

USE OF KVATERNARN LINEAR-FRACTIONAL FRACTAL FORMS IN ENCRYPTION - DECRYPTION IMAGES WITH ELEMENTS RSA ALGORITHM

An application of the kvaternarn fractional-linear form with using the standard elements of the RSA algorithm for encryption and decryption of two-dimensional images is resistant to unauthorized access to images clearly distinguished contours..

Keywords: the kvaternarn shape, image, contour, firmness encryption.

Introduction

The problem of improving the quality of information protection systems can be viewed from the point of view of economy, science and technology, which have contributed to the rapid development of computer technology, microelectronics, telecommunications, etc. Significant contribution to the development of information protection methods was made by such Russian and foreign scientists: І.Д. Горбенко, А.А. Молдован, В.М. Рудницький, В.Ф. Шаньгін, Б. Шнайдер and others.

One of the most prevalent and persistent information encryption algorithms is RSA algorithm [1]. He belongs to the most frequently used groups of algorithms and public key cryptography. The security of RSA is based on the resource cost factorization of large integers. The public and private keys are functions of two Prime numbers with a capacity of 100-200 or more decimal digits.

Using the RSA encryption algorithm [1], as the most resistant to unauthorized decryption of encrypted signals, for the images, which allow very strictly allocate contours, does not yield satisfactory results. On the encrypted image all the same, you can distinguish the basic contours of the input image. That is, there is the effect of incomplete degradation of the image.

An important characteristic of the image is the presence in the image paths. The problem of separation circuit requires the use of operations on the adjacent elements that are sensitive to changes and пригашають the field of permanent brightness levels, i.e. paths are those areas where changes occur, becoming pale, other parts of the image remain dark [2].

In relation to the image, there are certain problems encrypt it, namely partially preserved to the contours of the sharp fluctuation images [3, 4].

Mathematically - contour image this is the gap spatial function of the levels of brightness in the image plane. Therefore, the path selection in the image means finding the most dramatic change, i.e. the high module gradient vector [2]. This is one of the reasons for that contours remain in the image when encrypting the RSA algorithm, because the encryption here is based on a hill in the degree modulo a certain natural number. Thus, on the path, and on adjacent to loop pixels піднесення in the degree of brightness values gives even greater disparity.

For information protection is the most commonly used raster and vector graphics, and promising methods are methods of information protection through the use of fractal transformations of algebraic fractional-linear forms.

Among the common fractals decided to allocate three basic groups [5-6]:

– *Algebraic fractals*, which are created using non-linear computational processes in n-dimensional spaces. To this group, in particular, belongs to the Mandelbrot set.

– *Geometric fractals* that in the two-dimensional case are created using a broken generator. One-step algorithm for each of the segments of a broken replaced with a broken generator and thus the appropriate scale creates a geometric fractal image. To this group of fractals are триадное Koch curve and the dragon hurter.

– *Stochastic fractals* that are created iterative process with random parameters. Images of stochastic fractals are very similar to natural unbalanced tree.

We assume that the image corresponds to a matrix of flowers

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

Quarter of fractional-linear form has the form

$$t(x, y, z, m) = \frac{ax + by + fz + gm + \delta}{cx + dy + hz + km + \Delta}. \quad (1)$$

Using (1), fulfil the transformation

$$\begin{cases} x_n = \frac{Ax_{n-1} + By_{n-1} + Fz_{n-1} + Gm_{n-1} + \delta}{Cx_{n-1} + Dy_{n-1} + Hz_{n-1} + Km_{n-1} + \Delta}; \\ y_n = \frac{Bx_{n-1} + Fy_{n-1} + Gz_{n-1} + Km_{n-1} + \delta}{Ax_{n-1} + Cy_{n-1} + Dz_{n-1} + Hm_{n-1} + \Delta}; \\ z_n = \frac{Fx_{n-1} + Gy_{n-1} + Kz_{n-1} + Hm_{n-1} + \delta}{Bx_{n-1} + Ay_{n-1} + Cz_{n-1} + Dm_{n-1} + \Delta}; \\ m_n = \frac{Gx_{n-1} + Ky_{n-1} + Hz_{n-1} + Dm_{n-1} + \delta}{Fx_{n-1} + By_{n-1} + Az_{n-1} + Cm_{n-1} + \Delta}; \end{cases} \quad (2)$$

Where $A = P, B = Q, F = e, G = d, C = P, D = -Q, H = d, K = e, \delta = P, \Delta = Q$ – elements of the standard RSA algorithm, n - level number of fractality.

Reverse (2) the transformation has the form

$$\begin{cases} (x_n C - A)x_{n-1} + (x_n D - B)y_{n-1} + (x_n H - F)z_{n-1} + (x_n K - G)m_{n-1} = \delta - x_n \Delta; \\ (y_n A - B)x_{n-1} + (y_n C - F)y_{n-1} + (y_n D - G)z_{n-1} + (y_n H - K)m_{n-1} = \delta - y_n \Delta; \\ (z_n B - F)x_{n-1} + (z_n A - G)y_{n-1} + (z_n C - K)z_{n-1} + (z_n D - H)m_{n-1} = \delta - z_n \Delta; \\ (m_n F - G)x_{n-1} + (m_n B - K)y_{n-1} + (m_n A - H)z_{n-1} + (m_n C - D)m_{n-1} = \delta - m_n \Delta; \end{cases} \quad (3)$$

and if

$$\delta = \begin{vmatrix} x_n C - A & x_n D - B & x_n H - F & x_n K - G \\ y_n A - B & y_n C - F & y_n D - G & y_n H - K \\ z_n B - F & z_n A - G & z_n C - K & z_n D - H \\ m_n F - G & m_n B - K & m_n A - H & m_n C - D \end{vmatrix} \neq 0, \quad (4)$$

then

$$x_{n-1} = \frac{\delta_x}{\delta}, y_{n-1} = \frac{\delta_y}{\delta}, z_{n-1} = \frac{\delta_z}{\delta}, m_{n-1} = \frac{\delta_m}{\delta}; \quad (5)$$

where

$$\delta_x = \begin{vmatrix} \delta - x_n \Delta & x_n D - B & x_n H - F & x_n K - G \\ \delta - y_n \Delta & y_n C - F & y_n D - G & y_n H - K \\ \delta - z_n \Delta & z_n A - G & z_n C - K & z_n D - H \\ \delta - m_n \Delta & m_n B - K & m_n A - H & m_n C - D \end{vmatrix}, \quad (6)$$

$$\delta_y = \begin{vmatrix} x_n C - A & \delta - x_n \Delta & x_n H - F & x_n K - G \\ y_n A - B & \delta - y_n \Delta & y_n D - G & y_n H - K \\ z_n B - F & \delta - z_n \Delta & z_n C - K & z_n D - H \\ m_n F - G & \delta - m_n \Delta & m_n A - H & m_n C - D \end{vmatrix}, \quad (7)$$

$$\delta_z = \begin{vmatrix} x_n C - A & x_n D - B & \delta - x_n \Delta & x_n K - G \\ y_n A - B & y_n C - F & \delta - y_n \Delta & y_n H - K \\ z_n B - F & z_n A - G & \delta - z_n \Delta & z_n D - H \\ m_n F - G & m_n B - K & \delta - m_n \Delta & m_n C - D \end{vmatrix} \quad (8)$$

$$\delta_m = \begin{vmatrix} x_n C - A & x_n D - B & x_n H - F & \delta - x_n \Delta \\ y_n A - B & y_n C - F & y_n D - G & \delta - y_n \Delta \\ z_n B - F & z_n A - G & z_n C - K & \delta - z_n \Delta \\ m_n F - G & m_n B - K & m_n A - H & \delta - m_n \Delta \end{vmatrix}. \quad (9)$$

Encryption one row of the matrix of the image.

Encryption is performed using the elements of the matrix rows C by the formulas (2), where $x_{n-1} = c_{i,j}, y_{n-1} = c_{i,j+1}, z_{n-1} = c_{i,j+2}, m_{n-1} = c_{i,j+3}, i = \overline{1, n}, j = \overline{1, m}$. Selected four neighbouring elements of matrix rows so that each element has been selected only once and only to one of four.

Decryption occurs on the inverse transformation formulas (5) - (9) with the coefficients calculated on the RSA algorithm.

The results of encryption and decryption are shown on Fig.1 - 3.



Fig. 1. Original image

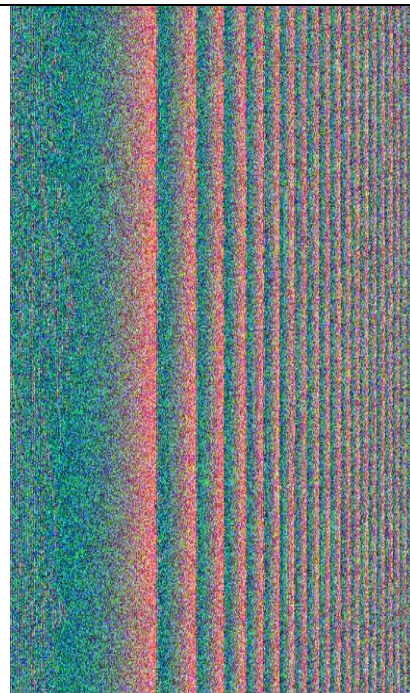


Fig.2. Encrypted image



Fig.3. Decrypted image

Encryption four rows of the matrix of the image.

Encryption is performed using elements of four rows by the formulas (2), where $x_{n-1} = c_{i,j}, y_{n-1} = c_{i+1,j}, z_{n-1} = c_{i+2,j}, m_{n-1} = c_{i+3,j}, i = \overline{1, n}, j = \overline{1, m}$. Selected four elements with identical numbers, one from each line, so that in every four each item has been selected only once.

Decryption occurs on the inverse transformation formulas (5) - (9) with coefficients $A = P, B = Q, F = e, G = d, C = P, D = -Q, H = d, K = e, \delta = P, \Delta = Q$.

The results of encryption and decryption are shown in Fig.4 - 6.

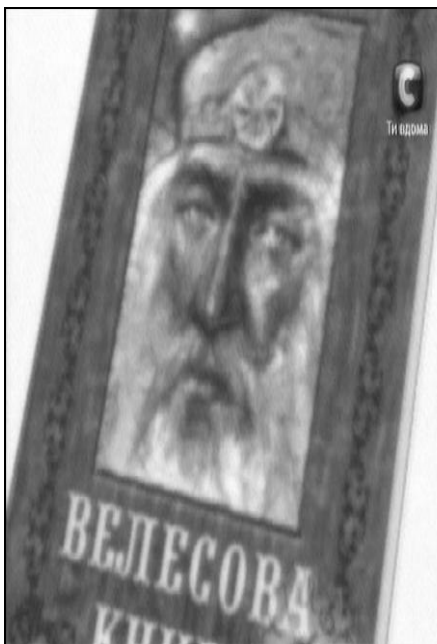


Fig. 4. Original image

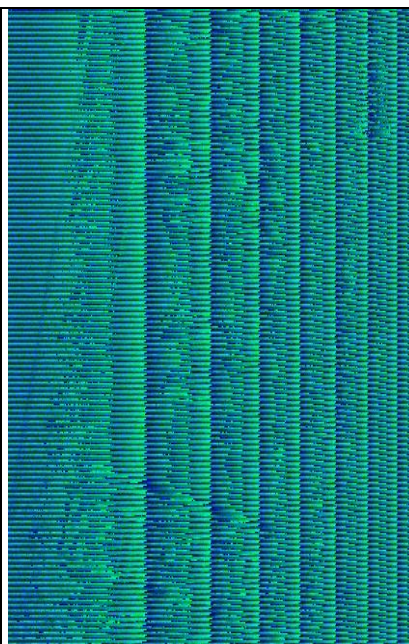


Fig.5. Encrypted image

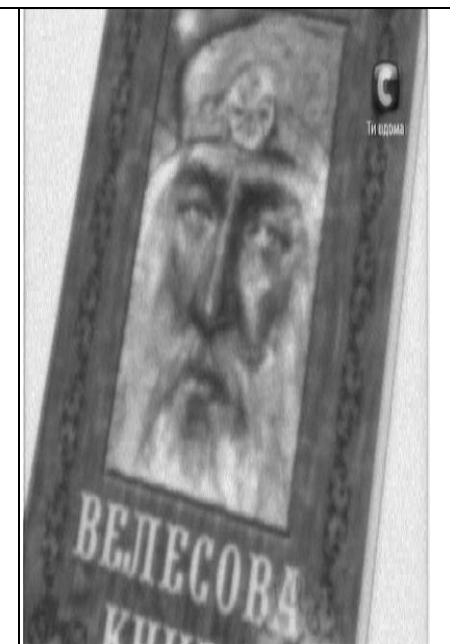

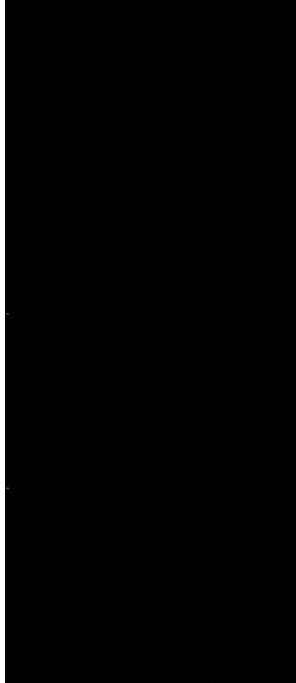
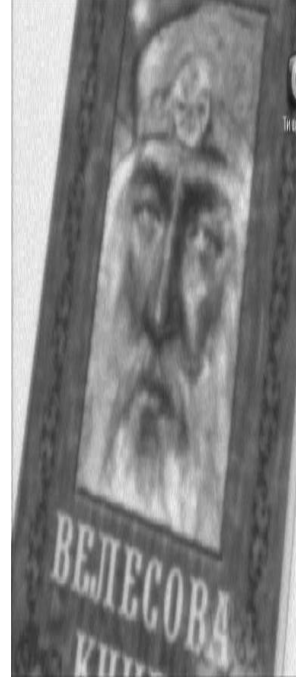
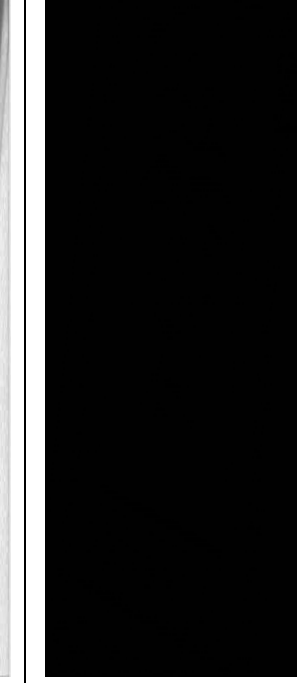


Fig.6. Decrypted image

Conclusion.

From the comparison of Fig. 2 and Fig. 5 shows that the encryption of one row of the matrix image is different from encryption four rows of this matrix. Contours in both encrypted images are missing. Proposed modifications can be used for any type of images, but the greatest benefits are achieved in the case of using images that accurately allocate contours. Both types of modification without any reservations can be used for color images. However, regardless of the type of the image is proportional to the dimension of the original image, can grow the size of the encrypted image.

The algorithms mother high криптологічну stability, which significantly depend on the choice of Prime numbers P and Q . This can be confirmed by the following examples.

			
<p>Fig. 7. Encryption-decryption when $P=103, Q=53, e=1667,$ $d=35$</p>	<p>Fig. 8. Decryption when $P=103, Q=61, e=4133,$ $d=77$</p>	<p>Fig. 9. Encryption-decryption when $P=103, Q=53, e=1667,$ $d=35$</p>	<p>Fig. 10. Decryption when $P=101, Q=53,$ $e=1981, d=21$</p>

From figures 7-10 it is seen that these algorithms are extremely sensitive to the choice of members of a standard algorithm RSA with the interpretation of the image. Minor changes in the values of these elements make it impossible to decipher the image.

Describes the algorithms can be used when the confidential transmission of images.

1. Брюс Шнайер. Прикладная криптография. – М.: Триумф, 2003. – 815с.
2. Б.Яне. Цифровая обработка изображений. – Москва, Техносфера, 2007.- 583с.
3. Ю.М. Рашкевич, Д.Д. Пелешко, А.М. Ковальчук, М.З. Пелешко. Модифікація алгоритму RSA для деяких класів зображень. *Технічні вісті* 2008/1(27), 2(28). С. 59 – 62.
4. Y.Rashkevych, A.Kovalchuk, D.Peleshko, M.Kurchak. Stream Modification of RSA Algorithm For Image Coding with precise contour extraction. *Proceedings of the X-th International Conference CADSM 2009. 24-28 February 2009, Lviv-Polyana, Ukraine*, Pp. 469-473.
5. Кроновер, Р. Фракталы и хаос в динамических системах [Текст] / Р. Кроновер. – М.: Техносфера, 2006.– 488 с.
6. Уэлстид, С. Фракталы и вейвлеты для сжатия изображений в действии [Текст] / С. Уэлстид. – М.: Триумф, 2003. – 320 с.