Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Аналіз методів цифрової стеганографії на основі дискретного косинусного перетворення

Виконав: студент II курсу, групи СБм-61
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

(підпис) Тернавчук І.В. (прізвище та ініціали)

Керівник (підпис) Оробчук О.Р. (прізвище та ініціали)

Нормоконтроль (підпис) Лечаченко Т.А. (прізвище та ініціали)

Завідувач кафедри (підпис) Загородна Н.В. (прізвище та ініціали)

Рецензент (підпис) (прізвище та ініціали)

Тернопіль
2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«____» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Тернавчуку Ігору Васильовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Аналіз методів цифрової стеганографії на основі дискретного косинусного перетворення

Керівник роботи Оробчук Олександра Романівна, PhD., ст.викладач кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «16» листопада 2023 року № 4/7-1061

2. Термін подання студентом завершеної роботи 14 грудня 2023р.

3. Вихідні дані до роботи

4. Зміст роботи (перелік питань, які потрібно розробити):
   1. Аналіз методів цифрової стеганографії
   2. Дослідження та огляд методу цифрової стеганографії на основі дискретно косинусного перетворення
   3. Дослідження стійкості алгоритму до поширених атак на стеганосистеми
   4. Охорона праці та безпека в надзвичайних ситуаціях

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Титульна сторінка. Мета. Завдання дослідження. Наукова новизна Задачі цифрової стеганографії, Недоліки ЗСЛ, Чутливість до контрасту та поріг непомітності , Класифікація методів цифрової стеганографії, Структурна схема роботи методів у часовому та частотному просторі, Результат проведеного аналізу методом компромісного рішення, Класифікація стегасистем та контейнерів, Алгоритм цифрової стеганографії на основі дискретно-косинусного перетворення Трансформація колірного простору Схема та мат.обгрунтування процеса дискретно-косинусного перетворення Процес та результат квантування, Зигзаг-сканування, Результати заміни різних біт пікселя Результати статистичної, візуальної та геометричної атаки. Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання 16 листопада 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	16.11.2023-17.11.2023	*Виконано*
2.	Підбір наукових джерел про стеганосистеми	18.11.2023-20.11.2023	*Виконано*
3.	Переклад та опрацювання наукових джерел про		
	дослідження стеганоалгоритмів, їх типів та		
	стійкості до атак	21.11.2023-23.11.2023	*Виконано*
4.	Виконання дослідження щодо стійкості		
	стеганоалгоритму , що базується на ДКП		
	Відносно різних атак	24.11.2023-27.11.2023	*Виконано*
5.	Оформлення розділу «Аналіз методів цифрової		
	стеганографії»	28.11.2023-30.11.2023	*Виконано*
6.	Оформлення розділу «Дослідження та огляд методу		
	цифрової стеганографії на основі дискретного		
	косинусного перетворення»	01.12.2023-04.12.2023	*Виконано*
7.	Оформлення розділу «Дослідження стійкості		
	алгоритму до поширених атак на стеганосистеми»	05.12.2023-07.12.2023	*Виконано*
8.	Виконання завдання до підрозділу «Охорона праці»	08.12.2023-09.12.2023	*Виконано*
9.	Виконання завдання до підрозділу «Безпека в надзви-		
	чайних ситуаціях»	10.12.2023-11.12.2023	*Виконано*
10.	Оформлення кваліфікаційної роботи	12.12.2023-13.12.2023	*Виконано*
11.	Нормоконтроль	14.12.2023-15.12.2023	*Виконано*
12.	Перевірка на плагіат	09.12.2023	*Виконано*
13.	Попередній захист кваліфікаційної роботи	16.12.2023	*Виконано*
14.	Захист кваліфікаційної роботи	27.12.2023	

Студент _____ Тернавчук І.В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Оробчук О.Р.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Аналіз методів цифрової стеганографії на основі дискретного косинусного перетворення // Кваліфікаційна роботи рівня «Магістр» // Тернавчук Ігор Васильович // Тернопільський національний технічний університет імені Івана Пулюя, Факультет комп'ютерно-інформаційних систем та програмної інженерії, кафедра кібербезпеки, група СБм–61 // Тернопіль, 2023 // с. - ___ , рис. - ___ , бібліогр. – ___ .

Ключові слова: СТЕГАНОГРАФІЯ, СТЕГАНОГРАФІЧНА СИСТЕМА, КОНТЕЙНЕР, ДИСКРЕТНО КОСИНУСНЕ ПЕРЕТВОРЕННЯ, ВБУДОВУВАННЯ ТА ВИЛУЧЕННЯ ІНФОРМАЦІЇ, АТАКИ НА СТЕГАСИСТЕМИ.

Метою роботи – дослідження методів цифрової стеганографії на основі дискретно косинусного перетворення.

Для дослідження були проведені: аналіз існуючих методів стеганографії, синтез для поєднання переваг та недоліків існуючих методів стеганографії, класифікація стеганографічних систем, класифікація контейнерів, порівняльний аналіз для оцінювання адекватності моделі процесів функціонування стеганографічних систем. Також була вивчена модель стиснення JPEG.

Для проведення досліджень був розроблений програмний продукт, що дозволяє проводити вбудовування конфіденційної інформації за допомогою метода цифрової стеганографії для контейнера-зображення та витягувати вбудовану інформацію з стегоконтейнера. В основі методу вбудовування конфіденційної інформації лежить метод на основі дискретного косинусного перетворення.Результати дослідження можуть бути використані в науково-дослідницьких закладах та підрозділах підприємств, що займаються проблемами захисту інформації.

ANNOTATION

Analysis of Methods of Digital Steganography Based on Discrete Cosine Transformation // Qualification paper of the educational level “Master” // Ihor Ternavchuk // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security, SBm-61 group // Ternopil, 2023 // P. , fig. - , tables - , annexes - , references - .

Key words: STEGANOGRAPHY, STEGANOGRAPHIC SYSTEM, CONTAINER, DISCRETE COSINE TRANSFORM, INSERTION AND RETRIEVAL OF INFORMATION, ATTACK ON STEGOSYSTEM.

The aim of this work is the study of methods of digital steganography based on discrete cosine transform.

For studies have been conducted: analysis of existing methods of steganography, the synthesis for the combinations of advantages and disadvantages of existing methods of steganography, steganography classification systems, classification of containers, a comparative analysis to assess the adequacy of models of processes of functioning steganographic systems. Also we studied the model of JPEG compression.

For research we have developed a software product that allows you to embed confidential information by using digital steganography to container-image and extract the embedded information from stegocontainer are. The method of embedding confidential information is the method based on the discrete cosine transform.

The results of the study can be used in scientific research institutions and departments dealing with information security.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

BMP - bitmap

JPEG - Joint Photographic Experts Group

ДКП – дискретне косинусне перетворення

ЗСЛ – зорова система людини

НС – надзвичайна ситуація

НЧ – низькі частоти

ВЧ – високі частоти

ЦЗ – цивільний захист

ЗМІСТ

ВСТУП

З переходом до цифрового представлення інформації загострилася і без того актуальна проблема захисту конфіденційної інформації від несанкціонованого доступу. Бо інформація така як відео, аудіо, текстові файли або зображення можуть виступати контейнерами для приховування конфіденційних даних. Дану проблему вирішують дві найдревніші науки: криптографія та стеганографія. Але більший інтерес являє собою наука – стеганографія, тому що найбільш успішний спосіб захистити інформацію – це приховати сам факт наявності в ній чогось конфіденційного, що може привернути увагу зловмисника.

Існує множина стеганографічних методів. Але як обрати найнадійніший? Насправді навіть на сьогоднішній день не існує такого методу, який на сто відсотків забезпечує безпеку інформації, бо технології не стоять на місці, вони розвиваються кожен день. Наприклад, якщо сьогодні було розроблено найбільш надійний метод цифрової стеганографії, то ніхто не дасть гарантії, що вже завтра проти нього буде розроблено відповідну атаку. Але можна обрати найбільш оптимальний метод, провівши аналіз завдяки набору якісних характеристик.

Такими характеристиками є: обсяг, невидимість та стабільність. Наскільки велику кількість інформації, можна вбудувати в контейнер показує така характеристика як обсяг. Те як добре схована інформація, що людина не може помітити сам факт її наявності, показує характеристика невидимість. Стабільність означає стійкість контейнера до помилок, а саме як модифікація контейнера впливає на приховані у ньому дані. Під модифікацією мається на увазі застосування різних фільтрів, обрізки, зміни розмірів контейнера.

Дана тема актуальна бо безпосередньо пов'язана з безпекою і захистом конфіденційної інформації. Стеганографічні методи дуже схожі з технологіями, застосовуваними для впровадження цифрових водяних знаків (ЦВЗ). ЦВЗ являє собою якусь цифровий підпис, який вбудовується в мультимедійний об'єкт з метою захисту авторських прав [23]. Відмінність від ЦВЗ стеганографії полягає

в тому, що стеганографія більше націлена на невидимість впроваджуваної інформації для людського сприйняття, а методи вбудовування ЦВЗ роблять упор на стійкість впроваджуваної інформації. Впровадження цифрових підписів дозволяє визначити власника інформації та відслідковувати її незаконне поширення [24].

Таким чином на сьогоднішній день найбільш актуальна проблема удосконалення алгоритмів і методів стеганографічного приховування конфіденційної інформації.

Предметом даної роботи є аналіз методів цифрової стеганографії на основі дискретно косинусного перетворення.

Об’єктом є процес забезпечення скритності інформації за допомогою методу цифрової стеганографії.

1 АНАЛІЗ МЕТОДІВ ЦИФРОВОЇ СТЕГАНОГРАФІЇ

1.1 Передумови виникнення цифрової стеганографії.

Передумовою виникнення цифрової стеганографії стало недоліки СЗЛ людини. Людське око більш чутливе до зміни яскравості, ніж зміни кольору, а також краще сприймає плавні переходи кольору, ніж його різкі зміни.

Властивості СЗЛ діляться на дві групи: галузеві («фізіологічні») та високого рівня («психофізіологічні»).

До високорівневих відносяться властивості, які безпосередньо пов'язані з роботою нервової системи людини, рівнем освіти, загальною культурою, родом діяльності (чутливість до розміром, формою, місцем розміщення об'єкта, до зовнішніх подразників). Дослідження цих властивостей безумовно перспективні, але на сьогоднішній день методи цифрової стеганографії ґрунтуються на основних властивостях СЗЛ.

Виділимо три найважливіші низькорівневих властивості: чутливість до зміни яскравості зображення, частотна чутливість і ефект маскування [4].

То що СЗЛ більш чутлива до зміни яскравості, перевіряємо шляхом проведення експериментів. Людині показують однотонне зображення (рис. 1.1.). Коли око адаптується до освітленості картинки I, поступово буде змінюватися яскравість навколо плями в центрі.

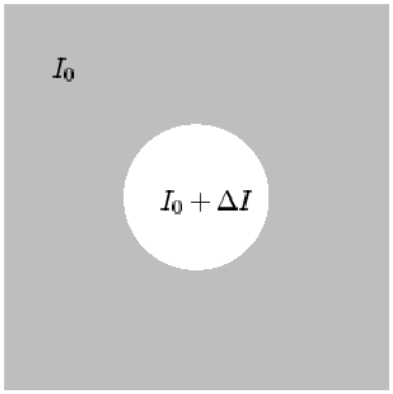


Рисунок 1.1 - Чутливість до контрасту і поріг непомітності ΔI

На рис. 1.2 представлений графік залежності. Провівши дослідження можна зробити висновок, що для малих і більших яскравостей поріг непомітності зростає, а для середнього діапазону яскравості він приблизно постійний.

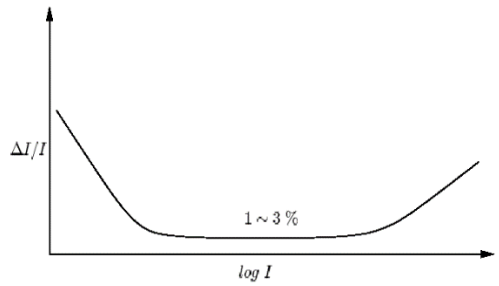


Рисунок 1.2 - Чутливість до контрасту та поріг непомітності ΔI

Якщо розглянути з точки частотної чутливості ЗСЛ, то можна зробити висновок, що людське око більш чутливе до низькочастотного, ніж до високочастотного шуму. Це відбувається тому, що низькочастотна (НЧ) область відповідає за загальний фон зображення.

Високочастотна (ВЧ) область відповідає за різкі перепади яскравості – висококонтрастні ділянки зображення. Для прикладу нижче представлена картинка, до якої застосовано два фільтра: низькочастотний (рис. 1.3.) і високочастотний (рис. 1.4.)

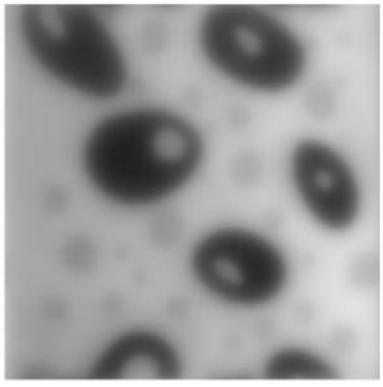


Рисунок 1.3 - Результат роботи низькочастотного фільтра

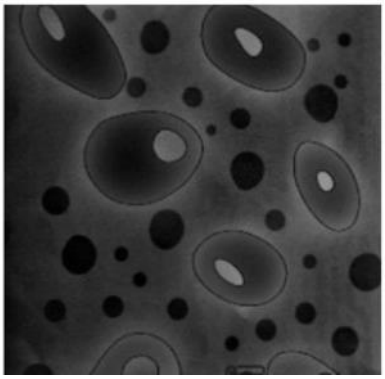


Рисунок 1.4 - Результат роботи високочастотного фільтра

Зробимо висновок, що на сьогодні одна з найбільш стародавніх наук стеганографія, базується на недоліках ЗСЛ, а також може гарантувати прихованість конфіденційної інформації.

1.2 Класифікація методів цифрової стеганографії

На основі проведеного аналізу представлена таблиця основних задач, областей застосування цифрової стеганографії:

Таблиця 1.1 - Основні задачі та області застосування цифрової стеганографії

Задача	Область застосування	Технологія та шляхи вирішення
1	2	3
Захист конфіденційної інформації від несанкціонованого доступу	Військові та інші додатки, а також застосування у випадках, коли не можна використовувати криптографію	Вбудовування прихованої інформації у загальнодоступній мультимедійну інформацію
Захист авторського права на інтелектуальну власність від копіювання та аутентифікація	Технології ЦВЗ та ІН використовуються для захисту від копіювання електронних носіїв і несанкціонованого використання інформації в електронній комерції, голосової пошти, системи відеоспостереження	Використовуються технології цифрових водяних знаків (ЦВЗ) і ідентифікаційних номерів (ІН)

Продовження таблиці 1.1

1	2	3
Подолання систем моніторингу та управління мережними ресурсами	За заявою авторів, ця програма була створена "для обходу національних міжмережевих екранів, що дає можливість безпечно обмінюватися будь-яким цифровим контентом через Інтернет"	Стегометоди, спрямовані на протидію промислового шпигунства, дозволяють протистояти контролю над інформацією в комп'ютерних мережах
Прихована анотація документів та оптимізація банків даних (інформації)	Використовується для прихованої анотації документів в медицині, картографії, мультимедійних банках даних, а також для пошуку в них необхідної інформації	Використовуються технології ЦВЗ та ІН
Маскування програмного забезпечення	Забезпечується багаторівневий санкціонований доступ до програмного забезпечення	У випадках, коли використання обмежене, воно може бути закамуфльовано під стандартні програми або приховано в медіафайли

Існує два напрямки методів цифрової стеганографії:

–перший спрямований на приховування інформації у часовій області мультимедійного об'єкта;

–другий заснований на приховування конфіденційної інформації в частотній області мультимедійного об'єкта.

В якості мультимедійного об'єкта можуть виступати: зображення, відео, аудіо, текстові або двійкові файли.

Класифікацію методів цифрової стеганографії подано на рис. 1.5.

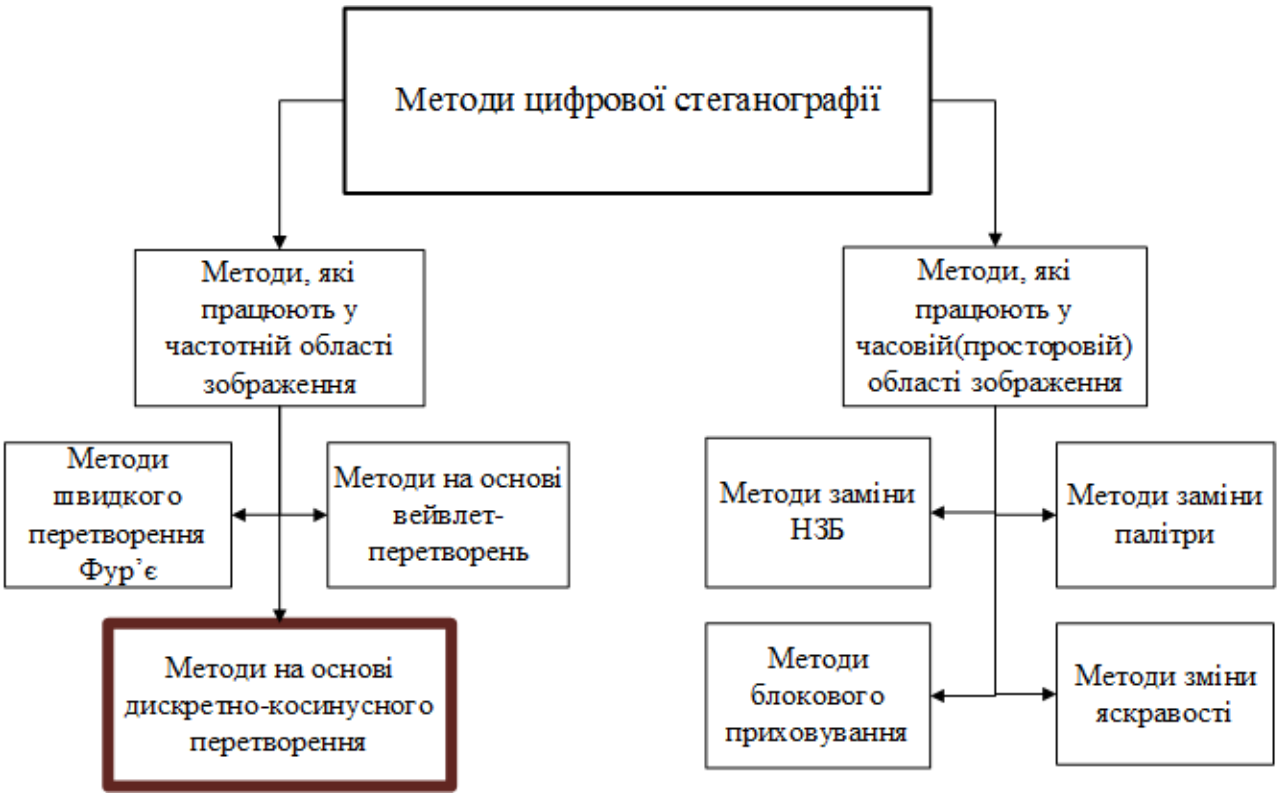


Рисунок 1.5 - Класифікація методів цифрової стеганографії

Методи першої категорії працюють безпосередньо з зображенням. Принцип вбудовування інформації у часовій області контейнера полягає в наступному: інформацію вбудовують в незначущі області зображення, щоб не змінити візуальне представлення зображення для зорової системи людини.

Проводять маніпуляції з найменш значущими бітами кольорових компонент зображення. Вони застосовні тільки до зображень, які не були підвернені стисненню, тому що при стисненні малозначима інформація просто відсікаються.

Найбільш поширеним методом цього класу є метод заміни найменшого значущого біта (НЗБ) бітом секретного повідомлення. Молодший значущий біт (НЗБ) зображення несе в собі менше всього інформації. Відомо, що людина зазвичай не здатна помітити зміну в цьому біті. Фактично, він є шумом. Тому його можна використати для вбудовування інформації.

Даний метод передбачає зміну найменш значущих біт колірних компонент зображення (кадру), щоб мінімізувати спотворення картинки в цілому [7]. Припустимо, використовується зображення у форматі RGB, у якому

відводиться по 1 байту на кожну колірну складову. Тоді зміна одного йди двох найменш значущих біт у кожної з компонент не матиме впливу на візуальне сприйняття картинки в цілому. Під зміною мається на увазі заміна вихідних біт, біти впроваджуваного повідомлення.

Однак невидимість інформації, впровадженої за допомогою цього способу може бути досить слабкою. Шум, упроваджений в ділянки зображення, з плавним переходом, може бути візуально помічений [15].

Розглянемо докладніше цей метод. Для прикладу візьмемо в якості контейнера картинку. Для початку звернімо увагу на структуру цього файлу. Файл умовно розділяємо на 4 складових: заголовок файлу, заголовок зображення, палітру і саме зображення. Нам важлива лише інформація, яку містить заголовок.

Перші два байти заголовка – це сигнатура, далі в подвійному слові записаний розмір файлу у байтах, наступні 4 байти зарезервовані і повинні містити нулі і, нарешті, у ще одному подвійному слові записано зсув від початку файлу, до власне байтів зображення.

Так як нам відомо як дістатися до зображення, то ми можемо працювати над даними, які необхідні для запису туди необхідної нам інформації. Будемо використовувати метод LSB.

Суть алгоритму – це заміна молодших бітів в байти, що відповідають за кодування кольору.

Розрахуємо максимальний обсяг інформації, який можна приховати за допомогою цього методу:

Зображення зберігається в трьох матрицях. Це масиви яскравостей червоного, зеленого та синього (RGB). В масивах зберігаються байти, це числа 0…255 – значення яскравостей кольорів. Так (0,0,0) – чорний колір, а (255, 255, 255) – білтй колір.

Наприклад, зображення розміром 100 х 100 містить 10000 пікселів. Існують три матриць, і таким чином, Фото має розмір 30000 байт. Ви можете

вставляти 30000 байт конфіденційної інформації, починаючи з 1 піксель TSE 3 байти 1 байт, але містить тільки 1 НЗБ.

Така заміна в загальному випадку не помітна для людського ока. Більш того, багато старі пристрої виведення, навіть не зможуть відобразити такі незначні зміни.

Для прикладу візьмемо зображення (рис. 1.6.):

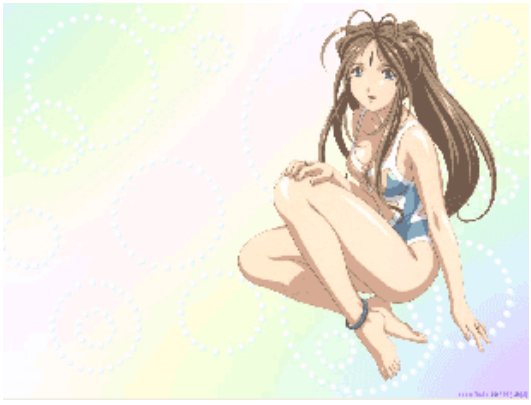


Рисунок 1.6 - Зображення у форматі BMP

Впроваджуємо в неї деяку кількість інформації за допомогою, наприклад, програми Stegograph. За допомогою дуже простої програми, що показує картинку побітно (тобто, тільки цікавлять нас біти потрібних колірних компонентів) дуже ясно видно впровадження даних (рис 1.7.). Більш того, можна легко уявити собі картину впровадження (які біти, які компоненти кольору), а при деяких додаткових зусиль і отримати приховану інформацію.

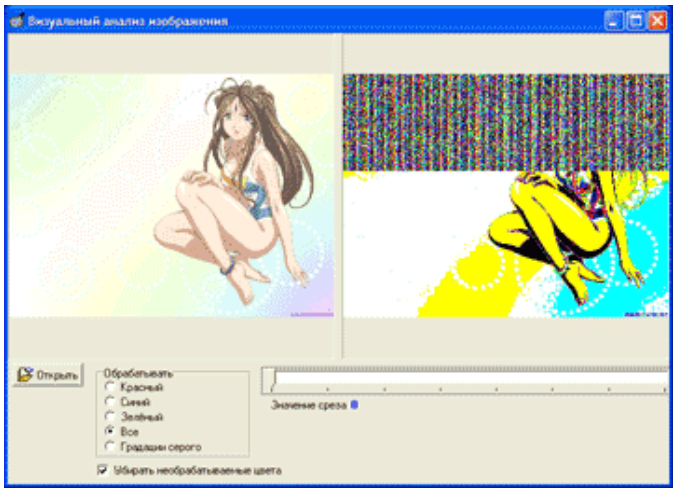


Рисунок 1.7 - Аналіз зображення у програмі Stegograph

Звичайно, для більшості спостерігачів досить і того, що візуально факт вбудовування конфіденційної інформації не можливо виявити, але слабкі місця свого захисту треба знати.

Аналізуючи рис.1.8 випливає такий результат: від кількості змінених біт залежить обсяг схованої інформації, тобто чим більше ми міняємо бітім, тим більше можемо сховати інформації, але це не вплине на вихідне зображення.

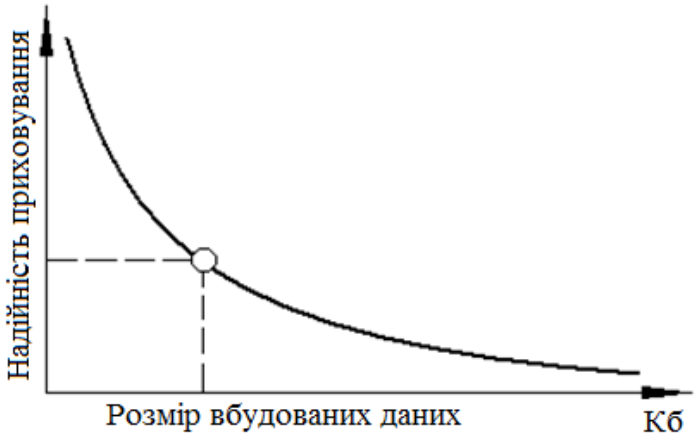


Рисунок 1.8 - Залежність надійності приховування інформації від обсягу повідомлення.

Отже, дана закономірність не дозволяє збільшувати ефективність стеганографічного методу шляхом збільшення обсягу вбудованої інформації. Але це має сенс, тільки якщо ми вбудовуємо інформацію, використовуючи тимчасову область.

Переваги:

– дозволяють приховувати у відносно невеликих файлах досить великі обсяги інформації;

– простота реалізації.

Недоліки:

– сильна чутливість до найменших спотворень контейнера.

Суть методів блочного приховування полягає в наступному: зображення розбивається на n блоків, які не перетинаються [17]. Для кожного з даних блоків вираховується біт парності.

Кожний блок призначений для приховування одного біта секретного повідомлення. Якщо, для прикладу, біт парності не рівний біту повідомлення, в такому випадку інвертуємо один з найменш значущих бітів блоку Однією з переваг даного методу є те, зміна одного з наймеш значущих бітів зображення, не буде візуально відчутною. Перевагою також є можливість вибору розміру блока, для зменшення наслідків вбудовування бітів секретного повідомлення.

Переваги:

– можливість модифікації найменш видимих бітів блоку, зміна яких не призведе до відчутних змін статистики контейнера;

–збільшення розміру блоку дозволить зменшити вплив наслідків вбудовування секретних даних в контейнер.

Недоліки:

–вразливість до спотворень стеганоконтейнера з вбудованим повідомленням

Методи заміни палітри полягають в тому, що використовується палітра кольорів зображення. Для приховування даних палітру з N кольорів визначають як перелік пар індексів, які відповідно визначають індекс і та його вектор кольоровості. Кожен піксель зображення позначається індексом в палітрі. Так як кольори в палітрі не завжди впорядковані, топослідовність зберігання кольорів в палітрі допомагає закодувати секретну інформацію. Загальна

кількість перестановок N-кольорової палітри дорівнює N!, чого цілком вистачає для приховування невеликого повідомлення.

Переваги:

– простота реалізації.

Недоліки:

– велика вразливість до атак, пов'язаних із заміною палітри.

Суть методів зміни яскравості можна пояснити наступним чином: зображення-контейнер ділиться на блоки пікселів. Після цього потрібно створити так звану маску, розмірність якої відповідає розмірності контейнера, а елементами маски є 0 і 1, розподілені псевдовипадковим чином. Кожен блок Б поділяється на два підмасива в залежності від вигляду маски, та характеризується середнім значенням яскравості - і. Вбудовування біта секретного повідомлення відбувається наступним чином:

$$S(x,y)=\begin{cases}1, при\ \lambda_1-\lambda_2>E\\0, при\ \lambda_1-\lambda_2<-E\end{cases}, \tag{1.1}$$

де Е – деяке значення порогу (необхідна різниця між зазначеними середніми значеннями яскравості).

У випадку, коли умова (2) не виконується, необхідно змінити значення яскравості пікселів одного з підмасивів відповідно до порогового значення. Для отримання бітів секретного повідомлення виконують обчислення відповідних середніх значень яскравості підмасивів - і. Обчислена різниця між даними значеннями дозволяє визначити значення прихованого біта:

$$b_i=\begin{cases}1, при\ \lambda_1*\lambda_2>0\\0, при\ \lambda_1*\lambda_2<0.,\\?, при\ \lambda_1*\lambda_2=0\end{cases} \tag{1.2}$$

Переваги:

– відносна стійкість до JPEG-компресії.

Недоліки:

–велике порогове значенні різниці між середніми значеннями яскравості блоків може спричинити доволі відчутне візуальне спотворення зображення-контейнера;

–обсяг повідомлення для вбудовування є відносно малим, оскільки для приховування одного біта необхідний цілий блок бітів.

У таких методів відсутня яка-небудь стійкість, але зате вони дозволяють вбудовувати великий обсяг інформації і у них досить проста реалізація.

У разі впровадження в частотній області модуляції піддаються амплітудні складові комплексного спектра зображення-контейнера. Для цього попередньо здійснюється обчислення амплітудної і фазової складових компонентів перетворення Фур'є.

Серед лінійних ортогональних перетворень було обрано найбільш популярне дискретне косинусне перетворення [1], його застосовують при стисненні зображень і відео в стандартах JPEG, MPEG. Метод стеганографічного приховування буде стійкий до наступної компресії зображення, тільки в тому випадку, якщо враховує особливості використовуваного методу компресії [2].

Пряме дискретне косинусне перетворення відповідно до алгоритму JPEG для блоку розміром 8×8 записується наступним чином:

$$\Phi(u,v) = \frac{1}{4}\zeta(u)\zeta(v)\sum_{x=0}^{7}\sum_{y=0}^{7} I(x,y) \mid \cos(\frac{\pi u(2y+1)}{16})\cos(\frac{\pi u(2x+1)}{16}) \qquad (1.3)$$

де x, y – просторові координати пікселів зображення;

υ,ν – координати в області перетворення,

I – блок вихідного зображення.

Нормувальні коефіцієнти записуються у вигляді:

$$\zeta(\varepsilon) = \begin{cases} \dfrac{1}{\sqrt{2}}, & \varepsilon = 0, \\ 1, \varepsilon > 0, \text{при u} \geq 0, \text{v} \leq 7 \end{cases} \qquad (1.4)$$

Для початку зображення розбивають на блоки, розміром 8×8 пікселів. Над кожним блоком обчислюється дискретне косинусне перетворення за формулою (3) враховуючи формулу (4). Результати, які вийшли записують в матриці розмірності 8×8 і позначають як Ф(u, v) з позиціями коефіцієнтів матриці u і v відповідно.

Перетворення відбувається таким чином - спочатку йдуть низькочастотні коефіцієнти, потім середньочастотні і високочастотні, як показано для наочності на малюнку

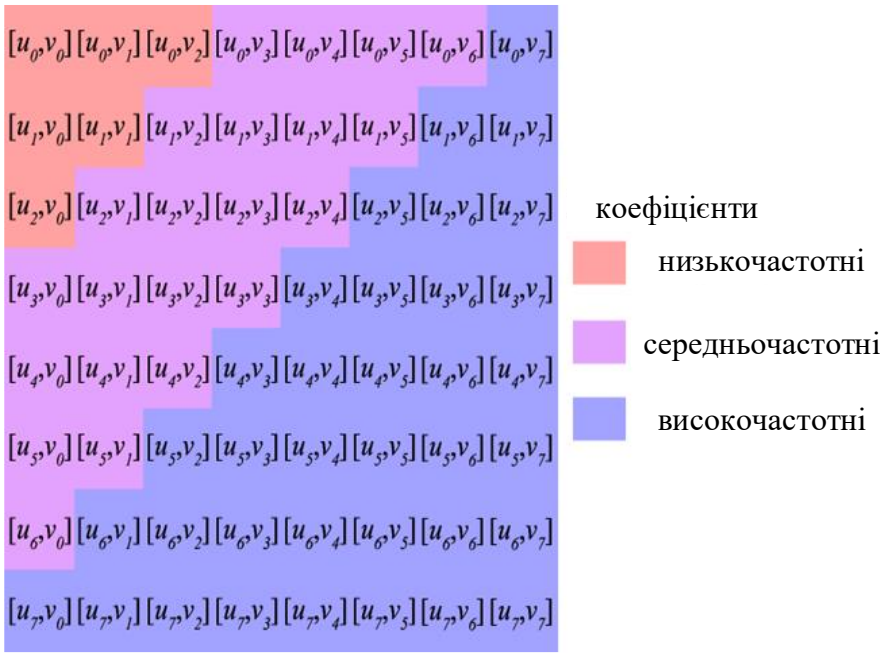


Рисунок 1.9 - Матриця ДКП

Підведемо підсумки та зробимо оцінку методів. Критерії оцінки методів вбудовування даних у зображення їх ступінь значущості за п'ятибальною шкалою (від 1 до 10) наведено у таблиці 1.2. Виконуватимемо це за допомогою методу компромісного рішення [14].

Бо цей метод допоможе визначити потрібний метод, тому що ми виберемо саме той метод, який відповідає нашим побажанням, оскільки нам наприклад потрібен, що б у методі було саме головне це стійкість до стиснення, значить він вибере саме найкращий метод, який його реалізує в кращому чином.

Переваги методу - завжди існує розв’язання, враховується не тільки рівень важливості параметрів, але й частка впливу кожного часткового параметру на загальне розв’язання.

Недоліки методу - значна величина інтегрального параметру (для певного варіанту) не гарантує його відповідності за всіма необхідними вимогами; низьке (неприйнятне) значення одного з параметрів може бути скомпенсовано (перекрито) високим значенням іншого (інших) значущого параметру.

Для зручного подання пронумеруємо методи:

1. Метод НЗБ
2. Метод блокового приховування
3. Метод зміни палітри
4. Метод заміни яскравості
5. Метод на основі ДКП
6. Метод швидкого перетворення Фур’є
7. Метод на основі вейвлет-перетворень

1. Для початку надамо оцінку важливості кожного критерія:

Критеріїв в нас 4, тому щоб визначити оцінку важливості, расставимо от 1 до 4 оцінки, де 1- найважливіший критерій.

2. Потім виставляємо бали шляхом віднімання від (n+1, де n-кількість критеріїв) у нашому випадку це число 5 усіх оцінок важливості:

B_i : 5-1, 5-2,5-3,5-4, отримавши бали складаємо їх, вийшла сума $\sum_{i=1}^{n} B_i = 10$.

Таблиця 1.2 - Значимість критеріїв оцінки методів

Критерій	Ступінь значущості	Бали
Обсяг інформації, який можна вбудувати	2	2
Стійкість до стиснення за алгоритмом JPEG	4	4
Візуальне спотворення	3	3
Простота реалізації	1	1

3. На наступному етапі рахуємо нормативну оцінку (1.5):

$$w_i = \frac{B_i}{\sum_{i=1}^{n} B_i}. \quad (1.5)$$

На останньому етапі скориставшись Microsoft Exel функцією СУМПРОИЗВ або попарно перемножуємо кожний критерій на нормативну оцінку и потім їх сумуємо і маємо числа - f(i). З них шукаємо максимум. У таблиці 1.3 показані результати методу компромісного рішення.

Таблиця 1.3 - Значимість критеріїв оцінки методів

Критерій	Методи (аналоги)									
	1	2	3	4	5	6	7	Важливість критерію	Бали	Wi
Обсяг інформації, який можна вбудувати	10	8	5	5	7	6	7	3	2	0,2
Стійкість до стиснення за алгоритмом JPEG	1	1	1	5	10	10	10	1	4	0,4
Візуальне спотворення	7	9	6	7	5	5	5	2	3	0,3
Простота реалізації	10	9	8	7	5	4	3	4	1	0,1
f(i)	5,5	5,6	4	5,8	7,4	7,1	7,2		10	

Методи, які використовують часову область для вбудовування інформації, явно поступаються методам, що використовують частотну область.

Стеганографія дозволяє не тільки успішно вирішувати основну задачу – таємно передавати інформацію, але і вирішувати цілий ряд інших актуальних проблем, в тому числі, завадостійкої автентифікації, захисту від несанкціонованого копіювання, моніторингу інформації в мережах зв'язку, пошуку інформації в графічних базах даних.

Проведений аналіз методів цифрової стеганографії показав, що всі існуючі на сьогоднішній час методи базуються в основному на надлишковості інформації, а також на невеликій чутливості людського ока в зміні характеристик зображення. Звичайно, найбільш ефективними є методи які

використовують частотну область для вбудовування конфіденційної інформації, бо вони більш стійкі до різних викривлень, в тому числі стиснення, вбудовування інформації відбувається на етапі перетворень вихідного зображення.

1.3 Вимоги до створення та класифікації стегосистем

Стегосистема – це сукупність засобів і методів, які вмкористовуються для формування схованого канала передачі даних.

Загальна схема стеганосистеми подана на рис. 1.10.

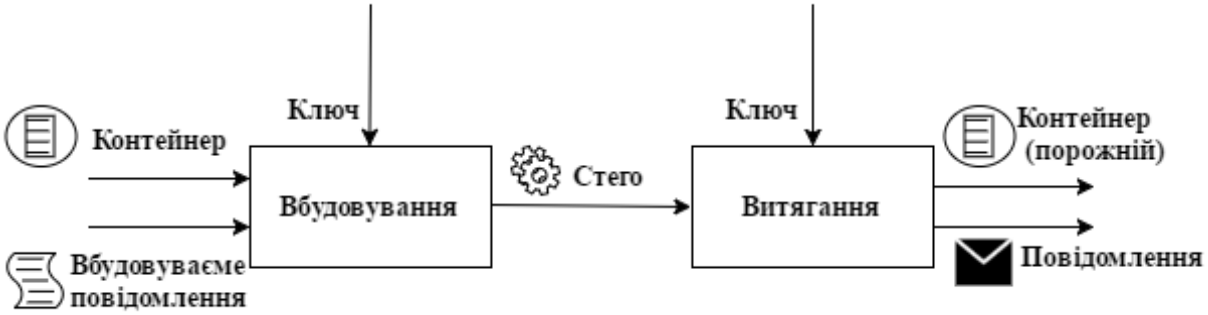


Рисунок 1.10 - Загальна схема стеганосистеми

У загальному випадку, в стеганосистему входить: порожній контейнер, який не містить конфіденційної інформації; заповнений контейнер, містить приховане повідомлення; прекодер, з допомогою якого виробляється початкова обробка приховуваної інформації; стеганокодер, призначений для упаковки повідомлення в контейнер, стеганографічний канал для передачі модифікованого контейнера; стеганодетектор, визначає наявність в контейнері прихованих даних; і стеганодекодер, необхідний для виділення секретного повідомлення з контейнера.

Приведемо класифікацію стегосистем на рис. 1.11:

Рисунок 1.11 - Класифікація стегосистем

За рівнем забезпечення секретності стегосистеми поділяються на теоретично стійкі системи, практично стійкі й нестійкі.

Для теоретично стійкої стегосистеми неможливо знайти метод виявлення прихованої інформації, оскільки вона може приховувати інформацію тільки в тих фрагментах контейнера, значення елементів яких не перевищує рівня шумів або помилок квантування.

Практично стійка стегосистема здійснює таким чином модифікацію фрагментів контейнера, що теоретично зміни можуть бути виявлені, але практично відомо, що на поточний час у зловмисника відсутні для цього ресурси і інструменти.

Нестійка стегосистема працює таким чином, що ресурси зловмисника дозволяють її виявити.

Кількість ключів в стегосистемі (бути один або кілька) визначає рівень її захисту. По аналогії з криптографією, можна виділити наступні типи стеганосистем:

– з секретним ключем, що використовується для приховування і отримання інформації, його необхідно передавати захищеним каналом, що є немалою проблемою;

– з відкритим ключем – для приховування та отримання повідомлення використовуються різні ключі, які пов’язані між собою, проте, обчислювально неможливо отримати один ключ з іншого, тому один із ключів (відкритий) може вільно передаватися незахищеним каналом.[4]

Стегосистему можна розглядати як систему зв'язку. Теорема Котельникова дає можливість як завгодно точного відновлення миттєвих значень сигналу з обмеженим спектром на основі з відлікових значень (вибірок), взятих через рівні проміжки часу [34].

Формулювання теореми: якщо функція x(t) має спектр, обмежений верхньою частотою FB, то x(t) повністю визначається послідовністю своїх значень у моменти часу, які віддалені один від одного на період $T \le 1/2F_в$.

Математичне формулювання теореми представлено формулою 1.5.

$$x(t) = \sum_{k=-\infty}^{\infty} x(kT) \frac{\sin \omega_в (t - kT)}{\omega_в (t - kT)} \qquad (1.5)$$

де $\omega_в = 2\pi F_в$,

$F_в$ - це верхня частота сигнала,

$T = \frac{1}{2F_в}$,

$x(kT)$ - значення функції $x(t)$ в моменти kT

Фізичний сенс теореми Котельникова (1.5) полягає в тому, що неперервна функція $x(t)$ з обмеженим спектром $F_в$ повністю може бути відновлена, якщо відомі її відліки, які взяті через даний інтервал $T \le 1/2F_в$. Ця теорема відіграє дуже велику роль у теорії зв'язку, т. до. дозволяє передачу аналогових сигналів замінити передачею дискретних та цифрових сигналів, що дозволяє суттєво підвищити ефективність систем зв'язку.

З практичної точки зору у всіх видах атак стеганоаналітика цікавить рішення трьох проблем: точне доведення факту наявності повідомлення у контейнері, визначення його довжини і знаходження сенсу прихованого

повідомлення. Досі друга з перелічених вище завдань залишається малодослідженою, хоча вона має безліч важливих аспектів. Суть даної задачі полягає у визначенні для кожної стеганографічної системи деякого порогу виявлення, що накладає обмеження на обсяг приховуваної інформації. При перевищенні такого порогу, тобто при приховуванні більшої кількості інформації, ніж це вважається можливим, система стає вразливою для стеганографічних атак.

При використанні методів приховування інформації в контейнерах стійкість стеганографичних систем визначається тим, якою мірою зберігається чи порушується природність їх сприйняття. Отже, важливими аспектами стеганографії є аналіз методів приховування інформації і виявлення найкращого, з допомогою якого можна оцінити якість приховування інформації в стеганоконтейнері.

Чим менше інформації ми впроваджуємо в контейнер, тим менше ймовірність виявлення прихованого повідомлення. При цьому контейнери різних форматів можуть приховувати різні обсяги інформації.

1.4 Класифікація контейнерів

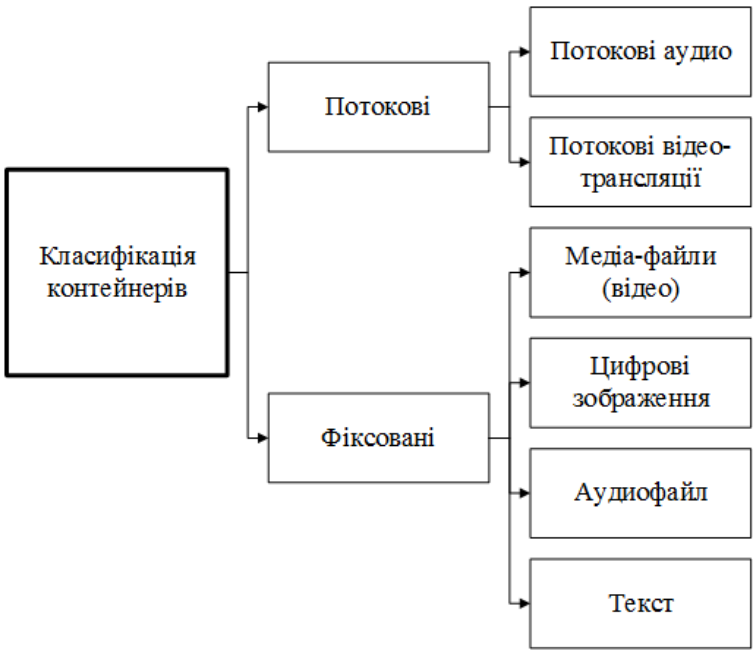


Рисунок 1.12 - Класифікація контейнерів

По протяжності контейнери розділяються на два типи: безперервні (потокові) і обмеженою (фіксованою) довжини.

У фіксованому контейнері вся описова інформація про відео-, аудіо - та інших даних зберігається в одному місці (початок або кінець файлу). Плюс - мінімальна надлишковість, мінус - якщо описова інформація втрачена, пошкоджена або ще не отримана, то відтворення або будь-яка інша обробка файлу буде неможливий або вкрай утруднений. Якщо інформація про файл зберігається на початку, то його можна почати програвати або обробляти з початку, не чекаючи повного завантаження файлу на комп'ютер (progressive download).

В потоковому контейнері описова інформація постійно присутня в потоці даних з певною періодичністю. Плюс - відтворення або обробка даних можлива практично з будь-якого моменту, мінус - надмірність описової інформації. Переваги фіксованого контейнера: його доступність та поширеність, бо на практиці найчастіше використовуються саме контейнери фіксованої довжини.

Таблиця 1.4 - Типи контейнерів

Характеристики	Тип контернера	
	Потоковий	Фіксований
Розмір контейнера	Розмір заздалегідь невідомий. В один контейнер великого розміру може бути вбудовано і кілька повідомлень.	Заздалегідь відомий розмір. Контейнери фіксованої довжини мають обмежений обсяг, і іноді вбудовується повідомлення може не помістится в файл-контейнер;
Інтервали між вбудованими бітами	Визначаються генератором псевдовипадковою послідовності з рівномірним розподілом інтервалів між відліками.	Рівномірно розподілені між найкоротшим і найбільш довгим заданими відстанями, в той час як справжній випадковий шум буде мати експоненційний розподіл довжин інтервалу.

Представниками фіксованих контейнерів є текст, зображення, медіафайл. Найбільш поширеними типами контейнерів комп'ютерної стеганографії на

даний момент є зображення та аудіодані, представлені в цифровій формі, і відео.

Багато сучасних систем комп'ютерної стеганографії використовує растрові графічні зображення різних форматів як контейнери стегосистем. Але вибір формату зображення не можна обмежувати лише можливістю розробки стійкої до атак стеганосистеми. Серед графічних форматів зображень, необхідно обирати такі, які широко використовуються на практиці. Передача нетипових форматів може сама по собі викликати підозри.

Формат JPEG є, мабуть, одним з найбільш популярних на сьогодні. Звичайно ж, є й інші широко розповсюджені графічні формати, такі як BMP, TIFF, PNG, PCX, TGA, PGM.

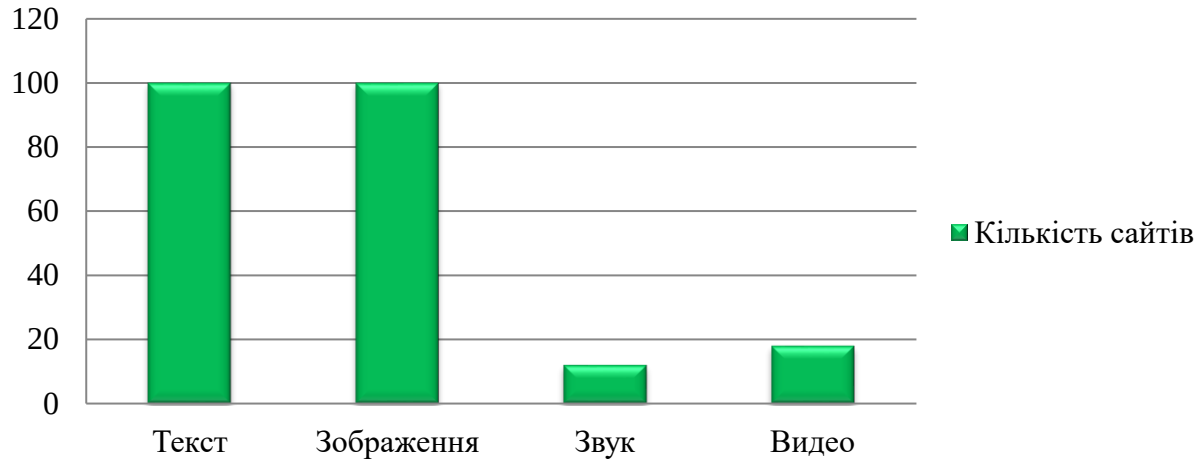
Вбудовування у контейнера-аудіофайли зумовлено тим, що особливості слухового апарату людини дозволяють вдало використовувати аудіосереду з метою стеганографічної захисту конфіденційної інформації. Але цього типу контейнерів в даний час приділяється набагато менше уваги.

Найбільш складнішим вважають приховування конфіденційної інформацію у контейнер-текст. Для приховування конфіденційних повідомлень у тексті (так звана лінгвістична стеганографія) використовується або звичайна надмірність писемного мовлення, або ж формати представлення тексту. У той час як у більшості випадків існує можливість внести непомітні оку і невідчутні на слух модифікації в зображення і звук, навіть додаткова буква або знак пунктуації в тексті можуть бути легко розпізнані випадковим читачем. Приховування даних у тексті вимагає пошуку таких модифікацій, які були б непомітними переважній більшості читачів.

Також була набрана статистика по використанню можливих контейнерів в сотні найбільш відвідуваних веб-сайтів за версією Top100-UA (зведений рейтинг найпопулярніших сайтів, розраховується за даними найбільших систем інтернет-статистики HotLog, LiveInternet, Rambler Top100, Openstat [33].

З'ясувалося, що кожен сайт використовує зображення і текст на головній сторінці, в той час як звукові і відео файли використовуються тільки на 12 і 18

сайтах відповідно. На рисунку 1.13. представлений графік використання контейнерів.



Рисисунок 1.13 - Графік використання контейнерів на першій сторінці сайту

Можна зробити висновок про те, що один з найбільш активно використовуваних і досліджуваних видів контейнерів – це цифрові зображення. Такі контейнери мають ряд переваг, таких як заздалегідь відомий відносно великий розмір цифрового представлення зображення, наявність у більшості областей зображень з шумовий структурою, а також слабка чутливість людського зору до незначних змін яскравості і контрасту зображення. Все це дозволяє впроваджувати в зображення досить великий обсяг прихованих даних. Технологія використання зображень як контейнер надає набагато ширші можливості, ніж текстові документи. При використанні графічних форматів з'являється можливість приховування не лише текстових повідомлень, а й інших зображень та файлів. Єдиною умовою є те, що обсяг захованого малюнка не повинен перевищувати розмір зображення-сховища.

Значна частина досліджень в області стеганографії присвячена запровадження конфіденційних повідомлень і цифрових водяних знаків у файли зображень. Це пов'язано з практичною необхідністю захисту авторських прав, добре розробленими методами обробки цифрових даних, слабкою

чутливістю людського ока до незначних змін яскравості, контрастності, зміни кольорів зображення.

1.5 Висновки до розділу 1

Методи цифрової стеганографії для приховування та передачі конфіденційної інформації можуть використовуватись для забезпечення конфіденційної інформації, захисту авторського права, подолання систем моніторингу та управління мережними ресурсами, прихованої анотації документів та оптимізація банків даних та маскування програмного забезпечення.

Проведений аналіз класифікації методів стеганографії показав, що в якості контейнера використовуються зображення, аудіо файли та текстові документи. І що інформацію краще приховувати за допомогою методів, які використовують частотну область для вбудовування конфіденційної інформації, бо вони більш стійкі до різноманітних маніпуляцій з контейнером, вбудовування інформації відбувається на етапі перетворень вихідного зображення.

Проаналізувавши стеганографічні системи можна зазначити, що більшість методів використовують контейнери без використання стиснення даних, саме цьому вони незахищені від поширеніших атак.

2 ДОСЛІДЖЕННЯ МЕТОДУ ЦИФРОВОЇ СТЕГАНОГРАФІЇ НА ОСНОВІ ДИСКРЕТНО КОСИНУСНОГО ПЕРЕТВОРЕННЯ

2.1 Математичний опис дискретно косинусного перетворення

Досить складний, але цікавий метод вбудовування повідомлень. Він заснований на зміні структури чи змісту формату стегозакону, але так, щоб для програм перегляду файлів, написаних за стандартними рекомендаціями, подібні зміни були б байдужі

ДКП являє собою різновид перетворення Фур'є і має інверсне перетворення. Зображення в ДКП можна уявити як сукупність просторових хвиль, для яких осі X і Y відповідають осям зображення, а вісь Z призначення для відповідного кольору пікселя зображення. Він є основою міжнародного стандарту, який використовується в алгоритмі стиснення зображень з втратами JPEG.

За допомогою ДКП алгоритм стиснення JPEG здійснює перехід від подання зображення в просторовому вигляді до її спектральної інтерпретації.

В результаті ДКП оригінальне зображення, що представлене в просторі атрицею пікселів транформується в матрицю частотних коефіцієнтів. У частотному представлення високочастотні коефіцієнти концентруються в лівому верхньому кутку, а низькочастотні – у нижньому(див. рис.2.1).

	1	2	3	4	5	6	7	8
1	1603	203	11	45	-30	-14	-14	-7
2	108	-93	10	49	27	6	8	2
3	-42	-20	-6	16	17	9	3	2
4	56	69	7	-25	-10	-5	-2	-2
5	-33	-21	17	8	3	-4	-5	-3
6	-16	-14	8	2	-4	-2	1	1
7	0	-5	-6	-1	2	3	0	1
8	9	5	-6	-9	0	3	3	1

- Низькочастотні компоненти
- середньочастотні компоненти
- високочастотні компоненти

Рисунок 2.1 - Матриця коефіцієнтів ДКП

Низькочастотні коефіцієнти відповідають за інтенсивність кольору, а тому вплив на них призведе до сильного спотворення даних після застосування оберненого перетворення. Натомість шумивідповідають високим частотам, а тому за звичай, їх можна відкринути. На рисунку 2.2 подано частотний спектр окремого фрагменту зображення:

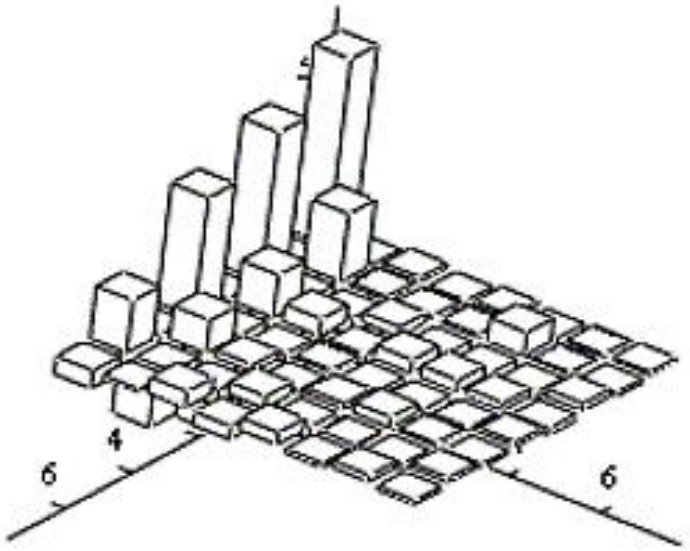


Рисунок 2.2 - Спектр ДКП окремого фрагмента зображення

ДКП та звоотнє ДКП представлено нижче формулами (2.1 та 2.2):

$$F[u,v] = a(u)a(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}F_{DCT}[x,y]\cos\frac{(2x+1)u\pi}{2N}\cos\frac{(2x+1)v\pi}{2N}, \qquad (2.1)$$

$$F_{DCT}[u,v] = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1}a(u)a(v)F[x,y]\cos\frac{(2x+1)u\pi}{2N}\cos\frac{(2x+1)v\pi}{2N}, \qquad (2.2)$$

де F_{DCT} – іcходна матриця,

F – матриця коеффіцієнтів ДКП,

N – розмір матриць F и F_{DCT},

$$a(k) = \begin{cases} \sqrt{\frac{1}{N}}, якщо\ k = 0 \\ \sqrt{\frac{2}{N}}, якщо\ k > 0 \end{cases}, \quad (2.3)$$

де k = u, або k = v;

u, v, x, y $\in$ [0, N)

Для обчислення дискретного косинусного перетворення розробники JPEG запропонували використовувати блоки розміром 8x8, на які розбивається зображення.

Збільшення розмірів блоку дискретного косинусного перетворення, дозволить ефективніше проводити стиснення.

Щоб уникнути два вкладених цикли для обчислення косинусного перетворення для кожного елемента матриці дискретного косинусного перетворення, можна використати підхід через перемноження матриць.

Тоід формула дискретного косинусного перетворення може бути записана в наступному вигляді:

$$ДКП = КП * Точки * КПт, \quad (2.4)$$

де ДКП - дискретне косинусне перетворення;

КП - матриця косинусного перетворення розміром NxN (елементи знаходимо за формулою):

$$C(i, j) = \begin{bmatrix} \frac{1}{\sqrt{N}}, i = 0 \\ \sqrt{\frac{2}{N}} * \cos\left(\frac{(2j+1)i\pi}{2N}\right), i > 0 \end{bmatrix}, \quad (2.5)$$

де точки - матриця розміром NxN, що складається з пікселів зображення;

КПт - транспонована матриця КП.

2.2 Алгоритм стиснення. Структурна схема алгоритму JPEG

В даній роботі реалізовується стеганографічний алгоритм на основі JPEG. JPEG – це метод стиснення зображень з втратами. Він прекрасно стискає зображення з безперервними тонами, у яких близькі пікселі зазвичай мають схожі кольору, але не дуже добре справляється з дворівневими чорно-білими образами.

Настільки мала поширеність цього формату при передачі зображень по мережі пов'язано це з тим, що в зображеннях, взагалі кажучи, багато надмірності і тому вони добре стискуються, особливо алгоритмами архівації з втратами. Найбільш поширений в даний момент формат JPEG (Joint Photographic Experts Group). Тут вже не вийде такий фокус, так як цей формат набагато більш складний, ніж bmp. У ньому застосовуються спеціальні алгоритми перетворення колірних просторів, архівації, квантування.

Структурна схема алгоритму подана на рис. 2.3.

Рисунок 2.3 - Структурна схема алгоритму

Для початку коротко розглянемо алгоритм JPEG. Кодек 8-бітних RGB-зображень можна описати наступними пунктами (на вхід подається масив компонент зображення)[18]. Ми будемо працювати не з усім зображенням відразу, а з його частинами – шматочками 8x8 пікселів.

Тобто для початку розбиваємо початкове зображення на такі під-зображення, як зображено на малюнку

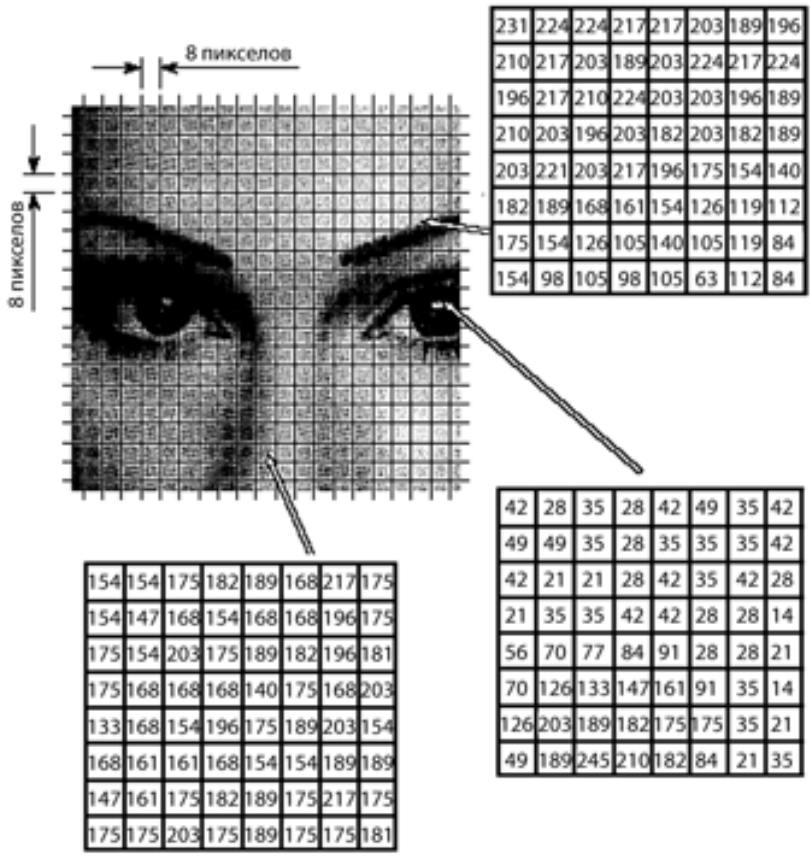


Рисунок 2.4 - Зображення розбите на фрагменти та три групи 8x8, показані у збільшеному вигляді, показують значення окремих пікселів

2.2.1 Трансформація колірного простору

Колірний простір RGB включає в себе три колірних каналу: червоний (red), зелений (green), синій (blue). Колір утворюється в результаті злиття трьох компонент. З допомогою різних комбінацій цих трьох каналів можна отримати абсолютно будь-який колір . Кількість кольорів залежить від кількості біт, що відводиться для зберігання чисельного значення компоненти кольору. Найбільш поширений формат RGB24, в якому на кожну колірну складову відводиться по вісім біт, відповідно, числове значення компоненти лежить в інтервалі [0; 255].

Колірний простір YCbCr складається з трьох компонент: компоненти яскравості Y і двох компонент кольоровості Cb і Cr. Такий поділ обумовлено тим, що людський зір має більшу чутливість до яскравості, ніж до кольору предмета, як було доведено в попередньому розділі. У зв'язку з цим компоненти

кольоровості Cb і Cr можна зберігати з меншою роздільною здатністю, що дозволяє зменшити обсяг збережених або переданих даних. Тому дане колірний простір широко використовується в цифрових зображеннях.

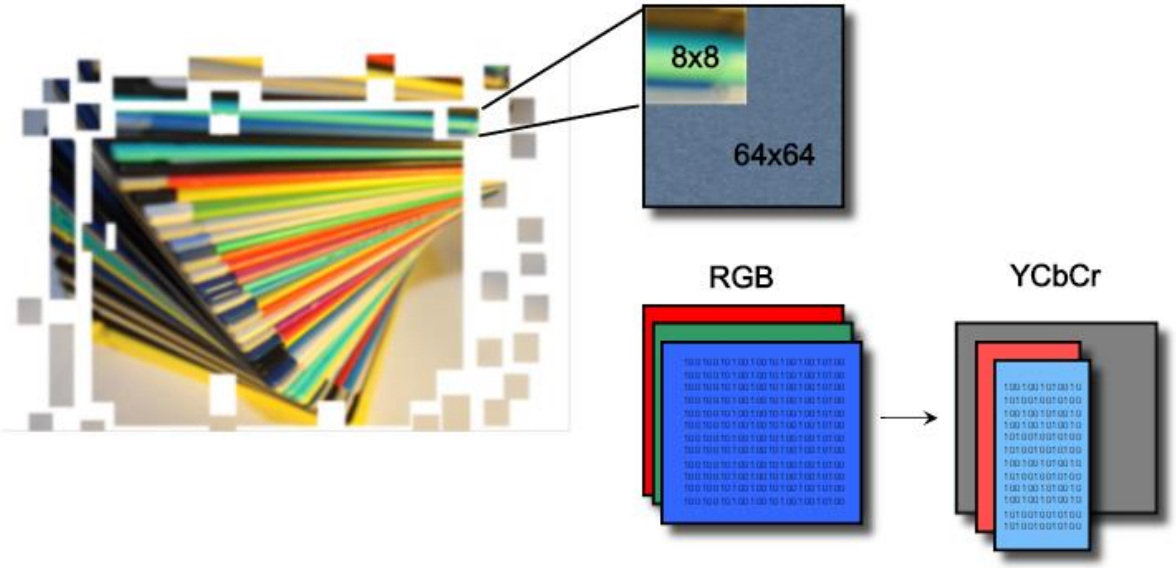


Рисунок 2.5 - Трансформація колірного простору

Око чутливе до малих змін яскравості пікселів, але не кольоровості. Це означає, що можна видалити значну частку інформації, пов’язану з компонентами кольоровсті, для досягнення високого стиснення без помітного візуального погіршення якості зображення. Без перетворення простору кольорів з компонентів RGB неможливо досягнути сильного стиснення.

Колірний простір RGB легко можна перетворити в YCbCr як і навпаки, якщо ваше зображення представлене у форматі JPEG, для цього потрібно буде скористатися виведеними формулами:

У формулі 2.6 компоненти простору RGB і простору YCbCr лежать в інтервалі [0;255].

$$\begin{cases} Y = 0.299R + 0.597G + 0.114B \\ C_b = 128 - 0.1687R - 0.3313G + 0.5B, \\ C_r = 128 + 0.5R - 0.4187G - 0.0813B \end{cases} \quad (2.6)$$

І зворотне перетворення колірного простору YCbCr в простір RGB можна виконати за допомогою формули , яка представлена нижче:

$$\begin{cases} R = Y + 1.402(C_r - 128) \\ G = Y - 0.34414(C_b - 128) - 0.71414(C_r - 128), \\ B = Y + 1.772(C_b - 128) \end{cases} \quad (2.7)$$

Нова величина Y названа яскравістю. Це – величина, використовувана монохромними моніторами, щоб представити колір RGB. Фізіологічно, передає інтенсивність кольору RGB, сприйнятого оком. Видно, що формула Y схожа на середньозважене значення з різною вагою для кожного спектрального компонента: око найбільш чутливе до зеленого кольору (G), потім червоний (R) компонент і в останню чергу – синій (B).

Величини Cb, Cr названі колірними величинами і представляють 2 координати в системі, яка вимірює відтінок і насичення кольору ([Наближено] ці величини вказують кількість синього і червоного в цьому кольорі). Ці 2 координати коротко названі кольоро-різницею.

Око, особливо сітківка, має як візуальні аналізатори два типи комірок: клітинки для нічного бачення, сприймають лише відтінки сірого (від яскраво-білого до темно-чорного) і осередку денного бачення, які сприймають колір. Перші осередки (їх називають паличками), виявляють рівень яскравості, подібний величиною Y. Інші клітинки(їх називають колбочками), відповідальні за сприйняття колірного відтінку, - визначають величину, пов'язану з кольоро-різницею. Вони відповідно бувають 3-х видів – сприймають краще червоний, зелений і синій кольори.Пример преобразования (ICT — Irreversible Color Transform) представлений на рисунку 2.6.

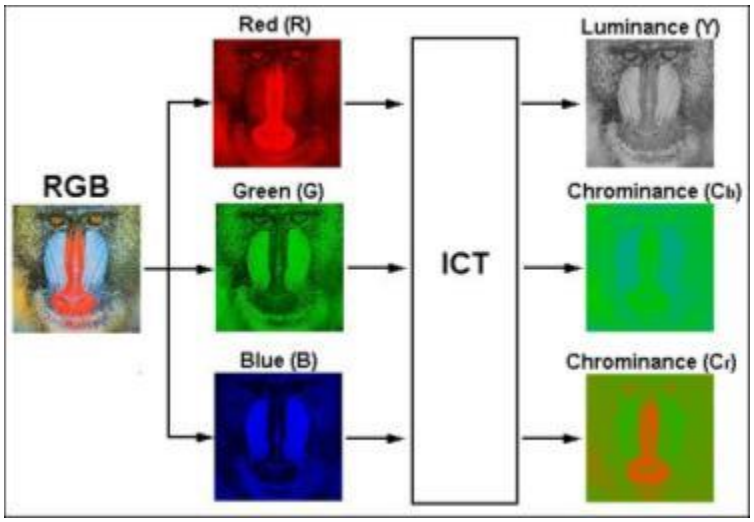


Рисунок 2.6 – Приклад роботи ICT перетворення

2.2.2 Дискретизація

Крім усього іншого, очей більш чутливий до яскравості світла, ніж до відтінку. Тому розумно брати значення яскравості для кожного пікселя. А значення кольорорізності – наприклад середнє блоку 2x2. Тобто на кожні 4 пікселя одне. Зрозуміло, це необов'язково, але майже завжди застосовується, так як веде до незначних втрат якості з точки зору сприйняття картини оком людини.

2.2.3 Зміщення за рівнем

Всі 8-бітові величини без знака (Y,Cb,Cr) в зображенні - "зміщені за рівнем": вони перетворюються в 8-бітове знакова подання відніманням 128 з їх величини.

Продемонструємо на прикладі. Нехай у нас є така матриця рис. 2.7, що описує одну з компонент Y, Cb або Cr.

$$\begin{bmatrix} 52 & 55 & 61 & 66 & 70 & 61 & 64 & 73 \\ 63 & 59 & 55 & 90 & 109 & 85 & 69 & 72 \\ 62 & 59 & 68 & 113 & 144 & 104 & 66 & 73 \\ 63 & 58 & 71 & 122 & 154 & 106 & 70 & 69 \\ 67 & 61 & 68 & 104 & 126 & 88 & 68 & 70 \\ 79 & 65 & 60 & 70 & 77 & 68 & 58 & 75 \\ 85 & 71 & 64 & 59 & 55 & 61 & 65 & 83 \\ 87 & 79 & 69 & 68 & 65 & 76 & 78 & 94 \end{bmatrix}$$

Рисунок 2.7 - Матриця описує одну з компонент Y, Cb або Cr

Після зсуву рівня на 128 відповідно:

$$\begin{bmatrix} -76 & -73 & -67 & -62 & -58 & -67 & -64 & -55 \\ -65 & -69 & -73 & -38 & -19 & -43 & -59 & -56 \\ -66 & -69 & -60 & -15 & 16 & -24 & -62 & -55 \\ -65 & -70 & -57 & -6 & -26 & -22 & -58 & -59 \\ -61 & -67 & -60 & -24 & -2 & -40 & -60 & -58 \\ -49 & -63 & -68 & -58 & -51 & -60 & -70 & -53 \\ -43 & -57 & -64 & -69 & -73 & -67 & -63 & -45 \\ -41 & -49 & -59 & -60 & -63 & -52 & -50 & -34 \end{bmatrix}$$

Рисунок 2.8 - Матриця описує одну з компонент Y, Cb або Cr після зсуву

2.2.3 Дискретно-косинусне перетворення (DCT)

Мета DCT-трансформації в тому, що замість обробки вихідних зображень, Ви працюєте з простором частот зміни яскравості і відтінку. Ці частоти дуже пов'язані з рівнем деталізації зображення. Високі частоти відповідають високому рівню деталізації. DCT-трансформація дуже схожа на 2-мірне перетворення Фур'є, яке отримує з тимчасового інтервалу (вихідний блок 8x8) частотний інтервал (нові коефіцієнти 8x8=64, які представляють амплітуди проаналізованого частотного простору).

Після цього перетворення ми отримаємо іншу матрицю, і в ній вже елементи будуть розташовані так, що найбільші за модулем скопятся в лівому

верхньому кутку – вони будуть нести в собі велику частину інформації – низькі частоти. А по мірі просування до правого нижнього – важливість елементів буде зменшуватися – високі частоти.

$$\begin{bmatrix} -415 & -30 & -61 & 27 & 56 & -20 & -2 & 0 \\ 4 & -22 & -61 & 10 & 13 & -7 & -9 & 5 \\ -47 & 7 & 77 & -25 & -29 & 10 & 5 & -6 \\ -49 & 12 & 34 & -15 & -10 & 6 & 2 & 2 \\ 12 & -7 & -13 & -4 & -2 & 2 & -3 & 3 \\ -8 & 3 & 2 & -6 & -2 & 1 & 4 & 2 \\ -1 & 0 & 0 & -2 & -1 & -3 & 4 & -1 \\ 0 & 0 & -1 & -4 & -1 & 0 & 1 & 2 \end{bmatrix}$$

Рисунок 2.9 - Матриця після DCT

2.2.4 Квантування

Саме на етапі квантування відбуваються втрати якості зображення, ціною яких і досягається стиснення. За визначеною заздалегідь матриці квантування відбувається розподіл елементів нашої матриці відповідно на елементи матриці квантування. Вона має наступний вигляд:

$$\begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

Рисунок 2.10 - Матриця на етапі перетворення

Ця матриця квантування спирається на "психовизуальный поріг". Зазвичай присутня одна таблиця для Y, та інші для відтінку Cb і Cr. Тут відбувається видалення високих частот, ми це робимо тому, що око більш

чутливий до низьких частот. Це відбувається при поділі тих елементів матриці, що знаходяться ближче до правого нижнього кута (вони відповідають за високі частоти) на великі, а тих, що в лівому верхньому кутку - на менші значення. Більше величини в таблиці квантування - більші втрати (згодом візуальні втрати) введені цим процесом, і менше – краще візуальне якість.

У результаті цієї операції в правому нижньому кутку накопичиться багато нулів, як зображено на рисунку.

$$\begin{bmatrix} -26 & -3 & -6 & 2 & 2 & -1 & 0 & 0 \\ 0 & -2 & -4 & 1 & 1 & 0 & 0 & 0 \\ -3 & 1 & 5 & -1 & -1 & 0 & 0 & 0 \\ -4 & 1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Рисунок 2.11 - Результат ділення на матрицю квантування

Далі примінемо до матриці зигзаг-сканування :

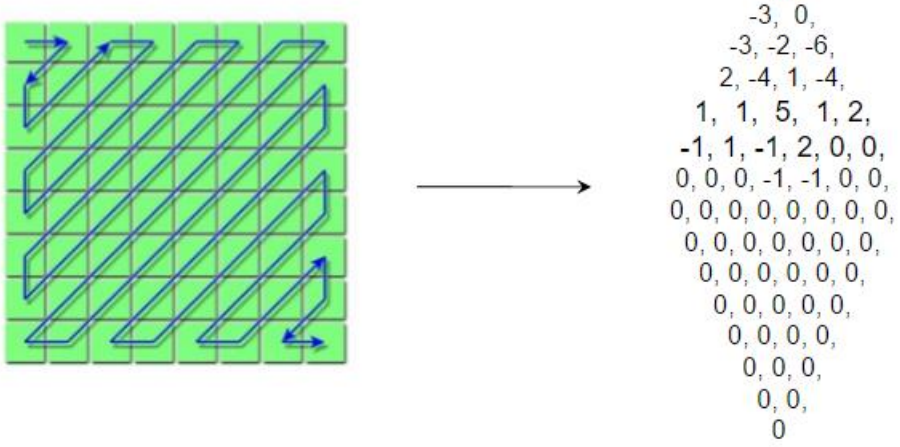


Рисунок 2.12 - Зигзаг-сканування

Після того, як ми пройшли по зигзаг матрицю 8x8, ми маємо тепер вектор з 64 коефіцієнтами. Сенс цього зигзагоподібного вектора – в тому, що ми

переглядаємо коефіцієнти в порядку підвищення просторових частот. Так ми одержуємо вектор, відсортований критеріями просторової частоти.

2.2.5 RLE – стиснення

Останнім етапом є кодування. Округлена матриця коефіцієнтів, отримана на етапі квантування, має певну кількість нульових елементів. Таким чином, елементи матриці записуються в ланцюжок. Отриманий вектор згортається за допомогою алгоритму групового кодування (RLE – Run Length Encoding). Кожен ненульовий елемент вектора представляється у вигляді пари чисел, перше з яких дорівнює кількості нулів перед цим числом, а друге – значенням цього елемента вектора. Потім отримані пари чисел кодуються за допомогою алгоритму Хаффмана з фіксованою таблицею. Принцип цього алгоритма заключається в присвоєнні часто використовуваних символах меншого числа бітів, а ті що рідше зустрічаються в символах — більшої кількості бітів.

2.3 Етапи алгоритму вбудовування інформації у стегоконтейнер

Розглянемо загальний принцип вбудовування даних. Кожний контейнер можна представити як бітову послідовність. Для початку необхідно визначити, які біти контейнера можна змінювати без внесення помітних спотворень.

Ці біти замінюються бітами конфіденційної інформації у відповідності до ключа.

Так як більшість зображень, є зображеннями у форматі JPG, тому буде доцільним, щоб метод занесення інформації в зображення був стійкий до JPEG-компресії. При розробці стегоалгоритму доречно використовувати алгоритм стиснення JPEG.

Заснований даний алгоритм на дискретному косинусном перетворення (ДКП), що застосовується до матриці непересічних блоків зображення, розміром 8x8 пікселів. ДКП розкладає ці блоки по амплитудам деяких частот. У результаті виходить матриця, в якій більшість коефіцієнтів, як правило, близькі

до нуля, які можна представити у грубій числовій формі, тобто у квантованном вигляді без істотної втрати якості відновлення.

Алгоритм вбудовування інформації в контейнер-зображення

Крок 1. Переклад зображення-контейнера з колірної моделі RGB модель YCbCr.

Крок 2. Розбиття матриці яскравості Y колірної моделі YCbCr на блоки пікселів як наведено на рисунку 2.11.

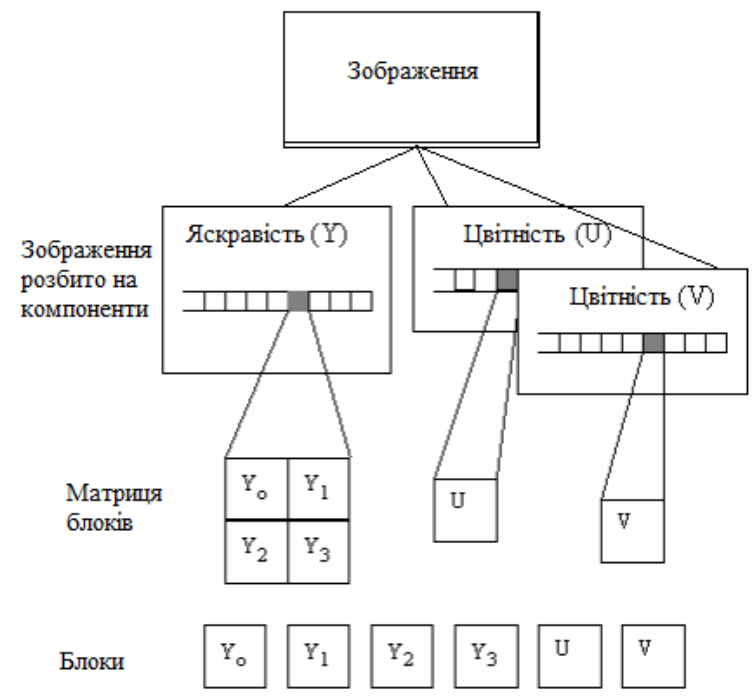


Рисунок 2.13 - Розбиття матриці яскравості Y колірної моделі YCbCr на блоки пікселів

Крок 3. Виконання ДКП над кожним блоком.

Крок 4. Вибір у кожному блоці двох пар коефіцієнтів ДКП з низькочастотної або середньочастотної області $w_1 = \Omega_b(u_1, v_1)$, $w_2 = \Omega_b(u_2, v_2)$, $w_3 = \Omega_b(u_3, v_3)$, $w_4 = \Omega_b(u_4, v_4)$,

де - Ω матриця коефіцієнтів ДКП блоку;

b – номер блоку;

u_1, v_1, u_2, v_2, u_3, v_3, u_4, v_4 - координати вибраних коефіцієнтів ДКП в блоці.

Крок 5. У кожен блок відбувається вбудовування двох бітів секретних даних і , де і – номер вбудованого біта повідомлення визначається за формулою. Вбудовування інформації здійснюється наступним чином: для передачі біта 0 домагаються того, щоб різниця абсолютних значень коефіцієнтів була б більшою за деяку позитивну величину, а для передачі біта 1 ця різниця робиться меншою за деяку негативну величину:

$$\begin{aligned} &\left| c_b\left(j_{i,j}, k_{i,1}\right)\right| - \left| c_b\left(j_{i,2}, k_{i,2}\right)\right| > \varepsilon,\ s_i = 0, \\ &\left| c_b\left(j_{i,j}, k_{i,1}\right)\right| - \left| c_b\left(j_{i,2}, k_{i,2}\right)\right| < -\varepsilon, s_i = 1.' \end{aligned} \tag{2.8}$$

Таким чином, початкове зображення спотворюється за рахунок внесення змін до коефіцієнти ДКП.

Для читання повідомлення у декодері виконується та ж процедура вибору коефіцієнтів, і рішення про переданому бите приймається згідно з правилом:

$$\begin{aligned} &s_i = 0, \quad \text{якщо} \left| c_b\left(j_{i,j}, k_{i,1}\right)\right| > \left| c_b\left(j_{i,2}, k_{i,2}\right)\right|, \\ &s_i = 1, \quad \text{якщо} \left| c_b\left(j_{i,j}, k_{i,1}\right)\right| < \left| c_b\left(j_{i,2}, k_{i,2}\right)\right|. \end{aligned}' \tag{2.9}$$

Крок 6. Над кожним блоком здійснюється зворотне ДКП.

Крок 7. Переклад зображення-контейнера з колірної моделі YCbCr в модель RGB.

2.4 Висновки до розділу 2

Стеганоалгоритм, що базується на дискретному косинусном перетворенні може досягати ступінь стиснення від 5 до 100 і більше разів. Слід зазначити, що при стисненні до 15 і зміни зображення фактично не помітні для людського ока.

Даний алгоритм і формат є найбільш поширеними для передачі і зберігання повнокольорових зображень.

3 ДОСЛІДЖЕННЯ СТІЙКОСТІ АЛГОРИТМУ ДО ПОШИРЕНИХ АТАК НА СТЕГАНОСИСТЕМИ

3.1 Класифікація атак на стеганосистеми

Можна вважати стегосистему зламаною, якщо виконан хоча б один пункт з нижченаведених:

– виявлений факт присутності конфіденційної інформації;

– приховане повідомлення вдалося витягти;

– секретна інформація видозмінена (модифікована);

– вдалося зробити заборону на виконання будь якої пересилки інформації, в тому числі прихованої.

Перші два етапи відносяться до пасивних атак на стегасистему, а останні – до активних (або зловмисним) атакам.

Класифікація атак на стегосистеми подана на рис 3.1:

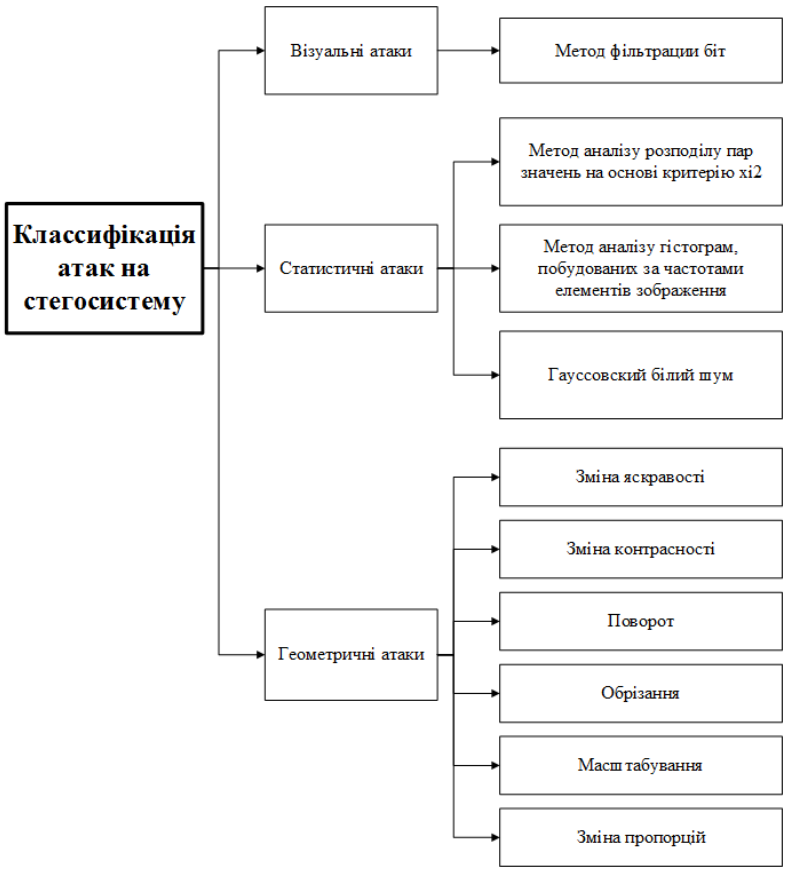


Рисунок 3.1 - Види атак на стегаграфічну систему

3.2 Візуальна атака на стегасистеми.

Суть в тому, що іноді, неможливо побачити факт вбудованого повідомлення неозброєним оком не скориставшись математичними алгоритмами.

Розглядати будемо тільки на окремі значущі біти:

Зробимо порівняльний аналіз алгоритму НЗБ і алгоритму на основі ДКП.

Беремо два зображення: одне у форматі BMP , іншу JPEG. Вмонтуємо в них інформацію за допомогою відповідних алгоритмів.

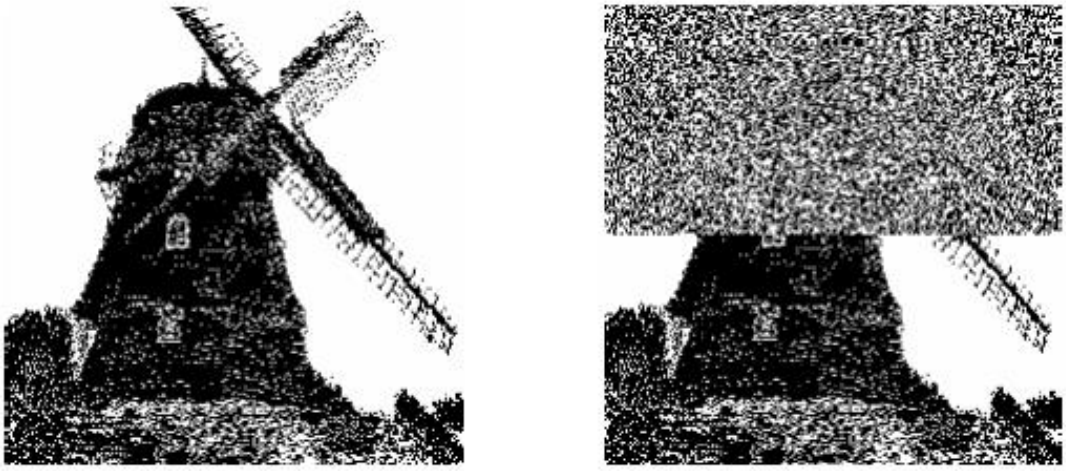


Рисунок 3.2 - Зліва початкове зображення .BMP не піддавалася ніяким змінам, праворуч – 50% контейнера містить вбудовану інформацію

Так як біти секретного зображення встраиваються в певну частину контейнера, тому досить легко побачити факт впровадження конфіденційної інформації за допомогою поширеною візуальної атаки.

Тепер проведемо такий експеримент для зображення .JPEG

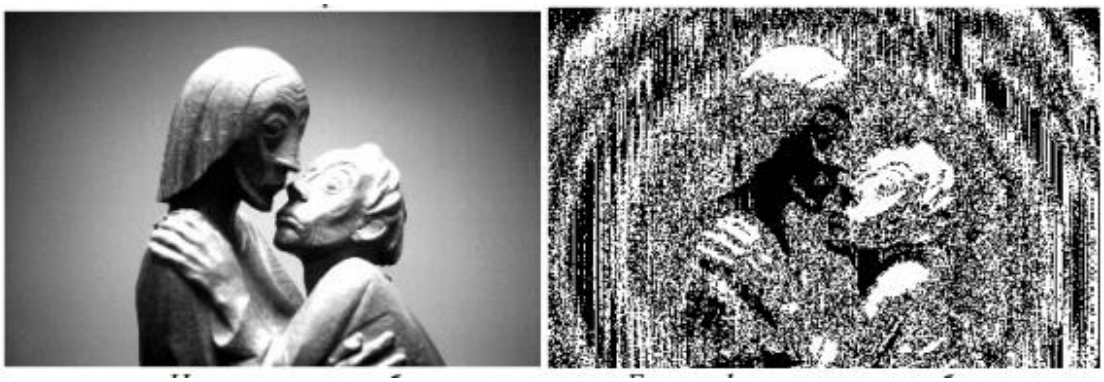


Рисунок 3.3 - Зображення до впровадження секретної інформації

Тут ще важливо врахувати особливості самого контейнера, тому що стиснені зображення (тобто JPEG) мають власні помітні шуми матриць.

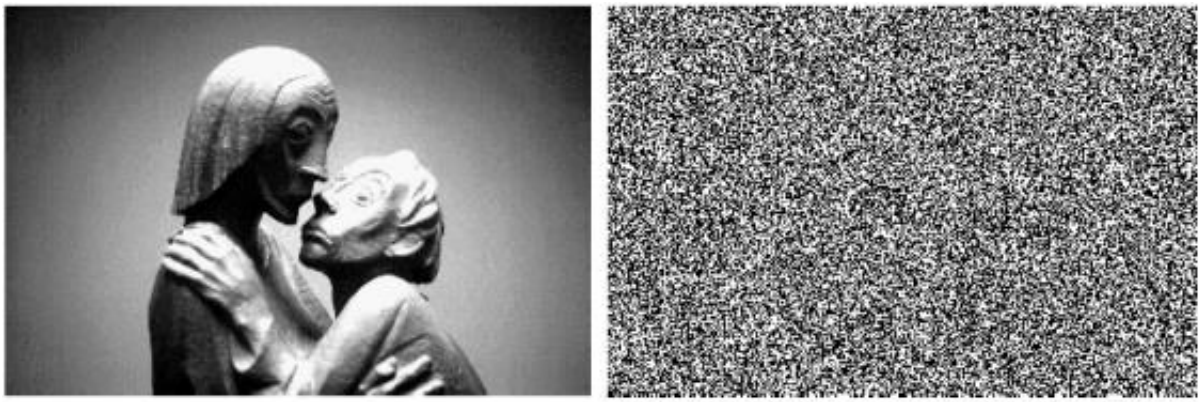


Рисунок 3.4 - Стеганограма з одним байтом прихованого повідомлення (зображення і відфільтрована частина)

За допомогою алгоритму ДКП один біт стеганограмми впливає відразу на 256 пікселів. Побачити факт вбудовування секретної інформації неможливо. Таким чином, алгоритм на основі ДКП стійкий до візуальних атак.

3.3 Статистичні атаки на стегосистеми із зображеннями-контейнерами.

Метод аналізу розподілу пар значень з використанням χ^2критерію.

У даному методі будуються гістограми для Для BMP-файлів – для значень пікселів зображення, для JPEG – для квантованих коефіцієнтів ДКП

Проводиться оцінка розподілу пар значень гістограми: пікселів зображення для bmp-формату, коефіцієнтів ДКП, які відрізняються за молодшим бітом (для jpeg-формату).

Виходять з міркування, що молодші біти зображень не є випадковими. На практиці, частоти двох сусідніх елементів контейнера за звичай суттєво відрізняються від значення частоти середнього арифметичного цих елементів. Під час вбудовування інформації ці частоти зближаються або стають рівними. Ідея атаки полягає в пошуку цих близьких значень і підрахунку ймовірності вбудовування на основі «близькості» значень частот парних і непарних елементів контейнера, що досліджується.

Аналіз зображення відбувається послідовно з накопиченням частот елементів.

Метод χ^2 є універсальним, адже не залежить від програми, якою вбудовуються конфіденційні дані.

Якщо робити заміну наймешзначущих бітів послідовно, то даний метод з високою вірогідністю виявляє наявність прихованих даних (рис. 3.2., а, б). Саме тому одним зі шляхів вдосконалення таких методів є псевдовипадковий вибір молодших бітів. В такому випадку метод не спрацьовує .

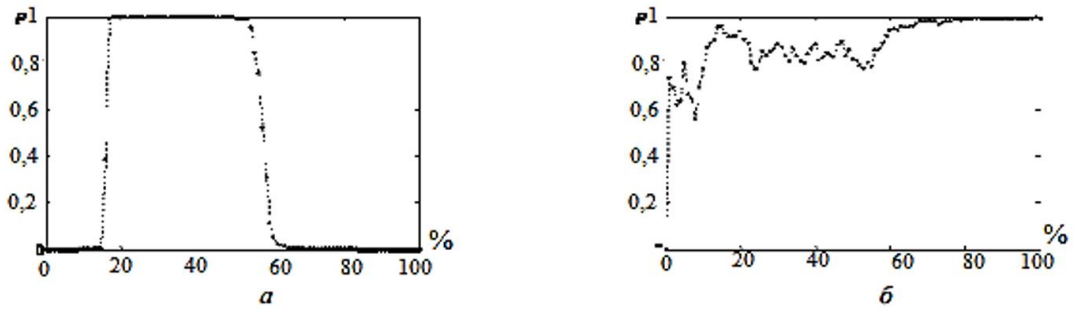


Рисунок 3.5 – Ймовірність вбудовування за критерієм χ^2 методом НЗБ: для а) послідовного вбудовування б) вбудовування з заповненням

Якщо розглянути метод на основі ДКП, то отримаємо наступну діаграму:

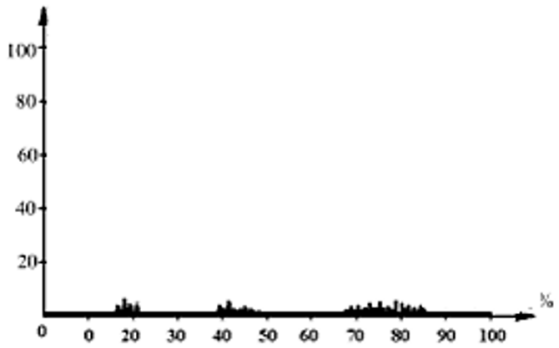


Рисунок 3.6 - Ймовірність вбудовування за критерієм χ^2 в JPEG

Таким чином, алгоритм на основі ДКП, який в якості контейнера використовує зображення JPEG стійкий до методу аналізу розподілу пар значень на основі критерію хі2, на відміну від методу НЗБ.

Метод аналізу гістограм, побудованих за частотами елементів зображення.

Даний метод, на відміну від попереднього, оцінює рівномірність розподілу елементів зображення, а також дає можливість визначити частоту появи конкретного елемента.

Діє наступне правило: якщо частоти двох сусідніх елементів BMP-зображення близькі за значенням і/або розташовані з різницею в одиницю (якщо використовувався класичний метод заміни наймеш значущого біта), то контейнер містить приховані дані (рис. 3.4., б). В протилежному випадку випадку, даний метод вважає контейнер незаповненим (рис. 3.4., а).

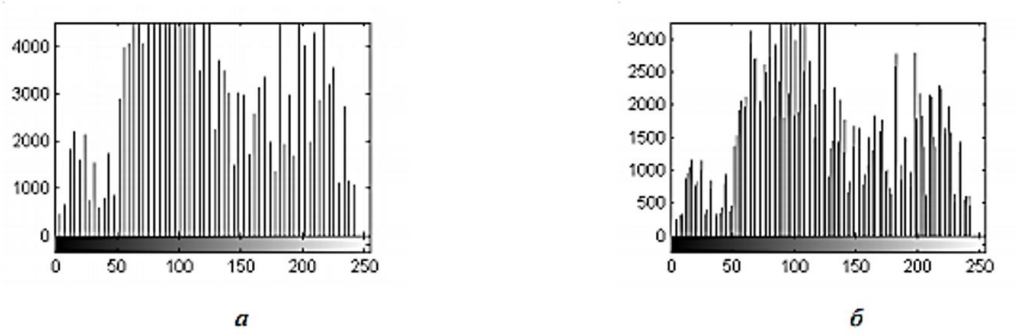


Рисунок 3.7 – Гістограма частот пікселів: а – початкового незаповненого bmp-зображення, б – заповненого bmp-контейнера

Для зображень в JPEG-форматі будується гістограма частот коефіцієнтів ДКП. Гістограма порожнього зображення наведена на рис 3.5, а гістограми зображень, що містять приховані дані - на рис. 3.6.

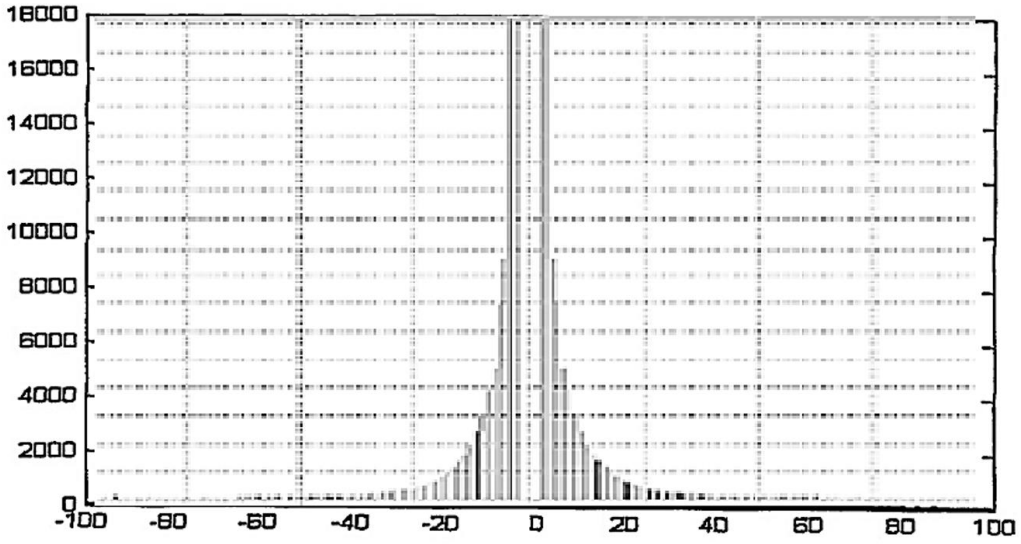


Рисунок 3.8 – Гістограма частот коефіцієнтів ДКП початкового незаповненого jpeg-зображення

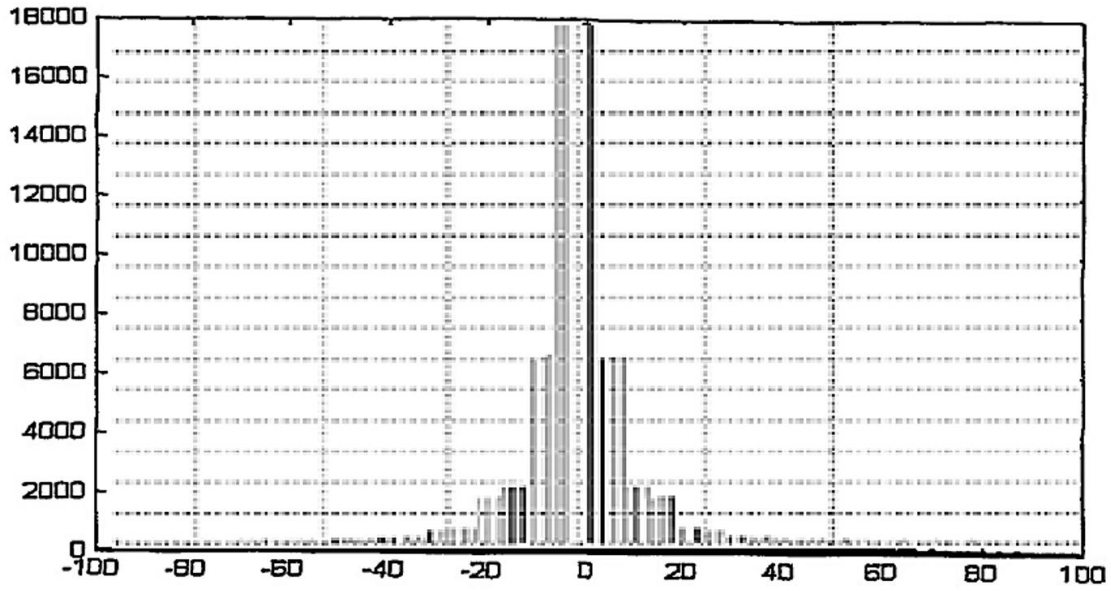


Рисунок 3.9 – Гістограма частот коефіцієнтів ДКП початкового заповненого jpeg-контейнеру

Важливим висновком, який можна зробити з вище наведених досліджень є той, що вбудовування інформації змінює загальний вигляд гістограм зображень. Більшість стеганографічних програм приховують дані у молодших бітах коефіцієнтів ДКП відмінних від 0 і 1 для JPEG-формату. Як наслідок, частоти 0-х і 1-х ДКП не змінюються, в той час, як усі інші частоти або зменшуються, або збільшуються, залежно від алгоритму вбудовування. Якщо кількість інформації для приховування доволі значна, то гістограми часто мають ступеневий характер, що нетипово для "звичайних" JPEG-зображень.

Висновок: на Підставі проведених експериментів наочно доведено, що метод НЗБ нестійкий навіть до найпростіших видів атак. Так що далі будемо досліджувати тільки вибраний метод на основі ДКП.

Застосуємо до нього наступну атаку: Гауссів білий шум.

Щоб проаналізувати зміни ДК коефіцієнтів при зашумленні зображення останнім вносився центрований білий гауссів шум з різними значеннями відхилення, від 0 до тих пір, поки деградація зображення не досягла рівня, абсолютно неприйнятного для використання в комерційних цілях. Результат представлений на рис. 3.7.

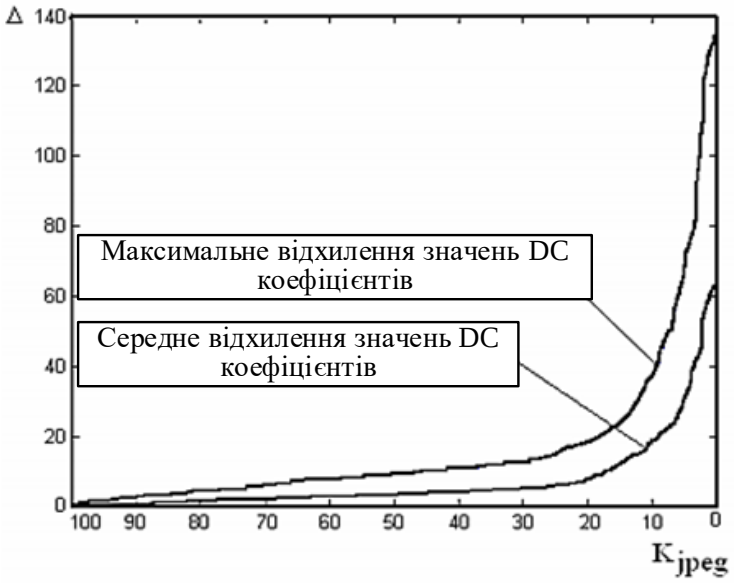


Рисунок 3.10 - Зміна DC коефіцієнтів зображення після стиснення з втратами JPEG

Зауважимо дуже незначні зміни значень коефіцієнтів ДК.

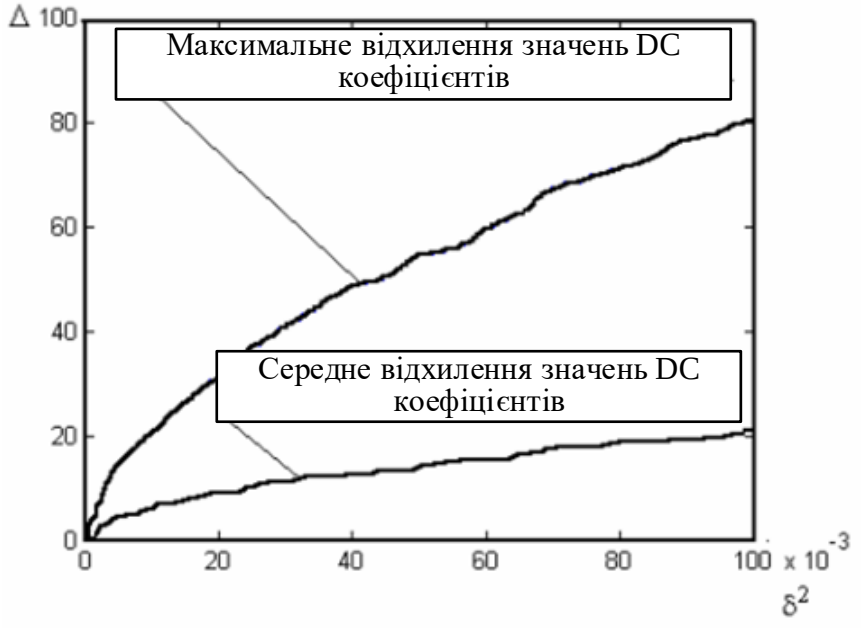


Рисунок 3.11 - Зміна DC коефіцієнтів зображення, яке зазнало зашумлення

3.4 Геометричні атаки

Для прикладу розглянемо масштабування. В ході експерименту з масштабуванням зображення-контейнер стискалося до різних розмірів аж до 80%-го стиснення, тобто в 5 разів. Обчислювати DC коефіцієнти стисненого зображення і порівнювати їх із коефіцієнтами оригінального зображення не має сенсу, принаймні, не зменшивши пропорційно розмір блоків, на які розбивається стиснуте зображення. Потрібно відновити зображення до розмірів вихідного, а вже потім обчислювати значення ДК коефіцієнтів. Це було зроблено в ході експерименту, результати якого представлені на рис.3.9.

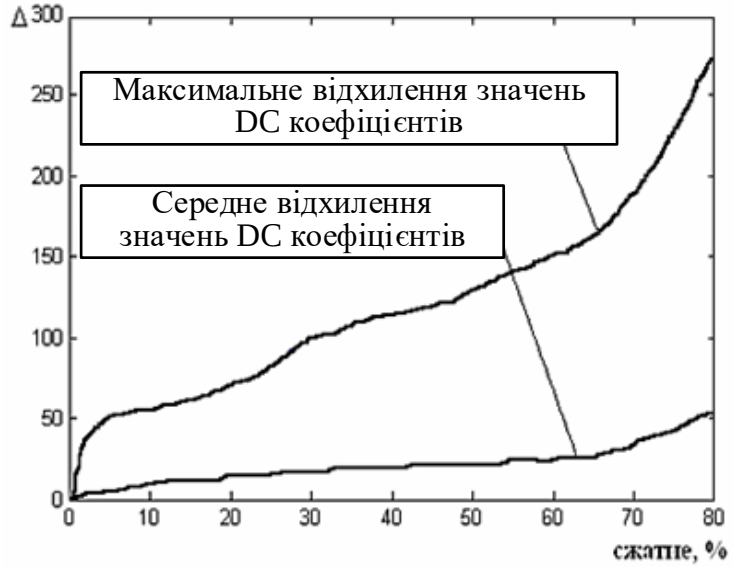


Рисунок 3.12 - Зміна ДК коефіцієнтів зображення, підданого масштабуванню

Фільтрація

Застосування фільтрів також можна віднести до розряду найбільш ймовірних зовнішніх атак на стеганосистему. Для цифрових зображень були обрані три види фільтрів: низькочастотний гауссів фільтр, усереднюються фільтр з розміром вікна 3×3 пікселя і контрастний фільтр, що підвищує різкість зображення, з тим же розміром вікна. Результати експерименту представлені в таблиці 3.1.

Таблиця 3.1 - Зміна ДК-коефіцієнтів зображення підданого фільтрації

Фільтрація	Максимальна зміна коефіцієнта ДК	Середня зміна коефіцієнта ДК
Низькочастотний	41	5,5
Усереднюються	126	17
Контрастний	211	34

Зробимо висновок, що активні атаки такі як зміна розміру, масштабу або структури файлу повністю знищують контейнер з секретним повідомленням. На відміну від активних, пасивні атаки лише допомагають виявити факт наявності конфіденційної інформації у стегоконтейнері. Таким чином обидва типа атак призводять до необхідності повторної передачі конфіденційної інформації.

Методи цифрової стеганографії основані на дискретно косинусних перетворень забезпечують більшу стійкість до атак. Перспективним напрямком подальших досліджень є вивчення методів на основі дискретно косинусного перетворення й збільшення швидкодії.

Висновки до розділу 3

Пасивні атаки дозволяють криптоаналитику виявити факт присутності конфіденційної інформації в стегаконтейнери.

Аналіз атак, який було проведено, показав, що активні атаки (такі як зміна структури файлу, розмір, масштаб і т. д.) призводять до повного знищення контейнера з секретними даними.

Методи цифрової стеганографії базуються на дискретно косинусному перетворенні забезпечують велику стійкість до атак.

ДК-коефіцієнти мають високу стійкість до зовнішніх впливів. Середнє значення змін ДК-коефіцієнтів практично для всіх зовнішніх впливів з великою інтенсивністю, розглянутих в даній роботі, не перевищує 3%, що гарантує стійкість впровадженої інформації. Візуальні спотворення зображення контейнера при таких незначних змінах, швидше за все, залишаться невиразні для системи людського зору. Слід зазначити, що для успішного впровадження інформації в ДК-коефіцієнти необхідно здійснювати якісний добір коефіцієнтів, найменш схильних до зовнішніх впливів, що, хоч і призведе до зниження пропускної спроможності, але може значно підвищити стійкість і скритність впровадження.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

У кваліфікаційній роботі магістра спроектовано систему для приховування та отримання секретної інформації шляхом вбудовування її в зображення-контейнери. Під час розв’язання задач дослідження, особливо практичної реалізації системи, враховано вимоги з охорони праці і техніки безпеки, пожежної та електробезпеки.

Виконання як теоретичної частини роботи, так і практичної, передбачає використання комп’ютерної техніки та обладнання з низькими напругами і силою струму. Зокрема, в якості блоку живлення плати ESP8266, використовувалась напруга живлення, яка становить 5 В. На платі використовуються можливі номінали напруги на рівні 5 В і 3,3 В, що не становить небезпеки для користувачів та розробника системи.

В якості регламентуючого документа з пожежної безпеки перед початком роботи над комп’ютерною системою для контролю параметрів мікроклімату теплиць використано вимоги «Типового положення про інструктажі, спеціальне навчання та перевірку знань з питань пожежної безпеки на підприємствах, в установах та організаціях України», які є діючим на даний час і затверджені постановою Кабінету міністрів України від 26 червня 2013 р. № 444.

Для організації захисту від негативного впливу екранів дотримано вимог Закону України "Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями" та НПАОП 0.00-7.15-18, який затверджений наказом Міністерства соціальної політики України 14.02.2018 N207. Робоче місце під час виконання кваліфікаційної роботи та проектування комп’ютерної системи облаштовано згідно наведених вимог та відповідає організаційним, ергономічним та вимогам з пожежної безпеки.

Електробезпеку робочого місця регламентують Правила безпечної експлуатації електроустановок споживачів, які затверджені наказом

Держнаглядохоронпраці від 09.01.98 N 4, зареєстрованих у Міністерстві юстиції України 10.02.98 за N 93/2533 (НПАОП 40.1-1.21-98). Електромережа, яка використовувалася при виконанні кваліфікаційної роботи магістра, відповідає правилам [23]:

– живлення електромережі проектовано, як окрему групову трьох провідну мережу з використанням фази, робочого «нуля» та захисного «нуля»;

– захисний «нуль» застосовано для реалізації заземлення електропристроїв;

– усі електричні та електронні пристрої мають захист від короткого замикання та непередбачуваних аварійних ситуацій;

– монтаж та експлуатація електромережі задовольняють вимогам щодо унеможливлення виникнення джерела загоряння через коротке замикання та перевантаження;

– усі лінії електроживлення виконанні не з легкозаймистого матеріалу або з негорючою ізоляцію;

– електричне устаткування підключено до мережі лише за допомогою справних штепсельних з’єднань і розеток заводського виготовлення;

– у розетках і штепселях передбачено контакти заземлення.

Вимоги електробезпеки при проектуванні компонентів комп’ютерної системи для контролю параметрів мікроклімату теплиць дотримано двома шляхами: використання безпровідних технологій передавання даних і напруги живлення в діапазоні 3,3В і 5 В, що дозволяє зменшити можливість ураження струмом при виникненні контакту з мережею чи в аварійних ситуаціях.

Щодо пожежної безпеки будівлі, де виконувався проект, то дотримано вимоги державних будівельних норм "Пожежна безпека об'єктів будівництва", які затверджені наказом Держбуду України від 03.12.2002 N 88, а також вимоги правил пожежної безпеки України, затвердженими наказом Міністерства України з питань надзвичайних ситуацій від 19.10.2004 N 126.

У приміщеннях, де розташовуються робочі місця користувачів ПК потрібно забезпечити відповідність вимогам санітарних норм і правил

наведених у ДСанПіН 3.3.2-007-98 [24]. Крім цього, на робочих місцях, обладнаних комп'ютерами і периферійною технікою забезпечено оптимальні значення параметрів мікроклімату: температури, руху повітря та відносної вологості, у відповідності до вимог нормативних документів.

Щодо освітлення, то приміщення де експлуатуються ПК, повинно бути обладнаним джерелами штучного освітлення та мати природне освітлення. Нормативний документ, який регламентує вимоги до рівнів природного і штучного освітлення – ДБН В.2.5-28-2018. Природне освітлення забезпечують прозорі вікна та інші світлові прорізи, що знаходяться на півночі або північному сході. У приміщеннях коефіцієнт природного освітлення повинен бути не нижче ніж 1,5 %. Розрахунок коефіцієнта природного освітлення виконують відповідно до методики, яка наведена у ДБН В.2.5-28-2018.

Штучне освітлення у приміщеннях з ПК забезпечується за допомогою системи загального освітлення, переважно рівномірного. В якості штучного джерела світла застосовуються люмінесцентні лампи типу ЛБ.

При використанні ПК для розробки проекту комп'ютерної системи для контролю параметрів мікроклімату теплиць на основі технологій інтернету речей було дотримано наступних вимог з техніки безпеки:

– не виконувався самостійний ремонт ПК і периферійних пристроїв;

– не вносились конструктивні чи інші зміни в апаратне забезпечення комп'ютера;

– використовувались тільки ті матеріали та предмети, які стосувались розробки комп'ютерної системи для контролю параметрів мікроклімату теплиць.

Для забезпечення вимог щодо безпечної експлуатації інформаційних технологій та мереж дотримано вимог СТУ EN 60950-1:2015 «Обладнання інформаційних технологій. Безпека. Частина 1. Загальні вимоги» (ДСТУ EN 60950- 1:2015).

4.2 Організація оповіщення і зв’язку у надзвичайних ситуаціях техногенного та природного характеру

Одним із головних заходів захисту населення від надзвичайних ситуацій (НС) є його своєчасне оповіщення про небезпеку, обстановку, яка склалася внаслідок її реалізації, а також інформування про порядок і правила поведінки в умовах НС. Під час організації оповіщення і доведення інформації до населення України необхідно керуватися вимогами Положення про організацію оповіщення і зв'язку у надзвичайних ситуаціях, затвердженого постановою Кабінету Міністрів України від 15 лютого 1999 року № 192. Кожний громадянин України повинен знати порядок подавання сигналу “Увага всім!”, діяти за ним та іншими сигналами цивільного захисту (ЦЗ) в умовах НС та особливого періоду.

Встановлено, що система оповіщення та інформування у сфері ЦЗ України включає:

– оперативне доведення до відома населення інформації про виникнення або можливу загрозу виникнення НС, у тому числі через загальнодержавну, територіальні і локальні автоматизовані системи централізованого оповіщення;

– завчасне створення та організаційно-технічне поєднання постійно діючих локальних систем оповіщення та інформування населення із спеціальними системами спостереження і контролю (включаючи державну мережу спостереження і лабораторного контролю) в зонах можливого ураження;

– централізоване використання мереж зв'язку, радіомовлення, телебачення та інших технічних засобів передачі інформації незалежно від форми власності та підпорядкування в разі виникнення НС.

Системи оповіщення населення України мають державний, регіональний, місцевий і об'єктовий рівні. Управління системою оповіщення кожного рівня організовується безпосередньо відповідними органами повсякденного

управління системи ЦЗ. Рішення на застосування системи оповіщення приймає відповідний голова державної адміністрації (начальник територіальної підсистеми Єдиної системи цивільного захисту). Відповідальність за організацію і практичне здійснення оповіщення несуть керівники органів виконавчої влади, місцевого самоврядування, підприємств, установ і організацій. Тому керівник об'єкта господарської діяльності і кожний громадянин повинні знати сигнали ЦЗ і уміти правильно за ними діяти.

В результаті наукової розвідки встановлено, що в Єдиній системі ЦЗ України оповіщення населення передбачає спочатку, за будь-якого характеру небезпеки, включення електричних сирен, переривчастий звук яких означає єдиний сигнал небезпеки "Увага всім!". Для вирішення завдань оповіщення на всіх рівнях Єдиної системи ЦЗ створюються спеціальні системи централізованого оповіщення (СЦО). Системою оповіщення будь-якого рівня є організаційно-технічне об'єднання оперативно чергових служб органів управління ЦЗ, спеціальної апаратури управління і засобів оповіщення, а також каналів (ліній зв'язку), які забезпечують передачу команд управління і мовної інформації у НС.

СЦО регіонального рівня є основною ланкою системи оповіщення в цілому. Саме з цього рівня планується організація централізованого оповіщення. Завданням СЦО регіонального рівня є оповіщення посадових осіб і сил даного рівня, органів управління, сил місцевого і об'єктового рівнів та їх посадових осіб, а також населення, яке проживає на території, на яку поширюється дія СЦО цього рівня. Інформація, яка доводиться до органів управління і посадових осіб, має оперативний характер, а до населення доводиться інформація про характер і масштаби загрози та про дії в умовах НС, які склалися.

Дослідженням встановлено, що основним способом оповіщення населення про НС в умовах мирного та воєнного часу є передача інформації з використанням державних мереж проводового, радіо і телевізійного мовлення. Для зосередження уваги населення перед передачею інформації вмикаються

сирени, виробничі гудки та інші сигнальні засоби, що буде означати подання попереджувального сигналу "Увага всім!", після якого негайно приводяться в готовність радіотрансляційні вузли, радіомовні і телевізійні станції, вмикаються мережі зовнішньої звукофікації. За сигналом населення зобов'язане увімкнути радіотрансляційні та телевізійні приймачі для прослуховування нагального повідомлення. У всіх випадках використання систем оповіщення, з увімкненням сирен, негайно доводиться до населення відповідне повідомлення засобами проводового, радіо та телевізійного мовлення. Тексти повідомлень передаються протягом 5 хвилин державною мовою і мовою, якою користується більшість населення в регіоні з припиненням іншої передачі. Тексти звернень записуються на магнітних стрічках на весь обсяг касети з обох сторін. Фонограми і друковані тексти звернень зберігаються в запечатаних конвертах в оперативних чергових з питань НС, які в необхідних випадках доводяться до населення. Дублікати фонограм і друкованих текстів звернень зберігаються в запечатаних конвертах на радіотрансляційних вузлах, в апаратних радіомовлення, студіях телебачення і використовуються в разі виходу з ладу апаратури оповіщення або аварії на з'єднувальній лінії зв’язку.

У разі повітряної тривоги: “Увага! Говорить Головне управління (управління, відділ) з питань НС облдержадміністрації (міськвиконкому, райдержадміністрації). Громадяни! Повітряна тривога! Відключіть світло, газ, погасіть вогонь у печах. Візьміть засоби індивідуального захисту, документи, запас харчів та води. Попередьте сусідів і допоможіть хворим та людям похилого віку вийти на вулицю. Якнайшвидше дістаньтеся захисної споруди або заховайтеся на місцевості. Дотримуйтеся спокою та порядку. Уважно слухайте повідомлення Головного управління (управління, відділу) з питань НС облдержадміністрації (міськвиконкому, райдержадміністрації)”.

Після повітряної тривоги: “Увага! Говорить Головне управління (управління, відділ) з питань НС облдержадміністрації (міськвиконкому, райдержадміністрації). Відбій повітряної тривоги! Усім повернутися до місць роботи або проживання. Допоможіть у цьому хворим та людям похилого віку.

Будьте готові до можливого повторного нападу противника. Завжди майте з собою засоби індивідуального захисту. Уважно слухайте повідомлення Головного управління (управління, відділу) з питань НС облдержадміністрації (міськвиконкому, райдержадміністрації)".

У разі загрози хімічного зараження: "Увага! Говорить Головне управління (управління, відділ) з питань НС облдержадміністрації (міськвиконкому, райдержадміністрації). Громадяни! Виникла безпосередня загроза хімічного зараження. Одягніть протигази, сховайте дітей у дитячих захисних камерах. Для захисту поверхні тіла використовуйте захисний одяг, комбінезони та чоботи. При собі майте плівкові (полімерні) накидки, куртки або плащі. Перевірте герметизацію житлових приміщень, стан вікон та дверей. Загерметизуйте продукти харчування і запасіться водою. Укрийте сільськогосподарських тварин і корми. Допоможіть хворим та людям похилого віку. Сповістіть сусідів про одержану інформацію. Відключіть електронагрівальні прилади. Надалі дійте відповідно до вказівок Головного управління (управління, відділу) з питань НС облдержадміністрації (міськвиконкому, райдержадміністрації)".

У разі загрози радіоактивного зараження: "Увага! Говорить Головне управління (управління, відділ) з питань НС облдержадміністрації (міськ-виконкому, райдержадміністрації). Громадяни! Виникла безпосередня загроза радіоактивного зараження. Приведіть у готовність засоби індивідуального захисту та постійно майте їх із собою. Після команди управління (відділу) з питань НС та у справах захисту населення від наслідків Чорнобильської катастрофи надягніть їх. Для захисту поверхні тіла від забруднення радіоактивними речовинами використовуйте захисний одяг, комбінезони та чоботи. При собі майте плівкові (полімерні) накидки, куртки або плащі. Перевірте герметизацію житлових приміщень, стан вікон та дверей. Загерметизуйте продукти харчування і запасіться водою. Укрийте сільськогос-подарських тварин і корми. Сповістіть сусідів про одержану інформацію. Допоможіть хворим та людям похилого віку. Надалі дійте відповідно до

вказівок Головного управління (управління, відділу) з питань НС облдержадміністрації (міськвиконкому, райдержадміністрації)".

Уразі загрози біологічного зараження: "Увага! Говорить Головне управління (управління, відділ) з питань НС облдержадміністрації (міськ-виконкому, райдержадміністрації). Громадяни! Виникла безпосередня загроза біологічного зараження. Для захисту поверхні тіла використовуйте захисний одяг, комбінезони та чоботи. Із собою майте плівкові (полімерні) накидки, куртки або плащі. Перевірте герметизацію житлових приміщень, стан вікон та дверей. Загерметизуйте продукти харчування і запасіться водою. Укрийте сільськогосподарських тварин і корми. Допоможіть хворим та людям похилого віку. Сповістіть сусідів про одержану інформацію. Відключіть електронагрівальні прилади. Надалі дійте відповідно до вказівок Головного управління (управління, відділу) з питань НС облдержадміністрації (міськвиконкому, райдержадміністрації)".

ВИСНОВКИ

Проведений аналіз методів цифрової стеганографії показав, що методи стеганографії не тільки дозволяють передавати приховані дані, але і успішно вирішують проблеми відстеження поширення інформації мережами зв'язку, захисту інформації від несанкціонованого копіювання. Сенс перших двох цілей є захист самого контейнера, а сенс третьої цілі - сама прихована передача даних.

Можно відзначити також, що краще використовувати методи, які впроваджують секретну інформацію у частотній області зображення (на етапі перетворень), бо це робить їх стійкими до основник атак (візуальних, статистичних та криптографічних).

На сьогодні не уснує стеганографічного методу повністю стійкого до усіх атак. Але проведений аналіз існуючих методів показав,що вести дослідження треба у частотній області та модифікувати існуючи методі, опираючись на їх недоліки та переваги, щоб створити найбіль модифікований стегонаграфічний метод.

У кваліфікаційнй роботі було проведено класифікацію та аналіз методів цифрової стеанографії. Розглянуто принципи впровадження конфіденційної інформації у частотному та часовому просторі контейнера.

Методом компромісного рішення визначили найбільш придатний метод цифрової стеганографії з розглянутих є метод на основі ДКП.

Проведено класифікацію найпоширеніших атак на стегосистему та аналіз методів за допомогою обраних атак. Було доведено, що методи, які працюють у частотному просторі зображення більш стійкіші до атак навідміну від методів які впроваджують інформацію використовуючи часовий простір. Такі методи не стійки до жодних перетворень стегоконтейнера.

Тому перспективним напрямком подальших досліджень є вивчення методів на основі дискретно косинусного перетворення і збільшення швидкодії, а також оцінка стійкості до основних видів атак на основі розробленого програмного макета.

Для проведення досліджень був розроблений модуль, що реалізує метод на основі дискретно косинусного перетворення для приховування конфіденційної інформації в контейнер-зображення.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бурячок В.Л. Інфомаційна та кібербезпека / В.Л.Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. –К.: ДУТ, 2015. –288 с.

2. Edited by Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p

3. Мельник С. Методи цифрової стеганографії: стан та напрями розвитку // С. Мельник, В. Кащук. // Information Security of the Person, Society and State. – 2013. – №3. – С. 65–70

4. Генне, О. В. Основні положення стеганографії [Електронний ресурс] / О. В. Генне. – 2006. – Режим доступу : http://www.citforum.ru/internet/securities/stegano.штмл.

5. Козюра В.Д. Захист інформації в комп’ютерних системах :підручник / В.Д.Козюра, В.О.Хорошко, М.Є.Шелест – Ніжин : ФОП Лукяненко В.В., ТПК «Орхідея», 2020. – 236 с.

6. Конахович Г.Ф. Компютерна стеганографічна обробка й аналіз мультимедійних дан6 : підручник /Г.Ф. Конафович, Д.О.Прогонов, О.Ю. Пузиренко. – К. – «Alex Print Centre», 2018/ – 558 с.

7. . Р. В. Грищук, та Ю. Г. Даник, “Синергія інформаційних та кібернетичних дій”, Труди університету. НУОУ, № 6 (127), с. 132–143. 2014.

8. В. Л. Бурячок, Р. В. Грищук, та В. О. Хорошко, під заг. ред. проф. В. О. Хорошка, “Політика інформаційної безпеки”, ПВП «Задруга»,. 2014.

9. Ю. Г. Даник та ін., “Основи захисту інформації” навч. пос., Житомир : ЖВІ ДУТ, 2015.

10. Р. В. Грищук, “Синтез систем інформаційної безпеки за заданими властивостями”, Вісник національного університету “Львівська політехніка”. Серія : Автоматика, вимірювання та керування : зб. наук. пр., ЛП, № 74, с. 271 – 276, 2012.

11. Р. В. Грищук, “Атаки на інформацію в інформаційно-комунікаційних системах”, Сучасна спеціальна техніка, №1(24), с.61 – 66. 2011.

12. Р. В. Грищук, і В. В. Охрімчук, “Постановка наукового завдання з розроблення шаблонів потенційно небезпечних кібератак”, Безпека інформації, Том 21, № 3, с. 276 – 282, 2015.

13. Ю. Г. Даник, Р. В. Грищук, “Синергетичні ефекти в площині інформаційного та кібернетичного протиборства”, Наук.-практ. конф. “Актуальні проблеми управління інформаційною безпекою держави”, Київ, 19 берез, 2015, с. 235 – 237.

14. Р. В. Грищук, В. В. Охрімчук, “Напрямки підвищення захищеності комп’ютерних систем та мереж від кібератак”, ІІ Міжнар. наук.-практ. конф. “Актуальні питання забезпечення кібербезпеки та захисту інформації” (Закарпатська область, Міжгірський район, село Верхнє Студене, 24-27 лют. 2016 р.). – К. : Видавництво Європейського університету, 2016 с. 60 – 61.

15. Захист інформації в комп’ютерних системах від несанкціонованого доступу. / За ред. С.Г. Лаптєва. – К., 2001. – 321 с.

16. Кузнецов О.О., Євсеєв С.П., Король О. Г. Стеганографія: навчальний посібник – 232с.

17. Метод компромісного рішення. [Електронний ресурс]. – Режим доступу до ресурсу: http://studopedia.org/3-22614.html

18. .

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

20. web.archive.org/web/20140221205846/http://er.nau.edu.ua/bitstream/NAU/8049/1/CompSteganoRU.pdf

21. https://books.google.com.ua/books?id=-clcDwAAQBAJ&printsec=frontcover&hl=ru&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

22. Персональні навчальні системи кафедри кібербезпеки НТУ “ХПІ” за дисципліною “ Основи стеганографічного захисту інформації ” https://iiiii-my.sharepoint.com/:f:/g/personal/serhii_yevseiev_khpi_eduua1/EpzTd_YZEZxKvyFvbzuXaiUBW3rVHBcQzLla6C1XvfbaEQ?e=H0hXDc.

23. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p.

24. . Євсеєв С.П. Кібербезпека: сучасні технології захисту. / Євсеєв С.П, Остапов С.Е., Король О.Г. // Навчальний посібник для студентів вищих навчальних закладів. Львів: “Новий Світ- 2000”, 2019. – 678. – Режим доступу: http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf

25. Ahmed N., Natarajan T., Rao K. Discrete Cosine Transform // IEEE Trans. Computers. – 1974. – V. 23.

26. Arnold M., Kanka S. MP3 robust audio watermarking // International Watermarking Workshop. 1999. – 548c.

27. Lu, C. -S. Multimedia security: Steganography and digital watermarking techniques for protection of intellectual property / C. -S. Lu. – Hershey: Idea Group Publishing, 2005. – 255 c.

28. Masoumi, M. A blind scene-based watermarking for video copyright protection / M. Masoumi, S. Amiri // AEU - International Journal of Electronics and Communications. – 2013. – № 67(6). – С. 528-535.

29. Singh, H. V. Robust copyright marking using Weibull distribution / H. V. Singh, S. Rai, A. Mohan, S. P. Singh // Computers & Electrical Engineering. – 2011. – № 37(5). – С. 714-728.

30. Стеганографія [Електронний ресурс]. – Режим доступу до ресурсу http://patents.com/search?top_keyword=steganography&keyword=steganography

31. Євсеєв С.П. Технології захисту інформації. Мультимедійне інтерактивне електронне видання комбінованого використання / уклад. Євсеєв

С. П., Король О. Г., Остапов С. Е., Коц Г. П. – Х.: ХНЕУ ім. С. Кузнеця, 2016. – 1013 Мб. ISBN 978-966-676-624-6

32. Top100-UA Рейтинг найпопулярніших сайтів. [Електронний ресурс]. – Режим доступу до ресурсу http://top.i.ua/

33. Теорема Котельнікова. [Електронний ресурс]. – Режим доступу до ресурсу http://sernam.ru/book_tec.php?id=14

ДОДАТКИ

Додаток А

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

XI НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

13-14 грудня 2023 року

ТЕРНОПІЛЬ
2023

УДК 004.056

І.Тернавчук
(Тернопільський національний технічний університет імені Івана Пулюя)

АНАЛІЗ МЕТОДІВ ЦИФРОВОЇ СТЕГАНОГРАФІЇ НА ОСНОВІ ДИСКРЕТНОГО КОСИНУСНОГО ПЕРЕТВОРЕННЯ

I.Ternavchuk

ANALYSIS OF DIGITAL STEGANOGRAPHY METHODS BASED ON DISCRETE COSINE TRANSFORMATION

З переходом до цифрового представлення інформації загострилася і без того актуальна проблема захисту конфіденційної інформації від несанкціонованого доступу. Дану проблему вирішують дві науки: криптографія та стеганографія. Але більший інтерес являє собою наука – стеганографія, тому що найбільш успішний спосіб захистити інформацію – це приховати сам факт наявності в ній чогось конфіденційного, що може привернути увагу зловмисника.

Існує два напрямки методів цифрової стеганографії:

– приховування інформації у часовій області мультимедійного об'єкта;

– приховування конфіденційної інформації в частотній області мультимедійного об'єкта.

Методи першої категорії працюють безпосередньо з зображенням. Принцип вбудовування інформації у часовій області контейнера полягає в наступному: інформацію вбудовують в незначущі біти області зображення, щоб не змінити візуальне представлення зображення для зорової системи людини. Вони застосовні тільки до зображень, які не були підвернені стисненню, тому що при стисненні малозначима інформація просто відсікаються. У разі впровадження в частотній області модуляції піддаються амплітудні складові комплексного спектра зображення-контейнера. Для цього попередньо здійснюється обчислення амплітудної і фазової складових компонентів перетворення Фур'є.

Серед лінійних ортогональних перетворень було обрано найбільш популярне дискретне косинусне перетворення [1], його застосовують при стисненні зображень і відео в стандартах JPEG, MPEG. Метод стеганографічного приховування буде стійкий до наступної компресії зображення, тільки в тому випадку, якщо враховує особливості використовуваного методу компресії [2].

Перевагами методу є стійкість до JPEG-компресії з малим коефіцієнтом стиснення. Але при цьоцу, основним недоліком – невелике візуальне спотворення зображення-контейнера при великому пороговому значенні різниці між коефіцієнтами ДКП блоків та малий обсяг повідомлення, який можна вбудувати. Проведений аналіз методів цифрової стеганографії показав, що всі існуючі на сьогоднішній час методи базуються в основному на надлишковості інформації, а також на невеликій чутливості людського ока в зміні характеристик зображення. Звичайно, найбільш ефективними є методи які використовують частотну область для вбудовування конфіденційної інформації, бо вони більш стійкі до різних викривлень, в тому числі стиснення, вбудовування інформації відбувається на етапі перетворень вихідного зображення. Методи цифрової стеганографії базуються на дискретно косинусному (DC) перетворенні забезпечують велику стійкість до атак.

Середнє значення змін DC-коефіцієнтів практично для всіх зовнішніх впливів з великою інтенсивністю, розглянутих в даній роботі, не перевищує 3%, що гарантує стійкість впровадженої інформації.

Література.

1. Мельник С. Методи цифрової стеганографії: стан та напрями розвитку // С. Мельник, В. Кащук. // Information Security of the Person, Society and State. – 2013. – №3. – С. 65–70

2. Генне О.В. Основные положения стеганографии // Защита информации. Конфидент – 2000. №3 – 56 с.

Додаток Б

Розробка додатку, який реалізує алгоритм приховування інформації на основі дискретно-косинусного перетворення

Для реалізації програми стеганографічного приховування даних у зображеннях JPEG було обрано мову програмування C#, середовище розробки Visual Studio 2013, графічного інтерфейсу Windows Forms і платформа .NET Framework 4.5

Нижче на малюнках представлена робота додатка.

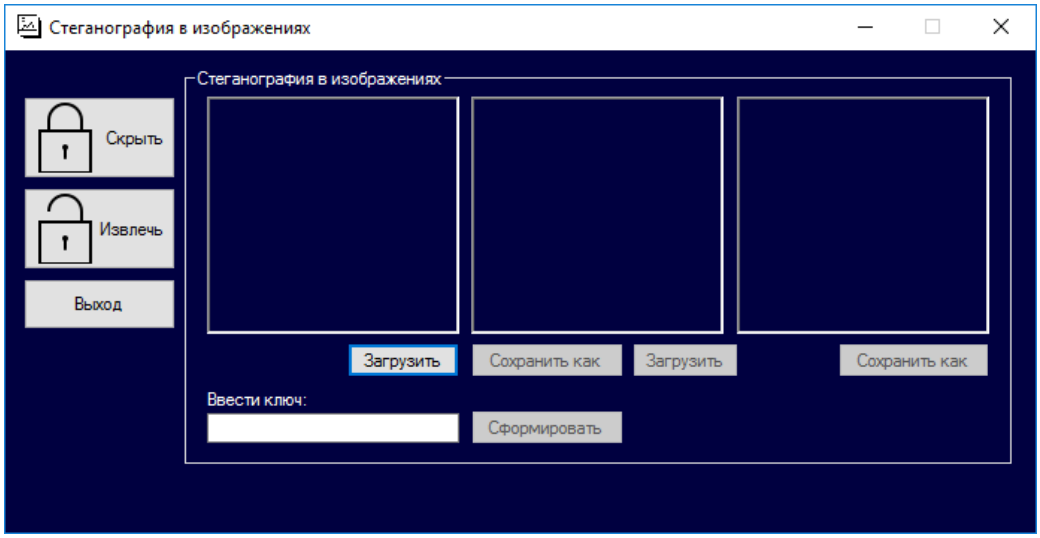


Рисунок 1 - Головне вікно додатка

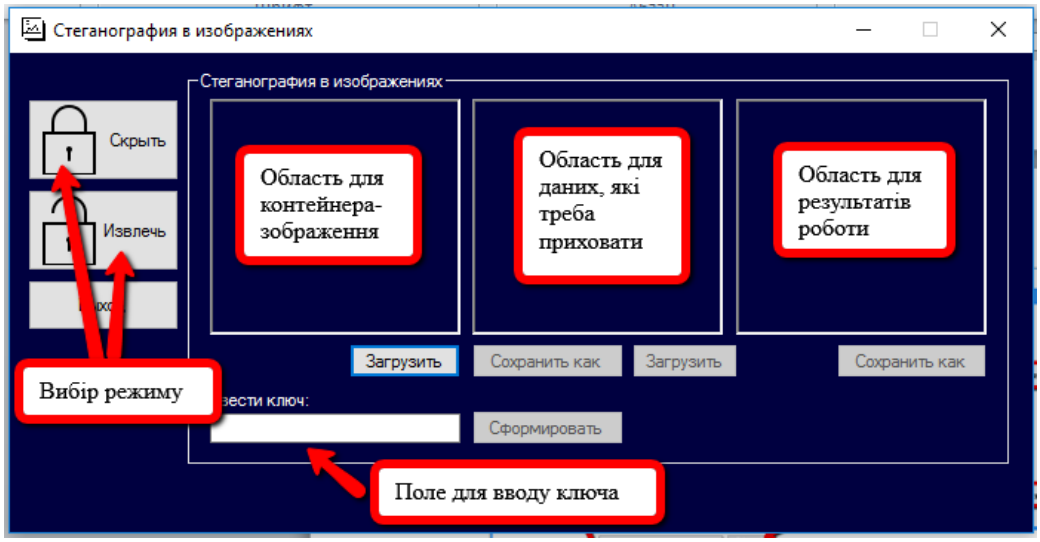


Рисунок 2 - Головне вікно додатка з підказками по застосуванню

Після завантаження зображення треба вибрати на скільки блоків його треба поділити, бо по алгоритму ми працюємо не з одразу усім зображенням, а з його частинами.

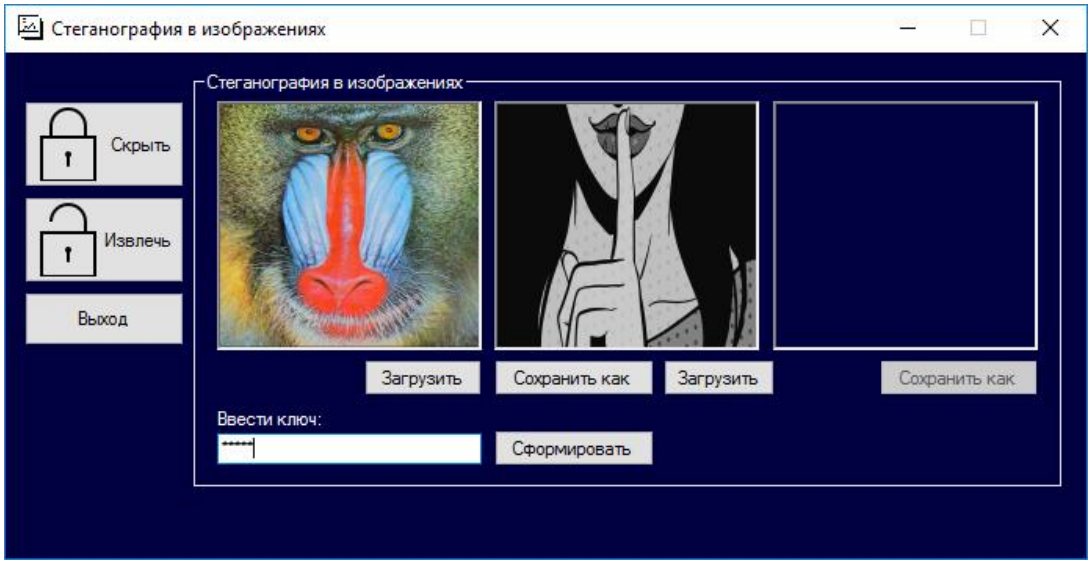


Рисунок 3 - Введення усіх потрібних вхідних даних для приховування секретного зображення (інформації)

Після введення необхідних вхідних даних треба натиснули кнопку «Сформировать». Та при успішному результаті у третю область будет завантажено зображення-стегоконтейнер. Його треба зберегти, щоб здійснити зворотнє перетворення.

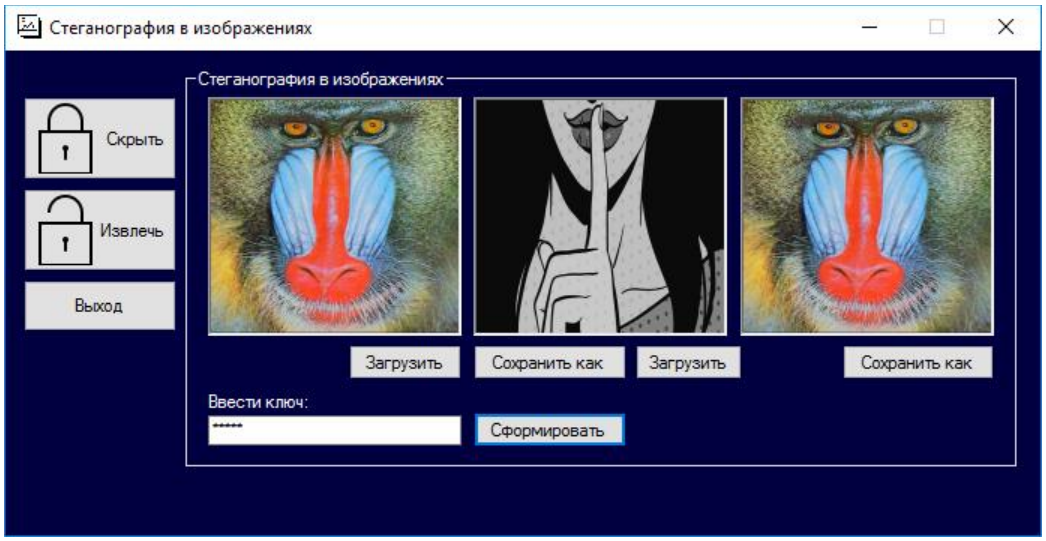


Рисунок 4 - Результат роботи програми (приховування конфіденційної інформації)

Для вилучення даних треба вибрати режим «Извлечь», завантажити зображення-стегоконтейнер, та ввести ключ. Та натиснути кнопку «Сформировать». Та при успішному результаті у другу область будет завантажено зображення, яке було приховано.

Рисунок 5 - Результат роботи програми (вилучення конфіденційної інформації)

Вилучення завершено. Результат вилученого зображення можна зберегти.

Додаток В

Вихідний код класів, що реалізують логіку роботи програми

```
using System;
using System.Collections;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using AForge.Imaging.Filters;

namespace Assignment_2
{
    public partial class Form1 : Form
    {
        public Form1()
        {
            InitializeComponent();
        }

        private void buttonBrowseSimple_Click(object sender, EventArgs e)
        {
            OpenFileDialog ofd = new OpenFileDialog();
            ofd.Filter = "Bitmap Image (.bmp)|*.bmp| Gif Image (.gif)|*.gif| JPG Image
(.jpg) |*.jpg| Png Image (.png)|*.png";

            if (ofd.ShowDialog() == DialogResult.OK)
            {
                pictureBoxSimple.ImageLocation = ofd.FileName;
                buttonBrowseSecret.Enabled = true;
            }
        }

        private void buttonBrowseSecret_Click(object sender, EventArgs e)
        {
            OpenFileDialog ofd = new OpenFileDialog();
            ofd.Filter = "Bitmap Image (.bmp)|*.bmp| Gif Image (.gif)|*.gif | JPG Image
(.jpg)|*.jpg| Png Image (.png)|*.png";

            if (ofd.ShowDialog() == DialogResult.OK)
            {
                Bitmap img = new Bitmap(ofd.FileName);
                pictureBoxSecret.Image = ToGreyScale(img);
                buttonSaveAsGrey.Enabled = true;
            }
        }

        private void buttonExit_Click(object sender, EventArgs e)
        {
            Application.Exit();
        }

        private Bitmap ToGreyScale(Bitmap bitmap)
        {
            int grey, i, j;
            Color color;

            for (i = 0; i < bitmap.Width; i++)
```

```
            {
                for (j = 0; j < bitmap.Height; j++)
                {
                    color = bitmap.GetPixel(i, j);
                    grey = (int)((color.R + color.G + color.B) / 3);
            //      grey = (int)((color.R * .3) + (color.G * .59) + (color.B * .11));

                    bitmap.SetPixel(i, j, Color.FromArgb(grey, grey, grey));
                }
            }

            return bitmap;
        }

        private void textBox1_TextChanged(object sender, EventArgs e)
        {
            if (textBoxKey.Text.Trim().Length < 4)
            {
                buttonGenerateResult.Enabled = false;
                errorProvider.SetError(textBoxKey, "Длина ключа должна быть больше 3
символов");
                return;
            }
            else
            {
                buttonGenerateResult.Enabled = true;
                errorProvider.SetError(textBoxKey, "");
            }

            try
            {
               int.Parse(textBoxKey.Text);
               errorProvider.SetError(textBoxKey, "");
            }
            catch (FormatException except)
            {
                errorProvider.SetError(textBoxKey, "Только целые числа");
                return;
            }
        }

        private void buttonSaveAs_Click(object sender, EventArgs e)
        {
            SaveFileDialog sfd = new SaveFileDialog();
            sfd.Filter = "Bitmap Image (.bmp)|*.bmp";

            if (sfd.ShowDialog() == DialogResult.OK)
            {

                pictureBoxResult.Image.Save(sfd.FileName);
            }
        }

        private void buttonDecryption_Click(object sender, EventArgs e)
        {
            groupBoxEncryption.Visible = false;
            groupBoxDecryption.Visible = true;
        }

        private void buttonEncryption_Click(object sender, EventArgs e)
        {
            groupBoxEncryption.Visible = true;
            groupBoxDecryption.Visible = false;
        }
```

```
        private void Form1_Load(object sender, EventArgs e)
        {
            groupBoxDecryption.Visible = false;
            groupBoxEncryption.Visible = true;
        }

        private void button2_Click(object sender, EventArgs e)
        {
            OpenFileDialog ofd = new OpenFileDialog();
            ofd.Filter = "Bitmap Image (.bmp)|*.bmp|Gif Image (.gif)|*.gif |JPEG Image
(.jpeg)|*.jpeg |Png Image (.png)|*.png ";
            if (ofd.ShowDialog() == DialogResult.OK)
            {
                pictureBoxEncryptedImage.ImageLocation = ofd.FileName;
            }
        }

        private byte getByte(byte[] bits)
        {
            String bitString = "";

            for (int i = 0; i < 8; i++)
                bitString += bits[i];
            byte newpix = Convert.ToByte(bitString, 2);
            int dePix = (int)newpix ^ key;
            return (byte)dePix;
        }

        private byte[] getBits(byte simplepixel)
        {
            int pixel = 0;
            pixel = (int)simplepixel ^ key;
            BitArray bits = new BitArray(new byte[] { (byte)pixel });
            bool[] boolarray = new bool[bits.Count];
            bits.CopyTo(boolarray, 0);
            byte[] bitsArray = boolarray.Select(bit => (byte)(bit ? 1 : 0)).ToArray();
            Array.Reverse(bitsArray);
            return bitsArray;
        }

        int key = 0;
        private void buttonGenerateResult_Click(object sender, EventArgs e)
        {
            Bitmap simple = new Bitmap(pictureBoxSimple.Image);
            Bitmap secretGreyScale = new Bitmap(pictureBoxSecret.Image);

            if (secretGreyScale.Height != simple.Height || secretGreyScale.Width !=
simple.Width)
            {
                ResizeBilinear resizeFilter = new ResizeBilinear(simple.Width,
simple.Height);
                secretGreyScale = resizeFilter.Apply(secretGreyScale);
            }

            /* Variables initialization */
            Color pixelContainerImage = new Color();
            Color pixelMsgImage = new Color();

            key = int.Parse(textBoxKey.Text);

            byte[] MsgBits;
            byte[] AlphaBits;
            byte[] RedBits;
            byte[] GreenBits;
            byte[] BlueBits;
```

```
            byte newAlpha = 0;
            byte newRed = 0;
            byte newGreen = 0;
            byte newBlue = 0;

            /* Image Encryption */
            #region Encryption

            for (int i = 0; i < simple.Height; i++)
            {
                for (int j = 0; j < simple.Width; j++)
                {
                    pixelMsgImage = secretGreyScale.GetPixel(j, i);
                    MsgBits = getBits((byte)pixelMsgImage.R);

                    pixelContainerImage = simple.GetPixel(j, i);
                    AlphaBits = getBits((byte)pixelContainerImage.A);
                    RedBits = getBits((byte)pixelContainerImage.R);
                    GreenBits = getBits((byte)pixelContainerImage.G);
                    BlueBits = getBits((byte)pixelContainerImage.B);

                    AlphaBits[6] = MsgBits[0];
                    AlphaBits[7] = MsgBits[1];

                    RedBits[6] = MsgBits[2];
                    RedBits[7] = MsgBits[3];

                    GreenBits[6] = MsgBits[4];
                    GreenBits[7] = MsgBits[5];

                    BlueBits[6] = MsgBits[6];
                    BlueBits[7] = MsgBits[7];

                    newAlpha = getByte(AlphaBits);
                    newRed = getByte(RedBits);
                    newGreen = getByte(GreenBits);
                    newBlue = getByte(BlueBits);

                    pixelContainerImage = Color.FromArgb(newAlpha, newRed, newGreen,
newBlue);
                    simple.SetPixel(j, i, pixelContainerImage);
                }
        //        richTextBox1.Text += "\n";
            }
            pictureBoxResult.Image = simple;
            // in the line below the value of pixels are changed
            //MessageBox.Show(((Bitmap)pictureBoxResult.Image).GetPixel(0, 0).B.ToString());
            // but if this will give the correct modified value
            //MessageBox.Show(simple.GetPixel(0, 0).B.ToString());

            buttonSaveAs.Enabled = true;
            #endregion
        }

        private void button4_Click(object sender, EventArgs e)
        {
            Bitmap EncryptedImage = (Bitmap)pictureBoxEncryptedImage.Image;
            //Bitmap hiddenImage = (Bitmap)EncryptedImage.Clone();
            Bitmap hiddenImage = new Bitmap (EncryptedImage.Width, EncryptedImage.Height);

            /* Variables initialization */
            Color pixelToDecrypt = new Color();

            try
```

```
            {
                key = int.Parse(textBoxDekey.Text);
            }
            catch (FormatException except)
            {
                MessageBox.Show("Допускаются только целые числа для ключа");
                return;
            }

            byte[] BitsToDecrypt = new byte[8];
            byte[] AlphaBits;
            byte[] RedBits;
            byte[] GreenBits;
            byte[] BlueBits;

            byte newGrey = 0;

            /* Image Decryption */
            #region Encryption

            for (int i = 0; i < EncryptedImage.Height; i++)
            {
                for (int j = 0; j < EncryptedImage.Width; j++)
                {
                    pixelToDecrypt = EncryptedImage.GetPixel(j, i);

                    AlphaBits = getBits((byte)pixelToDecrypt.A);
                    RedBits = getBits((byte)pixelToDecrypt.R);
                    GreenBits = getBits((byte)pixelToDecrypt.G);
                    BlueBits = getBits((byte)pixelToDecrypt.B);

                    BitsToDecrypt[0] = AlphaBits[6];
                    BitsToDecrypt[1] = AlphaBits[7];
                    BitsToDecrypt[2] = RedBits[6];
                    BitsToDecrypt[3] = RedBits[7];
                    BitsToDecrypt[4] = GreenBits[6];
                    BitsToDecrypt[5] = GreenBits[7];
                    BitsToDecrypt[6] = BlueBits[6];
                    BitsToDecrypt[7] = BlueBits[7];

                    //for (int k = 0; k < BitsToDecrypt.Length; k++)
                    //    richTextBox2.Text += BitsToDecrypt[k];
                    //richTextBox2.Text += " - ";

                    newGrey = getByte(BitsToDecrypt);

                   // MessageBox.Show(newGrey.ToString());

                    pixelToDecrypt = Color.FromArgb(newGrey, newGrey, newGrey);

                    hiddenImage.SetPixel(j, i, pixelToDecrypt);
                }
         //       richTextBox2.Text += "\n";
            }
            pictureBoxExtractedImage.Image = hiddenImage;
            buttonSaveAsFinal.Enabled = true;

            #endregion
        }

        private void button1_Click(object sender, EventArgs e)
        {
            SaveFileDialog sfd = new SaveFileDialog();
            sfd.Filter = "Bitmap Image (.bmp)|*.bmp|Gif Image (.gif)|*.gif |JPEG Image
(.jpeg)|*.jpeg |Png Image (.png)|*.png ";
```

```
            if (sfd.ShowDialog() == DialogResult.OK)
            {
                pictureBoxExtractedImage.Image.Save(sfd.FileName);
            }
        }

        private void button3_Click(object sender, EventArgs e)
        {
            SaveFileDialog sfd = new SaveFileDialog();
            sfd.Filter = "Bitmap Image (.bmp)|*.bmp|Gif Image (.gif)|*.gif |JPEG Image
(.jpeg)|*.jpeg |Png Image (.png)|*.png ";

            if (sfd.ShowDialog() == DialogResult.OK)
            {
                pictureBoxSecret.Image.Save(sfd.FileName);
            }
        }

        private void textBoxDekey_TextChanged(object sender, EventArgs e)
        {
            if (textBoxDekey.Text.Trim().Length < 4 && textBoxDekey.Text.Trim().Length > 7)
            {
                buttonDecrypt.Enabled = false;
                errorProvider.SetError(textBoxDekey, "Длина ключа должна быть больше 3
символов, но меньше 7");
                return;
            }
            else
            {
                errorProvider.SetError(textBoxDekey, "");
                buttonDecrypt.Enabled = true;
            }

            try
            {
                int.Parse(textBoxDekey.Text);
                errorProvider.SetError(textBoxDekey, "");
            }
            catch (FormatException except)
            {
                errorProvider.SetError(textBoxDekey, "Допускаются только целые числа");
                return;
            }
        }

        private void pictureBoxSimple_Click(object sender, EventArgs e)
        {

        }

        private void groupBoxDecryption_Enter(object sender, EventArgs e)
        {

        }
    }
}
```