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

Ю. Рашкевич, А. Ковальчук, Д. Пелешко
Національний університет "Львівська політехніка",
кафедра автоматизованих систем управління

ПРО ОДНЕ ЗАСТОСУВАННЯ АЛГОРИТМУ RSA ДЛЯ ШИФРУВАННЯ І ДЕШИФРУВАННЯ ЗОБРАЖЕНЬ З ЧІТКО ВИДІЛЕНИМИ КОНТУРАМИ

Запропоновано модифікацію алгоритму шифрування зображень з використанням алгоритму шифрування RSA як найстійкішого до несанкціонованого дешифрування сигналів, стосовно зображень, які дають змогу строго виділяти контури.
Ключові слова: зображення, контур, алгоритм RSA, колір.

A modification of encryption algorithm using image encryption algorithm RSA, the most resistant to unauthorized decoding of signals in relation to images that highlight the contours allow strictly.
Keywords: images, contour, algorithm RSA, color.

Вступ

Важливою характеристикою зображення є наявність в 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 ідеальний контур – це розрив просторової функції рівнів яскравості в площині зображення. Тому виділення контура 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 контура пікселах піднесення до степеня значення яскравостей дає ще більший розрив.

Вважатимемо, що зображенню у відповідність ставиться матриця кольорів

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

Шифрування і дешифрування по вісьми рядках матриці зображення

Нехай P і Q, R і T, V і U, F і G пари довільних простих чисел. Виберемо числа

$$N = PQ, \varphi(N) = (P-1)(Q-1), e_1 d_1 \equiv 1(\mathrm{mod}\,\varphi(N)), \quad (1)$$

$$M = RT, \varphi(M) = (R-1)(T-1), e_2 d_2 \equiv 1(\mathrm{mod}\,\varphi(M)), \quad (2)$$

$$L = UV, \varphi(L) = (U-1)(V-1), e_3 d_3 \equiv 1(\mathrm{mod}\,\varphi(L)), \quad (3)$$

$$K = FG, \varphi(K) = (F-1)(G-1), e_4 d_4 \equiv 1(\mathrm{mod}\,\varphi(K)), \quad (4)$$

Шифрування відбувається з використанням елементів восьми рядків за такою схемою:

з кожної послідовної пари рядків матриці зображення $\boldsymbol{C}$ вибираються два відповідні значення інтенсивності кольору і обчислюються наступні дві величини

$$u = x^e (\mathrm{mod}\, n), v = x^e (\mathrm{mod}\, n) - y^d (\mathrm{mod}\, n), \quad (5)$$

де числа $e = e_1, e_2, e_3, e_4$, $d = d_1, d_2, d_3, d_4$, $n = N, M, L, K$ отримуються з співвідношень (1)–(4) – відповідно.

Величини u, v, отримані з (5), записуються у два послідовні рядки зашифрованого зображення, кожне значення в один рядок.

Дешифрування проводиться у зворотному порядку за формулами

$$y = (v + u)^e \pmod{n}, \; x = u^d \pmod{n}.$$

Результати наведені на рис. 1–3.

Рис. 1. Початкове зображення

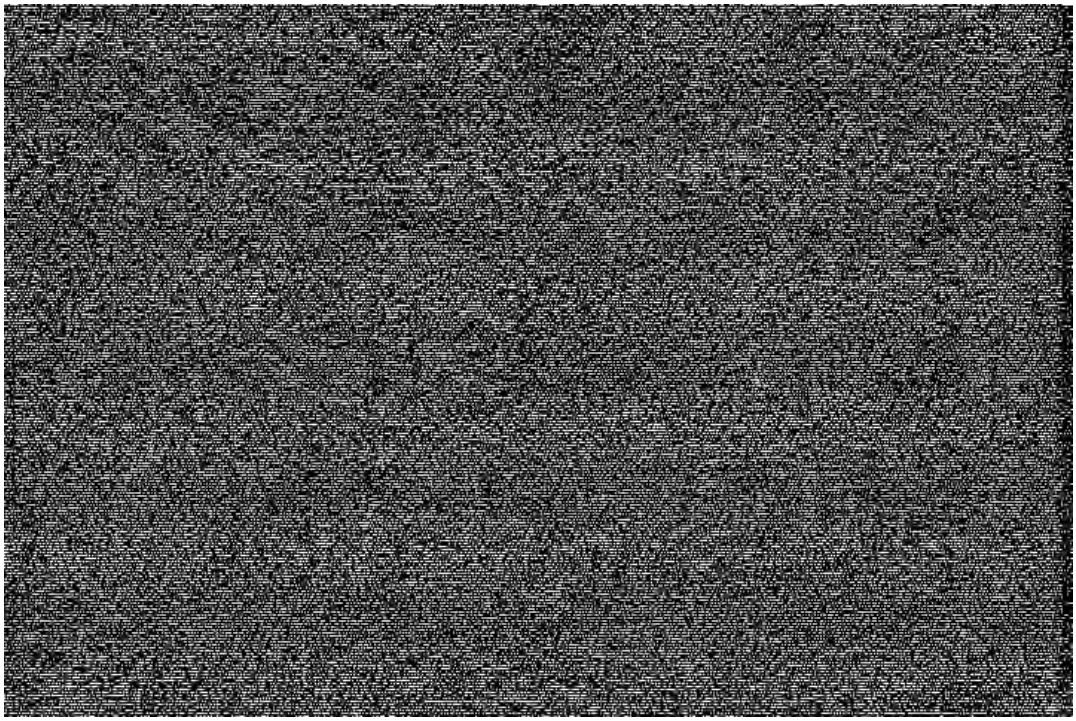

Рис. 2. Зашифроване зображення

Рис. 3. Дешифроване зображення

Шифрування і дешифрування за чотирма рядками матриці зображення

У кожних чотирьох рядках матриці зображення ***C*** вибираються два послідовні значення інтенсивності кольору з кожного рядка ***x*** і ***y***. За формулами (5) обчислюються величини u, v,

$$u = x^e \pmod n, v = x^e \pmod n - y^d \pmod n,$$

де числа $e = e_1, e_2, e_3, e_4$, $d = d_1, d_2, d_3, d_4$, $n = N, M, L, K$ отримуються з співвідношень (1)–(4) – відповідно.

Величини u, v записуються як два послідовні значення зашифрованого зображення, обидва значення в один рядок.

Дешифрування проводиться у зворотному порядку за формулами

$$y = (v + u)^e \pmod n, x = u^d \pmod n.$$

Результати наведені на рис. 4–6.

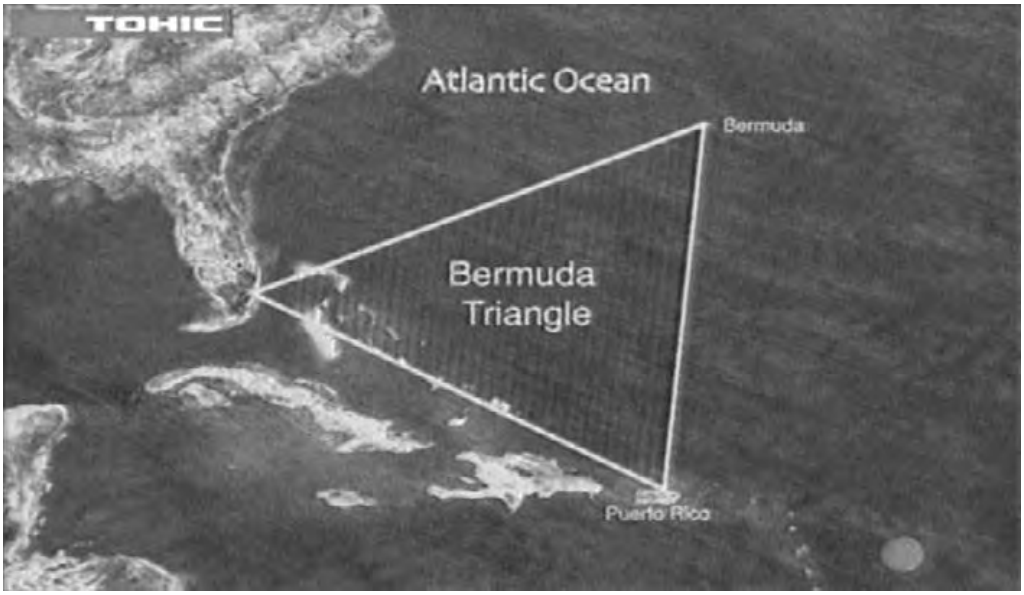

Рис. 4. Початкове зображення

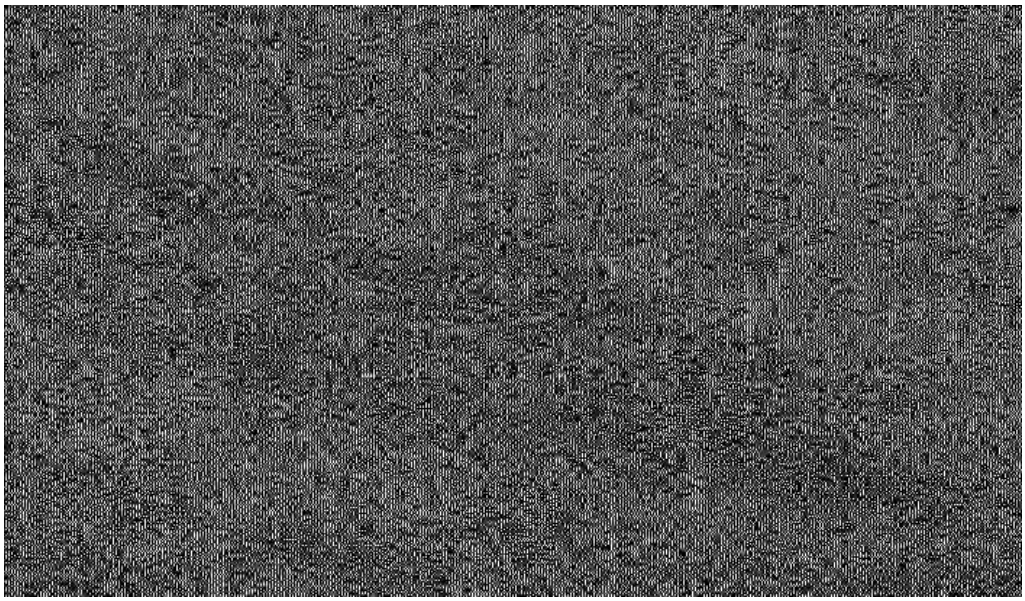

Рис. 5. Зашифроване зображення

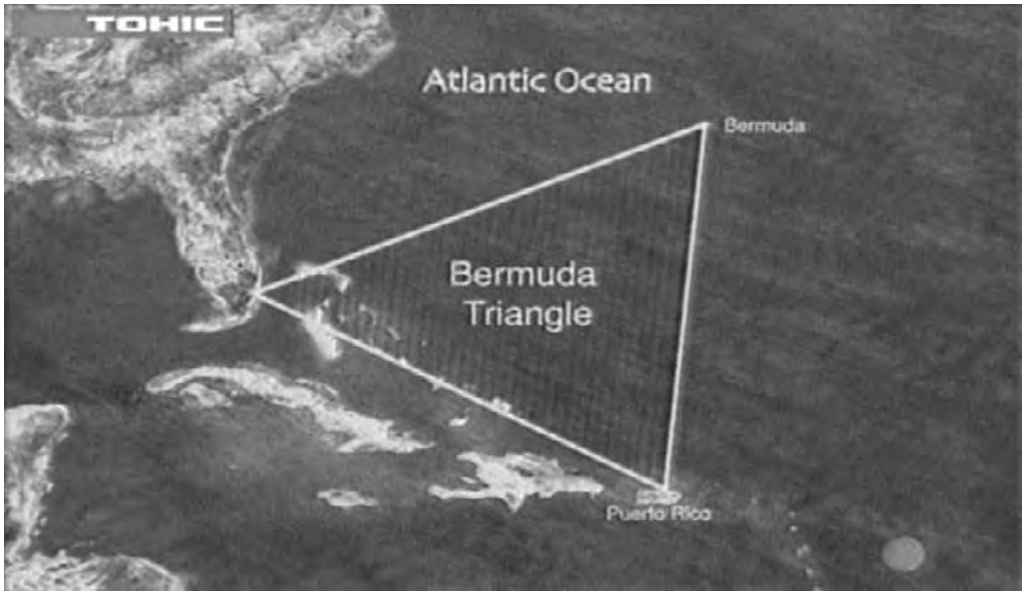

Рис. 6. Дешифроване зображення

Висновок

З порівняння рис. 2 і рис. 5 видно, що шифрування за одним рядком матриці зображення відрізняється від шифрування за трьома рядками цієї матриці. Контури в обох зашифрованих зображеннях відсутні. Вказаний алгоритм можна використати при передачі графічних зображень. Запропоновані модифікації можна використати стосовно будь-якого типу зображень, але найбільші переваги досягаються у випадку використання зображень, які дозволяють 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.

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.