An Efficient Chaotic Image Encryption Algorithm Based on Self-adaptive Model and Feedback Mechanism

Xiao Zhang[1], Chengqi Wang[1] and Zhiming Zheng[1]
[1] Key Laboratory of Mathematics, Informatics and Behavioral Semantics, Ministry of Education, and School of Mathematics and Systems Science, Beihang University
Beijing, 100191 - China
[e-mail: 09621@buaa.edu.cn, ChengqiWang@buaa.edu.cn and zzheng@pku.edu.cn]
*Corresponding author: Chengqi Wang

Received May 16, 2016; revised December 17, 2016; accepted January 23, 2017; published March 31, 2017

Abstract

In recent years, image encryption algorithms have been developed rapidly in order to ensure the security of image transmission. With the assistance of our previous work, this paper proposes a novel chaotic image encryption algorithm based on self-adaptive model and feedback mechanism to enhance the security and improve the efficiency. Different from other existing methods where the permutation is performed by the self-adaptive model, the initial values of iteration are generated in a novel way to make the distribution of initial values more uniform. Unlike the other schemes which is on the strength of the feedback mechanism in the stage of diffusion, the piecewise linear chaotic map is first introduced to produce the intermediate values for the sake of resisting the differential attack. The security and efficiency analysis has been performed. We measure our scheme through comprehensive simulations, considering key sensitivity, key space, encryption speed, and resistance to common attacks, especially differential attack.

Keywords: Image encryption, Chaotic systems, Self-adaptive model, Feedback mechanism, Network security

The authors would like to thank the editors and anonymous reviewers for their detailed reviews and constructive comments, which help improve the quality of this paper. We also would like to acknowledge Lijia Xie for her valuable discussion and feedback. This research is supported by the Major Program of National Natural Science Foundation of China (No.: 11290141), the National Natural Science Foundation of China (No.: 61402030), and the Fundamental Research of Civil Aircraft (No.: MJ-F-2012-04).

https://doi.org/10.3837/tiis.2017.03.029 **ISSN : 1976-7277**

1. Introduction

The rapid development of network communication and cloud computing leads to an overarching concern about security of image transmission. As cryptographic countermeasures, however, traditional algorithms such as DES, IDEA and AES are unsuitable for digital image encryption due to the high redundancy, bulky data capacity and high pixel correlation [1-2]. Chaos, a widespread phenomenon of definitive nonlinear systems, is considered analogous to the confusion and diffusion process of the cryptosystem specified by Shannon. Hence, the chaotic systems are practically applied in the field of image encryption algorithm [3-7, 32-33]. First, Fridrich employed the chaotic system to the image encryption algorithms and proposed the architecture of permutation-diffusionin in 1998 [8]. Since then, there are three different kinds of typical usages in the aspect of algorithm design: (1) creating position permutation relations; (2) generating pseudo-random bit sequence (PRBS); (3) producing cryptograph directly with initial parameters of cryptosystem [9-13]. Furthermore, with the development of chaotic theory, hyper-chaotic theory has become one of the pop research topics.

Over the last few years, there are a number of new chaotic image encryption algorithms which more or less borrow the ideas from the hyper-chaotic system have been presented. In 2012, a novel image encryption scheme was presented by Zhu [14], which the pseudo-random number sequence is generated by a hyper-chaotic system. Recently, Norouzi et al. [15] presented an image encryption algorithm which used only one round diffusion on the foundation of the hyper-chaotic system. In 2016, Wang et al. [30] proposed a novel low dimensional chaotic map to design an image encryption algorithm which balance the efficiency between security and computational complexity. According to the cryptanalysis of chaotic image encryption algorithm in proposed papers, a variety of weaknesses have been found such as small key space, key stream completely depended on the secret key, insensitiveness for the changes of the plain image, and security defects to the chosen and known plaintext attacks. In 2013, Li et al. [16] found that it was viable to break the Zhu's scheme [14] with only one known plain-image. Afterwards, Zhang et al. [17] proved that all the secret keys of Norouzi et al.'s algorithm [15] could be revealed by lauching known or chosen plaintext attacks. In 2016, Li [31] cracked a classical hierarchical chaotic image encryption algorithm based on permutation.

Due to the weak resistance to known and chosen plaintext attacks, most algorithms, though resilient against the statistical analysis, are vulnerable with some pairs of known plaintext and the corresponding cryptograph. In addition, a number of weaknesses have been recently found in typical chaotic maps such as Arnold cat map and Logistic map [18]. Specifically, Arnold cat map can only be applied to square plain image and available iteration time has been proven less than 1000. Logistic map may work inadequately for encryption purpose as the exhibition of massive periodic windows in range of 3.57 to 4 facilitates the analysis of the cryptograph. And some security defects for the existing algorithms based on the multiple encryption rounds has been found. Besides, the applicability of the all-zero image has not been well considered in the existing image encryption algorithms.

In order to meet these challenges, we propose a novel chaotic image encryption algorithm which generalizes our another scheme [30] and applies some more common chaotic maps to realize both security and efficiency. To ensure the sensitivity to the changes of plain-image, the algorithm adopts the self-adaptive model in the permutation stage. Besides, we employ a novel method to generate the more uniformly distributed initial values of iteration in the

self-adaptive model. To resist the chosen and known plaintext attacks effectively and satisfy the applicability of the all-zero image, the feedback mechanism is employed in the diffusion stage, in which the piecewise linear chaotic map is first introduced to produce the intermediate values for the sake of better complexity and randomness. In addition, this scheme applies the structure of single round permutation-diffusion to avoid the information leakage between the neighboring encryption rounds and reduce the amount of calculation while satisfying the security requirements. The performance and security analysis of the proposed algorithm have been performed by using the statistical analysis, such as key space and sensitivity analysis, differential analysis, applicability analysis, speed performance analysis, MSE and PSNR analysis.

The remaining of this paper is organized as follows. We first introduce the tent chaotic map, the piecewise linear chaotic map and the Chen's high-dimension hyper-chaotic system in Section 2. Next in Section 3, we outline the design of our algorithm. And then section 4 specifies the security, applicability and efficiency analysis of our algorithm. Lastly, we give our conclusion in Section 5.

2. Preliminaries

In this section, we introduce some knowledge briefly about the tent chaotic map, the piecewise linear chaotic map and the Chen's high-dimension hyper-chaotic system, which are utilized in our algorithm.

2.1 The tent chaotic map

Since the early 1990s, there are a variety of chaotic maps applied in the design of many image encryption algorithms. The tent chaotic map also has good characters as a classic discrete chaotic map, for instance the simplicity in representation and parameter sensitivity, which is adopted to generate the random bit sequences mainly. The asymmetric tent map has only one parameter, which can be described in formula (1).

$$x_{i+1} = \begin{cases} x_i/\alpha, & 0 \le x_i \le \alpha, \\ (1-x_i)/(1-\alpha), & \alpha \le x_i \le 1, \end{cases} \tag{1}$$

where $x_i \in [0,1]$ is the iteration trajectory value and $\alpha \in (0,1)$ is the parameter of one-dimensional chaotic map. The map has some good properties so that the map described above possesses good qualities, which is widely used [19].

2.2 The piecewise linear chaotic map

The piecewise linear chaotic map has gained a lot of attention in the research of chaotic maps recently due to the efficiency in implementation and the sensitivity to initial values. The piecewise linear chaotic map can be described in the formula (2).

$$x_{i+1} = \begin{cases} x_i/\beta, & 0 \le x_i \le \beta, \\ (x_i-\beta)/(0.5-\beta), & \beta \le x_i \le 0.5, \\ (1-x_i-\beta)/(0.5-\beta), & 0.5 \le x_i \le 1-\beta, \\ (1-x_i)/\beta, & 1-\beta \le x_i \le 1, \end{cases} \tag{2}$$

where $x_i \in [0,1]$ is the iteration trajectory value and $\beta \in (0,0.5)$ is the control parameter of the chaotic map. This piecewise linear chaotic map has the following features, which can be applied for chaotic image encryption algorithm: (1) the chaotic map behaves chaotically in (0, 1) and the results possess excellent properties such as ergodicity, mixing and determinacy in the interval of definition; (2) the chaotic map appears uniform invariant distribution from the statistical analysis perspective; (3) the chaotic map generates good random sequence easily, which can be adopted as the generation of keystream [20].

2.3 Chen's high-dimension hyper-chaotic system

In 1979, hyper-chaotic system was reported by Rössler at the first time. Since then, hyper-chaotic theory has been developed. The Chen's high-dimension hyper-chaotic system has more complex chaotic pathway than the chaotic system [21-22]. The Chen's high-dimension hyper-chaotic system can be described in the formula (3).

$$\begin{cases} \dot{X} = a(Y - X), \\ \dot{Y} = -XZ + dX + cY - V, \\ \dot{Z} = XY - bZ, \\ \dot{V} = X + k, \end{cases} \tag{3}$$

where a, b, c, d and k are system parameters. The results based on the experiments show that hyper-chaotic system has more than one positive Lyapunov exponents and more complex dynamical characteristics than chaos. The Chen's high-dimension hyper-chaotic system described above shows the hyper-chaotic dynamic behavior when the parameters are a = 36, b = 3, c = 28, d = -16, $-0.7 \le k \le 0.7$. For instance, when k = 0.2, the Lyapunov exponents of the Chen's high-dimension hyper-chaotic system are $\lambda_1 = 1.552$, $\lambda_2 = 0.023$, $\lambda_3 = 0$, $\lambda_4 = -12.573$, which show the system possesses the hyper-chaotic dynamic behavior.

3. The proposed algorithm

Without loss of generality, we set M×N as the size of original image. And we describe the algorithm in terms of three segments: initialization, permutation and diffusion. The multiple chaotic systems which consist of the tent chaotic map (1), the piecewise linear chaotic map (2) and the Chen's high-dimension hyper-chaotic system (3) are utilized to enlarge the key space and perform the complex dynamic behavior. Futhermore, single round permutation-diffusion is leveraged to avoid information leakage between the neighboring encryption rounds and reduce calculation amount while guaranteeing the security. **Fig. 1** shows the flowchart of our algorithm.

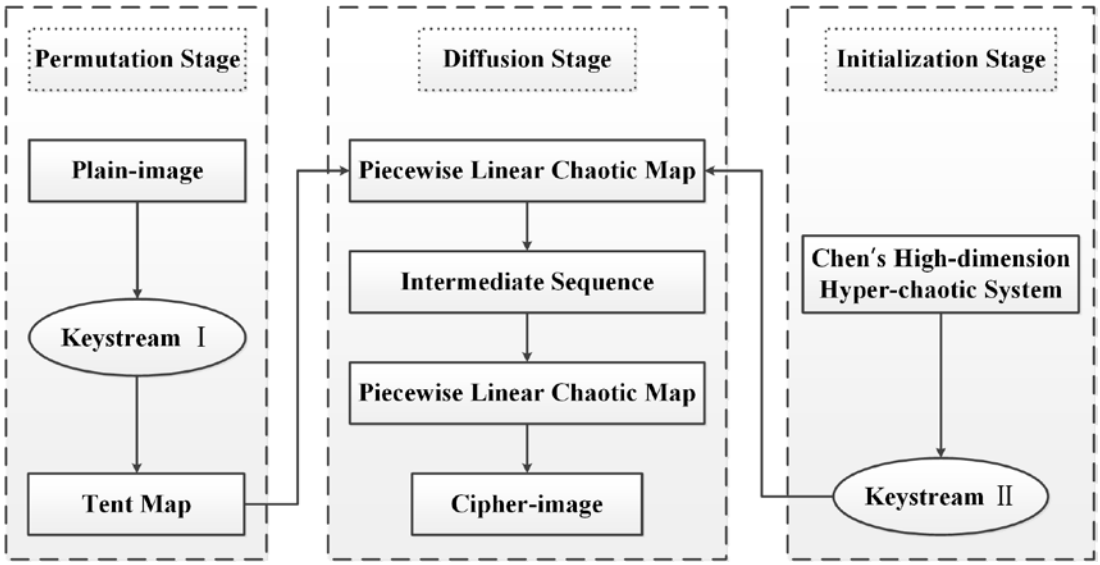


Fig. 1. The flowchart of our algorithm

The proposed algorithm is specified as follows.

3.1 Initialization

In initialization phase, the Chen's high-dimension hyper-chaotic system (3) is employed to generate the initial values of intermediate values, which is implemented by the fourth order Runge-Kutta method and the step size h = 0.001. The details are specified as follows:

Step 1: Let the Chen's high-dimension hyper-chaotic system (3) iterate I times to eliminate the transient effect. Give up the results of previous I times and take the (I+1)th value as the initial value $\left(x_0^*, y_0^*, z_0^*, v_0^*\right)$ of the Chen's high-dimension hyper-chaotic system (3).

Step 2: Let the Chen's high-dimension hyper-chaotic system (3) iterate $\lceil (L+4)/4 \rceil$ times with initial value $\left(x_0^*, y_0^*, z_0^*, v_0^*\right)$ and generate one real number sequence $\{a_i\}_{i=1}^{L+4}$, in which L denotes the M×N original image.

Step 3: Calculate one positive number sequence $\{b_i\}_{i=1}^{L+4}$ as equation (4),

$$b_i = |a_i| - \lfloor |a_i| \rfloor, \qquad i = 1, \cdots, L+4, \tag{4}$$

in which $|a_i|$ and $\lfloor |a_i| \rfloor$ denote absolute value and integer part of $|a_i|$, respectively.

Step 4: Calculate an integer sequence $\{x_i\}_{i=1}^{L+4}$ by equation (5),

$$x_i = \lfloor b_i \times 10^8 \rfloor \bmod 256, \qquad i = 1, \cdots, L+4, \tag{5}$$

in which x_i is an integer ranging from 0 to 255, namely $0 \le x_i \le 255$.

3.2 Permutation

This section shows how permutation is adopted to shuffle image pixels on the basic of the self-adaptive model. The pseudo-random sequence generated by the tent chaotic map (1) is applied to reduce pixel correlation, namely one of intrinsic characteristics of plain-image. Moreover, in order to achieve the objective of designing the dynamic permutation sequence, initial value of the tent chaotic map (1) is computed by pixels' values of the plain-image, which is different from traditional permutation sequences. Therefore, permutation sequence differs correspondingly even if only one pixel changes. The plain-image sequence is permutated by changing the order of iterated values. Without loss of generality, integer sequence $\{p_i\}_{i=1}^{L}$ denotes the pixels' values of plain-image and another integer sequence $\{p_i^*\}_{i=1}^{L}$ denotes the permutated version. Remark that $\sum_{i=1}^{L} p_i = \sum_{i=1}^{L} p_i^*$, which is also the fundamental of the decryption process.

The existing methods always adopt the formulas such as $\alpha = \dfrac{\sum_{i,j} A(i,j)}{\sum_{i,j} A(i,j)^2}$ or $\beta = \dfrac{\sum_{i,j} A(i,j)}{M \times N \times \max\left(A(i,j)\right)}$ to generate the initial values of iteration and then perform the permutation by self-adaptive model, where $A(i,j)$ is the pixel value of the row ith and column jth in the plain-image. **Table 1** is shown that there is asymmetrical distributions for initial values in (0, 1). Thus weakness is found in the selection of initial values, namely, initial values of the iteration are confined to a narrow range of values. As a remedy, the proposed scheme generates the initial values of iteration in a novel way as $average - \lfloor average \rfloor$, making the initial values more uniformly distributed and more random. Hence, different plain-images result in tremendous differences between the initial values of iteration. **Table 1** shows the results of distribution using the formula α, the formula β and the proposed algorithm.

Table 1. The results of initial values distribution

Category	(0, 0.2)	(0.2, 0.4)	(0.4, 0.6)	(0.6, 0.8)	(0.8, 1)
The algorithm used the formula α	99.2%	0.4%	0.2%	0.1%	0.1%
The algorithm used the formula β	0.3%	0.3%	98.9%	0.4%	0.1%
The proposed algorithm	18.9%	20.6%	19.4%	21.2%	19.9%

We demonstrates the details as follows:

Step 1: Calculate the sum of plain-image pixels' values by equation (6),

$$D = \sum_{i=1}^{L} p_i, \tag{6}$$

where D is an integer.

Step 2: Obtain the average of pixels' values by equation (7),

$$average = \frac{D}{L}, \tag{7}$$

and acquire the fractional part by equation (8),

$$E = average - \lfloor average \rfloor, \tag{8}$$

in which E belongs to [0, 1].

Step 3: Let the tent chaotic map (1) iterate L times with E to obtain one real number sequence $\{e_i\}_{i=1}^{L}$.

Step 4: Permute real number sequence $\{e_i\}_{i=1}^{L}$ to acquire permutation subscript sequence $\{y_i\}_{i=1}^{L}$, which is derived by $\{e_i\}_{i=1}^{L}$ with sorted version, where e_{y_i} is ith smallest number in the $\{e_i\}_{i=1}^{L}$.

Step 5: Set $p_i^* = p_{y_i}$ to obtain one permutated sequence $\{p_i^*\}_{i=1}^{L}$.

3.3 Diffusion

During the diffusion, feedback mechanism is leveraged to make the cipher-image dependent on plain-image and intermediate values which are produced by the piecewise linear chaotic map (2) and the Chen's high-dimension hyper-chaotic system (3) to resist chosen and known plaintext attacks and apply for the all-zero image. Furthermore, pixel values of cipher-image rely on corresponding pixel values in the plain-image, intermediate values generated by diffusion section and adjacent pixel values in the cipher-image using modulo 256 addition and XOR operation. By employing feedback mechanism, previous pixel values of cipher-image are fed back to the intermediate values. Hence, pixel values of cipher-image are influenced by corresponding pixel values in the plain-image, intermediate values generated in this section and adjacent pixel values in the cipher-image. Additionally, intermediate values are produced by feedback mechanism in a similar way, which utilize the pseudo-random number sequence generated by the Chen's high-dimension hyper-chaotic system (3) in initialization. During this section, cipher-image sequence $\{c_i\}_{i=1}^{L}$ is computed from pseudo-random number sequence $\{x_i\}_{i=1}^{L+4}$ and permutated sequence $\{p_i^*\}_{i=1}^{L}$. The details are specified as follows.

Step 0: Set $p_0^* = x_{L+1}$, $k_0 = x_{L+2}$, $c_{L+1} = x_{L+3}$, $k_{L+1} = x_{L+4}$.

Step 1: Calculate initial value t of the piecewise linear chaotic map (2) by equation (9) while i varying from 1 to L,

$$t = \frac{p_{i-1}^* + x_i}{2 \times \max\{x_i\}_{i=1}^{L+4}}, \tag{9}$$

and make the piecewise linear chaotic map (2) iterate twice to generate t_1 and t_2.

Step 2: Acquire t_3 and t_4 by equation (10) and equation (11),

$$t_3 = \left(|t_1| - \lfloor |t_1| \rfloor\right) \times 10^8 \bmod 256, \tag{10}$$

$$t_4 = \left(|t_2| - \lfloor |t_2| \rfloor\right) \times 10^8 \bmod 256, \tag{11}$$

Step 3: Obtain k_i as equation (12),

$$k_i = \left(\text{bitxor}\left(p_i^* + t_3\right) + \text{bitxor}\left(k_{i-1} + t_4\right)\right) \bmod 256, \tag{12}$$

in which $0 \le k_i \le 255$ and k_i is an integer, bitxor denotes bitwise XOR.

Step 4: Repeat step 1 to step 3 until sequence $\{k_i\}_{i=1}^{L}$ is computed.

Step 5: Calculate initial value t of the piecewise linear chaotic map (2) by equation (13) while i varying from 1 to L,

$$t = \frac{x_{L-i+1} + k_{i+1}}{2 \times \max\left\{x_i\right\}_{i=1}^{L+4}}, \tag{13}$$

and make the piecewise linear chaotic map (2) iterate twice to generate t_5 and t_6.

Step 6: Acquire the t_7 and t_8 by equation (14) and equation (15),

$$t_7 = \left(|t_5| - \lfloor |t_5| \rfloor\right) \times 10^8 \bmod 256, \tag{14}$$

$$t_8 = \left(|t_6| - \lfloor |t_6| \rfloor\right) \times 10^8 \bmod 256, \tag{15}$$

Step 7: Obtain c_i as equation (16),

$$c_i = \left(\text{bitxor}\left(k_i + t_7\right) + \text{bitxor}\left(c_{i+1} + t_8\right)\right) \bmod 256, \tag{16}$$

in which $0 \le c_i \le 255$ and c_i is an integer, bitxor denotes bitwise XOR.

Step 8: Repeat step 5 to step 7 until cipher-image sequence $\{c_i\}_{i=1}^{L}$ is computed.

4. Security and efficiency analysis

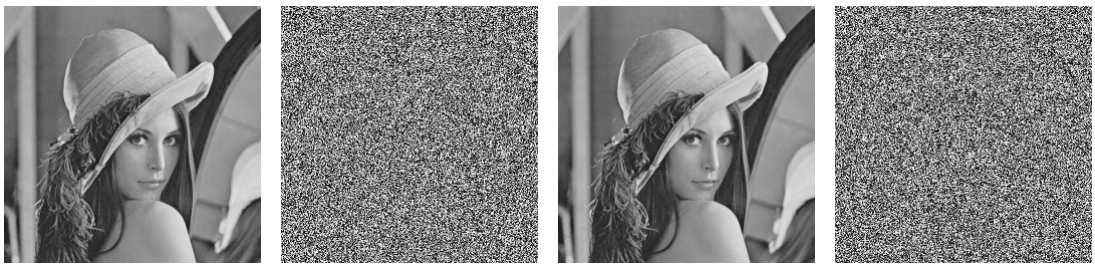
During this section, analysis includes nine subsections: key space, key sensitivity, histogram, adjacent pixels correlation, information entropy, differential, applicability of the all-zero image, speed performance, MSE and PSNR. According to the range of values discussed above, we set the parameter of the tent chaotic map (1) as $\alpha = 0.61$ and the parameter of the piecewise linear chaotic map (2) as $\beta = 0.29$. The parameters of the Chen's high-dimension hyper-chaotic system (3) are set as a = 36, b = 3, c = 28, d = -16, k = 0.2 and the initial values are $x_0 = 1.00$, $y_0 = -1.99$, $z_0 = 1.00$, $v_0 = -1.99$. Moreover, the number of iterations in the Chen's high-dimension hyper-chaotic system (3) for eliminating the transient effect is I = 3000. Remark that the program language is Visual C++.

4.1 Key space analysis

In order to guarantee the resistance for brute-force attack, key space of secure image encryption proposal should be larger than $2^{100} \approx 10^{30}$ [23]. As specified in Section 3, secret key of our proposal includes the control parameter of the tent chaotic map (1), the control parameter of the piecewise linear chaotic map (2) and the initial values of the Chen's high-dimension hyper-chaotic system (3), which are all double-precision floating-point representation. Secret key is $K = (\alpha, \beta, x_0, y_0, z_0, v_0)$, where significant digits of each parameter are set to 15. Thus, key space of our proposal is $(10^{15})^6 = 10^{90} \approx 2^{300}$, which is a lot larger than required size to avoid exhaustive search in an image encryption proposal.

4.2 Key sensitivity analysis

It is ideal to perform the high sensitivity to every secret key even with tiny changes for an image encryption proposal. To evaluate the key sensitivity, we first encrypt the plain-image with both control parameters and initial values as described above. Then we add 10^{-14} to initial value x_0 of the Chen's high-dimension hyper-chaotic system (3). Finally, we decrypt the cipher-image respectively. **Fig. 2** shows the results of key sensitivity. By comparing **Fig. 2(c)** and **Fig. 2(d)**, it is shown that a completely different decrypted image is generated by the wrong key, which has a 10^{-14} difference with the right key. As a consequence, the proposed proposal is highly sensitive to secret key.

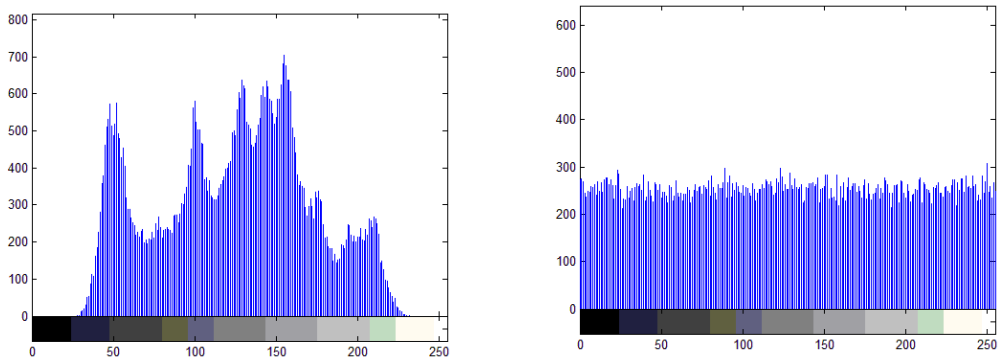


(a) (b) (c) (d)

Fig. 2. The results of the key sensitivity analysis: (a) plain-image, (b) cipher-image, (c) correct decryption, (d) decryption with 10^{-14} changed in the initial value x_0

4.3 Histogram analysis

Histogram, a kind of statistical analysis, can present the distribution of pixel values. The histograms of plain-image (**Fig. 2(a)**) and corresponding cipher-image (**Fig. 2(b)**) are given in this subsection. And results of histogram analysis is shown in **Fig. 3**. It can be seen that gray-scale pixel values of cipher-image (**Fig. 2(b)**) are almost uniformly distributed over the integer range [0, 255]. In contrast, distribution of cipher-image in the **Fig. 3(b)** is significantly different from **Fig. 3(a)**. Therefore statistical attack is unworkable towards our proposal.



(a) (b)

Fig. 3. The results of the histogram analysis: (a) plain-image, (b) cipher-image

4.4 Adjacent pixels correlation analysis

It is necessary to reduce correlation of adjacent pixels, which is considered as an inherent characteristic in the meaningful plain-images [26]. **Fig. 4** and **Table 2** show the results of adjacent pixels correlation. **Fig. 4(a)** and **Fig. 4(b)** respectively present horizontally adjacent pixels' correlation before encryption and after encryption. As shown in **Fig. 4(a)**, adjacent pixels are so asymmetrical that original image may be deciphered through statistical attack. We randomly select 5000 pairs of pixels from **Fig. 2(a)** and **Fig. 2(b)**. And we thereby calculate the correlation of horizontal, vertical and opposite angles direction by formula (17), (18), (19) and (20) as follows.

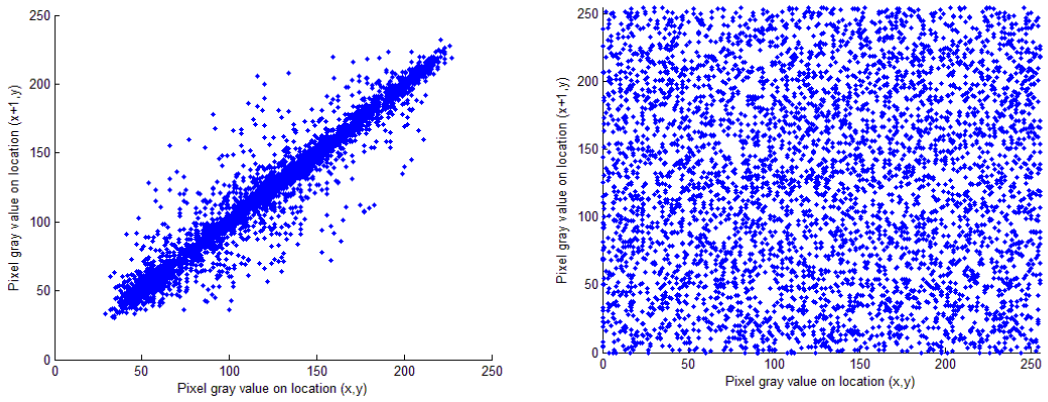
$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{17}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x_i))^2, \tag{18}$$

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x_i))(y_i - E(y_i)), \tag{19}$$

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{20}$$

where x and y represent gray-scale pixel values of two adjacent pixels in the same image. **Table 2** respectively shows correlation of horizontal, vertical and opposite angles direction before encryption and after encryption. Our image encryption proposal almost guarantees the adjacent pixel uncorrelation of cipher-plain, increasing the difficulty of statistical decipher so that our proposal provides a considerate ability of confusion and diffusion for resisting the correlation attack.



(a) (b)

Fig. 4. The results of the adjacent pixels correlation analysis: (a) before encryption, (b) after encryption

Table 2. The correlation of the adjacent pixel before and after encryption

Direction	Plain-image	Cipher-image
Horizontal	0.937084	-0.002065
Vertical	0.969142	-0.000767
Opposite angles	0.912509	-0.003012

4.5 Information entropy analysis

As an important feature of randomness, information entropy quantify the random-looking values distribution. Information entropy $H(m)$ can be computed as:

$$H(m) = -\sum_{i=0}^{2^N-1} p(m_i) \log_2 \frac{1}{p(m_i)}, \tag{21}$$

in which $p(m_i)$ is the probability of m_i and N denotes the pixel's binary bits. For gray-scale image, maximum value of pixel's binary is 8. It is also ideal Shannon entropy for uniformly distributed pixel values in the [0, 255]. Hence, in a good chaotic image encryption algorithm, the information entropy of the cipher-image should be close to 8. With the original image of size 256×256, we calculate the information entropy of proposed proposal and other image encryption proposals in Ref. [15, 24, 25, 27, 28]. **Table 3** shows that information entropy of our proposal is higher than the other five algorithms. The Ref. [27] is built with the feedback mechanism, which employs the Logistic map in diffusion stage to participate in the generation of intermediate values. Hereby, the proposed proposal has the less possibility to leak out the information. Furthermore, information entropy of ours is 7.99748, which is close to the ideal value 8, making the statistical attack infeasible.

Table 3. The results of the information entropy analysis

Category	Value
Expected value	8.00000
Plain-image	7.42662
Encrypted image by the proposed algorithm	7.99748
Encrypted image by Ref. [15]	7.99803

Encrypted image by Ref. [24]	7.99707
Encrypted image by Ref. [25]	7.99691
Encrypted image by Ref. [27]	7.99730
Encrypted image by Ref. [28]	7.99516

4.6 Differential analysis

Attackers usually make a slight change of the plain-image, e.g., modify only one pixel, and observe how the inputs affect the corresponding outputs, which is named differential analysis as one kind of effective attack methods. To evaluate the influence of one changed pixel value in the plain-image, two common measures are applied for a quantitative description: NPCR (number of pixels change rate) and UACI (unified average changing intensity) [29]. The NPCR and UACI are calculated by formula (22), (23) and (24).

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\%, \tag{22}$$

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{2^L - 1}\right] \times 100\%, \tag{23}$$

$$D(i,j) = \begin{cases} 0, & \text{if } C_1(i,j) = C_2(i,j) \\ 1, & \text{otherwise} \end{cases}, \tag{24}$$

in which M and N are width and height of image and L denotes pixel's binary bits. Remark that corresponding plain-images of C_1 and C_2 are different in a single pixel. Furthermore, $C_1(i,j)$ and $C_2(i,j)$ denote the gray-scale values at position (i,j) of C_1 and C_2, respectively.

Expected values of NPCR and UACI are obtained by formula (25) and (26) [24].

$$NPCR_{Expected} = \left(1 - 2^{-L}\right) \times 100\%, \tag{25}$$

$$UACI_{Expected} = \frac{1}{3}\left(1 + 2^{-L}\right) \times 100\%. \tag{26}$$

For instance, considering gray-scale pixel values (L = 8), ideal NPCR and UACI are 99.6094% and 33.4635%, respectively. With the original image of size 256×256, we calculate the NPCR and UACI of our proposal and other image encryption algorithms in Ref. [15, 24, 25, 27, 28]. As it can be seen in Table 4, the NPCR and UACI of our proposal are better than other algorithms. Based on the experiments results, our proposal can completely ensure two cipher-images different, even with only one pixel difference between the corresponding plain-images. Results demonstrate that our algorithm is able to effectively resist the differential analysis. NPCR and UACI of ours are 99.6094% and 33.4622%, which approach to expected NPCR and UACI, respectively.

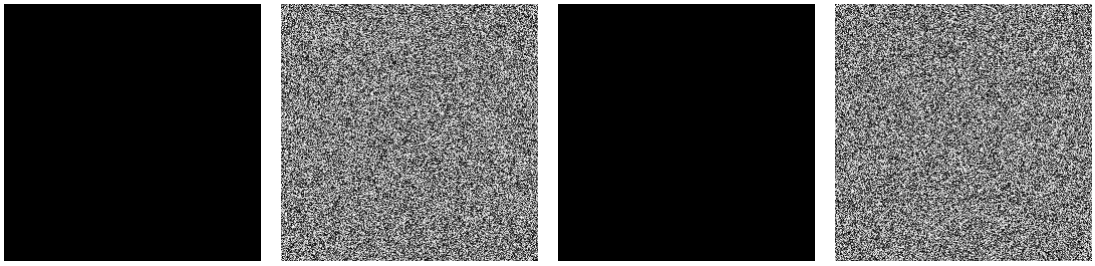
Table 4. The results of the differential analysis

Category	NPCR	UACI
Expected value	99.6094%	33.4635%
The proposed algorithm	99.6094%	33.4622%
Ref. [15]	99.5758%	33.4766%

Ref. [24]	99.6582%	33.4843%
Ref. [25]	99.6170%	33.4933%
Ref. [27]	99.6041%	33.4198%
Ref. [28]	99.6063%	33.3572%

4.7 Applicability analysis of the all-zero image

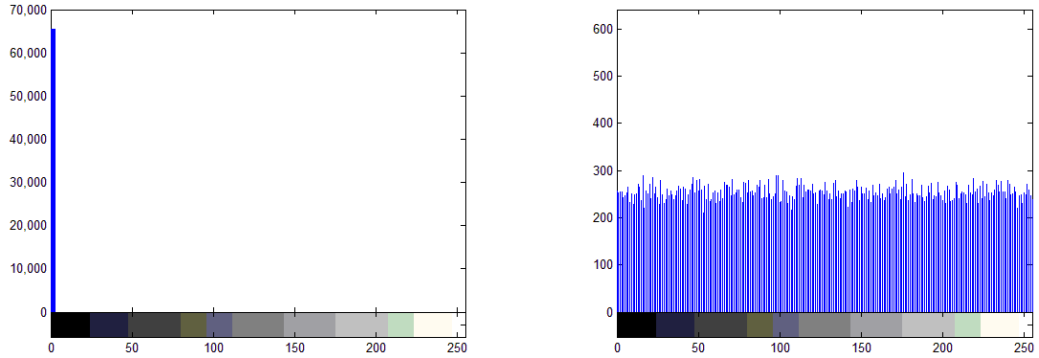
The applicability of all-zero image is an important standard to measure the algorithm, which is usually ignored in previous image encryption algorithms. In order to evaluate the key sensitivity, we encrypt the all-zero image with control parameters and initial values as mentioned above. We then add 10^{-14} to initial value x_0 of the Chen's high-dimension hyper-chaotic system (3) and decrypt the cipher-image. The results of the key sensitivity analysis is shown in **Fig. 5**. Compared with **Fig. 5(c)**, **Fig. 5(d)** performs completely different decrypted images with the wrong key. As a consequence, our algorithm holds high sensitivity to the secret key for an all-zero image.



(a) (b) (c) (d)

Fig. 5. The results of the key sensitivity analysis for the all-zero image: (a) all-zero image, (b) cipher-image, (c) correct decryption, (d) decryption with 10^{-14} changed in the initial value x_0

The distribution of pixels can be shown by the histogram analysis for an all-zero image. **Fig. 5** presents two histograms of all-zero image (**Fig. 5(a)**) and corresponding cipher-image (**Fig. 5(b)**). And results of histogram are shown in **Fig. 6**. Obviously, the gray-scale pixel values of the all-zero image (**Fig. 5(a)**) are all 0 and all gray-scale pixel values of encrypted all-zero image (**Fig. 5(b)**) almost follows uniform distribution in the [0, 255], making the statistical attack unworkable.



(a) (a)

Fig. 6. The results of the histogram analysis for the all-zero image: (a) histogram of plain-image, (b) histogram of cipher-image

For differential analysis of all-zero image, the NPCR and UACI can be computed based on formula (22), (23) and (24), which are calculated in **Table 5**. From the evaluation results, the proposed algorithm can guarantee two cipher-images different completely, even though there is only one pixel difference between the corresponding plain-images. For all-zero image, the NPCR and UACI of ours are 99.6124% and 33.4298%, which are respectively close to the expected values. Moreover, our proposal has the resilience against the chosen and known plaintext attacks.

Table 5. The results of the differential analysis for the all-zero image

Category	NPCR	UACI
Expected value	99.6094%	33.4635%
The proposed algorithm	99.6124%	33.4298%

From the above, the proposed algorithm satisfies the applicability of the all-zero image by key sensitivity analysis, histogram analysis and differential analysis.

4.8 Speed performance analysis

In this subsection, we consider the speed performance to analyze the efficiency of encryption algorithms. We realize the analysis equipped with a 2.27 GHz Intel Pentium Core 2 Duo CPU with 2 GB RAM memory and 200 GB hard-disk capacity. With the image of size 256×256, we implement the speed performance in Visual C++ under Windows 7 for our algorithm and others in Ref. [15, 24, 25, 27, 28]. As shown in **Table 6**, the speed performance of ours without the optimization is faster than other three algorithms for comparison. Thus our algorithm achieves a better eprformance with a fast manner, satisfying the required speed.

Table 6. The results of the speed performance analysis

Method	Platform	System characteristics	Time cost
The proposed algorithm	Visual C++	CPU 2.27 GHz	147 ms
Ref. [15]	Visual C++	CPU 2.27 GHz	304 ms
Ref. [24]	Visual C++	CPU 2.27 GHz	1184 ms
Ref. [25]	Visual C++	CPU 2.27 GHz	2837 ms
Ref. [27]	Visual C++	CPU 2.27 GHz	31 ms
Ref. [28]	Visual C++	CPU 2.27 GHz	137 ms

4.9 MSE and PSNR analysis

The mean square error (MSE) calculates the error between input image and output image, in which a high value corresponds to great difference between cipher-image and original image. Specially, MSE is obtained by Eq. (27) [30].

$$\mathrm{MSE} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(P(i,j) - C(i,j) \right)^2, \tag{27}$$

where $P(i,j)$ and $C(i,j)$ respectively mean the gray-scale values in the plain image P and cipher-image C. Based on the MSE, encryption quality is estimated by peak signal-to-noise ratio (PSNR) which measures the ratio between MSE and maximum intensity. In particular, PSNR is calculated by Eq. (28) for the resultant image [30].

$$\mathrm{PSNR} = 20\log_{10}\left[\frac{\mathrm{I}_{\max}}{\sqrt{\mathrm{MSE}}}\right], \tag{28}$$

in which $\mathrm{I}_{\max}$ is maximum possible for pixel value. Lower value of PSNR corresponds to bigger difference between plain image and cipher image. In order to determine the encryption quality, MSE and PSNR are respectively 7749 and 9.238 in the proposed algorithm, which satisfy the requirements.

5. Conclusion

With the assistance of our previous work, a novel chaotic image encryption algorithm based on self-adaptive model and feedback mechanism has been proposed in the present paper. Different from other existing methods, to make the distribution of initial values more uniform, the initial values of iteration are generated in a novel way by the self-adaptive model. The weakness in the selection of initial values can thereby be avoided. Besides, the feedback mechanism in the stage of diffusion has been improved. XOR between intermediate values is simplified and the piecewise linear chaotic map is first introduced for the resistance of the differential attack and the applicability of the all-zero image. Thus, balance between the resistance to differential attack and the computational complexity of algorithm has been raised to a better level. A minor change in the plain-image affects the all cryptographic operations and generates a completely different cipher-image, even though the same secret key is applied in the algorithm. In addition, proposed algorithm applies the single round permutation-diffusion to avoid leaking the information and improve the efficiency. Through simulation results and security analysis, the presented algorithm successfully guarantees high key sensitivity, tremendous key space, good encryption speed, and relisilience against common attacks, such as brute-force attack, statistical attack and chosen and known plaintext attacks. More particularly, the information entropy, NPCR and UACI of our algorithm are fairly satisfactory compared to conventional schemes. We believe that proposed algorithm satisfies the requirements of encryption quality and is an excellent candidate for practical image encryption schemes.

References

[1] Y. Wang, K. W. Wong, X. F. Liao, T. Xiang and G. R. Chen, “A chaos-based image encryption algorithm with variable control parameters,” *Chaos, Solitons & Fractals*, vol. 41, no. 4, pp. 1773-1783, 2009. Article (CrossRef Link)

[2] C. Fu, W. H. Meng, Y. F. Zhan, Z. L. Zhu, F. C. M. Lau, C. K. Tse and H. F. Ma, “An efficient and secure medical image protection scheme based on chaotic maps,” *Computers in biology and medicine*, vol. 43, no. 8, pp. 1000-1010, 2013. Article (CrossRef Link)

[3] N. K. Pareek, V. Patidar and K. K. Sud, “Cryptography using multiple one-dimensional chaotic maps,” *Communications in Nonlinear Science and Numerical Simulation*, vol. 10, no. 7, pp. 715-723, 2005. Article (CrossRef Link)

[4] Q. Mao, C. C. Chang and H. L. Wu, “An image encryption scheme based on concatenated torus automorphisms,” *KSII Transactions on Internet & Information Systems*, vol. 7, no. 6, pp. 1492-1511, 2013. Article (CrossRef Link)

[5] K. Muhammad, J. Ahmad, H. Farman, Z. Jan, M. Sajjad and S. W. Baik, "A Secure Method for Color Image Steganography using Gray-Level Modification and Multi-level Encryption," *KSII Transactions on Internet & Information Systems*, vol. 9, no. 5, pp. 1938-1962, 2015. Article (CrossRef Link)
[6] Y. J. Liu and Y. Q. Zheng, "Adaptive robust fuzzy control for a class of uncertain chaotic systems," *Nonlinear dynamics*, vol. 57, no. 3, pp. 431-439, 2009. Article (CrossRef Link)
[7] C. Q. Wang, X. Zhang and Z. M. Zheng, "Cryptanalysis and improvement of a biometric-based multi-server authentication and key agreement scheme," *PLoS One*, vol. 11, no. 2, pp. e0149173, 2016. Article (CrossRef Link)
[8] C. Q. Wang, X. Zhang and Z. M. Zheng, "A novel image encryption algorithm based on multiple chaotic systems and self-adaptive model," in *Proc. of the 2015 International Conference on Communications, Signal Processing, and Systems*, pp. 677-685, 2016.Article (CrossRef Link)
[9] O. Fatih, O. B. Ahmet and Y. Sirma, "Cryptanalysis of a novel image encryption scheme based on improved hyperchaotic sequences," *Optics Communications*, vol. 285, no. 24, pp. 4946-4948, 2012. Article (CrossRef Link)
[10] D. Xiao, X. F. Liao, S. J. Deng, "A novel key agreement protocol based on chaotic maps," *Information Sciences*, vol. 177, no. 4, pp.1136-1142, 2007. Article (CrossRef Link)
[11] C. C. Lee, C. L. Chen, C. Y. Wu and S. Y. Huang, "An extended chaotic maps-based key agreement protocol with user anonymity," *Nonlinear Dynamics*, vol. 69, no. 1, pp. 79-87, 2012. Article (CrossRef Link)
[12] C. Q. Li, Y. S. Liu, T. Xie and M. Z. Q. Chen, "Breaking a novel image encryption scheme based on improved hyper-chaotic sequences," *Nonlinear Dynamics*, vol. 73, no. 3, pp. 2083-2089, 2013. Article (CrossRef Link)
[13] C. Q. Wang, X. Zhang and Z. M. Zheng, "An improved biometrics based authentication scheme using extended chaotic maps for multimedia medicine information systems," *Multimedia Tools and Applications*, pp. 1-27, 2016. Article (CrossRef Link)
[14] C. X. Zhu, "A novel image encryption scheme based on improved hyperchaotic sequences," *Optics Communications*, vol. 285, no. 1, pp. 29-37, 2012. Article (CrossRef Link)
[15] B. Norouzi, S. Mirzakuchaki, S. M. Seyedzadeh and M. R. Mosavi, "A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion," *Multimedia tools and applications*, vol. 71, no. 3, pp. 1469-1497, 2014. Article (CrossRef Link)
[16] C. Q. Li, Y. S. Liu, T. Xie and M. Z. Q. Chen, "Breaking a novel image encryption scheme based on improved hyperchaotic sequences," *Nonlinear Dynamics*, vol. 73, no. 3, pp. 2083-2089, 2013. Article (CrossRef Link)
[17] Y. S. Zhang, D. Xiao, W. Y. Wen and M. Li, "Breaking an image encryption algorithm based on hyper-chaotic system with only one round diffusion process," *Nonlinear Dynamics*, vol. 76, no. 3, pp. 1645-1650, 2014. Article (CrossRef Link)
[18] E. Solak, C. Cokal, O. T. Yildiz and T. Biyikoglu, "Cryptanalysis of Fridrich's chaotic image encryption," *International Journal of Bifurcation and Chaos*, vol. 20, no. 5, pp. 1405-1413, 2010. Article (CrossRef Link)
[19] Y. T. Li, D. Xiao, S. J. Deng, Q. Han and G. Zhou, "Parallel Hash function construction based on chaotic maps with changeable parameters," *Neural Computing and Applications*, vol. 20, no. 8, pp. 1305-1312, 2011. Article (CrossRef Link)
[20] Y. P. Hu, C. X. Zhu and Z. J. Wang, "An improved piecewise linear chaotic map based image encryption algorithm," *The Scientific World Journal*, pp. 1-7, 2014. Article (CrossRef Link)
[21] G. R. Chen, Y. B. Mao and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749-761, 2004. Article (CrossRef Link)
[22] T. G. Gao and Z. Q. Chen, "A new image encryption algorithm based on hyper-chaos," *Physics Letters A*, vol. 372, no. 4, pp. 394-400, 2008. Article (CrossRef Link)
[23] G. Alvarez and S. J. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 8, pp. 2129-2151, 2006. Article (CrossRef Link)

[24] P. Ping, F. Xu and Z. J. Wang, "Image encryption based on non-affine and balanced cellular automata," *Signal Processing*, vol. 105, pp. 419-429, 2014. Article (CrossRef Link)
[25] X. Y. Wang and C. Q. Jin, "Image encryption using game of life permutation and PWLCM chaotic system," *Optics Communications*, vol. 285, no. 4, pp. 412-417, 2012. Article (CrossRef Link)
[26] R. J. Chen and J. L. Lai, "Image security system using recursive cellular automata substitution," *Pattern Recognition*, vol. 40, no. 5, pp. 1621-1631, 2007. Article (CrossRef Link)
[27] L. Y. Zhang, X. B. Hu, Y. S. Liu, K. W. Wong and J. Gan, "A chaotic image encryption scheme owning temp-value feedback," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 10, pp. 3653-3659, 2014. Article (CrossRef Link)
[28] V. Patidar, 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. Article (CrossRef Link)
[29] X. L. Huang and G. D. Ye, "An efficient self-adaptive model for chaotic image encryption algorithm," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 12, pp. 4094-4104, 2014. Article (CrossRef Link)
[30] C. Q. Wang, X. Zhang and Z. M. Zheng, "An efficient image encryption algorithm based on a novel chaotic map," *Multimedia Tools and Applications*, pp. 1-30, 2016. Article (CrossRef Link)
[31] C. Q. Li, "Cracking a hierarchical chaotic image encryption algorithm based on permutation," *Signal Processing*, vol. 118, pp. 203-210, 2016. Article (CrossRef Link)
[32] Z. X. Qian, H. Zhou, X. P. Zhang and W. M. Zhang, "Separable Reversible Data Hiding in Encrypted JPEG Bitstreams," *IEEE Transactions on Dependable and Secure Computing*, pp. 1-13, 2016. Article (CrossRef Link)
[33] Z. X. Qian, X. P. Zhang and S. Z. Wang, "Reversible data hiding in encrypted JPEG bitstream," *IEEE transactions on multimedia*, vol. 16, no. 5, pp. 1486-1491, 2014. Article (CrossRef Link)

Xiao Zhang received the Ph.D degree from Beihang University, Beijing, China, in 2013. She is currently the associate professor of Mathematics at Beihang University and the member of Key Laboratory of Mathematics, Informatics and Behavioral Semantics, Ministry of Education. Her research interests include cryptography, information security and complex information system.

Chengqi Wang received the B.S. degree with distinction from Beihang University, Beijing, China, in 2012. He is currently a Ph.D. candidate at Key Laboratory of Mathematics, Informatics and Behavioral Semantics and School of Mathematics and Systems Science, Beihang University. His research interests include network security and applied cryptography.

Zhiming Zheng received the Ph.D. degree from Peking University, Beijing, China, in 1987. He is currently the Professor of Mathematics at Beihang University and the Director of Key Laboratory of Mathematics, Informatics and Behavioral Semantics, Ministry of Education. His research interests include information security, complex information system, and dynamic system. He is the Editor in Chief of the journal Mathematical Biosciences and Engineering published by SPRINGER, and the journal Mathematics in Computer Science published by BIRKHAUSER.