УДК 004.94:517.21 DOI: 10.31673/2412-4338.2020.011524

Свинчук О.В., Барабаш О.В., Олімпієва Ю.І., Ільїн О.Ю.
Державний університет телекомунікацій, Київ

ЗАСТОСУВАННЯ ФРАКТАЛЬНИХ ФУНКЦІЙ ДЛЯ ШИФРУВАННЯ ДАНИХ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Анотація: *Захист інформації є важливою проблемою сьогодення. Конфіденційні дані потребують захисту від сторонніх користувачів. Для високого рівня безпеки сьогодні вже запропоновано багато різних методів шифрування тексту та зображень, але їх весь час потрібно постійно змінювати та вдосконалювати. Фрактали, які мають цікаву хаотичну будову, можуть бути використані при побудові нових методів захисту документів. У теорії шифрування фрактальні функції використовуються як надійні датчики псевдовипадкових послідовностей, які перетворюють вхідні набори символів у числову послідовність. Здійснити аналіз цієї послідовності практично неможливо. Проте, знаючи вихідну функцію та її початкові параметри, можливо легко відновити початковий набір символів. Також фрактальні об'єкти допомагають удосконалювати інструментальні засоби для підвищення якості захисту поліграфічної продукції, створюючи фрактальні сітки, які неможливо відтворити за допомогою звичайного копіювання. Дана стаття присвячена розробці та реалізації нової математичної моделі для шифрування даних на основі класу сингулярних функцій канторівського типу. Для таких функцій значення початкових наборів генеруються випадковим чином. Досліджується алгоритм побудови графіка, основних властивостей функцій та їх використання при створенні криптографічного ключа. Проаналізовано залежність між передачею інформації через канали зв'язку і початковими числовими наборами функції та її вплив на підвищення захисту інформації. Криптографічна стійкість отриманого алгоритму на основі фрактальних функцій, а також побудова нових класів функцій, які будуть давати мінімальний розмір ключа при максимальній стійкості системи шифрування, є предметом подальших досліджень.*

Ключові слова: *фрактал, фрактальні функції, сингулярні функції канторівського типу, фрактальний аналіз, шифрування даних, захист інформації.*

Svynchuk O.V., Barabash O.V., Olimpiyeva Yu.I., Ilin O. Yu.
State University of Telecommunications, Kyiv

THE APPLICATION OF FRACTAL FUNCTIONS FOR DATA ENCRYPTION IN INFORMATION SECURITY SYSTEMS

Abstract: *Information security is an important issue nowadays. Data should be protected from unauthorized users. At present, there are many different text and image encryption methods aimed at providing a high level of security. Fractals, which have an interesting chaotic structure, can be used to develop new document security methods. In the encryption theory, fractal functions are used as reliable detectors for pseudorandom sequences that turn input character sets into a numerical sequence. It is almost impossible to analyse this sequence. However, knowing the initial function and its initial parameters makes it easy to restore the original character set. Fractal objects also help to improve the tools for increasing the quality of printed products protection by means of creating fractal nets that cannot be reproduced with regular copying. This article deals with the development and implementation of a new mathematical model for data encryption based on a class of singular Cantor-type functions. The values of initial sets of these functions are randomly generated. The inverse solution is impossible, because finding the initial digits in the argument image is time-consuming. The algorithm of graphing, the key properties of functions and*

their use in creating a cryptographic key are investigated. The dependence between the information transmission through the communication channels and the initial numerical function sets and its effect on the increase in the information security are analyzed. The cryptographic stability of the obtained algorithm based on fractal functions and the development of new classes of functions that will give the minimum key size with the maximum stability of the encryption system are the subjects of further research.

Keywords: *fractal, fractal functions, singular functions of Cantor type, fractal analysis, data encryption, information security.*

Свинчук О.В., Барабаш О.В., Олимпиева Ю.И., Ильин О.Ю.
Государственный университет телекоммуникаций, Киев

ПРИМЕНЕНИЕ ФРАКТАЛЬНЫХ ФУНКЦИЙ ДЛЯ ШИФРОВАНИЯ ДАННЫХ В СИСТЕМАХ ЗАЩИТЫ ІНФОРМАЦИИ

Аннотация: *Защита информации является важной проблемой современности. Конфиденциальные данные нуждаются в защите от посторонних пользователей. Для высокого уровня безопасности сегодня уже предложено много различных методов шифрования текста и изображений. Фракталы, которые имеют интересное хаотическое строение, могут быть использованы при построении новых методов защиты документов. В теории шифрования фрактальные функции используются как надежные датчики псевдослучайных последовательностей, которые отражают входные наборы символов в числовую последовательность. Осуществить анализ этой последовательности практически невозможно. Однако, зная исходную функцию и ее начальные параметры, можно легко восстановить первоначальный набор символов. Также фрактальные объекты помогают совершенствовать инструментальные средства для повышения качества защиты полиграфической продукции, создавая фрактальные сетки, которые невозможно воспроизвести с помощью обычного копирования. Данная статья посвящена разработке и реализации новой математической модели для шифрования данных на основе класса сингулярных функций канторовского типа. Для этих функций значение начальных наборов генерируются случайным образом. Исследуется алгоритм построения графика, основных свойств функций и их использование при создании криптографического ключа. Проанализирована зависимость между передачей информации через каналы связи и начальными числовыми наборами функции и ее влияние на повышение защиты информации. Криптографическая стойкость полученного алгоритма на основе фрактальных функций, а также построение новых классов функций, которые будут давать минимальный размер ключа при максимальной устойчивости системы шифрования, является предметом дальнейших исследований.*

Ключевые слова: *фрактал, фрактальные функции, сингулярные функции канторовского типа, фрактальный анализ, шифрование данных, защита информации.*

1. Вступ. На сучасному етапі розвитку інформатизації суспільства виникає проблема забезпечення надійного захисту передачі та отримання інформації. Її можна розглядати з точок зору економіки, науки і техніки, які обумовили бурхливий розвиток обчислювальної техніки, інформатики, мікроелектроніки, телекомунікації, тощо. Із швидким розвитком інформаційних технологій та передачею даних через комп'ютерні мережі зараз постала більш гостро, оскільки методи захисту потрібно постійно вдосконалювати. Вчені-програмісти всього світу приділяють особливу увагу проблемі захисту інформації в комп'ютерних мережах та шукають ефективні шляхи її вирішення. Тому для спеціалістів різних сфер діяльності актуальною є підготовка в галузі захисту інформації.

У минулому математики вивчали множини та функції, які були простішими в дослідженні, до яких можна було застосовувати класичні методи обчислень. Функціям, які були не достатньо гладкими та регулярними, увага майже не приділялася. Але в останній час з'явилася потреба і можливості ґрунтовно вивчати такі функції, які мають нетривіальні локальні властивості і складну «варіаційну поведінку». Це фрактальні функції: сингулярні функції (неперервні функції, відмінні від константи, похідні яких майже скрізь дорівнюють нулю в розумінні міри Лебега), ніде не диференційовні функції (неперервні функції, які ніде не мають похідної), ніде не монотонні функції (неперервні функції, які не мають жодного як завгодно малого інтервалу монотонності), функції канторівського типу (функції, які не мають проміжків монотонності, крім проміжків сталості). Такі функції забезпечують краще уявлення багатьох природних явищ, які раніше методами класичної геометрії дослідити було важко. В останні роки зріс інтерес до таких функцій, оскільки вони є затребуваними в різних галузях суспільства при створенні математичних моделей різноманітних процесів та явищ, особливо для захисту інформації в комп'ютерних мережах, що є актуальним завданням у сучасному світі.

2. Аналіз останніх досліджень і публікацій. Поняття фрактала було запропоноване французько-американським математиком Бенуа Мандельбротом. У 1977 році він опублікував роботу «Фрактальна геометрія природи», в якій стверджував, що випадкові, на перший погляд, форми є насправді складними геометричними фігурами, що складаються з менших фігур, які при збільшенні масштабу точно повторюють велику фігуру. Фрактали володіють цікавими властивостями:

1) вони мають хаотичну поведінку;
2) вони мають дробову нескінченну розмірність;
3) вони складаються із частинок, подібних усій фігурі;
4) вони можуть бути представлені простим алгоритмом.

Значний вклад в розвиток фрактального аналізу був зроблений такими закордонними вченими як Кантором, Пуанкаре, Кляйном, Фату, Жуліа, Серпінським, Салемом, Мінковським, Кроновером, Божокіним, Паршиним, так і вітчизняними – Турбін А.Ф., Працьовитий М.В. та їх наукова школа [1].

Фрактали поділяються на:

1) алгебраїчні – створюються за допомогою нелінійних обчислювальних процесів в n-вимірних просторах (множина Мандельброта, фрактал Ляпунова);

2) геометричні – є самоподібними фігурами і генеруються за допомогою ітераційних функцій, що мають фіксоване правило геометричних заміщень (множина Кантора, килим Серпінського, крива Пеано, крива Коха, крива дракона, фрактальні функції);

3) стохастичні – створюються ітераційним процесом з випадковими параметрами (плазма, траєкторія броунівського руху на площині і в просторі); використовуються під час моделювання різних природних об'єктів – рельєфу місцевості, поверхні моря, тощо.

В останні роки з'явилася велика кількість праць, присвячена фрактальним об'єктам. За допомогою фракталів можна змоделювати та описати різноманітні явища в областях радіотехніки та електроніки, цифрової обробки інформації, комп'ютерній графіці [2,3,4,5,6]. У комп'ютерній графіці фрактали прискорюють створення зображень, забезпечуючи стискання інформації та відео на основі системи ітерованих функцій (IFS), де побудова такого фрактального зображення відбувається за деяким алгоритмом або шляхом автоматичної генерації зображень, використовуючи обчислення за певними формулами. В області розробки інформаційних технологій фрактальні методи допомагають обробити та проаналізувати величезні потоки астрономічних даних на основі логічних схем когнітивної аналітики розкодування прихованої в них інформації. Вони є незамінними при створенні природних об'єктів у тривимірній графіці (дерева, хмари, ландшафти, берегові рельєфи). Також фрактальні методи використовуються при розробці методів розпізнавання образів на радіолокаційних зображеннях.

У роботах [7,8,9,10,11,12] розглядаються особливості застосування теорії фракталів у вирішенні широкого кола задач економічного аналізу, що забезпечить не тільки єдиний підхід до проведення аналізу теорій циклічного розвитку, але й значно розширить інструментарій математичного моделювання і прогнозування на макрорівні. Також за допомогою фрактальних об'єктів можна моделювати процес забезпечення комплексної безпеки окремо взятого автоматизованого робочого місця спеціаліста і проектувати отримані результати на всю систему захисту інформації [13].

Протягом багатьох років залишається пріоритетним завданням усіх державних інституцій щодо захисту цінних паперів та документів суворого обліку від підроблення та фальсифікації [14]. Для розробки надійних методів захисту документів сьогодні активно застосовують фрактальний аналіз.

У роботі [15] автори застосовуть фрактальні функції для розроблення та удосконалення методів та інструментальних засобів підвищення якості захисту поліграфічної продукції. Вони будують математичну модель на основі використання алгебри регулярних подій, фрактальних функцій і мовних регулярних виразів, яка дозволять оцінити показники ефективності через задані умови і елементи рішення, а також розробляють алгоритмічне і програмне забезпечення для створення логіко-алгебраїчних та фрактально-геометричних зображень, які зорієнтовані на захист.

В [16] розглянуто фрактальний метод заповнення фону документа для захисту інформації. Оскільки фрактали будуються з великою кількістю ітерацій за певним алгоритмом, зберігаючи при цьому його вигляд однаковим при різних збільшеннях, то найменші фігури є настільки дрібними, що відтворити їх звичайним копіюванням неможливо. Тому фрактальна сітка зможе забезпечити високий рівень захисту документів, оскільки вона складається з дрібних елементів і дуже тонких ліній, а фрактальні фігури є настільки складними в побудові, що їх відтворення вимагає багато часу. Заповнення площини документа елементами захисту реалізовано за допомогою мови програмування PostScript, що забезпечує векторний формат, апаратну незалежність та високу поліграфічну якість.

Робота [17] присвячена новому методу побудови латентних елементів на основі фракталів, який дозволяє підвищити ефективність захисту друкованих документів. Такий спосіб захисту документів використовує векторну технологію побудови фрактальних сіток з використанням програмного коду, який повністю адаптований до виведення інформації на поліграфічній техніці для високоякісного друку, що дає можливість реалізувати захист. Фрактальні фонові сітки є складними для відтворення, адже при цьому необхідно використати алгоритм побудови вибраного типу фракталу. Перевагами такого методу є те, що його реалізація не вимагає великих фінансових затрат, тому він широко використовується для захисту бланків суворого обліку.

У роботі [18] автори розглядають принципи побудови об'єктів фрактальної природи для їх застосування при генерації довгих неперіодичних послідовностей, які використовуються в теорії шифрування даних в системах захисту інформації. Для побудови таких послідовностей можна використовувати уже відомі фрактальні об'єкти або будувати нові фрактальні структури. Змінюючи лише деякі характеристики, можна змоделювати величезну кількість різноманітних фрактальних об'єктів та функцій, які за своєю будовою будуть ще складнішими, а це, відповідно, забезпечить ще більш високий рівень захисту.

У закордонних виданнях [19,20] автори пишуть про перевагу фракталів та фрактальних функцій для створення високого рівня безпеки даних при їх передачі. Вони досліджують нові математичні методи та створюють математичні моделі. Розглядається симетричне шифрування ключа за допомогою ітераційних фрактальних функцій, що має перевагу з огляду на час генерування паролів та час шифрування, і є більш ефективним, ніж шифрування за RSA.

Є очевидним, що використання фрактальних об'єктів для шифрування даних посилює процес захисту інформації. І чим більш хаотична поведінка таких об'єктів, тим рівень безпеки стає вищим.

3. Ціль дослідження. Метою дослідження є моделювання класу фрактальних функцій, дослідження їх властивостей та встановлення можливості їх застосування для ефективного захисту інформації.

4. Результати дослідження. Сьогодні в галузі зв'язку науковці ведуть розробки щодо створення надійних каналів для передачі інформації та методів її захисту, використовуючи фрактальне моделювання. У криптографії для шифрування та передачі даних все частіше розглядають класи фрактальних функцій, які володіють властивістю самоподібності і поведінка яких залежить від заданих початкових умов. При цьому такі функції простою формулою задати неможливо. Вони будуються на основі ітерацій. І чим більше їх провести, тим краще, бо надійність шифрування стає значно вищою порівняно із звичайними методами. Для конструктивного задання таких функцій та зручності їх аналітичного задання використовують різні системи кодування (зображення) дійсних чисел із скінченними і нескінченними алфавітами. Це може бути класичне *s*-е зображення чисел і його узагальнення Q_s-зображення та Q_s^*-зображення [1].

Розглянемо один клас немонотонних сингулярних функцій канторівського типу з фрактальними властивостями, залежних від скінченного набору параметрів [12].

Нехай $A_5 = \{0,1,2,3,4\}$ – алфавіт п'ятіркової системи числення, $L \equiv A_5 \times A_5 \times \ldots$ – простір послідовностей алфавіту, $x = \sum_{k=1}^{\infty} \frac{\alpha_k(x)}{5^k} = \Delta^5_{\alpha_1\alpha_2\ldots\alpha_i\ldots}$ – п'ятіркове зображення дійсного числа $x \in [0;1]$, де $(\alpha_k) \in L$.

Використовуючи п'ятіркове зображення чисел, означимо функцію рівністю

$$f(x) = \delta_{\alpha_1(x)1} + \delta_{\alpha_2(x)2} g_{\alpha_1(x)1} + \delta_{\alpha_3(x)3} g_{\alpha_1(x)1} g_{\alpha_2(x)2} + \delta_{\alpha_4(x)4} g_{\alpha_1(x)1} g_{\alpha_2(x)2} g_{\alpha_3(x)3} + \ldots =$$

$$= \delta_{\alpha_1(x)1} + \sum_{k=2}^{\infty} \left(\delta_{\alpha_k(x)k} \prod_{j=1}^{k-1} g_{\alpha_j(x)j} \right) \equiv \Delta^{G_5^*}_{\alpha_1\alpha_2\ldots\alpha_k\ldots}, \qquad (1)$$

де $(\overline{g_n}) = (g_{0n}, g_{1n}, g_{2n}, g_{3n}, g_{4n})$ – послідовність векторів таких, що:

$$g_{0n} = g_{4n} = \frac{2+\varepsilon_n}{4},\ g_{1n} = g_{3n} = -\frac{\varepsilon_n}{4},\ g_{2n} = 0;$$

$$\delta_{0n} = 0,\ \delta_{1n} = \frac{2+\varepsilon_n}{4},\ \delta_{2n} = \frac{2}{4} = \delta_{3n},\ \delta_{4n} = \frac{2-\varepsilon_n}{4},\ \text{тобто } \delta_{i+1,n} = \delta_{in} + g_{in},\ i \in N;$$

(ε_n) – наперед задана послідовність дійсних чисел така, що $0 \le \varepsilon_n \le 1$.

Властивості функції:

1) функція є неперервною на [0;1]**;**

2) множиною значень функції є відрізок [0;1]**;**

3) якщо $\varepsilon_n \neq 0$ виконується для нескінченної множини значень *n*, то функція не має проміжків монотонності, крім проміжків сталості;

4) функція має обмежену варіацію тоді і тільки тоді, коли $\sum_{i=1}^{\infty} \varepsilon_i < \infty$;

5) функція є сингулярною функцією канторівського типу, множина несталості якої має фрактальну розмірність Гаусдорфа-Безиковича $\log_5 4$;

6) графік функції симетричний відносно точки $C\left(\frac{1}{2};\frac{1}{2}\right)$.

Якщо $\varepsilon_n = 1$, то $g_{0n} = g_{4n} = \frac{3}{4}$, $g_{1n} = g_{3n} = -\frac{1}{4}$, $g_{2n} = 0$ і $\delta_{0n} = 0$, $\delta_{1n} = \frac{3}{4}$, $\delta_{2n} = \frac{2}{4} = \delta_{3n}$, $\delta_{4n} = \frac{1}{4}$. Побудова відбувається згідно наступного алгоритму. Спочатку створюємо одиничний квадрат як основу. Фіксуємо точки $(0;0)$, $\left(\frac{1}{5};\frac{3}{4}\right)$, $\left(\frac{2}{5};\frac{2}{4}\right)$, $\left(\frac{3}{5};\frac{2}{4}\right)$, $\left(\frac{4}{5};\frac{1}{4}\right)$, $(1;1)$ відповідно до координат вектора $(\overline{g_1}) = \left(\frac{3}{4},-\frac{1}{4},0,-\frac{1}{4},\frac{3}{4}\right)$ і сполучаємо їх ламаними. Дані точки і відрізок сталості належать графіку функції. Далі навколо інших чотирьох ламаних будуємо прямокутники, вважаючи їх діагоналями. У кожному з цих прямокутників продовжуємо побудову нових ламаних відповідно до координат вектора $(\overline{g_2}) = \left(\frac{3}{4},-\frac{1}{4},0,-\frac{1}{4},\frac{3}{4}\right)$. На наступному кроці алгоритм повторюється, тобто кожна з чотирьох ламаних заміняється п'ятьма новими ламаними у відповідному масштабі. Наближений графік такої функції графік подано на рис. 1. Чим більше ітерацій зробити, тим графік функції буде більш точним.

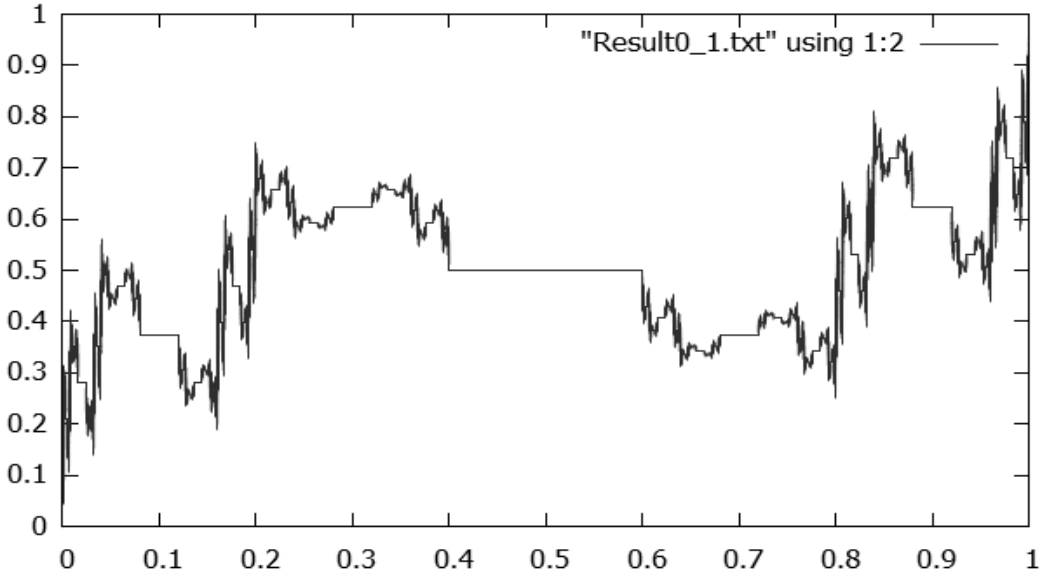

Рис. 1. Графік функції при $\varepsilon_n = 1,\ n = \overline{1,15}$

Для того, щоб зашифрувати дані, на кожному *i*-му кроці формується послідовність векторів $(\overline{g_i})$, що залежить від параметра ε_i, і після цього вихідний сигнал передається за допомогою функції (1). Початкові параметри ітераційної функції (1), яка забезпечує вибір одного перетворення із сукупності можливих для даного алгоритму, є криптографічним ключем. Якщо значення координат вектора $(\overline{g_i})$ будуть симетричними, то шифри з таким ключем будуть відносно короткі і матимуть велику пропускну здатність. Якщо ж початкові дані значень координат вектора $\overline{g_i}$ на кожному кроці змінювати, то захист передачі даних підвищується.

Функція (1) має певну особливість – маючи початкові значення, ми легко можемо обчислити значення цієї функції, але в зворотному порядку, коли відомі значення функції, дуже складно повернути початковий набір, оскільки таких може бути багато. І тому без ключа розшифровка даних буде займати немало часу і обчислювальних ресурсів.

Ще однією особливою властивістю для фрактального шифрування є прояв хаотичних властивостей графіку функції в залежності від параметра ε_i на проміжках, де функція не є сталою, тобто $G_i \equiv \{M(x,y): \alpha_1(x)=i,\ y=f(x)\}$ і при $i \neq 2$ $\varphi_i(\Gamma_f) = G_i$, де

$$\varphi_i : \begin{cases} x' = \frac{1}{5}x + \frac{i}{5}, \\ y' = g_{i1}y + \delta_{i1}. \end{cases}$$

Це дає можливість краще зашифрувати інформацію, що не вимагатиме частої зміни ключа, і збільшить ефективність передачі даних.

Для надійного шифрування можна використовувати ще образи множин, що є підмножинами відрізка [0;1], із заданими початковими наборами цифр при заданому відображенні f:

1. Образом множини $C_1 \equiv C[5;\{0,1\}]$ є відрізок $\left[0;\frac{3}{4}\right]$ (рис. 2), зліченна множина точок якого має рівно два G_2-зображення, а решта точок мають єдине G_2-зображення;

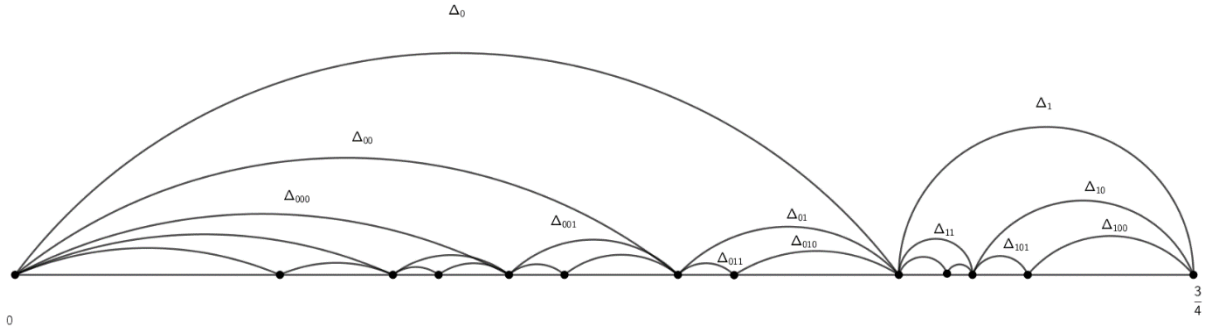

Рис.2. Образ множини C_1

2. Образом множини $C_2 \equiv C[5;\{1,3\}]$ є множина канторівського типу $C_3 \equiv C[4;\{1,2\}]$ (рис. 3);

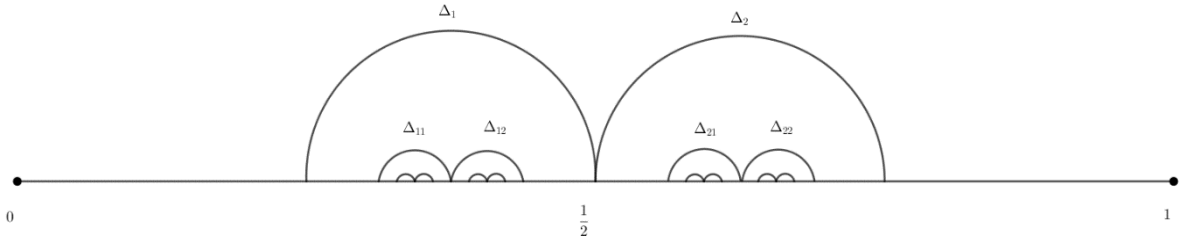

Рис.3. Образ множини C_2

3. Образом $C_4 \equiv C[5;\{1,2,3\}]$ є множина $E = C_3 \bigcup M$ (рис. 4), де M − дискретна підмножина множини четвірково-раціональних чисел, а саме:

$$M = \left\{y: y = \Delta^4_{\alpha_1\alpha_2\ldots\alpha_{m-1}2(0)},\ \alpha_i \in \{1,2\},\ m \in N\right\};$$

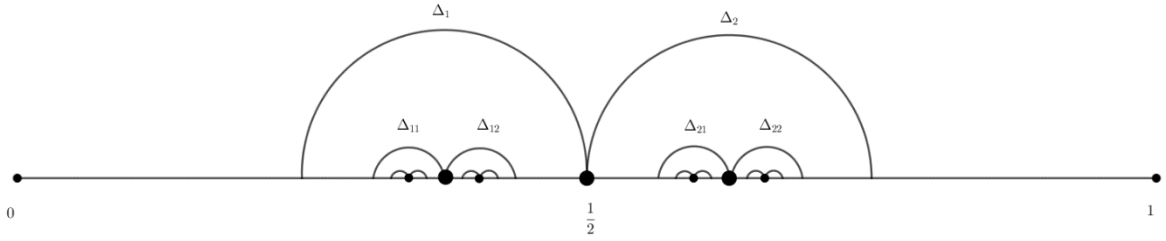

Рис.4. Образ множини C_4

4. Образом множини канторівського типу $C_5 \equiv C[5;V_n]$ (рис. 5), де

$$V_n = \begin{cases} \{0,4\}, \text{ якщо } n = 1(\mathrm{mod}\,3), \\ \{1,3\}, \text{ якщо } n \neq 1(\mathrm{mod}\,3), \end{cases}$$

є множина канторівського типу нульової міри Лебега.

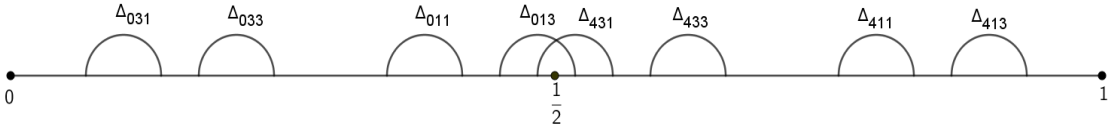

Рис.5. Образ множини C_5

Дані образи допоможуть криптографам швидше отримати інформацію із зашифрованих даних, оскільки знаючи початкові набори числових послідовностей, легко можна буде виявити область значень.

Наведена модель класу функцій дозволяє розробити нову технологію шифрування для передачі даних та розробити надійний метод для підвищення захисту інформації.

Подальше використання одержаних результатів можливе і доцільне при розробці систем інформаційної безпеки й вибору варіантів швидкодіючих та надійних рішень покращення якості функціонування систем захисту інформації.

5. Обговорення результатів проведеного дослідження. У даній статті запропонований алгоритм шифрування, заснований на одному класі немонотонних сингулярних функцій канторівського типу з фрактальними властивостями, залежних від скінченного набору параметрів. Цей підхід забезпечує набагато складніший процес генерації ключа шифрування завдяки фрактальним властивостям таких функцій і робить передавання інформації надійним.

У наукових дослідженнях [16,17,18] для захисту цінних паперів використовуються фрактали, які будуються рекурсивною процедурою, де кожен одиничний графічний елемент постає в ролі генератора, який задає величину захисного елемента. У роботах [19, 20] автори для шифрування даних використовують декілька фрактальних функцій і фрактальних множин одночасно, що дозволяє створити багато наборів різних надійних ключів. Завдяки властивостям таких функцій вони генерують симетричні ключі різної довжини, що дозволяє краще захистити дані при їх передачі. Дані алгоритми мають високу чутливість до початкових параметрів і невелика зміна значення параметра повністю змінить розшифроване повідомлення і фрактальну сітку, які будуть відомі тільки розробнику.

Незважаючи на те, що в останні роки науковці активно використовують фрактальний аналіз для побудови якісних методів захисту інформації, створення нових та вдосконалення уже існуючих залишається актуальним питанням сьогодення.

6. Висновки. Запропоновано нові математичні розробки для ефективного використання теорії фрактальних функцій в системах захисту інформації. На сьогодні існує велика кількість вже реалізованих різних моделей з використанням таких функцій, але з часом їх також потрібно вдосконалювати. Функції, які мають фрактальні властивості, на відміну від попередніх, враховують різноманітні вимоги до надійності методів захисту інформації та дають прийнятні результати для достатньо широкого класу задач в галузі зв'язку. Особливістю таких функцій є те, що вони задаються рекурсивною формулою і ведуть себе хаотично на різних проміжках часу. Генерація функцій займає немало часу, тому процес шифрування стане трудомістким, що дозволить уникнути криптоаналітичних нападів і значно покращить процес передачі інформації. Отримані результати разом з відомими методами дозволяють створити достатньо ефективне математичне забезпечення процесу захисту інформації та удосконалення існуючих методів з урахуванням різних вимог до якості.

Перспективи подальших досліджень вбачаються у створенні нових класів фрактальних функцій з використанням різних систем кодування дійсних чисел і їх використанням для створення нових методів шифрування інформації і її захисту при передачі даних.

Список використаної літератури

1. Працьовитий М.В. Фрактальний підхід у дослідженнях сингулярних розподілів. Київ: НПУ імені М.П. Драгоманова, 1998. 296 с.

2. Зайцева Э.Е., Скобелев В.Г. Шифр на основе отображения Мандельброта. Вестник ТГУ. Приложение. 2007. № 23. С.107 – 113.

3. Карпухин А.В., Кириченко Л.О., Грицив Д.И., Ткаченко А.А. Применение методов нелинейной динамики и фрактального анализа для оценивания работы инфокоммуникационных систем с протоколом TCP. Электронный журнал Cloud of Science. 2014. Том 1, № 2. С. 258 – 271.

4. Мандельброт Б. Фрактальна геометрія природи. Москва: Інститут комп'ютерних досліджень. 2002. 656 с.

5. Потапов А.А. Фракталы в радиофизике и радиолокаци. Москва: Логос, 2002. 664 с.

6. Уэлстид С. Фракталы и вейвлеты для сжатия изображений в действии. Москва: Триумф, 2003. 320 с.

7. Алмазов А.А. Фрактальная теория рынка Forex. Москва: Адмирал Маркетс, 2009. 291с.

8. Воробьев А.Д. Использование фрактальной теории в стратегическом планировании и управлении. Менеджмент в России и за рубежом. 2006. №1. С. 178 – 188.

9. Мандельброт Б. Фракталы, случай и финансы. Москва-Ижевск: Регулярная и хаотическая динамика, 2004. 256 с.

10. Михайловська О.В. Самоорганізація світового інвестиційного процесу в умовах глобалізації: можливості фрактального аналізу. Актуальні проблеми економіки. 2009. №1. С. 218 – 228.

11. Петерс Э. Фрактальный анализ финансовых рынков. Москва: Интернет-Трейдинг, 2004. 286 с.

12. Працьовитий М.В., Свинчук О.В. Розсіювання значень однієї фрактальної неперервної немонотонної функції канторівського типу. Нелінійні коливання. 2018. Том 21, № 1. С. 116 – 130.

13. Локтев А.А., Залетдинов А.В. Использование фракталов в задачах обеспечения информационной безопасности. Вестник ТГУ, т. 15, вып. 2, 2010. С. 599 – 604,

14. Киричок П.О., Коростіль Ю.М., Шевчук А.В. Методи захисту цінних паперів та документів суворого обліку. Київ: КПІ, 2008. 368 с.

15. Авраменко В.П., Ткаченко В.П., Чібірєв А.Д. Методи підвищення якості захисту інформації на основі використання фрактальних функцій. Біоніка інтелекту. 2010. №1 (72). С. 55 – 60.

16. Дронюк І., Рибалко Є. Метод захисту документів на основі фракталів. Вісник Національного університету «Львівська політехніка». Комп'ютерні науки та інформаційні технології. 2012. № 732. С. 389 – 394.

17. Назаркевич М.А., Дронюк І.М., Троян О.А., Томащук Т.Ю. Розробка методу захисту документів латентними елементами на основі фракталів. Захист інформації. 2015. Том 17, №1. С. 21 – 26.

18. Никонов В.Г., Зобов А.И. О возможности применения фрактальных моделей при построении систем защиты информации. Computational nanotechnology. 2017. № 1. С. 39 – 49.

19. Ortiz S.M., Parra O., Miguel J. Espitia R. Encryption through the use of fractals International Journal of Mathematical Analysis. 2017. Vol. 11, №21. P. 1029 – 1040.

20. Agarwal S. Symmetric Key Encryption using Iterated Fractal Functions. International Journal of Computer Network and Information Security (IJCNIS). 2019. Vol. 9, №4. P. 1 – 9.

References

1. Pratsovytyi M.V. (1998) "Fractal Approach in Singular Distribution Studies". Kyiv: NPU imeni M.P. Draghomanova. 296 p.

2. Zajczeva E.E., Skoblev B.G. (2007) "Cipher based on the Mandelbrot mapping". Vestnik TGU. Prilozhenie, No. 23. P.107 – 113.

3. Karpukhin A.V., Kirichenko L.O., Gricziv D.I., Tkachenko A.A. (2014) "Application of the methods of nonlinear dynamics and fractal analysis to evaluate the operation of infocommunication systems with the TCP protocol". Elektronnyj zhurnal Cloud of Science, Vol. 1, No. 2. P. 258 – 271.

4. Mandelbrot B. (2002) Nature's fractal geometry. Moskva: Instytut komp'iuternykh doslidzhen. 656 p.

5. Potapov A.A. (2002) Fractals in radiophysics and radiolocation. Moskva: Logos. 664 p.

6. Uelstid S. (2003) Fractals and wavelets to compress images in action. Moskva: Triumf. 320 p.

7. Almazov A.A. (2009) Fractal theory of Forex market. Moskva: Admiral Markets. 291 p.

8. Vorob'ev A.D. (2006) "The use of fractal theory in strategic planning and management". Menedzhment v Rossii i za rubezhom. No. 1. P. 178 – 188.

9. Mandel'brot B. (2004) Fractals, Case and Finance. Moskva-Izhevsk: Regulyarnaya i khaoticheskaya dinamika. 256 p.

10. Mykhailovska O.V. (2009) "Self-organization of the world investment process in the conditions of globalization: possibilities of fractal analysis". Aktualni problemy ekonomiky, No. 1. P. 218 – 228.

11. Peters E. (2004) Fractal analysis of financial markets. Moskva: Internet-Trejding. 286 p.

12. Pratsovytyi M.V., Svynchuk O. V. (2018) "Spread of values a Canor-type fractal continuous nonmonotone function". Neliniini kolyvannia, Vol. 21, No. 1. P. 116 – 130.

13. Loktev A.A., Zaletdinov A.V. (2010) "The use of fractals in the tasks of ensuring information security". Vestnik TGU, No. 15 (2). P. 599 – 604.

14. Kyrychok P.O., Korostil Yu.M., Shevchuk A.V. (2008) Methods of protection of securities and documents of strict accounting. Kyiv: KPI. 368 p.

15. Avramenko V.P., Tkachenko V.P., Chibiriev A.D. (2010) "Methods to improve the quality of information protection based on the use of fractal functions". Bionika intelektu, No. 1 (72). P. 55 – 60.

16. Droniuk I., Rybalko Ye. (2012) "A method of protecting documents based on fractals". Visnyk Natsionalnoho universytetu "Lvivska politekhnika": Komp'iuterni nauky ta informatsiini tekhnolohii. No. 732. P. 389 – 394.

17. Nazarkevych M.A., Droniuk I.M., Troian O.A., Tomashchuk T.Yu. (2015) "Developing a Method for Securing Documents with Fractal-Based Latent Elements". Zakhyst informatsii, No. 17 (1). P. 21 – 26.

18. Nikonov V.G., Zobov A.I. (2017) "On the Possibility of Using Fractal Models in Building Information Security Systems". Computational nanotechnology, No. 1. P. 39 – 49.

19. Ortiz S.M., Parra O., Miguel J. Espitia R. (2017) Encryption through the use of fractals International Journal of Mathematical Analysis, Vol. 11 (21). P.1029 – 1040.

20. Agarwal S. (2019) Symmetric Key Encryption using Iterated Fractal Functions. International Journal of Computer Network and Information Security (IJCNIS), Vol. 9 (4). P. 1 – 9.