IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 36, No. 1, February, 2019, pp. 31-36
Journal homepage: http://iieta.org/Journals/ts

A Secure Image Encryption Algorithm Based on Composite Chaos Theory

Qiuru Cai

School of Computer Engineering Jiangsu University of Technology, Changzhou 213001, China

Corresponding Author Email: cai_qiuru@sina.com

https://doi.org/10.18280/ts.360104

Received: 30 October 2018
Accepted: 13 January 2019

Keywords:
image encryption, permutation, diffusion, composite chaotic system

ABSTRACT

This paper introduces chaotic image encryption to realize the secure transmission of digital images, and combines 1D and 3D chaotic systems into an image encryption algorithm. Firstly, two sets of logistic chaotic sequences were generated iteratively for pixel permutation, so were the initial values of the Bao system. Then, the chaotic sequence for pixel permutation and diffusion was generated based on the plaintext pixel value and Bao system. After that, the plaintext image was encrypted and decrypted by encryption and decryption formulas. Finally, the encryption process was simulated, and the algorithm performance was analyzed in terms of key space and correlation of adjacent pixels. The results show that our algorithm achieved better security than the traditional methods.

1. INTRODUCTION

The development of network technology has given birth to images with huge data volume, high redundancy and strong correlation, which are increasingly important in such fields as business, military and medical aid. Therefore, more and more attention has been paid to protect the security of image transmission. Among the various security protection methods, the most easy, reliable and effective way is to encrypt the digital information of the target image before transmission and decrypt the information after transmission. The existing image encryption techniques, ranging from partial encryption, complete encryption to scrambling [1, 2], attempt to make the image exhibit a chaotic, disordered, noisy state, such that the attacker can never extract information of the image.

Most of the mature encryption algorithms are developed for encryption of text information, namely, the Advanced Encryption Standard (AES) and Data Encryption Standard (DES). However, image, as the encryption target, differs from text in many aspects. For example, the adjacent pixels often have strong correlation and high redundancy. If directly applied to image, the existing encryption algorithms may suffer from heavy computation and low efficiency, failing to satisfy the real-time demand of image transmission. What is worse, the traditional algorithms might destroy the storage mode of the original image.

To solve the above problem, this paper designs a secure image encryption algorithm based on composite chaos theory. Chaos is a complex dynamic behavior in nonlinear dynamical systems [3]. It reflects the inherent randomness of deterministic systems and carries natural similarities with cryptography. Thus, the chaos theory has been applied widely in image encryption. Compared with the traditional encryption, the chaotic encryption focuses on the generation of encryption sequence rather than the algorithm, and highlights the selection of proper chaotic system to generate a highly random sequence. This encryption approach is much more efficient and secure for images than the traditional algorithms.

2. LITERATURE REVIEW

The chaotic encryption was first proposed by Matthew in 1989 [4]. Later, Jakimoski et al. [5] developed a chaotic encryption structure of confusion and diffusion; the former disturbs the pixel position to eliminate the correlation between adjacent pixels, and the latter restores the even distribution of the pixel values. This structure has been accepted as a classical framework of chaotic image encryption.

The chaotic image encryption algorithms roughly fall into four categories: low-dimensional chaotic system, multi-dimensional chaotic system, hyper-chaotic system and composite chaotic system. The low-dimensional chaotic system stands out with simplicity and ease of implementation. Typical examples include logistic mapping [6], tent mapping [7] and Chebyshev mapping [8]. However, the low-dimensional chaotic system cannot withstand decoding attacks like spectrum analysis and phase space reconstruction. After all, the system has too few control parameters and a small key space.

To solve the defect, many scholars have designed high-dimensional chaotic system with complex dynamic features, such as Lorenz system [9], Chen system [10] and Bao system [11]. These high-dimensional chaos systems can effectively curb common attacks like phase space reconstruction. Nonetheless, the emerging chosen plaintext attack goes beyond the capacity of these systems. With a few plaintext pairs, the attacker can decipher the control parameters of the high-dimensional chaos systems.

In recent years, the chaos theory has been integrated with the concepts and theories of other disciplines for image encryption. For instance, Reference [12] puts forward a quantum chaotic encryption system in conjunction with quantum mechanics. Reference [13] design image encryption algorithms based on DNA encoding. Reference [14] presents a hybrid algorithm for image compression and encryption. These integrated methods greatly enrich the theory of chaotic image encryption.

For secure and efficient encryption, composite chaotic encryption algorithms have been created [15-17], either coupling low- and high-dimensional chaos or integrating low- and hyper-dimensional chaos. Two or more chaotic systems can complement each other. Their coupling can protect chaotic orbit information, reduce the computing complexity and support real-time communication. Seyedzadeh et al. [18] combined three chaotic maps, i.e. Logistic, Arnold and Kent, into a multi-chaotic fast encryption algorithm, which achieves good encryption effect at the expense of a small key space. Haroun et al. [19] formulated a composite encryption algorithm of low- and multi-dimensional chaos, which has good random sequence but weak differential resistance. To improve the encryption performance, it is necessary to combine hyper- and multi-dimensional chaotic systems properly, and design a rational plaintext association strategy.

3. DIGITAL IMAGE ENCRYPTION BASED ON CHAOS THEORY

3.1 Judgment of chaos

To judge if a system is chaotic, an important criterion is the Lyapunov exponent, which can determine the local stability of the orbit of a dynamical system.

Let $x_{n+1} = f(x_n)$ and $y_{n+1} = f(y_n)$ be the two state equations of a 1D discrete chaotic system, and $|x_0 - y_0|$ be the error of the initial values of the two state equations. After one iteration, the error can be expressed as: $|x_1 - y_1| = |f(x_0) - f(y_0)| \approx \left|\frac{df}{dx}|_{x_0}\right| \cdot |x_0 - y_0|$, where $\left|\frac{df}{dx}|_{x_0}\right| = \lim_{x_0 \to y_0} \frac{|f(x_0)-f(y_0)|}{|x_0-y_0|}$.

Then, the error after the second iteration is $|x_2 - y_2| \approx \left|\frac{df}{dx}|_{x_0} \cdot \frac{df}{dx}|_{x_1}\right| \cdot |x_0 - y_0|$.

The error after the *n*-th iteration is $|x_n - y_n| \approx \left|\prod_{n=0}^{n-1} \frac{df}{dx}|_{x_n}\right| \cdot |x_0 - y_0|$.

The mean deviation value of each iteration is $\left|\prod_{n=0}^{n-1} \frac{df}{dx}|_{x_n}\right|^{1/n}$.

The deviation will occur with the elapse of time, if there is an error in the initial errors of the two state equations. The degree of deviation can be expressed as:

$$\lambda = \frac{1}{n} \ln\left(\left|\prod_{n=0}^{n-1} \frac{df}{dx}|_{x_n}\right|\right) \quad (1)$$

where x_n is the *n*-th iteration error of the system. When $n \to \infty$, the Lyapunov exponent λ can be calculated by:

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{n=0}^{n-1} \ln\left|\frac{df}{dx}|_{x_n}\right| \quad (2)$$

The Lyapunov index measures the divergence/convergence speed of the system. If λ is positive, then the Lyapunov exponent is divergent; if it is negative, then the index is convergent.

For multi-dimensional chaotic systems, Eq. (2) should be replaced with the Jacobian matrix, which can compute the Lyapunov exponents of multi-dimensional chaotic systems more accurately.

For an m-dimensional chaotic system, the system equation can be expressed as:

$$\begin{cases} x_{n+1} = f_1(x_n, y_n, \dots, z_n) \\ y_{n+1} = f_2(x_n, y_n, \dots, z_n) \\ \quad \dots \dots \\ z_{n+1} = f_m(x_n, y_n, \dots, z_n) \end{cases} \quad (3)$$

The Jacobian matrix of the system equation is:

$$J = \begin{bmatrix} \frac{\partial f_1}{\partial x_n} & \frac{\partial f_1}{\partial y_n} & \dots & \frac{\partial f_1}{\partial z_n} \\ \frac{\partial f_2}{\partial x_n} & \frac{\partial f_2}{\partial y_n} & \dots & \frac{\partial f_2}{\partial z_n} \\ & \dots \dots & & \\ \frac{\partial f_m}{\partial x_n} & \frac{\partial f_m}{\partial y_n} & \dots & \frac{\partial f_m}{\partial z_n} \end{bmatrix} \quad (4)$$

Given the initial value of the system equation ($x_0, y_0, \dots, z_0$), the first *n-1* Jacobian matrix can be obtained as:

$$J_0 = J(x_0, y_0, \dots, z_0), J_1 = J(x_1, y_1, \dots, z_1), \\ \dots, J_{n-1} = J(x_{n-1}, y_{n-1}, \dots, z_{n-1}) \quad (5)$$

Then, each Lyapunov exponent of the system can be calculated as:

$$\lambda_1 = \frac{1}{n}\sum_{i=0}^{n-1} ln\, \lambda_{1i}, \lambda_2 = \frac{1}{n}\sum_{i=0}^{n-1} ln\, \lambda_{2i}, \\ \dots, \lambda_m = \frac{1}{n}\sum_{i=0}^{n-1} ln\, \lambda_{mi} \quad (6)$$

where λ_{1i}, λ_{2i}, …, λ_{mi} ($i \in [0, n-1]$) is the eigenvalue of each Jacobian matrix; λ_1, λ_2, …, λ_m are Lyapunov exponents of m-dimensional system.

To judge if a system is chaotic, the first step is to compute all the Lyapunov exponents of the system. If the maximum Lyapunov exponent is positive, the system is chaotic; otherwise, it is not chaotic. Out of the many Lyapunov exponents, there may be more than one positive exponent for multi-dimensional systems. If so, the system is hyper-chaotic.

3.2 Basic design method of chaotic encryption algorithm

The information of a digital image mainly covers two aspects: the value and the position of pixels, the smallest unit of an image. The pixel value generally falls in the interval [0,255]. The pixel position, i.e. the arrangement of all the pixel values, is basically unique. Hence, the key of an image encryption algorithm is to cover up the pixel value and pixel position of the target image.

Popular image encryption algorithms include the pixel value permutation [20] and the position permutation [21]. Here, permutation is a way to make the image visually chaotic. It refers to disrupting the original order of image pixels and reducing the correlation of adjacent pixels as much as possible, making it impossible to get useful information through the senses.

Generally, the information of an image can be represented as a 2D matrix. Each element in the matrix corresponds to each pixel in each image, including their position and size. For an image of the size M×N, its corresponding M×N matrix can be defined as:

$$P = \begin{pmatrix} P_{0,0} & P_{0,1} & \dots \dots & P_{0,N-1} \\ \dots \dots & \dots \dots & P_{i,j} & \dots \dots \\ P_{M-1,0} & \dots \dots & \dots \dots & P_{M-1,N-1} \end{pmatrix} \\ i \in [0, M-1], j \in [0, N-1] \quad (7)$$

where $P_{i,j}$ are the pixel values of i-th row and j-th column of the image. The essence of permutation is to transform the rows and columns in the matrix of Eq. (7), that is, changing the rules of pixel placement of the whole image. For example, a 512×512 image was subjected to Arnold transform for 0, 1, 3, 7, 356, 370, 373 and 374 times in turn. The results are presented in Figure 1 below.

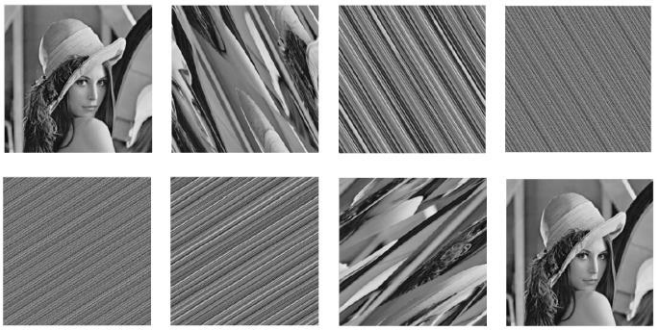

Figure 1. Example images of permutation

However, permutation can only conceal the image visually, instead of changing the statistical features. Taking a gray histogram for instance, the permutation will reduce the pixel correlation, but not sufficient to completely remove the relevance. This requires the complete change to the values and statistical features of image pixels, which is known as pixel replacement. Generally, the original information of plaintext is changed by simple addition, multiplication or exclusion. If the selected key sequence enjoys good randomness, there will be no correlation between the pixels. Through diffusion, the effect of the change of a single plaintext or key can spread to the whole image.

4. COMPOSITE IMAGE ENCRYPTION BASED ON LOGISTIC MAPPING AND BAO SYSTEM

4.1 Composite chaotic system theory

The image encryption algorithm based on single chaotic system has the problems of small key space and low security. Once a chaotic system fails to meet the requirements, it should be replaced with multiple chaotic systems. This idea is applied to composite chaotic encryption. As a result, this paper proposes an image encryption algorithm combining 1D and 3D chaotic systems.

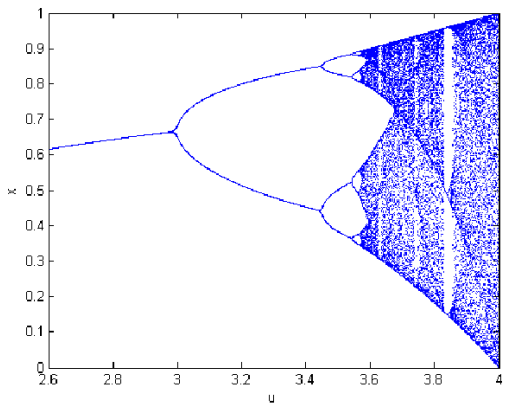

Figure 2. Logistic mapping bifurcation graph

The system equation of logistic mapping, the most common 1D chaotic system, can be expressed as:

$$x_{n+1} = \mu x_n(1 - x_n) \tag{8}$$

where $x \in [0,1]$. When $2.5<\mu<3$, the system presents a chaotic state (Figure 2).

The system equation of 3D Bao system, a continuous autonomous dissipative system with a quadratic nonlinearity term, can be expressed as:

$$\begin{cases} x' = \alpha(x_n - y_n) \\ y' = xz - \gamma y \\ z' = x^2 - \beta z \end{cases} \tag{9}$$

Being a continuous chaotic system, the system should be discretized before application. Here, the fourth-order Runge-Kutta algorithm [22, 23] is used to discretize Bao system. The equation of the discretized system can be expressed as:

$$\begin{cases} x_{n+1} = x_n + h(f_{x1} + 2f_{x2} + 2f_{x3} + f_{x4})/6 \\ y_{n+1} = y_n + h(f_{y1} + 2f_{y2} + 2f_{y2} + f_{y4})/6 \\ z_{n+1} = z_n + h(f_{z1} + 2f_{z2} + 2f_{z2} + f_{z4})/6 \end{cases} \tag{10}$$

The system shows a chaotic state, when the controller parameters $\alpha=20$, $\beta=3$ and $\gamma=32$. Figure 3 shows the trajectory map of the 3D Bao system when the initial value of (x, y, z) is (10, 10, 10), the step length is h=0.001, and the number of iterations n=5,000.

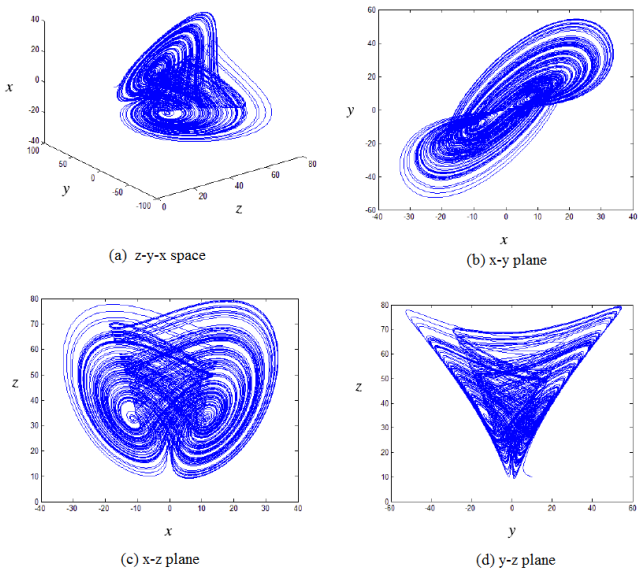

Figure 3. Trajectory map of 3D Bao system

4.2 Algorithm design

To set up the chaos-based image encryption algorithm, the initial value of the system should be determined to generate chaotic sequences. Then, these sequences should be processed and modified to obtain the sequence suitable for image encryption. After that, it is necessary to design the formulas of pixel permutation, replacement and diffusion. Let M×N be the size of the target image, and $p_{i,j}$ be the pixel value of i-th row and j-th column.

Step 1: Determine the two initial values of logistic mapping

system. First, perform N iterations on the system to prevent the transition effect. Then, generate two chaotic sequences, $\{X_{i=0}^{M-1}\}$ and $\{Y_{j=0}^{N-1}\}$, with length M and N through M and N iterations, respectively. Next, extract the N_1-th, N_2-th and N_3-th iteration values from both sets of sequences, and calculate the initial values x_{bao}, y_{bao} and z_{bao} of x, y and z parameters of Bao system.

$$\begin{cases} x_{bao} = (X_{N_1} + Y_{N_2})/2 \times 10 \\ y_{bao} = (X_{N_2} + Y_{N_2})/2 \times 10 \\ z_{bao} = (X_{N_3} + Y_{N_3})/2 \times 10 \end{cases} \quad (11)$$

The initial value of the chaotic system and the selected sequence pair can be used as the key in the algorithm design.

Step 2: Calculate by the two chaotic sequences.

$$X_i = mod((fabs(X_i) - floor(fabs(X_i)) \times 10^{14}), M) \quad (12)$$

$$Y_j = mod((fabs(Y_j) - floor(fabs(Y_j)) \times 10^{14}), N) \quad (13)$$

where $fabs()$ is an absolute value function for finding a floating-point number; $floor()$ is to find the maximum integer function that does not exceed the number itself; $X_i \in [0, M-1]$; $Y_i \in [0, N-1]$. Swap the pixel values of point (i, j) with those of point (X_i , Y_j):

$$P_{i,j} = P_{X_i,Y_j} \quad (14)$$

Perform the swap on all pixels in turn to complete the replacement.

Step 3: Input the x_{bao}, y_{bao} and z_{bao} into the Bao system. Iterate the chaotic system by the Runge-Kutta algorithm, such that a set of new values (b_1, b_2, b_3) is generated from the Bao system in each iteration. Denote the processed sequence as $\{B_k\}_{i=0}^{M\times N-1}$.

Step 4: Calculate the following formulas.

$$\begin{aligned} b_{i+1} &= mod((fabs(x_i) - floor(fabs(x_i)) \times 10^{14}), 256) \\ b_{i+2} &= mod((fabs(y_i) - floor(fabs(y_i)) \times 10^{14}), 256) \\ b_{i+3} &= mod((fabs(z_i) - floor(fabs(z_i)) \times 10^{14}), 256) \end{aligned} \quad (15)$$

Then, compute the value of $t = \mathrm{mod}(P_{i,j}, 3)$. If $t = 0$, insert b_{i+1}, b_{i+2} and b_{i+3} into B_k in turn; if $t = 1$, insert b_{i+2}, b_{i+3} and b_{i+1} into B_k in turn; if $t = 2$, insert b_{i+3}, b_{i+1} and b_{i+2} into B_k in turn. Repeat this process until M×N-1 b_i values are generated.

Step 5: Form a sequence of permutated image pixels P_i, and denote encrypted image pixel sequence as C_i . Define replacement and diffusion operations as:

$$C_i = B_k \oplus (\mathrm{mod}(P_i + S, 256)) \oplus C_{i-1} \quad (16)$$

where *S* is the sum of image pixel values. Each encrypted pixel value is related to the previous encrypted pixel value and also to *S*.

Step 6: Repeat the permutation, replacement and diffusion process T times to complete the encryption of the entire image.

5. EXPERIMENTAL SIMULATION AND ANALYSIS

The proposed encryption algorithm was verified through experiments on an 8-bit 256-color image. The initial parameters of logistic mapping system were set as (0.75, 0.85), N_0=500, C_0=120, *S*=11,520 and *T*=3. The encryption effect is presented in Figure 4 below.

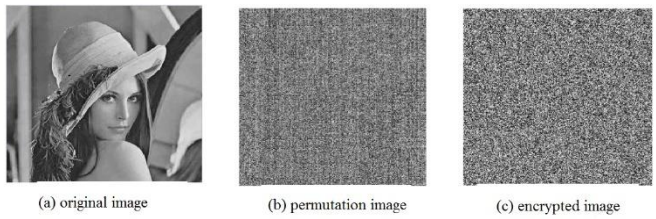

Figure 4. The encryption effect

As shown in Figure 4, the final encrypted image was completely confused, presenting no useful information, after replacement and diffusion to the encrypted image. Figure 5 compares the gray histograms of the original image and he encrypted image. It can be seen that the encrypted image exhibited a uniform distribution of pixel values and basically the same probability of different pixels, while the original image showed an uneven distribution and vastly different probabilities. This means the encrypted image can better resist the attack based on statistical analysis.

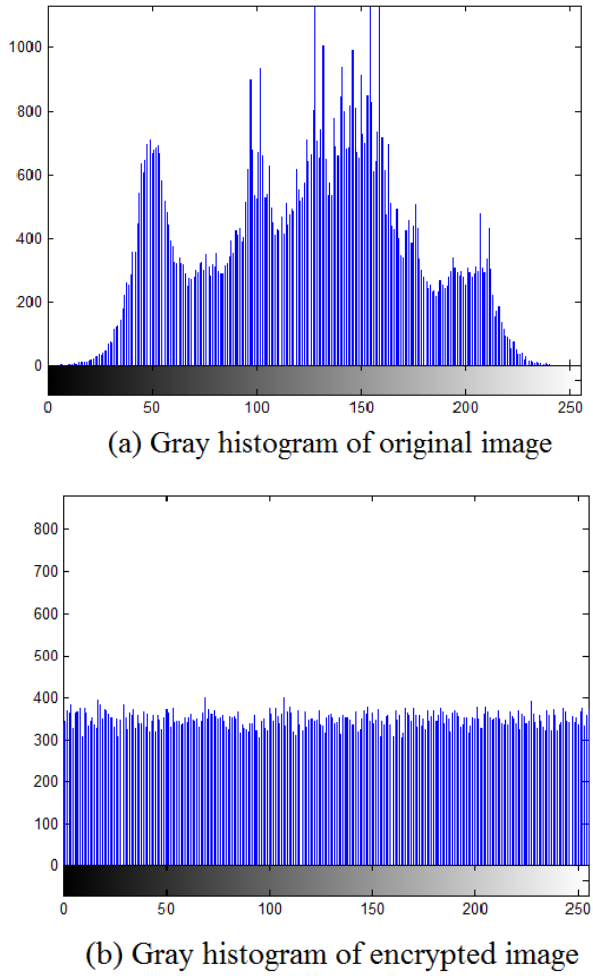

Figure 5. Gray histograms

Next, the horizontal and vertical adjacent pixels before and after image encryption were subjected to correlation analysis. The results are displayed in Figure 6 below.

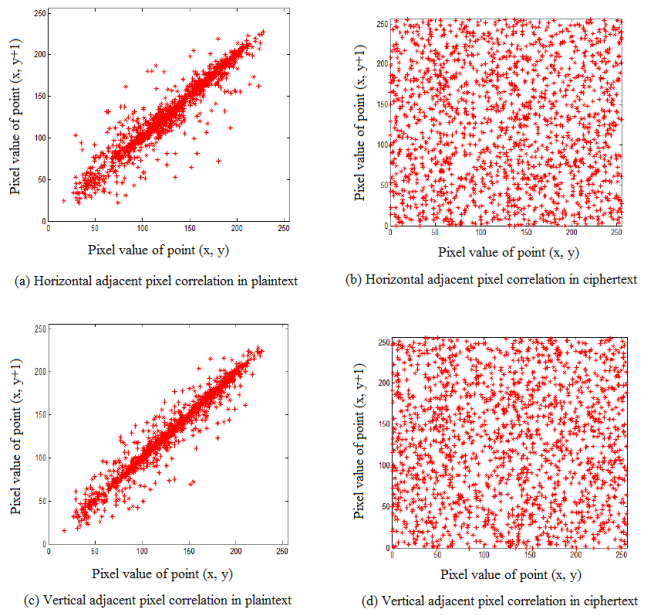

Figure 6. Correlation of horizontal and vertical adjacent pixels before and after encryption

Figure 6 shows a strong linear correlation between both horizontal and vertical adjacent pixels on the pre-encryption image. Meanwhile, the pixel values of the encrypted image were scattered in the space of adjacent pixels, with weak correlation and random distribution.

6. CONCLUSIONS

This paper presents an image encryption algorithm based on 1D and 3D chaotic systems, and verifies the algorithm performance through experiments. The results show that the proposed algorithm boasts a large key space and strong resistance to various attacks, including the statistical analysis by the attacker. Thus, our algorithm can greatly improve the security of chaotic encryption. The future research will further improve our algorithm, trying to achieve security requirements with fewer iterations.

ACKNOWLEDGMENT

Sponsored by the National Natural Science Foundation of China(Grant No. 61401226), the MOE (Ministry of Education in China) Project of Humanities and Social Sciences (Grant No.14YJAZH023), the Basic Research Program of Jiangsu University of Technology (Grant No.KYY14007), the Natural Science Foundation of Universities of Jiangsu province (No. 13KJB520005) and State Key Laboratory of Information Security (Grant No. 2015-MSB-10).

REFERENCES

[1] Norouzi B, Mirzakuchaki S, Seyedzadeh S, Mosavi MR. (2014). A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process. Multimedia Tools & Applications 71(3): 1469-1497. https://doi.org/10.1007/s11042-012-1292-9

[2] Norouzi B, Mirzakuchaki S. (2014). A fast color image encryption algorithm based on hyper-chaotic systems. Nonlinear Dynamics 78(2): 995-1015. https://doi.org/10.1007/s11071-014-1492-0

[3] El-Sayed AMA, Salman SM. (2016). Dynamic behavior and chaos control in a complex Riccati-type map. Quaestiones Mathematicae 39(5): 665-681. https://doi.org/10.2989/16073606.2015.1115441

[4] Matthews R. (1989). On the derivation of a “Chaotic” encryption algorithm. Cryptologia 13(1): 29-42. https://doi.org/10.1080/0161-118991863745

[5] Jakimoski G, Kocarev L. (2001). Analysis of some recently proposed chaos-based encryption algorithms. Physics Letters A 291(6): 381-384. https://doi.org/10.1016/S0375-9601(01)00771-X

[6] Liu B, Liu N, Li JX, Liang W. (2011). Research of image encryption algorithm base on chaos theory. Proceedings of 2011 6th International Forum on Strategic Technology 2: 1096-1098. https://doi.org/10.1109/IFOST.2011.6021211

[7] Wei Y, Dai Y, Zhang Y, Chen J, Ding J. (2013). Adaptive chaotic embedded particle swarm optimization algorithm based on tent mapping. Computer Engineering & Applications 49(10): 45-49.

[8] Yoon EJ, Jeon IS. (2011). An efficient and secure diffie–hellman key agreement protocol based on chebyshev chaotic map. Communications in Nonlinear Science & Numerical Simulation 16(6): 2383-2389. https://doi.org/10.1016/j.cnsns.2010.09.021

[9] Lee KW, Singh SN. (2011). Non-certainty-equivalent adaptive control of chaos in Lorenz system. International Journal of Modelling, Identification and Control 13(4): 310-321. http://dx.doi.org/10.1504/IJMIC.2011.041786

[10] Yassen MT. (2003). Chaos control of Chen chaotic dynamical system. Chaos, Solitons and Fractals 15(2): 271-283. https://doi.org/10.1016/S0960-0779(01)00251-X

[11] Khellat F. (2014). Delayed feedback control of bao chaotic system based on HOPF bifurcation analysis. Journal of Engineering Science & Technology Review 8(2): 7-11. https://doi.org/10.25103/jestr.082.02

[12] Ellatif AAA, Li L, Wang N, Han Q, Niu XM. (2013). A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces. Signal Processing 93(11): 2986-3000. https://doi.org/10.1016/j.sigpro.2013.03.031

[13] Chai X, Gan Z, Lu Y, Chen YR, Han D. (2017). A novel image encryption algorithm based on the chaotic system and DNA computing. International Journal of Modern Physics C 28(5): 1-13. https://doi.org/10.1142/S0129183117500693

[14] Zhang Y, Xu B, Zhou N. (2017). A novel image compression–encryption hybrid algorithm based on the analysis sparse representation. Optics Communications 392: 223-233. https://doi.org/10.1016/j.optcom.2017.01.061

[15] Liu Z, Zeng G, Xie FS. (2012). Chaotic image encryption method based on pixel value composite scrambling. Computer Engineering & Applications 48: 122-126. https://doi.org/10.3778/j.issn.1002-8331.2012.25.026

[16] Sun G, Bin S. (2018). A new opinion leaders detecting algorithm in multi-relationship online social netwoks. Multimedia Tools and Applications 77(4): 4295-4307.

[17] Zhu H, Zhang X, Yu H. (2016). A novel image encryption scheme using the composite discrete chaotic system. Entropy 18(8): 276-289. https://doi.org/10.3390/e18080276
[18] Seyedzadeh SM, Mirzakuchaki S. (2012). A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map. Signal Processing 92(5): 1202-1215. https://doi.org/10.1016/j.sigpro.2011.11.004
[19] Haroun MF, Gulliver TA. (2015). Real-time image encryption using a low-complexity discrete 3D dual chaotic cipher. Nonlinear Dynamics 82(3): 1523-1535. https://doi.org/10.1007/s11071-015-2258-z
[20] Li Y, Wang C, Chen H. (2017). A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. Optics & Lasers in Engineering 90: 238-246. https://doi.org/10.1016/j.optlaseng.2016.10.020
[21] Lang J. (2015). Color image encryption based on color blend and chaos permutation in the reality-preserving multiple-parameter fractional Fourier transform domain. Optics Communications 338(338): 181-192. https://doi.org/10.1016/j.optcom.2014.10.049
[22] Yang D, Wang N, Chen S, Song GJ. (2009). An explicit method based on the implicit runge-kutta algorithm for solving wave equations. Bulletin of the Seismological Society of America 99(6): 3340-3354. https://doi.org/10.1785/0120080346
[23] Sun G, Bin S. (2017). Router-level internet topology evolution model based on multi-subnet composited complex network model. Journal of Internet Technology 18(6): 1275-1283.