ISSN 2707-1898 (print)
Український журнал інформаційних технологій
Ukrainian Journal of Information Technology
http://science.lpnu.ua/uk/ujit
https://doi.org/10.23939/10.23939/ujit2024.02.098
Article received 05.07.2024 p.
Article accepted 19.11.2024 p.
UDC 004.832.3:519.711

Correspondence author
A. M. Kovalchuk
akm805@ukr.net

А. М. Ковальчук
Національний університет "Львівська політехніка", м. Львів, Україна

ВИКОРИСТАННЯ ФРАКТАЛЬНИХ ПЕРЕТВОРЕНЬ ТА ЇХ СИСТЕМ ПРИ ШИФРУВАННІ – ДЕШИФРУВАННІ МОНОХРОМНИХ ЗОБРАЖЕНЬ

У статті описано використання елементів алгоритму RSA у фрактальних квадратичних перетвореннях та системах фрактальних перетворень під час шифрування / дешифрування монохромних зображень. Зображення є одним із найчастіше використовуваних видів інформації. Зважаючи на це, актуальним завданням є захист зображень від несанкціонованого використання та доступу. Основною умовою для створення захисту зображення є припущення: зображення – це стохастичний сигнал. Це дає змогу переносити класичні методи шифрування сигналів на випадок зображень. Але зображення є таким сигналом, який має, окрім типової інформативності даних, ще й візуальну інформативність, що привносить до проблем захисту нові завдання. Фактично створення атаки на зашифроване зображення можливе у двох випадках: за допомогою традиційного зламу методів шифрування або методів візуального оброблення зображень (методи виокремлення контурів, фільтрації тощо). Останні не забезпечують повного відтворення вхідного зображення, але дають змогу отримати деяку інформацію із зображення. В зв'язку з цим до методів шифрування у випадку їх використання стосовно зображень ставлять ще одну вимогу – повну зашумленість зашифрованого зображення. Це потрібно для того, щоб унеможливити використання методів візуального оброблення зображень.

Тому актуальним завданням є розроблення такого використання алгоритму RSA, щоб зберегти стійкість до дешифрування і забезпечити повну зашумленість зображення, що дасть змогу унеможливити застосування методів подальшого візуального оброблення зображень.

Одним зі способів вирішення такого завдання є використання елементів алгоритму RSA у математичних перетвореннях, зокрема у фрактальних алгоритмічних перетвореннях. Фрактальні перетворення можуть бути як лінійнійними, так і квадратичними, існують також системи таких фрактальних перетворень.

Ключові слова: шифрування, дешифрування, фрактальний алгоритм, контур, зображення, лінійний фрактал, квадратичний фрактал, система фрактальних алгоритмів.

Вступ / Introduction

Основною складовою криптографічної безпеки є інформаційна безпека, яка [11] визначає захищеність систем оброблення і зберігання даних для забезпечення конфіденційності, доступності й цілісності інформації.

За визначенням державного стандарту [12], інформаційна безпека визначає заходи, спрямовані на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення. Отже, інформаційна безпека, а відтак функціональна безпека визначають захист від несанкціонованого доступу до даних і забезпечення надійності та стійкості до навмисних впливів. Усе це безпосередньо стосується ефективності функціонування інформаційних систем взагалі.

Наявність у зображенні контурів є важливою характеристикою зображення. Завдання виокремлення контурів потребує застосування операцій над сусідніми елементами, які чутливі до змін і пригашують ділянки сталих рівнів яскравості, тобто контур – це область, де здійснюють зміни, вона стає світлою, тоді як інші частини зображення можуть залишаютися незмінними [2].

Тобто ідеальний контур – це розрив функції просторових рівнів яскравості в площині зображення. Тому виокремлення контура призводить до пошуку найвідчутніших змін, а саме – максимумів модуля градієнта [6]. Це одна з причин того, що контури не зникають в зображенні у разі використання системи RSA для шифрування, оскільки таке шифрування ґрунтується на піднесенні до степеня за модулем деякого натурального числа. Через це на контурі й на близьких до нього пікселях підняття до степеня значення яскравостей створює ще більший розрив.

Існують різні алгоритми виокремлення контурів, наприклад, відстежувальні алгоритми. Такі алгоритми ґрунтуються на тому, що на зображенні відшукують об'єкт (першу точку об'єкта), а контур об'єкта відстежується і векторизується. Перевага цього алгоритму в його простоті. Недоліки – послідовна реалізація і деяка складність оброблення і пошуку внутрішніх контурів. Приклад такого алгоритму – "алгоритм жука" наведено на рис. 1.

Рух розпочинається з білого фрагмента у напрямку до чорного. Коли він потрапляє на елемент з чорного фрагмента, то повертає ліворуч і переходить до наступного. Якщо новий елемент білий, то жук повертає направо, інакше – наліво. Процес повторюється доти, доки жук не повернеться у вихідний елемент. Саме координати точок переходу з білого на чорне та з чорного на біле й описують контур об'єкта.

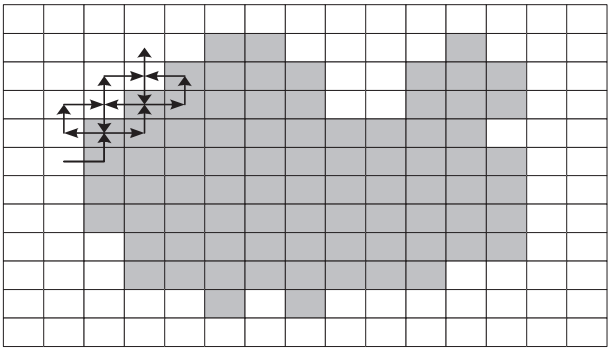

Рис. 1. Схема відстежувального алгоритму /
Scheme of the tracking algorithm

Об'єкт дослідження – використання елементів алгоритму RSA у фрактальних перетвореннях та їх системах для криптографічного захисту зображень.

Предмет дослідження – методи і засоби використання елементів алгоритму RSA в математичних перетвореннях з метою шифрування – дешифрування монохромних зображень.

Мета роботи – використання елементів алгоритму RSA в математичних перетвореннях для збереження криптографічної стійкості та забезпечення повної зашумленості зашифрованого зображення, з метою унеможливити застосування методів візуального оброблення зображень.

Для досягнення зазначеної мети встановлено такі основні завдання дослідження:

- виконати аналіз основних досліджень та публікацій;
- навести основні характеристики монохромних зображень та їх математичний опис;
- здійснити аналіз фрактальних алгоритмів та їх систем;
- вказати особливості шифрування – дешифрування по одному і по двох рядках матриці інтенсивностей пікселів зображення;
- навести результати прикладів шифрування – дешифрування у візуалізованому форматі.

Аналіз останніх досліджень та публікацій. Як відомо, *криптографічна стійкість* – це здатність криптографічного алгоритму протистояти криптоаналізу [4], [5], [6]. Стійким вважають алгоритм, який для успішної атаки вимагає від противника значних обчислювальних ресурсів, великого обсягу перехоплених відкритих і зашифрованих повідомлень чи такого ж часу розкриття, що після його закінчення захищена інформація буде вже не актуальна тощо. Здебільшого не можна математично довести криптостійкість, можна тільки уразливості криптографічного алгоритму. Такі системи можна будувати за допомогою випадкового ключа шифрування, довжина якого не менша від довжини відкритого тексту. На практиці використовують системи, які можна зламати, але за доволі тривалий час [7], [8], [9], [10].

Проблеми захисту зображень в інформаційних системах шифрування – дешифрування відображено в працях М. Діффі, К. Шеннона, М. Хелмана, М. Карпінського. Система асиметричного кодування RSA має особливе значення серед численних криптографічних перетворень. Ця система забезпечує високий рівень захисту будь-яких даних, якщо ключі цієї системи мають достатньо великі значення. Це, зокрема, і дає змогу забезпечити захист зашифрованих зображень.

Результати дослідження та їх обговорення / Research results and their discussion

Характеристики зображення. Нехай зображення має ширину l і висоту h. Його можна розглядати як матрицю пікселів

$$<dtp_{i,j}>_{1\le i\le n,\ 1\le j\le m}, \qquad (1)$$

де $dtp_{i,j}$ – піксель із координатами i та j; n і m – кількість точок по ширині l та висоті h.

У загальному випадку n і m залежать від l та h, тобто

$$n = n(l) \ \text{ і } \ m = m(h). \qquad (2)$$

Надалі вважатимемо, що зображенню у відповідність ставлять матрицю інтенсивностей пікселів зображення

$$\mathrm{C} = \begin{pmatrix} c_{1,1} & \dots & c_{1,m} \\ \dots & \dots & \dots \\ c_{n,1} & \dots & c_{n,m} \end{pmatrix}, \qquad (3)$$

де c_{ij} – значення інтенсивності напівтонових зображень пікселя dtp_{ij}.

Існують певні проблеми шифрування зображення, а саме на різкофлуктуаційних зображеннях частково можуть зберігатися контури [1, 4].

Математично ідеальний контур – це розрив просторової функції рівнів яскравості пікселів у площині зображення. Тому виокремлення контура означає пошук найрізкіших змін, тобто максимумів модуля вектора градієнта [2]. Це одна із причин того, що контури залишаються на зображенні у разі шифрування в системі RSA, оскільки шифрування тут ґрунтується на піднесенні до степеня за модулем натурального числа. На контурі й на сусідніх із ним пікселях таке піднесення до степеня значення яскравостей дає ще більший розрив.

У [7] для шифрування – дешифрування зображень в градаціях сірого запропоновано використання лінійних фрактальних перетворень. У цій роботі для шифрування – дешифрування різкофлуктуаційних зображень запропоновано використовувати і квадратичні фрактальні перетворення.

Шифрування і дешифрування за одним рядком матриці зображення

Нехай $\boldsymbol{P}$ і $\boldsymbol{Q}$ – пара довільних простих чисел. Шифрування здійснюється поелементно із використанням квадратичного фрактального перетворення елементів матриці зображення $\boldsymbol{C}$ за формулою:

$$x_n^{(k)} = P\left(x_n^{(k-1)} + f(n)\right)^2 - Q, \qquad (4)$$

де n – кількість елементів у рядку, $f(n)$ – деяка функція зашумлення, k – номер фрактальної ітерації, $x_n^{(0)} = x_n$ – n-й елемент рядка матриці інтенсивностей пікселів (3). Під час шифрування використано всі рядки матриці (3).

Дешифрування виконують за такою формулою оберненого перетворення

$$x_n^{(k-1)} = \sqrt{\frac{x_n^{(k)} + Q}{P}} - f(n), n = 1, 2, ..., N_0. \qquad (5)$$

Результати наведено на рис. 2–4 після п'ятої фрактальної ітерації.

Шифрування і дешифрування за двома рядками матриці зображення.

$$\left\{\frac{x_m = x_{m-1} - y_{m-1} + (M-i)\,j(P^e \bmod (K-i))}{y_m = 2x_{m-1} * y_{m-1} + (M-i)\,j(Q^e \bmod (K-i))}\right\},$$

$$i = 1,2,...,N;\ j = 1,2,...,M-1\ .$$

Нехай P і Q – пара довільних простих чисел, $K = (P-1)(Q-1)$, $L = P*Q$. Шифрування відбувається із використанням фрактального перетворення двох відповідних елементів двох послідовних рядків матриці зображення C за такими формулами:

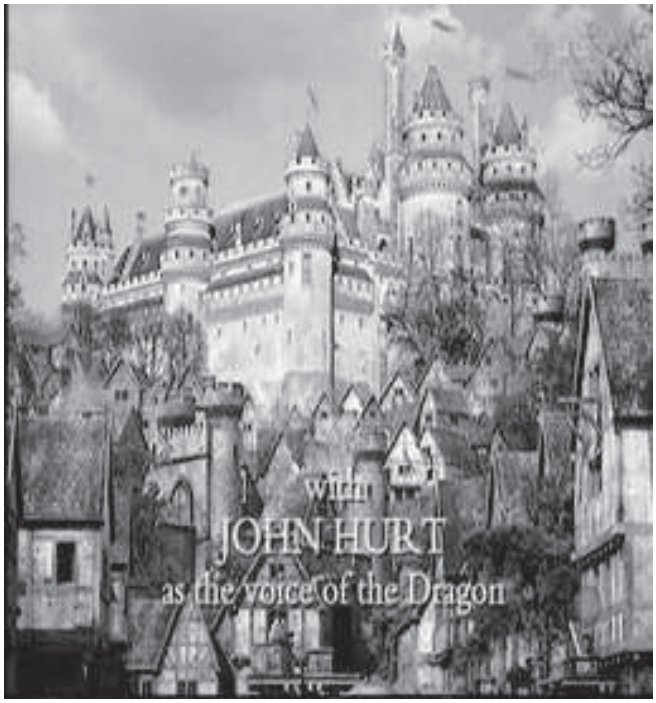

Рис. 2. Початкове зображення / Initial image

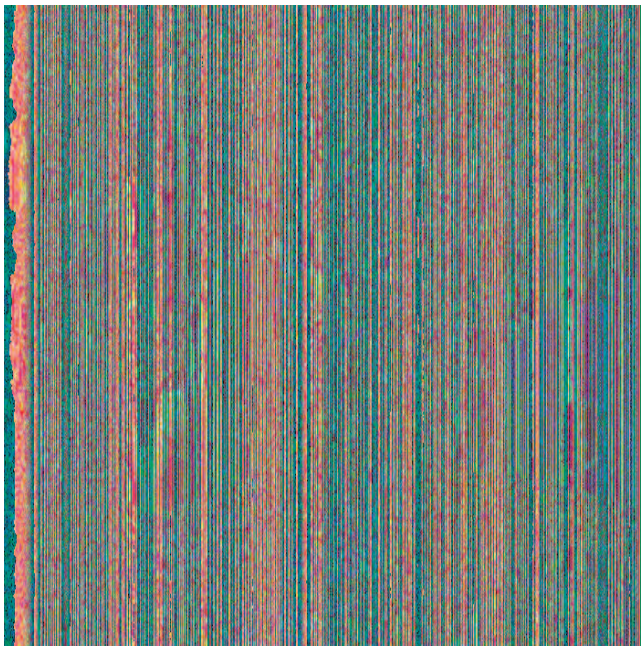

Рис. 3. Зашифроване зображення / Encrypted image

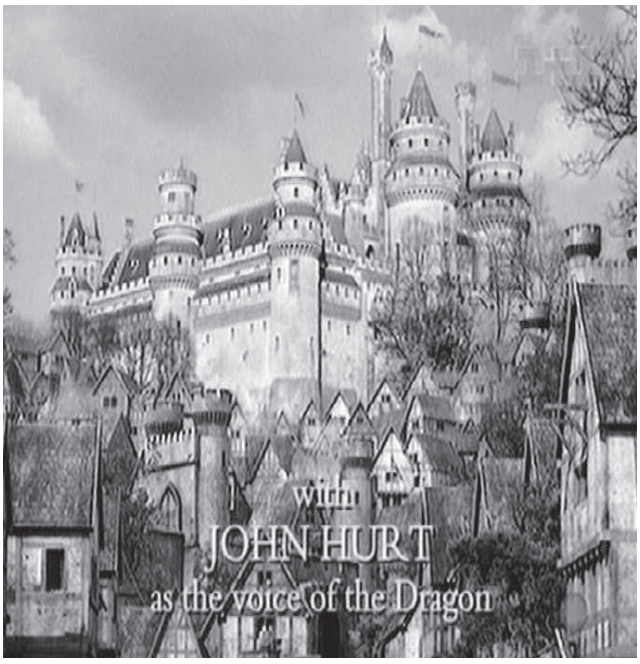

Рис. 4. Дешифроване зображення / Decrypted image

де N – кількість стовпців, M – кількість рядків, $ed \equiv 1 \bmod L, x_0 = c_{j,i}, y_0 = c_{j+1,i}$.

$$\left\{\begin{array}{l} x_{m-1} = \dfrac{A_m + \sqrt{D_m}}{2} \\ y_{m-1} = \dfrac{2B_m}{A_m + \sqrt{D_m}} \end{array}\right\},$$

де

$$D_m = A_m^2 + 4B_m,\ A_m = x_m - (M-i)j(P^e \bmod K - i),$$

$$B_m = \frac{y_m - (M-i) * j * (P^e \bmod (K-i))}{2}.$$

Результати шифрування – дешифрування за різних значень P і Q для того самого зображення наведено на рис. 5. Візуальне порівняння початкового і дешифрованого зображення вказує на незначну відмінність між ними, якщо вибрано прості числа P і Q. Зашифровані зображення за різних значень простих P і Q відрізняються, оскільки матрицю інтенсивностей пікселів зашифрованого зображення отримують, використовуючи значення вибраних простих у відповідних математичних фрактальних перетворень.

Обговорення результатів дослідження. Порівнюючи зашифровані зображення, можна зробити висновок, що використання елементів алгоритму RSA у фрактальних перетвореннях у разі шифрування монохромних зображень дає достатньо позитивний результат: усі контури під час шифрування повністю зникають, що повністю деформує зображення.

Наукова новизна отриманих результатів дослідження – розроблено математичні моделі використання елементів алгоритму RSA у фрактальних перетвореннях та системах фрактальних перетворень з використанням одного та двох рядків матриці інтенсивностей пікселів монохромного зображення. Це забезпечує криптографічну стійкість та повну зашумленість зашифрованих зображень, що унеможливлює використання методів їх візуального опрацювання.

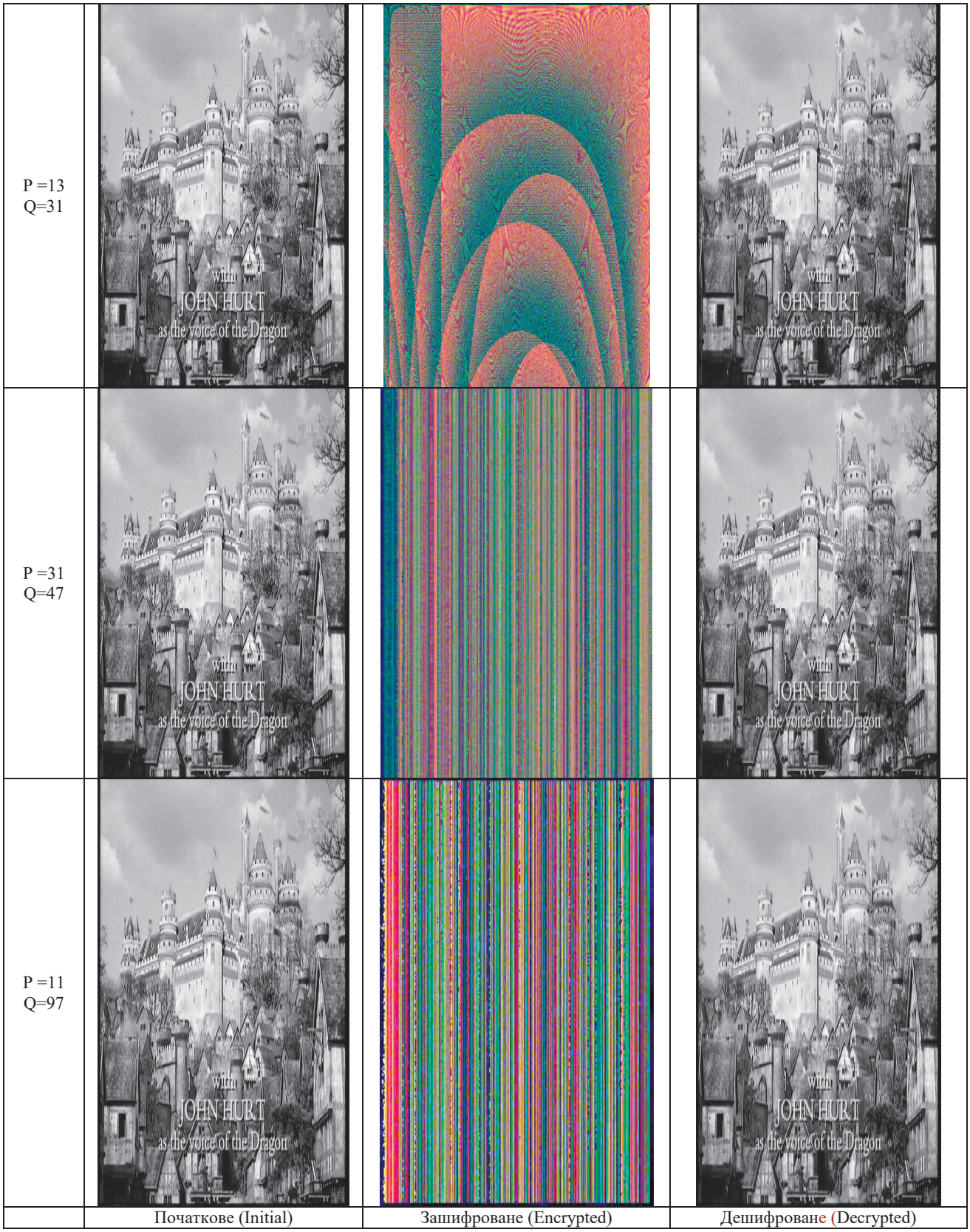

Рис. 5. Зашифроване – дешифроване зображення за різних P, Q / Encrypted-Decrypted image at different P, Q

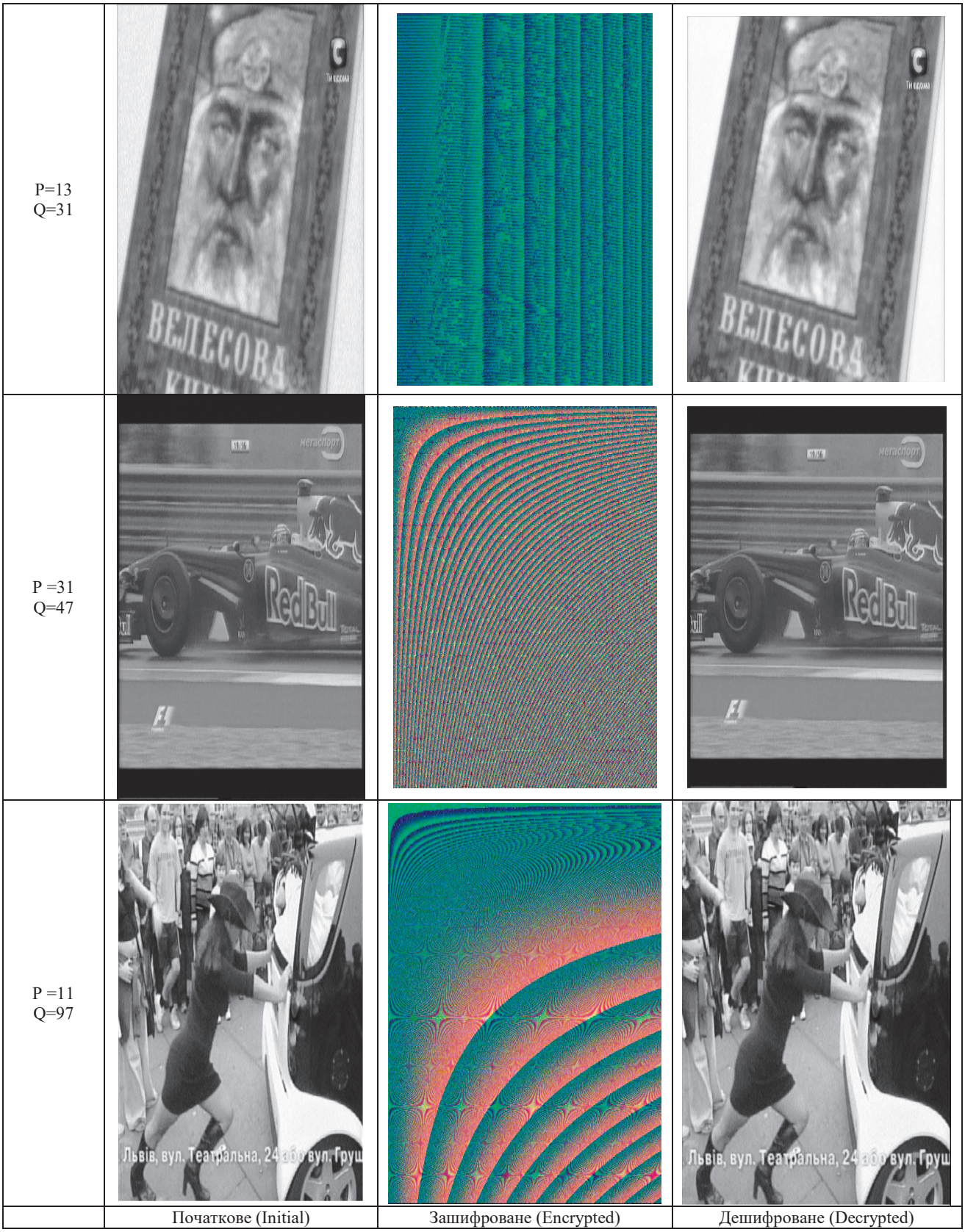

Рис. 6. Зашифровані – дешифровані зображення за різних P, Q / Encrypted-Decrypted images at different P, Q

Висновки/ Conclusions

У роботі розв'язано актуальну науково-прикладну задачу, яка полягає у розробленні інформаційної технології підвищення криптографічної стійкості інформаційно-керуючих систем, які ґрунтуються на комунікаційних процедурах із застосуванням універсальних засобів з метою мінімізації обчислювальних ресурсів у процесах забезпечення надійності, стійкості та безпеки функціонування таких систем.

Отримано такі науково-практичні результати:

1. Сумісне використання для шифрування елементів алгоритму RSA і фрактальних перетворень

дало змогу запропонувати метод підвищення криптографічної стійкості систем критичного застосування у разі передавання у комунікаційних процедурах цифрових зображень із глибиною кольору до 4 байт, що дає змогу підвищити стійкість функціонування інформаційних систем.

2. Інтегрування фрактальних операторів у схему криптографічного шифрування дає можливість підвищити загальний рівень криптографічної безпеки систем оброблення і комунікаційного обміну повноколірних зображень в автоматизованих системах критичного застосування.

З порівняння рис. 3-4 і рис. 5-6 видно, що шифрування із використанням одного рядка матриці зображення відрізняється від шифрування за двома рядками цієї ж матриці. Контури в обох зашифрованих зображеннях відсутні. Дешифроване зображення в першому випадку на рис. 4 візуально не відрізняється від дешифрованих зображень (рис. 5, 6) за другим алгоритмом. Зашифровані зображення відрізняються як структурно, так і за кольором. Вказані алгоритми можна використовувати для передавання графічних зображень і стосовно будь-якого типу зображень, але найбільша ефективність досягається у випадку шифрування зображень з чітко виокремленими контурами.

У разі шифрування за двома рядками матриці інтенсивностей пікселів за тих самих значень довільних простих чисел P і Q візуально зашифровані зображення відрізняються, оскільки відрізняються і початкові зображення. Це підтверджується попарним порівнянням зашифрованих зображень рис. 5–6 за тих самих значень простих чисел P і Q. Така відмінність зумовлена тим, що матриці інтенсивностей пікселів у різних зображень неоднакові.

Обидва вказані перетворення можна використати і стосовно кольорових зображень. Але, незалежно від типу зображення, пропорційно до розмірності вхідного зображення може зростати розмір шифрованого зображення.

Підвищується також стійкість процедури шифрування, оскільки для шифрування – дешифрування використовують довільні прості числа, які можуть бути доволі великими. А від цього залежить криптографічна стійкість шифрування. Для шифрування за одним рядком матриці інтенсивностей пікселів використано два довільні прості числа, а за двома рядками матриці – всі елементи алгоритму RSA.

Розроблене на основі отриманих теоретичних результатів вказаного дослідження програмне рішення забезпечує збереження інформації не лише у разі передавання її комунікаційними каналами зв'язку, а й у випадку організації стійкого персоніфікованого захисту.

Використання елементів алгоритму RSA з фрактальними перетвореннями дало змогу удосконалити метод досягнення необхідного рівня криптографічної безпеки в процедурах захисту напівтонових зображень із глибиною кольору до двох байтів, що дає можливість підвищити рівень безпеки систем без інформаційних втрат у комунікаційних процедурах автоматизованих систем загального і критичного застосування.

References

1. Kovalchuk, A., Izonin, I., Straus, C., & Kustra, N. (2019). Image encryption and decryption schemes using linear and quadratic fractal algorithms and their systems. *1-st International Workshop on Digital Content and Smart Multimedia, DCSMart, 2019. Lviv, Ukraine*.
2. Ozkaynak, F., Celik, V., & Ozer, A. B. (2017). A new S-box construction method based on the fractional-order chaotic Chen system. *Signal, Image and Video Processing, 11*, 659-664. https://doi.org/10.1007/s11760-016-1007-1
3. Kovalchuk, A., & Lotoshynska, N. (2018).Elements of RSA Algorithm and Extra Noising in a Binary Linear-Quadratic Transformations during Encryption and Decryption of Images. *Proceedings of the 2018 IEEE 2nd International Conference on Data Stream Mining and Processing, DSMP 2018, 8478471, pp. 542–544.* https://doi.org/10.1109/DSMP.2018.8478471
4. Medykovskyy, M., Lipinski, P., Troyan, O., Nazarkevych, M. (2015). Methods of protection document formed from latent element located by fractals. *In 2015 X-th International Scientific and Technical Conference "Computer Sciences and Information Technologies" (CSIT), Lviv, Ukraine. IEEE, 70–72.* https://doi.org/10.1109/STC-CSIT.2015.7325434
5. Bruce Schneier. (2003). Applied Cryptography. M.: Triumph, 815 p. (in Russian).
6. Вербіцький, О. В. (1998). Вступ до криптології. Львів: Видавництво науково-технічної літератури, *247* (in Ukrainian).
7. Kovalchuk, A., & Stupen, M. (2015). Binary linear-quadratic conversion with elements of RSA-algorithm and additional noise in the image protection. (Ser. Computer sciences and information technologies). *Bulletin of NULP,* 826, 191–196 (in Ukrainian).
8. Rashkevych, Y., Kovalchuk, A., Peleshko, D., & Kupchak, M. (2009). Stream Modification of RSA algorithm for image coding with contour extraction. *Proceedings of the X-th International Conference CADSM, 2009. Lviv-Polyana, Ukraine.*
9. Wang, J., Zhu, Y., Zhou, C., & Qi, Z. (2020). Construction Method and Performance Analysis of Chaotic S-Box Based on a Memorable Simulated Annealing Algorithm. *Symmetry,* 12, 2115. https://doi.org/10.3390/sym12122115
10. Wagh, D. P., Fadewar, H. S., & Shinde, G. N. (2020). Biometric Finger Vein Recognition Methods for Authentication. *In Computing in Engineering and Technology, pp. 45–53.* https://doi.org/10.1007/978-981-32-9515-5_5
11. Wikipedia (2024). Information security. Retrieved from: https://uk.wikipedia.org/wiki/Інформаційна_безпека
12. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Retrieved from: http://www.dstszi.gov.ua/_dstszi/doccatalog/document?_id=41650

A. M. Kovalchuk
Lviv Polytechnic National University, Lviv, Ukraine

THE USE OF FRACTAL CONVERTINGS AND THEIR SYSTEMS IN THE ENCRYPTION – DECRYPHATION OF MONOCHROME IMAGES

Fractals occupy a rather important and defining place in computer graphics. This is the construction of landscapes, trees, plants, even animals and the generation of fractal textures, as well as fractal image compression. Modern physics and mechanics are just beginning to study the behavior of fractal objects. And of course, fractals are used directly in mathematics itself, as well as in cryptography when protecting images.

The article describes the use of elements of the RSA algorithm in fractal quadratic transformations and systems of fractal transformations for encryption / decryption of monochrome images. Images are one of the most used types of information. Because of this, protecting images from unauthorized use and access is an urgent task. The main condition for creating image protection is the assumption that the image is a stochastic signal. This allows us to transfer classical signal encryption methods to the case of images. But the image is such a signal that, in addition to the typical informativeness of data, also has visual informativeness, which brings new challenges to the protection problems. In fact, creating an attack on an encrypted image is possible in two cases: through traditional hacking of encryption methods, or through methods of visual image processing (methods of extracting contours, filtering, etc.). The latter do not provide a complete reproduction of the input image, but provide an opportunity to obtain some information from the image. In this regard, another requirement is put forward to encryption methods in the case of their use in relation to images – complete noise of the encrypted image. This is necessary in order to prevent the use of visual image processing methods.

Therefore, the urgent task is to develop such a use of the RSA algorithm in order to: preserve the resistance to decryption and ensure full noise of the image in order to make it impossible to use the methods of further visual image processing. One of the ways to solve this problem is to use elements of the RSA algorithm in fractal algorithmic transformations and their systems.

One of the ways to solve this problem is to use elements of the RSA algorithm in mathematical transformations, in particular, in fractal algorithmic transformations.

Fractal transformations can be both linear and quadratic. And also systems of such fractal transformations. Encryption – decryption can be performed both with additional noise and without additional noise.

Keywords: encryption, decryption, fractal algorithm, contour, image, linear fractal, quadratic fractal, system of fractal algorithms.

Інформація про авторів:

Ковальчук Анатолій Михайлович, ст. викладач, кафедра інформаційних технологій видавничої справи.
E-mail: anatolii.m.kovalchuk@lpnu.ua; http://orcid.org/0000-0001-5910-4734

Цитування за ДСТУ: Ковальчук А. М. Використання фрактальних перетворень та їх систем при шифруванні – дешифруванні монохромних зображень. *Український журнал інформаційних технологій*. 2024, т. 6, № 2. С. 98–104.

Citation APA: Kovalchuk, A. M. (2024). The use of fractal convertings and their systems in the encryption – decryphation of monochrome images. *Ukrainian Journal of Information Tecnology*, *6*(2), 98–104. https://doi.org/10,23939/UJIT2024.02.098