УДК 01.05.02; 05.13.06; 05.13.21

[1)]A.Kovalchuk, [1)]D.Peleshko, [2)] Yu.Borzov
[1)]NU «Lviv Polytechnic», department ITVS,
[2)] Lviv State University of life safety

BINARY OPERATIONS AND ELEMENTS OF THE RSA ALGORITHM WHEN ENCRYPTING-INTERPRETATION OF COLOR IMAGES

Described combination of elements of the RSA algorithm and binary operations for the joint use for encryption - interpretation of images. Encryption - decryption is performed without additional noise.

Keywords: encryption, decryption, the RSA algorithm, binary operation.

Introduction

The RSA algorithm is one of the most popular industrial standards of encryption signals. Unlike symmetric encryption process in which the procedure decryption is easily restored by the procedure encryption and back, in the scheme of public-key cryptography is impossible to calculate the decryption procedure, knowing the encryption procedure. More precisely, the algorithm computes the decryption procedure, is so great that it cannot be implemented on any modern computers, as well as on any computer of the future. Such coding schemes are referred to as asymmetric.

The image of the object - play type, form and color of the subject of the light rays that have passed optical system центрируемых spherical surfaces that have one common optical axis. Full raster images come from cameras and scanners. In particular, using them is a mass digitization of cultural achievements - books and films.

Image as a stochastic signal are some of the most used types of information. The urgent task is the protection of such images from unauthorized access and use. This leads to the use of well-known classical methods of encryption in the case of encryption images. But the image is a signal that owns, in addition to the type of information content, and even visual informative.

This informative modern methods of image processing gives opportunity for organization of unauthorized access. Actually, the organization of the attack on the encrypted image is available in two versions: through the traditional evil of encryption, or through the methods of visual image processing (filtering methods, selecting paths etc). In this regard, the cipher when used for images, put forward another requirement - full noise encrypted image. This is necessary in order to make it impossible to use the methods of the visual image processing.

In relation to the image, there are certain problems encrypt it, namely partially preserved to the contours of the sharp fluctuation images [4, 5]. Selecting paths in the image you create a description of its content, and , therefore, the contours allocation affects the overall execution time of the search. On the other hand, while a search affect time spent on comparison of descriptions of the image content. So, the algorithm contours allocation should be different as can be more productive and create a compact description of the circuit suitable for later comparison.

Goal of work

In relation to the image urgent task is modified using the RSA algorithm to:

- does not reduce the cryptographic strength of the RSA algorithm;
- ensure full noisy image, to make it impossible to use visual methods of image processing.

One of ways of creation of such modification is a combination of elements of the RSA algorithm and binary operations in the software implementation .

The characteristics of the image

Let specified figure ***P*** with width ***l*** and height ***h***. It can be thought of as a matrix of pixel intensities

$$\mathbf{C}=\begin{pmatrix} c_{1,1} & \dots & c_{1,l} \\ \dots & \dots & \dots \\ c_{h,1} & \dots & c_{h,l} \end{pmatrix}, \tag{1}$$

where c_{ij} – the value of pixel intensity. That is, there is the compliance [1]

$$P=\mathbf{P}_{l,h}=\left[pxl_{ij}\right]_{1\le i\le n(l),1\le j\le m(h)}\to\mathbf{C}=\left[c_{ij}\right]_{1\le i\le n(l),1\le j\le m(h)}. \tag{2}$$

Under the gradation of brightness usually have a 1 bytes, where 0 is black.

The problem of separation circuit requires the use of operations on the adjacent elements that are sensitive to changes and пригашают the field of permanent brightness levels, i.e. paths are those areas where changes occur, becoming pale, other parts of the image are dark. Therefore, the path selection means finding the most dramatic change, i.e. the highs module gradient vector [2]. This is one of the reasons for that contours remain in the image when you encrypt the system of RSA, 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 exponentiation brightness values gives even greater disparity.

Description encryption algorithm..

Encryption one row of the matrix image.

Let ***P, Q*** - a couple of random numbers and $N = P * Q$, $\varphi(N) = (P - 1)(Q - 1)$. Encryption is elementwise using the following transformation of the elements of the matrix image ***C***:

1. Randomly selected natural number $e < \varphi(N)$ and this is natural ***d***, that is congruention $ed \equiv 1 (\mathrm{mod}\ \varphi(N))$.
2. If $i \equiv 0 \pmod 2$, $1 \le i \le l$, then randomly selected number of $m \equiv (i + P) \pmod{31}+1$, and built a number of $B \equiv m^e \pmod N$, $X = i*B*P$.
3. If $i \equiv 1 \pmod 2$, $1 \le i \le l$, then randomly selected number of $m \equiv (i + Q) \pmod{31}+1$, and built a number of $B \equiv m^d \pmod N$, $X = i*B*Q$.
4. Using binary operations ^ - bitwise excluded «OR» - is the number of $a = c_{i,j}$ ^ X.

5. Highlights each category of a_i of number ***a*** according to the following scheme: 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, where & - the operation of the arithmetic «And».

6. Button repeatedly substitution **$m + 1$** discharges of number ***a*** to the following scheme: $\boldsymbol{k = a_{m+1}}$ **,** $\boldsymbol{a_{m+1} = a_m}$, … , $\boldsymbol{a_2 = a_1}$ **,** $\boldsymbol{a_1 = k}$**.**

7. Encrypted have the image after the 5-th step.

8. All the numbers B are written in the following matrix

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

Decryption of one row of the matrix image.

Decryption is done with given numbers $\boldsymbol{e < \varphi(N)}$ i $\boldsymbol{d}$, $\boldsymbol{N = P * Q}$, $\boldsymbol{\varphi(N) = (P - 1)(Q - 1)}$**.**

1. If $\boldsymbol{i \equiv 0 \pmod 2}$**,** $\boldsymbol{1 \le i \le l}$, the built number $\boldsymbol{m \equiv B^d \pmod N}$ and number $\boldsymbol{X = i*B*P}$.

2. If $\boldsymbol{i \equiv 1 \pmod 2}$**,** $\boldsymbol{1 \le i \le l}$, the built number $\boldsymbol{m \equiv B^e \pmod N}$ and number $\boldsymbol{X = i*B*Q}$.

3. Highlights each category of $\boldsymbol{a_i}$ of number ***a*** to the following scheme: 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, where & - the operation of the arithmetic «And».

4. Button repeatedly substitution **$m + 1$** discharges of number ***a*** to the following scheme: $\boldsymbol{k = a_{m+1}}$ **,** $\boldsymbol{a_{m+1} = a_m}$, … , $\boldsymbol{a_2 = a_1}$ **,** $\boldsymbol{a_1 = k}$**.**

5. Using binary operations ^ **-** bitwise excluded «OR» - is the number of $\boldsymbol{c_{i,j} = a \wedge X}$**.**

6. Дешифрованим have the image after the 5th step.

The results are shown in Fig.1 - 3 at $\boldsymbol{P = 53, Q = 83}$.

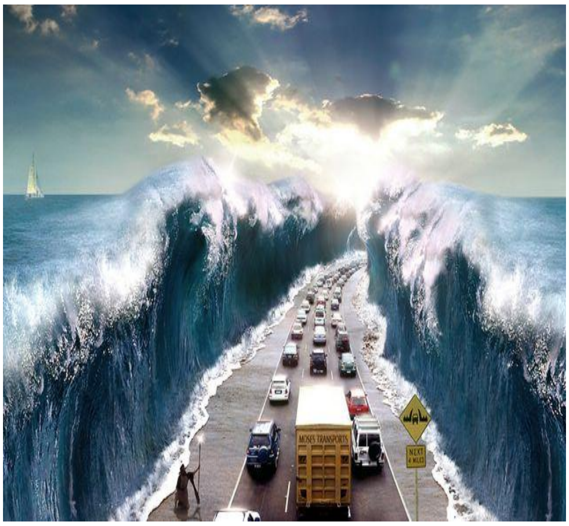

Fig.1. Original image

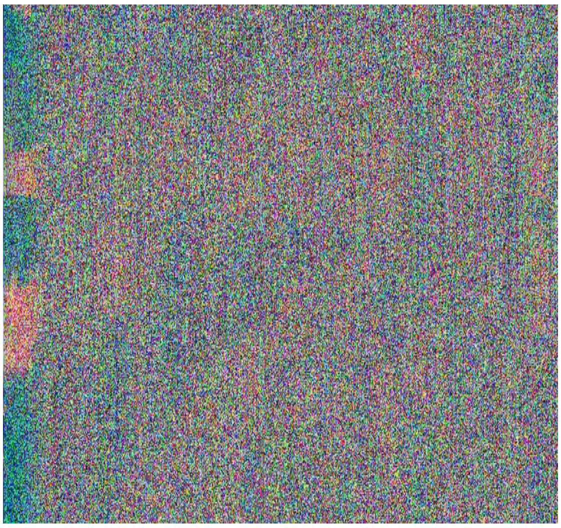

Fig.2. The encrypted image

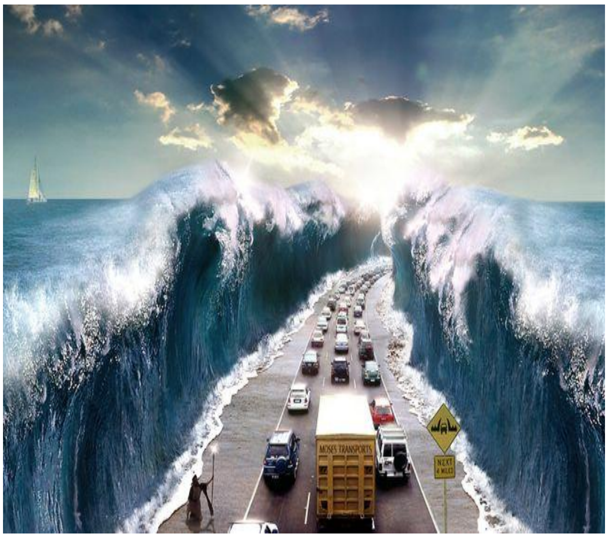

Fig.3. Decrypted image

The results are shown in Рис.4 – 6 at **P = 127,Q = 53.**

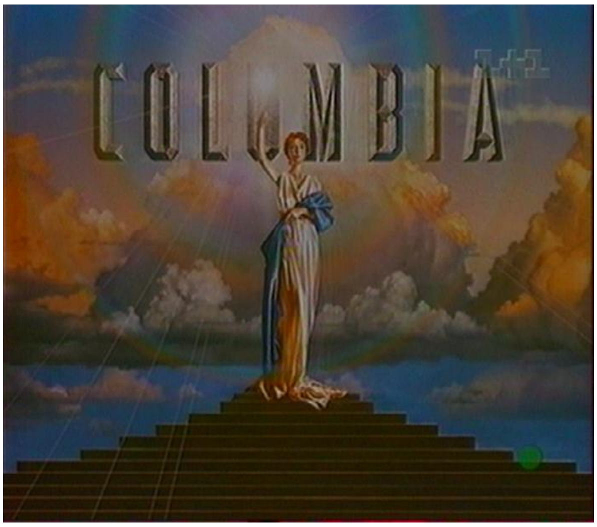

Рис.4. Original image

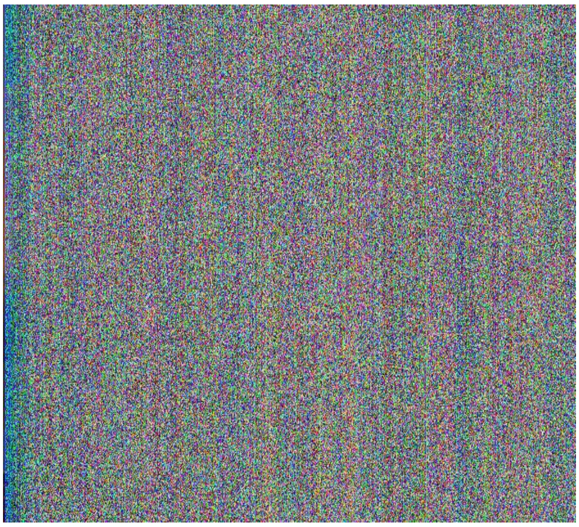

Рис.5. The encrypted image

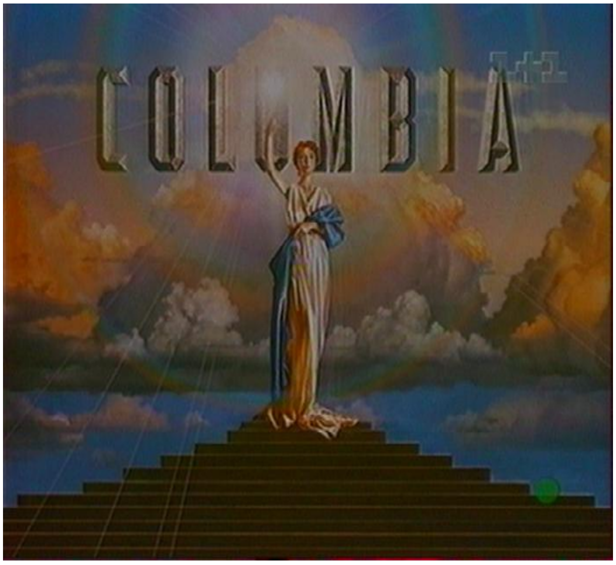

Рис.6. Decrypted image

From the comparison of figure 2 and Figure 5 shows that encryption for different values of the primes ***P*** and ***Q***, are not materially different. Contours in both encrypted images are missing. Initial and decrypted only image is a slightly different intensity levels

Conclusions

1. Proposed modification encryption is designed to encrypt images, and are based on the ideas underlying algorithm RSA. 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.
2. 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
3. Resistance to unauthorized decryption proposed modification of stream is provided by the RSA algorithm.

1. Павлидис Т. Алгоритмы машиной графики и обработки изображений. – М.: Радио и связь, 1986.-399с. 2. Б.Яне. Цифровая обработка изображений. – Москва, Техносфера , 2007.- 583с.
3. Брюс Шнайер. Прикладная криптография. – М.: Триумф, 2003. – 815с. 4. 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. 5. Y.Rashkevych, A.Kovalchuk, D.Peleshko, M.Kupchak. Stream Modification of RSA Algorithm For Image Coding with precize contour extraction. Proceedings of the X-th International Conference CADSM 2009. 24-28 February 2009, Lviv-Polyana, Ukraine, Pp. 469-473