УДК 01.05.02; 05.13.06; 05.13.21

А. М. Ковальчук, Н. Д. Лотошинська
Національний університет «Львівська політехніка»,
кафедра інформаційних технологій виддавничої справи

ШИФРУВАННЯ І ДЕШИФРУВАННЯ ПІВТОНОВИХ ТА КОЛЬОРОВИХ ЗОБРАЖЕНЬ

Зображення як стохастичний сигнал є одними із найбільш використовуваних видів інформації. Відповідно актуальною задачею є захист такого зображення від несанкціонованого доступу та використання. Це спричиняє можливість використання відомих класичних методів шифрування у випадку шифрування зображень. Запропоновано алгоритми шифрування – дешифрування, призначені для використання зображень у градаціях сірого, які грунтуються на використанні ідей базового алгоритму RSA. Шифрування – дешифрування можна проводити як з додатковим зашумленням, так і без нього. Описано також поєднання елементів алгоритму RSA і бінарних операцій для сумісного використання при шифруванні – дешифруванні кольорових зображень.

Ключові слова: шифрування, дешифрування, зображення, контур, криптографічна стійкість, афінне перетворення, бінарна операція.

A. Kovalchuk, N. Lotoshynska
Lviv Politechnik Nationall Univesity,
Department of Information Technology Publishing

ENCRYPTION AND DECRYPTION OF GRAYSCALE AND COLOR IMAGES

Images used as a stochastic signal are among the most commonly used types of information. Accordingly, the actual task is to protect such images from unauthorized access and use. This leads to the use of known classic encryption methods in the case of image encryption. Offered algorithms of encryption-decryption are intended for the use of images in grayscale and are based on using the ideas of basic RSA algorithm. Encryption – decryption can be carried out with extra noising and without too. A combination of elements of the RSA algorithm and binary operations is also described for co-use in encryption – decryption of color images.

Keywords: encryption, decryption, image, edge, cryptographic stability, affine transformation, binary operation.

Вступ

Основним базисом для захисту зображення є припущення, що зображення – це стохастичний сигнал. Але зображення є специфічним сигналом, який володіє, в додаток до типової інформативності (інформативності даних), ще й візуальною інформативністю, що привносить в питання захисту нові задачі.

Саме така інформативність в поєднанні із високорозвиненими сучасними методами обробки зображень надає можливість несанкціонованого доступу. Фактично організація атаки на зашифроване зображення можлива у двох варіантах: через традиційний злам методів шифрування або за

допомогою методів візуальної обробки зображень (методи фільтрації, виділення контурів тощо). Але останні не дають повного відтворення зашифрованого зображення, проте дають можливість отримати деяку інформацію із зображення. В зв'язку з цим до методів шифрування у випадку їх використання стосовно зображень висувається ще одна вимога – повна зашумленість зашифрованого зображення. Це потрібно для того, щоб унеможливити використання методів візуальної обробки зображень.

Побудовано алгоритм шифрування-дешифрування зображень із використанням елементів алгоритму RSA як найбільш криптографічно стійкого до несанкціонованого дешифрування [1, 8] стосовно зображень зі строго чіткими контурами. Елементи алгоритму RSA пропонується використовувати для побудови коефіцієнтів деяких афінних перетворень. Запропонований алгоритм володіє вищою криптографічною стійкістю порівняно з алгоритмом RSA [2, 8]. Описано використання елементів алгоритму RSA в афінних перетвореннях при шифруванні – дешифруванні зображень .

Відносно шифрування зображення актуальною задачею [4] є реалізація такого застосування алгоритму RSA, щоб:

– не зменшити криптографічну стійкість алгоритму RSA;

– забезпечити повну зашумленість зображення для запобігання використанню методів візуальної обробки зображень.

Ще одним шляхом створення такої модифікації є поєднання елементів алгоритму RSA і бінарних операцій у програмній реалізації.

Елементами алгоритму RSA називатимемо прості числа $\boldsymbol{P}$ і $\boldsymbol{Q}$ та числа $\boldsymbol{e}$ та $\boldsymbol{d}$ у конгруенції $\boldsymbol{ed} \circ \mathbf{1(mod}\ j\ \boldsymbol{(N))}$, $\boldsymbol{N = P*Q}$.

Аналіз останніх досліджень

Нехай задано зображення $\boldsymbol{P}$ ширини l і висоти h. Його можна розглядати як матрицю пікселів [4]

$$<dtp_{ij}>_{1\le i\le n,\ 1\le j\le m}, \tag{1}$$

де dtp_{ij} – піксел з координатами i та j, n і m – кількість точок за шириною l та висотою. В загальному випадку n і m є залежними від l та h, а тому коректнішим є запис

$$n = n(l) \text{ і } m = m(h). \tag{2}$$

Матриці (1) відповідає матриця інтенсивностей пікселів

$$\mathbf{C}=\begin{pmatrix} c_{1,1} & \dots & c_{1,m} \\ \dots & \dots & \dots \\ c_{n,1} & \dots & c_{n,m} \end{pmatrix}, \tag{3}$$

де c_{ij} – значення інтенсивності пікселя dtp_{ij} у напівтоновому зображенні. Тобто існує відповідність

$$P = \mathbf{P}_{l,h} = \left[pxl_{ij} \right]_{1\le i\le n(l),1\le j\le m(h)} \to \mathbf{C}=\left[c_{ij} \right]_{1\le i\le n(l),1\le j\le m(h)}. \tag{4}$$

Під градацію яскравості зазвичай приділяють 1 байт, причому 0 – чорний колір, а 255 – білий (максимальна інтенсивність).

Математично контур у зображенні – це розрив просторової функції рівнів яскравості в площині зображення. Тому виокремлення контура означає пошук найбільш різких змін, тобто максимумів модуля вектора градієнта [3,9]. Це є однією з причин, з яких контури залишаються в зображенні при шифруванні в системі RSA, оскільки шифрування тут грунтується на піднесенні до степеня за модулем деякого натурального числа [5–7]. При цьому на контурі і на сусідніх до контуру пікселах піднесення до степеня значення яскравостей дає ще більший розрив.

Основні матеріали досліджень

1. Шифрування і дешифрування за одним рядком матриці зображення

Нехай P, Q – пара довільних простих чисел і $N = P * Q$. Шифрування виконують поелементно з використанням такого перетворення елементів матриці зображення C:

1. Випадково вибирають натуральне число $e < j(N)$ і знаходять таке натуральне d, щоб виконувалася конгруенція $ed \equiv 1 (\mathrm{mod}\ j(N))$.

2. Будують число $A = c_{ij} + Q + P + i + j - d$.

3. Зашифрованим значенням інтенсивності i - го піксела, $i = 1, 2, \ldots, m$, m – кількість елементів у рядку, вибирають число $B \equiv A^e (\mathrm{mod}\ N)$.

Дешифрування проводять у послідовності, протилежній до шифрування після отримання числа $B^d \equiv (A^e)^d (\mathrm{mod}\ N)$, виконанням протилежних операції до змісту пунктів (3), (2), (1). Результати наведено на рис.1.

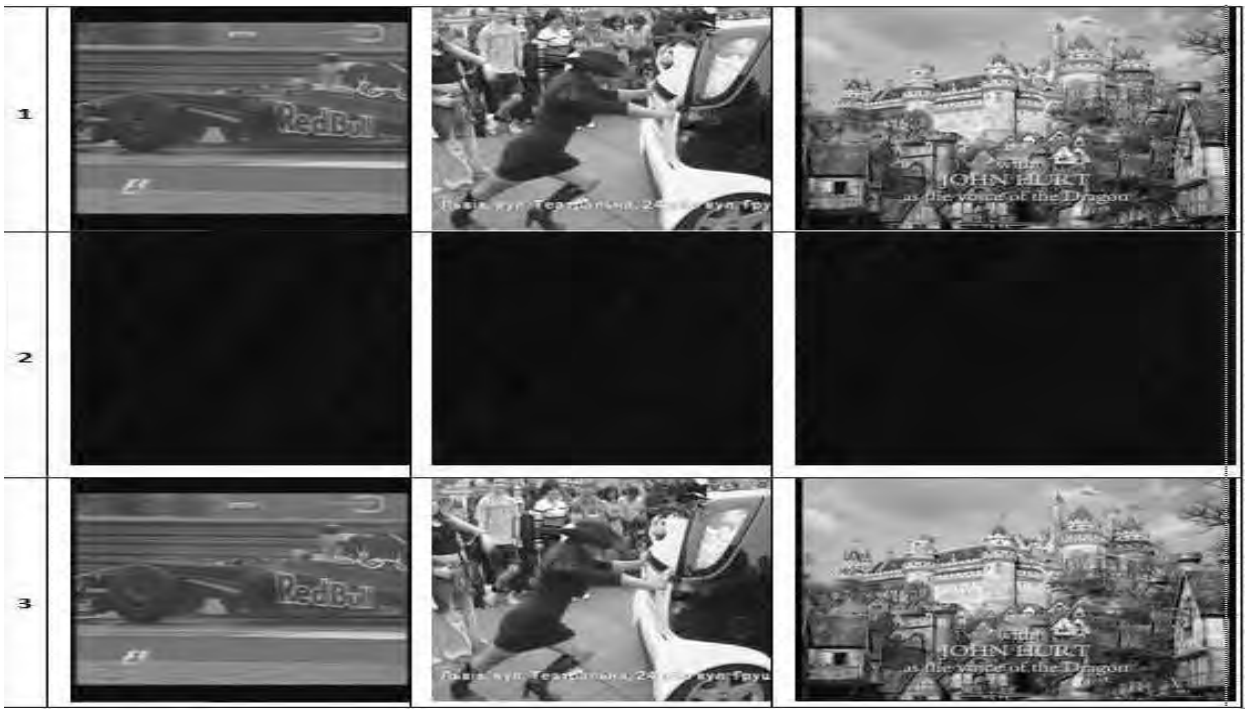

Рис. 1. Результати шифрування- дешифрування зображення:
1 – початкові зображення; 2 – зашифровані зображення; 3 – дешифровані зображення

2. Шифрування і дешифрування за одним рядком матриці зображення із додатковим зашумленням

Нехай P, Q – пара довільних простих чисел і $N = P * Q$. Шифрування відбувається поелементно з використанням такого перетворення елементів матриці зображення C:

1. Випадково вибирають натуральне число $e < j(N)$ і знаходять таке натуральне d, щоб виконувалася конгруенція $ed \equiv 1 (\mathrm{mod}\ j(N))$.

2. Будують число $A = c_{ij} + Q + P + i + j - d$.

Зашифрованим значенням інтенсивності i – го піксела, $i = 1, 2, \ldots, m$, m – кількість елементів у рядку, вибирають число $C \equiv A^e (\mathrm{mod}\ N) + f(i, j)$.

Дешифрування проводять у послідовності, протилежній до шифрування після отримання числа $(C - f(i, j))^d \equiv (A^e)^d (\mathrm{mod}\ N)$, виконанням протилежних операції до змісту пунктів (3), (2), (1).

Результати наведено на рис.2. Для шифрування вибирали такі функції додаткового зашумлення: $f(i, j) = i^2$, $f(i, j) = i * j$, $f(i, j) = j^2$.

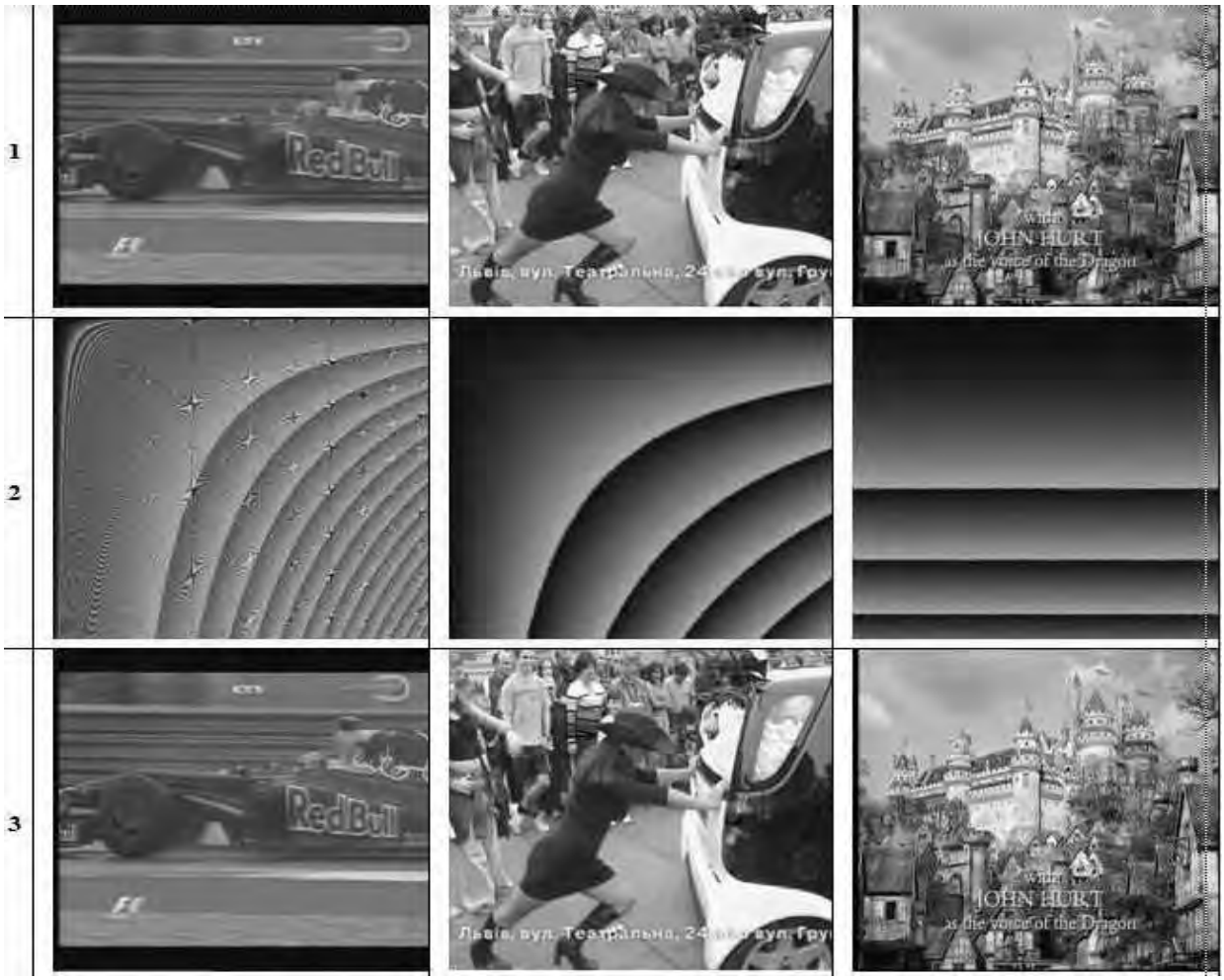

Рис. 2. Результати шифрування- дешифрування зображення:
1 – початкові зображення; 2 – зашифровані зображення; 3 – дешифровані зображення

З порівняння рис.1 і рис.2 видно, що шифрування із додатковим зашумленням відрізняється від шифрування без додаткового зашумлення. Контури в обох зашифрованих зображеннях відсутні. Початкові і дешифровані зображення тільки незначно відрізняються рівнем яскравості. Функції додаткової зашумленості $f(i, j)$ можуть бути довільними цілозначними функціями і додатково, до створюваної алгоритмом RSA криптографічної стійкості, підвищують криптографічну стійкість вказаних модифікацій.

3. Використання побітових операцій

3.1. Шифрування за одним рядком матриці зображення.

Нехай P, Q – пара довільних простих чисел і $N = P * Q$, $j(N) = (P - 1)(Q - 1)$. Шифрування відбувається поелементно з використанням такого перетворення елементів матриці зображення C:

1. Випадково вибирають натуральне число $e < j(N)$ і знаходять таке натуральне d, щоб виконувалася конгруенція $ed \equiv 1 \pmod{j(N)}$.

2. Якщо $i \equiv 0 \pmod 2$, $1 \le i \le l$, то вибирають число $m \equiv (i + P) \pmod{31}+1$ і будують числа $B \equiv m^e \pmod N$, $X = i*B*P$.

3. Якщо $i \equiv 1 \pmod 2$, $1 \le i \le l$, то вибирають число $m \equiv (i + Q) \pmod{31}+1$ і будують числа $B \equiv m^d \pmod N$, $X = i*B*Q$.

4. З використанням бінарної операції ^ – порозрядного виключеного «АБО» – будують число $a = c_{i,j} \wedge X$.

5. Виокремлюють кожний розряд a_i числа a за такою схемою:
a_1= a & 01; a_2= a & 02; a_3 = a & 04; a_4= a & 010; a_5 = a & 020; a_6 = a & 040;
a_7 = a & 0100; a_8 = a & 0200; a_9 = a & 0400; a_{10} = a & 01000; a_{11} = a & 02000;
a_{12} = a & 04000; a_{13} = a & 010000; a_{14} = a & 020000; a_{15} = a & 040000;
a_{16} = a & 0100000; a_{17} = a & 0200000; a_{18} = a & 0400000; a_{19} = a & 01000000;
a_{20} = a & 02000000; a_{21} = a & 04000000; a_{22} = a & 010000000; a_{23} = a & 020000000;
a_{24} = a & 040000000; a_{25} = a & 0100000000; a_{26} = a & 0200000000; a_{27} = a & 0400000000;
a_{28} = a & 01000000000; a_{29} = a & 02000000000; a_{30} = a & 04000000000;
a_{31} = a & 010000000000; a_{32} = a & 020000000000, де & – операція арифметичного «І».
6. Виконується циклічне заміщення m + 1 розрядів числа a за схемою:
k = am+1 , am+1 = am , … , a2 = a1 , a1 = k.
7. Зашифрованим є зображення після 5 – го кроку.
8. Усі числа B записують у матриці

$$V = \begin{pmatrix} b_{1,1} & \dots & b_{1,l} \\ \dots & \dots & \dots \\ b_{h,1} & \dots & b_{h,l} \end{pmatrix}.$$

3.2. Дешифрування за одним рядком матриці зображення

Дешифрування проводять при заданих числах $e < j(N)$ і d, $N = P*Q$.
$j(N) = (P-1)(Q-1)$.
1. Якщо $i \circ 0 \pmod 2$, $1 \le i \le l$, то будують число $m \circ B^d \pmod N$ і число $X = i*B*P$.
2. Якщо $i \circ 1 \pmod 2$, $1 \le i \le l$, то будується число $m \circ B^e \pmod N$ і число $X = i*B*Q$.
3. Виокремлюється кожний розряд a_i числа a за схемою:
4. a1= a & 01; a2 = a & 02; a3 = a & 04; a4 = a & 010; a5 = a & 020; a6 = a & 040;
a_7 = a & 0100; a_8 = a & 0200; a_9 = a & 0400; a_{10} = a & 01000; a_{11} = a & 02000;
a_{12} = a & 04000; a_{13} = a & 010000; a_{14} = a & 020000; a_{15} = a & 040000;
a_{16} = a & 0100000; a_{17} = a & 0200000; a_{18} = a & 0400000; a_{19} = a & 01000000;
a_{20} = a & 02000000; a_{21} = a & 04000000; a_{22} = a & 010000000; a_{23} = a & 020000000;
a_{24} = a & 040000000; a_{25} = a & 0100000000; a_{26} = a & 0200000000;
a_{27} = a & 0400000000; a_{28} = a & 01000000000; a_{29} = a & 02000000000;
a_{30} = a & 04000000000; a_{31} = a & 010000000000; a_{32} = a & 020000000000,
де **&** – операція арифметичного «**І**».
5. Виконують циклічне заміщення $m + 1$ розрядів числа a за схемою: $k = a_{m+1}$, $a_{m+1} = a_m$, … , $a_2 = a_1$, $a_1 = k$.
6. Із використанням бінарної операції ^ – порозрядного виключеного **«АБО»** – будують число $c_{i,j} = a \wedge X$.
7. Дешифрованим є зображення після 5 – го кроку.
Результати наведено на рис.3 – 5 при $P = 53$, $Q = 83$.

Рис. 3. Вхідне зображення

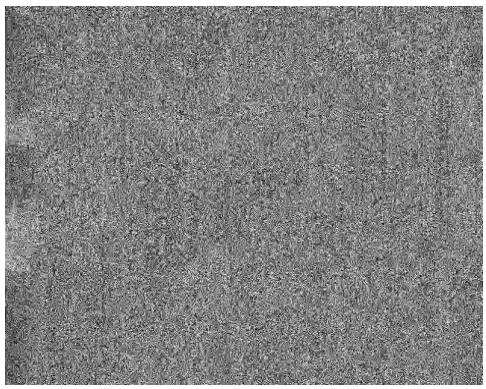

Рис. 4. Зашифроване зображення

Рис. 5. Дешифроване зображення

Висновки

1. Порівнюючи рис. 4 і рис. 1, бачимо, що шифрування з використанням побітових операцій і шифрування з використанням елементів RSA відрізняються суттєво. Контури в обох зашифрованих зображеннях відсутні. Вхідні і дешифровані зображення тільки незначно відрізняються за рівнем яскравості.

2. Запропоновані алгоритми призначені для шифрування зображень у градаціях сірого і ґрунтуються на використанні ідей базового алгоритму RSA.

3. Запропоновані алгоритми можна використати стосовно будь-якого типу зображень, але найбільших переваг досягають у випадку використання зображень, в яких можна чітко виокремлювати контури.

4. Обидва типи модифікацій без жодних застережень можна використати і стосовно кольорових зображень. Однак, незалежно від типу зображення, пропорційно до розмірності вхідного зображення, зростає розмір шифрованого зображення.

5. Стійкість до несанкціонованого дешифрування запропонованими модифікаціями забезпечується алгоритмом RSA.

6. Запропонований метод шифрування кольорових зображень може бути застосований до будь-яких кольорових зображень.

1. Kovalchuk A., Peleshko D., Navytka M. and Sviridova T., Using of affine transformations for the encryption and decryption of two images, 2011 11th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), Polyana-Svalyava, 2011, pp. 348–349. 2. Rashkevych Y., Kovalchuk A., Peleshko D. and Kupchak M., Stream modification of RSA algorithm for image coding with precize contoure extraction, 2009 10th International Conference – The Experience of Designing and Application of CAD Systems in Microelectronics, Lviv-Polyana, 2009, pp. 469–473. 3. Peleshko D., Ivanov Y., Sharov B., Izonin I. and Borzov Y., "Design and implementation of visitors queue density analysis and registration method for retail videosurveillance purposes", 2016 IEEE First International Conference on Data Stream Mining & Processing (DSMP), Lviv, 2016, pp. 159–162. doi: 10.1109/DSMP.2016.7583531. 4. Peleshko D., Rak T., Peleshko M., Izonin I. and Batyuk D., Two-frames image superresolution based on the aggregate divergence matrix, 2016 IEEE First International Conference on Data Stream Mining & Processing (DSMP), Lviv, 2016, pp. 235–238. doi: 10.1109/DSMP.2016.7583548. 5. Van den Braden Lambrecht C.J. and Farrell J.E. "Perceptual Quality Metric for Digitally Coded Color Images". In: Proceeding of EUSIPCO, pp. 1175–1178, Trieste, Italy, September 1996. 6. Majid Rabbani, Rajan Joshi. "An overview of the JPEG2000 still image compression standard" // Eastman Kodak Company, Rochester, NY 14650, USA, Signal Processing: Image Communication. – 2002. – Vol. 17. – P. 3–48. 7. Girod B. "The information theoretical significance of spatial and temporal masking in video signals" // Proc. of the SPIE Symposium on Electronic Imaging. 1989. – Vol. 1077.– P. 178–187. 8. A. Kovalchuk and N. Lotoshynska, "Elements of RSA Algorithm and Extra Noising in a Binary Linear-Quadratic Transformations During Encryption and Decryption of Images", 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP), Lviv, Ukraine, 2018, pp. 542–544. doi: 10.1109/DSMP.2018.8478471. 9. Gonzalez, Rafael C., Woods, Richard E., "Digital Image Processing", published by Pearson Education, Inc, Publishing as Prentice Hall, 2002.