УДК 681.142.2; 622.02.658.284; 621. 325

[1)]І. Цмоць, [2)]А. Ковальчук, [1)]М. Ступень
Національний університет "Львівська політехніка",
[1)]кафедра автоматизованих систем управління
[2)]кафедра інформаційних технологій видавничої справи

СИСТЕМИ ФРАКТАЛЬНИХ АЛГОРИТМІВ У ШИФРУВАННІ – ДЕШИФРУВАННІ ЗОБРАЖЕНЬ З ДОДАТКОВИМ ЗАШУМЛЕННЯМ

Запропоновано алгоритм застосування систем лінійних фрактальних перетворень до шифрування і дешифрування зображень з чітко виділеними контурами.

Ключові слова: лінійний фрактал, шифрування, дешифрування, контур.

Proposed algorithm application of linear transformations for fractal encrypting and decrypting images with well-selected contours.

Key words: linear fractal, encryption, decryption, contour.

Вступ

Нехай зображенню у відповідність ставиться матриця кольорів

$$\mathbf{C}=\begin{pmatrix} c_{1,1} & \dots & c_{1,N} \\ \dots & \dots & \dots \\ c_{M,1} & \dots & c_{M,N} \end{pmatrix}. \qquad (1)$$

По відношенню до зображення існують певні проблеми його шифрування, а саме: частково зберігаються контури на різко флуктуаційних зображеннях [3, 4].

Наявність у зображенні контурів є важливою характеристикою зображення. Задача виділення контуру вимагає використання операцій над сусідніми елементами, які є чутливими до змін і пригашають області постійних рівнів яскравості [2].

Математично ідеальний контур – це розрив просторової функції рівнів яскравості в площині зображення. Тому виділення контуру означає пошук найрізкіших змін, тобто максимумів модуля вектора градієнта [2]. Це є однією з причин, через що контури залишаються в зображенні під час шифрування в системі RSA, оскільки шифрування тут базується на піднесенні до степеня по модулю деякого натурального числа. При цьому на контурі і на сусідніх до контуру пікселах піднесення до степеня значення яскравостей дає ще більший розрив.

Фрактал (лат. fractus – подрібнений, дробовий) – нерегулярна, самоподібна структура. У широкому розумінні фрактал означає фігуру, малі частини якої в довільному збільшенні є подібними до неї самої.

Лінійні і квадратичні фрактальні алгоритми можуть бути застосовані і під час шифрування і дешифрування зображень [5, 6].

Шифрування і дешифрування по двох рядках матриці зображення

Нехай $\boldsymbol{P,Q}$ – пара довільних простих чисел, $\boldsymbol{K = (P-1)(Q-1)}$, $\boldsymbol{L = PQ}$ Шифрування відбувається з використанням фрактального перетворення двох відповідних елементів двох послідовних рядків матриці зображення $\boldsymbol{C}$ за такими формулами:

$$\begin{cases} x_m = x_{m-1} - y_{m-1} + (M-i)\,j\,(P^e \bmod K - i) \\ y_m = 2x_{m-1}y_{m-1} + (M-i)\,j\,(Q^d \bmod K - i) \end{cases}, \quad i = 1,2,\dots,N, \quad j = 1,2,\dots,M-1, \qquad (2)$$

де N – ширина зображення, M – висота зображення, $ed \equiv 1 \bmod L$, $x_0 = c_{j,i}$, $y_0 = c_{j+1,i}$.

Дешифрування проводиться у зворотному порядку за формулами

$$x_{m-1} = \frac{A_m + \sqrt{D_m}}{2}, \quad y_{m-1} = \frac{2B_m}{A_m + \sqrt{D_m}}, \tag{3}$$

де $D_m = A_m^2 + 4B_m$, $A_m = x_m - (M - i)\,j(P^e \bmod K - i)$, $B_m = (y_m - (M - i)\,j(Q^d \bmod K - i))/2$.
Результати наведені на рис. 1–3.

Рис. 1. Початкове зображення

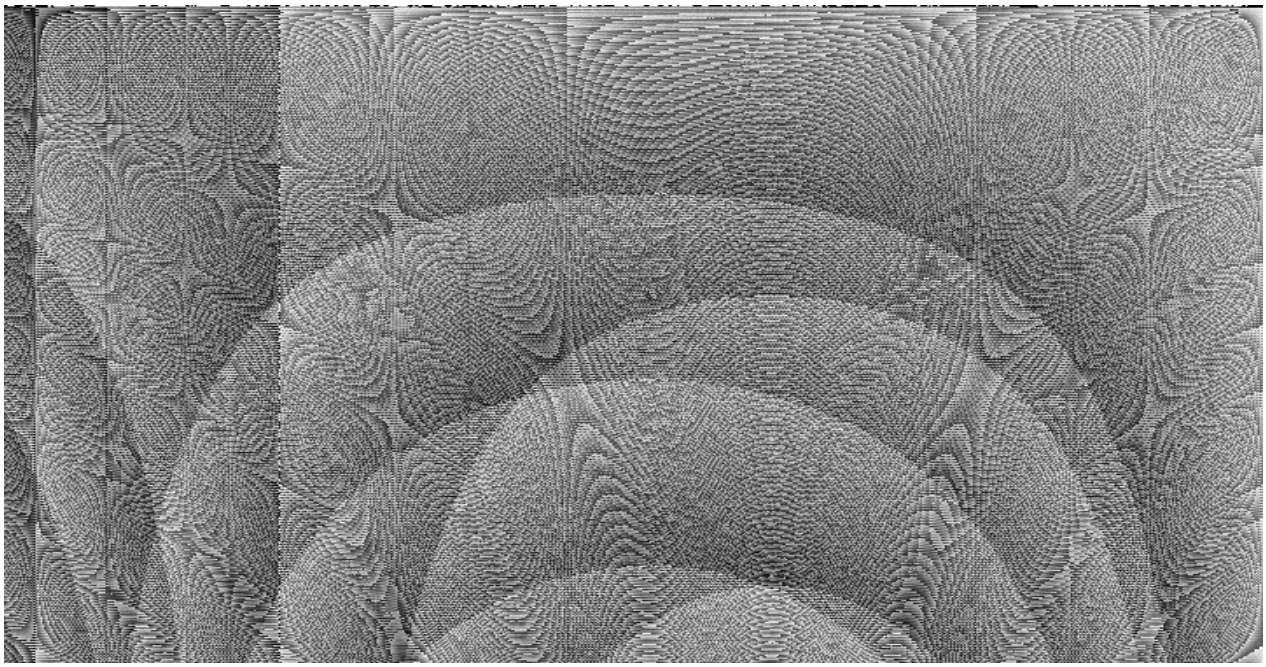

Рис. 2. Зашифроване зображення

Рис. 3. Дешифроване зображення

Шифрування і дешифрування по одному рядку матриці зображення

Нехай P, Q – пара довільних простих чисел, $K = (P-1)(Q-1)$, $L = PQ$. Шифрування відбувається з використанням фрактального перетворення двох за порядком елементів кожного рядка матриці зображення C за такими формулами:

$$\begin{cases} u_m = u_{m-1} - v_{m-1} + (M+i)j(P^e \bmod K - i) \\ v_m = 2u_{m-1}v_{m-1} + (M+i)j(Q^d \bmod K - i) \end{cases}, \quad i = 1,2,...,N, \quad j = 1,2,...,M-1, \tag{2}$$

де N – ширина зображення, M – висота зображення, $ed \equiv 1 \bmod L$, $u_0 = c_{j,i}$, $v_0 = c_{j+1,i}$.

Дешифрування проводиться у зворотному порядку за формулами

$$\begin{aligned} u_{m-1} &= \frac{A_m + \sqrt{D_m}}{2} \\ v_{m-1} &= \frac{2B_m}{A_m + \sqrt{D_m}} \end{aligned}, \tag{3}$$

де $D_m = A_m^2 + 4B_m$, $A_m = u_m - (M+i)j(P^e \bmod K - i)$, $B_m = (v_m - (M+i)j(Q^d \bmod K - i))/2$.

Результати наведені на рис. 4–6.

Рис. 4. Початкове зображення

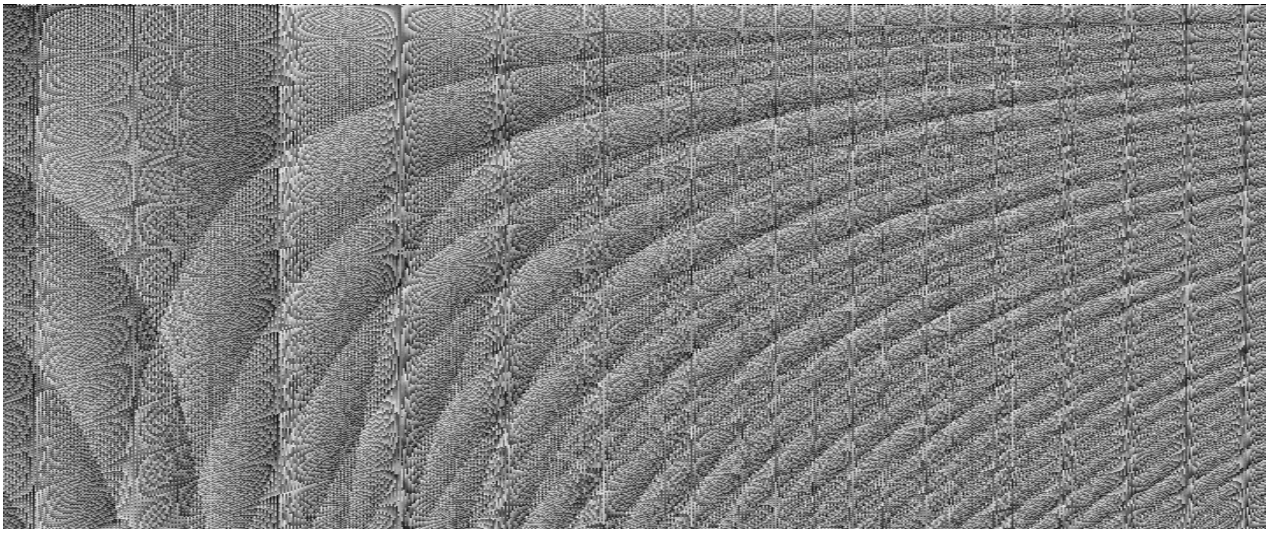

Рис. 5. Зашифроване зображення

Рис. 3. Дешифроване зображення

Висновки

З порівняння рис. 2 і 5 видно, що шифрування по одному рядку матриці зображення відрізняється від шифрування по двох рядках цієї матриці. Контури в обох зашифрованих зображеннях відсутні. Дешифроване зображення в першому випадку на рис. 3 візуально не відрізняється від дешифрованого зображення (рис. 6) по другому алгоритму. Відрізняються також зашифровані зображення структурно і по кольору. Вказані алгоритми можуть бути використані під час передавання графічних зображень і можуть бути застосовані до будь-якого типу зображень, але найбільші переваги досягаються у разі використання зображень з чітко виділеними контурами.

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

1. Брюс Шнайер. Прикладная криптография. – М.: Триумф, 2003. – 815с. 2. Б.Яне. Цифровая обработка изображений. – М.: Техносфера, 2007. – 583 с. 3. Ю.М. Рашкевич, Д.Д. Пелешко, А.М. Ковальчук, М.З. Пелешко. Модифікація алгоритму RSA для деяких класів зображень // Технічні вісті 2008/1(27), 2(28). С. 59 – 62. 4. Y.Rashkevych, A.Kovalchuk, D.Peleshko, M.Kupchak. Stream Modification of RSA Algorithm For Image Coding with precize contour extraction. Proceedings of the X-th International Conference CADSM 2009. 24–28 February 2009, Lviv-Polyana, Ukraine. – P. 469–473. 5. Фабрі Л., Ковальчук А., Ступень М. Застосування фрактальних алгоритмів для шифрування і дешифрування зображень // Комп'ютерні науки та інформаційні технології, № 672, 2010. – С.262–267. 6. Фабрі Л., Ковальчук А., Ступень М. Шифрування і дешифрування зображень з використанням квадратичних фрактальних алгоритмів // Комп'ютерні науки та інформаційні технології, № 694, 2011. – С.180–184.