МОДЕЛЮВАННЯ ПРОЦЕСІВ І СИСТЕМ

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

А. Ковальчук, Є. Кузнєцов, Ю. Артимич
Національний університет "Львівська політехніка",
кафедра автоматизованих систем управління

ЗАСТОСУВАННЯ АЛГОРИТМУ RSA У ШИФРУВАННІ І ДЕШИФРУВАННІ ЕЛЕМЕНТІВ ЛОКАЛЬНО-СКІНЧЕННОГО ТОПОЛОГІЧНОГО ПОКРИТТЯ ЗОБРАЖЕННЯ ЯК КОМПАКТУ

Запропоновано застосування алгоритму RSA шифрування і дешифрування елементів локально скінченного топологічного покриття зображення, яке має чітко виділені внутрішні контури.

Ключові слова: шифрування, дешифрування, зображення, контур, топологічне покриття.

An application of RSA algorithm encryption and decryption of locally finite topological elements cover image that is clearly marked internal contours.

Keywords: encryption, decryption, image, contour, stability, the topological coverage.

Вступ

Вважатимемо, що зображенню у відповідність ставиться матриця кольорів

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

Важливою характеристикою зображення є наявність у 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].

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].

Відносно зображення існують певні проблеми його шифрування, а саме частково зберігаються контури на різкофлуктуаційних зображеннях [3, 4]. Однією з причин того, що контури залишаються в зображенні при шифруванні в системі RSA, є те, що шифрування тут основане 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. Уникнути збереження контурів при шифруванні в системі RSA можна розділенням початкового зображення на частини так, щоб покриття зображення було топологічно локально скінченним, тобто компактом.

Шифрування і дешифрування за вісьмома рядками матриці зображення

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

$$N = PQ, \varphi(N) = (P-1)(Q-1), e_1 d_1 \equiv 1 \left(mod\, \varphi(N)\right), \quad (1)$$

$$M = RT, \varphi(M) = (R-1)(T-1), e_2 d_2 \equiv 1 \left(mod\, \varphi(M)\right), \quad (2)$$

$$L = VU, \varphi(L) = (V-1)(U-1), e_3 d_3 \equiv 1 \left(mod\, \varphi(L)\right), \quad (3)$$

$$K = FG, \varphi(K) = (F-1)(G-1), e_4 d_4 \equiv 1 \left(mod\, \varphi(K)\right), \quad (4)$$

Рис. 1. Початкове зображення

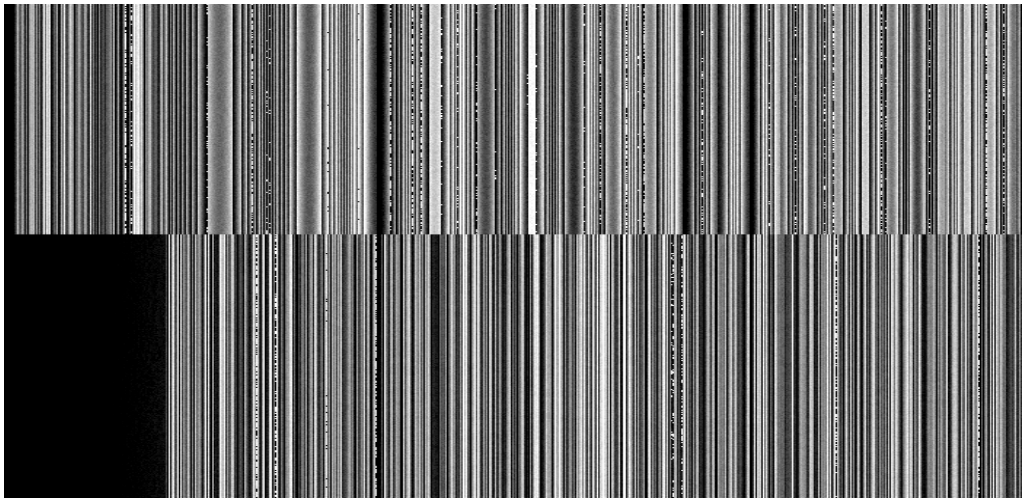

Рис. 2. Зашифроване зображення

Рис. 3. Дешифроване зображення

Шифрування відбувається з використанням елементів восьми рядків за такою схемою:

з кожної послідовної пари рядків матриці зображення $\boldsymbol{C}$ вибирають два відповідні значення інтенсивності кольору й обчислюються такі дві величини

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

де числа $e = e_1, e_2, e_3, e_4$, $d = d_1, d_2, d_3, d_4$, $n = N,\ M,\ L,\ K$ отримують зі співвідношень (1) - (4) відповідно.

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

Дешифрування виконують у зворотній послідовності за формулами

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

Результати наведені на рис. 1–3.

Шифрування і дешифрування за чотирма рядками матриці зображення

У кожних чотирьох рядках матриці зображення $\boldsymbol{C}$ вибирають два послідовні значення інтенсивності кольору з кожного рядка $\boldsymbol{x}$ і $\boldsymbol{y}$. За формулами (5) обчислюють величини u ,v,

$$u = x^e \ (mod\ n),\ v = x^e \ (mod\ n) - y^d \ (mod\ n),$$

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

Рис. 4. Початкове зображення

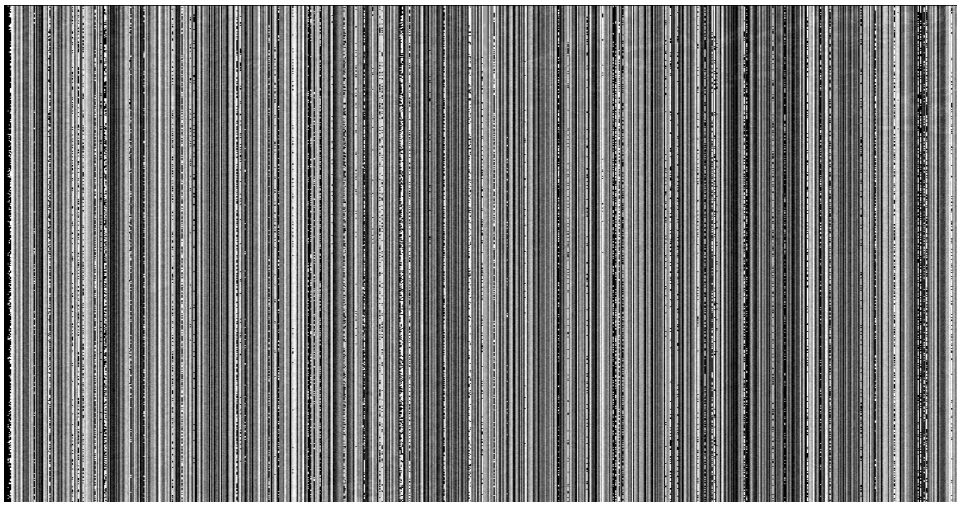

Рис. 5. Зашифроване зображення

Рис. 6. Дешифроване зображення

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

Дешифрування виконують у зворотній послідовності за формулами

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

Результати наведено на рис. 4–6.

Висновок

З порівняння рис. 2 і рис. 5 видно, що шифрування за вісьмома рядками матриці зображення відрізняється від шифрування за чотирма рядками цієї матриці. Контури в обох зашифрованих зображеннях відсутні. Вказаний алгоритм може бути використаний під час передавання графічних зображень. Запропоновані модифікації можуть бути використані стосовно будь-якого типу зображень, але найбільші переваги досягаються у разі 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.

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, Pp. 469–473.