МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук
«_____»_____ 2021 р.

На правах рукопису
УДК 003.26:004.056.55

ДИПЛОМНА РОБОТА

ВИПУСКНИКА ОСВІТНЬО СТУПЕНЯ «БАКАЛАВР»

Тема: Програмний модуль захисту графічної інформації цифровими водяними знаками

Автор: Г.І. Шило

Науковий керівник: к.т.н., доц. Н.К. Гулак

Нормоконтролер: к.т.н., доц. Н.К. Гулак

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки, комп'ютерної та програмної інженерії

Кафедра: Комп'ютеризованих систем захисту інформації

Освітній ступінь: «Бакалавр»

Спеціальність: 125 «Кібербезпека»

Освітньо-професійна програма: «Безпека інформаційно-комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ С.В. Казмірчук

«___» _____ 2021 р.

ЗАВДАННЯ

на виконання дипломної роботи

студентки Шило Ганни Ігорівни

1. Тема: *Програмний модуль модуль захисту графічної інформації цифровими водяними знаками*

затверджена наказом ректора від «26» квітня 2021 р. № 652/ст.

2. Термін виконання: з 10.05.2021 р. по 20.06.2021 р.

3. Вихідні дані: Методи стеганографії, алгоритми формування ЦВЗ, способи вставки ЦВЗ, програмне середовище MathLab.

4. Зміст пояснювальної записки: аналіз нормативно-правової бази України з захисту інтелектуальної власності та доцільність використання стенографічних методів для захисту графічної інформації; проаналізувати алгоритми формування ЦВЗ, властивості й життєвий цикл ЦВЗ; розробка і тестування програмного продукту на різних типах зображень та надання рекомендацій за тестуванням програмного продукту щодо використання ЦВЗ в різних типах зображень.

КАЛЕНДАРНИЙ ПЛАН

виконання дипломної роботи

№ п/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі	19.04.2021	Виконано
2.	Аналіз літературних джерел	26.04.2021	Виконано
3.	Обґрунтування рішення	30.04.2021	Виконано
4.	Збір інформації	10.05.2021	Виконано
5.	Аналіз нормативних документів з захисту інтелектуальної власності	12.05.2021	Виконано
6.	Аналіз стеганографічних методів	13.05.2021	Виконано
7.	Вибір методу стеганографічного захисту	14.05.2021	Виконано
8.	Складання алгоритму та програмного продукту. Реалізація методу у програмному середовищі MathLab.	17.05.2021	Виконано
9.	Апробація роботи	18.05.2021	Виконано
10.	Перевірка на антиплагіат	05.06.2021	Виконано
11.	Оформлення і друк пояснювальної записки	10.06.2021	Виконано
12.	Оформлення презентації	11.06.2021	Виконано
13.	Отримання рецензій	14.06.2021	Виконано

Дипломник Г.І. Шило

(підпис, дата)

Дипломний керівник Н.К. Гулак

(підпис, дата)

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатку, загальним обсягом робота складає 68 сторінок, має 49 рисунків, 2 таблиці, 3 сторінки додатків. Список використаних джерел містить 30 найменувань та займає 4 сторінки.

Метою роботи є розробка програмного продукту для різних типів зображення та надання рекомендацій щодо його використання на підставі побітового аналізу

Практична цінність роботи полягає в розробці і тестуванні програмного продукту для вставки цифрового водяного знаку задля забезпечення автентичності різних типів зображення, що дало можливість надати рекомендації щодо використання програмного продукту в цих типах.

Можливі напрями розвитку цієї роботи пов'язані з наданням можливості підвищення захисту ЦВЗ від спроб видалення.

Ключові слова: кібербезпека, стеганографія, цифровий водяний знак, авторське право, криптографія, найменший значущий біт, електронний цифровий підпис, мультімедіа.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ЦВЗ – Цифровий водяний знак

ЕЦП – Електронний цифровий підпис

LSB – Less Significant Bit

СБУ – Служба безпеки України

JPEG – Joint Photographic Experts Group

BMP – Bitmap Picture

ДКП – Дискретне косинусне перетворення

ЗСЛ – Зорова система людини

ВСТУП

Зберігання інформації у цифровому форматі являється найбільш визнаним способом зберігання інформації сучасності. Невід'ємну роль у житті сучасної людини відіграє мультимедійний простір. Ще не так давно для отримання будь-якої інформації люди звертались за допомогою до бібліотек та витрачали на це години, або навіть дні чи тижні, а в наші часи абиякий контент можна дістати за лічені секунди, для цього потрібно мати лише доступ до Інтернету. Втім, така доступність інформації також має свої наслідки. З кожним днем все більше авторів страждають від порушення авторського права та допомогою для них можуть служити стеганографічні та криптографічні способи захисту інформації. Суть різниці цих двох методів полягає в тому, що криптографічні методи захисту інформації маскують файлове наповнення, а стеганографічні методи приховують наявність конфіденційної інформації у файлі.

Оскільки криптографічні методи захисту інформації являються менш доступними у деяких куточках земного шару – це призвело до зросту зацікавленості у розвитку стеганографічних методів захисту інформації, що зберігається у цифровому форматі. Поштовхом для розробки методології ЦВЗ(цифрових водяних знаків) стала саме проблематика захищенності прав власності цифрової інформації.

Актуальність теми: Оскільки зберігання інформації у цифровому форматі являється найбільш визнаним способом зберігання інформації сучасності - невід'ємну роль у житті сучасної людини відіграє мультимедійний простір. З кожним днем все більше авторів страждають від порушення авторського права та допомогою для них можуть служити стеганографічні та криптографічні способи захисту інформації.

Метою роботи є розробка програмного продукту для різних типів зображення та надання рекомендацій щодо його використання на підставі побітового аналізу.

Основними **задачами роботи** є

- аналіз нормативно-правової бази України з захисту інтелектуальної власності та доцільність використання стенографічних методів для захисту графічної інформації;

- аналіз алгоритмів формування ЦВЗ, властивості й життєвий цикл ЦВЗ;

- розробка і тестування програмного продукту на різних типах зображень та надання рекомендацій за тестуванням програмного продукту щодо використання ЦВЗ в різних типах зображень.

Об'єкт дослідження: процес встановлення ЦВЗ в різні класи зображень

Предмет дослідження: алгоритми і методи вставки ЦВЗ в статичні зображення

Практична цінність *роботи полягає в розробці і тестуванні програмного продукту для вставки цифрового водяного знаку задля забезпечення автентичності різних типів зображення, що дало можливість надати рекомендації щодо використання програмного продукту в цих типах.*

Апробація роботи: Шило Г.І. Захист графічної інформації цифровими водяними знаками /Г.І. Шило // XIV міжнародна науково-практична конференція «Інтегровані інтелектуальні робото-технічні комплекси (ІІРТК-21)», 18-19 травня 2021 р. – Київ, Україна. – С.241-242.

РОЗДІЛ 1.АНАЛІТИЧНИЙ ОГЛЯД МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ОРИГІНАЛЬНОСТІ ГРАФІЧНИХ ЗОБРАЖЕНЬ

1.1 Аналіз нормативно-правової бази України з захисту інтелектуальної власності та авторських прав

Основними законами України пов’язаними з інтелектуальною власністю та захистом авторського права є: закон України “Про захист інформації в інформаційно-комунікаційних системах”, закон України “Про інформацію”, закон України “Про авторське і суміжні права”

Умови використання інформації в системі визначаються власником інформації, згідно закону України “Про захист інформації в інформаційно-комунікаційних системах”. Порядок доступу до цієї інформації у системі також визначає саме її власник.[20]

У статті 38 закону України “Про інформацію” інформація чітко визначена як об’єкт права власності громадянина. Там зазначається, що власник інформації має право використовувати інформацію будь-якими способами, якщо вони не порушують дії, передбачені законом. Інформація набуває права власності тільки при власноручному створенні, що також зазначено у цій статті.

Найбільш відповідним для детального опису є закон України “Про авторське та суміжні права”. У 8 статті є детальний опис і визначення об’єкта авторського права, яким являється автор твору. Всі види графічного або медіа зображення включені в перелік об’єктів авторського права.[19]

1.1.1 Закон України «Про авторське та суміжні права»

Стаття 11 закону “Про авторське і суміжні права” зазначає походження і використання авторського права:

« 1. Первинним суб’єктом, якому належить авторське право, є автор твору.

За відсутності доказів іншого автором твору вважається особа, зазначена як автор на оригіналі або примірнику твору (презумпція авторства).

Це положення застосовується також у разі опублікування твору під псевдонімом, який ідентифікує автора.

2. Авторське право на твір виникає внаслідок факту його створення. Для виникнення і здійснення авторського права не вимагається реєстрація твору чи будь-яке інше спеціальне його оформлення, а також виконання будь-яких інших формальностей.

3. Особа, яка має авторське право (автор твору чи будь-яка інша особа, якій на законних підставах передано авторське майнове право на цей твір), для сповіщення про свої права може використовувати знак охорони авторського права. Цей знак складається з таких елементів:

латинська літера "c", обведена колом, - (зображення знака не наводиться);

ім’я особи, яка має авторське право;

рік першої публікації твору.

Знак охорони авторського права проставляється на оригіналі і кожному примірнику твору.

4. Якщо твір опубліковано анонімно чи під псевдонімом (за винятком випадку, коли псевдонім однозначно ідентифікує автора), видавець твору (його ім’я чи назва мають бути зазначені на творі) вважається представником автора і має право захищати права останнього. Це положення діє до того часу, поки автор твору не розкриє своє ім’я і не заявить про своє авторство.

5 . Суб’єкт авторського права для засвідчення авторства (авторського права) на оприлюднений чи не оприлюднений твір, факту і дати опублікування твору чи договорів, які стосуються права автора на твір, у будь-який час протягом строку охорони авторського права може зареєструвати своє авторське право у відповідних державних реєстрах.

Державна реєстрація авторського права і договорів, які стосуються права автора на твір, здійснюється Установою відповідно до затвердженого Кабінетом

Міністрів України порядку. Установа складає і періодично видає каталоги всіх державних реєстрацій.

За підготовку Установою до державної реєстрації авторського права і договорів, які стосуються права автора на твір, сплачуються збори, розміри яких визначаються Кабінетом Міністрів України.

Про реєстрацію авторського права на твір Установою видається свідоцтво. За видачу свідоцтва сплачується державне мито, кошти від сплати якого перераховуються до Державного бюджету України. Розмір і порядок сплати державного мита за видачу свідоцтва визначаються законодавством.

Особа, яка володіє матеріальним об’єктом, в якому втілено (виражено) твір, не може перешкоджати особі, яка має авторське право, у його реєстрації.»[1]

Аналізуючи зміст наведених вище статей, можна зробити висновок, шо використання та публікування є правами автора зображення. Згідно розглянутим статтям, автор має право протидіяти будь-яким змінам свого зображення та відстоювати своє авторське право.

1.2 Порівняльний аналіз криптографічних та стеганографічних методів

Вирізняють два види захисту медіа-файлів: криптографія та стеганографія.

Криптографія представляє забезпечення цілісності та автентичності інформації математичними методами. Криптографія є однією з найстаріших наук та перші згадування датуються ще до народження Ісуса Христа, а приклади перших надійних криптосистем прийшли до нас ще із стародавнього Китаю. Криптографія найбільше прийшла до нагоди в стародавні часи у військовій справі, дипломатії та у сфері торгівлі.

Фундаментальним механізмом захисту інформації — є класичні алгоритми криптографічного шифрування.

Шифрування та дешифрування стали основною метою сучасної криптографії. Однак, криптографія використовується для розв’язання задач пов’язаних із забезпеченням захищеності систем захисту інформації, таких як

автентифікація користувачів, контроль цілісності інформації, незаперечність причетності до авторства чи до одержання документа або повідомлення.

Базисом криптографії є криптоалгоритми з ключем. Шифрування з використанням ключа являє собою способи кодування даних, значущою рисою котрих є обов'язкове забезпечення повної таємниці від третіх осіб.[2]

Методи сучасної криптографії виділені на рисунку 1.1:

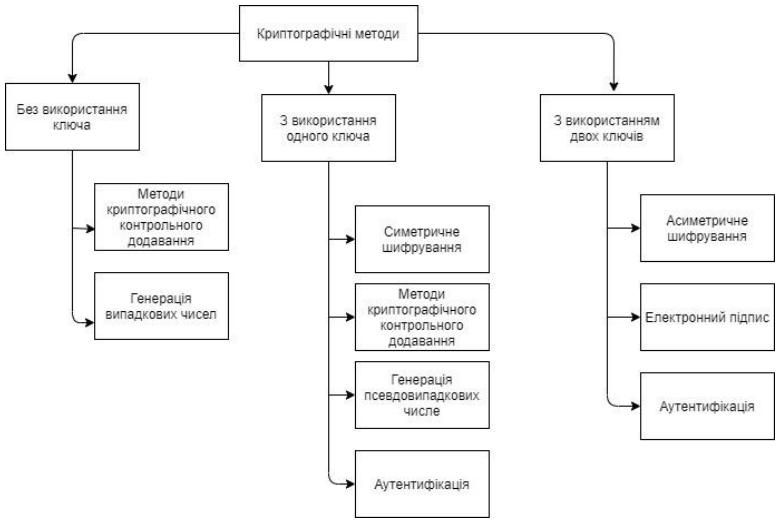

Рис. 1.1. Методи сучасної криптографії

Симетричні та асиметричні групи криптоалгоритмів - використовують шифрування з ключем. Симетричним називають шифрування, де використовуються ідентичні ключі для шифрування та дешифрування. В свою чергу, асиметричне шифрування представляє собою комплекс методів шифрування, у якому відкритий та секретний ключ, які не можуть бути взаємно обчислені, тобто відкритий ключ не може бути вирахуваний їх відкритого ключа.

На даний момент, симетричне та асиметричне шифрування являються основними криптографічними методами. Наприкінці XIX століття вийшла на світ робота О.Кергоффса "Військова криптографія", з чого і почалася історія криптографії із симетричними криптоалгоритмами. Початком криптографії з асиметричними криптоалгоритмами вважають роботи американських вчених В.Діффі та М.Хеллмана, які датуються 70-ми роками минулого століття.

Безумовно, ці два метода не ідеальні і мають свої переваги та недоліки. Асиметричні шифрування поступаються симетричним довжиною ключа та своєю

швидкодією. У випадках коли симетричні криптоалгоритми не можуть бути використані — на допомогу приходять асиметричні криптоалгоритми. Проте, ці два криптоалгоритми не піддаються порівнянню так як були створені для абсолютно різних цілей.

Для захисту графічних зображень найбільш дієвим та розповсюдженим є метод електронного цифрового підпису, тобто ЕЦП.

Електронний цифровий підпис являє собою точний аналог звичайного підпису ручкою на папері. Для надання документам юридичної сили, юридичні та фізичні особи можуть використовувати ЕЦП. Безпека використання ЕЦП забезпечується тим, що засоби, які використовуються для роботи з ЕЦП, проходять експертизу і сертифікацію в Департаменті спеціальних телекомунікаційних систем СБУ, яка гарантує неможливість злому та підробки ЕЦП.[3]

Переваги ЕЦП: безпека використання, юридична сила, забезпечення конфіденційності та цілісності.

Незважаючи на усі переваги, ЕЦП має свої недоліки. “Важливою проблемою всієї криптографії з відкритим ключем, в тому числі і систем ЕЦП, є управління відкритими ключами. Так як відкритий ключ доступний будь-якому користувачеві, то необхідний механізм перевірки того, що цей ключ належить саме своєму власникові. Необхідно забезпечити доступ будь-якого користувача до справжнього відкритого ключа будь-якого іншого користувача, захистити ці ключі від підміни зловмисником, а також організувати відгук ключа у разі його компрометації.”[3]

Стеганографія, у той самий час, направлена на приховування факту наявності приховуваної інформації. Саме на першій конференціх по приховуванню даних були винесені основні поняття стеганографії. Термін “стеганографія” можна розглядати як приховану передачу інформації, так і науку про непомітне та надійне приховування одних бітових послідовностей в інші.[12] На рисунку 1.2 зображені області застосування стеганографії

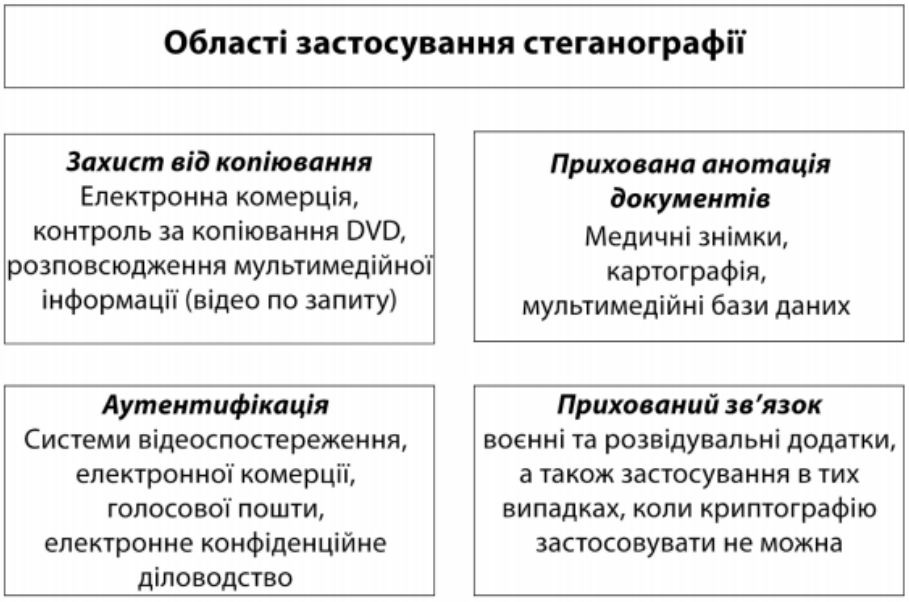

Рис. 1.2 Області застосування стеганографії

Виокремлюють такі напрями цифрової стеганографії:

1) Вставка інформації з метою приховування факту передачі інформації
2) Вставка ЦВЗ(цифрових водяних знаків)
3) Вставка номерів-ідентифікаторів
4) Вставка заголовків[2]

Більш детальна класифікація методів цифрової стеганографії представлена на рисунку 1.3

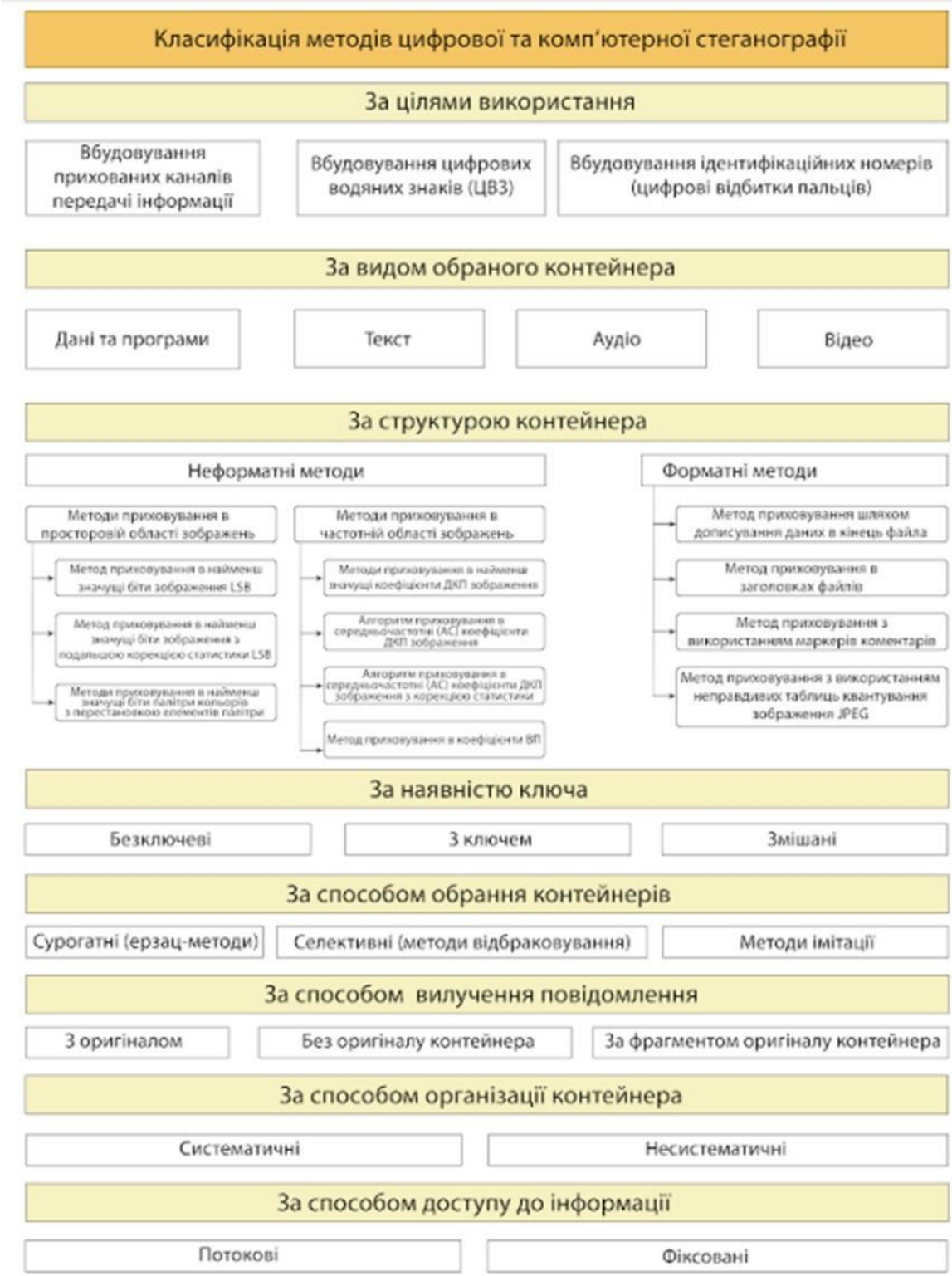

Рис. 1.3 Класифікація методів стеганографії

Зображення, аудіо дані та відео послідовності є одними із найпоширеніших типів контейнерів у комп’ютерній стеганографії сучасного часу. Поясненням цього є те, що всі перелічені види контейнеру мають шумову складову куди легко можна

приховати вбудоване повідомлення. Методи, що використовуються для приховування даних можна поділити по принципам, що лежать в їх основі. [4]

Форматними методами приховування називають методи, які формуються на особливостях формату зберігання графічних даних. Суть таких методів полягає у аналізі формату, з метою пошуку полів формату, зміна котрих при конкретних умовах не вплине на роботу з графічним зображенням.

Неформатними методами приховування називають методи які використовують самі дані, які є представленням зображення в цьому форматі, вони призводять до викривлення оригінального зображення, але являються більш стійкими до атак.

Отже, розглянемо класифікацію детальніше[3]

1) Неформатні методи приховування:
   - Неформатні методи приховування у JPEG:
   - Метод приховування у вхідних даних зображення
   - Метод приховування з використання квантових таблиць.
   - Метод використання хибних таблиць квантування.
   - Метод приховування у спектрі зображення після квантування
   - Методи приховування у графічних зображеннях з використанням палітри кольорів
   - Метод приховування з використанням наймолодших бітів даних зображення
   - Метод приховування з використанням молодших бітів елементів палітри.
   - Метод приховування, що основується на наявності однакових елементів у палітрі.
   - Метод приховування шляхом перестановки елементів палітри
2) Форматні методи :
   - Форматні методи приховування у файлах BMP
   - Форматні методи приховування у JPEG:
   - Додавання даних у кінці JPEG файлу;

- Метод приховування у непрямих даних
- Метод приховування використанням маркерів коментарів
- Метод приховування з використанням зменшеного зображення[3]

1.3 Висновки до розділу 1

Питання захисту авторського права є дуже розповсюдженою проблемою в наш час. Кількість веб-ресурсів зростає з кожним днем, що призводить до підвищення крадіжок графічної інформації.

У Законах України чітко окреслені права власника виготовленої цифрової інформації. Наприклад, закон України «Про авторське та суміжні права» прописує, що графічне зображення є об’єктом. Цей закон включає в себе список прав автора на володіння своїм унікальним контентом, його використання та розповсюдження.[22]

Криптографію та стеганографію виділяють як найефективніші способи захисту графічної інформації. Серед криптографічних методів найрозповсюдженішим методом захисту зображення є електронний цифровий підпис, але найбільш надійним його назвати складно, оскільки, в ньому використовується метод відкритого ключа. У той самий час, стеганографічні методи являються умовними лідерами у сфері забезпечення цілісності інформації, бо вони проявляють більш ефективну стійкість до спроб шахраїв, які намагаються привласнити чужий контент.

РОЗДІЛ 2.
АНАЛІЗ СТЕГАНОГРАФІЧНИХ МЕТОДІВ ЗАХИСТУ ГРАФІЧНОЇ ІНФОРМАЦІЇ

2.1 Формування ЦВЗ

Цифровий водяний знак(ЦВЗ) - методологія, яка допомагає захистити авторські права цифрових файлів. Найголовнішим плюсом ЦВЗ являється його непримітність. Частіше за усе, для захисту медіа-файлів, використовують видимі водяні знаки, якими виступають логотипи чи ідентифікатори автора.

Також існують системи захисту від копіювання унікального контенту та саме для них найкращим способом забезпечення захисту є невидимі цифрові водяні знаки. Такі системи застосовуються саме для захисту від копіювання даних зловмисниками та збереження авторського права для автора власного контенту. Присутність ЦВЗ облегшує процес доказу авторського права на цифрові медіа-файли.

В часи легкого доступу до інформації людство як ніколи потребує захисту своєї інтелектуальної власності, адже в Інтернеті за лічені хвилини можна знайти будь-яку інформацію. Автори унікального контенту, завдяки цифровим водним знакам, можуть почувати себе у безпеці. Так як, побачивши нелегальну копію свого витвору із вставленим ЦВЗ, навіть якщо вигляд цього контенту було змінено, авторство може бути легко встановлене.[6]

Стеганографічні системи цифрових водяних знаків діляться на три категорії: відкриті, напівзакриті та закриті.[8] Більш детальну класифікацію розглянемо на таблиці 2.1[9]

Таблиця 2.1

Види стегосистем ЦВЗ

Вид стегосистеми ЦВЗ		*Вхідні дані, що необхідні для детектування*		*Вихідні дані детектора*	
		Початковий сигнал	*Початковий ЦВЗ*	*Так\Ні*	*ЦВЗ*
Закриті	*Тип 1*	+	+	+	-
	Тип 2	+	-	-	+
Напівзакриті		-	+	+	-
Відкриті		-	-	-	+

Розглянемо систему вбудовування цифрового водяного знаку, коли він поданий у вигляді зображення X в зображення L – контейнер. H - заповнений контейнер, що підлягає під різноманітні перетворення для видобування ЦВЗ. Введемо означення K, Ji P для опису процесів вставки ЦВЗ в контейнер, перетворень заповненого контейнеру та видобування ЦВЗ.[10] Тоді схему стеганографічної системи можно представити у вигляді(рис. 2.2):

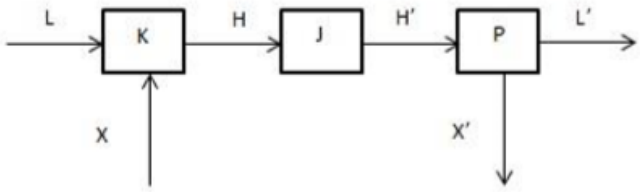

Рис. 2.2. Схема стеганографічної системи.

Використаний оператор J показує перетворення, наприклад, процес виводу зображення.

Візуально пустий та заповнений контейнер повинні бути схожими, що і є основною властивістю стегосистеми.

$$L \approx H$$

Підсумком до усього наведеного вище можна судити, що серед криптографічних методів захисту інформації найбільш ефективним є електронний цифровий підпис, а серед стеганографічних – цифровий водяний знак. Оскільки стеганографічні методи є більш стійкими та зручними у використанні у подальшому ми будемо розглядати саме їх.

2.2 Властивості та життєвий цикл ЦВЗ

Розглянемо структуру цифрової стегосистеми (рис 2.3)

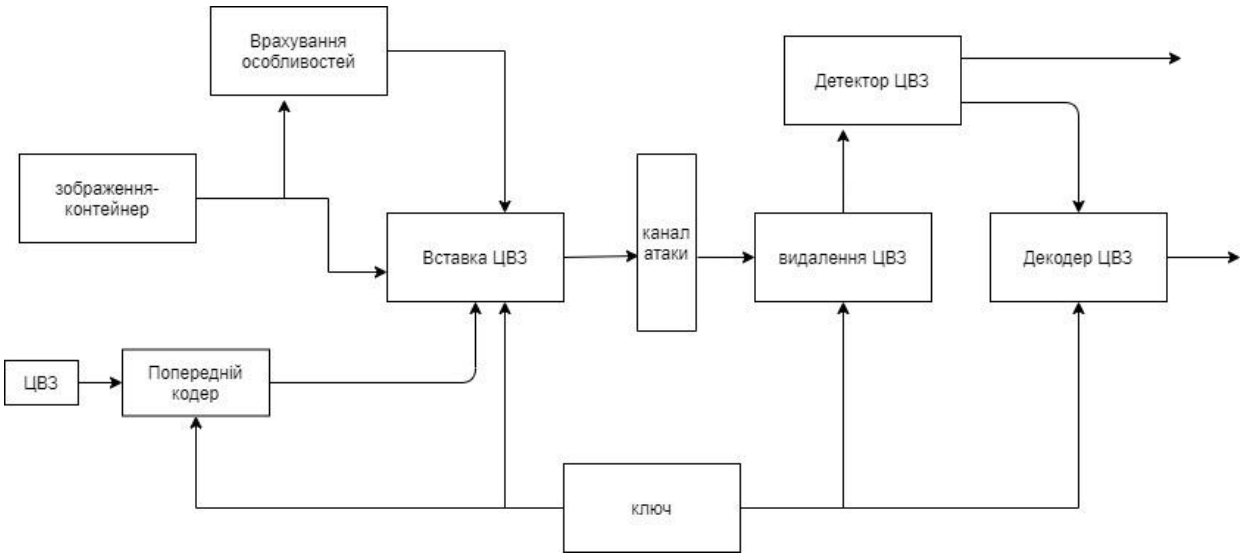

Рис.2.3 Структурна схема цифрової стегосистеми.

На схемі представлена стегонаграфічна система що виконує завдання вставки та читання водяного знаку із зображення-контейнера. Прилад вставки ЦВЗ створений для здійснення вставки приховуваного ЦВЗ в зображення контейнер. В стегосистемі вібувається злиття двох типів інформації. Це здійснюється для того щоб їх могли виявити два різних детектори. Детектором може бути як людське сприйняття так і система виявлення ЦВЗ. Ключ часто використовується для збільшення надійності і приховуваності інформації. Після цього водяний знак записується у контейнер. У стегодекодері відбувається виявлення ЦВЗ у захищеному ЦВЗ зображенні. [11]

Для розпізнавання ЦВЗ використовуються такі типи приладів:

1. Стегодекодери – прилади, що виділють цифрові водяні знаки
2. Стегодетектори – виявляють саме факт існування ЦВЗ

2.3 Способи вставки ЦВЗ

Серед способів приховування даних у зображеннях виділяються такі методи:

- Методи викривлень
- Широкосмугові методи
- Статистичні методи
- Структурні методи
- Методи приховування в частотній області
- Метод заміни в просторовій області

Надалі я буду розглядати саме метод заміни в просторовій області та метод приховування в частотній області, адже вони є найбільш розповсюдженими.

Від вичислень лінійних перетворень нас може позбавити саме алгоритм вставки даних в просторові області, що і є його основною перевагою, адже у цьому випадку вставка ЦВЗ забезпесується за допомогою маніпуляцій яскравістю або кольоровими компонентами.

Коротко розглянемо кожен метод у вигляді таблиці 2.2[15]:

Таблиця 2.2

Опис методів стеганографії

Назва методу	Прицип дії
Метод заміни найменшого значущого біта	Вбудовування інформації шляхом побітового запису в найменш значущі біти зображення. Переваги: швидкість(один крок-один біт), можливість запису великого обсягу інформації(до

	1\8 від обсягу контейнера при якісному приховуванні)

Продовження таблиці 2.2

1.	2.
Метод псевдовипадкової перестановки	Генератор псевдовипадкових чисел формує індекси j1...jM і зберігає К-й біт повідомлення в пікселі з індексом jK. Далі псевдовипадкова функція перестановки розміщує біти в повідомленні випадковим чином. Переваги: біти прихованого повідомлення розташовані по зображенню хаотично, що підвищує рівень надійності. Недоліки: якщо кількість біт приховуваного повідомлення не набагато менша за кількість молодших бітів зображення, то велика ймовірність перетину індексів як наслідок накладання одного біта повідомлення на інший
Метод псевдовипадкового	Полягає у випадковому розподілі

інтервалу	бітів секретної інформації по контейнеру. При цьому відстань між вбудованими бітами псевдовипадкова.

Продовження таблиці 2.2

1.	2.
Метод блокового приховування	Оригінал зображення розбивається на lM блоків, що не перетенається, Δi(1≤i≤ lM) довільної конфігурації, для кожного з яких формується біт парності b(Δi). У кожному блоці приховується один секретний біт Mi. Переваги: можливість модифікації пікселя зображення, зміна якого приводить до мінімальних змін у статистиці Недоліки: нестійкість до спотворень
Метод заміни палітри	Палітра з N кольорів представляється як список пар індексів (i,лi), що визначає

	відповідність між індексом і його вектором кольоровості. Кожному пікселю зображення відповідає певний індекс таблиці. так як заміна кольорів не впливає на загальний вигляд можливо приховування перестановкою палітри колоьорів. Продовження таблиці 2.2
Метод квантування зображення	Приховування інформації відбувається шляхом коригування розносного сигналу Δi. Сиегоключ є таблицею, яка кожному можливому значенню Δi ставить у відповідність певний біт. Щоб приховати нний біт повідомлення обчислюється різниця Δi. Якщо при цьому bi не відповідає серктеному біту, то значення Δi змінюється на найближчий Δj. Переваги: стійкість методу до стиснення Недоліки: ключ є обов'язковим, як і проведення коригування яскравості змінених біт.
Метод КуттераДжордана-Боссена	Секретний біт Mi вбудовується в зображення C={RGB} в канал

	синього кольору шляхом модифікації яскравості λx,y=0,29890* Rx,y+0,58662* Gx,y+0,11448* Bx,y Переваги: алгоритм стійкий до НЧ фільтрації, обрізання країв зображення та стиску(компресії)

Продовження таблиці 2.2

1.	2.
Метод ДармстедтераДелейгла-Квисквотера Макка	Інформація перетворюється до двійкового вектору, кожен біт якого вбудовується в окремий блок, розміром 8*8 пікселів. Блок попередньо розбивається на зони яскравості, відповідно до яких біт інформації записується в блок. Переваги: метод заснований на чутливому сприйнятті людини і стійкий до стиснення. Недоліки: громіздкість програмної реалізації, тривалість роботи програми.

Метод відносної заміни величин коефіцієнтів ДКП(Метод Коха і Жао)	Первинне зображення розбивається на блоки пікселів 8*8. Дискретне косинусне перетворення(ДКП) застосовується до кожного блоку. В результаті чого утворюються матриці коефіцієнтів ДКП. Кожен блок приховує один біт даних. Приховування починається з випадкового вибору блоку. Щоб приховати 0, щоб різниця абсолютних значень ДКП перевищувала певну величину >0. Продовження таблиці 2.2
Метод Бенгама-Мемона-Эо-Юнг	Удосконалення методу Коха і Жао шляхом накладення умов на вибір блоків(блоки не повинні мати різкі перепади яскравості або бути занадто монотонними) і збільшення числа коефіцієнтів ДКП з 2х до 3х. Переваги: зменшення похибки зчитування водяного знака. Недоліки: мала пропускна здатність.
Метод Фридрих	Зображення-контейнер конвертується в сигнал з

	нульовим математичним очікуванням і певним відхиленням, для того щоб НЧ-коефіцієнти ДКП потрапили в попередньо заданий діапазон. При обчисленні коефіцієнтів ДКП для модифікації відбираються тільки низькочастотні. Переваги: стійкість до стегоатак. Недоліки: складність читання ЦВЗ.

Як було наведено раніше, стеганосистеми можна розділити на відкриті, напівзакриті та закриті. Для створення свого програмного продутку, що зосереджений на аналізі залежності впливу параметрів вставки ЦВЗ на ступінь приховування інформації, я вирішила використовуввати відкриту стегосистему. На основі методу найменшого значущого біта(LSB) було розроблено програмний продукт[16].

Розглянемо переваги даного методу:

- Швидкість вставлення та вирізання водяного знаку
- Простота реалізації стегосистеми
- Висока пропускна здатність
- Метод може бути розширений викоритсанням двох і більше найменш значущий бітів, що збільшує пропускну здатність.[15]

Проте, статистично можна легко вичислити викоритсання цбого методу.[15]

Через те що цей метод є вразливим до стегоаналізу як ускладнюючий фактор додається білий Гауссовський шум. Інакше для якісного зчитування водяного знаку необхідно знати значення дисперсії шумової складової.

Алгоритм методу представлений на рисунку 2.4.

Рис 2.4. Алгоритм методу Найменшого значущого біт

2.4 Висновки до розділу 2

ЦВЗ (цифровий водяний знак) - це стеганографічний метод для захисту графічної інформації. ЦВЗ - це технологія, яка захищає авторські права на мультимедійні файли. Іншими словами, цифровий водяний знак буде служити власним підписом автора, що допоможе ідентифікувати та визначити власника контенту.

Методи введення ЦВЗ адаптовані до простору та частоти. Перевага алгоритму полягає в тому, що цифровий водний знак буде введено саме в області вхідного зображення, а це не потребує обчислення лінійних перетворень зображень.

Методом порівняльного аналізу методів приховування цифрового водяного знаку було обрано метод найменшого значущого біта. Метод був обраний для реалізації програмного продукту через свою легкість імплементації та швидкодію.

РОЗДІЛ 3.
ТЕСТУВАННЯ ПРОГРАМНОГО ПРОДУКТУ НА РІЗНИХ ТИПАХ ЗОБРАЖЕНЬ

3.1 Розробка програмного продукту

Опис алгоритму роботи програмного продукту:

1) Зчитування вхідного зображення з файлу

2) Отримання числа рядів та стовпців в матриці вхідного зображення

3) Видобування синього каналу, при умові наявності кольорового зображення.

4) Зчитування зображення для водяного знаку з файлу.

5) Отримання числа рядів і стовпців в зображенні для водяного знаку.

6) Зчитування синього каналу для кольорових зображень

7) Створення гістограми ЦВЗ для знаходження його порогового значення яскравості

8) Отримання розряду матриці де буде прихований водяний знак

9) Перевірка отриманого значення. Якщо значення не задовольняє умови програми – виведення повідомлення про помилку.

10) Вибір біта для запису водяного знаку

11) Вставка ЦВЗ в обрані біти

12) Додавання шуму для зображення з вставленим водяним знаком.

На рисунку 3.1 представлена блок-схема алгоритму. Повна схема представлена у додатку.

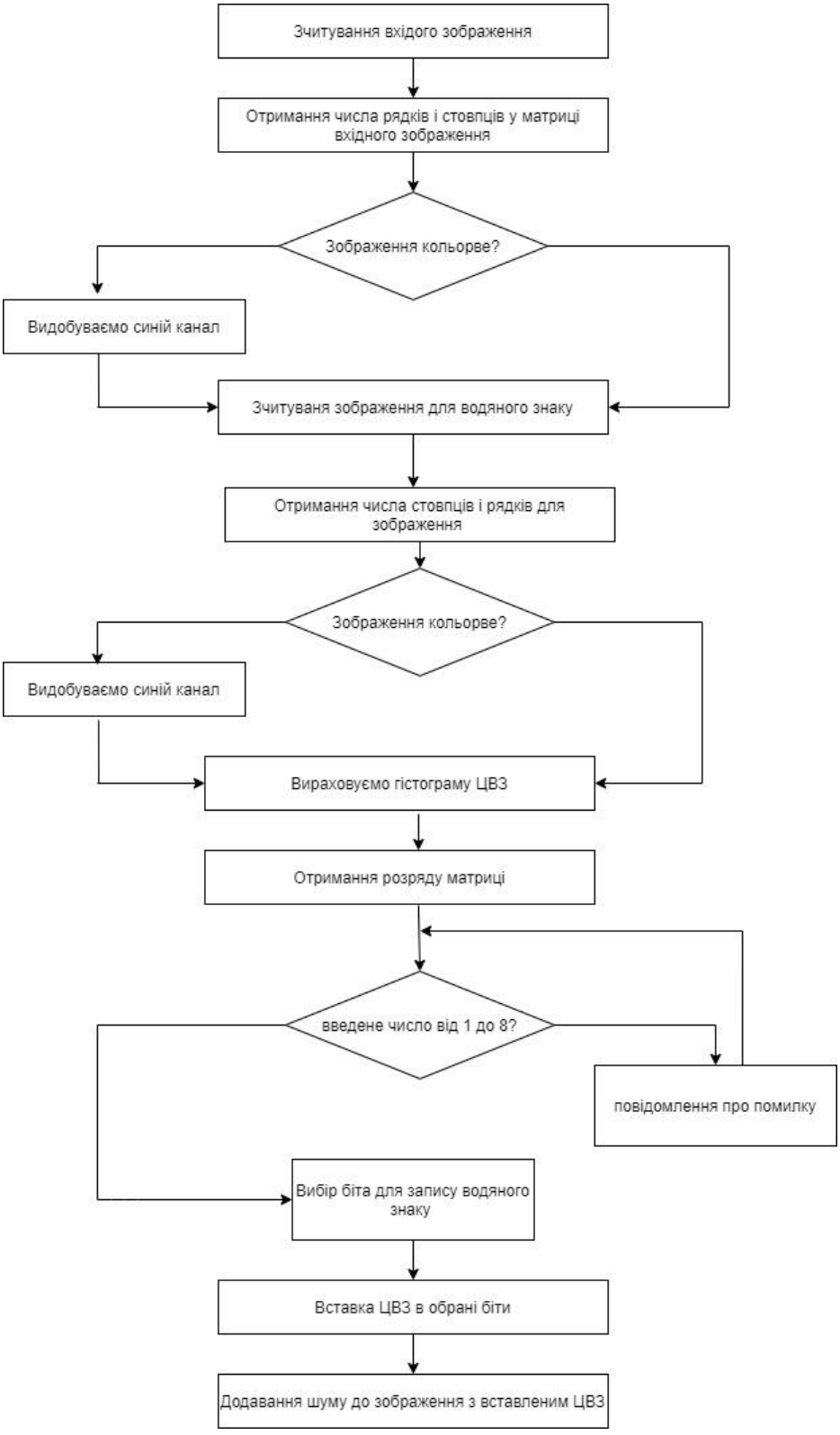

Рис 3.1. Блок схема роботи програми

3.1.1 Вибір синього каналу для вставки ЦВЗ

Для обрання найменшого значущого біта кольорового зображення, пропоную розглянути особливі ознаки зорової системи людини. Особливості низького рівня містять такі ознаки[22]:

- Низька чутливість ЗСЛ до малозначущої зміни яскравості зображень(від 3 до 5%)
- Низька чутливість ЗСЛ до малозначущої зміни контрасності зображень.
- Низька чутливість ЗСЛ до малозначущої зміни яскравості синьогокольору.

Співвідношення сприйняття:

$$Y= 0,3R + 0,6G + 0,1B$$

де R, G, B канали яскравості зображення одиничного пікселю.

Y – повнокольорова яскравість, що сприймається зоровою системою людини. Вона залежить від усіх каналів кольорності з різним коефіцієнтом. Підсумовуючи вищенаведені аргументи, я прийшла до висновку, що синій канал є найбільш ефективним для вставки цифрового водяного знаку.[23]

3.1.2 Розробка програмного коду

У ході роботи програмного продукту ми одержуємо таблицю з зображенням всіх перетворень, саме вхідне зображення та гістограму ЦВЗ. Приклад виводу програми, вікна помилки та вікна користувача пердставлені на рисунках 3.1, 3.2.

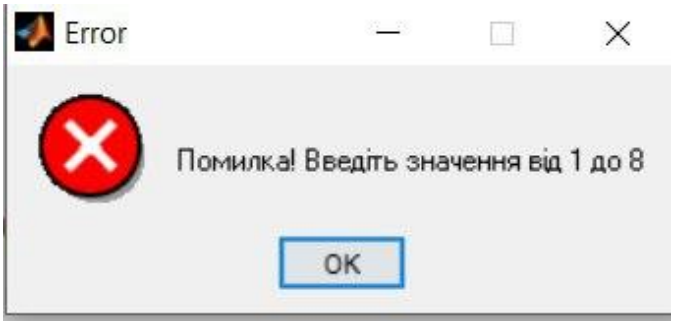

Рис 3.1. Вікно помилки

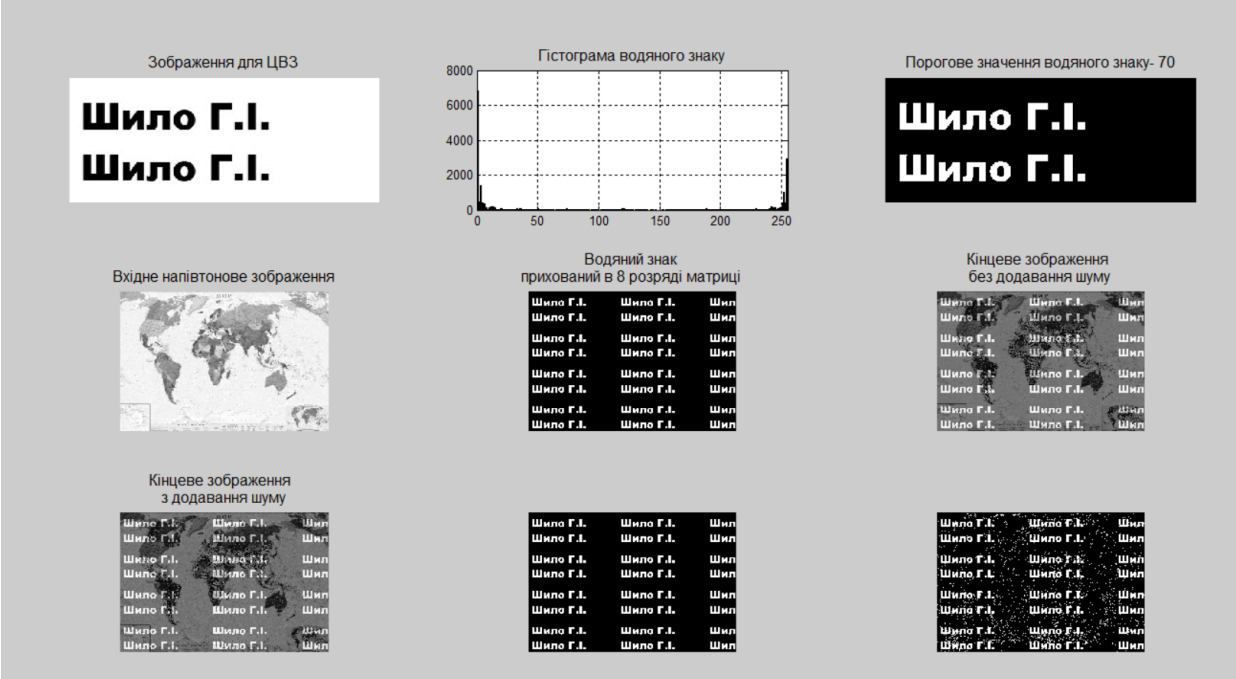

Рис. 3.2. Вікно користувача

3.2 Тестування програмного продукту

3.2.1 Побітовий аналіз вставки ЦВЗ в картографічне зображення

Для побітового аналізу вставки ЦВЗ я буду розглядати зображення, де ЦВЗ вставлений в 1-8 біт зображення. На рисунку 3.3 наведено вхідне зображення:

Рис 3.3 Вхідне зображення

Розглянемо побітову(з 8-го по 1-ший біт) вставку ЦВЗ у зображення на рисунках 3.4-3.11 відповідно:

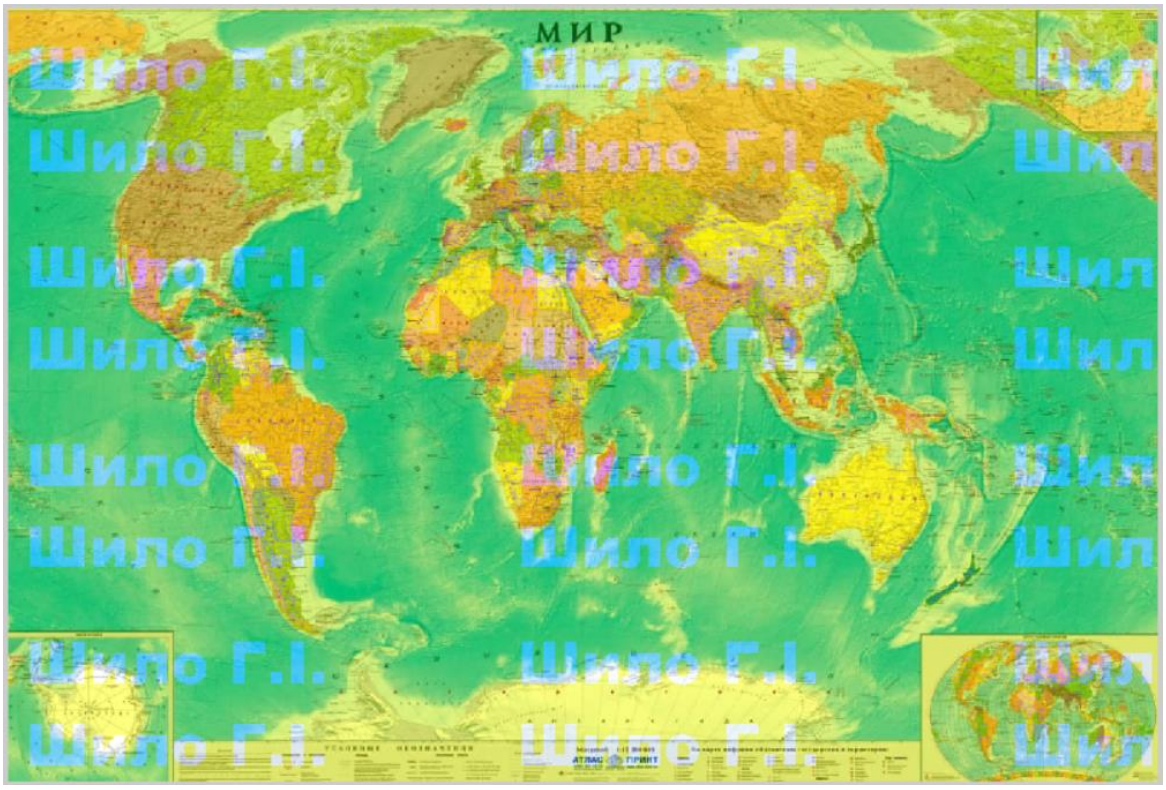

Рис.3.4 Зображення з прихованим ЦВЗ у 8-ому біті

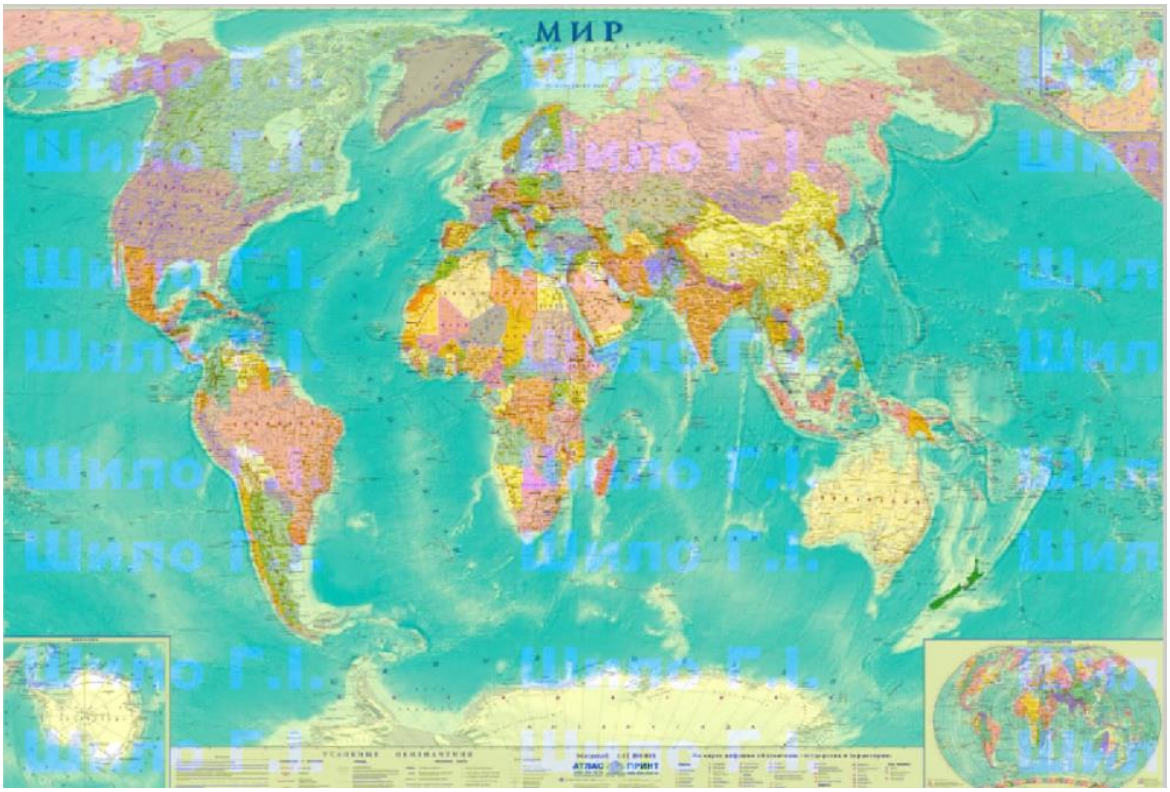

Рис.3.5 Зображення з прихованим ЦВЗ у 7-ому біті

Рис.3.6 Зображення з прихованим ЦВЗ у 6-ому біті

Рис.3.7 Зображення з прихованим ЦВЗ у 5-ому біті

Рис.3.8 Зображення з прихованим ЦВЗ у 4-ому біті

Рис.3.9 Зображення з прихованим ЦВЗ у 3-ому біті

Рис.3.10 Зображення з прихованим ЦВЗ у 2-ому біті

Рис.3.11 Зображення з прихованим ЦВЗ у 1-ому біті

На основі побітового аналізу даного картографічного зображення можемо виявити таку закономірність: зі зменшенням значення біта, яке використовується для вставки цифрового водяного знаку – збільшується непомітність ЦВЗ для людського ока. Якщо розглядати приклади більш детально, ми можемо побачити, що при вставці ЦВЗ у 6-ий біт, не беручи до уваги деформацію кольорів, сам водяний знак залишається непомітним, а при вставці ЦВЗ у 4-ий біт – різниці з вхідним зображенням і зовсім немає.

Виходячи з цього, можемо зробити висновок, що для картографічних типів зображення найефективнішими бітами для приховування ЦВЗ – будть біти 8-6, це забезпечить гарантований захист унікального контенту.

3.2.2 Побітовий аналіз вставки ЦВЗ в фотографічне зображення

Різницею між картографічними та фотографічними зображеннями можна назвати – кількість деталізацій та кольорів. Отже, розглянемо наш побітовий аналіз. Вхідну фотографію можемо побачити на рисунку 3.12 :

Рис. 3.12 Вхідне фотографічне зображення

Розглянемо результати вставки ЦВЗ у 8-1 біти фотографії. (рис. 3.13-3.20)

Рис.3.13 Зображення з прихованим ЦВЗ у 8-ому біті

Рис.3.14 Зображення з прихованим ЦВЗ у 7-ому біті

Рис. 3.15 Зображення з прихованим ЦВЗ у 6-ому біті

Рис. 3.16 Зображення з прихованим ЦВЗ у 5-ому біті

Рис. 3.17 Зображення з прихованим ЦВЗ у 4-ому біті

Рис.3.18 Зображення з прихованим ЦВЗ у 3-ому біті

Рис.3.19 Зображення з прихованим ЦВЗ у 2-ому біті

Рис. 3.20 Зображення з прихованим ЦВЗ у 1-ому біті

Отже, завдяки побітовому аналізу фотографічного зображення, можемо зробити висновок, що найвдалішим бітом для вставки ЦВЗ являється четвертий біт, адже викривлення кольорів майже непомітне, так само як і ЦВЗ.

3.2.3 Побітовий аналіз вставки ЦВЗ в схематичне зображення

Вхідне зображення представлено на рисунку 3.21:

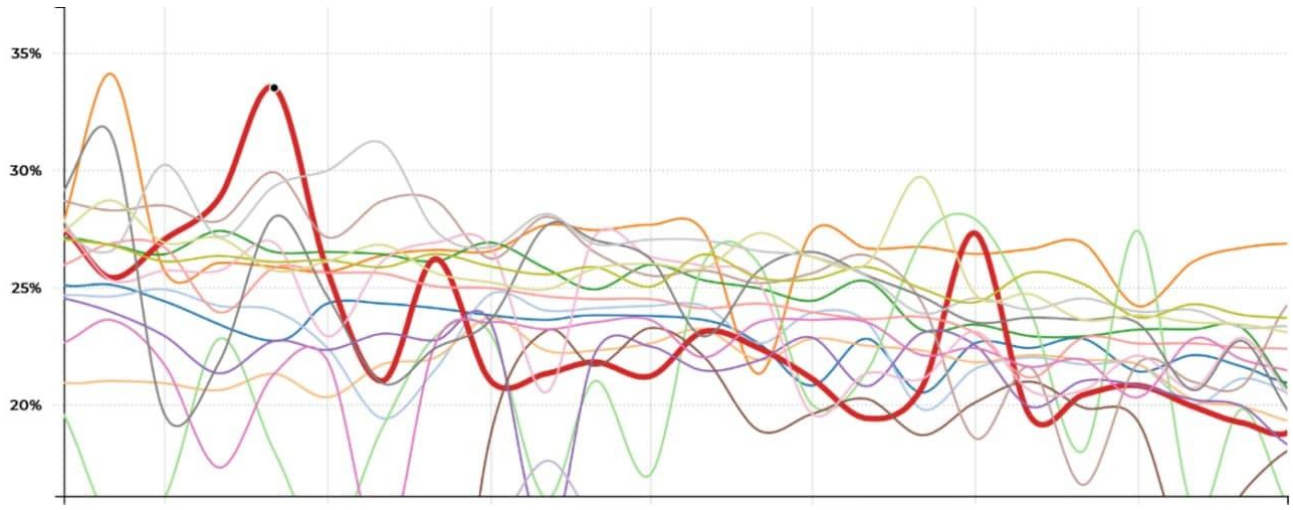

Рис.3.21 Вхідне зображення

Розглянемо результати вставки ЦВЗ у 8-1 біти фотографії. (рис. 3.22-3.29)

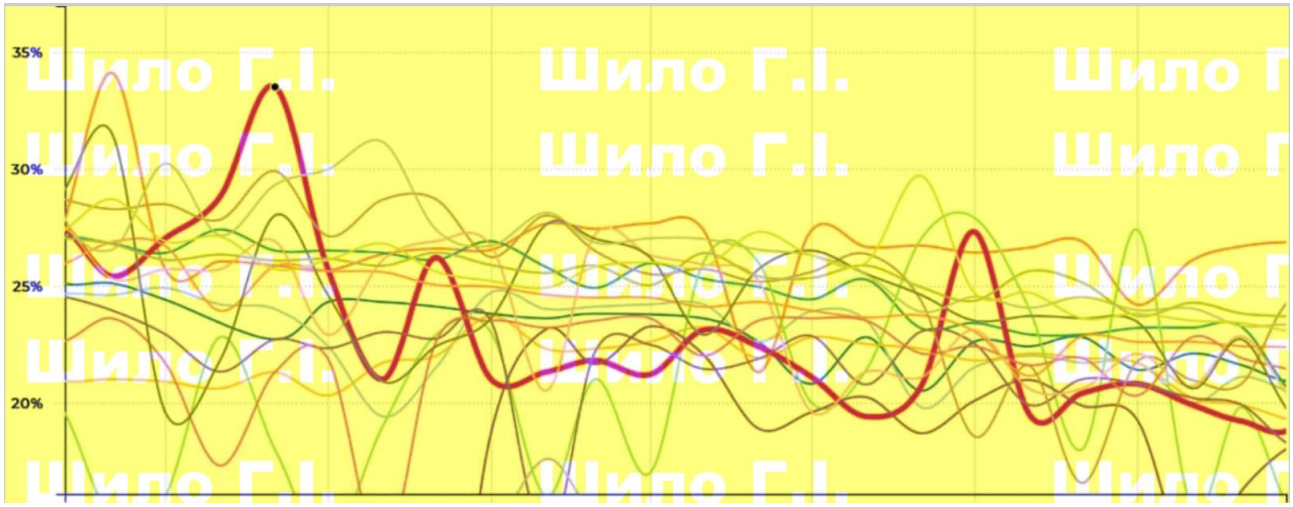

Рис.3.22 Зображення з прихованим ЦВЗ у 8-ому біті

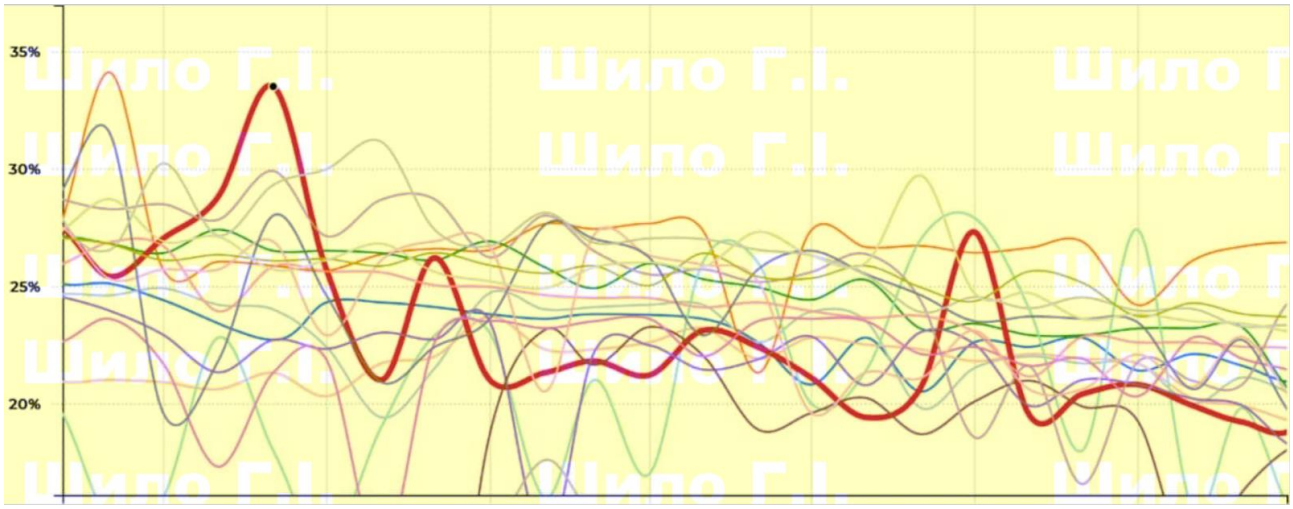

Рис.3.23 Зображення з прихованим ЦВЗ у 7-ому біті

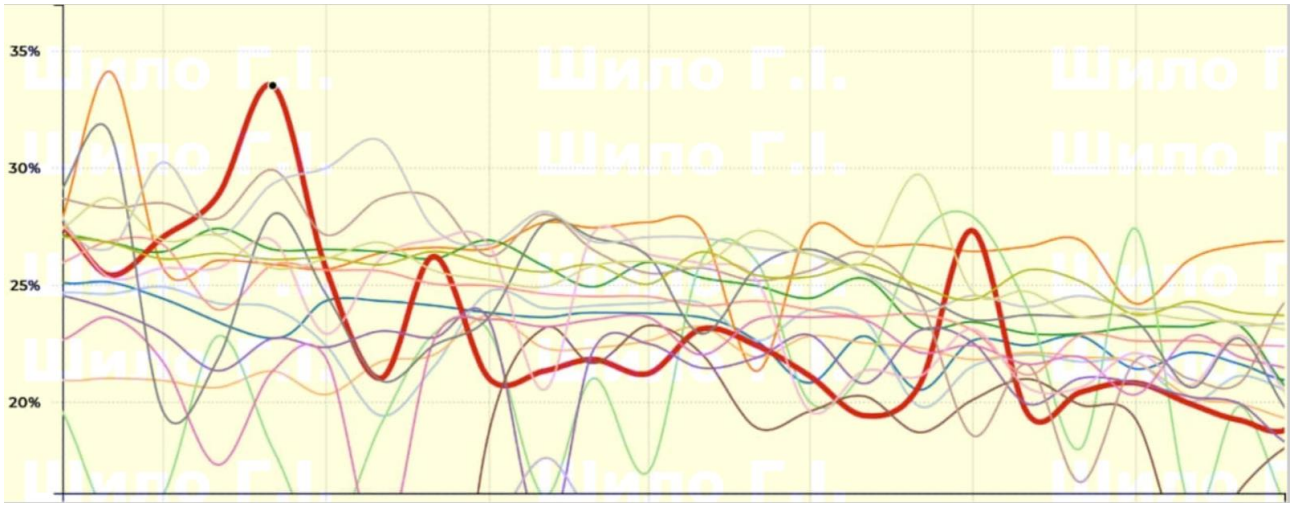

Рис.3.24 Зображення з прихованим ЦВЗ у 6-ому біті

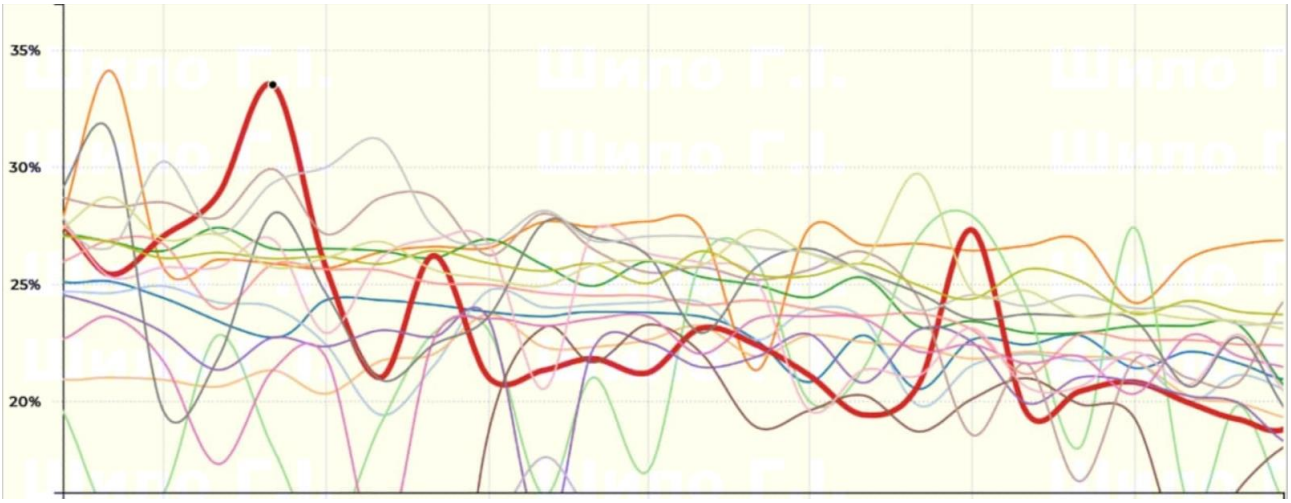

Рис. 3.25 Зображення з прихованим ЦВЗ у 5-ому біті

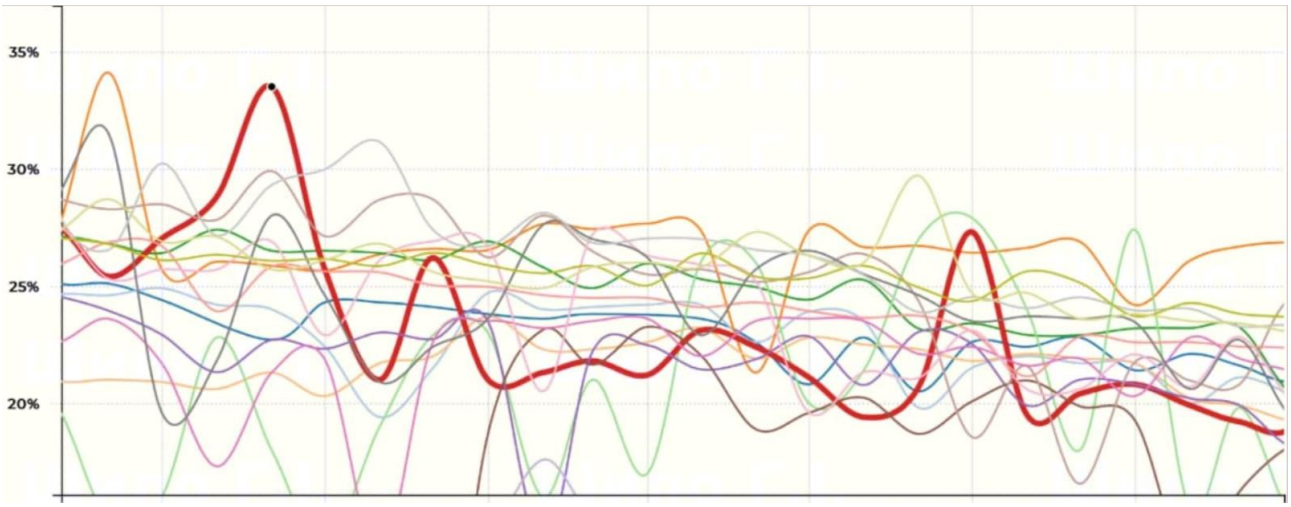

Рис.3.26 Зображення з прихованим ЦВЗ у 4-ому біті

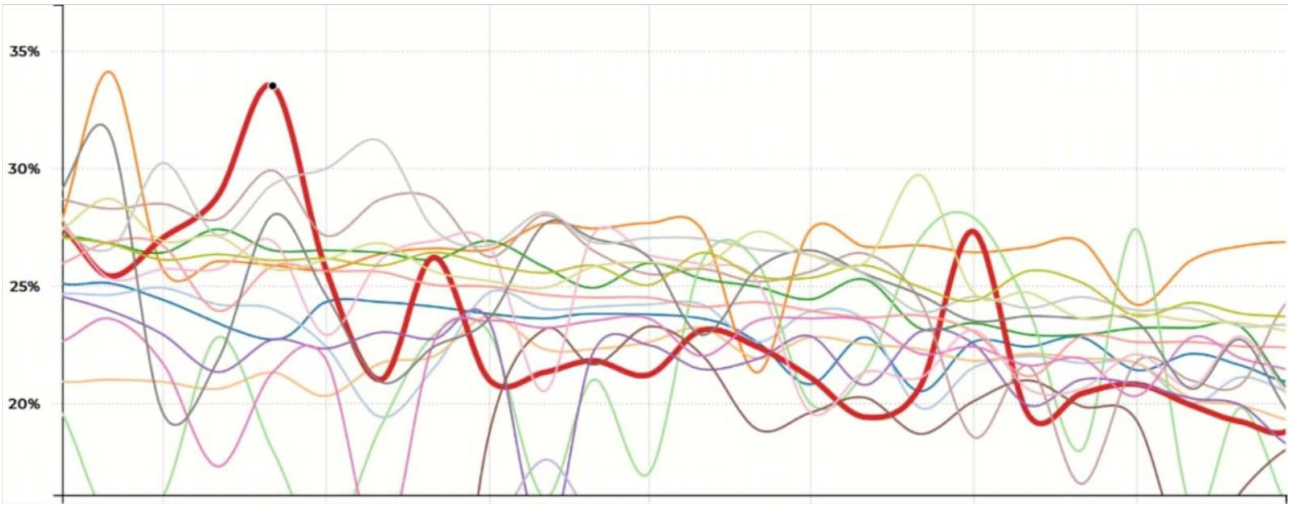

Рис. 3.27 Зображення з прихованим ЦВЗ у 3-ому біті

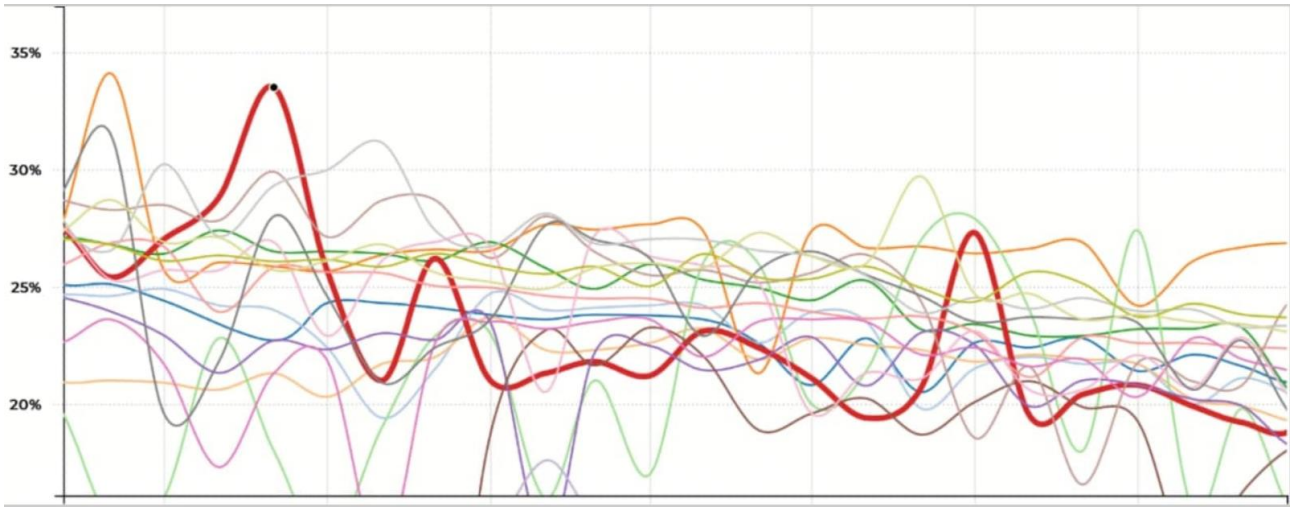

Рис.3.28 Зображення з прихованим ЦВЗ у 2-ому біті

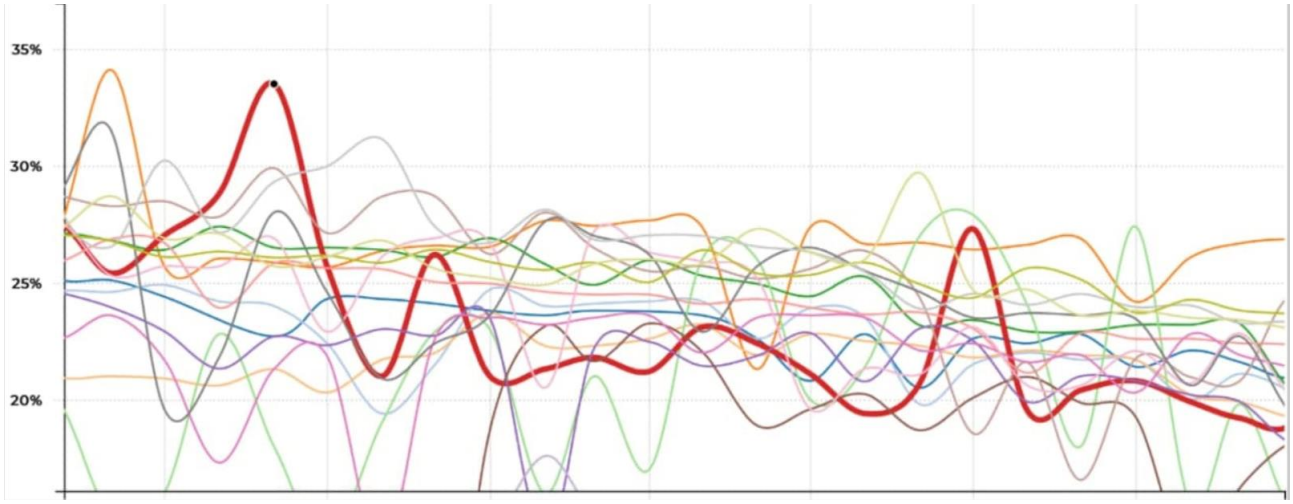

Рис. 3.29 Зображення з прихованим ЦВЗ у 1-ому біті

Отже, завдяки побітовому аналізу фотографічного зображення, можемо зробити висновок, що найвдалішим бітом для вставки ЦВЗ являється четвертий біт, адже викривлення кольорів майже непомітне, так само як і ЦВЗ.

3.2.4 Побітовий аналіз вставки ЦВЗ в комп'ютерну графіку

Розглянемо побітовий аналіз вставки ЦВЗ в комп'ютерну графіку, де цифровий водяний знак вставлений в 8-1 біти зображення.(рисунки 3.31-3.38) Вхідне зображення представлено на рисунку 3.30 :

Рис. 3.30 Вхідне зображення

Рис. 3.31 Зображення з прихованим ЦВЗ у 8-ому біті

Рис. 3.32 Зображення з прихованим ЦВЗ у 7-ому біті

Рис. 3.33 Зображення з прихованим ЦВЗ у 6-ому біті

Рис. 3.34 Зображення з прихованим ЦВЗ у 5-ому біті

Рис. 3.35 Зображення з прихованим ЦВЗ у 4-ому біті

Рис. 3.36 Зображення з прихованим ЦВЗ у 3-ому біті

Рис. 3.37 Зображення з прихованим ЦВЗ у 2-ому біті

Рис. 3.38 Зображення з прихованим ЦВЗ у 1-ому біті

Найвдалішими бітами для приховування ЦВЗ в комп'ютерній графіці є 8-5 біт, адже в бітах 4-1 цифровий водяний знак вже дуже важко розгледіти.

3.3 Рекомендації щодо вибору типу зображення за тестуванням програмного продукту

Для надання рекомендацій спочатку треба розглянути розбіжності приховування цифрових водяних знаків у 6 біт різних типів зображень.

Рис. 3.39 ЦВЗ у 6-ому біті картографічного зображення

Рис. 3.40 ЦВЗ у 6-ому біті фотографічного зображення

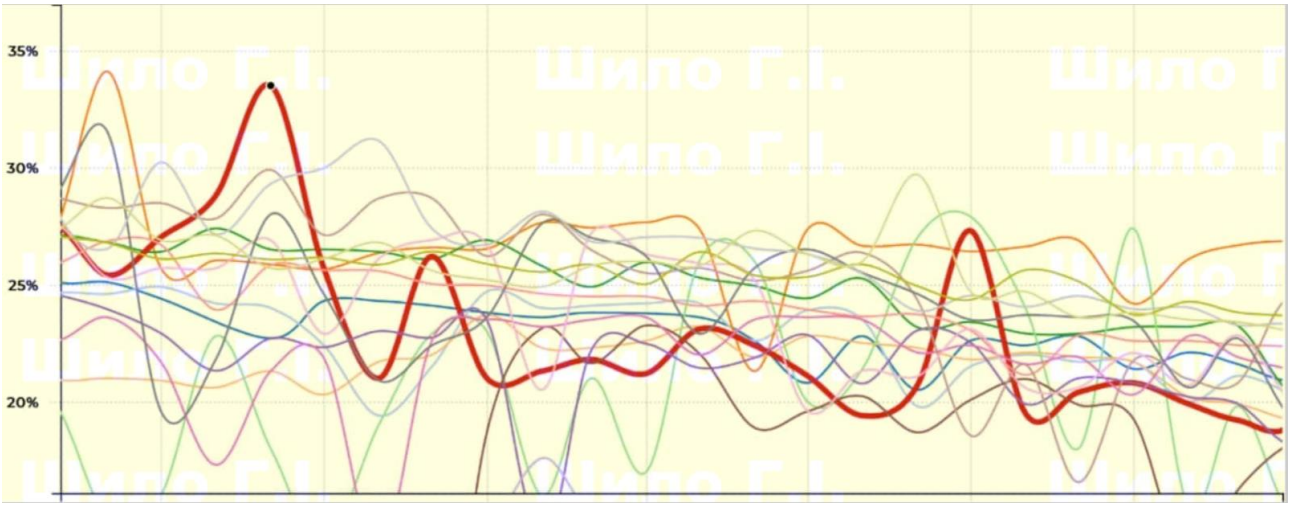

Рис. 3.41 ЦВЗ у 6-ому біті схематичного зображення

Рис. 3.41 ЦВЗ у 6-ому біті комп’ютерної графіки

Уважно роздивившись вищенаведені приклади чітко помітна різниця видимості цифрових водяних знаків. Підсумовуючи наші приклади, я можу сказати, що ступінь непомітності ЦВЗ напряму залежить саме від яскравості та деталізації зображення, тобто, картографічні типи зображень та комп’ютерна графіка найбільш вдало приховують ЦВЗ у 6-ому біті, проте фотографічні та схематичні краще справляються з цим у 1-4 бітах.

3.4 Висновки до розділу 3

У цьому розділі було розглянуто побітовий аналіз приховування ЦВЗ в різні типи графічних зображень та надано рекомендації щодо більш вдалого приховування ЦВЗ за тестуванням програмного продукту.

ВИСНОВКИ

В дипломній роботі на тему «Програмний модуль захисту графічної інформації цифровими водяними знаками» було проаналізовано:

- Нормативно-правову базу України з захисту інтелектуальної власності та стенографічні методи для доцільності використання ЦВЗ для захисту графічної інформації. Для аналізу було використано такі закони України:

- “Про інформацію”

- “Про авторське та суміжні права”

- “ Про захист інформації в інформаційно-комунікаційних системах ”

- Алгоритми формування ЦВЗ, властивості й життєвий цикл ЦВЗ

Методи введення ЦВЗ адаптовані до простору та частоти. Перевага алгоритму полягає в тому, що цифровий водний знак буде введено саме в області вхідного зображення, а це не потребує обчислення лінійних перетворень зображень.

Методом порівняльного аналізу методів приховування цифрового водяного знаку було обрано метод найменшого значущого біта. Метод був обраний для реалізації програмного продукту через свою легкість імплементації та швидкодію.

Також було розроблено програмний продукт, його було протестовано на різних типах зображень та надано рекомендації за тестуванням програмного продукту щодо використання ЦВЗ в картографічних типах зображень

На основі аналізу було обрано основу для розробки програмного продукту метод LSB

- В дипломній роботі було розроблено і протестовано програмного продукту для вставки цифрового водяного знаку задля забезпечення автентичності різних типів зображення, що дало можливість надати рекомендації щодо використання програмного продукту в цих типах.

Список використаних джерел:

1. Про авторське право і суміжні права. Закон України № 3792-XII від 23 грудня 1993 р. / Верховна Рада України // Відомості Верховної Ради України. – 1993. – №36. – Ст. 12.

2. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография М.: Солон-Пресс, 2009

3. Застосування електронного цифрового підпису-[Елктронний ресурс] -Режим доступу: https://www.bestreferat.ru/referat-143072.html

4. Белобокова Ю.А. Метод встраивания цифровых водяных знаков для доказательства подлинности фотоизображений. /Белобокова Ю.А. //Известия Тульского государственного университета. / Тула: «Известия ТулГУ» Технические науки, выпуск 3 , 2013

5. Оков И.Н., Ковалев Р.М. Электронные водяные знаки как средство аутентификации передаваемых сообщений // Защита информации. Конфидент. 2001. № 3, с.80-85.

6. Рябко, Б.Я. Основы современной криптографии и стеганографии / Б.Я. Рябко, А.Н. Фионов. – М: Горячая линия–Телеком, 2010. – 232 с

7. Оков И.Н., Ковалев Р.М. Электронные водяные знаки как средство аутентификации передаваемых сообщений // Защита информации. Конфидент. 2001. № 3, с.80-85.

8. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. — К.: «МК-Пресс», 2006.

9. Маховенко Е.Б., Ростовцев А.Г. Теоретическая криптография СПб.: АНО НПО "Профессионал", 2005. - 480 с.

10. Коржик, В.И. Исследование возможностей выявления скрытых сообщений в информационных ресурсах сети интернет: отчет о НИР «Ярус-СГ» /В.И. Коржик, Р.В. Чесноков, Е.Ю. Герлинг – СПб. :СПбГУТ. – 2010. – 181с

11. Быков С.Ф. Алгоритм сжатия JPEG с позиций компьютерной стеганографии // Защита информации. Конфидент. 2000. №3

12. Оков И.Н. Криптографические системы защиты информации. – СПб.:, ВУС, 2001. –236с

13. Яковлев В.А. Защита информации на основе кодового зашумления. Часть 1. Теория кодового зашумления. / Под ред. В.И. Коржика.– С.Пб.: ВАС, 1993.–245с.

14. Чиссар И., Кернер Я. Теория информации: Теоремы кодирования для дискретных систем без памяти / Пер. с англ. –М.: Мир, 1985, –400 с.

15. Р. Гонсалес, Р. Вудс, С. Эддинс Цифровая обработка изображений в среде MATLAB. Москва: Техносфера, 2006. - 616 с

16. Хорошко В.О., Азаров О.Д., Шелест М.Э. Основы компьютерной стеганографии: уч. пособие для студентов и аспирантов /– Винница: ВДТУ, 2003.

17. Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А. Стеганография, цифровые водяные знаки и стеганоанализ: Монография, М.: Вузовская книга, 2009.

18. Белобокова Ю.А. Метод встраивания цифровых водяных знаков для доказательства подлинности фотоизображений. /Белобокова Ю.А. //Известия Тульского государственного университета. / Тула: «Известия ТулГУ» Технические науки, выпуск 3 , 2013.

19. Про інформацію. Закон України 2657-XII від 2 жовтня 1992 р. / Верховна Рада України // Відомості Верховної Ради України. – 1992. – №48. – Ст. 12.

20. Про захист інформації в інформаційно-комунікаційних системах. Закон України від 5 червня 1993 р./ Верховна Рада України // Відомості Верховної Ради України. – 1993. – №31. – Ст. 9.

21. Стеганографія: навч. посіб (плагіат (реалізація методів, додатки) без посилань на монографії Грібуніна, Окова, Турінцева, Конаховича, Пузиренко). / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король ; М-во освіти і науки, молоді та спорту України, Харк. нац. екон. ун-т. — Х. : Вид-во ХНЕУ, 2011. — 232 с. : іл. — Бібліогр.: с. 202—206 (67 назв).

22. Jana Dittmann, David Megias, Andreas Lang, Jordi Herrera-Joancomarti; *Theoretical framework for a practical evaluation and comparison of audio watermarking schemes in the triangle of robustness, transparency and capacity*; In: Transaction on Data Hiding and Multimedia Security I; Springer LNCS 4300; Editor Yun Q. Shi; pp. 1–40

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

24. Patrick Bas, Teddy Furon, François Cayre, Gwenaël Doërr, Benjamin Mathon, "Watermarking Security, Fundamentals, Secure Designs and Attacks", Springer Briefs in Electrical and Computer Engineering, 2016

25. M. Cox and B. Miller, “Digital Watermarking,” Academic Press, San Diego, USA, ISBN 1-55860-714-5, 2002.

26. S. Katzenbeisser and J. Dittmann, “Malicious attacks on media authentication schemes based on invertible watermarks,” Proceedings of E.J. Delp III, P.W. Wong (Eds.): Security, Steganography, and Watermarking of Multimedia Contents VI, SPIE, Vol. 5306, pp. 838–847, Electronic Imaging Science and Technologies, San Jose, California, January 2004.

27. A. Lang, J. Dittmann, E. Lin, E.J. Delp III, “Application-oriented audio watermark benchmark service,” Proceedings of E.J. Delp III, P.W. Wong (Eds.): Security, Steganography, and Watermarking of Multimedia Contents VII, SPIE,

Vol. 5681, pp. 275–286, Electronic Imaging Science and Technologies, San Jose, California, USA, January 2005.

28. C.F. Osborne, R.G. van Schyndel, and A.Z. Tirkel, “A Digital Watermark,” IEEE International Conference on Image Processing, Austin, Texas, pp. 86–90, November 1994.

29. M. Kutter, S. Voloshynovskiy, and A. Herrigel, “Watermark Copy Attack,” Proceedings of SPIE: Security and Watermarking of Multimedia Contents II, San Jose, California, USA, Vol. 3971, January 2000, pp. 371–381.

30. F.A.P. Petitcolas, M. Steinebach, J. Dittmann, C. Fontaine, F. Raynal, and N. Fatès, “A public automated web-based evaluation service for watermarking schemes: StirMark Benchmark,” in P.W. Wong, E.J. Delp III (Eds.) Security and Watermarking of Multimedia Contents III, Proceedings of SPIE, Vol. 4314, 2001, pp. 575–584.

Додаток А
Програмний код продукту

```
lc;
close all;
imtool close all;
clear;
workspace;
fontSize = 12;
originalImage = imread('C:\diplom\20.jpg' [visibleRows, visibleColumns,
numberOfColorChannels] = size(originalImage);
if numberOfColorChannels > 1
   R=originalImage(:,:,1);
    G=originalImage(:,:,2);
    originalImage = originalImage(:,:,3);

end
subplot(3, 3, 4);
imshow(originalImage, []);
title('Вхідне напівтонове зображення', 'FontSize', fontSize);
set(gcf, 'units','normalized','outerposition',[0 0 1 1]);
hiddenImage = imread('C:\diplom\3.jpg');
[hiddenRows, hiddenColumns, numberOfColorChannels] = size(hiddenImage);
if numberOfColorChannels > 1
    hiddenImage = hiddenImage(:,:,3);
end
subplot(3, 3, 1);
imshow(hiddenImage, []);
title('Зображення для ЦВЗ', 'FontSize', fontSize);
```

```
[pixelCount, grayLevels] = imhist(hiddenImage);
subplot(3, 3, 2);
bar(pixelCount);
title('Гістограма водяного знаку', 'FontSize', fontSize);
xlim([0 grayLevels(end)]);
grid on;
thresholdValue = 70;
binaryImage = hiddenImage < thresholdValue;
subplot(3, 3, 3);
imshow(binaryImage, []);
caption = sprintf('Порогове значення водяного знаку- %d', thresholdValue);
title(caption, 'FontSize', fontSize);
prompt = 'Введіть розояд матриці для приховування ЦВЗ(від 1 - 8) ';
dialogTitle = 'Введіть розряд матриці щоб продовжити';
numberOfLines = 1;
defaultResponse = {'6'};
bitToSet = str2double(cell2mat(inputdlg(prompt, dialogTitle, numberOfLines,
defaultResponse)));
if isnan(bitToSet) || bitToSet>8 || bitToSet<1
   h=errordlg('Помилка! Введіть значення від 1 до 8','Error','on');
   set(h,'WindowStyle','modal')
else
      if hiddenRows > visibleRows || hiddenColumns > visibleColumns
         amountToShrink = min([visibleRows / hiddenRows, visibleColumns /
hiddenColumns]);
          binaryImage = imresize(binaryImage, amountToShrink);
           [hiddenRows hiddenColumns] = size(binaryImage);
      end
      if hiddenRows < visibleRows || hiddenColumns < visibleColumns
```

```
  watermark = zeros(size(originalImage), 'uint8');
        for column = 1:visibleColumns
            for row = 1:visibleRows
                watermark(row, column) = binaryImage(mod(row,hiddenRows)+1,
mod(column,hiddenColumns)+1);
            end
        end
        watermark = watermark(1:visibleRows, 1:visibleColumns);
    else
        watermark = binaryImage;
    end
    subplot(3, 3, 5);
    imshow(watermark, []);
    caption = sprintf('Водяний знак\nприхований в %d розряді матриці', bitToSet);
    title(caption, 'FontSize', fontSize);
    watermarkedImage = originalImage;
    for column = 1 : visibleColumns
        for row = 1 : visibleRows
            watermarkedImage(row, column) = bitset(originalImage(row, column),
bitToSet, watermark(row, column));
        end
    end
end
subplot(3, 3, 6);
imshow(watermarkedImage, []);
caption = sprintf('Кінцеве зображення \nбез додавання шуму');
title(caption, 'FontSize', fontSize);
noisyWatermarkedImage = imnoise(watermarkedImage,'gaussian', 0, 0.0005);
```

```
subplot(3, 3, 7);
imshow(noisyWatermarkedImage, []);
caption = sprintf('Кінцеве зображення  \nз додавання шуму');
title(caption, 'FontSize', fontSize);
recoveredWatermark = zeros(size(noisyWatermarkedImage));
recoveredNoisyWatermark = zeros(size(noisyWatermarkedImage));
for column = 1:visibleColumns
    for row = 1:visibleRows
        recoveredWatermark(row, column) = bitget(watermarkedImage(row, column),
bitToSet);
        recoveredNoisyWatermark(row, column) = bitget(noisyWatermarkedImage(row,
column), bitToSet);
    end
end
recoveredWatermark = uint8(255 * recoveredWatermark);
recoveredNoisyWatermark = uint8(255 * recoveredNoisyWatermark);
subplot(3, 3, 8);
```