Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Мірошниченко Дмитро Владиславович*

академічної групи *125-17-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Стеганографічне вбудовування інформації в цифрове зображення з використанням фрактального перетворення*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	к.т.н., доц. Герасіна О.В.			
розділів:				
спеціальний	ст викл. Начовний І.І.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2021

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Мірошниченко Дмитро Владиславович* **академічної групи** *125-17-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*

за освітньо-професійною програмою *Кібербезпека*

на тему *Стеганографічне вбудовування інформації в цифрове зображення з використанням фрактального перетворення*

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз принципів приховування даних в цифрових зображеннях і фрактального аналізу, а також існуючих підходів до вбудовування інформації у фрактально стиснені зображення.	25.02.2021 – 31.03.2021
Розділ 2	Розробка підходу до стеганографічного вбудовування інформації в зображення, стиснене фрактальним методом, з урахуванням потужності пікселів домену та оцінка його ефективності.	01.04.2021 – 12.05.2021
Розділ 3	Розрахунки капітальних витрат, витрат на експлуатацію системи безпеки та термін окупності інвестицій застосування запропонованого підходу.	13.05.2021 – 09.06.2021

Завдання видано _____ Герасіна О.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Мірошниченко Д.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 73 с., 21 рис., 4 додатки, 46 джерел.

Об’єкт розробки – фрактально стиснені зображення.

Предмет розробки – підхід до стеганографічного вбудовування інформації в зображення, стиснене фрактальним методом.

Мета кваліфікаційної роботи – забезпечення можливості прихованої передачі конфіденційних даних, використовуючи контейнер, представлений у вигляді фрактально стисненого зображення.

Наукова новизна результатів полягає у тому, що у запропонованому підході на етапі виділення доменів і рангових областей потужність пікселів домену коригується з урахуванням значення приховуваних біт інформації.

У першому розділі проаналізовано принципи приховування даних в цифрових зображеннях і фрактального аналізу, а також існуючі підходи до вбудовування інформації у фрактально стиснені зображення.

У спеціальній частині роботи запропоновано підхід до стеганографічного вбудовування інформації в зображення, стиснене фрактальним методом, з урахуванням потужності пікселів домену та оцінено його ефективність. За наслідками досліджень зроблено висновки щодо рішення поставленої задачі.

У економічному розділі виконані розрахунки капітальних витрат, витрат на експлуатацію системи безпеки та термін окупності інвестицій застосування запропонованого підходу.

СИСТЕМА ІТЕРАТИВНИХ ФУНКЦІЙ, АФІННІ ПЕРЕТВОРЕННЯ, ФРАКТАЛЬНЕ СТИСНЕННЯ, КОМП’ЮТЕРНА СТЕГАНОГРАФІЯ, ЦИФРОВЕ ЗОБРАЖЕННЯ, ПОТУЖНОСТІ ПІКСЕЛІВ ДОМЕНУ, РАНГОВІ ОБЛАСТІ, ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ

РЕФЕРАТ

Пояснительная записка: 73 с., 21 рис., 4 приложения, 46 источников.

Объект разработки – фрактально сжатые изображения.

Предмет разработки – подход к стеганографическому встраиванию информации в изображение, сжатое фрактальным методом.

Цель квалификационной работы – обеспечение возможности скрытой передачи конфиденциальных данных, используя контейнер, представленный в виде фрактально сжатого изображения.

Научная новизна заключается в том, что в предложенном подходе на этапе выделения доменов и ранговых областей мощность пикселей домена корректируется с учетом значения скрываемых бит информации.

В первой главе проанализированы принципы сокрытия данных в цифровых изображениях и фрактального анализа, а также существующие подходы к встраиванию информации во фрактально сжатые изображения.

В специальной части работы предложен подход к стеганографическому встраиванию информации в изображение, сжатое фрактальным методом, с учетом мощности пикселей домена и оценена его эффективность. По результатам исследований сделаны выводы относительно решения поставленной задачи.

В экономическом разделе выполнены расчеты капитальных затрат, затрат на эксплуатацию системы безопасности и срок окупаемости инвестиций применения предложенного подхода.

СИСТЕМА ИТЕРАТИВНЫХ ФУНКЦИЙ, АФФИННОЕ ПРЕОБРАЗОВАНИЕ, ФРАКТАЛЬНОЕ СЖАТИЕ, КОМПЬЮТЕРНАЯ СТЕГАНОГРАФИЯ, ЦИФРОВОЕ ИЗОБРАЖЕНИЕ, МОЩНОСТИ ПИКСЕЛЕЙ ДОМЕНА, РАНГОВЫЕ ОБЛАСТИ, ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ

ABSTRACT

Explanatory note: p. 73, fig. 21, 4 additions, 46 sources.

The object of development is fractally compressed images.

The subject of development is the approach to steganographic embedding of information in the image compressed by the fractal method.

The purpose of the qualification work is to ensure the possibility of covert transfer of confidential data using a container presented in the form of a fractally compressed image.

The scientific novelty of the results is that in the proposed approach at the stage of allocation of domains and rank areas, the power of the pixels of the domain is adjusted taking into account the value of the hidden bits of information.

The first section analyzes the principles of hiding data in digital images and fractal analysis, as well as existing approaches to embedding information in fractally compressed images.

In a special part of the work the approach to steganographic embedding of information in the image compressed by a fractal method, taking into account the pixel power of the domain is offered and its efficiency is estimated. Based on the results of research, conclusions were made regarding the solution of the problem.

In the economic section, calculations of capital costs, costs of operating the security system and the payback period of the application of the proposed approach.

SYSTEM OF ITERATIVE FUNCTIONS, ATHENS TRANSFORMATIONS, FRACTAL COMPRESSION, COMPUTER STEGANOGRAPHY, DIGITAL IMAGE, POWER STRENGTH, SIMULATION MODELING

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ДКП – Дискретне косинусне перетворення;

МНК – Метод найменших квадратів;

НЗБ – Найменш значущі біти;

СКВ – Середньоквадратичне відхилення;

ЦВЗ – Цифровий водяний знак;

IFS – Iterated Function System – Система ітеративних функцій.

ЗМІСТ

с.

ВСТУП

В області захисту інформації стеганографія зображень займає унікальну нішу і підтверджує свою ефективність стрімкими темпами розвитку. Це частково пояснюється популярністю криптографічних засобів захисту і необхідністю таємного зберігання ключа. Непомітна передача конфіденційних повідомлень теж складає значну частину практичного арсеналу. Широке застосування стеганографія зображень знайшла в області захисту авторських прав, що призвело до відокремленню напрямку розробки і впровадження цифрових водяних знаків (ЦВЗ).

Кожна з практичних задач вимагає конкретного підходу до її вирішення, однак в більшості стеганографічна ефективність забезпечується об'єднанням якостей секретності та робастності. При цьому рівень зазначених якостей необхідно співвідносити з обсягом вбудованих даних [1].

Підходи забезпечення необхідного рівня стійкості описані в [2]. На противагу робастності, питання секретності є неоднозначним, що пояснюється великою кількістю демаскуючих ознак. Це пояснює складність розробки абсолютно адекватного детектора. Однак відносний показник вірного детектування дає можливість оцінити ефективність стегоаналітичного критерію. Протистояння виявленню за умови підвищення пропускної здатності таємного каналу передбачає володіння критерієм кращим ніж у перехоплювача.

Незважаючи на різноманіття стегодетекторів, їх загальною структурною особливістю є бінарний класифікатор, який використовує певні чутливі до наявності таємного вмісту характеристики. Послідовність характеристик кожного зображення може бути представлена вектором, як в роботах [3, 4], де класифікація виконувалася за допомогою методу опорних векторів. Однак з метою поліпшення статистики детектування, навчання класифікатора має відбуватися на вибірці, що репрезентує два підмножини зображень: перша утворена оригінальними зображеннями; друга – стегозображеннями. Причому ефективність визначається ступенем відповідності параметрів вбудовування в

тренувальній вибірці дійсним параметрам тестової стегосистеми. Таким чином, якість стегоаналізу знижується при невідомих параметрах реальної (тестової) стегосистеми або за умови їх зміни в процесі вбудовування.

Другою особливістю стегокритерію є склад характеристик, які повинні сприяти розділенню стегозображень від оригінальних зображень. Одним із шляхів досягнення цього можна назвати облік притаманних певному формату зображень властивостей, які обумовлені алгоритмом обробки.

Широке поширення алгоритмів стиснення зумовлено значними досягненнями в області обробки зображень. Це пояснює той факт, що переважна більшість сучасних форматів представлення зображень забезпечують стиснення зі втратами. Файли форматів стиснених зображень рідко піддаються додатковій обробці і стисненню, тому забезпечують більшу робастність при встановленні даних. З іншого боку для більшості алгоритмів стиснення зі втратами важко оцінити змінені особливості оригінального зображення, що сприяє прихованню.

Фрактальні алгоритми забезпечують вдале співвідношення між коефіцієнтом стиснення та якістю і володіють унікальною властивістю деталізації при довільному масштабуванні [5, 6]. Розвиток фрактального стиснення забезпечує популярність форматів на його основі, що підтверджує доцільність їх стеганографічного використання.

Таким чином, вдосконалення підходів до стеганографічного вбудовування інформації у фрактально стиснені зображення наразі є актуальною задачею.

Метою роботи є забезпечення можливості прихованої передачі конфіденційних даних, використовуючи контейнер, представлений у вигляді фрактально стисненого зображення.

Постановка задачі:

• проаналізувати принципи приховування даних в цифрових зображеннях, а також фрактального аналізу;

• провести аналіз існуючих підходів до вбудовування інформації у фрактально стиснені зображення;

• запропонувати підхід до стеганографічного вбудовування інформації в зображення, стиснене фрактальним методом, з урахуванням потужності пікселів домену;

• оцінити ефективність запропонованого підходу.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Приховування даних в цифрових зображеннях

1.1.1 Модель системи стеганографічного приховування даних

Для побудови моделі системи стеганографічного приховування даних вводяться такі поняття [2, 7-9]:

Стеганографічне поле SF – простір стеганографічного каналу, його об'єкти, а також методи вбудовування та виявлення, тобто

$$SF = \left(SC, C, M, K, \hat{C}, E, D\right), \tag{1.1}$$

де об'єктами стеганографічного поля є: c – контейнер; $c \in C$ – множина всіх контейнерів; m – повідомлення; $m \in M$ – множина всіх повідомлень; k – ключ; $k \in K$ – множина всіх ключів; $\hat{c}$ – заповнений або модифікований контейнер, $\hat{c} \in \hat{C}$ – множина всіх заповнених контейнерів.

Метод вбудовування E – набір інструкцій здійснюваних над стеганографічним контейнером для вбудовування повідомлень і отримання модифікованого контейнера:

$$E : C \times M \times K \to \hat{C},\ \hat{c} = E(c, m, k). \tag{1.2}$$

Метод виявлення D – набір інструкцій здійснюваних над модифікованим контейнером для виявлення і вилучення повідомлень:

$$D : \hat{C} \times K \to M,\ m = D(\hat{c}, k). \tag{1.3}$$

Простір стеганографічного каналу SC – просторова, і / або часова, і / або частотна область мультимедійних даних, придатна для стеганографічної передачі повідомлень:

$$\begin{aligned} &F : C \to SC; \\ &SC \subset C. \end{aligned} \tag{1.4}$$

Стеганографічна система або стеганосистема SS – сукупність засобів і методів, які здійснюють дії над об'єктами стеганографічного поля в межах

простору стеганографічного каналу за допомогою методів вбудовування або виявлення:

$$\begin{aligned} &SS(SC,E): C \times K \times M \to \widehat{C},\ \widehat{c} = SS_{SC,E}(c,k,m); \\ &SS(SC,D): \widehat{C} \times K \to M,\ m = SS_{SC,D}(\widehat{c},k). \end{aligned} \tag{1.5}$$

Стеганографічна модифікація - модифікація контейнера на підставі алгоритму вбудовування:

$$\widehat{c} = E(c,m,k). \tag{1.6}$$

Стеганографічний процес можна розбити на 3 етапи. На першому етапі здійснюється вибір об'єктів стеганографічного поля $c \in C$, $m \in M$, $k \in K$. Як приховувані дані може використовуватися будь-яка інформація: текст, аудіо-файл, зображення і т.п. Дану інформацію прийнято називати прихованим повідомленням або просто повідомленням. Файлом-контейнером називається файл, призначений для приховування в ньому конфіденційної інформації, причому $M \subset C$. Вибір контейнера має суттєвий вплив на надійність стеганосистеми і на можливість виявлення факту передачі приховуваного повідомлення. Розмір контейнера безпосередньо впливає на пропускну здатність стеганографічного каналу передачі даних.

На другому етапі вибирається метод вбудовування / виявлення E, D.

На третьому етапі здійснюється генерація стеганоключа. Стеганоключ або просто ключ – деяка секретна інформація, відома тільки законному користувачеві, необхідна для приховування повідомлення. Залежно від рівня захисту (наприклад, вбудовування попередньо зашифрованого повідомлення) в стеганосистемі може бути один або декілька ключів. Ключ може бути представлений псевдовипадковою послідовністю біт, яку породжує генератор, що задовольняє певним вимогам (криптографічно безпечний генератор). Розрізняють два типи стеганосистем:

- з відкритим ключем;

- з секретним ключем.

У системах з відкритим ключем використовуються два ключа $k_o \in K_o$ і $k_{os} \in K_{os}$, незалежні один від одного. Один з ключів $k_o \in K_o$ є не секретним, тобто може передаватися вільно по незахищеному каналу зв'язку, другий $k_{os} \in K_{os}$, є секретним, і не може бути отриманий за допомогою обчислень з ключа $k_o \in K_o$.

Одним із прикладів використання систем з відкритим ключем може бути наступний набір ключів: k_o=«Дівоче прізвище матері?», k_{os}=«Іванова». Стеганографічна система в даному випадку буде здійснювати дію над об'єктами у відповідність з ключем k_{os}:

$$SS(SC,E): C \times K_{os} \times M \to \hat{C},\ \hat{c} = SS_{SC,E}(c,k_{os},m). \tag{1.7}$$

У стеганосистемі з секретним ключем використовується один секретний ключ $k_s \in K_s$, який повинен бути визначений або до початку обміну приховуваними повідомленнями, або переданий по захищеному каналу. Стеганографічна система буде здійснювати дію над об'єктами у відповідності з ключем $k_s \in K_s$:

$$SS(SC,E): C \times K_s \times M \to \hat{C},\ \hat{c} = SS_{SC,E}(c,k_s,m). \tag{1.8}$$

Таким чином, стеганографічний процес можна представити у вигляді, як на рис. 1.1.

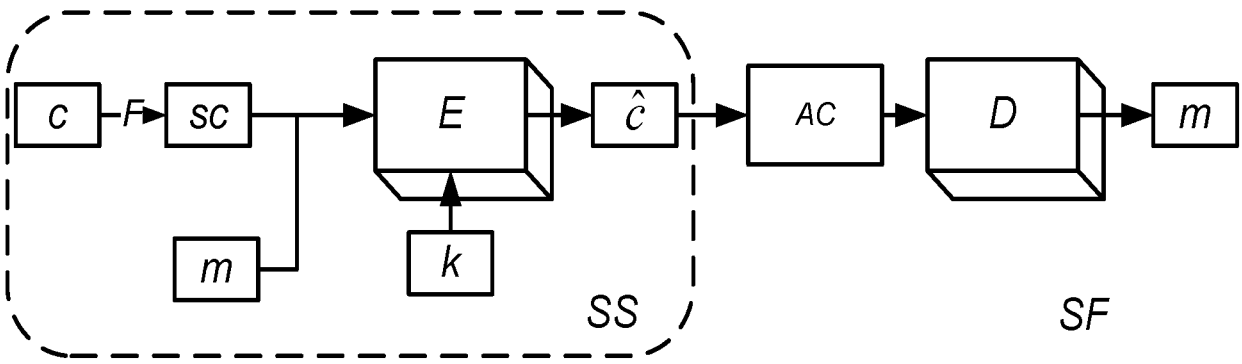


Рисунок 1.1 – Узагальнена схема процесу стеганографічного приховування даних

Під каналом атак AC мається на увазі складова стеганографічного поля, де здійснюються неправомірні дії порушника. Порушником називають особу, яка вчиняє протиправні дії, спрямовані на виявлення, вилучення або руйнування повідомлення. Під стійкістю різних стеганосистем або стеганостійкістю розуміється їх здатність приховувати від кваліфікованого порушника факт існування стеганографічного каналу, здатність протистояти спробам порушника зруйнувати, спотворити, видалити таємно передані повідомлення, а також здатність підтвердити або спростувати достовірність приховано переданої інформації. Стеганостійкість оцінюється процентним відношенням кількості цифрових файлів в яких порушнику вдалося виявити факт наявності вбудованих повідомлень або непомітно перешкодити їх прихованій передачі до загальної кількості досліджуваних файлів.

Під пропускною здатністю стеганосистеми розуміється відношення максимально можливого обсягу вбудованого повідомлення до обсягу файлу-контейнера при дотриманні вимог стеганостійкості.

1.1.2 Методи стеганоаналізу для графічних файлів

Стеганоаналіз – наука про вивчення методів виявлення існування секретної інформації у відкритих повідомленнях [10]. В стеганоаналізі розрізняють дві основних стратегії дій противника (стеганоаналітика): активну та пасивну. При активній стратегії противник намагається знищити секретну інформацію в відкритому повідомленні, при пасивній – виявити факт існування і саму секретну інформацію.

Найпростішими методами аналізу контейнерів-зображень є візуальні методи. Візуальні методи намагаються виявити існування стеганографічного вкраплення за допомогою візуального контролю (неозброєним оком) або за допомогою автоматизованих процесів. Візуальний контроль за допомогою неозброєного ока матиме успіх, коли стеганографічні дані вкраплені у однотонні фрагменти зображення. Автоматизовані комп'ютерні додатки

дозволяють розкласти зображення на його індивідуальні бітові площини. Бітова площина складається з одного біту пам'яті для кожного пікселя в зображенні, і є типовим місцем зберігання інформації, прихованої за допомогою стеганопрограм. Будь-який незвичний зовнішній вигляд у відображенні площини молодшого двійкового розряду буде, ймовірно, означати існування вкраплених стеганографічних даних.

Для методу візуального аналізу бітових площин велике значення має те, який метод використовувався при вкрапленні інформації. Так, якщо приховання інформації здійснювалося за допомогою методу послідовної заміни (рис. 1.2, а), або методу розподіленого вкраплення (на основі генератора псевдовипадкових чисел) (рис. 1.2, б), то факт приховання може бути встановлений з великою ймовірністю. Також, візуально можна визначити наявність вкрапленої інформації у випадку використання методу вкраплення повідомлення із заповненням. Оскільки ймовірнісні характеристики повідомлення не збігаються з ймовірнісними характеристиками молодших бітів пустого контейнера, то при перегляді бітового зрізу з вкрапленими даними буде чітко видно границю між заповненою і не задіяною вкрапленням частиною (рис. 1.2, в).

а *б* *в*

Рисунок 1.2 – Бітові площини стеганоконтейнерів: а – метод послідовної заміни; б – метод розподіленого вкраплення; в – метод вкраплення з заповненням

Існують стеганографічні програми, які використовують метод дописування даних у кінець файлу-контейнера завдяки використанню системи

маркерів. Всі стандартні програми перегляду, доходячи до маркера “кінець зображення” припиняють роботу, і прихована інформація залишається непізнаною. Цим способом можна розмістити досить багато інформації. Однак такий метод приховання є уразливим до методів структурного аналізу. Виявити зміни у форматі файлу даних можливо за допомогою шістнадцятирічного редактора. Використовуючи інформацію заголовка, можна виявити “кінець зображення”, а отже визначити місце розташування позиції вкраплених даних.

Деякі стеганографічні програми залишають після себе сигнатури – певні послідовності байтів, які завжди з’являються у файлі після вкраплення інформації. Методи сигнатурного аналізу зображення дозволяють відшукати бітові послідовності, специфічні для певних програм стеганоприховання (рис. 1.3). Стеганоаналіз на основі сигнатур може вимагати дуже багато часу, тому що спочатку потрібно розпізнати сигнатуру для певної стеганографічної програми з великої вибірки файлів, які були вкраплені з її допомогою. Крім того, повинні бути використані автоматизовані процеси для пошуку всіх потенційних файлів-контейнерів для цієї певної сигнатури.

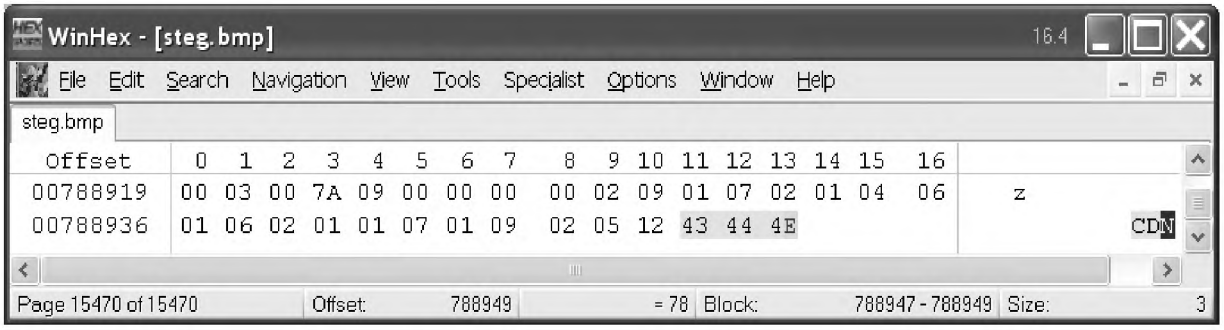


Рисунок 1.3 – Перегляд зображення в шістнадцятирічному редакторі на наявність сигнатур (CDN – сигнатура стеганографічної програми Hiderman)

До переваг сигнатурних методів відноситься можливість отримання результату, який однозначно характеризує застосовану для приховання даних стеганосистему. Основним недоліком є невелике (менш 10 %) число стеганопрограм, що залишають у контейнерах свої сигнатури.

Статистичні методи аналізу намагаються виявити найменші зміни в статистичній поведінці файлу, викликані вкрапленою стеганографією. Суть статистичних методів полягає в оцінюванні ймовірності існування стеганографічного приховання з невідомою стеганосистемою на основі критерію оцінки наближення досліджуваного контейнера до «природного».

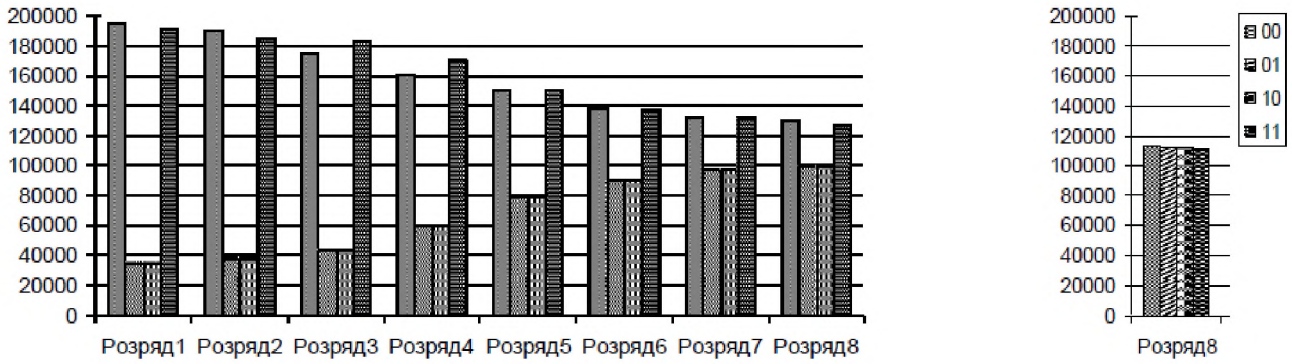
Метод оцінки числа переходів значень молодших бітів у сусідніх елементах контейнера використовує знання, що між молодшими бітами сусідніх елементів, і між ними і іншими бітами природних контейнерів є кореляційні зв'язки. При аналізі графічних файлів формату BMP в якості елементів послідовності, яка аналізується, вибираються найменш значущі біти (НЗБ) пікселів, що розташовуються поруч, колірних складових зображення. При дослідженні файлів формату JPEG – молодші біти сусідніх коефіцієнтів дискретного косинусного перетворення (ДКП,) відмінних від 0 і 1. Під «переходом» розуміють перехід значення i-го елемента послідовності в значення i+1 елемента послідовності x, i=1,2,…n-1, n – довжина послідовності. Оскільки послідовності є двійковими, то аналізуються чотири види переходів: з 0 в 0, з 0 в 1, з 1 в 0 і з 1 в 1. За отриманими результатами будується гістограма [10, 20]. Для кожного розряду перший стовпець гістограми показує число переходів у потоці НЗБ із 0 в 0, другий стовпець – з 0 в 1, третій стовпець – з 1 в 0, четвертий стовпець – з 1 в 1.

Для пустого контейнера і контейнера, що містить вкраплену інформацію, число переходів у потоці НЗБ буде різним. Розподіл НЗБ стеганоконтейнера має, як правило, випадковий характер. Відповідно число переходів у потоці НЗБ для всіх станів буде приблизно однаковим, що не властиво пустому контейнеру (рис. 1.4).

Статистичний критерій для оцінки частот переходів бітових значень [20]: файл, що аналізується розбивається на K блоків однакової довжини і вибирається деяке порогове значення h_M. Обчислюються значення статистик

$$M_j = \left[\frac{(\mu_{00} - \mu_{01})^2}{2} + \frac{(\mu_{11} - \mu_{10})^2}{2} \right], \; j = 1,2,...K \tag{1.9}$$

μ_{ij}, – кількість переходів у потоці НЗБ з і в j. У випадку якщо $M_j < h_M$, вважається, що в j-м блоці міститься прихована інформація.



а *б*

Рисунок 1.4 – Гістограма частот переходів бітових значень: а – пустого контейнера, б – стеганоконтейнера (восьмий розряд контейнера, в який були внесені зміни)

Застосування цього критерію до JPEG файлів виявилося ефективним при значному заповненні зображень контейнерів. Діапазон зміни значень M_j для пустих контейнерів становив від 40000 до 130000. Після приховання інформації значення M_j зменшувалися до 250-6000.

Метод оцінки частот появи k-бітових серій у потоці НЗБ елементів контейнера дозволяє оцінити рівномірність розподілу елементів в послідовності, яка досліджується, на основі аналізу частоти появи нулів і одиниць, і серій, що складаються з k бітів [10, 21]. У бітовому поданні послідовності x , що досліджується, підраховується скільки разів зустрічаються нулі і одиниці (k=1), серії-двійки (00, 01, 10, 11: k=2), серії-трійки (000, 001, 010, 011, 100, 101, 110, 111: k=3) і т.д. На основі результатів будується гістограма.

Для JPEG зображень гістограма будується за значеннями частот появи бітових серій у потоці НЗБ коефіцієнтів ДКП відмінних від –1, 0, 1.

Для незаповнених BMP і JPEG зображень не є характерним, щоб значення частот всіх компонентів знаходились досить близько (рис. 1.5,а). При

вкрапленні інформації, значення частот зближаються (рис. 1.5,б). Цей факт використовується при аналізі.

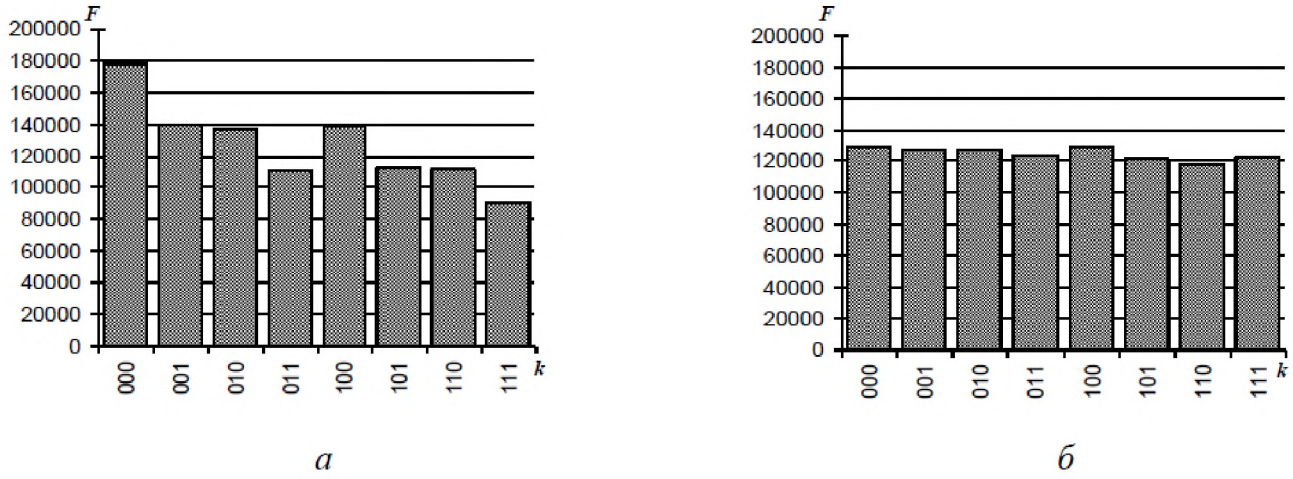


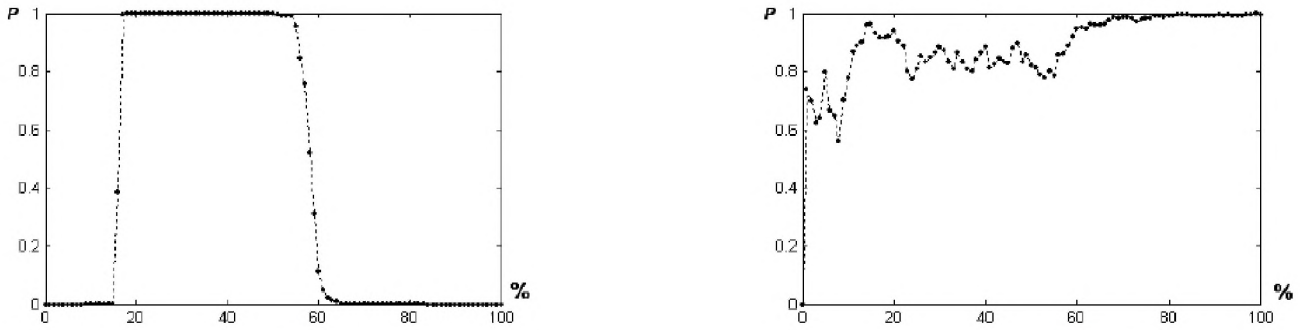
Рисунок 1.5 – Гістограма частот серії-трійки (k=3) у потоці НЗБ:
а – пустого контейнера, б – стеганоконтейнера

Результати роботи методу залежать від стеганографічного перетворення і від обсягу даних, що приховуються. Як правило, виявлення факту прихування здійснимо при заповненні контейнера на 60% і вище.

Метод аналізу розподілу пар значень на основі критерію χ^2 (хі-квадрат) використовує аналіз гістограми, отриманої за елементами зображення і оцінку розподілу пар значень цієї гістограми [10, 22]. Для BMP файлів пари значень формуються значеннями пікселів зображення, для JPEG – квантованими коефіцієнтами ДКП, які відрізняються за молодшим бітом. Молодші біти зображень не є випадковими. Частоти двох сусідніх елементів контейнера мають перебувати досить далеко від значення частоти середнього арифметичного цих елементів. В «пустому» зображенні ситуація, коли частоти елементів зі значеннями 2N і 2N+1 близькі за значенням, зустрічається досить рідко. При вкрапленні інформації дані частоти зближаються або стають рівними. Ідея атаки χ^2 полягає в пошуку цих близьких значень і підрахунку ймовірності вкраплення на основі того, як близько розташовуються значення частот парних і непарних елементів аналізованого контейнера. Особливістю

алгоритму є послідовний аналіз всього зображення і, відповідно, накопичення частот елементів.

Метод χ^2 є універсальним, оскільки підходить для аналізу зображень, в які інформація вкраплювалася за допомогою різних стеганографічних програм. Однак результати роботи методу за критерієм χ^2 значною мірою залежать від методу приховання даних. При послідовній заміні НЗБ елементів контейнера і вкрапленні повідомлення з заповненням метод виявляє наявність прихованих даних (рис. 1.6), а при псевдовипадковому виборі молодших бітів (розподіленому вкрапленні) метод не спрацьовує.

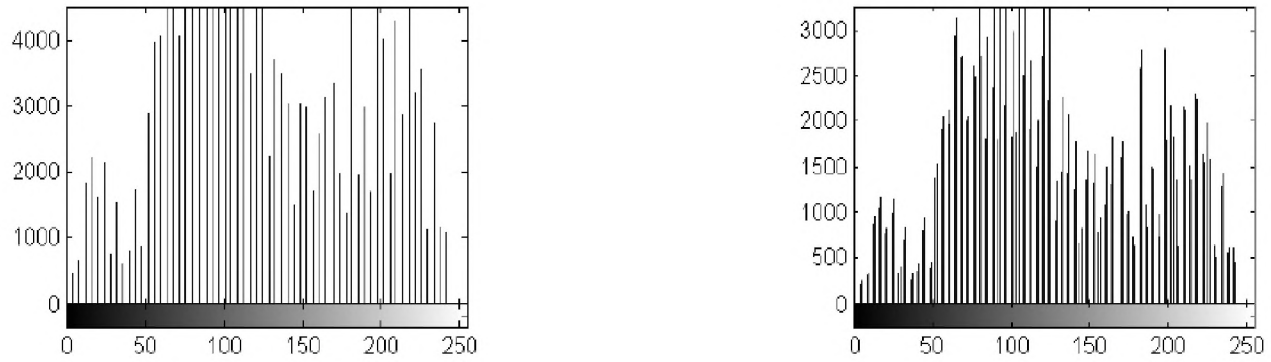


а *б*

Рисунок 1.6 – Ймовірність вкраплення за критерієм χ^2: а – послідовне вкраплення, б – вкраплення з заповненням

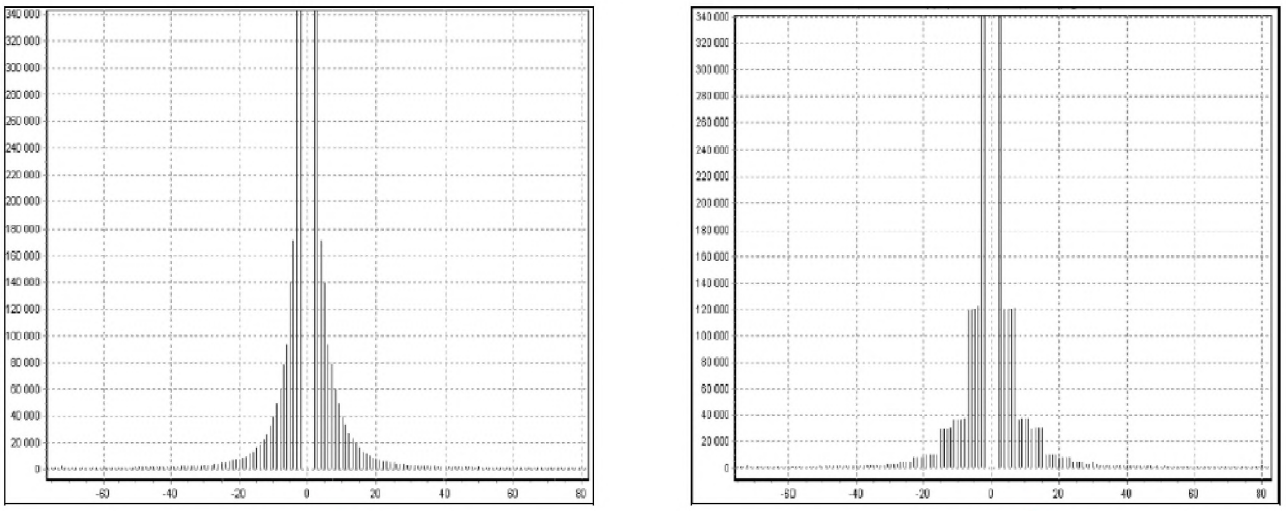
Метод аналізу гістограм, побудованих за частотами елементів зображення дозволяє оцінити рівномірність розподілу елементів зображення, що аналізується, а також визначити частоту появи конкретного елемента. Якщо частоти двох сусідніх елементів BMP зображення близькі за значенням і/або розташовані з різницею в одиницю (наслідок використання класичного методу НЗБ), то контейнер містить приховані дані (рис. 1.7,б). В іншому випадку контейнер вважається пустим (рис. 1.7,а) [21].

Для зображень в JPEG форматі будується гістограма частот квантованих коефіцієнтів ДКП. Експериментально виявлено, що огинаюча гістограми пустого зображення має більш гладкий характер (рис. 1.8,а), у порівнянні з гістограмами зображень, що містять приховані дані (рис. 1.8,б).



а *б*

Рисунок 1.7 – Гістограма частот пікселів: а – вихідного BMP зображення, б – BMP зображення, що містить приховану інформацію



а *б*

Рисунок 1.8 – Гістограма частот коефіцієнтів ДКП: а – вихідного JPEG зображення, б – JPEG зображення, що містить приховану інформацію

Звичайно, залежно від характеру і рівня стискання зображення, гістограми можуть змінюватися – у них можуть з’являтися стрибки і провали, але важливо те, що приховання інформації змінює загальний вид гістограм. Більшість стеганографічних програм, що працюють із JPEG, приховують дані в молодших бітах коефіцієнтів ДКП відмінних від 0 і 1. Як наслідок частоти 0-х і 1-х ДКП не змінюються, в той час як всі інші частоти або зменшуються, або збільшуються залежно від алгоритму вкраплення. При значних обсягах

приховуваної інформації гістограми часто мають ступеневий характер, що нетипово для “природних” JPEG зображень.

Метод аналізу розподілу елементів зображення на площині призначений для визначення залежностей між елементами послідовності, що досліджується. На площину (поле) розміром $(2^R - 1) \times (2^R - 1)$, де R – розрядність елемента послідовності, наносяться точки з координатами (x_i, x_{i+1}), x_i – елементи послідовності x, що досліджується, i=1,2,…n-1, n – довжина послідовності [10, 21]. За отриманим результатом проводиться аналіз.

Якщо точки по всьому полю розташовані хаотично, то між елементами послідовності відсутні залежності, що характерно для контейнерів з вкрапленими даними, як показано на рис. 1.9, б. У випадку пустого контейнера точки на полі будуть розташовані нерівномірно або утворювати «візерунки» , як показано на рис. 1.9, а.

Рисунок 1.9 – Розподіл на площині елементів: а – вихідного зображення, б – зображення, що містить приховану інформацію

Крім наведених вище, існує багато статистичних методів, заснованих на різних математичних моделях процесу стеганографії. Статистичні методи не є засобом, який дозволяє з 100% надійністю визначати наявність прихованої інформації. Вони дають можливість стеганоаналітику з певною ймовірністю судити про те, використовувалось стеганографічне перетворення чи ні.

1.2 Методи фрактального аналізу

1.2.1 Поняття «фрактал»

Термін фрактал, був запропонований Б. Мандельбротом у 1975 р. для позначення нерегулярних самоподібних математичних структур. Основне визначення фракталу, дане Мандельбротом, звучало так: «Фракталом називається структура, що складається із частин, які в якомусь змісті подібні до цілого» [11-19].

Головна особливість фракталів полягає у тому, що їх розмірність не укладається у звичні геометричні уявлення. Фракталам характерна геометрична «порізаність». Тому використовується спеціальне поняття фрактальної розмірності, введене Ф. Хаусдорфом та А. Безиковичем.

Розмірність фракталів не є цілим числом, характерним для звичних геометричних об'єктів.

Алгоритм побудови фрактальної множини Мандельброта (рис. 1.10) заснований на ітеративному обчисленні за формулою:

$$Z[i+1] = Z[i] \times Z[i] + C, \qquad (1.10)$$

де Z і C – комплексні змінні.

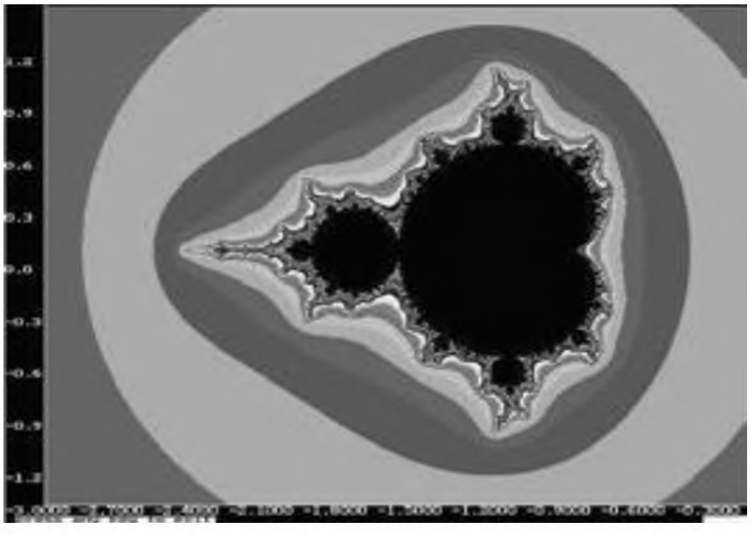


Рисунок 1.10 – Множина Мандельброта

Ітерації виконуються для кожної стартової точки C прямокутної або квадратної області – підмножині комплексної площини. Ітераційний процес триває доти, поки Z[i] не вийде за межі окружності заданого радіуса, центр якої лежить у точці (0,0), або після досить великої кількості ітерацій. Залежно від кількості ітерацій, протягом яких Z[i] залишається усередині окружності, встановлюються кольори точок.

Завдяки тому, що кількість ітерацій відповідає номеру кольору, то точки, що перебувають ближче до множини Мандельброта, мають більш яскраве забарвлення.

Побудова іншої фрактальної множини, сніжинки Коха, яка показана на рис. 1.11, починається із правильного трикутника, довжина сторони якого дорівнює 1.

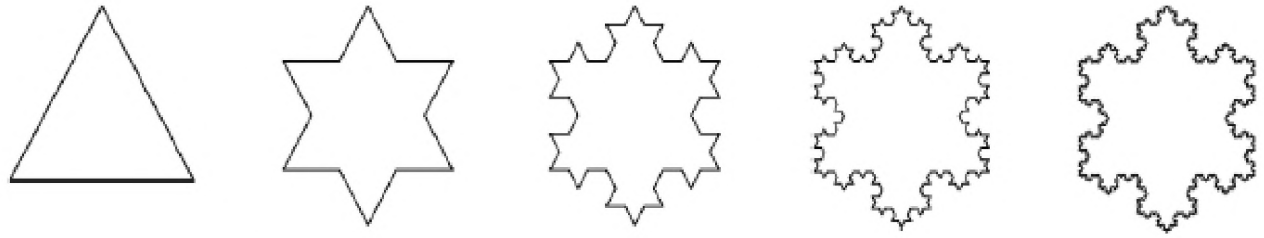


Рисунок 1.11 – Перші 5 поколінь сніжинки Коха

Сторона трикутника вважається базовою ланкою – вихідним положенням (рис. 1.11). Далі, на будь-якому кроці ітерації кожна ланка замінюється на утворюючий елемент – ламану, що складається по краях з відрізків довжиною 1/3 від довжини ланки, між якими розміщаються дві сторони правильного трикутника із стороною в 1/3 довжини ланки. Всі відрізки – сторони отриманої кривої вважаються базовими ланками для наступної ітерації. Крива, одержувана в результаті *n*-ї ітерації при будь-якому кінцевому *n*, називається предфракталом, і лише при *n*, що прямує до нескінченності, крива Коха стає фракталом. Одержана в результаті ітераційного процесу фрактальна множина являє собою лінію нескінченної довжини, що обмежує кінцеву площу. Дійсно, при кожному кроці число сторін результуючого багатокутника збільшується у 4

рази, а довжина кожної сторони зменшується тільки у 3 рази, тобто довжина багатокутника на *n*-й ітерації дорівнює $3*(4/3)^n$ і прямує до нескінченності з ростом *n*.

Площа під кривою, якщо прийняти площу утворюючого трикутника за 1, дорівнює:

$$S = 1 + 1/3 \sum_{k=0}^{\infty} (4/9)^k = 1,6. \quad (1.11)$$

У 80-х рр. XX ст. як простий метод одержання фрактальним структур з'явився метод «Систем Ітераційних Функцій» (Iterated Functions System – IFS). IFS являє собою систему функцій, що відображають одну багатомірну множина на іншу. Найбільш простою реалізацією IFS є афінні перетворення площини:

$$X' = A \times X + B \times Y + C; \quad (1.12)$$

$$Y' = D \times X + E \times Y + F. \quad (1.13)$$

У 80-х рр. американські вчені М. Барнслі та А. Слоан запропонували ідею стиску та зберігання графічної інформації, засновану на міркуваннях теорії фракталів і динамічних систем. На підставі цієї ідеї був створений алгоритм фрактального стиску інформації, що дозволяє стискати деякі зразки графічної інформації у 500-1000 разів. При цьому кожне зображення кодується декількома простими афінними перетвореннями.

За алгоритмом Барнслі відбувається виділення в зображенні пар областей, менша з яких подібна більшій, і збереження декількох коефіцієнтів, які кодують перетворення, що переводить більшу область у меншу. Потрібно, щоб множина таких областей покривало все зображення.

Як приклад використання IFS для побудови фрактальних структур, можна навести криву «дракона» Хартера-Хейтуея, яка представлена на рис. 1.12. IFS застосовується для стиску зображень, наприклад, фотографій, що засновано на виявленні локальної самоподібності (на відміну від фракталів, де спостерігається глобальна самоподібність).

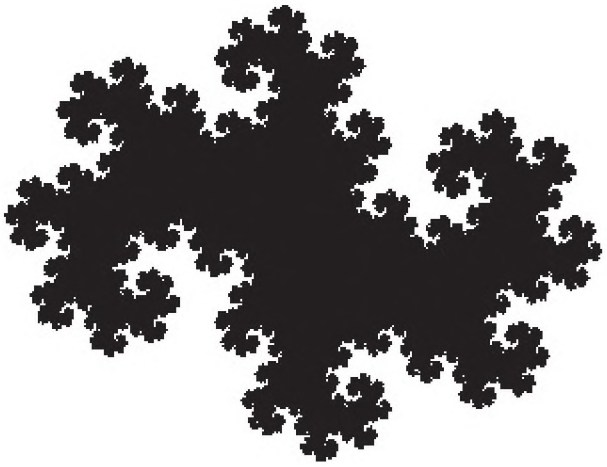


Рисунок 1.12 – «Дракон» Хартера-Хейтуея

Один із кращих прикладів прояву фракталів у природі – структура берегових ліній. Дійсно, інколи на кілометровому відрізку узбережжя виглядає настільки ж порізаним, як і на стокілометровому.

Досвід показує, що довжина берегової лінії L залежить від масштабу *l*, яким проводяться виміри, і збільшується із зменшенням останнього за степеневим законом $L = \Lambda l^{1-\alpha}, \Lambda = const.$ Так, наприклад, для узбережжя Великобританії α≈1.24, тобто фрактальна розмірність берегової лінії Великобританії дорівнює 1.24.

1.2.2 Інформаційний простір і фрактали

На цей час інформаційний простір прийнято розглядати як стохастичний [11]. У багатьох моделях інформаційного простору вивчаються структурні зв'язки між тематичними множинами, що входять у цей простір. Самоподібність інформаційного простору виражається, насамперед у тому, що при його лавиноподібному зростанні, частотні та рангові розподіли, одержувані в таких розрізах, як джерела, автори, тематика практично не міняють своєї форми. Застосування теорії фракталів при аналізі інформаційного простору дозволяє із загальної позиції глянути на закономірності, що становлять основи інформатики.

Наприклад, тематичні інформаційні масиви сьогодні представляють самоподібні структури, що розвиваються і за своєю суттю є стохастичними фракталами, тому що їхня самоподібність справедлива лише на рівні математичних очікувань, як наприклад, розподілу кластерів за розмірами.

В інформаційному просторі виникають, формуються, ростуть і розмножуються кластери – групи взаємозалежних документів. Системи, засновані на кластерному аналізі, самостійно виявляють нові ознаки об'єктів і розподіляють об'єкти за новими групами.

Фрактальні властивості характерні для кластерів інформаційних веб-сайтів, на яких публікуються документи, що відповідають певним тематикам. Ці кластери, як набори тематичних документів, являють собою фрактальні структури, що мають низку унікальних властивостей.

Топологія та характеристики моделей веб-простору виявляються приблизно однаковими для різних підмножин, підтверджуючи тим самим спостереження про те, що «веб – це фрактал», тобто властивості структури всього веб-простору Bow Tie вірні і для його окремих підмножин.

З іншого боку, теорія фракталів розглядається як підхід до статистичного дослідження, що дозволяє одержувати важливі характеристики інформаційних потоків, не вдаючись у детальний аналіз їхньої внутрішньої структури та зв'язків. Для послідовності повідомлень тематичних інформаційних потоків у відповідності зі скейлінговим принципом, кількість повідомлень, резонансів на події реального миру, пропорційна деякому ступеню кількості джерел інформації (кластерів).

Відомо, що всі основні закони наукової комунікації, такі як закони Парето, Лотки, Бредфорда, Ципфа, можуть бути узагальнені саме в рамках теорії стохастичних фракталів. Точно так само, як й у традиційних наукових комунікаціях, множина повідомлень в Інтернеті за однією тематикою в часі являє собою динамічну кластерну систему, що виникає в результаті ітераційних процесів. Цей процес обумовлюється републікаціями, однобічним або взаємним

цитуванням, різними публікаціями – відбиттями тих самих подій реального миру, прямими посиланнями тощо.

Фрактальна розмірність у кластерній системі, що відповідає тематичним інформаційним потокам, показує ступінь заповнення інформаційного простору повідомлень протягом певного часу:

$$N_{publ}(\varepsilon t) = \varepsilon^{\rho} N_k(t)^{\rho} \tag{1.14}$$

де N_{publ} – розмір кластерної системи (загальне число документів в інформаційному потоці); N_{k} – розмір – число кластерів (тематик або джерел); ρ – фрактальна розмірність інформаційного масиву; ε – коефіцієнт масштабування. У наведеному співвідношенні між кількістю документів і кластерів проявляється властивість збереження внутрішньої структури множини при зміні масштабів його зовнішнього розгляду.

1.2.3 Фрактальні шуми

1.2.3.1. Самоподібні степеневі закони.

Розглянемо однорідну степеневу функцію [19]:

$$f(x) = cx^{\beta}, \tag{1.15}$$

де c і β – постійні. При β=1 функція $f(x) = cx$ при c<0 описує відновлюючу силу лінійної пружини, а при β=-2 рівняння (1.15) стає законом всесвітнього тяжіння Ньютона $f(x) = cx^{-2}$. Ці прості степеневі закони, які в безлічі зустрічаються в природі, є, насправді самоподібними: якщо піддати x перетворенню подібності (помноживши його на деяку константу), то функція $f(x)$ як і раніше буде пропорційна x^{β}, хоча й з іншим коефіцієнтом пропорційності.

Таким чином, однорідні функції володіють цікавою властивістю масштабної інваріантності: при зміні масштабу вони відтворюють самі себе. Така інваріантність може пролити світло на деякі темні куточки фізики, біології та інших наук.

Масштабна інваріантність обумовлена тим, що однорідні степеневі закони не мають природних масштабів; в них немає місця характерній одиничній мірі (такій, як одинична довжина, одиниця часу або одинична маса). Тому такі закони називають масштабно-незалежними.

1.2.3.2. Фрактальний метод нормованого розмаху Херста (R/S-аналіз).

Стандартна гаусова статистика добре працює при деяких обмежуючих припущеннях [19]. Центральна гранична теорема (закон великих чисел) стверджує, що по мірі проведення дедалі більшої кількості випробувань граничний розподіл випадкової системи буде мати нормальний розподілом. Досліджувані події повинні бути незалежними та ідентично розподілені. Але що робити, якщо для системи не виконуються ці умови? На щастя, існує непараметрична методологія, відкрита ще у 1951 р. Х.Е. Херстом, знаменитим британським гідрологом. Він розробив метод нормованого розмаху (*R*/*S*-аналіз), який використовується для розрізнення випадкового часового ряду і фрактального ряду. Нижче опишемо цю методику на прикладі резервуара річки Ніл.

Протягом кожного проміжку часу t такий резервуар приймає приплив $\xi(t)$ з озера, в той час, як регульований обсяг води (стік) спускається з водосховища. Необхідно знайти потрібну кількість води в резервуарі, щоб щорічно можна було спускати з нього кількість води, якадорівнює середньому припливу за цей період.

Середній приплив за період вτ років дорівнює

$$\langle \xi \rangle_r = \frac{1}{\tau} \sum_{t=1}^{\tau} \xi(t). \tag{1.16}$$

Тоді $X(t)$ – накопичене відхилення припливу $\xi(t)$ від його середнього значення є сумою

$$X(t,\tau) = \sum_{u=1}^{t} (\xi(u) - \langle \xi \rangle_r). \tag{1.17}$$

Розмах відхилень буде визначатися як

$$R(\tau) = \max_{1 \le \tau \le \tau} X(t,\tau) - \min_{1 \le t \le \tau} X(t,\tau). \quad (1.18)$$

Стандартне відхилення можна отримати за формулою квадратного кореня з дисперсії

$$S(\tau) = \sqrt{\frac{1}{\tau}\sum(\xi(t) - \langle\xi\rangle_r)^2}. \quad (1.19)$$

Як виявив Херст, для багатьох часових рядів, що спостерігаються,нормований розмах R/S дуже добре описується емпіричним співвідношенням у вигляді степеневого закону:

$$R / S = (a\tau)^H, \quad (1.20)$$

де H – показник Херста. Тут слід зазначити, що розмах іменується нормованим, оскільки він за задумом Херста повинен ділитися на квадратний корінь з дисперсії. Це дозволяє застосовувати метод до самих різних систем. Показник Херста є стійкою мірою деяких статистичних явищ, для яких дисперсія такою не є.

1.2.3.3. Класифікація фрактальних шумів.

В основі класифікації шуму лежить однорідний степеневий закон [19]. Класифікацію проводять в залежності від значення показника ступеня β:

- β=0 – білий шум;
- β=1 – рожевий шум;
- β=2– коричневий шум;
- β=3 – чорний шум.

У білому шумі будь-яке його значення в момент часу t абсолютно не залежить від свого минулого – воно завжди несподівано (рис. 1.13,а). Навпаки, в «коричневій» музиці (броунівський рух – це теж «коричневий» шум) тільки інкременти не залежать від свого минулого, в результаті чого шум виходить стомливо одноманітним.

На рис. 1.13,*б* представлений зразок шуму з гіперболічним степеневим спектром f^{-1}. Такі функції відомі також під назвою рожевого шуму, тому що вони займають проміжне положення між коричневим (броунівським) (f^{-2}) і білим шумом ($1/f^{0}$). Оскільки спектр потужності будь-якого шуму, який підкорюється однорідному степеневому закону (f^{β}), самоподібний, відповідна часова діаграма також повинна бути самоподібна. Дійсно, якщо масштаб уздовж вісі частот змінити в *r* раз, то за законом взаємності Фур'є масштаб уздовж вісі часу відповідної часової діаграми зміниться в 1/*r* раз. Зрозуміло що, в разі шуму (і інших ймовірнісних явищ) самоподоба носить лише статистичний характер: збільшений фрагмент не є точною детермінованою копією форми сигналу до зміни масштабу.

Рисунок 1.13 – Часові діаграми шумів: *а* – білий шум з $1/f^{0}$-спектром потужності; *б* – «рожевий» шум з $1/f^{1}$-спектром; *в* – «коричневий» шум з $1/f^{2}$-спектром; *г* – чорний шум з $1/f^{3}$-спектром

Рожевий, білий і коричневий шум є ідеальними зразками статистично самоподібних процесів. Явища, спектри потужності яких представляють собою однорідні степеневі функції, не мають власних масштабів часу і частоти: вони масштабно-незалежні. Тут немає таких понять як характеристичний час або характеристична частота: те, що відбувається в одному часовому або частотному інтервалі, відбувається при *будь-якому* масштабуванні часу або частоти. Якщо такі шуми записати на магнітну стрічку і програти на різних швидкостях, то звучати вони будуть однаково.

Степеневі закони аж ніяк не обмежені цілочисельними показниками, як у випадку білого, рожевого і коричневого шумів. У природі в достатку зустрічаються прості степеневі закони з дробовими показниками, що описують найрізноманітніші явища: розливи річок, розподіл галактик у Всесвіті тощо. З цих законів виділимо головне: часто складні функції двох і більше змінних поводяться поблизу «критичних точок» як прості степеневі закони. Наприклад, функцію двох змінних $f(x, y)$ дуже часто можна представити в наступному загальному вигляді:

$$f(x,y) = x^{\alpha} g\left(y / x^{\beta}\right), \tag{1.21}$$

де функція $f(x,y)$ замінена функцією тільки однієї змінної g. Для будь-якого інтервалу змінних, на якому функція g постійна, функція $f(x,y)$ наближено може бути представлена простим степеневим законом від x.

Подібне представлення через степеневі закони і їх показники – виявляється надзвичайно плідним при аналізі різних критичних явищ.

Виявляється, і рожевий, і чорний шуми поширені досить широко. Рожеві процеси виникають у багатьох фізичних ситуаціях і знаходять дивовижні естетичні застосування в музиці та інших видах мистецтва.

Чорні спектри описують розвиток в часі багатьох природних і протиприродних катастроф, таких як розливи річок, засухи, ринки з тенденцією до зниження курсів і різні аварійні ситуації – наприклад, перебої в подачі електроенергії. Через свої чорні спектри подібні неприємності нерідко трапляються по кілька разів поспіль.

1.2.4 Принцип фрактального стиснення зображень

Фрактальні алгоритми забезпечують вдале співвідношення між коефіцієнтом стиснення та якістю і володіють унікальною властивістю деталізації при довільному масштабуванні [5, 6, 23]. Розвиток фрактального

стиснення забезпечує популярність форматів на його основі, що підтверджує доцільність їх стеганографічного використання.

Фрактальна архівація ґрунтується на поданні зображення в компактній формі за допомогою коефіцієнтів системи IFS. Як вже зазначалось, IFS – набір тривимірних афінних перетворень, які переводять одне зображення в інше. Перетворенню піддаються точки в тривимірному просторі (двомірний простір площинного зображення і яскравість).

Нехай парою (M, d) задається метричний простір цифрових зображень, де d – дана метрична міра. Для стиснення зображення IєM необхідно знайти відображення τ: M → M, яке задовольняє наступні умови:

$$\exists\, 0 < z < 1, \quad \forall \mu, \nu \in M, d(\tau(\mu), \tau(\nu)) \le z.d(\mu, \nu), \tag{1.22}$$

$$d(I, \tau(I)) \cong 0, \tag{1.23}$$

де μ і v є різними фрагментами зображення I.

Тоді за умови рівномірного розбиття

$$\forall \mu_i \in I, i = \overline{1,n}, \quad I = \bigcup_i \mu_i, \quad \mu_i \cap \mu_j = 0, i \ne j \tag{1.24}$$

і існування сукупності відображень T={τ_i} таких, що $d(\mu_i, \tau_i(\nu_i)) \le \varepsilon$, справедливий вираз

$$d(I, F^m(T)) \le \frac{\varepsilon}{1-z}, m \to \infty, \tag{1.25}$$

де $F^l(T) = \bigcup_i (\mu_i^l \leftarrow \tau_i(\nu_i^{l-1}))$.

Відображення τ_i є афінним перетворенням і

$$\tau_i = N_i \circ S_i \circ G_i, \tag{1.26}$$

де G – оператор геометричної частини, яка забезпечує стиснення з коефіцієнтом z, повороти на певні кути і симетричні відображення фрагментів зображення; S – оператор переносу, який реалізує зсув кожної елементарної частини фрагмента зображення в двомірному просторі; N – оператор інтенсивності фрагмента зображення, яке змінює значення інтенсивності e – елементарної

частини (пікселя) таким чином: $N_i(e) = s_i \cdot e + o_i$, де s – контрастність, o – яскравість [5, 6].

На практиці кількість ітерацій m обмежується невеликим числом, яке є достатнім для забезпечення візуальної подібності при задовільному ε. Метричний простір (M, d) визначається способом розбиття на рангові та доменні блоки μ і ν відповідно. У більшості випадків зображення I має прямокутну форму, рангові та доменні блоки є квадратами з розмірами k×k і 2k×2k пікселів, z=0,5 і

$$d(\mu_l, \mu_m) = \sqrt{\sum_{i=1}^{k}\sum_{j=1}^{k}(e_{i,j}^{\mu_l} - e_{i,j}^{\mu_m})^2}\ . \qquad (1.27)$$

Таким чином, метою фрактального алгоритму стиснення зображень є пошук сукупності перетворень T для деякого зображення I при достатньо малому ε. Важливим обмеженням цього процесу є умова *inf*(T)<<*inf*(I), де функція *inf* визначає кількість інформації, необхідної для опису аргументу. Однак на практиці інтерпретація (I, ε) в T не є однозначною. Можливість маніпулювання T дозволяє застосувати стеганографічну техніку, яка використовує різноманіття взаємозамінних фрагментів реальних зображень.

Особливості розбивки зображення на доменні і рангові блоки можуть суттєво впливати на вказане різноманіття варіантів зіставлень.

Ще одним важливим моментом практичної реалізації моделі фрактального стиснення є спосіб організації пошуку відповідностей між ранговими і доменними блоками.

Деякі модифікації методів фрактального стиснення відрізняються від описаного базового підходу значенням коефіцієнта масштабування z, набором афінних перетворень і оператором N [24-29]. Однак навіть опосередкований вплив таких змін на особливості вбудовування даних є незначним, оскільки стосується лише відображення блоків і не пов'язане з порядком їх вибору і кількістю.

1.3 Існуючі підходи до вбудовування інформації у фрактально стиснені зображення

Відомий підхід до передачі додаткової інформації при фрактальному кодуванні зображення [30], в якому вбудовування здійснюється в індекси орієнтації доменних блоків.

У відомому підході [30] на першому етапі афінних перетворень з урахуванням вбудованої додаткової інформації записується бінарна послідовність з трьох цифр (тому що можливе число поворотів дорівнює восьми). Далі з урахуванням даної комбінації цифр здійснюється поворот оброблюваного домену та пошук коефіцієнтів яскравості і контрастності. В результаті такого введення число поворотів знижується, що призводить до зменшення як часу пошуку відповідного домену, так і загального часу кодування в цілому. Після вбудовування додаткової інформації в якості індексів поворотів, ці дані разом з інформацією про індекси доменних блоків, яскравості і контрастності передаються по каналу зв'язку. У декодері відбувається виділення додаткової інформації та відновлення початкового зображення. Декодування зображення здійснюється шляхом ітеративного застосування афінних перетворень до довільного початкового зображення. Відповідно до теореми про стискаючі відображення ітерації будуть сходитись незалежно від вибору початкового зображення. Стискаюче відображення визначається як окреме перетворення для кожного рангового блоку. Кожен ранговий блок має пов'язані з ним перетворення і домен. Вміст цього рангового блоку обчислюється застосуванням перетворення до доменного блоку. Одна ітерація завершується, коли була здійснена обробка всіх рангових блоків. Вставка додаткової інформації в базовий алгоритм фрактального кодування згідно відомого підходу [30] здійснюється згідно алгоритму, зображеному на рис. 1.14.

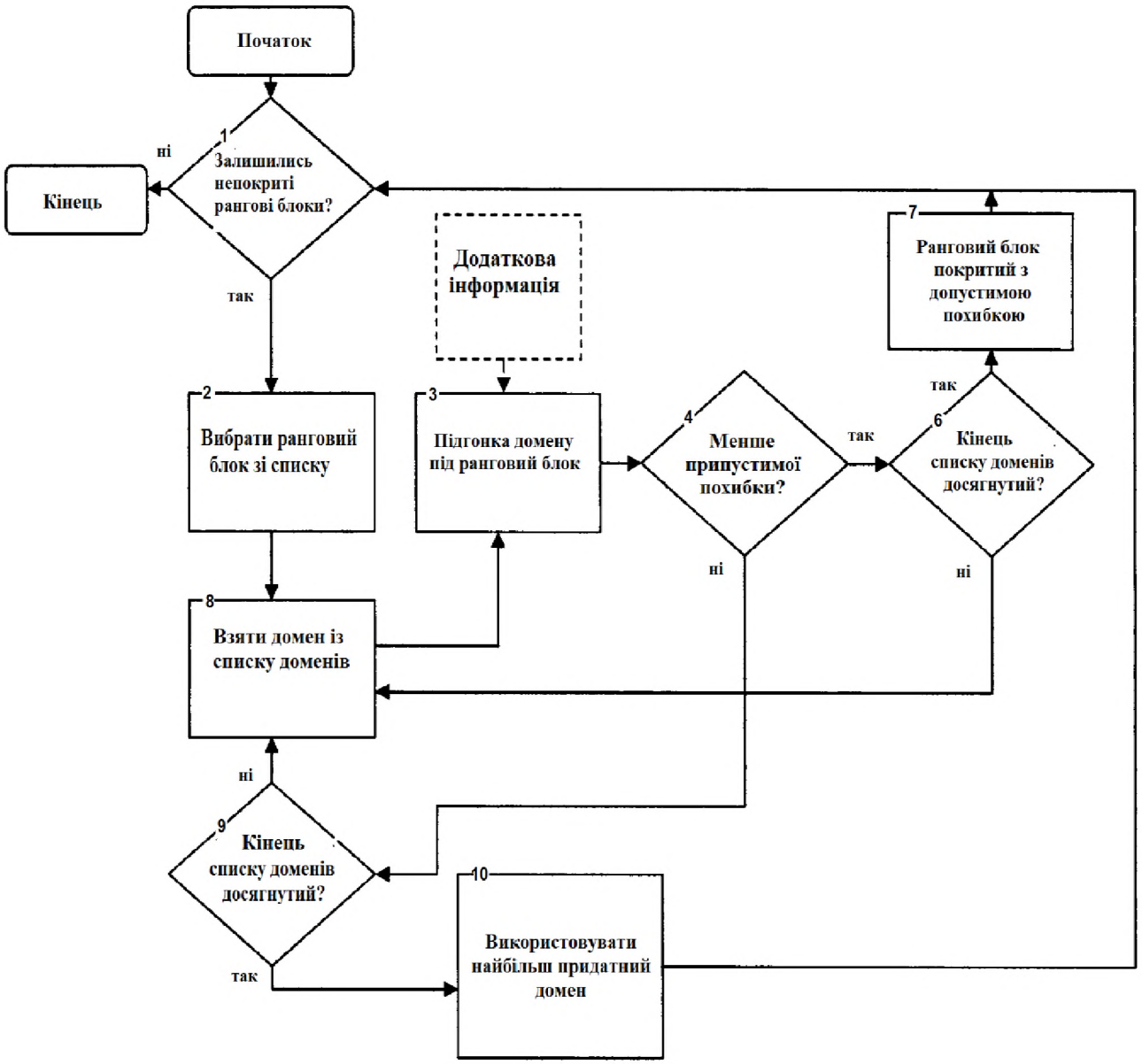


Рисунок 1.14 – Алгоритм вставки додаткової інформації в базовий алгоритм фрактального кодування згідно відомого підходу [30]

Недоліком відомого підходу [30] є сильне спотворення початкового зображення, в результаті переорієнтації доменів при встановленні в них додаткової інформації.

Також відомий підхід до передачі додаткової інформації при фрактальному кодуванні зображення [31], в якому вбудовування проводиться в молодші розряди індексів доменів.

Цей підхід [31] дозволяє при кодуванні зображень передавати додаткову інформацію. Це досягається тим, що при фрактальному методі стиснення в

молодші розряди індексів домену вводять додаткову інформацію, завдяки чому скорочується список використовуваних доменів, що призводить до суттєвого зменшення загального часу кодування. Вставка додаткової інформації в базовий алгоритм фрактального кодування згідно відомого підходу [31] здійснюється згідно алгоритму, зображеному на рис. 1.15.

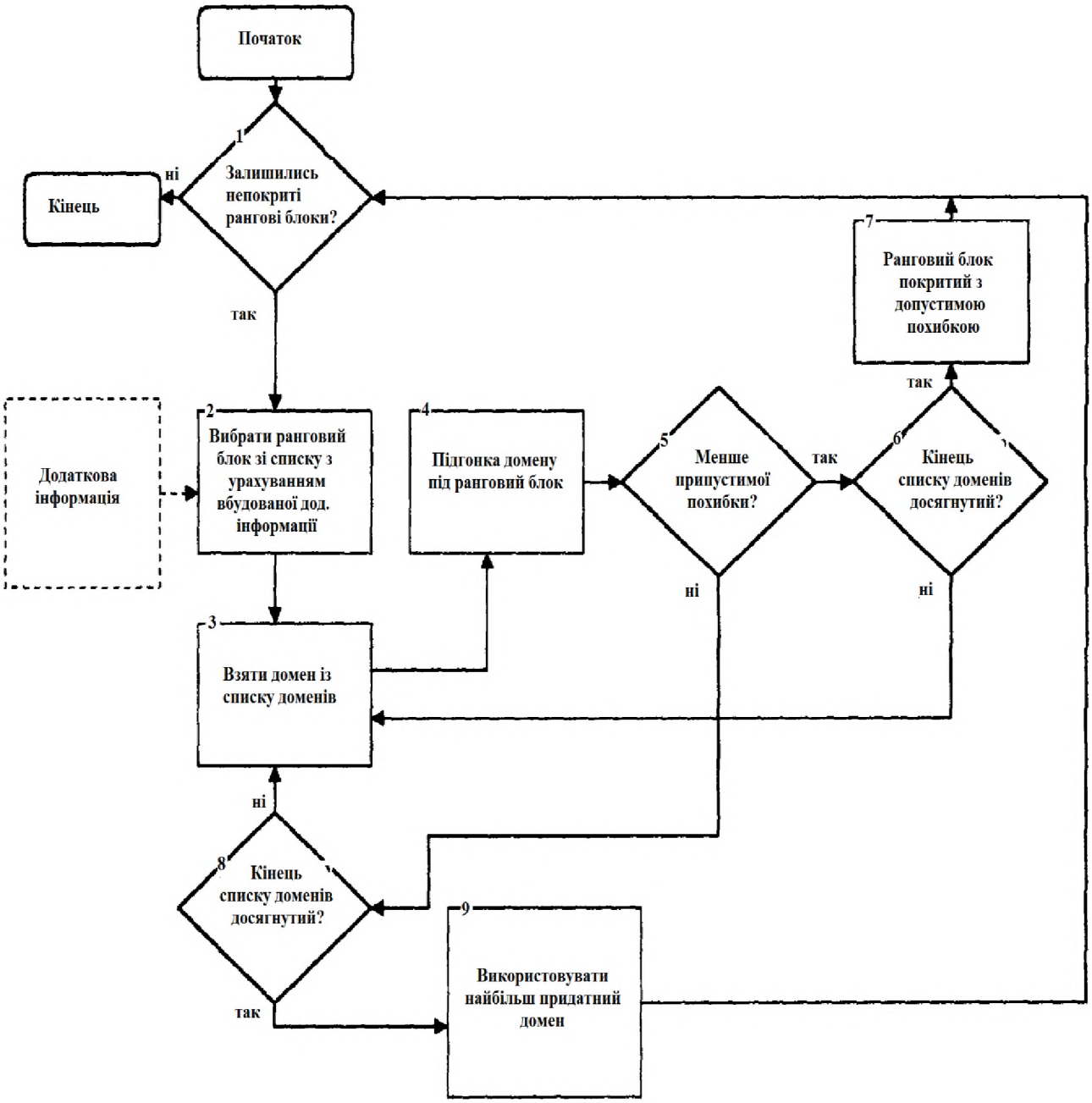


Рисунок 1.15 – Алгоритм вставки додаткової інформації в базовий алгоритм фрактального кодування згідно відомого підходу [31]

А до розрядів, що залишилися, застосовують процедуру пробної інверсії, в якій використовують відомий метод Гауса-Зейделя для розв'язання оптимізаційних задач з великим числом невідомих, що здійснюється згідно алгоритму пошуку оптимальних елементів індексів домену при введенні додаткової інформації для передачі по каналу зв'язку.

Недоліком відомого підходу [31] є те, що в результаті такої вставки зменшується простір можливих доменів для відображення ранговому блоку, що знижує якість відновленого зображення.

Найбільш близьким за технічною сутністю і виконуваних функцій є підхід до передачі додаткової інформації при спільному використанні векторного квантування і фрактального кодування зображень з урахуванням класифікації доменів і блоків з кодової книги [32], який було обрано як прототип. В цьому підході в вектор індексу доменів або блоку з кодової книги, що складається з n розрядів, вводиться m розрядів додаткової інформації, замість молодших розрядів даного вектора. Підхід-прототип дозволяє при кодуванні будь-якого типу зображень передавати додаткову корисну інформацію при збереженні швидкості передачі і довжині формату кадру. Це досягається тим, що при стисненні початкового зображення за допомогою спільного використання векторного квантування і фрактального кодування з урахуванням класифікації доменів і блоків з кодової книги в молодші розряди індексів домену або блоків з кодової книги вводять додаткову інформацію, завдяки чому скорочується список використовуваних доменів і блоків з кодової книги, що призводить до суттєвого зменшення загального часу кодування при незначному погіршенні якості відновленого зображення. До залишившихся розрядів застосовують процедуру пробної інверсії.

На рис.1.16 представлена процедура передачі додаткової інформації при спільному використанні векторного квантування і фрактального кодування зображення згідно відомого підходу-прототипу [32]. Попередньо в кодері і декодері формують ідентичні кодові книги з урахуванням розбивання їх на класи. Після цього в молодші розряди індексів домену або блоків з кодової

книги вбудовують додаткову інформацію. Далі здійснюється фрактальне кодування рангових блоків з урахуванням вбудованої додаткової інформації, а також пошук найбільш підходящого блоку зі сформованої раніше кодової книги. Якщо ранговий блок краще відображається доменним блоком, то декодеру передається індекс відповідного домену, при прийомі якого в декодері здійснюється фрактальне декодування початкового блоку. При виборі для рангового блоку фрагмента з кодової книги декодеру передається індекс, за яким з кодової книги в декодері вибирається необхідний фрагмент, яким після фрактального декодування заповнюється відтворене зображення.

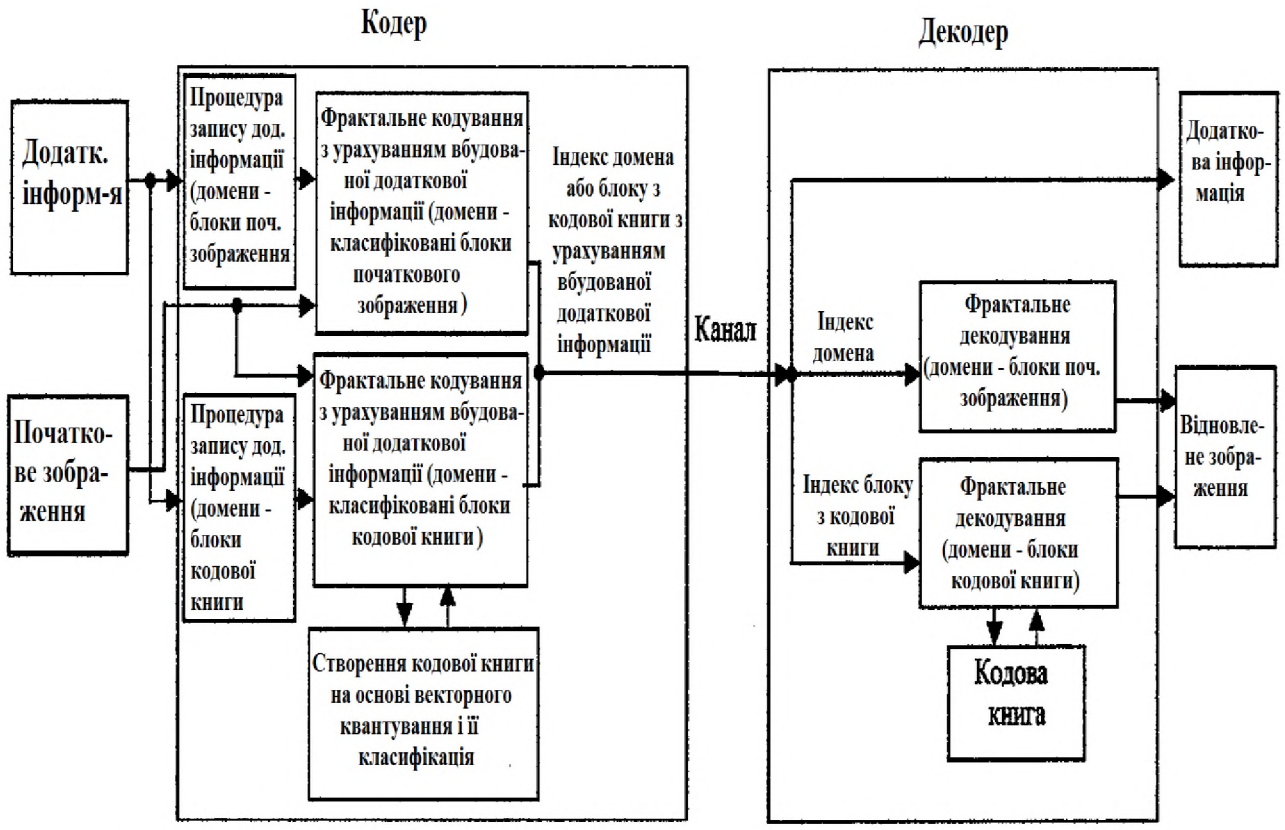


Рисунок 1.16 – Процедура передачі додаткової інформації при спільному використанні векторного квантування і фрактального кодування зображення згідно відомого підходу-прототипу [32]

Недоліком відомого підходу-прототипу [32] є зміщення доменів щодо початкового положення, що призводить до накладання сегментів початкового зображення один на одний, що є візуально помітним.

1.4 Висновок. Постановка задачі

В розділі проаналізовано принципи приховування даних в цифрових зображеннях, а також фрактального аналізу. Встановлено, що фрактальні алгоритми забезпечують вдале співвідношення між коефіцієнтом стиснення та якістю і володіють унікальною властивістю деталізації при довільному масштабуванні. Розвиток фрактального стиснення забезпечує популярність форматів на його основі, що підтверджує доцільність їх стеганографічного використання.

В розділі проаналізовано існуючі підходи до вбудовування інформації у фрактально стиснені зображення. Встановлено, що недоліком відомого підходу до передачі додаткової інформації при фрактальному кодуванні зображення, в якому вбудовування здійснюється в індекси орієнтації доменних блоків [30] є сильне спотворення початкового зображення, в результаті переорієнтації доменів при встановленні в них додаткової інформації.

Встановлено, що недоліком відомого підходу до передачі додаткової інформації при фрактальному кодуванні зображення, в якому вбудовування проводиться в молодші розряди індексів доменів [31] є те, що в результаті такої вставки зменшується простір можливих доменів для відображення ранговому блоку, що знижує якість відновленого зображення.

Встановлено, що недоліком відомого підходу до передачі додаткової інформації при спільному використанні векторного квантування і фрактального кодування зображень з урахуванням класифікації доменів і блоків з кодової книги (прототипу) [32] є зміщення доменів щодо початкового положення, що призводить до накладання сегментів початкового зображення один на одний, що є візуально помітним.

Таким чином, для усунення недоліків існуючих підходів необхідно:

• запропонувати підхід до стеганографічного вбудовування інформації в зображення, стиснене фрактальним методом, з урахуванням потужності пікселів домену;

• оцінити ефективність запропонованого підходу.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Підхід до стеганографічного вбудовування інформації в зображення, стиснене фрактальним методом, з урахуванням потужності пікселів домену

Запропонований підхід відноситься до області стеганографії, а саме до способів вбудовування повідомлення в цифрове зображення, і може бути використаний для організації прихованого зберігання і передачі конфіденційної інформації по відкритих каналах зв'язку.

Технічним результатом є забезпечення можливості прихованої передачі конфіденційних даних, використовуючи контейнер, представлений у вигляді фрактально стисненого зображення. Запропонований підхід включає етапи формування вектора параметрів стиснення зображення, введення інформації, що приховується, виділення доменів і рангових областей, співвіднесення рангових областей і доменів, формування кінцевого архіву. У запропонованому підході на етапі виділення доменів і рангових областей потужність пікселів домену коригується з урахуванням значення приховуваних біт інформації.

Завданням запропонованого підходу є створення способу вбудовування інформації в зображення, стисле фрактальним методом, з урахуванням потужності пікселів домену, що забезпечує можливість прихованої передачі конфіденційних даних, використовуючи контейнер, представлений у вигляді фрактально стисненого зображення.

Це завдання вирішується тим, що в підході до вбудовування інформації в зображення, стисле фрактальним методом, з урахуванням потужності пікселів домену, що включає етапи формування вектора параметрів стиснення зображення, введення інформації, що приховується, виділення доменів і рангових областей, співвіднесення рангових областей і доменів, формування кінцевого архіву, введений етап приховування інформації, за рахунок корекції потужності пікселів домену.

Промислова придатність запропонованого підходу обумовлена тим, що пристрій, що реалізує запропонований підхід, може бути здійснено за допомогою сучасної елементної бази, з досягненням зазначеного у підході призначення.

Реалізація запропонованого підходу полягає у включенні в процес фрактального стиснення етапу вбудовування інформації. Загальний алгоритм фрактального стиснення спочатку має на увазі введення параметрів стиснення [6]. Як параметри стиснення використовуються мінімальний розмір домену, мінімальний крок домену, значення порога середньоквадратичного відхилення (СКВ), глибина квадродерева.

Після введення параметрів стиснення в систему завантажується початкове зображення, призначене для стиснення. Першим етапом реалізується розбиття зображення на домени [6].

Для кожного рангового блоку потрібно знайти доменний блок, який ефективно відображається в цей ранговий блок. Для того щоб відображення було стискаючим, домен повинен бути більше рангового блоку. Гарне стиснення залежить від можливості знайти хорошу відповідність між доменними і ранговими блоками без необхідності додаткового розбиття рангових блоків. Занадто дробове розбиття рангових областей призводить до занадто великої їх кількості, а це погіршує коефіцієнт стиснення (що фактично призводить до збільшення зображення, а не до його стиснення, якщо не бути досить обережним). В ідеалі потрібно мати континуум розмірів і варіантів розташування доменних блоків і вибирати з нього відповідні для кожного рангового блоку. На жаль, обчислювальні витрати пошуку серед стількох варіантів занадто великі. Завдання визначення системи доменів - це компроміс між необхідністю, щоб множина доменів була досить великою для забезпечення можливості підбору найкращого варіанту відповідності рангових блоку і, в той же час, досить маленькою, щоб процес пошуку міг бути здійснений за прийнятний час.

Мінімальний розмір домену вказано в початкових параметрах. Також виділяються домени більшого розміру, причому для більш ефективного розрахунку, кожні наступні групи доменів більші за попередні у два рази. Максимально можливий розмір домена вибирається відповідно до розмірів початкового зображення. Після виділення доменів, здійснюється їх класифікація за алгоритмом Фішера, який є одним з найефективніших [6, 33].

Класифікацію доменних і рангових областей можна використовувати для зменшення обсягу обчислень, пов'язаних з доменно-ранговими зіставленнями. Тоді доменно-рангові зіставлення виконуються тільки для тих доменів, які належать класу подібності даної рангової області. Різновидом схеми класифікації є, наприклад, метод виділення особливостей [6]. Обчислення характеристик служить для визначення тих доменів, які належать класу підзображень, чиї вектора характеристик не виходять за межі допуску для вектора характеристик даного рангового блоку. Більш складні схеми класифікації використовують заздалегідь визначену множину класів. Алгоритм класифікації пов'язує кожен домен з одним з цих класів. При кодуванні алгоритм пов'язує цей ранговий блок з певним класом, і після цього доменно-рангове зіставлення проводиться тільки з доменами, віднесеними до цього класу (й, можливо, з іншими подібними класами). Заощадження часу при кодуванні відбувається за рахунок виконання меншого числа доменно-рангових зіставлень.

Класифікація згідно запропонованого підходу дозволяє виділити 72 класи. Під значеннями A мається на увазі математичне очікування інтенсивностей пікселів відповідних областей:

1 клас $A_1 \geq A_2 \geq A_3 \geq A_4$

2 клас $A_1 \geq A_2 \geq A_4 \geq A_3$

3 клас $A_1 \geq A_4 \geq A_2 \geq A_3$

Також в кожному з трьох класів виділяється ще по 24 класи, відповідно до значень дисперсії.

На наступному етапі відбувається виділення рангових областей, при цьому вони повинні повністю заповнювати всі зображення і не перетинатися одна з одною. Рангові області відповідно до алгоритму менше доменів по ширині в два рази.

Після формування бібліотеки доменів і визначення рангів, здійснюється основний етап співвіднесення рангових областей і доменів [6].

Співвіднесення доменної і рангової області – це головний обчислювальний крок у фрактальному кодуванні. Для кожного рангового блоку алгоритм порівнює варіанти перетворення всіх доменів (або хоча б усіх доменів заданого класу) до цього рангових блоку. Схема співвіднесення доменного і рангового блоків представлена на рис. 2.1. По-перше, до вибраного домену застосовується один з восьми (або менше) базових поворотів / відображень. По-друге, що обертається доменна область стискається, щоб відповідати розміру рангової області. Зауважимо, що на практиці рангова область повинна бути менше доменної, для того щоб сумарне відображення було стискає. І, нарешті, методом найменших квадратів обчислюються оптимальні параметри яскравості і контрастності.

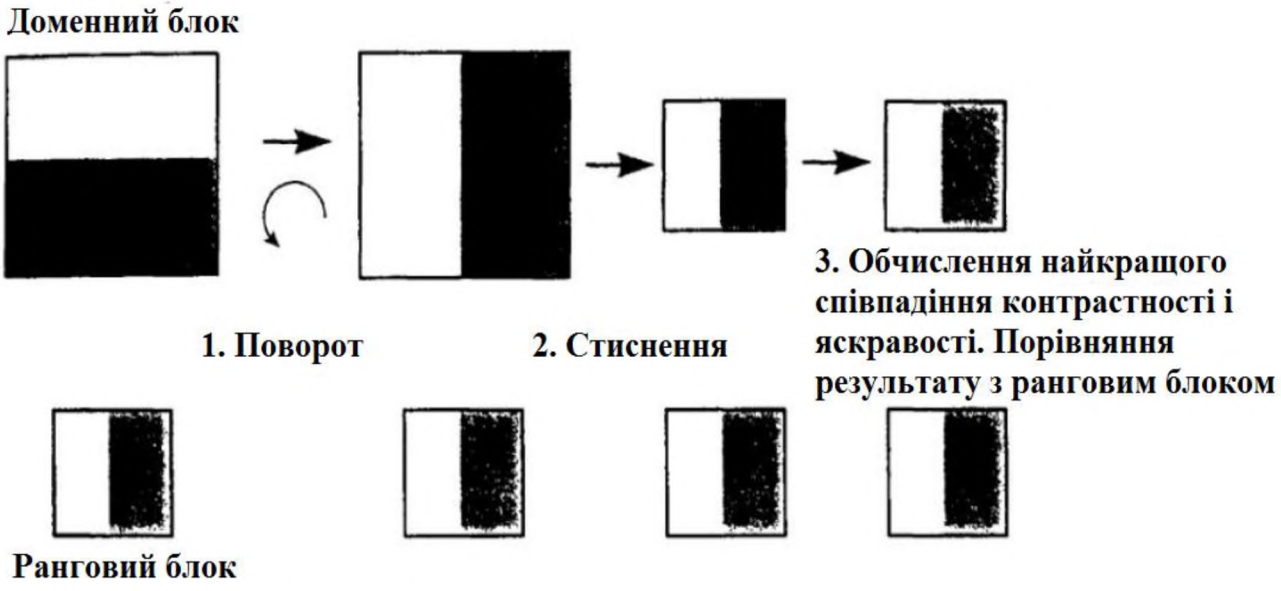


Рисунок 2.1 – Схема співвіднесення доменного і рангового блоків

Етап співвіднесення рангових областей і доменів відбувається шляхом підбору відповідних розглянутому рангу доменів. За рахунок попередньої класифікації даний етап скорочується в 72 рази, оскільки ранги також відбираються за алгоритмом класифікації Фішера [33].

Схожість доменів і рангів визначається за методом найменших квадратів (МНК) [19]. МНК є одним з методів регресійного аналізу і призначений для оцінки невідомих величин за результатами вимірів, що містять випадкові похибки. Він застосовується також для наближеного представлення заданої функції іншими (простішими) функціями і часто виявляється корисним при обробці спостережень.

Досліджуваний домен піддається афінним перетворенням для забезпечення максимальної схожості з рангом, після чого за значенням, отриманим за МНК, приймається рішення про продовження пошуку відповідності. Афінні перетворення мають на увазі під собою такі операції над сегментами зображення, як дзеркальне відображення, поворот на кути в 90, 180, 270 градусів [6]. Також можливе застосування масштабування. В параметрах стиснення заздалегідь вказується мінімальний поріг СКВ, одержуваний при розрахунку значення по МНК, чим він нижчий, тим якісніше буде стисле зображення, але збільшується час компресії, і навпаки. У разі, якщо для рангової області не буде знайдений відповідний домен, реалізується метод квадродерева [6], при якому рангова область розбивається на чотири рівні частини і з ними проводяться аналогічні дії.

Розбиття методом квадродерева (рис. 2.2) починається з грубого розбиття (зліва). Якщо для якогось рангового блоку виявляється неможливі підібрати підходящий домен і перетворення, то цей блок розбивається на чотири менших блоки (в центрі). Процес розбиття триває, поки або не знаходиться підходящий домен, або не досягається максимальна глибина квадродерева.

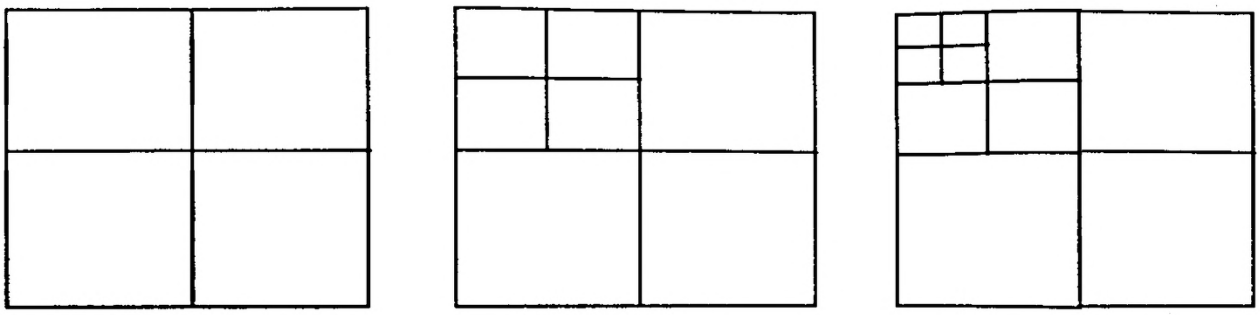


Рисунок 2.2 – Розбиття методом квадродерева

На рис. 2.3 показаний ефект використання меншої допустимої похибки і більшої глибини квадродерева.

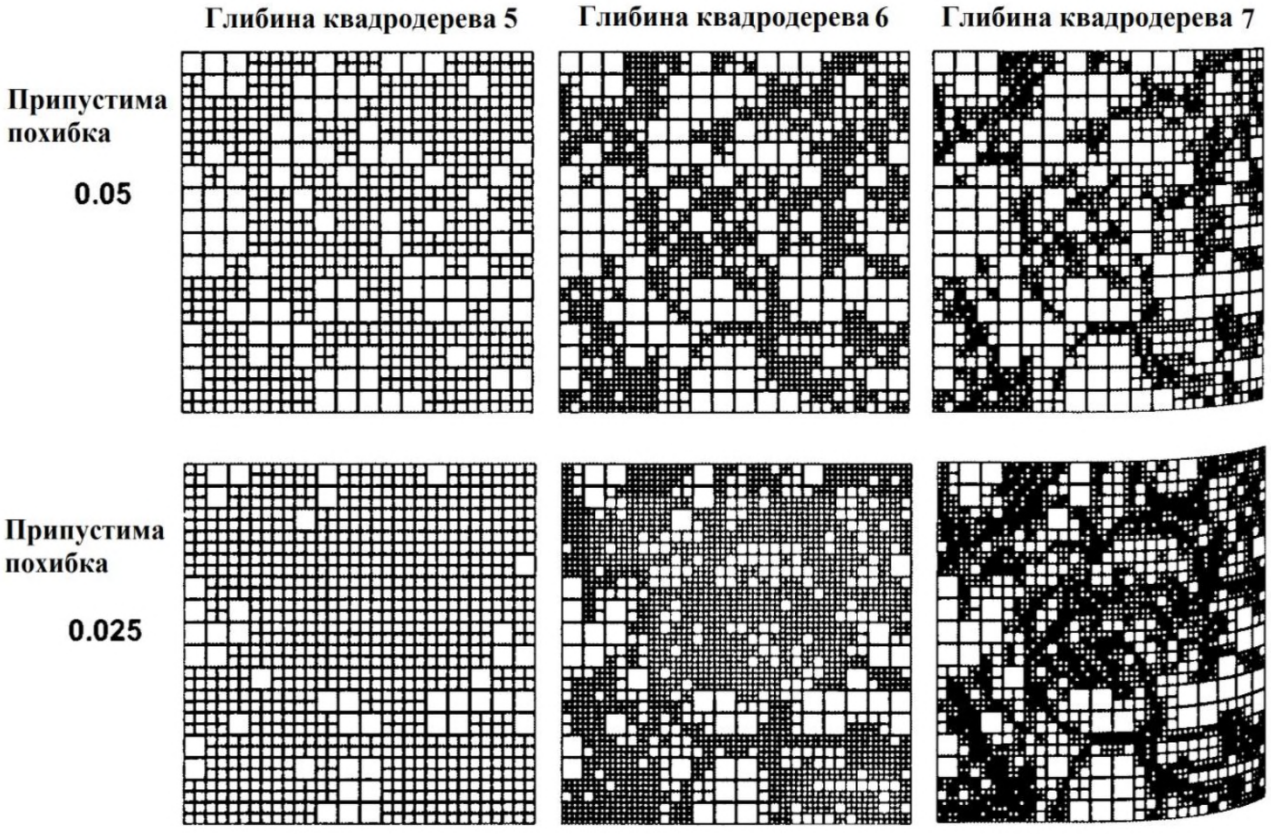


Рисунок 2.3 – Ефект використання меншої допустимої похибки і більшої глибини квадродерева

Як видно з рис. 2.3 у кожному разі більша кількість рангових блоків означає гіршу компресію (а іноді й відсутність компресії взагалі), але зазвичай кращу якість зображення.

В запропонованому підході до стеганографічного вбудовування інформації в зображення, стиснене фрактальним методом, з урахуванням потужності пікселів домену вводиться етап вбудовування інформації у фрактально стиснене зображення відповідно до алгоритму, представленому на рис. 2.4.

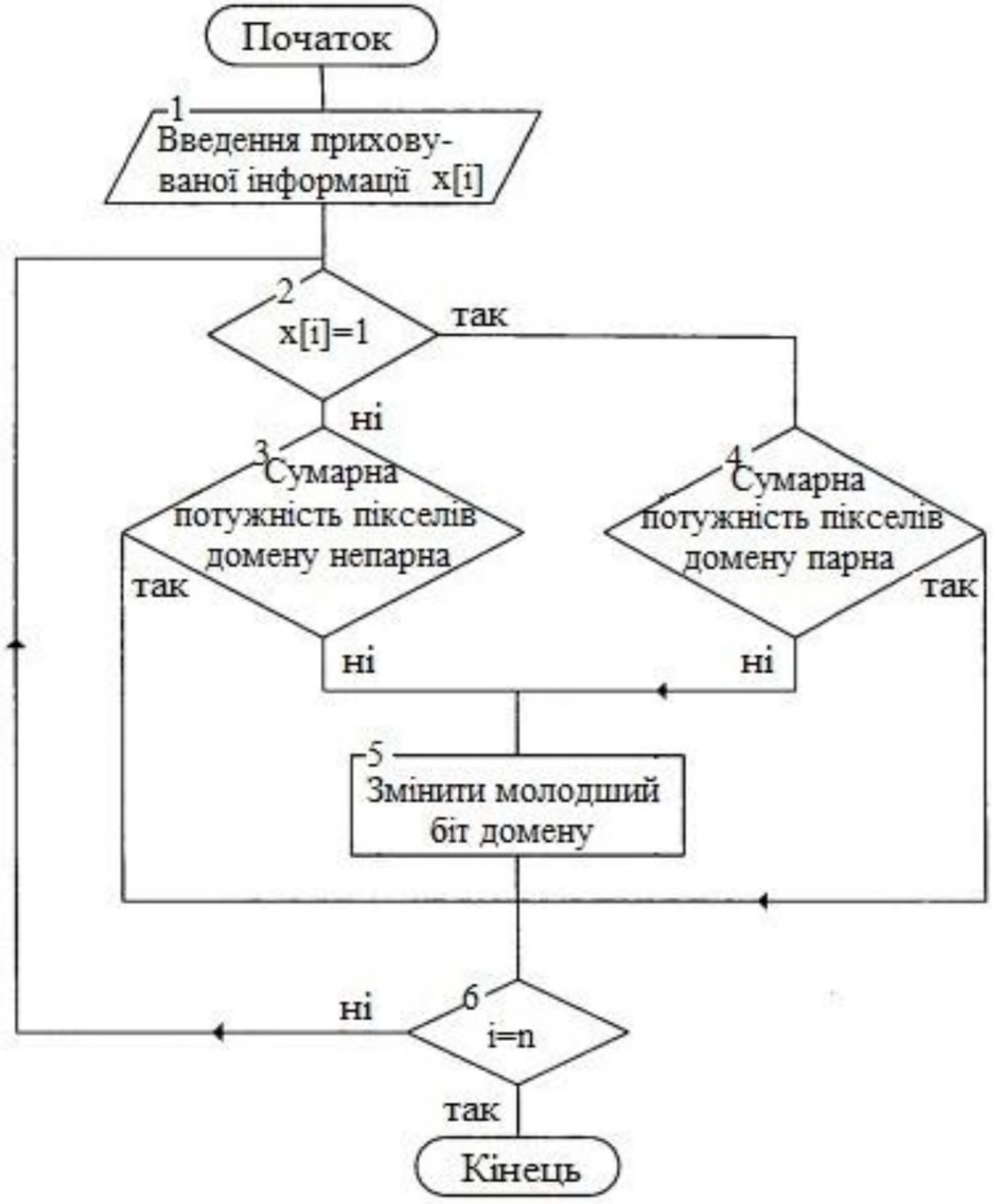


Рисунок 2.4 – Алгоритм, який реалізує запропонований підхід до стеганографічного вбудовування інформації в зображення, стиснене фрактальним методом, з урахуванням потужності пікселів домену

Реалізація даного етапу відбувається наступним чином (рис. 2.4). Інформація, передбачувана для вбудовування вводиться в двійковому вигляді. При здійсненні вбудовування відбувається побітне зчитування даних. Кожен біт вбудовується в ході реалізації етапу співвіднесення рангова область – домен. Поступаючи на фрактальний кодер значення вбудованого біта ідентифікується. У запропонованому підході розглядається запис одного біта на рангову область, у зв'язку з цим можливо значення «одиниця» і «нуль». У разі надходження на вхід кодера «одиниці», алгоритм передбачає розрахунок суми потужностей пікселів відповідного досліджуваній ранговій області домену. Якщо сумарна потужність пікселів домену парне число, то змін не проводиться і алгоритм переходить до розгляду наступного біта вбудовуваної інформації і наступної за рахунком рангової області. Якщо сума потужностей пікселів відповідного домену непарне число, то передбачається виправлення значення сумарної потужності на одиницю. Тобто відстежується відповідний даній ранговій області домен, який описується деякою кількістю пікселів, в залежності від його розміру.

Початкове зображення апріорі є 24 бітовим BMP, таким чином кожен піксель описується у вигляді трьох складових RGB. Алгоритм вибирає перший за рахунком піксель і інвертує значення молодшого біта, що описує цей піксель (рис. 2.4). Таким чином сумарне значення потужностей пікселів домену стає парним. Аналогічні дії проводяться при появи на вході фрактального кодера «нуля», Єдиною відмінністю є те, що необхідно сумарне значення потужностей пікселів домену привести до непарного.

Для збільшення обсягу вбудованої інформації можливо вбудовування двох і більше біт на рангову область. Для здійснення цього необхідно приводити сумарну потужність пікселів домену до чисел, які мають необхідне значення по модулю 4 для 2 біт, по модулю 8 для 3 біт і так далі. Природно, зі збільшенням кількості вбудованих біт початкове зображення буде сильніше спотворюватися.

Після виконання етапу співвіднесення рангів і доменів, формується архів, який складається із заголовка, в якому вказані параметри сформованого стисненого файлу, і поля даних, яке містить координати відповідних доменів, коефіцієнти афінних перетворювань, а також значення яскравості і контрастності.

2.2 Оцінка ефективності запропонованого підходу до стеганографічного вбудовування інформації в зображення, стиснене фрактальним методом, з урахуванням потужності пікселів домену

Оцінка ефективності запропонованого підходу до стеганографічного вбудовування інформації в зображення, стиснене фрактальним методом, з урахуванням потужності пікселів домену була проведена шляхом моделювання в середовищі Matlab / Simulink за допомогою стандартного і розробленого програмного забезпечення [34-46].

Ефективність функціонування запропонованого підходу до стеганографічного вбудовування інформації в зображення, стиснене фрактальним методом, з урахуванням потужності пікселів домену у порівнянні з підходом-прототипом полягає в тому, що в початковий файл практично не вносяться візуальні зміни і факт наявності вбудованої інформації визначити складно.

Реалізація запропонованого підходу до стеганографічного вбудовування інформації в зображення, стиснене фрактальним методом, з урахуванням потужності пікселів домену показала ефективність його застосування. На основі сформованої в середовищі Matlab / Simulink за допомогою стандартного і розробленого програмного забезпечення моделі фрактально стисненого зображення з інформацією, вбудованою запропонованим підходом, були отримані результати, які представлені на рис. 2.5.

На рис. 2.5 наведено графік залежності ймовірності наявності інформації від відсотку заповнення контейнера.

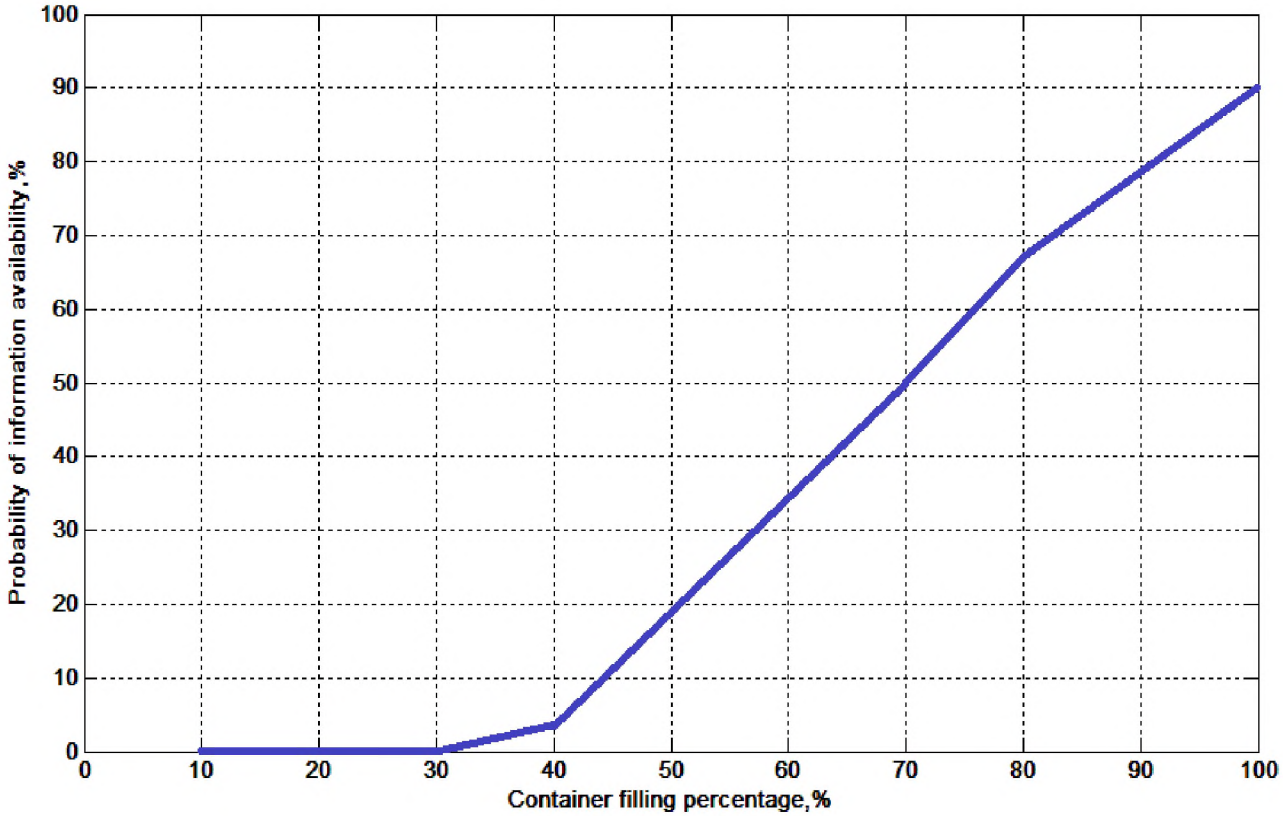


Рисунок 2.5 – Результат стеганографічного аналізу запропонованого підходу до стеганографічного вбудовування інформації в зображення, стиснене фрактальним методом, з урахуванням потужності пікселів домену

З рис. 2.3 видно, що стеганографічний аналіз, проведений за допомогою розроблених програм , що реалізують відомий алгоритм стеганоаналізу – метод аналізу розподілу пар значень на основі критерію χ^2, не дав результатів при встановленні одного біта на рангову область. При цьому обсяги переданої інформації в процентному співвідношенні складають від 1% і вище. Зокрема, якщо перевіряти значення суми потужностей пікселів домену по модулю 4, можливо вбудовування 2 біт в кожну рангову область, при цьому спотворення вихідного файлу буде рости. Отриманий відсоток вираховується на основі відношення кількості рангових областей в зображенні до загального розміру файлу. В ході моделювання використовувалося зображення розміром 345 кБ. При розбитті даного зображення було сформовано близько 27840 рангових

областей. Відповідно, обсяг вбудованої інформації становить 27840 біт (3480 байт), а відношення 3480/345000 = 0,011 (1,1%).

Таким чином, шляхом моделювання в середовищі Matlab / Simulink за допомогою стандартного і розробленого програмного забезпечення було встановлено ефективність застосування запропонованого підходу до стеганографічного вбудовування інформації в зображення, стиснене фрактальним методом, з урахуванням потужності пікселів домену.

2.3 Висновки

Запропонований підхід відноситься до області стеганографії, а саме до способів вбудовування повідомлення в цифрове зображення, і може бути використаний для організації прихованого зберігання і передачі конфіденційної інформації по відкритих каналах зв'язку.

Завданням запропонованого підходу є вбудовування інформації в цифрове зображення, стисле фрактальним методом, з урахуванням потужності пікселів домену, що забезпечує можливість прихованої передачі конфіденційних даних, використовуючи контейнер, представлений у вигляді фрактально стисненого зображення.

Це завдання вирішується тим, що в підході до вбудовування інформації в зображення, стисле фрактальним методом, з урахуванням потужності пікселів домену, що включає етапи формування вектора параметрів стиснення зображення, введення інформації, що приховується, виділення доменів і рангових областей, співвіднесення рангових областей і доменів, формування кінцевого архіву, введений етап приховування інформації, за рахунок корекції потужності пікселів домену. Реалізація запропонованого підходу полягає у включенні в процес фрактального стиснення етапу вбудовування інформації.

Оцінка ефективності запропонованого підходу до стеганографічного вбудовування інформації в зображення, стиснене фрактальним методом, з

урахуванням потужності пікселів домену була проведена шляхом моделювання в середовищі Matlab / Simulink.

Встановлено, що стеганографічний аналіз, проведений за методу аналізу розподілу пар значень на основі критерію χ^2, не дав результатів при встановленні одного біта на рангову область. При цьому обсяги переданої інформації в процентному співвідношенні складають від 1% і вище. Зокрема, якщо перевіряти значення суми потужностей пікселів домену по модулю 4, можливо вбудовування 2 біт в кожну рангову область, при цьому спотворення початкового файлу буде рости. Отриманий відсоток вираховується на основі відношення кількості рангових областей в зображенні до загального розміру файлу. В ході моделювання використовувалося зображення розміром 345 кБ. При розбитті даного зображення було сформовано близько 27840 рангових областей. Відповідно, обсяг вбудованої інформації становить 27840 біт (3480 байт), а відношення 3480/345000 = 0,011 (1,1%).

3 ЕКОНОМІЧНА ЧАСТИНА

Вбудовування інформації в цифрове зображення, стисле фрактальним методом, з урахуванням потужності пікселів домену, що забезпечує можливість прихованої передачі конфіденційних даних, використовуючи контейнер, представлений у вигляді фрактально стисненого зображення потребує економічного обґрунтування щодо доцільності його здійснення, що і є метою цього розділу. Досягнення цієї мети потребує виконання таких розрахунків, як:

– капітальні витрат на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов’язані з виготовленням апаратури, приладів, програмного забезпечення;

– річні експлуатаційні витрати на утримання і обслуговування об'єкта проектування;

– річний економічний ефект від впровадження запропонованих заходів;

– показники економічної ефективності впровадження системи захисту на підприємстві.

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Витрати на впровадження системи захисту інформації на підприємстві визначаються, виходячи з трудомісткості кожної операції, та належать до капітальних витрат.

Визначення трудомісткості розробки підходу щодо стеганографічного вбудовування інформації в цифрове зображення з використанням фрактального перетворення

Трудомісткість розробки підходу щодо стеганографічного вбудовування інформації в цифрове зображення з використанням фрактального перетворення визначається тривалістю кожної робочої операції, до яких належать наступні:

де $t_{тз}$ – тривалість складання технічного завдання на розробку підходу щодо стеганографічного вбудовування інформації в цифрове зображення з використанням фрактального перетворення, $t_{тз}$=18;

$t_в$ – тривалість аналізу існуючих інформаційних потоків організації, вивчення ТЗ, літературних джерел за темою тощо, $t_в$=*40*;

$t_а$ – тривалість аналізу існуючих загроз безпеки інформації, $t_а$=*30*;

$t_р$ – тривалість розробки підходу щодо стеганографічного вбудовування інформації в цифрове зображення з використанням фрактального перетворення, $t_м$=*60*;

$t_д$ – тривалість підготовки технічної документації, $t_д$=*14*.

Отже,

$$t = t_{тз} + t_в + t_а + t_р + t_д = 18+40+30+60+14= 162 \text{ години.}$$

Розрахунок витрат на розробку підходу щодо стеганографічного вбудовування інформації в цифрове зображення з використанням фрактального перетворення

Витрати на розробку системи захисту інформації на підприємстві $К_{рп}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації $З_{мч}$.

$$К_{рп} = З_{зп} + З_{мч} .$$

$$К_{рп} = З_{зп} + З_{мч} = 24624 +1268,5= 25892,5 \text{ грн.}$$

$$З_{зп} = t\, З_{пр} = 162*152 = 24624 \text{ грн.}$$

де t – загальна тривалість розробки політики безпеки, годин;

$З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн./годину.

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч} = t*С_{мч}=162*7,83=1268,5 \text{ грн.}$$

де $t_д$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = 1{,}1 \cdot 3 \cdot 1{,}68 + \frac{6400 \cdot 0{,}4}{1920} + \frac{9100 \cdot 0{,}2}{1920} = 7{,}83 \text{ грн.}$$

Реалізація запропонованого підходу щодо стеганографічного вбудовування інформації в цифрове зображення з використанням фрактального перетворення здійснюється за допомогою сучасної елементної бази, яка вже є наявною, тому додаткові витрати не виникають.

Оцінка ефективності запропонованого підходу до стеганографічного вбудовування інформації в зображення, стиснене фрактальним методом, з урахуванням потужності пікселів домену проведена шляхом моделювання в середовищі Matlab / Simulink. Зазначене програмне забезпечення вже використовується, тому в цьому випадку капітальні витрати не виникають.

Витрати на встановлення обладнання та налагодження системи інформаційної безпеки становитимуть 6000 грн.

Таким чином, капітальні (фіксовані) витрати на розробку засобів підвищення рівня інформаційної безпеки складуть:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} =$$

$$=25892{,}5+6000= 31892{,}5 \text{ грн.}$$

де $К_{рп}$ – вартість розробки політики інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн.;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн.;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн.;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн.;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу,

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, \quad грн.$$

де $С_в$ - вартість відновлення й модернізації системи ($С_в = 0$);

$С_к$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак} = 0$ грн.).

Оскільки середовище Matlab/Simulink, яке використовується для оцінки ефективності запропонованого підходу до стеганографічного вбудовування інформації в зображення, стиснене фрактальним методом, з урахуванням потужності пікселів домену, вже використовується, тому додаткові витрати щодо відновлення й модернізації системи не виникають.

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн.}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються сукупною величиною витрат на організаційні заходи, яка складає 1800 грн.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.}$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 18000 грн. Додаткова заробітна плата – 9% від основної заробітної плати. Виконання роботи щодо впровадження системи захисту

інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,15 ставки. Отже,

$$С_з = (18000*12 + 18000*12*0,09)*0,15= 35316 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2021 р. складає 22%.

$$С_{єв} = 35316*0,22 = 7769,5 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.},$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=1,1 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,68 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 1,1*3*1920*1,68 = 10644,8 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 2% ($С_{тос}$ = 31892,5*0,01=637,85 грн.).

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються:

$$С_к = 1800+35316+7769,5+10644,8+637,85 = 56168,15 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = 56168,15 \text{ грн.}$$

3.2 Оцінка можливого збитку

Запропонований підхід до стеганографічного вбудовування інформації в цифрове зображення з використанням фрактального перетворення може бути

використаний для організації прихованого зберігання і передачі конфіденційної інформації по відкритих каналах зв'язку.

Завданням запропонованого підходу є вбудовування інформації в цифрове зображення, стисле фрактальним методом, з урахуванням потужності пікселів домену, що забезпечує можливість прихованої передачі конфіденційних даних, використовуючи контейнер, представлений у вигляді фрактально стисненого зображення.

Для визначення величини збитку може бути застосована наступна спрощена модель оцінки. Забезпечення інформаційної безпеки передбачає відвернення загроз щодо витоку конфіденційної інформації по відкритих каналах зв'язку. Якщо підприємство передаватиме інформацію по відкритих каналах зв'язку, вартість якої потенційно складає 110000 грн., матиме біля 15 випадків витоку конфіденційної інформації на рік із вірогідністю реалізації цієї загрози щодо порушення конфіденційності інформації 22% (R=0,22), то можлива величина збитку (В) на рік становитиме:

$$B = 90000*15*0,22 = 297000 \text{ грн.}$$

3.2.1 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної:

$$E = B \cdot R - C \text{ грн.},$$

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації загрози (22%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

$$E = 297000 - 56168,15 = 240831,9 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Для встановлення економічної ефективності визначають такі показники як: коефіцієнт повернення інвестицій (ROSI) та термін окупності капітальних інвестицій (T_o).

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,}$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{240831,9}{31892,5} = 7,55, \quad \text{частки одиниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} - N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (6%);

$N_{інф}$ – річний рівень інфляції, (5%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$7,55 > (7 - 5)/100 = 7,55 > 0,02.$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{7,55} = 0,13 \text{ років.}$$

3.4 Висновок

Отже, виходячи з наведених розрахунків, розробка підходу щодо стеганографічного вбудовування інформації в зображення, стиснене фрактальним методом, з урахуванням потужності пікселів домену, може вважатися економічно доцільною. Про це свідчить значення коефіцієнт повернення інвестицій (ROSI=7,55), яке є вищим за дохідність альтернативного вкладення коштів. Економічний ефект величиною 240831,9 грн. при капітальних витратах величиною 31892,5 грн., дозволяє отримати 7,55 грн. на одну гривню вкладених коштів. Експлуатаційні витрати складають 56168,15 грн.

ВИСНОВКИ

1. В результаті аналізу принципів приховування даних в цифрових зображеннях, а також фрактального аналізу встановлено, що фрактальні алгоритми забезпечують вдале співвідношення між коефіцієнтом стиснення та якістю і володіють унікальною властивістю деталізації при довільному масштабуванні. Розвиток фрактального стиснення забезпечує популярність форматів на його основі, що підтверджує доцільність їх стеганографічного використання.

2. В результаті аналізу існуючих підходів до вбудовування інформації у фрактально стиснені зображення встановлено їх недоліки. Недоліком відомого підходу до передачі додаткової інформації при фрактальному кодуванні зображення, в якому вбудовування здійснюється в індекси орієнтації доменних блоків є сильне спотворення початкового зображення, в результаті переорієнтації доменів при встановленні в них додаткової інформації. Недоліком відомого підходу до передачі додаткової інформації при фрактальному кодуванні зображення, в якому вбудовування проводиться в молодші розряди індексів доменів є те, що в результаті такої вставки зменшується простір можливих доменів для відображення ранговому блоку, що знижує якість відновленого зображення. Недоліком відомого підходу до передачі додаткової інформації при спільному використанні векторного квантування і фрактального кодування зображень з урахуванням класифікації доменів і блоків з кодової книги (прототипу) є зміщення доменів щодо початкового положення, що призводить до накладання сегментів початкового зображення один на одний, що є візуально помітним.

3. Запропоновано підхід до стеганографічного вбудовування інформації в зображення, стиснене фрактальним методом, з урахуванням потужності пікселів домену, який включає в себе етапи формування вектора параметрів стиснення зображення, введення інформації, що приховується, виділення доменів і рангових областей, співвіднесення рангових областей і доменів,

формування кінцевого архіву. Також у запропонований підхід додатково введений етап приховування інформації, за рахунок корекції потужності пікселів домену. Це забезпечує можливість прихованої передачі конфіденційних даних, використовуючи контейнер, представлений у вигляді фрактально стисненого зображення.

4. В результаті оцінки ефективності запропонованого підходу до стеганографічного вбудовування інформації в зображення, стиснене фрактальним методом, з урахуванням потужності пікселів домену було встановлено, що стеганоаналіз не дав результатів при встановленні одного біта на рангову область. При цьому обсяги переданої інформації в процентному співвідношенні складають від 1% і вище. Зокрема, якщо перевіряти значення суми потужностей пікселів домену по модулю 4, можливо вбудовування 2 біт в кожну рангову область, при цьому спотворення початкового файлу буде рости. Отриманий відсоток вираховується на основі відношення кількості рангових областей в зображенні до загального розміру файлу. В ході моделювання використовувалося зображення розміром 345 кБ. При розбитті даного зображення було сформовано близько 27840 рангових областей. Відповідно, обсяг вбудованої інформації становить 27840 біт (3480 байт), а відношення 3480/345000 = 0,011 (1,1%).

ПЕРЕЛІК ПОСИЛАНЬ

1. Johnson N., Duric Z., Jajodia S. Information Hiding: Steganography and Watermarking – Attacks and Countermeasures. – New York: Kluwer Academic Pub., 2000. – 200 p.

2. Грибунин В.Г. Цифровая стеганография [Текст] : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М. : СОЛОН-Пресс, 2002. – 272 с.

3. Zou D., Shi Y., Su W., Xuan G. Steganalysis based on Markov Model of Thresholded Prediction-Error Image // IEEE ICME Conference Record, 2006. – P. 1365-1368.

4. Chen X., Wang Y., Tan T., Guo, L. Blind Image Steganalysis Based on Statistical Analysis of Empirical Matrix // IEEE ICPR'06, 2006. – № 3. – P. 1107-1110.

5. Barnsley M., Hard L. Fractal Image Compression. – Wellesley: A.K. Peters, Ltd., 1993. – 256 p.

6. Уэлстид С. Фракталы и вейвлеты для сжатия изображений в действии. Учебное пособие. / С. Уэлстид. – М.: Издательство Триумф, 2003. – 320 с.

7. Конахович, Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – Киев : МК-Пресс, 2006. – 288 с.

8. Хорошко, В.А. Методы и средства защиты информации [Текст] : научное издание / В.А. Хорошко, А.А. Чекатков; Ред. Ю.С. Ковтанюк. – К. : ЮНИОР, 2003. – 505 с.

9. Основы компьютерной стеганографии / А.В. Аграновский, П.Н. Девянин, Р.А. Хади, А.В. Черемушкин. – М.: Радио и связь, 2003. – 152 с.

10. Швідченко І.В. Методи виявлення стеганографічного приховання інформації в зображеннях / І.В. Швідченко // Штучний інтелект. – 2015. – № 4. – Р. 697-705.

11. Ланде Д.В. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки: навчальний посібник. / Д.В. Ланде, І.Ю. Субач, Ю.Є. Бояринова. – К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2018. – 297 с.

12. Гонсалес Р. Цифровая обработка изображений (перевод с английского) / Р. Гонсалес, Р. Вудс, под ред. П.А. Чочиа – М.: Техносфера, 2005. – 1072 с.

13. Федер Е. Фракталы / Е. Федер. – М.: Мир, 1991. – 254 с.

14. Stanislav A. Fractal research methodology / A. Stanislav // Nature Neurosci. – 1999. – № 1. – 10-140.

15. Кроновер Р.М. Фракталы и хаос в динамических системах. Основы теории. / Р.М. Кроновер. – М. : Постмаркет, 2000. – 352 с.

16. Шредер М. Фракталы, хаос, степенные законы / М. Шредер. – М.-И.: R&C Dynamics, 2001. – 527 с.

17. Mandelbrot B.B. The Fractal Geometry of Nature / B.B. Mandelbrot. – W.H. Freeman. – 1983. – 537 pp.

18. Hurst H.E. Long-term storage capacity of reservoirs. / H.E. Hurst // Trans. Amer. Soc. Civ. Eng. – 1951. – Vol. 116. – Pp. 770-808.

19. Корнієнко В.І. Інтелектуальне моделювання нелінійних динамічних процесів в системах керування, кібербезпеки, телекомунікацій: підручник / В.І. Корнієнко, О.Ю. Гусєв, О.В. Герасіна; за заг. ред. В.І. Корнієнка ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро : НТУ «ДП», 2020. – 536 с. – ISBN 978-966-350-735-4.

20. Барсуков В.С., Романцов А.П. Оценка уровня скрытности мультимедийных стеганографических каналов хранения и передачи информации // Специальная Техника. – 2000. – № 1.

21. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: КУДИЦ-ОБРАЗ, 2003. – 236 с.

22. Аграновский А.В. Стеганография, цифровые водяные знаки и стеганоанализ. / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. – М.: Вузовская книга, 2009. – 220 с.

23. Тропченко А.Ю. Методы сжатия изображений, аудиосигналов и видео: Учебное пособие / А.Ю. Тропченко, А.А. Тропченко– СПб: СПбГУ ИТМО, 2009. – 108 с.

24. Zhao E., Liu D. Fractal Image Compression Methods: A Review // ICITA'05, 2005. – P. 756-759.

25. Polvere M., Nappi M. Speed-up in Fractal Image Coding: Comparison of Methods // IEEE TIP, 2000. – № 6. – P. 1002-1009.

26. Davern P. Fractal based image steganography / P. Davern, M. Scott // Lecture Notes in Computer Science. 1996. – Vol. 1174. – P. 279-294.

27. Jacquin A.E. Fractal image coding based on a theory of iterated contractive image transformations / A.E. Jacquin // Proceedings of SPIE Visual Communications and Image Processing '90. – Vol. 1360. – 1990.

28. Laurencot T. Hybrid image block coders incorporating fractal coding and vector quantization, with a robust classification scheme / T. Laurencot, A.E. Jacquin // AT&T Tech. Memo. – February 1992.

29. Васюра А.С., Золотавкін Є.А. Визначення та забезпечення стійкості методу таємної передачі даних на основі фрактального стиснення зображення // Вісник Хмельницького національного університету. – Хмельницький, 2007. – № 2 .– С. 133-138.

30. Патент РФ 2339181. Способ передачи дополнительной информации при фрактальном кодировании изображения / А.В. Тезин, А.В. Ширко, А.А. Кириллов, А.В. Шмойлов – заявл. 25.06.2007, опубл. 20.11.2008.

31. Патент РФ 2292662. Способ передачи дополнительной информации при фрактальном кодировании изображения / А.В. Тезин, А.В. Шмойлов, М.В. Стремоухов – заявл. 18.04.2005, опубл. 27.01.2011.

32. Патент РФ 2327301. Способ передачи дополнительной информации при совместном использовании векторного квантования и фрактального кодирования изображений с учетом классификации доменов и блоков из кодовой книги / А.В. Тезин, А.В. Шмойлов – заявл. 07.04.2006, опубл. 27.12.2007.

33. Fisher Y. Fractal Image Compression. Theory and Application / Y. Fisher – New York: Springer-Verlag, 1995. – 342 p.

34. Cox I. Digital Watermarking and Steganography/ Cox Ingermar, Miller Matthew, Bloom Jeffrey, Fridrich Jessica, Kalker Ton. – London: Elsevier, 2008. – 593 p.

35. Wayner P. Disappearing Cryptography: Information Hiding: Steganography and Watermarking / P. Wayner // Wayner Peter. – London: Elsever, 2009. – 440 p.

36. Кошкина Н.В. Стеганоанализ изображений в формате jpeg на базе атаки контрольным внедрением / Н.В. Кошкина // УСиМ. – 2014. – № 4. – С. 3-17.

37. Швідченко І.В. Аналіз програмного забезпечення зі стеганоаналізу // Искусственный интеллект. – 2012. – № 3. – С. 487–495.

38. Hawi T.A., Qutayari M.A., Barada H. Steganalysis attacks on stego images using stego-signatures and statistical image properties // TENCON'2004, Region 10 Conf. – 2004. – 2. – P. 104–107.

39. Fridrich J., Goljan M. Practical steganalysis of digital images-state of the art // Proc. SPIE Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents. – 2002. – 4675. – P. 1–13.

40. Fridrich J., Goljan M., Du R. Steganalysis based on JPEG compatibility // SPIE Multimedia Syst. and Appl. IV. – 2001. – P. 275–280.

41. Солодуха Р.А., Машуков Д.В. Опыт сигнатурного анализа стеганографической программы S-Tools // Вестн. Воронеж. ин-та МВД России. – 2013. – № 2. – С. 253–259.

42. Image steganalysis with binary similarity measures / I. Avcibas, M. Kharrazi, N. Memon et al. // EURASIP J. on Appl. Signal Processing. – 2005. – P. 2749–2757.

43. Sheikhan M., Moin M., Pezhmanpour M. Blind image steganalysis via joint co-occurrence matrix and statistical moments of contourlet transform // 10th Int. Conf. on Intelligent Syst. Design and Appl. (ISDA). – 2010. – P. 368–372.

44. Dautrich J. Multi-class steganalysis // Machine learning course research project distinguishing images embedded using reversible steganographic schemes. – 2009. – P. 1–6.

45. Yan Y., Li L., Zhang Q. Universal steganalysis method based on multi-domain features // J. of Information & Comp. Sci. – 2013. – P. 2177–2185.

46. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека/ Упоряд.: О.В. Герасіна, Д.С. Тимофєєв, О.В. Кручінін, Ю.А. Мілінчук – Дніпро: НТУ «ДП», 2020. – 47 с.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	**Формат**	**Найменування**	**Кількість листів**	**Примітки**
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	3	
5	А4	Стан питання. Постановка задачі	31	
6	А4	Спеціальна частина	12	
7	А4	Економічний розділ	8	
8	А4	Висновки	2	
9	А4	Перелік посилань	5	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Презентація Мірошниченко.ppt

2 Диплом Мірошниченко.doc

ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу _____ Пілова Д.П.

(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-17-1 Мірошниченко Д.В. на тему: «Стеганографічне вбудовування інформації в цифрове зображення з використанням фрактального перетворення»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 73 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на забезпечення можливості прихованої передачі конфіденційних даних, використовуючи контейнер, представлений у вигляді фрактально стисненого зображення.

При виконанні роботи автор продемонстрував добрий рівень теоретичних знань і практичних навичок. На основі аналізу принципів приховування даних в цифрових зображеннях і фрактального аналізу, а також існуючих підходів вбудовування інформації у фрактально стиснені зображення в ній сформульовано задачі, вирішенню яких присвячений спеціальний розділ. У ньому було запропоновано підхід до стеганографічного вбудовування інформації в зображення, стиснене фрактальним методом, з урахуванням потужності пікселів домену та оцінено його ефективність.

Практична цінність роботи полягає у тому, що запропонований підхід може бути використаний для організації прихованого зберігання і передачі конфіденційної інформації по відкритих каналах зв'язку.

До недоліків роботи слід віднести недостатню проробку окремих питань.

Рівень запозичень у кваліфікаційній роботі не перевищує вимог «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Мірошниченко Д.В. заслуговує на оцінку « » та присвоєння кваліфікації «Бакалавр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,
к.т.н., доцент **О.В. Герасіна**