An Image Encryption Scheme Based on The Three-dimensional Chaotic Logistic Map

Chunhu Li, Guangchun Luo, and Chunbao Li

(Corresponding author: Chunhu Li)

School of Computer Science and Engineering, University of Electronic Science and Technology of China
Chengdu, Sichuan 610054, China
(Email: lchh-tiger@163.com)

(Received June 1, 2017; revised and accepted Sept. 12, 2017)

Abstract

Image encryption has been a popular research field in recent decades. This paper presents a novel image encryption scheme, which is based on the three-dimensional chaotic logistic map. Firstly, the three-dimensional chaotic logistic map is modified to generate key stream. Secondly, the chaos-based key stream is generated by a three-dimensional chaotic logistic map, which has a better performance in terms of randomness properties and security level. The design of the proposed scheme is efficient. It provides the necessary properties for a secure image encryption scheme including the confusion and diffusion properties. We use well-known ways to perform the security and performance analysis of the proposed image encryption scheme. Simulation results show that the suggested scheme satisfies the required performance tests such as large key space, high level security, and acceptable encryption speed. The fail-safe analysis is inspiring and it can be concluded that the proposed scheme is efficient and secure. These characteristics make it a suitable candidate for using in cryptographic applications.

Keywords: Cryptography; Three-dimensional Chaotic Logistic Map; Image Encryption

1 Introduction

Recently, with the rapid development of network technology and their increasing popularity, the roles of images in the exchange of information among people become more frequent, image data protection has become more and more important. To meet the needs of the image authentication, image encryption algorithms were proposed [11, 23, 25, 27, 42]. In 1970s, Chaos theory was proposed, which was used in a number of research areas, such as mathematics, engineering, physics, biology, and so on [15]. The first description of a chaotic process was made in 1963 by Lorenz [28], who developed a system called the Lorenz attractor that coupled nonlinear differential equations. The complex behavior of chaotic systems in nonlinear deterministic was described. The implementation of chaotic maps in the development of cryptography systems lies in the fact that a chaotic map is characterized by:

1) The initial conditions and control parameters with high sensitivity;
2) Unpredictability of the orbital evolution;
3) The simplicity of the hardware and software implementation leads to a high encryption rate [24].

These characteristics can be connected with some very important cryptographic properties such as confusion and diffusion, balance and avalanche properties [14, 37].

Over the past two decades, the image encryption based on Chaos theory has become a hot research topic. The classic encryption architecture based on chaotic map has been investigated. Researchers have proposed many chaos-based digital image encryption schemes [3, 6, 8, 12, 17, 20–22, 30, 31, 33, 36, 38, 39, 41, 45, 46], which utilize chaotic maps. For designing a real-time secure symmetric encryption scheme, Chen and his research group promoted the 2D chaotic cat map to 3D [19]. Mao and his research group proposed a new fast image encryption scheme based on 3D chaotic baker maps [44]. Kanso *et al.* suggested a novel image encryption algorithm, which based on a 3D chaotic map [26]. Ruisong Ye and his research group designed a chaos-based image encryption scheme using 3D skew tent map and coupled map lattice [35]. Haroun's Real-time image encryption using a low-complexity discrete 3D dual chaotic cipher [29]. Akhavan and his partner proposed a novel parallel hash function based on 3D chaotic map [4]. Guodong Ye's symmetric image encryption scheme using 3D chaotic cat maps [19].

The famous logistic map ($x_{n+1} = \alpha x_n(1 - x_n)$) was popularized by May in 1976, the system exhibits chaotic behaviors for most values of the growth coefficient α between 3.57 and 4 [34]. The simple one-dimensional logistic map has a chaotic behavior, and has been used to encrypt information for further transmission [5]. In this paper, we deeply analyze logistic map and three-dimensional chaotic logistic map. Based on three-dimensional chaotic logistic map and the properties of chaotic system, we propose a novel image encryption scheme. Using the three-dimensional chaotic logistic map, we can generate sequences that have very high randomness and complexity. The parameters and the initial variable of the three-dimensional chaotic logistic map in this algorithm can be modified during the encryption and decryption. The initial sensitivity performance of this map is the guarantee of the secure image encryption algorithm. When the small changes in control parameters and initial condition exist, the generated sequences change very large.

The organization of this paper is as follows: Section 2 introduces the three-dimensional chaotic logistic map and its properties. In Section 3, the details of our algorithm (include encryption and decryption) are proposed. The experimental are introduced in Section 4. The details of the security discussion are shown in Section 5. Finally, the conclusions are drawn in Section 6.

2 The Three-dimensional Chaotic Logistic Map

In the introduction section, we introduced the prototype of the logistic map in Equation (1) [10].

$$x_{n+1} = \alpha x_n(1 - x_n). \tag{1}$$

For $0 < x_n < 1$ and $\alpha = 4$ the equation exhibit the chaotic behavior. The logistic map is simplest chaos function.

A real example of the three-dimensional chaotic logistic map is:

$$x_{i+1} = \alpha x_i(1 - x_i) + \beta y_i^2 x_i + \gamma z_i^3 \tag{2}$$

$$y_{i+1} = \alpha y_i(1 - y_i) + \beta z_i^2 y_i + \gamma x_i^3 \tag{3}$$

$$z_{i+1} = \alpha z_i(1 - z_i) + \beta x_i^2 z_i + \gamma y_i^3. \tag{4}$$

Where α β γ are parameters, and for $3.68 < \alpha < 3.99$, $0 < \beta < 0.022$, $0 < \gamma < 0.015$, this system has a chaotic attractor, and can take the value between [0, 1].

Using MATLAB in the experiments, the equation parameters α, β and γ were selected as $\alpha = 3.89$, $\beta = 0.01$ and $\gamma = 0.01$, in this case the system has a chaotic behavior. The Figure 1 shows the distribution of 65536 points.

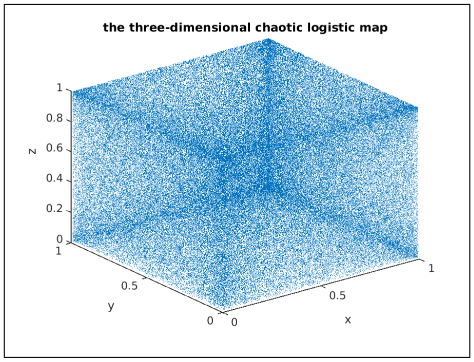

Figure 1: The image of the three-dimensional chaotic logistic map

3 Proposed Algorithm

In this proposed algorithm, We give the detail of the image encryption and decryption algorithm. We encrypt the images of different sizes. We also analyze the effect of encryption. After encryption we get the differences between the decrypted image and the original image. The detailed analysis of these algorithms are mainly recorded in the Section 4 and Section 5. The following is the proposed algorithms and analysis of the main processes of encryption and decryption.

3.1 The Image Encryption Algorithm

In this section, we use the three-dimensional chaotic logistic map Equation (2), Equation (3) and Equation (4) to implement encryption process. The flowchart of the encryption algorithm is shown in Figure 2. This paper proposes an image encryption algorithm includes the following main steps:

1) Reading plain-image (original-image) ($P_{a \times b \times c}$), get size of P, *e.g.* using $[a, b, c]$ save size of P, let $N = a * b$, get R-plain-image $PR_{a \times b \times 1}$, save to $PR_{(N)}$, get G-plain-image $PG_{a \times b \times 2}$, save to $PG_{(N)}$, get B-plain-image $PB_{a \times b \times 3}$, save to $PB_{(N)}$, let $x(0) = 0.100001$, $y(0) = 0.100001$ and $z(0) = 0.100001$;

2) Input the secret (encryption) key α β γ into the three-dimensional chaotic logistic map equation. Iterate the three-dimensional chaotic logistic map N times using system Equation (2), Equation (3) and Equation (4), obtain an array $X_{(N)}$, $Y_{(N)}$ and $Z_{(N)}$;

3) Diffusion: $CDR_{(N)} = X_{(N)} * PR_{(N)}$, $CDG_{(N)} = Y_{(N)} * PG_{(N)}$, $CDB_{(N)} = Z_{(N)} * PB_{(N)}$;

4) Confusion: Change $X_{(N)}$, $Y_{(N)}$ and $Z_{(N)}$ into $[0, 255]$, get $SX_{(N)}$, $SY_{(N)}$ and $SZ_{(N)}$, we can get $CCR_{(N)} = SX_{(N)} \oplus CDR_{(N)}$, $CCG_{(N)} = SY_{(N)} \oplus CDG_{(N)}$, $CCB_{(N)} = SZ_{(N)} \oplus CDB_{(N)}$;

5) Change $CCR_{(N)}$, $CCG_{(N)}$ and $CCB_{(N)}$ into $C_{a \times b \times c}$, which is encrypt each element of matrix ($P_{a \times b \times c}$) using the key array $X_{(N)}$, $Y_{(N)}$ and $Z_{(N)}$, namely, mix the confusion of the original image ($P_{a \times b \times c}$) ($X_{(N)}$, $Y_{(N)}$ and $Z_{(N)}$) components with the diffusion of the original image ($P_{a \times b \times c}$) ($X_{(N)}$, $Y_{(N)}$ and $Z_{(N)}$), get the resulting image is the ciphered image $C_{a \times b \times c}$.

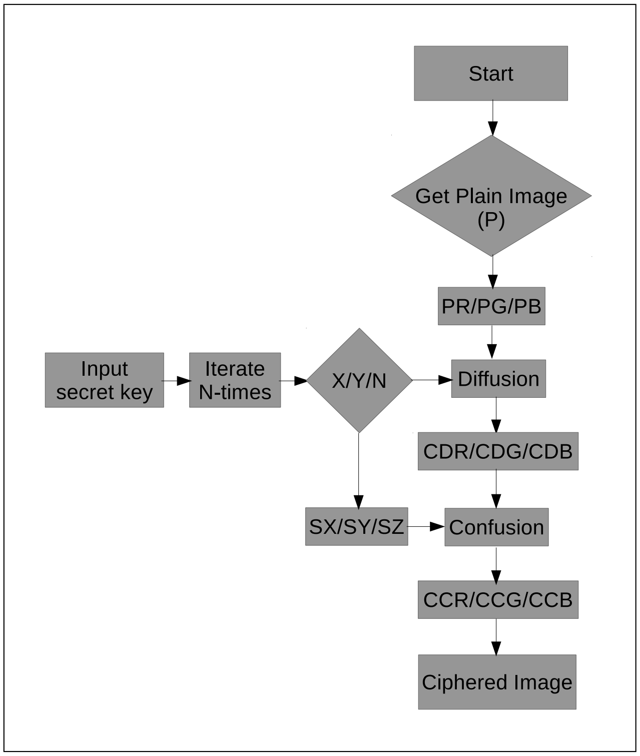

Figure 2: The flowchart of the encryption algorithm

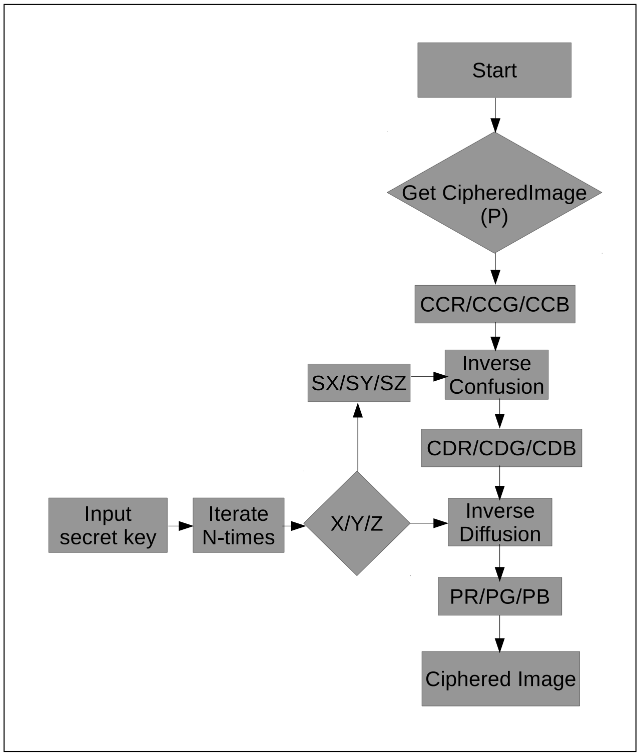

Figure 3: The flowchart of the decryption algorithm

3.2 The Image Decryption Algorithm

In this section, we use the three-dimensional chaotic logistic map Equation (2), Equation (3)and Equation (4) to implement decryption process. The flowchart of the decryption algorithm is shown in Figure 3. This paper proposes an image decryption algorithm includes the following main steps:

1) Reading ciphered-image (encrypted-image) $(C_{a\times b\times c})$, get size of C, *e.g.* using $[a, b, c]$ save size of C, let $N = a * b$, get R-ciphered-image $CR_{a\times b\times 1}$, save to $CCR_{(N)}$, get G-ciphered-image $CG_{a\times b\times 2}$, save to $CCG_{(N)}$, get B-ciphered-image $CB_{a\times b\times 3}$, save to $CCB_{(N)}$, let $x(0) = 0.100001$, $y(0) = 0.100001$ and $z(0) = 0.100001$, here $x(0)$, $y(0)$ and $z(0)$ must be same as encryption process;

2) Input the secret (encryption) key α β γ into the three-dimensional chaotic logistic map equation. Iterate the three-dimensional chaotic logistic map N times using system Equation (2), Equation (3) and Equation (4), obtain an array $X_{(N)}$, $Y_{(N)}$ and $Z_{(N)}$;

3) Inverse confusion: Change $X_{(N)}$, $Y_{(N)}$ and $Z_{(N)}$ into $[0, 255]$, get $SX_{(N)}$, $SY_{(N)}$ and $SZ_{(N)}$, we can get $CDR_{(N)} = SX_{(N)} \oplus CCR_{(N)}$, $CDG_{(N)} = SY_{(N)} \oplus CCG_{(N)}$, $CDB_{(N)} = SZ_{(N)} \oplus CCB_{(N)}$;

4) Inverse diffusion: $PR_{(N)} = CDR_{(N)} * X^{-1}_{(N)}$, $PG_{(N)} = CDG_{(N)} * Y^{-1}_{(N)}$, $PB_{(N)} = CDB_{(N)} * Z^{-1}_{(N)}$;

5) Change $PR_{(N)}$, $PG_{(N)}$ and $PB_{(N)}$ into $P_{a\times b\times c}$, decrypt each element of matrix $(C_{a\times b\times c})$ using the key array $X_{(N)}$, $Y_{(N)}$ and $Z_{(N)}$, namely, get the resulting image is the original image $P_{a\times b\times c}$.

4 Experimental Results

The efficiency of the proposed image encryption algorithm is shown in the following experimental results. The standard gray scale image peppers (Figure 4(a)) with the size 256 × 256 pixels is used for this experiment.

The results of the encryption are presented in Figure 4(b). As can be seen from the encrypted image Figure 4(b), there are no patterns or shadows visible in the corresponding cipher image. The result of the decryption is presented in Figure 4(c). As can be seen from the decrypted image Figure 4(c), it is not different from the original image.

The color image peppers with the size 512 × 512 × 3 pixels is used for this experiment. The Figure 5(a) is the color image of peppers, Figure 5(b) is the encrypted color image of peppers, and Figure 5(c) shows the decrypted color image of peppers from Figure 5(b).

We also do many experiments using different size of color images, 1024 × 1024 × 3 pixels and 2048 × 2048 × 3 pixels in Figure 6, the speed of those images is shown in Table 2.

The result of the decryption using wrong key is presented in Figure 4(f). As can be seen from the Figure 4(f), there are no patterns or shadows visible in the corresponding ciphered image.

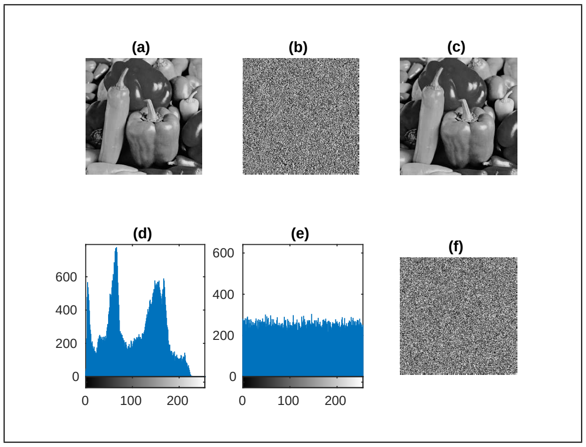

Figure 4: (a) The original image; (b) The encrypted image; (c) The decrypted image; (d) The histogram of original image; (e) The histogram of ciphered image; (f) The decrypted image with wrong key.

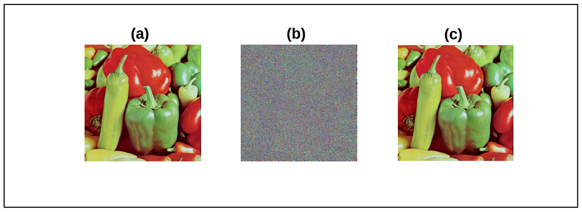

Figure 5: (a) The original image; (b) The encrypted image; (c) The decrypted image.

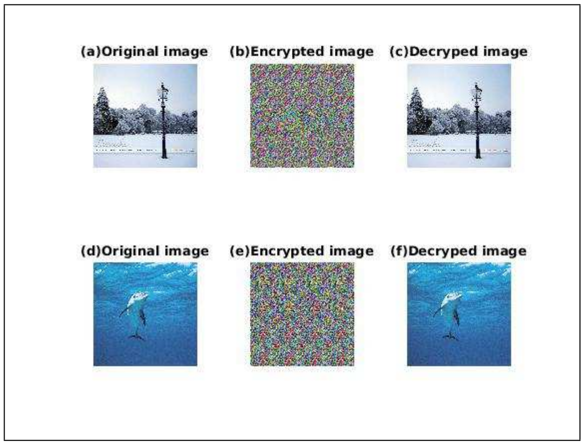

Figure 6: The encrypted-decrypted images.

5 Security Analysis

Security is a major issue of a cryptosystem. When a new cryptosystem is proposed, it should always be accompanied by some security analyses. A good encryption procedure should be robust against all kinds of cryptanalytic, statistical and brute-force attacks. Here, some security analyses have been performed on the proposed scheme like key space analysis, distribution of the cipher-text, correlation analysis of two adjacent pixels, information entropy, plain-text sensitivity analysis, etc. The security analysis demonstrates a high security level of the new scheme.

5.1 Key Space

For every cryptosystem, the key space is very important. The key space of an encryption algorithm should be large enough to resist brute-force attacks. In our proposed scheme, the key space of the image decryption is computed by:

$$T(\alpha, \beta, \gamma, x_0, y_0, z_0) = \theta(\alpha \times \beta \times \gamma \times x_0 \times y_0 \times z_0)$$

where $3.68 < \alpha < 3.99$, $0 < \beta < 0.022$, $0 < \gamma < 0.015$, $x_0 \in [0,1]$, $y_0 \in [0,1]$, $z_0 \in [0,1]$, the each precision of $\alpha, \beta, \gamma, x_0, y_0, z_0$ is 10^{-16}, namely, the size of key space is 10^{95} $(((10^{16})^6 * 10^{-1} * 10^{-2}) * 10^{-2})$. This key space is big enough for brute-force attacks [32,40]. In this scheme, we take the key to the original as follows: $x_0 = 0.100001$, $y_0 = 0.100001$, $z_0 = 0.100001$, $\alpha = 3.8900000001$, $\beta = 0.01$, $\gamma = 0.01$. When taking the wrong key: the difference between wrong and right key is 10^{-16}. For example, using $\alpha = 3.8900000001000001$ as the wrong key to decrypt the encryption image, we get a wrong decrypted image shown in Figure 4(f).

5.2 Distribution of The Ciphertext

An image histogram displays that how pixels in an image are distributed by plotting the number of pixels. Here we take a peppers image (its size is 256 × 256) as the original image. Histogram of the original peppers image and the corresponding ciphered peppers image are shown in Figure 4(d) and 4(e). As is shown, the histograms of the ciphered image is uniform and do not provide any clues to the use of any statistical analysis attack on the encrypted image [7] .

5.3 Correlation Analysis of Two Adjacent Pixels

The superior confusion and diffusion properties are shown in the correlations of adjacent pixels from the ciphered image [43]. We analyze the correlation between adjacent

Table 1: Correlation coefficient of two adjacent pixels in simulated original and ciphered image

Direction	Original image	Ciphered image
Horizontal	0.9158	0.0036
Vertical	0.9085	0.0073
Diagonal	0.8791	0.0059

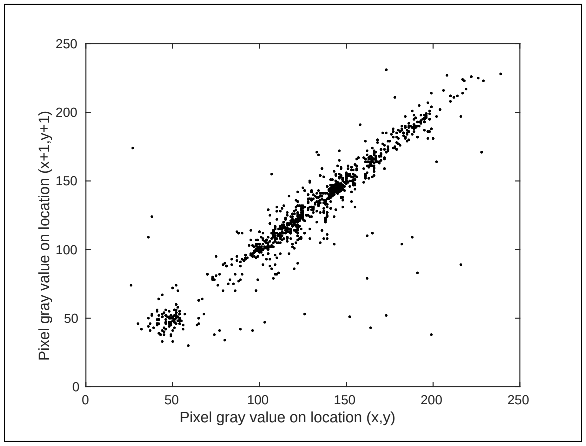

Figure 7: Correlation analysis of original image

pixels in original and ciphered peppers image. We calculate the correlation coefficient in the horizontal, vertical and diagonally, the following relation is used [1]:

$$C_r = \frac{(N\sum_{j=1}^{N} x_j y_j - \sum_{j=1}^{N} x_j \sum_{j=1}^{N} y_j)}{(N\sum_{j=1}^{N}(x_j)^2 - (\sum_{j=1}^{N} x_j)^2)(N\sum_{j=1}^{N}(y_j)^2 - (\sum_{j=1}^{N} y_j)^2)}$$

where x_j and y_j are the values of the adjacent pixels in the image and N is the total number of pixels selected from the image for the calculation. We choose randomly 3000 image pixels from the original image and the ciphered image respectively to calculate the correlation coefficients of the adjacent pixels in horizontal, vertical and diagonally direction. It demonstrates that the encryption algorithm covers up all the characters of the original image showing a good performance of balanced 0 1 ratio. The correlation of the original image and the encrypted image are shown in Figures 7 and 8.

5.4 Information Entropy

Information theory is a mathematical theory founded in 1949 by Shannon [13]. Modern information theory is concerned on data compression, error-correction, communications systems, cryptography, and related topics. There is a universal formula for calculating information entropy:

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

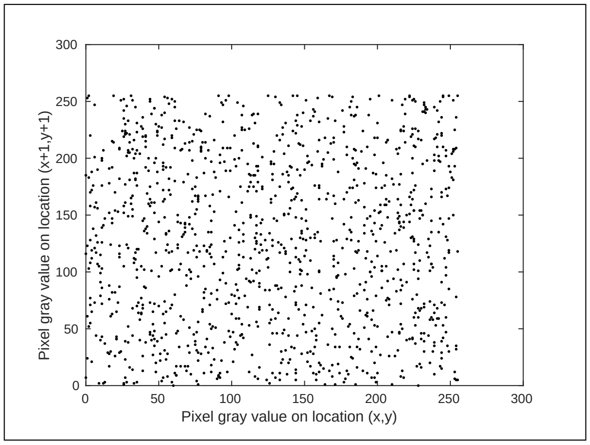

Figure 8: Correlation analysis of encrypted image

where $P(s_i)$ represents the probability of symbol s_i and the entropy is expressed in bits. The ideal entropy value for an encrypted image should be 8. The calculation of entropy for the ciphered image (Figure 4(b)) is presented below:

$$H(s) = \sum_{i=0}^{255} P(s_i)\log_2 \frac{1}{P(s_i)} = 7.9981632.$$

The result shows that the entropy of the encrypted image is very close to the ideal entropy value, higher than most of other existing algorithms. This indicates that the rate of information leakage from the proposed image encryption algorithm is close to zero.

5.5 Plain-text Sensitivity Analysis (Differential Attacks)

Attackers often make a slight change for the original image, use the proposed scheme to encrypt the original image before and after changing, and through comparing two encrypted images to find out the relationship between the original image and the encrypted image. This kind of attack is called differential attack [43]. In order to resist differential attack, a minor alternation in the plain-image should cause a substantial change in the ciphered image. To test the influence of one-pixel change on the whole image encrypted by the proposed algorithm, two common measures were used: $NPCR$ and $UACI$ [16]. $NPCR$ represents the change rate of the ciphered image provided that only one pixel of plain-image changed. $UACI$ which is the unified average changing intensity, measures the average intensity of the differences between the plain-image and ciphered image. For calculation of $NPCR$ and $UACI$, let us assume two ciphered images C_1 and C_2 whose corresponding plain images have only one-pixel difference. Label the gray-scale values of the pixels at grid (i, j) of C_1 and C_2 by $C_1(i, j)$ and $C_2(i, j)$, respectively. Define a bipolar array, D, with the same size as image C_1 or C_2. Then, $D(i, j)$ is determined by $C_1(i, j)$ and $C_2(i, j)$, namely, if $C_1(i, j) = C_2(i, j)$ then $D(i, j) = 0$; otherwise, $D(i, j) = 1$. $NPCR$ and $UACI$

are defined by the following formulas [9]:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_i(i,j) - C_2(i,j)|}{255}\right] \times 100\%$$

where W and H are the width and height of C_1 or C_2. Tests have been performed on the proposed scheme by considering the one-pixel change influence on a 256-gray scale image of size 256 × 256. Also in order to clarify the effect of small change in the secret key such as initial condition ($x_0 = 0.100001$ to $x_0 = 0.1000010000000001$, $y_0 = 0.100001$ to $y_0 = 0.1000010000000001$, $z_0 = 0.100001$ to $z_0 = 0.1000010000000001$) $NPCR$ is calculated. We obtained $NPCR = 0.00385$ $(1 - NPCR = 0.99615)$ and $UACI = 0.361$. The percentage of pixel changed in encrypted image is over 99% even with one-bit difference in plain-image. $UACI$ is near to 1/3 as security required [2]. Moreover, in order to analyze the effect of the control parameter μ in the cipher image, the $NPCR$ test is conducted on the algorithm over this parameter. The process of the analysis is almost the same as the one for a single bit change in the plain-text, but this time we keep plain-image as original, and analyze the number of bit changes between two different cipher texts achieved from encryption with two different parameters with very small change ($\alpha = 3.8900000001$ versus $\alpha = 3.8900000001000001$). The calculated value of $NPCR$ for the proposed algorithm is 0.003238 which is very close to the ideal value. Also, compared with other chaos based algorithms such as $NPCR$ and $UACI$ of the proposed algorithm has a good ability to anti differential attack [18].

Table 2: Average ciphering time taking of a few different size images

Images size(pixels)	Bits/pixels	Ciphered time(s)
256 × 256 × 3	24	1.27-1.32
512 × 512 × 3	24	5.07-5.21
1024 × 1024 × 3	24	20.56-21.63
2048 × 2048 × 3	24	67.81-69.35

5.6 Analysis of Speed

Apart from the security consideration, running speed of the algorithm is also an important aspect for a good encryption algorithm. We measure the encryption/decryption rate of several color images of different-size by using the proposed image encryption scheme. The time analysis is done on a core 2 duo 2.26Gz CPU with 4GB RAM notebook running on Debian 8.0 and using Matlab 2014b glnxa64. The average encryption/decryption time taken by the algorithm for different-sized images is shown in the Table 2.

6 Conclusion

In this paper we concentrate on the field of image encryption. The encryption and decryption schemes are given. In this algorithm, the three-dimensional chaotic logistic map is used to generate pseudo-random sequences, which are independent and approximately uniform. After a series of transformations, the sequences constitute a new pseudo-random sequence uniformly distributing in the value space, which covers the plain-text by executing Exclusive-OR and shifting operations some rounds to form the cipher. Experiments and a safety analysis are carried out. We analyze the performance, security and the resistance to difference and linear attack of this cryptographic system by a simulation. Simulation results show that the algorithm is efficient and usable for the security of the image encryption system.

Acknowledgment

This work is supported by the foundation of science and technology department of Sichuan province NO.2016GZ0077 and NO.2017JY0007. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] A. Afshin, M. Hadi, and A. Amir, "A novel block cipher based on hierarchy of one-dimensional composition chaotic maps," in *IEEE International Conference on Image Processing*, pp. 1993–1996, 2006.

[2] A. Akhavan, A. Samsudin, and A. Akhshani, "A symmetric image encryption scheme based on combination of nonlinear chaotic maps," *Journal of the Franklin Institute*, vol. 348, no. 8, pp. 1797–1813, 2011.

[3] A. Akif, C. Haris, K. Ismail, P. Ihsan, and I. Ayhan, "Chaos-based engineering applications with a 3d chaotic system without equilibrium points," *Nonlinear Dynamics*, vol. 84, no. 2, pp. 481–495, 2015.

[4] A. Amir, S. Azman, and A. Afshin, "A novel parallel hash function based on 3d chaotic map," *EURASIP Journal on Advances in Signal Processing*, vol. 2013, no. 1, pp. 126–126, 2013.

[5] M. S. Baptista, "Cryptography with chaos," *Physics Letters A*, vol. 240, no. 1–2, pp. 50–54, 1998.

[6] S. Behnia, A. Akhavan, A. Akhshani, and A. Samsudin, "Image encryption based on the jacobian elliptic maps," *Journal of Systems and Software*, vol. 86, no. 9, pp. 2429–2438, 2013.

[7] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, and A. Akhavan, "A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps," *Physics Letters A*, vol. 366, no. 4, pp. 391–396, 2007.

[8] S. Bouchkaren and S. Lazaar, "A new iterative secret key cryptosystem based on reversible and irreversible

cellular automata," *International Journal of Network Security*, vol. 18, no. 2, pp. 345–353, 2016.

[9] S. Bruce and S. Phil, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Wiley, 1995.

[10] S. H. Carl, *Chaos in Dynamical Systems*, Springer International Publishing, 2017.

[11] C. C. Chang, K. F. Hwang, M. S. Hwang, "A digital watermarking scheme using human visual effects", *Informatics*, vol. 24, no. 4, pp. 505–511, Dec. 2000.

[12] L. Chunhu, L. Guangchun, Q. Ke, and L. Chunbao, "An image encryption scheme based on chaotic tent map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 127–133, 2017.

[13] S. Claude, "Communication theory of secrecy systems*," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[14] S. J. Clinton, *Chaos and Time-Series Analysis*, Oxford University Press, vol. 1, 2003.

[15] F. Dachselt and W. Schwarz, "Chaos and cryptography," *IEEE Transactions on Circuits and Systems I Fundamental Theory and Applications*, vol. 48, no. 12, pp. 1498–1509, 2002.

[16] D. N. Delia, "Book review: Elementary statistics: A step by step approach, 9thed," *Teaching Sociology*, vol. 44, 2016.

[17] A. A. A. El-Latif, L. Li, W. Ning, H. Qi, and N. Xiamu, "A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces," *Signal Processing*, vol. 93, no. 11, pp. 2986–3000, 2013.

[18] A. A. A. El-Latif, L. Li, and N. Xiamu, "A new image encryption scheme based on cyclic elliptic curve and chaotic system," *Multimedia Tools and Applications*, vol. 70, no. 3, pp. 1559–1584, 2014.

[19] C. Guanrong, M. Yaobin, and C. Charles, "A symmetric image encryption scheme based on 3d chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[20] Z. Guomin, Z. Daxing, L. Yanjian, Y. Ying, and L. Qiang, "A novel image encryption algorithm based on chaos and line map," *Neurocomputing*, vol. 169, pp. 150–157, 2015.

[21] Z. Hegui, Z. Xiangde, Y. Hai, Z. Cheng, and Z. Zhiliang, "An image encryption algorithm based on compound homogeneous hyper-chaotic system," *Nonlinear Dynamics*, pp. 1–19, 2017.

[22] L. L. Hua and C. Z. Jun, "Analysis of two confidentiality-preserving image search schemes based on additive homomorphic encryption," *International Journal of Electronics & Information Engineering*, vol. 5, 2016.

[23] L. C. Huang, L. Y. Tseng, M. S. Hwang, "A reversible data hiding method by histogram shifting in high quality medical images", *Journal of Systems and Software*, vol. 86, no. 3, pp. 716–727, Mar. 2013.

[24] G. James, "Chaos: Making a new science," *The Quarterly Review of Biology*, vol. 56, no. 1, pp. 1053–1054, 1989.

[25] B. Jana, "Dual image based reversible data hiding scheme using weighted matrix," *International Journal of Electronics and Information Engineering*, vol. 5, no. 1, pp. 6–19, 2016.

[26] A. Kanso and M. Ghebleh, "A novel image encryption algorithm based on a 3d chaotic map," *Communications in Nonlinear Science & Numerical Simulation*, vol. 17, no. 7, pp. 2943–2959, 2012.

[27] L. Liu, Z. Cao, "Analysis of two confidentiality-preserving image search schemes based on additive homomorphic encryption," *International Journal of Electronics and Information Engineering*, vol. 5, no. 1, pp. 1–5, 2016.

[28] E. N. Lorenz, "Deterministic nonperiodic flow," *Journal of the Atmospheric Sciences*, vol. 20, no. 2, pp. 130–141, 1963.

[29] F. H. Mohamed and T. A. Gulliver, "Real-time image encryption using a low-complexity discrete 3d dual chaotic cipher," *Nonlinear Dynamics*, vol. 82, no. 3, pp. 1–13, 2015.

[30] M. A. Murillo-Escobar, C. Cruz-Hernndez, F. Abundiz-Prez, and O. R. A. Campo, "A rgb image encryption algorithm based on total plain image characteristics and chaos," *Signal Processing*, vol. 109, pp. 119–131, 2015.

[31] M. Naoki and A. Kazuyuki, "Cryptosystems with discretized chaotic maps," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 49, no. 1, pp. 28–40, 2002.

[32] S. Nigel *et al.*, "Ecrypt ii yearly report on algorithms and keysizes," *Framework*, pp. 116–116, 2010.

[33] P. Praveenkumar, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, "Mojette (d) secret image sedih in an encrypted double image - a histo approach," *International Journal of Network Security*, 2016.

[34] M. May Robert, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, no. 5560, pp. 459–467, 1976.

[35] Y. Ruisong and Z. Wei, "A chaos-based image encryption scheme using 3d skew tent map and coupled map lattice," *International Journal of Computer Network & Information Security*, vol. 4, no. 1, pp. 25–28, 2012.

[36] K. Sarah, H. Hamid, D. Sad, and B. Mamar, "A novel secure image transmission scheme based on synchronization of fractional-order discrete-time hyperchaotic systems," *Nonlinear Dynamics*, vol. 1, no. 1, pp. 1–17, 2017.

[37] B. Schneier, "Applied cryptography: Protocols, algorithms, and source code in C," *John Wiley & Sons, Inc, New York*, vol. 1, no. 1, pp. 53–54, 1996.

[38] L. Shiguo, "A block cipher based on chaotic neural networks," *Neurocomputing*, vol. 72, no. 4–6, pp. 1296–1301, 2009.

[39] S. Sowmya and S. V. Sathyanarayana, "Symmetric key image encryption scheme with key sequences derived from random sequence of cyclic elliptic curve

points over gf(p)," *International Journal of Network Security*, vol. 12, no. 3, pp. 137–150, 2011.

[40] P. Vinod, N. K. Pareek, G. Purohit, and K. K. Sud, "A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption," *Optics Communications*, vol. 284, no. 19, pp. 4331–4339, 2011.

[41] Z. Wei, W. Kwok-wo, Y. Hai, and Z. Zhi-liang, "An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion," *Communications in Nonlinear Science & Numerical Simulation*, vol. 18, no. 8, pp. 2066–2080, 2013.

[42] C. C. Wu, S. J. Kao, and M. S. Hwang, "A high quality image sharing with steganography and adaptive authentication scheme", *Journal of Systems and Software*, vol. 84, no. 12, pp. 2196–2207, 2011.

[43] W. Xiaopeng, G. Ling, Z. Qiang, Z. Jianxin, and L. Shiguo, "A novel color image encryption algorithm based on dna sequence operation and hyper-chaotic system," *Journal of Systems and Software*, vol. 85, no. 2, pp. 290–299, 2012.

[44] M. Yaobin, C. Guanrong, and L. Shiguo, "A novel fast image encryption scheme based on 3d chaotic baker maps," *International Journal of Bifurcation and Chaos*, vol. 14, no. 10, pp. 3613–3624, 2004.

[45] Z. Yicong, B. Long, and C. L. P. Chen, "A new 1d chaotic system for image encryption," *Signal Processing*, vol. 97, no. 7, pp. 172–182, 2012.

[46] W. X. Yuan and Z. J. Feng, "Cryptanalysis on a parallel keyed hash function based on chaotic neural network," *Neurocomputing*, vol. 73, no. 16–18, pp. 3224–3228, 2010.

Biography

Chunhu Li received his B.S. (2008) in computer science from Qingdao Agricultural University and M.S. (2011) in computer science from University of Electronic Science and Technology of China (UESTC), China. He is currently a Ph.D. candidate at UESTC. His research interests include cloud computing, network security, image encryption and artificial intelligence.

Guangchun Luo received his Ph.D. degree in computer science from UESTC in 2004. He is currently a professor of computer science at UESTC. His research interests include computer networks, mobile networks and network security.

Chunbao Li received his B.S. (2011) in computer science from China West Normal University and M.S. (2014) in computer science from University of Electronic Science and Technology of China (UESTC), China. He is currently a Ph.D. candidate at UESTC. His research interests include artificial intelligence, machine learning.