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

Нечитайлова Любов Володимирівна,
студентка групи РЗ-151

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Розробка стеганоаналітичного методу на основі класифікації статистичних показників нейронною мережею

Спеціальність:
125 Кібербезпека

Спеціалізація, освітня програма:
Кібербезпека

Керівник:
Кушніренко Наталія Ігорівна,
к.т.н., доцент

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 ІУЗІС

_____
д.т.н.,проф. А.А.Кобозєва
____ _____202_р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Нечитайловій Любові Володимирівні

1. Тема роботи: *Розробка стеганоаналітичного методу на основі класифікації статистичних показників нейронною мережею*

керівник роботи *Кушніренко Наталія Ігорівна, к.т.н., доцент,*

затверджені наказом ректора ОНПУ від „___”_____ 20__ р. №_____ .

2. Зміст роботи*: опис алгоритму вбудовування додаткової інформації в стеганоконтейнер, розробка методу, заснованого на розпізнаванні образів за допомогою технології машинного навчання для стеганоаналізу, програмна реалізація алгоритму та запропонованого методу. охорона праці.*

3. Перелік ілюстративного матеріалу: *схема реалізації алгоритму F5, структурні схеми нейронних мереж, ілюстрації роботи програмного інтерфейсу: головне вікно, результати детектування запропонованими методами.*

5. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
Охорона праці	Ярова І.А., к.т.н., доцент	Завдання видав	Завдання прийняв

6. Дата видачі завдання "_____"_____20___ р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання	Примітка
1	*Аналіз джерел з теми випускної кваліфікаційної роботи*	*15-09-2019*	*виконано*
2	*Дослідження алгоритму F5 та його особливостей*	*10-10-2019*	*виконано*
3	*Дослідження особливостей побудови нейронних мереж*	*21-10-2020*	*виконано*
4	*Розробка стеганоаналітичного методу для виявлення додаткової інформації в цифрових зображеннях*	*02-11-2020*	*виконано*
5	*Реалізація програмного коду та інтерфейсу програми*	*24-11-2020*	*виконано*
6	*Підготовка тексту роботи*	*10-12-2020*	*виконано*
7	*Підготовка презентації та доповіді*	*18-12-2020*	*виконано*
8	*Попередній захист*	*01-12-2020*	*виконано*
9	*Нормоконтроль, рецензування*	*15-12-2020*	*виконано*
10	*Занесення роботи в електронний архів*	*25-12-2020*	*виконано*
11	*Допуск до захисту у завідувача кафедри*	*25-12-2020*	*виконано*

Здобувач вищої освіти _____ *Нечитайлова Л.В.*

Керівник роботи _____ *Кушніренко Н.І..*

ЗАВДАННЯ

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

Нечитайловій Любові Володимирівні, група РЗ-151

Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій

Кафедра кібербезпеки та програмного забезпечення

Тема роботи *Розробка стеганоаналітичного методу на основі класифікації статистичних показників нейронною мережею*

Зміст розділу:

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

2 Аналіз техногенних небезпек і вибір заходів і засобів забезпечення безпеки у надзвичайних ситуаціях.

3 Розрахунок акустичної обробки приміщення.

Керівник роботи	Консультант з охорони праці
_____ (_____)	_____ (_____)
«____» _____ 2020 р.	«____» _____ 2020 р.

АНОТАЦІЯ

Кваліфікаційна робота на тему «Розробка стеганоаналітичного методу на основі класифікації статистичних показників нейронною мережею” на здобуття другого (магістерського) рівня вищої освіти за спеціальністю 125 - Кібербезпека спеціалізація, освітня програма: Кібербезпека, містить 14 рисунків, 2 таблиці, 2 додатки, 25 літературних джерел за переліком посилань. Робота виконана на 60 сторінках загального тексту і 50 сторінках основного тексту.

Метою роботи є підвищення ймовірності виявлення прихованого стеганоповідомлення в цифровому зображенні шляхом розробки методу аналізу статистики зображення-контейнеру з використанням нейронної мережі.

Основними етапами виконання роботи є: аналітичний огляд існуючих стеганографічних методів, опис обраного методу, аналіз сучасних методів стеганоаналізу з використанням нейронних мереж та розробка програми, що виконує стеганоаналіз.

В роботі представлено аналіз стеганографічного методу F5 для вбудовування додаткової інформації в цифровий контейнер та наведено метод для детектування стеганоповідомлення.

Результат виконання кваліфікаційної роботи – створення програмного продукту для вбудовування та детектування наявності секретного повідомлення методом з використанням нейронної мережі.

Результати роботи можуть бути використані для аналізу цифрових контейнерів на наявність вбудованого секретного повідомлення.

ЦИФРОВА СТЕГАНОГРАФІЯ, ВБУДОВУВАННЯ ДОДАТКОВОЇ ІНФОРМАЦІЇ, СТАТИСТИЧНІ ОСОБЛИВОСТІ, ДИСКРЕТНО-КОСИНУСНЕ ПЕРЕТВОРЕННЯ, JPEG, ДКП КОЕФІЦІЄНТИ, МЕТОДИ ДЕТЕКТУВАННЯ, НЕЙРОННА МЕРЕЖА.

ANNOTATION

Qualification work on the theme "Development of steganoanalysis method based on the classification of statistical indicators by neural network" for obtaining the second (master) level of higher education in the specialty 125 - Cybersecurity specialization, educational program: Cybersecurity, contains 14 figures, 2 tables, 2 attachments, 25 literature sources under the list of references. The work is done on 60 pages of general text and 50 pages of the main text.

The purpose of this work is to increase the probability of detecting a hidden stegano-message in a digital image by developing a method for analyzing image container statistics using a neural network.

The main stages of the work are: analytical review of existing steganographic methods, description of the chosen method, analysis of modern methods of steganalysis using neural networks and development of a program that performs steganalysis.

This paper presents an analysis of the F5 steganographic method for embedding additional information into a digital container and provides a method for detecting a steganographic message.

The result of the thesis is the creation of a software product for embedding and detecting a secret message by different methods.

The results of this work can be used to analyze digital containers for the presence of a built-in secret message.

DIGITAL STEGANOGRAPHY, ADDITIONAL INFORMATION, STATISTICAL FEATURES, DISCRETE COSINE TRANSFORMATION, JPEG, DCT COEFFICIENTS, DETECTION METHODS, NEURAL NETWORK.

ЗМІСТ

ВСТУП

Цифрові зображення формату JPEG є найбільш поширеними в Інтернеті, і їх щоденний обіг становить дуже значну частку всього інтернет-трафіку, включаючи соціальні мережі, месенджери, портали обміну зображеннями та інші ресурси. Висока популярність цього формату зображення стала однією з причин досить швидкої появи нових методів прихованої передачі інформації, де секретним контейнером є саме зображення JPEG.

Дуже серйозною проблемою є використання таких засобів прихованої передачі інформації в незаконних цілях (у тому числі терористичних), а також в обхід моніторингу систем запобігання витоку конфіденційної інформації (DLP-систем). Останнім часом розробники цих систем почали активно звертати увагу на проблему та впроваджувати відповідні інструменти. Тому можна говорити, що розроблення ефективних методів захисту цифрової інформації, а саме стеганоаналізу та стеганографії, є актуальними та важливими.

Актуальність кваліфікаційної роботи полягає в удосконалені та розробці нових методів виявлення стеганоповідомлень у цифрових контейнерах на основі стійкого до різних видів атак алгоритму F5.

Мета роботи – підвищити ймовірність детектування прихованого повідомлення в цифровому зображенні шляхом розробки методу аналізу статистики зображення-контейнеру з використанням нейронної мережі.

Для досягнення мети було поставлено задачі:

- ознайомитися з особливостями вбудовування секретного повідомлення у цифрові зображення, використовуючи стеганоалгоритм F5;

- вивчити та проаналізувати особливості використання штучних нейронних мереж для стеганоаналізу, запропонувати власний метод;

- порівняти ефективність запропонованого методу;

- створити власний готовий програмний продукт для вбудовування секретної інформації шляхом застосування алгоритму F5 та виявлення

прихованого стеганоповідомлення шляхом використання запропонованих розроблених методів.

Для вирішення задач використовувалися чисельні методи та методи обробки цифрових зображень.

Предмет роботи – стеганоаналітичні методи для цифрових зображень.

Об’єкт дослідження – процеси детектування стеганографіного каналу зв’язку.

Робота складається з 4 розділів. У першому розділі описані сучасні стеганографічні методи, методи стеганоаналізу на алгоритм F5, основні особливості використання нейронних мереж для вирішення задач стеганоаналізу. Другий розділ містить опис особливостей розробки стеганоаналітичного методу з використанням нейронної мережі для детектування прихованого повідомлення . У третьому – реалізація програмного продукту з описом середовища програмування, представлено реалізацію програмного коду та інтерфейс користувача. Четвертий розділ містить в собі аналіз умов праці і вибір основних заходів виробничої безпеки та аналіз пожежної безпеки і вибір заходів і засобів пожежної безпеки на робочому місці користувача персонального комп’ютеру.

Результати дослідження були подані у науковій статті «Стеганоаналітичний метод для контейнерів F5 на основі штучної нейронної мережі», що опублікована у Віснику інженерної академії України [1].

1 СУЧАСНІ МЕТОДИ ВБУДОВУВАННЯ ПРИХОВАНОЇ ІНФОРМАЦІЇ ТА ВИЯВЛЕННЯ ПОРУШЕНЬ ЦІЛІСНОСТІ ЦИФРОВИХ ЗОБРАЖЕНЬ

1.1 Огляд сучасних стеганографічних методів

Інформаційні технології та комп’ютерні мережі надають велику кількість послуг у сучасному інформаційному суспільстві. Тому, інформація, що циркулює в інформаційному просторі повинна надійно захищатись від втручання у вигляді отримання несанкціонованого доступу, знищення або підробки, витоку інформації, до якої було отримано доступ, порушення ліцензійних угод та авторських прав та інше. Законом України "Про основи національної безпеки України" від 19.06.2003 р. серед загроз національним інтересам і безпеці України в інформаційній сфері зазначені: комп'ютерні тероризм та злочинність; розголошення таємної чи конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; маніпулювання суспільною свідомістю, зокрема, шляхом поширення недостовірної інформації. [2].

Стеганографія - це техніка приховання секретних даних в звичайному, не секретному файлі або повідомленні щоб уникнути їх виявлення; секретні дані потім витягаються за призначенням. Використання стеганографии може поєднуватися з шифруванням в якості додаткового кроку для приховання або захисту даних [3].

Розробники шкідливих програм часто використовують LSB стеганографію для того, щоб приховати шкідливий код програми в зображеннях і виконати їх іншою програмою після завантаження файлу на комп'ютер жертви.

Розрізняють три види стеганографії:

- цифрова;
- комп’ютерна;
- класична.

Цифрова стеганографія заснована на приховуванні або вбудовуванні

додаткової інформації в цифрові об'єкти, викликаючи при цьому деякі спотворення самих об'єктів.

Цифрову стаганографію використовують для:

1. Вбудовування інформації з метою її прихованої передачі:

– використання спец-агентами для комунікації зі своїм командним центром без дипломатичного прикриття;

– використання терористичними організаціями для передачі прихованих повідомлень у кіберпросторі [4];

– використання фізичними і юридичними особами для приховування конфіденційної інформації у медіа-контенті.

2. Вбудовування цифрових водяних знаків:

– для систем захисту авторських прав та систем, що обмежують несанкціонований доступ;

– у якості аналогового ЕЦП, забезпечуючи зберігання інформації про переданий підпис і спроби порушення цілісності контейнера.

3. Вбудовування ідентифікаційних номерів, наприклад, у програмних продуктах, у системах цифрового друку.

4. Вбудовування заголовків, наприклад, у медичних картах, у системах цифрового друку.

Комп'ютерна стеганографія - підміна символів в імені файлів, приховування секретного файлу в іншому файлі або повідомленні. Дані можна приховувати в невикористаних областях жорстких дисків і оптичних носіях. При цьому запис відбувається так, щоб сама операційна система не змогла виявити внесені дані.

Завдяки стрімкому розвитку засобів обчислювальної техніки й створенню можливостей для швидкого обміну інформацією в мережі Інтернет: цифрові зображення, відео, аудіо-файлів, текстів та програм.

Класична стеганографія - основним її методом є невидимі чорнила, текст написаний ними стає видимим тільки при певних умовах (при певному освітленні і нагріванні, хімічній обробці, ІЧ- або УФ-випромінванні, тощо). До

класичної стеганографії можна віднести використання мікрокрапок і мікротекстів, які неможливо розпізнати неозброєним оком. Цим користувалися найбільші виробники принтерів – Canon, Dell, Epson, Hewlett-Packard, IBM, Toshiba, Xerox [5] – під час друку на кожній сторінці виявлялися жовті точки, що містять в собі інформацію про серійний номер принтера, дату і час друку.

Приклади використання стеганографії у період 2018-2020:

1. У жовтні 2018 року зловмисники приховували шкідливий код у мемах Twitter за допомогою стаганографії. Меми містять вбудовану команду, яка аналізується шкідливою програмою після її завантаження з шкідливого аккаунта Twitter на машину жертви. У мемах прихована команда "/print", яка дозволяє шкідливій програмі робити скриншоти зараженої машини, а також програма в змозі отримати доступ до списку запущених процесів, отримати уміст буферу обміну, отримати назви файлів [6].

2. У квітні 2019 року колишньому інженерові General Electric було пред'явлено звинувачення в економічному шпигунстві та змові з метою викрадення комерційних секретів, що стосуються турбінних технологій. У співробітника були зашифровані файли, що містять конфіденційну інформацію GE, сховані на фотографії заходу сонця [7].

3. Серпень 2019 - дослідники TrendMicro виявили новий варіант шкідливого програмного забезпечення LokiBot для кейлоггеров і викрадачів криптовалюти, яке використовує стеганографію, щоб приховати свій шкідливий код усередині файлу jpeg [8].

4. У січні 2020 року Guardicore Labs відреагувала на інцидент, пов'язаний з атакою на компанію середнього розміру в секторі медичних технологій. Мережа жертви була заражена добре замаскованим шкідливим ПЗ, що приховує криптомайнер Monero усередині файлів WAV [9].

5. Дослідники з Malwarebytes повідомили про код скіммеру кредитних карт, прихований у файлах зображень на взламаних сайтах електронної комерції.[10].

1.2. Класифікація та основні особливості стеганоаналітичних методів. Існуючі методи стеганоаналізу алгоритму F5

Стеганоаналіз вирішує задачі контролю за протиправним використанням стеганографії, а в деяких випадках виокремлює слабкості та відкриває шляхи вдосконалення існуючих стеганографічних методів [11].

Стегоаналіз дозволяє вирішити наступні важливі задачі:

– визначити стійкість стеганографічного алгоритму до атак зловмисників;

– запобігти несанкціонованій передачі таємної інформації методами стеганографії.

Існує безліч методів стеганоанализа, які розрізняються за характеристиками зображення, що використовуються і методами вбудовування, яким вони протидіють. Залежно від використовуваних початкових даних методи стеганоаналізу традиційно розділяють на:

- сигнатурні;
- статистичні;
- евристичні.

1. Сигнатурні методи стеганоаналізу призначені для роботи з форматними методами приховання інформації, які в процесі приховання залишають специфічні маркери (сигнатури), по яких і вдається детектувати приховане вкладення. Стеганографія змінює властивості носія за рахунок вставки бітів повідомлень у вигляді повторюваних шаблонів, які діють як сигнатури, що передають існування вбудованого повідомлення [12]. Такі методи розглядають таблиці палітри в зображеннях і будь-які аномалії, що виникають в них. Коли повідомлення вбудовано послідовно, такі атаки дають добрі результати, але їх важко автоматизувати і їх надійність дуже сумнівна.

2. Статистичні методи стеганоаналізу базуються на аналізі статистичних характеристик зображення з метою встановлення, як вони корелюють з характеристиками порожніх стеганоконтейнеров такого ж типу. Найбільш відомими статистичними методами є RS- стеганоанализ і WS-

стеганоаналіз [13], гістограма [14].

3. Евристичні методи стеганоаналізу представляють великий інтерес, вони більше універсальні, оскільки не прив'язані до якогось алгоритму впровадження прихованої інформації, хоч і дещо менш точні в цілому. В основному, ці методи базуються на рішенні задачі бінарної класифікації із застосуванням методів машинного навчання, наприклад, методи, запропоновані в роботах [16-19]. Розглянемо деякі їх них детальніше, так, в роботі [16] наводиться метод стеганоаналізу, грунтований на аналізі гістограм, побудованих на основі таблиці кодів Хаффмана, значень дискретного косинусного перетворення (ДКП), що використовуються для кодування, кодами змінної довжини. Для аналізу гістограм застосовується машинне навчання з використанням штучної нейронної мережі.

У роботі [19] представлено алгоритм стеганоаналізу, що заснован на сегментації зображень, але формовані фрагменти утворюються відповідно до складності текстури. Як вектор характеристик зображень використовується набір PEV - 274, запропонований в роботі [20]. Завдання класифікації вирішується за допомогою застосування методу опорних векторів. Точність методу для алгоритму F5 складає від 67 до 77%.

У [21] опис методу, який надійно виявляє приховані алгоритмом F5 повідомлення у JPEG зображеннях. Точна оцінка гістограми зображення важлива для роботи методу виявлення. Спочатку відбувається розпаковка стего-зображення в просторову область, потім обрізка зображення на 2 рядки і 4 стовпці і повторне стиснення обрізаного зображення, використовуючи ту ж матрицю квантування, що і у стего-зображенні. Метод обрізки зображення - це метод видалення зображення по похилому напрямку. Однак, обрізання одного зображення буде спотворювати дані і вплине на стегоаналіз зображень у форматі JPEG. Якщо обрізати зображення багато разів і обчислити середні коефіцієнти ДКП, процес зможе зменшити вплив аномальних значень. Це принципи, які використовуються в запропонованому методі, званому алгоритмом ESF.

Ключовим елементом методу є оцінка гістограми зображення зі стего-зображенням. За допомогою обрізання зображення формату JPEG якомога більше разів по косому напрямку, цей алгоритм може ефективно справлятися з даними і отримувати кращі результати.

У [22] представлено стеганоаналітичний метод, який може надійно виявляти повідомлення, приховані в зображеннях JPEG за допомогою стеганографічного алгоритму F5. Головний елемент методу - оцінка гістограми оригінального зображення зі стего-зображенням. Це робиться шляхом декомпресії стего-зображення, обрізання його на чотири пікселя в обох напрямках для видалення квантування в частотній області і повторного його стиснення з використанням того ж коефіцієнту якості, що використовувався. Експериментальні результати показують, що відносні модифікації, 10% коефіцієнтів ДКП, можуть бути достовірно виявлені. Метод перевірявся на різноманітному наборі тестових зображень, які включають як необроблені, так і оброблені зображення у форматах JPEG і BMP.

Кількість успішних робіт, пов’язаних зі стеганоаналізом зображень з вбудовуванням алгоритмом F5, невелика і в [14] проводився експеримент на малій вибірці зображень, тож має сумнівні результати ефективного детектування. Тому можна вважати напрям стеганоаналізу обраного алгоритму перспективним для проведення досліджень та експериментів.

1.3. Огляд нейронних мереж

Методи стегоаналізу засновані на використанні нейронних мереж малодосліджені. Вони використовують статистичні методи стегоаналізу в поєднанні з можливостями нейронних мереж до навчання та класифікації [24].

У статті [23] розглянута можливість застосування згорткові нейронних мереж для виявлення стеганографічного повідомлення в цифрових зображеннях. Як тренувальний набір даних були взяті зображення із із

застосуванням стеганографических алгоритмів LSB, FFT, DCT. Результати дослідження демонструють можливість виявлення до 85% фактів наявності стеганографических вкладень.

У роботі [24] проведено моделювання ефективності виявлення прихованих повідомлень шляхом стеганографічного аналізу за Rich моделлю без попередньої модифікації контейнера. Виявлено, що такий аналіз надійно виявляє приховані повідомлення у контейнері, з низькою ймовірністю помилок першого та другого роду ($\alpha, \beta<0.08$).

Також проведено моделювання роботи стеганографічного методу вбудовування додаткової інформації із модифікацією контейнера. Також проведено моделювання ефективності виявлення таких повідомлень при аналізі за Rich моделлю, порівняно ефективність виявлення без модифікації контейнера та з модифікацією. З отриманих результатів видно, що попередня модифікація контейнера призводить до значного збільшення ймовірністю помилок першого та другого роду при виявленні ($\alpha, \beta \sim 0.35$). Таким чином, забезпечується помітне зменшення ефективності виявлення прихованих повідомлень при стеганографічному аналізі за Rich моделлю.

2 РОЗРОБКА СТЕГАНОАНАЛІТИЧНОГО МЕТОДУ ДЛЯ ВИЯВЛЕННЯ ДОДАТКОВОЇ ІНФОРМАЦІЇ, ВБУДОВАНОЇ АЛГОРИТМОМ F5

2.1 Опис та реалізація алгоритму F5. Вихідні дані до експериментів

Для досліджень було обрано стеганографічний алгоритм F5, що має ряд переваг:

- запобігає візуальним атакам;
- стійкий до статистичних атак (хі-квадрат);
- має високу здатність до вбудовування;
- висока ефективність завдяки матричному кодуванню;
- використовує JPEG-формат зображень.

Багато стеганографічних систем слабкі проти візуальних і статистичних атак. Системи без цих недоліків пропонують лише відносно невеликий обсяг для поширення стеганографічних повідомлень. Нещодавно розроблений алгоритм F5 витримує візуальні і статистичні атаки, але все ж має великий стеганографічний потенціал.

Алгоритм F5 був розроблений е 2001 Андреасом Вестфілдом з метою підвищення пропускної спроможності і ефективності вбудовування в зображення формату JPEG, а також стійкості до візуальних і статистичних атак [11]. Пропускна спроможність – максимальна кількість інформації, що може бути вкладена в 1 елемент контейнеру (біт/піксель). Замість заміни найменш значущих бітів квантованих коефіцієнтів ДКП бітами повідомлень, вбудовування в алгоритмі F5 є аддитивним і полягає в зменшенні на одиницю абсолютних значень окремих коефіцієнтів. Алгоритм F5 вбудовує біти повідомлення у випадково вибрані коефіцієнти ДКП і використовує матричне кодування, яке мінімізує необхідну кількість змін для вбудовування повідомлення певної довжини. При послідовному процесі вбудовування зміни накопичуються на початку файлу, а невикористаний простір залишається в кінці. Тому для запобігання атак функція вбудовування використовує весь контейнер, а щільність повинна бути

однаковою в усьому файлі. Обраний алгоритм має 2 особливості, що покращують ефективність вбудовування та допомагають запобігати статистичним атакам.

1. Перестановка. Механізм розподілу, який використовується в стеганографічному алгоритмі F5, перетасовує, змінюючи місце розташування всіх коефіцієнтів, використовуючи перестановку. Потім стеганоповідомлення вбудовується алгоритмом F5 в перестановочну послідовність. Усадка змінює значення коефіцієнтів, не змінюючи їх кількість. Стеганографічні змінені коефіцієнти доставляються у вихідній послідовності в кодер Хаффмана. Таким чином, алгоритм F5 дозволяє розподіляти зміни по всьому зображенню (рисунок 1.1), де сірі області – вбудоване повідомлення. Перестановка має лінійну складність O (n). Маючи правильний ключ одержувач може повторити перестановку та розшифрувати вкладене стеганоповідомлення.

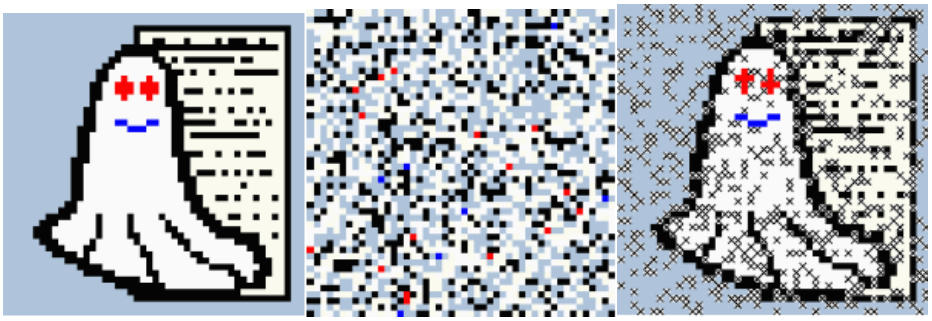

Рисунок 1.1 – Приклад розподілу змін по зображенню

2. Матричне кодування. Рон Кределл [28] ввів матричне кодування як нову техніку для поліпшення ефективності вбудовування. F5 є першою реалізацією матричного кодування. Якщо більша частина ємності не використовується в стеганограмі, матричне кодування зменшує необхідну кількість змін. Маємо рівномірно розподілене секретне повідомлення і рівномірно розподілені значення на позиціях, які необхідно змінити. Одна половина повідомлення викликає зміни, інша половина – залишається незмінною. Без матричного кодування ефективність вбудовування 2 біт на

зміну. Наприклад, якщо відбувається вбудовування дуже короткого повідомлення, що містить лише 217 байт (1736 біт). F5 вбудовує одне і те ж повідомлення за допомогою матриці кодування з 459 змінами, тобто з ефективністю вбудовування 3,8 біт на зміну. Для вбудовування двох бітів *x1*, *x2* у три модифікованих бітові місця *a1*, *a2*, *a3*. Може виникнути чотири випадки, де змінюється не більше одного біта:

А) $x1=a1 \oplus a3$, $x2=a2 \oplus a3 \Rightarrow$ без змін;

Б) $x1 \neq a1 \oplus a3$, $x2=a2 \oplus a3 \Rightarrow$ змінити a1;

В) $x1=a1 \oplus a3$, $x2 \neq a2 \oplus a3 \Rightarrow$ змінити a2;

Г) $x1 \neq a1 \oplus a3$, $x2 \neq a2 \oplus a3 \Rightarrow$ змінити a3.

Реалізація алгоритму F5 відбувається відповідно до схеми, зображеної на рисунку 1.3:

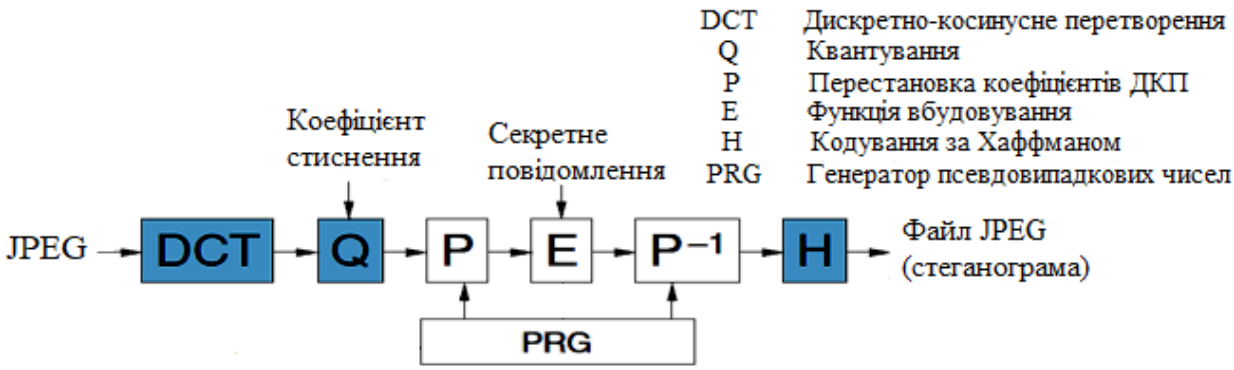

Рисунок 1.2 – Схема реалізації алгоритму F5

Формат файлу JPEG зберігає дані зображення з втратами у вигляді квантових частотних коефіцієнтів.

Кодування по Хаффману забезпечує кодування без надмірності квантованих коефіцієнтів.

Для проведення експерименту в якості контейнерів використано цифрові зображення з мережі Інтернет, формату JPEG загальною кількістю 1205 одиниць. Розмір кожного із зображень 1920 х 1080 пікселів, а коефіцієнт

стиснення (Q) - 90. У подальшому цей набір цифрових зображень випадковим чином було порівну розподілено на 2 набори: перший застосовано для тренування нейронної мережі (TrainSet), а другий – набір для перевірки ефективності аналізаторів (TestSet), для порівняльного тесту обох методів. Два набори містять в собі подібні за розмірами та характеристиками зображення для того, аби нейронна мережа була здатна натренуватися на зображеннях, що будуть використовуватися надалі.

За умовами експерименту відбувається вбудовування бітів псевдовипадкової послідовності з рівномірним розподілом, тому що реальне секретне повідомлення перетворюється, шляхом застосування шифрування, і приводиться до такого виду, що розподіл бітової послідовності (1 і 0) близький до рівномірного. Вбудовування здійснюється у кожний постійний коефіцієнт, виходячи з максимально теоретично можливої пропускної спроможності алгоритму, тобто контейнер максимально заповнений.

Контейнер перевіряється двома методами детектування наявності приховуваного секретного повідомлення: аналітичним методом або методом машинного навчання.

Алгоритм аналітичного методу містить такі кроки:

- виділення числового параметру – *k* – розбаланс компонентів ДКП зі значенням 1 та -1, виключаючи 0 та компоненти ДКП менше -1 та більше 1. Значення параметру помітно змінюється при наявності вбудовування в зображенні;
- визначення порогу параметру *k* для отримання заданих помилок першого і другого роду.

Метод, заснований на розпізнаванні образів за допомогою технології машинного навчання виконується так:

- тренування нейронної мережі, налаштованої на розпізнавання гістограм зображень з вбудованим повідомленням і без нього;
- нейронна мережа видає ймовірність наявності вбудованого повідомлення, до якого згодом теж застосовується поріг.

Якщо жоден із методів не зможе виявити наявність вбудовування при максимально заповненому контейнері, то не зможе зробити цього і в частково заповненому через особливості обраного алгоритму F5.

Один із кроків виконання алгоритму – ініціалізація криптографічно стійкого генератора, який використовуватиметься для перестановки квантованих значень ДКП. Але можливе використання звичайної перестановки коефіцієнтів, тому що для обраних методів криптостійкість не критична по причині того, що методи працюють на основі аналізу отриманих гістограм. Гістограми залежать від кількості коефіцієнтів з певним значенням, а не від їх позицій.

Нормалізована гістограма - спосіб графічного представлення відносної долі коефіцієнтів з кожним обраним значенням x від загальної кількості коефіцієнтів у контейнері. Значення 0 ігноруються по причині того, що при ентропійному кодуванні ці значення будуть відкинуті.

Для опису ефективності обраних стеганоаналітичних методів використовується ймовірність виявлення пустого контейнера, а також контейнера, що зазнав змін; помилки першого та другого роду.

Також застосовується службова функція, що визначає поріг розпізнавання. Тобто розраховує, яке значення потрібно використати для того, щоб ймовірність помилок першого та другого роду були приблизно однакові. Беручи до уваги той факт, що заздалегідь невідомо взагалі, чи вбудовано секретне повідомлення, а якщо вбудовано, то в якому контейнері. Важливо забезпечити максимальну ймовірність детектування методом.

Визначення порогу на тренувальному наборі: підрахунок суму з накопиченням параметрів (ймовірність вбудовування для пустого контейнеру та для заповненого). А потім серед отриманих результатів обрати таке значення, щоб різниця між сумами була мінімальною.

Гістограми, що зображують статистику коефіцієнтів по заповненим та порожнім контейнерам наведені на рисунках 2.1 та 2.2.

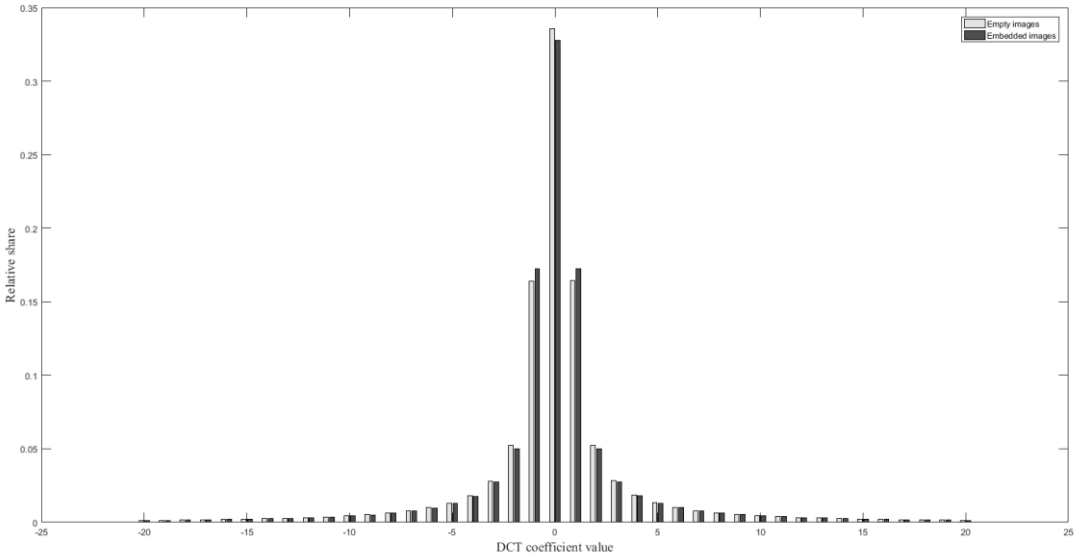

Рисунок 2.1 – Порівняння гістограм заповнених та порожніх контейнерів зображень набору для перевірки ефективності аналізаторів набору

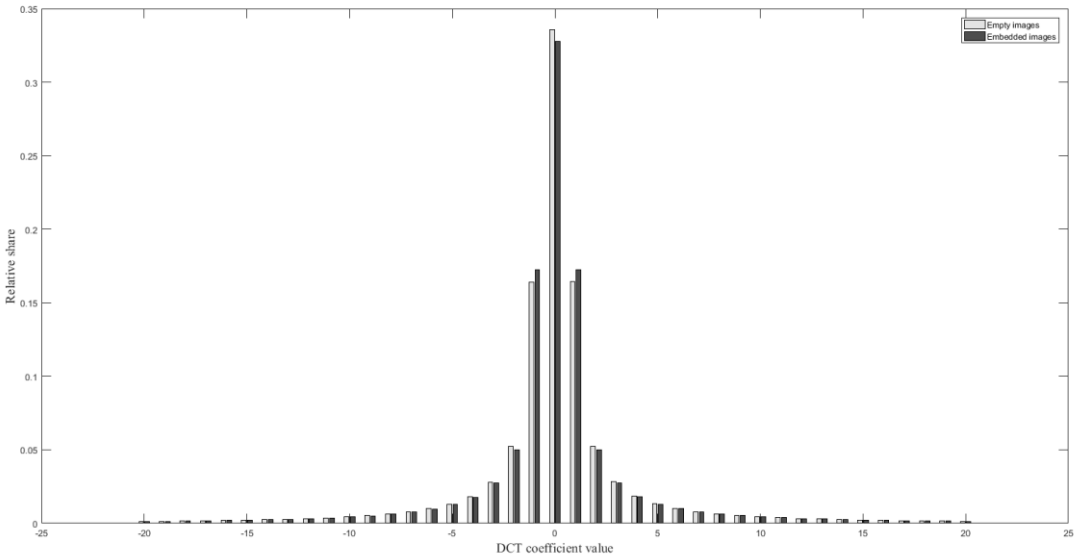

Рисунок 2.2 – Порівняння гістограм заповнених та порожніх контейнерів зображень для тренувального набору

2.2 Стеганоаналітичний метод на основі аналізу статистики зображення-контейнера на основі аналітичного підходу

2.2.1 Опис аналітичного методу

F5 для вбудовування секретного повідомлення використовує декремент – зменшення значень коефіцієнтів ДКП на 1 (відбувається зменшення модулю компонентів). Тому гістограма контейнера, у який вкладено повідомлення, змінюється таким чином: кількість значень коефіцієнтів ДКП 1 та -1 збільшується у порівнянні з пустим контейнером, а кількість інших значень зменшується.

Для розрахунку розбалансу коефіцієнтів (*k)* використовується діапазон значень [-100; 100], тому що значень, які були б більше або менше заданого діапазону, невелика кількість – можна знехтувати. Також однією з причин обрання саме такого діапазону – підвищує точність розпізнавання. На статистику впливають значення [-10; -2] та [2;10]. Використано наступну формулу (2.1):

$$k = \frac{b}{a + b}, \tag{2.1}$$

де a – кількість неодиничних коефіцієнтів ДКП;

b – кількість зареєстрованих коефіцієнтів ДКП зі значеннями -1 та 1.

Алгоритм перевірки: за допомогою службової функції отримано порогове значення, що використовується для тренувального набору зображень (в ньому відомо, які саме контейнери містять в собі вбудовування серед усіх, а які порожні). Потім застосовується набір зображень для перевірки ефективності аналізаторів, для кожного проводиться розрахунок розбалансу коефіцієнта k, а потім порівняння отриманих значень зі значенням порогу t. Якщо значення розбалансу більше значення порогу, тоді можна сказати, що зображення містить вбудоване повідомлення, якщо значення менше – контейнер порожній і вбудовування не проводилось.

2.2.2 Дослідження ефективності методу та результати

На наборі для перевірки ефективності аналізаторів розраховано ймовірність розпізнавання заповненого або пустого контейнеру обраним методом.

Ймовірність правильного розпізнавання (*Pe*) заповненого контейнеру розраховується відповідно за формулою:

$$Pe = \frac{K}{L}, \tag{2.2}$$

де *K* – кількість зображень, у яких метод правильно розпізнав вбудовування секретного повідомлення;

L – загальна кількість контейнерів, що містять вбудовування – відомо завчасно.

Формула для розрахунку ймовірності правильного виявлення порожнього контейнеру (*Pp*):

$$Pp = \frac{M}{N}, \tag{2.3}$$

де *M* – кількість порожніх контейнерів, що розпізнав метод;

N - загальна кількість порожніх контейнерів, яка відома заздалегідь.

Помилки першого роду (false positive) – хибне спрацьовування, при якому метод розпізнає наявність вбудовування в контейнері, де насправді його не було.

Помилки другого роду (false negative) – пропуск події, зображує відсутність секретного повідомлення в контейнері, де наперед відомо, що воно є.

Ймовірність помилки першого та другого роду розраховуються за

формулами (2.4) та (2.5) відповідно:

$$P1 = 1 - Pp, \tag{2.4}$$

$$P2 = 1 - Pe, \tag{2.5}$$

Результати, які використовувалися для визначення ефективності аналітичного методу для розпізнавання наявності вбудованого секретного повідомлення наведено у таблиці 2.3.

Таблиця 2.3 – Параметри оцінки ефективності аналітичного методу

		Правильна гіпотеза	
		H_0	H_1
Результат застосування критерію	H_0	57,8 %	Помилка 2 роду 42,57 %
	H_1	Помилка 1 роду 42,2 %	57,43 %

У якості вихідної гіпотези H_0 було взято припущення, що контейнер порожній, а альтернативною гіпотезою H_1 стало припущення, що у контейнері є приховане повідомлення. З отриманих результатів видно, що ймовірність розпізнавання порожнього контейнеру серед усього набору зображень аналітичним методом дорівнює 57,8 %, а заповненого – 57,43%. Результати досить непогані, але для того, аби отримувати більш точніший результат детектування запропоновано метод, заснований на використанні нейронної мережі, яка налаштована на розпізнавання наявності вбудованого секретного повідомлення у стеганоконтейнерах, аналізуючи їх гістограми.

2.3 Стеганоаналітичний метод на основі нейронної мережі

2.3.1 Опис нейронних мереж

Нейронна мережа - це серія алгоритмів, які намагаються розпізнати основні взаємозв'язки в наборі даних через процес, що імітує спосіб роботи людського мозку. Нейронні мережі можуть адаптуватися до зміни вхідних даних; тому мережа генерує найкращий можливий результат без необхідності перепроектування критерії виводу [29]. Нейрон - це обчислювальна одиниця, яка отримує інформацію, виконує над нею прості обчислення і передає її далі. Вони діляться на три основні типи: вхідний, прихований і вихідний [30]. Глибокі нейронні мережі одночасно навчаються створювати процеси, що приховують або розкривають наявність секретного повідомлення у зображенні [31-34], тому знаходять широке застосування у розробці стеганографічних та стеганоаналітичних методів.

Було використано при проведенні експерименту:

1. Нейронна мережа типу «Patternnet», яка складається з 2 нейронів у прихованому шарі [35]. Нейронна мережа містить 2 шари: перший tansig - гіперболічна тангенціальна функція активації, другий – logsig – логістична сигмоїдальна функція. Структуру нейронної мережі представлено на рисунку 2.3.

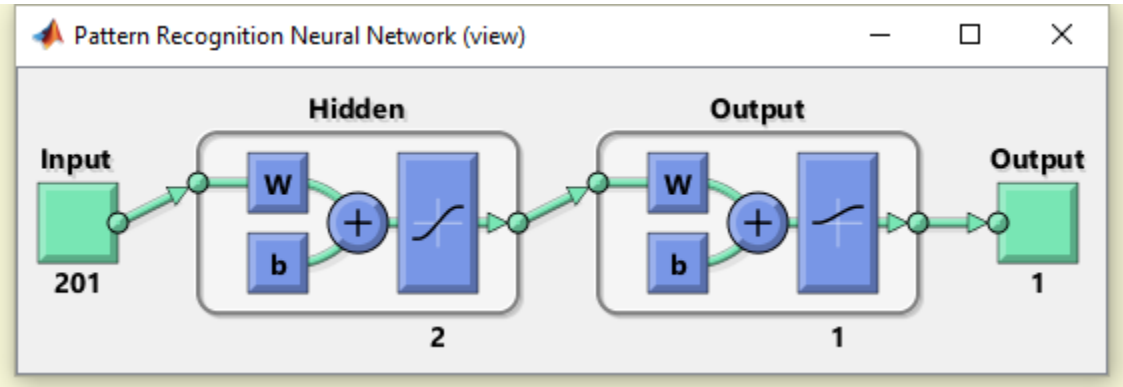

Рисунок 2.3 - Структура нейронної мережі типу «Patternnet»

2. Нейронна мережа Елмана - це тип рекурентної мережі, що

складається з багатошарового персептрону, весь прихований шар покритий динамічним зворотним зв'язком, тільки з'єднання надходять не з виходу мережі, а з виходів внутрішніх нейронів. Це дозволяє враховувати передісторію, накопичувати інформацію для розробки правильної стратегії управління. Ці мережі можна використовувати в системах управління рухомими об'єктами, так як їх головною особливістю є запам'ятовування послідовностей [39]. Структуру нейронної мережі представлено на рисунку 2.4.

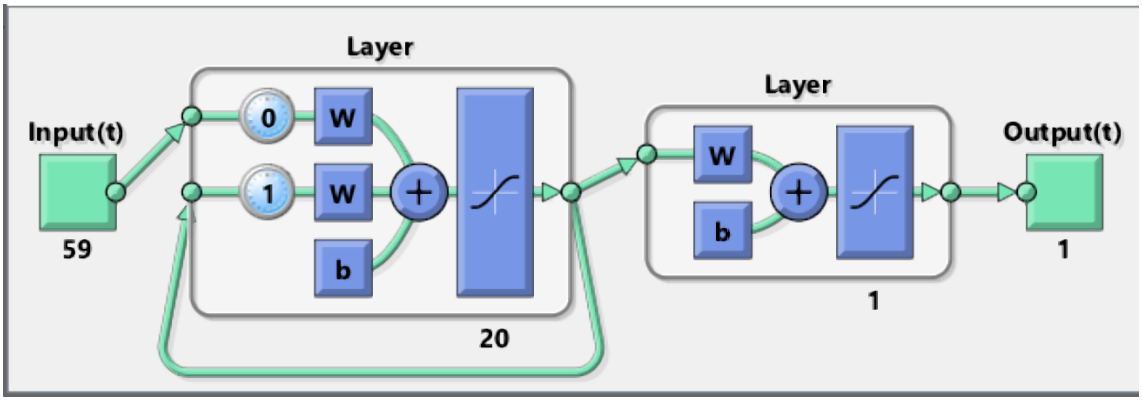

Рисунок 2.4. – Структура нейронної мережі Елмана

3. Нейронна мережа Feed-forward. Головне завдання - навчити нейрон. Навчання полягає в тому, щоб знайти правильні вага для кожного нейрона. Якщо на виході нейрона відомо, який має бути відповідь, і відомо, якій він вийшов, стає відома ця різниця - помилка. Цю помилку можна відправити назад до усіх входів нейрона і зрозуміти, який вхід наскільки сильно вплинув на цю помилку, і відповідно, підкоригувати вагу на цьому вході так, щоб помилку зменшити. Цей процес можна прогнати по усій мережі і для кожного нейрона знайти, як його ваги можна модифікувати.

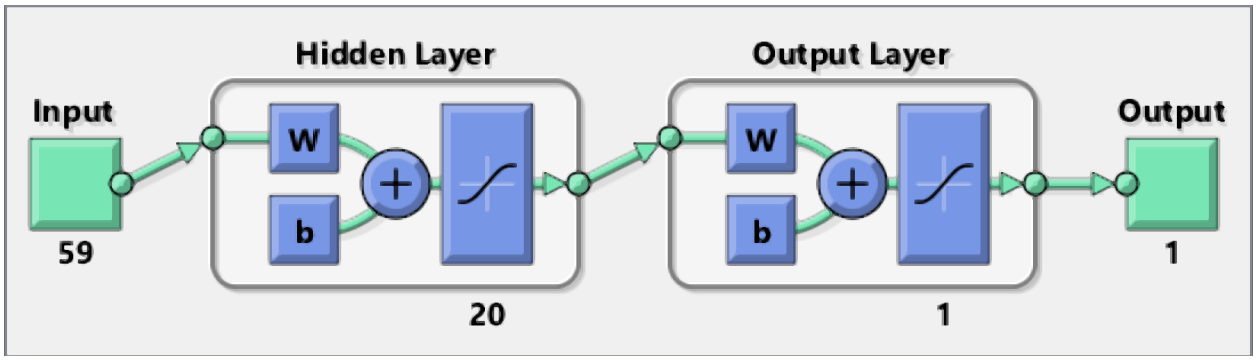

Рисунок 2.4. – Структура нейронної мережі Feed-forward

Прямі нейронні мережі (FF або FFNN) дуже прямолінійні, вони передають інформацію з входу на вихід. Нейронні мережі часто описують як шари, що мають, де кожен шар складається або з вхідних, або з прихованих, або з вихідних нейронів паралельно. Шар сам по собі ніколи не має з'єднань і, як правило, два сусідні шари повністю сполучені (кожен нейрон утворює один шар з кожним нейроном до іншого шару). Найпростіша, в деякій мірі практична мережа має два вхідні нейрони і один вихідний нейрон. Зазвичай тренують FFNN через зворотне поширення, даючи мережевим парним наборам даних "те, що входить" і "те, що ми хочемо, щоб виходило". Це називається контрольованим навчанням, на відміну від неконтрольованого навчання, де ми тільки вводимо його і дозволяємо мережі заповнити пропуски. Помилка, що виникає в результаті зворотної передачі, часто є деякою варіацією різниці між входом і виходом (наприклад, MSE або просто лінійну різницю).

Враховуючи, що в мережі досить прихованих нейронів, вона теоретично завжди може змоделювати співвідношення між входом і виходом. На практиці їх використання набагато більше обмежене, але вони популярно комбінуються з іншими мережами для формування нових мереж [30].

2.3.2 Дослідження ефективності методу та результати

Алгоритм детектування: на тренувальному наборі цифрових зображень визначається поріг, на вхід до нейронної мережі подається гістограма кожного із зображень тренувального набору. Нейронна мережа розпочинає

свій процес навчання на тренувальному наборі цифрових зображень. У результаті отримано натреновану нейронну мережу, що використовуватиметься для детектування.

Потім на другому наборі цифрових зображень перевіряється ефективність розпізнавання нейронною мережею наявності вбудовування. А саме, подається на її вхід гістограму кожного із зображень з набору для перевірки ефективності аналізаторів. Нейронна мережа видає значення діапазону (0; 1), що згодом порівнюється з пороговим значенням. Якщо виведене нейронною мережею значення менше порогу – вбудовування секретного повідомлення в цифровий контейнер не здійснювалось. У протилежному випадку, коли значення більше порогу – контейнер містить вбудоване секретне повідомлення.

Розрахунок показників ймовірності правильного розпізнавання пустого та заповненого контейнеру, помилки першого та другого роду відбувається за формулами наведеними вище (2.2, 2.3, 2.4, 2.5). Отримані результати наведені у таблиці 2.4.

Таблиця 2.4– Параметри ефективності методу з використанням нейронної мережі

		Правильна гіпотеза	
		H_0	H_1
Результат застосування критерію	H_0	93,8 %	Помилка 2 роду 4,5 %
	H_1	Помилка 1 роду 6,2 %	95,5 %

Ймовірність успішного виявлення порожнього контейнеру складає 93,8%, а секретного повідомлення – 95,5 %. Помилки першого роду – 6,2% та другого –4,5 %.

2.4 Порівняння ефективностей розроблених стеганоаналітичних методів

Порівняння ефективності правильного виявлення заповнених та порожніх контейнерів аналітичним методом та методом, що заснований на розпізнаванні образів за допомогою машинного навчання та отримання результатів (таблиця 2.5).

Таблиця 2.5– Порівняння ефективностей методів

		Правильна гіпотеза			
		Аналітичний метод		Нейронна мережа	
		H_0	H_1	H_0	H_1
Результат застосування критерію	H_0	57,8%	Помилка 2 роду 42,57 %	93,8 %	Помилка 2 роду 4,5 %
	H_1	Помилка 1 роду 42,2 %	57,43 %	Помилка 1 роду 6,2 %	95,5 %

Метод, що використовує нейронну мережу для розпізнавання наявності вбудованого повідомлення в контейнер, дає кращі результати, тому вважається набагато ефективнішим у порівнянні з аналітичним методом.

Якщо обчислювальну складність методів починати розраховувати з розпакованого зображення (має вигляд вже квантованих ДКП компонентів), то складність така:

а) збір статистики: O (кількість блоків в зображенні) – лінійна складність;

б) класифікація: O (1) – константна складність. Константна складність спрацьовування нейронної мережі:

1) множення вектора входів на матрицю ваг прихованого шару;

2) функція активації прихованого шару;

3) скалярний добуток результатів прихованого шару на ваги другого

шару;

4) функція активації другого шару.

Пропускну спроможність алгоритму F5 (яка досягається в експерименті) в бітах можна розрахувати за формулою (2.6):

$$T = N - N_0 - N_{DC} - N_S, \tag{2.6}$$

де N - загальна кількість коефіцієнтів ДКП контейнера;

N_0 – кількість ненульових коефіцієнтів;

N_S – кількість коефіцієнтів, у які не було змоги вбудувати біт повідомлення через усадку (shrinkage). Цей параметр залежить від конкретного контейнеру та секретного повідомлення;

Ndc– кількість постійних коефіцієнтів у блоках ДКП (по одному на блок розміром 8x8), що розраховується за формулою (2.7):

$$Ndc = \frac{N}{64}, \tag{2.7}$$

Аналіз результатів, отриманих в ході експерименту і наведених у таблиці 2.5, вказує на те, що запропонований стеганоаналітичний метод, заснований на розпізнанні образів за допомогою технології машинного навчання дає кращі показники розпізнавання наявності вбудованого повідомлення, у порівнянні із аналітичним методом, тому вважається набагато ефективнішим.

3 РЕАЛІЗАЦІЯ ПРОГРАМНОГО ПРОДУКТУ

3.1 Вибір середовища програмування

Сучасні програмні засоби дають великі можливості для виконання швидкого проведення процесу обчислення математичних моделей. Одним з найбільш поширених є пакет програм Matlab.

Система має великий набір спеціальних функцій, які реалізують різні числові методи, зокрема, знаходження коренів рівнянь систем, наближення табличних функцій, інтегрування, розв’язання задач лінійної алгебри, оптимізація, розв’язання систем звичайних диференціальних рівнянь. Числові розрахунки в Matlab виконують з використанням спеціальних функцій, кількість аргументів яких може бути різною.

Matlab являє собою потужну операційну середу для виконання величезної кількості математичних і науково-технічних розрахунків, обчислень і створення користувачами своїх пакетів розширення, бібліотек процедур і функцій. Нові версії системи мають вбудований компілятор і дозволяють створювати виконувані файли.

Ефективність обумовлена, перш за все, її орієнтацією на матричні обчислення з програмною емуляцією паралельних обчислень та спрощеними засобами завдання циклів.

Матрична система комп'ютерної математики Matlab дозволяє аналізувати різні дані, розраховувати моделі, алгоритми і додатки, що мають зручні інструменти ефективної обробки зображень, а також засоби обробки зображень. Пакет являє собою широкий набір числових викладів і функцій для створення, обробки та аналізу цифрових зображень. Обробка зображень, що має гнучкий інтерфейс, дозволяє ефективно маніпулювати зображеннями, розбираючи інтерактивну графіку, візуалізуючи різні набори даних [29].

На сьогоднішній день система Matlab, зокрема пакет прикладних програм Image Processing Toolbox, є найбільш потужним інструментом для моделювання та дослідження методів обробки зображень. Він надає велику

кількість вбудованих функцій, реалізуючих найбільш поширені методи обробки зображень.

Однією з основних завдань при створенні системи Matlab завжди було надання користувачам потужної мови програмування, орієнтованої на технічні та математичні розрахунки для реалізації чисельних методів. При цьому особлива увага приділялася як підвищенню швидкості обчислень, так і адаптації системи до вирішення найрізноманітніших завдань користувачів.

Matlab реалізує три важливі концепції програмування:

- процедурне модульне програмування, засноване на створенні модулів - процедур і функцій;

- об'єктно-орієнтоване програмування, особливо цінне в реалізації графічних засобів системи;

- візуально-орієнтоване програмування, спрямоване на створення засобів графічного інтерфейсу користувача GUI (Graphics User Interface).

Вбудоване середовище розробки надає можливість створювати призначені для користувача графічні інтерфейси з різними елементами управління, такими як кнопки, поля введення і іншими.

Мова Matlab є високорівневою інтерпретованою мовою програмування, яка включає засновані на матрицях структури даних, широкий спектр функцій, інтегроване середовище розробки, об'єктно-орієнтовані можливості і інтерфейси до програмам, що написані на інших мовах програмування [29], [30].

Тому для розробки стеганоалгоритму та стеганоаналітичних методів був обраний Matlab. Адже він має багато вбудованих засобів для обробки зображень. Завдяки його математичній базі дуже просто реалізувати алгоритм та впровадити потрібний функціонал майбутнього програмного продукту.

Програмний продукт був розроблений за допомогою App Designer - рекомендоване середовище для створення додатків в Matlab, що об'єднує дві основні задачі побудови програми - створення візуальних компонентів

графічного інтерфейсу користувача (GUI) і поведінку додатку для програмування.

App Designer автоматично генерує об'єктно-орієнтований код, який визначає макет і дизайн додатку [31].

3.2 Інтерфейс програмного продукту

Для вбудовування секретного повідомлення та виконання стеганоаналізу цифрового зображення розробленими методами в середовищі Matlab було реалізовано програмний інтерфейс, представлений на рисунку 3.1.

Форма інтерфейсу містить елементи:

- «Обране зображення» - область, яка відображає зображення, обране користувачем, у форматі JPEG, за допомогою Matlab зображення із кольорового перетворюється на зображення в градаціях сірого.

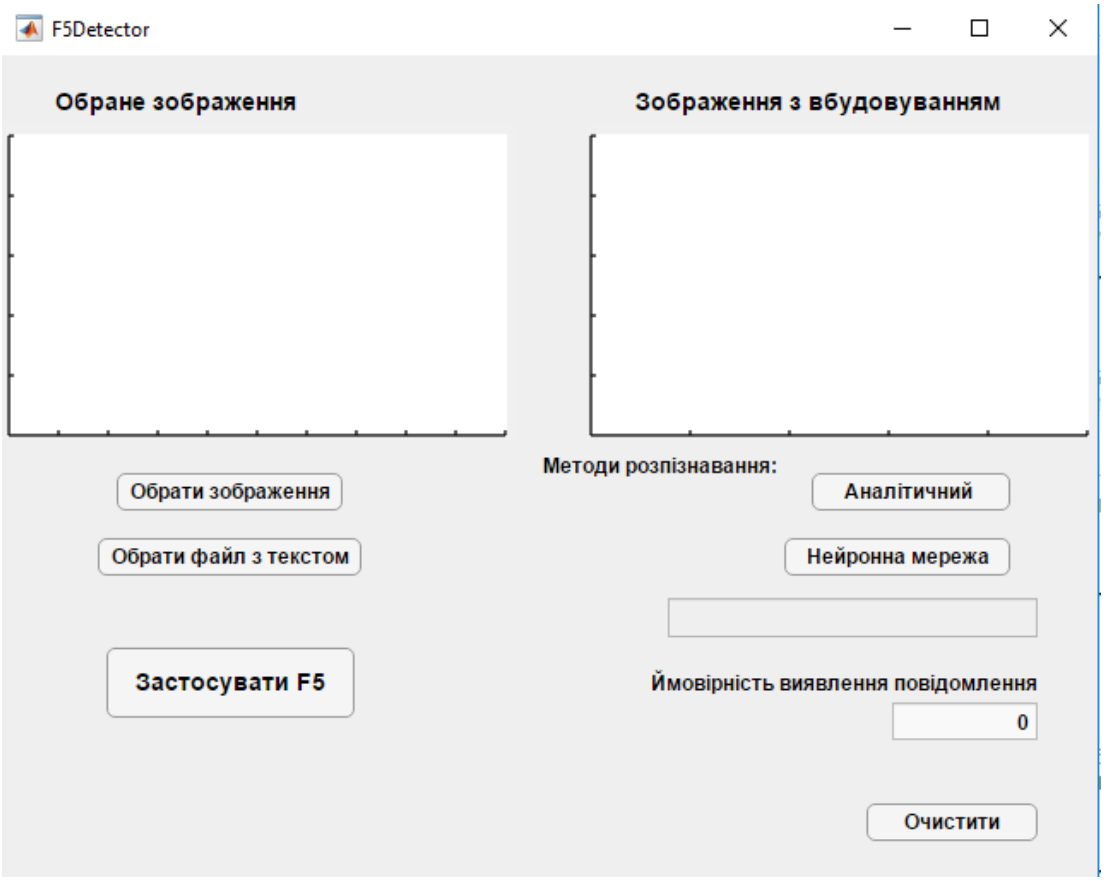

Рисунок 3.1 - Інтерфейс програмної реалізації стеганоаналітичного алгоритму

- «Обрати зображення» - кнопка, яка дозволяє завантажити зображення для застосування після натиску на неї (рисунок 3.2). Результат: в області «Обране зображення» виведено те зображення, яке обрав користувач (рисунок 3.3).

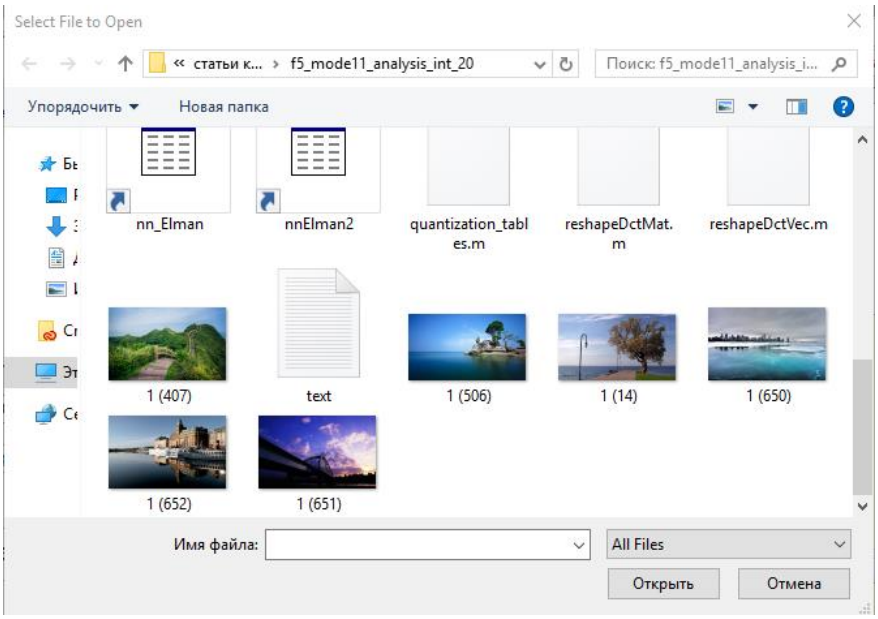

Рисунок 3.2 – Вибір зображення

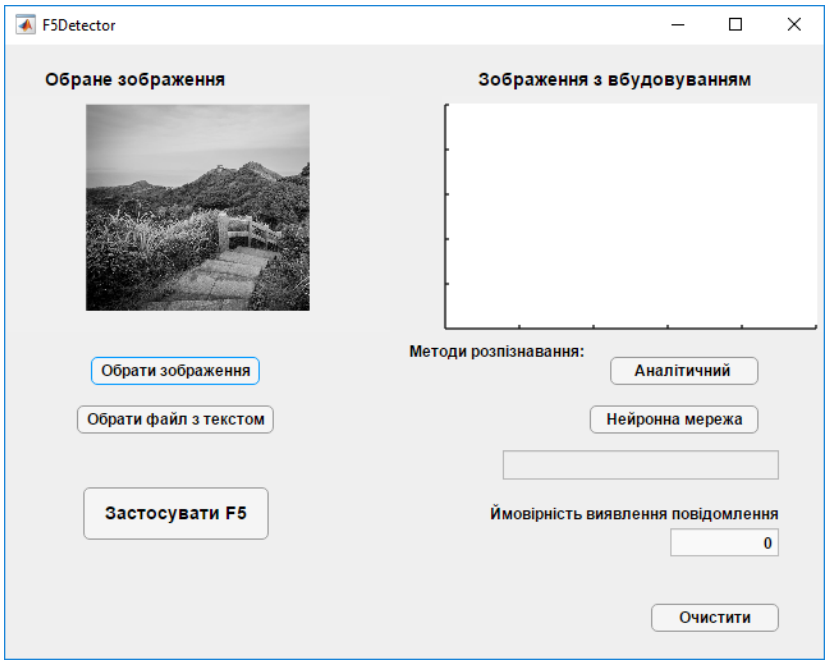

Рисунок 3.3 – Відображення обраного зображення

- «Обрати файл з текстом» - кнопка, що призначена для вибору файлу, в якому міститься секретне повідомлення, яке буде вбудовано у цифровий контейнер (рисунок 3.4). Повідомлення буде перетворено у бітову послідовність за допомогою шифрування і надалі буде вбудовано в зображення.

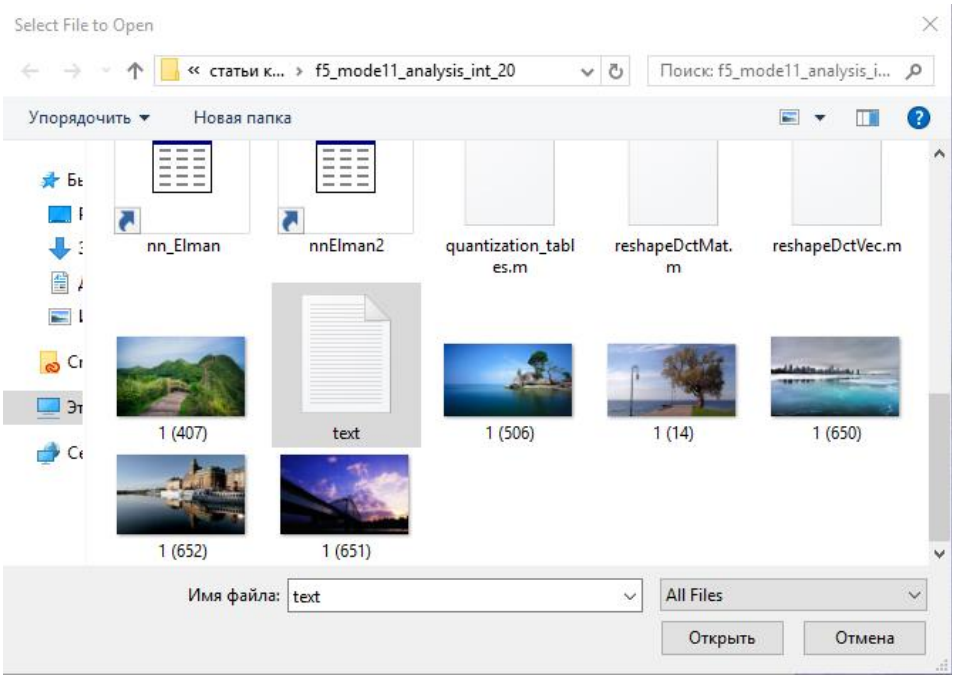

Рисунок 3.4 – Вибір файлу з секретним повідомленням

- Пусте поле, у якому з’явиться текст червоного кольору «Знайдено повідомлення», якщо зображення містить у собі вбудовування. У протилежному випадку – відображатиметься текст зеленого кольору «Повідомлення не знайдено».
- «Зображення з вбудовуванням» - відображає цифрове зображення, отримане в результаті застосування алгоритму F5 і містить в собі стеганоповідомлення.
- «Застосувати F5» - кнопка натискається користувачем після вибору файлу з секретним повідомленням. Результат: в області «Зображення з вбудовуванням» з’являється зображення, в яке вбудовано повідомлення за допомогою алгоритму F5 (рисунок 3.5).

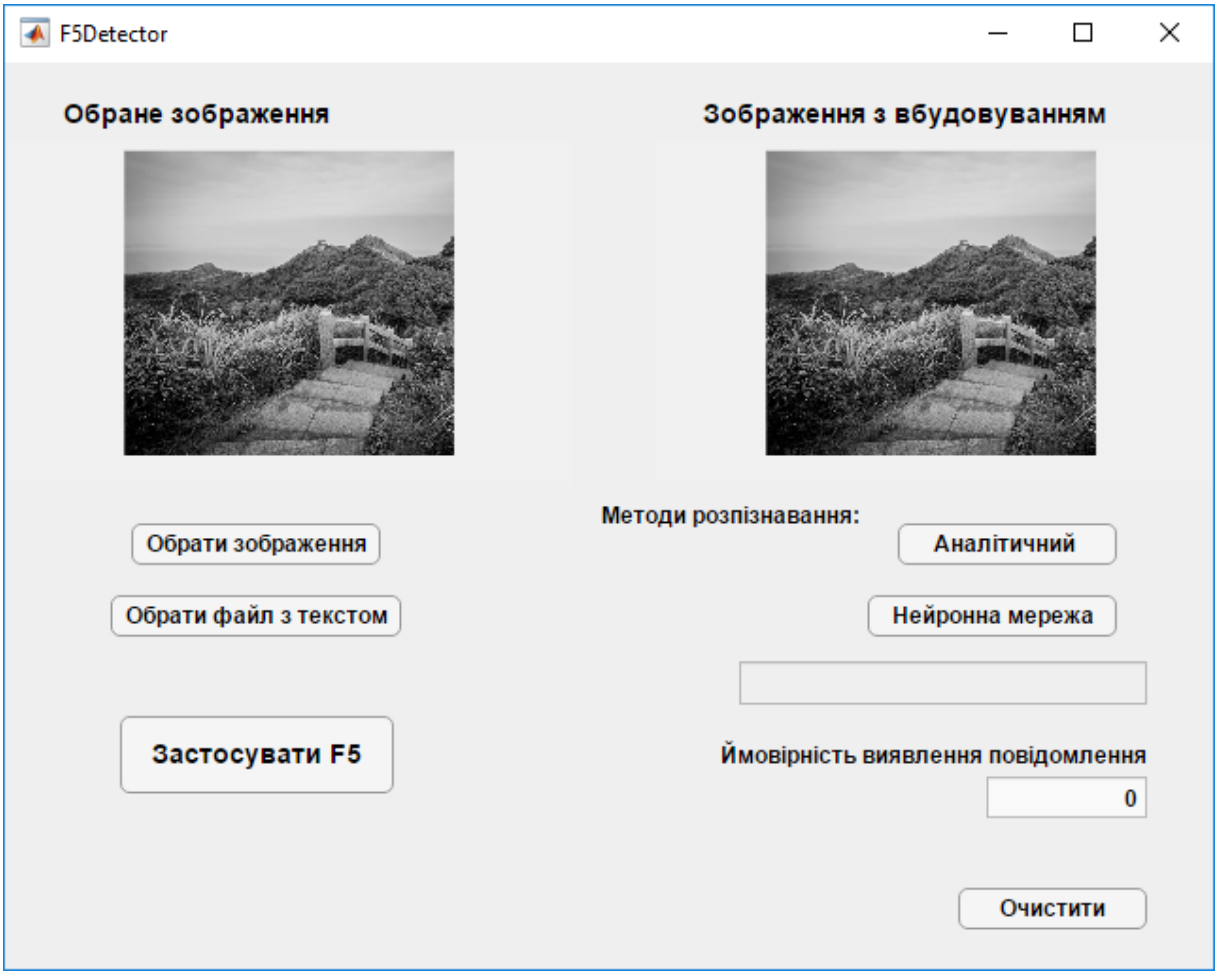

Рисунок 3.5 – Застосування F5

- «Методи розпізнавання» - блок, що дозволяє виконати аналіз отриманого зображення одним із двох запропонованих методом: аналітичним (кнопка «Аналітичний», рисунок 3.6) або нейронною мережею (кнопка «Нейронна мережа», рисунок 3.7). У результаті отримано відповідь про наявність або відсутність вбудованого повідомлення.
- «Ймовірність виявлення повідомлення» - поле, у якому відображається числове значення, що являє собою ймовірність правильного детектування зображення з вбудовуванням.
- «Очистити» - кнопка очищає робочий інтерфейс після проведеної роботи детектування, даючи змогу обрати інше зображення.

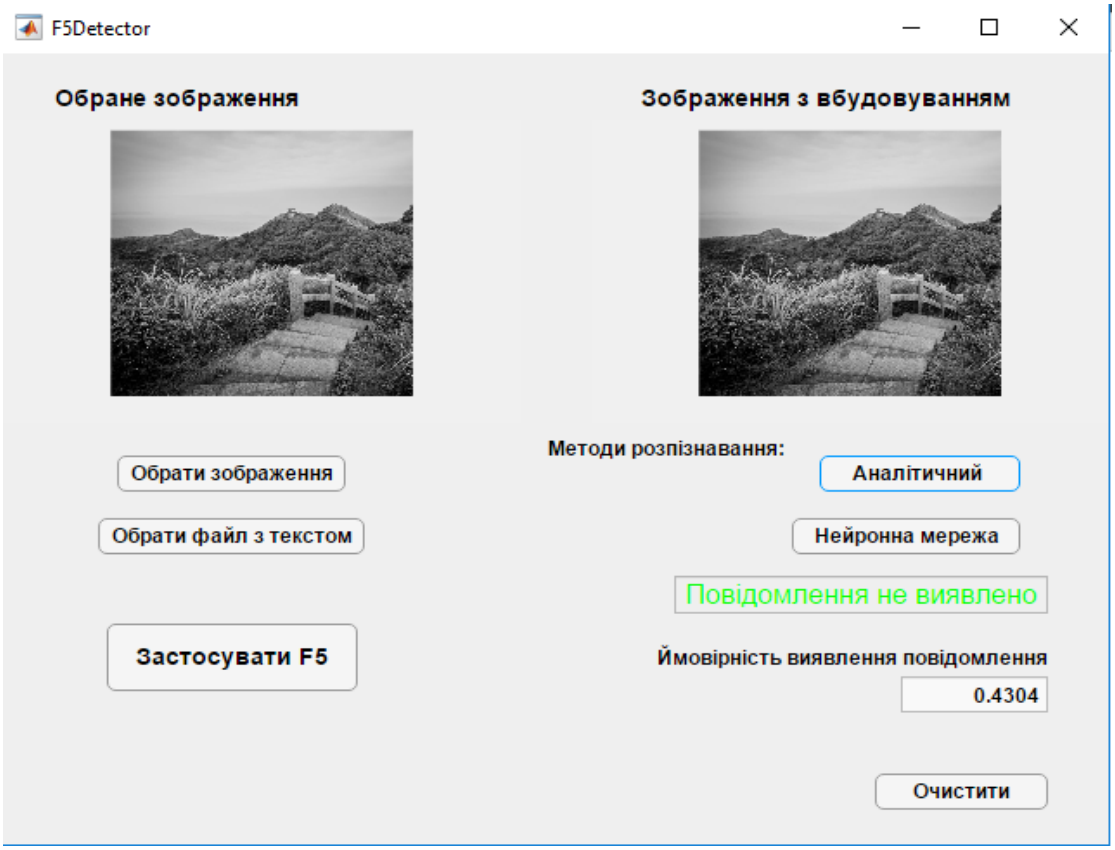

Рисунок 3.6 – Результат детектування аналітичним методом

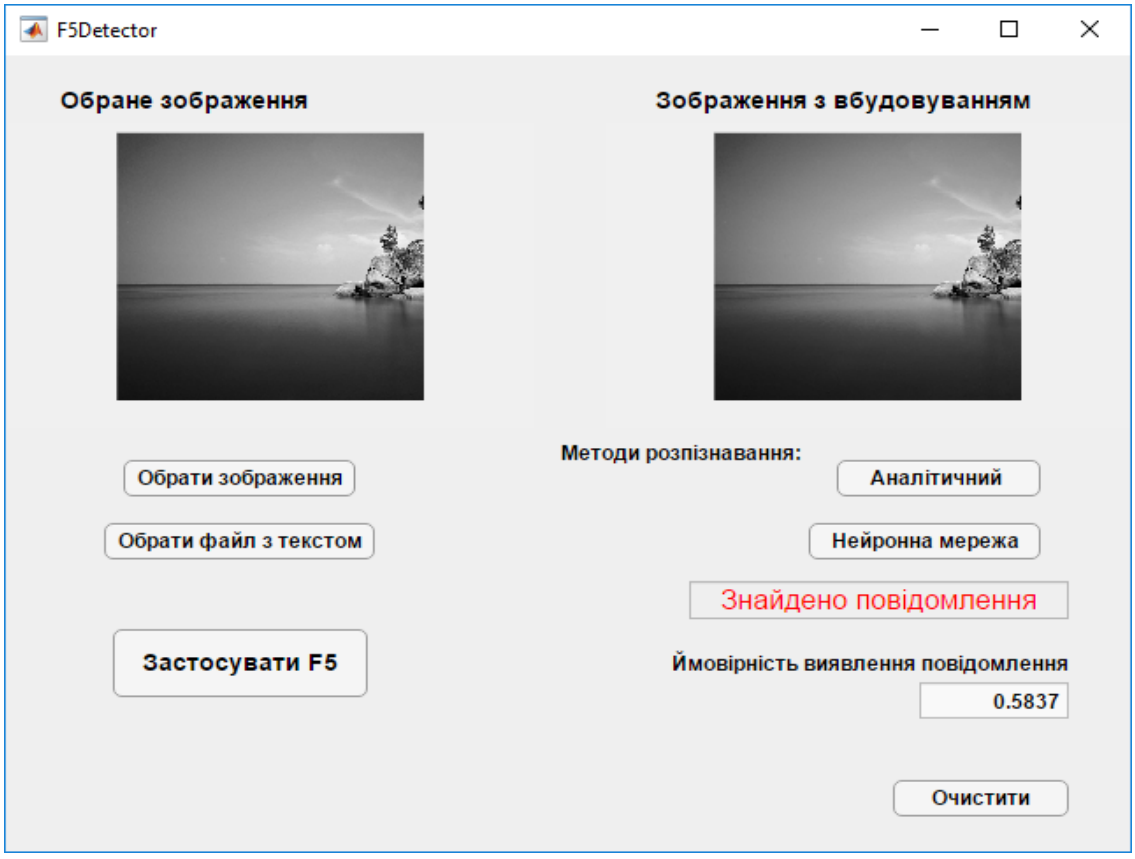

Рисунок 3.7 – Результат детектування методом на основі нейронної мережі

Таким чином, програмний продукт був розроблений за допомогою App Designer та має зручний, інтуїтивно простий інтерфейс, який містить області для виведення зображень, кнопки та числове поле.

Інтерфейс націлений на можливість вбудовування текстового повідомлення у зображення алгоритмом F5 та розпізнавання наявності стеганоповідомлення у цифровому зображенні одним з двох обраних методів (аналітичний метод або метод, заснований на розпізнаванні образів за допомогою технології машинного навчання), даючи ймовірність правильного детектування наявності стеганоповідомлення у цифровому зображенні-контейнері.

Код програмного продукту подано у додатку А.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи була досягнута мета - підвищення ймовірності детектування прихованого повідомлення в цифровому зображенні шляхом розробки методу аналізу статистики зображення-контейнеру з використанням нейронної мережі . Було проаналізовано сучасні методи стеганографії та запропоновано власний стеганоаналітичний метод.

Проведено дослідження, яке підтверджує ефективність використання обох методів для детектування. Результати детектування наявності секретного повідомлення показали, що метод з використанням нейронної мережі дає кращі показники детектування – 97-98%, в свою чергу аналітичний метод - 57,8%.

Розроблено програмний продукт для застосування алгоритму F5 та подальшого використання методів для перевірки наявності вбудованого повідомлення в контейнер-зображення.

ПЕРЕЛІК ПОСИЛАНЬ

1. Нечитайлова Л.В., Калашніков М.В., Яковенко О.О., Кушніренко Н.І., Белека І.А. Стеганоаналітичний метод для контейнерів F5 на основі штучної нейронної мережі. Вісник Інженерної академії України. 2019. №2. С. 34-39.
2. Про національну безпеку України : Закон України від 21.06.2018р. №2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19
3. Encryption technology. Network security. Steganography. Defenition. URL: https://searchsecurity.techtarget.com/definition/steganography.
4. Sean Gallagher. Steganography: how al-Qaeda hid secret documents in a porn video. URL: https://arstechnica.com/information-technology/2012/05/steganography-how-al-qaeda-hid-secret-documents-in-a-porn-video/.
5. Patrick Trech. List of printers which do or do not display tracking dots. URL: https://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots/.
6. Trend Micro. Malicious Memes that Communicate with Malware. URL: https://www.trendmicro.com/en_us/research/18/l/cybercriminals-use-malicious-memes-that-communicate-with-malware.html.
7. Department of justice. Former GE Engineer and Chinese Businessman Charged with Economic Espionage and Theft of GE's Trade Secrets. URL: https://www.justice.gov/opa/pr/former-ge-engineer-and-chinese-businessman-charged-economic-espionage-and-theft-ge-s-trade.
8. Ang M.C., Mendoza E., Yaneza J. LokiBot Gains New Persistence Mechanism, Steganography. URL: https://www.trendmicro.com/en_us/research/19/h/lokibot-gains-new-persistence-mechanism-uses-steganography-to-hide-its-tracks.html.

9. Guardicore Labs Team. Threats Making WAVs – Incident Response To A Cryptomining Attack. URL: https://www.guardicore.com/2020/01/threats-making-wavs-incident-reponse-cryptomining-attack/.
10. Jérôme Segura. New evasion techniques found in web skimmers. URL: https://blog.malwarebytes.com/threat-analysis/2019/12/new-evasion-techniques-found-in-web-skimmers/.
11. Грибунин В. Г., Костюков В. Е., Мартынов А. П., Николаев Д. Б., Фомченко В. Н. Стеганографические системы. Критерии и методическое обеспечение. Саров: Російський федеральний ядерний центр – ВНИИЭФ, 2016. 210 с.
12. Westfeld A., Pfitzmann A. Attacks on steganographic systems. URL: https://link.springer.com/chapter/10.1007/10719724_5.
13. Jókay M., Gulášová M. Steganalysis of Stegostorage Library. URL: https://www.researchgate.net/publication/314110775_Steganalysis_of_Stegostorage_Library.
14. Fridrich J., Goljan M., Hogea D. Steganalysis of JPEG Images: Breaking the F5 Algorithm. URL: https://link.springer.com/chapter/10.1007/3-540-36415-3_20.
15. Евсютин О., Шумская О. Сравнение линейного дискриминанта Фишера и наивного байесовского классификатора в задаче стегоанализа JPEG-изображений. URL: https://www.elibrary.ru/item.asp?id=30732443.
16. Hendrych J., Kunčický R., Ličev L. New Approach to Steganography Detection via Steganalysis Framework. URL: https://www.researchgate.net/publication/320124276_New_Approach_to_Steganography_Detection_via_Steganalysis_Framework.
17. Jafari R., Ziou D. Efficient steganalysis of images: Learning is good for anticipation. URL: https://www.researchgate.net/publication/257472327_Efficient_steganalysis_of_images_Learning_is_good_for_anticipation.

18. Watanabe S., Murakami K., Furukawa T. Steganalysis of JPEG image-based steganography with support vector machine. URL: https://www.researchgate.net/publication/305676731_Steganalysis_of_JPEG_image-based_steganography_with_support_vector_machine.
19. Ping X., Wang R., Xu M., Zhang T. Steganalysis of JPEG images by block texture based segmentation.URL: https://www.researchgate.net/publication/260530015_Steganalysis_of_JPEG_images_by_block_texture_based_segmentation.
20. Fridrich J., Pevný T. Merging Markov and DCT features for multi-class JPEG steganalysis. URL: https://www.researchgate.net/publication/228821328_Merging_Markov_and_DCT_features_for_multi-class_JPEG_steganalysis. \
21. Mahamuni S., Sutar A. New Steganalysis Approach for JPEG Image Steganography using F5 Algorithm URL: http://europub.co.uk/articles/24816/view.
22. Смірнов О., Мелешко Є. Дослідження методів стегоаналізу цифрових зображень. URL: http://dspace.kntu.kr.ua/jspui/handle/123456789/3341.
23. Полунін А., Яндашевская Е. Использование аппарата свёрточных нейронных сетей для стегоанализа цифровых изображений. URL: https://ispranproceedings.elpub.ru/jour/article/view/1321.
24. Калашніков М, Коханов О., Яковенко О., Кушніренко Н. URL: http://journals.uran.ua/eejet/article/download/201731/202313.
25. R. Crandall. Some Notes on Steganography. URL: http://os.inf.tu-dresden.de/west-feld/crandall.pdf.
26. Schmidhuber J. Deep Learning in Neural Networks: An Overview. URL: https://arxiv.org/abs/1404.7828/.
27. Leijnen S. The neural network zoo. URL: http://www.asimovinstitute.org/neural-network-zoo.
28. Baluja S. Hiding images in plain sight: Deep Steganography. URL: https://arxiv.org/ftp/arxiv/papers/1912/1912.13156.pdf.

29. Sumathi C., Umamaheswari J., Santanam T. A study of various steganographic techniques used for information hiding. URL: https://www.researchgate.net/publication/259844912_A_Study_of_Various_Steganographic_Techniques_Used_for_Information_Hiding.
30. Brandao A. Artificial Neural Networks Applied to Image Steganography. URL: https://www.researchgate.net/publication/301665889_Artificial_Neural_Networks_Applied_to_Image_Steganography.
31. Hu D., Wang L., Jiang W., Zheng S. A novel image steganography method via deep convolutional generative adversarial networks. URL: https://www.researchgate.net/publication/326192682_A_Novel_Image_Steganography_Method_via_Deep_Convolutional_Generative_Adversarial_Network
32. Струкова В. Основы работы с изображениями в пакете Image Processing Toolbox среды MATLAB. URL: https://www.elibrary.ru/item.asp?id=28096711.
33. Офіційний сайт розробника MatLab. URL: www.mathworks.com.
34. Дьяконов В. MATLAB. Полный самоучитель. URL: https://elprivod.nmu.org.ua/files/mathapps/Дьяконов_matlab_полный_самоучит.pdf
35. MATLAB. Creating Graphical User Interfaces. URL: http://www.apmath.spbu.ru/ru/staff/smirnovmn/files/buildgui.pdf
36. Elman, J.L. Finding structure in time. URL: https://www.semanticscholar.org/paper/Finding-Structure-in-Time-Elman/668087f0ae7ce1de6e0bd0965dbb480c08103260/