UDC 004.056.55:510.644.4 **doi: 10.32620/reks.2022.4.09**

Mykola KUSHNIR, Hryhorii KOSOVAN, Petro KROIALO

Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine

METHOD OF ENCRYPTING IMAGES BASED ON TWO MULTIDIMENSIONAL CHAOTIC SYSTEMS USING FUZZY LOGIC

The subject of the study: *it is proposed to develop a method of image encryption with pixel permutation implemented using fuzzy logic and Hainaut mapping, as well as diffusion, which is implemented using the Lorenz system. Study objectives: To propose an effective way to apply the rules of fuzzy logic in relation to the values generated by the Henon mapping to implement the permutation of pixels in the image, which will provide a random permutation and increase the efficiency of the encryption method. Also, to achieve better security in the process of image encryption, the use of the diffusion process implemented using the Lorenz system. In addition, to increase the sensitivity of the encryption method to change the initial value of the component colors of the pixels will also be used in the encryption process.* ***Investigation methods and research results:*** *developed and presented a method of image encryption with pixel permutation implemented using fuzzy logic and Henon mapping, as well as diffusion, implemented using the Lorenz system. The initial values for the Henon mapping and the Lorenz system will be determined from the entered keyword, and the control parameters are set by the operator, while the values of the component colors of the pixels will also participate in the encryption process. In addition, before the process of rearranging the pixels in the image, the rules of fuzzy logic are implemented by Henon mapping. Also, the values of the component pixels before and after the diffusion procedure will be reduced to a single interval. Thus, as a result of image encryption, the original image changes completely, loses its content and shape, and the color intensity distribution of pixels becomes uniform. The program implementation of the proposed encryption method was also carried out and the qualitative characteristics of the proposed image encryption method were evaluated, namely: analysis of histograms of original and encrypted images, correlation of adjacent image pixels, root mean square error (MSE), peak signal-to-noise ratio (PSNR), entropy before changing the color components of the pixels.* ***Conclusions:*** *the implementation of the method has shown that it has a large number of encryption keys, which makes brute force (the process of their selection) resource-intensive and complex, and the implementation of the encryption process in two stages and using two different chaotic systems significantly improves the security of the encrypted image. The resulting cryptosystem is also resistant to the following attacks: approximation of chaotic orbits, correlation, analytical and statistical attacks.*

Keywords: *cryptography; encryption; decryption; fuzzy logic; permutation; diffusion; image; chaos; security.*

Introduction

In today's world, most people use digital services. Through such services, people exchange all kinds of information and often such information is personal and therefore needs protection. This is the reason for the need to protect digital images and videos during their storage and transmission. Due to the rapid progress of telecommunication systems such as mobile and Internet networks, the protection of digital images / videos is becoming more and more important [1-3].

Image encryption is an important part of information security. Due to high redundancy, high data capacity, low entropy and high correlation between pixels in image files, traditional algorithms such as International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are not fully suitable for encryption of images. Moreover, these algorithms require quite a lot of computation time and energy in the process of performing encryption. Chaos-based encryption methods demonstrate better performance and security compared to these methods [4, 5].

The work is devoted to the development of a new method of image encryption in two stages, namely permutation, implemented on the basis of fuzzy logic and Henon mapping, and diffusion - based on three-dimensional chaotic Lorenz system, increase encryption stability, and evaluate the effectiveness of the proposed image encryption method.

1. Motivation for research

Chaotic systems are nonlinear and deterministic [4]. Due to their characteristics, such as random behavior, ergodicity, sensitivity to initial conditions and control parameters generated by chaotic sequence systems, they are often pseudo-random and their structures are very complex to analyze and predict. Thus, chaotic systems can improve the security of encrypted images. Permutation and diffusion are fundamental techniques of image en-

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

cryption implemented by chaotic systems. At the permutation stage, the pixel positions of the original image change, while the pixel values remain unchanged, and therefore the histograms of the encrypted and original images are the same. In addition, permutation-only encryption methods are not sufficiently stable for statistical analysis. At the diffusion stage, the pixel values of the original image change. Most diffusion methods implement encryption by directly superimposing a chaotic sequence on the pixel intensity of the image. Compared to permutation, diffusion can provide a higher level of security, but the encryption effect is not sufficient, which is why it is necessary to use both encryption techniques [6, 7].

2. Work related analysis

Chaos-based cryptography always implements one of the stages of chaos encryption. In order to achieve the greatest resistance to cryptographic attacks, it is necessary to perform substitution-permutation, which are widely used in both conventional block ciphers and chaotic. As a rule, the substitution-permutation structure realized in chaotic ciphers by means of a combination of confusion and diffusion processes [7, 8].

For most crypto-encrypted cryptosystems, a chaotic system used to generate pseudo-random values that are used for permutation and diffusion. First, the permutation rule can be static in the form of a table or dynamic by induction from chaotic values. Second, the substitution is usually realized by combining chaotic values and values of the component colors of pixels [9].

Most successful attacks on chaotic ciphers are based on weaknesses in the algorithms of permutation and diffusion processes, and are described in the literature [6, 7]. In addition, the works [10, 11] indicate the criteria and evaluation of chaotic encryption methods. From a cryptographic point of view, the more complex the dynamics of chaos, the stronger the chaos-based cryptosystem will be. Many cryptosystems have recently been proposed using more complex chaotic systems, namely hyper chaotic systems, delayed systems, fractional order, and spatio-temporal chaotic systems [12].

A chaos-based cryptosystem becomes much stronger if its encryption keys depend on the content of the image. The use of image content in chaotic dynamics is created by external perturbations. There are two ways to associate image content with encryption keys. The first is that the connection between the image content and the encryption keys is established by means of state perturbation [13]. The second is a selection mechanism in which the content of the image is used to select one of the chaotic sequences to generate key streams [14]. The initial values of the chaotic system are fixed, and neither the state variables nor the control parameters of the chaotic system are violated during the generation of chaotic sequences.

Friedrich in [15] first introduced permutation-substitution or substitution-diffusion. In this proposed technique, the position of the pixels is first mixed to reduce the correlation between adjacent pixels. After that, the pixel values change alternately during diffusion.

Liu et al. [16] introduced an image encryption system based on an iterative chaotic 2D Sine map with an infinite collapse modulation map and a closed loop modulation connection. In this technique, chaotic shift transformation is used for both mixing and diffusion. In [17], Hamza and Tituna proposed a technique for encrypting images based on the process of confusion-diffusion using the chaotic sequence of Zaslavsky. Zaslavsky's sequence is used to obtain pseudo-random numbers, based on which the encryption key was obtained.

Ping et al. [18] developed a method of image encryption based on confusion and diffusion using Henon mapping. In [19], Mishra and Saharan proposed a method of encrypting images based on the Henon map and a 128-bit private key, in which the permutation is performed using a permutation matrix created by the Henon mapping.

In [20], the authors have proposed a new technique of image encryption using a chaotic system with cyclic shift at the bit level, which was implemented using Henon mapping. The proposed method has less computational complexity and shows promising results in terms of various security tests.

Fuzzy logic is also often used in cryptography, and the main problem in its application is the formulation of the rules of its application. In the literature [21], a method of image encryption based on fuzzy logic for the transmission of confidential data has been proposed. The method focuses on the secret separation of the key using fuzzy logic, i.e. values are generated on the basis of which it is decided which part of the key to use for further encryption of the image.

In [22], a new method is proposed with automatic image encryption as an alternative to manual selective encryption of color images. Fuzzy logic rules for pixel color information are used to select the encryption area.

3. Purpose and objectives of the study

It should be noted that not all methods of encrypting information with the use of chaos can provide a sufficient level of security during transmission or storage. Over time, the stability of encryption methods may decline as new types of attacks emerge. That is why, there is a need to develop new methods with increased security.

The development of new methods requires the application of new approaches in their design. Therefore, we determine the purpose of this work as to develop a method of image encryption using the rules of fuzzy logic

in relation to the values generated by the chaotic Henon mapping and diffusion using the Lorenz system.

Also, the task of the study is to assess the effectiveness of the proposed method of encryption, i. e. statistical analysis, key space, information entropy, analysis of sensitivity and resistance against cryptographic attacks.

4. Description of the encryption and decryption algorithm

Image encryption is conversion the image data into a form that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back to its original form.

To easily recover the contents of an encrypted message, you need the correct decryption key [2, 5]. The key is an algorithm that cancels the encryption algorithm. Alternatively, a computer can be used for an attempt to crack the cipher.

4.1. Encryption algorithm

The encryption algorithm consists of two stages, namely permutation and diffusion. The Hénon mapping and the chaotic Lorenz system were chosen to implement the encryption method.

With the help of Hénon mapping and fuzzy logic, the permutation process is implemented. The Hénon mapping is a time-discrete dynamical system [4] that exhibits chaotic behavior. The equations describing the Hénon map are as follows:

$$\begin{aligned} x_{n+1} &= y_n + 1 - ax_n^2, \\ y_{n+1} &= bx_n^2. \end{aligned} \qquad (1)$$

The Hénon mapping takes a point (x_n , y_n) on a plane and maps it to a new point. The mapping depends on two parameters, a and b, which have values a = 1.4 and b = 0.3 for the canonical Hénon mapping, and at such values the mapping behavior becomes chaotic. For other values of a and b, the mapping may be chaotic, periodic, or convergent to a periodic orbit.

To implement the diffusion process, a dynamic chaotic Lorenz system was used, which includes three ordinary differential equations [4]:

$$\begin{aligned} \frac{dx}{dt} &= \sigma(y-x), \\ \frac{dy}{dt} &= Rx - y - xz, \\ \frac{dz}{dt} &= xy - \beta z, \end{aligned} \qquad (2)$$

where x, y and z – dynamic parameters of the system; σ, β and R - static parameters of the system, σ=10, R=28, and $b=\frac{8}{3}$. Solving this system sequentially, we obtain points that form the trajectory of the state of the Lorenz system in the phase space. Fig. 1 shows the change in the trajectory of the system between two variables x and z.

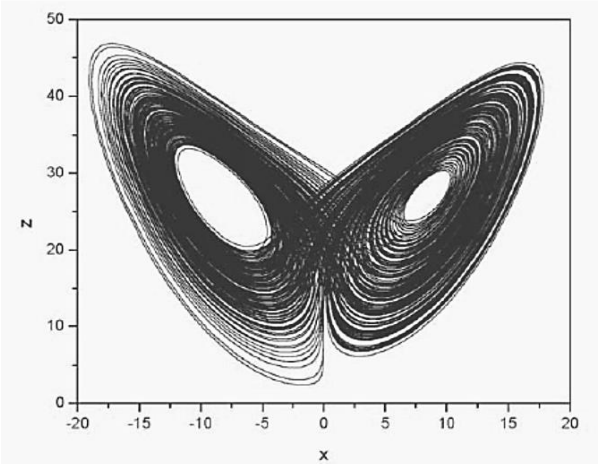


Fig. 1. Trajectory of the Lorenz system in phase space

The encryption algorithm proposed will consist of two stages, namely permutation and diffusion [12, 16, 18, 20, 29]. To implement the process of diffusion and permutation, it is necessary to create initial conditions for chaotic systems. To do this, the proposed method uses a foreign secret key 256 bits (K) of length, which is divided into blocks of 8 bits each and is called the permutation key. In general, the 256-bit key K is set as follows:

$$K = k_1, k_2, \ldots k_{32}. \qquad (3)$$

The initial conditions for both chaotic systems are determined as:

$$\begin{aligned} key(1) &= \mathrm{mod}\left(\frac{1}{256}\left(k_1 \text{Å} \ldots \text{Å} k_8 + \sum_{k=1}^{32}\frac{k_i}{32}\right)\right), \\ key(2) &= \mathrm{mod}\left(\frac{1}{256}\left(k_9 \text{Å} \ldots \text{Å} k_{16} + \sum_{k=1}^{32}\frac{k_i}{32}\right)\right), \\ key(3) &= \mathrm{mod}\left(\frac{1}{256}\left(k_{17} \text{Å} \ldots \text{Å} k_{24} + \sum_{k=1}^{32}\frac{k_i}{32}\right)\right), \\ key(4) &= \mathrm{mod}\left(\frac{1}{256}\left(k_{25} \text{Å} \ldots \text{Å} k_{32} + \sum_{k=1}^{32}\frac{k_i}{32}\right)\right), \\ key(5) &= \frac{\sum_{k=1}^{32} k_i}{k_1 \text{Å} \ldots \text{Å} k_{32}\left(256^2 \times 32\right)}, \end{aligned} \qquad (4)$$

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

where operation mod(x, y) returns the remainder of the division and the symbol $\oplus$ represents the bitwise operation excluding XOR. Obviously, equations (3) and (4) show that the initial conditions for both chaotic systems are very sensitive to changes even in the first bit of the secret key. As a result, the key space is 2^{256}, which makes it possible to resist any brute-force attack.

Two keys, key (1) and key (2), will be used as initial conditions for the Hénon mapping, while key (3), key (4) and key (5) – as those for the Lorenz system.

To implement permutation using fuzzy logic, it is necessary to form rules, according to which we will determine to what number of positions the shift of pixels to the right will occur. In general, the process of permutation of pixels occurs according to the following algorithm:

1. Since the image is a two-dimensional array of pixel coordinates, we first converted it into a one-dimensional dynamic array, sequentially writing the rows of the two-dimensional array one after the other from the first one to the last.

2. We create a dynamic one-dimensional array of the same size as the one-dimensional array of pixels of the original image.

3. We take the first pixel from the one-dimensional array of the original image, and using the Hénon mapping and the fuzzy logic rule we calculate the new position (coordinate) of the pixel in the one-dimensional dynamic array of the encrypted image and write its value there.

4. The shifted pixel is written into the one-dimensional array of the encrypted image and removed from the dynamic one-dimensional array. Thus, one-dimensional dynamic array is reduced by one element.

5. Then we take the second pixel from the one-dimensional array of the original image, substitute it into the Hénon map and define a new position for it. Then it is written to a new position in the one-dimensional dynamic array, while the one-dimensional array of encrypted image and one-dimensional dynamic array are reduced by another element. Thus, in a one-dimensional dynamic array, there will always be only free pixel coordinates, and its size will decrease after moving each pixel.

6. The process is repeated until all elements of the original image array are moved to the position in the new one-dimensional array of the encrypted image.

7. For permutation of the last pixel of the original image, there will be only one option for it to be moved, because only one coordinate will remain in the one-dimensional dynamic array – the only free space where it can be moved.

8. After shifting all the pixels from the one-dimensional array of the original image and creating the one-dimensional array of the encrypted image, the latter will be the Hénon transformation into a two-dimensional array of coordinates of the encrypted image.

Because you need to permutate both square and rectangular images, the rows and columns of the original and encrypted images must be the same.

Since the height of the image is the value of H, and the width – that of W and such an image is converted from a two-dimensional array into one-dimensional one, we used both Hénon mapping equations to convert it. The original values of both equations are added and the maximum value of the total range will be divided into equal intervals; then using the rules of fuzzy logic we will determine to which place of the one-dimensional dynamic array the pixel will move. In this case, the maximum value of the range will be divided by the size of the dynamic one-dimensional array and will gradually decrease during encryption, as the size of the array is reduced by one element each time the pixel is encrypted

$$W_1=W_2=W_3=W_4=W_5=W_6=W_7,$$
$$W=W_1+W_2+W_3+W_4+W_5+W_6+W_7.$$

The rules of fuzzy logic for permutation along the length of a one-dimensional array W are:

If the input value is in the range from 0 to 1, then the output value is in the range from 0 to W_1;

If the input value range is from 1.1 to 2, then the output value range is from W_1 to W_2;

If the input value range is from 2.1 to 3, then the output value range is from W_2 to W_3;

If the input value range is from 3.1 to 4, then the output value range is from W_3 to W_4;

If the input value range is from 4.1 to 5, then the output value range is from W_4 to W_5;

If the input value range is from 5.1 to 6, then the output value range is from W_5 to W_6;

If the input value range is from 6.1 to 7, then the output value range is from W_6 to W_7.

Pixel permutation may not always provide a high degree of protection for the encryption method, even with a sufficiently large key space [10, 23]. Therefore, it is necessary to introduce an additional stage of encryption, called diffusion. As a result of diffusion, the color gradation of the component pixels changes. Changing the gradation further increases the resistance of the encryption method to various types of attacks.

To implement the diffusion process, a three-dimensional Lorenz system (2) is used, and each component of the pixel will be encrypted using a separate component of the Lorenz system. For example, the red component

will be encrypted with a variable x, the green one – y and the blue one – z.

For encryption of each component, the Lorenz system is solved 1000 times at first, to avoid transients, and after the last solution, the encryption process will take place. Next, to encrypt each pixel, the Lorenz system is solved 10 times and the values of the component pixels, i.e. 256-level gradation of the pixel component color, converted to decimal value by equation (6), will be added to the generated value of the Lorenz system.

$$x_C = x_{min} + \delta x \left(\frac{C}{255} \right), \quad \delta x = x_{max} - x_{min}, \tag{5}$$

where C is the gradation of the color component of the pixel x_{min}, – the minimum initial value of the Lorenz system, reduced to a single interval, x_{max} – the maximum initial value of the Lorenz system and x_C – the converted gradation value of the color component to decimal, which will be the initial condition for the Lorenz system.

Therefore, the cipher of each component of a pixel is the sum of two values, and mathematically it will look like this:

$$C_R = x_{n+1} + x_C, \tag{6}$$

where C_R is the resulting encrypted pixel, x_{n+1} is the Lorenz system value obtained after 10 reiterative solutions, and x_C is the current unencrypted pixel value. If the obtained decimal value is greater than x_{max}, the value of δx is subtracted from it.

Since the Lorenz system is three-dimensional and each pixel is described by three components, equation (5) will be used three times to encrypt all three components.

After encryption, the obtained encrypted value of the component pixels in decimal form must be transformed back into color gradation using equation

$$C = \text{round}\left[\frac{(C_R - x_{min})255}{\delta x} \right]. \tag{7}$$

4.2. Decryption algorithm

The process of decrypting the image, as well as the process of encryption, is also performed in two stages, but in the opposite direction. First, the values of the pixel colors components are restored after the diffusion performed, and then the initial positions of the pixels in the image are restored.

Restoration of color gradation occurs in the same way as the encryption procedure: first the image obtained after the diffusion process is restored. To do this, we take the encrypted value of the penultimate pixel, solve the Lorenz system 10 times and subtract the encrypted value of each of the pixels in the encrypted image from the value obtained. If the obtained decimal value is smaller than x_{min}, the value of δx will be added to it.

To restore the pixels positions, the Hénon mapping is solved using the same initial conditions and control parameters. By means of fuzzy logic rules we determine the place of the pixel that is to be moved to the first position of the one-dimensional array, then we determine the position to be moved to the place of the second pixel, and the process continues until the original image is fully restored.

5. Practical implementation of the method and the results of encryption

The proposed encryption method was implemented in the Delphi 7 programming language. To demonstrate the work of the encryption methods, the colored image "Flowers" 300,300 pixels in size was used. The result of encryption is presented in Fig. 2.

a) b)

Fig. 2. The original image "Flowers" (a) and the encrypted image after both stages of pixel encryption (b)

6. Analysis of the security of the encryption method

A high-quality encryption method must resist all known attacks, such as known plaintext attacks, encrypted only text attacks, statistical attacks, differential attacks, and various brute-force attacks [13–15, 29]. To confirm the effectiveness of the proposed method of image encryption, we conducted a number of assessments of the level of protection, namely: statistical analysis (histograms), key space analysis, information entropy analysis, sensitivity analysis and avalanche effect.

One of the most important characteristics for evaluating the security of the image encryption method is the homogeneity of the histogram of encrypted images [24-26]. We evaluated the histograms of the original and

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

encrypted images after each encryption step. Accordingly, Fig. 3 presents a histogram of the original image, which has large rises and they are accompanied by declines. In Fig. 4, there are histograms of encrypted images after both stages of encryption, they are quite homogeneous and significantly different from the histogram of the original image. The obtained result indicates that it will be difficult to perform a statistical attack. Therefore, the statistical distribution does not provide any clues for the implementation of statistical analysis of the encrypted image.

Pixels in the original images have high correlation, so a secure encryption method should eliminate this correlation to improve the stability against statistical analysis [10, 27, 28]. Correlation between adjacent pixels is estimated in three directions, such as horizontal, vertical, or diagonal. The correlation coefficients of each pair of pixels in all directions are calculated in the same way and are as follows:

$$\begin{aligned} r_{xy} &= \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)D(y)}}, \\ E(x) &= \frac{1}{N}\sum_{i=1}^{N} x_i, \\ D(x) &= \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)^2, \\ \operatorname{cov}(x,y) &= \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right), \end{aligned} \quad (8)$$

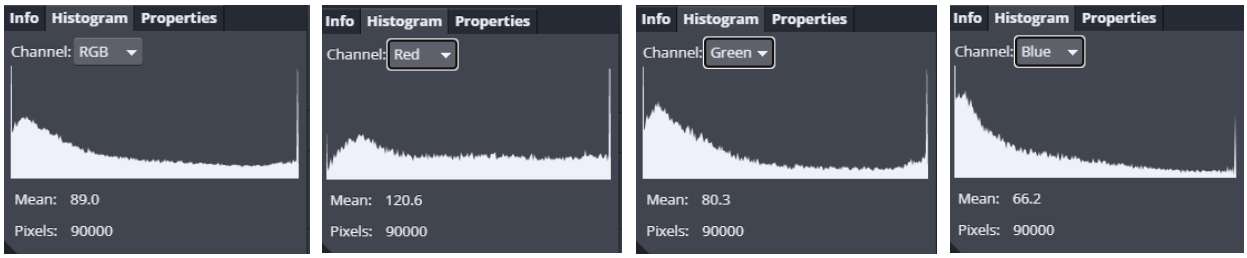
where x and y are the values of the gray scale for two adjacent pixels in the image. N is the total number of pixel pairs (x, y) obtained from the image. The correlation coefficients of the original and encrypted images are presented in Table 1 of the encrypted image shown in Fig. 2.

The correlation between different pairs of original / encrypted images was also analyzed by calculating two-dimensional correlation coefficients (CC) between original and encrypted images [10, 27, 28]. The following equation is used to calculate CC:

$$CC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(A_{ij} - \bar{A}\right)\left(B_{ij} - \bar{B}\right)}{\sqrt{\left(\sum_{i=1}^{M}\sum_{j=1}^{N}\left(A_{ij} - \bar{A}\right)^2\right)\left(\sum_{i=1}^{M}\sum_{j=1}^{N}\left(B_{ij} - \bar{B}\right)^2\right)}}. \quad (9)$$

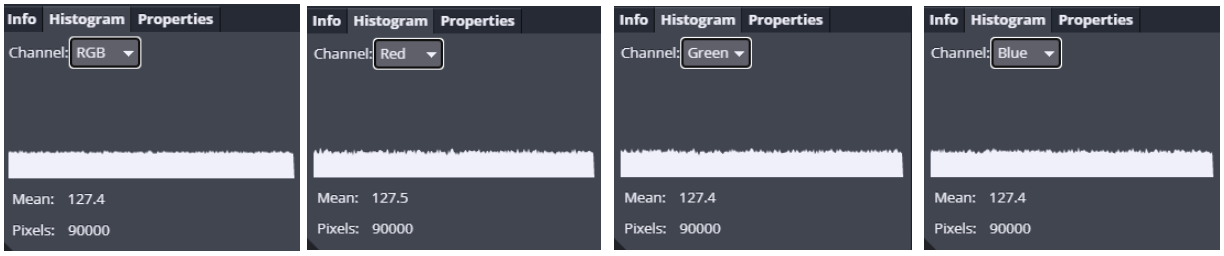
In this equation, A is the original image; B is an encrypted image. $\bar{A}$ and $\bar{B}$ are the average values of the elements of the matrices A and B, respectively. M and N are the height and width of the original / encrypted image, respectively. The CC values between the pairs of original and encrypted images are very small (Table 1), indicating that the encrypted and original images differ significantly.

Another criterion for estimating the difference between the original and encrypted images is the root mean square error (MSE). Mathematically, MSE is defined as [10, 27, 28]:



a) b) c) d)

Fig. 3. Histograms of the original image as a whole a), and separately red b), green c) and blue components d)



a) b) c) d)

Fig. 4. Histogram of the image after encryption as a whole a), and separately red b), green c) and blue components d)

$$MSE=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(a(i,j)-b(i,j)\right)^2}{M\times N}. \quad (10)$$

The parameters a(i,j) and b(i,j) refer to the pixels located in the i-th row and the j-th column of the original image and the encrypted image, respectively. The higher the MSE value is, the better the encryption security will be. In addition, the quality of the encrypted image is estimated using the peak signal-to-noise ratio (PSNR) [33], which is described by the following expression:

$$PSNR=20\log_{10}\left[\frac{I_{MAX}}{\sqrt{MSE}}\right], \quad (11)$$

where I_{MAX} is the maximum value of the image pixels. The PSNR value should be low, which corresponds to the large difference between the original image and the encrypted image. The obtained values of MSE and PSNR after image encryption by the proposed method are presented in Table 2.

Gradations of the original image color components change during encryption, so the magnitude of the change in pixel gradation will characterize the efficiency of encryption. This change may be irregular. This means that the higher the change in pixel values, the more efficient the image encryption and, consequently, the encryption quality (EQ). Therefore, EQ can be expressed through the general change of pixel values between the original image and the encrypted image [10, 27, 28]. The quality of image encryption can be determined using equation (12).

$$EQ=\frac{\sum_{L=0}^{255}\left(H_L(C)-H_L(P)\right)^2}{256}, \quad (12)$$

where $H_L(P)$ and $H_L(C)$ – Gray levels in the original and encrypted image. The obtained EQ value is given in Table 2.

Further, the analysis of key space and entropy for the proposed encryption method was performed. The key space should be large enough to make brute-force attacks impossible [23]. Since the secret key to determine the initial conditions of the proposed method of 256 bits, as well as the control parameters are set by the operator with an accuracy of 5 decimal places, the key space is about $2^{256}+10^{25}$, which is large enough for the proposed system to resist any brute-force attack.

Entropy is the most dominant sign of randomness [10, 27, 28]. Taking into account the source of statistically independent random events from a discrete set of possible events $\{s_1,s_2,...s_i\}$ with related probabilities $\{P(s_1),P(s_2),...,P(s_i)\}$, the average information at the output of the message source is called the entropy of the message source and is calculated by the formula:

$$H(s)=\sum_{i=0}^{2^{L-1}}P(s_i)\log_2\frac{1}{P(s_i)}, \quad (13)$$

where s_i – symbols of a message source, a 2^L – general state of an information source. For a purely random message source, the entropy should be maximal.

For a perfectly random image, the information entropy value is 8. The entropy value of the encrypted message is given in Table 2. This value is very close to the theoretical value of 8 and this means that information leakage during encryption is negligible and the encryption scheme is protected from entropy attack. The entropy value of the image "Flowers" is 5,454 before encryption and 7,932 after encryption.

Table 1

The values of the correlation coefficients of the original and encrypted images

Original image		Encrypted image
vertical	0.917	0.0189
horizontal	0.894	0.0774
diagonal	0.866	0.017

Table 2

Encryption performance indicators

Performance indicators				
CC	MSE	PSNR	EQ	Entropy
0.0018	8845	9.471	132.04	7.932

Another method that confirms the effectiveness of the encryption method is the analysis of the sensitivity of the method to changes in the component pixels. To test the sensitivity of the encryption method, you need to make a small change (for example, to change only one pixel) in the original image, and after the encryption, you get a completely different encrypted image. It would be the same, if you change one pixel in an encrypted image and then try to decrypt it [27, 28]. Such verification can reveal a significant relationship between a simple image and an encrypted one. This type of attack is called a differential attack. If one small change in a simple image can cause a significant change in the cipher image, then this differential attack will be very ineffective and practically useless. Typically, researchers use the mean absolute error (MAE), the pixel change rate (NPCR), and the

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

uniform average change of intensity (UACI) as three criteria to study the effectiveness of resisting a differential attack. Let C(i,j) and P(i,j) be the level of gray pixels in the i-th line and the j-th column of the cipher M×N and the regular image, respectively. The MAE between these two images is defined as:

$$MAE=\frac{\sum_{j=1}^{M}\sum_{i=1}^{N}\left|C(i,j)-P(i,j)\right|}{M\times N}. \quad (14)$$

The evaluation showed that MAE = 92.33. The greater the MAE value, the better the encryption security.

To test the effect of changing one pixel in the original image on the entire encrypted image using our algorithm, we can use two common indicators: NPCR and UACI. We denote two images that have a difference of only one pixel C_1, and $C_2(i,j)$, respectively. Next, we denote the values of the pixel gradation in the grid(i,j) as $C_1(i,j)$ and $C_2(i,j)$ respectively, and determine the two-dimensional array D, which has the same size as C_1 and C_2, as follows:

$$D(i,j)=\begin{cases}0, & C_1(i,j)=C_2(i,j);\\ 1, & C_1(i,j)\neq C_2(i,j).\end{cases} \quad (15)$$

NPCR of these two images is determined as:

$$NPCR=\frac{\sum_{i,j}D(i,j)}{M\times N}\times 100\%. \quad (16)$$

NPCR measures the percentage of different pixels between two images. The higher the NPCR value, the better the encryption security.

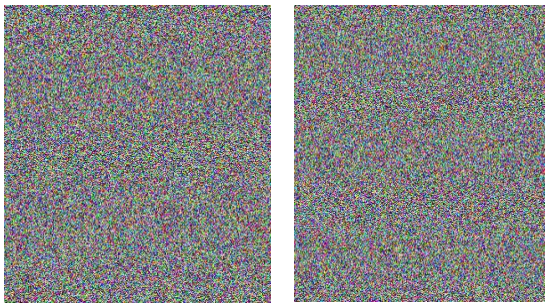
UACI is determined by:

$$UACI=\frac{\sum_{i,j}\left|C_1(i,j)-C_2(i,j)\right|}{255\times M\times N}\times 100\%. \quad (17)$$

The higher the UACI value, the better the encryption security [27, 28].

A good encryption algorithm should also be sensitive to secret keys. This means that changing one bit of a secret key should create a completely different encrypted image. For the proposed method of image encryption, sensitivity to the change the encryption key was analyzed, and the results are generalized in the following way. We encrypted a colored image with two almost identical keys. The only difference was the change of one bit, and the values of the control parameters remained unchanged. Then we compared the result obtained. Fig. 5 shows the test result when a 256-bit key is used to decrypt the image, while another trivially modified key is used to decrypt the encrypted image, the decryption scheme fails completely.

The difference between two encrypted colored images can be observed using calculations of encryption efficiency indicators such as NPCR, UACI, CC and PSNR (NPCR = 99.78, UACI = 32.89, CC = -0.0007 and PSNR = 7.92). This test shows that although the two keys differ by only one bit, there is a difference of up to 99.78 % in the values of the pixels color components of the gray scale between the images encrypted with key 1 and the image encrypted with another key.



a) b)

Fig. 5. The result of encrypting the original message with the selected encryption key a) and changed in one bit encryption key b)

Conclusions

This paper proposes a new method of image encryption based on two chaotic systems. Encryption was performed in two stages: in the first stage, Hénon mapping and fuzzy logic were used to permutate the pixels in the image, and in the second stage, the color gradation of the pixels in the image was changed using the Lorenz system. The initial conditions were generated using a 256-bit external secret key, and the systems control parameters were set by the operator. The result was a key space large enough to withstand brute-force attacks. The encryption process depends on both the original keys and the regular image. Statistical analysis shows that the scheme can well protect images from statistical attacks.

The results of the evaluation of the effectiveness of encryption show that the method has a high sensitivity to the encryption key and to changes in the original image and can resist differential attacks. The distribution of the histogram of the encrypted image was more uniform if compared to the original image. Correlation analysis showed that the correlation coefficients between adjacent pixels in a normal image are significantly reduced after the encryption. The difference between the encrypted and the corresponding original image was measured using MSE and PSNR criteria. The results of the information entropy test indicate that the entropy values are very

close to the theoretical value of 8. Therefore, the proposed encryption method protects the message from entropy attack. MAE, NPCR and UACI were used as the three criteria to study the effectiveness of resisting a differential attack. The results show that a small change in the original image or encryption key will lead to significant changes in the encrypted image and the attacker will not be able to obtain any information when trying to find the approximate key and get the original image.

Future research will be dedicated to using the rules of fuzzy logic in cryptography of communication chaotic systems with direct spread spectrum.

Contribution of authors: analysis of available information resources related to the application of fuzzy logic rules and chaotic systems in encryption. Statement of the problem of studying the methods and algorithms necessary for the development of new methods of image encryption; clarification of requirements for their practical implementation; translation of source materials from Ukrainian into English **– Mykola Kushnir;** development of the method of encryption and decryption of images in two stages: the first stage permutation based on the rules of fuzzy logic and Eno mapping, the second - diffusion based on the Lorenz system; formulation of the main conclusions based on the results of the research and recommendations for their practical use, general editing of the article **– Hryhorii Kosovan;** software implementation; evaluation of the efficiency and stability of the encryption method to various kinds; conducting appropriate experimental research **– Petro Kroialo.**

All authors have read and agreed with the published version of the manuscript.

References (GOST 7.1:2006)

1. Study of the Influence of Changing Signal Propagation Conditions in the Communication Channel on Bit Error Rate [Text] / J. Boiko, I. Pyatin, L. Karpova, O. Eromenko // Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, Springer. – June 2021. – Vol. 69. – P. 79-103. DOI: 10.1007/978-3-030-71892-3_4.

2. A The fuzzy-controller for WiMAX networks [Text] / O. Semenova, A. Semenov, O. Voznyak, D. Mostoviy, I. Dudatyev // 2015 International Siberian Conference on Control and Communications (SIBCON). – 2015. – P. 1-4. DOI: 10.1109/SIBCON.2015.7147214.

3. Hybrid quantum random number generator for cryptographic algorithms [Text] / M. Iavich, T. Kuchukhidze, G. Iashvili, S. Gnatyuk // Radioelectronic and Computer Systems. – 2021. – No. 4(100). – P. 103-118. DOI: 10.32620/reks.2021.4.09.

4. May, R. M. Simple mathematical model with very complicated dynamics [Text] / R. M. May // Nature. – 1976. – Vol. 261. – P. 459–467. DOI: 10.1038/261459a0.

5. Methodology for Assessing Synchronization Conditions in Telecommunication Devices [Text] / J. Boiko, I. Pyatin, O. Eromenko, O. Barabash // Advances in Science Technology and Engineering Systems Journal. – 2020. – Vol. 5, iss. 2. – P. 320-327. DOI: 10.25046/aj050242.

6. Ali, T. S. A new chaos based color image encryption algorithm using permutation substitution and Boolean operation [Text] / T. S. Ali, R. Ali // Multimedia Tools and Applications. – 2020. – Vol. 79, iss. 27. – P. 19853–19873. DOI: 10.1007/s11042-020-08850-5.

7. Panduranga, H. Image encryption based on permutation-substitution using chaotic map and Latin Square Image Cipher [Text] / H. Panduranga, S. Naveen Kumar, Kiran // Eur. Phys. J. Spec. Top. – 2014. – Vol. 223, iss. 8. – P. 1663-1677. DOI: 10.1140/epjst/e2014-02119-9.

8. A new design of cryptosystem based on S-box and chaotic permutation [Text] / M. A. Ben Farah, R. Guesmi, A. Kachouri, M. Samet // Multimedia Tools and Applications. – 2020. – Vol. 79, iss. 27. – P. 19129-19150. DOI: 10.1007/s11042-020-08718-8.

9. Alvarez, G. Some basic cryptographic requirements for chaos-based cryptosystems [Text] / G. Alvarez, S. Li // Int. J. Bifurc. Chaos. – 2006. – Vol. 16, iss. 8. – P. 2129-2151. DOI: 10.1142/S0218127406015970.

10. Cryptanalysis of a chaotic image encryption scheme based on permutation-diffusion structure [Text] / M. Li, Y. Guo, J. Huang, Y. Li // Signal Process. Image Commun. – 2018. – Vol. 62. – P. 164–172. DOI: 10.1016/j.image.2018.01.002.

11. Hoang, T. M. Cryptanalysis and security improvement for a symmetric color image encryption algorithm [Text] / T. M. Hoang, H. X. Thanh // Optik. – 2018. – Vol. 155. – P. 366–383. DOI: 10.1016/j.ijleo.2017.10.072.

12. Bit-level image cryptosystem combining 2D hyper-chaos with a modified non-adjacent spatiotemporal chaos [Text] / S. Guo, Y. Liu, L. Gong, W. Yu, Y. Gong // Multimedia Tools and Appliactions. – 2018. – Vol. 77, iss. 16. – P. 21109–21130. DOI: 10.1007/s11042-017-5570-4.

13. A Chaotic Image Encryption Algorithm Based on Information Entropy [Text] / G. Ye, C. Pan, X. Huang, Z. Zhao, J. He // Int. J. Bifurc. Chaos. – 2018. – Vol. 28, iss. 01. – Article Id: 1850010. – P. 750-758. DOI: 10.1142/S0218127418500104.

14. A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism [Text] / J.-X. Chen, Z.-L. Zhu, C. Fu, H. Yu, L.-B. Zhang // Communications in Nonlinear Science and Numerical Simulation. – 2015. – Vol. 20, iss. 3. – P. 846–860. DOI: 10.1016/j.cnsns.2014.06.032.

15. Fridrich, J. Symmetric Ciphers Based on Two-Dimensional Chaotic Maps [Text] / J. Fridrich // Int. J.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Bifurcation Chaos. – 1998. – Vol. 8, iss. 6. – P. 1259–1284. DOI: 10.1142/S021812749800098X.

16. Liu, W. A fast image encryption algorithm based on chaotic map [Text] / W. Liu, K. Sun, C. Zhu // Opt Lasers Eng. – 2016. – Vol. 84. – P. 26–36. DOI: 10.1016/j.optlaseng.2016.03.019.

17. Hamza, R. A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map [Text] / R. Hamza, F. Titouna // Information Security Journal: A Global Perspective. – 2016. – Vol. 25, iss. 4-6. – P. 162–179. DOI: 10.1080/19393555.2016.1212954.

18. Designing permutation–substitution image encryption networks with Henon map [Text] / P. Ping, F. Xu, Y. Mao, Z. Wang // Neurocomputing. – 2018. – Vol. 283. – P. 53–63. DOI: 10.1016/j.neucom.2017.12.048.

19. Mishra, K. A fast image encryption technique using Henon chaotic map [Text] / K. Mishra, R. Saharan // Progress in Advanced Computing and Intelligent Engineering. Advances in Intelligent Systems and Computing. – Springer, Singapore, 2019. – Vol. 713. – P. 329–339. DOI: 10.1007/978-981-13-1708-8_30.

20. Wang, X. Cryptanalysis of a parallel sub-image encryption method with high-dimensional chaos [Text] / X. Wang, L. Liu // Nonlinear Dynamics. – 2013. – Vol. 73, iss. 1. – P. 795–800. DOI: 10.1007/s11071-013-0832-9.

21. Mudia, H. M. Fuzzy Logic Based Image Encryption for Confidential Data Transfer Using (2, 2) Secret Sharing Scheme [Text] / Hinal M. Mudia, Pallavi V. Chavan // Procedia Computer Science. – 2016. – Vol. 78. – P. 632-639. DOI: 10.1016/j.procs.2016.02.110.

22. Pandurangi Ramacharya, B. Fast partial image encryption with fuzzy logic and chaotic mapping [Text] / B. Pandurangi Ramacharya, M. R. Patil, S. Keralkar // Evol. Intel. – 2022. – 17 p. DOI: 10.1007/s12065-021-00693-9.

23. Zhang, G. A novel image encryption method based on total shuffling scheme [Text] / G. Zhang, Q. Liu // J Opt Commun. – 2011. – Vol. 284, iss. 12. – P. 2775–2780. DOI: 10.1016/j.optcom.2011.02.039.

24. A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process [Text] / B. Norouzi, S. Mirzakuchaki, S. M. Seyedzadeh, M. R. Mosavi // Multimedia Tools and Applications. – 2014. – Vol. 71, iss. 3. – P. 1469–1497. DOI: 10.1007/s11042-012-1292-9.

25. A novel image encryption based on hash function with only two-round diffusion process [Text] / B. Norouzi, S. M. Seyedzadeh, S. Mirzakuchaki, M. R. Mosavi // Multimedia Systems. – 2014. – Vol. 20, iss. 1. – P. 45–64. DOI: 10.1007/s00530-013-0314-4.

26. A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps [Text] / S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, A. Akhavan // Physics Letters A. – 2007. – Vol. 366, iss. 4-5. – P. 391–396. DOI: 10.1016/j.physleta.2007.01.081.

27. Rhouma, R. Cryptanalysis of a spatiotemporal chaotic image/video cryptosystem [Text] / R. Rhouma, S. Belghith // Chaos, Solitons & Fractals. – 2009. – Vol. 41, iss. 4. – P. 1718–1722. DOI: 10.1016/j.chaos.2008.07.016.

28. On the security defects of an image encryption scheme [Text] / C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, G. Chen // Image and Vision Computing. – 2009. – Vol. 27, iss. 9. – P. 1371–1381. DOI: 10.1016/j.imavis.2008.12.008.

29. Ahmed, M. H. An efficient confusion-diffusion structure for image encryption using plain image related henon map [Text] / M. H. Ahmed, A. K. Shibeeb, F. H. Abbood // International Journal of Computing. – 2020. – Vol. 19, iss. 3. – P. 464-473. DOI: 10.47839/ijc.19.3.1895.

References (BSI)

1. Boiko, J., Pyatin, I., Karpova, L., Eromenko O. Study of the Influence of Changing Signal Propagation Conditions in the Communication Chan-nel on Bit Error Rate. *Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, Springer*, June 2021, vol. 69, pp. 79-103. DOI: 10.1007/978-3-030-71892-3_4.

2. Semenova, O., Semenov, A., Voznyak, O., Mostoviy, D., Dudatyev, I. The fuzzy-controller for WiMAX networks. *2015 International Siberian Conference on Control and Communications* (SIBCON), 2015, pp. 1-4. DOI: 10.1109/SIBCON.2015.7147214.

3. Iavich, M., Kuchukhidze, T., Iashvili, G., Gnatyuk, S. Hybrid quantum random number generator for cryptographic algorithms. *Radioelectronic and Computer Systems*, 2021, no. 4 (100), pp. 103-118. DOI: 10.32620/reks.2021.4.09.

4. May, R. M. Simple mathematical model with very compli-cated dynamics. *Nature*, 1976, vol. 261, pp. 459–467. DOI: 10.1038/261459a0.

5. Boiko, J., Pyatin, I., Eromenko, O., Barabash O. Methodology for Assessing Synchronization Conditions in Telecommunication Devices. *Advances in Science Technology and Engineering Systems Journal*, 2020, vol. 5, iss. 2, pp. 320-327. DOI: 10.25046/aj050242.

6. Ali, T. S., Ali, R. A new chaos based color image encryption algorithm using permutation substitution and Boolean operation. *Multimedia Tools and Applications*, 2020, vol. 79, iss. 27, pp. 19853–19873. DOI: 10.1007/s11042-020-08850-5.

7. Panduranga, H., Kumar, S. N., Kiran. Image encryption based on permutation-substitution using chaotic map and Latin Square Image Cipher. *Eur. Phys. J. Spec.*

Top., 2014, vol. 223, iss. 8, pp. 1663–1677. DOI: 10.1140/epjst/e2014-02119-9.

8. Ben Farah, M. A., Guesmi, R., Kachouri, A., Samet M. A new design of cryptosystem based on S-box and chaotic permutation. *Multimedia Tools and Applications*, 2020, vol. 79, iss. 27, pp. 19129–19150. DOI:10.1007/s11042-020-08718-8.

9. Alvarez, G., Li, S. Some basic cryptographic requirements for chaos-based cryptosystems. *Int. J. Bifurc. Chaos*, 2006, vol. 16, iss. 8, pp. 2129–2151. DOI: 10.1142/S0218127406015970.

10. Li, M., Guo, Y., Huang, J., Li, Y. Cryptanalysis of a chaotic image encryption scheme based on permutation-diffusion structure. *Signal Process. Image Commun.*, 2018, vol. 62, pp. 164–172. DOI: 10.1016/j.image.2018.01.002.

11. Hoang, T. M., Thanh, H. X. Cryptanalysis and security improvement for a symmetric color image encryption algorithm. *Optik*, 2018, vol. 155, pp. 366–383. DOI: 10.1016/j.ijleo.2017.10.072.

12. Guo, S., Liu, Y., Gong, L., Yu, W., Gong, Y. Bit-level image cryptosystem combining 2D hyper-chaos with a modified non-adjacent spatiotemporal chaos. *Multimedia Tools and Applications*, 2018, vol. 77, iss. 16, pp. 21109–21130. DOI: 10.1007/s11042-017-5570-4.

13. Ye, G., Pan, C., Huang, X., Zhao, Z., He, J. A Chaotic Image Encryption Algorithm Based on Information Entropy. *Int. J. Bifurc. Chaos*, 2018, vol. 28, iss. 01, article id: 1850010, pp. 750-758. DOI: 10.1142/S0218127418500104.

14. Chen, J.-X., Zhu, Z.-L., Fu, C., Yu, H., Zhang, L.-B. A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. *Communications in Nonlinear Science and Numerical Simulation*, 2015, vol. 20, iss. 3, pp. 846–860. DOI: 10.1016/j.cnsns.2014.06.032.

15. Fridrich, J. Symmetric Ciphers Based on TwoDimensional Chaotic Maps. *Int. J. Bifurcation Chaos*. 1998, vol. 8, iss. 6, pp. 1259–1284. DOI: 10.1142/S021812749800098X.

16. Liu, W., Sun, K., Zhu, C. A fast image encryption algorithm based on chaotic map. *Opt Lasers Eng.*, 2016, vol. 84, pp. 26–36. DOI: 10.1016/j.optlaseng.2016.03.019.

17. Hamza, R., Titouna, F. A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map. *Information Security Journal: A Global Perspective*, 2016, vol. 25, iss. 4-6, pp. 162–179. DOI: 10.1080/19393555.2016.1212954.

18. Ping, P., Xu, F., Mao, Y., Wang, Z. Designing permutation–substitution image encryption networks with Henon map. *Neurocomputing*, 2018, no. 283, pp. 53–63. DOI: 10.1016/j.neucom.2017.12.048.

19. Mishra, K., Saharan, R. A fast image encryption technique using Henon chaotic map. *Progress in advanced computing and intelligent engineering. Advances in Intelligent Systems and Computing. Springer, Singapore*, 2019, vol. 713, pp. 329–339. DOI: 10.1007/978-981-13-1708-8_30.

20. Wang, X., Liu, L. Cryptanalysis of a parallel sub-image encryption method with high-dimensional chaos. *Nonlinear Dynamics*, 2013, vol. 73, iss.1, pp. 795–800. DOI: 10.1007/s11071-013-0832-9.

21. Mudia, H. M., Chavan, P. V. Fuzzy Logic Based Image Encryption for Con-fidential Data Transfer Using (2, 2) Secret Sharing Scheme. *Procedia Computer Science*, 2016, vol. 78, pp. 632-639. DOI: 10.1016/j.procs.2016.02.110.

22. Pandurangi Ramacharya, B., Patil, M. R., Keralkar, S. Fast partial image encryption with fuzzy logic and chaotic mapping. *Evol. Intel.*, 2022. 17 p. DOI: 10.1007/s12065-021-00693-9.

23. Zhang, G., Liu, Q. A novel image encryption method based on total shuffling scheme. *J Opt Commun.*, 2011, vol. 284, iss. 3, pp. 2775–2780. DOI: 10.1016/j.optcom.2011.02.039.

24. Norouzi, B., Mirzakuchaki, S., Seyedzadeh, S. M., Mosavi, M. R. A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process. *Multimedia Tools and Applications*, 2014, vol. 71, iss. 3, pp. 1469–1497. DOI: 10.1007/s11042-012-1292-9.

25. Norouzi, B., Seyedzadeh, S. M., Mirzakuchaki, S., Mosavi M. R. A novel image encryption based on hash function with only two-round diffusion process. *Multimedia Systems*, 2014, vol. 20, iss. 1, pp. 45–64. DOI: 10.1007/s00530-013-0314-4.

26. Behnia, S., Akhshani, A., Ahadpour, S., Mahmodi, H., Akhavan, A. A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps. *Physics Letters A*, 2007, vol. 366, iss. 4-5, pp. 391–396. DOI: 10.1016/j.physleta.2007.01.081.

27. Rhouma, R., Belghith, S. Cryptanalysis of a spatiotemporal chaotic image/video cryptosystem. *Chaos, Solitons & Fractals*, 2009, vol. 41, iss. 4, pp. 1718–1722. DOI: 10.1016/j.chaos.2008.07.016.

28. Li, C., Li, S., Asim, M., Nunez, J., Alvarez, G., Chen, G. On the security defects of an image encryption scheme. *Image and Vision Computing*, 2009, vol. 27, iss. 9, pp. 1371–1381. DOI: 10.1016/j.imavis.2008.12.008.

29. Ahmed, M. H., Shibeeb, A. K., Abbood, F. H. An efficient confusion-diffusion structure for image encryption using plain image related henon map. *International Journal of Computing*, 2020, vol. 19, iss. 3, pp. 464-473. DOI: 10.47839/ijc.19.3.1895.

Надійшла до редакції 17.07.2022, розглянута на редколегії 20.11.2022

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

МЕТОД ШИФРУВАННЯ ЗОБРАЖЕНЬ НА ОСНОВІ ДВОХ БАГАТОВИМІРНИХ ХАОТИЧНИХ СИСТЕМ ІЗ ЗАСТОСУВАННЯМ НЕЧІТКОЇ ЛОГІКИ

Микола Кушнір, Григорій Косован, Петро Крояло

Предмет дослідження. Пропонується розробка методу шифрування зображень із перестановкою пікселів реалізованій при застосуванні нечіткої логіки та відображення Ено, а також дифузії, що реалізовується за допомогою системи Лоренца. **Об'єкт дослідження**: Запропонувати ефективний спосіб застосування правил нечіткої логіки по відношенню до значень сформованих відображенням Ено для реалізації перестановки пікселів в зображенні, що забезпечить випадково подібну перестановку ті підвищить ефективність роботи методу шифрування. Також для досягнення кращої захищеності в процесі шифрування зображення передбачено застосування процесу дифузії, реалізованого за допомогою системи Лоренца. Крім того для збільшення чутливості методу шифрування до зміни початкового значення складових кольорів пікселів теж використовуватимуться в процесі шифрування. **Методи дослідження та результати дослідження**: розроблено та представлено метод шифрування зображень із перестановкою пік-селів реалізованій при застосуванні нечіткої логіки та відображення Ено, а також дифузії, що реалізовується за допомогою системи Лоренца. Початкові значення для відображення Ено та системи Лоренца визначатимуться із введеного ключового слова, а параметри керування задаються оператором, при цьому значення складових кольорів пікселів теж прийматимуть участь в процесі шифрування. Крім того перед початком процесу перестановки пікселів в зображенні здійснюється реалізація правил нечіткої логіки для відображення Ено. Також значення складових пікселів до та після процедури дифузії будуть приведені до одиничного інтервалу. Отже в результаті шифрування зображень початкове зображення повністю змінюється, втрачає свій зміст та форму, а також розподіл інтенсивності кольорів пікселів стає рівномірним. Також було здійснено програмну реалізацію запропонованого методу шифрування та оцінку якісним характеристикам запропонованого методу шифрування зображення, а саме: аналіз гістограм оригінального і зашифрованого зображень, кореляції сусідніх пікселів зображень, середньоквадратичної помилки (MSE), пікового співвідношення сигнал / шум (PSNR), ентропії та чутливості до зміни складових кольорів пікселів. **Висновки**. Реалізація методу показала, що він володіє великою кількістю ключів шифрування, що робить атаку грубої сили (процес їх підбору) ресурсовитратною і складною, а здійснення процесу шифрування в два етапи і з застосування двох різних хаотичних систем значно покращує захищеність зашифрованого зображення та ускладнює можливість реалізації різного роду атак.

Ключові слова: криптографія; нечітка логіка; перестановка; дифузія; зображення; хаос; захищеність.

Кушнір Микола Ярославович – канд. фіз.-мат. наук, доц., доц. каф. радіотехніки та інформаційної безпеки, Чернівецький національний університет імені Юрія Федьковича, Чернівці, Україна.

Косован Григорій Васильович – канд. техн. наук, асист. каф. радіотехніки та інформаційної безпеки, Чернівецький національний університет імені Юрія Федьковича, Чернівці, Україна.

Крояло Петро Михайлович – асп. каф. радіотехніки та інформаційної безпеки, Чернівецький національний університет імені Юрія Федьковича, Чернівці, Україна.

Mykola Kushnir – PhD in physical and mathematical Sciences, Assoc. Prof., Assoc. Prof. of Radio Engineering and Information Security Department, Yuri Fedkovych Chernivtsi National University, Chernivtsi, Ukraine,
e-mail: myk.kushnir@chnu.edu.ua, ORCID: 0000-0001-9480-3856.

Hryhorii Kosovan – PhD in technical Science, Assist. of Radio Engineering and Information Security Department, Yuri Fedkovych Chernivtsi National University, Chernivtsi, Ukraine,
e-mail: g.kosovan@chnu.edu.ua, ORCID: 0000-0002-3351-3852.

Petro Kroialo – PhD Student of Radio Engineering and Information Security Department, Yuriy Fedkovych National University of Chernivtsi, Chernivtsi, Ukraine,
e-mail: p.kroialo@chnu.edu.ua.