IMAGE ENCRYPTION ALGORITHM FOR TORSIONAL COMPONENTS OF GENERATOR BASED ON COMPOUND CHAOTIC MODEL

by

Yu SHAO

School of Electronic and Information Engineering, SIAS International University, XinZheng, China

Original scientific paper
https://doi.org/10.2298/TSCI190717078S

In order to solve the problem that the image encryption algorithm cannot eliminate the strong correlation between adjacent pixels in the image, with poor ability to resist attack and low efficiency, an Image encryption algorithm for torsional components of generators based on complex chaotic model is proposed. Extracting the RGB torsional vibration component of the image for discrete cosine transform transformation, it is then rotated and fused to complete the initial encryption of the image information. In order to further enhance the security of image information, 2-D discrete cosine transform and 2-D compressed sensing measurement are applied to the initial encrypted image information. The real number matrix of measurement is merged into the complex value matrix, and the adaptive random phase coding is applied. The image information complex chaotic encryption model is constructed according to the coding result, so as to eliminate the strong correlation between the adjacent pixels. Particle swarm optimization is used to co-ordinate and optimize the parameters of the compound chaotic encryption model to improve the encryption performance of the model. Experimental results show that the pixel has low correlation, high security and strong ability to resist attacks after encrypting with this algorithm.

Key words: *compound chaotic encryption, component fusion, image encryption, discrete cosine transform, generator torsion member image*

Introduction

The increasing frequency of information exchange has been prompted to transfer from old information transmission mod to more convenient transmission mod. With the rapid development of computer and network, network transmission has been highly paid attention [1]. The text, image, video data and other information involved in transmission are insignificant, and some are related to state secrets, trade secrets or personal privacy. For example, the design of a military map or frontier technology transmitted through the network may be destroyed intentionally or unintentionally, which threats the safety of a country with the leakage of technology [2]. Because there is no absolute information security, there are always some security holes in the network environment. Therefore, how to ensure the integrity and confidentiality of information is particularly important, especially the integrity and secrecy of the image data has become the focus of people's concern [3]. Image encryption is the key technology to solve information security. It is also an important technology in the application of digital watermarking

Author's e-mail: michelle_shao@163.com

and information hiding. The study of image encryption has a very high theoretical and practical significance [4].

In recent years, scholars have proposed some new image encryption algorithms. Song *et al.* [5], which describes an image encryption algorithm combining self-coding and hyper-chaotic mapping. The main control key is used to determine the improved discrete Henon mapping parameters, and the intermediate key matrix of the image size is generated by several iterations. The random sequence is generated by its self-return encoding and Logistic chaotic mapping disturbance, and the random sequence generated by the 2-D discrete hyper chaos mappings is fused by an improved 3-D Lorenz reversible mapping. A new 2-D reversible product operation is used to generate the ciphertext image. The algorithm can resist differential and chosen plaintext attacks, but the efficiency of image encryption is low. Bao and Liu [6] proposes an image encryption algorithm based on inline delay chaotic map coupled with Lorenz system. The time delay is introduced into the Logistic mapping and the initial value of the Arnold mapping is generated. Based on the plaintext pixels, the iteration number calculation model of the Arnold mapping is constructed. According to the iteration times of the Arnold mapping, the calculation function of the mapping control parameters is established, and a set of random sequences is generated and the image scrambling is completed by the set of bit sets, the iterative hyper mixing is performed. The chaotic Lorenz system generates the 4-D sequence group, introduces the key stream to modify the 4-D sequence group, and constructs the pixel diffusion mechanism to complete the image encryption. The scrambling algorithm of pixel location is independent of plaintext content, and it is difficult to resist plaintext and differential attacks. Cui and Ding [7] proposes an improved image encryption algorithm based on chaotic encryption and cyclic shift in wavelet transform domain. The corresponding key is generated according to the original image, and the original image is circulated and shifted with the key. The image is transformed by wavelet transform to obtain the wavelet transform domain, and the image is mapped by 2-D chaos, and scrambling processing is made. The ability of the algorithm to resist attack is poor.

In view of the aforementioned problems, an image encryption algorithm for torsional components of generators based on composite chaotic model is proposed [8].

Image encryption algorithm

Image torsional vibration component fusion

The torsional vibration components R, G, and B are extracted from the matrix transformation of images. The three components are passed through a low pass filter with a size of 1, filtered out the high frequency part and transformed the component size into the original 1/3, in order to transform and fuse the next step, and then are carried into the DCT transformation. For forward DCT, the original image is regarded as a space function [9], which makes x a row of pixels, the Y is a column in pixels, and the 2-D DCT and IDCT, respectively:

$$X(u,v) = \frac{2}{N} c(u)c(v) \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \cos \frac{(2i+1)\pi i}{2N} \cos \frac{(2j+1)\pi v}{2N} \tag{1}$$

$$x(i,j) = \frac{2}{N} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} c(u)c(v)X(u,v) \cos \frac{(2i+1)\pi u}{2N} \cos \frac{(2j+1)\pi v}{2N} \tag{2}$$

where $c(u)$ represents the low frequency component, $c(v)$ – the high frequency component, $X(u,v)$ – the coefficient after DCT transformation, $x(i,j)$ – the pixels in the image, (i,j) – the

pixel co-ordinates, N – the total number of pixels, i – the pixel points, v – the compensation coefficient, and u – the DC coefficient obtained after DCT transformation. The torsional vibration components of the two images after DCT transform are rotated 0°, 45°, and 90° and fused, respectively. In order to make a picture of the fused picture for encoding, the R, G, and B components of the same picture are taken separately from left, right and right. The fusion process can be completed by using the following blending:

$$S(p,j)=\frac{s_1(i,j)n_1+s_2(i,j)n_2+s_3(i,j)n_3}{\lambda H}\sqrt{\alpha\beta} \tag{3}$$

$$\begin{aligned} &n_1=1,\quad n_2=\frac{\alpha}{\alpha+\beta},\quad n_3=\frac{\beta}{\alpha+\beta},\quad 0<p\le\frac{H}{3}\\ &n_2=1,\quad n_1=\frac{\alpha}{\alpha+\beta},\quad n_3=\frac{\beta}{\alpha+\beta},\quad \frac{H}{3}<p\le\frac{2H}{3}\\ &n_3=1,\quad n_1=\frac{\alpha}{\alpha+\beta},\quad n_2=\frac{\beta}{\alpha+\beta},\quad \frac{2H}{3}<p\le H \end{aligned} \tag{4}$$

$$\begin{aligned} \alpha&=|s_1||s_2||s_3|\\ \beta&=|s_1(s_2)^{-1}s_3|\\ i&=0,1,\cdots,H/3\\ j&=0,1,\cdots,H \end{aligned} \tag{5}$$

Among them, $S(p,j)$ represents the image after the completion of the fusion, $s_1(i,j)$, $s_2(i,j)$, $s_3(i,j)$ represent three torsional vibration components of the image, λ – the constant, H – the horizontal length of the image matrix. The n_1, n_2, and n_3 are variables, which determine their value based on the evolution of p. The α, β, represents the variable attribute value of the change in the fusion process, the features of s_1, s_2, and s_3 are fused into the transformed images, and finally the fused images are obtained.

Image complex chaotic encryption model

In order to prevent excessive number of keys, the parameters of the chaotic maps logistic-tent system (LTS), logistic-sine system (LSS), and tent-sine system (TSS) are unified as keys [10-12]. The plaintext and each torsional vibration component are sparse processed by discrete cosine transform, respectively. The result of sparsity is compressed and measured and encrypted, and the compressed sensing measurement matrix is generated by 1-D compound chaotic map. In each round of adaptive process, the random phase mask and random matrix are generated by chaos mapping control, and then the Li and Zhao [13] is reordered by the cross control of the RGB component of the image. The detailed encryption process is:

– Step 1: A complex chaotic mapping is used to generate a matrix, Φ_k. The steepest descent method is used to optimize the image information measurement matrix, Φ_k, based on chaos. The specific steps are:
  (1) The parameter selection of LTS is κ_1, the initial value is κ_2, to generate image information encrypted complex chaotic sequence $S_1=\{0<s_i<1|i=1,2\cdots,\}$. Among it, s_i means Chaotic sequence elements. As parameter setting of LSS is κ_1, the initial value of κ_2, used to generate complex chaotic sequence.

(2) One element is selected from S_1 and S_2 of complex chaotic sequences to form a new pseudo random sequence $S_{\Phi_1}(k) = S_1(20k-19)$, $S_{\Phi_2}(k) = S_1(20k+20MN-19)$, in which S_{Φ_1} and S_{Φ_2} are rearranged to generate matrices Φ_1 and Φ_2, respectively:

$$\Phi_i = \sqrt{\frac{2}{M}}\begin{bmatrix} s_{\Phi_i}(1),\cdots,s_{\Phi_i}(MN-M+1) \\ \vdots \\ s_{\Phi_i}(M),\cdots,s_{\Phi_i}(MN) \end{bmatrix} \tag{6}$$

The $M \times N$ means image size, k means compound operation. So Φ_3 and Φ_4 are generated with S_2.

Equation (3) optimizes the matrix Φ_1, Φ_2, Φ_3, and Φ_4 with the steepest descent method [14]. The $D_k = \Phi_k \psi^T$, correlation coefficients between Φ_k, κ and ψ^T by the formula:

$$u(D_\kappa) = \max G_\kappa \left\{ \frac{\left| d_{k,i} d_{k,j} \right|}{\left\| d_{k,i} \right\| \left\| d_{k,j} \right\|} \right\} \tag{7}$$

where $d_{k,i}$ means the i column of D_κ, $d_{k,j}$ – the j column of D_κ, ψ^T – the control parameters of chaotic sequence characteristics, T – the dimension. The more the G_κ value tends to the unit matrix, the better the reconstruction effect of image compressed sensing.

– Step 2: The RGB components of the two images are measured by 2-D discrete cosine transform and 2-D compressed sensing, respectively, [15], get x_{cj}, $y_{cj} \in R^{M \times M}$:

$$\alpha_{j'} = \psi \psi^T, \quad x_{cj} = \breve{\Phi}_1 \alpha_{j'} \breve{\Phi}_2 \tag{8}$$

$$\beta_{j'} = \psi \psi^T, \quad y_{cj} = \breve{\Phi}_3 \alpha_{j'} \breve{\Phi}_4 \tag{9}$$

Among them, $\alpha_{j'}$ means the h discrete component obtained from the j' discrete cosine transformed, $\beta_{j'}$ – the h approximate value obtained from the j' discrete cosine transformed, $\breve{\Phi}_1$, $\breve{\Phi}_2$, $\breve{\Phi}_3$, $\breve{\Phi}_4$ – the chaotic matrix of discrete cosine transform [16].

– Step 3: The x_{cj} and y_{cj} are combined into complex matrices, x_{cj} of them as the real part, the imaginary part is y_{cj}.

$$z_{cj} = x_{cj} + \dot{i} y_{cj} \tag{10}$$

where z_{cj} is a complex valued matrix.

– Step 4: compress encryption results by image compounding chaotic encryption model.

The particle swarm algorithm is used to optimize the control parameters of the model.

According to the Shannon cryptography theory [17], the uniformity of U_{nif} is introduced to evaluate the uniform distribution characteristics of the image ciphertext information. Setting U_{nif} indicates the ratio of ciphertext sequence $X_e(i)$ and variance $\sigma^2_{X_e}$ to uniform noise sequence $X_n(i)$ and variance $\sigma^2_{X_n}$. That is:

$$U_{nif}(X_e, X_n) = \frac{\sigma^2_{X_e}}{\sigma^2_{X_n}} = \frac{\sum_{i=1}^{\dot{N}} (X_e(i) - \bar{X}_e)^2}{\sum_{i=1}^{\dot{N}} (X_n(i) - \bar{X}_n)^2} \tag{11}$$

where $\overline{X}_e = E(X_e) = [\sum_{i=1}^{\dot{N}} X_e(i)]/N$ means the mathematical expectation of X_e, X_n – the uniform noise sequence, $\overline{X}_n$ – the mathematical expectation of X_n. The normalized similarity S_{im} is introduced to measure the approximate degree between the ciphertext sequence $X_n(i)$ and the plaintext sequence and $X_e(i)$. The following formula is set:

$$S_{im}(X_e, X_n) = \frac{\sum_{i=1}^{\dot{N}} X_e(i) X_n(i)}{\sqrt{\sum_{i=1}^{\dot{N}} X_e^2(i) \sum_{i=1}^{\dot{N}} X_n^2(i)}} \tag{12}$$

According to the theory of Shannon cryptography, the encryption effect of a cryptographic system is not only reflected in the correlation between the ciphertext and the plaintext, that is, the correlation, but also the degree of the concealment of the ciphertext, which causes the third party's subjective desire to crack, that is, uniformity. Therefore, the correlation coefficient and evenness index are selected to construct the objective function J, the parameter coordination optimization problem can be expressed as:

$$\begin{aligned} &\min J(K_c, T_{c1}, T_{c2}) = a_1 f_1 + a_2 f_2 \\ &s.t.\ \ K_{c,\min} \le K_c \le K_{c,\max} \\ &T_{c1,\min} \le T_{c1} \le T_{c1,\max} \\ &T_{c2,\min} \le T_{c2} \le T_{c2,\max} \end{aligned} \tag{13}$$

By minimizing the objective function, the encryption effect of the image composite chaotic encryption model can be optimized. The particle swarm optimization algorithm is used to globally co-ordinate and optimize the parameters of the image composite chaotic encryption model K_c, T_{c1} and T_{c2}:

$$T = \min f_1 \frac{T_{c2} \times K_c}{T_{c1} \times a_1 f_1} \tag{14}$$

The encryption performance of image composite chaotic encryption model can be improved to a great extent by the upper formula.

Experiments simulation

In order to prove the validity of the proposed image encryption algorithm for torsional components of generators based on compound chaos model, which is performed on the IS-3210M CPU of the hardware platform with 4 GB memory, and is simulated by the simulation software under Matlab R2010a. Two 256 × 256 × 8 grayscale images are the original images to be encrypted. The encryption effect is included following methods: image encryption algorithm using the combination of the proposed algorithm, self-encoding and hyper chaos mapping, image encryption algorithm coupled with Lorenz system of in-line delay chaotic map, and single-based Chaos image encryption algorithm for image local scrambling and dynamic feedback.

Statistical analysis

Performing double random phase encoding based on chaotic maps and fractional-order random transforms for complex-valued matrices. The complex chaotic sequence generated by it has a very good distribution of 0 and 1 characteristics. The encrypted image has a better uniform distribution. In fig. 2, the image histogram is performed before and after encryption of

Figure 1. Original image

fig. 1. The encrypted image has good uniform distribution characteristics, with high anti-statistical analysis capabilities.

The 2000 points are randomly selected from a 256 × 256 × 8 encrypted images, which are calculated according to the eq. (17). As shown in tab. 1, the correlation coefficients between the horizontal, vertical and diagonal pixels are represented by L, V, and D, respectively. As the original image has an ornamental significance, the change of the pixel value is relatively gentle, and 3 adjacent situations are found. The correlation coefficient between the pixels is larger, and

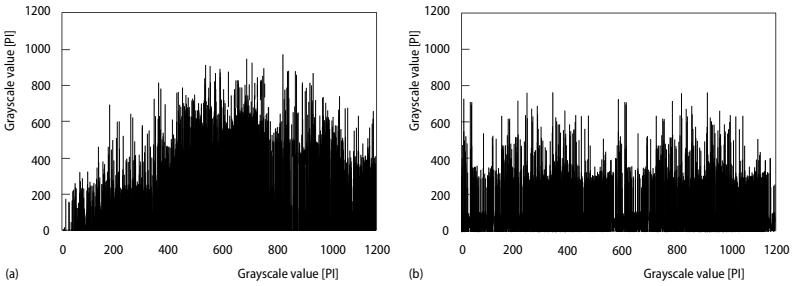

Figure 2. Original and encrypted histogram; (a) histogram before encryption and (b) histogram after encryption

the encrypted image is similar to the *noise* image, and the corresponding correlation system values are smaller. This is in accordance with the statistical law. From the point of view of cryptography, it also shows that the proposed algorithm has good encryption performance.

Table 1. Correlation coefficient between pixels

Pixel relation	Contiguous level	Perpendicularly adjacent	Contiguous object
Original image	0.9854	0.9521	0.9754
Encrypted images	0.0125	0.0124	0.0125

Analysis of anti cutting attack

The ability to resist the clipping attack is one of the criteria for measuring the image encryption algorithm. The image after the clipping part is decrypted by the proposed algorithm. The decrypted image, is shown in fig. 3(a) as a part of the right lower right corner from figs. 1, and 3(b) is the decryption result of the clipping part of the encrypted image.

In fig. 3, it can be seen that the proposed algorithm carries out 2-D discrete cosine transform and 2-D compression perception measurement for the first encrypted image information. The real number matrix of the measured data is merged into a complex value matrix, and the complex matrix is adaptive random phase encoding, which breaks the linearity of the whole encryption process, and the attacker is difficult to deduce plaintext from the ciphertext and deduce the key from the known information, which has a good ability to resist clipping attack.

Figure 3. Experimental results of the anti-clipping attack of the proposed algorithm; (a) clipped image (b) decrypted image

Analysis of resistance to damaged

The ability of anti-breakage attack is also a standard to measure the image encryption algorithm, using the proposed algorithm to decrypt a partially damaged encrypted image. The decrypted image is shown in fig. 4(a) with two partially damaged encrypted images, and fig. 4(b) is a decryption result of partially damaged encrypted images.

In fig. 4 it is shown that the proposed algorithm carries out 2-D discrete cosine transform and 2-D compression perception measurement for the first encrypted image information. The real number matrix of the measured data is merged into a complex value matrix, and the complex value matrix is adaptive random phase encoding, which makes the change of a single plaintext pixel influence the global information of the ciphertext. Comparing figs. 4(a) and 4(b), it can be seen

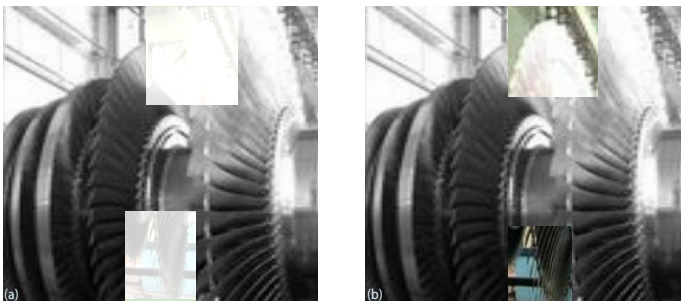

Figure 4. Experimental results of the anti-breakage ability of the proposed algorithm; (a) partially damaged encrypted images, (b) decryption results of partially damaged encrypted images

that the image features become clearer. At the same time, the generation of random phase encoding and random matrix not only depends on chaotic mapping, but also changes with the change of the image of the plaintext. The attacker cannot deduce the key from the known information. It has better ability to resist damage and greatly improves the security of the image information.

Conclusion

In order to solve the problem that the current image encryption algorithm cannot eliminate the strong correlation between adjacent pixels, and make its ability to resist various attacks in low efficiency, an image encryption algorithm for torsional components of generators based on complex chaotic model is proposed. Based on the DCT transform, the algorithm can

effectively remove the visual insensitive high frequency part of the image, and effectively resist the attack of known plaintext. At the same time, in the coding process, the key sequence is not only generated by chaotic mapping, but also influenced by the plaintext. The encryption process is still different in different plaintexts even if the key is the same. The proposed algorithm does not need to replace the key frequently, and the security of the system is enhanced. The design of adaptive and RGB component interaction greatly enhances the security of the system, and solves the problems that are difficult to resist some common attacks caused by the linear properties of compressed sensing and many optical transformations. Simulation results and theoretical analysis show that the algorithm has good anti-attack performance and compression performance, good encryption effect and high security performance.

Acknowledgment

This work was supported by the Key Science and Technology Project of Henan Province (No. 202102210157).

References

[1] Shen, Y., *et al.*, Prediction of Nearest Neighbor Effects on Backbone Torsion Angles and NMR Scalar Coupling Constants in Disordered Proteins, *Protein Science, 27* (2017), 1, pp. 146-158
[2] Wang, X., *et al*., Image Encryption Scheme Using Chaos and Simulated Annealing Algorithm, *Nonlinear Dynamics, 84* (2016), Jan., pp. 1417-1429
[3] Ferretti, L., *et al.*, A Symmetric Cryptographic Scheme for Data Integrity Verification in Cloud Databases, *Information Sciences, 422* (2017), Jan., pp. 497-515
[4] Zhao, F., Wu, C. M., Image Encryption Algorithm Combined Self-encoded Theory with Super-chaotic Mapping (in Chinese), *Journal of Computer-Aided Design & Computer Graphics, 28* (2016), Jan., pp. 119-128
[5] Song, X. C., *et al.,* Image Encryption Algorithm Based on Inline Time Delay Chaotic Map Coupled with Lorenz System (in Chinese), *Computer Engineering and Design, 37* (2016), pp. 1757-1761
[6] Bao, L. X., Liu, W., Chaotic Encryption in Wavelet Transform and Cycle Shift Based Improved Image Encryption Algorithm (in Chinese), *Application Research of Computers,. 33* (2016), pp. 3074-3077
[7] Cui, Y. Q., Ding, G. C., Chaotic Image Encryption Algorithm Based on Single Image Local Scrambling and Dynamic Feedback Diffusion (in Chinese), *Telecommunications Science. 32* (2016), pp. 93-100
[8] Liang, L. X., *et al.,* Simulation of Double Digital Watermarking Algorithm for Color Image (in Chinese), *Computer Simulation, 34* (2017), pp. 150-153
[9] Ge, X., *et al.,* Cryptanalyzing an Image Encryption Algorithm with Compound Chaotic Stream Cipher Based on Perturbation, *Nonlinear Dynamics, 90* (2017), Aug., pp. 1141-1150
[10] Gong, L. H., *et al.,* Quantum Image Encryption Algorithm Based on Quantum Image XOR Operations, *International Journal of Theoretical Physics, 55* (2016), Mar., pp. 3234-3250
[11] Garcia-Planas, M. I., Klymchuk, T., Perturbation Analysis of a Matrix Differential Equation $\dot{x} = ABx$, *Applied Mathematics & Nonlinear Sciences, 3* (2018), 1, pp. 97-104
[12] Baig, A.Q., *et al.,* Revan and Hyper-Revan Indices of Octahedral and Icosahedral Networks, *Applied Mathematics & Nonlinear Sciences, 3* (2018), 1, pp. 33-40
[13] Li, P., Zhao, Y., A Simple Encryption Algorithm for Quantum Color Image, *International Journal of Theoretical Physics, 56* (2017), Mar., pp. 1961-1982
[14] Zhu, H., *et al.,* An Image Encryption Algorithm Based on Compound Homogeneous Hyper-Chaotic System, *Nonlinear Dynamics, 89* (2017), Mar., pp. 61-79
[15] Gao, Z., *et al.,* Colour Image Encryption Algorithm Using One-time Key and FRFT, *IET Image Processing, 12* (2018), 4, pp. 472-478
[16] Tan, R. C., *et al.,* Quantum Color Image Encryption Algorithm Based on a Hyper-Chaotic System and Quantum Fourier Transform, *International Journal of Theoretical Physics, 55* (2016), Sept., pp. 1-17
[17] Wang, X., Zhang, H. L., A Novel Image Encryption Algorithm Based on Genetic Recombination and Hyper-Chaotic Systems, *Nonlinear Dynamics, 83* (2016), Aug., pp. 333-346

Paper submitted: July 17, 2019
Paper revised: September 15, 2019
Paper accepted: September 16, 2019