УДК 681.142.2; 622.02.658.284; 621. 325

А. Ковальчук[1], М. Ступень[2]
Національний університет "Львівська політехніка",
[1]кафедра інформаційних технологій та видавничої справи,
[2]кафедра автоматизованих систем управління

БІНАРНІ ЛІНІЙНО-КВАДРАТИЧНІ ПЕРЕТВОРЕННЯ З ЕЛЕМЕНТАМИ АЛГОРИТМУ RSA І ДОДАТКОВИМ ЗАШУМЛЕННЯМ У ЗАХИСТІ ЗОБРАЖЕНЬ

Запропоновано алгоритм шифрування-дешифрування зображень з використанням елементів алгоритму RSA як найбільш криптографічно стійкого до несанкціонованого дешифрування, стосовно зображень зі строго чіткими контурами. Елементи алгоритму RSA пропонується використовувати як коефіцієнти деякого лінійно-квадратичного афінного перетворення. Запропонований алгоритм має вищу криптографічну стійкість порівняно з алгоритмом RSA.

Ключові слова: шифрування, дешифрування, зображення, контур, криптографічна стійкість.

Suggested algorithm encryption-decryption images with using elements RSA algorithm, as most cryptographically stability to unauthorized decryption, concerning images with clear contours strictly. Elements of the RSA algorithm is proposed to use as the coefficients of a linear-quadratic affine transformation. The proposed algorithm has a higher stability cryptography compared with the RSA algorithm

Key words: encryption, decryption, image, contour, cryptographic stability.

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].

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 контура означає пошук найрізкіших 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.

Будемо вважати, що зображенню відповідає матриця кольорів

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

Розглянемо афінне лінійно-квадратичне перетворення, де коефіцієнти *A, B, C, D* – довільні дійсні числа:

$$\begin{cases} Ax + By = u \\ Cx^2 + Dy^2 = v \end{cases} \quad (1)$$

Шифрування і дешифрування за одним рядком матриці зображення

Нехай P і Q — пара довільних простих чисел. Виберемо числа

$$N = PQ, \varphi(N) = (P-1)(Q-1), \quad (2)$$

$$e_1 d_1 \equiv 1 \pmod{\varphi(N)}, \quad (3)$$

$$e_2 d_2 = 1 \pmod{\varphi(N)}, \quad (4)$$

$$e_3 d_3 \equiv 1 \pmod{\varphi(N)}. \quad (5)$$

Шифрування відбувається з використанням елементів одного рядка за такою схемою:

з кожного рядка матриці зображення C вибираються два послідовні значення інтенсивності кольору (кожне значеня вибирається один раз) і обчислюються наступні три величини

$$I - P^{e_1} \pmod{N}, \quad J - Q^{d_2} \pmod{N}, \quad K = (P+Q)^{e_3} \pmod{N}, \quad (6)$$

де числа e_1, e_2, e_3, d_1, d_2, d_3 отримуються з співвідношень (3)–(5) відповідно.

У (1) вибираються коефіцієти *A = I, B = C = J, D = K* і $x = c_{i,j}$, $y = c_{i,j+1}$, $1 \le i \le n$, $1 \le j \le m$. Величини $u + f(i)$, $v + g(i)$, (u, v отримані з (1)) записуються як два послідовні в рядку значення зашифрованого зображення, кожне значення в один рядок.

Дешифрування проводиться за наступними формулами (після розв'язання системи (1) відносно *x* і *y*)

$$y = \frac{\beta \pm \sqrt{\beta^2 - 4\alpha\gamma}}{2\alpha},$$

$$x = \frac{u - By}{A},$$

де

$$\alpha = CB^2 + A^2 D,$$

$$\beta = 2CBu,$$

$$\gamma = Cu^2 - A^2 v.$$

Результати при $I = -1, C = B = J, D = K, P = 23, Q = 13, f(i) = Pi^2$, $g(i) - Qi^2$ наведені на рис. 1–3.

Шифрування і дешифрування за двома рядками матриці зображення

В кожних двох рядках матриці зображення C вибирають відповідні значення інтенсивності кольору з кожного рядка x і y. Рядки вибираються послідовно. Кожний рядок вибирається тільки один раз.

Рис. 1. Початкове зображення

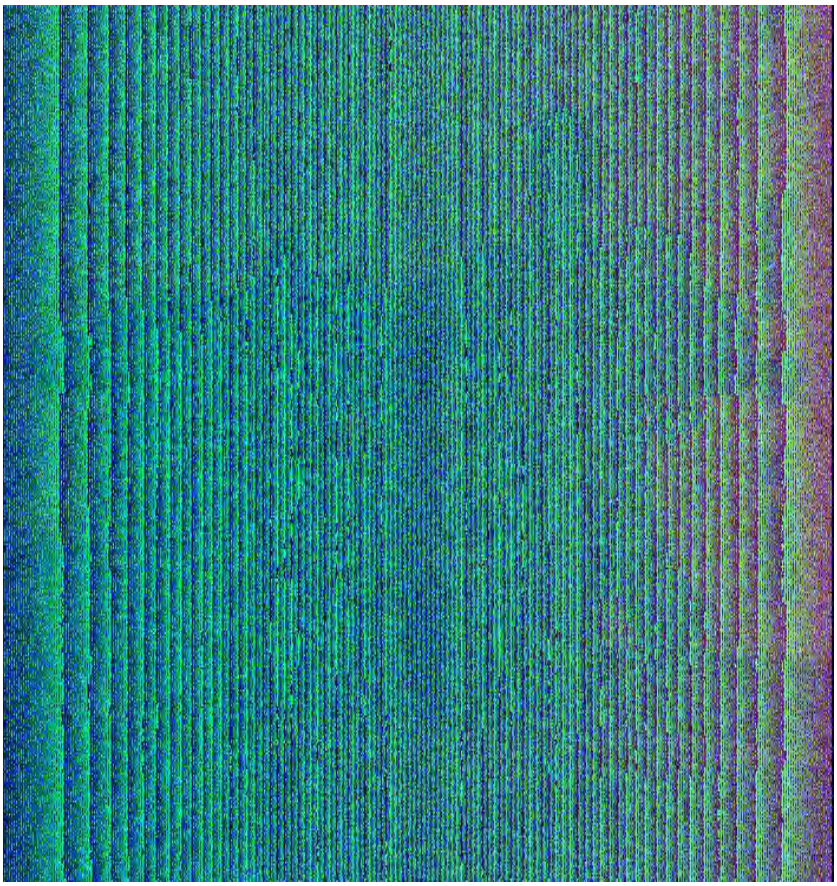

Рис. 2. Зашифроване зображення

Рис. 3. Дешифроване зображення

Шифрування проводиться як і у випадку використання одного рядка матриці зображення за формулами (1) – (6) з іншими функціями зашумлення. Дешифрування проводиться за тими самими формулами, що і у випадку використання одного рядка:

$$y - \frac{\beta \pm \sqrt{\beta^2 - 4\alpha\gamma}}{2\alpha}, \quad x - \frac{u - By}{A},$$

$$\alpha = CB^2 + A^2D, \beta = 2CBu, \gamma = Cu^2 - A^2v.$$

Результати при $I = -1, C = B = J, D = K, P = 23, Q = 13, f(i) = i^3, g(i) = i^3$ наведено на рис. 4–6.

Висновок

З порівняння рис. 2 і рис. 5 видно, що шифрування по одному рядку матриці зображення відрізняється від шифрування за трьома рядками цієї матриці. Контури в обох зашифрованих зображеннях відсутні. Візуально всі зашифровані зображення відрізняються між собою. Цей алгоритм можна використати при передаванні графічних зображень. Запропоновані модифікації можуть бути використані стосовно будь-якого типу зображень, але найбільших переваг досягають у випадку використання зображень, які дозволяють чітко виділяти контури.

Обидва способи шифрування-дешифрування можна використати і стосовно кольорових зображень. Однак, незалежно від типу зображення, пропорційно до розмірності вхідного зображення може зрости розмір шифрованого зображення.

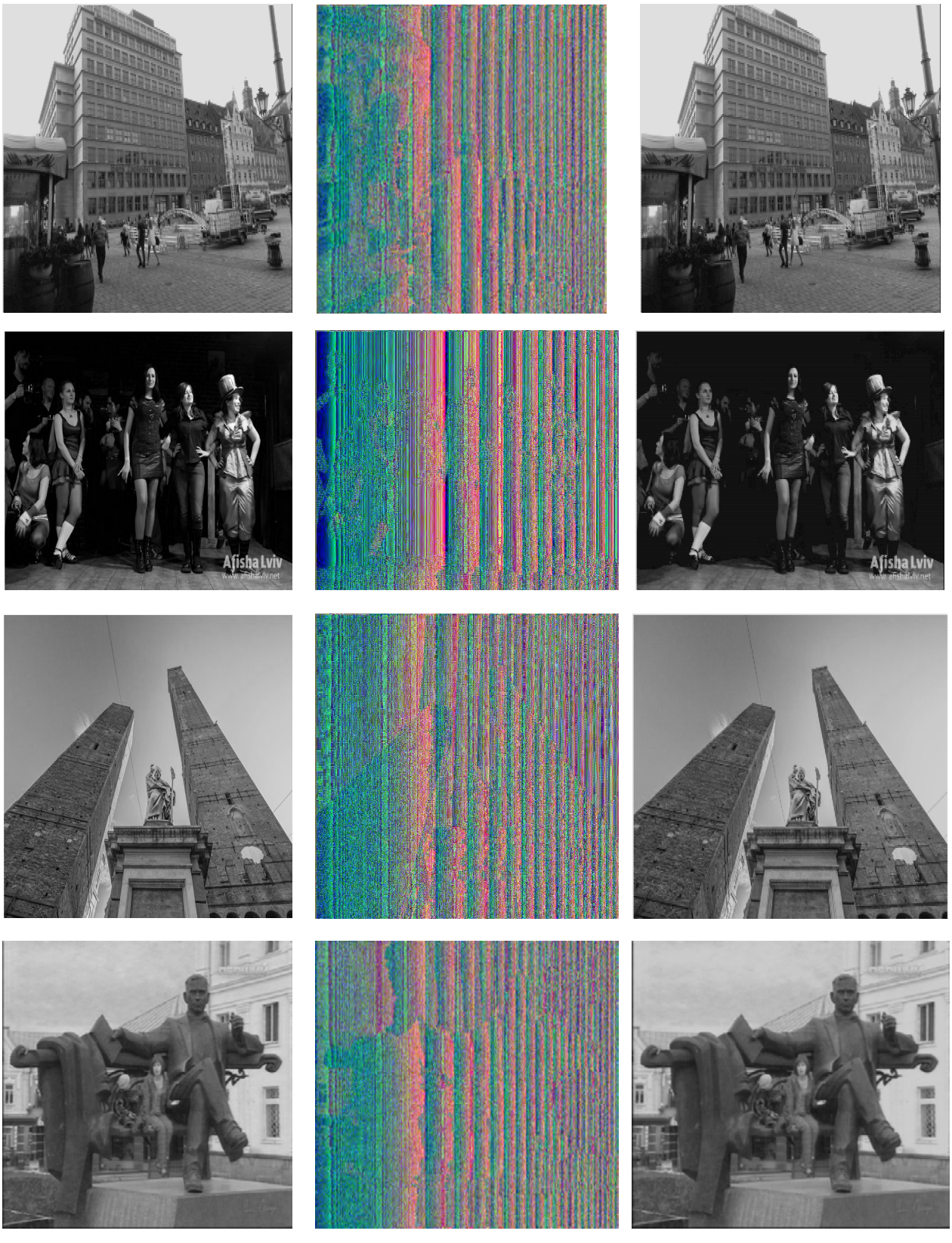

Рис. 4. Початкові зображення *Рис. 5. Зашифровані зображення* *Рис. 6. Дешифровані зображення*

1. Шнайер Б. Прикладная криптография / Б. Шнайер. – М.: Триумф, 2003. – 815 с. 2. Яне Б. Цифровая обработка изображений / Б. Яне. – М.: Техносфера , 2007. – 583 с. 3. Ковальчук А. Кубічні і лінійні фрактали з елементами алгоритму RSA в шифруванні і дешифруванні зображень /

А. Ковальчук, І. Цмоць, М. Ступень // Вісник Нац. ун-ту "Львівська політехніка" "Комп'ютерні науки та інформаційні технології". – 2014. – № 800. – С. 149–153. 4. Ковальчук А. Бінарні операції та елементи алгоритму RSA при шифруванні-дешифруванні кольорових зображень / А. Ковальчук, Д. Пелешко, Ю. Борзов // Вісник Нац. ун-ту "Львівська політехніка" "Комп'ютерні науки та інформаційні технології". – 2013. – № 771. – С. 121–125.

УДК 621.317.73

E. Pokhodylo, V. Yuzva
Lviv Polytechnic National University,
Department of Metrology, Standardization and Certification

MEASUREMENT OF ELECTROPHYSICAL PARAMETERS OF ALCOHOLIC SOLUTIONS

Mathematical models are analyzed which describe active and reactive components multielement two-terminal admittance, which provides system "electrode-alcohol solution."

Key words: admittance, capacity double layer, dielectric conductivity, specific conductance.

Introduction

Today, the need to control the quality of any products is known. The evaluation of quality of liquor (vodka, whiskey, gin, etc.) and ethanol is especially important. This is due to the advent of mass production of such low quality, which is dangerous for society, imitations of the products of large manufacturers, unaccounted products beyond the production control and replacement products on counterfeit analogue during transport from manufacturer to consumer. That is why speed control, eliminating subjective errors of assessment of product quality, comparing the quality control results of production by manufacturer with the results of monitoring by consumer provides its identification.

Control of electrophysical parameters for the components immittance.

One method of such controlling is a method, which is based on measuring electrophysical parameters, namely the dielectric permeability ε_x and conductivity σ_x of control object [1, 2]. Realized measuring of these parameters can be simple technical means of a special purpose or using serial wide-range meters of complex impedance parameters or conductivity (immitance) [3]. You must additionally have a primary converter of dielectric permittivity and conductivity of control object in measurable parameters applied device. Preferably these parameters are resistance R, and capacitance C, active G and reactive B, which are components of complex resistance Z (impedance) or active G and reactive B, which are components of complex conductivity Y (admittance). In this case permittivity and conductivity using capacitive primary converter of plane parallel constructures is determined by known formulas:

$$C = \frac{e_0 e_x S}{d}, \tag{1}$$

$$G = s\,\frac{d}{S}, \tag{2}$$

from which get:

$$e_x = C \cdot \frac{d}{S} \cdot \frac{1}{e_0} = \frac{A}{e_0} \cdot C, \tag{3}$$