DOI: 10.18721/JCSTCS.14101
УДК 004.056

IMAGE ENCRYPTION ALGORITHM BASED ON CONTROLLED CHAOTIC MAPS

V.N. Shashikhin, A.V. Turulin, S.V. Budnik

Peter the Great St. Petersburg Polytechnic University,
St. Petersburg, Russian Federation

The article reviews the problem of ensuring the security of storage, processing, and transmission of images based on a cryptographic method using chaotic maps. The encryption algorithm is based on a three-dimensional mapping. The encryption algorithm strength when using systems with chaotic dynamics depends on the value of the largest (positive) Lyapunov characteristic exponent. Therefore, the problem of increasing resistance to various kinds of attacks is reduced to determining the control parameters, at which the leading Lyapunov characteristic exponent increases. The authors propose a procedure for changing the chaotic map characteristics (entropy and Lyapunov characteristic exponents) based on introducing feedback into the system. The procedure is developed using the modal control method based on reducing the system to the canonical Frobenius form. The use of the proposed algorithm is considered on the example of the Rössler system. The test results confirmed an increase in the strength of the proposed encryption algorithm against statistical and differential analysis due to an increase in the Lyapunov characteristic exponent.

Keywords: Image encryption, chaotic maps, control of the spectrum of Lyapunov characteristic exponents, modal control, canonical Frobenius form.

Citation: Shashikhin V.N., Turulin A.V., Budnik S.V. Image encryption algorithm based on controlled chaotic maps. Computing, Telecommunications and Control, 2021, Vol. 14, No. 1, Pp. 7–21. DOI: 10.18721/JCSTCS.14101

АЛГОРИТМ ШИФРОВАНИЯ ИЗОБРАЖЕНИЙ НА ОСНОВЕ УПРАВЛЯЕМЫХ ХАОТИЧЕСКИХ ОТОБРАЖЕНИЙ

В.Н. Шашихин, А.В. Турулин, С.В. Будник

Санкт-Петербургский политехнический университет Петра Великого,
Санкт-Петербург, Российская Федерация

Рассмотрена задача обеспечения безопасности хранения, обработки и передачи изображений на основе криптографического метода с использованием хаотических отображений. Алгоритм шифрования построен на базе трехмерного отображения. Стойкость алгоритма шифрования при использовании систем с хаотической динамикой зависит от величины старшего (положительного) характеристического показателя Ляпунова. Поэтому задача повышения стойкости к различного рода атакам сводится к определению параметров управления, при котором старший характеристический показатель Ляпунова увеличивается. Предложена процедура изменения свойств хаотического отображения (энтропии и характеристических показателей Ляпунова) на основе введения в систему обратной связи. Процедура построена на использовании метода модального управления на основе приведения системы к канонической форме Фробениуса. Рассмотрено применение предлагаемого алгоритма шифрования для системы Рёсслера. Результаты тестирования подтвердили увеличение стойкости предложенного алгоритма шифрования к статистиче-

скому и дифференциальному анализу за счет увеличения старшего характеристического показателя Ляпунова.

Ключевые слова: шифрование изображений, хаотические отображения, управление спектром характеристических показателей Ляпунова, модальное управление, каноническая форма Фробениуса.

Ссылка при цитировании: Shashikhin V.N., Turulin A.V., Budnic S.V. Image encryption algorithm based on controlled chaotic maps // Computing, Telecommunications and Control. 2021. Vol. 14. No. 1. Pp. 7–21. DOI: 10.18721/JCSTCS.14101

Introduction

The problem of ensuring the security of image transmission is currently becoming more and more urgent in connection with the increasing flow of information transmitted over open communication lines. Reliable encryption methods for storing and transmitting digital images are required in various fields: medical information systems, confidential video conferencing, government and military communications systems.

Cryptographic methods stand out among various methods of protecting information and ensuring its integrity. However, traditional encryption algorithms, for example, AES and DES, were developed without taking into account the specific requirements for image encryption [1, 13] (a large amount of memory occupied, limited processing and transmission time) [2]. Therefore, it became necessary to create new encryption algorithms based on the use of nonlinear functions [3, 14].

One of the promising directions in modern cryptography is the development and research of data encryption algorithms based on dynamic chaos [4–7, 15, 16]. Such properties of chaotic systems as the exponential divergence of trajectories, ergodicity, and randomization are useful in the development of encryption schemes for digital images [8, 17–20]. Modern approaches to encryption use various chaotic maps and algorithms based on the composition of two maps that implement the operation of randomization and entanglement [9, 21, 22].

The paper considers an image encryption algorithm based on a chaotic mapping, which simultaneously implements the operation of randomizing and confusion. To improve the cryptographic stability of the algorithm, a procedure is proposed for changing the chaotic map characteristics (entropy and Lyapunov characteristic exponents) based on introducing feedback into the system. A procedure for changing the spectrum of Lyapunov characteristic exponents of a chaotic map is developed using the modal control method based on reducing the system to the canonical Frobenius form.

Image encryption problem statement

Mathematical model of the image. Let the raster model of the original rectangular image be represented by the following map:

$$I:[a,b]\times[c,d]\to L\left(R^{N\times M}\right), \tag{1}$$

where $L\left(R^{N\times M}\right)$ is the space of numerical dimension matrices of $N\times M$ size.

The N, M values are related to the dimensions of the pixel grid:

$$\Delta^{WH}=\left\{(i,j):i=\overline{1,N}=[W],j=\overline{1,M}=[H]\right\}, \tag{2}$$

where [*] is the integer part of the number.

With the help of digitalization and quantization operations, the description of digital images is reduced to a set of samples, which can be represented in the form of a matrix:

$$\mathrm{I} = \left(I_{ij}\right)_{i,j=1}^{N,M} \in L\left(R^{N\times M}\right), \tag{3}$$

whose elements are realizations on a discrete grid of continuous functions of two variables $\mathrm{I}:\left(0,W\right)\otimes\left(0,H\right)\to R$. The elements of these matrices take integer values from the [0; 255] interval when coding the pixel intensity with an eight-bit code.

Mathematical model of a system with chaotic dynamics. A nonlinear differential equation with a given initial state is considered as an evolutionary operator for the implementation of the encryption algorithm:

$$\dot{x}\left(t\right) = F\left(x\left(t\right)\right),\ x\left(t_0\right) = x_0, \tag{4}$$

where $x\left(t\right)\in \mathrm{P}\subseteq \mathrm{R}^n$ is the phase vector of the system; region P – phase space of the system; t – time function, $F:\mathrm{R}^n\to\mathrm{R}^n$ – vector function with $f_i\left(x\left(t\right)\right), i=\overline{1,n}$ components.

Among the set of nonlinear dynamical systems $S=\left\{\mathrm{P},F\right\}$, we will consider systems with a chaotic mapping for which the following conditions are satisfied.

1. The f map has an essential dependence on the initial data or it is sensitive (if there is such a number $\delta > 0$, that for any $\varepsilon > 0$ and any $x'\in X$ point there is a $x''\in X$ and the $m\in M$ number such that $\rho\left(x',x''\right)<\varepsilon$, but $\rho\left(f^{(m)}\left(x''\right)-f^{(m)}\left(x'\right)\right)\geq\delta$).

2. The f map p is transitive (for any U, V pair of open sets there is $m\geq 0$, that $f^{(m)}\left(U\right)\bigcap V\neq \mathrm{O}$).

The problem of controlling the spectrum of Lyapunov characteristic exponents. The mathematical model of a chaotic system in the synthesis of an encryption algorithm is a heterogeneous differential equation with a control

$$\dot{x}\left(t\right) = F\left(x\left(t\right)\right) + Bu\left(t\right),\ x\left(t_0\right) = x_0. \tag{5}$$

Lyapunov spectrum of the original nonlinear system (4)

$$\sigma\left(F\right) = \left\{\chi_i\left(F\right), i=\overline{1,n}\right\}$$

consists of n various Lyapunov characteristic exponents $\chi_1\left(F\right)\geq\chi_2\left(F\right)\geq\ldots\geq\chi_n\left(F\right)$ in descending order.

The problem of controlling the Lyapunov spectrum is to determine the feedback from the phase vector of the nonlinear system:

$$u\left(t\right) = K^*x\left(t\right) \tag{6}$$

such that the closed nonlinear system

$$\dot{x}\left(t\right) = F\left(x\left(t\right)\right) + BK^*x\left(t\right),\ x\left(t_0\right) = x_0 \tag{7}$$

had the following spectrum

$$\sigma\left(F+BK^*\right) = \left\{\chi_i\left(F+BK^*\right), i=\overline{1,n}\right\}, \tag{8}$$

equal to the required spectrum

$$\sigma(G)=\left\{\chi_i(G), i=\overline{1,n}\right\}. \quad (9)$$

The encryption algorithm strength when using systems with chaotic dynamics depends on the value of the largest (positive) Lyapunov characteristic exponent. Therefore, the problem of increasing resistance to various kinds of attacks is reduced to determining the control parameters (6), at which the leading Lyapunov characteristic exponent (9) increases in the closed-loop system (7). Besides, the feedback factor will expand the "keyspace" of the encryption algorithm.

Evaluation of the encryption algorithm strength. It is necessary to build a grayscale image encryption algorithm based on a chaotic map and to carry out a comparative assessment of the algorithm's strength with and without control action.

As a result of statistical cryptanalysis, it is necessary:

- to assess the uniformity of the distribution of pixels by brightness values, construct a histogram of this distribution;
- to calculate the pairwise correlation between two adjacent pixels horizontally, vertically, and diagonally;
- to calculate informational entropy.

To assess the strength of the algorithm to differential analysis, calculate:

- the percentage of pixels that changed the brightness value;
- the average change in gray intensity.

Encryption algorithm based on a 3D chaotic map

Chaotic map and its properties. In the process of image encryption, a three-dimensional chaotic Rössler map is used as a model of a nonlinear system (4)

$$\begin{cases} \dot{x}_1 = -(x_2 + x_3); \\ \dot{x}_2 = x_1 + ax_2; \\ \dot{x}_3 = b + x_3(x_1 - c). \end{cases} \quad (10)$$

For $a = 0.2$, $b = 0.2$, $c = 5.7$ values of the parameters, this map has a spectrum of Lyapunov characteristic exponents equal to

$$\sigma(F)=\left\{\chi_1(F)=0.1016; \chi_2(F)=0.0922; \chi_3(F)=-5.6953\right\}, \quad (11)$$

and a trajectory in three-dimensional phase space, which has the form shown in Fig. 1.

The spectrum of Lyapunov characteristic exponents and a strange attractor indicate the presence of chaotic dynamics in system (10).

Encryption algorithm. The grayscale image encryption algorithm of $N \times M$ size using nonlinear map (10) has the following steps in one round of encryption.

Step 1. Based on the original image, a raster model of the original image (1) with a matrix of the form (3) is formed:

$$\mathrm{I}=\left(I_{ij}\right)_{i,j=1}^{N,M} \in L\left(\mathrm{R}^{N\times M}\right),$$

where i is the number of pixel in the vertical row; j – the number of pixel in the horizontal row; $I_{i,j}$ – pixel with the i, j number brightness value; N – number of rows, and M – number of columns of the pixel matrix determined by the grid size (2).

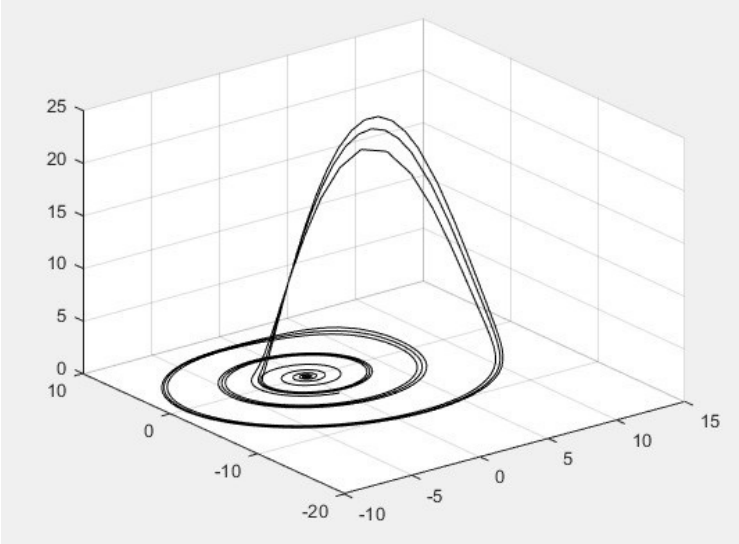

Fig. 1. Trajectory of the Rössler system

Step 2. For some initial state $x(0)=(x_1(0), x_2(0), x_3(0))$, determined by the point of exit of the chaotic system trajectory (10) to a strange attractor, three sequences are generated:

$$\begin{aligned} X_1 &= \{x_1(t_1), \dots x_1(t_k), \dots x_1(t_s)\}; \\ X_2 &= \{x_2(t_1), \dots x_2(t_k), \dots x_2(t_s)\}, \quad s = N \times M; \\ X_3 &= \{x_3(t_1), \dots x_3(t_k), \dots x_3(t_s)\}. \end{aligned} \tag{12}$$

Sequences X_1 and X_2 define the randomization of pixels, and the X_3 sequence defines the scattering (brightness changes) of pixels.

Here, the elements of sequences (12) are formed according to the rule:

$$\begin{aligned} \dot{x}_1(t) &= f_1[x(t)], \\ \dot{x}_2(t) &= f_2[x(t)], \Leftrightarrow \dot{x}(t) = F[x(t)], \\ \dot{x}_3(t) &= f_3[x(t)], \end{aligned} \tag{13}$$

where $F[x(t)] = \left(f_1\left(x(t), f_2\left(x(t), f_3\left(x(t)\right)\right)\right)\right)^T$ is a vector function whose components are the functions on the right-hand side of equations (10).

Step 3. A chaotic matrix of the encrypted image of the first round is formed using the third equation (13):

$$E^{(1)} = \begin{bmatrix} e_{1,1}^{(1)} & e_{1,2}^{(1)} & \dots & e_{1,M}^{(1)} \\ e_{2,1}^{(1)} & e_{2,2}^{(1)} & \dots & e_{2,M}^{(1)} \\ \dots & \dots & \dots & \dots \\ e_{N,1}^{(1)} & e_{N,2}^{(1)} & \dots & e_{N,M}^{(1)} \end{bmatrix} \in \mathrm{R}^{N \times M}, \tag{14}$$

where $e_{i,j}^{(1)} = \left[x_3(t) \bmod 255 \right]$ is the intensity of gray pixel with the $i = \left[x_1(t) \bmod M \right]$ row number and the $j = \left[x_2(t) \bmod N \right]$ column number; [*] is the integer part of number.

Further, repeating steps 2–3 for the image (14) for p rounds, we get an encrypted image $\hat{E}^{(p)}$ of the following form:

$$\hat{E}^{(1)} = \left(\hat{e}_{i,j}^{(1)} \right)_{i,j}^{N,M} \in \mathrm{R}^{N \times M}. \tag{15}$$

The number of rounds is determined by the required cipher strength indicators.

Cryptanalysis of the encryption algorithm. The assessment of the algorithm strength is carried out using statistical and differential cryptanalysis [2]. The 512 × 512 gray-scale Lena photo is used as the source image.

To determine the distribution of pixels of the encrypted image $\hat{E}^{(p)}$ (15) in grayscale, the following probability is calculated:

$$P(m_s) = \frac{m_s}{N \times M}, \tag{16}$$

where m_s is the number of pixels e_{ij}, for the gray intensity takes on $s \in [0; 255]$ values. The distribution of pixels by gray intensity values for the original image is shown in Fig. 2, and for the encrypted image – in Fig. 3.

Pairwise correlation between two adjacent pixels horizontally, vertically and diagonally of the original and encrypted images is calculated by the formula:

$$\rho(u_i, v_{i+1}) = \frac{\dfrac{\sum_{i=1}^{N \times M} (u_i - \bar{U})(v_{i+1} - \bar{V})}{N \times M}}{\sqrt{\dfrac{\sum_{i=1}^{N \times M} (u_i - U)^2}{N \times M}} \sqrt{\dfrac{\sum_{i=1}^{N \times M} (v_{i+1} - V)^2}{N \times M}}}, \tag{17}$$

$$\bar{U} = \frac{\sum_{i=1}^{N \times M} u_i}{N \times M}, \ \bar{V} = \frac{\sum_{i=1}^{N \times M} v_i}{N \times M},$$

where u_i, v_{i+1} – the intensity of the i^{th} gray pixel and the pixel adjacent to it, $U = \{u_1, u_2, \ldots u_i, \ldots u_{N \times M}\}$, $V = \{v_1, v_2, \ldots v_i, \ldots v_{N \times M}\}$ – a series of gray intensity values of pixels in the image and a series of gray intensity values of neighboring pixels.

Information entropy is determined by the expression:

$$H(m_s) = \sum_{s=0}^{2^n - 1} P(m_s) \log_2 \left(1 / P(m_s) \right), \tag{18}$$

where $P(m_s)$ is the probability of the gray intensity belonging to the $s \in [0; 255]$ level.

To assess the strength of the algorithm against the differential analysis, the following are calculated:

- number of changing pixel rate (NPCR):

$$\Pi(I_1, I_2) = \frac{\sum_{i=1}^{N} \sum_{j=1}^{M} D(i, j)}{N \times M} \times 100\%, \tag{19}$$

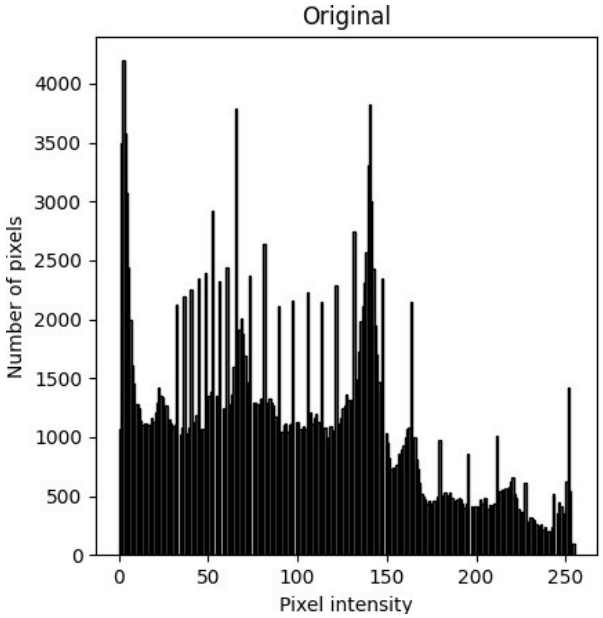

Fig. 2. Original image histogram

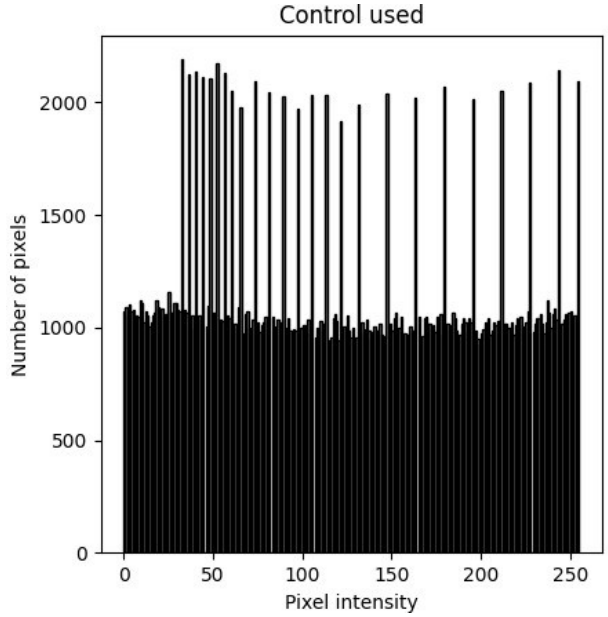

Fig. 3. Encrypted image histogram

where

$$D(i,j)=\begin{cases}1, & if \quad e_1(i,j)=e_2(i,j)\\ 0, & if \quad e_1(i,j)\neq e_2(i,j)\end{cases} \quad \forall i=\overline{1,N}, \quad \forall j=\overline{1,M},$$

I_1 – the original image, I_2 – the original image with the gray level of one pixel being changed;

$\hat{E}_1^{(p)} \cdot \hat{E}_2^{(p)}$ – the encrypted images corresponding to the I_1, I_2 original images;

$\hat{e}_1^{(p)}(i, j), \hat{e}_2^{(p)}(i, j)$ – the value of the gray level for the pixel with the (i, j) number in the $\hat{E}_1^{(p)}$ and $\hat{E}_2^{(p)}$ images;

- unified averaged changed intensity (UACI)

$$C(E_1, E_2) = \frac{1}{N \times M} \sum_{i=1,\, j=1}^{N,\, M} \frac{\left| e_1(i, j) - e_2(i, j) \right|}{255} \times 100\,\%. \tag{20}$$

The results of calculating the strength criteria after two rounds of encryption using the chaotic map with and without control are shown in Table 1.

Table 1

Encryption algorithm strength criteria

Chaotic map	Largest LCE	Image	Correlation coefficient			Entropy	NPCR, %	UACI, %
			Horizontal	Vertical	Diagonal			
–	–	original	0.0293	0.0263	0.0653	7.55	–	–
No control	0.1016	encrypted	0.000175	0.000192	0.000380	7.76	99.54	33.42
With control	0.2862	encrypted	0.000101	0.000186	0.000117	7.96	99.55	33.45

Control of Lyapunov characteristic exponent of chaotic map

To increase the strength of the proposed image encryption algorithm, a control action is introduced into a system with chaotic dynamics to increase the positive Lyapunov characteristic exponent and information entropy. Control is sought in the form of linear feedback in phase coordinates.

The solution to the problem of changing the spectrum of characteristic exponents of a nonlinear system is based on the Grobman-Hartman theorem [11]. Any system in a neighborhood of a hyperbolic singular point is locally topologically equivalent to its linear approximation. Thus, the behavior of a nonlinear system in the neighborhood of a hyperbolic singular point is similar to the behavior of a linearized system. A singular point is hyperbolic if the Jacobi matrix has no eigenvalues in it on the imaginary axis. A change in the characteristic exponents of a linearized system, which coincides with the real part of the eigenvalues of the Jacobi matrix, entails a change in the characteristic exponents of a nonlinear system.

Synthesis of linearized system control. It is possible to provide the desired eigenvalues of the Jacobi matrix of the linearized system using the method of synthesis of a modal controller based on a reduction to the canonical Frobenius form [12].

Let the equations of state of the linearized system have the form:

$$\dot{y}(t) = Ay(t) + bu(t), \;\; y(t_0) = y_0, \tag{21}$$

where $y(t) \in R^n$ is the vector of state coordinates; $u(t) \in R^1$ – the control action; $A \in R^{n \times n}$ – the Jacobi matrix of the nonlinear system (10) at the hyperbolic singular point.

It is required to determine the $k = (k_1, k_2, \ldots k_n)^T$ parameters of the linear feedback control law $u(t) = kx(t)$ providing the given eigenvalues $\overline{v}_i, \; i = 1, \ldots, n$ of the matrix of the closed system $A_c = A + bk$. From the expression for the matrix of the $A_c = A + bk^T$ closed system, it is impossible to directly obtain

the values of the feedback coefficient, since the matrix is unknown. Therefore, such a change of variables $y = Q\tilde{y}$ is used that the mathematical model of the transformed system $\dot{\tilde{y}} = \left(\tilde{A} + \tilde{b}\tilde{k}^T\right)\tilde{y}$ has the canonical Frobenius form with the A matrix and the b vector of the following form:

$$A_f = \begin{bmatrix} 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \\ -a_n & -a_{n-1} & \dots & -a_1 \end{bmatrix}, \; b_f = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix},$$

where a_i are the coefficients of the characteristic polynomial of the matrices A and A_f.

To bring the matrix of the system to the canonical form, the matrix T formed from the coefficients of the characteristic polynomial of the matrix A is used as follows:

$$T = \begin{bmatrix} a_{n-1} & a_{n-2} & \dots & 1 \\ a_{n-2} & a_{n-3} & \dots & 0 \\ a_{n-3} & 1 & \dots & 0 \\ 1 & 0 & \dots & 0 \end{bmatrix}.$$

The similarity transformation $y = Q\tilde{y}$ uses the matrix $Q = S_y T$, where S_y is the system controllability matrix. If this similarity transformation is performed in system (21):

$$\dot{\tilde{y}} = Q^{-1}AQ\tilde{y} + Q^{-1}bk^TQ\tilde{y}$$

and the following notation is introduced

$$\tilde{k} = Q^T k, \; \tilde{b} = Q^{-1}b, \; \tilde{A} = Q^{-1}AQ,$$

then the system model will take the following form:

$$\dot{\tilde{y}} = \left(\tilde{A} + \tilde{b}\tilde{k}^T\right)\tilde{y}.$$

Considering the peculiarities of constructing the Q matrix, the matrix of the system will have the Frobenius matrix form, and the b vector will be reduced to the simplest form:

$$\tilde{A} = I_n^{(1)} - e_n a^T, \; \tilde{b} = e_n,$$

where $I_n^{(1)}$ is a matrix of $n \times n$ size, having unities over the main diagonal, and the remaining elements being zero; e_n is a unit vector of n, the n^{th} coordinate of which is equal to unity, and the rest are equal to zero; $a = (a_n, a_{n-1}, ..., a_1)^T$.

The closed-loop matrix will take the form:

$$\tilde{A}_c = \tilde{A} + \tilde{b}\tilde{k}^T = I_n^{(1)} - e_n\left(a - \tilde{k}\right)^T.$$

For this matrix to have the required eigenvalues, the coefficients of its characteristic equation must correspond to the $a_{est} = \left(a_n^{est}, a_{n-1}^{est}, ..., a_1^{est}\right)^T$ vector, where a_i^{est} are the coefficients of the characteristic

polynomial of the matrices A_c and $\tilde{A}_c$. Then $a_{est} = a - \tilde{k},$ and the coefficients of the controller for linearized system (21) are determined by the relation:

$$k = \left(Q^T\right)^{-1}\left(a - a_{est}\right). \tag{22}$$

Synthesis of a nonlinear system control. Let the Jacobian matrix equal J^* at the singular point x^* of system (4) in the absence of control, and the vector of its eigenvalues is equal to v^*. Let us set the vector of the desired eigenvalues $\overline{v}^*$ of the Jacobian $\overline{J}^*$ of the nonlinear system (5) in the form:

$$\overline{v}_i^* = v_i^* + \alpha \operatorname{Re}\left(v_i^*\right), \tag{23}$$

where α is the coefficient selected according to the graph in Fig. 4.

For the Jacobian $\overline{J}^*$ of system (21) to have given eigenvalues, we choose a control in the form:

$$u(t) = kx(t), \tag{24}$$

then the Jacobian of system (21) with control (24) will be equal to

$$\overline{J}^* = J^* + Bk, \tag{25}$$

where $k \in R^{1\times n}$ is the feedback coefficient, which is found by the method of synthesis of modal control according to formula (22).

The largest Lyapunov characteristic exponent of system (5) with control (24) will differ from the largest Lyapunov characteristic exponent of uncontrolled nonlinear system (4). It is necessary to increase the largest Lyapunov characteristic exponent to increase chaos in the system, which is achieved by the appropriate choice of the α coefficient in formula (23).

A graph of the dependence of the largest characteristic exponent of the nonlinear system with control from the α coefficient is built to select the α (see Fig. 4). Based on this graph, the α* coefficient is selected that satisfies the desired value of the largest characteristic exponent of the nonlinear system.

After choosing the α* coefficient, the corresponding feedback coefficient k^* is substituted into formula (24) instead of k.

We will illustrate the control synthesis technique for the Rössler system, the model of which in dimensionless variables and parameters has the following form:

$$\begin{cases} \dot{x}_1 = -\left(x_2 + x_3\right) \\ \dot{x}_2 = x_1 + ax_2 \\ \dot{x}_3 = b + x_3\left(x_1 - c\right) \end{cases} \Leftrightarrow \dot{x}(t) = F\left(x(t)\right).$$

The Rössler system, with the $a = 0.2$, $b = 0.2$, $c = 5.7$ values of the parameters, has two singular points:

$$x1^* = \left(0.0070 \quad -0.0351 \quad 0.0351\right),$$
$$x2^* = \left(5.6930 \quad -28.4649 \quad 28.4649\right),$$

and the Jacobi matrix equals:

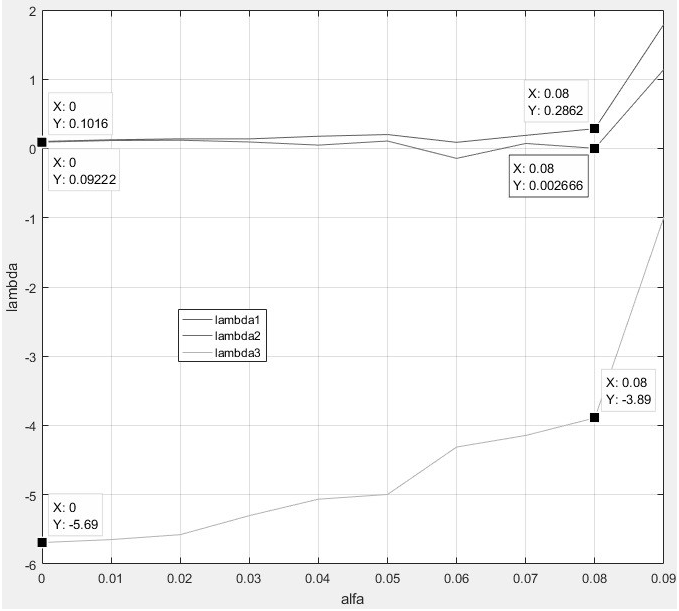

Fig. 4. Dependence of the largest Lyapunov characteristic exponent χ_1 on α

$$J = \begin{bmatrix} 0 & -1 & -1 \\ 1 & a & 0 \\ x_3 & 0 & x_1 - c \end{bmatrix}.$$

Eigenvalues of the Jacobi matrix calculated at singular points are:

$$v\left(J\left(x1^*\right)\right) = \begin{cases} v_1 = 0.0970 + 0.9952i \\ v_2 = 0.0970 - 0.9952i, \\ v_3 = -5.6870 \end{cases}$$

$$v\left(J\left(x2^*\right)\right) = \begin{cases} v_1 = 5.4280i \\ v_2 = -5.4280i. \\ v_3 = 0.1930 \end{cases}$$

We will change the eigenvalues of the Jacobian at the hyperbolic singular point $x1^*$. The desired eigenvalues of the Jacobian (25) of the closed system calculated at $x1^*$ point are determined by equality (23). Fig. 4 shows the graph of the dependence of the largest Lyapunov characteristic exponent of the nonlinear system (7) on α.

According to the graph shown in Fig. 4, we select the $a^* = 0.08$ value of the coefficient at which the condition $\chi_1^* > \chi_1\left(F\right)$ is fulfilled. Using the selected $a^* = 0.08$ value, we calculate the required eigenvalue of the Jacobian, and using formula (22) we calculate the feedback coefficient in the nonlinear system:

$$k^* = \left(1.0426 \quad -0.4943 \quad -22.8945\right).$$

Spectrum (8) of a nonlinear system (7) with synthesized control is equal to:

$$\sigma\left(F + bk^*\right) = \left\{\chi_1 = 0.2862; \chi_2 = 0.0026; \chi_3 = -3.8931\right\}.$$

The largest indicator of a closed system is 2.82 times higher than the largest indicator of the original system, which indicates an increase in chaos in the system.

Properties of an encryption algorithm based on controlled chaos

The strength of the encryption algorithm based on a chaotic feedback system is estimated according to the same criteria of statistical and differential cryptanalysis that were used when testing the algorithm with no control, namely: the probability of gray intensity distribution was calculated by formula (16); correlation coefficients – according to formulas (17); information entropy – according to formula (18), and the percentage of changed pixels and average change in gray color intensity – according to formulas (19) and (20), respectively. The results of testing the encryption algorithm with control are shown in Table 1.

It follows from the above test results that all the compared cryptographic strength criteria are improved when using an encryption algorithm with the control in comparison with an algorithm with no control.

Conclusion

An algorithm for encrypting a grayscale image based on the use of a three-dimensional chaotic map, which implements simultaneous randomization and scattering, is presented. To increase the cryptographic strength of the algorithm, a method for synthesizing feedback on the phase vector of a nonlinear system is proposed, which ensures an increase in the largest Lyapunov characteristic exponent responsible for the degree of chaos. The synthesis technique is based on the modal control method using the canonical Frobenius form, which is extended to nonlinear chaotic systems.

The use of the proposed algorithm is considered using the example of the Rössler system. The test results confirmed an increase in the strength of the proposed encryption algorithm against statistical and differential analysis due to an increase in the Lyapunov characteristic exponent, which is achieved by introducing feedback into the chaotic system used for encryption.

REFERENCES

1. **Sidorenko A.V., Shakinko I.V., Sidorenko Yu.V.** Algoritm shifrovaniya izobrazheniy s ispolzovaniyem dvumernykh khaoticheskikh otobrazheniy [Image encryption algorithm using two-dimensional chaotic maps]. *Sistemnyy analiz i prikladnaya informatika* [*System analysis and applied information science*], 2016, No. 2, Pp. 44–49. (rus)

2. **Sidorenko A.S., Shishko M.S.** Shifrovaniye izobrazheniy na osnove khaoticheskikh otobrazheniy s ispolzovaniyem parallelnykh vychisleniy [Encryption of images on the basis of chaotic mapping and parallel computing]. *Informatika* [*Informatics*], 2017, No. 4(56), Pp. 78–88. (rus)

3. **Novitskiy V.V., Tsvetkov V.Yu.** Szhatiye polutonovykh izobrazheniy na osnove klasterizatsii i progressivnogo vlozhennogo kodirovaniya veyvlet-koeffitsiyentov [Halftone image compression based on clustering and progressive nested encoding of wavelet coefficients]. *Telekommunikatsii: Seti i Tekhnologii, Algebraicheskoye Kodirovaniye i Bezopasnost Dannykh, Materialy nauchno-tekhnicheskogo seminara* [*Materials of the Scientific and Technical Seminar on Telecommunications: Networks and Technologies, Algebraic Coding and Data Security*], Minsk, BGUIR, 2015, Pp. 45–51. (rus)

4. **Sidorenko A.V., Mulyarchuk K.S.** Shifrovaniye dannykh s ispolzovaniyem khaoticheskoy dinamiki v sensornoy seti [ATA encryption using the chaotic dynamics in wireless sensor networks]. *Doklady BGUIR*, 2015, Vol. 92, No. 6, Pp. 41–47. (rus)

5. **Sidorenko A.V., Mulyarchuk K.S.** Shifrovaniye dannykh na osnove diskretnykh khaoticheskikh sistem i otobrazheniy [The data encryption based on discrete chaotic systems and maps]. *Doklady BGUIR*, 2013, Vol. 71, No. 1, Pp. 62–67. (rus)

6. **Burkin I.M.** Ob odnoy sisteme tretyego poryadka s 3-D reshetkoy khaoticheskikh attraktorov [On a third-order system with a 3-D lattice of chaotic attractors]. *Vestnik YeGU. Differentsialnyye uravneniya i prikladnyye zadachi* [*TSU Bulletin. Differential equations and applied problems*], 2020, No. 1, Pp. 3–8. (rus)

7. **Gulyayev Yu.V., Belyayev R.V., Vorontsov G.M., et al.** Informatsionnyye tekhnologii na osnove khaoticheskoy dinamiki dlya peredachi, obrabotki, khraneniya i zashchity informatiki [Dynamic-chaos information technologies for data transmission, storage, and protection]. *Informatsionnyye tekhnologii, RENSIT* [*Information technology, RENSIT*], 2018, Vol. 10, No. 2, Pp. 279–312. (rus). DOI: 10.17725/rensit.2018.10.279

8. **Ten T.A., Beysenbi M.A., Kogay G.D.** *Kriptograficheskiye sistemy po upravleniyu khaosom: Monografiya* [*Cryptographic systems for managing deterministic chaos*]. Gamburg: LAP LAMBERT Academic Publishing, 2014. 228 p. (rus)

9. **Sidorenko A.S., Shishko M.S.** Shifrovaniye izobrazheniy na osnove khaoticheskoy dinamiki s elementami geneticheskogo algoritma [The image encryption based on chaotic dynamics and genetic algorithm elements]. *Informatika* [*Informatics*], 2018, Vol. 29, No. 1, Pp. 95–100. (rus)

10. **Shashikhin V.N., Budnik S.V.** *Upravleniye krupnomasshtabnymi dinamicheskimi sistemami* [*Managing large-scale dynamic systems*]. St. Petersburg: POLITEKhPRESS, 2020. 308 p. (rus)

11. **Grobman D.** Gomeomorfizm sistem differentsialnykh uravneniy [Homeomorphism of systems of differential equations]. *DAN SSSR*, 1959, Vol. 128, No. 5, Pp. 880–881. (rus)

12. **Budnik S.V., Shashikhin V.N.** Upravleniye khaoticheskoy dinamikoy nelineynykh sistem [Control of chaotic dynamics of nonlinear systems]. *XXIII Mezhdunarodnaya nauchnaya uchebno-prakticheskaya konferentsiya "Sistemnyy analiz v proyektirovanii i upravlenii"* [*XXIII International Scientific Educational and Practical Conference on System Analysis in Design and Management*], St. Petersburg, 2019, Pp. 12–19. (rus)

13. **Chen P.** A fast image encryption based on chaotic map and lookup table. *Nonlinear Dynamics*, 2015, Vol. 79, No. 3, Pp. 2121–2131.

14. **Seyedzadeh S.M., Norouzi B., Mirzakuchaki S.** RGB image encryption algorithm based on choquet fuzzy integral. *The Journal of Systems and Software*, 2014, Vol. 97, No. 11, Pp. 128–139.

15. **Faraoun K.M.** A parallel block-based encryption schema for digital images using reversible cellular automata. *Engineering Science*, 2014, Vol. 17, Pp. 85–94.

16. **Behnia S., Akhshani A., Mahmodi H.** Applications of tripled chaotic maps in cryptography. *Chaos, Solitons & Fractals*, 2009, Vol. 40, No. 1, Pp. 505–519.

17. **Li C., Luo G., Qim K.** An image encryption scheme based on chaotic map. *Nonlinear Dynamics*, 2017, Vol. 87, No. 3, Pp. 127–136.

18. **Jaryal S., Marwaha C.** Comparative analysis of various image encryption techniques. *International Journal of Computational Intelligence Research*, 2017, Vol. 13, No. 2, Pp. 273–286.

19. **Xu L., Li Z., Li J.** A novel bit-level image encryption based on chaotic map. *Optics and Lasers in Engineering*, 2016, Vol. 78, No. 3, Pp. 17–25.

20. **Kanso A., Ghebleh M.** A robust chaotic algorithm for digital image. *Communications in Nonlinear Science and Numerical Simulation*, 2014, Vol. 19, No. 6, Pp. 1898–1907.

21. **Xiuli C., Xiaoyu Z., Zhihua G.** An image encryption algorithm based on chaotic system and compressive sensing. *Signal Processing*, 2018, Vol. 148, No. 7, Pp. 124–144.

22. **Kaur M., Singh D., Sun K.** Color image encryption using non-dominated sorting generated algorithm with local chaotic search based 5D chaotic map. *Future Generation Computer Systems*, 2020, Vol. 107, No. 6, Pp. 333–350.

23. **Rossler O.E.** An equation for continuous chaos. *Physics letters*, 1976, Vol. 57, No. 5. Pp. 397–398.

Received 14.02.2021.

СПИСОК ЛИТЕРАТУРЫ

1. **Сидоренко А.В., Шакинко И.В., Сидоренко Ю.В.** Алгоритм шифрования изображений с использованием двумерных хаотических отображений // Системный анализ и прикладная информатика. 2016. № 2. С. 44–49.

2. **Сидоренко А.С., Шишко М.С.** Шифрование изображений на основе хаотических отображений с использованием параллельных вычислений // Информатика. 2017. № 4(56). С. 78–88.

3. **Новицкий В.В., Цветков В.Ю.** Сжатие полутоновых изображений на основе кластеризации и прогрессивного вложенного кодирования вейвлет-коэффициентов // Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных: Матер. науч.-техн. Семинара. Минск, БГУИР, 2015. С. 45–51.

4. **Сидоренко А.В., Мулярчук К.С.** Шифрование данных с использованием хаотической динамики в сенсорной сети // Доклады БГУИР. 2015. Т. 92. № 6. С. 41–47.

5. **Сидоренко А.В., Мулярчук К.С.** Шифрование данных на основе дискретных хаотических систем и отображений // Доклады БГУИР. 2013. Т. 71. № 1. С. 62–67.

6. **Буркин И.М.** Об одной системе третьего порядка с 3-D решеткой хаотических аттракторов // Вестник ЕГУ. Дифференциальные уравнения и прикладные задачи. 2020. № 1. С. 3–8.

7. **Гуляев Ю.В., Беляев Р.В. Воронцов Г.М. и др.** Информационные технологии на основе хаотической динамики для передачи, обработки, хранения и защиты информатики // Информационные технологии. РЭНСИТ. 2018. Т. 10. № 2. С. 279–312.

8. **Тен Т.А., Бейсенби М.А., Когай Г.Д.** Криптографические системы по управлению хаосом: Монография. Гамбург: LAP LAMBERT Academic Publishing, 2014. 228 с.

9. **Сидоренко А.С., Шишко М.С.** Шифрование изображений на основе хаотической динамики с элементами генетического алгоритма // Информатика. 2018. Т. 29. № 1. С. 95–100.

10. **Шашихин В.Н., Будник С.В.** Управление крупномасштабными динамическими системами. СПб.: ПОЛИТЕХПРЕСС, 2020. 308 с.

11. **Гробман Д.** Гомеоморфизм систем дифференциальных уравнений // ДАН СССР. 1959. Т. 128. № 5. С. 880–881.

12. **Будник С.В., Шашихин В.Н.** Управление хаотической динамикой нелинейных систем // XXIII Междунар. науч. учеб.-практич. конф. «Системный анализ в проектировании и управлении». Санкт-Петербург, 10-11 июня 2019. С. 12–19.

13. **Chen P.** A fast image encryption based on chaotic map and lookup table // Nonlinear Dynamics. 2015. Vol. 79. No. 3. Pp. 2121–2131.

14. **Seyedzadeh S.M., Norouzi B., Mirzakuchaki S.** RGB image encryption algorithm based on choquet fuzzy integral // The J. of Systems and Software. 2014. Vol. 97. No. 11. Pp. 128–139.

15. **Faraoun K.M.** A parallel block-based encryption schema for digital images using reversible cellular automata // Engineering Science. 2014. Vol. 17. Pp. 85–94.

16. **Behnia S., Akhshani A., Mahmodi H.** Applications of tripled chaotic maps in cryptography // Chaos, Solitons & Fractals. 2009. Vol. 40. No. 1. Pp. 505–519.

17. **Li C., Luo G., Qim K.** An image encryption scheme based on chaotic map // Nonlinear Dynamics. 2017. Vol. 87. No. 3. Pp. 127–136.

18. **Jaryal S., Marwaha C.** Comparative analysis of various image encryption techniques // Internat. J. of Computational Intelligence Research. 2017. Vol. 13. No. 2. Pp. 273–286.

19. **Xu L., Li Z., Li J.** A novel bit-level image encryption based on chaotic map // Optics and Lasers in Engineering. 2016. Vol. 78. No. 3. Pp. 17–25.

20. **Kanso A., Ghebleh M.** A robust chaotic algorithm for digital image // Communications in Nonlinear Science and Numerical Simulation. 2014. Vol. 19. No. 6. Pp. 1898–1907.

21. **Xiuli C., Xiaoyu Z., Zhihua G.** An image encryption algorithm based on chaotic system and compressive sensing // Signal Processing. 2018. Vol. 148. No. 7. Pp. 124–144.

22. **Kaur M., Singh D., Sun K.** Color image encryption using non-dominated sorting generated algorithm with local chaotic search based 5D chaotic map // Future Generation Computer Systems. 2020. Vol. 107. No. 6. Pp. 333–350.

23. **Rossler O.E.** An equation for continuous chaos // Physics letters. 1976. Vol. 57. No. 5. Pp. 397–398.

Статья поступила в редакцию 14.02.2021.

THE AUTHORS / СВЕДЕНИЯ ОБ АВТОРАХ

Shashikhin Vladimir N.
Шашихин Владимир Николаевич
E-mail: shashihin@bk.ru

Turulin Aleksandr V.
Турулин Александр Владимирович
E-mail: sanya.turulin.98@list.ru

Budnik Svetlana V.
Будник Светлана Владимировна
E-mail: budnik.sveta@mail.ru