УДК 519.246.8

ШИФРУВАННЯ ЗА ДОПОМОГОЮ ФРАКТАЛЬНИХ СТРУКТУР

Полуляхова Д.І.
Науковий керівник – д-р техн. наук, проф. Кіріченко Л.О.
Харківський національний університет радіоелектроніки, каф. ПМ,
м. Харків, Україна
e-mail: daria.poluliakhova@nure.ua

This study presents a data encryption system using fractal structures. It is based on diffusion and entanglement processes in which the image information is hidden in the complex details of fractal images. In this paper, a cryptosystem is proposed in which encryption keys are generated based on Mandelbrot factorial and Julian set. The secret keys are based on images of the proposed factorials constructed in Python language using various mathematical libraries. The results obtained show the proposed encryption method as efficient, simple and secure.

Криптографія – це наука про захист інформації від несанкціонованого доступу та від використанням шляхом шифрування даних. У сучасному світі, де технології швидко розвиваються, а кількість інформації для передачі та зберігання постійно зростає. Важливість криптографії набуває особливого значення в забезпеченні конфіденційності, цілісності та доступності цих даних.

Актуальність криптографії в сучасному світі підкреслюється високим ризиком кіберзлочинності, крадіжкою особистої інформації та шпигунством. Організації та індивіди повинні вдосконалювати свої методи шифрування, щоб протистояти постійно зростаючим технічним викликам. Криптографія стає фундаментальним елементом безпеки в цифровій епохі, забезпечує надійний захист для зберігання та обміну інформацією у віртуальному просторі.

У контексті криптографії, розширення методів шифрування включає в себе застосування фракталів, що представляє собою розділ математики, де вивчаються форми, які виявляють схожість на різних масштабах. Фрактали в криптографії можуть використовуватися для створення комплексних та непередбачуваних структур шифрування, збільшуючи тим самим стійкість інформації до аналізу атакуючих [1, 2].

Фрактали, в математичному розумінні, – це геометричні структури, які виявляють самоподібність на різних рівнях масштабу [3]. Їх властивості дозволяють створювати велику кількість унікальних форм, які залишаються нерозкритими від звичайного спостереження. Графічні фрактали представляють собою візуально привабливі, непередбачувані та складні структури, що забезпечують не тільки безпеку, але й велику ефективність в процесі шифрування та декриптування.

У роботі було розглянуто фрактальні множини Мандельброта та Жуліа.

Бенуа Мандельброт у 1979 році натрапив на складну структуру, яка зараз називається множиною (фракталом) Мандельброта [4]. Множина Мандельброта обчислюється за допомогою набору точок на комплексній площині і відображається за допомогою функції, наведеної нижче:

$$z_{k+1} = z_k^2 + c,\ k = 0,1,2,\ldots,\ z_0 = c. \quad (1)$$

Зображення множини Мандельброта при 100 ітераціях наведено на рис. 1.

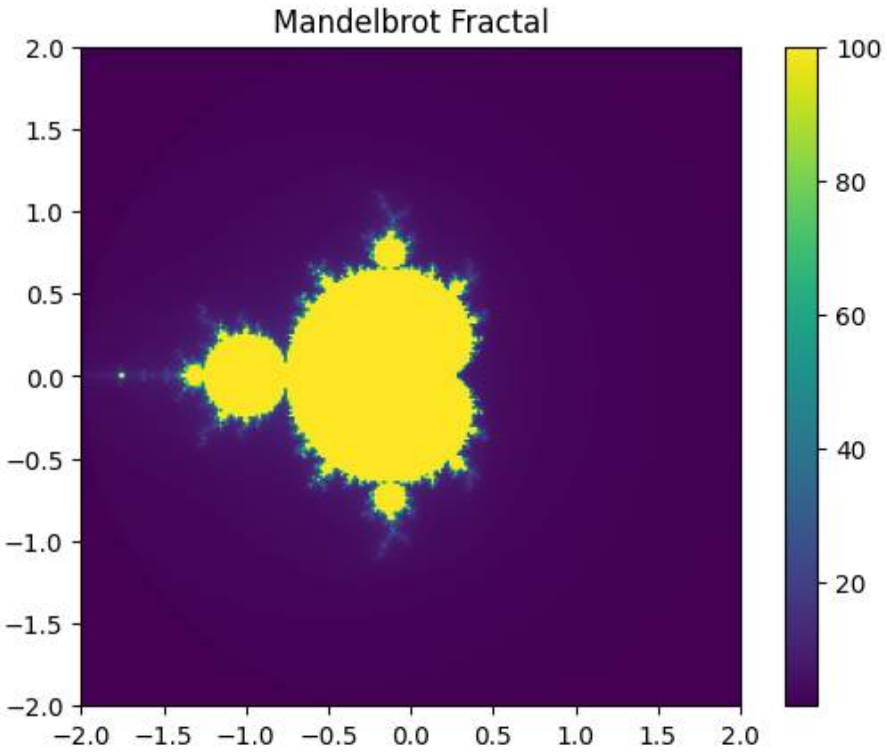

Рисунок 1 – Фрактал Мандельброта при 100 ітераціях

Множина Жуліа визначається через ітераційну функцію у комплексній площині [4]. Зазвичай ця функція має вигляд:

$$f(z) = z^2 + c, \quad (2)$$

де c є комплексним числом, значення якого залишається статичним. Зображення множини Жуліа наведено на рис. 2.

У роботі описується схема шифрування даних за допомогою згенерованих зображень фракталів, які генеруються за формулами (1) та (2). Отримані зображення переводяться у двовимірні масиви. Проводиться попередня обробка зображень для шифрування, а саме: поділ на 3 кольорових канали RGB та запис отриманих даних в окремі масиви. Шифрування виконується операцією XOR між шифрувальним набором та зображенням.

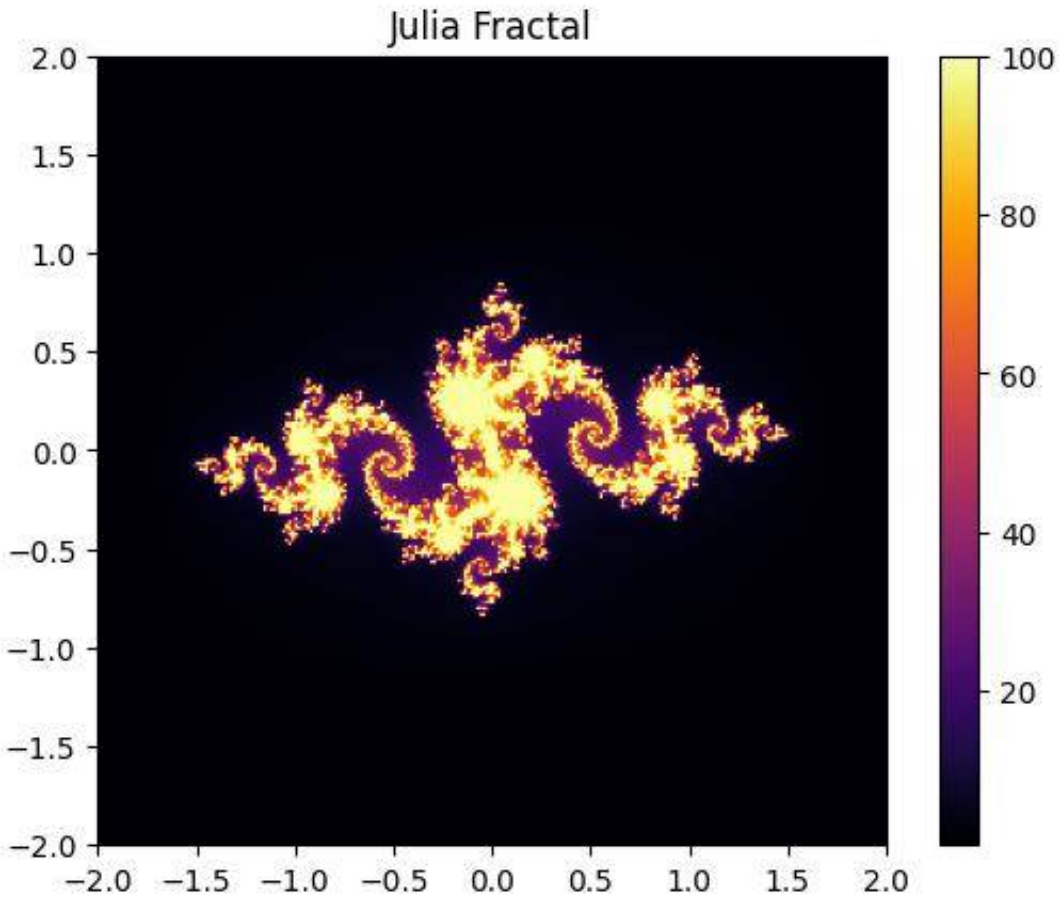

Рисунок 2 – Множина Жуліа

Список використаних джерел:

1. Agarwal S. Image encryption techniques using fractal function : a review. International journal of computer science and information technology. 2017. Т. 9, № 2. С. 53–68. URL: https://doi.org/10.5121/ijcsit.2017.9205 (дата звернення: 03.03.2024).

2. Radivilova, T., Kirichenko, L., Alghawli, A. S., Kulbachnyi, V., Bondarenko, O. Statistical and 2 Signature Analysis Methods of Intrusion Detection Lecture Notes on Data Engineering and Communications Technologie, 2022, 115, Springer, Cham., pp. 115–131.

3. Malina R. F., Pickover C. A. Computers, pattern, chaos and beauty: graphics from an unseen world. Leonardo. 1991. Т. 24, No. 1. С. 93. URL: https://doi.org/10.2307/1575492 (дата звернення: 03.03.2024).

4. Doyle J. F. An introduction to fractals and chaos. Teaching mathematics and its applications. 1992. Т. 11, № 4. С. 166–174. URL: https://doi.org/10.1093/teamat/11.4.166 (дата звернення: 03.03.2024).