УДК 004.8; 932.72; 511; 512; 004.932; 004.932.4

А. Ковальчук, О. Годлєвський, Б. Бішко
Національний університет "Львівська політехніка",
кафедра автоматизованих систем управління

ШИФРУВАННЯ І ДЕШИФРУВАННЯ ЗОБРАЖЕНЬ З ВИКОРИСТАННЯМ ЕЛЕМЕНТІВ АЛГОРИТМУ RSA КВАТЕРНАРНИМИ ДРОБОВО-ЛІНІЙНИМИ ФОРМАМИ

Запропоновано алгоритм шифрування зображень кватернарними дробово-лінійними формами з використанням елементів алгоритму RSA як найстійкішого до несанкціонованого доступу до сигналів стосовно зображень з строго виділеними контурами.

Ключові слова: шифрування, зображення, кватернарний, контур.

An image encryption algorithm quaternary fractional-linear forms using elements of encryption RSA, as the most resistant to unauthorized access to signals for images is strictly dedicated circuits.

Keywords: countur, encryption, image, decryption.

Вступ

Важливою характеристикою зображення є наявність в зображенні контурів. Задача виділення контуру 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].

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

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

Одним із найбільш поширених і стійких алгоритмів шифрування інформації є алгоритм RSA [1]. Він належить до найбільш вживаної групи алгоритмів з відкритим ключем. Безпека алгоритму RSA ґрунтується на ресурсно затратній 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 дають змогу дуже строго виділяти контури, не дає задовільних результатів. На зашифрованому зображенні все ж таки можна розрізнити основні контури вхідного зображення. Тобто має місце ефект неповного зашумлення зображення.

Будемо вважати, що зображенню відповідає матриця кольорів

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

Кватернарна дробово-лінійна форма має вигляд

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

Використавши (1), виконаємо перетворення

$$\begin{cases} u = \dfrac{Ax + By + Fz + Gm + \delta}{Cx + Dy + Hz + Km + \Delta}; \\ v = \dfrac{Bx + Fy + Gz + Km + \delta}{Ax + Cy + Dz + Hm + \Delta}; \\ w = \dfrac{Fx + Gy + Kz + Hm + \delta}{Bx + Ay + Cz + Dm + \Delta}; \\ l = \dfrac{Gx + Ky + Hz + Dm + \delta}{Fx + By + Az + Cm + \Delta}; \end{cases} \tag{2}$$

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

Обернене до (2) перетворення має вигляд

$$\begin{cases} (uC - A)x + (uD - B)y + (uH - F)z + (uK - G)m = \delta - u\Delta; \\ (vA - B)x + (vC - F)y + (vD - G)z + (vH - K)m = \delta - v\Delta; \\ (wB - F)x + (wA - G)y + (wC - K)z + (wD - H)m = \delta - w\Delta; \\ (lF - G)x + (lB - K)y + (lA - H)z + (lC - D)m = \delta - l\Delta; \end{cases} \tag{3}$$

і якщо

$$\delta = \begin{vmatrix} uC - A & uD - B & uH - F & uK - G \\ vA - B & vC - F & vD - G & vH - K \\ wB - F & wA - G & wC - K & wD - H \\ lF - G & lB - K & lA - H & lC - D \end{vmatrix} \neq 0, \tag{4}$$

то

$$x = \frac{\delta_x}{\delta}, y = \frac{\delta_y}{\delta}, z = \frac{\delta_z}{\delta}, m\frac{\delta_m}{\delta}; \tag{5}$$

де

$$\delta_x = \begin{vmatrix} \delta - u\Delta & uD - B & uH - F & uK - G \\ \delta - v\Delta & vC - F & vD - G & vH - K \\ \delta - w\Delta & wA - G & wC - K & wD - H \\ \delta - l\Delta & lB - K & lA - H & lC - D \end{vmatrix}, \tag{6}$$

$$\delta_y = \begin{vmatrix} uC - A & \delta - u\Delta & uH - F & uK - G \\ vA - B & \delta - v\Delta & vD - G & vH - K \\ wB - F & \delta - w\Delta & wC - K & wD - H \\ lF - G & \delta - l\Delta & lA - H & lC - D \end{vmatrix}, \tag{7}$$

$$\delta_z = \begin{vmatrix} uC - A & uD - B & \delta - u\Delta & uK - G \\ vA - B & vC - F & \delta - v\Delta & vH - K \\ wB - F & wA - G & \delta - w\Delta & wD - H \\ lF - G & lB - K & \delta - l\Delta & lC - D \end{vmatrix} \tag{8}$$

$$\delta_m = \begin{vmatrix} uC - A & uD - B & uH - F & \delta - u\Delta \\ vA - B & vC - F & vD - G & \delta - v\Delta \\ wB - F & wA - G & wC - K & \delta - w\Delta \\ lF - G & lB - K & lA - H & \delta - l\Delta \end{vmatrix}. \tag{9}$$

Шифрування по одному рядку матриці зображення

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

Дешифрування відбувається по формулах оберненого перетворення (5) – (9) з коефіці-єнтами, обчисленими за алгоритмом RSA.

Результати шифрування і дешифрування наведені на рис.3.35 – 3.37.

Рис. 1. Початкове зображення

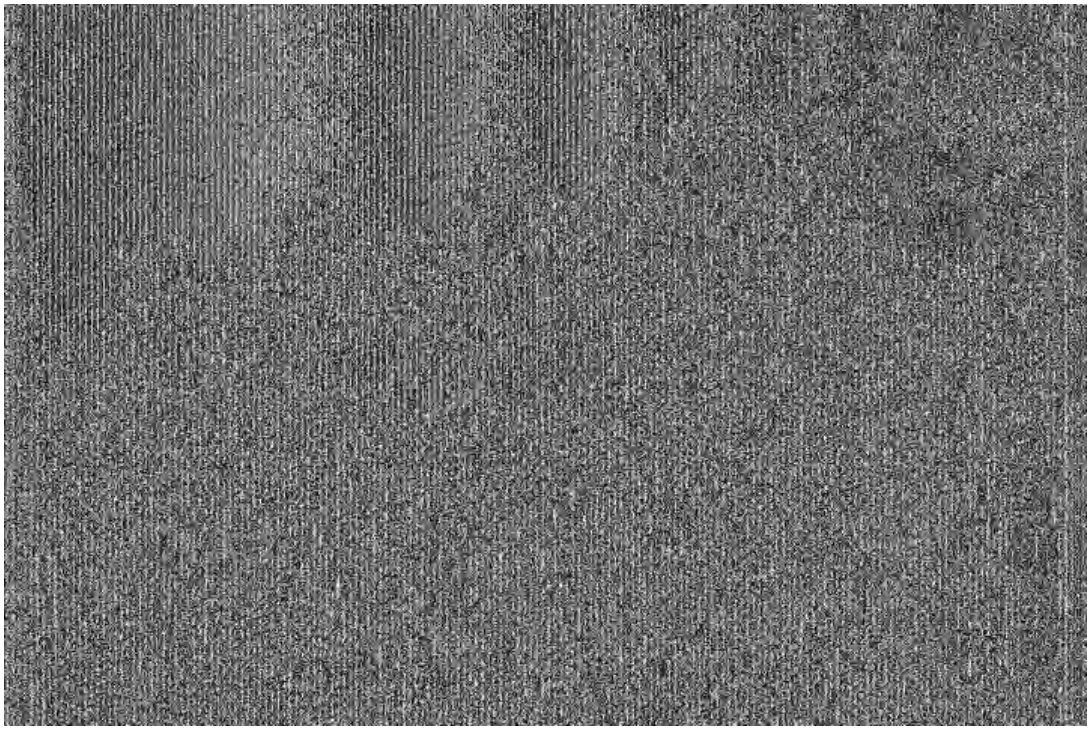

Рис. 2. Зашифроване зображення

Рис. 3. Дешифроване зображення

Шифрування за чотирма рядками матриці зображення

Шифрування відбувається з використанням елементів чотирьох рядків за формулами (2), де $x = c_{i,j}, y = c_{i+1,j}$, $z = c_{i+2,j}$, $m = c_{i+3,j}$, $i = \overline{1,n}$ $j = \overline{1,t}$. 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 по формулах оберненого перетворення (5)–(9) з коефіцієнтами $A = P, B = Q, F = e, G = d, C = P, D = -Q, H = d, K = e, \delta = P, \Delta = Q$

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

Рис. 4. Початкове зображення

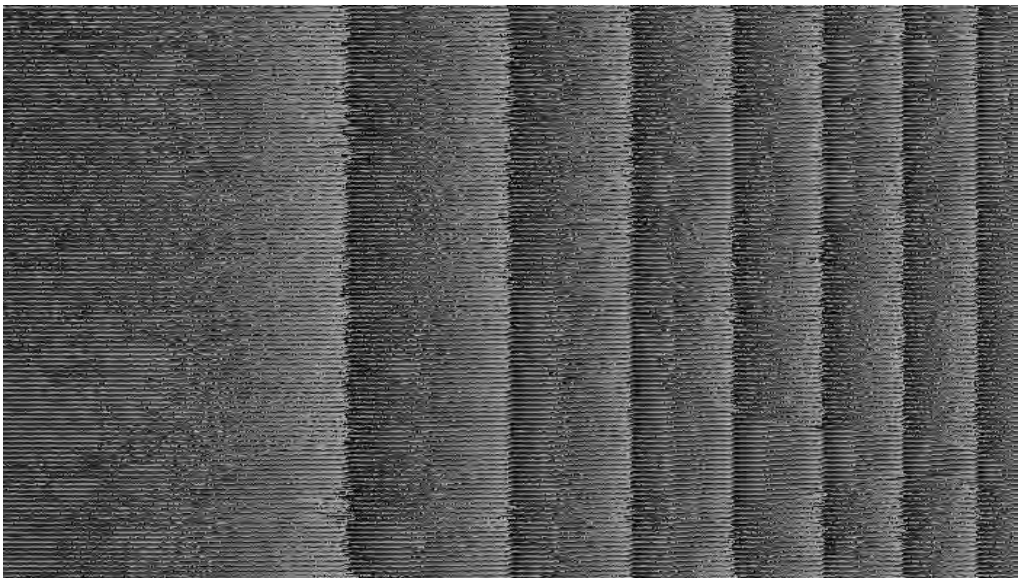

Рис. 5. Зашифроване зображення

Рис. 6. Дешифроване зображення

Висновок

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 найбільших переваг досягають у випадку використання зображень, які дають змогу чітко виділяти контури. Обидва типи модифікацій без жодних застережень можна використати і стосовно кольорових зображень. Однак, незалежно від типу зображення, пропорційно до розмірності вхідного зображення, може зрости розмір шифрованого зображення.

Алгоритм можна використати для передавання графічних зображень.

1. Шнайер Б. Прикладная криптография. – М.: Триумф, 2003. – 815 с. 2. Яне Б. Цифровая обработка изображений. – М.: Техносфера , 2007. – 583 с. 3. Рашкевич Ю.М., Пелешко Д.Д., Ковальчук А.М., Пелешко М.З.. Модифікація алгоритму RSA для деяких класів зображень. Технічні вісті 2008/1(27), 2(28). – С. 59–62. 4. Rashkevych Y., Kovalchuk A., Peleshko D., Kupchak M. 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.