IEEE Second International Conference on Data Stream Mining & Processing
August 21-25, 2018, Lviv, Ukraine

Elements of RSA Algorithm and Extra Noising in a Binary Linear-Quadratic Transformations During Encryption and Decryption of Images

Anatoliy Kovalchuk
Lviv Polytechnic National University
Department of Information Technology Publishing
Lviv, Ukraine
akm0519@gmail.com

Nataliia Lotoshynska
Lviv Polytechnic National University
Department of Information Technology Publishing
Lviv, Ukraine
nsvlot@gmail.com

***Abstract* — An algorithm is proposed for encrypting-decrypting images using RSA algorithm elements, as the most cryptographically resistant to unauthorized decryption related to images with strictly clear edges. It is proposed to use RSA algorithm elements as coefficients of some linear-quadratic affine transformation. The proposed algorithm has a higher cryptographic stability compared to RSA algorithm.**

Keywords — encryption, decryption, image, outline, cryptographic stability.

I. INTRODUCTION

An important image feature is the image edges availability. The edge separation task requires using of operations on adjacent elements sensitive to changes and obliterating regions of constant brightness levels, that is, edges are those areas where changes occur, becoming bright, while other parts of the image remain dark [2].

There are certain issues with image encryption, namely, the edges are partially preserved on sharply fluctuating images [3, 4].

The mathematically perfect edge is the rupture of brightness levels spatial function within image plane. Therefore, the edge determination means a search for the sharpest changes, that is, the maxima of the gradient vector module [2]. This is one of the reasons why edges remain within the image while encrypting in RSA system, since encryption here is based on the elevation up to the degree by modulus of a certain natural number [1]. In this case, brightness gives an even greater gap on the edge and edge adjacent pixels of raising to a degree.

As is known [5, 6], the theoretical stability is determined on the condition that there are no time limits for unauthorized decryption, and therefore it is an answer to the question that the cryptosystem cannot be split in principle. They can be constructed using a random equally probable encryption key, which key length is not less than the length of the open text. Completely stable systems are extremely expensive in implementation. Therefore, the systems are used in practice, which in principle can be split, but at an unacceptable time.

Let us assume that the image is assigned a matrix of color

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

Consider the next affine linear quadratic transformation, where *A, B, C, D* coefficients are arbitrary real numbers

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

II. ENCRYPTING AND DECRYPTING BY ONE LINE OF IMAGE MATRIX

Let ***P*** and ***Q*** be a pair of arbitrary prime numbers.

Construct numbers:

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

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

$$e_2 d_2 \equiv 1(\mathrm{mod}\,\varphi(N)), \quad (4)$$

$$e_3 d_3 \equiv 1(\mathrm{mod}\,\varphi(N)). \quad (5)$$

Encryption occurs using elements of the same line according to the following scheme:

Two consecutive values of color intensity are selected from image matrix ***C*** line (each value is selected once) and the following three values are calculated:

$$I = P^{e_1} (\mathrm{mod}\, N),\ J = Q^{d_2} (\mathrm{mod}\, N), \quad (6)$$

$$K = (P+Q)^{e_3} (\mathrm{mod}\, N),$$

where $e_1, e_2, e_3, d_1, d_2, d_3$ is the number, which are obtained from the relations (3) - (5) – respectively.

In (1), the coefficients are chosen *A* = *I*, *B* = *C* = *J*,

D = *K* і $x = c_{i,j}$, $y = c_{i,j+1}$, $1 \le i \le n$, $1 \le j \le m$.

Encoded are the values $u' = u + f(i)$ and $v' = v + g(i)$, where $f(i)$ and $g(i)$ are some of the noises (u, v derived from (1)) are recorded as two consecutive values in the line of encrypted image, each value per one line.

Decryption is carried out according to the following formulas (after solving system (1) relative x, y)

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

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

where $u = u' - f(i)$, $v = v' - g(i)$.

Results for $I = -1$, $C = B$, $D = K$, $P = 23$, $Q = 13$, $f(i) = Pi^2$, $g(i) = Qi^2$ are shown in Fig. 1 - Fig.3.

Fig.1 Initial Image

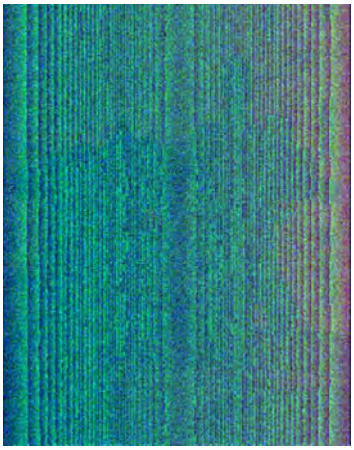

Fig.2 Encrypted image

Fig. 3 Decrypted image

III. ENCRYPTING AND DECRYPTING BY TWO LINES OF IMAGE MATRIX

In each two lines of the image matrix C the corresponding color intensity values are selected from each line of ***x*** and ***y***. The lines are selected sequentially. Each line is selected only once. Encryption is performed similar to using one line of the image matrix by the formulas (1) – (6) with other functions of noise masking. Decryption is performed using the same formulas as in case of using one line:

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

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

Results for $I = -1$, $C = B = J$, $D = K$, $P = 23$, $Q = 13$, $f(i) = i^3$, $g(i) = i^3$ are shown in Fig. 4 - Fig.9.

Fig. 4 Initial Image

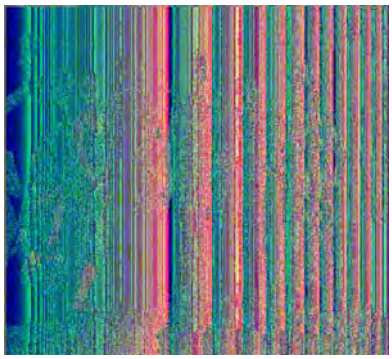

Fig. 5 Encrypted image

Fig.6. Decrypted image

Fig.7. Initial Image

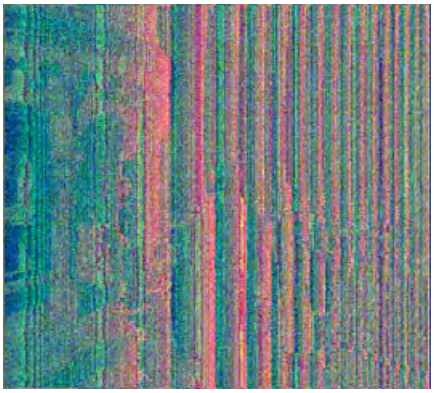

Fig. 8 Encrypted image

CONCLUSION

Comparison of Fig. 2 and Fig. 5, Fig. 8 shows that the encryption by one line of the image matrix differs from encryption by two lines of this matrix. There no edges in the encrypted images. All encrypted images are visually different. The specified algorithm can be used for the graphic images transmission.

- The proposed encryption modifications are intended for encryption of images in grayscale and are based on using the ideas of basic RSA algorithm.
- The proposed algorithms can be used for any type of image, but the greatest benefits are achieved when using the images that allow for clear edge definition.
- Both modifications can be used with no reservations for color images. However, regardless of the image type, the size of the encrypted image increases proportionally to the size of the input image.
- Resistance to unauthorized decryption in the proposed modifications is provided by RSA algorithm with additional stability, which is determined by binary transformations.
- Modified encryption methods are constructed so that at the low key values it is also possible to achieve qualitative encryption, but provided the correct selection of encryption parameters. This allows achieving the high speed of the algorithm.

Fig.9. Decrypted image

REFERENCES

[1] Bryus Shnayer, Prykladna kryptohrafiya. M .: Tryumf, 2003.

[2] B. Jähne. Digitale image processing (6th ed.), Springer-Verlag Berlin Heidelberg, 2005.

[3] A. Kovalchuk, D. Peleshko, M. Navytka and T. Sviridova, "Using of affine transformations for the encryption and decryption of two images," 11th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), Polyana-Svalyava, Ukrane, pp. 348-349, 2011.

[4] Y. Rashkevych, A. Kovalchukm, D. Peleshko and M. Kupchak, "Stream modification of RSA algorithm for image coding with precize contoure extraction," 10th International Conference - The Experience of Designing and Application of CAD Systems in Microelectronics, Lviv-Polyana, Ukrane, pp. 469-473, 2009.

[5] M. Nazarkevych, R. Oliarnyk, O. Troyan and H. Nazarkevych, "Data protection based on encryption using Ateb-functions," XIth International Scientific and Technical Conference Computer Sciences and Information Technologies (CSIT), Lviv, Ukrane, pp. 30-32, 2016. doi: 10.1109/STC-CSIT.2016.7589861

[6] M. Nazarkevych, R. Oliiarnyk, H. Nazarkevych, O. Kramarenko and I. Onyshschenko, "The method of encryption based on Ateb-functions," IEEE First International Conference on Data Stream Mining & Processing (DSMP), Lviv, Ukrane, pp. 129-133, 2016. doi:10.1109/DSMP.2016.