A Fast Image Encryption Scheme Based on AES

Yong Zhang, Xueqian Li, Wengang Hou
School of Software and Communication Engineering
Jiangxi University of Finance and Economics
Nanchang, P.R. China
e-mail: zhangyong@jxufe.edu.cn

Abstract—**A fast image cryptosystem based on AES is verified in this paper. The plain image is divided into data blocks of size 128 bits. The first block of plain image is permutated by an initial vector. Then, AES in cipher block chaining mode is used to encrypt each block sequentially. The initial vector and cipher image are transmitted to the decryption party through the public information channel. The decryption party use the secret key and initial vector to decrypt the cipher image to obtain the original image. Simulation results show that this image cryptosystem is both secure and high-speed, which can be used as the comparison basement of newly proposed image cryptosystems based on chaotic systems.**

Keywords-information security; image encryption; aes; cipher block chaining

I. INTRODUCTION

Image cryptosystem has become a hot research topic in the area of information security [1-3]. The image cryptosystem needs a large quantity of key streams, and the chaotic systems can produce the pseudo-random sequences of encryption security, thus scholars have put forward a large number of image encryption research results based on chaotic systems [4-6]. Recently, in order to make the image cryptosystem resist the chosen/known plain image attacks, the plaintext-related image encryption systems were widely in-depth studied [7-10]. This kind of image cryptosystem possesses the excellent characteristics that even for the same key, the different plain images correspond to different key streams, i.e. different plain images correspond to different equivalent keys. So, the plaintext-related image cryptosystem can resist the chosen/known plaintext attacks.

In recent years, many scholars pointed out that the text encryption standard AES is not suitable for image encryption. Due to the image's huge volume and redundancy compared to text data, AES is considered to be quite slow for image encryption although it is fairly safe [11-13]. In this paper, we tried to employ the AES in cipher block chaining (CBC) mode to encrypt the image data. We used look-up table method to quickly implement the AES algorithm. The research shows that AES can be used to encrypt images, it can achieve higher encryption speed than some existing image cryptosystems based on chaotic systems [14-16], and the encryption scheme is safe. This paper is organized as follows: Section 2 presents the image cryptosystem based on AES. Section 3 gives the simulation results. Section 4 analyzes the security performance of the AES based system. Section 5 summarizes the paper.

II. TESTED IMAGE CRYPTOSYSTEM

AES, the current text data encryption standard, is a block cipher. The length of each block is fixed to128 bits, whereas the key length is 128 bits, 192 bits, or 256 bits. On a general-purpose computer, AES can be fast implemented via the look-up table method, and applied to image encryption.

Assume that the plain image $\boldsymbol{P}$ is 8-bit grayscale one with size of $M\times N$. Divide $\boldsymbol{P}$ into n pieces of small blocks of length 16 bytes (i.e. 128 bits), where, n=ceil(MN/16), and ceil(x) returns the smallest integer which is greater than x. The image blocks are denoted by $\boldsymbol{P}_i$,i=1,2,...,n. The redundant bytes in the n-th block is filled with 0. The image cryptosystem based on AES is structured as shown in Fig. 1.

In Fig. 1, $\boldsymbol{IV}$ is the initial vector with length of 128 bits, which is generated by chaotic systems. In this paper, we used Tent map to produce $\boldsymbol{IV}$. For each encryption process, the image cryptosystem uses different $\boldsymbol{IV}$s. $\boldsymbol{IV}$ is not secret information. Both $\boldsymbol{IV}$ and the ciphered image $\boldsymbol{C}$ are transmitted to the receiver by public information channel. $\mathrm{AES_e}$ represents the encryption system of AES, and $\mathrm{AES_d}$ represents the decryption system of AES. The ciphered blocks are denoted by $\boldsymbol{C}_i$, i=1,2,...,n, which are combined into the ciphered image $\boldsymbol{C}$. $\boldsymbol{K}$ is the secret key with size of 128 bits, 192 bits or 256 bits. Here, 128-bit key is used.

As can be seen in Fig. 1, the detailed encryption process is as follows:

Step 1. Tent map is used to generate $\boldsymbol{IV}$. $\boldsymbol{IV}$ is public but different $\boldsymbol{IV}$s corresponds to different plain images. Use the pseudo-random number generator function (e.g. *rand* function in MATLAB) to generate one random number, denoted by x_0, as the initial value of Tent map (as shown in Eq. (1)). Iterate Eq. (1) for 16 times to get 16 states, denoted by x_i, i=1,2,...,16.

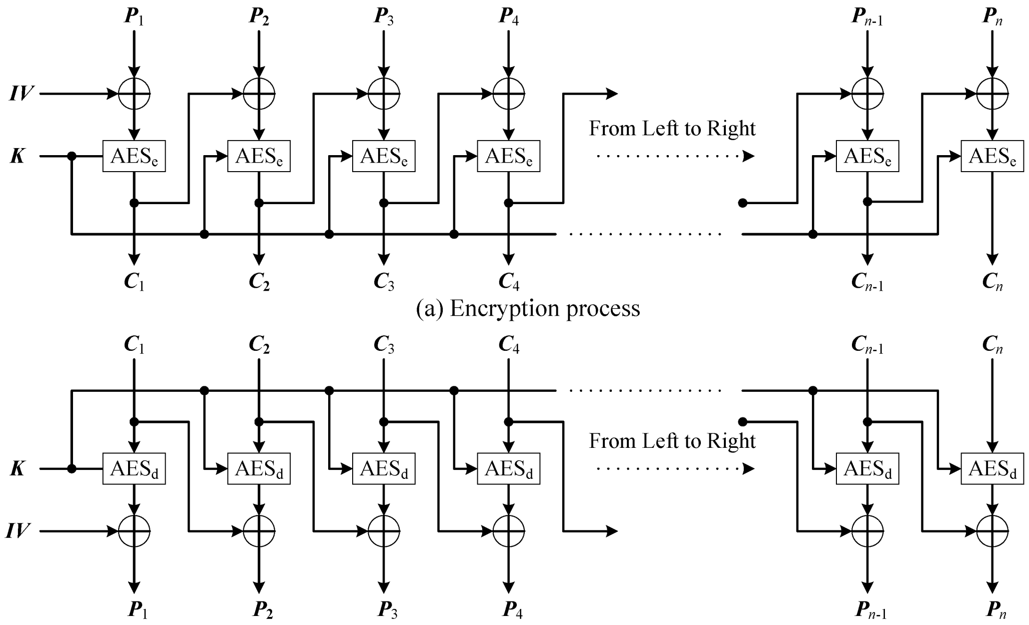
$$F(x)=\{2x, \text{ when } 0<x<0.5;\ 2(1-x), \text{ when } 0.5<x<1\} \quad (1)$$

Then, convert x_i-s into integers according to Eq. (2), denoted by X_i, i=1,2,...,16. Let $\boldsymbol{IV}$=[$X_1X_2...X_{16}$].

$$X_i=\text{floor}(10^4\, x_i) \bmod 256 \quad (2)$$

where, floor(x) returns the largest integer which is smaller than x.

978-1-5090-6238-6/17/$31.00 ©2017 IEEE



(a) Encryption process

(b) Decryption process

Figure 1. Proposed image cryptosystem

Step 2. For the first block $\boldsymbol{P}_1$ of plain image $\boldsymbol{P}$, use Eq. (3) to encrypt it, namely,

$$\boldsymbol{C}_1=\text{AES}_\text{e}(\boldsymbol{K}, \boldsymbol{IV}\ \text{XOR}\ \boldsymbol{P}_1) \tag{3}$$

where, AES$_\text{e}$ represents the AES encryption algorithm with the inputs of secret key $\boldsymbol{K}$ and $\boldsymbol{IV}$ XOR $\boldsymbol{P}_1$. $\boldsymbol{C}_1$ is the first block of ciphered image $\boldsymbol{C}$.

Step 3. For the i-th block $\boldsymbol{P}_i$ of plain image $\boldsymbol{P}$, use Eq. (4) to encrypt it, namely,

$$\boldsymbol{C}_i=\text{AES}_\text{e}(\boldsymbol{K}, \boldsymbol{C}_{i\text{-}1}\ \text{XOR}\ \boldsymbol{P}_i),\ i=2,...,n \tag{4}$$

The decryption process is the inverse of encryption process. The detailed decryption process is as follows:

Step 1. The decryption party obtains the $\boldsymbol{IV}$ and ciphered image $\boldsymbol{C}$ (i.e. $\{\boldsymbol{C}_i\}$, i=1,2,...,n) from the encryption party through public information channel.

Step 2. For the first block $\boldsymbol{C}_1$ of ciphered image $\boldsymbol{C}$, use Eq. (5) to decrypt it, namely,

$$\boldsymbol{P}_1=\text{AES}_\text{d}(\boldsymbol{K}, \boldsymbol{C}_1)\ \text{XOR}\ \boldsymbol{IV} \tag{5}$$

where, AES$_\text{d}$ represents the AES decryption algorithm with the inputs of secret key $\boldsymbol{K}$ and cipher block $\boldsymbol{C}_1$.

Step 3. For the i-th block $\boldsymbol{C}_i$ of ciphered image $\boldsymbol{C}$, use Eq. (6) to decrypt it, namely,

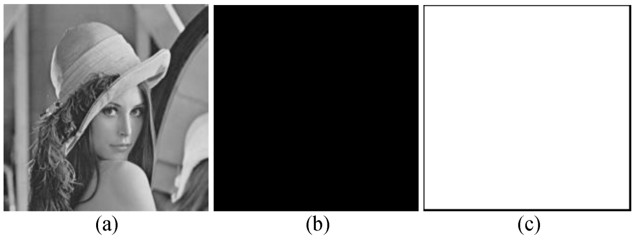
$$\boldsymbol{P}_i=\text{AES}_\text{d}(\boldsymbol{K},\boldsymbol{C}_i)\ \text{XOR}\ \boldsymbol{C}_{i\text{-}1},\ i=2,3,...,n \tag{6}$$

Combine $\{\boldsymbol{P}_i$, i=1,2,...,$n\}$ into an image of size M×N, which is the recovered image.

III. SIMULATION RESULTS

Without loss of generality, take the images of Lena, all-black and all-white (as shown in Figs. 2a-2c, respectively) as examples, let the secret key $\boldsymbol{K}$ be "169, 86, 165, 171, 81, 123, 164, 61, 76, 193, 188, 58, 7, 166, 200, 64" (in decimal format). Here, fix x_0 to 0.8147 to facilitate the test, then $\boldsymbol{IV}$="22,244, 55, 176, 191, 127, 255, 255, 32, 223, 191, 160, 223, 191, 127, 255" (in decimal format). The encrypted images of Figs. 2a-2c are as shown in Figs. 2d-2f, respectively.

As can be seen from Fig. 2, the tested image encryption system encrypts the plain images (as shown in Figs. 2a-2c, respectively) into the noise-like cipher images (as shown in Figs. 2d-2f) without any information leakage. The tested image decryption system decrypts the cipher images (as shown in Figs. 2d-2f, respectively) into the original plain images (as shown in Figs. 2g-2i, respectively). The histograms of plain images (as shown in Figs. 2j-2l, respectively) have obvious fluctuation, while the histograms of cipher images (as shown in Figs. 2m-2o, respectively) have approximately flat features.



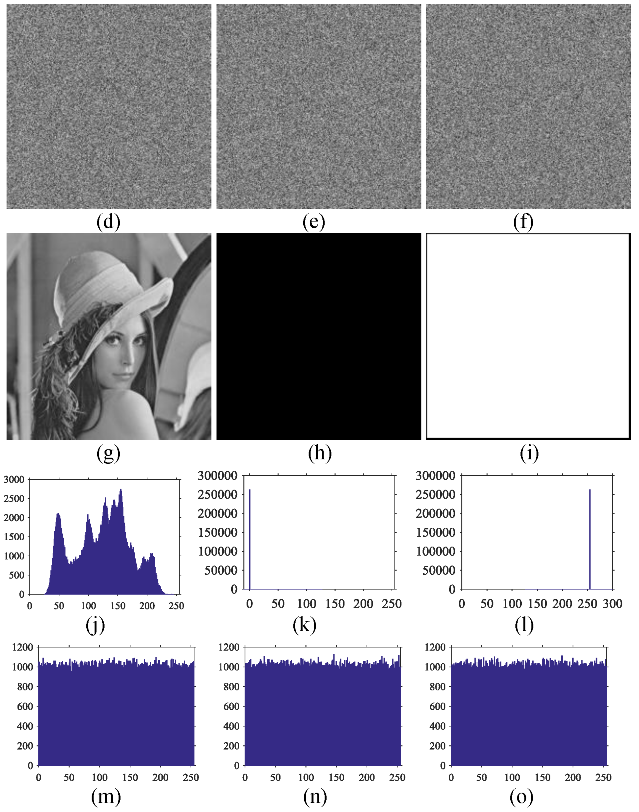


Figure 2. Simulation results. (a)Lena; (b) All-black image; (c) All-white image; (d-f) Cipher images of (a)-(c), respectively; (g-i) Decrypted images of (d)-(f), respectively; (j-l) Histograms of (a)-(c), respectively; (m-o) Histograms of (d)-(f), respectively.

IV. Security Analysis

A. Key Space

The tested image cryptosystem uses AES to achieve the image encryption/decryption. The secret key of AES is also the key of the image cryptosystem, whose length is 128 bits, 192 bits or 256 bits. So, the size of key space is also 2^{128}, 2^{192} or 2^{256}, the same as that of AES. Currently, AES is secure against the brute-force attack, so the tested image cryptosystem is secure against the brute-force attack.

B. Encryption/Decryption Speed

The simulation test uses a computer configured with Intel(R) Core(TM) i7-4720HQ CPU@2.60GHz, 8GB DDR3 RAM, Windows 10(64-bit), and Eclipse C/C++ with MinGW GCC Tool Chain. We designed the encryption /decryption program with C language. AES is implemented by the look-up table method. The encryption algorithm of AES is faster than the decryption algorithm of AES. Without losing generality, the test takes the grayscale image Lena of size 512×512 as an example. The encryption speed of tested system is about 48.7710Mbps, while the decryption speed is about 44.6203Mbps. The encryption /decryption speed is much faster than many image crypto-systems based on chaotic systems [14-16]. On our tested computer, the encryption/decryption speed of the schemes in [14-16] is less than 13Mbps as shown in Table I. This demonstrates that the AES based system has satisfactory encryption/decryption speed.

TABLE I. Encryption/Decryption SPEED

Scheme	Encryption Speed	Decryption Speed
Ref. [14]	0.5175Mbps	0.6833Mpbs
Ref. [15]	12.9454Mbsp	12.9454Mbsp
Ref. [16]	11.9156Mbps	11.9156Mbps
AES scheme	48.7710Mbps	44.6203Mbps

C. Statistical Analysis

Statistical analysis includes histogram analysis and correlation analysis. Section 3 analyzes the difference between histograms of plain and cipher images. This part will analyze the correlation characteristics of plain and cipher images. The correlation is characterized by the correlation coefficient of adjacent pixels of image. Generally, randomly select N pairs of adjacent pixels from the image in horizontal, vertical and diagonal directions, and denote each pair as (u_i,v_i), i=1,2,..., N. Then, the correlation coefficient r_{uv} is calculated by the following Eq. (7).

$$r_{uv}=\Sigma_{i=1..n}(u_i-\mathrm{E}(\boldsymbol{u}))(v_i-\mathrm{E}(\boldsymbol{v}))/\mathrm{Sqrt}(\mathrm{D}(\boldsymbol{u})\mathrm{D}(\boldsymbol{v})) \qquad (7)$$

where, E($\boldsymbol{x}$) returns the mean value of vector $\boldsymbol{x}$, D($\boldsymbol{x}$) represents the variance of vector $\boldsymbol{x}$, and Sqrt(y) means the arithmetic square root of y. $\boldsymbol{u}=\{u_i\}$, $\boldsymbol{v}=\{v_i\}$, i=1,2,...,N.

TABLE II. Correlation Coefficients

Image		Horizontal	Vertical	Diagonal
Lena	Fig. 2a	0.987795	0.970813	0.967978
	Fig. 2d	0.049565	0.000860	-0.005083
All-black	Fig. 2b	1.000000	1.000000	1.000000
	Fig. 2e	0.033805	-0.008710	-0.026632
All-white	Fig. 2c	1.000000	1.000000	1.000000
	Fig. 2f	-0.026956	0.010966	0.051041

Without loss of generality, take Figs. 2a-2f as examples. Here, N=2000. The calculated results of correlation coefficient are listed in Table II, and correlations in the horizontal direction are as shown in Fig. 3. As can be seen from Figs. 3a-3c, the adjacent pixels in horizontal direction of plain images are distributed in the vicinity of straight line y=x. While Figs. 3d-3f show that the adjacent pixels of encrypted images are scattered throughout the phase portrait.

Table II shows that the correlation coefficients of plain images in all directions tend to 1 (where, the correlation coefficients of all-black and all-white images are 1), whereas the correlation coefficients of cipher images tend to 0. So, from Table II and Fig. 3, we can conclude that the adjacent pixels in plain images have strong correlation, but the adjacent pixels in cipher images are nearly uncorrelated. The cipher images can frustrate the analysis method based on correlation characteristics.

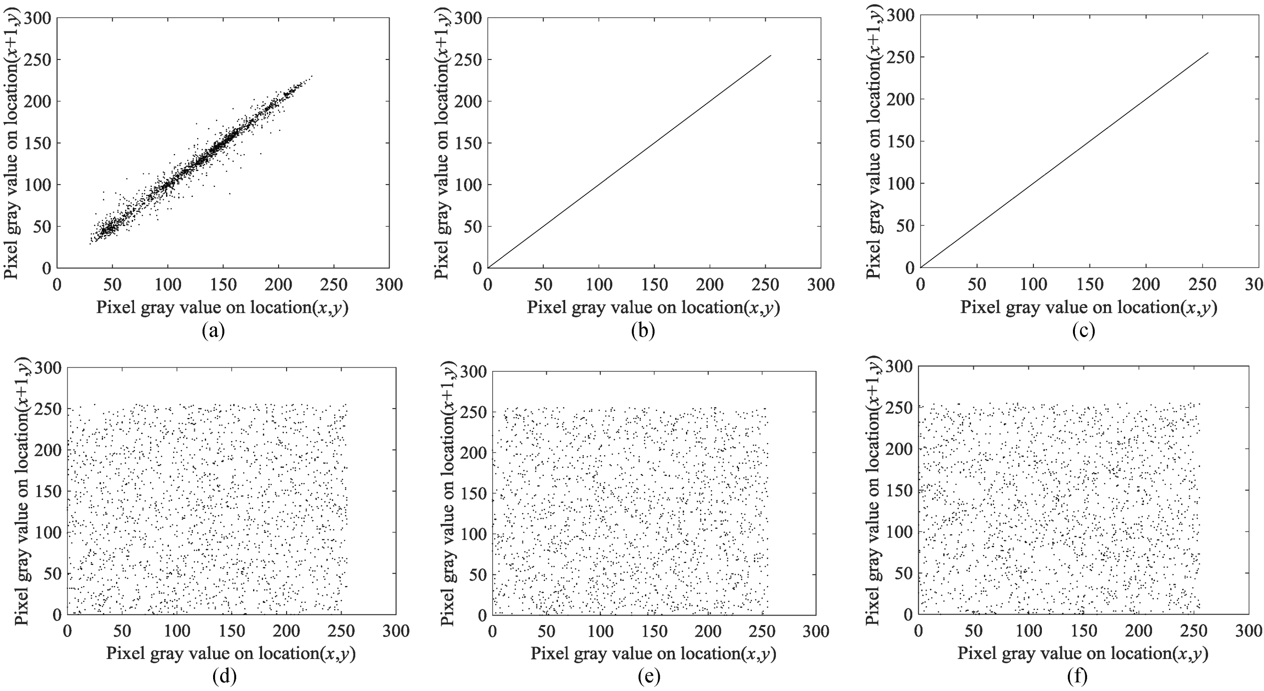


Figure 3. Results of correlation analysis. (a)-(c) Correlations in horizontal direction for Lena, all-black, and all-white, respectively; (d)-(f) Correlations in horizontal direction for the cipher images of Lena, all-black, and all-white, respectively.

D. *Information Entropy*

Information entropy is used to measure the amount of information contained in an image. Generally, the greater the value of information entropy, the greater the amount of information contained in the image. For an 8-bit grayscale image, suppose that the probability of each gray value is denoted by $p(i)$, i=0,1,2,...,255, the information entropy of image can be calculated using Eq. (8).

$$\mathrm{H}=-\sum_{i=0..255}p(i)\log_2(p(i)) \tag{8}$$

Obviously, for an 8-bit random image, H achieves its maximum value of 8. Without losing generality, we calculated the information entropies of plain images (as shown in Figs. 2a-2c, respectively) and cipher images (as shown in Figs. 2d-2f, respectively), and listed the results in Table III. As can be seen from Table III, the information entropies of plain images deviate from 8 (where, the information entropies of both all-black and all-white images are 0). The information entropies of cipher images are fairly close to 8. So, the tested image encryption scheme can resist the analysis based on information entropy.

TABLE III. RESULTS OF INFROMATION ENTROPY ANALYSIS

Image	**Lena**	**All-black**	**All-white**
Plain	7.445061	0	0
Cipher	7.999437	7.999303	7.999313

E. *Key and Plaintext Sensitivities*

NPCR and UACI are commonly used to characterize the sensitivities of image encryption systems [1]. Suppose that two images with the same size of $M\times N$ are denoted by $\boldsymbol{I}_1$ and $\boldsymbol{I}_2$, respectively. Then, NPCR and UACI are defined by Eqs. (9) and (10), respectively.

$$\mathrm{NPCR}=\sum_{i=1..M}\sum_{j=1..N}\boldsymbol{D}(i,j)/(MN)\times 100\% \tag{9}$$

where, $\boldsymbol{D}(i,j)$={1, if $\boldsymbol{I}_1(i,j)\neq\boldsymbol{I}_2(i,j)$; 0, otherwise}, i=1,2,...,M, j=1,2,...,N.

$$\mathrm{UACI}=\sum_{i=1..M}\sum_{j=1..N}|\boldsymbol{I}_1(i,\mathrm{j})-\boldsymbol{I}_2(i,j)|/(255MN)\times 100\% \tag{10}$$

For two 8-bit random grayscale images, the theoretical values of NPCR and UACI are separately 99.6094% and 33.4635%.

TABLE IV. KEY AND PLAIN BLCOK SENSITIVITIES

Image	**Key Sensitivity (%)**		**Plain block Sensitivity (%)**	
	NPCR	***UACI***	***NPCR***	***UACI***
Theoretical	99.6094	33.4635	99.6094	33.4635
Lena	99.6059	33.4418	99.6033	33.3913
All-black	99.5874	33.4894	99.5991	33.4400
All-white	99.6019	33.4950	99.6119	33.5093

The key sensitivity means a small change of secret key will lead to a huge change of cipher images generated by the same plain image. And the plaintext sensitivity means a small change of plain image will lead to a huge change of cipher images generated by the same key. Without losing generality, take Figs. 2a-2c as examples. Test results are in Table IV. Note that a random key is used in the trial.

Table IV shows the calculated results of NPCR and UACI are very close to their theoretical values, respectively. This indicates that the tested image cryptosystem based on AES has strong key sensitivity and plain block sensitivity. So, the system can fight against the differential attack analysis based on the secret key and plain images.

F. *Other Security Features*

For the image cryptosystems based on chaotic systems, we generally need to carry out security performance analysis to illustrate the proposed system being secure. But there is no sufficient conditions so far to prove that those systems are secure. However, Our tested image cryptosystem based on AES employs AES to encrypt/decrypt image blocks. Since AES is secure, this system is secure.

In addition, in tested image encryption system, the encryption party uses chaotic system to produce the initial vector ***IV*** for image encryption. Different ***IV***s are used in each encryption process, even for encrypting the same plain image. Both ***IV***s and ciphered images are transferred to the decryption party through the common information channel. The tested system is secure under the condition that ***IV*** is public. Due to the use of different ***IV***s for each encryption process, the same plain image can be encrypted into totally different cipher images with different encryption processes. This can prevent the eavesdropper to build up the plaintext-cipher-text pairs, which can resist the active attack based on modifying plain images.

V. Conclusion

This paper attempts to study the image cryptosystem based on AES to testify the viewpoints of AES not suitable for image encryption. However, we conclude that AES in CBC mode can be used for image encryption. In the tested system, the initial vector (***IV***) is generated by chaotic system and AES is implemented by look-up table method. The key of AES is also the key of image cryptosystem. AES is secure by far, so the tested image cryptosystem is secure. And simulation results show that the image cryptosystem based on AES are faster than some image cryptosystems based on chaotic systems. Thus, the tested system can be used as the comparison basement of newly proposed image cryptosystems. Those image cryptosystems whose encryption/decryption speed is slower than the AES based scheme in the same computer need to be improved.

Acknowledgment

This work was fully supported by the National Natural Science Foundation of China (No. 61562035), and the Natural Science Foundation of Jiangxi Province, China (No. 20161BAB202058), the Science and Technology Project of Education Department of Jiangxi Province (No. GJJ160426), the Graduate Innovative Special Fund Project of Jiangxi Province, China (No. YC2016-S200), and the Graduate Innovative Special Fund Project of JXUFE, Jiangxi Province (No. XS16392).

References

[1] G. R. Chen, Y. Mao, and C. K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps.” Chaos Soliton. Fract., vol. 21, pp. 749–761, Mar. 2004.

[2] Y. Q. Zhang, and X. Y. Wang, “A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice,” Inform. Sciences, vol. 273, pp. 329–351, Aug. 2014.

[3] R. Enayatifar, A. H. Abdullah and I. F. Isnin, “Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence,” Opt. Laser. Eng., vol. 56, pp. 83–93, May 2014.

[4] Z. Tang, X. Zhang, and W. Lan, “Efficient image encryption with block shuffling and chaotic map,” Multimed. Tools Appl., vol. 74, pp. 1–20, Aug. 2015.

[5] Y. Liu, X. Tong, and J. Ma, “Image encryption algorithm based on hyper-chaotic system and dynamic S-box,” Multimed. Tools Appl., vol. 75, pp. 7739–7759, July 2016.

[6] C. Li, G. Luo, K. Qin, and C. Li, “An image encryption scheme based on chaotic tent map,” Nonlinear Dyn., vol. 87, pp. 1–7, Jan. 2017.

[7] Y. Zhang, “The image encryption algorithm with plaintext-related shuffling,” IETE Tech. Rev., vol. 33, pp. 310–322, Mar. 2016.

[8] Y. Zhang, “Plaintext related image encryption scheme using chaotic map,” TELKOMNIKA, vol. 12, pp. 635–643, Jan. 2014.

[9] J. X. Chen, Z. L. Zhu, C. Fu, L. B. Zhang, and Y. Zhang, “An efficient image encryption scheme using lookup table-based confusion and diffusion,” Nonlinear Dyn., vol. 81, pp. 1151–1166, Mar. 2015.

[10] X. Zhang, X. Fan, J. Wang, and Z. Zhao, “A chaos-based image encryption scheme using 2D rectangular transform and dependent substitution,” Multimed. Tools Appl., vol. 75, pp. 1-19, April 2016.

[11] X. Y. Wang, and D. H. Xu, “A novel image encryption scheme based on Brownian motion and PWLCM chaotic system,” Nonlinear Dyn., vol. 75, pp. 345–353, Febr.2014.

[12] Q. Liu, P. Li, M. Zhang, Y. Sui, and H. Yang, “A novel image encryption algorithm based on chaos maps with Markov properties,” Commun. Nonlinear Sci. Numer. Simulat., vol. 20, pp. 506–515, Febr. 2015.

[13] Z. Hua, and Y. Zhou, “Image encryption using 2D Logistic-adjusted-Sine map,” Inform. Sci. An Int. J., vol.339, pp. 237–253, July 2016.

[14] K. W. Wong, “A fast chaotic cryptographic scheme with dynamic look-up table,” Phys. Lett. A, vol. 298, pp. 238–242, Apr. 2002.

[15] Z. Eslami, and A. Bakhshandeh, “An improvement over an image encryption method based on total shuffling,” Opt. Commun., vol. 286, pp. 51–55, Jan. 2013.

[16] P. Cheng, H. Yang, P. Wei, and W. Zhang, “A fast image encryption algorithm based on chaotic and lookup table,” Nonlinear Dyn., vol. 79, pp. 2121–2131, Mar. 2015.