

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет навчально-науковий центр заочної форми навчання
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Методи шифрування інформації
за допомогою алгебраїчних фракталів

(тема)

Виконав:

студент II курсу, групи СПзм-20-1
Караджян Б. Ю.
(прізвище, ініціали)

Спеціальність _____

123 «Комп'ютерна інженерія»

(код і повна назва спеціальності)

Тип програми освітньо-наукова

(освітньо-професійна або освітньо-наукова)

Освітня програма _____

Системне програмування

(повна назва освітньої програми)

Керівник: доц. Ільїна І. В.

(посада, прізвище, ініціали)

Допускається до захисту

Завідувач кафедри ЕОМ

(підпис)

Коваленко А.А.

(прізвище, ініціали)

2023 р.

Харківський національний університет радіоелектроніки

Факультет навчально-науковий центр заочної форми навчання

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп'ютерна інженерія»
(код і повна назва)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма Системне програмування
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)

“ _____ ” _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Караджян Богдан Юрійович
(прізвище, ім'я, по батькові)

1. Тема роботи Методи шифрування інформації за допомогою алгебраїчних фракталів

затверджена наказом по університету від “ 25 ” березня 2022 р. № 33Стз

2. Термін подання студентом роботи до екзаменаційної комісії 18 травня 2022 р.

3. Вхідні дані до роботи Різновиди фракталів, набір зображень

4. Перелік питань, що потрібно опрацювати у роботі _____

Аналіз теорії фракталів;

Аналіз сфер застосування фракталів;

Розробка методів шифрування для зображень та тексту

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) 10 слайдів презентації

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

| Найменування розділу | Консультант (посада, прізвище, ім'я, по батькові) | Позначка консультанта про виконання розділу | |
|----------------------|--|---|------|
| | | підпис | дата |
| | | | |
| | | | |

КАЛЕНДАРНИЙ ПЛАН

| № | Назва етапів роботи | Термін виконання етапів роботи | Примітка |
|---|--|--------------------------------|----------|
| 1 | Огляд основних положень теорії фракталів | 29.03.22-04.04.22 | |
| 2 | Вибір та обґрунтування методики дослідження | 05.04.22-12.04.22 | |
| 3 | Огляд сфер застосування фракталів | 13.04.22-19.04.22 | |
| 4 | Розробка методів шифрування | 20.04.22-26.04.22 | |
| 5 | Проведення експериментів | 27.04.22-04.05.22 | |
| 6 | Оформлення матеріалів кваліфікаційної роботи | 05.05.22-10.05.22 | |
| 7 | Подання кваліфікаційної роботи керівникові та її попередній захист | 11.05.22-12.05.22 | |
| 8 | Подання кваліфікаційної роботи на рецензування | 13.05.22-17.05.22 | |
| | | | |
| | | | |

Дата видачі завдання 28 березня 2022 р.

Студент _____
(підпис)

Керівник роботи _____
(підпис)

доц. Ільїна І.В.
(посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 80 с., 44 рис., 3 дод.,
14 джерел.

ФРАКТАЛИ, ЗОБРАЖЕННЯ, ШИФРУВАННЯ, БЕЗПЕКА,
КІБЕРБЕЗПЕКА.

Метою кваліфікаційної роботи є розробка методів шифрування інформації на основі алгебраїчних фракталів.

У ході виконання кваліфікаційної роботи були вирішені наступні завдання:

- проаналізовано сфери застосування фракталів;
- проаналізовано типи алгебраїчних фракталів;
- розроблено алгоритм шифрування зображень;
- розроблено алгоритм шифрування тексту.

ABSTRACT

Master's thesis: 80 pages, 44 figures, 3 appendices, 14 sources.

FRACTALS, IMAGES, ENCRYPTION, SECURITY, CYBER SECURITY.

The major goal of this thesis is to develop methods of encrypting information based on algebraic fractals

During the qualification work the following tasks were solved:

- the spheres of application of fractals are analyzed;
- types of algebraic fractals are analyzed;
- the algorithm of image encryption is developed;
- the algorithm of text encryption is developed.

ЗМІСТ

| | |
|---|----|
| ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ | 7 |
| ВСТУП | 8 |
| 1 ОСНОВНІ ПОНЯТТЯ ТЕОРІЇ ФРАКТАЛІВ | 10 |
| 1.1 Теорія фракталів..... | 10 |
| 1.2 Конструктивні фрактали | 15 |
| 1.3 Динамічні фрактали | 20 |
| 1.4 Стохастичні фрактали..... | 25 |
| 2 ДЕЯКІ ПРОГРАМИ ФРАКТАЛЬНОГО АНАЛІЗУ | 27 |
| 2.1 Фрактальні криві та поверхні..... | 27 |
| 2.2 Рангові розподіли | 28 |
| 2.3 Фрактальна графіка та обробка зображень | 32 |
| 2.4. Фрактальна криптографія..... | 33 |
| 2.5 Фрактальні мережі та лабіринти..... | 35 |
| 2.6 Фрактали у технічних науках | 38 |
| 3 ВИКОРИСТАННЯ ФРАКТАЛІВ У КРИПТОГРАФІЇ..... | 42 |
| 3.1 Огляд існуючих методів | 42 |
| 3.2 Метод шифрування зображень за допомогою фракцій алгебри | 42 |
| 4 ЕКСПЕРИМЕНТАЛЬНА ЧАСТИНА | 45 |
| 4.1 Побудова фракталів | 45 |
| 4.2 Шифрування та дешифрування зображень | 51 |
| 4.3 Шифрування та дешифрування текстів | 60 |
| ВИСНОВКИ..... | 63 |
| ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ | 64 |
| ДОДАТОК Б ЛІСТИНГ ПРОГРАМИ ДЛЯ ПОБУДОВИ ФРАКЦІЙ АЛГЕБРИ | 72 |
| ДОДАТОК В ЛІСТИНГ ПРОГРАМИ ДЛЯ ШИФРУВАННЯ | 77 |

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ
І ТЕРМІНІВ

СІФ – системи функцій, що ітеруються

ОДА – модель обмеженої дифузії агрегації

DLA – Diffusion Limited Aggregation

ФС – фрактальні сигнатури

ЕМА – клас електричних малих антен

ВСТУП

Починаючи з кінця ХХ століття, питання, пов'язані зі збереженням та передачею інформації в різних галузях математики, набули дуже великого значення. Завдання, що виникають при цьому, вирішує криптографія – наука про методи перетворення інформації з метою її захисту від несанкціонованого доступу.

Усю історію криптографії, що налічує понад чотири тисячі років, можна розділити на п'ять основних етапів. Перший (приблизно з 3-го тисячоліття до н.е.) характеризується пануванням моноалфавітних шифрів. Основний принцип полягав у заміні алфавітного тексту іншим алфавітом через заміну літер на інші літери або символи.

Другий етап (з ІХ століття на Близькому Сході і з ХV століття в Європі – до початку ХХ століття) охарактеризувався запровадженням поліалфавітних шифрів (циклічне застосування моноалфавітних шифрів до певного числа літер тексту, що шифрується).

Третій етап (з початку ХХ століття і до середини ХХ століття) обумовлений введенням електромеханічних пристроїв у роботу шифрувальників. Це перетворювало криптографію, оскільки розширилися можливості доступу до шифрованого тексту та з'явилися можливості впливу на відкритий текст. Одним з найбільш відомих електромеханічних шифраторів, що з'явилися в той час, була роторна шифрмашинка «Енігма», винайдена в 1917 році. Вона застосовувалася аж до 1942 року, коли з'явилася перша обчислювальна машинка «Колос», створена Аланом Тюрінгом для перебору ключів.

У цей період також розвивалися методи дешифрування, засновані на парах відкритих і шифрованих текстів, на шифротекстах, отриманих на одному ключі, на використанні ймовірнісних ключів. У математичному плані розвивалися імовірно-статистичні методи, що використовують

частоту значень.

Четвертий етап розпочався після публікації роботи Клода Шеннона «Теорія зв'язку в секретних системах» у 1949 році і тривав до 70-х років ХХ століття. Цей період є переходом до математичної криптографії. У роботі Шеннона викладається теорія секретних систем, які є математичною моделлю шифрів, формулюються принципи розсіювання та перемішування. Також Клодом Шенноном були розроблені концепції теоретичної та практичної секретності, що дозволяють кількісно оцінити криптографічні якості шифру. Криптографію цього періоду називають «класичною» або криптографією із секретним ключем.

Сучасний (п'ятий) етап криптографії починається з виходом статті американських учених Вітфілда Діффі та Мартіна Хеллмена «Нові напрямки у криптографії» у 1976 році. У статті було сформульовано принцип шифрування без збереження ключа в секреті, що дало початок новому напрямку – асиметричній криптографії (або криптографії з відкритим ключем). Її поява характеризується не лише новими технічними можливостями, а й порівняно широким поширенням криптографії для використання приватними особами, оскільки раніше використання криптографії було лише прерогативою держави.

В даний час у криптографії існує безліч методів для захисту текстової інформації, але через велику обчислювальну складність ці алгоритми не завжди можна застосувати до шифрування зображень.

Одним із цікавих підходів є використання фракцій алгебри в криптографії. Для їх побудови потрібна порівняно невелика кількість даних, але на виході виходить зображення досить складного об'єкта з хаотичними межами, яке можна використовувати як шифрувальне зображення, а параметри для його побудови будуть ключем.

У роботі розглядаються основи теорії фракталів та криптографії та пропонуються кілька алгоритмів шифрування зображень та текстів, що ґрунтуються на фрактальному моделюванні.

1 ОСНОВНІ ПОНЯТТЯ ТЕОРІЇ ФРАКТАЛІВ

1.1 Теорія фракталів

У 1970-х роках французький математик Бенуа Мандельброт відкрив новий погляд на природу та світ у цілому. За основу він взяв дуже просту ідею: нескінченну за красою та різноманітністю безліч фігур можна отримати з простих конструкцій за допомогою всього двох операцій – копіювання та масштабування. Таким дивним і повторюваним формам, маленький шматочок яких у точності, як об'єкт цілком, Мандельброт 1975 року дав назву – фрактали і став основоположником нового розділу математики – фрактальної геометрії. Поняття фрактал і фрактальна геометрія з середини 80-х міцно увійшли в ужиток як математиків та програмістів, так і інших дослідників. Слово фрактал утворене від латинських слів: fractus – зламаний, розбитий, дробовий та відповідного дієслова frangere – ламати, розламувати, тобто створювати фрагменти неправильної форми.

Фрактал – структура, що складається з частин, які в якомусь сенсі подібні до цілого. Це визначення містить суттєву відмітну ознаку – фрактал виглядає однаково, в якому б масштабі ми його не спостерігали. Але, маючи лише зовнішнім виглядом, оцінка фрактальних властивостей утруднена, а здебільшого неможлива.

Основні властивості фрактальних множин:

- фрактал має тонку структуру, тобто містить довільно малі масштаби;
- фрактал занадто нерегулярна множина, щоб бути описана традиційною геометричною мовою;
- фрактал має форму самоподібності (наближену або статистичну);
- фрактальна розмірність більша за топологічну розмірність;
- в більшості випадків фрактал визначається дуже просто, наприклад, рекурсивно.

Одна з основних властивостей, що поєднують усі фрактали – це геометричне повторення самого себе на будь-якому масштабному рівні (самоподібність). Іншими словами, самоподібний об'єкт у точності або приблизно збігається з частиною себе самого, тобто ціле має ту ж форму, що й одна або більше частин. Самоподібність (симетрія) – інваріантність щодо паралельних переносів та скейлінгу (зміни масштабу). У найпростішому випадку невелика частина фрактал містить інформацію про весь фрактал. Більшість природних об'єктів демонструє самоподібність – головний організуючий принцип фракталів. Тому фрактали нагадуватимуть один одного, незалежно від використовуваної шкали.

Самоподібність може бути:

- "точним", але тільки в математичних об'єктах (наприклад, крива Коха),
- «якісним», тобто об'єкт чи процес є подібними до різних масштабів, просторових чи тимчасових, статистично (кожен масштаб нагадує інші масштаби, але не ідентичний їм).

Строго кажучи, у другому випадку треба говорити про фракталоподібні структури. На рисунку 1.1 показаний приклад самоподібності у природі.



Рисунок 1.1 – Самоподібність у природі

Від гілки, як і від стовбура дерева, відходять менші відростки, від них – ще менші, і інше, тобто гілка подібна до всього дерева.

Приклад «якісної» самоподібності – графіки курсу біткоїну за хвилинами протягом доби та за рік відповідно представлено на рисунку 1.2.

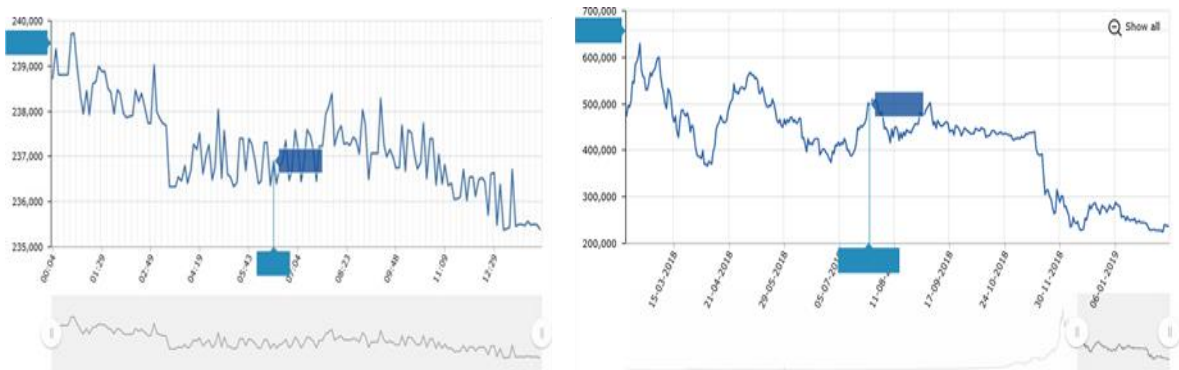


Рисунок 1.2 – Приклад «якісної» самоподібності – графіки курсу біткоїну за хвилинами протягом доби та за рік відповідно

Фрактали діляться на два великі класи: конструктивні та динамічні. З іншого боку, фрактали за способом побудови (завдання) поділяються на такі групи.

Геометричні (конструктивні). Цей тип фракталів виходить шляхом простих геометричних побудов: береться набір відрізків, на підставі яких будуватиметься фрактал, потім до цього набору застосовується набір правил, який перетворює його на якусь геометричну фігуру. Далі до кожної частини цієї фігури застосовується той же набір правил, і, зробивши нескінченну кількість таких перетворень (принаймні подумки), отримаємо геометричний фрактал. Прикладами можуть бути сніжинка Коха, килим Серпінського, крива Пеано тощо.

Алгебраїчні фрактали будуються за допомогою алгебраїчних формул, іноді дуже простих. Один з методів побудови є ітераційним процесом

$$z_{n+1} = f(z_n) \quad (1.1)$$

де z – деяке комплексне число;

$f(z)$ – нелінійна функція.

Розрахунок функції продовжується до виконання певної умови. Як приклади можна розглянути множину Мандельброта, фрактали Ньютона та Жюліа.

Системи функцій, що ітеруються (СІФ). Цей засіб отримання фрактальних структур став широко відомий завдяки М. Барнслі (M. Barnsley). Система функцій, що ітеруються, являє собою сукупність стискаючих відображень разом з ітераційною схемою, заданою за допомогою перетворення Хатчинсона. Результат застосування системи ітерованих функцій називається атрактором, причому атрактор часто виявляється фрактальною множиною. Найбільш проста СІФ складається з афінних перетворень на площині. Теорія ітерованих функцій є складовою теорії динамічних систем. Системи функцій, що ітеруються, застосовуються в основному для кодування зображень. Листок папороті – приклад побудови фракталу за допомогою СІФ представлено на рисунку 1.3.



Рисунок 1.3 – Приклад «якісної» самоподібності – графіки курсу біткоїну за хвилинами протягом доби та за рік відповідно

Стохастичні (випадкові) фрактали. Тут у дослідженнях зустрічається два підходи. Перший підхід – до побудови фракталів вносяться випадкові обурення. Береться, наприклад, прямокутник і кожного його кута визначається колір. Далі знаходиться центральна точка прямокутника і розфарбовується в колір, що дорівнює середньому арифметичному кольору по кутах прямокутника, плюс деяке випадкове число. Чим воно більше, тим рванішим буде. За допомогою таких фракталів моделюються гори у більшості програм, створених для цього. Другий підхід не зводиться до випадкових збурень у класичних фракталах. Навпаки, вважається, що випадковий характер закладений у них спочатку і пов'язаний із випадковими процесами, основною моделлю яких є фрактальний броунівський рух [1].

Фрактальні кластери. Кластери - це скупчення близько розташованих, тісно пов'язаних один з одним частинок будь-якої природи. Використовуються для опису фрактальних структур, що зустрічаються як на мікрооб'єктах (атоми, молекули, іони тощо), так і на системах, що складаються з великої кількості пов'язаних макроскопічних частинок (скупчення галактик). Фрактальний кластер - це фрактал, який виходить системою з безліччю частинок, що рухаються хаотично за броунівським законом руху, які злипаються при дотику до центру агрегації, і утворюють розгалужений кластер. Одним із способів для збирання таких фракталів є модель обмеженої дифузії агрегації (ОДА) або Diffusion Limited Aggregation (DLA-модель). На рисунку 1.4 представлено приклади побудови фрактального кластера за допомогою ОДА

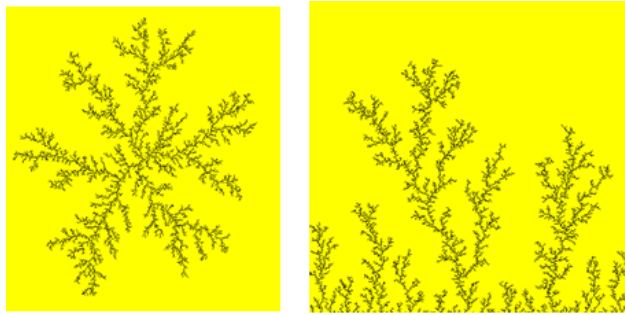


Рисунок 1.4 – Приклад «якісної» самоподібності – графіки курсу біткоїну за хвилинами протягом доби та за рік відповідно

1.2 Конструктивні фрактали

Конструктивні чи геометричні фрактали є наочними, у яких самоподібність видно відразу. Для побудови геометричних фракталів характерне завдання "основи" та "фрагменту", що повторюється при кожному зменшенні масштабу. Методика: спочатку зображується основа. Потім деякі частини основи замінюються фрагментом. На кожному наступному етапі частини вже побудованої фігури, аналогічні до заміненних частин основи, знову замінюються на фрагмент, взятий у відповідному масштабі. Щоразу масштаб зменшується. Для отримання самого фрактала потрібна нескінченна кількість етапів. Змінюючи основу та фрагмент, можна отримувати різні геометричні фрактали. Розглянемо побудову класичних фракталів.

Множина Кантора. Береться відрізок одиничної довжини. На першому етапі він ділиться на три рівні частини, і виймається середній відрізок. На другому кроці подібної процедури розподілу на три рівні частини і подальшого видалення середини піддається кожен з двох відрізків, що залишилися. Продовжуючи так до нескінченності, отримаємо безліч точок, описаних Георгом Кантором в 1883 р. Хоча варто зауважити, що існування цього фракталу відзначалося ще Генрі Смітом в 1875 р. На Заході подібні множини називають іноді пилом Кантора. множина Кантора добре відоме з

курсу функціонального аналізу як приклад множина нульової міри Лебега, чия потужність дорівнює потужності континууму $[0, 1]$. На рисунку 1.5 представлено приклад множини Кантора.

Крива Коха. Цю криву побудував Хельге фон Кох в 1904 р., як приклад кривої, яка ніде немає дотичної, тобто ніде не диференційована, хоча всюди безперервна. Ця крива самоподібна: кожна її частина є копією цілого. До того ж кожна частина кривої має нескінченну довжину. Процес її побудови виглядає так: беремо одиничний відрізок, розділяємо на три рівні частини і замінюємо серединний інтервал рівностороннім трикутником без цього сегмента. В результаті утворюється ламана, що складається з чотирьох ланок довжини $1/3$.



Рисунок 1.5 – Множина Кантора (6 ітерацій)

На наступному кроці повторюємо операцію для кожного з чотирьох ланок, що вийшли та інше. Гранична крива є крива Коха (рисунок 1.6)

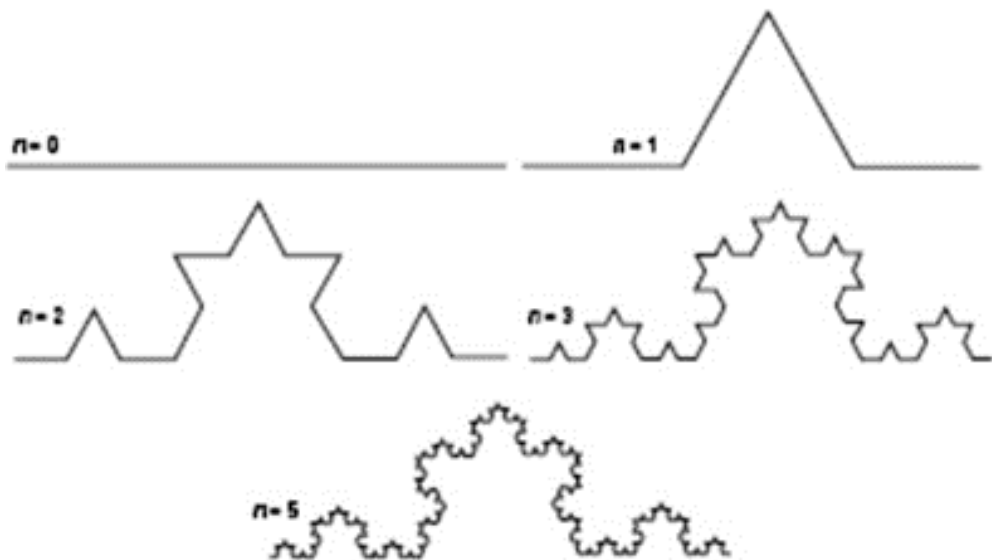


Рисунок 1.6 – Приклад «якісної» самоподібності – графіки курсу біткоїну за хвилинами протягом доби та за рік відповідно

Інший спосіб побудови кривої Коха починається із замкнутого рівнобедреного трикутника з кутами 30° , 120° та 30° . Цей трикутник розбивається на три трикутники: один – правильний, а два інших подібні до початкового рівнобедреного трикутника. Правильний трикутник видаляється. Третій крок - повторюємо операцію до кожного з рівнобедрених трикутників, що залишилися. Продовжуючи процес, в результаті отримаємо спадкову послідовність замкнутих множин і крива Коха – це їхнє перетинання (рисунок 1.7). Крива Коха самоподібна: кожна її частина є копією цілого. Крива Коха є основою для отримання таких фігур, як острови, хрести та сніжинки Коха. Можна отримувати і тривимірні уявлення кривої Коха, використовуючи як основу тетраедр і додаючи менші за розмірами тетраедри до кожної його грані.



Рисунок 1.7 – Приклад «якісної» самоподібності – графіки курсу біткоїну за хвилинами протягом доби та за рік відповідно

Килим Серпінського. Розглянемо ще один приклад простого самоподібного фракталу – килим, збудований у 1915 р. польським математиком Вацлавом Серпінським. Для його побудови береться квадрат із довжиною боку, що дорівнює одиниці. Потім кожна сторона квадрата ділиться на три рівні частини, а весь квадрат, відповідно, на дев'ять однакових квадратиків зі стороною рівною $1/3$. З отриманої фігури вирізається центральний квадрат. Потім такій же процедурі піддається кожен з 8 квадратиків, що залишилися, і т.д.; цей процес продовжується нескінченно. Перетин отриманих на кожному кроці об'єднань квадратів, що залишилися, називається килимом Серпінського (рисунок 1.8).

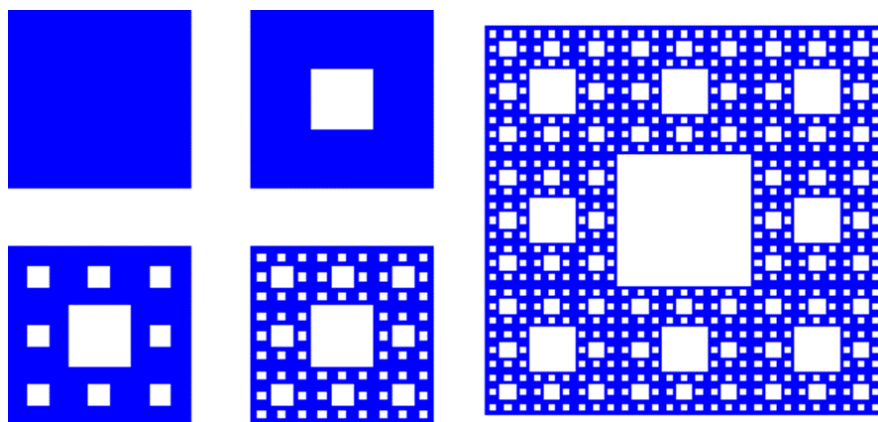


Рисунок 1.8 – Побудова килима Серпінського (нульовий-четвертий етапи)

Решето (серветка) Серпінського. Аналогічно можна побудувати решето Серпінського, використовуючи замість квадрата трикутник. Нульовий крок – за основу береться рівносторонній трикутник. Перший крок – потрібно знайти середини кожної зі сторін, з'єднати їх і викинути центральний з чотирьох маленьких трикутників, що утворилися. Другий крок - дії потрібно повторити з кожним з трьох трикутників, що залишилися при вершинах вихідного. Продовжуючи повторювати крок за кроком цей процес, у результаті залишається об'єкт, що складається з одних лише дірок (рисунок 1.9)

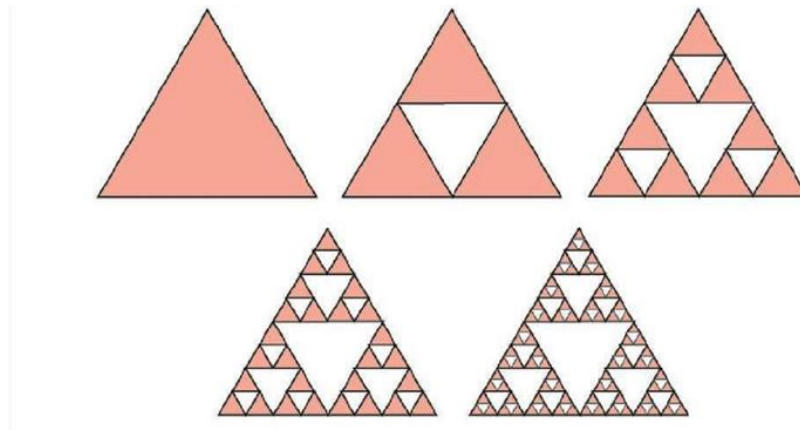


Рисунок 1.9 – Побудова решета Серпінського (0-4 кроки)

Аналогічно можна побудувати решето Серпінського, використовуючи замість квадрата трикутник. Нульовий крок – за основу береться рівносторонній трикутник. Перший крок – потрібно знайти середини кожної зі сторін, з'єднати їх і викинути центральний з чотирьох маленьких трикутників, що утворилися. Другий крок - дії потрібно повторити з кожним з трьох трикутників, що залишилися при вершинах вихідного. Продовжуючи повторювати крок за кроком цей процес, у результаті залишається об'єкт, що складається з одних лише дірок (рисунок 1.9).

1.3 Динамічні фрактали

Використовуватимемо деякі класи двовимірних нелінійних відображень, які відносяться до дискретних динамічних систем. Аналіз таких систем є досить важким. Розглянемо одновимірне комплексне відображення, що зіставляє одному комплексному числу $z_n = x_n + iy_n$ інше комплексне число $z_{n+1} = x_{n+1} + iy_{n+1}$ за ітераційним правилом $z_{n+1} = f(z_n)$, де $f(z)$ – деяка нелінійна функція змінної z , n – номер ітерації. Комплексні відображення такого роду породжують динамічні фрактали, до яких належать фрактали Жюліа, Мандельброта та Ньютона. Перш ніж перейти до їх побудови та визначення введемо деякі поняття.

Нерухливою точкою \tilde{z} відображення $z_{n+1} = f(z_n)$ або нерухомою точкою функції $f(z)$ називається корінь рівняння $f(z) = z$. Почавши ітераційний процес у цій точці, ми ніколи її не покинемо. Її ще називають станом рівноваги [1]. За аналогією з трьома типами рівноваги (стійким, нестійким і байдужим) нерухома точка відображення теж буває трьох типів: притягає, відштовхує та нейтрально. Якщо, стартувавши у безпосередній близькості від нерухомої точки, ми в процесі ітерацій до неї необмежено наближатися, то така нерухома точка називається притягує. Стартувавши в безпосередній близькості від відштовхуючої нерухомої точки, ми будемо від неї віддалятися. Нейтральна нерухома точка характеризується тим, що, стартувавши в досить малій її околиці, ми весь час знаходитимемося в цьому околиці, не наближаючись і не віддаляючись від неї. Для визначення характеру нерухомої точки \tilde{z} відображення $f(z)$, використовується похідна $f'(\tilde{z})$.

Теорема 1 (про характер нерухомої точки). Якщо $|f'(\tilde{z})| < 1$, то точка z є притягує, якщо $|f'(\tilde{z})| > 1$, то відштовхує, якщо $|f'(\tilde{z})| = 1$, то нерухома точка \tilde{z} є нейтральною.

При аналізі відображень поруч із нерухомими точками важливу роль грають звані періодичні точки і цикли, що з цих періодичних точок.

Наприклад, цикл періоду два складається з двох точок ξ_1 і ξ_2 таких, що $f(\xi_1) = \xi_2$ і $f(\xi_2) = \xi_1$. Почавши ітераційний процес у одній із точок циклу, ми його будь-коли залишимо і по черзі переходити з однієї точки циклу на іншу. Точки циклу ξ_1 та ξ_2 є нерухомими точками відображення $z_{n+1} = f(f(z_n)) \stackrel{\text{def}}{=} f\{2\}(z_n)$.

Крім циклу періоду два у раціональних відображень існують цикли і всіх вищих порядків з $n = 3, 4, \dots$. Якщо ξ_0 – періодична точка періоду n , то вона є нерухомою точкою функції

$$f(f(\dots(f(z))\dots)) \stackrel{\text{def}}{=} f\{n\}(z). \quad (1.2)$$

Твердження. Якщо точка \tilde{z} є нерухомою для $f(z)$, то вона є нерухомою і для $f\{n\}(z)$.

Атрактором на комплексній площині називається точка, до якої сходиться ітераційний процес $z_{n+1} = f(z_n)$ при $n \rightarrow \infty$. Як такий атрактор може виступати притягує нерухома точка або притягує цикл певного періоду. Іноді таких атракторів може бути кілька, вони також можуть складатися з незліченної кількості точок і являти собою безперервну лінію, так і деяка множина. Якщо ж у процесі ітерацій точка, що зображує їх, йде на нескінченність, то атрактором такого процесу вважається нескінченно віддалена точка.

Множина Жюліа. Багато Жюліа дають найбільш вражаючі ілюстрації того, як простий процес може призвести до надзвичайно заплутаних множин. Ітерації відображення виду $z_{n+1} = f(z_n)$, $n = 0, 1, 2 \dots$ із простою функцією на комплексній площині викликають появу різних екзотичних фракталів. Багато Жюліа функції f – це межа безлічі тих точок z , які при ітеруванні $f(z)$ прагнуть до нескінченності.

Найбільш вивченим прикладом відображень такого виду є квадратичне комплексне відображення $f(z) = z^2 + c$, де $c = a + ib$ – ненульова комплексна константа:

$$z_{n+1} = z_n^2 + c. \quad (1.3)$$

Після поділу речовинної та уявної частин відображення запишеться у вигляді:

$$x_{n+1} = x_n^2 - y_n^2 + a, \quad y_{n+1} = 2x_n y_n + b \quad (1.4)$$

Таке відображення дає безліч фракталів, що відповідають множині Жюліа $J(c)=J(a, b)$.

Нехай значення комплексної константи $c = 0$. У цьому випадку відображення $f(z) = z^2$ має дві нерухомі точки $z_1 = 0$ та $z_2 = 1$, які виходять з рівняння $z^2 = z$. Оскільки $f'(z_1) = 0$, $f'(z_2) = 2$, то перша точка є притягає, а друга – відштовхує теорему про характер нерухомої точки.

Розглянемо ітераційний процес для початкової точки z_0 :

$$z_0 \rightarrow z_0^2 \rightarrow z_0^4 \rightarrow \dots \quad (1.5)$$

Отримуємо геометричну прогресію, для якої залежно від z_0 є три можливості:

1 якщо $|z_0| < 1$, то ітераційний процес сходиться до нуля, тобто $z_1 = 0$ є аттрактором для такого процесу та притягує нерухомою точкою даного відображення;

2 если $|z_0| > 1$, то итерационный процесс сходится к бесконечности. В этом случае аттрактором является бесконечно удаленная точка;

3 якщо $|z_0| = 1$, то початкова точка лежить на колі одиничного радіусу. В цьому випадку і всі точки послідовності продовжують залишатися на цьому одиничному колі.

Таким чином, на комплексній площині є дві області тяжіння. Одна

лежить всередині кола одиничного радіусу, і точки, що їй належать, мають своїм аттрактором $z_1 = 0$ притягуючу нерухому точку. Інша розташована зовні від цього кола і має аттрактором нескінченно віддалену точку. Кордоном між цими двома областями тяжіння є коло одиничного радіусу. Це і є множину Жюлі $J(0,0)$. На ньому лежить друга відштовхувальна нерухома точка квадратичного відображення $z_2 = 1$.

У випадку, коли $c \neq 0$, цілком очікувано, що межа залишатиметься гладкою і матиме форму деформованого кола, а нерухома точка, що притягує, просто переміститься з початку координат. Але інтуїція нас підводить. Наприклад, хай $c = -0.12 + 0.74i$. Тоді в ітераційного процесу $z_0 \rightarrow z_1 \rightarrow z_2 \rightarrow z_3 \rightarrow \dots$ також є три вище наведені можливості. Але межа вже не буде гладкою, вона складається з нескінченного числа деформованих кіл, а внутрішні точки цієї множини притягуються циклом періоду 3, а не однією нерухомою точкою (рисунок 1.10). Кордон безлічі самоподібний і має фрактальну структуру. Трапляється так, що області тяжіння можуть зникнути і зв'язна межа перетворюється на хмару ізольованих точок, які називаються пилом Фату (рисунок 1.11).

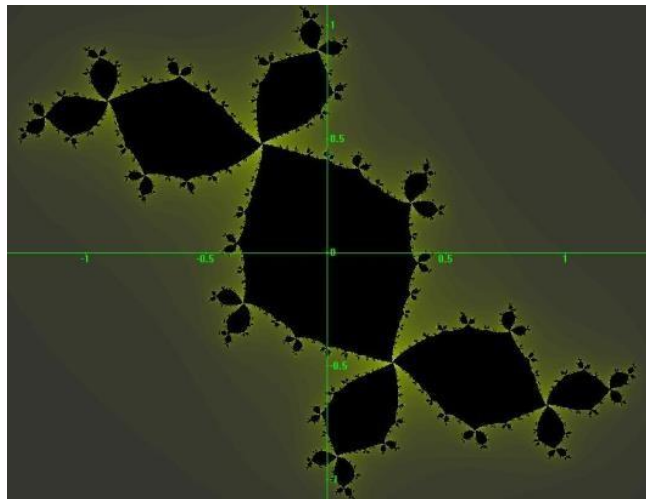


Рисунок 1.10 – Множина Жюліа ($c = -0.12 + 0.74i$)

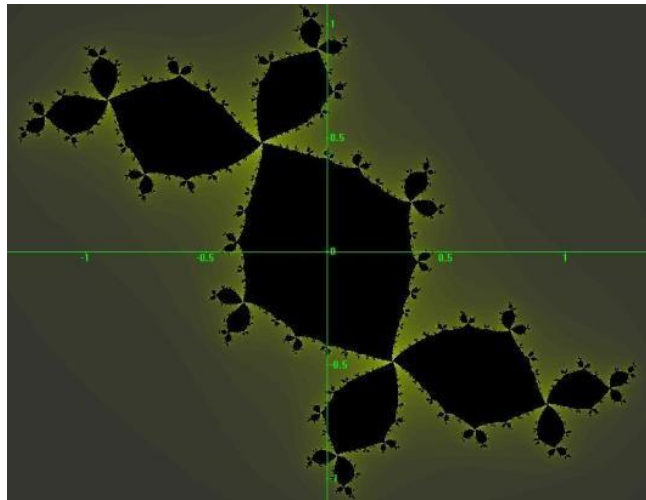


Рисунок 1.11 – Множина Жюліа ($c = -0.12 + 0.74i$)

Вивченням властивостей більш загальному випадку раціональних відображень на комплексній площині займалися французькі математики Гастон Жюліа і П'єр Фату під час першої світової війни. Зокрема, їм було відомо про самоподібність. Так само вони довели, що всю межу можна відновити за будь-якою доволі малою її частиною шляхом кінцевого числа ітерацій формули $z \rightarrow z^2 + c$. На жаль, у той час не було сучасної комп'ютерної графіки, щоб передати їх тонкі ідеї, тому їх дослідження залишилися невідомими для більшості математиків того періоду. І лише завдяки Мандельброту та розвитку комп'ютерної техніки, відродився інтерес до їх результатів. Жюліа докладно досліджував властивості подібних множин, ось деякі з них:

- для кожного значення комплексного параметра $c \in$ множина Жюліа, що обмежує ті області комплексних чисел z_0 , які в процесі ітерацій не йдуть на нескінченність;

- зі зміною константи c змінюється і геометрія меж областей тяжіння, тобто множин Жюліа. Може статися так, що області тяжіння зникнуть і зв'язна межа перетвориться на хмару ізольованих точок – пил Фату;

- фрактали Жюліа завжди симетричні щодо початку координат. Якщо ж $b = 0$, то щодо обох осей абсцис та ординат;

- множина Жюлі є зв'язковим, за винятком пилу Фату.

Жюліа $J(c)$, що обмежує ті області комплексних чисел z_0 , ітераційний процес з яких не йде в нескінченність. Зі зміною c , змінюється і геометрія меж областей тяжіння, отже, змінюються і множини Жюліа, які є фракталами.

Для побудови фракталів Жюліа корисна наступна теорема [2], що у разі $|c| < 2$ дозволяє припинити ітераційний процес, як тільки величини досягають значення 2 за модулем, тому що послідовність ітерацій таких точок гарантовано прагне до нескінченності.

Теорема 2. Нехай $|c| < 2$, $z_n = f\{n\}(z)$ при $n = 1, 2, \dots$, де z - комплексні числа. Якщо існує таке n_0 , Що $|z_{n_0}| \geq 2$, то має місце

$$\lim_{n \rightarrow \infty} z_n = \infty, \quad (1.6)$$

Багато Жюліа навіть для відображення $z^2 + c$ мають велику різноманітність. Для кожного значення c отримуємо нове зображення, проте існує всього два типи множини, що вивчається. Кожна множина Жюліа або складно, або цілком нескладно. Індикатором для двох типів множин Жюліа служить множина Мандельброта, про яку йдеться нижче.

1.4 Стохастичні фрактали

Стохастичні (або випадкові) фрактали також є досить відомим класом. Через велику схожість фракталів цього класу з природними об'єктами їх використовують для моделювання несиметричних рослин, берегових ліній, рельєфу місцевості та поверхні моря.

Приклади стохастичних фракталів:

- траєкторія броунівського руху на площині та у просторі;
- рандомізовані фрактали, що виходять при хаотичній зміні параметрів

в ітераційному процесі.

Одним із типових представників стохастичних фракталів у комп'ютерній графіці є плазма, за допомогою якої можна моделювати ландшафт тощо.

2 ДЕЯКІ ПРОГРАМИ ФРАКТАЛЬНОГО АНАЛІЗУ

2.1 Фрактальні криві та поверхні

Фрактальні ВР, розглянуті на другому розділі – окремий випадок фрактальних кривих, які мають досліджувану величину залежить від часу. Вони широко використовуються при описі та моделюванні різних явищ у різних галузях. Відповідні алгоритми побудови таких кривих докладно описані [3]: алгоритм зміщення середньої точки, метод Фур'є та ін. Цими методами можна отримати фрактальні криві із заздалегідь заданою фрактальною розмірністю, різні способи обчислення якої можна знайти в [3].

В інженерній практиці дуже часто мають справу з поверхнями або поверхневими властивостями у найширшому спектрі контекстів. У деяких випадках мета полягає в тому, щоб зробити поверхню із заданими фізичними або хімічними властивостями, але найчастіше поверхні виникають як невід'ємний прояв певних індустриальних та природних процесів. Процеси формування поверхонь можна віднести до трьох основних типів [4]:

1 процеси, у яких зростання поверхні зумовлено потоками речовини. Приклади: кристалічне зростання, осадження атомного пучка або пари хімічних сполук, відкладення осаду, гальванопокриття, напилення, зростання біологічних організмів типу колоній бактерій та пухлин;

2 процеси, у яких матеріал розчиняється чи видаляється з поверхні. Приклади: хімічне розчинення, корозія, ерозія, вивітрювання, шліфування, багато видів полірування;

3 процеси, що ведуть до спонтанного формування поверхонь та меж розділу. Приклади: тріщиноутворення та руйнування, згоряння та розповсюдження полум'я, турбулентність, змочування, вбирання, інвазія та формування фазових кордонів між різними станами речовини.

Фрактальна геометрія стала використовуватися як у теоретичному, так

і в модельному та експериментальному дослідженні поверхонь. Алгоритми моделювання фрактальних поверхонь із заздалегідь заданими характеристиками (розмірність, показник Херста) детально представлені в [1,2]. В останні роки було опубліковано багато досліджень про фрактальну структуру поверхонь. Фрактальним оголошувалося все – від молекулярних поверхонь білків до злітних смуг аеродромів. Методи фрактального аналізу поверхонь можна знайти у [1]. Зауважимо, що показник Херста в загальному випадку пов'язаний із фрактальною розмірністю співвідношенням: $\infty = *$, де E – евклідова розмірність задачі.

Проблеми формування якості поверхні, і зокрема, такої найважливішої його характеристики як шорсткість, набувають у час особливу актуальність у зв'язку з створенням нових технологій обробки матеріалів [3]. За підсумками проведених експериментів А.А. Потапов вперше запропонував методи оцінок із використанням різних фрактальних характеристик якості поверхні виробів та властивостей мікрорельєфу сучасних конструкційних матеріалів. За словами Потапова А.А., «розробка фрактально-синергетичної моделі процесу формування рельєфу поверхні, заснованої на аналізі закладених у методах групового впливу процесів самоорганізації, дозволить не лише прогнозувати механізми формування шорсткості та фізико-механічних властивостей поверхневого шару, а й керувати ними» [5].

2.2 Рангові розподіли

Ранг у систематиці - це рівень в ієрархічно організованій безлічі елементів. Рангові розподіли застосовуються при аналізі складних багатокомпонентних систем різної природи: соціальних систем (табелі про ранги), систем живих організмів (види, класи, загони, сімейства), техноценозів (номенклатура виробів) тощо. Ранги в систематиці впорядковані значеннями натурального ряду та визначають розбиття системи на компоненти, що характеризуються певним статусом (доходом,

поширеністю, вартістю, споживанням електроенергії тощо). Кожному рангу відповідає певна чисельність його представників, що дозволяє говорити про представленість того чи іншого рангу як функції відповідного йому статусу. У будь-якій системі існують компоненти, порівняно нечисленні, але які мають, у певному сенсі, високий статус, і порівняно численні компоненти з низьким статусом, причому у міру зниження статусу кількість відповідних рангів збільшується. Ціотична парадигма стверджує, що ця залежність носить зазвичай гіперболічний характер

$$P(i) = \frac{P(1)}{i} \quad (2.1)$$

де i – номер рангу;

$P(1)$ – представленість першого рангу. [1]

На таку частотну закономірність вперше звернув увагу стенографіст французького парламенту Ж.-Б. Еступ (1916 р.). У пошуках оптимальних методів стенографії він виявив, що при досить великому обсязі інформації в таких повідомленнях має місце наступна частотна залежність: го слова у словниковому списку. У 1935 р. вийшла монографія американського лінгвіста Дж. Ципфа «Психобіологія мови», в якій наведено змістовне трактування виявленої Еступом залежності: «Слова, що вимагають більше часу для їх прочитання вголос, повинні зустрічатися рідше, ніж короткі, які легко вимовляються». Після виходу книжки ця закономірність стала називатися законом Ципфа. [2]

У 1954 р. Бенуа Мандельброт вніс невеликі зміни до формули Ципфа, досягнувши більш точної відповідності теорії практиці. Пізніше він запропонував його теоретичне обґрунтування, вважаючи, що письмову мову можна порівнювати з кодуванням, причому всі знаки повинні мати певну «вартість». Виходячи з вимог мінімальної вартості повідомлень, Б. Мандельброт математичним шляхом прийшов до аналогічної закону Ципфа

залежності:

$$P(i) = \frac{c}{(a+i)^\gamma}, i=1,2,\dots,n, C, a, \gamma = const \quad (2.2)$$

Ця закономірність відома як закон Ципфа-Мандельброта. З'ясувалося, що закон добре узгоджується з частотними даними окремих літературних творів з точною сюжетною лінією і практично не виконується для частотних даних за довільними лексичними вибірками, що не мають смислової кореляції. Іншими словами, закон Ципфа-Мандельброта виявився законом не мови, а тексту, що представляє окреме семантично-корельоване інформаційне повідомлення [2]. Подібні рангово-статечні закономірності надалі виявили універсальний характер. Наведемо деякі з них.

Популярний в економічній статистиці розподіл італійського економіста та соціолога В. Парето, що описує доходи населення, у ранговій формі також має гіперболічний вигляд (1897):

$$P(i) = (P(1) - b) \left(\frac{a+1}{a+i} \right)^\beta + b, \quad (2.3)$$

де a та b – параметри розподілу. За $b = 0$ співвідношення зводиться до формули Мандельброта [1].

Американський математик А. Лотки показав (1926), що діяльність вчених, що характеризується кількістю їх публікацій, виражається законом Ципфа-Мандельброта з параметрами $\gamma = 0$, $\beta = 2$. Розподіл наукової продуктивності вчених носить асиметричний, нерівномірний. Інваріантність і стійкість закономірності Лотки в багатьох наукових галузях дозволяє говорити про нього як один з найважливіших бібліометричних законів. Докладніше про методи дослідження документальних інформаційних потоків та закономірності, виявлені у світовій системі наукової комунікації, про стохастичну подобу та фрактальність інформаційних масивів можна знайти в

роботах [6, 7].

Німецький географ Ф. Ауербах, аналізуючи чисельність населення міст в адміністративному регіоні, виявив закономірність, аналогічну до закону Ципфа.

Г.Г. Малинецький зазначає, що закономірності Ципфа-Мандельброта спостерігаються у статистиці надзвичайних ситуацій (аварій, повеней, ураганів тощо) з ранжуванням за кількістю загиблих; описують поширення вірусів в Інтернеті та ВІЛ-інфікованого населення; використовуються при побудові прогнозів, мінімізації ризиків для складання тезаурусів пошукових комп'ютерних систем [5-7].

У роботах [8, 9] проілюстровано на прикладах прояв закону Ципфа-Мандельброта у навчальному процесі, зокрема, при аналізі помилок результатів тестування та статистиці професійної спрямованості ЄДІ-респондентів. Природа статечних статистик така, що для них ймовірність рідкісних подій виявляється вищою, ніж для статистик із нормальним законом розподілу. Поведінка такого роду характерна для складних систем, коли одна неординарна подія зумовлює виникнення довгих причинно-наслідкових кореляцій, що породжують лавину змін (не виключаючи катастрофічний сценарій), за допомогою яких система набуває нової якості. У системі ЄДІ рідкісні події обумовлені вибором ЄДІ-респондентами профільного предмета, що цікавить, на основі індивідуальних переваг, що відбивається на статистиці з профільних предметів.

Гіперболічна рангова параметризація складних ієрархічних структур пов'язана з їх самоподібністю. Цей зв'язок показаний у роботі [10] з використанням екологічної фразеології та інструментарію мультифрактального формалізму.

2.3 Фрактальна графіка та обробка зображень

Фрактали часто використовуються для створення різноманітних візуалізацій, відеоінсталяцій, створення спецефектів у комп'ютерній графіці. У багатьох іграх, де присутні різні природні ландшафти, використовуються фрактальні алгоритми. Цей метод досить ефективно зарекомендував себе. Оскільки справжні природні об'єкти мають основу своєї фрактальної структури, програмісти успішно створюють комп'ютерні ландшафти з урахуванням фрактальних алгоритмів. Більше того, на сьогоднішній день існує велика кількість програм для генерації ландшафтів і пейзажів.

Той самий принцип, як і в іграх, використовують у кіно для створення різних фантастичних пейзажів за допомогою комп'ютерних програм, що працюють на фрактальних алгоритмах. Цікавий факт: у відомому космічному фільмі Рідлі Скотта "Чужий" в епізоді, коли команда спускається на поверхню планети, монітор у кораблі передає зображення поверхні планети у вигляді сітки. Саме це зображення було отримано за допомогою фрактальної геометрії. Фрактальна геометрія дозволяє художникам за спецефектами легко створювати такі об'єкти як хмари, дим, полум'я, зоряне небо та ін. Фрактальні зображення, змодельовані в різних генераторах, надзвичайно красиві. Що вже тоді говорити про фрактальну анімацію – це справді приголомшливе видовище. Фрактальну анімацію з успіхом застосовують віджеї у відеосетах за допомогою так званих програм віджеїнгу.

Фрактали чудово зарекомендували себе при обробці зображень, покращенні якості та чіткості зображення. Фрактальне оброблення зображень набагато покращує розпізнання об'єктів на фотографіях та інших зображеннях для будь-якої області її застосування.

В Інституті радіотехніки та електроніки (ІРЕ) створені ефективні методи вимірювання фрактальних характеристик (фрактальних сигнатур) та обробки зображень, які широко застосовуються у різних фізико-технічних, астрономічних, біологічних, медичних тощо. дослідженнях. Зокрема, за

допомогою синтезованих фрактальних алгоритмів вдається виділити номери автомобілів, оптичні зображення яких отримані в умовах сильних перешкод (пил, дим, туман). Вперше запропоновані та розроблювані науковою школою Потапова О.О. цифрові фрактальні методи дозволяють частково долати апріорну невизначеність у радіолокаційних задачах за допомогою інформації про геометрію (топологію) вибірки – одномірну або багатовимірну. У методах фрактальної обробки необхідний облік скейлінгових ефектів реальних радіосигналів та електромагнітних полів. Запропоновані фрактальні методи суттєво доповнюють текстурні та дозволяє більш надійно робити операцію кластеризації. Після цифрової фрактальної обробки зображень поверхні, крім сталого поділу за типами земних покривів, відзначаються невидимі (приховані) до цієї обробки особливості: наприклад, дані кластеризації дистанційного зондування різних земних покривів. Це відзначаються невидимі (приховані) до цієї обробки особливості: наприклад дані кластеризації дистанційного зондування різних земних покривів. Це відзначаються невидимі (приховані) до цієї обробки особливості: наприклад дані кластеризації дистанційного зондування різних земних покривів . Це

дозволяє говорити про застосування створених методів фрактального розпізнавання для ідентифікації ділянок зображення, «невидимих» за класичних методів кластеризації по полю яскравостей. Експериментально також доведено можливість ефективної кластеризації однорідних протяжних зв'язкових областей за допомогою фрактальної фільтрації. Цікаві приклади з цифрової фрактальної обробки зображень можна знайти в [2-4]: стелс-об'єкти, медичні зображення та ін.

2.4. Фрактальна криптографія

В багатьох роботах пропонує ітераційно-функціональний підхід до використання алгебраїчних фракталів у шифруванні переданих даних. Пропонований підхід є варіантом гамування – процесу «накладання» гамма-

послідовності на відкриті дані, де як таку послідовність псевдовипадкових елементів використовується фрактальна послідовність. Ключовою проблемою технічних засобів захисту є породження дійсно випадкової послідовності бітів. Застосування шумоподібних систем, заснованих на фрактальних сигналах, дає потенційну перевагу над традиційними системами псевдовипадкових послідовностей.

Алгоритм фрактального шифрування (для зображення):

1 зображення має бути представлене потоком бітів;

2 ключ формується наступним чином: вибирається вид фракції алгебри; вказується кількість ітерацій та параметри для функції кольору; визначається масштаб і розміри зображення, що шифрує (вони повинні співпадати з вихідним зображенням);

3 на основі цих даних будується ітераційний фрактал (шифрує зображення), який представляється як потоку бітів;

4 потім, застосовуючи деяку оборотну функцію до пар значень точок вихідного зображення та зображення побудованого фрактала, виходить нове зображення, яке передається по каналу зв'язку.

Для розшифровки повідомлення потрібно, знаючи початкові значення процедури побудови фрактальної послідовності, відновити зображення фрактала і, застосовуючи операцію, зворотну по відношенню до операції сторони, що передає, відновити вихідне зображення.

Цей метод застосовується для будь-яких типів даних. При цьому послідовність кодів символів (текст) або відліків деякої фізичної величини (звук), що шифрується, розташовується по рядках прямокутної матриці, після чого застосовують описаний вище метод. Фрактальне шифрування також демонструє можливість передачі додаткової інформації без збільшення обсягу даних, що передаються. При оптимальному виборі початкових умов ітераційного процесу використання асиметричного фрагмента фрактала можна забезпечити значимість всіх бітів обраного ключа під час операції шифрування. Отриманий сигнал складно відрізнити від шуму, до того ж, для

розшифровки необхідно знати конкретний вид динамічної системи та початковий параметр процесу.

Фрактали за невеликою кількістю початкових даних дозволяють отримувати псевдовипадкову числову послідовність, сучасні методи криптоаналізу якої на сьогоднішній день не дадуть високого результату. У той самий час, знаючи вихідну ітераційну функцію та її початкові параметри, шифрування і дешифрування секретних повідомлень проводиться шляхом нескладних обчислень, що дозволяє реалізації цього методу без особливих проблем. У статті [11] використовуються фрактальні зображення як секретні ключі при впровадженні цифрових водяних знаків у зображення.

Фрактали в алгоритмах шифрування застосовуються для:

- підвищення стійкості алгоритму рахунок можливості генерації ключа необмеженої довжини;
- генерації псевдовипадкових послідовностей;
- реалізації шифрів підстановки та шифрів заміни;
- реалізації візуальної криптографії різних зображень.

В даний час фрактальні послідовності використовуються при шифруванні зображень, а також у різних методах ідентифікації табіометричного шифрування: сканування відбитка пальця, сітківки та райдужки ока, лінії руки, обличчя та ін.

2.5 Фрактальні мережі та лабіринти

Фрактальні лабіринти зустрічаються у природі та техніці повсюдно [1]. Це транспортні та комунікаційні мережі, фільтраційні канали, системи збирання та розподілу ресурсів та інформації, річкові системи, системи кровопостачання, блискавкові розряди тощо. Відомо, що щільність фрактальних структур зменшується за статечним законом зі зростанням їх лінійних розмірів. Завдяки цьому транспортні властивості фрактальних мереж помітно відрізняються від регулярного випадку. Також у сфері

мережових технологій було проведено безліч досліджень, що показують самоподібність трафіку, що передається мережами різного роду. Особливо це стосується мовних, аудіо та відео сервісів. Тому зараз ведуться розробки та дослідження можливості фрактального стиснення трафіку з метою більш ефективної передачі інформації.

При проектуванні, запуску та експлуатації телекомунікаційних мереж однією з основних проблем є завдання забезпечення якості обслуговування. Донедавна вирішення такого завдання під час проектування систем розподілу інформації забезпечувала теорія телетрафіку. Вона є однією з гілок теорії масового обслуговування і з'явилася в результаті досліджень А.К. Ерланга, Т. Енгсета, Г.О. Делла, К. Пальма, А.Я. Хінчина та інших. Теорія масового обслуговування добре визначає процеси, які у таких системах розподілу інформації, як телефонні мережі, побудованих за принципом комутації каналів. Найбільш поширеною моделлю потоку викликів (даних) теоретично телетрафіку є найпростіший потік (стаціонарний, ординарний потік без післядії). Справжній період бурхливого розвитку високих технологій привів до появи і поширення мереж з пакетною передачею даних, які поступово стали витіснити системи з комутацією каналів, але ті, як і раніше, проектувалися на основі загальних положень теорії телетрафіку.

Проте, в 1993 р. група американських дослідників W. Leland, M. Taqqu, W. Willinger та D. Wilson опублікували результати своєї нової роботи, яка докорінно змінила існуючі уявлення про процеси, що відбуваються в телекомунікаційних мережах з комутацією пакетів. Ці дослідники вивчили трафік в інформаційній мережі корпорації Bellcore і виявили, що потоки в ній не можна апроксимувати найпростішими потоками, тому що вони мають зовсім іншу структуру, ніж у класичній теорії телетрафіку. Зокрема, було встановлено, що трафік такої мережі має властивість самоподібності., тобто виглядає якісно однаково при майже будь-яких масштабах тимчасової осі, має пам'ять (наслідок), а також характеризується високою пачечністю. В результаті теоретичний розрахунок параметрів системи розподілу інформації,

призначеної для обробки такого трафіку, за класичними формулами дає некоректні та не виправдано оптимістичні результати. Більш того, звичні алгоритми обробки трафіку, створені для роботи з найпростішими потоками, є недостатньо ефективними для потоків із самоподібністю. Проблемі самоподібності телетрафіку за останні роки присвячено тисячі робіт, і вона досі не втратила своєї актуальності. Згадаймо лише деякі з них, не претендуючи на повноту огляду.

У книзі [12] розглянуто основи теорії фрактальних стохастичних процесів. На основі реальних змін трафіку телекомунікаційних мереж сформульовано математичні моделі цих процесів.

У роботі [13] були проведені дослідження сумарного мережевого трафіку, що передається, і відповідних апаратних процесів сервера мережі університету. Для всіх процесів було встановлено самоподібність і розрахований показник Херста, що характеризує довгострокову пам'ять тимчасового ряду. На основі цього робиться висновок про можливість подальшого застосування фрактальних моделей для роботи з даними, у тому числі використання методів прогнозування. Показником цієї пам'яті є коефіцієнт Херста H – міра самоподібності або статистичної інерції процесу.

Інтерпретація показника Херста тут така:

- $H = 0,5$ - має на увазі білий шум, тобто трафік представляє незалежний, випадковий процес;

- $0,5 < H < 1$ означає чорний шум або персистентність трафіку. Трафік характеризується ефектом довготривалої пам'яті і має схильність до трендів (добре передбачуваний).

Оцінка якості обслуговування є одним із найважливіших завдань при створенні та конфігуруванні сучасних систем телекомунікації. Протягом багатьох років при аналізі потоків «голосових» і текстових повідомлень успішно використовувалися марківські процеси, що у багатьох випадках дозволяють отримати явні формули для розрахунку стаціонарних характеристик продуктивності в моделях. Однак інформація в сучасних

системах телекомунікації має складну структуру, кардинально відмінну від звичайної телефонії або поштових сервісів. У роботі [13] отримано оцінку для ймовірності переповнення великого буфера для неоднорідної моделі вхідного трафіку.

2.6 Фрактали у технічних науках

У телекомунікаціях фрактали використовують для створення фрактальних антен. Фрактальні антени - відносно новий клас електричних малих антен (ЕМА), що відрізняється своєю геометрією від відомих рішень. Традиційна еволюція антен базувалася на евклідовій геометрії (лінія, коло, еліпс, параболоїд тощо). Фрактальна антена з напрочуд компактним дизайном забезпечує чудову широкосмугову продуктивність у маленькому форм-факторі. Досить компактні для встановлення або вбудовування у різних місцях, фрактальні антени використовуються для морських, повітряних транспортних засобів або мобільних телефонів.

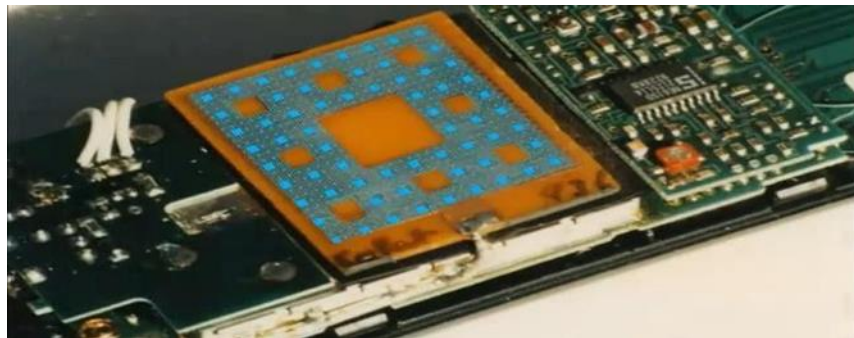


Рисунок 2.1 – Антена на основі килима Серпінського

Антенні пристрої та частотно-вибірчі поверхні (ЧП) є невід'ємною частиною радіосистеми. Досвід аналізу та синтезу фрактальних антен доводить їх ефективність при розробці багаточастотних радіолокаційних та телекомунікаційних систем. Області застосування фрактальних антен:

сучасні телекомунікації, шумова радіолокація, нелінійна радіолокація, системи пошуку, локалізації та трасування мобільних об'єктів, пеленгація у складних міських умовах, визначення місця розташування несанкціонованих джерел радіовипромінювання під час боротьби з терористами, оперативний зв'язок у військах, маркери на різних предметах, космічний зв'язок, сучасний фізичний експеримент тощо. Унікальною особливістю фрактальних антен є теоретично нескінченне ущільнення обмеженої області простору геометрій антени, і як результат – додаткові резонансні частоти в діапазоні довжин хвиль, які часто значно перевищують геометричні розміри фрактальної структури. На сьогоднішній день не існує суворої електродинамічної теорії, яка пояснює і передбачає досить унікальні властивості структур, побудованих на основі фрактальних множин [14]. Але всі спроби використовувати геометричні фрактали в реальних завданнях радіофізики мають на увазі обмеження кількості ітерацій побудови фракталу, тобто використання передфракталу (рисунок 2.2).

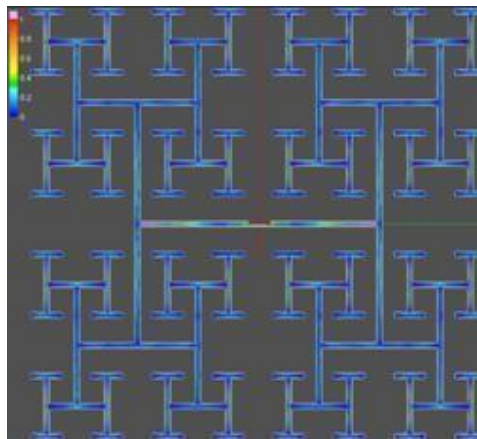


Рисунок 2.2 – Розподіл струмів за фрактальною антеною «Дерево Кейлі»

При розробці сучасних радіопоглинаючих покриттів та матеріалів, які повинні забезпечувати поглинання широкого спектра електромагнітного випромінювання при довільних кутах зондування та поляризації падаючого випромінювання, перспективне застосування фрактальних штучних

композитів та метаматеріалів. Крім прямого призначення, вони можуть мати різноманітне функціональне призначення і їх відносять до «інтелектуальних» або «розумних» матеріалів. Застосування рекурсивного процесу дозволяє створювати самоподібну ієрархічну структуру, аж до окремих провідних доріжок у мікросхемі та в наноструктурах. При цьому необхідно враховувати та навчитися розраховувати взаємний та колективний вплив усіх електромагнітних полів з усіма компонентами мікросхеми: провідні доріжки, напівпровідник, діелектрик тощо.

Фрактальні фотонні і магнонні кристали мають цілу низку переваг перед своїми класичними аналогами і є важливо новими середовищами передачі інформації. Традиційні матеріали з фотонними забороненими зонами використовують брегівське розсіювання, щоб створити заборонені зони. Природним наслідком брегівського механізму розсіювання є те, що товщина та поперечні розміри фотонних кристалів мають становити кілька довжин хвиль. Застосування планарних фракталів, що проводять, дає можливість створювати складні відбивають і пропускають зони в широкому діапазоні частот. У цьому випадку фрактальна структура може бути надхвильовою. При конструюванні фрактальних фотонних і магнонних кристалів зручні детерміновані геометричні фрактали, які мають прогнозовані характеристики і можуть бути досить просто згенеровані. Аналіз результатів чисельного моделювання показав, що електромагнітна хвиля збуджує струми в металевих провідниках фрактала, амплітуда яких досягає максимуму в діапазоні частот, що сильно відображають. Крім того, такі фрактальні структури можна використовувати як радіолокаційні екрани, спотворюють радіопортрети досліджуваних об'єктів.

Міліметрові хвилі (ММВ) активно взаємодіють з газами земної атмосфери, особливо з киснем та водяною парою, а також з гідрометеорними утвореннями, до яких належать дощі, хмари, снігопади тощо. В результаті цієї взаємодії ММВ сильно поглинаються та розсіюються в тропосфері. Для завдань Потапов А.А. запропонував такі основні шляхи: а) мініатюрні

фрактальні антени; б) фрактальні структури у фотонних та магнонних кристалах; в) фізичне моделювання фрактальних імпедансів та дробових операторів; г) перколяційний синтез наноструктурованих композитів тощо. Моделі утворення фрактальних кластерів використовуються для створення та аналізу матеріалів із незвичайними фізичними властивостями.

3 ВИКОРИСТАННЯ ФРАКТАЛІВ У КРИПТОГРАФІЇ

3.1 Огляд існуючих методів

Використання теорії фракталів у криптографії є новим напрямом, якому присвячені такі роботи.

Основний принцип симетричного шифрування з використанням фракталів розглянуто у статті Куклешова С.В. "Фрактальне шифрування".

У статті Yuanyuan Sun, Lina Chen, Rudan Xu, Ruiqing Kong. "An Image Encryption Algorithm Utilizing Julia Sets and Hilbert Curves" розглянуто спосіб шифрування зображень за допомогою кривої Гільберта та безлічі Жюлія.

Застосування фракталів для систем з асиметричним шифруванням розглянуто в статтях Shafali Agarwal, Ashish Negi "Key greyment protocol based on superior fractal sets" та Ojha DB, Shree Ms., Dwivedi A., Mishra A. "An ap-proach for Embedding" elliptic curve в fractal based digital signature scheme».

3.2 Метод шифрування зображень за допомогою фракцій алгебри

Метод шифрування зображень за допомогою фракцій алгебри можна представити наступними етапами.

1 Етап. Зображення має бути представлене потоком бітів. (Кожний піксель займає 3 байти пам'яті і його можна представити у вигляді беззнакового цілого в діапазоні від 0 до 16777215, а потім це значення переводиться в 24-бітне двійкове число.)

2 Етап. Ключ формується так:

2.1 вибирається вид фракції алгебри;

2.3 якщо вибрано множину Жюлі, то задається константа;

2.3 вказується кількість ітерацій та параметри для функції кольору;

2.4 визначається масштаб (що більша кількість ітерацій і чим сильніше

наближення, тим цікавіша та складніша структура фракталу, що добре відображається на шифруванні) та розміри шифруючого зображення (вони повинні співпадати з вихідним зображенням).

3 Етап. На основі цих даних створюється шифруюче зображення, яке так само, як і шифрується, представляється у вигляді потоку бітів.

4 Етап. Виконується операція XOR між зображенням, що шифрується і шифрує, і потік бітів назад переводиться в пікселі, виходить первинне зашифроване зображення.

5 Етап. До отриманого зображення застосовується алгоритм дифузії, який можна подати за такою формулою:

$$c_i = c_{i-1} \oplus c'_{i+1}, i = 1, \dots, N, \quad (3.1)$$

де c - це пікселі підсумкового зашифрованого повідомлення;

c' - первинного;

N - загальна кількість пікселів. Значення є ключем процесу дифузії.

3.2 Метод шифрування текстів за допомогою алгебраїчних фракталів

Метод шифрування текстів за допомогою алгебраїчних фракталів можна представити наступними етапами.

1 Етап. Кожен символ тексту займає 1 байт пам'яті, тобто його можна уявити двійковою восьмибітовою послідовністю.

2 Етап. Ключ формується так само, як і при шифруванні зображення (тут, кількість пікселів має бути більшою або дорівнює кількості символів у тексті).

3 Етап. Оскільки піксель кодується 3 байтами, а символ лише одним (і тому зробити операцію XOR стає проблематично) можливі наступні варіанти:

3.1 піксель шифруючого зображення відповідно до RGB моделі

розпадається на три компоненти по одному байту: Red(r_i), Green(g_i) і Blue(b_i), $i = 0, \dots, 7$. Далі виконується логічна операція AND (І) між непарними бітами Red і Green, і між парними бітами Red і Blue. Цей процес відображено у формулі (10):

$$a_i = \begin{cases} r_i \& g_i, i = 1, 3, 5, 7 \\ r_i \& b_i, i = 0, 2, 4, 6 \end{cases} \quad (3.2)$$

3.2 виконується операція XOR між бітами Red(r_i), Green(g_i) і Blue(b_i), $i = 0, \dots, 7$.

4 Етап. Завдяки проведеним перетворенням, виходить необхідна шифруюча послідовність, між якою і потоком бітів тексту, що шифрується, проводиться операція XOR. Потім біти переводять у символи, і виходить шифротекст.

Оскільки запропоновані алгоритми є симетричними, дешифрація даних проводиться у зворотному порядку з тим самим ключем.

4 ЕКСПЕРИМЕНТАЛЬНА ЧАСТИНА

4.1 Побудова фракталів

Програма побудови фракцій алгебри була написана мовою C/C++ з використанням графічної бібліотеки OpenGL, вершинного і піксельного шейдерів – комп'ютерних програм, що виконуються на відеокарті. Лістинг програми наведено у додатку Б.

Програмна реалізація фракталів була виконана на основі алгоритмів, наведених у розділі 1

Результат роботи програми для множини Мандельброта при виконанні 100 ітерацій з градієнтною заливкою від бірюзового кольору до синього представлений на рисунку 4.1. Опис роботи функції кольору наведено в Додатку Б.

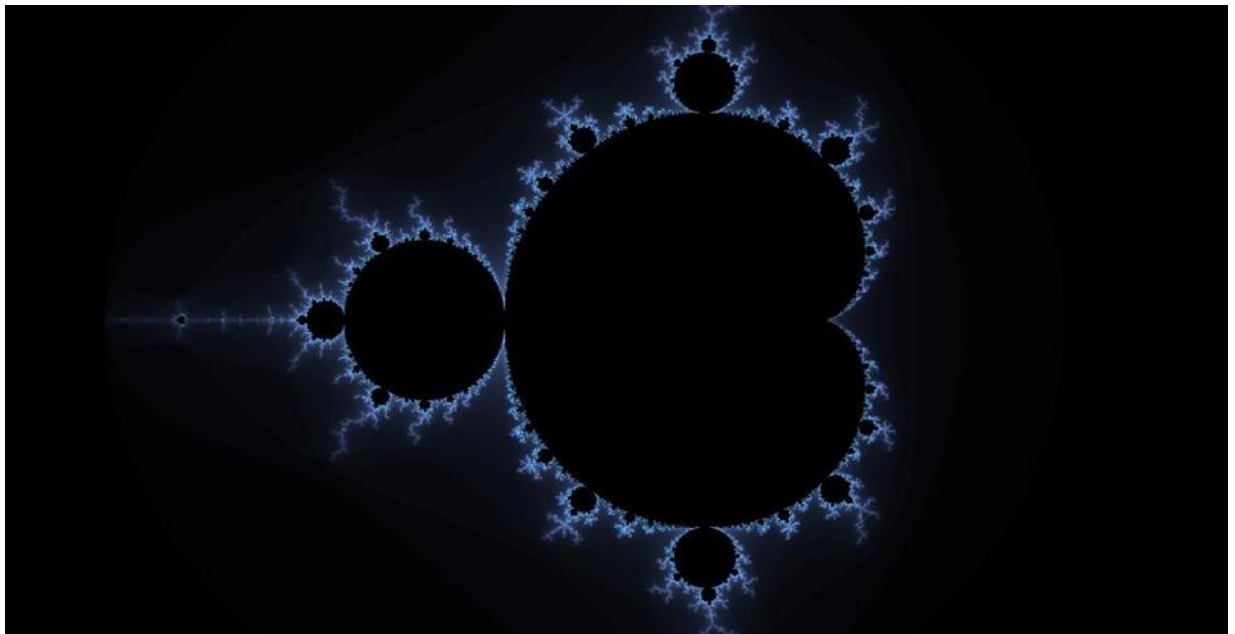


Рисунок 4.1 – Множина Мандельброта (100 ітерацій)

На рисунку 4.2 фрактал показаний при семиразовому збільшенні для

100 ітерацій. На рисунку 43 фрагмент множини представлений при одинадцятикратному збільшенні, але вже для 500 ітерацій.

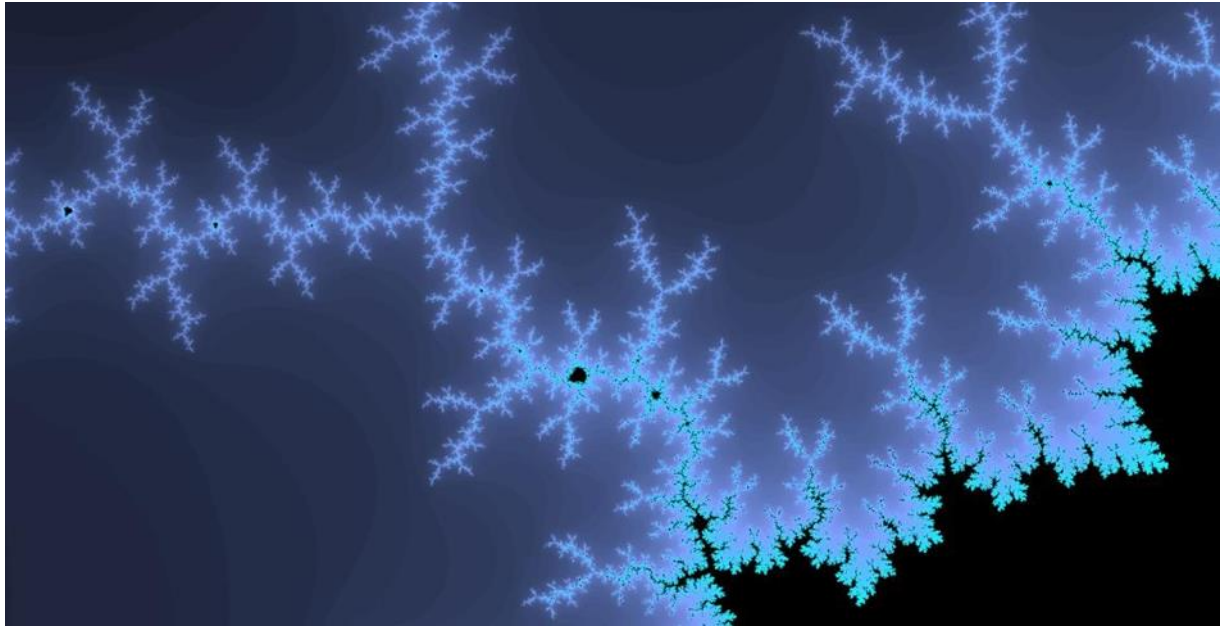


Рисунок 4.2 – Фрагмент множини при семикратному збільшенні (100 ітерацій)

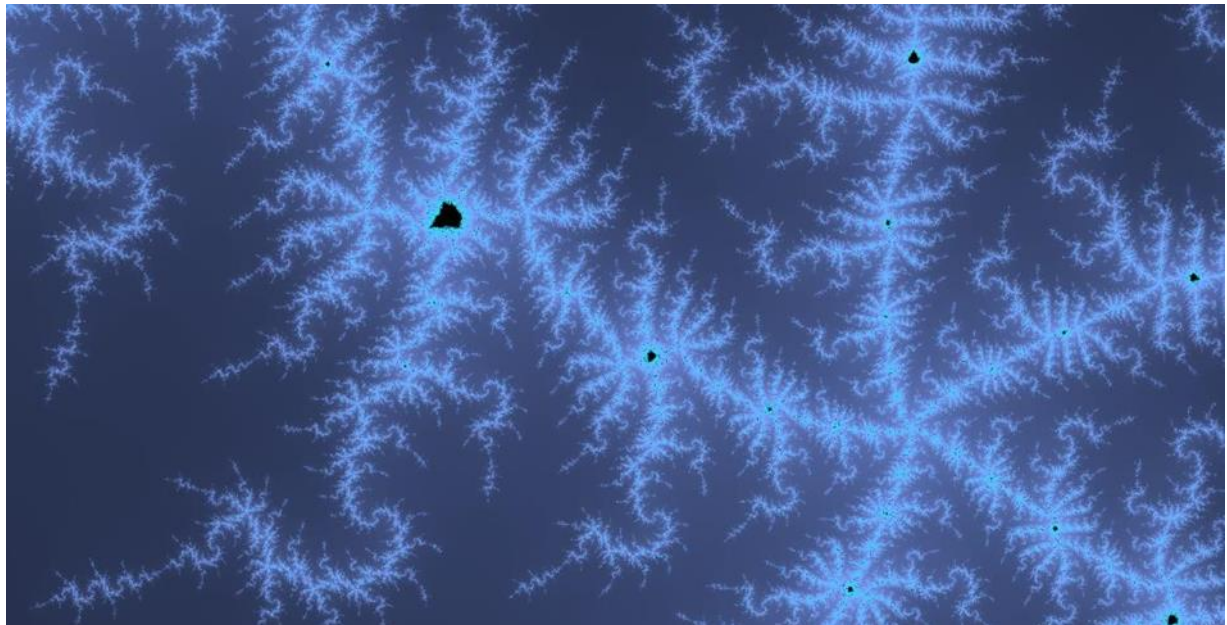


Рисунок 4.3 – Множина при одинадцятикратному збільшенні (500 ітерацій)

Чим більше буде виконано ітерацій, тим більш точне графічне уявлення фракталу можна отримати і тим більше його наблизити. Але велика кількість ітерацій потребує величезних обчислювальних потужностей. Найоптимальнішим варіантом є використання 100-500 ітерацій, починаючи від 1000 ітерацій, сильно збільшується час роботи програми.

Множина Жюлі будується за тим же принципом, що і множина Мандельброта, але вже з фіксованою константою c . На рисунку 4.4 представлено множина Жюліа для полінома другого ступеня $z^2 - 0,7382 + 0,0827i$ відповідно $c = 0,7382 + 0,0827i$ з градієнтом від синього до червоного. На рисунку 4.5 показаний фрагмент множини при чотириразовому збільшенні для 500 ітерацій.

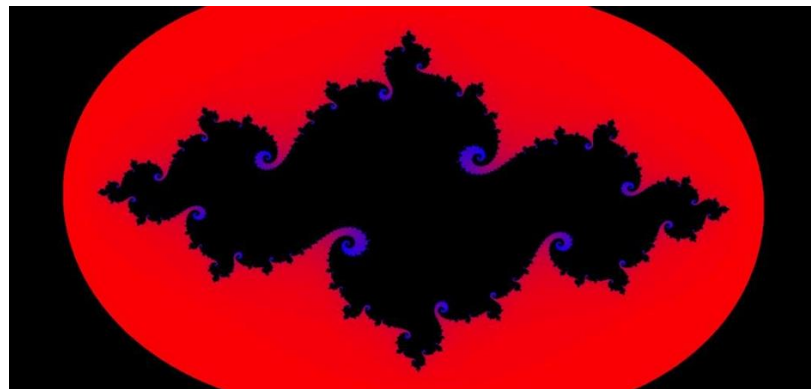


Рисунок 4.4 – Множина Жюліа (500 ітерацій)

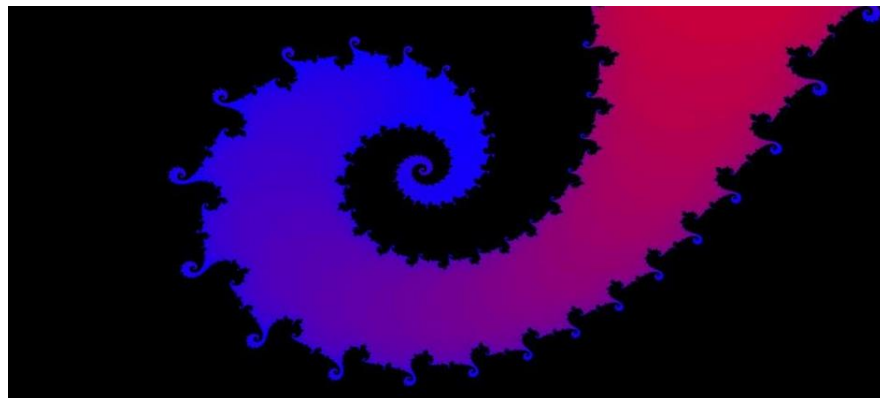


Рисунок 4.5 – Множина Жюліа при чотириразовому збільшенні (500 ітерацій)

Якщо змінити константу на значення $c = -0,20 + 0,827i$, а червоний замінити синім, отримаємо Множина Жюліа, показане рисунку 4.6. На рисунку 4.7 зображено фрагмент множини при шестикратному збільшенні.

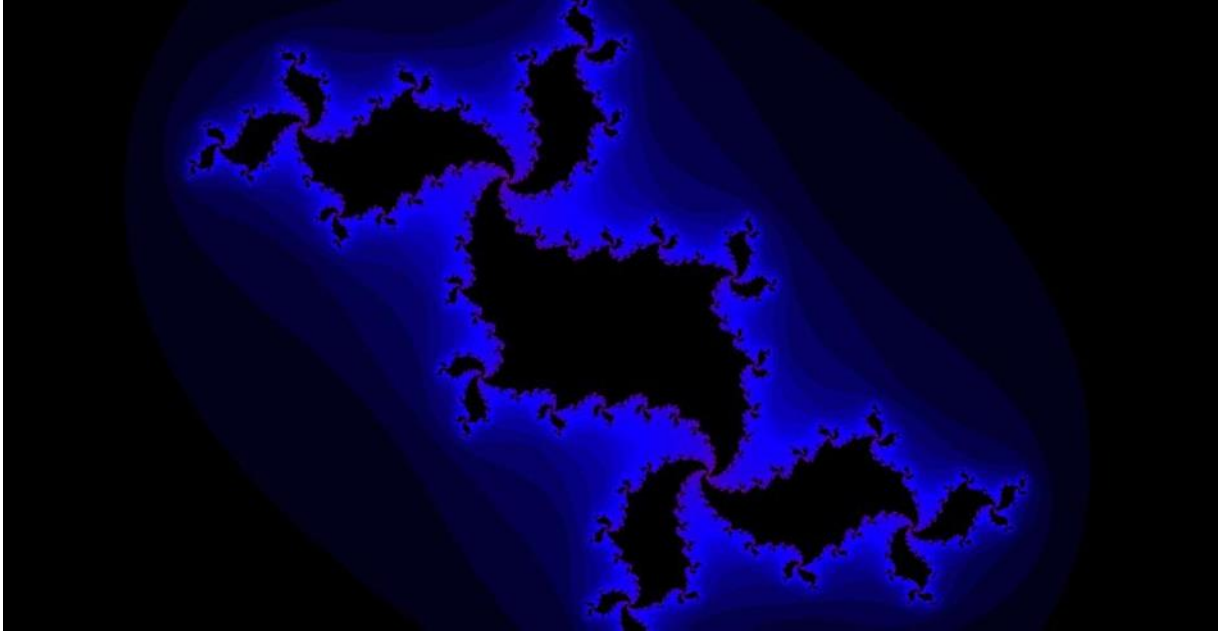


Рисунок 4.6 – Множина Жюліа (500 ітерацій)

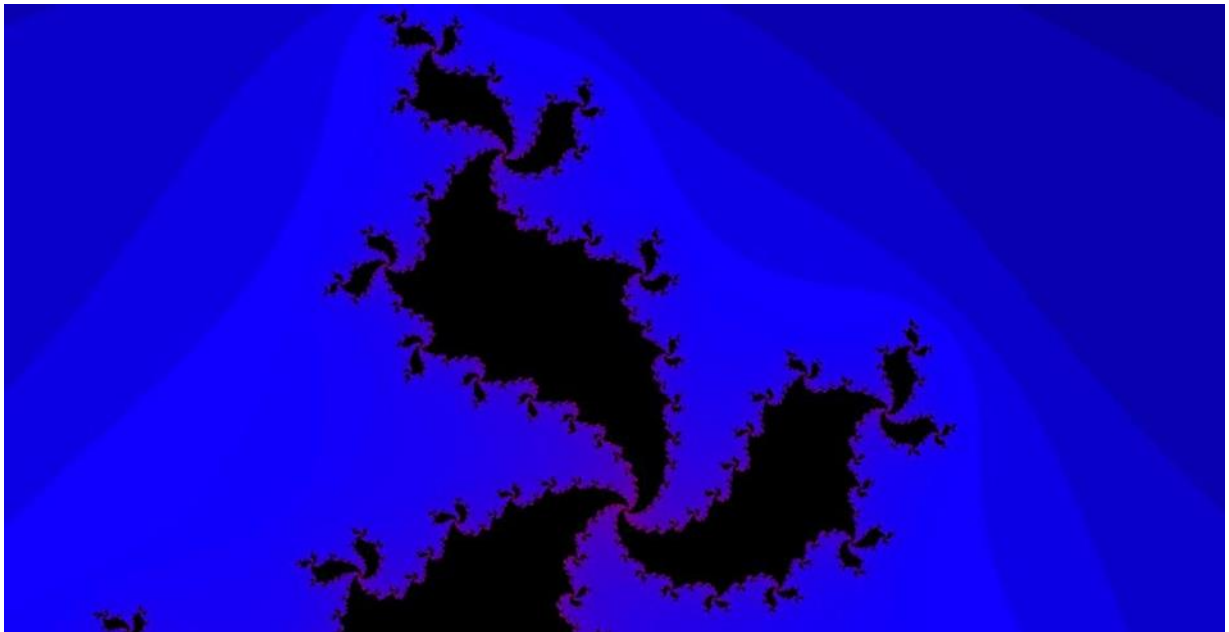


Рисунок 4.7 – Множина Жюліа із шестикратним збільшенням (500 ітерацій)

При значенні константи рівному $c=0,8i$ виходить один із варіантів нескладного Множина Жюліа (рисунок 4.8). Якщо збільшити кількість ітерацій до 700, то при семикратному масштабуванні отримаємо зображення, представлено на рисунку 4.9.

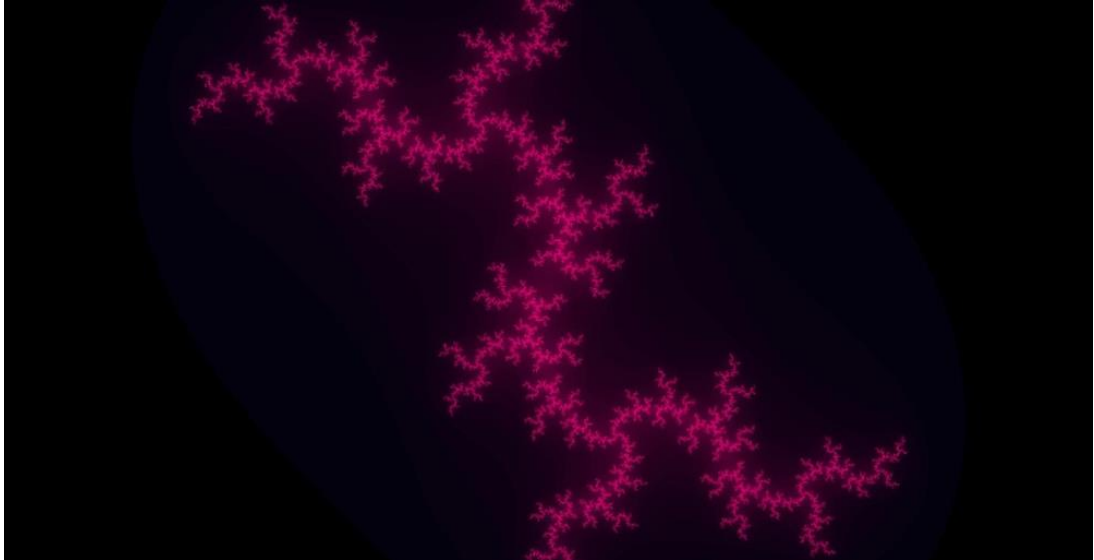


Рисунок 4.8 – - Нескладна множина Жюліа (600 ітерацій)



Рисунок 4.9 – Множина Жюліа із семикратним збільшенням (700 ітерацій)

Басейни Ньютона для багаточлена третього ступеня z^3-1 четвертого

ступеня z^4-1 представлені на рисунках 4.10 та 4.11

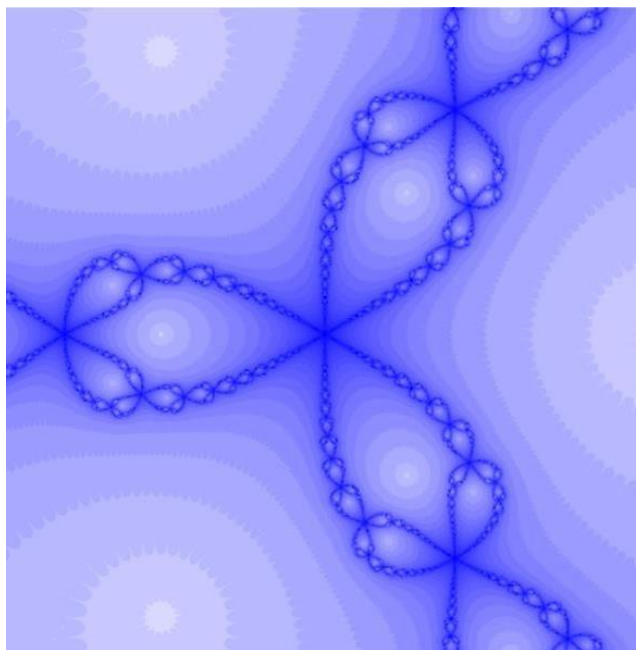


Рисунок 4.10 – Басейни Ньютона для багаточлена третього ступеня

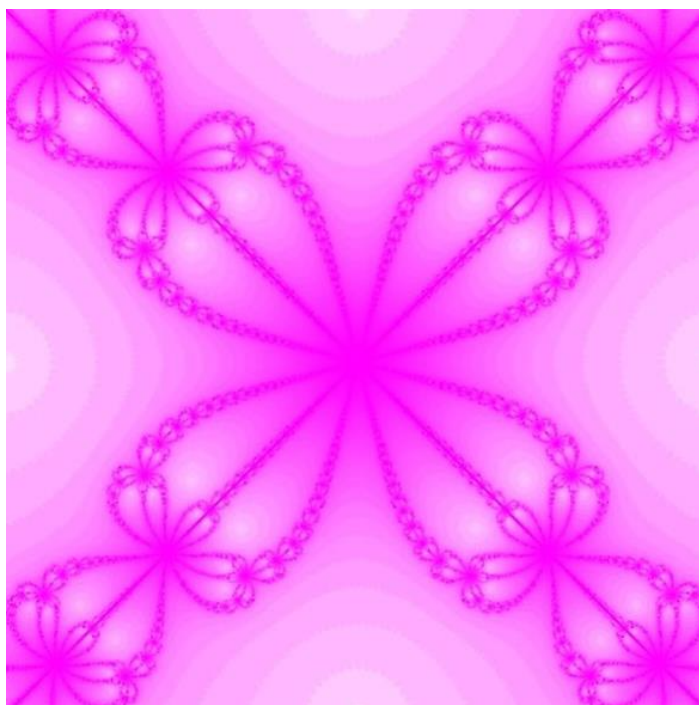


Рисунок 4.11 – Басейни Ньютона для багаточлена четвертого ступеня

4.2 Шифрування та дешифрування зображень

На основі алгоритму, представленого в розділі 3.2, мовою C/C++ з використанням графічної бібліотеки `gl` із зібрання бібліотек `boost` була написана програма для шифрування та дешифрування зображень формату `png`. Лістинг програми наведено у додатку В.

Розглянемо таке зображення (рисунок 4.12).



Рисунок 4.12 – Відкрите зображення (ілюстрація)

Як шифруюче зображення був використаний фрагмент фракталу Мандельброта при 200 ітераціях з червоним параметром кольору та п'ятикратним збільшенням (рисунок 4.13).

Результат, отриманий після виконання алгоритму 3.2 (тобто виконання операції XOR між вихідним зображенням та фракталом та застосування

алгоритму дифузії (8)) наведено на рисунок 4.14.

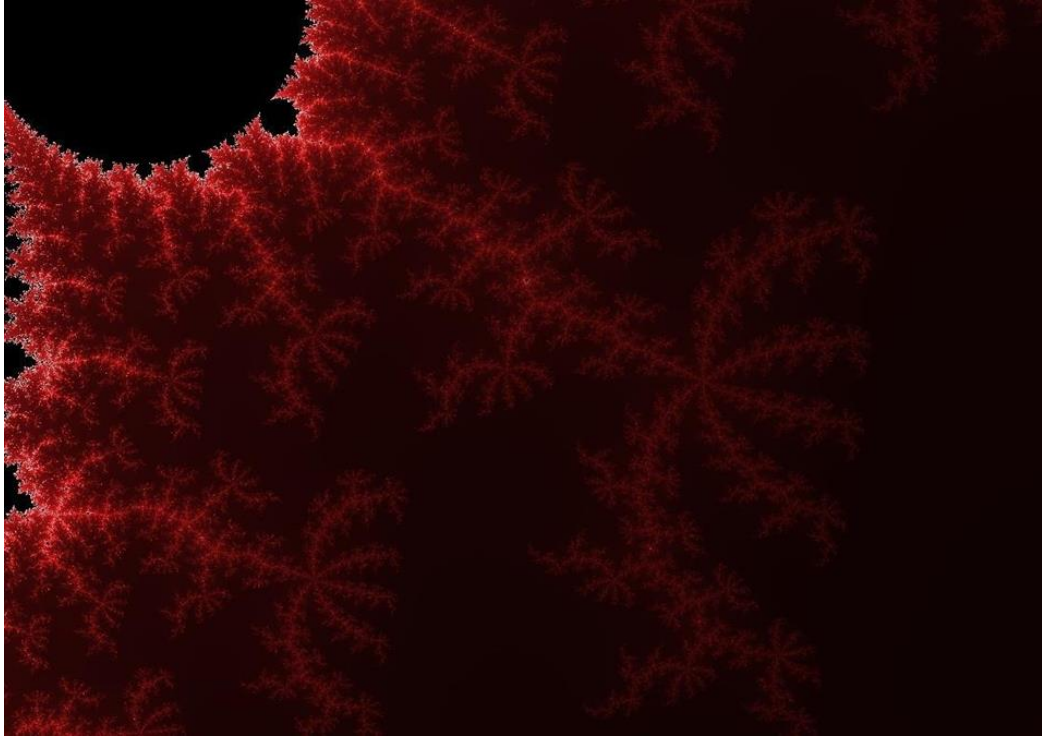


Рисунок 4.13 – Відкрите зображення (ілюстрація)

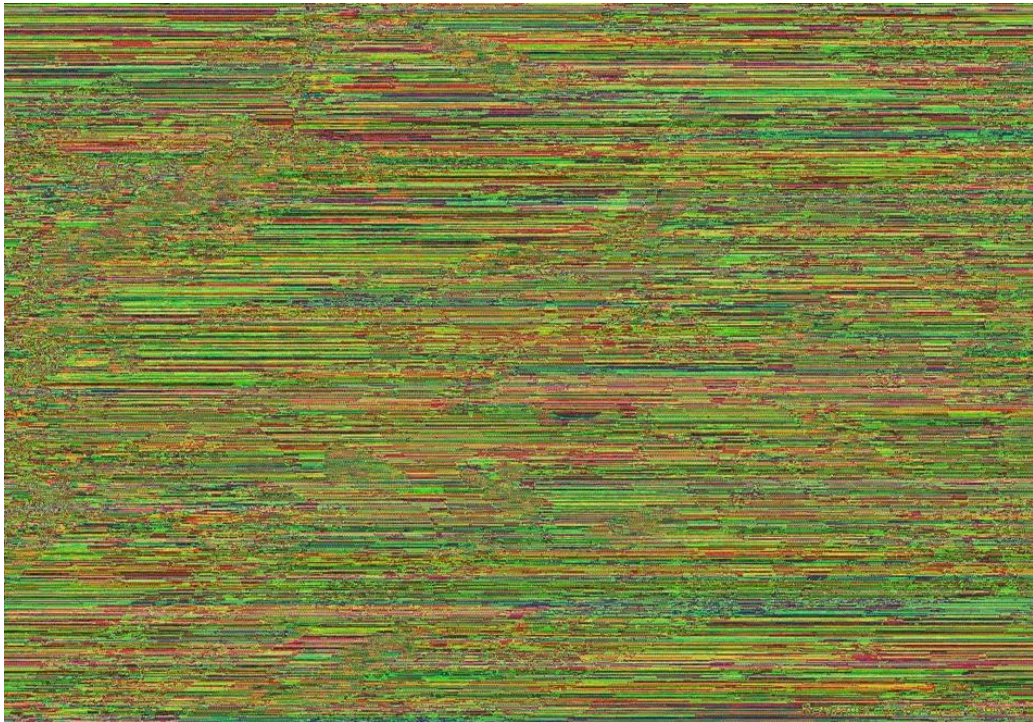


Рисунок 4.14 – Зашифроване зображення

Зображення, отримане при дешифрації, наведено рисунок 4.15.



Рисунок 4.15 – Зображення після дешифрації

Розглянемо інший тип відкритого зображення – нотну сторінку, що містить також текстову інформацію (рисунок 4.16).

Як шифруючий зображення знову був використаний фрактал Мандельброта (рисунок 4.17 – фрагмент рисунок 4.3, з тими ж параметрами).

Отримане зашифроване зображення представлено рисунок 4.18, а дешифроване рисунок 4.19.

Як і в попередньому прикладі, при дешифрації з'являється жовтий колір, і є невеликі сліди від фракталу, але оскільки були вибрані фрагменти з сильно розгалуженою структурою – сліди не значні.

GOOD ENOUGH

Moderately slow $\text{♩} = 92$ Words and Music by
AMY LEE

© 2006 PROFESSOR SCREWEYE PUBLISHING (BMI) and DWIGHT FRYE MUSIC, INC. (BMI)
All Rights Administered by DWIGHT FRYE MUSIC, INC.
All Right s Reserved

Рисунок 4.16 – Відкрите зображення (нотна сторінка)

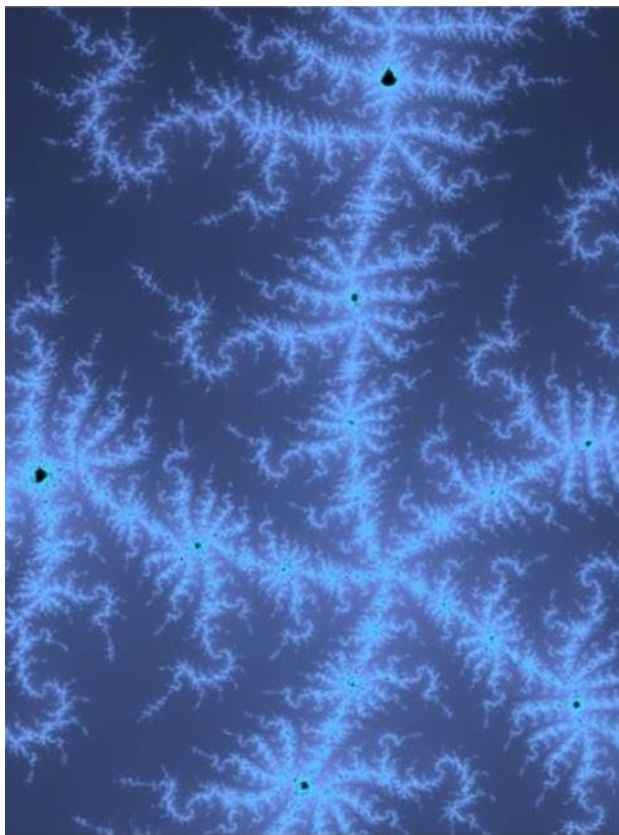


Рисунок 4.17 – Фрагмент фракталу Мандельброта (500 ітерацій)

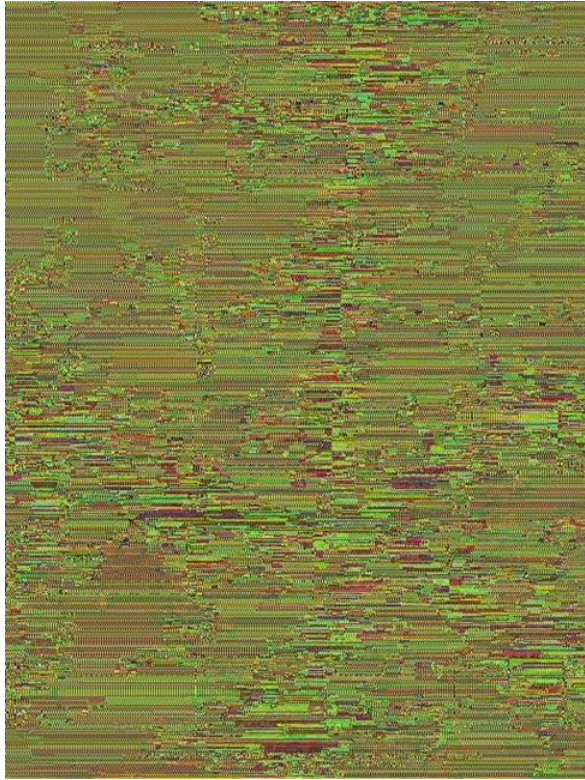


Рисунок 4.18 – Зашифроване зображення (нотна сторінка)

GOOD ENOUGH

Moderately slow $\text{♩} = 92$ Words and Music by
AMY LEE

mf (with pedal)

cresc. *poco rit. decresc.*

a tempo

rit. N.C.

© 2008 PROFESSOR SCHEWEYE PUBLISHING (BMI) and DWIGHT FRYE MUSIC, INC. (BMI)
All Rights Administered by DWIGHT FRYE MUSIC, INC.
All Rights Reserved

Рисунок 4.19 – Дешифроване зображення (нотна сторінка)

Для демонстрації шифрування за допомогою множини Жюліа було вибрано зображення лісу в жовто-зеленій колірній гамі (рисунок 4.20). Як шифруючий фрактал було взято фрагмент (рисунок 4.21) множини Жюліа, представленого на рисунку 4.4.

Зображення після виконання алгоритму 3.2 представлено на рисунку 4.20.



Рисунок 4.20 – Відкрите зображення (ліс)

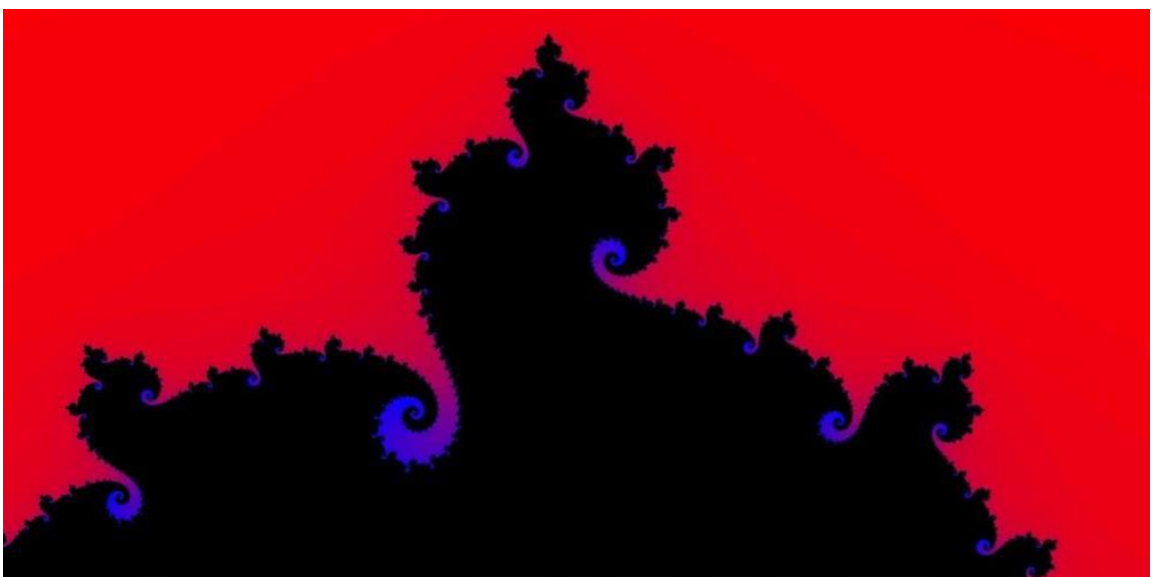


Рисунок 4.21 – Фрагмент множини Жюліа

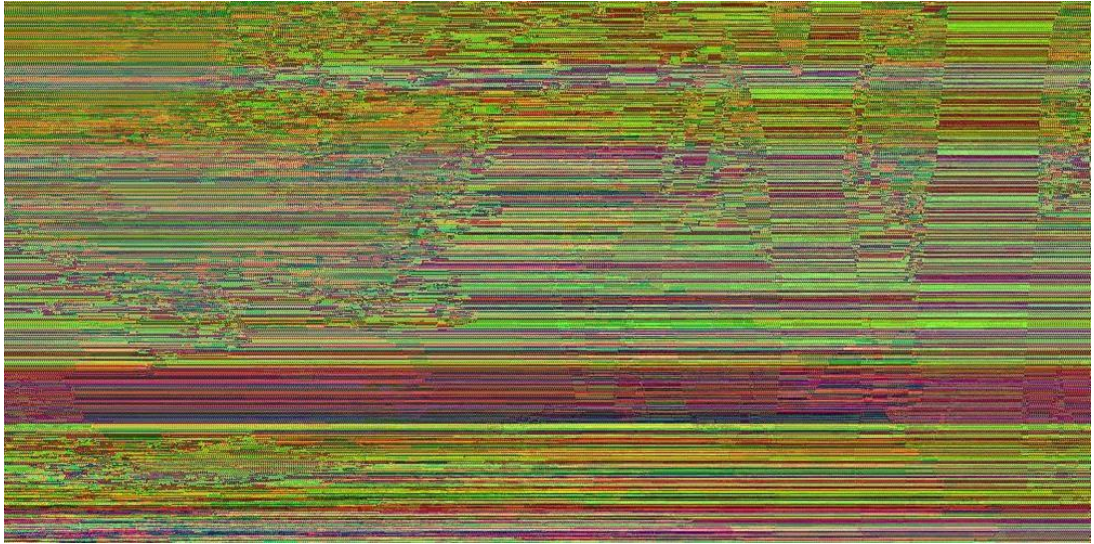


Рисунок 4.22 – Зашифроване зображення (ліс)

Дешифроване зображення представлено на рисунку 4.23. Тут залишковий жовтий колір не сильно впливає на отримане зображення, оскільки кольорова гама спочатку була жовто-зеленою, але сліди фракталу в даному прикладі простежуються сильніше, ніж при шифруванні за допомогою фрактала.



Рисунок 4.23 – Дешифроване зображення (ліс)

Розглянемо наступний приклад із використанням у шифруванні фракталу Ньютона п'ятого ступеня.

Як відкрите зображення було взято фрагмент фотографії зоряного неба (рисунок 4.24).



Рисунок 4.24 – Відкрите зображення

Фрактал Ньютона, використаний як шифруючий зображення, представлений на рисунку 4.25. Зашифроване зображення показано на рисунку 4.26, а дешифроване на рисунку 4.27.

Так само як і при використанні багатьох Жюліа, після дешифрації залишаються досить помітні фрактальні сліди.

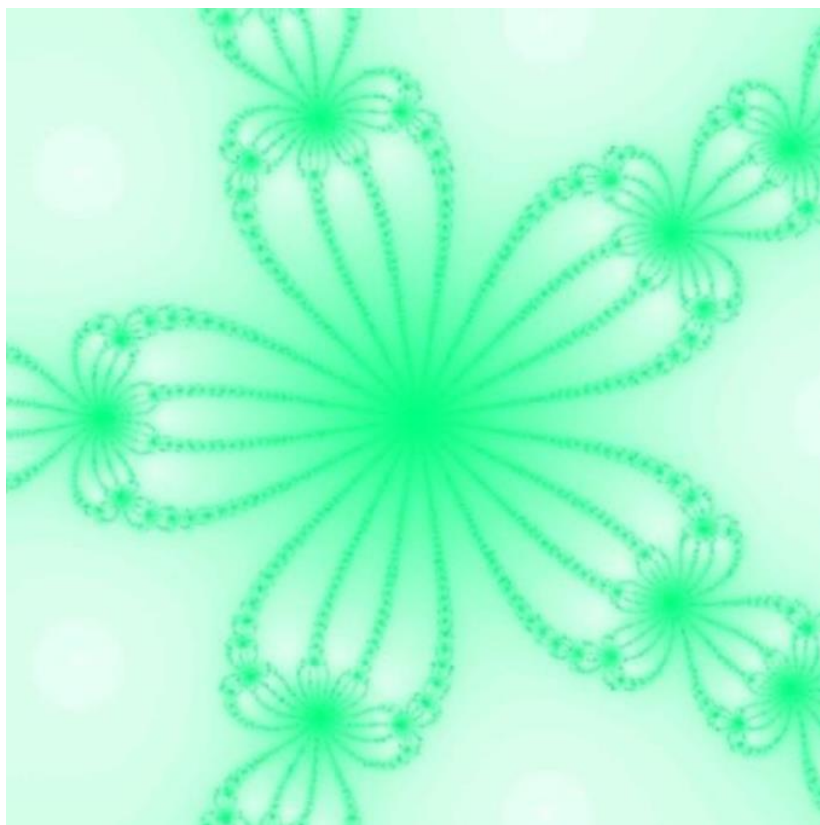


Рисунок 4.25 – Фрактал Ньютона (100 ітерацій)

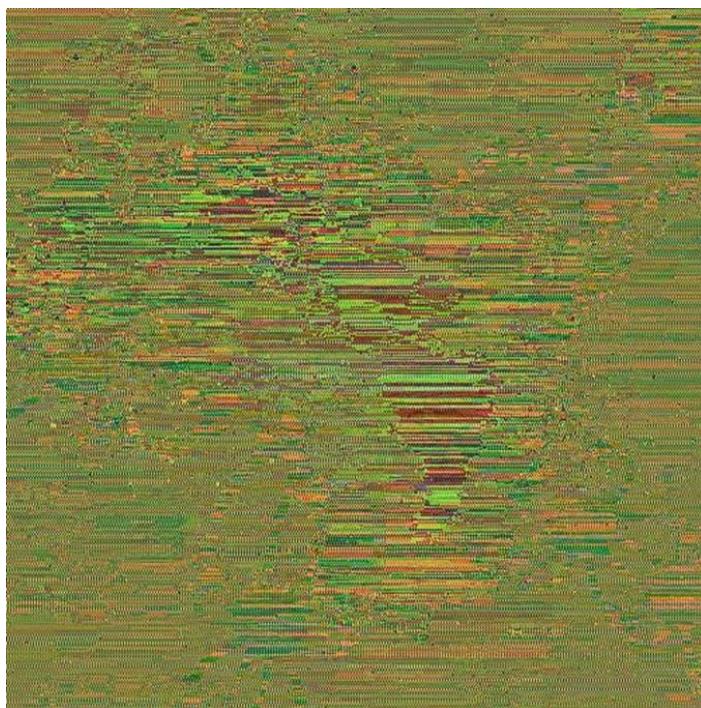


Рисунок 4.26 – Зашифроване зображення

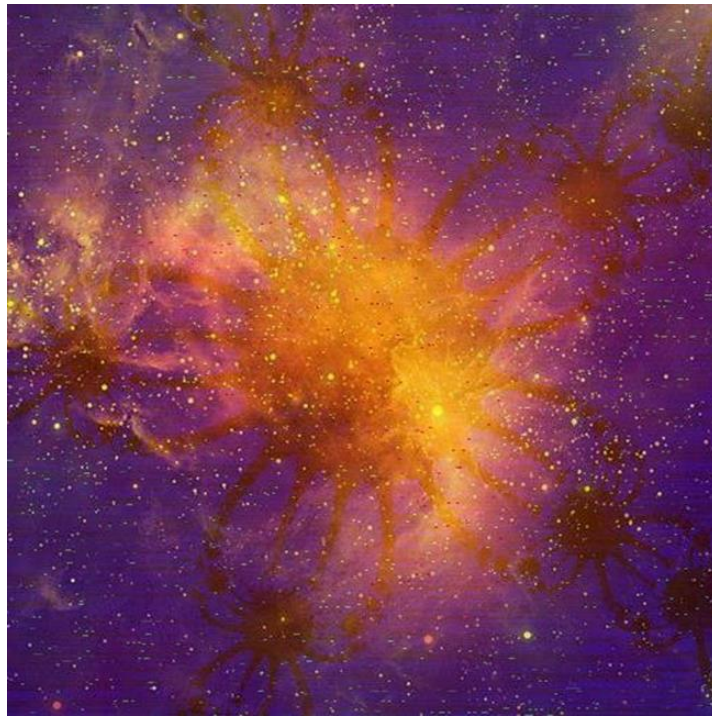


Рисунок 4.27 – Зашифроване зображення

4.3 Шифрування та дешифрування текстів

Як відкритий текст було взято уривок з твору Льюїса Керролла «Аліса в Країні Чудес», представлений на рисунку 4.28 (кількість символів у тексті $N=707$).

"Curiouser and curiouser!" cried Alice (she was so much surprised, that for the moment she quite forgot how to speak good English); "now I'm opening out like the largest telescope that ever was! Good-bye, feet!" (for when she looked down at her feet, they seemed to be almost out of sight, they were getting so far off). "Oh, my poor little feet, I wonder who will put on your shoes and stockings for you now, dears? I'm sure I shan't be able! I shall be a great deal too far off to trouble myself about you: you must manage the best way you can; --but I must be kind to them," thought Alice, "or perhaps they won't walk the way I want to go! Let me see: I'll give them a new pair of boots every Christmas."

Рисунок 4.28 – Відкритий текст

Як шифруюче зображення було обрано фрагмент фрактала Мандельброта (рисунок 4.29):

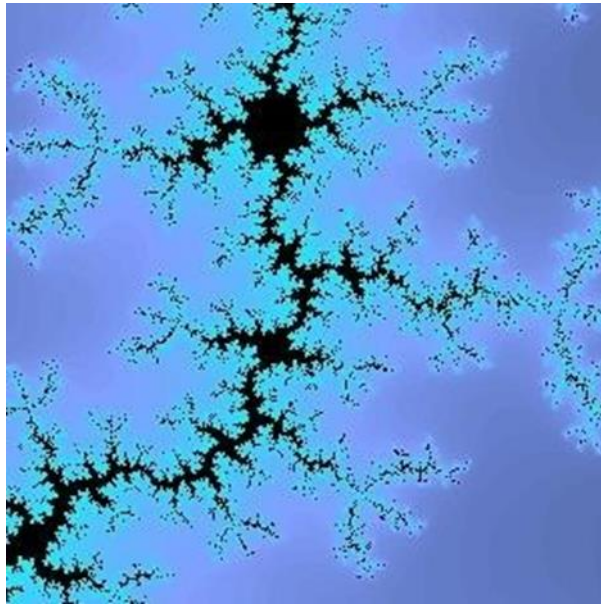


Рисунок 4.29 – Шифруюче зображення

Якщо була використана шифруюча послідовність на основі пункту 3.1 алгоритму 3.3, то зашифрований текст буде виглядати так (рисунок 4.30).

```
oF;u8n$$srpb?'uf%v9n'r7ss#pg&o3bvQ8m7gt8|0u0y {HtAE*тці*ен- PANH-
OEZ[OPUGEjF-V0s$ но4' &/BR Eq@G/4d%ngm+;( ; *;ou I&m opeNxQ'c'=7p,?IL
8A/ 5;0d&EEBQ@]PIAcpO©aye- зee5K0Hvb@qc8&%`5 <o>k4dpd+w> 1td'%v`b.d<-
it!e0 1a-m&dcv, *dig,m+s] xtV E8pm@4!'wG%D'a4r9n7 #opf1rpn4d{,r -h}
=ytt;k'$8mvuBvu8FY□цuM KowQppTJLOV[S-OSYAEXRFJO_BFbpe3u .?_t'7Un+%@l} {c3%0)
1(.sH be abhe!©hIy\,' #t}x&#MbrDu!'0E A-DHPTKbeHI31tВнцф8|.lneA}c&geart8eqb4q$ 'h=
)o7%#d.?.j,dc<tilim>p?#)alh#j($8jmp%e-T,J17e#!)HeBM E,e4wdr"m) 'g$/>
'c<kqt8eqw0yrM@sj$нBw 1F\E}0QkrI<@U E E ARXO-HSVR-4@f?5=a'.H
```

Рисунок 4.30 – Шифротекст (3.1)

Для пункту 3.2 шифротекст представлено рисунку 4.31.

ВИСНОВКИ

В результаті виконаної роботи було розроблено криптографічні алгоритми шифрування зображень та текстів з використанням теорії фрактального моделювання. На основі запропонованих алгоритмів у середовищі C++ були написані програми, що реалізують побудову фракцій алгебри та шифрування графічної та текстової інформації за допомогою них.

Результати роботи програм показали, що використовувати фрактали як ключ для шифрування досить зручно і ефективно. Для їх побудови потрібна невелика кількість параметрів, при цьому на виході виходять об'єкти зі складними хаотичними межами.

Так як шифруюча послідовність будується на основі алгебраїчного фракталу, кращий результат можна досягти, якщо використовувати фрактали з досить порізаною структурою. Наприклад, фрагменти сильно наближеної на межі множини Мандельброта або нескладне безліч Жюліа.

При дешифрації зображень з'являється жовтий колір і залишкові сліди від фракталу, але зображені об'єкти, інформація, представлена у графічному вигляді, зберігаються. Це добре видно на прикладі нотної сторінки (рисунки 4.16, 4.19).

При дешифрації тексту жодних проблем не виникло. При цьому результат роботи програми не показав суттєвої різниці між використанням пункту 3.1 з алгоритму 3.3 та пункту 3.2. Але існують відмінності при використанні певного виду фракталу, і якщо розглядати зашифровані тексти з розділу 4.3, то можна зробити висновок, що використання фракталу Мандельброта дає найкращий результат під час шифрування.

Таким чином, запропоновані методи та розроблені на їх основі програми ефективно та зручно використовувати для шифрування текстової інформації, представленої як у графічному вигляді, так і у символному.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Потапов А.А. Фракталы, скейлинг и дробные операторы в физике и радиотехнике // Радиоэлектроника. Наносистемы. Информационные технологии. – №1-2. Т.1, 2009. – С. 64-128.
2. Пителинский К.В., Синьковский А.В. Роль коммуникаций в информационном обществе и фрактальные алгоритмы шифрования данных // Вопросы защиты информации. – М.: НТЦ оборонного комплекса «Компас», 2005. – Вып. 4 (71). – С. 15-17. – ISSN 2073-2600.
3. Шишкин Е.И. Моделирование и анализ пространственных и временных фрактальных объектов. – Екатеринбург: Изд-во УрГУ, 2004. – 89 с
4. Иудин Д.И. Фракталы: от простого к сложному / Д.И. Иудин, Е.В. Копосов; Нижегород. гос. архитектур.-строит. ун-т – Н. Новгород: ННГАСУ, 2012. – 200 с., ISBN 978-5-87941-829-3
5. Потапов А.А. Фракталы, скейлинг и дробные операторы в физике и радиотехнике // Радиоэлектроника. Наносистемы. Информационные технологии. – №1-2. Т. 1, 2009. – С. 64-128.
6. Кроновер Р.М. Фракталы и хаос в динамических системах. – М.: Техносфера, 2006. – 488 с. – ISBN 5-94836-068-7
7. Малинецкий Г.Г., Курдюмов С.П. Синергетика, прогноз и управление риском // Синергетическая парадигма. Нелинейное мышление в науке и искусстве. – М.: Прогресс-Традиция, 2002. – С. 378-405.
8. Морозов А.Д. Введение в теорию фракталов. Учеб. пособие. Н.Новгород: Изд-во Нижегородского ун-та, 1999. – 140 с. – ISBN 5- 85746-282-7
9. Иванов С.А. Стохастические фракталы в информатике // НТИ. Сер. 2. Информ. процессы и системы. – 2002. №8 – С. 7-18. – ISSN 0548-0027.
10. Иудин Д.И. Фракталы: от простого к сложному / Д.И. Иудин, Е.В.

Копосов; Нижегород. гос. архитектур.-строит. ун-т – Н. Новгород: ННГАСУ, 2012. – 200 с., ISBN 978–5–87941–829–3

11. Магомедова Д.І., Симонян А.Г., Смичек М.А. Використання фракцій алгебри для захисту інформації стеганографічними методами від несанкціонованих впливів // Вісник НДІЕІ. - 2018. № 8 (87). – С. 5–15

12. Басараб М.А., Колесніков А.В., Іванов І.П. Аналіз мережевого трафіку корпоративної мережі університету методами нелінійної динаміки // Наука та освіта: Електронний науково-технічний журнал. – 2013. №8 – Режим доступу:<http://technomag.edu.ru/doc/587054.html>

13. Шелухін О.І. Фрактальні процеси у телекомунікаціях/О.І. Шелухін, А.М. Тенякшев, А.В. Осин; За ред. О.І. Шелухіна. - М.: Радіотехніка, 2003. - 479 с.: іл., табл. - ISBN 5-93108-030-9

14. Потапов А.А. Фрактали, скейлінг та дробові оператори у фізиці та радіотехніці // Радіоелектроніка. Наносистеми. Інформаційні технології. - №1-2. Т.1, 2009. - С. 64-128.