Міністерство освіти і науки України
Київський Національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА
Дипломної роботи

магістра
(назва освітньо–кваліфікаційного рівня)

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній рівень ***магістр***
(назва освітнього рівня)

кваліфікація
(код і назва кваліфікації)

на тему: *Методи стеганоаналізу в задачах захисту інформаційних потоків даних*

Виконавець: студентка *2* **курсу, групи** *КБм–21*

Симониченко Анна Андріївна
(підпис) (прізвище ім'я по–батькові)

	Прізвище, ініціали	Оцінка	Підпис
Науковий керівник	Бучик С. С.		
Рецензент	Самохвалов Ю. Я.		
Нормоконтроль	Мирутенко Л. В.		

Київ
2021

Міністерство освіти і науки України
Київський Національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри
кібербезпеки та захисту інформації

_____ Лукова-Чуйко Н.В.

«_____»_____20___року

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студенту *КБм–21* (група) *Симониченко Анні Андріївні* (прізвище ім'я по–батькові)

Тема дипломного роботи *Методи стеганоаналізу в задачах захисту інформаційних потоків даних*

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол №2 від 08.10.2020 р.

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень *процес приховування даних у нерухомих зображеннях при використанні стеганографічних методів в задачах захисту інформаційних потоків даних.*

Предмет досліджень *стеганографічні методи приховування даних та стеганоаналіз в задачах захисту інформаційних потоків даних.*

Мета *удосконалення методу стеганографічного аналізу з метою підвищення стійкості стеганографічних систем при використанні удосконаленого стеганографічного методу.*

Вихідні дані для проведення роботи *Методи стеганоаналізу в задачах захисту інформаційних потоків даних*

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна *отримав подальший розвиток механізм визначення сучасного формату графічного файлу. З метою підвищення стійкості стегоконтейнера до атак удосконалено механізм аналізу колірних моделей зображення. Удосконалено існуючі методи приховування даних у нерухомих зображенях за рахунок методу округлення значень елементів компонент колірної моделі. Удосконалений метод стеганографічного аналізу для перевірки стійкості удосконалених стеганографічних методів.*

Практична цінність *матеріали можна використовувати при побудові стеганографічної системи передачі захищених даних каналами зв'язку та реалізації стеганографічних методів приховування даних.*

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок–кінець)
Уточнення постановки задачі	12.10.2020 – 16.10.2020
Аналіз літературних джерел	17.10.2020 – 24.01.2020
Обґрунтування вибору рішення	25.01.2021 – 12.02.2021
Збір інформації	13.02.2021 – 26.02.2021
Аналіз даних та їх класифікація	27.02.2021 – 16.04.2021
Визначення особливостей побудови стеганографічних систем та реалізація існуючих методів приховування даних	17.04.2021 – 07.05.2021
Вдосконалення існуючих стеганографічних методів	08.05.2021 – 17.05.2021
Створення програмної реалізації удосконалених методів та оцінка їх ефективності на базі	18.05.2020 – 19.05.2021

запропонованого методу стеганоаналізу	
Оформлення і друк пояснювальної записки	20.05.2021 – 25.05.2021

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект *Зниження збитків через викрадення даних через захист інформаційних потоків даних*

Соціальний ефект *Покращення технологій забезпечення захисту інформації в організаціях різних форм власності.*

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ _____
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ _____
(підпис) (прізвище, ініціали)

Дата видачі завдання: _____

Термін подання дипломної роботи до ЕК _____

УДК 004.492.2

РЕФЕРАТ

Пояснювальна записка до дипломної роботи "Методи стеганоаналізу в задачах захисту інформаційних потоків даних" складається з: 138 сторінок, 84 рисунків, 16 таблиць, 25 використаних джерел.

Об’єкт дослідження – процес приховування даних у нерухомих зображеннях при використанні стеганографічних методів в задачах захисту інформаційних потоків даних.

Мета роботи – удосконалення методу стеганографічного аналізу з метою підвищення стійкості стеганографічних систем при використанні удосконаленого стеганографічного методу.

Методи дослідження – моделювання та аналіз стеганографічних систем в задачах інформаційних потоків даних.

Наукова новизна дослідження полягає в наступному: отримав подальший розвиток механізм визначення сучасного формату графічного файлу. З метою підвищення стійкості стегоконтейнера до атак удосконалено механізм аналізу колірних моделей зображення. Удосконалено існуючі методи приховування даних у нерухомих зображенях за рахунок методу округлення значень елементів компонент колірної моделі. Удосконалений метод стеганографічного аналізу для перевірки стійкості удосконалених стеганографічних методів.

Матеріали дипломної роботи можна використовувати при побудові стеганографічної системи передачі захищених даних каналами зв’язку та реалізації стеганографічних методів приховування даних.

Ключові слова: стеганографічна система, стеганоаналіз, стеганографічний метод, найменший значущий біт, приховування даних, графічний формат, колірна модель.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ІБ – Інформаційна безпека

СЗІ – Система захисту інформації

ПЗ – Програмне забезпечення

АСУ – Автоматизована система управління

ПК – Персональний комп’ютер

APT – Advanced Persistent Threat

DNS – Domain Name System

HTTP – Hyper Text Transfer Protocol

CPU – Central processing unit

SSL – Secure Sockets Layer

TLS – Transport layer security

OS – Operating system

SMB – Server Message Block

IPS – Intrusion Prevention System

REST – Representational State Transfer

API – Application programming interface

EPP – Extensible Provisioning Protocol

ВСТУП

Актуальність. Інформаційна безпека держави чи суспільства характеризується безпосередньо, по-перше, ступенем їх захищеності, а по-друге, стійкістю важливих сфер життя у відношенні до небезпечних інформаційних загроз. Інформаційну безпеку можна характеризувати як здатність нейтралізувати такі впливи.

У сучасному світі інформаційних технологій інформація виступає як найбільша цінність. Як наслідок цього, потрібно створювати нові, більш надійні методи для захисту інформації. Щоб вирішити цю задачу використовують методи стеганографії, які дають можливість приховати не тільки інформацію, а й факт того, що вона існує при передачі каналом зв'язку.

Методи стеганографії дозволяють не лише приховано передавати дані, але й вдачно вирішувати задачі завадостійкої аутентифікації, відстеження поширення інформації мережами зв'язку, захисту інформації від несанкціонованого копіювання тощо.

Використання стеганографічних методів найбільш ефективно при вирішенні проблем захисту конфіденційної інформації. Захист конфіденційної інформації від несанкціонованого доступу є найбільш ефективним при вирішенні проблеми захисту інформації. Іншою важливою задачею стеганографії є захист авторського права. Стеганографічні методи, які спрямовані на захист від систем моніторингу і управління мережними ресурсами промислового шпигунства, дозволяють перешкоджати спробам контролю безпосередньо над інформаційним простором при проходженні інформаційного потоку через певні сервери локальних і глобальних обчислювальних мереж. Також областю використання стеганографічних систем є камуфлювання програмного забезпечення. Саме тоді, коли використання програмного забезпечення незареєстрованними користувачами є непотрібним, воно може бути закамуфльовано під певні стандартні програмні продукти, що є універсальними.

Використання методів стеганографічного захисту приводять до створення стеганографічної системи. Термін стеганографічна система – це безпосередньо об'єднання засобів і методів, що використані для створення прихованого каналу для передачі інформації. Стеганографічна система виконує вбудовування повідомлення у контейнер, передавання цього заповненого контейнера через стеганоканал та виконання декодування цього приховуваного повідомлення.

Мета роботи – удосконалення методу стеганографічного аналізу з метою підвищення стійкості стеганографічних систем при використанні удосконаленого стеганографічного методу.

Задачі роботи:

1. Здійснити оцінку засобів захисту інформації в автоматизованих системах та здійснити аналіз методів стеганографічного захисту в інформаційній безпеці;
2. Визначити особливості побудови стеганографічних систем та критерії оцінки стеганографічних методів;
3. Удосконалити стеганографічний метод приховування даних та створити програмну реалізацію удосконалених методів;
4. Запропоновати метод стеганографічного аналізу для перевірки стійкості удосконалених стеганографічних методів.

Об’єктом досліджень – це процес приховування даних у нерухомих зображеннях при використанні стеганографічних методів в задачах захисту інформаційних потоків даних.

Предмет досліджень – стеганографічні методи приховування даних та стеганоаналіз в задачах захисту інформаційних потоків даних.

Методи дослідження – моделювання та аналіз стеганографічних систем в задачах інформаційних потоків даних.

Наукова новизна дослідження полягає в наступному: отримав подальший розвиток механізм визначення сучасного формату графічного файлу. З метою підвищення стійкості стегоконтейнера до атак удосконалено механізм аналізу колірних моделей зображення. Удосконалено існуючі методи приховування даних у нерухомих зображенях за рахунок методу округлення значень елементів компонент

колірної моделі. Удосконалений метод стеганографічного аналізу для перевірки стійкості удосконалених стеганографічних методів.

Практичне значення. Матеріали дипломної роботи можна використовувати при побудові стеганографічної системи передачі захищених даних каналами зв'язку та реалізації стеганографічних методів приховування даних.

Апробація роботи. Матеріали роботи були представлені на 9 наукових конференціях та було опубліковано 6 наукових статей, з яких 3 публікації в Scopus. Основні представлені нижче**:**

1. Buchyk S., Symonychenko Y., Symonychenko A. The Method of Detection of Hidden Information Using Steganographic Methods // Information Technology and Interactions (Satellite): Conference Proceedings, December 04, 2020, Kyiv, Ukraine // Taras Shevchenko National University of Kyiv. – С. 68–71.

2. Бучик С.С., Симониченко Я.А., Симониченко А.А. Стеганографічні методи для реалізації послуг захисту інформації // Наукове видання ПРИКЛАДНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ – 2020 Збірник тез IV Міжнародної науково–практичної конференції 30 вересня 2020 року м. Київ. – С. 27–30.

3. Serhii Buchyk, Sergey Tolyupa, Yaroslav Symonychenko and Anna Symonychenko. Improvement of steganographic methods based on the analysis of image color models. // Workshop on Cybersecurity Providing in Information and Telecommunication Systems. CPITS 2021. – 28 January 2021 – Kyiv, Ukraine.

4. Сергій Бучик, Ярослав Симониченко, Анна Симониченко. Методологічні основи захисту від атак на стеганографічні системи. // IV Міжнародна науково–практична конференція "Проблеми кібербезпеки інформаційнотелекомунікаційних систем" (PCSITS) 15 – 16 квітня 2021, Київ, Україна.

5. Yudin, O., Symonychenko, Y., Symonychenko A.The Method of Detection of Hidden Information in a Digital Image Using Steganographic Methods of Analysis // 2019 IEEE International Conference on Advanced Trends in Information Theory, ATIT 2019 – Proceedings – 2019. – С. 262–266, 9030479.

6. Konakhovich, G., Symonychenko, Y., Symonychenko, A., Daradkeh, Y.I. The research of realization of hidden channel for information transmission with the use of steganographic tools // CEUR Workshop Proceedings – 2020, 2654, – С. 504–514.

7. Юдін О. К., Симониченко Я. А., Симониченко А. А. Дослідження сучасних стеганографічних методів та засобів обробки цифрових зображень // Наукоємні технології. – 2017. – №2 (34). – С. 126–133.

8. Юдін О. К., Симониченко Я. А., Симониченко А. А. Використання стеганографічних методів в задачах захисту державних інформаційних ресурсів // Наукоємні технології. – 2017. – №4(36). – С. 329–334.

9. Юдін О. К., Симониченко Я. А., Симониченко А. А. Дослідження стеганографічної системи на базі сучасних програмних стеганографічних засобів // Вісник інженерної академії України. – 2018. – №4. – С. 86–91.

10. Конахович Г. Ф., Єлізаров А. Б., Симониченко Я. А., Симониченко А. А. Реалізація послуг захисту інформації з використанням стеганографічних методів: матеріали Другої міжнародної науково–практичної конференції «Сучасні технології в науці та освіті», 5–7 березня 2019р.– Сєвєродонецьк: вид–во СНУ ім. В. Даля, 2019. – С.99–101.

11. Єлізаров А. Б., Симониченко Я. А., Симониченко А. А. Дослідження сучасних програмних стеганографічних засобів приховування інформації: матеріали Всеукраїнської науково–практичної конференції здобувачів вищої освіти й молодих учених «Комп'ютерна інженерія і кібербезпека: досягнення та інновації»., 27–29 листопада 2018р.– Кропивницький, 2018. – С.108–110.

12. Єлізаров А. Б., Симониченко Я. А., Симониченко А. А. Дослідження показників якості стеганографічної системи: матеріали IX міжнародної науково–технічної конференції ITSec–2019: Безпека інформаційних технологій, 22–27 березня 2019 р. – Київ, 2019. – С.12.

13. Конахович Г. Ф., Симониченко Я. А., Симониченко А. А. Використання методів стеганографічного захисту при реалізації послуг захисту інформації: матеріали Міжнародної науково–практичної конференції "Научная индустрия

европейского континенту”, 22–30 листопада 2018 р. – Прага. – К.:Education and Science, 2018. – №9. –С.25–28.

14. Юдін О. К., Симониченко Я. А., Симониченко А. А. Сучасні стеганографічні засоби та методи приховування інформації: матеріали Міжнародної наукової конференції ”Фундаментальная и прикладная наука”, 30 жовтня– 7 листопада 2017 р. – Шеффілд. – К.:Education and Science, 2017. – №8. –С.71–73.

15. Юдін О. К., Симониченко Я. А., Симониченко А. А. Методи стеганоаналізу в задах захисту інформаційних ресурсів держави: матеріали Міжнародної наукової конференції ”Современная европейская наука”, 30 червня – 7 липня 2018 р. – Шеффілд. – К.:Education and Science, 2018. – №9. – С.23–26.

РОЗДІЛ 1
ЗАХИСТ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

1.1. Поняття інформаційної безпеки держави

Стан інформаційної безпека (далі – ІБ) держави та суспільства характеризує ступінь її захищеності та стійкості головних сфер життєдіяльності по відношенню до небезпечних інформаційних впливів. ІБ визначається здатністю передбачати такі впливи.

Згідно Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки»: інформаційна безпека – це стан певної захищеності важливих інтересів людини, держави і суспільства, при якому запобігається нанесення певної шкоди через: неповноту та невірогідність інформації, яка використовується; негативні наслідки застосування різноманітних інформаційних технологій; негативний інформаційний вплив; несанкціонований доступ, розповсюдження та порушення цілісності, конфіденційності або доступності інформації [1].

Джерела ІБ можуть бути внутрішніми та зовнішніми. Внутрішні джерела характеризуються відсутністю історичного, соціального та політичного о досвіду життя у правових державах, що межує їх процесами практичних реалізації конституційного права та свободи громадян в інформаційній сфері. Зовнішні джерела характеризуються діяльністю іноземних політичних, економічних, військових та розвідувальних структур щодо інформаційного стану держави; діяльністю міжнародних терористичних груп; розробка концепцій інформаційних війн різними структурами; культурна експансія у відношенні до певних країн.

Важливим в сфері інформаційної безпеки держави є досягнення стану повної її захищеності, підтримка і створення відповідних інженерних та технічних потужностей організації інформаційної, яка буде відповідати дійсним і відомим загрозам. Питання забезпечення ІБ актуальні для всіх держав.

Згідно Закону України «Про інформацію», інформація – це будь–які відомості (дані), що можуть бути збережені за допомогою матеріальних носіїв або можуть бути відображені в електронному вигляді [2].

Згідно НД ТЗІ 1.1–003–99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу»: одним із важливих завдань ІБ є збереження властивостей інформації. До них належать: конфіденційність, цілісність та доступність інформації [3].

Цілісність інформації – це властивість інформації, яка передбачає те, що інформаційні дані не можуть бути модифікованими або зміненими неавторизованими користувачами або процесами.

Доступність – властивість інформації, яка передбачає те, що інформація може бути отриманою авторизованими користувачами, за основі у них відповідних повноважень, в необхідний час.

Конфіденційність інформації – властивість інформації, яка передбачає те, що інформаційні дані не можуть бути отримані неавторизованими користувачами або процесами.

Конфіденційність інформації зберігається, якщо дотримуються встановлені певні правила ознайомлення з нею. Цілісність інформації зберігається, якщо дотримуються певні встановлені правила її модифікації та зміни. Доступність інформації зберігається, якщо зберігаються можливість ознайомлення з інформацією або її модифікації відповідними до встановлених правил, упродовж певного проміжку часу.

Інформаційна безпека забезпечується тільки при комплексному використанні всіх наявних засобів захисту на всіх етапах обробки інформації, а саме системи інформаційної безпеки. Під системою інформаційної безпеки розуміється організована сукупність спеціальних органів, служб, методів і засобів, що знижують кількість уразливостей інформації та перешкоджають НСД до інформації, її розголошення або витоку.

Головна мета будь–якої системи інформаційної безпеки полягає у забезпеченні сталого функціонування об'єкта захисту:

- запобігання загрозам його безпеки;
- постійний захист законних інтересів власника інформації від протиправних посягань;
- забезпечення нормальної діяльності всіх підрозділів об'єкта.

Таким чином, інформаційна безпека – це безпосередньо захищеність інформаційного середовища. А захист інформації – це діяльність щодо уникання витоку захишенної інформації, а також несанкціонованих і навмисних дій на інформацію, тобто процес, спрямований на досягнення захищеності інформаційного середовища. Інформаційна безпека – комплексне завдання, спрямоване на забезпечення безпеки, яке реалізується впровадженням системи безпеки. Проблеми захисту інформації є багатоплановою та комплексною.

1.2. Загрози, об’єкти та суб’єкти інформаційної безпеки держави

При зберігання інформації у цифровому вигляді, виникає питання захисту інформації, адже велика кількість факторів що впливають на збереження конфіденційності даних. При організації безпечного зберігання інформаційних даних, необхідно провести повний аналіз загроз, для правильного проектування та створення системи.

Загроза інформаційній безпеці – це сукупність певних умов та факторів, які зумовлюють створення небезпеки для важливих інтересів суспільства та держави в інформаційній сфері.

Загрози інформаційної безпеки можуть бути двох основних типів – це штучні та природні загрози. Природні загрози включають пожежі, урагани, повені та інші стихійні лиха та явища, що не залежать від людського фактору. При забезпеченні інформаційної безпеки, однією з необхідних умов є обладнання всіх приміщень, в яких будуть знаходитися елементи системи (сервери, носії цифрових даних, архіви та інше). Необхідне встановлення протипожежних датчиків та призначення відповідальних осіб за протипожежну безпеку та постійної наявність протипожежних засобів. Дотримання цих правил дозволить зменшити до мінімальних рівнів загрозу втрати інформації при пожежі.

Штучні загрози діляться на навмисні та ненавмисні загрози. Ненавмисними загрозами називаються дії, що здійснює людина через необережність, неуважність або з цікавості. До таких загроз відносять інсталювання програмного продукту, який не входить до списку необхідного для роботи, і в наслідок чого може виникнути нестабільна робота системи і втрата інформації. Цей вид загроз важко піддається контролюванню, адже необхідно щоб кожний робітник усвідомлював ризик, який виникає при несанкціонованих діях.

Навмисні загрози – це загрози, які пов'язані з метою навмисного руйнування після виведення з ладу системи. До цих загроз відносяться зовнішні та внутрішні атаки. У сучасній історії є безліч прикладів реалізації навмисних внутрішніх загроз – це дії конкуруючих організацій, що вербують агентів для подальшого дезорганізування конкурентів, помста співробітників, які залишилися незадоволені заробітною платою та інше.

До зовнішніх навмисних загроз можна віднести хакерські атаки. Якщо інформаційна система пов'язана із Інтернетом, тоді для запобігання таких атак необхідно використовувати міжмережеві екрани, які можуть бути, як вбудованими в устаткування, так і реалізовані програмно.

Основні загрози ІБ розділяють на 3 групи:

- загрози спрямовані на вплив неякісної інформації (недостовірної, дезінформації) на суспільство, державу;
- загрози несанкціонованого впливу сторонніх осіб на інформаційні ресурси;
- загрози щодо інформаційних прав і свободи особистості.

Згідно НД ТЗІ 1.1–002–99, а саме «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу»: з всієї множини доступних способів класифікації загроз, найпридатнішими для аналізу є використання класифікації загроз за результатами їх впливу на інформацію, тобто порушення власитовості конфіденційності, доступності або цілісності інформації [4].

Загрози конфіденційності реалізуються при НСД до даних, програмами або каналам зв'язку. Зняття інформації може бути проведене через технічні канали

витоку інформації. При цьому використовується апаратура, яка здійснює аналіз електромагнітних випромінювань, які виникають при роботі комп'ютера. Дане знімання інформації являє собою складне технічне завдання і вимагає залучення кваліфікованих фахівців.

Несанкціоноване модифікування інформації про безпеку системи може призвести до несанкціонованих дій (невірної маршрутизації або втрати переданих даних) чи спотворення сенсу переданих повідомлень.

Загрози доступності інформаційних даних виникають при умові, якщо об'єкт не отримує доступу до певних служб або ресурсів, що виділені йому абсолютно законно. Ці загрози реалізується захопленням ресурсів, блокуванням або обмеження дій ліній зв'язку несанкціонованими об'єктами в результаті передавання з них своєї інформації або вилученням необхідної системної інформації. Дана загроза може призвести до ненадійної або не дуже гарної якості в обслуговуванні певної системі, а це означає, що є можливість впливати на достовірність та своєчасність доставки інформації.

Для захисту інформації від певних загроз створюється політика інформаційної безпеки. Політика інформаційної безпеки – це набір вимог, обмежень, правил, рекомендацій, що установлює порядок інформаційної діяльності і спрямована на досягнення та підтримку стану інформаційної безпеки. Метою політики ІБ має бути впровадження та управління системою забезпечення інформаційною безпекою, спрямованої на: захист інформаційних активів; мінімізації ризиків ІБ; створення позитивних інформаційних відносин із партнерами.

Основними завданнями ІБ є захист активів інформації від певних зовнішніх та внутрішніх загроз.

Об'єктами ІБ можуть бути: психічний стан людини; інформаційні системи абсолютно різноманітного масштабу або призначення. Соціальними об'єктами ІБ зазвичай є особистість, суспільство, державу та світове товариство.

До суб'єктів ІБ відносяться [4]:

- держава, яка здійснює свої функції відповідними органи;

- громадяни, організації або об'єднання, які володіють повноваженнями по забезпеченню ІБ у відповідності щодо законодавства.

Інформаційна безпека особистості – це стан захищеності психіки і свідомості людини від шкідливого впливу інформації: можливе маніпулювання, дезінформація і т.д.

ІБ суспільства (держави) характеризується мірою захищеності суспільства (держави) та стійкості в основних сферах життєдіяльності (науки, економіки, техносфери, військової справи, сфери управління та інше) відносно небезпечних (деструктивних, дестабілізуючих, що уражають державні інтереси та інше) інформаційних впливів. ІБ держави визначається здатністю нейтралізувати дані впливи.

Концепція інформаційної безпеки держави – систематизована сукупність даних про інформаційну безпеку держави та шляхи забезпечення інформаційної безпеки держави.

В концепції інформаційної безпеки держави проводяться:

- класифікація шкідливих факторів та інформаційних загроз безпеці держави;
- обґрунтування основних положень з організації забезпечення ІБ;
- розробки пропозиції щодо способів і форм забезпечення ІБ.

1.3. Сучасний стан нормативно–правової бази інформаційної безпеки в Україні

Із становленням суверенності української держави, реформуванням певних сфер суспільного життя, постала проблема створення та впровадження нових систем захисту інформації (далі – ЗІ) зокрема в автоматизованих системах (далі – АС) та законодавчого регулювання інформаційних відносин у сфері охорони таємниць.

Конституція України, що стала основою для побудови демократично–правової держави, враховує загальносвітові тенденції інформатизації суспільства. Таким чином, ряд її статей визначають забезпечення ІБ, як одну з важливих функцій держави та має стати основою інформаційного законодавства.

Захист державної таємниці є складовою для національної безпеки України. Тому, при превалюванні особливих інтересів держави, чинне законодавство має забезпечувати їх захист, устаткування інформаційного суверенітету України, її прав на встановлення особливих порядків користування інформацією з обмеженим доступом, важливішою складовою якої є державні таємниці.

В інформаційному просторі дана інформація займає незначну частку та стосується чітких сфер державної діяльності – економіки, оборони, зовнішніх відносин, державної безпеки та охорони правопорядку, що указано у шостій статті Закону “Про державну таємницю” [5].

Закон України "Про інформацію" установлює загальні правові основи одержання, поширення, використання і збереження інформації [2].

Відповідно до даного закону: інформація – це документовані або привселюдно оголошені певні відомості щодо події або явища, які відбуваються в товаристві або навколишньому природному середовищі.

Закон визначає правові відносини особистості на інформацію в різних сферах життя, а також систему інформатизації, її джерела, зазначає статус учасників даних інформаційних відношень, визначає регулювання доступу до інформації і забезпечує охорону даної інформації, захищає товариство від помилкової або хибної інформації. Дія даного закону поширюється на стан інформаційних відношень, які виникають в різних сферах держави при одержанні, поширенні, використанні і збереженні інформаційних даних. Суб'єктами інформаційних відносин є громадяни держави, безпосередньо держава, а також її громадяни, їхні міжнародні організації та особи що не мають громадянства. Для задоволення потреб в інформаційній діяльності створюються певні інформаційні служби, мережі, системи, бази і банки даних. Даний закон передбачає створення єдиної системи охорони інформації.

Основними видами інформації, відповідно до закону, є: масова інформація; статистична інформація; інформація щодо діяльності державних органів влади; інформація про особистість; правова інформація; інформація довідкового характеру; соціологічна інформація.

Мета Закону України "Про захист інформації в автоматизованих системах" – це встановлення основних аспектів регулювання правових відношень щодо захисту інформації в автоматизованій системі при умові дотримання прав власності громадянина України і юридичної особи на інформацію або право доступу до неї, прав власника інформації при її захисті, а також установленого сьогоднішнім чинним законодавством певних обмежень на доступ до інформаційних даних [6].

Чинність даного Закону має поширення на будь–яку інформацію, яка оброблюється в АС. У даному Законі основні терміни використовуються в наступних значеннях.

Автоматизована система – система, яка здійснює автоматизовану обробку даних (інформації), до її складу належать технічні засоби обробки, а також методи та програмне забезпечення.

Інформація в автоматизованих системах – сукупність всіх даних та програм, що застосовуються в АС незалежно від методу їх фізичного і логічного уявлення.

Захист інформації – це об’єднання організаційно–технічних методів і правових норм для подальшого попередження заподіяння збитків інтересів власників інформації або АС і осіб, що використовують інформацію.

Порядок проведення обігу інформацією з обмеженим доступом врегульовує ст.30 Закону України «Про інформацію». Така інформація своїми правовими режимами поділяється на таємну та конфіденційну.

Конфіденційна інформація – відомості, що перебувають у володінні, розпорядженні або користуванні окремих осіб і поширюється за їх відповідним бажанням до передбачених умов.

Питання захисту інформації в інформаційних, інформаційно–телекомунікаційних та телекомунікаційних системах регулює Закон України «Про захист в інформаційно–телекомунікаційних системах».

Закон України «Про Концепцію Національної програми інформатизації» має зміст, що включає певну характеристику сучасного інформаційного стану, стратегічних цілей та основних принципах інформатизації, очікувані наслідків її реалізації. Має визначення основних напрямків інформатизації в Україні [7].

Закон України «Про електронні документи та електронний документообіг» містить перелік основних умов електронного документообігу та детального описання кожного з його етапів, зазначено порядок організування електронного документообігу та визначено обов'язки суб'єктів і їх права [8].

Правовий статус електронно–цифрового підпису, особливості його застосування та призначення встановлено Законом України «Про електронний цифровий підпис» [9].

Отже, забезпечення інформаційної безпеки державною політикою визначає основні напрямки в діяльності органів державної влади, що закріплює права і зобов'язання щодо захисту інтересів держави, які ґрунтуються на дотриманні певного балансу інтересів суспільства і держави.

Державна політика забезпечення ІБ України ґрунтується на таких засадах: дотримання законодавства України, Конституції України, загальновизнаних принципів міжнародного права для здійснення діяльності щодо забезпечення ІБ України; відкритості при реалізаціях функцій органами державної влади України та суспільних об'єднань, що передбачають інформування суспільства про їх діяльність із огляду на певні обмеження встановлених законодавством України; правової рівноправності усіх учасників інформаційного процесу незалежно від їхнього соціального, політичного та економічного статусу, що базується на конституційному праві суспільства на вільний пошук, передачу, одержання, виробництво і розповсюдження інформації довільними законними способами; пріоритетного розвитку вітчизняних інформаційних та телекомунікаційних технологій, виробництво програмних і технічних засобів, які здатні забезпечити вдосконалення телекомунікаційних мереж, підключенням їх до інформаційних мереж з метою повного забезпечення та підтримання інтересів України.

Правове забезпечення ІБ України повинно ґрунтуватися на дотриманні певних принципів законності, балансу інтересів суспільства та держави в інформаційній сфері:

- дотримання певних принципів законності при вирішенні будь–яких конфліктів, які виникають в інформаційній сфері, вимагаючи від органів державної

влади неухильного керування законодавчим та іншим нормативно–правовим актом, який регулює відносини у даній сфері;

- дотримання принципів балансування державних інтересів в інформаційній сфері передбачає насамперед законодавче підтвердження пріоритету інтересів в різних галузях життя і діяльності сучасного суспільства, а також при використанні форм суспільного контролю діяльності органів влади.

1.4. Класифікація автоматизованих систем обробки інформації

На сьогоднішній день автоматизовані системи грають ключову роль у забезпеченні ефективного функціонування інформаційних систем. Під АС слід розуміти організаційно–технічну систему, яка реалізує інформаційну технологію та об’єднує ОС, фізичне середовище, персонал та інформацію, що обробляється.

Згідно чинного НД ТЗІ 2.5–005–99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від НСД», за сукупністю характеристик АС поділяються на три класи [10].

Клас «1» – одномашинний комплекс (однокористувачевий), який виконує обробку інформації певних категорій конфіденційності.

Особливостями даного класу є :

- в довільний момент часу з даним комплексом може працювати лише один із користувачів, хоча осіб, що мають права доступу до комплексу, може бути кілька, але вони всі повинні мати однакові права розмежування доступу до даної інформації;
- технічні засоби або носії інформації відносяться до однієї категорії та можуть використовуватися для зберігання або редагування всієї інформації.

Узагальнюючи визначення можна зробити висновок, що АС класу «1» – це 1 комп'ютер, який не має підключення до локальної мережі або Інтернету і яким одночасно може користуватися тільки 1 користувач.

Клас «2» – це локалізований багатомашинний комплекс (багатокористувачевий), що виконує обробку конфіденційної інформації. Відмінністю від АС класу «1» є одночасна наявність користувачів із різними

повноваженнями до технічних засобів, що можуть одночасно проводити обробку інформації різних ступенів обмеження.

Клас «3» – це розподілений багатомашинний комплекс (багатокористувачевий), що проводить обробку конфіденційної інформації. Відмінністю від АС класу «2» є необхідність передавати інформацію через певне незахищене середовище, або існування певних вузлів, що реалізують політику безпеки.

1.5. Типові засоби захисту інформації в автоматизованих системах

Використання певної автоматизованої системи при зберіганні, обробці або передачі інформації призводить до часткового підвищення актуальності проблеми, пов'язаної із її захистом. Згідно діючого Закону України «Про захист інформації в автоматизованих системах», оброблення інформації в АС – це вся сукупність операцій, яка здійснюються за допомогою технічних та програмних засобах, що включають обмін по каналах передачі інформаційних даних [11].

Де-факто, будь–яка АС може бути об'єктом інформаційної атаки, що може бути зіставлена як сукупність дій порушника, спрямована на спотворення процесів обробки інформації або одного з трьох властивостей інформації – доступності, цілісності та конфіденційності. В результаті порушення даних властивостей інформації порушник тим самим може порушити процеси обробки інформації, які грунтуються на певних інформаційних ресурсах, які виступали об'єктом певної атаки.

Для здійснення інформаційної атаки атакуючому потрібно використовувати певну вразливість АС. Вразливість є причиною виникнення інформаційних атак. Наявність слабких місць в АС може бути обумовлено різними чинниками, починаючи з простої недбалості співробітників, і закінчуючи навмисними діями порушників. Вразливість може бути присутня в програмно–апаратному та організаційно–правовому забезпеченні інформаційної системи. Важлива частина уразливостей організаційно–правового забезпечення зумовлена недосконалістю нормативних документів, що стосуються питань інформаційної безпеки.

Уразливості програмно–апаратного забезпечення мають змогу бути в програмних чи апаратних складових робочих станцій користувачів автоматизованої системи, серверів, або певного комунікаційного устаткування, а атакож каналів зв'язку автоматизованої системи.

Наслідки, що зроблені інформаційними атаками, можуть по–різному розглядатися і залежать від певної ситуації. Такі атаки безпесередньо можуть мати вплив на апаратне або прикладне чи загальносистемне програмне забезпечення, і на інформацію, яка обробляються та зберігається в автоматизованій системі.

На сьогоднішній день існує створюється велика кількість технічних та організаційних засобів захисту, що використовуються для того, щоб захистити від атак на інформацію – це і організаційні, і технічні. Безпосередньо, організаційні засоби мають можливість постійного створення і впровадження в установах чи організаціях нормативно–правових актів, які регулюють вимоги до інформаційної безпеки. А відповідно технічні реалізовані через відповідні апаратних або програмних комплексів. Найпоширенішими засобами захисту інформації слід виділити: криптографічний захист інформації, розмежування доступу користувачів до ресурсів АС, засоби виявлення атак, засоби антивірусного захисту та міжмережевий екран.

Засоби криптографічного захисту інформації представляють собою обчислювальну техніку, яка здійснює перетворення інформації криптографічного характеру для забезпечення конфіденційності інформації та контролю її цілісності. Захист інформації може відбуватися протягом передавання по певним каналам зв'язку або ж в процесі обробки та зберігання інформації на вузлах автоматизованої системи.

Засоби розмежування доступу призначені для захисту від НСД до інформаційних активів системи. Розмежування доступу здійснюється засобами захисту інформації на основі процедур ідентифікації, автентифікації та авторизації користувачів, які хочуть отримати доступ до інформаційних аткивів автоматизованої системи. Під ідентифікацією слід розуміти процедуру присвоєння ідентифікатора об’єкту або встановлення відповідностей між об’єктами і їх

ідентифікаторами. Автентифікація – це процедура перевірки відповідності отриманого ідентифікатора об’єктам комп’ютерної системи на ознаки належності його даному об’єкту. Авторизація – це надання повноважень або встановлення відповідностей між повідомленнями і його джерелом.

Системи виявлення атак є спеціалізованими програмними або програмно–апаратними комплексами, що мають призначення для знаходження інформаційних атак на компоненти АС з використанням збору чи аналізу інформації про події, відбуваються в системі.

Відповідно засоби антивірусного захисту застосовуються для знаходження і руйнування шкідливого програмного забезпечення, присутнього в АС. Міжмережеві екрани реалізують методи контролю за інформацією, що надходить та виходять з АС, та відповідної захищеності АС з використанням фільтрування інформації через певні критерії, що задаються адміністратором. За допомогою фільтрування міжмережеві екрани забезпечують захист від атак на мережу через видалення з інформаційного потоку саме тих пакетів даних, що становлять певну небезпеку для АС.

1.6. Роль методів стеганографічного захисту інформації

На сучасному етапі всебічного розвитку інформаційних технологій, найбільшою цінністю є інформація. Таким чином, виникає необхідність створення більш надійніших методів захисту інформації. При вирішенні даної задачі доречно використовувати стеганографічні методи, які дають можливість сховати не тільки інформацію, але також і той факт, що вона наявна безпосередньо при передачі каналом зв’язку [12].

Методи стеганографії дозволяють не лише приховано передавати дані, а також вдало розв’язувати задачі завадостійкої аутентифікації, і захисту інформації при несанкціонованому копіювання, відстеження розповсюдження інформації по мережам зв’язку тощо. На сучасному етапі стеганографічні методи активно застосовуються для вирішення таких завдань:

- захист конфіденційності інформації від НСД;

- захист авторського права щодо інтелектуальної власності;
- подолання системи моніторингу та управління ресурсами мережі;
- камуфлювання програмного забезпечення;
- утворення прихованого від законного користувача каналу витоку інформації.

Використання стеганографічних методів найбільш ефективні при вирішенні проблем захисту конфіденційної інформації. Захисту конфіденційної інформації від несанкціонованого доступу є найбільш ефективним при вирішенні проблеми захисту секретної інформації. Ще однією важливою метою стеганографії є захищеність авторського права. Графічні зображення і на них наноситься певна мітка, яка є невидимою для людини, але розпізнається спеціалізованим програмним забезпеченням. Стеганографічні методи, які спрямовані на захист від систем моніторингу і управління мережними ресурсами промислового шпигунства, дозволяють перешкоджати спробам контролю безпосередньо над інформаційним простором при проходженні інформаційного потоку через певні сервери локальних і глобальних обчислювальних мереж. Також областю використання стеганографічних систем є камуфлювання програмного забезпечення. Саме тоді, коли використання програмного забезпечення незареєстрованними користувачами є непотрібним, воно може бути закамуфльовано під певні стандартні програмні продукти, що є універсальними.

Використання методів стеганографічного захисту приводять до створення стеганографічної системи. Під стеганографічною системою слід розуміти об'єднання методів і засобів, що використані для створення прихованого каналу для передачі інформації. Стеганографічна система виконує вбудовування повідомлення у контейнер, передавання цього заповненого контейнера через стеганоканал та виконання декодування цього приховуваного повідомлення. В якості контейнера, для приховування та передавання прихованого повідомлення, можуть використовуватися нерухомі зображення, текст, аудіозаписи та ін.

Цифрова стеганографія (Рисунок 1.1) – заснована на приховуванні або вбудовуванні додаткових інформаційних даних в цифрові об'єкти, забезпечуючи при цьому їх мінімальне змінення. Здебільшого, такі об'єкти мають бути

мультимедійними і створення спотворень, які знаходяться безпосередньо нижче порога чутливості звичайної людини, не призводить до їх помітних змін.

Рисунок 1.1 - Цифрова стеганографія

Проведення приховування даних в просторовій області може здійснюватися безпосередньо за допомогою наступних методів: методом заміни найменш значущого біта, який полягає в безпосередній заміні останніх бітів в контейнері на біти приховуваного повідомлення; методом псевдовипадкового інтервалу, який полягає у довільному розподілі бітів прихованого повідомлення по контейнеру, в результаті чого, відстань між вбудованими бітами визначається псевдовипадково; методом блокового приховування, який полягає в тому, що зображення–оригінал розбивається на l_M неперетинних блоків $\Delta_i (1 \le i \le l_M)$ певної довільної конфігурації, і безпосередньо для кожного обчислюється біт парності $b(\Delta_i) : b(\Delta_i) = \sum_{J=\Delta_i}^{\mathrm{mod}2} LSB(C_J)$.

При виконанні підрахунку у кожному блоці виконується приховування 1–го засекреченого біту M_i. Якщо біт парності $b(\Delta_i \neq M_i)$, то здійснюється деяке інвертування одного з НЗБ блоку $\Delta_i d$ в результаті чого $b(\Delta_i = M_i)$ [14].

1.7. Актуальність та постановка задачі

Для ІБ держави є важливим досягнення стану захищеності, створення та підтримка відповідних інженерних і технічних потужностей інформаційної організації, які відповідають реальним та потенційним загрозам. Дане питання забезпечення ІБ актуальні певною мірою для всіх держав.

Захист інформації – це безпосередньо діяльність проти витоку захищеної інформації, а також несанкціонованих і навмисних дій на інформацію, тобто процес, спрямований на досягнення захищеності інформаційного середовища. Інформаційна безпека – комплексне завдання, яке спрямоване на забезпечення певної безпеки, що реалізується впровадженням системи безпеки. Проблеми захисту інформації є багатоплановими і комплексними.

На сучасному етапі всебічного розвитку інформаційних технологій найбільшою цінністю є інформація. Таким чином актуальним питання є створення нових, надійніших методів захисту інформаційних даних. При вирішенні даної задачі використовується стеганографічні методи, які дозволяють приховувати інформацію та факт її передачі каналом зв’язку [14].

Використання методів стеганографічного захисту приходить до створення стеганографічної системи. Стеганографічна система – це об'єднання методів і засобів, що використані для створення певного прихованого каналу для передачі інформації. Стеганографічна система виконує вбудовування повідомлення у деякий контейнер, здійснює передавання цього заповненого контейнера через стеганоканал, а також декодування цього приховуваного повідомлення. Метою та задачею роботи є підвищення ефективності та стійкості стеганографічних систем при використанні удосконалених стеганографічних методів на базі методів стеганоаналізу [12].

Об’єктом досліджень є існуючі стеганографічні методи приховування даних у нерухомих зображеннях при проведенні моделювання та аналізу стеганографічних систем передачі захищених даних.

Наукова новизна дослідження полягає в визначенні оптимального формату графічного файлу та колірної моделі зображення, удосконалення існуючих методів приховування даних у нерухомих зображеннях. Таким чином, стеганографічні методи найбільш ефективні при вирішенні проблем захисту конфіденційної інформації.

Висновки по розділу 1

В даному розділі шляхом аналізу літературних джерел наведено узагальнене визначення поняття інформаційної безпеки, визначено існуючі напрямки реалізації загроз для інформаційної безпеки. Таким чином, головне завдання інформаційної безпеки – це захист інформаційних ресурсів від певних зовнішніх та внутрішніх навмисних або ненавмисних загроз. Були розглянуті автоматизовані системи та визначена їх роль у забезпеченні ефективного функціонування інформаційних систем. Це дозволило безпосередньо перейти до забезпечення інформаційної безпеки автоматизованих систем. Де-факто, будь–яка автоматизована система може бути об'єктом інформаційної атаки, що спрямована на спотворення процесу обробки інформації або одного з трьох властивостей інформації – конфіденційності, цілісності та доступності.

Отримані результати дозволяють визначити пріорітетні напрямки, за якими можливо використання стеганографічних методів для захисту інформації в автоматизованих системах. Таким чином, стеганографічні методи найбільш ефективні при вирішенні проблем захисту конфіденційної інформації.

Використання методів стеганографічного захисту приходить до створення стеганографічної системи. Стеганографічна система – це об'єднання методів і засобів, що використані для створення певного прихованого каналу для передачі інформації. Стеганографічна система виконує вбудовування повідомлення у деякий контейнер, здійснює передавання цього заповненого контейнера через стеганоканал, а також декодування цього приховуваного повідомлення.

РОЗДІЛ 2
ОСОБЛИВОСТІ ПОБУДОВИ СТЕГАНОГРАФІЧНИХ СИСТЕМ ТА ПРИНЦИП СТЕГАНОАНАЛІЗУ

2.1. Базові методи захисту інформації в автоматизованих системах класу 3

В наш час інформація стає найдорожчим ресурсом. Оперативне використання інформації надає перевагу над конкурентами, що не мають її, конфіденційна інформація, яка потрапила до зловмисників має можливість дійсно вам нашкодити (наприклад, якщо про вашу новітню технологію дізнаються конкуренти та використають її, уникнувши витрат на удосконалення та дослідження; або ваші подальші плани стануть відомі і суперники вживуть швидших заходів).

Для полегшення обробки інформації використовують ПК, які приєднані до мережі Інтернет. Використання комп'ютерів та Інтернету ввійшли майже у всі аспекти діяльності суспільства: від укладення ділових договорів до особистих відносин у суспільстві, від придбання товарів через глобальну мережу в Інтернет–магазині до навчання. Інтегрування комп'ютерів значно спростило діяльність людини, які виконують за неї машинну роботу. Глобальна мережа Інтернет викликала зменшення обсягу часу на пошук певної необхідної інформації при використанні пошукових серверів [16].

Використання сучасних новітніх інформаційних технологій спричинило виникнення проблеми забезпечення безпеки обробляючої в ній інформації. Таким чином, створилась можливість витоку інформаційних даних, порушення цілісності інформації або її блокування. Витік конфіденційної інформації, що становить державну або передбачену законом державну таємницю, яка є власністю держави, – одна з головних можливих загроз для стану національної безпеки держави в інформаційній сфері. Захист інформації – це об’єднання організаційних та технічних заходів, певних правових норм при запобіганні заподіяної шкоди щодо інтересів власника інформації або автоматизованої системи, які використовують інформацію

(частина 4 статті 1 Закону України "Про захист інформації в автоматизованих системах") [11].

Одним з основних методів захисту конфіденційної інформації є метод криптографічного захисту, що безпосередньо виражається у прихованні змісту повідомлення через шифрування за певним алгоритмом, який має зробити повідомлення незрозумілим інших людей. Але такий метод захисту є не досить ефективним з двох причин.

Перше, зашифрована інформація більш–менш стійкою криптосистемою є недоступною (це час, який визначає стійкість криптосистеми) для ознайомлення без знання певного алгоритму, а також ключа. Як наслідок, силові структури певних країн накладають адміністративні санкції проти такої "стійкої криптографії", не дозволяючи використання криптографічних засобів юридичними та приватними особами без ліцензії.

Друге, потрібно звернути увагу на те, що криптографічний захист має змогу захистити тільки зміст конфіденційної інформації. А наявність певної зашифрованої інформації може привернути увагу зловмисника, який, оволодівши криптографічно захищеним файлом, може здійснити дешифрування цих даних. У такому випадку проблема інформаційної безпеки звону вертається до стійкості криптографічного кодування.

На противагу описаному вище, стеганографічний захист здійснює приховання самого факту існування певних конфіденційних відомостей при їх передачі, обробці чи зберіганні. Приховування факту існування – це не тільки не можливість знаходження в перехопленому повідомленні наявності іншого повідомлення, що є прихованим, а також взагалі зробити неможливим викликання будь–яких підозр. Ситуація неможливості неавторизованого витягування інформації при цьому відступає на задній пріоритет і вирішується додатковим використанням певних стандартних криптографічних методів. Спільною рисою стеганографічних методів є те, що повідомлення, яке приховане розміщується в певний не дуже приваблюючий увагу об’єкт (контейнер), який потім відкрито транспортується (пересилається) адресату.

Використання методів стеганографії для приховування повідомлення значно зменшує ймовірність виявлення прихованого каналу передачі даних або факту передавання повідомлення. При використанні криптографічного захисту, повідомлення має додатковий, рівень захисту. У теперішній час із стрімким розвитком обчислювальної техніки та використанням нових каналів передавання інформації з'являються нові стеганографічні методи В їх основі лежать особливості обробки інформації комп'ютерними системами, обчислювальних мережах та інше. Це надає можливість говорити про виникнення нового напрямку – використання методів комп'ютерної стеганографії [17].

На сьогоднішній день автоматизовані системи грають основну роль при забезпеченні ефективного функціонування інформаційних систем. Під АС слід розуміти організаційно–технічну систему, яка реалізує інформаційну технологію та фізичне середовище, об’єднує обчислювальну систему, персонал і інформацію, що обробляється. За сукупністю характеристик АС виділено 3 ієрархічні класи АС [10].

Клас «1» – одномашинний комплекс (однокористувачевий), який виконує обробку інформації певних категорій конфіденційності.

Клас «2» – це локалізований багатомашинний комплекс (багатокористувачевий), що виконує обробку конфіденційної інформації. Відмінністю від АС класу «1» є одночасна наявність користувачів із різними повноваженнями до технічних засобів, які можуть одночасно проводити обробку інформації різних ступенів обмеження.

Клас «3» – це розподілений багатомашинний комплекс (багатокористувачевий), що проводить обробку конфіденційної інформації. Відмінністю від АС класу «2» є необхідність передавати інформацію через якесь середовище, яке є незахищений або наявність вузлів, реалізації політики безпеки.

2.2. Особливості побудови стеганографічних систем

На сьогоднішній день виділяють три напрямки використання стеганографії: приховування даних, цифрові водяні знаки та заголовки. Приховування даних, які

мають достатньо великий обсяг, виокремлює суворі вимоги до стеганографічного контейнера: розмір фіксованого контейнера в декілька раз перевищувати об’єм вбудованих даних. Цифрові водяні знаки (далі – ЦВЗ) використовуються при захисті авторського або майнового права на цифрові зображення чи інші оцифровані твори. Основними вимогами, що висуваються до таких вбудованих даних – це надійність та стійкість до спотворень. ЦВЗ має невеликий обсяг, проте, із врахуванням викладених вище вимог, при їх вбудовуванні використовуються більш складніші методи, ніж при вбудовуванні просто повідомлення чи заголовка. Заголовки, використовується для маркування зображень що зберігаються у великих електронних сховищах цифрових зображень та іншої мультимедії. В даному випадку методи стеганографії використовуються для впровадження ідентифікатора заголовка та інших індивідуальних ознак мультимедійного файлу.

Основними положеннями сучасної комп'ютерної стеганографії є наступні [18]:
1. Методи приховування мають дбати про автентичність і цілісність файлу.
2. Враховується, що атакуючому відомі всі можливі стеганографічні методи.
3. Безпека методів має основу на збереженні стеганографічним перетворенням головних властивостей файлу, який передається відкрито, при внесенні до нього певного секретного повідомлення і деякої невідомої атакуючому інформації – ключа.
4. Також якщо приховування повідомлення стало відомим атакуючому через спільника, видобування цього секретного повідомлення являє досить складну = задачу.

Із збільшенням ролі комп'ютерних мереж стає дуже важливим значення стеганографії. Аналізування інформаційних джерел комп'ютерної мережі Internet дає модливість зробити певний підсумок, про те, що у сучасному світі стеганосистеми дуже активно використовують для вирішення певних завдань [18]:

1. Захист конфіденційної інформації від несанкціонованого доступу;
2. Обхід систем моніторингу, а також управління мережевими ресурсами;
3. Приховування програмного забезпечення;
4. Захищеність авторського права на певні види інтелектуальної власності.

Реалізація стеганографічного захисту призводить до створення стеганографічної системи. Під стеганографічною системою слід розуміти об'єднання методів та засобів, що використовують для створення прихованого каналу для передачі інформації. Стеганографічна система виконує вбудовування повідомлення у контейнер, передавання заповненого контейнера стеганоканалом та декодування прихованого повідомлення. В якості контейнера може використовуватися будь–яка інформація: текст, звук, зображення, відео та ін. Узагальнену структурну схему стеганосистеми зображено на Рисунок 2.1.

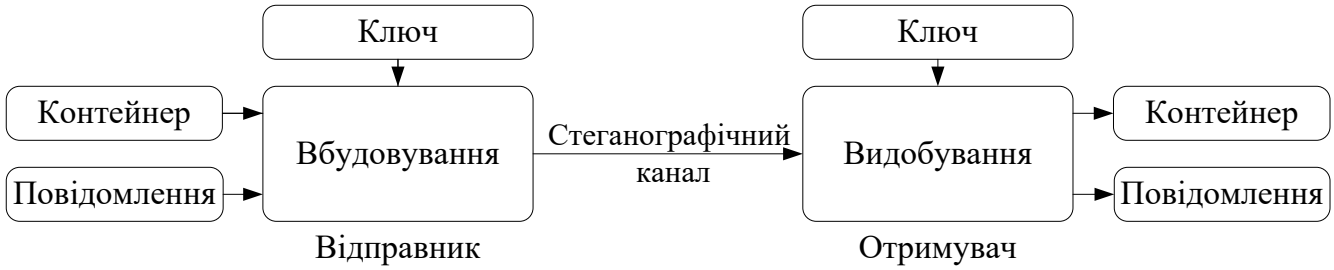


Рисунок 2.1. Структурна схема стеганографічної системи

При побудові стеганосистеми повинні бути враховувані наступні положення [19]:

- порушник має повне уявлення про стеганосистему та деталях її реалізації. При цьому, єдиною інформацією, що залишається невідомою потенційному порушникові, є ключ, за допомогою якого можливо встановити факт присутності і приховане повідомлення;
- якщо порушник дізнається про факт існування прихованої інформації, це не повинно надати йому можливості видобувати подібні повідомлення з інших інформаційних даних, поки зберігається ключ;
- потенційний порушник повинен бути позбавлений будь–яких переваг при розпізнаванні або розкритті змісту прихованих повідомлень.

Головними поняттями стеганографії є повідомлення і контейнер. Безпосередньо, повідомлення – це інформація, наявність якої необхідно приховати. Контейнер – це будь–яка інформація, що використовується для приховування

повідомлення. Порожній контейнер (контейнер–оригінал) – контейнер, що не містить повідомлення. Заповнений контейнер (стеганоконтейнер або контейнер–результат) – контейнер, що містить приховану інформацію.

Є два головних типи контейнерів: потоковий і фіксований. По-перше, потоковий контейнер – це послідовність біт, що безперервно змінюється. Повідомлення вбудовується в реальному часу, так що невідомо заздалегідь, чи вистачить області приховування даних контейнера для передачі всього повідомлення. Особливістю потокового контейнера є неможливість визначення початку або кінця [20].

При використанні фіксованих контейнерів, відправник заздалегідь знає розмір контейнера і може обрати приховані біти у відповідній псевдовипадковій послідовності.

Контейнер може бути випадковим або нав’язаним. Обраний контейнер залежить від повідомлення, що вбудовується у контейнер. Такий контейнер більш характерний для стеганографії. Але нав’язаний контейнер -це ситуація, коли особа, що надає цей контейнер, підозрює про можливість стеганографічного каналу. Але практично, найбільш часто мають справу з певним випадковим контейнером. При підвищенні надійності стеганографічної системи, необхідно прагнути якнайменше проводити зміни в структурних ознаках контейнера.

Для підвищення надійності стеганосистеми, вбудовування повідомлення в певний контейнер може здійснюватися з використанням ключа. Ключ – це послідовність біт, що визначає порядок внесення повідомлення до контейнера. Залежно від кількості рівнів захисту у стеганосистеми може бути один або кілька ключів. Приховування повідомлення виконується відповідно до ключа в ті елементи контейнера, спотворення яких не призводить до суттєвих змін контейнера.

Стеаганоситема використовує ключі двох типів: секретні та відкриті. Якщо в стеганосистемі використовується секретний ключ, тоді він повинен створюватися до початку обміну повідомленням, або переданий за допомогою захищеного каналу. Стеганосистема, яка використовує відкритий ключ, повинна влаштовуватися таким

чином, щоб не було можливим отримати закритий ключ. При цьому, відкритий ключ можна передавати по незахищеному каналу [20].

Передавання стеганоконтейнера від відправника до отримувача здійснюється по стеганографічному каналу передачі. Стеганографічний канал або стеганоканал – канал передавання контейнера–результату.

Будь–яка стеганографічна система повинна відповідати таким вимогам [21]:

- властивості контейнера повинні модифікуватися таким чином, щоб не було можливим виявити зміни при його візуальному контролі. Дана вимога визначає ступінь якості приховування повідомлення: для забезпечення надійного проходження стеганографічного контейнера по каналам зв'язку, він не повинен привернути увагу порушника;
- стеганографічний контейнер повинен бути стійким до стеганографічних спотворень. В процесі передачі зображення можлива різна трансформація: зменшення або збільшення, перетворення в інший формат і т. д.;
- при збереженні цілісності передаючого повідомлення необхідне подальше використання завадостійкого кодування;
- при підвищенні надійності системи, повідомлення має бути продубльоване.

2.2.1. Типи стеганографічних систем

Розрізняють чотири типи стеганографічної системи: безключові, системи з відкритим ключем, системи із секретним ключем, а також змішані стеганосистеми.

Безключові системи характеризуються відсутністю використання ключа для вбудовування та видобування повідомлення з контейнеру. Надійність безключових стеганосистем залежить лише від таємності стеганографічних перетворень.

У системі із використанням секретного ключа використовується певний ключ, який повинен бути визначений до початку обміну повідомленням, або переданий за допомогою захищеного каналу. Даний тип систем припускає наявність захищеного каналу обміну ключами.

У системі з відкритими ключами використовується два ключа, які розрізняються наступним чином, що за допомогою обчислень не є можливим виведення одного ключа з іншого. Таким чином, відкритий ключ може передаватися по незахищеному каналу зв'язку, секретний необхідно зберігати в таємниці. Таким чином, відкритий ключ використовується при вбудовуванні повідомлення, а секретний – для її видобування.

Змішані стеганографічні системи характеризуються використанням декількох засобів захисту, наприклад, використання відкритих системи із особливостями криптографічних систем з відкритим та/або секретним ключем. Більшість систем такого типу підвищують надійність передавання повідомлення стеганографічним каналом [22].

2.2.2. Протоколи стеганографічних систем

Для досягнення цілей стеганографії важливе місце займають протоколи. Протокол – це “дії, які вживаються декількома сторонами, призначені для вирішення якоїсь задачі”. Є можливість розробки ефективного алгоритму для приховання інформації, але якщо його неправильно застосувати не досягти поставленної мети. Протокол та алгоритм – це певна послідовність дій. Різниця між ними у тому, що до протоколу мають бути залучені дві або більше сторін. Припускається таке, коли учасники зобов’язуються тримати дотримання протоколу. Протокол складається з певних кроків. На кожному кроці є виконання певних дій, наприклад, проведення певних обчислень, або у здійснення певних дій [21].

Стеганографічні системи бувають із секретним ключем та з відкритим ключем. У перших використовують один деяких ключ, що має бути відомий абонентам ще до початку такого прихованого обміну секретними повідомленнями (або ж пересилається захищеним каналом під час такого обміну). А у системах із відкритим ключем для вбудовування і видобування інформації, що є прихованою використовують різні ключі, а саме відкритий і секретний.

Стеганографічні системи бувають чотирьох типів: системи з відкритим ключем, безключові стеганосистеми, змішані стеганосистеми та системи із секретним ключем.

При використанні безключових стеганосистем відсутня потреба в жодних додаткових даних, таких як стеганоключ. Щоб підвищити безпеки безключових систем, на початку стеганографічного приховування потрібно виконати криптографічне шифрування приховуваної інформації. Цей метод збільшує захищення процесу зв'язку, так як ускладнює виявлення наявності прихованого повідомлення. Але так звані "сильні" стеганосистеми здатні виконувати функції, які на них покладені, без такого попереднього криптографічного захисту певного вбудованого повідомлення.

Стеганосистема із відкритим ключем безпосередньо не має потреби в додаткових каналах певного ключового обміну. Щоб вони функціонували потрібно мати два стеганоключі: секретний, що потрібно зберігати в таємниці, а другий – відкритий, що може зберігатися в певному доступному місці. Відкритий ключ використовується безпосередньо для вбудовування повідомлення, а секретний тільки для дешифрування.

Праткична перевага надається звичайно безключовим стеганосистемам, хоча вони можуть бути миттєво розкриті у випадку, коли атакуючий знає про метод стеганоперетворення, який застосовується. Безключові системи часто використовують певні особливості криптографічних систем з відкритим і/або певним секретним ключем [23].

2.3. Растрові зображення та основні характеристики стеганоконтейнера

Комп'ютерна графіка – двовимірні або тривимірні зображення, що створюються, оцифровуються, обробляються та відображаються певними засобами обчислювальної техніки, включаючи програмні і апаратні засоби. Рухома графіка називається комп'ютерною анімацією. Для проведення відображення графіки використовуються монітори, принтери, плотери тощо [24].

Робота з графікою – один з популярніших напрямків використання ПК. У функціонування будь–якого підприємства виникає певна необхідність в постійній подачі рекламних оголошень в ЗМІ або випуску рекламного буклету.

Розрізняють три види комп. графіки: растрова, векторна і фрактальна. Вони розрізняються принципами формування структури зображення при його відображенні на екрані пристрою або друці на папері [24].

Растрова графіка використовується при розробці мультимедійних і поліграфічних видань. Такі ілюстрації, виконуються засобами растрової графіки, за допомогою спеціалізованих програм. Найчастіше для даної реалізації використовують відсканованої ілюстрації, підготовлені художниками на паперах, або фотографіях. Останнім часом, для реалізації вводу растрових зображень в ПК використовують цифрові камери.

Більшість графічних редакторів, що спрямовані для роботи з растровими елементами ілюстраціями, які орієнтовані не тільки на створення зображення, а на їх обробку. Поки що використовуються тільки растрові ілюстрації. Програмне забезпечення, яке використовується для обробки векторної графіки, призначене, в першу чергу, для конструювання ілюстрацій і в меншій ступені для її обробки. Дані засоби використовують в рекламних агентствах, редакціях та виданнях. Оформлювальні роботи, що основані на застосуванні різноманітних шрифтів та геометричних елементів, вирішуються спеціальними засобами векторної комп'ютерної графіки набагато простіше. На сьогоднішній день, існують приклади високохудожніх творів, які створені засобами векторної графіки. Вони скоріше виключення, адже художня підготовка ілюстрації засобами векторної комп'ютерної графіки надзвичайно складна.

Програмне забезпечення що призначене для роботи з фрактальною комп'ютерною графікою призначене для автоматичної генерації різних зображень шляхом проведення математичних розрахунків. Сучасний етап створення фрактальної композиції полягає не в оформленні чи створенні, а в програмуванні. Фрактальну комп'ютерну графіку рідко використовують при створенні друкованих

або електронних документів, але частіше використовують у різноманітних розважальних програмах.

Основними сферами застосування комп'ютерної графіки є [24]:

- графічні інтерфейси користувачів;
- спецефекти та цифрова кінематографія;
- цифрові засоби телебачення, Інтернету, відеоконференцій;
- цифрові засоби фотографування;
- візуалізація наукових та ділових даних;
- різноманітні комп'ютерні ігри та системи реалізації віртуальної реальності;
- різні системи для реалізації автоматизованого проектування;
- комп'ютеризована система томографії;
- комп'ютерна графіка для кіно та телебачення.

Растрове зображення – це зображення, що представляє собою матрицю пікселів на комп’ютерному моніторі або інших пристроях і матеріалах. Растр – це матриця пікселів. Кожний піксель має свій колір. Сукупність певної кількості пікселів різного кольору створюють зображення.

Кожен піксель зображення – це об'єкт, який характеризується певним кольором, яскравістю і прозорістю. Кожен піксель може зберігати інформацію лише про певний колір, який і асоціюється з ним. Всі пікселі, що містяться у растровому зображенні, вони розташовуються по рядках та стовпцях.

Як наслідок, якщо більше пікселів на одиницю площі зображення, тим вище його деталізація. Максимальна деталізація зображення задається при створенні та не може збільшуватися. Якщо збільшити масштаб зображення, ступінь деталізації зображення при цьому не зростає (Рисунок 2.2). Забезпечення певного переходу, між початковими пікселями, зумовлено додаванням нових, їх значення обчислюється на підставі значень сусідніх пікселів даного зображення. Для опису розміщення пікселів використовують координати пікселів, які створюють дискретний ряд значень. Найбільш поширеною є система цілих координат із нумерацією пікселів з (0,0) у верхньому лівому куті.

а б

Рисунок 2.2. Відображення пікселів зображення:
а – повне растрове зображення; б – відображення пікселів цього зображення

На сучасному етапі растрове зображення має свої певні характеристики. Розглянемо їх більш детальніше (Рисунок 2.3).

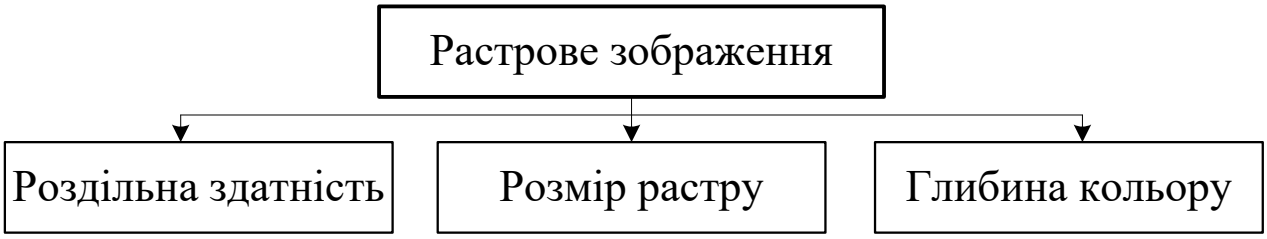


Рисунок 2.3. Основні характеристики растрового зображення

2.3.1. Роздільна здатність зображення

Будь–яке цифрове зображення складається з сукупності пікселів, кожен з яких пікселів має свій певний колір. Сукупність таких пікселів являє собою зображення, яке ми бачимо на екрані монітора.

Роздільна здатність растрового зображення визначається в пікселях на 1 дюйм (ppi – pixels per inch). А чіткість зображення безпосередньо залежить від того, скільки пікселів розміщується на один дюйм для відтворення графічної інформації – чим більше пікселів, тим чіткіше зображення [24].

А роздільна здатність зображень, що десь надруковані, вимірюється в точках на 1 дюйм (dpi – dot per inch), так як найменшою часткою такого зображення є надрукована точка на певному аркуші паперу. Отже, екран монітора має можливість відображати 72 (іноді навіть – 96) пікселі на 1 дюйм по вертикалі, а також по горизонталі, в той час як зображення для надрукування має мати 100 – 300 ppi.

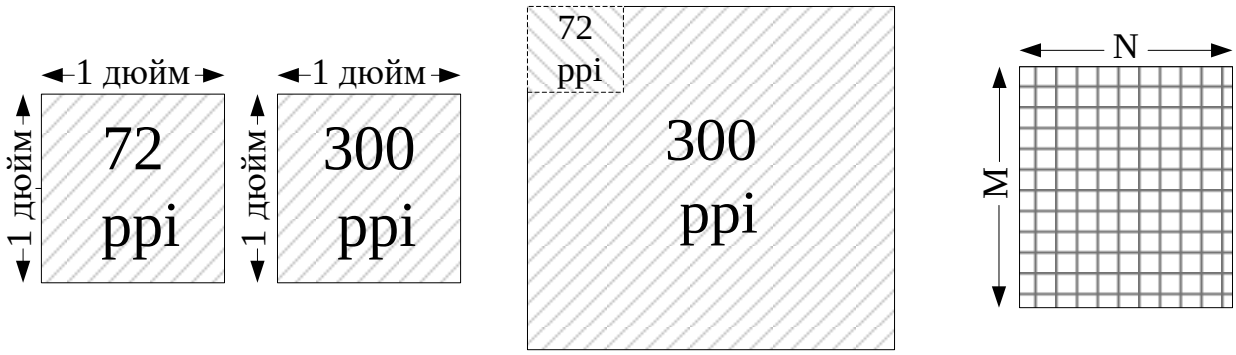
Візьмемо два цифрових зображення із роздільною здатністю 72 та 300 ppi (Рисунок 2.4, а). Безпосередньо фізичний розмір обраних картинок дорівнює 1 дюйму (тобто, 2,54 см) як по вертикалі, так і по горизонталі. При друкуванні цих зображень, при таких самих фізичних розмірах, безпосередньо якість роздрукованого зображення буде різною. Краща чіткість буде у зображення 300 ppi і гірша у 72 ppi.

При відтворенні цих зображень на екрані монітора відбудеться значне збільшення розмірів картинки із 300 ppi (це при 100% масштабуванні). Збільшення здійснюється через те, що монітор відображає тільки 72 пікселя на 1 дюйм. Отже, певна частина картинки 300 ppi має бути збільшена до розміру в 1 дюйм по відношенню до екрану монітора.

На Рисунок 2.4, б – пунктирною лінією, зображена ділянка в 1 квадратний дюйм екрану монітора, що показує 72 пікселі як по горизонталі так і по вертикалі. Розміри картинок становлять 72 та 300 пікселі по ширині та по висоті для кожної картинки. А фізичний розмір картинок – це 1 дюйм із роздільною здатністю в 72 та 300 dpi.

2.3.2. Розмір растру зображення

Растр – являє собою матрицю N x M пікселів (Рисунок 2.4, в), де N і M – піксельні розміри растру [24].



а б в

Рисунок 2.4. Характеристики растрового зображення:
а – роздільна здатність зображення з 72 та 300 ppi;
б – відображення 72 ppi та 300 ppi на моніторі; в – растр зображення

Для комп'ютерної графіки найбільш оптимальним є растр із однаковим кроком, тобто ppi_X = ppi_Y. Це зручно для багатьох алгоритмів відображення графічної інформації.

Розмір растрового зображення задається у вигляді двох чисел, що визначають розмір зображення в пікселях по горизонталі та вертикалі, наприклад 640x480. У даному випадку, ширина зображення становить 640, а висота – 480 пікселів. Таким чином, зображення складається з 307 200 пікселів. Кількість пікселів по горизонталі та вертикалі може бути різною для різних зображень. Чим вище роздільна здатність та розмір зображення, тим вища деталізація зображення. Для оптимального розміщення зображення на екрані, необхідно погоджувати кількість пікселів у зображенні, пропорції сторін зображення з відповідними параметрами пристрою відображення.

Потрібно розрізняти: роздільність екранного зображення; роздільність оригінала; роздільність друкованого зображення.

Роздільність оригінала. Дана характеристика має вимірювання у точках на 1 дюйм (dpi – dots per inch) та залежить від основних вимог, що висуваються до якості зображень та розмірів файлів, способів оцифровування або методів створення готових зображень, обраного формату файлу або інших параметрів. Чим вище вимоги стосовно якості, тим більша буде роздільність. Елементарною точкою

растра, для екранного зображення, називають пікселом. Розміри пікселів коливаються в залежності від обраної екранної роздільності, обраної роздільності оригіналу та масштабу відображення. Сучасні монітори можуть забезпечувати роздільність від 640x480 до 1600x1200 і вище. Відстань, в якісному моніторі, між сусідніми точками люмінофора найчастіше становить від 0,22 до 0,25 мм. Для найпоширенішого екранного зображення достатньою роздільністю є 72 dpi.

Роздільність друкованих зображень. Розміри точки растрових зображень залежать від застосованих методів та параметрів растрування оригіналів. При виконанні растрування на оригінали накладаються сітки ліній, комірки яких утворюють елементи растру. Частоти сіток растрів вимірюються числами ліній на дюйм (lpi – lines per inch) та називаються лінеатурою. Розміри точок растрів розраховуються для кожних елементів і залежать від інтенсивності тону в даних комірках. Якщо у растрах є абсолютний чорний колір, тоді розміри точок растрів збігаються з розмірами елементів растрів (100% заповненість). При абсолютно білому кольорі заповненість складає 0 відсотків. На практиці заповненість змінюється у межах 3–98%.

Всі точки растрів мають однакові оптичні щільності, які наближуються до абсолютно чорних кольорів. Ілюзія темного кольору складається за рахунок збільшення розміру точок та скорочень проміжкових полів між ними при однакових відстанях між центрами елементів растра. Даний метод називається раструванням із застосуванням амплітудної модуляції.

Інтенсивність тону, при застосуванні різних методів з частотною модуляцією, регулюється змінами відстані між сусідніми точками однакових розмірів, тобто в комірках растрів з різною інтенсивністю тонів знаходяться різна кількість точок. Зображення, які растровані за частотно–модульним методами, якісніші, оскільки розмір даних точок є мінімальним.

При методах стохастичного растрування, враховуються кількість точок, що необхідні для відображення необхідної інтенсивності тонів у комірках растрів. Потім, дані точки розташовуються всередині комірок на відстані, яка підраховується квазівипадковими методами. Регулярна структура растрів всередині комірки та у

зображеннях відсутня. Даний спосіб потребує певних затрат обчислювальних ресурсів та високої точності поліграфічного забезпечення, тому це застосовується лише для виконання художніх робіт.

2.3.3. Глибина кольору зображення

Глибина кольору – одна з важливих характеристик растру. Кількість кольорів – це важлива характеристика будь–якого зображення. Згідно дослідженнь око людини має здатність розрізнити 350 000 кольорів [24].

Для кодування кольору пікселя може бути виділеною різна кількість біт. Від цього залежить кількість колірних відтінків, які можуть бути відображені на моніторі одночасно. І чим більша довжина двійкового коду певного кольору, тим більша кількість кольорів може використовуватись при відтворенні графічного об'єкту. Глибина кольору – це кількість біт, що використовують при кодуванні одного пікселя. Глибина кольору растрового зображення вимірюється в біт на 1 піксель (bits per pixel, bpp).

Можна класифікувати зображення, безпосередньо за глибиною кольору, таким чином [24]:

- бінарні зображення (бітове) – 1 біт на піксель.
- напівтонові – градації деякого кольору (1 байт на 1 піксель).
- зображення у кольорі. Два байти (16 bpp) дають змогу визначити 65 536 різноманітних кольорів. Таким режим отримав назву High Color. У випадку коли для кодування певному кольору використовують 3 байти (24 bpp), можливе відображення 16,7 млн кольорів (режим – True Color). У графічних системах використовується і більша глибина кольору – 32/48 bpp та інші.

Для зберігання і представлення бітового зображення, у цифровому вигляді, використовують бітову карту, де на кожен 1 піксель відводять 1 біт певної інформації. Таке виділяння одного байту (8 біт) дає можливість закодувати 256 різноманітних колірних відтінків. Такий режим High Color, який розроблений для представляння відтінків ніби з «реального життя», і як наслідок, найбільш зручно

сприймається оком людини. Цей колір має кодування 16 бітами. True Color кодується 24 bpp та відображає 16,7 різноманітних кольорів. Цей колір найбільш придатний для сприйняття оком людини різноманітних фотографій.

А 32–бітний колір – це реальний 24–бітний колір із додаванням додаткового 8–бітного каналу, який або є Альфа–каналом, або заповнений нулями, а також задає степінь прозорості зображення для кожного певного пікселя. Наприклад, для відображення ефекту напівпрозорих елементів сторінки. Основна причина використовування такого Альфа–каналу – це мета оптимізації роботи з відеопам'яттю, що у більшості комп'ютерів сучасного світу має 32–бітну переадресацію, а також 32–бітову шину даних.

Отже, колір кожного пікселя створюється через змішування трьох основних кольорів RGB–моделі. RGB – це адитивна колірна модель, яка описує спосіб утворення кольору. Синтез кольору утворюється шляхом кодуванням градацій складових трьох каналів (Red, Green, Blue). Змішавши 3–и базові кольори в довільних пропорціях, можна отримати все різноманіття доступних відтінків.

Дана модель відображається як тривимірна система координат. У якій кожна координата – це відображення певного внеску складової в результуючий колір, який знаходиться в діапазоні від мінімуму (нуль) до максимального значення. Усередині отриманого куба і знаходяться всі кольори, що утворюють колірний простір (Рисунок 2.5). Кількість градацій кожного кольору залежить від бітових значень RGB. Зазвичай використовується 24–х бітна модель, у якій відведено по 8 біт на кожен канал, тому кількість градацій становить від 0 до 255 (Рисунок 2.6).

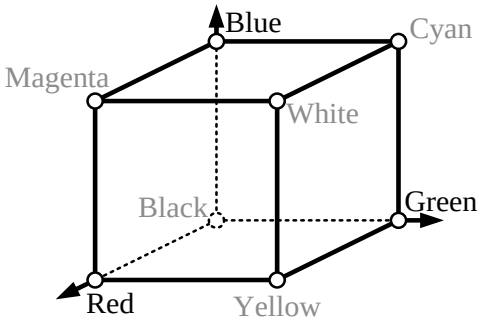


Рисунок 2.5. Колірний простір RGB.

В моделі RGB центральна точка, з координатами (0,0,0) – чорний колір. Білий колір відповідає максимальним значенням складових – (255,255,255). Відповідно, червоний – (255,0,0), синій – (0,0,255) та зелений – (0,0,255).

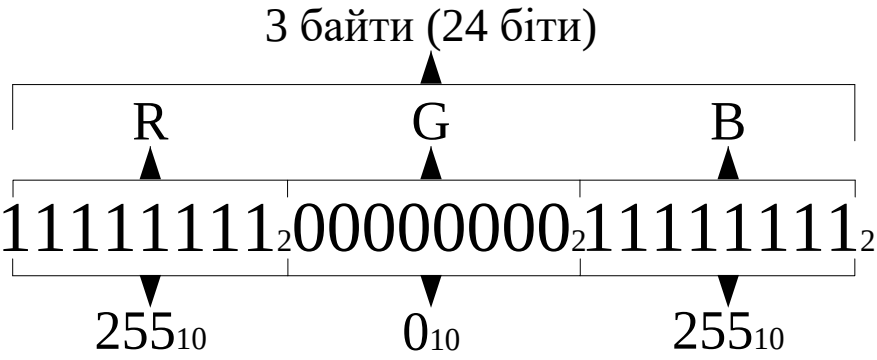


Рисунок 2.6. 24–х бітна RGB модель синтезу кольору.

Колірна модель RGB призначена відображати зображення в електронних системах, таких як телебачення, комп’ютери, фотографії та інші.

2.3.4. Класи зображень

Для того, щоб детальніше оцінити ступінь спотворення контейнера після стеганоперетворення та підвищення стійкості методів до стеганоаналізу, потрібно ввести поняття класу зображень [25].

Перший клас. Зображення з малою кількістю кольорів (4–16) і досить великими областями, які характеризуються заповненням одним кольором. Плавних переходів кольорів немає. Наприклади: ділова графіка.

Другий клас. Зображення, з певними плавними переходами кольорів, які побудовані з допомогою комп'ютера. Наприклад: графіка презентацій.

Третій клас. Фотографії. Наприклад: відсканові фотографії.

Четвертий клас. Фотографії з діловою графікою. Наприклад: реклама.

2.3.5. Колір та його сприйняття людиною

Колір – це характеристика сприйняття оком людини електромагнітних хвиль різної довжини. Видимий колір ока визначається довжиною хвилі. У процесі сприйняття і обробки беруть участь дві сторони, предмет, на який ми дивимося і власне людське око. Сприйняття кольору людиною визначається її індивідуальністю, а також спектральним складом, коліром і контрастом яскравості з джерелами світла. Спектр – це послідовність монохроматичних випромінювань, кожна з яких відповідає певній довжині хвилі електромагнітного коливання [21].

Відчуття кольору виникає при збудженні і гальмуванні світлочутливих клітин – рецепторів ока сітківки людини. У сітківці ока знаходяться рецептори – колбочки і палички. Палички є високочутливими елементами, що працюють в умовах слабкого освітлення. Палички нечутливі до довжини хвилі. Колбочки мають вузьку спектральну криву і реагують на кольори. Колбочки, відповідають за сприйняття кольору, а палички в свою чергу за сутінковий зір. Наприклад, вночі ми бачимо все сірим, бо працюють палички, а вдень працюють і колбочки і палички.

Вважається, що у людини існує три види колбочок, які розрізняються по спектральній чутливості – ρ («червоні»), γ («зелені») і β («сині»). Ці колбочки проявляють найбільшу чутливість до 3–х основних кольорів видимого спектру – червоного, зеленого та синього (Рисунок 2.7). Найбільшу чутливість мають колбочки, що сприймають кольори червоного спектра, трохи слабкіше – зелені колбочки й істотно слабкіші – сині. Таким чином, для сприйняття будь–якого кольору, наш мозок змішує ці три кольори, враховуючи ще один параметр – інтенсивність. Інтенсивність світла – це певна міра енергії цього самого світла, яка має вплив на око, а яскравість – це те, як сприймається людським оком цей вплив. Самою фізіологічною системою кодування кольору є RGB. Змішування кожного кольору, дає білий світ. А відсутність всіх кольорів призводить до відсутності світла або чорний колір [24].

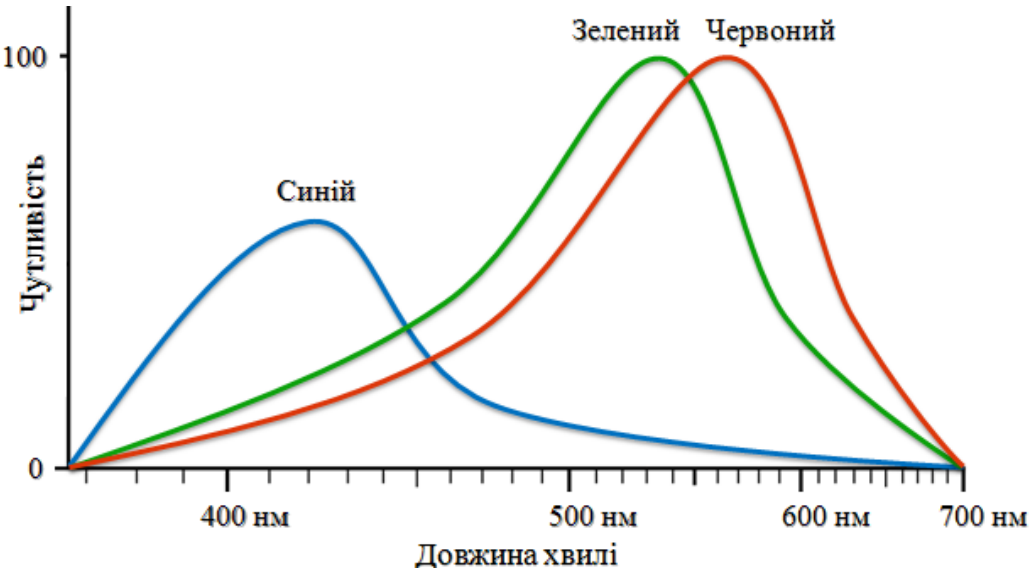


Рисунок 2.7. Криві чутливості всіх трьох видів колбочок

Формування кольору предмета відбувається таким чином: денне світло, потрапляючи на предмет частково поглинається, а частково відбивається, ось цей відбитий спектр і бачить око людини. Видимими є хвилі, що лежать в діапазоні 380 – 760 нм. Якщо світло містить всі видимі довжини хвиль у рівних кількостях, тоді він називається ахроматичним. При максимальній інтенсивності, він сприймається як білий. Якщо світло містить нерівні пропорції однакових довжин хвиль, то він є хроматичним. Такий об'єкт, сприймається як кольоровий, при умові, якщо він відбиває світло у вузькому діапазоні довжин хвиль.

2.3.6. Незначущі елементи растрового зображення

Растрове зображення являє собою матрицю (растр) пікселів. Кожен піксель має змогу зберігати певну інформацію тільки про один якийсь певний колір. Всі пікселі такого кольорового зображення можна розкладати на компоненти кольору R, G і B, що побудовані в колірній схемі RGB (Рисунок 2.8). Як наслідок, картинки можуть розкладатися на три компоненти кольору, які розміщені один за одним у масиві, який є спільним. Для обробки зображення, колірні характеристики зображення переводиться у числову матрицю.

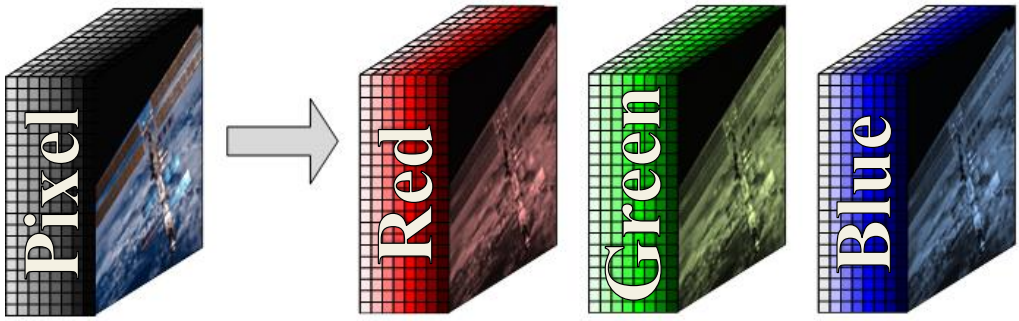


Рисунок 2.8. Розміщення колірних компонентів

Приховування інформації можна проводити у всі три колірні компоненти. Зміна у кожному окремому колірному компоненті може призвести до різних візуальних спотворень результуючого зображення. Око людини найбільшу чутливість має до спектру червоного кольору, більш слабшу – до зеленого та набагато більш слабку– до синього. Отже, людське око має найслабшу чутливість до синьої компоненти спектру, а це означає, що деякі зміни в колірній компоненті синього кольору будуть найменше помітні. Тому приховування інформації оптимальніше проводити у синю компоненту [20].

Під час кодуванні пікселів кольорового зображення використовують 24 біти, а це означає, що по 8 бітів на кожну компоненту кольору (Рисунок 2.9). Глибина кольору компоненти становить 8 біт.

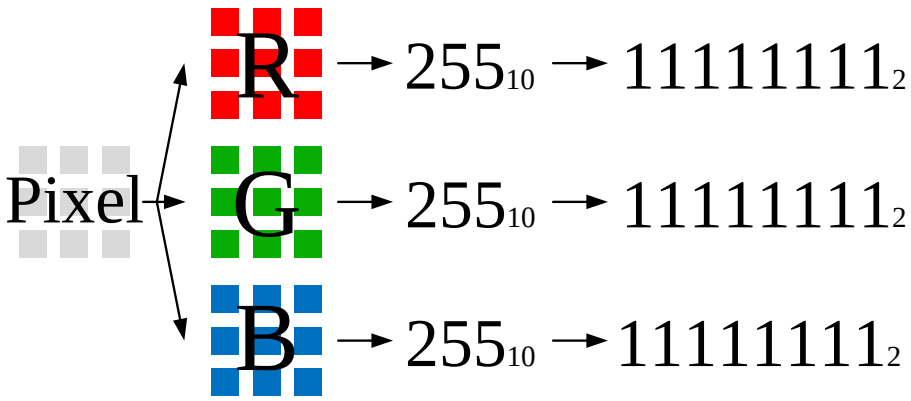


Рисунок 2.9. Числові значення колірних матриць

Найменш значущий біт має у собі менше всього певної інформації. Людське око у більшості випадкість не здатне побачити певні зміни в такому біті. Як наслідок, його використовуються для приховання інформації, через заміну найменш значущого біта пікселів картинки бітами прихованого повідомлення. Так, обсяг інформації, що можливо приховати у зображенні розміром NxM, можна порахувати за формулою:

$$V = \frac{C \times N \times M}{8} \tag{2.1}$$

де V – обсяг прихованої інформації у байтах, C – кількість бітів, що змінюються в одному елементі зображення, N та M – висота та ширина зображення (Рисунок 2.10).

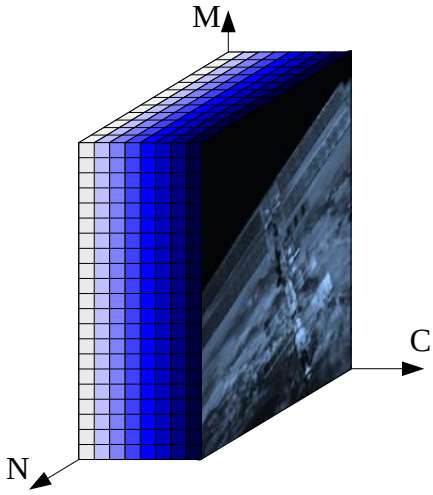


Рисунок 2.10. Колірна компонента синього кольору у тривимірному просторі

Таким чином, обсяг прихованих даних у синій складовій розміром 240x240 становитиме 7,2 кілобайти, якщо модифікувати один молодший біт. Такий об’єм інформації дозволяє приховати 7200 символів згідно таблиці ASCII–кодів (табл. 2.1). Обсяг інформації можна збільшити при заміні двох молодших бітів. У такому випадку об’єм прихованої інформації збільшиться вдвічі, тобто 14,4 кілобайти (14400 символів). Тим самим відбувається збільшення прихованої пропускної спроможності.

Під прихованою пропускною здатністю слід розуміти максимальну кількість інформаційних даних, яка може бути вбудована до одного елементу контейнера

(пікселя). Обов'язковою умовою є безпомилковість передачі приховуваних даних одержувачеві та захищеність від атак порушника. Контейнером називається інформаційна послідовність, в якій приховується повідомлення (Рисунок 2.11).

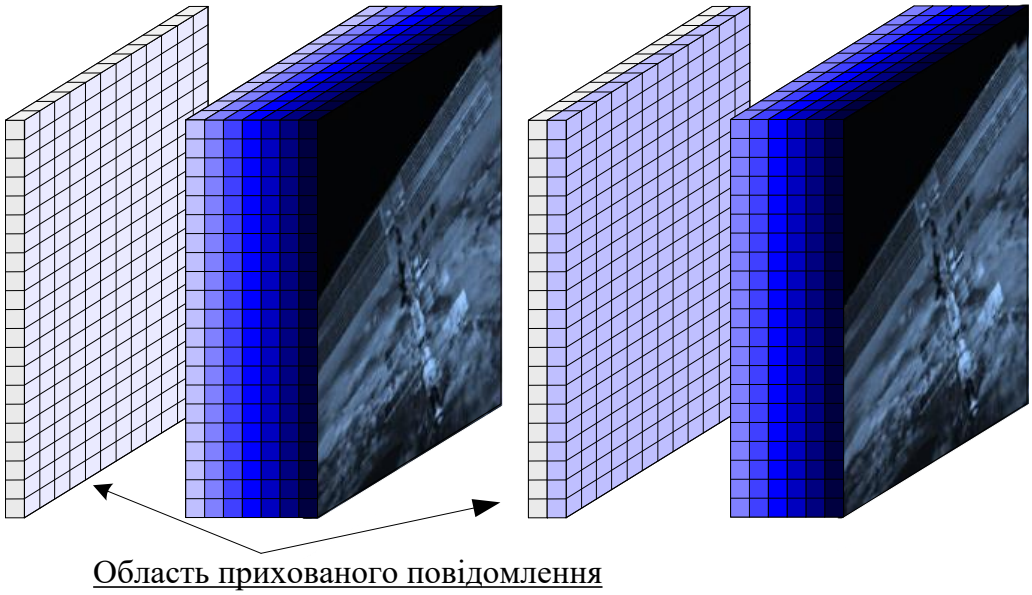


Рисунок 2.11. Область прихованого повідомлення при використанні 1–го та 2–х бітів в одному елементі зображення

Таблиця 2.1.

Обсяг прихованої інформації

№	Колірна компонента	Кількість бітів, що змінюються в одному елементі зображення	Розмір зображення	Об'єм прихованої інформації (кБ/символів)
1	Blue	1	240x240	7,2 / 7200
2	Green + Blue	1	240x480	14,4 / 14400
3	Red + Green + Blue	1	240x620	21,6 / 21600
4	Blue	2	240x240	14,4 / 14400
5	Green + Blue	2	240x480	28,8 / 28800
6	Red + Green + Blue	2	240x620	42,2 / 42200

2.4. Вибір функціонального профілю захищеності

Метою введення класифікацій автоматизованих систем та стандартних функціональних профілів захищеності є полегшення виконання задач зіставлення вимог до КЗЗ обчислювальних систем АС з певними характеристиками АС. Автоматизована система представляє собою організаційно–технічну систему, яка об'єднує операційну систему, фізичне середовище, оброблювану інформацію і персонал. Вимоги що висувається до функціонального складу комплексів засобів захисту залежать від характеристик ОІ, самої ОС, персоналу, фізичного середовища і організаційної підсистеми. Вимоги щодо гарантій визначаються характером (важливістю) ОІ і призначенням АС [10].

В межах певного класу АС класифікують на підставах вимог щодо забезпечення певних властивостей інформації. Інформація, з точки зору безпеки, може характеризуватися 3–ма властивостями: цілісність, конфіденційність та доступність. У зв'язку з тим, в кожному класі автоматизованої системі виділяють такі підкласи АС [10]:

- підвищення вимог до – забезпечення конфіденційності ОІ (підкласи «х. К»);
- підвищення вимог до – забезпечення цілісності ОІ (підкласи «х.Ц»);
- підвищення вимог до – забезпечення доступності ОІ (підкласи «х.Д»);
- підвищення вимог до – забезпечення конфіденційності і цілісності ОІ (підкласи» х.КЦ»);
- підвищення вимог до – забезпечення конфіденційності і доступності ОІ (підкласи «х.КД»);
- підвищення вимог до – забезпечення цілісності і доступності ОІ (підкласи «х.ЦД»).
- підвищення вимог до – забезпечення конфіденційності, цілісності і доступності ОІ (підкласи «х.КЦД»).

Для кожних підкласів кожних класів вводиться певна кількість ієрархічних стандартних профілів функціональності, що може бути різною щодо кожного класу

та підкласу автоматизованої системи. Дані профілі є ієрархічними тому, що їх реалізація має забезпечувати наростаючу захищеність від певних загроз відповідного типу. Стрімке наростання ступенів захищеності може досягатись підсиленнями певних послуг, тобто внесення включень до профілів більш високих рівнів послуг, так і включенням до профілів нових послуг.

Дана класифікація корисна при полегшені вибору переліку різних функцій, що повинен реалізовувати КЗЗ обробки інформації, проектованої або існуючої автоматизованої системи. Даний підхід дозволяє насамперед мінімізувати витрати щодо початкових етапів створення КСЗІ автоматизованої системи. Для створення комплексів засобів захисту, який найповніше відповідає висунутим характеристикам та вимогам до конкретної автоматизованої системи, необхідно виконати проведення в певному обсязі аналізу загроз та оцінку ризиків [11].

Стандартні функціональні профілі захищеності являють собою перелік мінімальних необхідних рівнів послуг, що повинен реалізовувати КЗЗ ОС АС, з метою задовольняти певні вимоги захищеності інформації, що обробляється в даній автоматизованій системі.

Стандартні функціональні профілі захищеності будуються на підставах існуючих вимог захисту певних інформаційних даних від певних загроз та відомих на сьогодні день функціональних послуг, які дозволяють протистояти певним загрозам та забезпечувати виконання заявлених вимог, що пред'являються.

До стандартних функціональних профілів не висуваються вимоги політики безпеки, рівнів гарантій, хоч їх наявність частково допускається в разі певної необхідності. Політика безпеки комп'ютеризованої системи, яка реалізує певні стандартні профілі, має бути «успадкована» із відповідних документів, які встановлюють вимоги щодо порядку обробки інформації в автоматизованій системі. Таким чином, одні і ті ж профілі захищеності можливо використовувати для опису функціональних вимог із захисту ОІ для ОС, та СУБД, в той час, коли їх реалізація політики безпеки буде різною.

Функціональні профілі захищеності можуть використовуватись для зрівняльної оцінки функціональності комп'ютеризованих систем за певними критеріями інших держав із оцінкою за певними національними критеріями [10]:

3.КД.1 = { КД–2, КА–2, КО–1, КВ–2, ДР–1, ДВ–1, НР–2, НИ–2, НК–1, НО–2, НЦ–2, НТ–2, НВ–1 }

В автоматизованих системах, призначених для автоматизації певної діяльності органів державної влади, часто виконується обробка інформації з обмеженим доступом. Основними загрозами для даної інформації в даних системах є загроза, що призводить до несанкціонованого ознайомлення із інформацією, тобто загроза (порушення) конфіденційності. Таким чином, КЗЗ ОС, що входить до складу АС, в І–у чергу пред'являються вимоги до забезпечення конфіденційності ОІ, персональної відповідальності користувачів за дотримання режиму секретності [11].

Політика безпеки, яка реалізована, має відповідати встановленим в Україні правилам роботи з певними секретними документами. Отже, механізми, які реалізовують послугу адміністративної конфіденційності, мають виконувати розмежування доступу на основі грифів докмуентації (тобото, пасивних об'єктів), а також рівнів рівнів допуску користувачів.

Висновки по розділу

В даному розділі шляхом аналізу літературних джерел визначено перспективні напрямки, за якими можливе використання стеганографії для захисту інформації в автоматизованих системах, показана суть головних понять стеганографії таких як повідомлення, контейнер, стеганоконтейнер, стеганографічний ключ та стеганографічний канал. Розглянуті основні типи стеганосистем, а саме: змішані стеганосистеми, системи із секретним ключем, безключові стеганосистеми, системи з відкритим ключем. Отримані результати дозволяють визначити напрямки розвитку та здійснення стеганоаналізу на основі атак на стеганосистеми.

Була розглянута структура контейнера растрового зображення та його основні характеристики. До них належать: роздільна здатність, розмір растру та глибина

кольору зображення. Опрацьований матеріал дозволяє визначити основні принципи та реалізувати методи приховування інформації у незначущі елементи растрового зображення. Таким чином, стеганографічні методи найбільш ефективні при вирішенні проблем захисту конфіденційної інформації.

Був обраний фуекціональний профіль захищеності для полегшення виконання задач зіставлення вимог до КЗЗ обчислювальних систем АС з певними характеристиками АС. Автоматизована система представляє собою організаційно–технічну систему, яка об'єднує операційну систему, фізичне середовище, оброблювану інформацію і персонал. Вимоги щодо гарантій визначаються характером (важливістю) ОІ і призначенням АС

РОЗДІЛ 3
ДОСЛІДЖЕННЯ СТЕАГНОГРАФІЧНИХ МЕТОДІВ ПРИХОВУВАННЯ ДАНИХ В РАСТРОВИХ ЗОБРАЖЕННЯХ

3.1. Стеганографічні методи приховування даних та їх реалізація у MathCAD

Найпоширенішим методом стеганографічного захисту є приховування даних у нерухомих растрових зображеннях. Для реалізації даного методу використовують фіксовані контейнери. Використання такого контейнера дає змогу здійснювати вбудовування повідомлення оптимальнішим методом, знаючи його характеристики. Важливими характеристиками контейнера є: розмір растру, глибина кольору, роздільна здатність. Зміна даних характеристик впливає на структурні ознаки контейнера.

Під час кодування пікселів колірного зображення використовують 24 біти, це означає, що по 8 бітів на кожну компоненту кольору. У рамках даної дипломної роботи будуть розглянуті та реалізовані такі методи приховування даних:

- метод заміни найменшого значущого біта;
- метод псевдовипадкового інтервалу;
- метод блокового приховування.

3.1.1. Метод заміни найменшого значущого біта

Внесення прихованого повідомлення до зображення виконаємо методом заміни найменше значущих бітів пікселя. Людське око у більшості випадкість не здатне побачити певні зміни в такому біті. Як наслідок, його використовуються для приховання інформації, через заміну найменш значущого біта пікселів картинки бітами прихованого повідомлення.

Для приховування інформації буде використана синя складова статичного 24–х бітового RGB зображення з розміром растру – 240x240 (Рисунок 3.1). Інформація для приховування – текст англійською мовою.

Перед імпортом зображення в документ MathCAD підготуємо його у відповідному редакторі і запишемо у вигляді BMP–файлу. Імпорт зображення в документ MathCAD проводимо за допомогою вбудованої функції – READ_IMAGE("директорія та ім’я файлу"). Для обробки зображення, необхідно перевести колірні характеристики кожного пікселя у числову матрицю та виконати розклад зображення на компоненти R, G і B. Для цього використовуємо функцію READRGB("директорія та ім’я файлу").

Рисунок 3.1. Контейнер–оригінал

Після ініціалізації зображення виконаємо виокремлення синьої складової зображення. Для цього використаємо функції виділення колірних компонентів, кожна з яких відповідає певному колірному компоненту графічного файлу: READ_RED( ), READ_GREEN( ), READ_BLUE( ) (Рисунок 3.2).

Визначення розміру синьої компоненти кольорового зображення виконуємо вбудованими функціями MathCAD: cols(BLUE) та rows(BLUE) – функція, яка повертає кількість рядків та стовпців. Після того, слід виконати імпорт текстового повідомлення за допомогою функції READBIN(" ").

ORIGIN := 1

Picture := "PictureBMP.bmp"

IMAGE := READ_IMAGE(Picture)

RGB := READRGB(Picture)

RED := READ_RED(Picture) GREEN := READ_GREEN(Picture) BLUE := READ_BLUE(Picture)

Рисунок 3.2. Блок М.1.1

Перевірку імпортування файлу повідомлення можна виконати функцією vec2str(Mes). Така функція здіснює повернення рядку символів, які дорівнюють вектору Mes. Визначення розміру прихованого повідомлення виконаємо функцією rows(Mes). Після того, визначимо відсоток заповнення синьої складової інформаційною послідовністю повідомлення – P.

Таким чином, ми використали синю складову зображення. Кількість рядків та стовпців становить – 240. Кількість байт повідомлення становить – 547. Для оцінювання відсотку заповнення синьої компоненти інформаційною послідовністю, визначимо кількість біт у повідомленні – Bs, яка становить 4376 біт. Відсоток заповнення – 8%.

Наступний етап – внесення прихованої інформації до синьої складової зображення. Для виконання приховування необхідно виконати переведення десяткового числа у формат двійкового та навпаки. Перетворення двійкового числа в десяткове будемо виконувати за допомогою функції B2D(x), десяткове у двійкове – D2B(x) (Рисунок 3.3).

C := BLUE

Cc := cols(C) = 240

Rc := rows(C) = 240

Mes := READBIN("Text.txt" ,"byte")

S := rows(Mes) = 547

Bs := S·8 = 4376

$$P := \text{round}\left(\frac{100 \cdot Bs}{Cc \cdot Rc}\right) = 8$$

$$B2D(x) := \sum_{i=1}^{8} \left(x_i \cdot 2^{i-1}\right)$$

$$D2B(x) := \left| \begin{array}{l} \text{for } i \in 1..8 \\ \quad \left| \begin{array}{l} V_i \leftarrow \text{mod}(x,2) \\ x \leftarrow \text{floor}\left(\frac{x}{2}\right) \end{array} \right. \\ V \end{array} \right.$$

Рисунок 3.3. Блок М.1.2

Для більшої зручності внесення повідомлення до контейнеру виконаємо перетворення числової матриці синьої складової у вектор–стовпець. Дане перетворення виконує модуль – Vec.

Внесення прихованої інформації до зображення виконує модуль Nvec. Даний модуль виконує перетворення кожного байту елементу масиву Vec в двійковий код та замінює молодший біт на біт інформаційного повідомлення. Після цього, даний модуль виконує зворотне перетворення двійкового коду у байт елементу зображення.

За допомогою модуля Np, виконуємо перетворення вектора–стовпця Nvec у масив розмірами – C. Функція submatrix (A,m,n,i, j), яка здійснює повернення підмасиву з масиву A, який складається з певних елементів, що спільні для рядків від m до n та спільні для стовпців від i до j. Наступним етапом реалізації є об’єднання колірних компонентів зображення в один масив, а саме RED, GREEN та Np за допомогою функції augment( ).

Збереження зображення з повідомленням виконаємо за допомогою вбудованої функції WRITERGB(x), де x – директорія нового файлу та його ім’я (Рисунок 3.4).

На рисунку 3.5 зображена байтова та бітова послідовність контейнера – (Vec) та стеганоконтейнера (Nvec). Молодший біт елементу синьої складової зазнав модифікації та змінився на відповідний біт повідомлення.

На рисунку 3.6 відображено візуальне заповнення або модифікація контейнеру – оригінал та контейнера – результату методом заміни найменшого значущого біта при 8% заповненні.

```
Vec := | Vec ← C^(1)
       | for i ∈ 2..cols(C)
       |   Vec ← stack(Vec, C^(i))

Nvec := | for μ ∈ 1..rows(Mes)
        |   b ← D2B(Mes_μ)
        |   for i ∈ 1..8
        |     P ← D2B[Vec_(i+8·(μ−1))]
        |     P_1 ← b_i
        |     Vec_(i+8·(μ−1)) ← B2D(P)
        | Vec

Np := for i ∈ 1,2..cols(C)
        Np^(i) ← submatrix[Nvec, (i − 1)·rows(C) + 1, i·rows(C), 1, 1]

Pic := augment(RED, GREEN, Np)

WRITERGB("PictureBMP_2.bmp") := Pic
```

Рисунок 3.4. Блок М.1.3

Після цього, при реалізації стеганографічної системи, відбувається передача зображення стеганографічний каналом. Після отримання зображення, отримував повинен здійснити видобування повідомлення з контейнера. Для реалізації початкового етапу виділення повідомлення виконаємо дії блоку М.1.1. Виділення повідомлення з зображення виконується за допомогою модуля Nmes (Рисунок 3.7).

Vec =

	1
1	3
2	4
3	4
4	4
5	4
6	4
7	4
8	4
9	5
10	…

Nvec =

	1
1	3
2	5
3	4
4	4
5	5
6	4
7	5
8	4
9	4
10	…

Vec =

	1
1	11b
2	100b
3	100b
4	100b
5	100b
6	100b
7	100b
8	100b
9	101b
10	…

Nvec =

	1
1	11b
2	101b
3	100b
4	100b
5	101b
6	100b
7	101b
8	100b
9	100b
10	…

Рисунок 3.5. Байтова та бітова послідовність контейнера та стеганоконтейнера

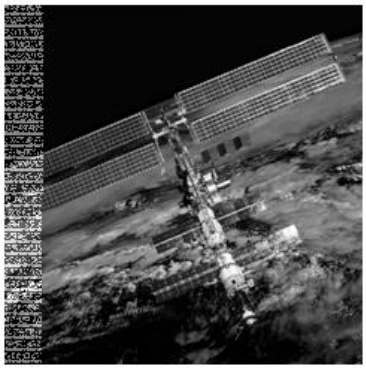


Рисунок 3.6. Розташування бітів повідомлення по масиву контейнера

$$Kn := \frac{Bs}{8}$$

Nmes :=
- Vec ← C^(1)
- for i ∈ 2.. cols(C)
  - Vec ← stack(Vec, C^(i))
- for j ∈ 1.. Kn
  - for i ∈ 1.. 8
    - P ← D2B[Vec_(i+8·(j−1))]
    - b_i ← P_1
  - Nmes_j ← B2D(b)
- vec2str(Nmes)

Рисунок 3.7. Блок М.1.4

Зміна Kn містить мітку кінця повідомлення у контейнера. Таким чином, після виконання даного модуля, зміна Nmes буде містити виділене приховане повідомлення.

3.1.2. Метод псевдовипадкового інтервалу

Метод випадкового інтервалу, полягає у тому що біти повідомлення розподіляються псевдовипадково по контейнеру. Ця методика ефективна у випадку,

коли бітова довжина прихованого повідомлення є істотно меншою за кількість пікселів зображення [21].

Для реалізації даного методу виконаємо дії блоку М.1.1 – М.1.2. Для більшої зручності внесення повідомлення до контейнеру виконаємо перетворення числової матриці синьої складової у вектор–стовпець. Далі, виконаємо вбудовування повідомлення у контейнер. Приймемо, що для внесення бітів повідомлення до певного контейнеру із замінним кроком, а величина його зумовлена кількістю одиниць у безпосередньо двійковому значенні кожного номеру елементу контейнера, над яким було здійснено перетворення. Для визначення інтервалу позиції вбудовування біта повідомлення застосуємо формулу (3.1).

$$S = K \times \sum_{i=1}^{n} x_i, \tag{3.1}$$

де K – стеганографічний ключ. Реалізація формули (3.1) виконано функцією step(x).

Наступним етапом даного методу є процес вбудовування бітової послідовності повідомлення до елементів синьої складової. Для цього використаємо блок М.2.1, який зображено на рисунку 3.8.

$$\text{step}(x) := K \cdot \sum_{i=1}^{\text{rows}(x)} x_i \qquad K := 2$$

```
Nvec := | z ← 1
        | for μ ∈ 1..rows(Mes)
        |     b ← D2B(Mes_μ)
        |     for i ∈ 1..8
        |         z ← z + step(D2B(z))
        |         P ← D2B(Vec_z)
        |         P_1 ← b_i
        |         Vec_z ← B2D(P)
        | Vec
```

Рисунок 3.8. Блок М.2.1

Даний модуль виконує перетворення кожного байту елементу масиву Vec в двійковий код та замінює молодший біт на біт інформаційного повідомлення.

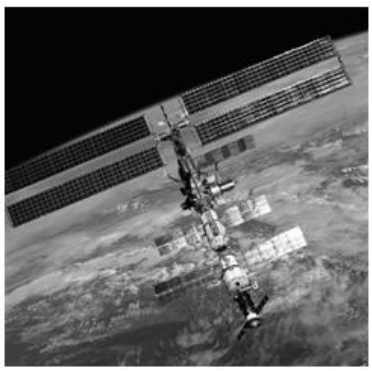
Позиція елементу зображення визначається за допомогою функції step( ). Коефіцієнт K, у даному методі, виступає ключем. Сама функція step використовує кількість двійкових символів, значення яких дорівнює одиниці. Після цього, даний блок виконує зворотне перетворення двійкового коду у байт елементу зображення.

За допомогою модуля Np, виконуємо перетворення вектора–стовпця Nvec у масив розмірами – C. Наступним етапом реалізації є об'єднання колірних компонентів зображення в один масив, а саме RED, GREEN та Np за допомогою функції augment( ) та збереження зображення у файлі BMP–формату (Рисунок 3.9).

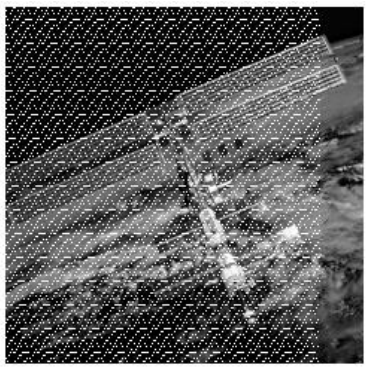
```
Np := for i ∈ 1,2.. cols(C)
        Np^⟨i⟩ ← submatrix[Nvec,(i − 1)·rows(C) + 1,i·rows(C),1,1]
Pic := augment(RED,GREEN,Np)
WRITERGB("PictureBMP_2.bmp") := Pic
```

Рисунок 3.9. Блок М.2.2

На рисунку 3.10 відображено візуальне заповнення або модифікація контейнеру – оригінал та контейнера – результату після стеганоперетворення.



а



б

Рисунок 3.10. Візуальне відображення заповнення стеганоконтейнера:
а – оригінал, б – модифікований контейнер

Для реалізації видобування повідомлення виконаємо дії блоку М.1.1 та М.2.3. Зміна К має значення ключа для видобування повідомлення. Для визначення

інтервалу позиції вбудовування біта повідомлення застосуємо формулу (3.1). Значення змінної Kn відповідає мітці кінця повідомлення в контейнері. Виділення повідомлення з зображення виконується за допомогою модуля Nmes. Таким чином, після виконання даного модуля, зміна Nmes буде містити виділене приховане повідомлення (Рисунок 3.11).

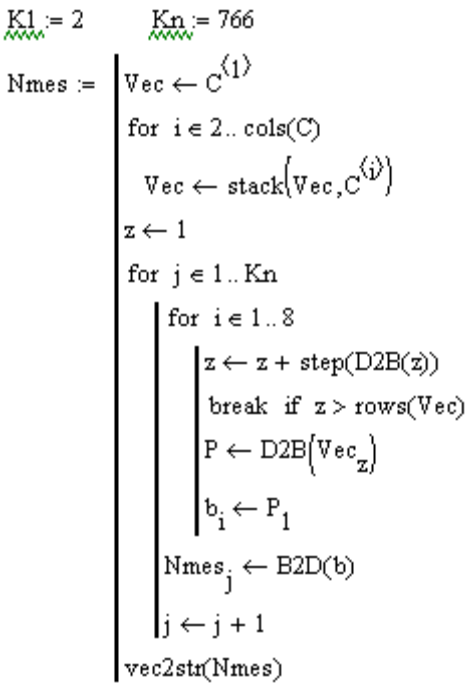


Рисунок 3.11. Блок М.2.3

3.1.3. Метод блокового приховування

Реалізація даного методу полягає в наступному. Контейнер розбивається на l(m) неперетинних блоків Ii, довільної конфігурації та для безпосередньо кожного з них здійснюється обчислення біт парності p(Ii):

$$p(I_i) = \sum_{j \in I_i} LSB(c_j) \bmod 2 \qquad (3.2)$$

Також у кожному блоці проводять приховання одного певного секретного біту mi. У разі коли біт парності p(Ii) не співпадає з секретним бітом Ii, то здійснюється певне інвертування одного з цих НЗБ блоку Ii, у результаті чого p(Ii)= mi. Для реалізації даного методу у системі MathCAD, необхідно виконати наступні етапи

реалізації. Для реалізації даного методу виконаємо дії блоків М.1.1 – М.1.2. Для більшої зручності внесення повідомлення до контейнеру виконаємо перетворення байтової послідовності повідомлення у бітову за допомогою блоку М.3.1 (Рисунок 2.23). Поділ синьої складової зображення на блоки здійснюватимемо таким чином: якщо кількість біт у повідомленні Bs ≤ C, то кожен блок відповідає окремому стовпцю матриці C. Якщо Bs > Cc, тоді матриця синьої компоненти розбивається на певну кількість стовпців, що відповідає значенню 1/K·Cc, де K = ceil(Bs ÷ Cc). Значення K використовують у якості ключа (Рисунок 3.12). Процес вбудовування бітової послідовності повідомлення до елементів синьої складової реалізований у блоці М.3.2.

```
T := | T ← D2B(Mes_1)
     | for j ∈ 2..rows(Mes)
     |   T ← stack(T, D2B(Mes_j))
```

Рисунок 3.12. Блок М.3.1

```
K := ceil(Bs ÷ Cc) = 26

Np := | Np ← C
      | for σ ∈ 1..K
      |   x1 ← (σ − 1)·floor(Rc ÷ K) + 1
      |   x2 ← σ·floor(Rc ÷ K)
      |   for y ∈ 1..Cc
      |     break if y + (σ − 1)·Cc > Bs
      |     △ ← submatrix(Np, x1, x2, y, y)
      |     b ← 0
      |     for x ∈ 1..rows(△)
      |       P ← D2B(△_x)
      |       LSB ← P_1
      |       b ← b ⊕ LSB
      |     if b ≠ T_(y+(σ−1)·Cc)
      |       n ← ceil(rnd(rows(△)))
      |       △_n ← △_n + 1 if mod(△_n, 2) = 0
      |       △_n ← △_n − 1 otherwise
      |       Np ← putregion(Np, △, x1, y)
      | Np
```

Рисунок 3.13. Блок М.3.2

Змінна σ виокремлює відповідну частину від довжини певного блоку масиву. x1 та x2 – відповідні індекси початку та кінця кожного виділеного блоку. Для кожного блоку обчислюється біту парності, де b – біт парності кожного відокремленого блоку. Якщо bi = Ti, тоді переходимо до наступного блоку для внесення біту послідовності повідомлення. Якщо bi ≠ Ti тоді з блоку, випадковим чином, обирається індекс елементу зображення що входить до даного блоку для модифікації його у потрібне значення. Використовуючи функцію putregion() виконується вбудовування модифікованого блоку до загального масиву Np. На рисунку 3.14 відображені пікселі контейнера які були модифіковані внаслідок застосування даного методу стеганоперетворення.

Наступним етапом реалізації даного методу є об'єднання колірних компонентів зображення в один масив та збереження зображення–результату.

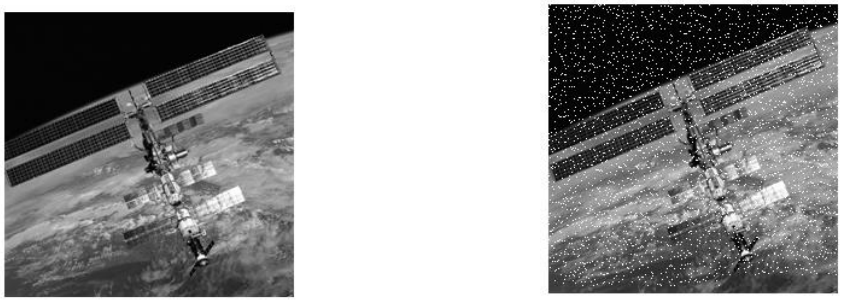


Рисунок 3.14. Контейнер–оригінал – зліва та контейнер–результат – справа

Для видобування повідомлення виконаємо дії блоку М.3.3 на Рисунок 3.15.

У результаті виконання даного блоку, зміна Nmes буде містити текст повідомлення. Реалізація даних методів була здійснена на основі літератури.

```
K := 26                K2 := 6144
Nmes := | for σ ∈ 1..K
        |   x1 ← (σ − 1)·floor(Cr ÷ K) + 1
        |   x2 ← σ·floor(Cr ÷ K)
        |   for y ∈ 1..Cc
        |     Δ ← submatrix(C, x1, x2, y, y)
        |     b ← 0
        |     for x ∈ 1..rows(Δ)
        |       P ← D2B(Δ_x)
        |       LSB ← P_1
        |       b ← b ⊕ LSB
        |     M_{y+(σ−1)·Cc} ← b
        | for j ∈ 1..K2/8
        |   Nmes_j ← B2D(submatrix(M, 8·j − 7, 8·j, 1, 1))
        | vec2str(Nmes)
```

Рисунок 3.15. Блок М.3.3

У результаті виконання даних методів було отримано три вихідних зображення із вбудованим повідомлення, яке було зчитано із текстового файлу. На рисунку 3.16 можна побачити зображення до стеганоперетворення та після внесення повідомлення до зображення.

а б в г

Рисунок 3.16. Зображення: а – оригінал зображення, б – метод заміни НЗБ, в – метод псевдовипадкового інтервалу, г – метод блокового приховування

3.2. Критерії оцінки стеганографічних методів

Для оцінювання якості стеганографічного методу застосовують аналітичні методи дослідження на основі аналізу їхніх статистичних характеристик. Для здійсненя порівняння якості засобів стеганографії розробляють різноманітні показники, які дають можливість кількісної оцінки. У рамках даної дипломної роботи будуть використані такі показники оцінки стеганографічної системи:

- зміна розміру графічного файлу у якому зберігається контейнер–результат;
- кореляція зображення–оригіналу та зображення–результату;
- якість зображення після стеганоперетворення;
- час вбудовування повідомлення до контейнера.

3.2.1. Показник зміни розміру файлу

У сучасному світі є багато форматів файлів для безпосередньо растрових зображень. Таке зображення зберігається тільки у стиснутому вигляді. І залежить від алгоритму стиснення можливе чи не можливе подальше відновлення картинкиу відповідній точності таким, як було до того як було стиснено. В залежності від того, який формат файлу використовується для зберігання контейнера–результату, можлива зміна розміру файлу. При проведенні атаки на основі відомого порожнього контейнеру, можливе виявлення стеганосистеми через зміну розміру файлу після стеганоперетворення.

3.2.2. Кореляція зображень

Під кореляцією розуміють статистичну залежність двох випадкових величин. Математична міра кореляції двох випадкових величин – це коефіцієнт кореляції. Найбільш відомий коефіцієнт кореляції Пірсона. При визначенні взаємозв’язку двох різних зображень використаємо наступну формулу коефіцієнта кореляції Пірсона:

$$r_{xy} = \frac{\frac{1}{n} \times \sum_{i=1}^{n} (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n} (x_i - \bar{x})^2} \times \sqrt{\sum_{i=1}^{n} (y_i - \bar{y})^2}}. \quad (3.3)$$

Формулу (3.3) можливо подати у такому вигляді:

$$r_{xy} = \frac{\frac{1}{n} \times \sum_{i=1}^{n} (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{S_x^2} \times \sqrt{S_y^2}}, \quad (3.4)$$

де $\bar{x}, \bar{y}$ – це середні значення для вибірки x та y; S – це відповідно середньоквадратичне відхилення.

Такий коефіцієнт кореляції має вимірювання у межах від –1,00 до +1,00. У випадку, коли коефіцієнт кореляції з мінусом, це свідчить про наявність протилежного зв'язку: коли вище значення однієї змінної, тоді нижче значення безпосередньо іншої. А сила зв'язку описується і величиною коефіцієнта кореляції, яка є абсолютною. Щоб описати величини коефіцієнта кореляції використовуються градації, що наведені в табл. 3.1.

Таблиця 3.1. Градації коефіцієнта кореляції

№	Значення	Інтерпретація
1	0,0 – 0,2	дуже слабка кореляція
2	0,2 – 0,4	слабка кореляція
3	0,4 – 0,7	середня кореляція
4	0,7 – 0,9	висока кореляція
5	0,9 – 1,0	дуже висока кореляція

3.2.3. Якість зображення після стеганоперетворення

Показник якості зображення належить до групи різницевих показників спотворення, який базується на різницях між контейнером–оригіналом і контейнером–результатом. Щоб визначити показники спотворення якості зображення використаємо наступну формулу:

$$IF = 1 - \frac{\sum_{i=1}^{n} (C_i - S_i)^2}{\sum_{i=1}^{n} (C_i)^2}, \quad (3.5)$$

де Ci – піксель порожнього контейнера, а через Si – відповідний піксель заповненого контейнера. Для визначення величини спотворення якості зображення застосуємо формулу, що базується на різниці між якістю контейнера–оригіналу та якості контейнера–результату:

$$DIF = 1 - (1 - \frac{\sum_{i=1}^{n} (C_i - S_i)^2}{\sum_{i=1}^{n} (C_i)^2}). \quad (3.6)$$

Вираз (3.6) можна виразити таким чином:

$$DIF = 1 - (IF), \quad (3.7)$$

де 1 – значення якості зображення–оригіналу, а IF – якість зображення після стеганоперетворення. Розглянуті показники базуються на аналізі елементів контейнера (пікселів зображення).

3.2.4. Час вбудовування повідомлення до контейнера

Даний показник оцінки стеганографічної системи базується на кількості часу необхідного для вбудовування повідомлення до стеганографічного контейнера для подальшого передавання по стеганографічній системі. Зменшення даного показника призводить до виграшу часу обробки інформації та збільшенні кількості обробляючої інформації.

3.3. Формат файлів растрового зображення

Зберігання растрових зображень відбувається під виглядом якихось файлів. У сучасному світі є безліч форматів файлів для растрових зображень. А растрове зображення безпосередньо зберігається в стиснутому вигляді. Отже, в залежності від певних алгоритмів стиснення може бути можливим чи неможливим відновлення

зображення в точності таким самим, яким воно було до стиснення. На рисунку 3.17 зображені найпоширеніші формати файлів растрового зображення.

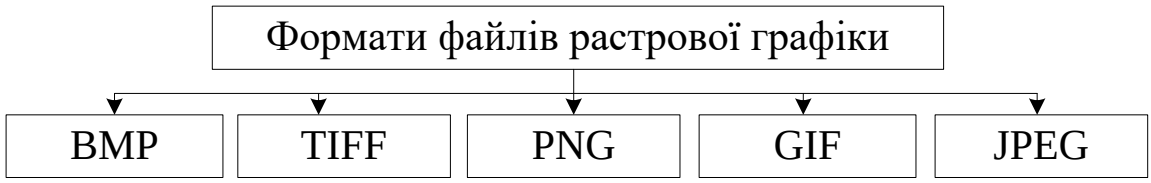


Рисунок 3.17. Формати файлів растрового зображення

3.3.1. Формат BMP файла

З даним форматом працює велика кількість програм, через те, що його підтримка інтегрована в ОС Windows. Колірна глибина BMP формату може бути 2 – 48 біт на піксель, а при максимальних розмірах растру – 65535×65535. BMP – файл містить 4 частин.

Частина BITMAPFILEHEADER, що має у собі опис файлу, і його розмір дорівнює 14 байтів (Рисунок 3.18). Далі розташований заголовок зображення – BITMAPINFOHEADER, в ньому міститься опис розмірної скаладової растру та пікселів колірного формат. Його розмір – 40 байт. Ще одгна складова – це палітра (RGBQUAD). Розміри такої палітри залежать від кількості різних кольорів. У деяких випадках палітра може бути не у складі. Згодом після палітри, у BMP–файлі, розташовується растр як масив [24].

Кількість байт, у масиві, визначається розмірами растрової компоненти та безпосередньо бітовою кількістю на 1 піксель. Формат BMP має підтримку стиснення без певниз втрат за використанням алгоритму RLE (Рисунок 3.19). Цей алгоритм базується на такому принципі: заміна повторювані групи елементів вихідної певної послідовності на 1 пару (а саме “довжина–символ”), також можливий варіант тільки довжину. Отже, стиснення в RLE спостерігається за рахунок певної послідовності однакових байт в початковому зображенні. Заміна їх на пари зменшує надлишковість даних [25].

Рисунок 3.18. Структура BMP–файлу

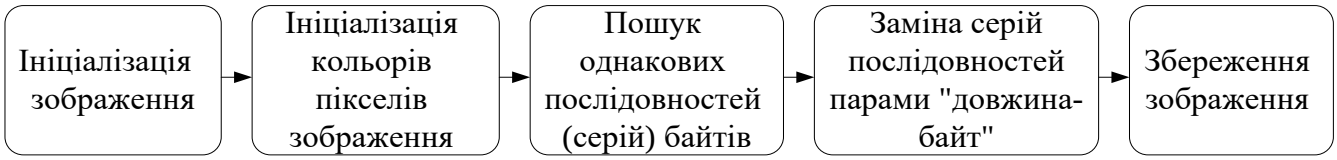


Рисунок 3.19. Структурна схема реалізації алгоритму RLE

3.3.2. Формат GIF файла

GIF (Graphics Interchange Format) – це растровий графічний формат, який використовує до 256–и індексованих кольорів безпосередньо із певного 24–х бітного діапазону кольору RGB. Картинка цього формату спостерігається зберіганням порядкове, з підтримкою тільки формату з певною кількістю палітри кольорів.

GIF–формат використовує стиснення за алгоритмом, який має назву LZW (Рисунок 3.20), що у складі із індексованими різноманітними кольорами дає можливість бути даному формату ідеальним для зберігання, а також передачі картинок з невеликою кількістю кольорів. Алгоритм стискання LZW відносять до такого формату стиснення, що відбувається без втрат. Тобто, при відновлені з формату GIF, певна інформація точно буде відповідати оригіналу. За такого виду стисненні створюється пошук комбінацій різних кольорів, які повторюються ("фраз"), і вписуються під виглядом ключів. Щоб закодувати каритинку використовують ключі, які вже бути створені. Такий вид методу є більш

досконалим RLE при роботі з областями, що мають переходи кольорів, однак кодування в LZW вимагає більше системних ресурсів [25].

Отже, можна зробити висновок, що гарно стискаються картинки, рядки у яких містять у собі ділянки, що повторюються. Формат GIF дозволяє це через строкове збереження даних. Під час цього рядки розбивають на певні групи, а також змінюють безпосередньо порядок зберігання рядків у певному файлі. Коли відбувається завантаження, картинка зображується поступово. Дякуючи такому, коли є тільки частина певного файлу, є можливість побачити картинку повністю, але з більш меншим дозволом.

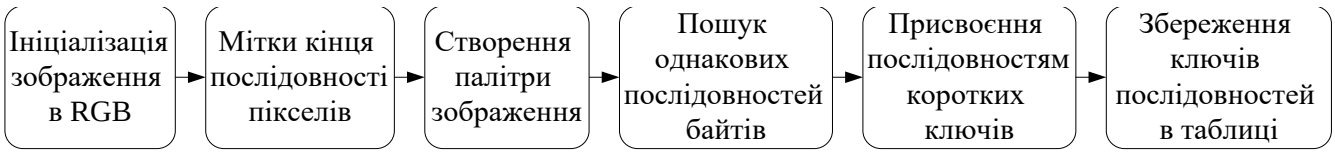


Рисунок 3.20. Структурна схема реалізації алгоритму LZW

Особливістю GIF–формату є підтримка анімаційних картинок, які визначаються під виглядом певної послідовності з деяких кадрів, що є статичними, і одночасно інформацією про те, за скільки часу має бути кожен кадр відображено екраном.

3.3.3. Формат PNG файла

PNG–формат спроектований для заміни більш простого GIF–формату. Растровий формат для збереження графічної інформації PNG, що використовується для стиснення без втрат. Формат PNG був розрахований, перш за все, для використання в мережі Інтернеті та редагування графіки. Даний формат підтримує растрові зображення з глибиною кольорів 16, або 24, а також 48 біт.

Такому формату характерний більш сильніший рівень стиснення файлів з великою кількістю кольорів ніж формат GIF. В PNG–форматі використовується

стиснення без втрат за алгоритмами Deflate. В цьому алгоритмі використовується комбінація алгоритмів LZ77 і Хаффмана [25].

Алгоритм LZ77 побудований за принципом ковзаючого вікна та механізмом кодування певних збігів (Рисунок 3.21). Така методика кодування разом з принципом ковзаючого вікна має у собі вже раніше переглянуту частину інформації, яку використовує як словник. Він намагається замінити черговий фрагмент повідомлення на покажчик у зміст певного словника. А ковзаюче вікно можливо відобразити під виглядом буфера, що організований так, щоб запам'ятовувати переглянуту раніше інформацію, а також давати доступ до неї. Через це, друга і ще одна поява збігів однакової послідовності кольорів пікселів може бути замінено на посилання на першу їх появу. Якщо виникають збіги, то вони мають кодування парою: зміщення, а також довжина збігу. Кодована пара має трактування як команда, що здійснює копіювання символів, певною довжиною збігу, з безпосередньо позиції ковзаючого вікна, що має вигляд зміщенного. Використовування такої пари, що є кодованою довжина–зміщення є дуже ефективним у випадку, коли значення довжини перевищує значення зміщення [25].

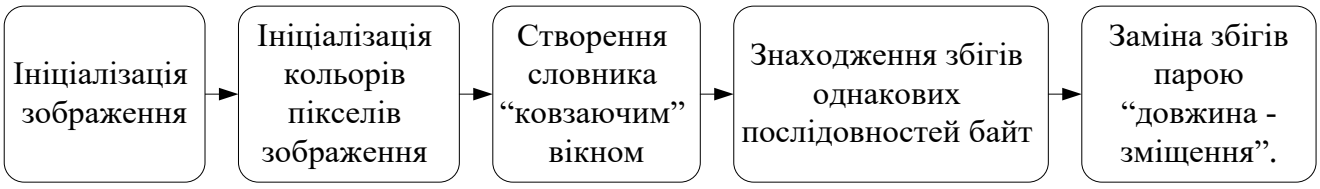


Рисунок 3.21. Схема реалізації алгоритму LZ77

Алгоритм Хаффмана використовує частоти появи однакових байт елементів зображення (Рисунок 3.22). Зіставляються символам вхідного потоку, що зустрічаються більшу кількість разів, послідовність цих біт, що є меншої довжини, а також навпаки. Перший етап алгоритму – це безпосередньо зчитування файлу картинки та вирахування частоти відображення кожного байту певного кольору. Згодом створюється таблиця відповідності байту кольору його частоті та впорядковуємо за зменшенням. Ще один етап – це побудова деревоподібної

структури з використанням створених вузлів таблиці. Після створення дерева відбувається шифрування файлу та зберігання дерева, що є декодуючим. Тоді алгоритм Хаффмана читає вхідний файл двічі, один раз підраховуючи частоти появи байтів, іншим разом виконуючи безпосередньо кодування.

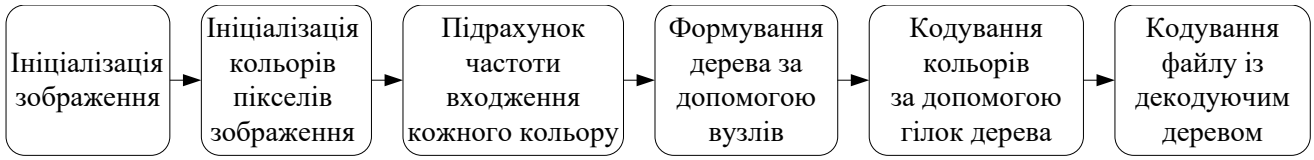


Рисунок 3.22. Схема реалізації алгоритму Хаффмана

Дані, які кодуються у форматі Deflate мають певний набір блоків, і їх порядок збігається разом з порядком певних блоків, що є вихідними даними. Блоки першого типу не можуть бути більше, ніж 64 кбайт. Кожний блок другого та третього типу містить у собі дві частини: описи двох таблиць кодів Хаффмана, які використовуються для кодування даних блоку та власне закодованих даних [25].

Щоб знайти фрази використовують метод хеш–ланцюгів. Хеш–функція рахується через три байти даних. У кожний крок компресор зчитує черговий 3–байтовий рядок, який має розташування на початку буфера. Хеш–ланцюжок має аналізування з метою знайти найдовший збіг між фразами та буфером, на котрі дають посилання елементи (вузли) хеш–ланцюжка. Відновлення хеш–ланцюжків виконано так, що пошук розпочинається з нових вузлів, які дають змогу змістити розподіл певних частот зсувів фраз, що є кодованими на користь певних коротких зміщень, таким чином покращити стискання, через те, що малі зсуви містять коди невеликої довжини. Для прискорення кодування в разі обробки певних даних, які є надлишковими досить довгі хеш–ланцюжки здійснюють скорочення до довжини, яка задана параметрами цього алгоритму. Таке скорочення відбувається в залежності від таких довжин вже знайдених збігів: якщо вони довші, то більше скорочуємо.

3.3.4. Формат JPEG файла

JPEG – це такий формат збереження інформації, що є растровим, та з використанням стиснення з втратами. Даний алгоритм стиснення найбільш підходить для фотографій та картинок, що мають реалістичні дані із певними змінами кольору та яскравості. Найбільшого застосування, цей формат отримав у цифрових фото та передавання графічної інформації через мережу Інтернет.

Безпосередньо при проведенні стиснення, зображення перетворюється з колірного моделі RGB в YUV (Рисунок 3.23). Після перетворення, для каналів зображення U і V, які відповідають за кольори, може виконуватися "проріджування ", а саме, кожний блок з 4 пікселів яскравого каналу Y зіставлені у певну відповідність усереднені значення U і V. Отже, кожний блок 2 на 2 замість дванадцяти значень (4Y, 4U і 4V) використовує всього шість (4Y, а це означає, що по одному усередненому U і V). Наступний компонент Y та компоненти U і V, що відпровідають за колір, розділяються на блоки 8 на 8 пікселів. Кожен з такий блоків піддається дискретномо–косинусному перетворенню (ДКП). Коефіцієнти ДКП, що отримались, квантуються та пакуються з використанням коду Хаффмана [24].

Рисунок 3.23. Структурна схема для реалізування алгоритму JPEG

Матриці, що використовують для кількісного визначення коефіцієнтів DCT, зберігаються в заголовку файлу JPEG. Здебільшого, вони будуються таким чином, що високочастотні коефіцієнти піддаються сильнішому квантуванню, ніж низькочастотні. Як результат, картинка стає менш детальною. Отже, вищий ступінь стиснення, то сильніше квантування всіх коефіцієнтів.

3.3.5. Формат TIFF файла

TIFF – це формат збереження растрових зображень графіки. TIFF застосовується при зберіганні зображення з великою глибиною кольору. Завдяки своїй сумісності з більшістю професійного програмне забезпечення, що призначене для обробки зображень, формат TIFF має зручність при передачі зображень між різними типами комп'ютерів (наприклад, з ПК на Mac). Структура формату дає можливість збереження картинок за допомогою палітри, а також у різних просторах кольору. TIFF має можливість зберігати зображення із стисненням та без стиснення. Ступень стиснення залежить від особливостей самого зберігається зображення, а також від алгоритму. Формат TIFF має можливість використання таких алгоритмів стиснення: LZW, RLE та JPEG. Алгоритм JPEG – це інкапсуляція JPEG-формату у формат TIFF. Формат TIFF дає можливість збереження зображення, по алгоритму стандарту JPEG, не втрачаючи дані (JPEG–LS) [25].

Тому формат файлу зображення вказує, як стиснути растрове зображення. Таким чином, стиснення без втрат здійснюється при збереженні картинок у форматах GIF, PNG та BMP (зменшення надмірності). Стиснення з певними втрат проходить у форматі JPEG (частина інформації відкидається). Формат TIFF має стиснення як з втратами так і без втрат.

3.4. Дослідження сучасних графічних форматів в умовах реалізації процесів стеганозахисту

В якості носія прихованої інформації, найчастіше, використовується растрове зображення. Растрове зображення зберігається як певний файл. Кожний файл картинки відповідає своєму формату, залежно від алгоритму збереження графіки. Залежно від формату, є можливість змінити розмір файлу під час введення повідомлення в зображення. Метою проведення аналізу є знаходження оптимальнішого типу графічного файл для передавання повідомлення стеганоканалом.

Для оцінки зміни розміру файлу оригіналу контейнера та результату контейнера використано синій компонент статичного 24-бітового RGB-зображення із розміром растру безпосередньо 240x240. Для проведення визначення оптимального формату файлу розмір місця синьої складової, що модифікувався, складав від 20% до 100%. Модифікування виконувалось методом заміни найменше значущого біту елементу зображення (Рисунок 3.24).

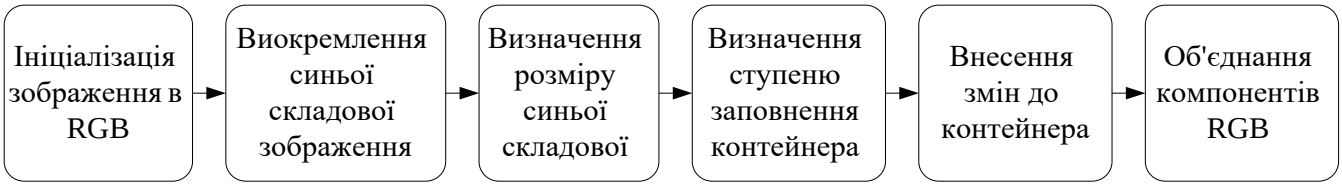


Рисунок 3.24. Реалізація структурної схеми приховування інформації в компоненту синього кольору

Наведемо приклад програми у MathCAD, яка дозволяє здійснити модифікацію певної частини зображення BMP–формату та збереження нового зображення.

Першим етапом реалізація даного стеганоперетворення є ініціалізація зображення в RGB–форматі за допомогою вбудованої функції – READRGB("директорія та ім’я файлу"). Виокремлення синьої складової зображення виконаємо за допомогою функції READ_BLUE("директорія та ім’я файлу"). Дана функція відокремить масив числових значень елементів синьої складової із зображення. Наступним етапом є визначення розміру синьої компоненти зображення. Для цього виконаємо такі дії: визначимо кількість рядків та стовпців компоненти та знайдемо їх добуток – Sc (Рисунок 3.25). У результаті виконання даних дії можна побачити, що кількість рядків та стовпців становить – 240×240. Таким чином, розмір синьої складової становить – 57600 елементів зображення.

Визначення ступеню заповнення контейнера, у відсотках, задається користувачем – P (1% – 100%). Змінна Bs відображає кількість елементів зображення, що будуть модифіковані при даному параметрі P. У даному випадку процент заповнення становить 20% від розміру синьої компоненти зображення.

ORIGIN := 1

Picture := "PictureBMP.bmp"

RED := READ_RED(Picture) GREEN := READ_GREEN(Picture) BLUE := READ_BLUE(Picture)

C := BLUE

Cc := cols(C) = 240

Rc := rows(C) = 240

Sc := Cc·Rc = 57600

Рисунок 3.25. Блок А.1.1

Для більш зручного виконання модифікації виконаємо перетворення масиву числових значень контейнера у вектор – стовпець за допомогою модуля Vec (Рисунок 3.26). Функція stack виконує об'єднання кожного стовпця масиву у вектор–стовпець один під одним.

$$P := 20$$

$$Bs := \frac{P \cdot Sc}{100} = 11520$$

$$Vec := \left| \begin{array}{l} Vec \leftarrow C^{\langle 1 \rangle} \\ \text{for } i \in 2..cols(C) \\ \quad Vec \leftarrow stack\left(Vec, C^{\langle i \rangle}\right) \end{array} \right.$$

Рисунок 3.26. Блок А.1.2

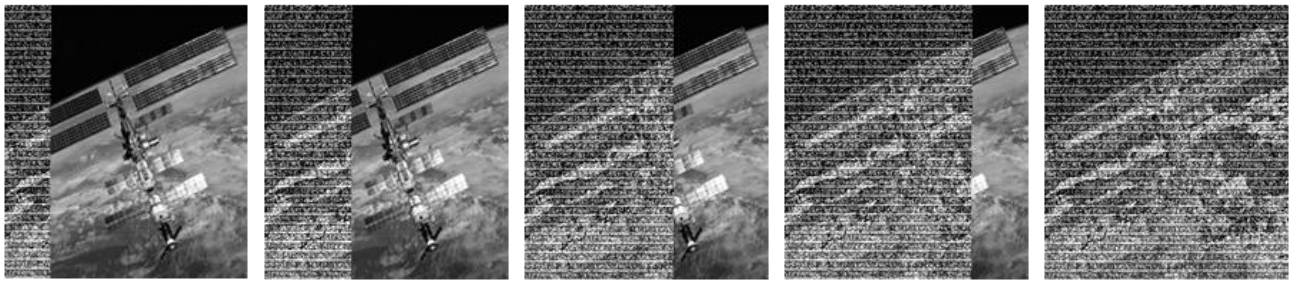
Внесення змін до контейнера виконує модуль Nvec. Даний модуль виконує перетворення кожного байту елементу масиву Vec в двійковий код та замінює молодший біт на протилежний. Після цього, даний блок виконує зворотне перетворення двійкового коду у байт елементу зображення. У результаті виконання роботи даного модуля ми отримаємо модифікований вектор–стовпець елементів синьої складової зображення. Останній етап реалізації стеганоперетворення полягає у тому, щоб об'єднати колірні компоненти зображення в один масив та зберегти результуюче зображення у файлі BMP–формату (Рисунок 3.27).

Для знаходження оптимального формату файлу для стеганографічного перетворення виконаємо порівняння цих зображень, які були отримані на основі показника змінювання розміру файлу.

```
Nvec := | Nvec ← Vec
        | for μ ∈ 1..Bs
        |   P ← D2B(Vec_μ)
        |   P_1 ← 1 if P_1 = 0
        |   P_1 ← 0 otherwise
        |   Nvec_μ ← B2D(P)
        | Nvec
Np := | for i ∈ 1,2..cols(C)
      |   Np^(i) ← submatrix[Nvec,(i − 1)·rows(C) + 1,i·rows(C),1,1]
      | augment(RED,GREEN,Np)
WRITERGB("PictureBMP_2.bmp") := Np
```

Рисунок 3.27. Блок А.1.3

На Рисунок 3.28 візуально зображено ступінь заповнення контейнера для здійснення аналізу графічних форматів.



20% 40% 60% 80% 100%

Рисунок 3.28. Візуальне відтворення ступеню заповнення стеганоконтейнера

Результати розмірів файлів після стеганоперетворення в залежності від ступеня заповнення наведені у таблиці 3.2.

Таблиця 3.2.

Розмір графічного файлу

№	Формат файлу	Ступінь заповнення стеганоконтейнера, %					
		0 %	20%	40%	60%	80%	100%
		Розмір файлу після стеганографічного перетворення, байт					
1	TIFF	201 201	201 209	201 209	201 217	201 209	201 213
2	BMP	171 853	171 853	171 853	171 853	171 853	171 853
3	PNG	109 184	109 468	109 578	109 657	109 720	109 808
4	JPEG	48 016	48 019	48 021	48 029	48 010	48 019
5	GIF	41 555	41 620	41 625	41 569	42 587	41 639

При оцінюванні отриманих зображень за показником розміру файлу, можна побачити, що при заповненні зображення із форматом BMP, інформаційним повідомленням, розмір файлу не змінюється. При заповненні зображення JPEG, GIF, TIFF та PNG–формату – розмір файлу змінюється.

Отже, за даним показником оцінювання, BMP–формат є оптимальнішим для реалізації стеганографічного методу приховування інформації. Розмір файлу не змінюється (Рисунок 3.29). Це зумовлено насамперед тим, що стиснення, відбувається за рахунок за рахунок послідовності однакових байт, в початковому зображенні.

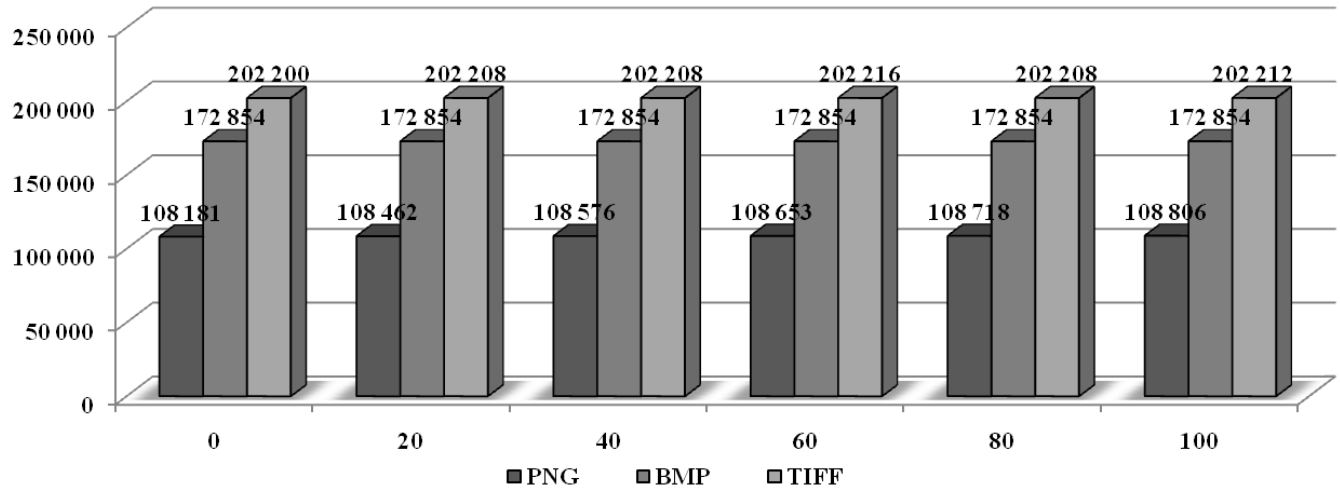


Рисунок 3.29. Розмір PNG, BMP та TIFF–файлів в залежності від ступеню заповнення

Зміна розмірів файлу інших графічних форматів зумовлена певним алгоритмом стиснення безпосередньо інформаційної послідовності. Найменш надійний – це формат файлу JPEG. Максимальний розмір даного файлу становив 47 027 байтів. Як можна побачити, зміна у розмірі при проведенні аналізу становила від 1 до 12 байтів (Рисунок 3.30). JPEG використовує стиснення з втратами.

При використанні файлу із форматом TIFF, розмір файлу змінювався в діапазоні 8 – 16 байтів. Максимальним розмір файлу становив – 202 216 байт при 60% заповненні контейнера. Формат TIFF дозволяє використовувати такі алгоритми стиснення: RLE, LZW та JPEG.

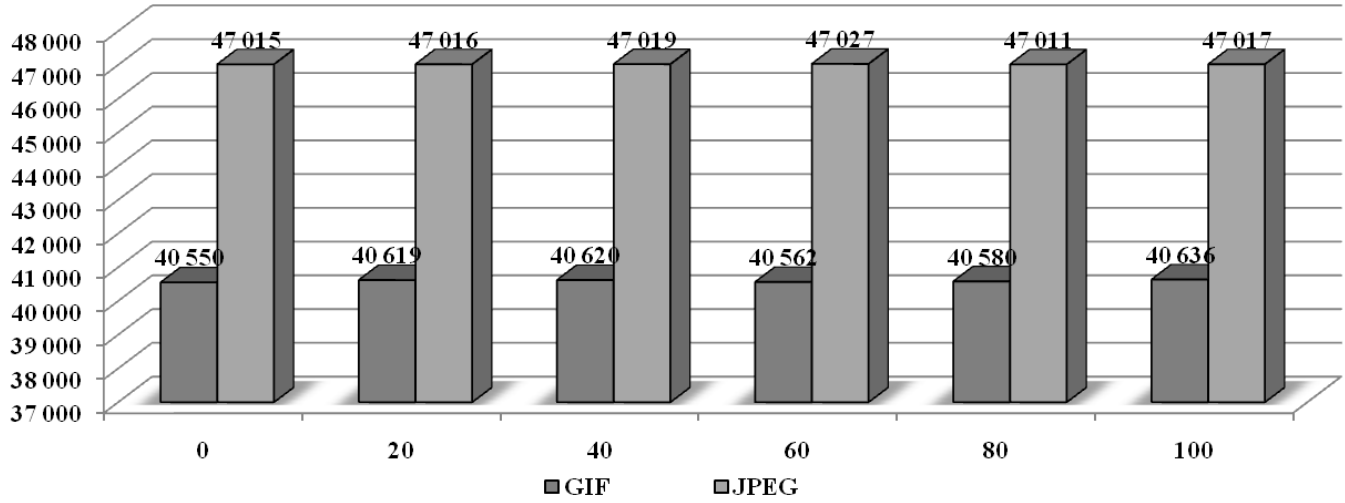


Рисунок 3.30. Розмір GIF та JPEG–файлів в залежності від ступеню заповнення

Під час проведення випробувань стійкості файлів до стеганоперетворювань, зміна розміру файлу із форматом GIF змінювався від 12 до 70 байтів. У GIF–форматі використовується стиснення за алгоритмом LZW. При даному стисненні відбувається пошук повторюючих комбінацій байт, які записуються у вигляді ключів. Максимальне значення розміру файлу становило 40 636 байт при умові, що оригінал зображення мав розмір – 40 550 байт.

При використанні файлу із форматом PNG, розмір файлу змінювався від 354 до 625 байтів. Оригінал зображення мав розмір – 108 181 байт, а максимальне значення розміру становило 108 806 байт при 100% заповненні. PNG використовує

стиснення за допомогою алгоритма Deflate. Такий алгоритм використовує комбінацію алгоритмів LZ77 та Хаффмана.

Отже, на основі проведених досліджень, визначено найстійкіший оптимальніший формат файлу до стеганографічний перетворень. За результатами досліджень, найоптимальнішим є BMP–формат. При внесенні прихованих повідомлень зберігається розмір файлу, що підвищує стійкість стеганосистеми до стеганоаналізу. Такі формати графічних файлів не досить стійкі до стеганографічний перетворень. Отже, це зумовлено змінами у розмірі файлу, що підвищує шанси порушника до виявлення стеганоканалу.

3.5. Колірні моделі растрового зображення

Більшість відтінків утворюється шляхом змішування основних кольорів. Спосіб поділу колірних відтінків на складові називається колірною моделлю. Існує багато різноманітних типів колірних моделей – RGB, CMYK, XYZ, HSV, RYB, LAB, PMS, LMS і т.д.

Колірні моделі можна класифікувати за областю застосування та спрямованості [24]:

- адитивні моделі – методи отримання кольору на екрані монітора (приклад, RGB).
- моделі поліграфії – отримуєтья колір при використанні різноманітних систем фарб, а також обладнання поліграфії (приклад, CMYK).
- моделі, що не пов'язані з фізикою обладнання, що є безпосередньо стандартом для передачі інформації.
- моделі математичні, які корисні для будь–яких способів коректування, і не пов'язані з обладнанням, наприклад HSV.

В комп’ютерній графіці, як правило, застосовуються колірні моделі що зазначені на Рисунок 3.31.

Рисунок 3.31. Найпоширеніші колірні моделі

3.5.1. Модель HSV (HSB).

HSV – це така модель, що здатна тописати колірний простір, який побудований на 3–х характеристиках кольору: тоні (Hue), насиченості (Saturation), значення яскравості (Value або Brightness). Колірний простір моделі HSV має конусне відображення (Рисунок 3.32). Розглянемо більш детально колірний простір [25]:

- тон кольору (спектральний колір) – характеризується позицією компоненти H на колірному колі, а також рахується величиною кута $0 – 360^0$;
- насиченість (S) – це параметр, що визначає чистоту кольору. Насиченість змінюється в діапазоні 0% – 100%. По краям колірного кола розташовані дуже насичені кольори (тобто, значення насиченості має показник 100%). Це означає, що із зменшенням S колір освітлюється. Якщо насиченість 0 відсотків, будь–який колір буде білим;
- яскравість (B або V) – колірний параметр, який характеризується освітленістю кольору. Яскравість має діапазон від 0 до 100%. Щоб зменшити яскравость кольору потрібно додавати до кольору чорний колір. Зменшення яскравості означає затемнення кольору.

Колірну модель HSV використовують комп’ютерні художники при створенні зображень у графічних редакторах. Після створення зображення, його треба перетворити на колірну модель CMYK або RGB. Модель перетворюється в RGB для того, щоб відобразити картинку на екрані монітора, а в безпосередньо CMYK – щоб отримати друковане зображення. Розглянемо перетворення колірних компонентів між моделями RGB та HSV.

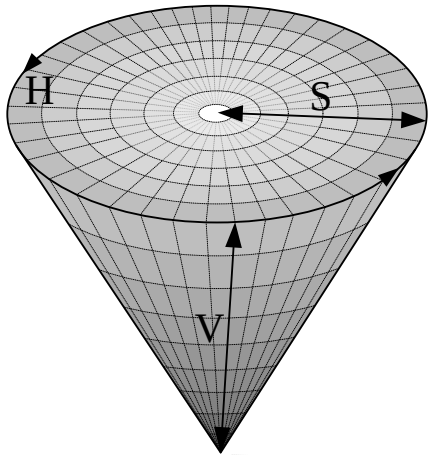


Рисунок 3.32. Колірний простір HSV.

RGB→HSV. Нехай, нам відомо значення пікселя – P(R,G,B). Для знаходження його значень в моделі HSV – P(H,S,V), необхідно виконати перетворення (3.8) – (3.14).

Для більш зручнішого виконання перетворення колірних компонентів моделі RGB у модель HSV, виконаємо перетворення за формулами:

$$R = \frac{r}{255}, \qquad G = \frac{g}{255}, \qquad B = \frac{b}{255}, \tag{3.8}$$

де r, g, b – відповідні значення елементів колірних компонентів моделі RGB.

Значення кольору – V, відповідає максимальному значенню серед R,G,B, що обчислюється за формулою:

$$V = \max(R, G, B). \tag{3.9}$$

Визначення насиченості S, відбувається з наступних умов:

$$S = \frac{\max(R, G, B) - \min(R, G, B)}{\max(R, G, B)}. \tag{3.10}$$

Для визначення значень H, S, V, необхідно виконати такі попередні підрахунки:

$$DR = \frac{\left(\left(\frac{\max(R,G,B) - R}{6}\right) + \left(\frac{\max(R,G,B) - \min(R,G,B)}{2}\right)\right)}{\max(R,G,B) - \min(R,G,B)}, \tag{3.11}$$

$$DG = \frac{\left(\left(\frac{\max(R,G,B) - G}{6}\right) + \left(\frac{\max(R,G,B) - \min(R,G,B)}{2}\right)\right)}{\max(R,G,B) - \min(R,G,B)}, \quad (3.12)$$

$$DB = \frac{\left(\left(\frac{\max(R,G,B) - B}{6}\right) + \left(\frac{\max(R,G,B) - \min(R,G,B)}{2}\right)\right)}{\max(R,G,B) - \min(R,G,B)}. \quad (3.13)$$

Значення тону кольору (H) визначається наступним чином:

$$H = \begin{cases} DR - DG, \text{ якщо } R = \max(R,G,B) \\ \frac{1}{3} + DR - DB, \text{ якщо } G = \max(R,G,B). \\ \frac{2}{3} + DG - DR, \text{ якщо } B = \max(R,G,B) \end{cases} \quad (3.14)$$

У результаті виконання попередніх підрахунків можливо отримати значення елементів колірних компонентів моделі HSV із RGB.

HSV→RGB. При відомих значеннях пікселя P(H,S,V), в моделі HSV, можливо визначити значення R, G, B. Для більш зручного визначення виконаємо перетворення:

$$H = \frac{h}{360}, \qquad S = \frac{s}{255}, \qquad V = \frac{v}{255}. \quad (3.15)$$

де h, s, v – відповідні значення елементів колірних компонентів моделі HSV.

Для визначення значень r, g, b, необхідно виконати такі попередні підрахунки:

$$M = V \times (1 - S), \quad (3.16)$$

$$N = V \times (1 - S \times (6 \times H - \lfloor 6 \times H \rfloor)), \quad (3.17)$$

$$K = V \times (1 - S \times (1 - (6 \times H - \lfloor 6 \times H \rfloor))). \quad (3.18)$$

Після виконання підрахунків та знаходження допоміжних значень, можливо виконати обчислення значень r, g, b:

$$(r,g,b) = \begin{cases} (V,K,M) \times 255, \text{ якщо } I = 0 \\ (N,V,M) \times 255, \text{ якщо } I = 1 \\ (M,V,K) \times 255, \text{ якщо } I = 2 \\ (M,N,V) \times 255, \text{ якщо } I = 3 \\ (K,M,V) \times 255, \text{ якщо } I = 4 \\ (V,M,N) \times 255 \end{cases}. \quad (3.19)$$

Таким чином, можливо здійснювати перетворення колірних компонентів між моделями RGB та HSV.

3.5.2. Модель HLS.

HLS – це колірна модель, в якій координатами кольору є: Hue – що є тоном кольору, Lightness – що є світлістю кольору, а також Saturation – насиченість. Взагалі, колірна модель HLS є розширеною моделлю HSV. Різниця між цими моделями полягає в заміні компоненту яскравості (V) на компонент світлості кольору (L). У HLS колірний простір представляється у вигляді подвійного конуса (Рисунок 3.33), де вертикальна ось L – це світліть, а два інші компонети задані, як було в попередній моделі.

Світлость має діапазон від 0 до 100%. Значення 0% – це вершина нижнього конуса і вона відповідає за чорний колір. А білий колір великої інтенсивності світла задається вершиною верхнього конуса і відповідає значенню 100%. Максимально інтенсивні колірні тони відповідають основам конусів з L = 50%, що не зовсім зручно. Загалом, систему HLS можна представити як отриману з HSV шляхом витягуванням точки V = 100%, S = 0%, яка задає білий колір, вгору для утворення верхнього конуса. Розглянемо перетворення колірних компонентів між моделями RGB та HLS.

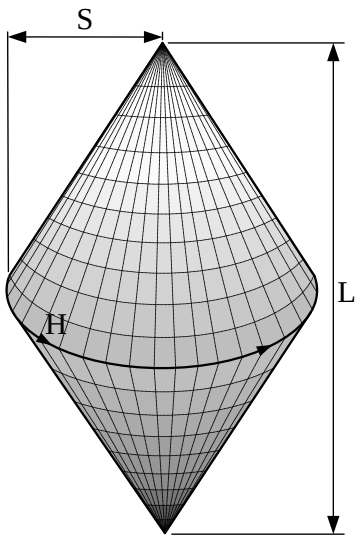


Рисунок 3.33. Колірний простір HLS.

RGB→HLS. Нехай, нам відомо значення елементу колірної моделі RGB. Для знаходження його значень в моделі HLS, необхідно виконати підрахунки (3.20) – (3.21).

Після виконання підрахунків визначення значень компоненти L виконаємо з наступної формули:

$$L = \frac{\max(R,G,B) + \min(R,G,B)}{2}. \tag{3.20}$$

Визначення насиченості S відбувається з наступних умов:

$$S = \begin{cases} \dfrac{\max(R,G,B) - \min(R,G,B)}{\max(R,G,B) + \min(R,G,B)}, \text{якщо } L \prec \dfrac{1}{2} \\ \dfrac{\max(R,G,B) - \min(R,G,B)}{2 - \max(R,G,B) + \min(R,G,B)} \end{cases}. \tag{3.21}$$

Знаходження значення компоненти (H) виконується аналогічно попереднього методу перетворення колірної моделі RGB у HSV.

3.5.3. Модель CMYK.

Дану модель використовують при підготовці не екранного, а друкованого зображення. Для підготовки друкованих зображень використовується не адитивна модель, а субтрактивна модель. Такою моделлю є CMYK, де C – це Cyan (тобто, блакитний), M – це Magenta (тобто, пурпурний), Y – Yellow (тобто, жовтий), а K – це BlacK (чорний). Просторова модель представлена у вигляді куба (Рисунок 3.34). Початок координат відповідає білому кольору. Три вершини даного куба дають чисті первинні відтінки кольорів, інші три – відображають подвійне суміщення вихідних кольорів.

У даній моделі кольори утворюються шляхами віднімання від білого основних кольорів моделі RGB. Наприклад, при відніманні червоного кольору від білого, утвориться блакитний колір.

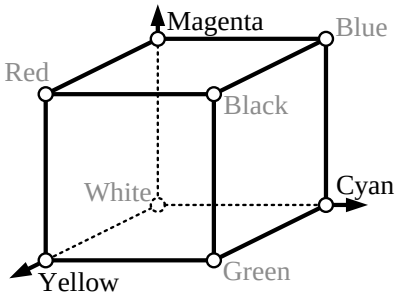


Рисунок 3.34. Колірна модель CMYK.

При відніманні синього кольору виникає жовтий, а при зеленому – пурпурний колір. Якщо встановити, що діапазон кожного кольору може змінюватися 0 – 255, тоді зв'язок між цими компонентами R, G, B і C, M, Y для однакового кольору може бути виражений формулою:

$$\begin{pmatrix} R \\ G \\ B \end{pmatrix} + \begin{pmatrix} C \\ M \\ Y \end{pmatrix} = \begin{pmatrix} 255 \\ 255 \\ 255 \end{pmatrix}, \qquad (3.22)$$

де R, G, B і C, M, Y – відповідні компоненти колірних моделей.

Теоретично чорний колір можна отримати суміщенням блакитного, пурпурного та жовтого кольору. Насправді змішування цих трьох відтінків дає невизначений темний колір. Такий відтінок не дає насиченості й глибини чорного кольору. При спробі надрукувати чорні елементи зображення, без чорного пігменту, відбувається неякісний збіг точок трьох різних кольорів, який призводить до деформації паперу. Перед друком, зображення розділяється на чотири складові. Тобто, при друкуванні зображення відбувається почергове накладання на папір блакитного, пурпурного, жовтого та чорного кольору, отримуючи повно кольорову ілюстрацію.

3.5.4. Модель YUV.

У колірному просторі YUV є один компонент, який представляє яскравість (Y – сигнал яскравості) і два інших компоненти, які представляють колір (U та V –

сигнал кольоровості). Модель широко застосовується в телемовленні, зберіганні та обробці відеоданих. Яскравість компонента містить «чорно–біле» (у відтінках сірого) зображення, а інші дві компоненти містять інформацію для відновлення належного кольору. Це було зручно в момент появи кольорового телебачення для сумісності зі старими чорно–білими телевізорами.

RGB → YUV. Виконання перетворення елементів моделі RGB в YUV.

$$Y = 0.299 \times R + 0.587 \times G + 0.114 \times B, \tag{3.23}$$

$$U = -0.14713 \times R - 0.28886 \times G + 0.436 \times B, \tag{3.24}$$

$$U = 0.615 \times R - 0.51499 \times G - 0.10001 \times B. \tag{3.25}$$

YUV → RGB. Перетворення компонентів YUV в RGB виконується з наступних формул.

$$R = Y + 1.13983 \times V, \tag{3.26}$$

$$G = Y - 0.39465 \times U - 0.5806 \times V, \tag{3.27}$$

$$B = Y + 2.03211 \times U. \tag{3.28}$$

3.5.5. Модель YIQ.

Модель застосовується в телемовленні за стандартами M–NTSC і M–PAL, де смуга частот відеосигналу помітно менше, ніж в інших телевізійних стандартах. Яскравість компонента містить «чорно–біле» (у відтінках сірого) зображення, а інші дві компоненти містять інформацію для відновлення належного кольору. Колір представляється як 3 компоненти – яскравість (Y) і двох штучних сигналів кольоровості (I і Q). Сигнал I називається синфазним, Q – квадратурний.

RGB → YIQ. Виконання перетворення елементів моделі RGB в YIQ.

$$Y = 0.299 \times R + 0.587 \times G + 0.114 \times B, \tag{3.29}$$

$$I = 0.596 \times R - 0.274 \times G + 0.322 \times B, \tag{3.30}$$

$$Q = 0.211 \times R - 0.522 \times G - 0.311 \times B. \tag{3.32}$$

YIQ → RGB. Конвертування елементів YUV в RGB виконується наступним чином.

$$R = Y + 0.956 \times I + 0.623 \times Q, \quad (3.33)$$

$$G = Y - 0.272 \times I + 0.648 \times Q, \quad (3.33)$$

$$B = Y - 1.105 \times I + 1.705 \times Q. \quad (3.34)$$

Використання моделі YIQ було вимушеною мірою. Психофізіологічні дослідження з'ясували, що роздільна здатність ока в кольорі менша, ніж у складовій яскравості очей. За рахунок цього при створенні сумісної системи кольорового телебачення вдалося зменшити смугу частот сигналу кольоровості в 3 – 4 рази. Подальші дослідження встановили, що до колірних переходів різного роду око має різну чутливість, що дозволило згрупувати так звані "теплі" і "холодні" відтінки, і в одній групі зменшити роздільну здатність ще в 3 рази. Тепер для передачі одного із сигналів було достатньо смуги всього в 0,5 МГц, при цьому верхня і нижня бічні смуги передавалися без обмежень.

3.6. Оцінка колірних моделей зображення в умовах реалізації процесів стеганозахисту для різних класів зображення

З результатів можна зробити висновок про доцільність використання, у якості контейнера, графічний файл із форматом BMP.

Різноманіття колірних моделей, на сучасному етапі розвитку, викликало питання про використання тих або інших моделей при підвищенні стійкості стеганосистеми до атак порушника. Метою даного аналіз є вибір оптимальнішої колірної моделі зображення для здійснення стеганоперетворення. При проведенні аналізу будуть використовуватись колірні моделі, що були розглянуті у пункті 4.2.

Попередні дані, що є вихідними відповідають деяким принятим при моделюванні форматам файлів.

Використаємо програми у MathCAD, що дає можливість зробити модифікацію певної частини зображення для реалізації аналізу колірних моделей. Проведемо перетворення компонентів R, G, B у компоненти H, S, V, здійснимо модифікацію контейнера та зворотне перетворення у модель RGB.

Першим етапом реалізація даного перетворення є ініціалізація зображення в RGB–форматі за допомогою вбудованої функції – READRGB("") та виділення кожної компоненти окремо. Наступним кроком є виконання перетворення, що здійснюються за допомогою формул (3.8). Виконання даних дії у системі MathCAD реалізовані у блоці А.2.1 на Рисунок 3.35.

$$BMP := \text{"D:\BMP\PictureBMP.bmp"}$$

$$PictureBMP := READ\_IMAGE(BMP)$$

$$RED := READ\_RED(BMP) \qquad GREEN := READ\_GREEN(BMP) \qquad BLUE := READ\_BLUE(BMP)$$

$$R(x,y) := \left(\frac{RED_{x,y}}{255}\right) \qquad G(x,y) := \left(\frac{GREEN_{x,y}}{255}\right) \qquad B(x,y) := \left(\frac{BLUE_{x,y}}{255}\right)$$

Рисунок 3.35. Блок А.2.1.

Наступним етапом перетворення є реалізація функції V(x,y), що виконує створення компоненти V за формулою (3.4). Виконання реалізації знаходження значень компоненти S, у колірній моделі HLS, проводиться за формулою (3.5) та зображено на Рисунок 3.36.

$$V(x,y) := \max(R(x,y), G(x,y), B(x,y))$$

$$S(x,y) := \frac{\max(R(x,y), G(x,y), B(x,y)) - \min(R(x,y), G(x,y), B(x,y))}{\max(R(x,y), G(x,y), B(x,y))}$$

Рисунок 3.36. Блок А.2.2

Для знаходження числового масиву значень компоненти H необхідно виконати попередні підрахунки за формулами (3.6) – (3.8). Реалізація функцій для виконання допоміжних підрахунків реалізована у блоці А.2.3.

Після виконання реалізації допоміжних функцій необхідно виконати підрахунок числовиго масиву компоненти H за формулою (3.14). Після виконання реалізації попередньої функції, виконаємо створення циклів, що виконують

підрахунок значень та створення масивів значень кожної компонентти H – Hue, S – Sat, V – Val. Реалізація даних циклів зображена на Рисунок 3.38 у блоці А.2.4

$$Max(x,y) := \max(R(x,y), G(x,y), B(x,y))$$

$$Min(x,y) := \max(R(x,y), G(x,y), B(x,y))$$

$$DR(x,y) := \frac{\left[\left[\frac{(Max(x,y) - R(x,y))}{6}\right] + \left(\frac{Max(x,y) - Min(x,y)}{2}\right)\right]}{Max(x,y) - Min(x,y)}$$

$$DG(x,y) := \frac{\left[\left[\frac{(Max(x,y) - G(x,y))}{6}\right] + \left(\frac{Max(x,y) - Min(x,y)}{2}\right)\right]}{Max(x,y) - Min(x,y)}$$

$$DB(x,y) := \frac{\left[\left[\frac{(Max(x,y) - B(x,y))}{6}\right] + \left(\frac{Max(x,y) - Min(x,y)}{2}\right)\right]}{Max(x,y) - Min(x,y)}$$

Рисунок 3.37. Блок А.2.3

В результаті виконання циклів, було отримано три числові масиви колірної моделі HSV. Далі виконаємо модифікацію певної частини контейнера. Модифікацію виконаємо згідно алгоритму блоків А.1.2 – А.1.3. Зворотне перетворення компонентів у модель RGB виконаємо згідно формули (3.2) – (3.6) (Рисунок 3.39).

$$H(x,y) := \begin{cases} H1 \leftarrow DB(x,y) - DG(x,y) \text{ if } R(x,y) = Max(x,y) \\ H1 \leftarrow \frac{1}{3} + DR(x,y) - DB(x,y) \text{ if } G(x,y) = Max(x,y) \\ H1 \leftarrow \frac{2}{3} + DG(x,y) - DR(x,y) \text{ if } B(x,y) = Max(x,y) \\ H1 \end{cases}$$

$$Sat := \text{for } i \in 1..cols(RED) \quad \text{for } j \in 1..rows(RED) \quad Sat_{j,i} \leftarrow S(j,i) \cdot 255$$

$$Val := \text{for } i \in 1..cols(RED) \quad \text{for } j \in 1..rows(RED) \quad Val_{j,i} \leftarrow V(j,i) \cdot 255$$

$$Hue := \text{for } i \in 1..cols(RED) \quad \text{for } j \in 1..rows(RED)$$
$$Hue_{j,i} \leftarrow (H(j,i) + 1) \cdot 360 \text{ if } H(j,i) < 0$$
$$Hue_{j,i} \leftarrow (H(j,i) - 1) \cdot 360 \text{ if } H(j,i) > 1$$
$$Hue_{j,i} \leftarrow 0 \text{ if } Max(j,i) - Min(j,i) = 0$$
$$Hue_{j,i} \leftarrow H(j,i) \cdot 360 \text{ otherwise}$$

Рисунок 3.38. Блок А.2.4

```
R1(x,y) := | R1 ← Val_2(x,y)  if  floor(Hue_2(x,y)·6) = 0
           | R1 ← Val_2(x,y)·[1 − Sat_2(x,y)·(Hue_2(x,y)·6 − floor(Hue_2(x,y)·6))]  if  floor(Hue_2(x,y)·6) = 1
           | R1 ← Val_2(x,y)·(1 − Sat_2(x,y))  if  floor(Hue_2(x,y)·6) = 2
           | R1 ← Val_2(x,y)·(1 − Sat_2(x,y))  if  floor(Hue_2(x,y)·6) = 3
           | R1 ← Val_2(x,y)·[1 − Sat_2(x,y)·[1 − (Hue_2(x,y)·6 − floor(Hue_2(x,y)·6))]]  if  floor(Hue_2(x,y)·6) = 4
           | R1 ← Val_2(x,y)  otherwise
           | R1·255
G1(x,y) := | G1 ← Val_2(x,y)·[1 − Sat_2(x,y)·[1 − (Hue_2(x,y)·6 − floor(Hue_2(x,y)·6))]]  if  floor(Hue_2(x,y)·6) = 0
           | G1 ← Val_2(x,y)  if  floor(Hue_2(x,y)·6) = 1
           | G1 ← Val_2(x,y)  if  floor(Hue_2(x,y)·6) = 2
           | G1 ← Val_2(x,y)·(1 − Sat_2(x,y))  if  floor(Hue_2(x,y)·6) = 3
           | G1 ← Val_2(x,y)·(1 − Sat_2(x,y))  if  floor(Hue_2(x,y)·6) = 4
           | G1 ← Val_2(x,y)·(1 − Sat_2(x,y))  otherwise
           | G1·255
B1(x,y) := | B1 ← Val_2(x,y)·(1 − Sat_2(x,y))  if  floor(Hue_2(x,y)·6) = 0
           | B1 ← Val_2(x,y)·(1 − Sat_2(x,y))  if  floor(Hue_2(x,y)·6) = 1
           | B1 ← Val_2(x,y)·[1 − Sat_2(x,y)·[1 − (Hue_2(x,y)·6 − floor(Hue_2(x,y)·6))]]  if  floor(Hue_2(x,y)·6) = 2
           | B1 ← Val_2(x,y)  if  floor(Hue_2(x,y)·6) = 3
           | B1 ← Val_2(x,y)  if  floor(Hue_2(x,y)·6) = 4
           | B1 ← Val_2(x,y)·[1 − Sat_2(x,y)·(Hue_2(x,y)·6 − floor(Hue_2(x,y)·6))]  otherwise
           | B1·255
```

Рисунок 3.39. Блок А.2.5.

Після реалізації функцій, виконаємо створення масивів компонентів R, G, B. Для цього створемо 3 цикли перетворення Red, Green, Blue (Рисунок 3.40).

```
Red := for i ∈ 1..cols(R)
         for j ∈ 1..rows(R)
           Red_{j,i} ← R1(j,i)

Green := for i ∈ 1..cols(R)
           for j ∈ 1..rows(R)
             Green_{j,i} ← G1(j,i)

Blue := for i ∈ 1..cols(R)
          for j ∈ 1..rows(R)
            Blue_{j,i} ← B1(j,i)
```

Рисунок 3.40. Блок А.2.6

Таким чином, було практично реалізовано метод перетворення моделі RGB у HSV та навпаки. Виконаємо реалізацію перетворення моделі RGB в HLS. Для

створення числової компоненти L та S використаємо формули (3.21) та (3.20), відповідно. Реалізація даних функцій перетворень зображена на Рисунок 3.41.

$$var\_Min(x,y) := min(var\_R(x,y), var\_G(x,y), var\_B(x,y))$$

$$var\_Max(x,y) := max(var\_R(x,y), var\_G(x,y), var\_B(x,y))$$

$$del\_Max(x,y) := var\_Max(x,y) - var\_Min(x,y)$$

$$L(x,y) := \frac{(var\_Max(x,y) + var\_Min(x,y))}{2}$$

$$S(x,y) := \begin{cases} S1 \leftarrow 0 \text{ if } del\_Max(x,y) = 0 \\ S1 \leftarrow \dfrac{del\_Max(x,y)}{(var\_Max(x,y) + var\_Min(x,y))} \text{ if } L(x,y) < \dfrac{1}{2} \\ S1 \leftarrow \dfrac{del\_Max(x,y)}{(2 - var\_Max(x,y) - var\_Min(x,y))} \text{ otherwise} \end{cases}$$

Рисунок 3.41. Блок А.3.1

Перетворення компонентів моделі RGB в компоненту H виконаємо аналогічно алгоритму, що представлений у блоках А.2.3 – А.2.4. Після цього здійснимо створення числових масивів компонентів моделі HLS (Рисунок 4.15).

$$Sat := \text{for } i \in 1..cols(R) \quad \text{for } j \in 1..rows(R) \quad Sat_{j,i} \leftarrow S(j,i) \cdot 255$$

$$Lig := \text{for } i \in 1..cols(R) \quad \text{for } j \in 1..rows(R) \quad Lig_{j,i} \leftarrow L(j,i) \cdot 255$$

$$Hue := \text{for } i \in 1..cols(R) \quad \text{for } j \in 1..rows(R) \quad \begin{cases} Hue_{j,i} \leftarrow (H(j,i) + 1) \cdot 360 \text{ if } H(j,i) < 0 \\ Hue_{j,i} \leftarrow (H(j,i) - 1) \cdot 360 \text{ if } H(j,i) > 1 \\ Hue_{j,i} \leftarrow 0 \text{ if } del\_Max(j,i) = 0 \\ Hue_{j,i} \leftarrow H(j,i) \cdot 360 \text{ otherwise} \end{cases}$$

Рисунок 3.42. Блок А.3.2

Далі виконаємо модифікацію певної частини контейнера для проведення аналізу колірних компонент. Модифікацію виконаємо згідно алгоритму, що здійснений у блоках А.1.2– А.1.3. Після внесення змін, необхідно виконати зворотне

перетворення компонентів HLS у компоненти моделі RGB. Для виконання зворотного перетворення скористаємося функцією, що реалізована у блоці А.3.3.

$$
\begin{aligned}
&\text{HLS2RGB}(v1, v2, vH) := \\
&\quad vH1 \leftarrow vH + 1 \ \text{ if } \ vH < 0 \\
&\quad vH1 \leftarrow vH - 1 \ \text{ if } \ vH > 1 \\
&\quad vH1 \leftarrow vH \ \text{ otherwise} \\
&\quad HR \leftarrow [v1 + (v2 - v1)\cdot 6\cdot vH1] \ \text{ if } \ vH1 < \frac{1}{6} \\
&\quad HR \leftarrow v2 \ \text{ if } \ \frac{1}{6} \le vH1 < \frac{1}{2} \\
&\quad HR \leftarrow \left[v1 + (v2 - v1)\cdot\left[\left(\frac{2}{3}\right) - vH1\right]\cdot 6\right] \ \text{ if } \ \frac{1}{2} \le vH1 < \frac{2}{3} \\
&\quad HR \leftarrow v1 \ \text{ otherwise} \\
&\quad HR
\end{aligned}
$$

Рисунок 3.43. Блок А.3.3.

Наступним етапом виконання перетворення є написання функцій створення масивів компонентів моделі RGB (Рисунок 3.44).

$$
\begin{aligned}
&R1(x,y) := \\
&\quad var\_2 \leftarrow Lig\_2(x,y)\cdot(1 + Sat\_2(x,y)) \ \text{ if } \ Lig\_2(x,y) < \frac{1}{2} \\
&\quad var\_2 \leftarrow (Lig\_2(x,y) + Sat\_2(x,y)) - (Lig\_2(x,y)\cdot Sat\_2(x,y)) \ \text{ otherwise} \\
&\quad var\_1 \leftarrow 2\cdot Lig\_2(x,y) - var\_2 \\
&\quad R1 \leftarrow \text{HLS2RGB}\left[var\_1, var\_2, \left(Hue\_2(x,y) + \frac{1}{3}\right)\right] \\
&\quad R1\cdot 255 \\
&G1(x,y) := \\
&\quad var\_2 \leftarrow Lig\_2(x,y)\cdot(1 + Sat\_2(x,y)) \ \text{ if } \ Lig\_2(x,y) < \frac{1}{2} \\
&\quad var\_2 \leftarrow (Lig\_2(x,y) + Sat\_2(x,y)) - (Lig\_2(x,y)\cdot Sat\_2(x,y)) \ \text{ otherwise} \\
&\quad var\_1 \leftarrow 2\cdot Lig\_2(x,y) - var\_2 \\
&\quad G1 \leftarrow \text{HLS2RGB}[var\_1, var\_2, (Hue\_2(x,y))] \\
&\quad G1\cdot 255 \\
&B1(x,y) := \\
&\quad var\_2 \leftarrow Lig\_2(x,y)\cdot(1 + Sat\_2(x,y)) \ \text{ if } \ Lig\_2(x,y) < \frac{1}{2} \\
&\quad var\_2 \leftarrow (Lig\_2(x,y) + Sat\_2(x,y)) - (Lig\_2(x,y)\cdot Sat\_2(x,y)) \ \text{ otherwise} \\
&\quad var\_1 \leftarrow 2\cdot Lig\_2(x,y) - var\_2 \\
&\quad B1 \leftarrow \text{HLS2RGB}\left(var\_1, var\_2, Hue\_2(x,y) - \frac{1}{3}\right) \\
&\quad B1\cdot 255
\end{aligned}
$$

Рисунок 3.44. Блок А.3.4.

Після реалізації функцій, виконаємо створення масивів компонентів R, G, B.

Для створення масивів створимо 3 цикли перетворення за допомогою написаних функцій Red, Green, Blue (Рисунок 3.45).

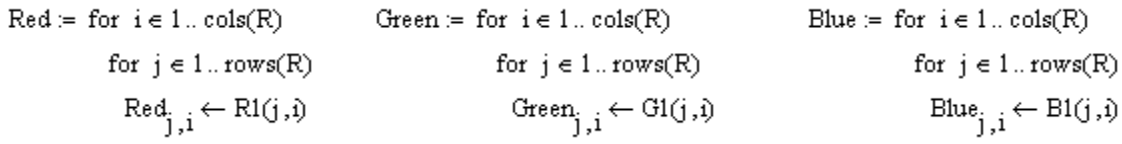


Рисунок 3.45. Блок А.3.5.

Таким чином, було практично реалізовано метод перетворення моделі RGB у HLS та навпаки.

Реалізацію перетворення моделі RGB в YUV та навпаки здійснювалося аналогічним чином згідно формул (3.23) – (3.28). Перетворення RGB в YIQ виконувалась згідно формул (3.29) – (3.34). В результаті виконання даних дії були отримані модифіковані зображення для проведення аналізу колірних компонентів.
При знаходженні оптимальної колірної моделі при передачі стеганографічного повідомлення проведемо порівняння зображень на основі таких показників: кореляція зображень та якість зображень після стеганоперетворення.

Було використано п’ять колірних моделей, а саме: RGB, HLS, HSV, YIQ та YUV. Ступінь модифікації контейнера становив 10% – 100%.

Значення коефіцієнтів кореляції, при використанні колірної моделі RGB, наведені у табл. 3.3.

Таблиця 3.3.

Коефіцієнт кореляції RGB моделі

№	Компонента	Ступінь заповнення контейнера, %					
		10%	20%	40%	60%	80%	100%
		Коефіцієнт кореляції					
1	R	0.99999666	0.99999314	0.99998523	0.99997628	0.99996663	0.99995669
2	G	0.99998724	0.999976	0.99995487	0.99993542	0.9999162	0.99989636
3	B	0.99999891	0.99999761	0.99999497	0.99999201	0.99998865	0.99998499

Графічне відображення значень коефіцієнтів зображено на Рисунок 3.46. Як можна побачити, кращою компонентою для приховування даних є синя компонента. Вона стійкіша до стеганоперетворення порівняно з іншими компонентами, червоною та зеленою.

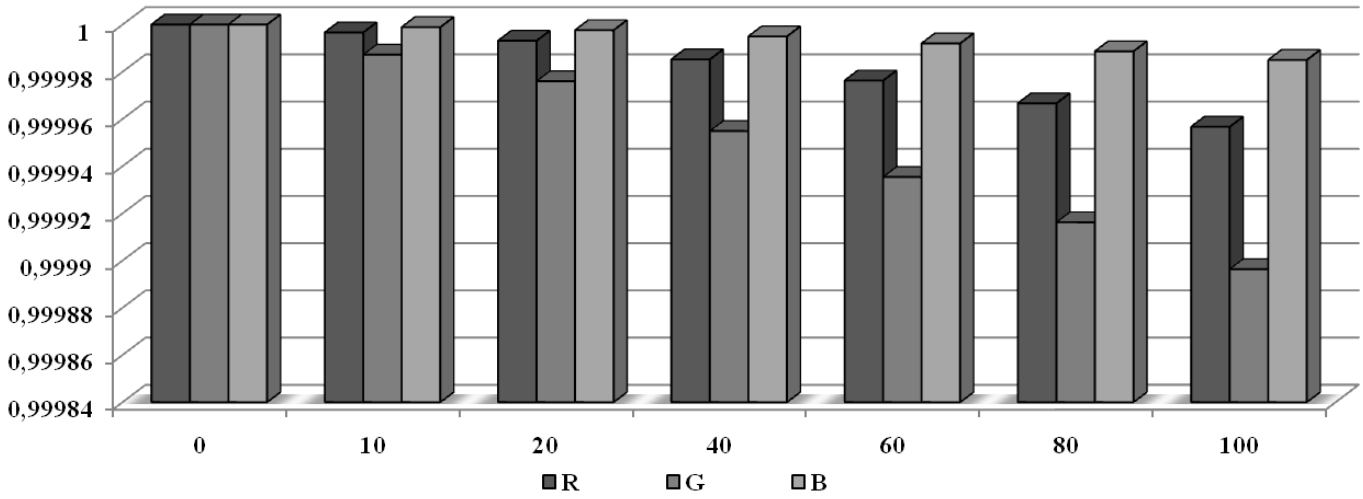


Рисунок 3.46. Значення коефіцієнтів кореляції колірної моделі RGB в залежності від ступеню заповнення

Значення коефіцієнтів кореляції, при моделі HSV, наведені у табл. 3.4.

Таблиця 3.4.

Коефіцієнт кореляції HSV моделі

№	Компонента	Ступінь заповнення контейнера, %					
		10%	20%	40%	60%	80%	100%
		Коефіцієнт кореляції					
1	H	0.99997916	0.9999629	0.99992519	0.99981694	0.99975364	0.99972187
2	S	0.99999908	0.99999774	0.99999465	0.99999094	0.99998537	0.99997924
3	V	0.99998575	0.99997189	0.99994632	0.99992114	0.99989385	0.99986322

Використання компоненти S є більш стійкішою до стеганоперетворення при використанні колірної моделі HSV (Рисунок 3.47).

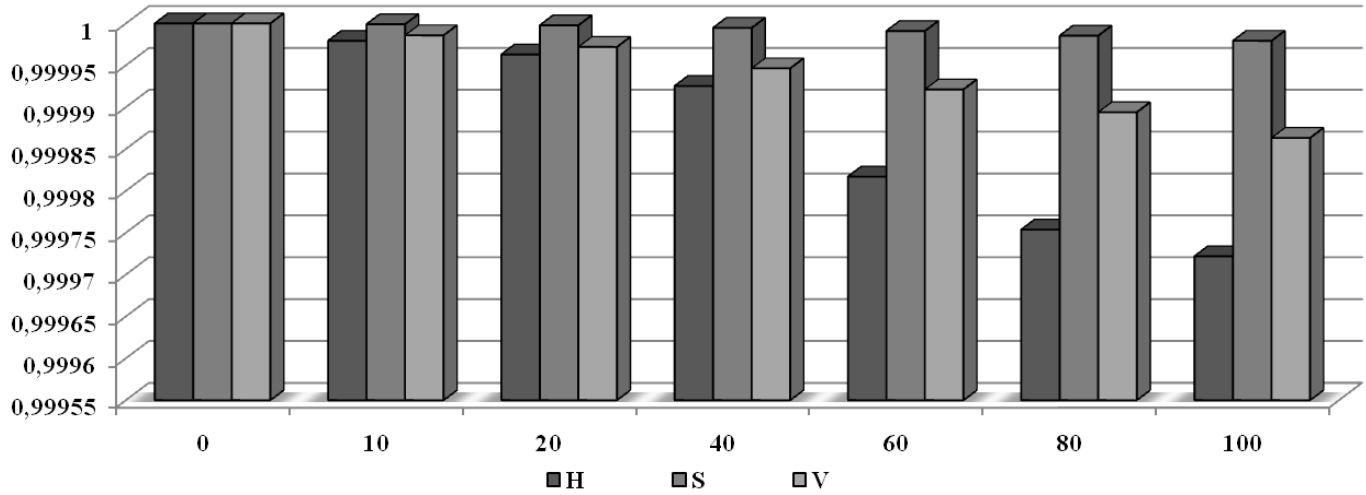


Рисунок 3.47. Значення коефіцієнтів кореляції колірної моделі HSV

Значення коефіцієнта даної компоненти при 100% заповненні становить 0.99997924, при тому що значення компоненти H – 0.99972187, а V – 0.99986322. Таким чином використання компоненти S є більш оптимальнішим при даній колірній моделі (Рисунок 3.48).

При використанні моделі HLS, оптимальнішим для приховування даних є компонента S (табл. 3.5). Значення коефіцієнта кореляції, при використання даної компоненти становить 0.99999994, що є більш прийнятним порівняно з іншими компонентами. Таким чином при використані даної моделі, приховування даних слід виконувати у компоненту S (Рисунок 4.21).

Таблиця 3.5.

Коефіцієнт кореляції HLS моделі

№	Компонента	Ступінь заповнення контейнера, %					
		10%	20%	40%	60%	80%	100%
		Коефіцієнт кореляції					
1	H	0.99997916	0.99996289	0.99992517	0.99981702	0.99975367	0.9997219
2	L	0.99998311	0.99996628	0.99993253	0.99989592	0.99982089	0.99978616
3	S	1	0.99999999	0.99999998	0.99999998	0.99999996	0.99999994

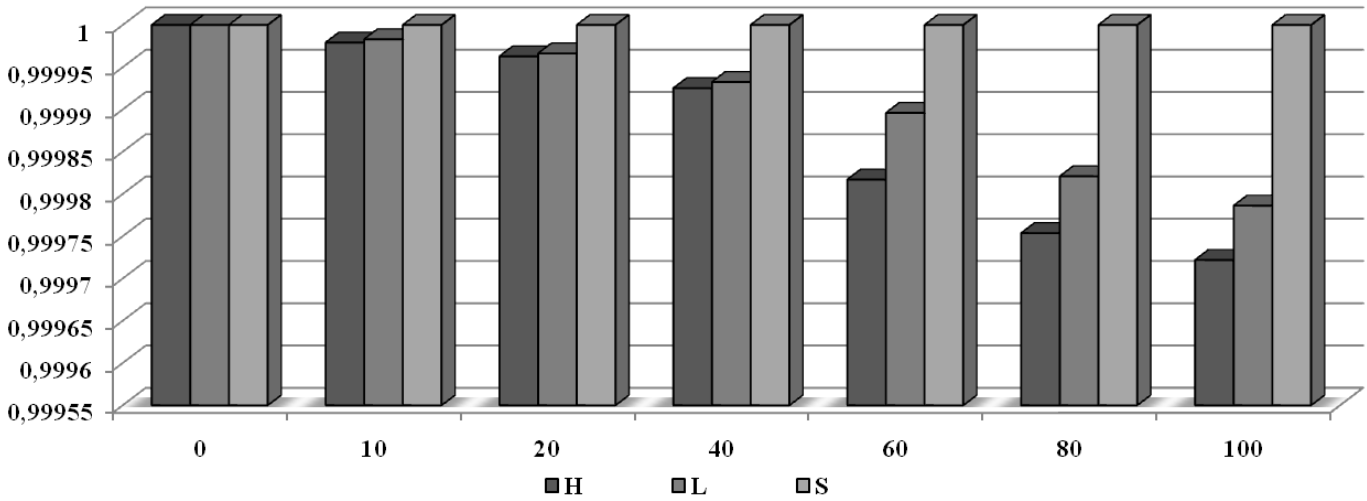


Рисунок 3.48. Значення коефіцієнтів кореляції колірної моделі HLS

Значення коефіцієнтів кореляції для моделей YUV та YIQ наведені у табл. 3.6 та 3.7. При використанні даних моделей, компоненти показали слабку стійкість до стеганоперетворення, що є неприйнятним для створення стеганографічної системи.

Таблиця 3.6.

Коефіцієнт кореляції YUV моделі

№	Компонента	Ступінь заповнення контейнера, %					
		10%	20%	40%	60%	80%	100%
		Коефіцієнт кореляції					
1	Y	0.99933513	0.99854982	0.99720302	0.99611186	0.99440492	0.99386294
2	U	0.98911739	0.97885676	0.9564895	0.92917633	0.90321687	0.89022825
3	V	0.96317777	0.92300178	0.83108853	0.73791727	0.62552825	0.49200698

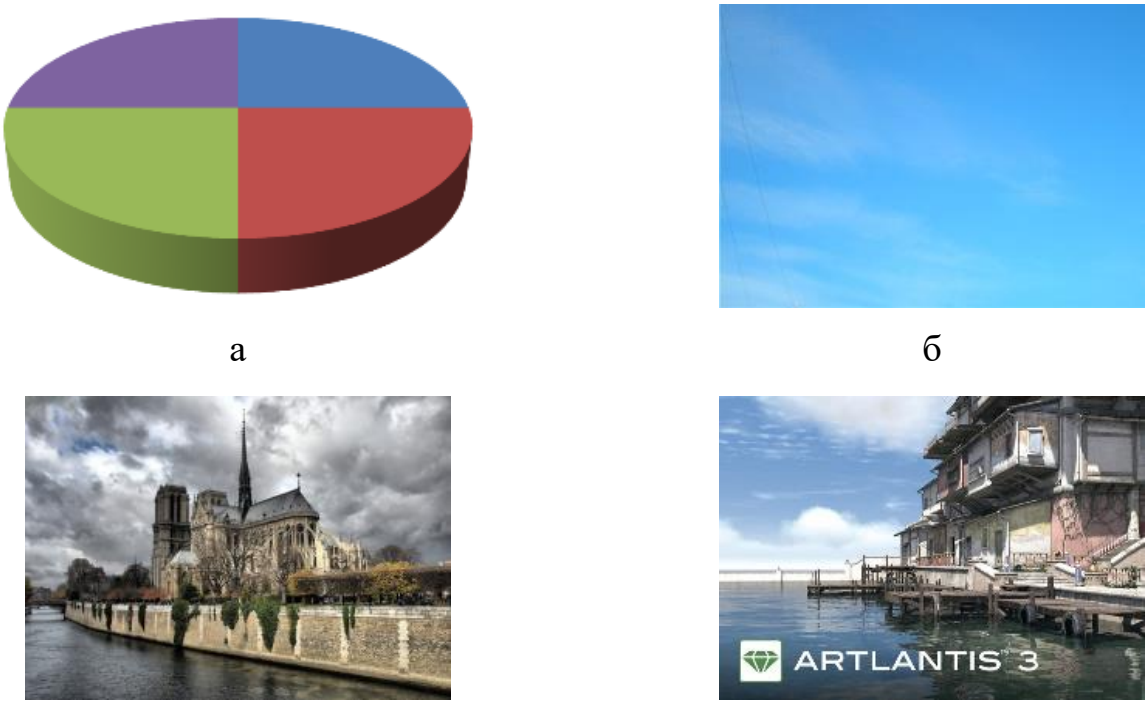
Таблиця 3.7.

Коефіцієнт кореляції YIQ моделі

№	Компонента	Ступінь заповнення контейнера, %					
		10%	20%	40%	60%	80%	100%
		Коефіцієнт кореляції					
1	Y	0.99933513	0.99854982	0.99720302	0.99611186	0.99440492	0.99386294
2	I	0.97752753	0.95444717	0.90927906	0.8665559	0.80822919	0.75213616
3	Q	0.89338212	0.79885773	0.64092727	0.52176569	0.43242287	0.38871811

Отже, найкращою колірною моделлю, при створенні оптимальнішої стеганосистеми, є HLS модель. При використанні даної моделі, приховування повідомлення слід проводити у компоненту S. При визначенні взаємозв'язку двох оригінального зображення та зображення–результату при 100% заповненні, значення кореляції відповідає дуже високій кореляції. Наступною компонентою, менш стійкішою, є синя компонента моделі RGB. Що є прийнятним при використанні моделі RGB. Показник кореляції зображень, даної компоненти, теж становить дуже високу кореляцію. Використання моделей YUV та YIQ є неприйнятним для створення стеганографічної системи. Тому, що значення показників кореляції, при 100% заповненні, становлять слабку кореляцію.

Таким чином, для створення оптимальнішої стеганосистеми доречно використовувати HLS та RGB моделі, при вирішенні поставленої задачі. Після того, як було визначено дві оптимальніші моделі виконаємо дослідження кожної моделі для чотирьох класів зображення. Зображення, що будуть використані для виконання дослідження зображені на Рисунок 3.49.



а б в г

Рисунок 3.49. Зображення: а – перший класу б – другий класу, в – третій класу, г – четвертий класу

Оскільки метою є створення оптимальної стеганосистеми, тому будемо досліджувати синю компоненту в моделі RGB та компоненту насиченості в моделі HLS. При дослідженні різних класів кольорового зображення виконувалася модифікація компонент від 10% до 100%. Таким чином, показник коефіцієнта кореляції для першого класу при відповідному ступені заповнення наведені у табл. 3.8.

Таблиця 3.8.

Коефіцієнт кореляції для 1–го класу зображення

№	Компонента	Ступінь заповнення контейнера, %					
		10%	20%	40%	60%	80%	100%
		Коефіцієнт кореляції					
1	Blue	0,99999975	0,9999996	0,99999897	0,99999872	0,99999846	0,99999841
2	Saturation	0,99999995	0,9999995	0,9999994	0,9999994	0,9999993	0,9999992

Як можна побачити за результатами дослідження компонента S є більш стійкішою до стеганоперетворення ніж компонента B моделі HLS (Рисунок 3.50). Відхилення від значення оригінального зображення компоненти S при 100% заповненні становить – 0,0000008, а компоненти B – 0,00000269.

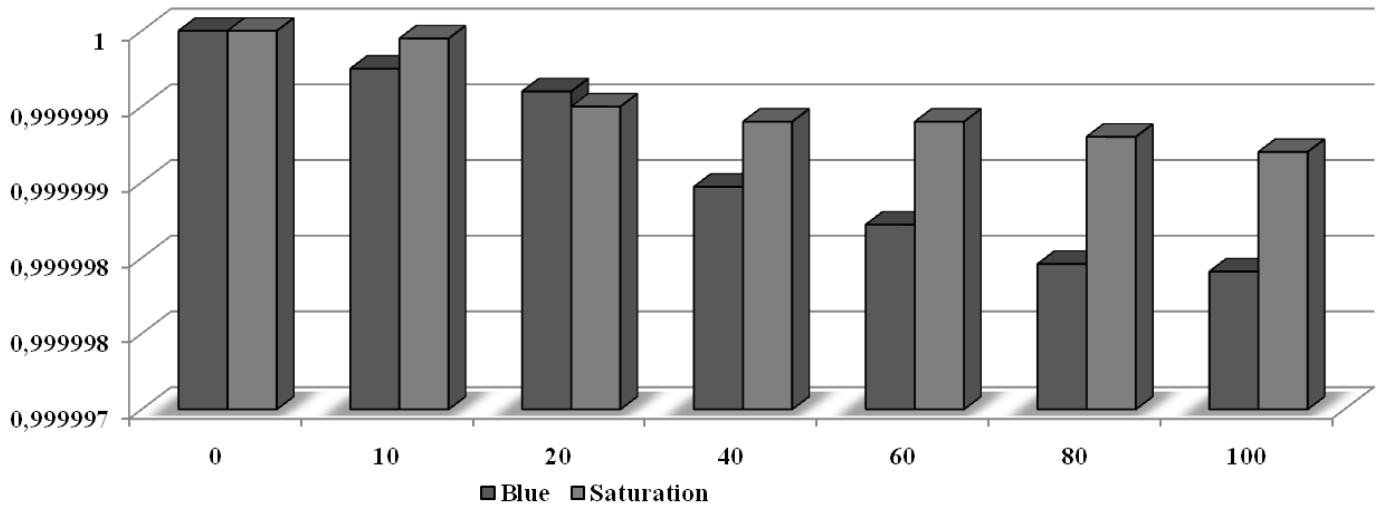


Рисунок 3.50. Значення коефіцієнта кореляції для першого класу зображення

При дослідження другого класу зображення були отримані результати, що наведені у табл. 3.9.

Таблиця 3.9.

Коефіцієнт кореляції для 2–го класу зображення

№	Компонента	Ступінь заповнення контейнера, %					
		10%	20%	40%	60%	80%	100%
		Коефіцієнт кореляції					
1	Blue	0,99999066	0,99998316	0,99996518	0,99994637	0,99993275	0,9999208
2	Saturation	0,99999768	0,99999732	0,99999701	0,99999678	0,99999651	0,99999618

З таблиці 3.8 можна побачити, що оптимальнішим є використання компоненти насиченості для приховування повідомлення у зображенні другого класу (Рисунок 3.51).

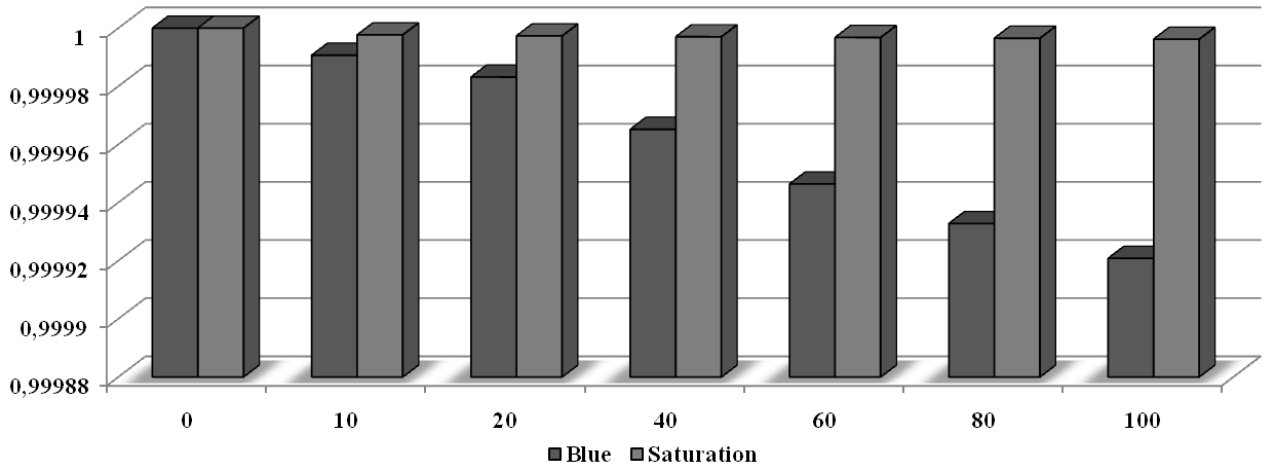


Рисунок 3.51. Значення коефіцієнта кореляції для другого класу зображення

Показник коефіцієнта кореляції для третього класу при відповідному ступені заповнення наведені у табл. 3.10.

Таблиця 3.10.

Коефіцієнт кореляції для 3–го класу зображення

№	Компонента	Ступінь заповнення контейнера, %					
		10%	20%	40%	60%	80%	100%
		Коефіцієнт кореляції					
1	Blue	0,99999862	0,99999766	0,99999547	0,99999296	0,99999063	0,99998887
2	Saturation	0,99999962	0,99999946	0,99999917	0,99999880	0,99999852	0,99999832

Після проведення заповнення та визначення коефіцієнта кореляції можна побачити, компонента S є більш стійкішою до стеганоперетворення ніж компонента B моделі HLS (Рисунок 3.52). Відхилення від значення оригінального зображення компоненти S при 100% заповненні становить – 0,00000278, а компоненти B – 0,00002223.

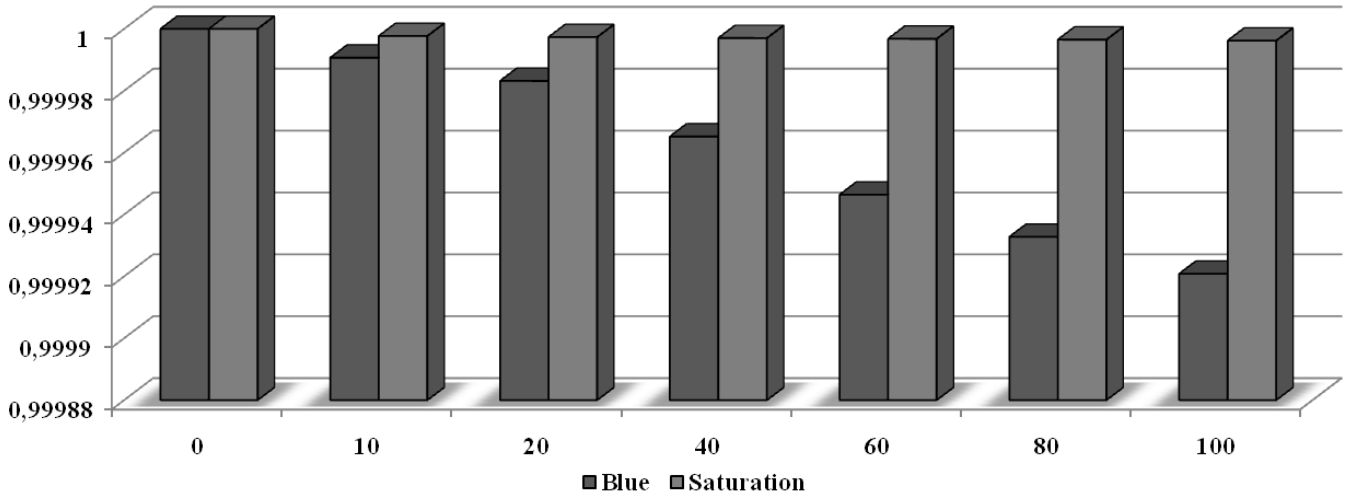


Рисунок 3.52. Значення коефіцієнта кореляції для третього класу зображення

При дослідженні останнього типу зображення, показник кореляції зображень при різних ступенях заповнення наведений у табл. 3.11.

Таблиця 3.11.

Коефіцієнт кореляції для 4–го класу зображення

№	Компонента	Ступінь заповнення контейнера, %					
		10%	20%	40%	60%	80%	100%
		Коефіцієнт кореляції					
1	Blue	0,99999927	0,99999857	0,99999707	0,99999554	0,99999416	0,9999927
2	Saturation	0,99999967	0,99999942	0,99999930	0,99999901	0,99999873	0,99999832

Отже, при реалізації стеганографічної системи більш надійнішим є використання компоненти насиченості в моделі HLS (Рисунок 3.53). При дослідженні чотирьох класів зображення було з’ясовано, що компонента S є більш стійкішою при стеганоперетворенні.

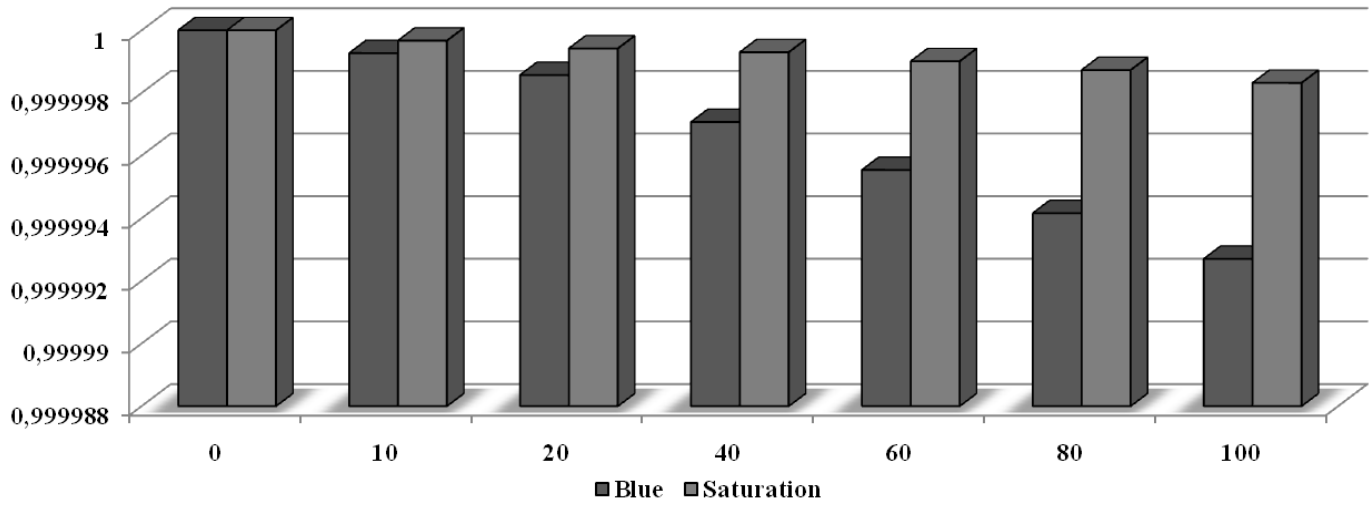


Рисунок 3.53. Значення коефіцієнта кореляції для четвертого класу зображення

Для більш детальнішого проведення аналізу та дослідження використаємо показник спотворення якості зображення. Виконаємо дослідження компоненти синього кольору та компоненти насиченості. Результати дослідження якості зображення для першого класу наведені у табл. 4.12.

Таблиця 3.12.

Якість зображення для 1–го класу зображення

№	Компонента	Ступінь заповнення контейнера, %					
		10%	20%	40%	60%	80%	100%
		Коефіцієнт кореляції					
1	Blue	0,99999993	0,99999988	0,99999969	0,99999962	0,99999954	0,99999952
2	Saturation	0,99999999	0,99999999	0,99999999	0,99999998	0,99999998	0,99999997

Спотворення якості зображення при заповненні синьої компоненти на 100% становить 0,00000058, а компоненти насиченості – 0,00000003. Таким чином, можливо побачити, що спотворення якості зображення більш відбулося при використанні синьої компоненти моделі RGB. Оптимальнішою є компонента насиченості (Рисунок 3.54). Значення якості оригінального зображення становить – 1.

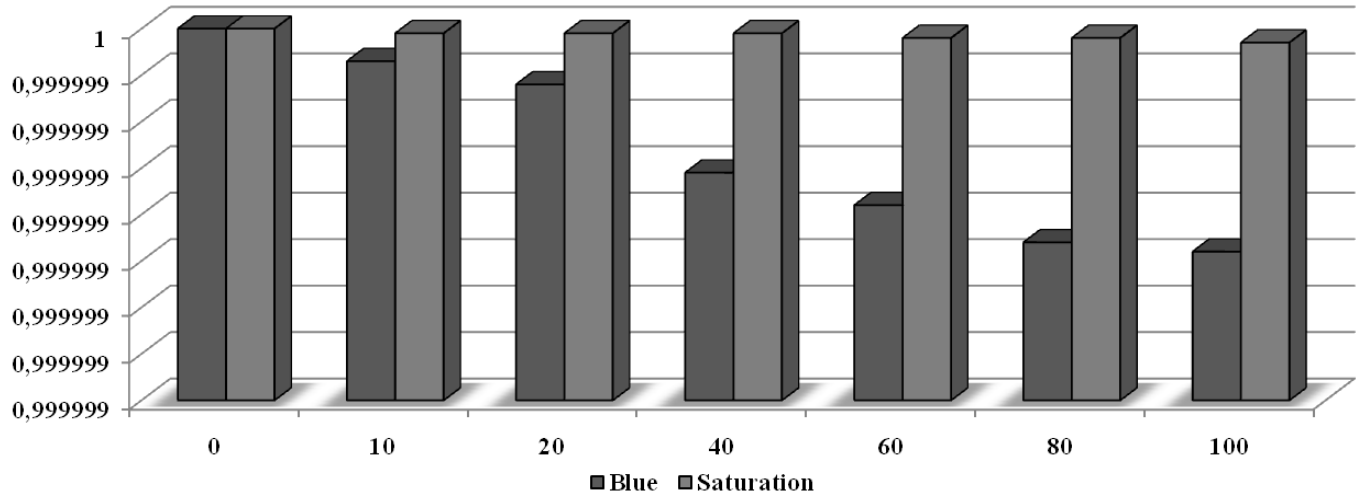


Рисунок 3.54. Значення якості зображення для першого класу

Показники якості зображення для другого класу при відповідному ступені заповнення наведені у табл.3.13.

Таблиця 3.13.

Якість зображення для 2–го класу зображення

№	Компонента	Ступінь заповнення контейнера, %					
		10%	20%	40%	60%	80%	100%
		Коефіцієнт кореляції					
1	Blue	0,99999982	0,99999967	0,99999932	0,99999895	0,99999867	0,99999843
2	Saturation	0,99999999	0,99999999	0,99999998	0,99999998	0,99999997	0,99999996

При використанні зображення першого класу, спотворення якості з компонентою синього кольору становить 0,00000267, а компоненти насиченості – 0,00000004. Оптимальнішим є використання компоненти насиченості (Рисунок 3.55).

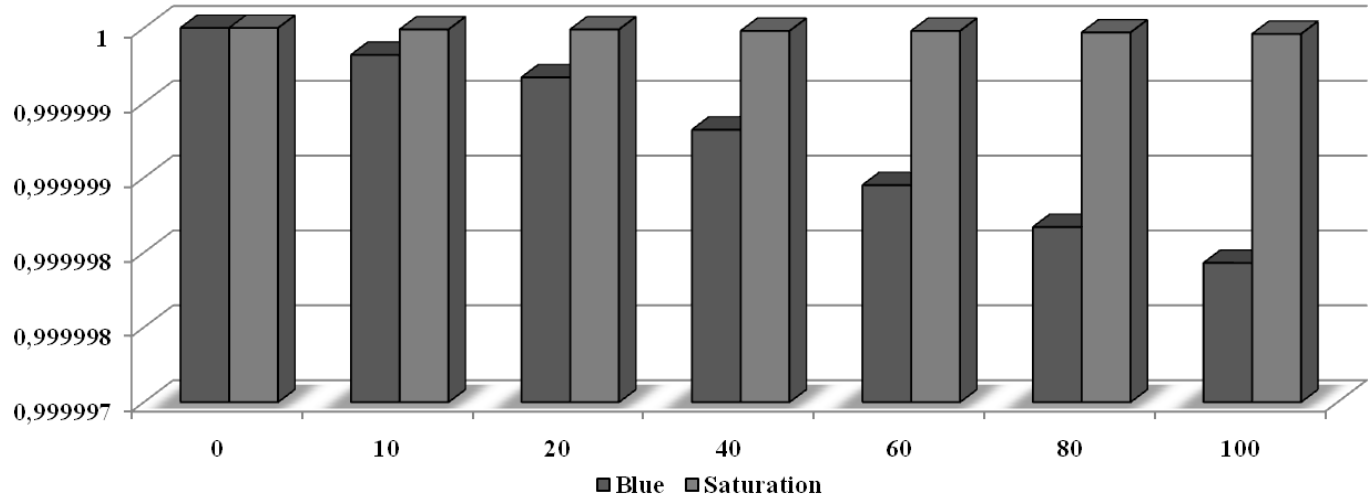


Рисунок 3.55. Значення якості зображення для другого класу

Значення якості зображення для третього класу відображені у табл.3.14. У цьому випадку слід використовувати кольорову модель HLS (Рисунок 3.56).

Таблиця 3.14.

Якість зображення для 3–го класу зображення

№	Компонента	Ступінь заповнення контейнера, %					
		10%	20%	40%	60%	80%	100%
		Коефіцієнт кореляції					
1	Blue	0,99999958	0,9999993	0,99999863	0,99999788	0,99999718	0,99999665
2	Saturation	1	0,99999999	0,99999999	0,99999999	0,99999998	0,99999998

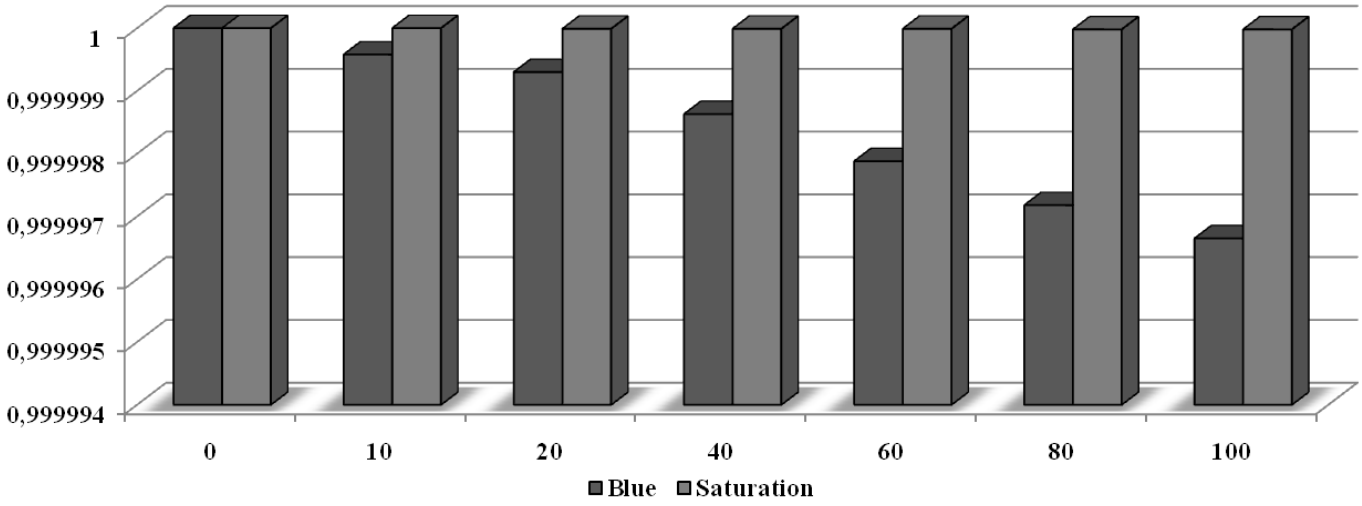


Рисунок 3.56. Значення якості зображення для третього класу

При дослідженні якості зображення останнього типу зображення були отримані результати, що відображені у табл. 3.15.

Таблиця 3.15.

Якість зображення для 4–го класу зображення

№	Компонента	Ступінь заповнення контейнера, %					
		10%	20%	40%	60%	80%	100%
		Коефіцієнт кореляції					
1	Blue	0,9999997	0,99999943	0,99999882	0,9999982	0,99999765	0,99999706
2	Saturation	1	1	0,99999999	0,99999999	0,99999999	0,99999998

Спотворення якості зображення при заповненні синьої компоненти на 100% становить 0,00000394, а компоненти насиченості – 0,00000002. Таким чином, спотворення якості зображення більш відбулося при використанні синьої компоненти (Рисунок 3.57).

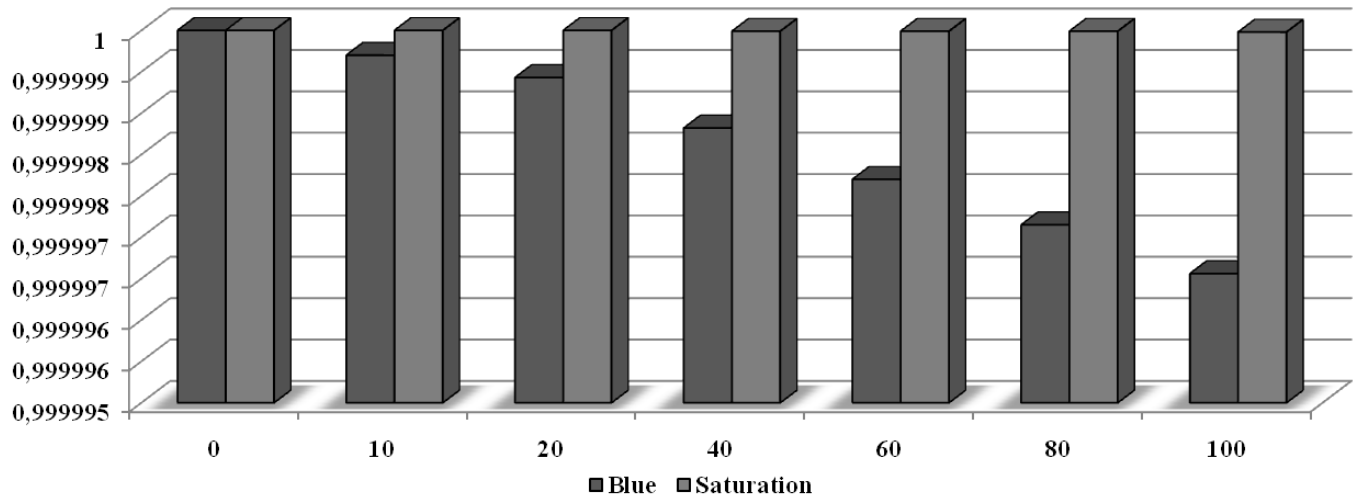


Рисунок 3.57. Значення якості зображення для четвертого класу

При підведенні підсумків слід зазначити, що за всіма показниками спотворення більш стійкою виявилась модель HLS, а саме безпосередньо компонента складова S. Це зумовлено тим, що використання даної компоненти можливо для реалізації оптимальнішої стеганографічної системи. Таким чином, при використованні такої компоненти зростає стійкість стеганоганосистеми до стеганоаналізу, а також стабільність передачі стеганоповідомлення каналом зв'язку.

Компонента синього кольору моделі RGB э менш стійкішою ніж компонента насиченості. Використання компоненти B дещо зменшує стійкість стеганосистеми до стеганоаналізу. Але використання цієї моделі теж доречно при приховуванні невеликого повідомлення, порівняно з іншими колірними моделями зображення.

3.7. Підвищення стійкості стеганоконтейнера шляхом удосконалення існуючих стеганографічний методів

При проведенні аналізу та дослідженні графічних форматів файлів та колірних моделей було виявлено, що оптимальнішими є використання BMP–формату графічного файлу та колірної моделі HLS.

Виростовуючи колірну модель HLS, зображення розкладається на три компоненти: Hue – тон кольору, Lightness – світлість та Saturation – насиченість. Кожній компоненті відповідає числовий масив значень елементів компоненти.

Виростовуючи моделі HLS, елементи компонентів можуть бути виражені як десятковий дріб. Значення елементів компонентів H, L, S при використанні зображення першого класу зображено на Рисунок 3.58.

H =

	138	139
110	79.79	79.79
111	79.79	79.79
112	79.79	79.79
113	79.79	79.79
114	79.79	79.79
115	79.79	79.79
116	79.79	79.79
117	79.79	79.79
118	79.79	79.79
119	79.79	79.79
120	79.79	...

а

L =

	117	118
80	136.5	136.5
81	136.5	136.5
82	136.5	136.5
83	136.5	136.5
84	136.5	136.5
85	136.5	136.5
86	136.5	136.5
87	136.5	136.5
88	136.5	136.5
89	136.5	136.5
90	136.5	...

б

S =

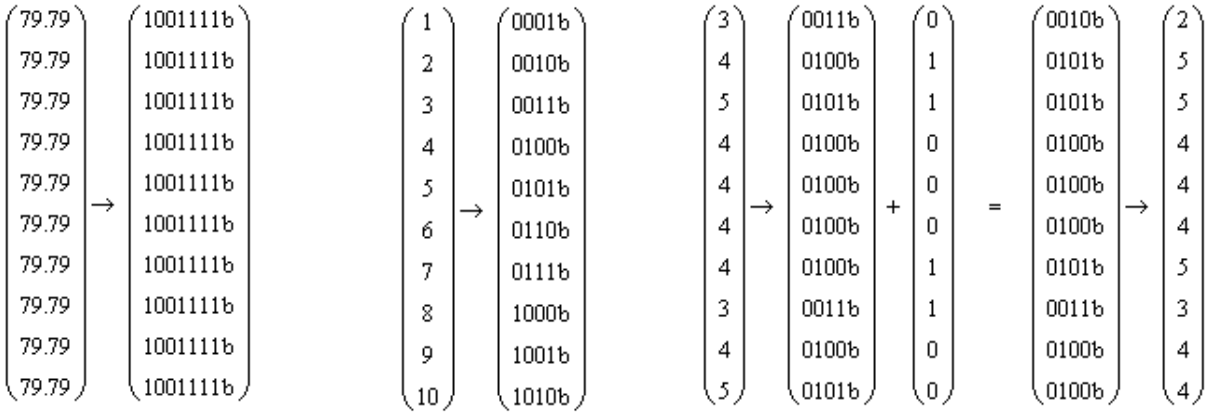
	146	147
10	61.97	61.97
11	61.97	61.97
12	61.97	61.97
13	61.97	61.97
14	61.97	61.97
15	61.97	61.97
16	61.97	61.97
17	61.97	61.97
18	61.97	61.97
19	61.97	61.97
20	61.97	...

в

Рисунок 3.58. Значення елементів компонент:
а – тон кольору, б – світлість, в – насиченість

При проведенні приховування даних кожне значення елементів відповідної компоненти переводитьсь у двійкових формат для модифікації молодшого біту елементу бітом повідомлення, але перетворення у двійковий формат відбувається тільки цілої частини числа (Рисунок 3.59, а). це відбувається через те, що у двійковому форматі не може бути дробової частини. При використанні двійкової системи кожен біт може приймати значення або 1, або 0. Таким чином, чергування молодшого біту числової послідовності відбувається почергово (Рисунок 3.59, б). При виконання приховування відбувається заміна молодшого біту елементу зображення на біт повідомлення. Таким чином, байт елементу зображення, при зміні молодшого біту, змінюється на одиницю (Рисунок 3.59, в). Така зміна є суттєвою при підвищенні стійкості стеганосистеми до стеганоаналізу [21].

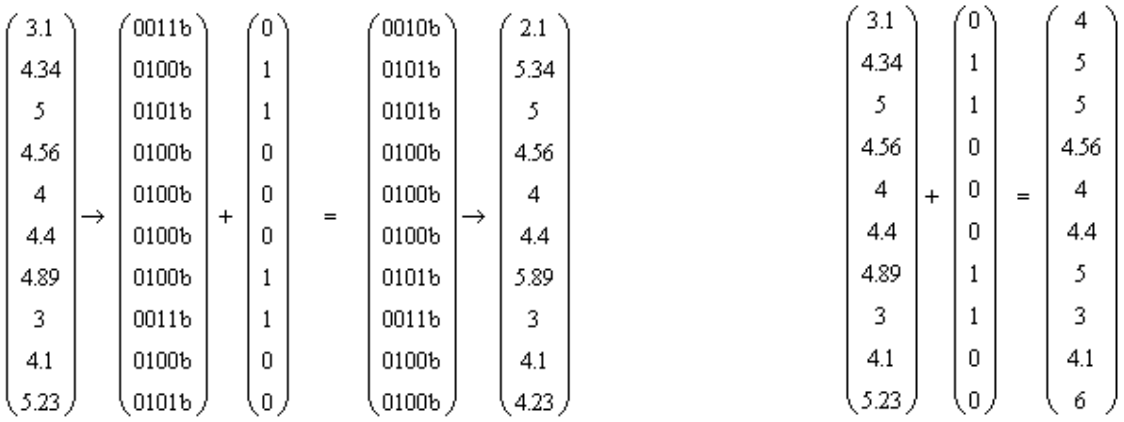
Більш надійнішим буде виконання округлення десятого значення елементу зображення до наступного значення. Для виконання модифікації молодшого біту, що не відповідає значенню відповідного біту повідомлення, проводимо округлення десяткового числа до наступної цілої частини. Наприклад, число 79,79 округлюємо до 80. Використання даного методу призводить до зменшення різниці значення елементів зображення–оригіналу та зображення–результату. Для даного випадку різниця становить: 80–79,79=0,21. При використанні цілої частини, зірниця становила б: 80,79–79,79=1. Таким чином, відбулося зменшення різниці у 5 разів, що підвищує стійкість стеганографічної системи до стеганоаналізу.



а б в

Рисунок 3.59. Двійкові представлення десяткових чисел

Сума різниць оригінальних та модифікованих байтів елементів зображення становить 4 (Рисунок 3.60, а). При використанні округлення різниця становить 2,44, що майже в 2 рази менше при модифікації молодшого біту (Рисунок 3.60, б).



а б

Рисунок 3.60. Модифікація молодшого біту:
а – методом заміни молодшого буту, б – методом заокруглення.

Таким чином, використання округлення дозволяє насамперед зменшити спотворення зображень після стеганографічного перетворення та підвищити надійність стеганосистеми. Для практичного підтвердження удосконалення методів виконаємо приховування даних у зображення за допомогою методу заміни НЗБ, та псевдовипадкового інтервалу. Для приховування використаємо растрове 24–х бітне кольорове зображення – 240x240. Повідомлення – текст англійською мовою.

Виконаємо реалізацію даного методу у Mathcad. Для початкового етапу реалізації даного методу виконаємо дії блоків М.1.1 – М.1.2 розділу 2 даної дипломної роботи. Для більшої зручності внесення повідомлення до контейнеру виконаємо перетворення числової матриці синьої складової у вектор–стовпець. Дане перетворення виконує модуль – Vec. Внесення прихованої інформації до зображення виконує модуль Nvec. Даний модуль виконує перетворення кожного значення елементу масиву Vec в двійковий код та замінює молодший біт на біт інформаційного повідомлення якщо значення елементу – ціле число. Якщо число дробове – виконуємо округлення числа. Після цього, даний модуль виконує зворотне перетворення двійкового коду у байт елементу зображення (Рисунок 3.61).

```
Vec := | Vec ← C^(1)
       | for i ∈ 2..cols(C)
       |   Vec ← stack(Vec, C^(i))
Nvec := | for μ ∈ 1..rows(Mes)
        |   b ← D2B(Mes_μ)
        |   for i ∈ 1..8
        |     if Vec_(i+8·(μ-1)) - floor[Vec_(i+8·(μ-1))] = 0
        |       P ← D2B[Vec_(i+8·(μ-1))]
        |       P_1 ← b_i
        |       Vec_(i+8·(μ-1)) ← B2D(P)
        |     Vec_(i+8·(μ-1)) ← ceil[Vec_(i+8·(μ-1))]  otherwise
        | Vec
Np := for i ∈ 1,2..cols(C)
        Np^(i) ← submatrix[Nvec,(i - 1)·rows(C) + 1,i·rows(C),1,1]
Pic := augment(H,L,Np)                WRITE_HLS("PictureHLS.bmp") := Pic
```

Рисунок 3.61. Блок М.4.1

За допомогою модуля Np, виконуємо перетворення вектора–стовпця Nvec у масив розмірами – C. Наступним етапом реалізації є об'єднання компонентів зображення в один масив, а саме Hue, Lightness та Saturation за допомогою функції augment( ). Збереження зображення з повідомленням виконаємо за допомогою вбудованої функції WRITE_HLS(x), де x – директорія нового файлу та його ім'я.

При внесенні однакового повідомлення до одного зображення двома різними методами було отримано такі результати спотворення зображення: коефіцієнт кореляції моделі HLS методом заміни НЗБ становив – 0,99999645, а методом округлення значень елементів зображення – 0,99999999. Якість зображення при застосуванні першого методу становить – 0,99999728, а при другому – 0,99999999.

Для реалізації методу псевдовипадкового інтервалу виконаємо дії блоків М.1.1 – М.1.2 розділу 2 даної дипломної роботи. Для більшої зручності внесення повідомлення до контейнеру виконаємо перетворення числової матриці синьої складової у вектор–стовпець. Далі, виконаємо вбудовування повідомлення у контейнер (Рисунок 3.62).

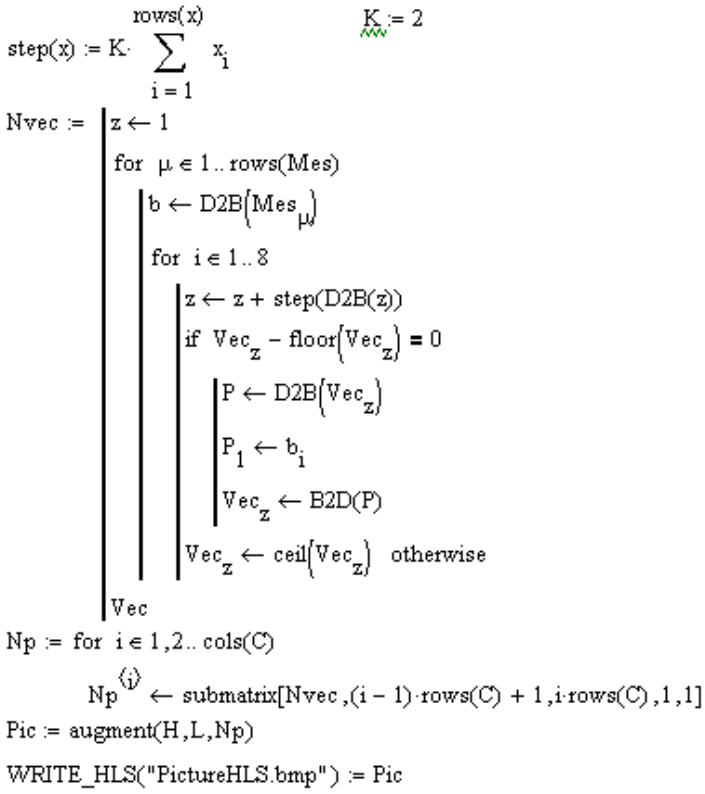


Рисунок 3.62. Блок М.5.1

Значення коефіцієнта кореляції при використанні першого методу становить – 0,99999946, а при використанні другого – 1. Якість зображення при застосуванні першого методу становить – 0,99999959, а при другому – 1. Таким чином, використання округлення дає більш вищий результат підвищення стійкості стеганосистеми.

Таким чином, для реалізації більш стійкішої стеганографічної системи оптимальніше використовувати графічний файл з форматом BMP та колірною моделлю – HLS. Використання колірної моделі HLS для вбудовування повідомлення за допомогою удосконаленого методу підвищує стійкість стеганосистеми до стеганоаналізу.

Висновки по розділу 3

В даному розділі шляхом аналізу сучасних графічних форматів растрового зображення та колірних моделей було визначено основні аспекти реалізації

оптимальнішої стеганосистеми. Для оцінки якості стеганографічний методів було виділено ряд показників, таких як: зміна розміру файлу після стеганоперетворення, кореляція зображень та спотворення якості зображення після реалізації стеганографічного методу приховування даних. Оптимальнішим формат файлу для приховування даних є BMP. Тому, що розмір файлу після стеганоперетворення не змінюється порівняно з іншими форматами файлів, які розглядалися у даній дипломній роботі. Для виконання процесу приховування повідомлення слід використовувати колірну модель – HLS. Вона є більш стійкішою до спотворення зображення при реалізації приховування даних у нерухомих зображеннях.

Для підвищення надійності стеганографічної системи слід використовувати удосконалений метод заміни НЗБ при умові, що повідомлення є великим та метод псевдовипадкового інтервалу при значно меншому повідомленні ніж контейнер. Удосконалення методів полягає в округлення значень елементів компонент при використанні моделі HLS. Використання стеганографічного ключа підвищує стійкість стеганосистеми до реалізації атак. Використання ключа реалізовано у методі псевдовипадкового інтервалу. Таким чином було виділено практичні рекомендації щодо підвищення надійності стеганографічної системи.

РОЗДІЛ 4
МЕТОДИ СТЕГАНОАНАЛІЗУ В ЗАДАЧАХ ЗАХИСТУ ІНФОРМАЦІЙНИХ ПОТОКІВ ДАНИХ

4.1. Принципи стеганографічного аналізу

Головна мета стеганографічного аналізу – це звісно моделювання стеганографічних систем та їх дослідження, для того щоб була можливість отримати якісні та кількісні оцінки стабільності використовуваної стеганотрансформації, і будування методів виявлення інформації, що прихована в контейнері, її модифікації або знищення [20].

Терміни стеганоаналізу мають схожість з термінами криптоаналізу, але є деякі суттєві відмінності. Криптоаналіз використовується для розшифровки вмісту криптограм, а стеганоаналіз безпосередньо для виявлення присутності якоїсь прихованої інформації.

За рівнем секретності стеганографічні системи поділяють на теоретично стабільні, практично стабільні та нестабільні системи.

Теоретично стійка (абсолютно надійна) стеганосистема здійснює приховування інформації лише в тих фрагментах стеганоконтейнера, значення деяких елементів, що не можуть перевищити рівня шуму або помилки безпосередньо квантування, і це в теорії означає, що неможливо зробити стеганоаналітичний метод виявлення такої інформації (Рисунок 3.1, a) [23].

У практиці надійна стеганографічна система здійснює певну модифікацію частин контейнера, зміни, які можна знайти, але необхідна інформація про те, що в даний час стеганоаналітичні методи в повідомленнях, які відмовляються або залишають не розробленими (Рисунок 3.1, b).

Нестабільність стеганосистеми ховає інформацію так, що сучасні стеганоаналітичні засоби можуть її виявити (Рисунок 3.1, в). Таким чином, коли таким стеганограяіний аналіз дає змогу знайти вразливісті стеганоперетворення та

вдосконалити його таким чином, щоб певні зміни, які були внесені в контейнер, знову були в області теоретичної або практичної нерозривності (Рисунок 3.1, а, б) [23].

Фактично будь–яке стеганографічне перетворення базується на двох визначальних принципах [22]:

• об'єктом вибирається носій прихованої інформації (контейнер), структура якого передбачає можливість деякого спотворення певної інформації контейнера, але зберігає при цьому функції;

• рівень спотворень, що вводяться в структуру контейнера, має бути менше, ніж рівень чутливостей засобів розпізнавання (включаючи розпізнавання органами людського чуття).

Стеганоконтейнером, як згадувалося вище, можуть бути майже всі існуючі носії, що використовуються в сучасних мережах передачі даних. У цьому випадку методи сховування інформації зосереджуються головним чином на внутрішній структурі контейнера, яка може бути символічними або розрядними даними, коефіцієнтами перетворення Фур'є, широкосмуговим кодуванням, коефіцієнтами ущільнення і т.д. Сховування інформації у медіа середовищі потребує дотримування деяких вимог при внесенні певних змін, за мету яких мається на увазі, усунути прояв слідів використання операцій стегано-трансформації. Як приклад, у разі якщо у зображенні ці зміни можуть за деяких дій з боку атакуючого (навмисних і випадкових) бути видимі для ока людини, а це чітко свідчать про наявність стеганографічних засобів. Такі сліди, що залишаються, можуть суттєво спростувати виявлення існування повідомлення, що є прихованим, тим самим компрометуючи систему стеганографії в цілому.

Одним з основних завдань стеганоаналізу є вивчення існуючих залишків використання стеганографічних засобів та розробка методів, що можуть дозволити знайти факти їх використовування. Застосування конкретного стеганографічного перетворення вимагає від стеганоаналітика індивідуального підходу до його дослідження.

4.1.1.Модель порушника та модель загроз

Модель порушників визначає: категорії або типи порушників, які можуть впливати на об'єкти; цілі, які переслідують порушники кожної категорії, насамперед можливий кількісний склад, використані інструменти, оснащення, зброя та ін.; типові сценарії можливих різних дій порушників, що описують послідовність дій груп або окремих порушників, способів дій на кожному етапі.

Модель загроз – це формалізований або неформалізований абстрактний опис різних методів та засобів реалізації загрози. Модель порушника – це формалізований або неформалізований абстрактний опис порушника [3].

Під порушником в загальному вигляді можна розглядати особа або групування певних осіб, що як наслідок навмисних чи ненавмисних дій дає можливість виникнення загроз ІБ. З боку права на постійний або одноразовий доступ до контрольованої території, порушників можна розділити на два типи: порушники, що не володіють правами доступу до контрольованої території (приміщення) – це зовнішні порушники; а також порушники, що володіють правами доступу до контрольованої території (приміщення) – це внутрішні порушники [3].

Всі порушники можуть мати такі характеристики, як пасивість, активість та злісним. Залежно від цього можуть представлятися різні порушення безпеки. У випадку пасивного порушника є можливість лише на виявлення стеганографічного каналу та (мало ймовірно) відомості про зміст прихованого повідомлення. Чи зможе він дізнатися повідомлення після того, як його знайде, залежить від стабільності систем кодування, але це зазвичай не розглядається в стеганографії. Спектр дій активного порушника набагато ширший. Повідомлення, що є прихованим, можна видалити або знищити. Порушення зловмисного зловмисника є самими небезпечними. Такий вид порушників може не тільки знищувати, але і робити помилкові стеганограми (тобто, дезінформацію). Щоб реалізувати загрозу, порушник використовує певні атаки [21].

Порушники класифікуються за рівнями можливостей, які надаються їм штатними засобами автоматизованої системи і ЗОТ, поділяються на чотири рівні. І

рівень визначає найменьший рівень можливостей ведення діалогів в АС – це запуск задач з фіксованого набору, які реалізують заздалегідь передбачені набори функції по обробці інформації. ІІ рівень визначає можливість створення та запуску власної програми з новими функціями із обробки інформації. ІІІ рівень визначає можливість управління функціонуванням автоматизованої системи, тобто впливом на базові програмні системи та на склад і конфігурацію устаткування. IV рівень визначається обсягом можливих осіб, що здійснюють проектування, ремонт та реалізацію технічних засобів автоматизованої системи, до включення до складів СВТ власних технічних засобів із новими функціями з ОІ. В своїх рівнях порушники є спеціалістами вищої кваліфікації, знає все про автоматизовану систему, зокрема, про систему та засоби її захисту.

Так само, модель порушника можна представити так: 1) Розробляючі; 2) Персонал людей; 3) Юзери; 4) Сторонні особи з вулиці.

4.1.2. Атаки на стеганографічні системи

Використання методу стеганографічного захисту призвело до застосування стеганографічного аналізу. Метою даного стеганоаналізу є дослідження кількісних та якісних оцінок надійності стеганосистеми, а також побудова різноманітних методів виявлення, модифікації або руйнування прихованих даних. Для виявлення прихованої інформації застосовують атаки на стеганографічну систему. Під атакою розуміється спроба знайти, виділити, змінити приховане повідомлення. Виділяють такі види атак на стеганографічні системи [20]:

- атаки на основі відомих заповнених контейнерів;
- атаки на основі відомих вбудованих повідомлень;
- атаки на основі обраних прихованих повідомлень;
- адаптивні атаки на основі обраних прихованих повідомлень;
- атаки на основі обраних заповнених контейнерів;
- атаки на основі відомих порожніх контейнерів;
- атаки на основі обраних порожніх контейнерів;

- атаки на основі відомих математичних моделей контейнерів або його частин.

У випадку атаки на основі відомого контейнера або повідомлення, порушник має у своєму розпорядженні 1 або декілька заповнених контейнерів або повідомлень. При використанні атаки на основі обраного повідомлення або контейнера, порушник може пропонувати для передачі свої повідомлення або контейнери й аналізувати отримувані при цьому контейнери–результати.

При атаці на основі відомих математичних моделей контейнера, атакуючі намагаються визначити відмінності підозрілих повідомлень від відомих йому моделі. Атаки на основі відомих порожніх контейнерів виконується на основі того, що відомий порожній контейнер, то порівнюючи його з передбачуваним стеганоконтейнером можливо встановити наявність стеганоканала.

У випадку атаки на основі відомих заповнених контейнерів атакуючий може мати у своєму арсеналі один або декілька контейнерів, що є заповненими. Завдання порушника може складатися у виявленні фактів того, що стеганоканал існує (це і є основним завданням), але і у знаходженні повідомлення або ключа. Якщо атакуючий знає ключ, то він може аналізувати інші стеганоповідомлення.

Атаки на основі відомих вбудованих повідомлення. Даний тип атаки більшою мірою характерний для системи захисту інтелектуальної власності, в якій ЦВЗ, наприклад, використовує відомі логотипи фірм. Завданнями аналізування є отримання ключа. У разі коли відповідаючий повідомленню, що є прихованим контейнер заповнений невідомий, тоді завдання є вкрай важко розв’язуваним.

Атаки на основі обраних прихованих повідомлень. У даному разі атакуючий має змогу надавати свої дані для передачі та здійснювати аналіз отриманих при цьому контейнери–результати.

Адаптивні атаки на основі обраних прихованих повідомлень. Таке атакування – це окремий випадок. У такому випадку атакуючий може вибрати повідомлення для їх нав’язання, і від того, які результати були отримані здійснює аналіз попередніх контейнерів–результатів.

Атаки на основі обраних заповнених контейнерів. Таке атакування більш подібне для систем ЦВЗ. Стеганографічний аналітик використовує детектор

контейнерів(заповнених) під виглядом “чорного ящика” та ще деяких таких контейнерів. Виконуючи аналіз таких повідомлень, атакуючий здійснює намагання дізнатися ключ.

Атаки на основі відомих порожніх контейнерів. Якщо останній є відомим порушнику, тоді шляхом порівняння його із підозрюваним на присутність прихованих даних контейнером, той завжди взмозі встановити факт наявності стеганоканалу. Незважаючи на тривіальність даного випадку, у ряду роботи роблять інформаційно–теоретичне описування. Трохи більш цікавим є сценарії, коли контейнери відомі приблизно, з деякою похибкою (коли додається до нього певний шум). Так є можливість для побудови стабільної стеганографічної системи.

Атаки на основі обраних порожніх контейнерів. У такому разі атакуючий може заставити користуватися контейнером, який він запропонує. Отже, він має можливість мати однорідніші області, і тоді буде важко забезпечити таємність вбудовування.

Атаки на основі відомих математичних моделей контейнерів або його частин. При цьому атакуючі намагаються визначити відмінності підозрілих повідомлень від відомих йому моделей. Як приклад, можеме допустити, що біти безпосередньо у середині деякої частини картинки може бути корельованим. А отже, такої кореляції має показати наявність прихованого повідомлення. Основна мета того, хто приховує повідомлення, є у тому, щоб не порушити статистичні ознаки контейнера. відправляючий та атакуючий можуть володіти різними моделями сигналів, а перемагає той, у кого більш оптимальна модель.

Найбільш прості атаки – це суб'єктивні. Уважно розглядаються зображення, прослуховується звукозапис зі спробами знайти ознаки існування прихованого повідомлення. Зазвичай це перший етап зламу стеганосистеми. У більшості випадків виділяють такі етапи зламу стеганографічної системи [21]:

- знаходження інформації, що є прихованою;
- добування такого повідомлення;
- змінювання такої інформації;
- накладання заборони на пересилання інформаційних потоків.

Однією з задач стеганографічного аналізу є дослідження наслідків застосування стеганографічних перетворень. Застосування конкретного стеганографічного методу вимагає від стеганоаналітика індивідуального підходу до його дослідження.

Головна мета атаки на стеганографічну систему схожа на атаку на криптосистему, але є певні відмінності, що важливість активних (зловмисних) атак різко зростає. Кожен контейнер може бути замінений, щоб видалити або знищити приховане повідомлення, навіть не знаючи є воно там або ні. Знаходження існування прихованого повідомлення економить час на етапі модифікації, оскільки буде є необхідність обробляти лише такі контейнери, що мають у собі приховані повідомлення. Якщо навіть мати найкращі умови для здійснення атаки завдання отримання прихованого повідомлення з контейнера може бути дуже надзвичайно складним. Точно стверджувати про існування прихованого повідомлення є можливість тільки після її розподілу в досить явному вигляді. Час від часу, мета стеганоганалізу є зовсім не певний алгоритм, а знаходження певного ключа стеганографії, який використовують для знаходження бітів контейнеру в стеганоконверсії.

4.2. Критерії оцінки стеганографічних методів

При оцінюванні якості стеганографічних методів та виявлення стеганоконтейнера застосовують методи стеганографічного аналізу на основі їхніх статистичних характеристик. У рамках даної дипломної роботи будуть використані такі показники методів стеганографічного аналізу:

- кореляція зображення–оригіналу та зображення–результату;
- подібність гістограмм;
- час виконання стеганографічного аналізу.

4.2.1. Кореляція зображень

Під кореляцією розуміють статистичну залежність двох випадкових величин. Математичною мірою кореляції 2–х величин є коефіцієнт кореляції. Найбільш відомий коефіцієнт кореляції Пірсона. Для визначення взаємозв'язку двох вибірок використаємо формулу коефіцієнта кореляції Пірсона:

$$r_{xy} = \frac{\frac{1}{n} \times \sum_{i=1}^{n} (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n} (x_i - \bar{x})^2} \times \sqrt{\sum_{i=1}^{n} (y_i - \bar{y})^2}}. \quad (4.1)$$

Формулу (4.1) можливо подати у такому вигляді:

$$r_{xy} = \frac{\frac{1}{n} \times \sum_{i=1}^{n} (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{S_x^2} \times \sqrt{S_y^2}}, \quad (4.2)$$

де $\bar{x}, \bar{y}$ – це середні значення для вибірки x та y; S – це відповідно середньоквадратичне відхилення.

Такий коефіцієнт кореляції має вимірювання у межах від –1,00 до +1,00. У випадку, коли коефіцієнт кореляції з мінусом, це свідчить про наявність протилежного зв'язку: коли вище значення однієї змінної, тоді нижче значення безпосередньо іншої. А сила зв'язку описується і величиною коефіцієнта кореляції, яка є абсолютною.

4.2.2. Подібність гістограмм

Показник подібності гістограм належить до кореляційних показників спотворення. Він базується на відмінності між гістограмою контейнера–оригіналу і гістограмою контейнера–результата. Для визначення показника подібності гістограм використаємо наступну формулу:

$$HS = \sum_{i=0}^{255} |f_C(c) - f_S(c)|, \quad \textbf{(4.3)}$$

де $f_C(c)$ – це певна частота градаційних частин кольору c у деякому зображенні–оригіналу з 256 рівнями кольорів, а $f_S(c)$ – відносна частота градації кольору s у зображенні–результату з 256 рівнями кольорів. Даний показник порівнює гістограми кольорів зображення та вираховує показник подібності гістограм аналізуючи зображень.

4.2.3. Час виконання стеганографічного аналізу

Даний показник оцінки тривалості часу, необхідного для виконання стеганографічного аналізу контейнера–оригіналу та контейнера–результату. Зменшення даного показника призводить до виграшу часу обробки інформації та збільшенні кількості обробляючої інформації. При створенні методу стеганоанлізу слід прагнути зменшення тривалості проведення стеганографічного аналізу для збільшення об'ємів аналізуючої інформації з метою знаходження прихованої інформації.

4.3. Дослідження та удосконалення методів стеганографічного аналізу в задачах захисту інформаційних потоків даних

При оцінюванні якості стеганографічних методів та виявлення стеганоконтейнера застосовують методи стеганографічного аналізу на основі їхніх статистичних характеристик. При створенні стеганоаналітичної системи з метою здійснення перевірки стійкості стеганографічних методів або виявлення прихованого каналу зв'язку, слід прагнути підвищити точність (чутливість) стеганоаналітичної системи. Тому слід прагнути зменшення помилок стеганоаналітичної системи до пропуску цілі (помилка другого роду).

Помилки першого роду і помилки другого роду – це основні ключові поняття певних завдань перевірки статистичних гіпотез. Дані поняття використовуються, коли при прийнятті «бінарних» рішень на основі якихось критеріїв, які з деякою вірогідністю можуть давати помилковий результат. Помилку I–го роду частіше

називають помилковою тривогою або помилковим спрацьовуванням. Помилку II–го роду називають пропуском цілі або помилково–негативним спрацьовуванням. Ступінь чутливості системи повинна являти собою компроміс між ймовірністю помилок I–го і II–го роду. Де знаходиться точка рівномірного балансу, залежить від оцінки ризику обох видів помилок.

У даній дипломній роботі запропонований гістограм ний аналіз з метою оцінки удосконаленої стеганографічної системи з використанням методу округлення значень елементів зображення з метою приховування повідомлення у фіксованому контейнері, а саме растровому зображенні.

При виконанні роботи будуть використані зображення, що були отримані при виконанні розділу 3. Так, для приховування інформації буде використовувалась синя складова деякого статичної 24–бітової RGB картинки із розміром безпосередньо растру – 240x240 та компонента насиченості колірної моделі HLS. Інформація для приховування – текст англійською мовою. Заповнення контейнера буде виконано двома методами: заміни НЗБ та округлення значень елементів зображення. Ступінь заповнення становив від 10 до 100% обраної компоненти.

Імпорт BMP–зображення в документ MathCAD проводимо за допомогою вбудованої функції – READ_IMAGE("директорія та ім’я файлу"). Після того, слід побудувати гістограму за допомогою функції Hist(x), де x – масив значень кольорів зображення (Рисунок 4.1).

```
K := READ_IMAGE("PictureBMP.bmp")
Hist(x) := | for i ∈ 0..255
           |   g ← 0
           |   for j ∈ 0..cols(x) − 1
           |     for k ∈ 0..rows(x) − 1
           |       g ← g + 1 if x[k,j] = i
           |   Hist[i] ← g
           | Hist
```

Рисунок 4.1. Блок А.4.1.

Для візуального відображення створеної гістограми слід виконати побудову графіку створеної залежності частот попадання елементів вибірок від відповідного інтервалу вибірки (Рисунок 4.2).

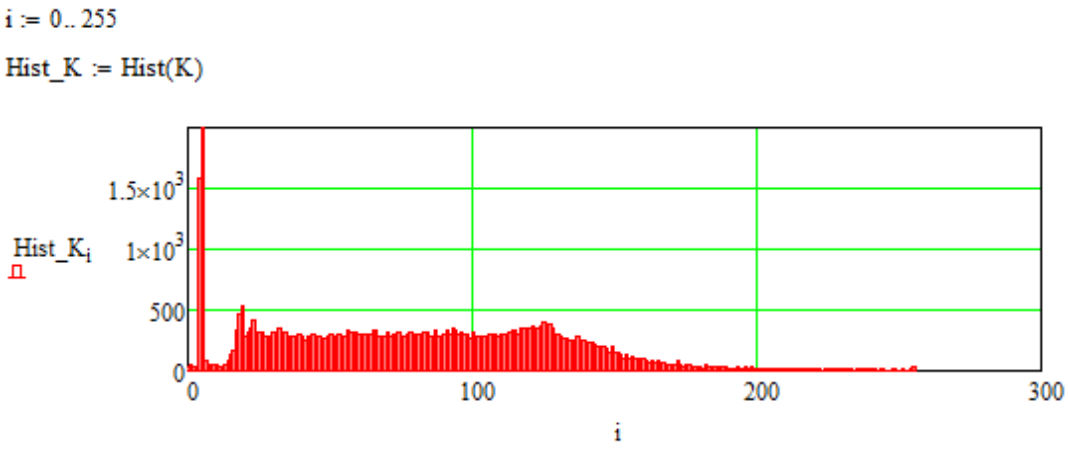


Рисунок 4.2. Блок А.4.2.

Для отримання показника кореляції гістограм слід виконати підрахунки за допомогою написаної функції Korr(x,y) (формули 4.1–4.2), де x та y – вибірки показників гістограм зображення–оригіналу та зображення–результату (Рисунок 4.3).

$$M(C) := \frac{1}{rows(C)} \cdot \sum_{i=0}^{rows(C)-1} C_i$$

$$St(C) := \sqrt{\frac{1}{rows(C)} \cdot \sum_{i=0}^{rows(C)-1} \left(C_i - M(C)\right)^2}$$

$$Korr(C,S) := \frac{\frac{1}{rows(C)} \cdot \sum_{j=0}^{rows(C)-1} \left[\left(C_j - M(C)\right) \cdot \left(S_j - M(S)\right)\right]}{St(C) \cdot St(S)}$$

Рисунок 4.3. Блок А.4.3.

Для порівняльного методів стеганоаналізу виконаємо дослідження коефіцієнта кореляції гістограм зображень та безпосередньо зображень. Виконання

перевірки подібності гістограм слід провести за допомогою написаної функції за формулою 4.3., де x та y – вибірки показників гістограм зображення–оригіналу та зображення–результату (Рисунок 4.4).

$$HS(C,S) := \sum_{i=0}^{rows(C)-1} \left| C_i - S_i \right|$$

Рисунок 4.4. Блок А.4.4.

Після проведення стеганографічного аналізу за допомогою гістограмнного та безпосереднього методу, що базуються на різниці між контейнерами, виконаємо порівняння результатів дослідження. На Рисунок 4.5 зображені показники коефіцієнта кореляції зображень при заповненні компоненти насиченості колірної моделі HLS. З результатів можна побачити, що гістограмний метод стеганоаналізу більш чутливий порівняно із звичайним порівнянням двох зображень при однакових умовах порівняння.

На Рисунок 4.6 зображені показники коефіцієнта кореляції зображень при заповненні синьої компоненти колірної моделі RGB двома методами: заміни та округлення. При обробці результатів видно, що порівняно із компонентою насиченості, використання синьої компоненти менш стійкіша до стеганоаналізу. У даному випадку гістограмний метод більш ефективніший.

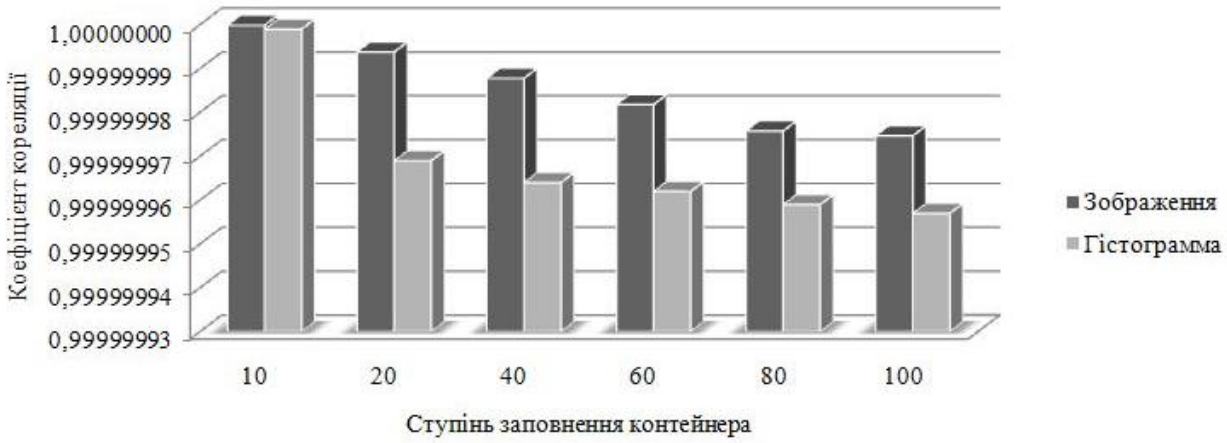


Рисунок 4.5. Коефіцієнти кореляції при використанні методу заміни компоненти S

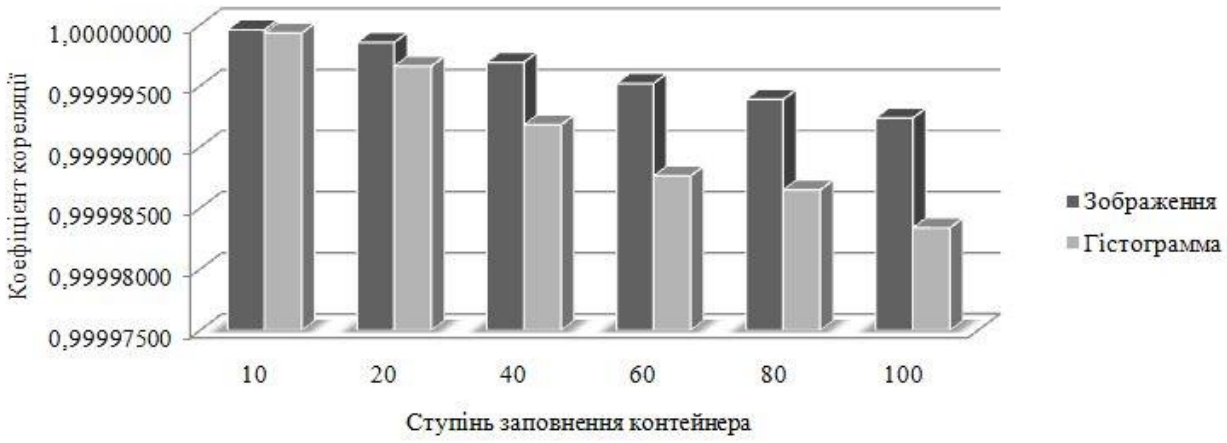


Рисунок 4.6. Коефіцієнти кореляції при використанні методу заміни синьої компоненти

Результати дослідження компоненти насиченості колірної моделі HLS при заповненні методом округлення значень елементів зображено на Рисунок 4.7. З результатів можна побачити, що використання гістограмнного аналізу більш ефективніше при виконанні стеганографічного аналізу.

Таким чином, використання компоненти насиченості більш оптимальніше при підвищенні стійкості стеганографічної системи до стеганографічного аналізу. При порівнянні методу заміни та округлення при дослідженні на базі показників коефіцієнтів кореляції, можна зробити висновок, що використання методу округлення призводить до меншого спотворення стеганографічного контейнера після стеганоперетворення. Це зумовлено тим, що коефіцієнт кореляції, при використанні гістограмного аналізу, вищий ніж у методу заміни НЗБ (Рисунок 4.8).

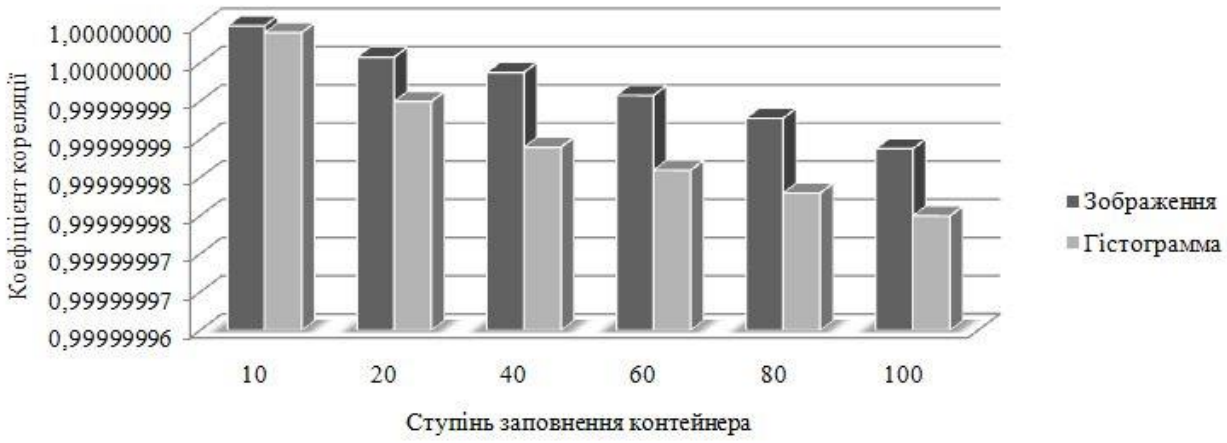


Рисунок 4.7. Коефіцієнти кореляції при використанні методу округлення компоненти S

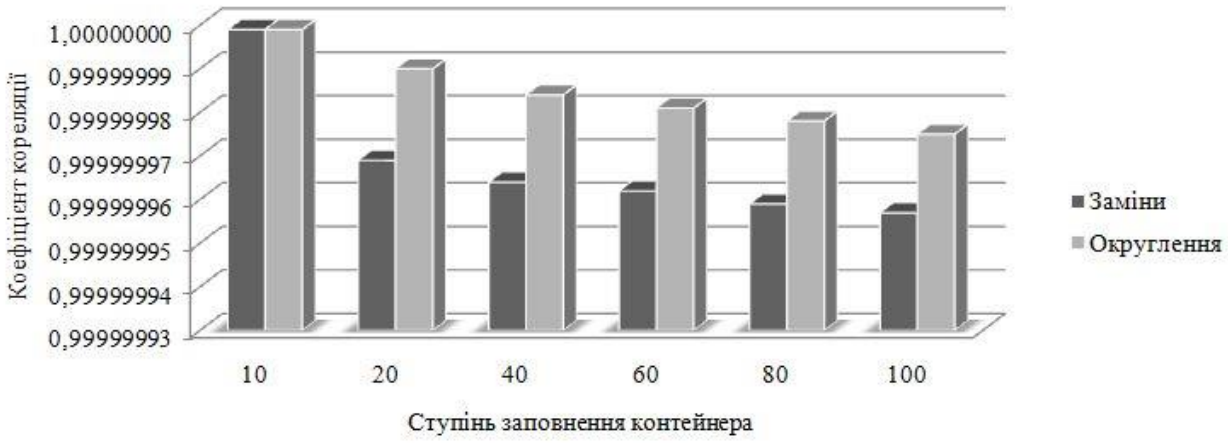


Рисунок 4.8. Коефіцієнти кореляції при використанні методу заміни та округлення значень елементів компоненти насиченості S

Характерним показником при використанні гістограммного аналізу є подібність гістограмм (Рисунок 4.9). Таким чином, результати дослідження гістограммним методом стеганографічного аналізу показують що округлення більш прийнятне для створення більш стійкішої стеганографічної системи. При використанні методу заміни, показники більш порівняно із методом округлення.

Показник тривалості виконання стеганографічного аналізу зображений у табл..4.1. Таким чином,середній час необхідний на проведення аналізу обома методами відносно однаковий і становить: при використанні методу порівняння зображень – 1,1 с, а при гістограмному методі – 1,2 с.

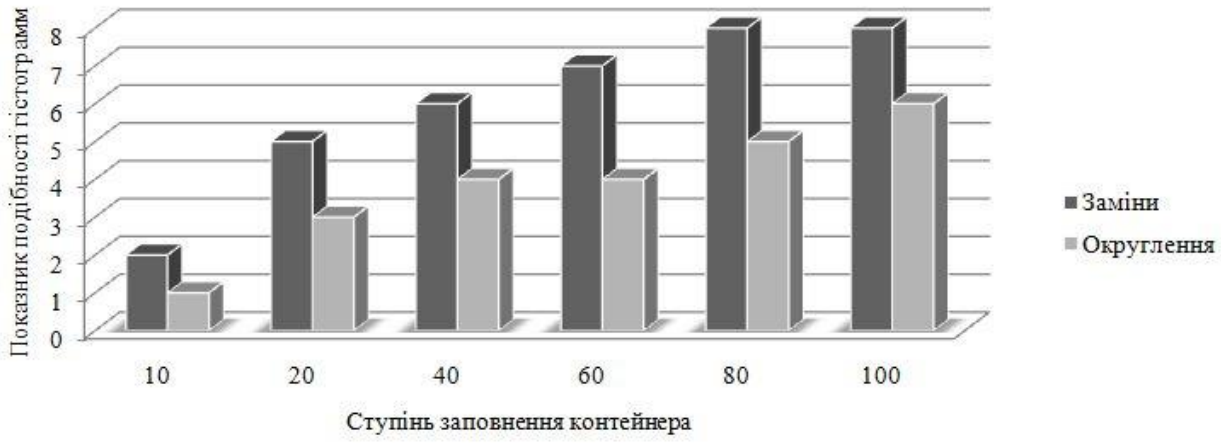


Рисунок 4.9. Показники подібності гістограмм при використанні методу заміни та округлення значень елементів компоненти насиченості S

Таблиця 4.1.

Час виконання стеганографічного аналізу

№	Тип аналізу	Ступінь заповнення контейнера, %						
		10 %	20%	40%	60%	80%	100%	Середній час
		Тривалість виконання стеганографічного аналізу, с						
1	Гістограммний	0,9	1,1	1,2	1,2	1,3	1,1	1,1
2	Порівняльний	1,1	1,0	1,1	1,2	1,3	1,2	1,2

Підводячи підсумок слід зазначити, що для підвищення стійкості стеганографічного контейнера до атак при передачі його каналами зв'язку необхідно використовувати метод округлення елементів компоненти насиченості у колірній моделі HLS. Це зумовлено рядом досліджень проведених у даній дипломній роботі та показниками досліджень, що були проведені у 3 та 4 розділі. При необхідності провести аналіз стійкості стеганографічного методу доречно використовувати гістограмний метод стеганографічного аналізу. Використання цього методу дозволяє оптимальніше оцінити спотворення стеганоконтейнера після стеганоперетворення. При спотворенні одного елементу зображення відбувається зміна двох значень у гістограммі. Тому що, зміна значення елементу зображення призводить до зменшення кількості значень у стовпчику що змінилось та збільшенні кількості значень на яке змінилося. На Рисунок наведені уривки гістограмми значень елементів зображення до стеганоперетворення (Hist_K) та після стеганоперетворення (Hist_K1) (Рисунок 4.10).

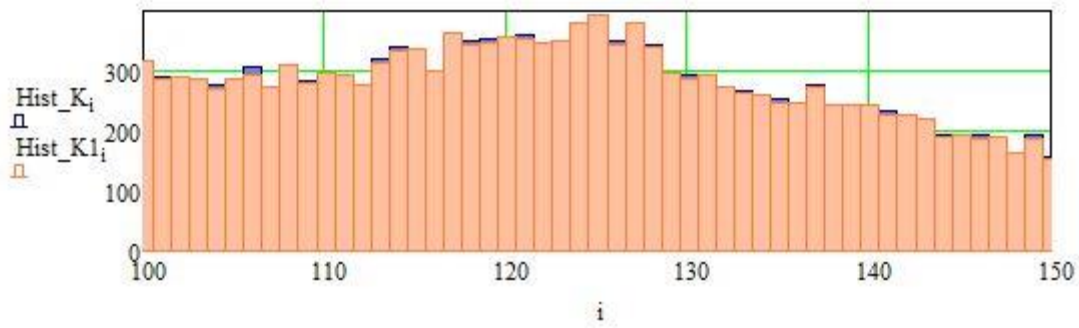


Рисунок 4.10. Уривки гістограмми значень елементів зображення до стеганоперетворення та після стеганоперетворення

Висновки по розділу 4

У даному розділі були розглянуті основні принципи стеганографічного аналізу. Таким чином, головний напрямк стеганографічного аналізу є безпосередньо модель стеганографічних систем та їх попереднє визначення, щоб отримати якісні та кількісні оцінки стійкості стеганотрансформації, а ще будування методів знаходження інформації, що прихована в контейнерах, її модифікації та знищення.

Було запропоновано гістограмний аналіз з метою оцінки удосконаленої стеганографічної системи з використанням методу округлення значень елементів зображення з метою приховування повідомлення у фіксованому контейнері, а саме растровому зображенні.Для оцінки якості стеганографічний методів було виділено ряд показників, таких як: кореляція зображення–оригіналу та зображення–результату; подібність гістограмм; час виконання стеганографічного аналізу.

Після проведення досліджень у даному розділі слід зазначити, що при необхідності провести аналіз стійкості стеганографічного методу доречно використовувати гістограмний метод стеганографічного аналізу. Використання цього методу дозволяє оптимальніше оцінити спотворення стеганоконтейнера після стеганоперетворення. При спотворенні одного елементу зображення відбувається зміна двох значень у гістограммі.

ВИСНОВКИ

При виконі даної дипломної роботи було визначено існуючі напрямки реалізації загроз для інформаційної безпеки. Отже, головна мета інформаційної безпеки – це захищенність ресурсів інфоормації від певних зовнішніх та внутрішніх або навмисних, або ненавмисних загроз. Отримані результати дозволяють визначити сучасні та можливі шляхи, за якими можна використовувати стеганографічні методи для захисту інформації в автоматизованих системах. Таким чином, стеганографічні методи найбільш ефективні при вирішенні проблем захисту конфіденційної інформації.

Були розглянуті основні етапи та принципи побудови стеганографічних систем. Розглянуті основні типи стеганосистем, а саме: системи із секретним ключем, змішані стеганосистеми, системи з відкритим ключем, безключові стеганосистеми. Для оцінки якості стеганографічний методів було виділено ряд показників, таких як: зміна розміру файлу після стеганоперетворення, кореляція зображень та спотворення якості зображення після реалізації стеганографічного методу приховування даних. Були виділені основні характеристики растрового зображення. До них належать: роздільна здатність, розмір растру та глибина кольору зображення.

Стеганографічні методи, що застосовувались у даній дипломній роботі, були реалізовані у прикладному програмному забезпеченні Mathcad, а саме: метод заміни НЗБ, метод псевдовипадкового інтервалу та метод блокового приховування.

При аналізі сучасних форматів файлів растрового зображення було визначено, що оптимальнішим форматом файлу для приховування даних є BMP. Тому, що розмір файлу, після стеганоперетворення, не змінюється порівняно з іншими форматами файлів, які розглядалися у даній дипломній роботі. Наступним кроком підвищення стійкості стеганосистеми був аналіз та оцінка колірних моделей растрового зображення. Для виконання процесу приховування повідомлення слід використовувати колірну модель – HLS, а саме компоненти насиченості – S. Вона є

більш стійкішою до спотворення зображення при реалізації приховування даних у нерухомих зображеннях.

Для підвищення стійкості стеганосистем до атак було виконано удосконалення стеганографічних методів приховування даних у нерухомих зображеннях. Удосконалення методів полягає в округлення десяткових значень елементів компонент при використанні моделі HLS для модифікації молодших бітів елементів компоненти. Використання стеганографічного ключа підвищує стійкість стеганосистеми до реалізації атак. Використання ключа реалізовано у методі псевдовипадкового інтервалу.

Було запропоновано гістограмний аналіз з метою оцінки удосконаленої стеганографічної системи з використанням методу округлення значень елементів зображення з метою приховування повідомлення у фіксованому контейнері, а саме растровому зображенні. При використанні гістограмного методу стеганографічного аналізу можливо оптимальніше оцінити спотворення стеганоконтейнера після стеганоперетворення. При виконанні спотворення одного елементу зображення відбувається зміна двох значень у гістограммі. Таким чином, зміна значення елементу зображення призводить до зменшення кількості значень у стовпчику що змінилось та збільшенні кількості значень на яке змінилося.

Отже, для організації передачі захищених даних слід використовувати графічний файл з форматом BMP та колірну модель – HLS. При реалізації стеганографічної системи на нерухомих зображень слід використовувати стеганографічний ключ, що підвищує надійність передачі даних. Особливу увагу слід приділити контейнеру, а особливо його характеристикам: роздільна здатність, розмір растру та глибина кольору зображення. При збільшенні роздільної здатності зменшується можливість виявити зміни при візуальному контролі. Збільшення розміру растру зображення збільшує крок занесення бітів повідомлення до контейнера. Глибина кольору зображення характеризує кількість бітів в одному елементі зображення, що може бути модифікований без значних змін структурних ознак контейнера.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 9 січня 2007 року // Відомості Верховної Ради України. – 2007. – №12. – ст.102.

2. Закон України «Про інформацію» від 2 жовтня 1992 року // Відомості Верховної Ради України (ВВР). – 1992. – №48. – ст.650.

3. НД ТЗІ 1.1–003–99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» // Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 р. № 22.

4. НД ТЗІ 1.1–002–99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» // Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 р. № 22.

5. Закон України від 21 січня 1994 р. «Про державну таємницю» // Відомості Верховної Ради. – 1994. – № 52. – с. 420.

6. Закон України «Про захист інформації в автоматизованих системах » від 5 липня 1994 року // Відомості Верховної Ради України. – 1994. – №31. – ст.286.

7. Закон України «Про Концепцію Національної програми інформатизації» від 02.02.98 р. № 75/98 ВР // Офіц. вісн. України. – № 10. – Ст. 376.

8. Закон України «Про електронні документи та електронний документообіг» від 22 травня 2003 р. // Відомості Верховної Ради. – 2003. – № 36. – Ст.275–78.

9. Закон України «Про електронний цифровий підпис» від 22 травня 2003 р. // Відомості Верховної Ради. – 2003. – № 20. – Ст.276

10. НД ТЗІ 2.5–005–99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» // Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 р. № 22.

11. Закон України «Про захист інформації в автоматизованих системах » від 5 липня 1994 року // Відомості Верховної Ради України. – 1994. – №31. – ст.286.

12. Юдін О.К., Симониченко Я.А. Аналіз сучасних графічних форматів в умовах реалізації процесів стеганозахисту: матеріали VII міжнародної науково–практичної конференції [”Актуальные проблемы современных наук – 2011”], 07–15 червня 2011 р. – Польща. – К.:Наука і студія, 2011. – №26. –С.69.

13. Стасюк О.І., Гнатюк С.О., Довгич Н.І., Літош М.С. Сучасні стеганографічні методи захисту інформації // Науково–технычний журнал ”Захист інформації” №1, – 2011. – С.15.

14. Симониченко Я.А. Підвищення стійкості стеганоконтейнера на базі аналізу колірних моделей зображення: VII міжнародної науково–практичної конференції [”Актуальные научные достижения – 2011”], 27 червня –05 серпня 2011 р. – Прага. – К.:Education and Science, 2011. – №20. –С.65.

15. Сердюк В. Информационная безопасность автоматизированных систем предприятий // Бухгалтер и комп’ютер. – 2007. – №1.

16. Таранчук А.А. Стеганографічний метод приховування даних в області частотних перетворень зображень / А.А. Таранчук, Л.Г. Гальпер, О.О. Марценюк // Вісник Хмельницького національного університету – 2009. – №2. – С. 197.

17. Федік Л.Ю. Аналіз колірних моделей HSV/HSB, HLS, lab / Л.Ю. Федік // Комп’ютерно–інтегровані технології: освіта, наука, виробництво – 2010. – №2. – С.103.

18. Бельська В.Ю. Метод надлишкового представлення та збереження даних у графічних контейнерах / В.Ю. Бельська, П.П. Костенко, О.Є. Сухарев, В.О. Шевченко // Електромеханічні і енергозберігаючі системи – 2010. –№4. – С.113.

19. Поліновський В.В. Інформаційна технологія для дослідження методів стеганографії і стегоаналізу / В.В.Поліновський, В.Ю. Корольов, В.А.Герасименко, М.Л. Горинштейн // Комп’ютерно–інтегровані технології: освіта, наука, виробництво – 2011. – №5. – С.236.

20. Хорошко В.О., Азаров О.Д., Шелест М.Є., Яремчук Ю.Є. Основи комп'ютерної стеганографії : Навч. посіб. для студентів і аспірантів. – Вінниця: ВДТУ, 2003.

21. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – К.: "МК–Пресс", 2006. – 288 с., ил.

22. Грибунин В.Г., Оков И.Н., Туринцев И.В. *Цифровая стеганография*. – М.: Солон–Пресс, 2002.

23. Генне О.В. Основные положения стеганографии // Защита информации. Конфидент. – 2000. – №3.

24. Виктор Порев Компьютерная графика. Учебное пособие. – БВХ–Петрбург, 2004. – 432 стр.

25. Ватолин Д., Ратушняк А., Смирнов М., Юкин В. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. – М.: ДИАЛОГ–МИФИ, 2002. – 384 с.