

5. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ГАЛУЗІ

УДК 681.142.2; 622.02.658.284; 621.325

*Проф. Ю.М. Рашкевич,
д-р техн. наук; ст. викл. А.М. Ковальчук; доц. Д.Д. Пелешко,
канд. техн. наук – НУ "Львівська політехніка"*

ШИФРУВАННЯ І ДЕШИФРУВАННЯ ЗОБРАЖЕНЬ ТЕРНАРНИМИ АФІННИМИ ФОРМАМИ З ЕЛЕМЕНТАМИ АЛГОРИТМУ RSA

Запропоновано алгоритм шифрування зображень тернарними афінними формами з використанням елементів алгоритму шифрування RSA, як найстійкішого до несанкціонованого дешифрування сигналів, стосовно зображень, які дають змогу суворо виділяти контури.

*Prof. Yu.M. Rashkevych; senior lecturer A.M. Kovalchuk;
assoc. prof. D.D. Peleshko – NU "L'vivs'ka Politekhnik"*

Enciphering and decoding of images of ternary by affine forms with elements of algorithm of RSA

The algorithm of encoding of the images by the figurative affine forms with usage of elements of algorithm of encoding RSA is offered, as steadiest to unauthorized decoding of the images, which one resolve strictly to excrete contours

Вступ. Одним із найбільш поширених і стійких алгоритмів шифрування інформації є алгоритм RSA [1]. Він належить до найбільш вживаної групи алгоритмів із відкритим ключем. Безпека алгоритму RSA базується 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 суворо 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.

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]. За відношенням до 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 контура означає пошук

найбільш різких змін, тобто максимумів модуля вектора градієнта [2]. Це є однією з причин, через що контури залишаються в зображенні під час шифрування в системі RSA, оскільки шифрування тут базується на піднесенні до степеня за модулем певного натурального числа. При цьому, на контурі і на сусідніх до контура пікселях піднесення до степеня значення яскравостей дає ще більший розрив.

Будемо вважати, що зображенню у відповідність ставиться матриця кольорів

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

Тернарне афінне перетворення

Введемо означення тернарного афінного перетворення евклідового простору в декартових координатах. Перетворення евклідового простору називається афінним, якщо це перетворення відображає кожну площину на площину. Нехай тернарне афінне перетворення евклідового простору в декартових координатах має такий вигляд

$$\begin{aligned} x' &= a_1x + b_1y + d_1z, \\ y' &= a_2x + b_2y + d_2z, \\ z' &= a_3x + b_3y + d_3z, \end{aligned} \quad \text{де } \delta = \begin{vmatrix} a_1 & b_1 & d_1 \\ a_2 & b_2 & d_2 \\ a_3 & b_3 & d_3 \end{vmatrix} \neq 0. \quad (1)$$

Обернене до (1) перетворення також існує і тоді

$$x = \frac{\Delta_x}{\delta}, \quad y = \frac{\Delta_y}{\delta}, \quad z = \frac{\Delta_z}{\delta}, \quad (2)$$

$$\text{де: } \Delta_x = \begin{vmatrix} x' & b_1 & d_1 \\ y' & b_2 & d_2 \\ z' & b_3 & d_3 \end{vmatrix}, \quad \Delta_y = \begin{vmatrix} a_1 & x' & d_1 \\ a_2 & y' & d_2 \\ a_3 & z' & d_3 \end{vmatrix}, \quad \Delta_z = \begin{vmatrix} a_1 & b_1 & x' \\ a_2 & b_2 & y' \\ a_3 & b_3 & z' \end{vmatrix}.$$

Шифрування і дешифрування по рядках матриці зображення

Шифрування і дешифрування одним рядком матриці зображення.

Нехай P, Q довільні прості числа. Виберемо

$$\begin{aligned} n &= PQ, \quad j(n) = (P-1)(Q-1), \quad e_1d_1 \equiv 1 \pmod{j(n)}, \quad e_2d_2 \equiv 1 \pmod{j(n)}, \\ e_3d_3 &\equiv 1 \pmod{j(n)}, \quad e_1 < j(n), \quad d_1 < j(n), \quad e_2 < j(n), \quad d_2 < j(n), \\ e_3 &< j(n), \quad d_3 < j(n). \end{aligned} \quad (3)$$

Шифрування відбувається з використанням елементів одного рядка матриці зображення за формулами (1), де $x = c_{i,j}, y = c_{i,j+1}, z = c_{i,j+2}, i = \overline{1, n}, j = \overline{1, m}$. Вибираються три сусідні елементи рядка матриці, так щоб кожний елемент був вибраний тільки один раз і тільки в одну трійку. Коефіцієнти $a_1 = b_3 = d_2 = P^{e_1} \pmod{n}, b_1 = a_2 = d_3 = Q^{d_2} \pmod{n}, d_1 = b_2 = a_3 = Q^{e_3} \pmod{n}$, – цілі числа. (Коефіцієнти можуть бути інакшими, але такими, щоб в (2) виконувалася умова $\delta \neq 0$).

Дешифрування відбувається за формулами оберненого перетворення (2) з коефіцієнтами, обчисленими за алгоритмом RSA

$$a_1 = b_3 = d_2 = P^{d_1}(\text{mod } n), \quad b_1 = a_2 = d_3 = Q^{e_2}(\text{mod } n), \quad d_1 = b_2 = a_3 = Q^{d_3}(\text{mod } n).$$

Результати наведено на рис. 1–3.



Рис. 1. Початкове зображення

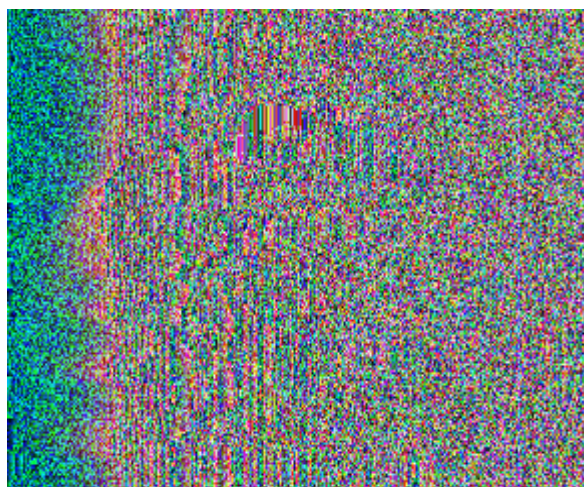


Рис. 2. Зашифроване зображення



Рис. 3. Дешифроване зображення

Шифрування і дешифрування трьома рядками матриці зображення. Шифрування відбувається з використанням елементів трьох рядків за формулами (1), де $x = c_{i,j}, y = c_{i+1,j}, z = c_{i+2,j}, i = \overline{1, n}, j = \overline{1, m}$. Вибираються три елементи з однаковими номерами, по одному з кожного рядка, так щоб в кожну трійку кожний елемент був вибраний тільки один раз. Коефіцієнти

$$a_1 = b_3 = d_2 = Q^{e_1}(\text{mod } n),$$

$$b_1 = a_2 = d_3 = P^{d_2}(\text{mod } n), \quad d_1 = b_2 = a_3 = (Q + P)^{e_3}(\text{mod } n) - \text{цілі числа.}$$

Дешифрування виконують за формулами оберненого перетворення (2) з коефіцієнтами

$$a_1 = b_3 = d_2 = Q^{d_1}(\text{mod } n), \quad b_1 = a_2 = d_3 = P^{e_2}(\text{mod } n), \quad d_1 = b_2 = a_3 = (Q + P)^{d_3}(\text{mod } n).$$

Результати наведені на рис. 4–6.



Рис. 4. Початкове зображення

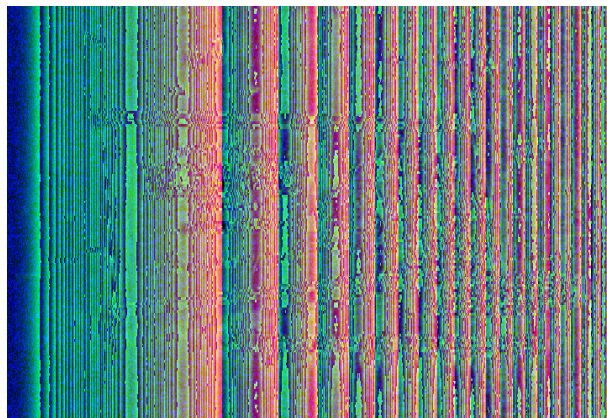


Рис. 5. Зашифроване зображення



Рис. 6. Дешифроване зображення

Висновок. З порівняння рис. 2 і 5 видно, що шифрування одним рядком матриці зображення відрізняється від шифрування трьома рядками цієї матриці. Контури в обох зашифрованих зображеннях відсутні. Вказаний алгоритм можна використати для передачі графічних зображень. Запропоновані модифікації можна застосовувати 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.

Література

1. Брюс Шнайер. Прикладная криптография. – М. : Изд-во "Триумф", 2003. – 815 с.
2. Яне Б. Цифровая обработка изображений. – М. : Изд-во "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. Rashkevych Y. Stream Modification of RSA Algorithm For Image Coding with precise contour extraction / Rashkevych Y., Kovalchuk A., Peleshko D., Kupchak M. // Proceedings of the X-th International Conference CADSM 2009. 24-28 February 2009, Lviv-Polyana, Ukraine. – PP. 469-473.

УДК 681.3+519.6

Доц. О.А. Пастух, канд. техн. наук –
Тернопільський ДТУ ім. Івана Пулюя

ОБЧИСЛЕННЯ ІНДИКАТОРНИХ ФУНКЦІЙ КВАНТОВИХ НЕЧІТКИХ ВІДНОШЕНЬ

Уточнено означення понять: квантової нечіткої множини, яке вперше було введено і уточнено у роботах [6-9]; квантового нечіткого бінарного відношення, квантового нечіткого тернарного відношення та квантового нечіткого N -арного відношення. Запропоновано методи обчислення індикаторних функцій квантового нечіткого бінарного відношення, квантового нечіткого тернарного відношення, квантового нечіткого N -арного відношення за допомогою індикаторних функцій квантових нечітких множин, що утворюють дані квантові нечіткі відношення.

Assoc. prof. O.A. Pastukh – Ternopol state technical university of Ivan Pulyuj

Computation of indicated functions of quantum fuzzy relations

Accurate definition notions: of quantum fuzzy set, what first has been weak and accurate definition by author in the him articles [6-9]; of quantum fuzzy binary relation, of quantum fuzzy ternary relation, of quantum fuzzy N relation has been analyzed. Methods computation of indicated functions of quantum fuzzy binary relation, of quantum fuzzy ter-