Міністерство освіти і науки України
Одеський національний політехнічний університет
Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій
Кафедра кібербезпеки та програмного забезпечення

Баранюк Ганна Андріївна,
студентка групи РЗ-151

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Розробка системи вбудови цифрових водяних знаків в зображення на основі DCT-LWT-SVD перетворень

Спеціальність:
125 Кібербезпека

Спеціалізація, освітня програма:
Кібербезпека

Керівник:
Ахмаметьєва Ганна Валеріївна,
к.т.н.

Одеса – 2020

Міністерство освіти і науки України
Одеський національний політехнічний університет
Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій
Кафедра кібербезпеки та програмного забезпечення
Рівень вищої освіти другий (магістерський)
Спеціальність 125 – Кібербезпека
Освітня програма – Кібербезпека

ЗАТВЕРДЖУЮ

Завідувач кафедри КБПЗ

_____

д.т.н.,проф. А.А.Кобозєва

____ _____202_р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

Баранюк Ганні Андріївні

1. Тема роботи: *Розробка системи вбудови цифрових водяних знаків в зображення на основі DCT-LWT-SVD перетворень*,

керівник роботи: *Ахмаметьєва Ганна Валеріївна, к. т. н.,*

затверджені наказом ректора ОНПУ від “ 16 ” листопада 2020 р. № 468-в.

2. Зміст роботи*: аналіз проблемної області, постановка задачі, аналіз сучасних методів вбудови ЦВЗ, розробка методу вбудови ЦВЗ в зображення, експериментальне дослідження розробленого методу, дослідження його стійкості до атак, розробка програмного інтерфейсу для алгоритмічної реалізації запропонованого методу, охорона праці*.

3. Перелік ілюстративного матеріалу: *схеми роботи прямого та оберненого ліфтингу, схеми вбудовування та детектування цифрового водяного знаку.*

4. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
Охорона праці і безпека в надзвичайних ситуаціях	Ярова І. А. к.т.н., доцент	Завдання видав	Завдання прийняв
		05.11.2020	19.11.2020

5. Дата видачі завдання "_____"_____20___ р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання	Примітка
1	*Аналіз джерел з теми випускної кваліфікаційної роботи та збір даних*	*01-09-2020*	*виконано*
2	*Розробка методу вбудови ЦВЗ в цифрові зображення та проведення його оцінки*	*01-10-2020*	*виконано*
3	*Розробка програмного інтерфейсу*	*16-11-2020*	*виконано*
4	*Підготовка тексту роботи*	*02-11-2020*	*виконано*
5	*Підготовка презентації та доповіді*	*18-12-2020*	*виконано*
6	*Попередній захист*	*01-12-2020*	*виконано*
7	*Нормоконтроль, рецензування*	*15-12-2020*	*виконано*
8	*Занесення роботи в електронний архів*	*25-12-2020*	*виконано*
9	*Допуск до захисту у завідувача кафедри*	*25-12-2020*	*виконано*

Здобувач вищої освіти _____ *Баранюк Г.А.*

Керівник роботи _____ *Ахмаметьєва Г.В.*

ЗАВДАННЯ

на розробку розділу “Охорона праці і безпека в надзвичайних ситуаціях”

Баранюк Ганні Андріївні, група РЗ-151

Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій
Кафедра кібербезпеки та програмного забезпечення

Тема роботи “*Розробка системи вбудови цифрових водяних знаків в зображення на основі DCT-LWT-SVD перетворень”*

Зміст розділу:

1 Аналіз умов праці і вибір заходів і засобів захисту від небезпечних і шкідливих виробничих факторів.
2 Аналіз техногенних небезпек, вибір заходів і засобів забезпечення безпеки у надзвичайних ситуаціях на робочому місці користувача ПК.
3 Розрахунок захисного заземлення.

Керівник роботи	Консультант з охорони праці
_____ (_____)	_____ (_____)
“___” _____ 2020 р.	“____” _____ 2020 р.

АНОТАЦІЯ

Кваліфікаційна робота на тему “Розробка системи вбудови цифрових водяних знаків в зображення на основі DCT-LWT-SVD перетворень” на здобуття освітньо-кваліфікаційного рівня “Магістр” з спеціальності 125 – “Кібербезпека” містить 24 рисунки, 2 таблиці, 3 додатки та 50 джерел з переліком посилань. Робота виконана на 77 сторінках загального тексту та 54 сторінках основного тексту.

Метою роботи є підвищення якості стеганоповідомлень шляхом розробки нового методу вбудови цифрового водяного знаку в зображення на основі послідовного використання різних областей перетворень.

Методи досліджень базуються на використанні чисельних методів та методів обробки цифрових зображень.

Розроблено новий метод системи цифрових водяних знаків на основі дискретного косинусного перетворення, ліфтингового вейвлет-перетворення та сингулярного розкладу. Створено програмний продукт для вбудовування та вилучення цифрових водяних знаків, а також для проведення аналізу заповненого контейнеру на предмет збереження високої якості зображення і ступеню подібності вбудованого та детектованого цифрового водяного знаку. Проведено дослідження, у результаті якого зроблено висновок, що метод забезпечує високу якість заповненого контейнеру, високу ступінь подібності вбудованого та вилученого цифрового водяного знаку, стійкість до різних видів атак.

Результати проведеної роботи можуть бути використані для вирішення питання авторського права на медіа-контент.

СТЕГАНОГРАІФІЯ, ЦИФРОВИЙ ВОДЯНИЙ ЗНАК, ЗАХИСТ ІНФОРМАЦІЇ, ДИСКРЕТНЕ КОСИНУСНЕ ПЕРЕТВОРЕННЯ, ЛІФТИНГОВЕ ВЕЙВЛЕТ-ПЕРЕТВОРЕННЯ, СИНГУЛЯРНЕ РОЗКЛАДАННЯ.

ABSTRACT

Qualification work on the topic “Development of a system for digital watermarks embedding into images based on DCT-LWT-SVD transformations” to obtain the educational qualification level “Master” in the specialty 125 – “Cyber Security” contains 24 figures, 2 tables, 3 annexes and 50 sources with references. The work is performed on 77 pages of the general text and 54 pages of the main text.

The aim of the work is to improve the quality of stegos by developing a new method of embedding a digital watermark into the image based on the gradual use of different domains of transformation.

The research methods are based on the use of numerical and digital image processing methods.

A new method of digital watermark system has been developed using discrete cosine transformation, lifting wavelet transformation and singular decomposition. A software product has been developed for embedding and extracting digital watermarks, as well as for analyzing a full container to maintain the high image quality and degree of similarity between the embedded and detected digital watermark. A study was carried out, which concluded that the method ensures the high quality of the filled container, a high degree of similarity between the embedded and removed digital watermark and resistance to various types of attacks.

The results of this work can be used to resolve the issue of copyright in media content.

STEGANOGRAPHY, DIGITAL WATERMARK, INFORMATION PROTECTION, DISCRETE COSINE TRANSFORM, LIFTING WAVELET TRANSFORM, SINGULAR DECOMPOSITION.

ЗМІСТ

ВСТУП

У XXI столітті інформація зберігається у цифровому вигляді і знаходиться на цифрових носіях та у вільному доступі у всесвітній мережі Інтернет. Майже до будь-якого матеріалу можна отримати доступ. З цим вникає проблема зростання ризику стороннього незаконного впливу на данні, які повинні бути захищені.

Захист авторського права – одна з актуальних проблем сьогодення. З кожним роком кількість контенту, що було викрадено, модифіковано, скопійовано дедалі зростає. Вирішенням даного питання стало створення і використання цифрових водяних знаків (ЦВЗ), які дають змогу довести своє авторство.

Кількість досліджень в області цифрових водяних знаків тільки збільшується. Роботи присвячені не тільки обробці цифрових сигналів у просторовій області, але і в області перетворень, зокрема перетворенню Фур'є, дискретному косинусному та вейвлет-перетворенню. Дослідження в останній – почали проводитися тільки на початку дев'яностих років двадцятого століття, проте методи використовуються та вдосконалюються і на сьогоднішній день. Однак для більшості сучасних методів залишається невирішеною задача забезпечення якості заповненого контейнеру (стеганоповідомлення), тому тема роботи є актуальною.

Метою роботи є підвищення якості стеганоповідомлень шляхом розробки нового методу вбудови цифрового водяного знаку в зображення на основі послідовного використання різних областей перетворень.

Для досягнення поставленої мети необхідно виконати завдання:

- дослідити параметри областей перетворення для забезпечення найкращої якості заповненого контейнеру та вилучення ЦВЗ;
- провести аналіз характеристик колірних матриць зображення-контейнеру, що впливають на результат вилучення ЦВЗ;
- розробити метод вбудови ЦВЗ в цифрові зображення;
- провести оцінку розробленого методу;
- розробити програмний інтерфейс алгоритмічної реалізації нового методу.

Об’єкт дослідження – процеси захисту авторської власності на мультимедійну інформацію.

Предмет дослідження – стеганографічні системи та системи цифрових водяних знаків.

Методи дослідження. При розробці теоретичного базису методу вбудови ЦВЗ були використані чисельні методи та методи обробки цифрових зображень. Для оцінки ефективності стеганографічного методу використовувались методи обробки цифрових зображень.

Наукова новизна одержаних результатів полягає в наступному.

1. Вперше розроблено метод вбудови ЦВЗ, заснований на використанні комбінації дискретного косинусного перетворення, ліфтингового-вейвлет перетворення та сингулярного розкладання матриць, що забезпечує високу якість заповненого контейнеру.
2. Проведено дослідження впливу характеристик цифрового зображення та параметрів областей перетворень блоків зображення, використовуваних в стеганографічному методі, що дозволило підвищити якість вилучення вбудованого ЦВЗ.

Практична цінність роботи полягає в програмній реалізації нового методу, отриманні високих показників якості заповненого контейнеру і показників ступеню подібності вилученого та вбудованого цифрових водяних знаків, а також доведення факту стійкості результату роботи методу до атак.

Розроблений програмний продукт можна використовувати для захисту інформації як на підприємствах, так і в особистих цілях.

Робота складається з чотирьох розділів, коротких опис яких наведено нижче.

У першому розділі наведено основні відомості з предметної області та проведено аналіз сучасних стеганографічних методів з використанням різних областей перетворення.

У другому розділі детально описано новий метод вбудови ЦВЗ, із врахуванням усіх особливостей, а також наведено результати експериментальних досліджень на предмет його ефективності.

У третьому розділі представлено: опис програмного забезпечення, що було використано для проведення дослідження та розробки програми, поетапний процес реалізації програми та інтерфейс розробленого програмного продукту.

Четвертий розділ – розділ з охорони праці. У ньому описано робоче місце користувача персонального комп'ютеру, а саме опис приміщення із робочим місцем людини, проведено аналіз шкідливих та небезпечних виробничих факторів, проаналізовано техногенні небезпеки та обґрунтовано вибір засобів і заходів забезпечення безпеки у надзвичайних ситуаціях на робочому місці, а також розв'язано задачу, пов'язану із розрахунком захисного заземлення.

Публікації. Матеріали кваліфікаційної роботи магістра опубліковані в [1].

1 СТЕГАНОГРАФІЯ ТА СИСТЕМИ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ

1.1 Стеганографія як наука про методи захисту інформації

Зловмисники всюди і завжди намагаються отримати секретну інформацію будь-яким шляхом (у тому числі – злам електронної пошти та різних меседжерів). Тому, для того, щоб захистити конфіденційну інформацію від її витоку, слід звернутися до стеганографії, адже навіть якщо порушник отримає доступ до каналу зв'язку, потрібну інформацію буде важко виявити.

Стеганографія має велику перевагу над криптографією, а саме: у випадку криптографії – конфіденційна інформація зберігається у зашифрованому вигляді і при отриманні доступу до такого файлу у зловмисника не буде жодних сумнівів у тому, що дана інформація не є для широкого користування, проте у випадку із стеганографією – зловмисник не буде підозрювати, що у файлі, зображенні або відео, до якого йому вдалося встановити доступ, може бути прихована інформація. За умови, що порушнику відомо про закритий канал зв'язку, який утворено стеганографічними методами, він може отримати конфіденційну інформацію, проте для цього він повинен знати метод, що використано для приховування інформації та ключ.

Основними перевагами стеганографії є:

- передача секретної інформації по відкритому каналу зв'язку без використання цензури та страху того, що інформацію буде викрито;
- зберігання необхідної інформації (секретні паролі, таємниці);
- використання цифрових водяних знаків для захисту медіа-контенту;
- стеганографія дозволяє передавати конфіденційні дані повз підслухувачів, що не здогадуються, що таємна інформація вже передана.

Отже, стеганографія – це наука про методи захисту інформації, шляхом її приховування таким чином, щоб запобігти виявленню прихованих повідомлень. Сьогодні широкою популярністю користується комп'ютерна стеганографія. Вона поділяється на два види: стеганографія, що пов'язана з цифровою обробкою сигналів і та, що не пов'язана. Перша застосовується для вбудовування додаткової

інформації у цифровий контент, друга – секретні дані вбудовуються у заголовки файлів, документів та пакетних даних.

Стеганографією також користуються зловмисники для передачі таємної інформації. Прикладом цього може слугувати ситуація, що відбулася у 2001 – терористи намагалися підірвати посольство США на території Франції. Лідер групи зізнався у тому, що йому було наказано відправляти всі повідомлення через фотографії, що знаходилися в мережі Інтернет. У статі журналу New-York Times [2] можна зустріти слова доктора з університету Джорджа Мейсона Ніла Ф. Джонсона – експерта з стеганографії, про те, що науковець стурбований тим, наскільки дана наука стала поширеною у рядах терористів та злочинців, настільки, що перестав публікувати свої дослідження в даній області.

Щодо цифрової стеганографії, слід зазначити, що це відносно нова наука. Вона включає у себе наступні напрями дослідження:

- вбудовування інформації з метою її прихованої передачі;
- вбудовування цифрових водяних знаків (ЦВЗ, watermarking);
- вбудовування ідентифікаційних номерів (fingerprinting; в таких стеганосистемах у кожен екземпляр контейнера, що надається певному користувачеві, вбудовується її індивідуальний номер. Таким чином, в якості приховуваного повідомлення передається унікальний номер, який може бути використаний для відстеження будь-якого неавторизованого використання даного контейнера конкретним користувачем);
- вбудовування заголовків (captioning) [3].

Серед методів вбудовування інформації з метою її прихованої передачі цікавими є метод С. Чандри та С. Паіра “Secure transmission of data using image steganography”, у якому таємне повідомлення шифрується за допомогою методу RSA та додається у верхній та нижній колонтитули контейнеру (перевага методу – поєднання криптографії та стеганографії, що забезпечує високу стійкість стеганосистеми), та метод С. Рубаб та М. Юнус “Improved Image Steganography Technique for Colored Images using Huffman Encoding with Symlet Wavelets” [4,5],

основною ідеєю якого є застосування перетворення Хаффмана до стего, побудова його таблиці та переведення даних у бінарний вид, виконання дворівневого вейвлет-перетворення контейнеру для кожної з колірних матриць, після чого вбудувати додаткову інформацію (ДІ) (результати роботи даного методу є досить високими: показники відношення пікового сигналу/шум складають від 60.1 дБ для зображень розміром (512×512).

Щодо методів вбудовування ідентифікаційних номерів, слід зазначити, що по своїм функціям методи аналогічні методам вбудовування цифрових водяних знаків.

Вбудовування заголовків використовується для надання об’єктам певної категорії. Метою таких методів є зберігання різного роду інформації в одному цілому. Вбудовування заголовків є актуальними для різних сховищ, медичних та освітніх установ, де необхідно здійснювати пошук даних.

Методи вбудовування цифрових водяних знаків є найбільш поширеними у стеганографії. Слід зазначити, що стеганографія призначена для передачі вбудованого повідомлення так, щоб спостерігач (третя сторона) не зміг помітити вбудовані дані у контейнері. Проте водяні знаки призначені не лише для непомітної (якщо це невидимі ЦВЗ) передачі секретної інформації, але і слугують інструментом для захисту авторських прав та захисту від фальсифікацій даних.

Останнім часом дослідження в області цифрових водяних знаків, порівняно із іншими напрямами, стрімко зростають. З кожним роком кількість робіт, присвячених даній темі збільшується, а методи, що існували до сьогоднішнього дня – вдосконалюються. За останні роки цікавими роботами по даній темі можна вважати праці авторів А. Актера, Н. Тайніни, М. А. Уллаха [6] та науковців К. Сю, Ю. Ню, К. Зенг і Ю. Хан [7]. Перша стаття розглядає технологію водяних знаків, що заснована на дискретному вейвлет-перетворенні (ДВП) та дискретному косинусному перетворенні (ДКП) – гібридний водяний знак. Гібридне водяне маркування виконується дворівневим, трирівневим та чотирьохрівневим ДВП з подальшим відповідним ДКП на головному зображенні.

Другий метод заснований на диференціальній еволюції ЦВЗ [8]. Кольорове основне зображення спочатку переноситься з простору RGB у простір YIQ, що більше підходить для зорової системи людини. Наступним кроком є застосування трирівневого ДВП до складової Y. Цифровий водяний знак шифрується за допомогою скремблювання і після виконується ДВП, після чого відбувається операція вбудовування водну з частотних областей. Експериментальні результати показують, що запропонований алгоритм має кращі показники невидимості та надійності.

1.2 Цифрові водяні знаки – їх функції та особливості

Цифровий водяний знак - це сигнал, що є вбудованим на постійній основі у цифрові дані (аудіо, зображення, відео та текст), який можна виявити або витягти за допомогою обчислювальних операцій, щоб зробити їх підтвердження. ЦВЗ – це спеціальна мітка, вбудована в цифровий контент з метою захисту авторських прав і підтвердження цілісності самого документа [3]. Він являє собою вбудовування цифрового підпису у дані. Водяний знак приховується у зображення-контейнер таким чином, що стає невіддільним від нього, і, таким чином, він є стійким до багатьох операцій, що не погіршують контейнер. Стеганографія та водяні знаки належать до категорії приховування інформації, але цілі та умови двох методів є протилежними. Відмінність полягає у тому, що при нанесенні водяних знаків важливою інформацією є “зовнішні” дані (наприклад, зображення, голоси тощо). “Внутрішні” дані (наприклад, водяний знак) – це додаткові дані для захисту зовнішніх даних та підтвердження права власності. Однак у стеганографії зовнішні дані (дані про контейнер) є носіями інформації, важливішою є внутрішня інформація.

Цифрові водяні знаки поділяються на три типи:

- крихкі ЦВЗ (руйнуються навіть при малих модифікаціях заповненого контейнеру);

- напівкрихкі ЦВЗ (такі ЦВЗ є стійкими до певних видів атак, проте можуть бути вразливими до окремих видів операцій);
- робасті (стійкі до будь-якого впливу на стеганографічну систему).

Цифрові водяні знаки бувають видимі та невидимі. Видимі ЦВЗ – об’єкти, що можна побачити у медіа-контенті. В основному у ролі водяних знаків виступають особисті підписи авторів продукту або логотип компаній. Головним недоліком такого виду захисту інформації є те, що видимі ЦВЗ легко видаляються або підмінюються [9].

Невидимі цифрові водяні знаки являють собою цифрові вставки, що є непомітними та через це їх не легко виявити у контейнері. Такі ЦВЗ можуть бути вбудовані у просторову область та область перетворення, в залежності від обраного методу для захисту інформації. Вбудовування інформації у просторову область означає зміну значень пікселів зображення – біти зображення-контейнеру заміняються бітами конфіденційної інформації. Серед найпоширеніших методів просторової області є метод заміни найменших значущих бітів (LSB), метод різниці значень пікселів (PVD), метод зсуву гістограми.

Метод заміни найменших значущих бітів є найпопулярнішим методом просторової області. Головною перевагою методу є його простота та легкість реалізації, проте у нього присутні вагомі недоліки – відсутня стійкість до різних видів атак, у тому числі до збереження зображення у форматі із втратами.

В основі методу різниці значень пікселів лежить вибір двох значень послідовних пікселів. Розрахунок різниці визначають для пікселів з фонової області чи області контуру. Корисне навантаження визначається шляхом обчислення різниці між двома звичайними пікселями.

Метод зсуву гістограми. Зображення представляють у вигляді гістограми. Значення пікселів будуть відображатись для кожної частини зображення: можна буде відслідкувати щільність та значення конкретного пікселя. Гістограми корисні для визначення тонального розподілу, розподілу пікселів та щільності кольорів. Окрім ідентифікації цих деталей, гістограма також надає максимальні та мінімальні значення пікселя на графіку. Найбільше значення гістограми у точці буде

називатися максимумом, а найменше – мінімумом. При вбудовування додаткової інформації у контейнер, відслідковується зміна значень пікселів – значення не повинно перевищувати максимум та мінімум [10].

Стеганосистема виконує задачу вбудовування та виділення/детектування секретного повідомлення і конструктивно складається з таких елементів:

- попередній кодер (інструмент, що відповідає за перетворення секретного повідомлення у вигляд, що є підходящим для вбудовування у контейнер);
- кодер (використовується для вбудовування додаткової інформації у контейнер, враховуючи його особливості);
- засіб виділення секретного повідомлення;
- детектор (виділення додаткової інформації із повного контейнеру);
- декодер (інструмент для відновлення секретних даних).

Розробка системи цифрових водяних знаків залежить від:

- робастості (ЦВЗ повинен бути стійким до різних видів атак та маніпуляцій);
- місткості (кількість інформації, що можна вбудувати);
- безпеки (дані ЦВЗ не повинні впливати на об’єкт або його роботу, якщо він змінюється або витягується);
- ефективності (швидкість вилучення та розміщення цифрового водяного знаку);
- непомітності (ЦВЗ не повинен впливати на вміст контейнеру).

Стеганографічні системи ЦВЗ поділяються на: закриті, напівзакриті (першого та другого типу), відкриті.

ЦВЗ мають виконувати наступні функції: приховування секретних даних в контейнері, захист авторських прав, секретне спілкування, аутентифікація зображень, запобігання створення підробок, контроль копіювання.

Вбудовування ЦВЗ може здійснюватися в області перетворень: перетворення Фур’є, область дискретного косинусного перетворення, область дискретного вейвлет-перетворення, перетворення Адамара.

Перетворення Фур’є є спектральним методом. Його основою слугує інтегральне перетворення та ряди Фур’є. Властивостями фазового спектру перетворення Фур’є є:

- симетрія (так як фазовий спектр Фур’є – непарна функція; якщо відбувається зміна деякого фазового значення, тоді необхідно поміняти симетрично розташоване значення фази на протилежне, замінивши знак на протилежний);
- для вбудовування інформації не використовуються елементи, які розташовані на межі нецентрованого Фур’є образу (дана операція може значно погіршити якість зображення та його сприйняття) [11].

Дискретне косинусне перетворення – один із різновидів перетворення Фур’є. Використовуючи ДКП, є змога перейти від просторової обробки зображення до спектральної і навпаки. Саме тому ця область перетворення використовується в алгоритмах стиснення JPEG.

ДКП має наступні особливості:

- коефіцієнти є некорельованими, тобто вони є незалежними один від одного;
- ущільнення енергії – важлива інформація зберігається у невеликій кількості коефіцієнтів [12].

Дискретне вейвлет-перетворення – ще один із різновидів перетворення Фур’є. Найчастіше його використовують в алгоритмах стиснення JPEG2000 та, іноді, JPEG. Основною відмінністю ДВП є те, що зображення, у процесі обробки, розкладається на підгрупи зображень у різних частотних та просторових областях. Під час застосування ДВП, аналізується 4 частотні області: низькі частоти по вертикалі та по горизонталі (LL), високі частоти по вертикалі та по горизонталі (HH), високі частоти по горизонталі та низькі по вертикалі (HL), низькі по горизонталі та високі по вертикалі (LH). ДВП застосовується для вирішення наступних питань: обробка зображень, стиснення даних, обробка експериментальних даних, аналіз даних, системи передачі даних та цифрової обробки сигналів.

Для того, щоб можливо було виконати вейвлет-перетворення, необхідно визначити материнський вейвлет. До них належать наступні: функції Добеші, Хаара та Гауса, койфлети та стимлети, мексиканська шляпа, вейвлети Меєра, Морл'є, Шенона, дискретні вейвлети Меєра, комплексні Гауса та Морл'є, біортогональні та обернено ортогональні функції [13].

Перетворення Адамара – спрощене перетворення Фур'є. Спрощення полягає у тому, що перетворення Адамара використовує прості операції додавання та віднімання, оскільки операції множення та ділення йому не потрібні. Усі коефіцієнти перетворення є "1" або "-1". Даний метод використовується на простих машинах для розрахунку, тому на сьогоднішній день це перетворення не є актуальним для розгляду та використання, тому у подальшому цей вид перетворення розглядатися не буде [11, 14-16].

До ЦВЗ застосовуються наступні вимоги:

- секретність – вбудовування ЦВЗ не повинно погіршувати якість стеганоповідомлення;
- безпека системи – безпека системи залежить від секретності ключа;
- стійкість – ЦВЗ не повинен пошкоджуватись у результаті виконання різних операцій із стеганоповідомленням;
- у стеганосистеми ЦВЗ повинен бути низький рівень помилкового виявлення секретної інформації, якщо він відсутній у контейнері;
- пропускна здатність повинна бути відповідною до каналу зв'язку;
- система ЦВЗ повинна мати відповідну обчислювальну складність;
- ЦВЗ має легко детектуватись законним користувачем;
- знання факту існування секретного каналу зв'язку не повинно допомогти порушнику або зловмиснику розкрити секретну інформацію.

Система цифрових водяних знаків складається з цифрового водяного знаку, алгоритму вбудовування та алгоритму вилучення [17].

Слід зауважити, що деструктивні операції по відношенню до стеганоповідомлення можуть бути націленими на ЦВЗ або на стеганосистему. Серед найпоширеніших впливів на стеганографічну систему існують атаки на

основі: відомого заповненого контейнеру, відомого вбудованого повідомлення, обраного скритого повідомлення, вибраного заповненого контейнеру, відомого пустого контейнеру та атаки стисненням.

До атак на ЦВЗ необхідно віднести:

- атака видаленням (повне видалення ЦВЗ з контейнеру без порушення безпеки алгоритму водяних знаків);
- геометрична атака (спотворення синхронізації детектора ЦВЗ з прихованою інформацією);
- криптографічна атака (знищення методів безпеки у ЦВЗ та пошук варіантів видалення інформації про вбудовані водяні знаки);
- атаки протоколами (напад на всю концепцію програми ЦВЗ);
- атака оцінювання (використання статистики вихідних даних і сигналу ЦВЗ);
- оцінка оригінальних даних;
- атака копіюванням;
- атака видаленням синхронізації (виявлення шаблонів синхронізації, їх видалення і застосування десинхронізації) [18].

1.3 Огляд літературних джерел та методів з предметної області

Як було згадано вище, вбудовування ЦВЗ може здійснюватися як у просторову область, так і у області перетворень. Так як найбільш цікавими, з точки зору реалізації та складності, є методи, що засновані на області перетворень, слід розглянути деякі роботи науковців у цій області.

1.3.1 Дослідження в області перетворення Фур’є

Серед робіт в області перетворення Фур’є варто виділити наступні.

У науковій праці [19] запропоновано нову техніку стеганографії для приховування текстової інформації у контейнер за допомогою кватеріону.

Кватеріон має чотири компоненти: одну реальну та три явних. Кватеріон – геометричний оператор, що відображає відношення (відносну довжину та відносний напрям) між двома векторами у 3-D просторі. Вони є узагальненням комплексних чисел і поєднуються за звичайними правилами алгебри. Вбудовування інформації відбувається за наступною схемою: зображення обрізається до максимального квадратного розміру та обчислюється максимальна довжина прихованого повідомлення (для контейнеру). Контейнер представляється у вигляді трьох матриць R, G, B, для кожної с ним будується перетворення Фур'є. До кватеріону секретного повідомлення застосовується перетворення Фур'є. Кватеріон ЦВЗ вбудовується у контейнер адитивним шляхом. Даний метод показав досить високі показники "піковий сигнал/шум" (PSNR = 89.6317), проте існують недоліки: не було проаналізовано факт стійкості до атак (якість повного контейнеру), якість вилученої інформації та складність реалізації.

Робота [20] А. Чедада пропонує новий метод шифрування із паролем, що заснований на розширеній версії SHA-1, який може шифрувати масиви даних у 2D – такі як зображення. Тут швидке перетворення Фур'є включається у процес для підвищення рівня маскування. Недоліком методу є відсутність досліджень на предмет стійкості алгоритму до різних видів атак та аналіз якості отриманих повних контейнерів.

Метод, що наведено у роботі російських дослідників Дружкової, Щепилової та Юдіна [21], використовує надмірність монохромної моделі зображення. Основою для алгоритму слугує перетворення Фур'є, а саме субсмуговий аналіз енергії зображення і зміні компонент в обраній просторової області частот. Метод показав точний результат детектування ЦВЗ, проте не було проведено аналізу щодо якості зображення-контейнеру та вбудованого ЦВЗ на предмет стійкості до атак.

У дослідженні [22] автор описує перевагу дискретного перетворення Фур'є у порівнянні з іншими областями перетвореннями (швидке перетворення Фур'є) при роботі з цифровими зображеннями. Результат моделювання показує однакову PSNR в обох областях, але перетворення у дискретну фракцію дає додатковий стеганографічний ключ, тобто параметр порядку цього перетворення.

1.3.2 Дослідження в області дискретного косинусного перетворення

До цікавих робіт в області дискретного косинусного перетворення можна віднести наукову працю [23], що представляє нову методику приховування даних на основі коефіцієнтів ДКП та модифікованих значень таблиці квантування. Стійкість методу вбудовування кожного коефіцієнта визначається за математичною формулою, яка порівнює коефіцієнт ДКП та відповідне значення таблиці квантування для вбудовування секретних бітів у частотні компоненти квантованих коефіцієнтів ДКП за допомогою методу найменшого значущого біта, щоб забезпечити велику потужність вбудовування без деградації зображення. Техніка реалізації є досить не складною та включає наступні етапи: контейнер розбивається на блоки 8×8, до кожного блоку застосовується ДКП, порівняння значення ДКП із значенням таблиці квантування, що використовується для задоволення наступного рівняння: якщо показник n – новий квантований коефіцієнт буде дорівнювати модулю відношення коефіцієнта ДКП до відповідного значення у таблиці квантування – вбудовано 1 біт інформації. У порівнянні з аналогами, даний метод має наступні результати: покращено показники MSE, а також важливим є факт зростання об'єму інформації, що необхідно вбудувати (більше, ніж у 2 рази), проте у метода є недоліки – відносно високий показник середньоквадратичної помилки та низький показник PSNR (до 45 дБ).

Робота [24] заснована на використанні алгоритму, що використовує ортогональне дискретне косинусне перетворення для зображення-контейнеру. Алгоритм залежить від нормованого секретного зображення шляхом множення його на масштабний коефіцієнт α, а потім вбудовування додаткової інформації у високочастотну складову контейнеру після застосування дискретного косинусного перетворення. Щодо ефективності методу, слід зазначити, що метод непогано працює при збереженні стеганоповідомлення у форматі без втрат, проте, якщо до нього застосувати атаку стисненням – результати детектування значно погіршуються, при цьому, показники PSNR майже не змінюються – у середньому

34 дБ. Недоліком нової технології є відносно мала пропускна здатність секретного каналу зв’язку, низький показник відношення пікового сигнал/шум.

Дослідження у методі [25] спрямовані на покращення якості стеганоповідомлень та збільшення об’єму інформації, що необхідно погрузити у зображення. Особливістю методу є те, що контейнер розбивається на блоки 16×16. У даному алгоритмі стійкість стеганоповідомлення забезпечується застосування таблиці квантування, що у два рази більша за стандартну. Метод включає наступні етапи вбудовування інформації: обирається контейнер (бажано, щоб розмір контейнеру був кратний 16) та повідомлення. Повідомлення шифрується за допомогою ASCII та переводиться у бінарний формат, контейнер розбивається на блоки 16×16 та до них застосовується ДКП. Застосовується нова модифікована таблиця квантування 16×16, яка генерує квантовані коефіцієнти альтернативного потоку. Два секретні біти методом LSB вбудовуються в принаймні два значущих біта коефіцієнтів усіх елементів матриці, окрім крайнього лівого, які відповідають значенню 1 у таблиці квантування. Результати досліджень даного методу показали досить високий об’єм вбудованої інформації, але все ж таки метод має і недоліки – використання матриці тільки певного розміру, а саме – кратної числу 16 та відсутнє проведення дослідження на якість вилученої додаткової інформації.

Стаття [26] авторів М. Гунал та Д. Джа висвітлює ідею науковців щодо розробки стійкого методу, використовуючи який можна досягти високих показників відношення пікового сигнал/шум. Основними етапами методу є: необхідне секретне повідомлення зашифрувати за допомогою алгоритму BlowFish; контейнер розділити на блоки 8×8, що є непересічними; до кожного блоку контейнера застосовується ДКП; розрахунок LSB для кожного DC-коефіцієнту і останній біт замінюється на біт додаткової інформації. У порівнянні з методами-аналогами – з використанням ДКП або ДВП – даний алгоритм показав результат PSNR у 71,25 дБ, на відміну від інших – 48,1 дБ та 50,1 дБ відповідно. Серед недоліків слід зазначити високу обчислювальну складність методу за рахунок використання алгоритму Blowfish та відсутність проведення досліджень з використанням атак, стеганографічна система є напівзакритою.

1.3.3 Дослідження в області вейвлет-перетворення

Дослідження в області дискретного вейвлет-перетворення не є такими популярними у порівнянні із дослідженнями в області дискретного косинусного перетворення. Це обумовлено тим, що дискретне косинусне перетворення використовується із форматом JPEG, а вейвлет-перетворення – із форматом JPEG2000. Проте, сучасні дослідження в даній області доводять, що стеганографічні методи, що засновані на використанні ДВП, можуть бути достатньо стійкими до різних видів атак, а також до стиснення JPEG.

Підтвердженням того факту, що стеганографічні методи із використанням ДВП є досить стійкими, є робота “Модифікація стеганографічного методу вбудови цифрового водяного знаку в зображення на основі вейвлетперетворення” [27] Г.В. Ахмаметьєвої та Г.А. Баранюк. Метод був модифікований для того, щоб забезпечити високу точність детектування ЦВЗ в умовах стиску та різних атак, зокрема накладання фільтрів, шумів та застосування афінних перетворень. Метод ґрунтується на наступних кроках: до синьої складової сигналу контейнера застосовується трирівневе вейвлет-перетворення, отримується матриця апроксимуючих та деталізованих коефіцієнтів; ЦВЗ переводиться у полутонове зображення та до нього застосовується ДКП; обирається матриця деталізованих коефіцієнтів для вбудовування таким чином, щоб кількість коефіцієнтів, що перевищують кількісний параметр, що встановлено, було меншим за розмір матриці; вбудовування додаткової інформації відбувається шляхом множення вектору перетвореного ЦВЗ на константу α у ті коефіцієнти ДВП, що більші за параметр, що визначено раніше. Запропонований метод показав дуже високий результат детектування додаткової інформації, навіть при сильному стисненні – при коефіцієнті якості “5” вірогідність детектування ЦВЗ у середньому становить приблизно 95%. Проте метод використовує напівзакриту стеганографічну систему, тобто для детектування інформації необхідно мати вхідний ЦВЗ, метод встановлює лише наявність ЦВЗ у контейнері, але не може його вилучити.

У науковому дослідженні [28] авторів Д. Бабі та Д. Томаса пропонується техніка захисту даних, яка використовується для приховування кількох кольорових зображень в одному за допомогою дискретного перетворення вейвлетів. Приховування інформації відбувається наступним чином: у зображенні-контейнері виділяються кольорові матриці R, G, B та до кожної з них застосовується ДВП, після чого матриця розкладається на 4 діапазони; піддіапазон LL обробляється для отримання наступного значення вейвлет-коефіцієнтів до досягнення деякого остаточного значення; секретне повідомлення аналогічно розділяється на 3 складові матриці сигналу, до кожної з них застосовується ДВП. Піддіапазон LL обробляється далі, щоб отримати наступне значення вейвлет-коефіцієнтів. Інформація, що міститься в області LL секретних зображень, окремо вбудовується в різні області контейнеру. Розглянутому методу відповідають досить непогані результати відпрацювання методу, проте алгоритм не було перевірено на стійкість до атак та якість зображення, після їх проведення.

У роботі [29] Б. Сінга запропоновано новий підхід до стеганографії зображень для підвищення візуальної якості стеганоповідомлення. Зображення-контейнер розкладається за допомогою ДВП, щоб отримати вейвлет-піддіапазони, а також для кожного високочастотного вейвлет-піддіапазону обчислюється порогове значення. Запропоновано напівшістнадцятковий код (SHC) для перетворення значення пікселя секретного зображення в менше – еквівалентне значення, щоб воно якомога менше спотворювало зображення стеганоповідомлення. Недоліком методу можна вважати те, що невідомі результати досліджень на предмет стійкості до атак та детектування додаткової інформації.

“High PSNR based Image Steganography” – стаття індійського вченого Н. Сінга [30]. Даний метод заслуговує окремої уваги, адже в алгоритмі вбудовування секретної інформації використовується ліфтингове вейвлет-перетворення (LWT), ДКП та сингулярний розклад коефіцієнтів ДКП. Дану технологію можна застосовувати як до зображень, так і до відео-файлів. Основні кроки методу: спочатку контейнер та ЦВЗ переводиться у полутонове зображення.

Контейнер розбивається на блоки 8x8, до кожного з них застосовується дискретне косинусне перетворення, а потім – ліфтингове вейвлет-перетворення, використовується сингулярний розклад до області низьких коефіцієнтів по горизонталі та високих по вертикалі (LH / ВЧНЧ), у матрицю сингулярних чисел вбудовується ЦВЗ адитивним шляхом.

Метод показав досить високий результат: показник пікового відношення “сигнал/шум” досягає 51 дБ, проте необхідно зазначити, що стеганографічна система є напівзакритою, а це, у свою чергу, означає, що для детектування додаткової інформації з контейнеру необхідно мати оригінальний ЦВЗ. Цей недолік послугував основою для розробки нового методу, якому для вилучення ЦВЗ не потрібно мати ані оригінальний контейнер, ані оригінальний цифровий водяний знак, до того ж результати роботи системи будуть кращими за результати, що наведені у праці “High PSNR based Image Steganography”.

Отже, зважаючи на проведений вище аналіз різних досліджень в області цифрових водяних знаків та стеганосистем, а також недостатність методів, що забезпечують високу якість стеганоповідомлень, є необхідність розробки нового методу системи цифрових водяних знаків, який буде мати відкриту стеганографічну систему, досить високу якість заповненого контейнеру та стійкість до деструктивного впливу на стеганоповідомлення.

2 РОЗРОБКА СИСТЕМИ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ НА ОСНОВІ DCT-LWT-SVD

2.1 Основні відомості про ліфтингове вейвлет-перетворення

Для вбудовування цифрових водяних знаків зазвичай використовують дискретне косинусне або дискретне вейвлет-перетворення. Проте у 1996 році науковець Свелдемс [31] ввів нове поняття в обробці цифрових зображень – ліфтингове вейвлет-перетворення. На відміну від дискретного вейвлет-перетворення, ліфтингове вейвлет-перетворення не використовує дискретне перетворення Фур'є, тим самим забезпечуючи низьку обчислювальну складність алгоритмів.

Слід зауважити, що дослідження в області LWT раніше проводилися небагато, у порівнянні з стеганографічними методами, що використовують інші області перетворення. Проте за останні кілька років кількість робіт, що присвячено цій сфері, зросла [32-37].

Ліфтингове вейвлет-перетворення піднімає коефіцієнти ДВП. Для отримання коефіцієнтів апроксимації та діапазонів деталей LWT, виконуються наступні кроки:

- поділ (сигнал розділяється на дві частини, що залежать від положення елемента в початковому сигналі – парні і непарні);
- прогнозування (парні вибірки використовуються для передбачення непарних, піксель на непарних позиціях передбачається двома його сусідами на парних позиціях, тоді різниця між передбаченим значенням і реальним непарних значень зберігається в місці розташування непарних вибірок; діапазон деталей створюється шляхом заходження різниці між вихідною непарною вибіркою і передбаченою, яка є середнім значенням двох парних вибірок, прилеглих до непарної);
- оновлення (створює діапазон апроксимацій, оновлюючи середнє значення на значення різниці, яка розраховується на етапі прогнозування) [38].

Зворотний хід схеми ліфтингу здійснюється шляхом зміни порядку дій та

знаку кроку прогнозування та оновлення.

На рисунках 2.1 та 2.2 зображено схеми прямої роботи ліфтингу та оберненої відповідно.

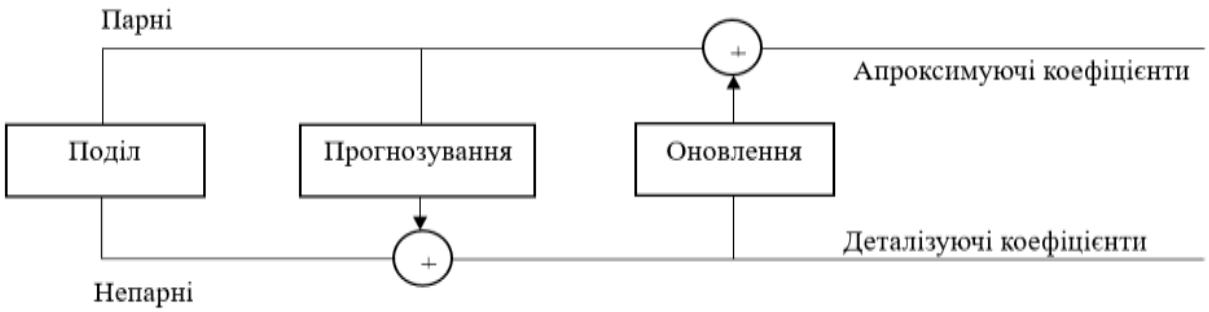

Рисунок 2.1 – Робота ліфтингу

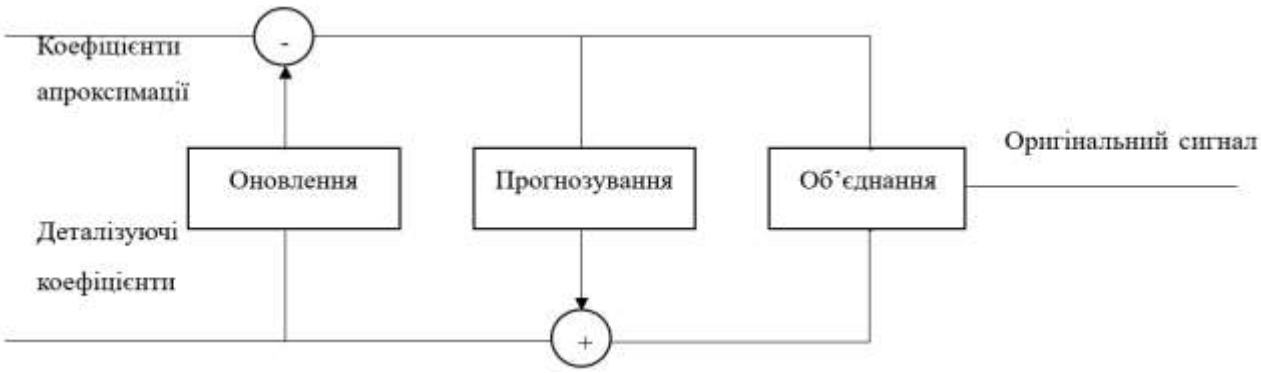

Рисунок 2.2 – Робота оберненого ліфтингу

Хоча дискретне вейвлет-перетворення та ліфтингове перетворення ділять вхідний сигнал (зображення) на деталі та діапазони, кожен з них має свої коефіцієнти, що не є однаковими. Це означає, що результати детектування у цих двох областях будуть відрізнятися.

У роботі Тахи [39] наведено порівняльні значення детектування ЦВЗ з контейнерів, які свідчать про те, що LWT поступається ДВП.

Незважаючи на результати, що представлені у науковій праці Таха, застосування LWT може давати кращі результати з використанням сингулярного розкладу та дискретного косинусного перетворення.

2.2 Розробка системи ЦВЗ

Для реалізації методу вбудови цифрового водяного знаку необхідно обрати цифрове кольорове (RGB) зображення-контейнер та ЦВЗ (полутонове зображення або кольорове зображення, що переведено у градації сірого).

Значення пікселів ЦВЗ з діапазону від 0 до 255 переводиться у діапазон від 0 до 10 розраховується за формулою (2.1):

$$M' = \frac{M}{255} \cdot 10, \tag{2.1}$$

де M – полутонове зображення ЦВЗ, M' – нормований ЦВЗ.

Вбудовування додаткової інформації відбувається наступним шляхом. Обирається одна колірна матриця контейнеру та розбирається на блоки 8×8, що не перетинаються. До кожного з блоків зображення застосовується дискретне косинусне перетворення. Після проведення даної операції до кожної з матриць коефіцієнтів ДКП застосовується LWT. Після операції LWT виділяється діапазон низьких частот – LL та до кожного блоку застосовується сингулярний розклад та визначається матриця сингулярних чисел.

Безпосередньо процес вбудовування буде здійснюватися у перше сингулярне число за формулою (2.2):

$$s_1' = \begin{cases} \left[s_1 / 10 \right] + m', s_1 \geq 20, \\ 1.8m', m' \geq 5, \\ m' + 4, m' < 5, \end{cases} \tag{2.2}$$

де s_1 – перше сингулярне число (СНЧ), s_1' – модифіковане значення першого СНЧ, $m', m' \in M'$ – нормоване значення яскравості ЦВЗ.

Таким чином, в один блок контейнеру можна вбудувати один елемент цифрового водяного знаку.

Проаналізувавши СНЧ матриці діапазону низьких частот ліфтингового вейвлет-перетворення, отримано результати, які пояснюють вибір сингулярного числа для вбудовування ЦВЗ: у переважній більшості друге, третє та четверте СНЧ дуже схильні до округлень. Слід відмітити, що значення m' знаходиться в одному з двох встановлених піддіапазонів: $[0,5)$ та $[5,10]$, до яких застосовуються різні формули вбудовування додаткової інформації. У кінцевому випадку піддіапазон $[0,5)$ дає значення першого сингулярного числа, що відповідають діапазону $[0,9)$, а піддіапазон $[5,10]$ – значення першого СНЧ, що відповідають діапазону $[9,18]$.

Для детектування цифрового водяного знаку виконуються аналогічні дії: обирається колірна матриця захищеного контенту, розділяється на блоки 8×8. До кожного з блоків застосовується DCP, LWT, виділяється піддіапазон низьких частот та використовується SVD, після чого виділяється матриця сингулярних чисел та перше СНЧ. Детектування виконується за формулою (2.3):

$$\tilde{m} = \begin{cases} s_1' - \left\lfloor s_1'/10 \right\rfloor \cdot 10, s_1' \geq 20, \\ s_1'/1.8, s_1' \geq 9, \\ s_1' - 4, s_1' < 9, \end{cases} \qquad (2.3)$$

де $\tilde{m}$ – детектований ЦВЗ, s_1' – перше сингулярне число блоку заповненого контейнеру, $[\bullet]$ - операція округлення до найближчого цілого.

Було проведено експерименти на вбудовування та детектування ЦВЗ при використанні різних складових сигналу зображення та отримано наступні результати, що свідчать про те, що вилучені ЦВЗ відрізняють один від одного: при застосуванні однієї з матриць кількість помилок з точки зору візуальної цілісності ЦВЗ є мінімальною, проте у двох інших спостерігається значне погіршення результату вилучення ЦВЗ. Першою причиною отримання таких результатів є те,

що цифровий водяний знак вбудовується з використанням дискретного косинусного перетворення, ліфтингового вейвлет-перетворення та сингулярного розкладу, кожен з яких призводить до округлення значень коефіцієнтів, а також представлення ЦВЗ в діапазоні $[0,10]$. Також однією з причин введення значень у такий діапазон є те, що вбудовування відбувається шляхом модифікації першого сингулярного числа. Для того, щоб зберегти високу якість повного контейнеру необхідно мало змінити сингулярне число. Проведено дослідження і встановлено, що яскравості оригінального ЦВЗ та вилученого можуть відрізняти на 5-10 одиниць, проте візуальна цілісність зображення зберігається. Саме тому визначення точності детектованого цифрового водяного знаку стандартними показниками аналізу NCC, SIM, BCR може дати низькі показники. Тому запропоновано оцінювати точність вилучення додаткової інформації з контейнеру ступенем подібності, алгоритм розрахунку якого наведено нижче.

Обчислення ступеню подібності.

1. Якщо $\left|m_{i,j}-m'_{i,j}\right|\le 10$, то $count=count+1$, де $m_{i,j}, m'_{i,j}$ k – значення яскравості вбудованого і вилученого ЦВЗ відповідно, $i=\overline{1,H}$, $j=\overline{1,W}$, $H\times W$ - розмір ЦВЗ.
2. Обчислити $SD=\dfrac{count}{H\cdot W}$.

Другою причиною отримання незадовільного результату детектування є неправильно обрана колірна матриця зображення-контейнеру, а саме та, блоки якої містять більшість значень, які прагнуть до 0 або до 255. У разі вбудовування додаткової інформації в такий блок, значення яскравостей пікселів можуть вийти за діапазон [0, 255] і при введенні в той самий діапазон, значення вкладень буде втрачено. При детектування цифрового водяного знаку з такого блоку призведе до виникнення великої кількості помилок. Для підтвердження цього факту на рисунку 2.3 наведено результат детектування цифрового водяного знаку, що було вбудовано у різні складові сигналу: червону, зелену та синю колірну компоненту

сигналу. На рисунку можна помітити як сильно відрізняються однин від одного вилучені ЦВЗ.

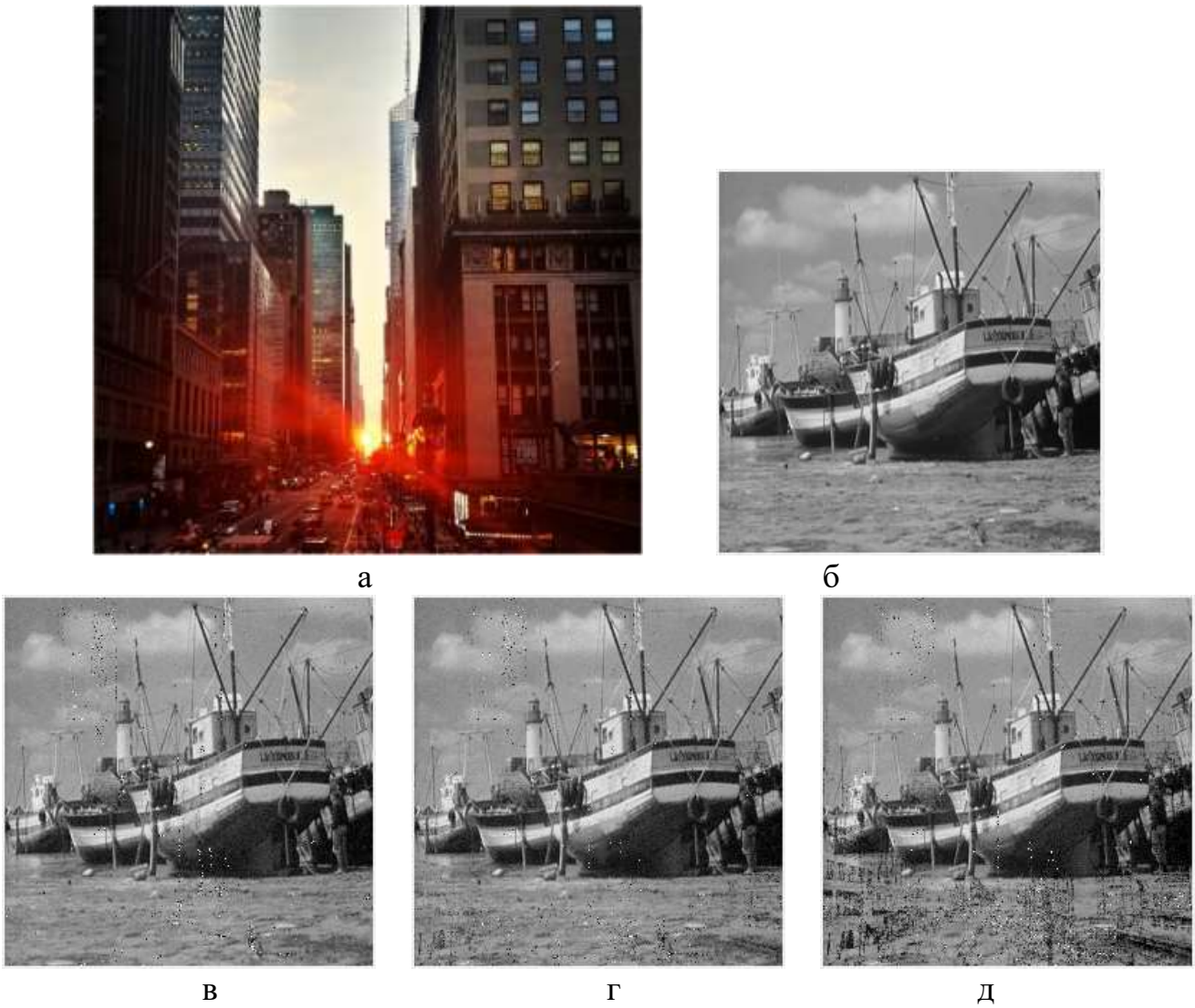

Рисунок 2.3 – Результат детектування ЦВЗ: а – зображення-контейнер, б – оригінальний, в – результат вилучення ЦВЗ з червоної колірної складової сигналу, г – результат вилучення ЦВЗ із зеленої колірної складової сигналу, д – результат вилучення ЦВЗ з синьої колірної складової сигналу

Результати NCC, SIM, BCR детектованого ЦВЗ, що зображено на рисунку 2.3 є наступними: червона колірна складова зображення – SD=0.9408, NCC=0.3788, SIM=0.6724, BCR=0.3106, зелена – SD=0.9142, NCC=0.3651, SIM=0.6657, BCR=0.3175, синя – SD=0.8205, NCC=0.3270, SIM=0.6438, BCR=0.3365. Не дивлячись на те, що показники є низькими, візуальна цілісність цифрового

водяного знаку збережена. Найкращий результат аналізу отримано при використанні матриці червоної складової, а найгірший – при використанні синьої складової сигналу.

Отримавши незадовільні результати детектування, вирішено проводити аналіз RGB-матриць для визначення найбільш підходящої для вбудовування інформації.

Алгоритм вибору колірної складової зображення-контейнеру для вбудови та вилучення цифрового водяного знаку наведено нижче.

1. Розбити колірну складову $I^y, y \in \{R, G, B\}$ розміром $M \times N$ цифрового зображення на блоки B^y розміром 8×8, що не перетинаються.
2. Для кожного блоку B^y:

2.1 Обчислити $R = \sum_{i,j=1}^{8} b_{i,j} / (255 \cdot 64)$.

2.2 Якщо $R < 0.1$, то $E_1^y = E_1^y + 1$, де E_1^y – кількість блоків зі значеннями яскравості, що наближаються до 0, y-ої колірної складової.

2.3 Якщо $R > 0.9$, то $E_2^y = E_2^y + 1$, де E_2^y – кількість блоків зі значеннями яскравості, що наближаються до 255, y-ої колірної складової.

3. Обчислити $P^y = (E_1^y + E_2^y)/k$, де $k = \left\lfloor \frac{M}{8} \right\rfloor \cdot \left\lfloor \frac{N}{8} \right\rfloor$ – кількість блоків 8×8 колірної складової I^y, $\lfloor \bullet \rfloor$ – округлення до меншого цілого.
4. Для вбудови/вилучення ЦВЗ обирається колірна складова з мінімальним значенням P.

Щодо вейвлет-функції, яку використовує метод, необхідно зазначити, що тестування проводилося з усіма материнськими вейвлетами, проте найефективнішими функціями виявилися “Добеші-8” та “Хаара”. Після проведення дослідження, встановлено, що функція “Добеші-8” дає менші спотворення ЦВЗ аніж “Хаара”, хоча показники відношення “піковий сигнал/шум” відрізнялися на декілька одиниць, проте безпосередньо результат вилучення був у рази гірше. Порівняння результатів виявлення ЦВЗ показано на рисунку 2.4.

а

б

в

г

Рисунок 2.4 – Порівняння результатів детектування з використанням різних вейвлетів: а – оригінальне зображення-контейнер, б – оригінальний ЦВЗ, в – вилучений ЦВЗ з вейвлетом “Хаара”, г – вилучений ЦВЗ з вейвлетом “Добеші-8”

З огляду на результати проведених досліджень при формуванні основних кроків розроблюваного методу слід враховувати наступні моменти:

- система є відкритою (для детектування додаткової інформації не потрібно знати оригінального контейнеру або/та ЦВЗ);
- проведення аналізу ступеню подібності вилученого ЦВЗ та оригінального;
- перед вбудовуванням водяного знаку, необхідно провести аналіз матриць та вибрати найбільш підходящу;
- використання вейвлет-функції “Добеші-8”.

Отже, сам процес вбудовування ЦВЗ включає у себе наступні етапи.

1. Визначення складової сигналу зображення для вбудови цифрового водяного знаку.

2. Нормалізація ЦВЗ згідно з формулою (2.1).
3. Обрану матрицю сигналу ЦЗ I розміром $M \times N$ розбити на блоки B розміром 8×8, що не перетинаються.

Для кожного блоку B виконати кроки 4-10.

4. Виконати дискретне косинусне перетворення. Результат – B_{dct}.
5. До коефіцієнтів DCT B_{dct} застосувати ліфтингове вейвлет перетворення. Результат – матриці LL, LH, HL, HH розміром 4×4.
6. Для матриці LL виконати сингулярне розкладання. Результат – S – матриця СНЧ, U, V – матриці сингулярних векторів.
7. Замінити перше СНЧ у відповідності з формулою (2.2).
8. Відновити матрицю низьких частот LL': $LL' = U \cdot S' \cdot V$, де S' – модифікована матриця СНЧ.
9. Застосувати обернене ліфтингове перетворення. Результат – B'_{dct}.
10. Виконати обернене дискретне косинусне перетворення. Результат – B'.
11. Зберегти заповнений контейнер.

Схематично етапи вбудовування ЦВЗ представлені на рисунку 2.5.

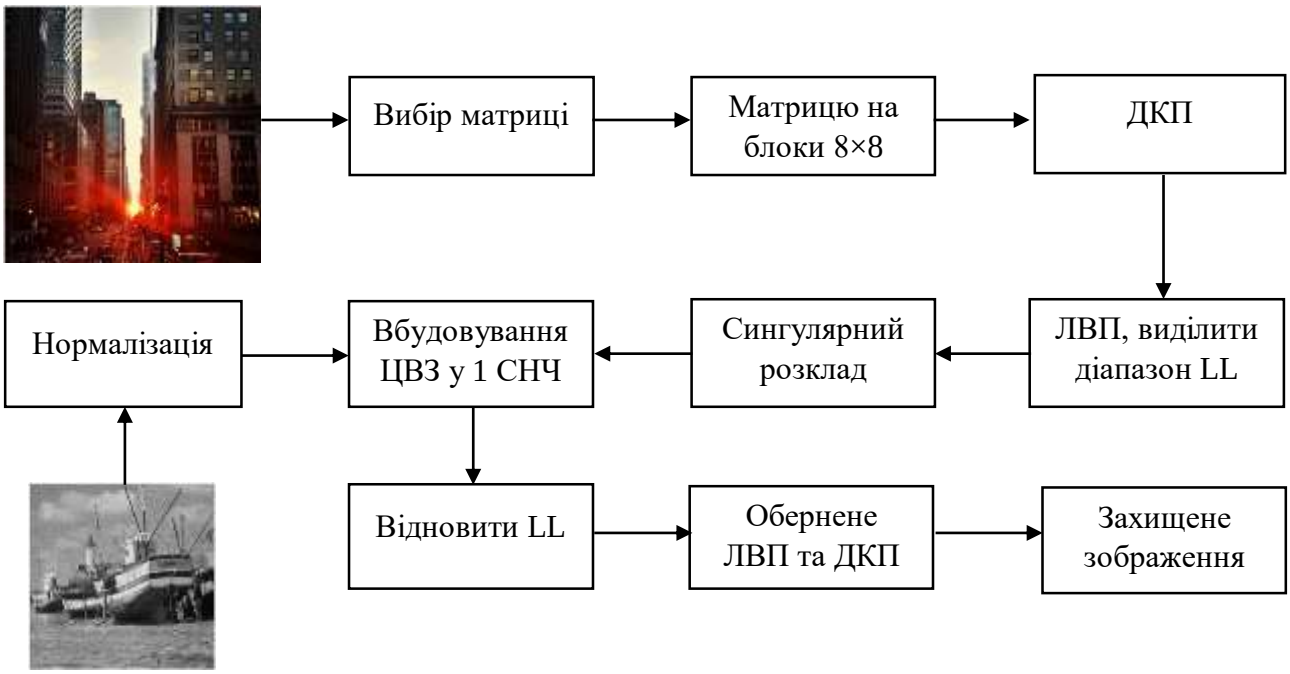

Рисунок 2.5 – Схема вбудовування ЦВЗ

Детектування цифрового водяного знаку проводить наступним чином.

1. Визначити колірну складову для детектування ЦВЗ.
2. Обрану колірну складову ЦЗ I' розміром $M \times N$ розбити на блоки B' розміром 8×8, що не перетинаються.
3. Виконати дискретне косинусне перетворення. Результат – B'_{dct}.
4. До коефіцієнтів DCT B'_{dct} застосувати ліфтингове вейвлет перетворення. Результат – матриці LL', LH', HL', HH' розміром 4×4.
5. Для матриці LL' виконати сингулярне розкладання. Результат $-S'$ – матриця СНЧ, U', V' – матриці сингулярних векторів.
6. Обчислити нормалізоване значення ЦВЗ у відповідності з формулою (2.3).
7. Перевести нормалізоване значення до діапазону $[0, 255]$ у відповідності з формулою (2.4).
8. З отриманих значень яскравості сформувати ЦВЗ.

Схематично детектування продемонстроване на рисунку 2.6.

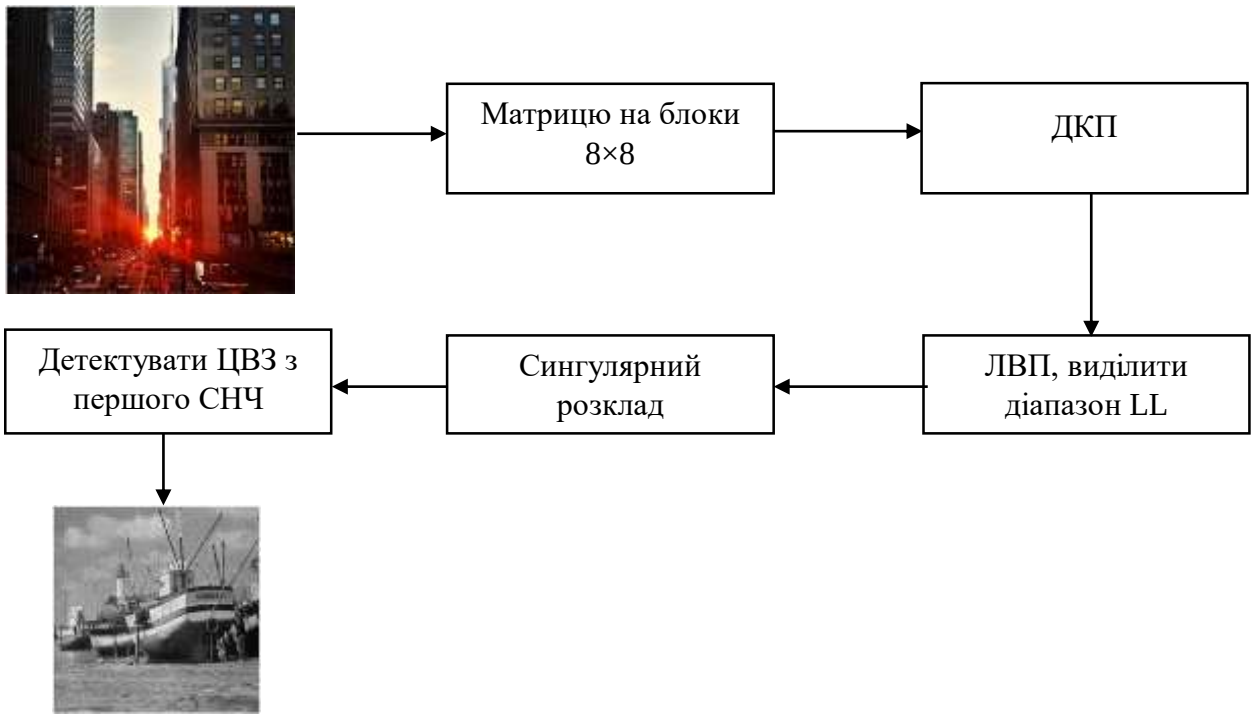

Рисунок 2.6 – Схема детектування ЦВЗ

Проведено дослідження ефективності запропонованого методу на основі 200 цифрових зображень з використанням різних цифрових водяних знаків. Ефективність методу оцінюється показником пікового відношення “сигнал/шум” (PSNR), шляхом порівняння оригінального зображення-контейнеру та заповненого, а також ступенем подібності детектованого ЦВЗ та вбудованого ЦВЗ.

Також метод перевірено на стійкість до різних видів атак: гаусів та мультиплікативний шум, шум “сіль/перець”, фільтр підвищення різкості “Unsharp” та медіанний фільтр. Результати представлені у таблиці 2.1.

Таблиця 2.1 – Ефективність вилучення ЦВЗ із заповненого контейнеру

Атака	Параметр	Середнє значення PSNR, дБ	Середнє значення ступеню подібності, %
Без атаки		50.45	93.85
Гаусів шум	$m = 0.0001,$ $d = 0.0000005$	48.67	93.44
	$m = 0.001,$ $d = 0.00005$	50.40	81.86
Мультиплікативний шум	$d = 0.0001$	50.45	81.76
	$d = 0.00001$	41.96	85.73
	$d = 0.000001$	48.62	93.72
Шум “Сіль та перець”	$d = 0.0001$	44.01	93.50
Фільтр підвищення різкості “Unsharp”		41.79	35.20
Медіанний фільтр		39.50	50.47

Виходячи з результатів тестування, можна сказати, що метод є ефективним при збереженні повного контейнеру у форматі без втрат: значення PSNR знаходиться у межах від 46,71 дБ до 55,36 дБ, забезпечується висока пропускна здатність прихованого каналу зв’язку, що перевищує результати існуючих аналогів. Також метод виявився стійким до усіх вищезгаданих накладених шумів: показники PSNR для гаусового шуму знаходяться у проміжку між 48,66 дБ до 55,21 дБ, для мультиплікативного шуму – від 42,6 дБ до 55,34 дБ, для шуму “Сіль та перець” - від 35,63 дБ до 48,22 дБ, а також середні значення ступеню подібності

перевищують 81%. Але метод виявився нестійким до атаки фільтрацією: незважаючи непогані показники PSNR, значення ступеню подібності є занизькими.

Розроблений метод перевірено на стійкість до атаки стисненням: повний контейнер було збережено з коефіцієнтами якості від 60 до 100 з кроком 5. Отримані результати наведено у таблиці 2.2.

Таблиця 2.2 – Ефективність детектування ЦВЗ з повного контейнеру, що збережено у форматі JPEG

Показник якості		*QF*								
		60	65	70	75	80	85	90	95	100
Середнє значення PSNR, дБ		38.9	40.7	42.9	47.9	44.5	43.6	46	47.1	47.8
	Подібність ЦВЗ									
Ступень подібності, %	Максимальне значення	87.5	89.2	88.1	88.9	87.9	87.8	87.8	89.2	91.9
	Мінімальне значення	1.8	1.9	1.8	2.2	2.5	2.5	1.6	1.5	2.2
	Середнє значення	28.9	26.8	26.8	24.1	25	26.7	27.9	29.2	34.2

Результати дослідження показали, що при стисненні показники подібності вбудованого та вилученого ЦВЗ знаходяться в діапазоні від 1,5% до 91,5%. Проте, незважаючи на низькі показники після стиснення, вилучений ЦВЗ залишається візуально помітним і зберігає можливість визначення автора (рисунок 2.7 і 2.8).

а

б

Рисунок 2.7 – Оригінальні зображення: а – контейнер розміром 1200×1200, б – ЦВЗ розміром 150×150

а б в

Рисунок 2.8 – Результати детектування ЦВЗ після атаки стисненням:
а – вилучений ЦВЗ зі стиснутого з $QF = 100$ заповненого контейнеру(SD=15.72%);
б – вилучений ЦВЗ зі стиснутого з $QF = 90$ заповненого контейнеру(SD=1.88%);
в – вилучений ЦВЗ зі стиснутого з $QF = 80$ заповненого контейнеру(SD=1.52%)

Отже, розроблений метод забезпечує достатньо високу якість заповненого контейнеру, високу пропускну здатність прихованого каналу зв’язку та ступінь подібності вбудованого та вилученого ЦВЗ, а також є стійким майже до усіх видів атак, його можна використовувати за призначенням. Для забезпечення швидкого використання методу, розроблено програмний продукт, який буде описано у наступному розділі.

3 РОЗРОБКА ПРОГРАМНОГО ПРОДУКТУ

3.1 Середовище розробки програмного продукту

Реалізація програмного інтерфейсу запропонованого методу вбудови цифрових водяних знаків на основі дискретного косинусного перетворення, ліфтингового вейвлет-перетворення та сингулярного розкладу проводилася у середовищі Matlab. Matlab – високорівнева мова технічних розрахунків, інтерактивне середовище розробки різних алгоритмів та сучасний засіб аналізу даних. Мова Matlab – мова матриць та масивів високого рівня з управлінням потоками, функціями, структурами даних, вводом-виведенням та особливостями об’єктно орієнтованого програмування [40]. Область застосування даного середовища велика: захист інформації, IoT, обробка сигналів, фінанси, розробка систем управління, автоматика, інженерія, робототехніка та інше.

У порівнянні з іншими мовами програмування, слід відмітити, що Matlab має велику кількість вбудованих функцій (Toolboxes), які використовуються для розрахунків та аналізу, цим самим оптимізуючи код, а також зберігає час користувача на написання усіх функцій та дій, які програма повинна виконати.

До переваг використання середовища Matlab необхідно віднести:

- простота написання коду/скрипту, на відміну від інших мов;
- використання вбудованих функцій;
- інтегроване середовище розробки;
- висока швидкість обробки даних;
- засоби інтеграції з C/C++;
- вбудована матрична та комплексна арифметика;
- легка адаптація до конкретних завдань користувача;
- обробка помилок;
- створення власних функцій та використання їх як шаблонів;
- об’єктно-орієнтована направленість;
- проектування та імітація нейронних мереж;
- можливість створення додатків та програмних продуктів;

- розпаралелення виконання операцій програми;
- візуалізація аналізу та обробки даних з використанням 2D і 3D графіки [41, 42].

Використовуючи Matlab, код записується у файл-скрипт або у файл-функцію. Відмінність між цими файлами полягає у тому, що функції мають власний робочий простір і вхідні та вихідні дані, скрипти – використовують тільки загальний простір. Скрипт/функцію, що написано у цих файлах, зберігається у вигляді текстового документу і не переводиться у машинний код.

Так як основним об'єктом аналізу даної кваліфікаційної роботи є зображення, Matlab у своїй системі має пакет для швидкого виконання усіх дій – Image Processing Toolbox, що значно спрощує роботу дослідника. Image Processing Toolbox має такі функції, як:

- робота з графічними форматами файлів;
- зміна формату представлення даних;
- визначення типу зображення та перетворення типів даних;
- виведення зображення на екран;
- конвертація колірних систем;
- геометричні перетворення зображення;
- аналіз зображень, їх покращення;
- фільтрація та сегментація зображень;
- перетворення Фур'є, ДКП, сингулярний розклад, ЛВП, ДВП;
- операції з масивами [43].

Програмні модулі GUIDE та App Designer – конструктори, які використовуються для розробки програмного інтерфейсу. Усі необхідні інтерактивні елементи можна з легкістю запрограмувати та допомогою виклику функції "callback" є змога описати поведінку кожної компоненти інтерфейсу.

Враховуючи все вищесказане, можна зробити висновок, що середовище програмування Matlab якнайкраще підходить для вирішення поставленої задачі, а саме реалізацію запропонованого методу. Для розробки інтерфейсу обрано модуль App Designer.

3.2 Розробка програмного коду метода

Розробка програмного коду починається із завантаження контейнеру та ЦВЗ, що переводиться у полутонове зображення (рисунок 3.1). Для контейнеру проводиться аналіз колірних складових сигналу щоб обрати найбільш підходящу матрицю. На рисунку 3.2 показано початковий етап аналізу матриць контейнеру.

```
image=imread('Container\1.jpg');
figure; imshow(image);
container_R=image(:,:,1);
container_G=image(:,:,2);
container_B=image(:,:,3);
stego=image;

Mess=imread('C:\Users\anya_\Downloads\boat.512.tiff');
Mess=rgb2gray(Mess);
k=8;%размір блоку
```

Рисунок 3.1 – Завантаження контейнеру та ЦВЗ, визначення розміру блоку зображення

```
%R
[A,C]=size(container_R);
P=A*C;
A0 = A+(k-mod(A,k)) ;
C0 = C+(k-mod(C,k)) ;

I1 = uint8(zeros(A0,C0)) ;
I1(1:A,1:C) = container_R ;

A0 = A0/k ;
C0 = C0/k ;

if A0>C0
    A1=C0;
else
    A1=A0;
end

BLOCKS = mat2cell(I1, repmat(k,[1 size(I1,1)/k]), repmat(k,[1 size(I1,2)/k]));
```

Рисунок 3.2 – Вилучення червоної складової сигналу, розбиття зображення на блоки необхідного розміру

Операції, що показані на рисунку 3.2 ідентичні для кожної колірної матриці зображення. Після розбиття контейнеру на блоки, встановлюється розмір матриці цифрового водяного знаку для уникнення спотворення розмірів при вилученні (рисунок 3.3) та вводиться лічильники для встановлення кількості блоків, що прагнуть до 0 або до 255: розраховується сума елементів кожного блоку та нормалізується (вводиться в діапазон [0, 1]). Підраховується кількість блоків, що є меншими або більшими за 0.1 чи 0.9 відповідно (рисунок 3.4).

```
Mess=imresize(Mess,[A0-1 A1-1]);
mess=double(Mess)/255;
[M,N]=size(mess);
```

Рисунок 3.3 – Нормалізація ЦВЗ

```
% Впровадження лічильника
EE1=0; %R
EE2=0;
R=0;

for i=1:1:A0-1
    for j=1:1:C0-1
        var_BLOCKS(i,j) = [BLOCKS(i,j)];
        a=var_BLOCKS(i,j);
        block_var=cell2mat(a);
        K=sum(block_var);
        K=sum(K);
        R=K/(255*64);

        if R<0.1          %прагнуть до 0
            EE1=EE1+1;
        elseif R>0.9      %прагнуть до 255
            EE2=EE2+1;
        end

    end
end
count_block_R=(EE1+EE2)/8;
```

Рисунок 3.4 – Розрахунок кількості блоків, що не підходять для вбудови цифрового водяного знаку

Дії, аналогічні тим, що представлено на рисунку 3.3 виконуються для кожної матриці сигналу контейнеру. Коли кількість блоків, що не підходять для забезпечення ефективного вбудовування та вилучення додаткової інформації, розраховано, обирається та матриця, у якої кількість таких блоків буде меншою. На рисунку 3.5 – вибір матриці (n – колірний сигнал зображення). Змінні “count_block_R”, “count_block_G”, “count_block_B” відповідають блокам матриць червоної, зеленої та синьої колірної компоненти сигналу відповідно, що є результатом умови вище. “BLOCKS”, “BLOCKS1” та “BLOCK2” – колірні матриці блоків зображення, що обрано на попередньому етапі.

```
if count_block_R<count_block_G & count_block_R<count_block_B

    BLOCKS = BLOCKS;
    n=1;

elseif count_block_G<count_block_R & count_block_G<=count_block_B

    BLOCKS=BLOCKS1;
    n=2;

elseif count_block_B<=count_block_R & count_block_B<count_block_G

    BLOCKS =BLOCKS2;
    n=3;

end
```

Рисунок 3.5 – Вибір матриці для вбудовування інформації

Безпосередньо час процес вбудовування інформації представлено на рисунку 3.6: до кожного блоку зображення застосовується дискретне косинусне перетворення, потім – ліфтингове вейвлет-перетворення, виділяється діапазон низьких частот, після – сингулярний розклад. Використовуючи формулу 2.2, що наведено у розділі 2, ЦВЗ вбудовується у цифрове зображення. Змінна “block_var” містить у собі матрицю блоку раніше обраної колірної складової зображення-

контейнеру. Змінна “DCT_BLOCK” - матриця коефіцієнтів ДКП блоку зображення. “S_lh” - матриця сингулярних чисел. “ss2_1” та “ss2_2” - нормалізований ЦВЗ, що буде вбудовано у контейнер.

```
for i=1:1:A0-1
    for j=1:1:C0-1
        var_BLOCKS(i,j) = [BLOCKS(i,j)];
        a=var_BLOCKS(i,j);
        block_var=cell2mat(a);
        DCT_BLOCK=dct2(block_var);
        [ll,hl,lh,hh] = lwt2(DCT_BLOCK,'db8');
        [U,S,V]=svd(ll);
        [M,N]=size(U);
        S_lh=S;
        s1=S(1,1); s2=S(2,2); s3=S(3,3);
        ss2_1=mess(i,j)*10;
        ss2_2=mess(i,j);

        if s1>=20
            d=floor(s1/10);

        elseif ss2_1>=5
            S_lh(1,1)=d*10+ss2_1;
            S_lh(1,1)=ss2_1*1.8;

        else %ss2_1<5
            S_lh(1,1)=4+ss2_1;
            S_lh(2,2)=ss2_1;
        end
```

Рисунок 3.6 – Вбудовування ЦВЗ у цифрове зображення

Завершаючий етап – відновлення матриці низьких частот, застосування зворотного ліфтингового перетворення, зворотного дискретного косинусного перетворення та отримання захищеного повного контейнеру (рисунок 3.7). Змінна “new_BLOCK” - результат вбудови цифрового водяного знаку, “stego_BLOCKS” - колірна матриця з додатковою інформацією, “stego” - зображення, що захищено цифровим водяним знаком.

```
for i=A0:1:A0
    for j=1:1:C0
        new_BLOCKS{i,j}=BLOCKS{i,j};
        new_BLOCKS{i,j}=double(new_BLOCKS{i,j});
    end
end

for i=1:1:A0
    for j=C0:1:C0
        new_BLOCKS{i,j}=BLOCKS{i,j};
        new_BLOCKS{i,j}=double(new_BLOCKS{i,j});
    end
end

stego_BLOCKS = cell2mat(new_BLOCKS);
[bX,bY]=size(container_B);
stego_BLOCKS=stego_BLOCKS(1:bX,1:bY);

stego(:,:,n)= uint8(stego_BLOCKS);
imshow(stego);
```

Рисунок 3.7 – Отримання захищеного зображення

Детектування відбувається наступним чином. Завантажується цифрове зображення, у якому знаходиться ДІ. Зображення розділяється на 3 колірні матриці, кожна з яких розбивається на блоки 8x8. Проводиться аналіз матриць (рисунок 3.8).

```
if block_stego_R<block_stego_G & block_stego_R<block_stego_B
    BLOCKS = mat2cell(I1,repmat(k,[1 size(I1,1)/k]),repmat(k,[1 size(I1,2)/k]));
    BLOCKS = BLOCKS;
    n=1;
    WM=WM;
elseif block_stego_G<block_stego_R & block_stego_G<block_stego_B
    BLOCKS1 = mat2cell(I11,repmat(k,[1 size(I11,1)/k]),repmat(k,[1 size(I11,2)/k]));
    n=2;
    BLOCKS=BLOCKS1;
    WM=WM1;
elseif block_stego_B<=block_stego_R & block_stego_B<=block_stego_G
    BLOCKS2 = mat2cell(I12,repmat(k,[1 size(I12,1)/k]),repmat(k,[1 size(I12,2)/k]));
    BLOCKS =BLOCKS2;
    WM=WM2;
n=3;
```

Рисунок 3.8 – Аналіз стего

До кожного блоку обраної матриці застосовується ДКП, ЛВТ, виділяється діапазон низьких частот та застосовується сингулярний розклад. Враховуючи особливості зміни значень сингулярних чисел, реалізується процес вилучення ЦВЗ за формулою (2.3), яку наведено у другому розділі роботи (рисунок 3.9).

```
for i=1:1:A0-1
    for j=1:1:C0-1
        var_BLOCKS(i,j) = [BLOCKS(i,j)];
        a=var_BLOCKS(i,j);
        block_var=cell2mat(a);
        DCT_BLOCK=dct2(block_var);
        [ll,hl,lh,hh] = lwt2(DCT_BLOCK,'db8');
        [U,S,V]=svd(ll);

        s1=S(1,1); s2=S(2,2);
        s2x=S(1,1);
        dx=floor(s2/10);
        if s1>=20
            dx=floor(s1/10);
            wm=s1-dx*10;
        elseif s1>=9
            wm=s1/1.8;
        else %s2x<9
            wm=s1-4;
        end
        wm=round(wm/10*255);
```

Рисунок 3.9 – Процес вилучення ЦВЗ з контейнеру

3.3 Реалізація програмного продукту

Програмний інтерфейс було реалізовано з використанням додатку App Designer. App Designer – сучасний інструмент для розробки програмного інтерфейсу від програмного забезпечення Matlab. На відміну від GUIDE, код записується не у файл з розширенням “.m” або “.fig”, а у файл “.mlapp”. Написати власний інтерфейс можна за допомогою макету для додатків. Вікно макету називається “Design View”, а редактор (безпосередньо код) – “Code View”. Для усіх

елементів інтерфейсу можна написати функції, так звані “відгуки” (“callbacks”), натиснення на яких буде задавати певну дію, що прописана у функції.

Інтерфейс програмного продукту для використання методу систем цифрових водяних знаків на основі DCP-LWT-SVD складається з двох вкладок: перша – “Вбудовування ЦВЗ”, друга – “Детектування ЦВЗ”. Перша вкладка містить у собі елементи, що описано нижче.

Кнопка “Обрати контейнер” відповідає за завантаження цифрового зображення, яке необхідно захистити. Після натиснення даної кнопки відкриється папка с великою кількістю зображень на вибір (рисунок 3.10). Обравши необхідний контейнер, програма виводить його на осях, що розташовані біля кнопки.

Рисунок 3.10 – Вибір та завантаження контейнеру

Кнопка “Обрати ЦВЗ” завантажує цифровий водяний знак, який необхідно вбудувати у контейнер. Натиснувши дану кнопку, відкриється папка із запропонованими зображеннями. Обраний результат буде розміщено на осях біля кнопки (рисунок 3.11)

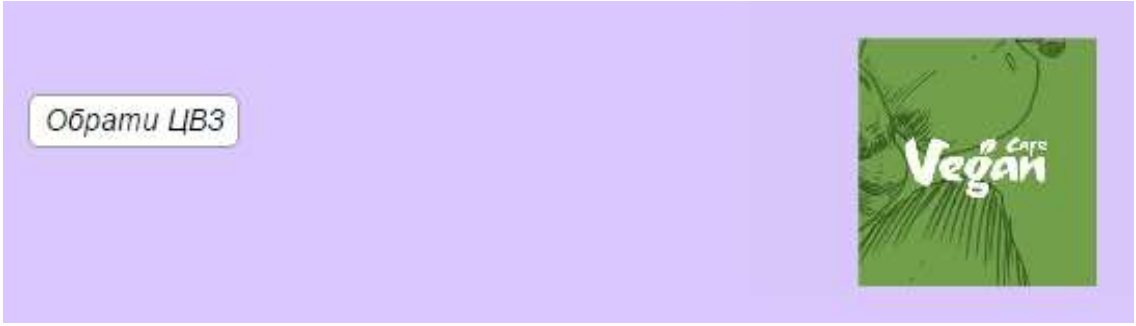

Рисунок 3.11 – Вибір ЦВЗ

Натиснувши кнопку “Вбудувати ЦВЗ”, відбувається процес вбудовування додаткової інформації у контейнер. Алгоритм вбудовування наведений у пункті 2.2. Після завершення виконання програми, захищене зображення зберігається у спеціальній бібліотеці з аналогічними зображеннями та результат виводиться на осі, що відведено для демонстрації повного контейнеру (рисунок 3.12).

Рисунок 3.12 – Результат вбудови ЦВЗ

Також, для проведення аналізу якості отриманого стеганоповідомлення, інтерфейс має спеціальне текстове поле, у якому виводиться значення показника відношення пікового “сигнал/шум” (рисунок 3.13).

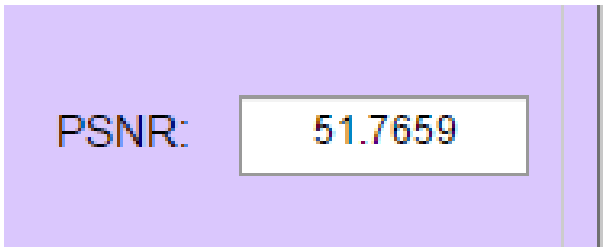

Рисунок 3.13 – Виведення значення PSNR

Друга вкладка призначена для детектування додаткової інформації з повного контейнеру. Вона складається з наступних елементів інтерфейсу.

Кнопка “Завантажити стего” призначена для вибору зображення, яке вважається захищеним. Натисненням даної кнопки, програма завантажує необхідний цифровий контент та відображає його на осях (рисунок 3.14).

Рисунок 3.14 – Завантаження повного контейнеру

Кнопка “Детектувати ЦВЗ” відповідає за виконання алгоритму вилучення цифрового водяного знаку з контейнеру, що наведено у пункті 2.2 попереднього розділу. Результат вилучення відтворюється на осях поруч з кнопкою (рисунок 3.15).

Рисунок 3.15 – Вилучення ЦВЗ

Натиснувши кнопку “Аналіз” програма проведе розрахунок ступеню подібності між вбудованим та вилученим ЦВЗ. Результат аналізу буде наведено у текстовому полі (рисунок 3.16).

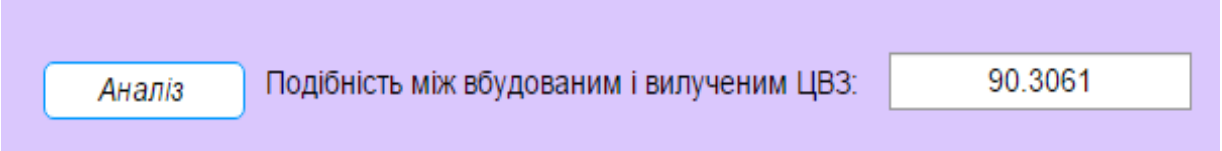

Рисунок 3.16 – Ступінь подібності вбудованого і вилученого ЦВЗ

Кнопка “Оновити дані” відповідає за очищення робочого інтерфейсу від попередньої інформації: зображень та результатів проведеного аналізу.

Загальний вигляд інтерфейсу наведено у Додатку А, код програмного продукту – Додаток Б.

У результаті розроблення програмного продукту, створено зручний користувацький інтерфейс, що розділено на дві вкладки. У кожній з вкладок елементи розташовані у прямій послідовності їх використання, що дає змогу виконати усі операції безпомилково. Програма досить швидко виконує поставлені задачі, проте сам процес вбудовування та детектування займає трохи більше часу у порівнянні із проведенням аналізу та завантаженням зображення. Не дивлячись на цей невеликий недолік, даний програмний продукт можна використовувати для вирішення задач системи цифрових водяних знаків із використання DCT-LWT-SVD.

4 ОХОРОНА ПРАЦІ І БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Аналіз умов праці і вибір заходів і засобів захисту від небезпечних і шкідливих виробничих факторів

Розробка системи вбудови цифрових водяних знаків в зображення на основі DCT-LWT-SVD виконується за допомогою персонального комп'ютеру (ПК). Відповідно, необхідно розглянути та проаналізувати робоче місце користувача ПК.

Робоче місце користувача знаходиться у приміщенні, площею 15 м^2 та загальним об'ємом 45 м^3. Категорія робіт, що виконується – перша (а) категорія. Кабінет має суміщену вентиляцію, а саме: природна вентиляція – неорганізована, забезпечується тепловим та вітряним напором, механічна вентиляція – загальнообмінна витяжна. Для додаткової нормалізації мікроклімату присутнє кондиціонування повітря у приміщенні.

У кабінеті присутнє центральне опалення, яке являє собою водяне опалення низького тиску.

У приміщенні є штучне та природнє освітлення. Штучне освітлення є комбінованим, а саме: загальне освітлення – світильники (4 люмінесцентні лампи денного світла із покращеною передачею кольорів) із розсіювачами та екрануючими гратами [44] знаходиться на висоті 3 м над рівнем підлоги, місцеве – світильник (люмінесцентна лампа денного світла із покращеною передачею кольорів) із просвічуючим відбивачем, розташований на робочому місці.

Природнє освітлення у приміщенні представлено вікном у зовнішній стіні, що орієнтовано на північний схід. Площа світлового прорізу складає 3,06 м^2. Вікно оснащене жалюзі для коригування рівня освітлення кімнати; предметів, що ускладнюють проходження денного світла у кабінет, немає. Природнє освітлення має ряд переваг над штучним, зокрема позитивно впливає на організм людини, приміщення, під його дією, зігрівається та знезаражується, проте існує і суттєвий недолік – воно не є постійним упродовж дня та різних пір року, а також не може забезпечити необхідний рівень освітленості на робочому місці.

Мікроклімат на робочому місці відповідає усім нормам: у холодний період року температура повітря становить від 22˚ до 24˚ за Цельсієм та відносна вологість складає від 40% до 60%, у теплий період температура – від 23˚ до 25˚ за Цельсієм, відносна вологість – 40% – 60% (ДСН 3.3.6.042-99 [45]).

Безпосередньо робоче місце користувача знаходиться на відстані 1,5 метри від вікна, що зліва, та на відстані 0,5 та 1,5 метрів від стін приміщення і представлене робочим столом, на якому розташовані монітор, клавіатура, миша, камера, принтер-сканер, джерело місцевого штучного освітлення. Є достатня кількість простору для встановлення робочих органайзерів.

Робочий стіл має наступні параметри: висота – 750 мм, ширина – 1500 мм, глибина – 1000 мм. Такі характеристики дозволяють розташувати усі предмети, що вказані вище, так, як буде зручно користувачеві, але із дотриманням усіх норм. Стіл оснащений підставкою для ніг, шириною 700 мм, що дозволяє підтримувати оптимальне положення тіла.

Крісло-стілець має функцію регулювання висоти положення тіла відносно столу (оптимальною є висота 400 мм від рівню підлоги) та регулювання спинки (кут її нахилу та висоту). Крісло є стійким та дозволяє людині вільно пересуватися. Воно оснащене підлокітниками для забезпечення прийняття комфортного положення виконавцем робіт. Матеріали спинки та сидіння повинні бути виконані з напівм’яких матеріалів, що легко очищаються (дотримано вимог [46]).

Монітор розташований на відстані 700 мм від органів зору, перпендикулярно лінії зору. Присутня можливість зміни кута нахилу, висоти та кута повороту екрану. Так як робочий екран – ЖК-екран, забезпечено мінімальні випромінювання. Екран є стабільним, без миготіння, із встановленням комфортної яскравості та контрастності.

Клавіатура розташована на спеціальній поличці, що виїздить з-під поверхності столу, та знаходиться на відстані 250-300 мм від її краю. Вона має спеціальні підставки для встановлення зручного кута нахилу (5˚-15˚) для оптимального положення рук. Поверхня пристрою є матовою.

Принтер-сканер встановлено на відстані 400 мм зліва від монітору, що дає змогу користуватися ним не встаючи з робочого крісла. Принтер має низький рівень шуму та випромінювання.

Щодо оздоблення кімнати, поверхня підлоги є рівною, матовою та неслизькою, а інтер'єр виконано у нейтральних тонах, без застосування полімерних матеріалів, що можуть виділяти шкідливі хімічні речовини (ДСанПіН 3.3.2.007-98).

У кабінеті є шафа, що розташована позаду робочого місця, яка щільно прилягає до стіни. Вона призначена для зберігання документів, флеш-накопичувачів, дисків та аптечки.

Приміщення, у якому знаходиться робочий кабінет, має кімнату відпочинку для фізичного та психологічного розвантаження. Вона обладнана місцем відпочинку (диванами), пристроями для зберігання та підігріву їжі, а також пристроями для приготування тонізуючих напоїв.

Необхідно провести аналіз небезпечних виробничих факторів

До небезпечних виробничих факторів для користувача персонального комп'ютеру слід віднести ураження електричним струмом – отримання електротравми. Небезпека такої травми несе непередбачувані наслідки, а саме: невідомо, чи буде жити людина після отриманих ушкоджень.

Найбільш поширеними причинами електротравматизму при роботі з ПК є:

- поява напруги там, де за нормальних умов її не повинно бути (наприклад, пошкодження ізоляції);
- недостатня навченість працівників та відсутність перевірок рівня знань персоналу з даного питання або некваліфікований інструктаж;
- порушення правил технічної експлуатації засобів;
- використання засобів, що не відповідають умовам робіт або є несправними;
- застосування пошкоджених кабелів та проводів;
- живлення декількох пристроїв від загального пускового пристрою;
- дотик до струмоведучих частин під напругою.

Ураження електричним током справляє на тіло людини термічну, електричну, механічну та біологічну дії. Внаслідок термічної дії, тканини людини нагріваються, волога випаровується та з'являються опіки різних ступенів усіх видів біологічних тканин; електричної дії – розклад органічних рідин, у тому числі крові; механічної дії – ушкодження різних тканин організму людини шляхом їх розриву та розшарування; біологічної дії – порушення нормальної роботи нервової системи, що призводить до збудження та подразнення тканин.

До електротравм слід віднести опіки, металізацію шкіри, електричні знаки, електричні удари, механічні пошкодження, електроофтальмія.

Серед засобів захисту від ураження електричним током використовують заземлення, занулення, захисне вимкнення, електричну ізоляцію, використання малої напруги та розташування струмоведучих частин на недосяжній висоті.

Захисне заземлення – навмисне електричне з'єднання з землею або з її еквівалентом металевих неструмоведучих частин, які можуть опинитись під напругою. У даному випадку напруга в мережі становить 220 В, опір захисного заземлення не перевищує 4 Ом. Занулення – головний спосіб захисту від електротравм у випадку дотику до металевих конструкцій, що опинились під напругою в наслідок пошкодження ізоляції [47].

Для уникнення ймовірності ураження електричним струмом забороняється використовувати несправні розетки та вимикачі, пошкоджені кабелі та дроти, або якщо їх ізоляція відсутня чи зіпсована, саморобні пристрої та обігрівачі, що заборонені на підприємстві, закривати або накривати засоби опалення, вмикати саморобні пристрої.

Потрібно виділити шкідливі виробничі фактори, які існують при роботі з персональним комп'ютером.

Шкідливими виробничими факторами можуть бути: підвищена або низька температура повітря робочої зони, зависока або низька вологість повітря та швидкість його руху, підвищений рівень шуму, вібрації, випромінювання, недостатня або надмірна кількість освітлення; запиленість приміщення, психофізіологічні фактори.

Підвищена або низька температура повітря робочої зони впливають на стан та самопочуття робітника безпосередньо. За підвищеної температури повітря людина буде відчувати дискомфорт та згодом може отримати перегрів, гіпертермію. Занизька температура повітря призведе до переохолодження організму та спровокує появу захворювань, таких як застуда.

Висока або низька вологість повітря також впливають на організм людини, що виконує роботу. Висока вологість призводить до накопичення конденсату на робочій поверхності, вікнах, техніці. Недостатня вологість повітря може спричинити пересушування слизових оболонок, шкіри та її потріскування, а також розмноження різних бактерій.

На робочому місці працівника з ПК параметри мікроклімату відповідають вимогам ДСН 3.3.6.042-99 [48].

Якщо вищезгадані фактори не відповідають нормі, необхідно застосувати наступні засоби та заходи: налагодження системи вентиляції, кондиціонування та опалення, раціональне розміщення пристроїв та техніки, удосконалення або заміна робочого устаткування.

Підвищений рівень шуму та вібрації може призвести до професійних захворювань, зниження ефективності роботи працівника, підвищення рівня знервованості. Так як, сучасні комп'ютери та організаційна техніка працюють досить тихо, можна сказати, що шум майже відсутній на робочому місці і не несе ніяких подразнень. На даному робочому місці шум сягає 40 дБ, що не перевищує норму, яка становить 65 дБ згідно до ДСН 3.3.6.037-99 [49].

Фактор недостатньої кількості освітлення може привести до хвороб органів зору або до засліплення (при надмірній освітленості) та перевтомлення очей. Вирішенням даного питання можу бути нормування освітлення шляхом зміни ламп, їх розташування та кількість. На місці роботи користувача ПК в зоні розташування комп'ютеру та документів освітленість складає 400.

Запиленість приміщення – один із шкідливих факторів виробництва. У випадку користувача, що працює за ПК, можливі наступні наслідки: потрапляння пилу в органи дихання та зору, що призведе до їх подразнення, виникненню

кон’юнктивіту, алергії, хвороби легень, подразнення на шкірі. На запиленість можуть впливати параметри мікроклімату. Запиленість даного робочого місця не перевищує 0,3 мг/м^3. Для уникнення запиленості приміщення необхідно налагодити систему кондиціонування та вентиляції, а також регулярно проводити вологе прибирання кабінету.

Психофізіологічні фактори при роботі за комп’ютером – нервово-психічні та фізичні навантаження. Перші виникають при емоційному виснажені на робочому місці, при виконанні монотонної роботи, при розумовому перенапруженні, навантаженні на органи слуху та зору, при отримані та обробці великого об’єму інформації, при недостатній кількості часу, що виділено на відпочинок та сон. Як результат – організм завчасно зношений, виникають депресивні настрої, слабка імунна система та хронічна перевтома.

При фізичному навантаженні страждає опорно-руховий апарат: з’являються болі у спині (сколіоз, остеохондроз), у шийному та поперековому відділі, болі у руках та ногах, головні болі. Щоб уникнути фізичного перенавантаження необхідно робити перерви, час від часу змінювати положення тіла, розминати м’язи, регулярно проходити медичні огляди.

4.2 Аналіз техногенних небезпек та вибір засобів і заходів забезпечення безпеки у надзвичайних ситуаціях на робочому місці користувача ПК

Головною техногенною небезпекою на робочому місці користувача є виникнення пожежі. Як відомо, пожежа – неконтрольоване горіння, що виникає поза межами спеціального вогнища і може розповсюджуватися у просторі та часі, створюючи загрозу здоров’ю та життю людей, навколишньому середовищу та наносить матеріальні збитки [47]. Перебуваючи у місці, де спалахнула пожежа, людина може отримати переляк (у кращому випадку), травми і не тільки (у гіршому випадку), будучи під впливом наступних небезпечних факторів: вогонь, дим, недостатня кількість кисню, токсичні продукти згорання, вибух, руйнування приміщення, паніка як однієї людини, так і групи людей.

Причинами виникнення пожеж у приміщенні, де люди працюють з організаційною технікою, можуть бути: недотримання правил пожежної безпеки на підприємстві, несправність електроприладів (у тому числі, обігрівачів), підключення великої кількості пристроїв до одного джерела живлення, недотримання правил експлуатації електроприладів, підключення саморобних або/і несертифікованих приладів, підключення проводів та кабелів, які пошкоджені або у яких відсутня або зіпсована ізоляція, стрибки напруги, коротке замикання, паління заборонених місцях (у тому числі, на робочому місці), DDos-атаки, що призводять до фізичного руйнування техніки внаслідок її перегріву.

Для зниження імовірності виникнення пожеж, згідно до нормативу ДБН В.1.1-7-2002 С 25 [50], потрібно на підприємстві створити систему запобігання пожеж, у яку будуть входити: пожежна сигналізація та засоби пожежогасіння, системи сповіщення та протидимний захист, системи автоматичного пожежогасіння та засоби автоматичного контролю за параметрами, призначені для визначення джерела та місця спалахування, заземлення пристроїв.

Для запобігання виникненню пожеж необхідно впровадити наступні організаційні заходи:

- регулярно проводити перевірку рівня знань працівників з пожежної безпеки, контролювати дотримання протипожежних стандартів та норм;
- проводити навчальні евакуації та розробляти план евакуації людей;
- розташовувати робочі місця, зважаючи на вимоги до пожежної безпеки;
- встановлювати у будівлі протипожежних перешкод;
- визначити безпечне місця для паління;
- підтримувати порядок на шляхах евакуації.

Кожного співробітника необхідно забезпечити засобами індивідуального захисту (респіратор чи противогаз). У кабінеті працівника повинен бути вуглекислотний чи порошковий переносний вогнегасник.

Приміщення обробляються штукатуркою, фарбами та лаками, що не займаються. Робочі місця та меблі повинні розташовуватися так, аби евакуаційний

прохід був вільний. Додатково дерев'яні меблі обробляються антипіренами та лаками, що не займаються.

Отже, виконуючи усі вищезгадані заходи, можна повністю забезпечити пожежну безпеку як на робочому місці користувача персонального комп'ютеру, так і на підприємстві в цілому.

4.3 Розрахунок захисного заземлення

Вихідні дані: глибина занурення заземлювача в ґрунт складає $h_з = 80\ см$, вид заземлювача – стрижневий, довжина заземлювача – $l_{тр} = 500\ см$, діаметр заземлювача – $d_{тр} = 2\ см$, ширина з'єднувальної смуги – $b_c = 5\ см$, ґрунт – супісок, кліматична зона – III.

Так як мережа з напругою до 1000 В, допустимий опір розтікання струму в заземленні складає 4 Ом ($R_з = 4\ Ом$). Питомий опір супіску складає 30000 $Ом \cdot м$. Підвищувальний коефіцієнт для труб вертикальних заземлювачів $К_{П.Т} = 1.4$, для з'єднувальної полоси $К_{П.С} = 2.5$.

Питомий розрахунковий опір ґрунту для вертикальних електродів обчислено у формулі (4.1).

$$\rho_{розр.т} = \rho_{табл} \cdot К_{П.Т} = 30000 \cdot 1.5 = 42000\ (Ом \cdot м) \qquad (4.1)$$

Питомий розрахунковий опір ґрунту для горизонтального заземлювача у (4.2).

$$\rho_{розр.п} = \rho_{табл} \cdot К_{П.С} = 30000 \cdot 2.5 = 75000\ (Ом \cdot м) \qquad (4.2)$$

Розрахунок відстані від поверхні землі до середини вертикального заземлювача наведено у формулі (4.3).

$$t = h_з + \frac{l_{тр}}{2} = 80 + \frac{500}{2} = 300\ (см) \qquad (4.3)$$

Опір розтікання струму для одиночного вертикального заземлення, що розташований нижче поверхні землі розраховано у (4.4).

$$R_{розр.Т} = 0.366 \frac{\rho_{розр.т}}{l_{тр}} (\lg \frac{2l_{тр}}{d} + \frac{1}{2} \lg \frac{4t + l_{тр}}{4t - l_{тр}}) = 88.3\ (Ом) \qquad (4.4)$$

Відстань між вертикальними заземлювачами обчислено у (4.5).

$$L_{ст} = l_{тр} \cdot c = 500\ (см) \qquad (4.5)$$

Розрахунок необхідної кількості вертикальних заземлювачів без урахування коефіцієнта екранування наведено у (4.6).

$$n_Т = \frac{R_{розр.Т}}{R_з} = \frac{88.3}{4} \approx 22\ (шт) \qquad (4.6)$$

Коефіцієнт екранування труб 22 вертикальних заземлювачів $\eta_{Е.Т}$ складає 0,48. Кількість вертикальних заземлювачів з коефіцієнтом екранування становить:

$$n_{Т.Е} = \frac{R_{розр.Т}}{R_з \cdot \eta_{Е.Т}} = \frac{88.3}{4 \cdot 0.48} \approx 46\ (шт) \qquad (4.7)$$

Розрахунковий опір розтіканню струму:

$$R_{розр.n_{Т.Е}} = \frac{R_{розр.Т}}{n_{Т.Е} \cdot \eta_{Е.Т}} = \frac{88.3}{46 \cdot 0.48} = 4\ (Ом) \qquad (4.8)$$

Довжина з’єднувальної смуги розраховано у формулі 4.9.

$$L_{З.С} = 1.05 L_{см}(n_{Т.Е} - 1) = 1.05 \cdot 500(46 - 1) = 23625\ (см) \quad (4.9)$$

Опір розтікання струму в з’єднувальній смузі обчислено 4.10.

$$R_{зс} = 0.366 \frac{\rho_{розр.п}}{L_{З.С}} \lg \frac{2L_{З.С}^2}{h_з \cdot b_с} = 7.5\ (Ом) \quad (4.10)$$

Коефіцієнт екранування для з’єднувальної смуги $\eta_{\text{Е.З.С}}$ при розташуванні 46 заземлювачів в ряд становить 0,21. Розрахунковий опір для розтікання електричного струму в з’єднувальній смузі визначено у 4.11.

$$R_{розр.С} = \frac{R_{З.С}}{n_{ЕС} \cdot \eta_{Е.З.С.}} = \frac{7.5}{1 \cdot 0.21} = 35.7\ (Ом) \quad (4.11)$$

Загальний розрахунковий теоретичний опір розтікання струму від вертикальних заземлювачів та з’єднувальної смуги обчислено у 4.12.

$$R_{заг.розр} = \frac{1}{\frac{1}{R_{розр.Т}} + \frac{1}{R_{розр.С}}} = \frac{1}{\frac{1}{88.3} + \frac{1}{35.7}} = 26.3\ (Ом) \quad (4.12)$$

У результаті порівняння загального розрахункового теоретичного опору розтікання струму від вертикальних заземлювачів та з’єднувальної смуги та опору розтікання струму в заземленні встановлено, $R_{заг.розр}$ у 7 разів перевищує $R_{доп}$. У “Додаток В” зображено схему розташування заземлення в ґрунті заземлення.

ВИСНОВКИ

У кваліфікаційній роботі розроблено новий метод системи цифрових водяних знаків на основі дискретного косинусного перетворення, ліфтингового вейвлет-перетворення та сингулярного розкладу. Розроблено програмний продукт для використання даного методу.

Проведено дослідження, яке доводить ефективність методу, шляхом оцінки пікового відношення “сигнал/шум” та ступеню подібності вбудованого та детектованого цифрового водяного знаку. Так при збереженні повного контейнеру у форматі без втрат показник PSNR досягає 55,36 дБ із ступенем подібності майже 94%, а при збереженні у форматі з втратами при коефіцієнті від 75 середні значення – 47,9 дБ та ступінь подібності досягає 90%.

Тестування методу проводились на предмет стійкості до атак. Визначено, що метод є стійким не тільки до атаки стисненням, а й до накладання гаусового, мультиплікативного шуму, шуму “Сіль та перець”. Середні показники PSNR при зашумленні зображення становлять від 42 дБ до 50,45 дБ, а середні показники ступеню подібності – від 81,75% до 93,72%. Проте метод виявився нестійким до атаки фільтрацією.

Розроблено інтерфейс користувача програмного продукту. Він є простим у використанні, тому що всі його елементи, які відповідають за правильність виконання операцій, розташовані послідовно, у прямому порядку їх застосування. Тому будь-який користувача, незалежно від рівня знань персонального комп’ютеру, зможе вільно користуватися програмою.

У всіх організаціях та державних установах існує інформаційний потік та обмін даними, у них можна впроваджувати розроблений програмний продукт. Його необхідно використовувати з метою захисту будь-якого контенту, шляхом вбудовування власного цифрового водяного знаку або логотипу компанії.

ПЕРЕЛІК ПОСИЛАНЬ

1. Ахмаметьєва, Г.В. Розробка системи вбудови цифрових водяних знаків в зображення на основі DCT-LWT-SVD. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*. 2020. №68. С. 23-31.
2. Kolata G. Veiled Messages of Terror May Lurk in Cyberspace. URL: https://www.nytimes.com/2001/10/30/science/veiled-messages-of-terror-may-lurk-in-cyberspace.html?auth=link-dismiss-google1tap.
3. Грибунин, В. Оков И. Туринцев И. Цифровая стеганография. Москва : СОЛОН-Пресс, 2017.
4. Chandra S., Paira S. Secure transmission of data using image steganography. *Ictact journal on image and video processing*. 2019. №10. P. 2049–2053.
5. Rubab S., Younus M. Improved Image Steganography Technique for Colored Images using Huffman Encoding with Symlet Wavelets. *International Journal of Computer Science Issues*. 2012. №1. P. 194-196.
6. Akter A., Tajnina N. Digital image watermarking based on dwt-dct: evaluate for a new embedding algorithm. *International Conference on Informatics, Electronics & Vision (ICIEV)*. 2014. № 10. P. 1-6.
7. Cui X., Niu Y., Zheng X., Han Y. An optimized digital watermarking algorithm in wavelet domain based on differential evolution for color image. *PLoS ONE*. 2018. №13. P. 1-15.
8. Santoyo-Garcia H., Fragoso-Navarro E., Reyes-Reyes R., Cruz-Ramos C., Nakano-Miyatake M. Visible Watermarking Technique Based on Human Visual System for Single Sensor Digital Cameras. *Security and Communication Networks*. 2017. №10.1155. P. 1-15.
9. Kesa N. Steganography – A Data Hiding Technique. St. Cloud State University theRepository at St. Cloud State. 2018.

10. Кокурина А.С., Шумская О.О. Исследование стеганографических свойств дискретного преобразования Фурье при встраивании сообщения в фазовый спектр. *Инновации – разработки и технологии*. 2015. С. 1-5.
11. Преобразование Уолша — Адамара. *Национальная библиотека им. Н. Э. Баумана*. URL: https://ru.bmstu.wiki/Преобразование_Уолша_-_Адамара.
12. Сжатие изображений с потерями. *Национальный Открытый Университет "ИНТУИТ"*. URL: https://intuit.ru/studies/courses/993/163/lecture/4517?page=2
13. Юр Т. Обзор применений вейвлет-преобразования в задачах интелектуального анализа. *Збірник наукових праць Харківського університету Повітряних Сил*. 2015. №4. С. 85–88.
14. Bhattacharyya S., Mondal S., Sanyal G. A Robust Image Steganography using Hadamard Transform. *International Conference on Information Technology in Signal and Image Processing*. 2013. P. 416-426.
15. Zhang Y., Lu. Z., Zhao D. A Blind Image Watermarking Scheme Using Fast Hadamard Transform. *Information Technology Journal*. 2010. №9. P. 1369-1375.
16. Батура В., Тропченко А. Эффективность алгоритмов маркирования цифровых изображений в частотной области на основе дискретного преобразования адамара. *Информационные технологии*. 2014. №4. P. 7-12.
17. Nasereddin H.O. Digital watermarking a technology overview. *IJRRAS*. 2011. №6. P. 89-93.
18. Voloshynovskiy S., Shelby P., Pun T. Attacks on Digital Watermarks: Classification, EstimationBased Attacks, and Benchmarks. *Digital Watermarking For Copyright Protection: A Communication Perspective*. 2001. №1. P. 118–126.
19. Khalil M.I. Using Quaternion Fourier Transform in Steganography Systems. *International Journal of Communication Networks and Information Security*. 2018. № 2. P. 425-431.

20. Cheddad A., Condell J., Curran K., Mc Kevitt P. Securing Information Content using New Encryption Method and Steganography. *Third IEEE International Conference on Digital Information Management (ICDIM)*. 2008. P. 563-568.
21. Дружкова І., Щепилова Д., Юдін Д. Обеспечение скрытности дополнительной информации, кодируемой в пространственных компонентах монохромного изображения. *Научный результат. Информационные технологии*. 2017. №3. С. 31-37.
22. Soni A., Jain J., Roshan R. Image Steganography using Discrete Fractional Fourier Transform. *International Conference on Intelligent Systems and Signal Processing*. 2013. P. 99-103.
23. Senthooran V., Ranathunga L. DCT Coefficient Dependent Quantization Table. Modification Steganographic Algorithm. *First International Conference on Networks & Soft Computing*. 2014. P. 432-436.
24. Alwan I., Mohammed F. Image Hiding Using Discrete Cosine Transform. *J. Of College Of Education For Women*. 2016. №27. P. 393-399.
25. Nagpal C., Goel R. Modified quantization based steganography for color images. *International Journal of Electrical and Electronics Engineering*. 2013. №2. P. 9-17.
26. Gunjal M., Jha J. Image Steganography Using Discrete Cosine Transform (DCT) and Blowfish Algorithm. *International Journal of Computer Trends and Technology (IJCTT)*. 2014. №11. P. 144-150.
27. Ахмаметьєва Г.В., Баранюк Г.А. Модифікація стеганографічного методу вбудови цифрового водяного знаку в зображення на основі вейвлетперетворення. *Інформатика та математичні методи в моделюванні*. 2019. №1. С. 76-87.
28. Babya D., Thomasa J., Augustinea G., Georgea E., Michaela N. A Novel DWT based Image Securing Method using Steganography. *International Conference on Information and Communication Technologies*. 2014. №2. P. 612-618.

29. Singh B. Image Steganography Using DWT and Semi Hexadecimal Code Based on PSNR. *International Journal of Emerging Research in Management & Technology*. 2017. №8. P. 230-234.
30. Singh N. High PSNR based Image Steganography. *International Journal of Advanced Engineering Research and Science*. 2019. №1. P. 109-115.
31. Sweldens W. The Lifting Scheme: A New Philosophy in Biorthogonal Wavelet Constructions. *PROCEEDINGS OF SPIE*. 1995. P. 68-89.
32. Binny A., Duche R., Maddulety K. Lifting Wavelet Transform and Singular Value. Decomposition based Image Steganography. *International Journal of Emerging Technology and Advanced Engineering*. 2017. №9. P. 453-458.
33. Seyyedi S., Sadau V., Ivanov N. A Secure Steganography Method Based on Integer Lifting Wavelet Transform. *International Journal of Network Security*. 2016. №1. P. 124-132.
34. Al-Saad S., Kadum A. Image Hiding Using Lifting Wavelet Transform. *International Journal of Scientific & Engineering Research*. 2016. № 4. P. 1600-1609.
35. Xianye L., Xiangfeng M., Xiulun Y., Yurong W. Multiple-image encryption via lifting wavelet transform and XOR operation based on compressive ghost imaging scheme. *Optics and Lasers in Engineering.* 2018. P. 106-111.
36. Vohra S., Kumar B. Image Steganography Using Hybrid Method LWT-DWT-SVD. *International Journal of Innovative Research in Science, Engineering and Technology*. 2017. №8. P. 16274-16285.
37. Kumar S., Reddy P., Ramesh G., Maddumala V. Image Transformation Technique Using Steganography Methods Using LWT Technique. *Traitement du Signal*. 2019. №3. P. 233-237.
38. Taha T., Ehkan P., Ngadiran R. A New Perceptual Mapping Model Using Lifting Wavelet Transform. *MATEC Web of Conferences*. 2017. P. 1-5.
39. Taha D., Taha T., Dabagh N. A comparison between the performance of DWT and LWT in image watermarking. *Bulletin of Electrical Engineering and Informatics*. 2020. №3. P. 1005-1014.

40. Getting Started with MATLAB – Natick: The MathWorks, 2005. 187 p.
41. Бубнов И. MATLAB: инструмент будущего или дорогая игрушка. URL: https://geekbrains.ru/posts/how_to_matlab?utm_source=cityads&utm_medium=cpa&utm_campaign=cityads&utm_content=courses&utm_term=30%2F09%2F2017&partner_id=cityads&click_id=7IbZ1SVA6FZe2ye&sub_id=2NKZ.
42. Манзон Б. Matlab: где её применяют. URL: https://www.itweek.ru/themes/detail.php?ID=46804.
43. Список функций Image Processing Toolbox. URL: https://hub.exponenta.ru/post/spisok-funktsiy-image-processing-toolbox152#up.
44. ДСанПІН 3.3.2.007-98. Гігієнічні вимоги до організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин. [Чинний від 1998.12.10]. Київ, 1998.
45. ДСН 3.3.6.042-99. Державні санітарні норми мікроклімату виробничих приміщень. [Чинний від 1999.12.01]. Київ, 1999. 63 с.
46. ДСТУ ISO 9241-5:2004. Ергономічні вимоги до роботи з відеотерміналами в офісі. Частина 5. Вимоги до компонування робочого місця та до робочої пози (2286). [Чинний від 01.01.2006]. Київ, 2004. 27 с.
47. Жидецький В.Ц., Джигирей В.С., Мельник О.В. Основи охорони праці. Львів: Афіша, 2001. 350 с.
48. ДСН 3.3.6.042-99. Державні санітарні норми мікроклімату виробничих приміщень. [Чинний від 01.12.1999]. Київ, 1999. 19 с.
49. ДСН 3.3.6.037-99. Державні санітарні норми виробничого шуму, ультразвуку та інфразвуку. [Чинний від 01.12.1999]. Київ, 1999. 36 с.
50. ДБН В.1.1-7-2002 С 25. ПОЖЕЖНА БЕЗПЕКА ОБ'ЄКТІВ БУДІВНИЦТВА. [Чинний від 01.01.2007]. Київ, 2007. 42 с.