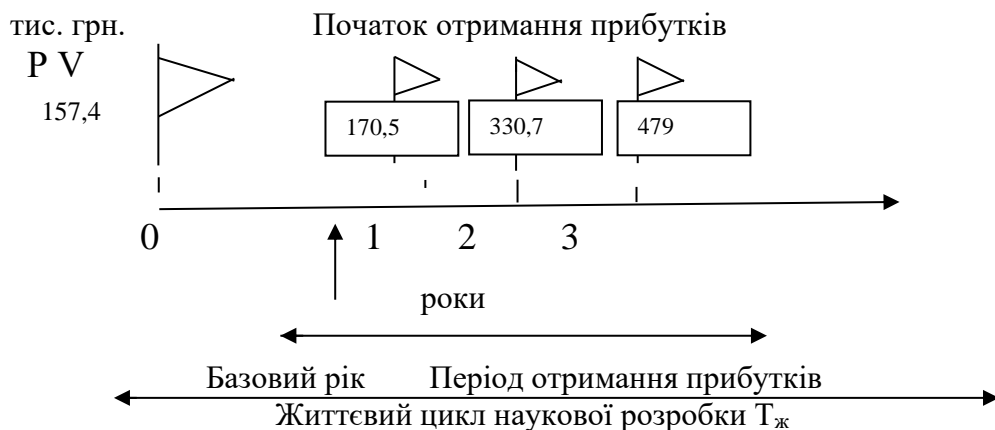


Рисунок 4.1 – Вісь часу з фіксацією платежів, що мають місце під час розробки та впровадження результатів НДДКР

4-й крок. Розрахуємо абсолютну ефективність вкладених інвестицій $E_{абс}$ за формулою:

$$E_{абс} = (ПП - PV), \text{ (грн.)} \quad (4.8)$$

де $ПП$ – приведена вартість всіх чистих прибутків, що їх отримає підприємство (організація) від реалізації результатів наукової розробки, грн.;

PV – теперішня вартість інвестицій $PV = 3B$, грн.

Приведена вартість всіх чистих прибутків $ПП$ розраховується за формулою:

$$ПП = \sum_1^T \frac{\Delta\Pi_i}{(1 + \tau)^t}, \text{ (грн)} \quad (4.9)$$

де $\Delta\Pi_i$ – збільшення чистого прибутку у кожному із років, протягом яких виявляються результати виконаної та впровадженої НДДКР, грн.;

T – період часу, протягом якого виявляються результати впровадженої НДДКР, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні – 0,1;

t – період часу (в роках) від моменту отримання чистого прибутку до точки «0»;

$$ПП = \frac{170\,590,9}{(1 + 0,1)^1} + \frac{330\,702,5}{(1 + 0,1)^2} + \frac{479\,075,9}{(1 + 0,1)^3} = 980\,369,3 \text{ (грн.)}$$

$$E_{абс} = 980\,369,3 - 157\,653,4 = 822\,715,9 \text{ (грн.)}$$

Оскільки $E_{абс} > 0$, результат від проведення наукових досліджень щодо розробки програмного продукту та їх впровадження принесе прибуток, тобто є доцільним, проте це ще не свідчить про те, що інвестор буде зацікавлений у фінансуванні даної програми.

5-й крок. Розрахуємо відносну (щорічну) ефективність вкладених в наукову розробку інвестицій E_B за формулою:

$$E_B = \sqrt[T_{ж}]{\left(1 + \frac{E_{абс}}{PV}\right) - 1} \quad (4.10)$$

де $E_{абс}$ – абсолютна ефективність вкладених інвестицій, грн.;

PV – теперішня вартість інвестицій $PV = 3B$, грн.

$T_{ж}$ – життєвий цикл наукової розробки, роки.

$$E_B = \sqrt[3]{1 + \frac{822\,715,9}{157\,653,4}} - 1 = \sqrt[3]{6,21} - 1 = 0,81 \text{ або } 81\%$$

Порівняємо E_B з мінімальною (бар'єрною) ставкою дисконтування τ_{min} , яка визначає ту мінімальну дохідність, нижче за яку інвестиції вкладатися не будуть.

Спрогнозуємо величину τ_{min} .

У загальному вигляді мінімальна (бар'єрна) ставка дисконтування τ_{min} визначається за формулою:

$$\tau_{min} = d + f \quad (4.11)$$

де d – середньозважена ставка за депозитними операціями в комерційних банках; $d = 0,2$;

f – показник, що характеризує ризикованість вкладень;

величина $f = 0,5$.

$$\tau_{min} = 0,2 + 0,5 = 0,7$$

Оскільки $E_B = 82\% > \tau_{min} = 70\%$, то у інвестора є потенційна зацікавленість у фінансуванні даної наукової розробки.

6-й крок. Розрахуємо термін окупності вкладених у реалізацію наукового проекту інвестицій $T_{ок}$ за формулою:

$$T_{ок} = \frac{1}{E_B}, \text{ рік} \quad (4.12)$$

$$T_{ок} = \frac{1}{0,81} = 1,2 \text{ (року)}$$

Оскільки термін окупності вкладених у реалізацію наукового проекту інвестицій менше трьох років ($T_{ок} < 3$ років), то фінансування нової розробки є доцільним.

4.5 Висновки до розділу

В даному розділі було виконано оцінювання комерційного потенціалу розробки програмного засобу на основі алгоритму для підвищення стійкості

вбудовуваного цифрового водяного знаку у потоковий відеозапис на основі вдосконаленого диференціального вбудовування енергії.

Проведено технологічний аудит з залученням трьох незалежних експертів. Визначено, що рівень комерційного потенціалу розробки вище середнього. Проведено порівняння з аналогом.

Згідно з проведеним оцінюванням нова розробка є якісною та конкурентоспроможною.

Рівень комерційного потенціалу розробки, становить 43,3 бала, що відповідає рівню «високий».

Згідно із розрахунками всіх статей витрат на виконання науково-дослідної, дослідно-конструкторської та конструкторсько-технологічної роботи загальні витрати на розробку складають 157 653,4 (грн.). Розрахована абсолютна ефективність вкладених інвестицій в сумі 822 715,9 (грн.) свідчить про отримання прибутку інвестором від комерціалізації програмного продукту.

Щорічна ефективність вкладених в наукову розробку інвестицій складає 81%, що вище за мінімальну бар'єрну ставку дисконтування, яка складає 70%. Це означає потенційну зацікавленість інвесторів у фінансуванні розробки.

Термін окупності вкладених у реалізацію проекту інвестицій становить 1,2 (року), що також свідчить про доцільність фінансування нової розробки.

Отже, проаналізувавши отримані економічні показники, можна вважати, що запропонована розробка програмного засобу має високий комерційний потенціал, а тому є доцільною для подальшого впровадження.

ВИСНОВОК

Отже, в даній магістерській кваліфікаційній роботі здійснюється дослідження та розробка за темою «Підвищення стійкості вбудовуваного цифрового водяного знаку у потоковий відеозапис на основі вдосконаленого диференціального вбудовування енергії (DEW)».

На даний момент стеганографічні алгоритми широко використовуються для впровадження прихованої інформації в мультимедіа файли з метою захисту авторських прав на продукцію. Одним із засобів реалізації даного процесу є застосування ЦВЗ. Питанню підвищення стійкості вбудовуваного цифрового водяного знаку у потоковий відеозапис була присвячена подальша робота.

У першому розділі було здійснено аналіз теоретичних матеріалів з обраної галузі, досліджено актуальність даної теми, особливості цифрового водяного знаку, методів його вбудовування, проаналізовано атаки на системи ЦВЗ, розроблено подальші задачі роботи.

У другому розділі було здійснено вдосконалення обраного алгоритму задля підвищення стійкості вбудовуваного цифрового водяного знаку у потоковий відеозапис.

Обраний алгоритм вбудовування цифрового водяного знаку, що базується на ідеї диференціального енергетичного водяного знаку, та є методом вбудовування ЦВЗ, заснований на вибіркового відкиданні частини високочастотних коефіцієнтів ДКП стислих зображень і відеозображень.

Враховуючи, що однією із проблем стійкості алгоритму до атак є вразливість високочастотних коефіцієнтів контейнера, в модифікованому варіанті алгоритму в даній роботі було враховано лише низькочастотні коефіцієнти дискретно-косинусного перетворення.

Для усунення недоліку суттєвої помітності візуальних змін контейнера застосовано метод сегментації Канні, який використовує багаторівневий обчислювальний підхід виявлення меж сегментів на зображенні.

В ході написання розділу було описано особливості обраних методів та засобів вдосконалення, розроблено алгоритм роботи онлайн-сервісу, який практично реалізовуватиме застосування вдосконаленого методу та обґрунтовано вибір обраних засобів програмування.

У третьому розділі роботи описано програмну розробку на основі вдосконаленого методу за рахунок використання наступних програмних засобів: платформи ASP.NET Core 3.1 та мови програмування C# (backend); фреймворку Angular та мови програмування Java Script (frontend). Також здійснено проектування користувацького інтерфейсу, наведено особливості програмної реалізації описано інструкцію користувача для роботи на сервісі, а також проведено аналіз результатів та тестування розробки.

Проаналізувавши результати наведеного тестування за показниками візуального впливу (SSIM, SNR, PSNR, AD, NAD, IF) та стійкості до атак, можемо зробити висновок, що в загальному застосування вдосконаленого методу дозволяє підвищити показники орієнтовно на 12%, зокрема усуває недолік візуальної помітності змін у відео та має підвищену стійкість до атак перекодування та стиснення. Цифровий водяний знак, що вбудовується у файл не здійснює на нього суттєвого впливу, а вбудовування даних у низькочастотні коефіцієнти дозволяє підвищити стійкість до атак.

У четвертому розділі роботи здійснено аналіз економічної доцільності розробки при практичному впровадженні. Наведені отримані економічні показники, свідчать, що запропонована розробка програмного засобу має високий комерційний потенціал, а тому є доцільною для подальшого впровадження.

Таким чином, в результаті виконання поставлених завдань та отриманих практичних результатів, можемо вважати, що під час виконання магістерської кваліфікаційної роботи було досягнуто її основну мету, а саме здійснено вдосконалення методу вбудовування цифрового водяного знаку на основі алгоритму DEW та практично реалізовано онлайн-сервіс із застосуванням вдосконаленого алгоритму.

ПЕРЕЛІК ПОСИЛАНЬ

1. Юдін О.К. Аналіз стеганографічних методів приховування інформаційних потоків у контейнери різних форматів / О. К. Юдін, Р. В. Зюбіна, О. В. Фролов // *Радиоэлектроника и информатика*. - 2015. - № 3. - С. 13-21.
2. Галамба М., Петрик В. Інформаційна безпека України: поняття, сутність та загрози. *Justinian*. веб-сайт. URL: <http://www.justinian.com.ua> (дата звернення: 14.10.2022).
3. Яремчук, Ю. Є., and В. В. Карпинець. "Аналіз стійкості стеганографічного перетворення до вбудовування цифрових водяних знаків у зображення." *Інформаційні технології та компютерна інженерія*. № 1: 212-217. (2007).
4. Захист авторських прав мультимедійних даних. *Legalactivity*: веб-сайт. URL: https://legalactivity.com.ua/index.php?option=com_content&view=article&id=1327%3A28092016-14&catid=161%3A2-1016&Itemid=201&lang= (дата звернення: 14.10.2022).
5. Д.О. Козак Розробка захищеного веб-додатку для обробки запитів користувачів. *Тези конференції*: веб-сайт. URL: <https://conferences.vntu.edu.ua/index.php/mn/mn2022/paper/viewFile/14254/12090> (дата звернення: 14.10.2022).
6. Захист авторського права. *Helpx*: веб-сайт. URL: <https://helpx.adobe.com/ua/photoshop/using/digimarc-copyright-protection.html> (дата звернення: 14.10.2022).
7. Стеганографія. *Навчальний посібник*. веб-сайт. URL: <http://tks.nau.edu.ua/wp-content/uploads/2016/05/Steganografiya.pdf> (дата звернення: 14.10.2022).
8. Хорошко В.О., Азаров О.Д., Шелест М.Є., Яремчук Ю.Є. Основи комп'ютерної стеганографії : Навчальний посібник для студентів і аспірантів. – Вінниця:ВДТУ, 2003. – 143 с.

9. Конахович Г.Ф. Комп'ютерна стеганографія. Теорія і практика / Г.Ф. Конахович, А. Ю. Пузиренко. – Київ: МК-Пресс, 2006. – 288 с.
10. Хорошко В.О., Азаров О.Д., Шелест М.Є., Яремчук Ю.Є. Основи комп'ютерної стеганографії: Навч. посіб. для студентів і аспірантів. – Вінниця: ВДТУ, 2003.
11. Kalker T. Considerations on watermarking security / T. Kalker //IEEE International Workshop on Multimedia Signal Processing. – Cannes (France), 2001. – P. 201–206.
12. Cayre F. Watermarking security: Theory and practice / F. Cayre, C. Fontaine, T. Furon //IEEE Trans. Signal Processing. – 2005. – Vol. 53. – P. 3976–3987.
13. Задирака В. К. Комп'ютерна стеганографія / В. К. Задирака, І. В. Серієнко, І. М. Коваленко, П. І. Андон та ін. // Стан та перспективи розвитку інформатики в Україні : монографія. – К. : Наук. думка, 2010. – С. 736–747.
14. Водяні знаки *Plumamazing*. веб-сайт. URL: <https://plumamazing.com/uk/watermark-faq/> (дата звернення: 14.10.2022).
15. Що таке файл MPEG. *Articles*: веб-сайт. URL: <https://ua.savtec.org/articles/howto/what-is-an-mpeg-file-and-how-do-i-open-one.html>. (дата звернення: 15.10.2022).
16. Навроцький Д.О. Методи комп'ютерної стеганографії / Навроцький Д.О. // Вісник Національного технічного університету України "КПІ" Серія – Радіотехніка. Радіоапаратобудування.-2007.-№35. – С.105-108.
17. Генне О. В. Основні положення стеганографії. *Посібник*: веб-сайт. URL: <http://www.citforum.ru/internet/securities/stegano.shtml>. (дата звернення: 24.10.2022).
18. Управління правами інтелектуальної власності для цифрових інновацій. *Eufordigital*: веб-сайт. URL: <https://eufordigital.eu/uk/managing-intellectual-property-rights-for-digital-innovation-meeting-a-key-challenge-for-innovative-smes/> (дата звернення 16.10.2022).
19. Сімейство форматів mpeg. *Studfile*: веб-сайт. URL: <https://studfile.net/preview/9024668/page:18/> (дата звернення 16.10.2022).

20. Яремчук, Ю. Є., and В. В. Карпинець. "Аналіз стійкості стеганографічного перетворення до вбудовування цифрових водяних знаків у зображення." *Інформаційні технології та компютерна інженерія.* № 1: 212-217. (2007).

21. Navrotskyi, D. O. (2007). *Методи комп'ютерної стеганографії.* *Visnyk NTUU KPI Seriii-Radiotekhnika Radioaparotobuduvannia*, (35), 105-108.

22. Юдін О.К., Зюбіна Р.В., Фролов О.В. Аналіз стеганографічних методів приховування інформаційних потоків у контейнери різних форматів. - *Pedram // 31st International Conference on Distributed Computing Systems Workshops.* Minneapolis, USA, 2011. P. 1-6.

23. *Secure spread spectrum watermarking for multimedia / I. J. Cox, J. Kilian, T. Leighton, T. G. Shamoan // Proceedings of the IEEE International Conference on Image Processing. – 1997. – Vol. 6. – P. 1673–1687*

24. *Attack Modelling: Towards a Second Generation Watermarking Benchmark / S. Voloshynovskiy, S. Pereira, V. Iquise, T. Pun. // Preprint. University of Geneva, 2001. – 58 p.*

25. *Collberg C. On the limits of software watermarking / C. Collberg, C. Thomborson // Technical report, University of Auckland, New Zealand, 1998.*

26. Романюк О.Н. Система стеганографічного захисту повідомлень / О.Н. Романюк, К.В. Огородник, В.В. Мартинюк // *Вісник Вінницького національного технічного університету.* - 2013. - № 1. - С. 126 – 129.

27. Аналіз стійкості стеганографічних систем в моделі пасивного противника / Задірака В. К., Кошкіна Н. В., Олексюк О. С. – *Штучний інте*, 2004.– 801–805 с.

28. Gutierrez-Cardenas J.M. *Steganography and data loss prevention: an overlooked risk? // International Journal of Security and Its Applications.* 2017. V. 11. N 4. P. 71–84.

29. *Digital Image Watermarking: An Overview. Researchgate: веб-сайт.* URL: <https://www.researchgate.net/publication/272747716> (дата звернення: 15.10.2022).

30. Provos N. Detecting Steganographic Content on the Internet / N. Provos, P. Honeyman // Proceeding of the 10 USENIX Security Symposium. – 2001. – P. 323–335.
31. Canny J.A Computational Approach to Edge Detection / J.Canny // IEEE Transactions on Pattern Analysis and Machine Intelligence, 1986. –pp. 679-698.
32. Secure spread spectrum watermarking for images, audio and video / I. J. Cox, J. Kilian, T. Leighton, T. G. Shamoan // Proceedings of the IEEE International Conference on Image Processing. – 1996. – P. 243–246.
33. Prewitt J.M.S. Object enhancement and extraction / J.M.S. Prewitt, B. Lipkin, A. Rosenfeld // Picture Processing and Psychopictorics. –Academic Press, 1970. – USA. –pp. 75-149.
34. Стеганографія *Стаття:* веб-сайт. URL: <https://www.wiki.uk-ua.nina.az/Стеганографія.html> (дата звернення: 14.10.2022).
35. Scharr H. An anisotropic diffusion algorithm with optimized rotation invariance / H. Scharr, J. Weickert // In DAGM. –Germany. –2000. –pp. 460–467.
36. Формати відео і їх характеристики *Ipkey:* веб-сайт. URL: <http://ipkey.com.ua/uk/faq/550-video-formats.html> (дата звернення: 15.10.2022).
37. ASP.NET Core 3.1. *Microsoft.* веб-сайт. URL: <https://dotnet.microsoft.com/en-us/download/dotnet/3.1> (дата звернення: 24.05.2022).
38. Вступ в C#. *programm.top:* веб-сайт. URL: <https://programm.top/uk/c-sharp/tutorial/introduction/> (дата звернення: 24.10.2022).
39. Angular. *Angular.* веб-сайт. URL: <https://angular.io> (дата звернення: 24.10.2022).
40. Вступ до мови Java. *myservername.com:* веб-сайт. URL: <https://uk.myservername.com/10-best-free-tftp-servers-download> (дата звернення: 24.10.2022).
41. .NET Framework *Microsoft.* веб-сайт. URL: <https://support.microsoft.com/microsoft-net-framework-9d23f658-3b97-68ab-d013-aa3c3e7495e0> (дата звернення: 24.10.2022).

42. Інститут кібернетики ім. В.М. Глушкова НАН України, 2005. –76-78
сWayner P. Disappearing Cryptography: Information Hiding: Steganography and Watermarking / Wayner Peter.– London: Elsever, 2009. – 440 p.

43. Весельська О. В., Зюбіна Р. В., Фролов О. В. Систематизація та класифікація наявних стеганографічних методів приховування інформації / Весельська О. В., Зюбіна Р. В., Фролов О. В. // Наукоємні технології № 2 (30), 2016. – С.188-194.

44. Gutierrez-Cardenas J.M. Steganography and data loss prevention: an overlooked risk? // International Journal of Security and Its Applications. 2017. V. 11. N 4. P. 71–84.

45. Nayak MR, Tudu B, Basu A, Sarkar SK (2015) On the implementation of a secured digital watermarking frame work. Inf Secur J Glob Perspect 24(1):1– 9.

46. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. – Вінниця : ВНТУ, 2021. – 42 с.

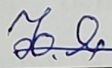
ДОДАТКИ

Додаток А. Технічне завдання

Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

ЗАТВЕРДЖУЮ

Голова секції “Управління інформаційною
безпекою” кафедри МБІС

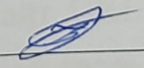
д.т.н., професор
 Юрій ЯРЕМЧУК
“ 24 ” вересня 2022 р.

ТЕХНІЧНЕ ЗАВДАННЯ

до магістерської кваліфікаційної роботи на тему:

Підвищення стійкості вбудовуваного цифрового водяного знаку у потоковий відеозапис на основі вдосконаленого диференціального вбудовування енергії (DEW)

08-72.МКР.005.00.000.ТЗ

Керівник магістерської кваліфікаційної роботи
к.т.н., доцент Василь Карпинець 

Вінниця – 2022 р.

1. Найменування та область застосування

Підвищення стійкості вбудовуваного цифрового водяного знаку у потоковий відеозапис на основі вдосконаленого диференціального вбудовування енергії (DEW). Область застосування: захист інтелектуальної власності у вигляді відеофайлів, що розміщені на онлайн-сервісі.

2. Підстава для розробки

Розробка виконується на основі наказу ректора ВНТУ №203 від 14. 09. 2022 р.

3. Мета та призначення розробки

3.1 Мета розробки: підвищення стійкості вбудовуваного цифрового водяного знаку у потоковий відеозапис на основі вдосконаленого диференціального вбудовування енергії (DEW) та програмна розробка онлайн-сервісу для практичної реалізації алгоритму.

3.2 Призначення: розроблений програмний засіб виконує захист інтелектуальної власності у вигляді відеофайлів, що розміщені на онлайн-сервісі.

4. Джерела розробки

4.1. Хорошко В.О., Азаров О.Д., Шелест М.Є., Яремчук Ю.Є. Основи комп'ютерної стеганографії : Навчальний посібник для студентів і аспірантів. – Вінниця: ВДТУ, 2003. – 143 с.

4.2 Конахович Г.Ф. Комп'ютерна стеганографія. Теорія і практика / Г.Ф. Конахович, А. Ю. Пузиренко. – Київ: МК-Пресс, 2006. – 288 с.

4.3 Kalker T. Considerations on watermarking security / T. Kalker //IEEE International Workshop on Multimedia Signal Processing. – Cannes (France), 2001. – P. 201–206.

4.4 Digital Image Watermarking: An Overview. *Researchgate*: веб-сайт. URL: <https://www.researchgate.net/publication/272747716> (дата звернення: 14.10.2022).

5. Вимоги до програми

5.1 Вимоги до функціональних характеристик:

5.1.1 Програмний засіб повинен мати зручний, легкий у використанні інтерфейс користувача;

5.1.2 Реалізація методу не повинна вимагати спеціальних ліцензійних програмних додатків;

5.1.3 Програмний засіб повинен виконувати процес автентифікації користувачів у системі.

5.2 Вимоги до надійності:

5.2.1 Програмний засіб повинен працювати без помилок, у випадку виникнення критичних ситуацій необхідно передбачити виведення відповідних повідомлень;

5.2.2 Бази даних повинні бути налаштовані на автоматичне створення резервних копій;

5.2.3 Програмний засіб повинен виконувати свої функції.

5.3 Вимоги до складу і параметрів технічних засобів: процесор – Pentium 1500 МГц і подібні до них; оперативна пам'ять – не менше 512 Мб; середовище функціонування – операційна система сімейство Windows; вимоги до техніки безпеки при роботі з програмою повинні відповідати існуючим вимогам та стандартам з техніки безпеки при користуванні комп'ютерною технікою.

6. Вимоги до програмної документації

6.1 Обов'язкова поетапна інструкція для майбутніх користувачів, наведена у пункті 3.3.

7. Вимоги до технічного захисту інформації

7.1 Необхідно забезпечити захист відеофайлів від несанкціонованого копіювання.

7.2 Неможливість отримання доступу незареєстрованих користувачів до онлайн-сервісу.

8. Техніко-економічні показники

8.1 Цінність результатів використання даного проекту повинна перевищувати витрати на його реалізацію.

8.2 Має бути реалізований таким чином, щоб підходити для використання широкого загалу.

9. Стадії та етапи розробки

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Початок	Закінчення
1	Визначення напрямку магістерської роботи, формулювання теми	15.09.2022	30.09.2022
2	Аналіз предметної області обраної теми	01.10.2022	10.10.2022
3	Апробація отриманих результатів	11.10.2022	15.10.2022
4	Розробка алгоритму роботи	16.10.2022	31.10.2022
5	Написання магістерської роботи на основі розробленої теми	01.11.2022	15.11.2022
6	Розробка економічної частини	15.11.2022	23.11.2022
7	Передзахист магістерської кваліфікаційної роботи	24.11.2022	25.11.2022
8	Виправлення, уточнення, корегування магістерської кваліфікаційної роботи	26.11.2022	15.11.2022
9	Захист магістерської кваліфікаційної роботи	19.12.2022	21.12.2022

10. Порядок контролю та прийому

10.1 До приймання магістерської кваліфікаційної роботи надається:

- ПЗ до магістерської кваліфікаційної роботи;
- програмний додаток;
- презентація;
- відзив керівника роботи;
- відзив опонента

Технічне завдання до виконання прийняв Д.О. Козак Д.О. Козак

Додаток Б. Лістинг HTML-сторінки

```

<div>
  <form #myForm="ngForm">
    <h5>Інформація про відео</h5>
    <div class='form-group'>
      <label for="Name" class="form-label">Ім'я</label>
      <input type='text' class="form-control" placeholder="Ім'я" id='name' name="name"
#name='ngModel'
      [(ngModel)]="videoAdd.name" minlength="3" required>
    </div>
    <!-- <div class='form-group'>

      <input type="file" class="form-control" id='photo' name="photo"
(change)="loadPhoto($event)" />
    </div> -->

    <div class="upload__section">
      <div class='form-group'>
        <label for="Name" class="form-label">Прев'ю до відео</label>
        <div class="input-container">
          <button #file mat-flat-button color="primary" style="border-radius: 8px;color:
#fff;background-color: #0d6efd;border-color: #0d6efd;height: 39px;width: 171px;">Оберіть
прев'ю...
          <input multiple (change)="onFileSelectedPhotos($event)" style="opacity: 0;
position:absolute; left:0px; top:0px; width:100%; height:100%;" type="file"/>
          </button>
          {{photos|json}}
        </div>
      </div>
    </div>
  </div>

  <!-- <div class='form-group'>

    <input type='file' class="form-control" id='video' name='video'
(change)="loadVideo($event)" />
  </div> -->
  <div class="upload__section">
    <div class='form-group'>
      <label for="video" class="form-label">Відео</label>
      <div class="input-container">

        <button #file mat-flat-button color="primary" style="border-radius: 8px;color:
#fff;background-color: #0d6efd;border-color: #0d6efd;height: 39px;width: 171px;">Оберіть
відео...
        <input multiple (change)="onFileSelectedVideos($event)" style="opacity: 0;
position:absolute; left:0px; top:0px; width:100%; height:100%;" type="file"/>
        </button>
      </div>
    </div>
  </div>

```

```

        {{videos|json}}
    </div>
</div>
<div class='form-group'>
    <label for="description" class="form-label">Опис</label>
    <input type='text' class="form-control" placeholder="Опис" id="description"
name="description"
    #description='ngModel' [(ngModel)]="videoAdd.description">
</div>
    <label for="Name" class="form-label"></label>
<label for="Name" class="form-label"></label>
<h5>Інформація для ЦВЗ (введіть текст або оберіть файл)</h5>
<div class='form-group'>
    <label for="Name" class="form-label">Текст</label>
    <input type='text' class="form-control" placeholder="Ім'я" id='name1'
name="name1"
        minlength="3" required>
</div>
<!-- <div class='form-group'>

    <input type="file" class="form-control" id='video1' name="photo"
(change)="loadPhoto($event)" />
</div> -->
<div class="upload__section">
    <div class='form-group'>
        <label for="Name" class="form-label">Файл</label>
        <div class="input-container">
            <button #file mat-flat-button color="primary" style="border-radius: 8px;color:
#fff;background-color: #0d6efd;border-color: #0d6efd;height: 39px;width: 171px;">Оберіть
файл...
                <input multiple (change)="onFileSelected1($event)" style="opacity: 0;
position:absolute; left:0px; top:0px; width:100%; height:100%;" type="file"/>
            </button>
            {{files|json}}
        </div>
    </div>
</div>
    <div class="form-group d-flex justify-content-center">
        <button class="btn btn-primary" (click)="addEnc()">Інформація для ЦВЗ</button>
    </div>
    <div class="form-group d-flex justify-content-center">
        <button class="btn btn-primary" [disabled]='myForm.invalid || this.photo == null ||
this.video == null'
            (click)="load()">Завантажити</button>
    </div>
</form>
</div>

```

Додаток В. Лістинг фрагментів frontend-частини

```
import { NgModule } from '@angular/core';
import { CommonModule } from '@angular/common';
import { LoginComponent } from './component/login.component';
import { RouterModule, Routes } from '@angular/router';
import { FormsModule } from '@angular/forms';
import { LoginService } from '../aCommon/services/login.service';
```

```
const routes: Routes =
[
  {
    path: "",
    component: LoginComponent
  }
];
```

```
@NgModule({
  declarations: [LoginComponent],
  imports: [
    CommonModule,
    FormsModule,
    RouterModule.forChild(routes)
  ],
  providers:[
    LoginService
  ]
})
export class LoginModule { }
```

```
import { NgModule } from '@angular/core';
import { CommonModule } from '@angular/common';
import { VideoWatchComponent } from './components/video-watch/video-
watch.component';
import { CommentaryService } from './services/commentary.service';
import { UserService } from 'src/app/aCommon/services/user.service';
import { VideoSelectionService } from 'src/app/aCommon/services/video-selection.service';
import { RouterModule, Routes } from '@angular/router';
import { VideoService } from 'src/app/aCommon/services/video.service';
```

```
const routes: Routes = [
  {
    path: "",
    component: VideoWatchComponent
  }
]
```



```

@NgModule({
  declarations: [VideoWatchComponent],
  imports: [
    CommonModule,
    RouterModule.forChild(routes)
  ],
  providers: [
    CommentaryService,
    VideoSelectionService,
    VideoService,
    UserService
  ]
})
export class VideoWatchModule { }

import { NgModule } from '@angular/core';
import { Routes, RouterModule } from '@angular/router';
import { CommonModule } from '@angular/common';
import { VideoMyComponent } from './components/video-my/video-my.component';
import { VideoLikedComponent } from './components/video-liked/video-liked.component';
import { VideoDislikedComponent } from './components/video-disliked/video-
disliked.component';
import { VideoAddComponent } from './components/video-add/video-add.component';
import { ProfileComponent } from './components/profile/profile.component';
import { FormsModule } from '@angular/forms';
import { VideoService } from '../aCommon/services/video.service';
import { VideoComponent } from './src/app/aCommon/components/video/video.component';
import { SharedModule } from 'src/app/aCommon/shared.module';

const itemRoutes: Routes = [
  {
    path: 'myvideo',
    component: VideoMyComponent
  },
  {
    path: 'likedvideo',
    component: VideoLikedComponent
  },
  {
    path: 'dislikedvideo',
    component: VideoDislikedComponent
  },
  {
    path: 'addvideo',
    component: VideoAddComponent
  },
],

```

```
    {
      path: "",
      redirectTo: 'myvideo'
    }
  ];

const router: Routes = [
  {
    path: ':id',
    component: ProfileComponent,
    children: itemRoutes
  },
  {
    path: "",
    component: ProfileComponent,
    children: itemRoutes
  }
];

@NgModule({
  declarations: [
    ProfileComponent,
    VideoAddComponent,
    VideoMyComponent,
    VideoLikedComponent,
    VideoDislikedComponent
  ],
  imports: [
    RouterModule.forChild(router),
    CommonModule,
    FormsModule,
    SharedModule
  ],
  providers: [
    VideoService
  ]
})
export class ProfileModule { }
```

Додаток Г. Інтерфейс онлайн-сервісу

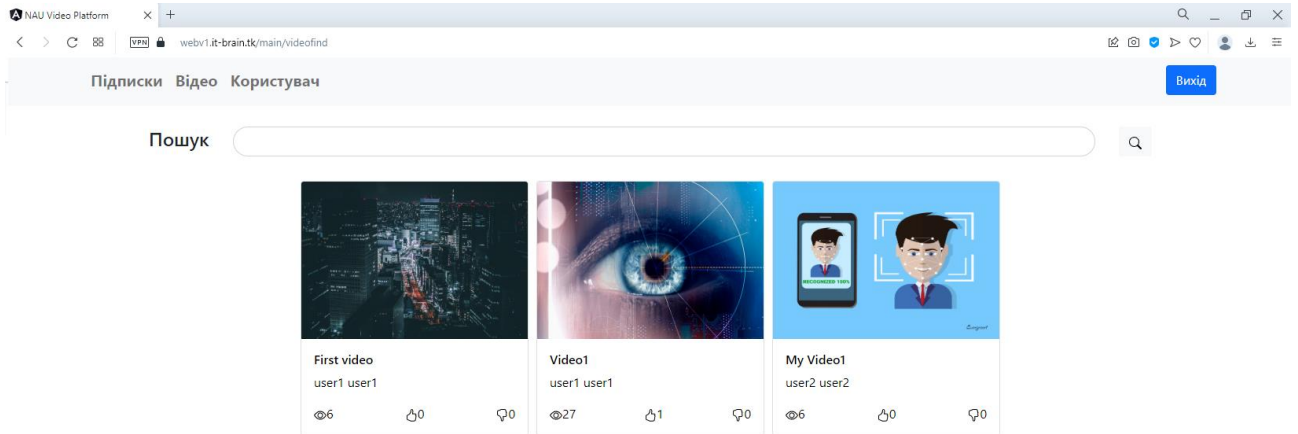


Рисунок 1 – Вигляд сторінки «Відео»

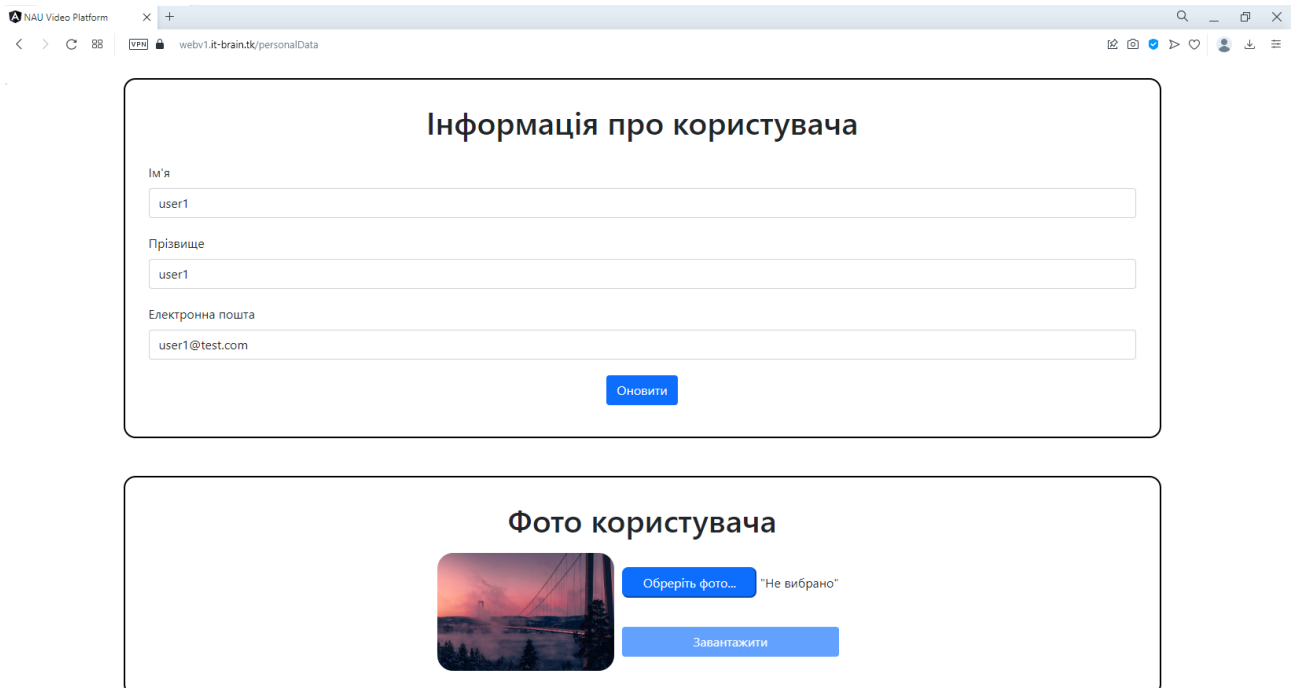


Рисунок 2 – Вигляд сторінки «Інформація про користувача»

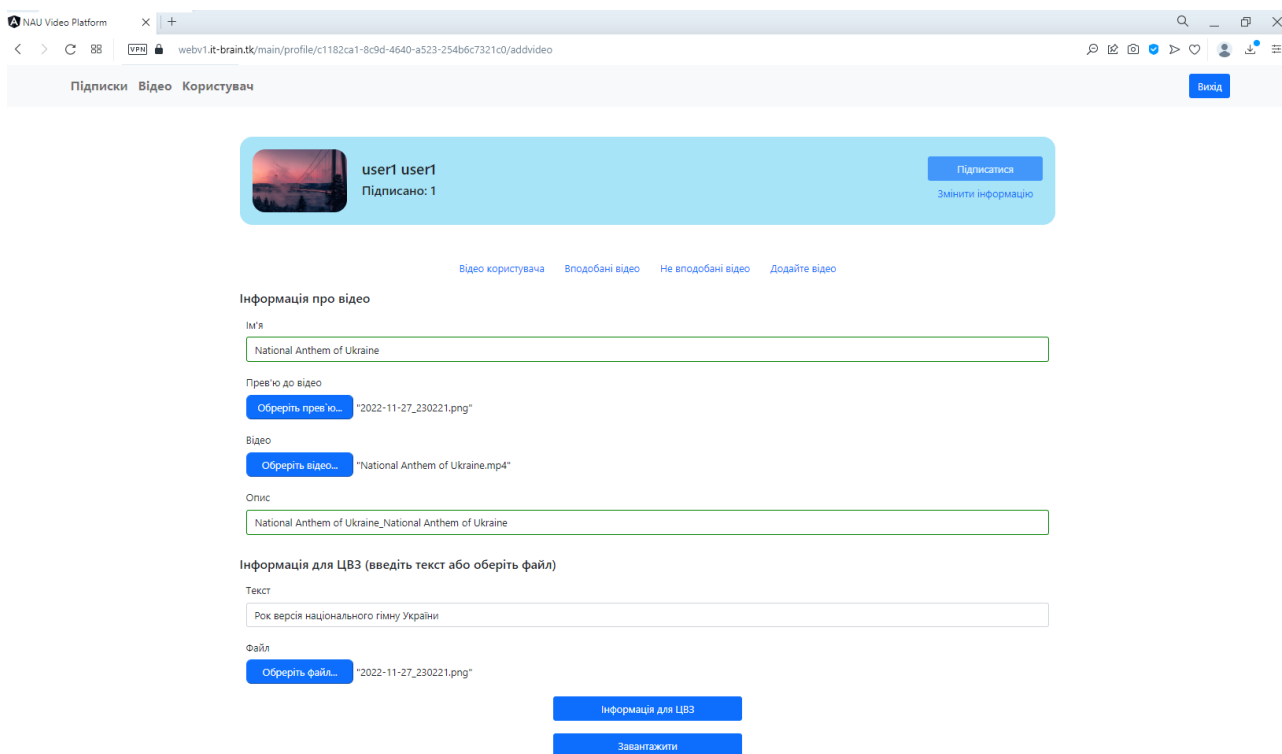


Рисунок 3 – Вигляд сторінки «Додати відео»

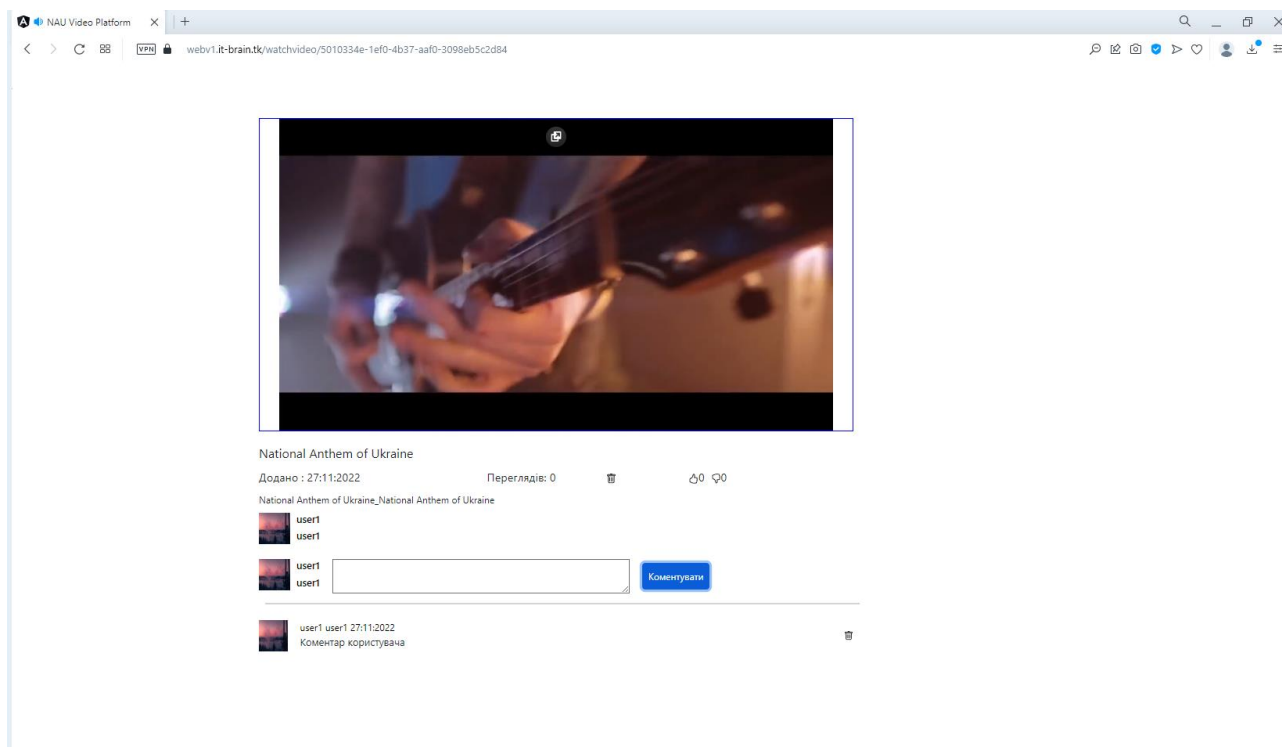


Рисунок 4 – Вигляд сторінки для перегляду відео

Додаток Д. Ілюстративний матеріал

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

Підвищення стійкості вбудовуваного цифрового водяного знаку у потоковий відеозапис на основі вдосконаленого диференціального вбудовування енергії (DEW)

ВИКОНАЛА: СТ. ГРУПИ УБ-21М КОЗАК Д.О.

КЕРІВНИК: К.Т.Н., ДОЦ. КАФ. МБІС КАРПІНЕЦЬ В.В.

Вступ

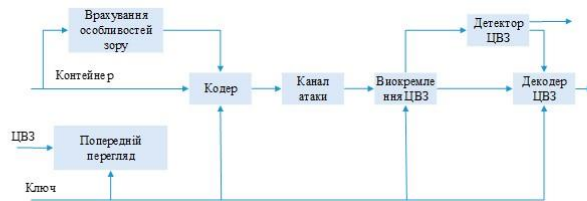
Актуальність. Технології цифрових водяних знаків (ЦВЗ) успішно використовуються для вирішення завдань підтвердження авторського права. Проте, із швидкими темпами розвитку технологій, зростає також потреба у постійному вдосконаленні методів вбудовування ЦВЗ, з метою уникнення зниження стійкості ЦВЗ до атак. Таким чином, дослідження у галузі підвищення стійкості методів ЦВЗ залишається наразі актуальним.

Метою роботи є підвищення стійкості вбудовуваного цифрового водяного знаку у потоковий відеозапис на основі вдосконаленого диференціального вбудовування енергії (DEW) та програмна розробка онлайн-сервісу для практичної реалізації алгоритму.

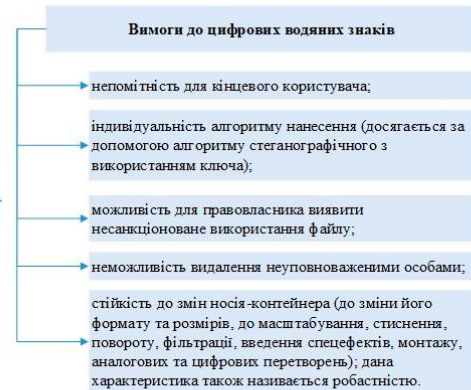
Практична цінність: розроблено програмний продукт, який реалізує вдосконалений метод вбудовування ЦВЗ у потокове відео з метою захисту авторського права.

Особливості цифрових водяних знаків та стегосистеми

Цифровий водяний знак (ЦВЗ) – спеціальна мітка, що непомітно впроваджується у зображення або інший сигнал з метою тим чи іншим чином контролювати його використання.



Завдання вбудовування та виділення повідомлень з іншої інформації виконує стегосистема, структура стегосистеми наведена на схемі.



Аналіз алгоритмів генерування та вбудовування ЦВЗ

Найбільш популярними стандартами кодування відео є MPEG-2 та MPEG-4.

Стеганографічні методи, що застосовуються для вбудовування інформації у відео, стиснуте за стандартом MPEG-2 повинні працювати в реальному часі.

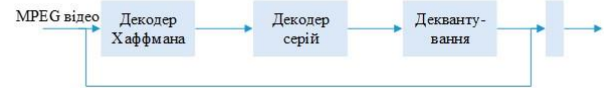
Проаналізовані аналоги (алгоритми Wu, Hartung, Langelaar-1, Langelaar-2) мають ряд недоліків, зокрема, високу обчислювальну складність та появу видимих спотворень.



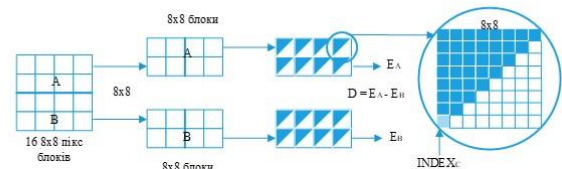
Вдосконалення алгоритму DEW для підвищення стійкості ЦВЗ

Враховуючи, що однією із проблем стійкості алгоритму до атак є вразливість височастотних коефіцієнтів контейнера, в модифікованому варіанті алгоритму в даній роботі врахуємо лише низькочастотні коефіцієнти дискретно-косинусного перетворення.

Для усунення недоліку суттєвої помітності візуальних змін контейнера застосуємо метод сегментації Канні, який використовує багаторівневий обчислювальний підхід виявлення меж сегментів на зображенні.



Алгоритм вбудовування ЦВЗ на основі DEW



Візуалізація вбудовування алгоритму DEW

Метод Канні

У більшості випадків, особливо при аналізі зашумлених зображень, цей метод має певні переваги перед іншими.

Регульованим параметром методу Канні є поріг чутливості: двоелементний вектор, у якому перший елемент нижній поріг, а другий елемент верхній поріг.

Перевагою методу Канні контурної сегментації зображень є використання морфологічної операції нарощування точок контуру в результаті вирішуються такі завдання, як деталізація зображення та яскравість/колірність сегментації.



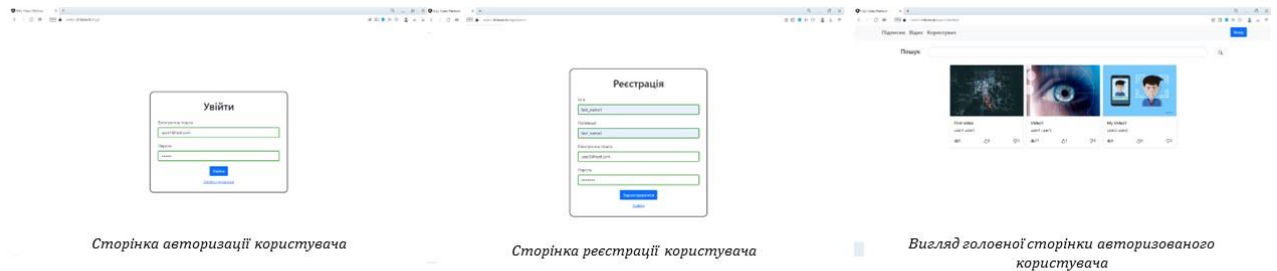
Програмні засоби реалізації

Виходячи із поставлених задач роботи програмну розробку здійснено за рахунок використання наступних програмних засобів:

- платформи ASP.NET Core 3.1 та мови програмування C# (backend);
- фреймворку Angular та мови програмування JavaScript (frontend).



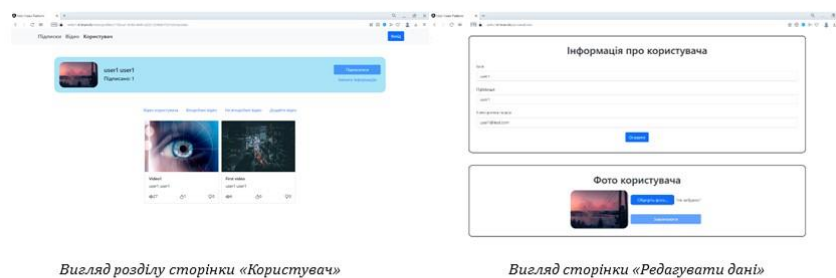
JavaScript



Сторінка авторизації користувача

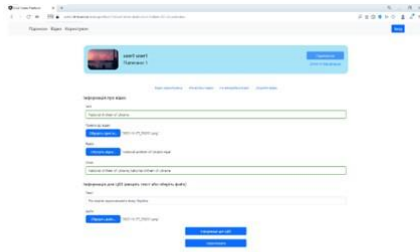
Сторінка реєстрації користувача

Вигляд головної сторінки авторизованого користувача



Вигляд розділу сторінки «Користувач»

Вигляд сторінки «Редагувати дані»



Вигляд сторінки «Додати відео»

✓ Фото завантажено.

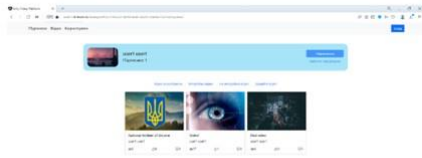
✓ Відео завантажено.

Сповіщення про успішне завантаження файлів

Підтвердіть дію на сторінці webv1.it-brain.tk
ЦВЗ успішно додано

OK

Повідомлення про успішне додавання ЦВЗ



Вигляд сторінки із завантаженням відео



Вигляд сторінки для перегляду відео

Підтвердіть дію на сторінці webv1.it-brain.tk
Ви бажаєте видалити цей коментар?

OK Отмена

Сповіщення про видалення коментаря

Підтвердіть дію на сторінці webv1.it-brain.tk
Ви хочете видалити це відео?

OK Отмена

Сповіщення про видалення відео

Дослідження змін контейнера

Показники зміни контейнера у досліді 1

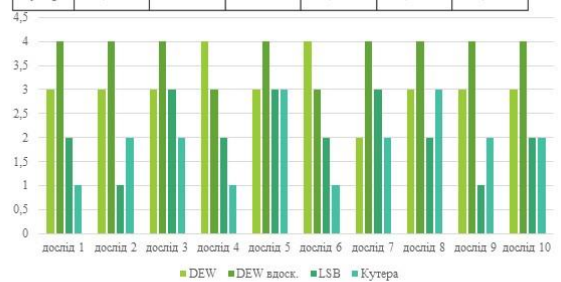
	SSIM	SNR	PSNR	AD	NAD	IF
DEW	0,723	85362	103681	0,9114	0,0181	99,8%
DEW удоск.	0,812	92548	126458	0,8754	0,0089	99,9%
LSB	0,652	65746	98535	0,4712	0,0082	99,8%
Кутера	0,689	36241	26854	0,6251	0,0095	98,7%

Показники зміни контейнера у досліді 2

	SSIM	SNR	PSNR	AD	NAD	IF
DEW	0,693	18204,3	127271	0,652	0,0068	99,99%
DEW вдоск.	0,931	24526,8	131185	0,855	0,009	99,99%
LSB	0,762	21852,6	118897	0,785	0,008	99,98%
Кутера	0,625	17233,6	100197	0,568	0,005	99,85%

Показники зміни контейнера у досліді 3

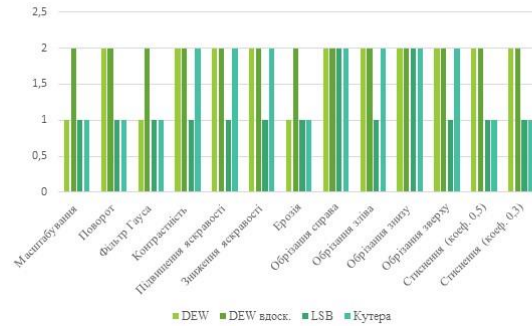
	SSIM	SNR	PSNR	AD	NAD	IF
DEW	0,893	856427	144825	0,894	0,007	99,98%
DEW вдоск.	0,925	945632	236587	0,987	0,008	99,99%
LSB	0,862	876325	128964	0,793	0,006	99,96%
Кутера	0,747	154369	5865	0,642	0,054	96,92%



Дослідження робастності стежоконтейнера

Розглянемо результати тестування, в якому проводилось дослідження робастності стежоконтейнера до певних видів змін (поворот контейнера на 90 градусів, стиснення в 2 рази, згладжування за допомогою функції Гауса, збільшення контрастності, збільшення та зменшення яскравості, ерозія зображення, обрізання 15% з різних сторін, стиснення з різними показниками якості).

Для представлення результатів тестування також було застосовано метод оцінок (у випадку переважної стійкості алгоритму до змін – надається значення 2, якщо алгоритм уразливий до певних змін – значення 1).



Дослідження стійкості ЦВЗ

	DEW	DEW (влос.)	LSB	Кутера
mpeg1				
mpeg2				
mpeg3				
Flv				
h.264				

Результати вилучення ЦВЗ після перекодування

	DEW	DEW (влос.)	LSB	Кутера
$q = 5$				
$q = 10$				

Результати вилучення ЦВЗ після стиснення

Висновки

В магістерській кваліфікаційній роботі було здійснено дослідження та розробку за темою «Підвищення стійкості вбудованого цифрового водяного знаку у потоковий відеозапис на основі вдосконаленого диференціального вбудовування енергії».

Проаналізувавши обраний базовий алгоритм DEW для вбудовування цифрового водяного знаку, здійснено удосконалення для усунення недоліків. Зокрема, в модифікованому варіанті алгоритму враховано лише низькочастотні коефіцієнти дискретно-косинусного перетворення. Для усунення недоліку суттєвої помітності візуальних змін контейнера застосовано метод сегментації Канні, який використовує багаторівневий обчислювальний підхід виявлення меж сегментів на зображенні.

В ході виконання роботи розроблено програмний продукт який реалізує вдосконалий метод вбудовування ЦВЗ у потокове відео з метою захисту авторського права.

Проаналізувавши результати тестування за показниками візуального впливу та стійкості до атак, можемо зробити висновок, що в загальному застосування вдосконаленого методу дозволяє підвищити показники орієнтовно на 12%, зокрема усуває недолік візуальної помітності змін у відео та має підвищену стійкість до атак перекодування та стиснення. Цифровий водяний знак, що вбудовується у файл не здійснює на нього суттєвого впливу, а вбудовування даних у низькочастотні коефіцієнти дозволяє підвищити стійкість до атак.

Отримані економічні показники, свідчать, що запропонована розробка програмного засобу має високий комерційний потенціал, а тому є доцільною для подальшого впровадження.

Таким чином, в результаті виконання поставлених завдань та отриманих практичних результатів, можемо вважати, що під час виконання магістерської кваліфікаційної роботи було досягнуто її основну мету.

**ДЯКУЮ
ЗА УВАГУ!**

Додаток Е. Протокол перевірки на антиплагіат

ПРОТОКОЛ ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Підвищення стійкості вбудованого цифрового водяного знаку у потоковий відеозапис на основі вдосконаленого диференціального вбудовування енергії (DEW)

Тип роботи: магістерська кваліфікаційна робота
(БДР, МКР)

Підрозділ: Кафедра менеджменту та безпеки інформаційних систем
Факультет менеджменту та інформаційної безпеки
(кафедра, факультет)

Показники звіту подібності Unicheck

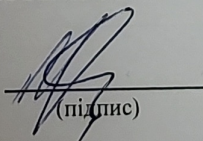
Оригінальність 98%

Схожість 2 %

Аналіз звіту подібності (відмітити потрібне):

1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.
2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.
3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

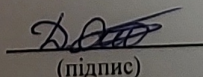
Особа, відповідальна за перевірку


(підпис)

Коваль Н.П.
(прізвище, ініціали)

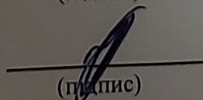
Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи


(підпис)

Козак Д.О.
(прізвище, ініціали)

Керівник роботи


(підпис)

Карпинець В.В.
(прізвище, ініціали)