RSA ALGORITHM ELEMENTS IN TERNARY AFFINE TRANSFORMATIONS IN ENCRYPTION-DECRYPTION OF IMAGES

Anatoliy Kovalchuk, Senior Lecturer, Nataliia Lotoshynska, Ph.D., Associate Professor
Mariia Podavalkina, 4th-grade student, Khrystyna Pelekh 4th-grade student
Lviv Polytechnic National University Ukraine
e-mail: akm0519@gmail.com

Abstract

Regarding image encryption, a crucial task is to implement the application of such an RSA algorithm which will provide an opportunity:

– not to decay the cryptographic stability of the RSA algorithm;

– to ensure complete noisiness of an image to prevent the application of methods of visual image processing.

An algorithm for encryption-decryption of monochrome images using elements of the RSA algorithm as the most resistant to unauthorized signal decryption in ternary affine transformations is proposed. The developed algorithm is applied to images in which there are strictly delineated contours. Elements of the RSA algorithm are proposed to be used to construct the coefficients of ternary affine transformations. The proposed algorithm has higher cryptographic stability compared to the RSA algorithm. The ways of applying the elements of the RSA algorithm in affine transformations in encryption-decryption of images are described in this article.

The results of modeling the affine modified cipher for cryptographic transformations of black and white monochrome images of a given dimension are presented. Modified models and algorithmic procedures of key generation processes, direct and inverse cryptographic transformations, which are reduced to matrix element-by-element operations by module, are developed.

Keywords

Encryption, Monochrome image, Ternary affine transformation, Contour, Decryption.

1. Introduction

The necessity to solve theoretical and practical problems of information security and achieve the required level of protection of different content led to the era of information technology and mass communications and the corresponding rapid development of cryptography.

An image can be defined as a two-dimensional function $\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{y})$, where $\boldsymbol{x}$ and $\boldsymbol{y}$ are coordinates in space (specifically, on a plane). The value of $\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{y})$ at any point is called the intensity or level of gray at that point. If the values $\boldsymbol{x}$, $\boldsymbol{y}$, and $\boldsymbol{f}$ ***(x, y)*** take a finite number of discrete values, then we are talking about a digital image. Digital image processing is the processing of digital images via computers. Note that a digital image consists of a finite number of elements, each of which is located in a specific place and acquires a certain meaning. These elements are called image elements or pixels.

Mathematically, a digital image is represented by a matrix of $\boldsymbol{n}\times\boldsymbol{m}$ pixel intensities, where $\boldsymbol{n}$ is the number of image rows, and $\boldsymbol{m}$ is the number of columns.

The most common and stable information encryption algorithm is the RSA algorithm [1, 2], which is relevant to most public-key search algorithms. The security of the RSA algorithm is based on the resource-intensive factorization of large natural numbers. The use of the RSA algorithm [1, 2] as the most resistant to unauthorized decryption for images with strictly delineated contours does not give satisfactory results. In the encrypted picture, it is possible to distinguish the main contours of the input image — there is an effect of incomplete noisiness.

Contour isolation means finding the maxima of the modulus of the gradient vector [2]. This is one of the reasons why contours remain in the image when encrypted via the RSA system since the encryption in RSA is based on the exponentiation of some natural number.

In this case, on the contour and the adjacent to the contour pixels elevation to the degree of brightness gives an even greater gap [3-10]. The presence of contours in the image is an important characteristic of the image. The task of contour isolation requires the use of operations on neighboring elements that are sensitive to a change and dampen the magnitude of brightness levels, i.e., contours are those areas where changes occur, becoming light, while other parts of the image remain dark [11, 12].

Concerning pictures, there are certain problems of image encryption, namely partially preserved contours on sharply fluctuating images. Below we will apply the following definition of the affine transformation of Euclidean space in

Cartesian coordinates: the transformation of Euclidean space is called affine if this transformation reflects each plane to the plane.

2. Disadvantages

Studies [13-14] have revealed that within the contours of the image during encryption, significant deviations in the values of pixel intensities can be created, which makes it impossible to blur these contours at some values of the selected prime numbers.

3. Purpose

The purpose of this work is to construct the modification of the RSA algorithm using ternary affine transformations and various elements of the RSA algorithm that allows us to obtain complete blurring of the image contours.

4. Encryption Technique

Elements of the RSA algorithm are called prime numbers ***P*** and ***Q***, as well as numbers e and d from the congruence ed ≡ 1 (mod φ(N)), N = P *Q, φ(N), is an Euler's function. Let us assume that the image is matched by a color matrix (matrix of pixel intensities) [13-15]

$$R = \begin{pmatrix} r_{1,1} & \dots & r_{1,m} \\ \dots & \dots & \dots \\ r_{n,1} & \dots & r_{n,m} \end{pmatrix}.$$

Let the ternary affine transformation of Euclidean space in Cartesian coordinates has the following form:

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

Then the inverse to (1) transformation exists and

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

where

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

4.1. ENCRYPTION AND DECRYPTION BY ROWS OF COLOR MATRIX

4.1.1. Encryption and decryption by one row of the color matrix.

Let ***P***, ***Q*** be random prime numbers. We choose the numbers

$$\begin{gathered} n = PQ,\ \ \varphi(n) = (P - 1)(Q - 1),\ \ e_1d_1 \equiv 1\,(mod\ \varphi(n)),\ \ e_2d_2 \equiv 1\,(mod\ \varphi(n)), \\ e_3d_3 \equiv 1\,(mod\ \varphi(n)),\ \ e_1 < \varphi(n),\ \ d_1 < \varphi(n),\ e_2 < \varphi(n),\ \ d_2 < \varphi(n), \\ e_3 < \varphi(n),\ \ d_3 < \varphi(n). \end{gathered} \qquad (3)$$

Encryption is performed using the elements of each row of the image matrix according to formulas (1), where $x = r_{i,j}, y = r_{i,j+1},\ z = r_{i,j+2},\ i = \overline{1,n}\ , j = \overline{1,m}.$

Three consecutive elements of the matrix row are selected so that each element is selected only once and only in one triple. The coefficients (the choice may be different, however, the chosen coefficients must satisfy the condition $\boldsymbol{\delta} \neq \mathbf{0}$ in (2)) are selected as follows:

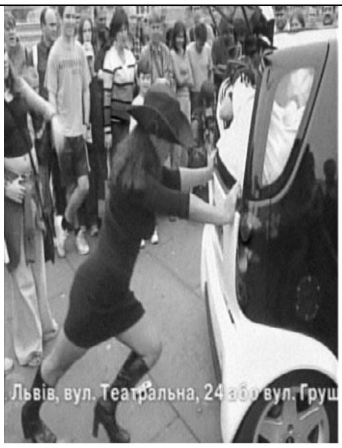
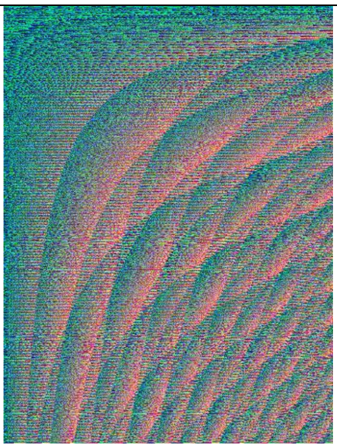
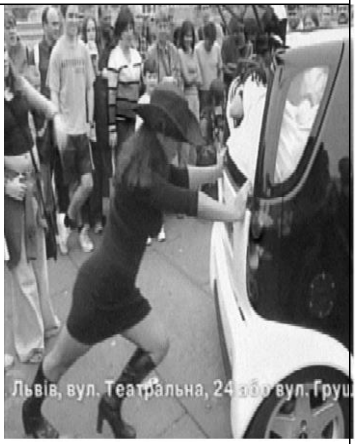
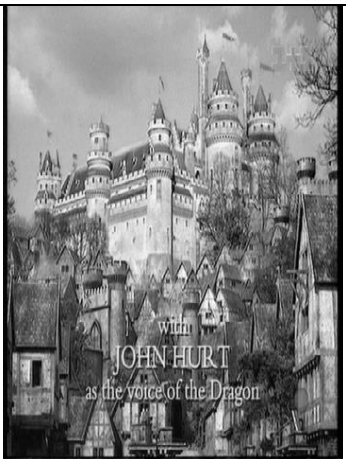
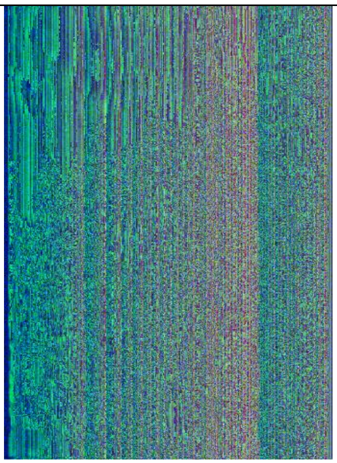
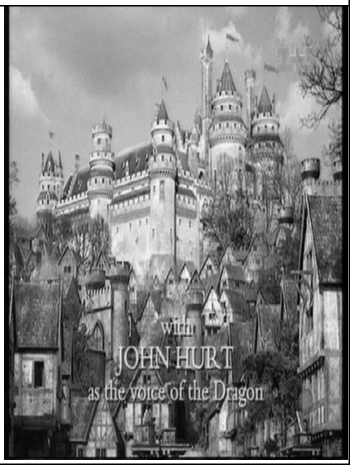
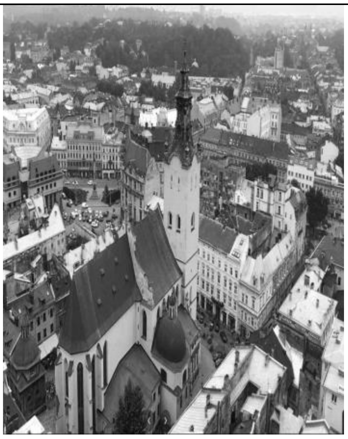
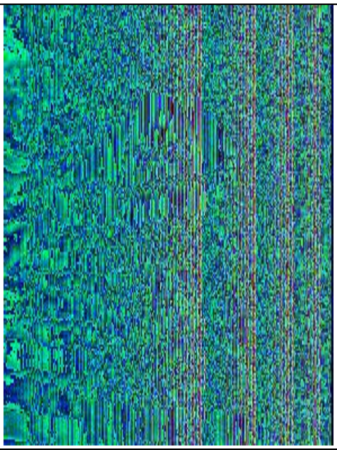
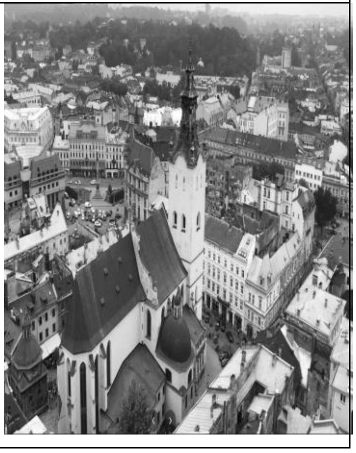
$$\boldsymbol{a_1 = b_3 = d_2 = P^{e_1}(\mathrm{mod}\, n)}, \qquad \boldsymbol{b_1 = a_2 = d_3 = Q^{d_2}(\mathrm{mod}\, n)}, \; d_1 = \boldsymbol{b_2 = a_3 = Q^{e_3}(\mathrm{mod}\, n)}, \text{ - natural numbers.}$$

Decryption takes place according to the formulas of inverse transformation (2) with coefficients calculated by the RSA algorithm:

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

The results for different values ***P*** and ***Q*** are shown in Table 1.

Tabl. 1. Results of encryption and decryption by one row of the color matrix

Prime numbers ***P*** and ***Q***	Original image	Encrypted image	Decrypted image
23 **53**			
23 **73**			
43 **103**			

4.1.2. Encryption and decryption by three rows of the color matrix.

Encryption is performed using the elements of three rows according to formulas (1), where $x = r_{i,j}, y = r_{i+1,j}$, $z = r_{i+2,j}$, $i = \overline{1,n}$, $j = \overline{1,m}.$ Three elements with the same numbers are selected (one from each row) so that in every three elements each element is selected only once. The coefficients

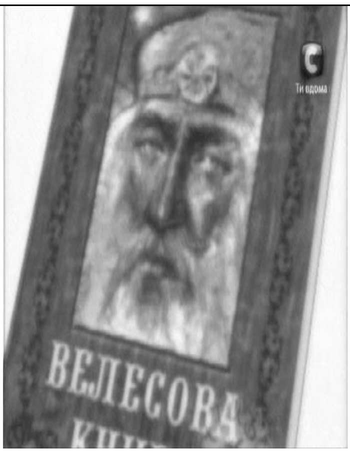
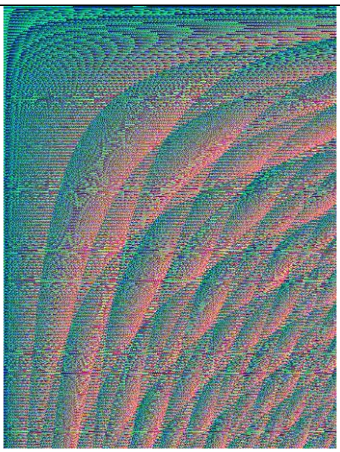
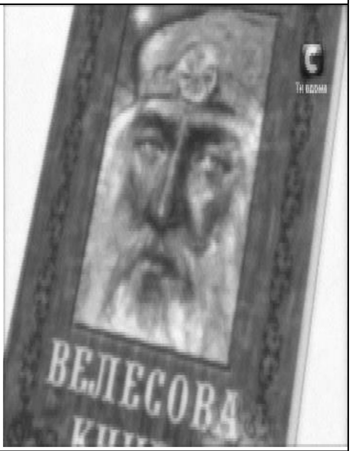
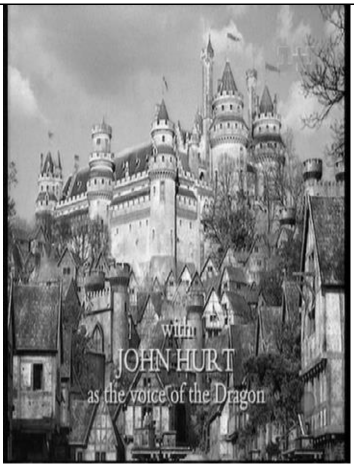
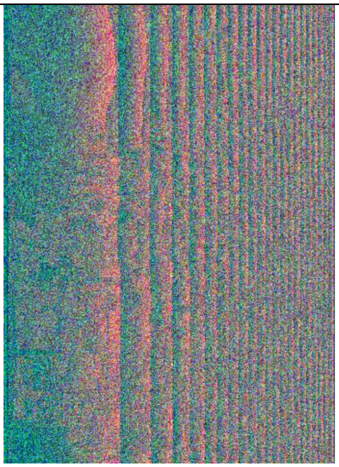
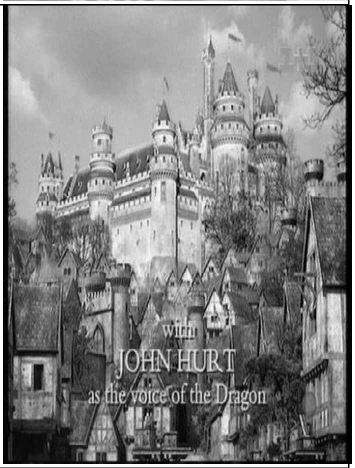
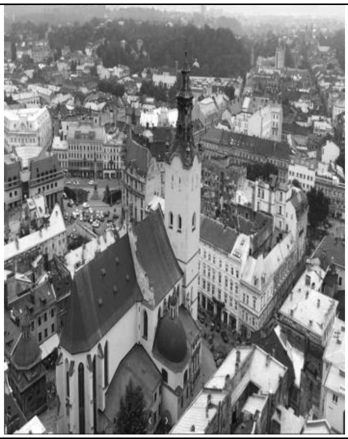
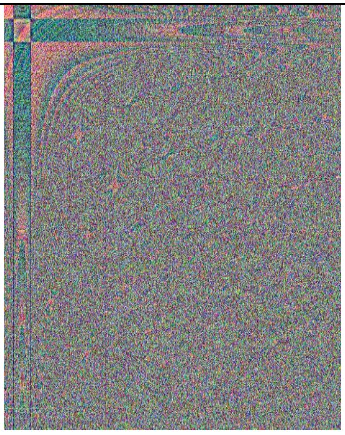
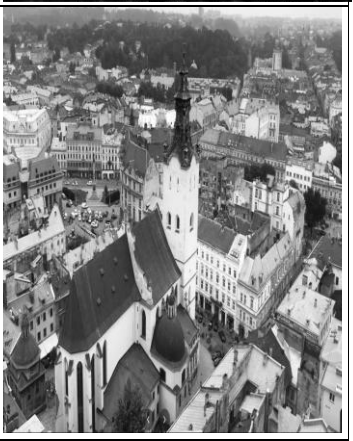
$\boldsymbol{a_1 = b_3 = d_2 = Q^{e_1}}(\bmod \boldsymbol{n})$, $\boldsymbol{b_1 = a_2 = d_3 = P^{d_2}}(\bmod \boldsymbol{n})$, $d_1 = \boldsymbol{b_2 = a_3 = (Q + P)^{e_3}}(\bmod \boldsymbol{n})$ are integers.

Decryption is performed according to the formulas of the inverse transformation (2) with coefficients

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

The results for different values ***P*** and ***Q*** are shown in Table 2.

Tabl. 2. Results of encryption and decryption by three rows of the color matrix

Prime numbers ***P*** and ***Q***	Original image	Encrypted image	Decrypted image
23 **53**			
23 **73**			
43 **103**			

5. Conclusions

Employing a visual comparison of encrypted images, it is evident that the encryption by one row of the image matrix differs from the encryption by three rows of this matrix. The contours are absent in both encrypted images. This algorithm can be applied when transmitting graphic images. The proposed modifications are applicable for any type of image, but the greatest advantages are achieved when is applied for images with clearly visible contours.

There is also a slight difference between the original and decrypted images. That is, the implementation of the proposed algorithms does not impair the image quality. However, in situations where there are certain requirements and quality criteria, it usually takes a certain number of attempts to select such prime numbers $\boldsymbol{P}$ and $\boldsymbol{Q}$ as well as the numbers $\boldsymbol{e}$ and $\boldsymbol{d}$ in the congruence $\boldsymbol{ed} \equiv \mathbf{1}\ (\mathbf{mod}\ \varphi(N))$, $\boldsymbol{N} = \boldsymbol{P} * \boldsymbol{Q}$ to achieve the criteria for the equivalence of the original and decrypted image quality.

Based on numerical experiments with different monochrome images in encryption and decryption using the described algorithms, it is established that the proposed modifications have the advantage — enhancement of the cryptographic stability of the RSA algorithm. Both types of modifications can be applied without any reservations for color images. However, regardless of the type of image, the size of the encrypted image increases proportionally to the dimension of the input image.

6. Acknowledgments

The authors express their gratitude to the staff of the Department of Information-Measuring Technologies of Lviv Polytechnic National University, Ukraine, for the assistance in the preparation of this article.

7. Conflict of Interests

Conflict of interest while writing, preparing, and publishing the article as well as mutual claims by the co-authors is absent.

References

[1] B. Schneier, *Applied Cryptography: Protocols, Algorithms and Source Code in C. – RF*. Triumf, 2003.

[2] B. Jane, *Digital Image Processing*. Springer–Verlag Berlin Heidelberg, 2005.

[3] B. Girod, “The information theoretical significance of spatial and temporal masking in video signals”, *Proc. of the SPIE Symposium on Electronic Imaging*.1989, vol. 1077. pp.178–187.

[4] M. Rabbani, R. Joshi, “An overview of the JPEG2000 still image compression standard” , Eastman Kodak Company, Rochester, NY 14650, USA, Signal Processing: Image Communication, vol.17, pp.3–48, 2002.

[5] S. X. Liao, M. Pawlak, “On image analysis by moments”, IEEE Transaction on Pattern Analysis and Machine Intelligence, no.3, pp.254–266, 1996.

[6] E. Haacke, R. Brown, M. Thompson, R. Vencatesan, *Magnetic Resonanse Imagin: Physical Principles and Sequence Design.* John Wiley & Sons, 1999.

[7] J. Kajiya, *The rendering equation*, 1986.

[8] M. Sarfraz, *Introductory Chapter: On Digital Image Processing*. 2020.

[9] E. Samei, Donald J Peck, *Projection X- ray Imaging, Hendee's Physics of Medical Imaging*. 2019.

[10] M. Vollmer, K- P. Mollmann, *Infrared Thermal Imaging*. 2017.

[11] R. Gonzales, R. Woods. *Digital image processing*. Prentice Hall, Upper Saddle River, NJ, 2nd edn., 2002.

[12] R. Gonzalez, R. Woods, *Digital Image Processing*. Publ. Pearson Education, Inc, Publishing as Prentice Hall, 2002.

[13] A. Kovalchuk, I. Izonin, C. Strauss, M. Podavalkina, N. Lotoshynska, N. Kustra, “Image encryption and decryption schemes using linear and quadratic fractal algorithms and their systems”, *CEUR Workshop Proceedings*, no.2533, 2019, pp.139-150.

[14] A. Kovalchuk, I. Izonin, M. Gregush, N. Lotoshyiiska, “An approach towards image encryption and decryption using quaternary fractional-linear operations”, Procedia Computer Science, no.160, pp.491– 496, 2019.

[15] A. Kovalchuk, N. Lotoshynska, “Elements of RSA Algorithm and Extra Noising in a Binary Linear-Quadratic Transformations During Encryption and Decryption of Images”, in *Proc. IEEE Second International Conference on Data Stream Mining & Proc*essing (DSMP), Lviv, Ukraine, 2018, pp.542–544.