УДК 681.142.2; 622.02.658.284; 621. 325

А. Ковальчук[1], І. Цмоць[2], Б. Гавриш[1]
Національний університет “Львівська політехніка”,
[1]кафедра інформаційних технологій видавничої справи,
[2]кафедра автоматизованих систем управління

РЕКУРЕНТНІ БІНАРНІ ПЕРЕТВОРЕННЯ З ЕЛЕМЕНТАМИ RSA І ДОДАТКОВЕ ЗАШУМЛЕННЯ ПІД ЧАС ШИФРУВАННЯ/ДЕШИФРУВАННЯ ЗОБРАЖЕНЬ

Запропоновано алгоритм рекурентного шифрування-дешифрування зображень з чітко видимими контурами, бінарними лінійними формами та з використанням елементів алгоритму RSA як найбільш стійкого до несанкціонованого доступу до сигналів.

Ключові слова: зображеня, контур, несанкціонований доступ, сигнал.

The algorithm encryption-decryption recurrent images with clearly visible outlines binary linear forms and using elements of the RSA algorithm as the most resistant to unauthorized access to signals.

Key words: image, contour, unauthorized access, signal.

Вступ

Наявність у зображенні контурів є його важливою характеристикою. Задача виокремлення контура передбачає застосування операцій над сусідніми елементами зображення, які є чутливими до змін і пригашають області постійних рівнів яскравості, тобто, контури – це області, які є світлими, тоді як інші частини зображення залишаються темними [3].

Рис. 1. Зображення і контури в зображенні

Відносно до такого зображення існують певні проблеми його шифрування, а саме частково зберігаються контури на різко флуктуаційних зображеннях [1, 4, 5].

Контур – розрив просторової функції рівнів яскравості в площині зображення. Тому виокремлення контура означає пошук найбільш різких змін, тобто максимумів модуля вектора градієнта [3]. Це є однією з причин того, що контури залишаються в зображенні під час шифрування в системі RSA (шифрування тут ґрунтується на піднесенні до степеня за модулем деякого натурального числа), оскільки на контурі і на сусідніх до контура елементах піднесення до степеня значень інтенсивностей дає ще більший розрив.

RSA є одним з найбільш поширених і стійких алгоритмів шифрування [2]. Цей алгоритм належить до групи найчастіше використовуваних алгоритмів з відкритими ключами. Алгоритм безпеки RSA оснований на ресурсі затратної факторизації великих натуральних чисел. Використання алгоритму шифрування RSA [2] як найстійкішого до несанкціонованого дешифрування кодованих сигналів, стосовно зображень, які дають змогу дуже строго виділяти контури, не дає задовільних результатів. У зашифрованому зображенні все ще інколи можна розрізнити основні контури початкового зображення. Тобто ефект неповного зашумлення частини зображення наявний.

Приймемо, що зображенню відповіає така матриця інтенсивностей пікселів:

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

Шифрування/дешифрування без додаткового зашумлення

Нехай бінарна лінійна форма має вигляд

$$\begin{cases} T(x,y) = Ax + Dy \\ S(x,y) = Cx + Dy \end{cases}. \quad (1)$$

Використовуючи (1), виконаємо наступні бінарні перетворення

$$\begin{cases} f = Ax + By \\ g = Cx + Dy \end{cases}; \begin{cases} F = Af + Bg \\ G = Cf + Dg \end{cases}, \quad (2)$$

де $A = P$, $B = Q$, $C = e$, $D = d$ – елементи стандартного алгоритму RSA, тобто P і Q – довільні прості числа, $ed \equiv 1\ mod(\varphi(n))$, $\varphi(n) = (P-1)(Q-1)$.

Обернені до (2) перетворення існують, якщо

$$\Delta = AD - CD \neq 0,$$

і тоді

$$f = (FD - GB)/\Delta,\ g = (AG - CF)/\Delta,\ x = (fD - gB),\ y = (Ag - Cf)/\Delta. \quad (3)$$

Шифрування за одним рядком матриці зображення

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

Дешифрування відбувається за формулами оберненого перетворення (3) з коефіцієнтами, обчисленими за алгоритмом RSA.

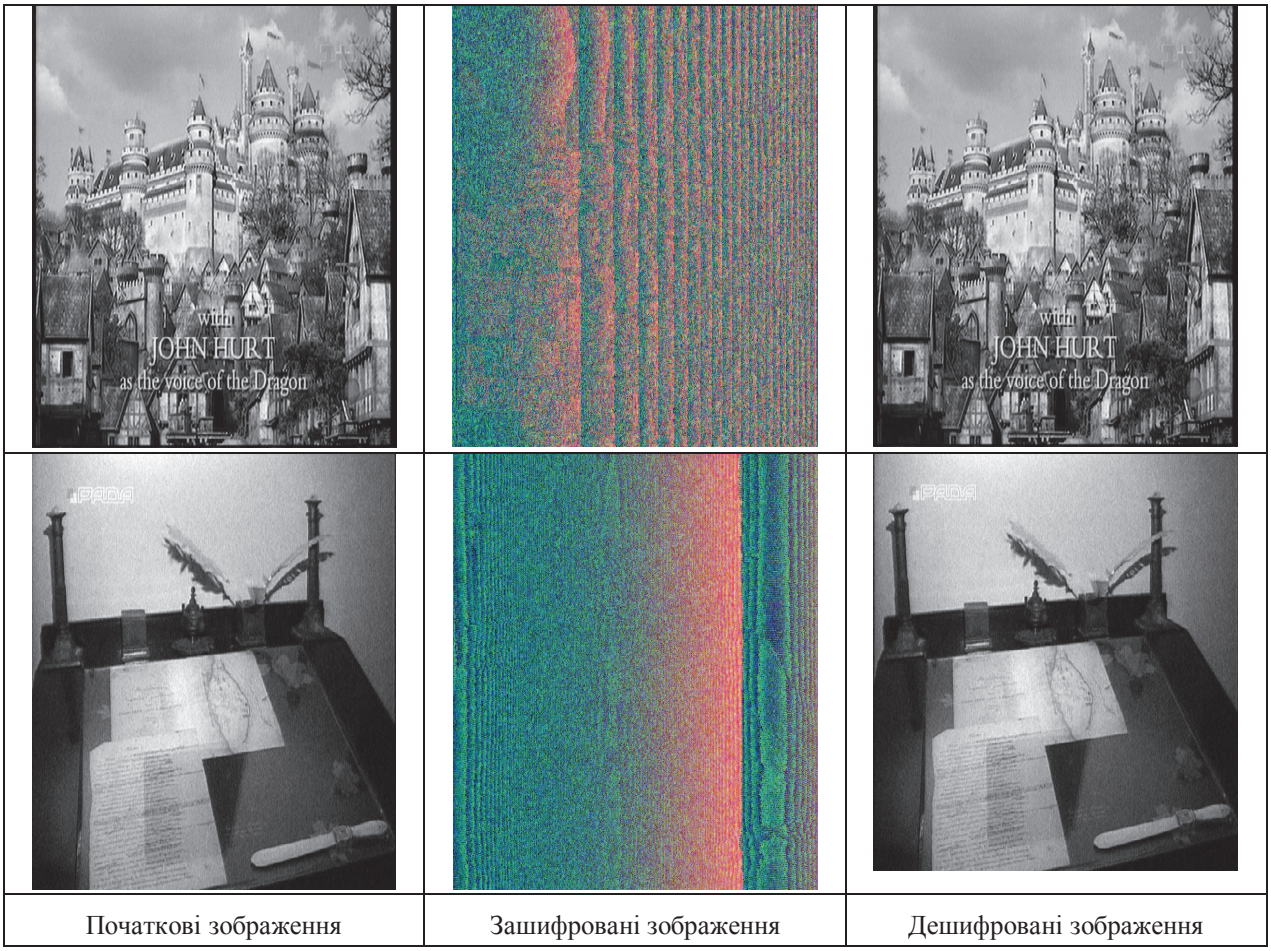
Результати шифрування і дешифрування наведен на рис. 2.

Шифрування за двома рядками матриці зображення

Шифрування відбувається з використанням елементів двох рядків за формулами (2), де $x = c_{i,j}, y = c_{i+1,j}$,, $i = \overline{1,n}$, $j = \overline{1,m}$. Вибирають два елементи з однаковими номерами, по одному з кожного рядка так, щоб до кожної пари кожний елемент було вибрано лише один раз.

Дешифрування відбувається за формулами оберненого перетворення (3) з коефіцієнтами $A = P$, $B = Q$, $C = e$, $D = d$.

Результати шифрування і дешифрування наведено на рис. 2.



Початкові зображення	Зашифровані зображення	Дешифровані зображення

Рис. 2. Шифрування/дешифрування за одним і двома рядками без додаткового зашумлення

Шифрування/дешифрування з додатковим зашумленням

Нехай бінарна лінійна форма має вигляд

$$\begin{cases} T(x,y) = Ax + Dy \\ S(x,y) = Cx + Dy \end{cases}. \tag{4}$$

Використовуючи (4), виконаємо такі бінарні перетворення

$$\begin{cases} f = Ax + By \\ g = Cx + Dy \end{cases}, \quad \begin{cases} F = Af + Bg + s(x,y) \\ G = Cf + Dg + t(x,y) \end{cases}, \tag{5}$$

де $A = P$, $B = Q$, $C = e$, $D = d$ – елементи стандартного алгоритму RSA, тобто P і Q – довільні прості числа, $ed \equiv 1\, mod(\varphi(n))$, $\varphi(n) = (P-1)(Q-1)$, $s(x,y), t(x,y)$ – деякі функції зашумлення.

Обернені до (5) перетворення існують, якщо

$$\Delta = AD - CD \neq 0,$$

і тоді

$$f = \frac{\begin{vmatrix} F-s(x,y) & B \\ G-t(x,y) & D \end{vmatrix}}{\Delta}, g = \frac{\begin{vmatrix} A & F-s(x,y) \\ C & G-t(x,y) \end{vmatrix}}{\Delta}, x = \frac{\begin{vmatrix} f & B \\ g & D \end{vmatrix}}{\Delta}, y = \frac{\begin{vmatrix} A & f \\ C & g \end{vmatrix}}{\Delta}. \quad (6)$$

Шифрування за одним рядком матриці зображення

Шифрування відбувається з використанням елементів одного рядка матриці **C** за формулами (5), де $x = c_{i,j}, y = c_{i,j+1}, \quad i = \overline{1,n}, j = \overline{1,m}.$ Вибираються два сусідні елементи рядка матриці так, щоб кожний елемент був вибраний тільки один раз і тільки в одну пару.

Дешифрування відбувається за формулами оберненого перетворення (6) з коефіцієнтами, обчисленими за алгоритмом RSA.

Результати шифрування і дешифрування наведено на рис. 3.

Шифрування за двома рядками матриці зображення

Шифрування відбувається з використанням елементів двох рядків за формулами (5), де $x = c_{i,j}, y = c_{i+1,j}$,, $i = \overline{1,n}, j = \overline{1,m}.$ Вибирають два елементи з однаковими номерами, по одному з кожного рядка так, щоб в кожну пару кожний елемент був вибраний тільки один раз.

Дешифрування відбувається за формулами оберненого перетворення (6) з коефіцієнтами $A = P$, $B = Q$, $C = e$, $D = d$.

Результати шифрування і дешифрування наведено на рис. 3.

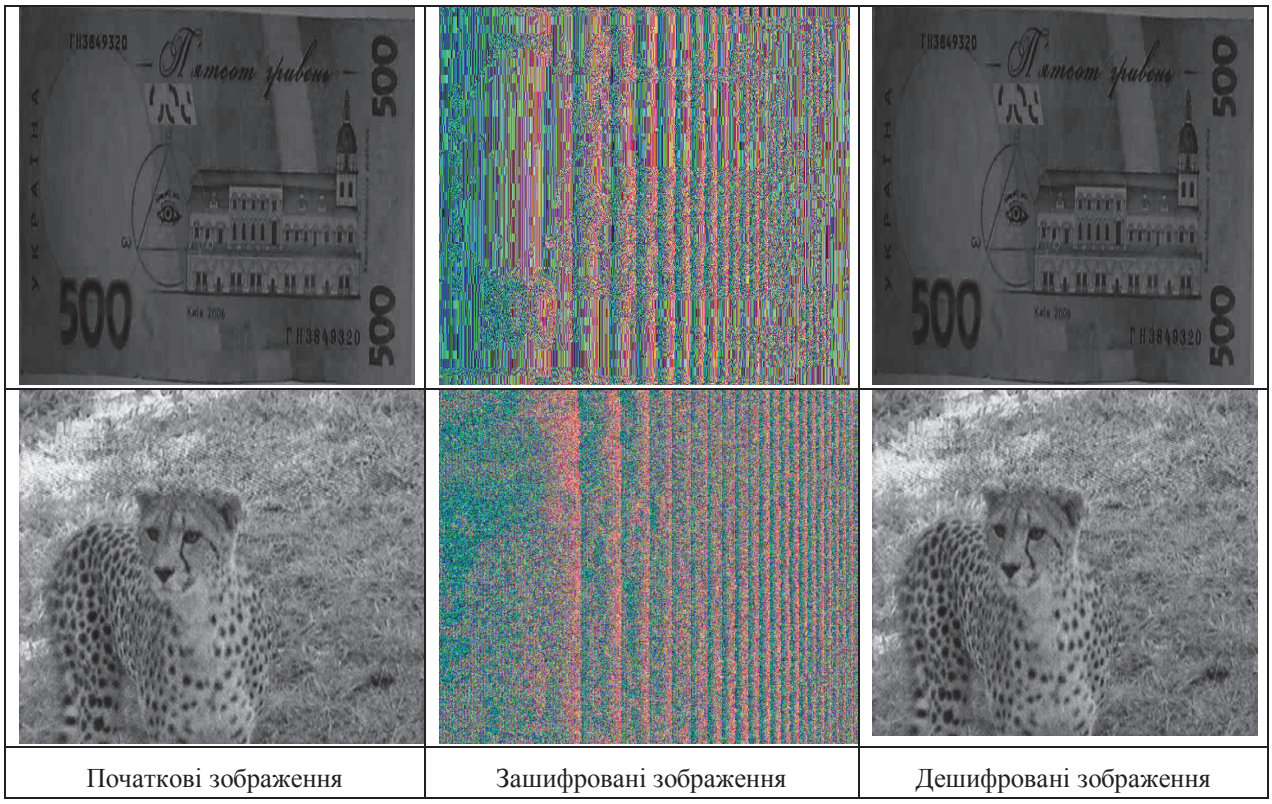


Рис. 3. Шифрування/дешифрування за одним і двома рядками з додатковим зашумленням

Висновок

Порівнюючи рис. 2 і 3, бачимо, що шифрування за одним рядком матриці зображення відрізняється від шифрування за двома рядками цієї матриці. Контури в обох зашифрованих зображеннях відсутні. Незначно візуально відрізняється також і дешифроване зображення від початкового у випадку шифрування за двома рядками матриці зображення.

Запропоновані алгоритми можна використати стосовно будь-якого типу зображень, але найбільших переваг досягають у випадку використання зображень, які дають можливість чітко виокремлювати контури. Обидва алгоритми можна використати і стосовно кольорових зображень. Однак, незалежно від типу зображення, пропорційно до розмірності вхідного зображення може зрости розмір шифрованого зображення.

Цей алгоритм можна використати для мультимедійного передавання графічних даних, тобто як лінійне або нелінійне комбінування різних форм представлення інформації, наприклад, текстової, звукової і графічної, або, останнім часом все частіше – анімації і відео.

1. 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. 2. Брюс Шнайер. Прикладная криптография. – М.: Триумф, 2003. – 815 с. 3. Яне Б. Цифровая обработка изображений. – М.: Техносфера, 2007. – 583 с. 4. 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. 5. Ковальчук А. М., Попадинець К. С. Бінарні перетворення з елементами алгоритму RSA у захисті зображень за додаткового зашумлення // Комп'ютерні науки та інформаційні технології. – 2016. – № 843. – С. 79–84.