буферної зони між рухомим передньоплановим об'єктом та нерухомим фоном, тобто перехідної зони між зонами повного змазу та неспотвореною зоною.

Отримана методологія визначення буферної зони може бути основою розроблення ефективних деконволюційних методів усунення глобальних та локальних спотворень, які виникають внаслідок руху об'єкта чи пристрою реєстрації.

1. Дискретне перетворення Фур'є. [Електронний ресурс]. – Режим доступу :http://uk.wikipedia.org/wiki /%D0%94%D0%B8%D1%81%D0%BA%D1%80%D0% B5%D1%82%D0% BD%D0%B5_%D0%BF%D0%B5%D1%80%D0%B5%D1%82%D0%B2%D0%BE%D1%80%D0%B5% D0%BD%D0%BD%D1%8F_%D0%A4%D1%83%D1%80%27%D1%94. 2. Oliveira, João P., Mário AT Figueiredo, José M. Bioucas-Dias. Blind estimation of motion blur parameters for image deconvolution // Pattern Recognition and Image Analysis. Springer Berlin Heidelberg, 2007. 604-611. 3. Molina, Rafael, Javier Mateos, Aggelos K. Katsaggelos. Blind deconvolution using a variational approach to parameter, image, and blur estimation // Image Processing, IEEE Transactions on 15.12 (2006): 3715-3727. 4. Lucy, L. B. An iterative technique for the rectification of observed distributions // Astronomical Journal 79 (6), 1974, p *745–754. 5. Vaseghi S.V. Advanced Digital Signal Processing and Noise Reduction / Saeed V. Vaseghi. – 3rd ed, John Wiley & Sons Ltd, 2006. – 453 p.*

УДК 681.142.2; 622.02.658.284; 621. 325

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

ВИКОРИСТАННЯ КВАТЕРНАРНИХ ДРОБІВО-ЛІНІЙНИХ ФРАКТАЛЬНИХ ФОРМ ПРИ ШИФРУВАННЯ – ДЕШИФРУВАННІ ЗОБРАЖЕНЬ З ЕЛЕМЕНТАМИ АЛГОРИТМУ RSA

Запропоновано використання кватернарних дробово-лінійних форм з використанням елементів стандартного алгоритму RSA під час шифрування і дешифрування двовимірних зображень, як стійкого до несанкціонованого доступу до зображень з чітко виокремленими контурами.

Ключові слова: кватернарна форма, зображення, контур, стійкість шифрування.

An application of the kvaternarn fractional-linear form with using the standard elements of the RSA algorithm for encryption and decryption of two-dimensional images is resistant to unauthorized access to images clearly distinguished contours.

Key words: kvaternarna shape, image, contour, firmness encryption.

Вступ

Проблему підвищення якості систем захисту інформації можна розглядати з позиції економіки, науки і техніки, які зумовили бурхливий розвиток обчислювальної техніки, інформатики, мікроелектроніки, телекомунікацій тощо. Значний внесок у розвиток методів захисту інформації зробили такі вітчизняні й закордонні науковці: І.Д. Горбенко, А.А. Молдован, В.М. Рудницький, В.Ф. Шаньгін, Б. Шнайдер та інші.

Одним із найбільш поширених і стійких алгоритмів шифрування інформації є алгоритм RSA [1]. Він належить до найвживанішої групи алгоритмів з відкритим ключем. Безпека алгоритму RSA основана на ресурсозатратній факторизації великих натуральних чисел. При цьому відкритий і закритий ключі є

функціями двох простих чисел з розрядністю 100–200 десяткових цифр або більше.

Використання алгоритму шифрування RSA [1], як найстійкішого до несанкціонованого дешифрування кодованих сигналів, стосовно зображень, які дозволяють дуже строго виділяти контури, не дає задовільних результатів. На зашифрованому зображенні все ж таки можна розрізнити основні контури вхідного зображення. Тобто спостерігається ефект неповного зашумлення зображення.

Важливою характеристикою зображення є наявність у зображенні контурів. Задача виділення контура вимагає використання операцій над сусідніми елементами, які є чутливими до змін і пригашають області постійних рівнів яскравості, тобто контури – це ті області, де виникають зміни, стаючи світлими, тоді як інші частини зображення залишаються темними [2].

Існують певні проблеми шифрування зображення, а саме частково зберігаються контури на різко флуктуаційних зображеннях [3, 4].

Математично контур зображення – це розрив просторової функції рівнів яскравості в площині зображення. Тому виділення контура в зображенні означає пошук найрізкіших змін, тобто максимумів модуля вектора градієнта [2]. Це є однією з причин, через які контури залишаються в зображенні у разі шифрування в алгоритмом RSA, оскільки шифрування тут ґрунтується на піднесенні до степеня за модулем деякого натурального числа. При цьому на контурі й на сусідніх до контура пікселах піднесення до степеня значення яскравостей дає ще більший розрив.

Для захисту інформації найчастіше застосовують растрову і векторну графіку, а перспективними методами вважаються методи захисту інформації на основі використання фрактальних перетворень алгебраїчних дробово-лінійних форм.

Серед поширених фракталів прийнято виділяти три основні групи [5, 6]:

– *Алгебраїчні фрактали*, котрі створюються за допомогою нелінійних обчислювальних процесів у *n*-вимірних просторах. До цієї групи, зокрема, належить множина Мандельброта.

– *Геометричні фрактали*, котрі у двовимірному випадку створюються за допомогою ламаної – генератора. За один крок алгоритму кожен із відрізків ламаної замінюється на ламану-генератор і, отже, у відповідному масштабі створюється геометричний фрактальний образ. До цієї групи фракталів належать тріадна крива Коха і дракон Хартера.

– *Стохастичні фрактали*, котрі створюються ітераційним процесом з випадковими параметрами. Образи стохастичних фракталів дуже схожі на природні несиметричні дерева.

Вважатимемо, що зображенню у відповідність ставиться матриця кольорів

$$\mathbf{C}=\begin{pmatrix} c_{1,1} & \dots & c_{1,m} \\ \dots & \dots & \dots \\ c_{n,1} & \dots & c_{n,m} \end{pmatrix}.$$

Кватернарна дробово-лінійна форма має вигляд

$$t(x,y,z,m)=\frac{ax+by+fz+gm+d}{cx+dy+hz+km+\Delta}\ . \tag{1}$$

Використавши (1), виконаємо перетворення

$$\begin{cases} x_n=\dfrac{Ax_{n-1}+By_{n-1}+Fz_{n-1}+Gm_{n-1}+d}{Cx_{n-1}+Dy_{n-1}+Hz_{n-1}+Km_{n-1}+\Delta}; \\ y_n=\dfrac{Bx_{n-1}+Fy_{n-1}+Gz_{n-1}+Km_{n-1}+d}{Ax_{n-1}+Cy_{n-1}+Dz_{n-1}+Hm_{n-1}+\Delta}; \\ z_n=\dfrac{Fx_{n-1}+Gy_{n-1}+Kz_{n-1}+Hm_{n-1}+d}{Bx_{n-1}+Ay_{n-1}+Cz_{n-1}+Dm_{n-1}+\Delta}; \\ m_n=\dfrac{Gx_{n-1}+Ky_{n-1}+Hz_{n-1}+Dm_{n-1}+d}{Fx_{n-1}+By_{n-1}+Az_{n-1}+Cm_{n-1}+\Delta}; \end{cases} \tag{2}$$

де $A = P$, $B = Q$, $F = e$, $G = d$, $C = P$, $D = -Q$, $H = d$, $K = e$, $d = P, \Delta = Q$ – елементи стандартного алгоритму RSA, n – номер рівня фрактальності.

Обернене до (2) перетворення має вигляд

$$\begin{cases}(x_nC-A)x_{n-1}+(x_nD-B)y_{n-1}+(x_nH-F)z_{n-1}+(x_nK-G)m_{n-1}=d-x_n\Delta;\\(y_nA-B)x_{n-1}+(y_nC-F)y_{n-1}+(y_nD-G)z_{n-1}+(y_nH-K)m_{n-1}=d-y_n\Delta;\\(z_nB-F)x_{n-1}+(z_nA-G)y_{n-1}+(z_nC-K)z_{n-1}+(z_nD-H)m_{n-1}=d-z_n\Delta;\\(m_nF-G)x_{n-1}+(m_nB-K)y_{n-1}+(m_nA-H)z_{n-1}+(m_nC-D)m_{n-1}=d-m_n\Delta;\end{cases} \quad (3)$$

і якщо

$$d=\begin{vmatrix}x_nC-A & x_nD-B & x_nH-F & x_nK-G\\ y_nA-B & y_nC-F & y_nD-G & y_nH-K\\ z_nB-F & z_nA-G & z_nC-K & z_nD-H\\ m_nF-G & m_nB-K & m_nA-H & m_nC-D\end{vmatrix}\neq 0, \quad (4)$$

то

$$x_{n-1}=\frac{d_x}{d}, y_{n-1}=\frac{d_y}{d}, z_{n-1}=\frac{d_z}{d}, m_{n-1}=\frac{d_m}{d}; \quad (5)$$

де

$$d_x=\begin{vmatrix}d-x_n\Delta & x_nD-B & x_nH-F & x_nK-G\\ d-y_n\Delta & y_nC-F & y_nD-G & y_nH-K\\ d-z_n\Delta & z_nA-G & z_nC-K & z_nD-H\\ d-m_n\Delta & m_nB-K & m_nA-H & m_nC-D\end{vmatrix}, \quad (6)$$

$$d_y=\begin{vmatrix}x_nC-A & d-x_n\Delta & x_nH-F & x_nK-G\\ y_nA-B & d-y_n\Delta & y_nD-G & y_nH-K\\ z_nB-F & d-z_n\Delta & z_nC-K & z_nD-H\\ m_nF-G & d-m_n\Delta & m_nA-H & m_nC-D\end{vmatrix}, \quad (7)$$

$$d_z=\begin{vmatrix}x_nC-A & x_nD-B & d-x_n\Delta & x_nK-G\\ y_nA-B & y_nC-F & d-y_n\Delta & y_nH-K\\ z_nB-F & z_nA-G & d-z_n\Delta & z_nD-H\\ m_nF-G & m_nB-K & d-m_n\Delta & m_nC-D\end{vmatrix} \quad (8)$$

$$d_m=\begin{vmatrix}x_nC-A & x_nD-B & x_nH-F & d-x_n\Delta\\ y_nA-B & y_nC-F & y_nD-G & d-y_n\Delta\\ z_nB-F & z_nA-G & z_nC-K & d-z_n\Delta\\ m_nF-G & m_nB-K & m_nA-H & d-m_n\Delta\end{vmatrix}. \quad (9)$$

Шифрування за одним рядком матриці зображення

Шифрування відбувається з використанням елементів одного рядка матриці **C** за формулами (2), де $x_{n-1}=c_{i,j}, y_{n-1}=c_{i,j+1}$, $z_{n-1}=c_{i,j+2}, m_{n-1}=c_{i,j+3}$, $i=\overline{1,n}$, $j=\overline{1,m}$. Вибираються чотири сусідні елементи рядка матриці, так щоб кожний елемент був вибраний тільки один раз і тільки в одну четвірку.

Дешифрування відбувається за формулами оберненого перетворення (5) – (9) з коефіцієнтами, обчисленими за алгоритмом RSA.

Результати шифрування і дешифрування наведено на рис.1 – 3.

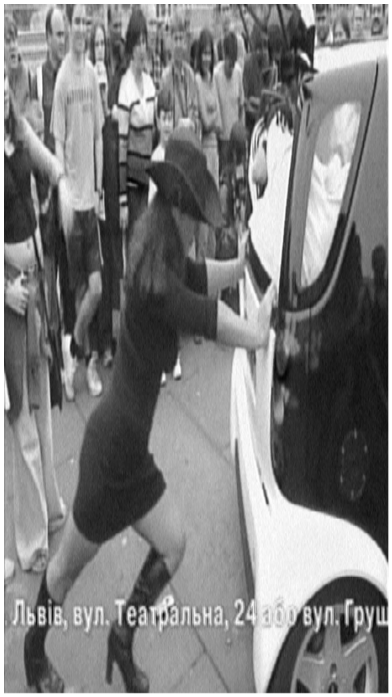

Рис. 1. Початкове зображення

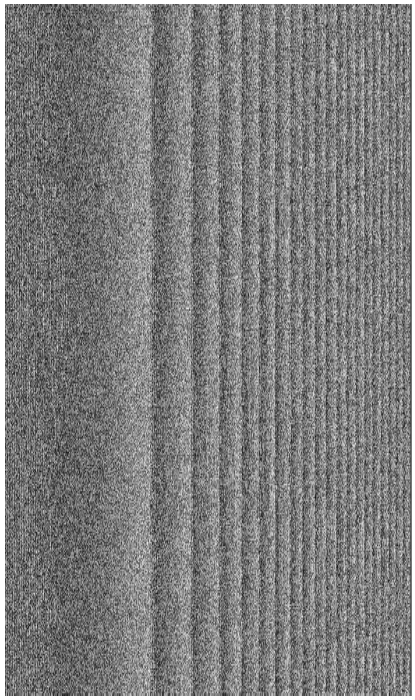

Рис. 2. Зашифроване зображення

Рис. 3. Дешифроване зображення

Шифрування за чотирма рядками матриці зображення

Шифрування відбувається з використанням елементів чотирьох рядків за формулами (2), де $x_{n-1} = c_{i,j}, y_{n-1} = c_{i+1,j}$, $z_{n-1} = c_{i+2,j}$, $m_{n-1} = c_{i+3,j}$, $i = \overline{1,n}$, $j = \overline{1,m}$. Вибираються чотири елементи з однаковими номерами, по одному з кожного рядка, так, щоб в кожну четвірку кожний елемент був вибраний тільки один раз.

Дешифрування відбувається за формулами оберненого перетворення (5) – (9) з коефіцієнтами $A = P, B = Q, F = e, G = d, C = P, D = -Q, H = d, K = e, d = P, \Delta = Q$.

Результати шифрування і дешифрування наведено на рис. 4 – 6.

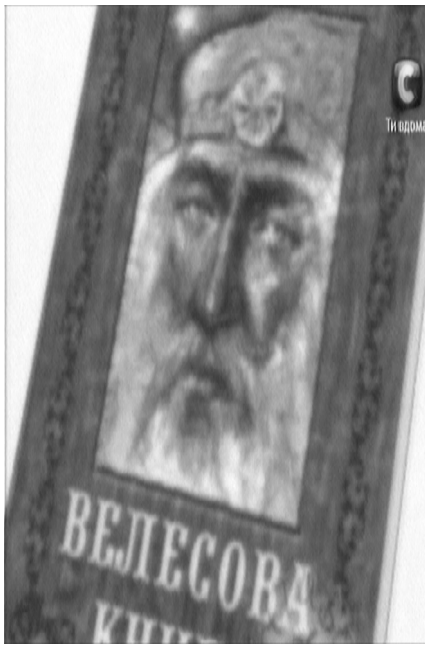

Рис. 4. Початкове зображення

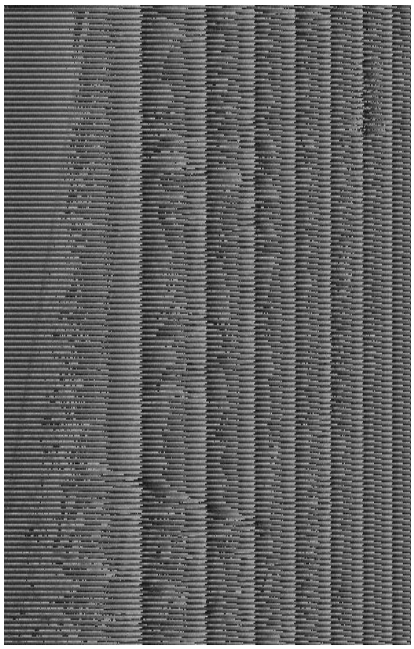

Рис. 5. Зашифроване зображення

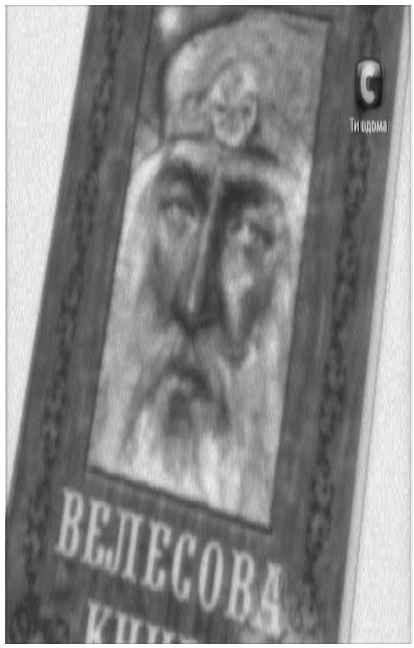

Рис. 6. Дешифроване зображення

Висновки

З порівняння рис. 2 і рис. 5 видно, що шифрування за одним рядком матриці зображення відрізняється від шифрування за чотирма рядками цієї матриці. Контури в обох зашифрованих зображеннях відсутні. Запропоновані модифікації можуть бути використані стосовно будь-якого типу зображень, але найбільші переваги забезпечує використання зображень, які дають змогу чітко виділяти контури. Обидві типи модифікації без жодних застережень можна використати і стосовно кольорових зображень. Однак, незалежно від типу зображення, пропорційно до розмірності вхідного зображення, може зрости розмір шифрованого зображення.

Запропоновані алгоритми мать високу криптологічну стійкість, яка істотно залежить від вибору простих чисел ***P*** і ***Q***. Це можна підтвердити прикладами (рис. 7–10).

Рис. 7.

Шифрування–дешифрування при ***P=103, Q=53, e=1667, d=35***

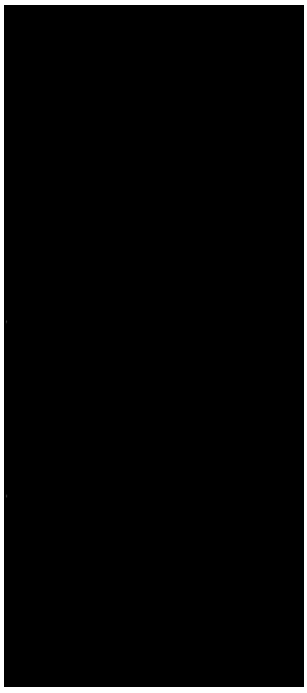

Рис. 8.

Дешифрування при ***P=103, Q=61, e=4133, d=77***

Рис. 9.

Шифрування–дешифрування при ***P=103, Q=53, e=1667, d=35***

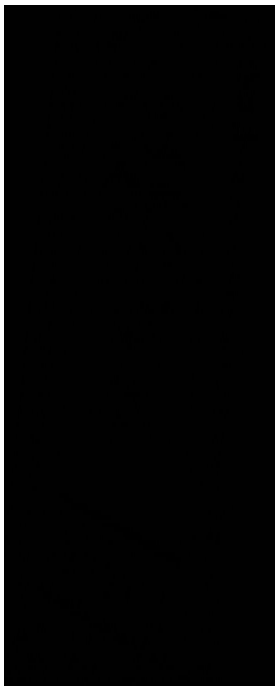

Рис. 10.

Дешифрування при ***P=101, Q=53, e=1981, d=21***

З рис. 7–10 видно, що вказані алгоритми надзвичайно чутливі до вибору елементів стандартного алгоритму RSA при дешифруванні зображення. Незначні зміни значень цих елементів унеможливлюють дешифрування зображення.

Описані алгоритми можна використовувати для конфіденційного передавання зображень.

1. Шнайер Брюс. Прикладная криптография. – М.: Триумф, 2003. – 815 с. 2. Яне Б. Цифровая обработка изображений. – М.: Техносфера, 2007. – 583 с. 3. Рашкевич Ю.М. Модифікація алгоритму RSA для деяких класів зображень / Рашкевич Ю.М., Пелешко Д.Д., Ковальчук А.М., Пелешко М.З. // Технічні вісті. – 2008/1(27), 2(28). С. 59 – 62. 4. Stream Modification of RSA Algorithm For Image Coding with precize contour extraction / Y. Rashkevych, A. Kovalchuk, D. Peleshko, M. Kupchak // Proceedings of the X-th International Conference CADSM 2009. 24-28 February 2009, Lviv-Polyana, Ukraine, P. 469–473. 5. Кроновер Р. Фракталы и хаос в динамических системах [Текст] / Р. Кроновер. – М.: Техносфера, 2006.– 488 с. 6. Уэлстид С. Фракталы и вейвлеты для сжатия изображений в действии [Текст] / С. Уэлстид. – М.: Триумф, 2003. – 320 с.