BIT OPERATIONS WITH ELEMENTS OF THE RSA ALGORITHM IN ENCRYPTION-DECRYPTION OF COLOR IMAGES

***Anatoliy Kovalchuk**, Senior Lecturer, **Yuriy Peleckh**, Ph.D., As.-Prof., **Tetiana Bubela**, Dr. Sc., Prof.*
Lviv Polytechnic National University, Ukraine,
e-mail: anatolii.m.kovalchuk@lpnu.ua

Abstract. An image as a stochastic signal is one of the most common forms of information. Protecting images from unauthorized access and applying is a correspondingly urgent task. This causes the use of well-known classical encryption methods in the case of image encryption. But the image is a signal that possesses, in addition to typical informativeness, also visual informativeness.

Informativeness for modern image processing methods makes it possible to ensure unauthorized access. Creating an attack on an encrypted image is possible in two ways: by traditional hacking of encryption methods, or by classical methods of visual image processing (filtering, highlighting contours, etc.). In this regard, one more requirement is put forward to encryption methods in the case of their application concerning images - this is the complete noise of the encrypted image. This is necessary so that the use of visual image processing methods becomes impossible.

The RSA algorithm is one of the most widely known industrial standards for encrypting signals. Unlike symmetric encryption, in an open-key encryption scheme, it is impossible to calculate the decryption procedure, knowing the encryption procedure. Namely, the working time of the algorithm for calculating the decryption procedure is so great that it cannot be implemented on any modern computers, as well as on computers of the future. Such coding schemes are called asymmetric.

Therefore, the urgent task is to implement the application of the RSA algorithm so that when encrypting an image:

– the cryptographic stability of the RSA algorithm has not become worse;

– the full image noise was achieved to prevent the use of visual image processing techniques.

The algorithm of elements of the RSA algorithm, as the most resistant to unauthorized decryption of signals, and bitwise operations for a compatible combination during encryption and decryption of images is proposed by the authors. Encryption - decryption is performed without additional noise. The proposed algorithm is applied to images in which there are strictly extracted contours. Elements of the RSA algorithm are assigned to perform bitwise operations on the intensity values of pixels of a color image.

The developed algorithm has higher cryptographic stability compared to the traditional RSA algorithm. The authors described the possibilities of using elements of the RSA algorithm in bitwise transformations when encrypting and decrypting images.

The results of encryption simulation for cryptographic transformations of color images of a given dimension are presented. Modified models and algorithmic procedures of key formation processes of direct and inverse cryptographic transformations have been developed. They are reduced to elemental mathematical operations.

Key words: Encryption, Color image, Bitwise operations, Contour, Pixel intensity, Decryption, Matrix of pixel intensities.

1. Introduction

The need to solve the theoretical and practical tasks of information security and achieve the necessary level of protection of information of various contents became the reason for the corresponding accelerated development of cryptography in the era of information technologies and mass communications.

An image can be defined as a two-dimensional function F(x, y), where x and y are coordinates in space (specifically, on a plane). If the values x, y, and F(x, y) take a finite number of discrete values, then we speak of a digital image. Digital image processing is the processing of digital images using computers. A digital image consists of a finite number of elements, each of which is located in a specific place and acquires a certain value. These elements are called picture elements or pixels.

Mathematically, a digital image is displayed by a matrix of pixel intensities of dimension n × m, where n is the number of rows of the image matrix m is the number of columns.

The security of the RSA algorithm is based on the resource-intensive factorization of large natural numbers. Using the RSA algorithm, as the most resistant to unauthorized decryption of images with clearly defined contours, does not always give satisfactory results. This means that it is possible to distinguish the main contours of the input image on the encrypted image - that is, the effect of incomplete noise occurs [1-2].

Extracting the contour means finding the maxima of the modulus of the gradient vector [2, 3]. This is one of the reasons why contours remain in the image when encrypting in the RSA system since RSA encryption is based on exponentiation modulo some natural number.

The presence of contours in the image is an important characteristic of the image. The task of extracting a contour requires the application of operations on neighboring elements that are sensitive to changes and suppress the values of brightness levels, that is, contours are those areas where changes occur. Some parts of the image become bright, while other parts of the image remain dark [4-5].

At the same time, on the contour and pixels adjacent to the contour, raising the brightness values to the power gives an even greater gap [6-7, 10-15].

Concerning the image, there are certain problems with its encryption, namely, contours on sharply fluctuating images are partially preserved [16-20].

In the future, we will use the following definition of an affine transformation of Euclidean space in Cartesian coordinates: a transformation of Euclidean space is called affine if this transformation maps every plane to a plane.

2. Disadvantages

Numerical experiments [8, 9] established that there are values of prime numbers at which significant deviations of pixel intensities may occur in the area of contours in the image during encryption. This makes it impossible to blur these contours at these values of the selected primes.

3. Aim of the work

Concerning the image, the aim is to use the classic RSA algorithm in such a way that:

the cryptographic stability of the RSA algorithm was not reduced;

to prevent the application of visual image processing methods, complete image noise was ensured [6].

The combination of the RSA algorithm elements and bitwise operations in the software implementation is one of the ways to create such a modification.

4. Encryption method

Elements of the RSA algorithm are prime numbers P and Q and numbers e and d, which are obtained from the congruence $ed \equiv 1 \pmod{\varphi(N)}$, $N = P * Q$, where $\varphi(N)$ is the Euler function.

Let the image S of width l and height h be given. We will assume that the color matrix (matrix of pixel intensities) is matched to the image [4, 6, 7]

$$S = \begin{pmatrix} s_{1,1} & \dots & s_{1,l} \\ \dots & \dots & \dots \\ s_{h,1} & \dots & s_{h,l} \end{pmatrix}, \qquad (1)$$

here s_{ij} is a pixel intensity value. The task of extracting a contour requires operations on neighboring elements that are sensitive to changes and fade out areas of constant brightness levels, that is, contours are those areas where changes occur. They become light, while other parts of the image remain dark. Therefore, contour extraction means searching for the most drastic changes, i.e. the maxima of the modulus of the gradient vector [3]. This is one of the reasons why contours remain in the image when encrypting in the RSA system since the encryption here is based on exponentiation modulo some natural number. At the same time, on the contour and the pixels adjacent to the contour, raising the luminance value to the power gives an even greater gap.

Description of encryption algorithms.

Encryption along two lines of the image matrix.

Let P and Q be a pair of arbitrary prime numbers and $N = PQ$, $\varphi(N) = (P - 1)(Q - 1)$. Encryption takes place element by element using the following transformation of elements of the matrix S of pixel intensities:

1. According to the RSA algorithm, the numbers $e < \varphi(N)$, $d < \varphi(N)$ are chosen such that, which satisfies the congruence $ed \equiv 1 (mod\ \varphi(N))$.
2. For i *th* row of the matrix, $1 \le i \le l$, the number $m \equiv (i + P)$ (mod 32) is selected, and the numbers $A \equiv m^e \pmod N$, $X = i*A*P$, are constructed.
3. For the $i + 1$ th row of the matrix, $1 \le i \le l$, the number $n \equiv (i + Q)$ (mod 32) is selected, and the numbers $B \equiv nd\ (mod\ N)$, $Y = i*B*Q$, are constructed.
4. The numbers $a = s_{i,j} \wedge X$ and $b = s_{i+1,j} \wedge Y$ are constructed using the binary operation ^ - bitwise excluded "OR".
5. Each digit a_i of the number a is distinguished according to the following scheme:

$$a_1 = a \,\&\, 01;\ a_2 = a \,\&\, 02;\ a_3 = a \,\&\, 04;\ a_4 = a \,\&\, 010;$$
$$a_5 = a \,\&\, 020;\quad a_6 = a \,\&\, 040;$$
$$a_7 = a \,\&\, 0100;\quad a_8 = a \,\&\, 0200;\ a_9 = a \,\&\, 0400;$$
$$a_{10} = a \,\&\, 01000;\ a_{11} = a \,\&\, 02000;$$
$$a_{12} = a \,\&\, 04000;\ a_{13} = a \,\&\, 010000;\ a_{14} = a \,\&\, 020000;$$
$$a_{15} = a \,\&\, 040000;\ a_{16} = a \,\&\, 0100000;$$
$$a_{17} = a \,\&\, 0200000;\ a_{18} = a \,\&\, 0400000;$$
$$a_{19} = a \,\&\, 01000000;\ a_{20} = a \,\&\, 02000000;$$
$$a_{21} = a \,\&\, 04000000;\ a_{22} = a \,\&\, 010000000;$$
$$a_{23} = a \,\&\, 020000000;\ a_{24} = a \,\&\, 040000000;$$
$$a_{25} = a \,\&\, 0100000000;\ a_{26} = a \,\&\, 0200000000;$$
$$a_{27} = a \,\&\, 0400000000;\ a_{28} = a \,\&\, 01000000000;$$
$$a_{29} = a \,\&\, 02000000000;\ a_{30} = a \,\&\, 04000000000;$$
$$a_{31} = a \,\&\, 010000000000;$$
$$a_{32} = a \,\&\, 020000000000,$$

here & is arithmetic AND operation.

6. Cyclic substitution of $m + 1$ digits of the number a is performed according to the scheme:

$$k = a_{m+1}, \qquad a_{m+1} = a_m, \dots, a_2 = a_1, a_1 = k.$$

7. Each digit b_i of the number b is distinguished according to the following scheme:

$$b_1 = b \,\&\, 01;\ b_2 = b \,\&\, 02;\ b_3 = b \,\&\, 04;$$
$$b_4 = b \,\&\, 010;\ b_5 = b \,\&\, 020;\ b_6 = b \,\&\, 040;\ b_7 = b \,\&\, 0100;$$
$$b_8 = b \,\&\, 0200;\ b_9 = b \,\&\, 0400;\ b_{10} = b \,\&\, 01000;$$
$$b_{11} = b \,\&\, 02000;\ b_{12} = b \,\&\, 04000;$$
$$b_{13} = b \,\&\, 010000;\ b_{14} = b \,\&\, 020000;\ b_{15} = b \,\&\, 040000;$$

$b_{16} = b$ & 0100000; $b_{17} = b$ & 0200000;
$b_{18} = b$ & 0400000; $b_{19} = b$ & 01000000;
$b_{20} = b$ & 02000000; $b_{21} = b$ & 04000000;
$b_{22} = b$ & 010000000; $b_{23} = b$ & 020000000;
$b_{24} = b$ & 040000000; $b_{25} = b$ & 0100000000;
$b_{26} = b$ & 0200000000; $b_{27} = b$ & 0400000000;
$b_{28} = b$ & 01000000000; $b_{29} =$ b & 02000000000;
$b_{30} = b$ & 04000000000;
$b_{31} = b$ & 010000000000; $b_{32} = b$ & 020000000000,
where & - arithmetic AND operation.

8. Cyclic substitution of $n + 1$ digits of the number b according to the scheme is performed:

$k = b_{n+1}$, $b_{n+1} = b_n$, … , $b_2 = b_1$, $b_1 = k$.

9. The image after steps 5 – 8 is encrypted.

10. All obtained numbers are recorded in a matrix, which is a matrix of pixel intensities of the encrypted image:

$$\boldsymbol{V} = \begin{pmatrix} v_{1,1} & \cdots & v_{1,l} \\ \cdots & \cdots & \cdots \\ v_{h,1} & \cdots & v_{h,l} \end{pmatrix}. \qquad (2)$$

The description along two lines of the image matrix.

Decryption is carried out at given numbers $e < \varphi(N)$ i d, $N = P*Q$, $\varphi(N) = (P - 1)(Q - 1)$.

1. For i *th* row of the matrix V, $1 \le i \le l$, the number $m \equiv (i + P) \pmod{32}$ is selected, and the numbers

$A \equiv m^e \pmod{N}$, $X = i*A*P$ are constructed.

2. For the $i +1$ th row of the matrix, $1 \le i \le l$, the number $m \equiv (i + Q) \pmod{32}$ is selected, and the numbers

$B \equiv m^d \pmod{N}$, $Y = i*B*Q$ are constructed.

3. Each digit a_i of the number a is distinguished 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 & is arithmetic AND operation.

4. Cyclic substitution of m + 1 digits of the number a is performed according to the scheme:

$k = a_{m+1}$, $a_{m+1} = a_m$, … , $a_2 = a_1$, $a_1 = k$.

5. The numbers $\boldsymbol{s_{i,j}} = \boldsymbol{a} \wedge \boldsymbol{X}$ are constructed using the binary operation ^ - bitwise excluded "OR".

6. Each digit $\boldsymbol{b_i}$ of the number $\boldsymbol{b}$ is distinguished according to the following scheme:

$b_1 = b$ & 01; $b_2 = b$ & 02; $b_3 = b$ & 04; $b_4 = b$ & 010;
$b_5 = b$ & 020; $b_6 = b$ & 040; $b_7 = b$ & 0100;
$b_8 = b$ & 0200; $b_9 = b$ & 0400; $b_{10} = b$ & 01000;
$b_{11} = b$ & 02000; $b_{12} = b$ & 04000;
$b_{13} = b$ & 010000; $b_{14} = b$ & 020000; $b_{15} = b$ & 040000;
$b_{16} = b$ & 0100000; $b_{17} = b$ & 0200000;
$b_{18} = b$ & 0400000; $b_{19} = b$ & 01000000; $b_{20} = b$ & 02000000; $b_{21} = b$ & 04000000;
$b_{22} = b$ & 010000000; $b_{23} = b$ & 020000000;
$b_{24} = b$ & 040000000; $b_{25} = b$ & 0100000000;
$b_{26} = b$ & 0200000000; $b_{27} = b$ & 0400000000;
$b_{28} = b$ & 01000000000; $b_{29} =$ b & 02000000000;
$b_{30} = b$ & 04000000000; $b_{31} = b$ & 010000000000;
$b_{32} = b$ & 020000000000,
where & - arithmetic AND operation.

7. Cyclic substitution of $m + 1$ digits of the number $\boldsymbol{b}$ according to the scheme is performed:

$k = b_{m+1}$, $b_{m+1} = b_m$, … , $b_2 = b_1$, $b_1 = k$.

8. The number $s_{i+1,j} = b \wedge Y$ is constructed using the binary operation ^ - bitwise excluded «OR»**.**

9. The image after steps 5 – 8 is encrypted.

The results are shown in Fig. 1. – 3 at $P = 53$, $Q = 83$.

Encryption along one line of the image matrix.

Let P and Q be a pair of arbitrary prime numbers and $N = P*Q$, $\varphi(N) = (P - 1)(Q - 1)$. Encryption takes place element by element using the following transformation of elements of the matrix S of pixel intensities:

1. A natural number $e < \varphi(N)$ is randomly selected and a natural number d is found such that the congruence $ed \equiv 1(mod\ \varphi(N))$ holds.

2. If $i \equiv 0 \pmod{2}$, $1 \le i \le l$, then a number $m \equiv (i + P) \pmod{31}+1$ is randomly selected and numbers $B \equiv m^e \pmod{N}$, $X = i*B*P$ are constructed.

3. If $i \equiv 1 \pmod{2}$, $1 \le i \le l$, then a number $m \equiv (i + Q) \pmod{31}+1$ is randomly selected and numbers $B \equiv m^d \pmod{N}$, $X = i*B*Q$ are constructed.

4. The number $\boldsymbol{a} = \boldsymbol{s_{i,j}} \wedge \boldsymbol{X}$ is constructed using the binary operation ^ - bitwise excluded «OR»**.**

5. Each digit $\boldsymbol{a_i}$ of the number $\boldsymbol{a}$ is distinguished 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;

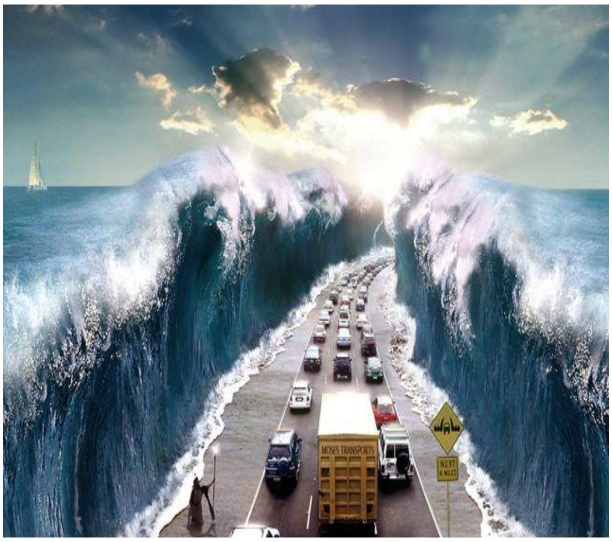

Fig. 1. Original image

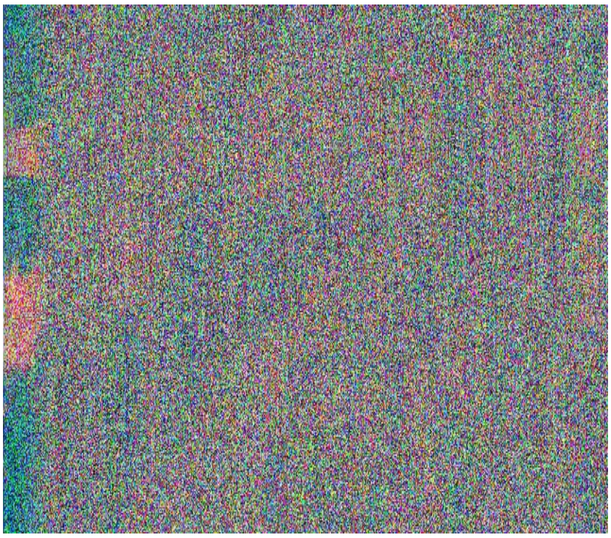

Fig. 2. Encrypted image

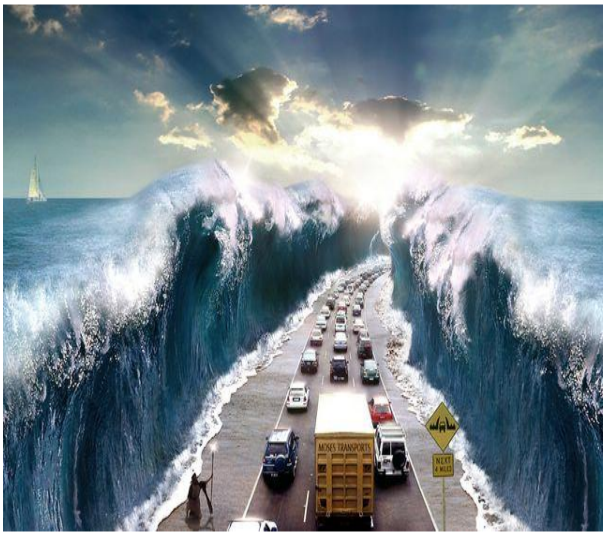

Fig. 3. Decrypted image

$a_{23} = a \,\&\, 020000000;\;\; a_{24} = a \,\&\, 040000000;$
$a_{25} = a \,\&\, 0100000000;\;\; a_{26} = a \,\&\, 0200000000;$
$a_{27} = a \,\&\, 0400000000;\;\; a_{28} = a \,\&\, 01000000000;$
$a_{29} = a \,\&\, 02000000000;\; a_{30} = a \,\&\, 04000000000;$
$a_{31} = a \,\&\, 010000000000;$
$a_{32} = a \,\&\, 020000000000,$

where & is arithmetic AND operation.

6. Cyclic substitution of $m + 1$ digits of the number $\boldsymbol{a}$ according to the scheme is performed:

$k = a_{m+1}\,,\quad a_{m+1} = a_m\,,\;\dots\,,\; a_2 = a_1\,,\; a_1 = k.$

7. The image after step 5 is encrypted.

8. All obtained numbers are recorded in a matrix, which is a matrix of pixel intensities of the encrypted image:

$$\boldsymbol{V} = \begin{pmatrix} b_{1,1} & \dots & b_{1,l} \\ \dots & \dots & \dots \\ b_{h,1} & \dots & b_{h,l} \end{pmatrix}. \tag{3}$$

Decryption along one line of the image matrix.

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

1.If $\boldsymbol{i} \equiv 0 \pmod 2$, $1 \le i \le l$, then a number $m \equiv B^{\mathrm{d}} \pmod N$ and a number $X = i{*}B{*}P$ are constructed.

2.If $i \equiv 1 \pmod 2$, $1 \le i \le l$, then a number $m \equiv B^{\mathrm{e}} \pmod N$ and a number $X = i{*}B{*}Q$ are constructed.

3.Each digit a_{i} of the number a is distinguished according to the following scheme:

$\boldsymbol{a}_1 = \mathrm{a} \,\&\, 01;\; \boldsymbol{a}_2 = \boldsymbol{a} \,\&\, 02;\; \boldsymbol{a}_3 = \boldsymbol{a} \,\&\, 04;\;\; \boldsymbol{a}_4 = \boldsymbol{a} \,\&\, 010;$
$\boldsymbol{a}_5 = \boldsymbol{a} \,\&\, 020;\;\; \boldsymbol{a}_6 = \boldsymbol{a} \,\&\, 040;$
$\boldsymbol{a}_7 = \boldsymbol{a} \,\&\, 0100;\;\; \boldsymbol{a}_8 = \boldsymbol{a} \,\&\, 0200;\; \boldsymbol{a}_9 = \boldsymbol{a} \,\&\, 0400;$
$\boldsymbol{a}_{10} = \boldsymbol{a} \,\&\, 01000;\; \boldsymbol{a}_{11} = \boldsymbol{a} \,\&\, 02000;$
$\boldsymbol{a}_{12} = \boldsymbol{a} \,\&\, 04000;\; \boldsymbol{a}_{13} = \boldsymbol{a} \,\&\, 010000;\; \boldsymbol{a}_{14} = \boldsymbol{a} \,\&\, 020000;$
$\boldsymbol{a}_{15} = \boldsymbol{a} \,\&\, 040000;\;\; \boldsymbol{a}_{16} = \boldsymbol{a} \,\&\, 0100000;$
$\boldsymbol{a}_{17} = \boldsymbol{a} \,\&\, 0200000;\;\; \boldsymbol{a}_{18} = \boldsymbol{a} \,\&\, 0400000;$
$\boldsymbol{a}_{19} = \boldsymbol{a} \,\&\, 01000000;\;\; \boldsymbol{a}_{20} = \boldsymbol{a} \,\&\, 02000000;$
$\boldsymbol{a}_{21} = \boldsymbol{a} \,\&\, 04000000;\; \boldsymbol{a}_{22} = \boldsymbol{a} \,\&\, 010000000;$
$\boldsymbol{a}_{23} = \boldsymbol{a} \,\&\, 020000000;\;\; \boldsymbol{a}_{24} = \boldsymbol{a} \,\&\, 040000000;$
$\boldsymbol{a}_{25} = \mathrm{a} \,\&\, 0100000000;\;\; \boldsymbol{a}_{26} = \boldsymbol{a} \,\&\, 0200000000;$
$\boldsymbol{a}_{27} = \boldsymbol{a} \,\&\, 0400000000;\;\; \boldsymbol{a}_{28} = \boldsymbol{a} \,\&\, 01000000000;$
$\boldsymbol{a}_{29} = \boldsymbol{a} \,\&\, 02000000000;\; \boldsymbol{a}_{30} = \boldsymbol{a} \,\&\, 04000000000;$
$\boldsymbol{a}_{31} = \boldsymbol{a} \,\&\, 010000000000;$
$\boldsymbol{a}_{32} = \boldsymbol{a} \,\&\, 020000000000,$

where & - arithmetic AND operation.

8. Cyclic substitution of $m + 1$ digits of the number $\boldsymbol{a}$ according to the scheme is performed:

$k = a_{m+1}\,,\; a_{m+1} = a_m\,,\;\dots\,,\; a_2 = a_1\,,\; a_1 = k.$

4. The number $\boldsymbol{s}_{\mathbf{i,j}} = \boldsymbol{a} \wedge \boldsymbol{X}$ is constructed using the binary operation ^ – bitwise excluded «OR»**.**

5. The image after step 5 is decrypted.

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

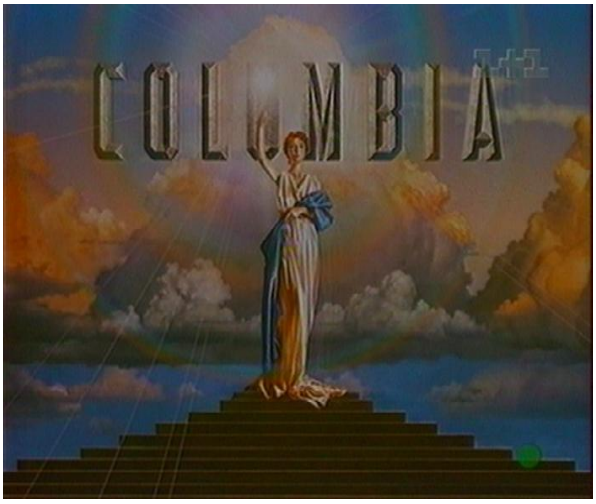

Fig. 4. Original image

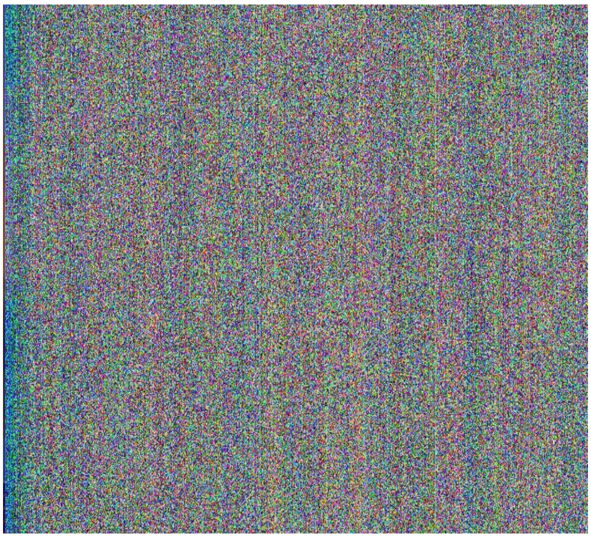

Fig. 5. Encrypted image

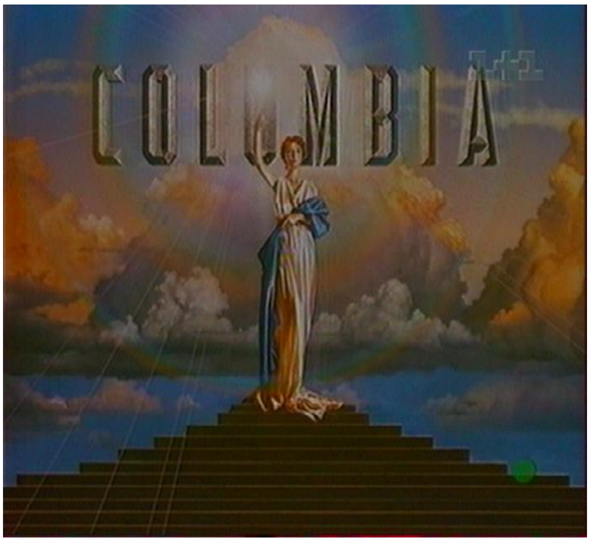

Fig. 6. Decrypted image

5. Conclusion

The conclusion can be made by visually comparing the encrypted images, namely: the images differ slightly for different values of the prime numbers P and Q during encryption of the matrix of pixel intensities. There are no contours in both encrypted images. The proposed modifications apply to any type of image, but the greatest benefits are achieved with clearly defined image contours. The described algorithm can be used if it is necessary to transfer encrypted graphic images.

It can be seen visually that the original and decrypted images are slightly different, which indicates that the application of the proposed algorithm does not deteriorate the quality of the image. But in the presence of established requirements for quality criteria, a certain number of attempts to select such prime numbers P and Q and numbers e and d in the congruence $ed \equiv 1 \ (mod\ \varphi(N))$, $N = P*Q$ is usually necessary to achieve the specified achievement criteria the quality of the input and decoded image.

Numerical experiments with different color images showed that the proposed modification has the advantage of increasing the cryptographic stability of the RSA algorithm.

6. Gratitude

The authors express their gratitude to the Staff of the Department of Publishing Information Technologies and Department of Information and Measuring Technologies of Lviv Polytechnic National University.

7. Conflict of interest

The authors state that there are no financial or other potential conflicts regarding this work.

References

[1] Michael Vollmer, Klaus-Peter Mollmann, *Fundamentals of Infrared Thermal Imaging*. Infrared Thermal Imaging, 10.1002 9783527693306, 2017. https://www.wiley.com/enus/Infrared+Thermal+Imaging:+Fundamentals,+Research+and+Applications,+2nd+Edition-p-9783527413515

[2] B. Usmonov, O. Evsutin, A. Iskhakov, A. Shelupanov, A. Iskhakova, R. Meshcheryakov, "The cybersecurity in development of IoT embedded technologies", in *Proc. International Conference on Information Science and Communications Technologies (ICISCT) IEEE*, 2017, pp. 1-4. DOI: 10.1109/ICISCT.2017.8188589

[3] D. Wagh, H. Fadewar, & G. Shinde, "Biometric Finger Vein Recognition Methods for Authentication", Computing in Engineering and Technology, pp. 45-53, 2020. DOI: 10.1007/978-981-32-9515-5-5

[4] P. Chanukya, T. Thivakaran, "Multimodal biometric cryptosystem for human authentication using fingerprint and

ear", Multimedia Tools and Applications, 79(1-2), pp. 659-673, 2020. DOI: 10.1007/s11042-019-08123-w

[5] L.Valechha, H. Valecha, V. Ahuja, T. Chawla, & S. Sengupta, "Orisyncrasy - An Ear Biometrics on the Fly Using Gabor Filter", In Advances in Data Sciences, Security and Applications, pp. 457-466, 2020. DOI: 10.1007/978-981-15-0372-6-37

[6] J. Yang, L. Liu, T. Jiang, Y. Fan, "A modified Gabor filter design method for fingerprint image enhancement", Pattern Recognition Letters, 24(12), pp. 1805-1817, 2003. DOI: 10.1016/S0167-8655(03)00005-9.

[7] Majid Rabbani, Rajan Joshi. "An overview of the JPEG2000 still image compression standard", Eastman Kodak Company, Rochester, NY 14650, USA, Signal Processing: Image Communication, no. 17, vol. 1, pp. 3–48, 2002. https://scirp.org/reference/referencespapers.aspx?referenceid=727652

[8] 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, vol. 2533, 2019, pp. 139-150. https://doi.org/10.23939/istcmtm2020.04.025

[9] A. Kovalchuk, I. Izonin, Gregush Ml, M., N. Lotoshyiiska, "*An approach towards image encryption and decryption using quaternary fractional-linear operations*", Procedia Computer Science, vol. 160, 2019, pp. 491-496. Conference Paper (Open Access), DOI : 10.1016 /j.procs. 2019.11.059

[10] S. X. Liao and M. Pawlak, "On image analysis by moments", IEEE Transaction on Pattern Analysis and Machine Intelligence, 18, no. 3, pp. 254–266. https://ieeexplore.ieee.org/document/485554

[11] [E. M. Haacke, R.W. Brown, M.R. Thompson and R. Venkatesan, *Magnetic Resonance Imagin: Physical Principles and Sequence Design.* John Wiley & Sons, New York, 1999. https://www.wiley.com/ensg/Magnetic+Resonance+Imaging:+Physical+Principles+and+Sequence+Design,+2nd+Edition-p-9780471720850

[12] J. T. Kajiya, The rendering equation. *Computer Graphics,* vol. 20, is. 4, 143-150, 1986. https://dl.acm.org/doi/10.1145/15886.15902

[13] [M. Sarfraz. *Introductory Chapter: On Digital Image Processing,* 2020. DOI: 10.5772 intechopen.92060, https://www.intechopen.com/chapters/71817

[14] Ehsan Samei, Donald J Peck, Projection X□ray Imaging, Hendee's Physics of Medical Imaging, 10.1002 9781118671016, 217-242, 2019. https://onlinelibrary.wiley.com/doi/10.1002/9781118671016.ch6

[15] B. Schneier. *Applied Cryptography: Protocols, Algorithms and Source Code in C***,** Triumf, 2003. https://www.amazon.com/Applied-Cryptography-Protocols-Algorithms-Source/dp

[16] [B. Jane. *Digital Image Processing*. Springer–Verlag Berlin Heidelberg, 2005. https://www.amazon.com/Digital-Image-Processing-Algorithms-Applications/dp/3540592989

[17] R. C. Gonzales and R.E. Woods, *Digital image processing,* Prentice Hall, Upper Saddle River. 2002. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://sdeuoc.ac.in/sites/default/files/sde_videos/Digital%20Image%20Processing%203rd%20ed.%20-%20R.%20Gonzalez%2C%20R.%20Woods-ilovepdf-compressed.pdf

[18] I. Tsmots, O. Riznyk, V. Rabyk, Y. Kynash, N. Kustra, M. Logoid, Implementation of FPGA-Based Barker's-Like Codes. In: Lytvynenko V., Babichev S., Wójcik W., Vynokurova O., Vyshemyrskaya S., Radetskaya S. (eds) "*Lecture Notes in Computational Intelligence and Decision Making*", ISDMCI 2019, Advances in Intelligent Systems and Computing, vol. 1020. Springer, Cham, 2020. DOI: 10.1007/978-3-030-26474-1_15

[19] Rafael C. Gonzalez, Richard E. Woods, "*Digital Image Processing*", published by Pearson Education, Inc, Publishing as Prentice Hall. 2002. http://sdeuoc.ac.in /sites/default /files/sde_videos /Digital%20Image%20Processing%203rd%20ed.%20-%20R.%20Gonzalez%2C%20R.%20Woods-love pdf-compressed.pdf

[20] B. Girod, "*The information theoretical significance of spatial and temporal masking in video signals*", Proc. of the SPIE Symposium on Electronic Imaging, vol. 1077, 1989, pp.178–187. https://typeset.io/papers/the-information-theoretical-significance-of-spatial-and-2bas6i0mgw.