A Novel Scheme for the Preview of the Image Encryption Based on Chaotic Ikeda 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 01, 2017; revised and accepted Sept. 12, 2017)

Abstract

Image encryption has been a popular research field in recent decades. This paper presents a novel scheme for the preview of the encrypted image. Using the scheme can preview the encrypted-image before decryption. So we can get to know that this image is really needed before decryption. Using the scheme can save a lot of unnecessary decryption time. To the best of our knowledge, this work is the first attempt to present such a scheme in the field of image encryption. We present the design and implementation of the scheme. The design of the proposed scheme is efficient. The experiments results show that the suggested scheme satisfies the requirement. It provides the necessary properties for a secure image encryption scheme. These characteristics make it a suitable candidate for using in cryptographic applications.

Keywords: Chaotic Ikeda Map; Image Encryption; Image Encryption Preview

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 [21, 22, 45]. In 1970s, Chaos theory was proposed, which was used in a number of research areas, such as mathematics, engineering, physics, biology, and so on. The first description of a chaotic process was made in 1963 by Lorenz [30], 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 [16].

These characteristics can be connected with some very important cryptographic properties such as confusion and diffusion, balance and avalanche properties [39].

Over the past two decades, the image encryption based on Chaos theory has become a hot research topic. A large number of digital image encryption schemes have been proposed with demonstrated success. The classic encryption architecture based on chaotic map has been investigated. Researchers have proposed many chaos-based digital image encryption schemes [2, 8, 9, 12, 20, 28, 29, 34, 38, 43, 49], which utilize chaotic maps. Jawad and his research group promoted a chaotic map-embedded Blowfish algorithm for security enhancement of color image encryption [25]. Mao and his research group proposed a new color image encryption scheme based on chaotic nonlinear adaptive filter [19]. Mirzaei and his research group designed a parallel encryption algorithm based on hyper chaos [31]. Haroun's real-time image encryption used a low-complexity discrete 3D dual chaotic cipher [18]. Xiao-Jun Tong and his partner proposed an image encryption algorithm based on cross chaotic map [40]. Guodong Ye's chaotic image encryption algorithm using wave-line permutation and block diffusion [47].

The average decryption time of images with different sizes is different. The larger the encrypted image is, the longer it takes to decrypt. Decrypting a 2048 × 2048 image takes about 50 times as much time as a 256 × 256 image [6, 7, 13, 33]. So how do we get to know that this image is really what we need before decryption? In order to solve this problem, this paper gives a novel solution. Before decryption, we can decrypt the key region that has been set up in advance, so as to find out if it is the image we are interested in. We can manually or automatically select one or more key regions of the image that will be encrypted. We encrypt the key region image and the entire image separately. The two encrypted images are combined into an encrypted image. The image segmentation and recognition algorithm will be employed.

The organization of this paper is as follows: Section 2 presents the related works. In Section 3, the details of our scheme are proposed. The experimental results are introduced in Section 4. The security discussion is shown in Section 5. Finally, the conclusions are drawn in Section 6.

2 Related Works

We categorize the related work into three topics, and each topic is summarized separately.

2.1 Image Encryption

There are many image encryption algorithms. They have some common characteristics, which are some very important cryptographic properties such as confusion and diffusion, balance and avalanche properties. In [28], we proposed an encryption algorithm based on chaotic tent map. In [26], Manish and his team presented a new algorithm for image security using ECC (Elliptic Curve Cryptography) diversified with DNA encoding. Zang *et al.* suggested a novel optical image encryption algorithm, which based on spatially incoherent illumination [48]. Akhavan and his partners proposed a novel parallel hash function based on 3D chaotic map [4]. Choosing a suitable image encryption algorithm is not difficult.

In this paper, we presents an image encryption algorithm, which is based on the chaotic Ikeda map. The design of the proposed algorithm is simple and efficient. It provides the necessary properties for a secure image encryption algorithm including the confusion and diffusion properties. We use well-known ways to perform the security and performance analysis of the proposed image encryption algorithm. Simulation results show that the suggested algorithm 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 algorithm is efficient and secure. These characteristics make it a suitable candidate for using in cryptographic applications.

In physics and mathematics, the Ikeda map is a discrete-time dynamical system given by the complex map [23]. The original map was proposed first by Ikeda as a model of light going around across a nonlinear optical resonator in a more general form. In 1979, Kensuke Ikeda did an experiment on brain simulation [24]. The result confirms that the Ikeda model with its multiple extrema nonlinear function is a good candidate for chaos generation dedicated to encryption [27].

$$z_{n+1} = A + Bz_n e^{i(|z_n|^2+C)}. \tag{1}$$

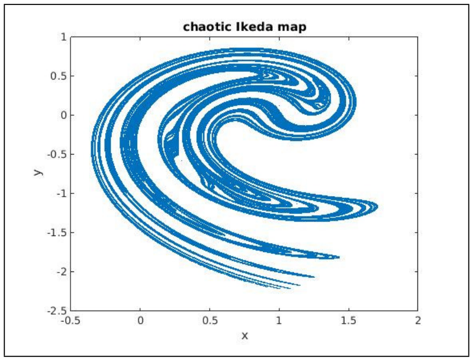

Figure 1: The image of the chaotic Ikeda map

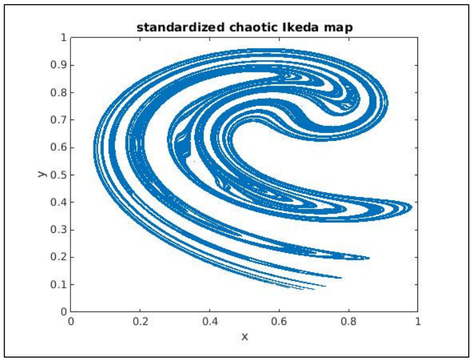

Figure 2: The image of the standardized chaotic Ikeda map

The complex Ikeda map is reduced to the above simplified form by Ikeda, Daido and Akimoto. Where z_n stands for the electric field inside the resonator at the n-th step of rotation in the resonator, A, B and C are parameters which indicate laser light applied from the outside, and linear phase across the resonator, respectively. In particular the parameter $B \leq 1$ is called dissipation parameter characterizing the loss of resonator, and in the limit of B = 1 the Ikeda map becomes a conservative map.

A 2D real example of the complex map is:

$$x_{n+1} = 1 + \mu(x_n cost_n - y_n sint_n) \tag{2}$$

$$y_{n+1} = \mu(x_n sint_n - y_n cost_n) \tag{3}$$

where μ is a parameter and $t_n = 0.4 - \frac{6}{1+x_n^2+y_n^2}$.

For $\mu \geq 0.6$, this system has a chaotic attractor. The Ikeda map has the dynamical behavior of nonlinear systems.

Using MATLAB in the experiments, the Ikeda equation parameter μ was selected as $\mu = 0.9$, in this case the system has a chaotic behavior. Figure 1 shows trajectories of 10000 random points for various values.

In order to apply the chaotic Ikeda map to image encryption, we made the transformation, let all $x_n \in (0, 1)$ and $y_n \in (0, 1)$, $n \in [0,1,2,\cdots]$, showing in Figure 2.

2.1.1 The Image Encryption Algorithm

In this section, we use the chaotic Ikeda map Equation (2) and Equation (3) to implement encryption process. This paper proposes an image encryption algorithm includes the following main steps:

1) Read plain-images (original-image) ($P_{a\times b\times c}$), get size of P, *e.g.* using $[a, b, c]$ save size of P, let $N = a*b*c$, let $x(0) = 0.100001$, $y(0) = 0.100003$;

2) Input the secret (encryption) key μ into the chaotic ikeda map equation. Iterate the chaotic ikeda map N times using system Equation (2) and Equation (3), obtain an array $X_{(N)}$ and $Y_{(N)}$;

3) Confusion: Change $X_{(N)}$ into $[0, 255]$ using $X_{(N)} * 1000 \ mod \ 256$, we can get $C_{X_{(P)}} = X_{(N)} \ XOR \ P_{a\times b\times c}$;

4) Diffusion: $C_{Y_{(P)}} = Y_{(N)} * C_{X_{(P)}}$;

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

2.1.2 The Image Decryption Algorithm

In this section, we use the chaotic Ikeda map Equation (2) and Equation (3) to implement decryption process. This paper proposes an image decryption algorithm includes the following main steps:

1) Read ciphered-images (encrypted-image) ($C_{a\times b\times c}$), get size of C, *e.g.* using $[a, b, c]$ save size of C, let $N = a * b * c$, let $x(0) = 0.100001$, $y(0) = 0.100003$, here $x(0)$ and $y(0)$ must be same as encryption process;

2) Input the secret (encryption) key μ into the chaotic ikeda map equation. Iterate the chaotic ikeda map N times using system Equation (2) and Equation (3), obtain an array $X_{(N)}$ and $Y_{(N)}$;

3) Inverse confusion: Change $X_{(N)}$ into $[0, 255]$ using $X_{(N)} * 1000 \ mod \ 256$, we can get $P_{X_{(C)}} = X_{(N)} \ XOR \ C_{a\times b\times c}$;

4) Inverse diffusion: $P_{Y_{(C)}} = P_{X_{(C)}} * Y^{-1}_{(N)}$;

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

2.2 Image Segmentation

Many image segmentation techniques are available in the articles [1, 11]. They proposed a number of related algorithms and schemes. In [17], a novel method is proposed for performing multi-label, interactive image. In [10], Boykov and his partners focused on possibly the simplest application of graph-cuts: segmentation of objects in image data. Vese and his research group proposed a new multiphase level set framework for image segmentation using the Mumford and Shah model, for piecewise constant and piecewise smooth optimal approximations [42]. We can choose an image segmentation algorithm for image segmentation.

2.3 Image Recognition

Image recognition technology has been studied by many scholars in recent years. In [37], Shi and his research group proposed a novel approach for learning coupled mappings to improve the performance of low-resolution (LR) face image recognition. In [46], Wu and his research partners presented a state-of-the-art image recognition system, Deep Image, developed using end-to-end deep learning. In [41], a neural network model, the hyper-column model (HCM), which is applicable to general image recognition, was proposed by Tsuruta and his partners. We can choose an image recognition algorithm to automatically select the feature regions from the image.

3 Proposed Scheme

Before introducing the preview scheme, we first introduce a definition that is the Preview-Region-Image. The Preview-Region-Image is the key region which is a part of the original image. Then we can find out if the original image is the image we are interested in.

We can manually or automatically select one or more Preview-Region-Image from the original image that will be encrypted. The Preview-Region-Image and the original image are encrypted separately. The two encrypted images are combined into an encrypted image. The decryption process is exactly the opposite of the encryption process. In order to preview the image, we extract and decrypt the encrypted Preview-Region-Image from the encrypted image. Details are given in the following encryption and decryption schemes.

3.1 The Image Encryption Preview Scheme

In this section, we give the processing flow of the image encryption scheme. The flowchart of the image encryption scheme is shown in Figure 3. This paper proposes an image encryption scheme which includes the following main steps:

1) Select the Preview-Region-Image. Two methods of selection can be used. Get the original image I$[a \times b \times c]$, $c = 2$ or 3.

   - Using the mouse click spot as the center manually selects a region.

     a. $a > 256$ and $b > 256$, selects a region ($256 \times 256 \times c$), save to an array K$[256 \times 256 \times c]$;

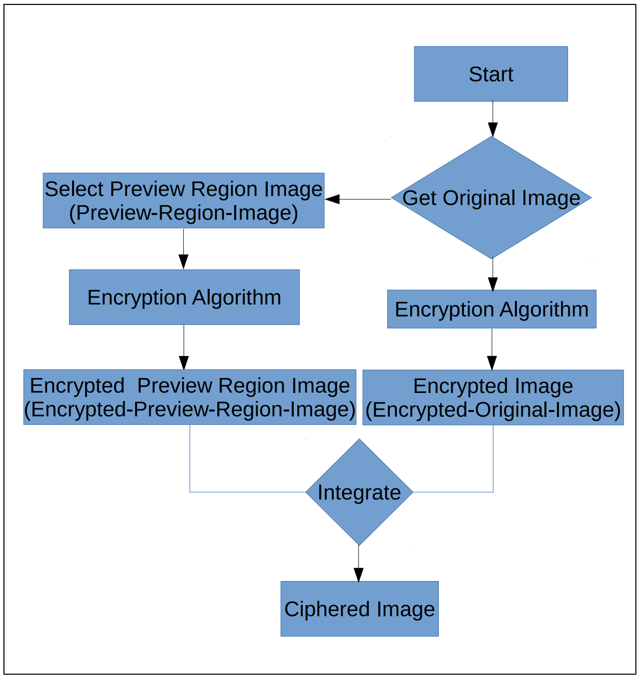
Start
Get Original Image
Select Preview Region Image (Preview-Region-Image)
Encryption Algorithm
Encryption Algorithm
Encrypted Preview Region Image (Encrypted-Preview-Region-Image)
Encrypted Image (Encrypted-Original-Image)
Integrate
Ciphered Image

Figure 3: The flowchart of the image encryption scheme

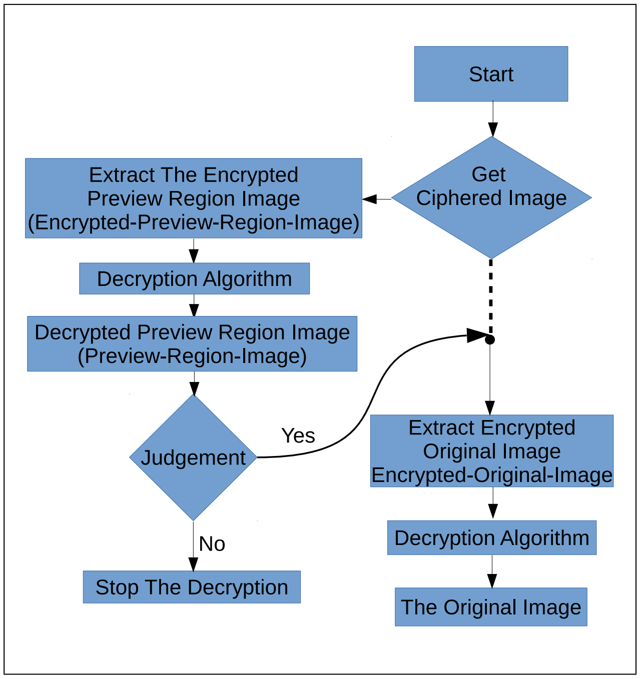
Start
Get Ciphered Image
Extract The Encrypted Preview Region Image (Encrypted-Preview-Region-Image)
Decryption Algorithm
Decrypted Preview Region Image (Preview-Region-Image)
Judgement
Yes
No
Stop The Decryption
Extract Encrypted Original Image Encrypted-Original-Image
Decryption Algorithm
The Original Image

Figure 4: The flowchart of the image decryption scheme

b. $a > 256$ and $b < 256$, selects a region $(256 \times b \times c)$, save to an array K$[256 \times b \times c]$;

c. $a < 256$ and $b < 256$, selects a region $(a \times b \times c)$, save to an array $K[a \times b \times c]$;

d. standardize the array K to $SK[256 \times 256 \times c]$, insufficient 0 fill. the array $SK[256 \times 256 \times c]$ is named as Preview-Region-Image, before we encrypt the original image.

- Before encrypting the original image ($I[a \times b \times c]$), we can use image recognition technology to automatically select a Preview-Region-Image from the original image, and standardize to $SK[256 \times 256 \times c]$, insufficient 0 fill.

2) Encryption. Using the image encryption algorithm. We encrypt the Preview-Region-Image ($SK[256 \times 256 \times c]$) that is selected in step (1), named as Encrypted-Preview-Region-Image ($CSK[256 \times 256 \times c]$). Encrypt the original image, named as Encrypted-Original-Image ($CI[a \times b \times c]$).

3) Integration. In this step, we integrate two encrypted images (Encrypted-Preview-Region-Image $CSK[256 \times 256 \times c]$ and Encrypted-Original-Image $CI[a \times b \times c]$) save to the array $C[(a + (256 \times 256/b)) \times b \times c]$. We place Encrypted-Preview-Region-Image (the encrypted preview region image) in front of Encrypted-Original-Image (the encrypted original image).

3.2 The Image Decryption Preview Scheme

In this section, we give the processing flow of the image decryption scheme. Before decryption, we first decrypt Encrypted-Preview-Region-Image to preview the original image. The flowchart of the image decryption scheme is shown in Figure 4. This paper proposes an image decryption scheme which includes the following main steps:

1) Extract the encrypted preview image. Extract the Encrypted-Preview-Region-Image $CSK[256 \times 256 \times c]$ from the encrypted image $C[(a + (256 \times 256/b)) \times b \times c]$, Get the image region (its size is $256 \times 256 \times 3$), namely, the Encrypted-Preview-Region-Image $CSK[256 \times 256 \times c]$, from the beginning of the encrypted image $C[(a + (256 \times 256/b)) \times b \times c]$;

2) Decrypt the encrypted preview image. Decrypt the Encrypted-Preview-Region-Image (the encrypted preview image) $CSK[256 \times 256 \times c]$, get the Preview-Region-Image (the preview region image) $SK[256 \times 256 \times c]$, and show it;

3) Decrypt the encrypted original image. In Step 2, if we find that this image is the image we need. Extract the Encrypted-Original-Image (the entire encrypted original image) $CI[a \times b \times c]$) from the encrypted image $C[(a + (256 \times 256/b)) \times b \times c]$, and decrypt it. In Step 2, if we find that this image is not the image we need, stop the decryption.

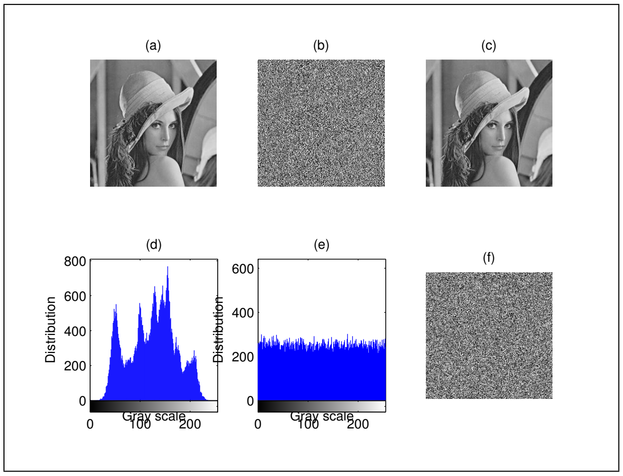

Figure 5: (a) The original image; (b) The encrypted image; (c) The decrypted image; (d) The histogram of original image; (e) The histogram of ciphered image; (f) The decrypted image with wrong key.

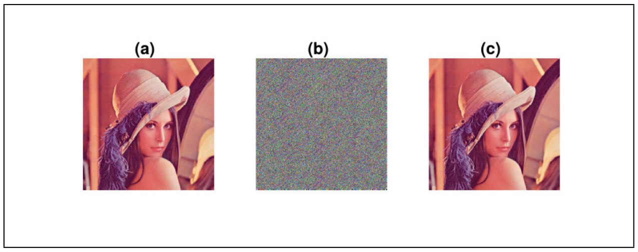

Figure 6: (a) The original image; (b) The encrypted image; (c) The decrypted image.

4 Experimental Results

4.1 Experimental Results of The Image Encryption

The efficiency of the proposed image encryption algorithm is shown in the following experimental results. The standard gray scale image Lenna (Figure 5(a)) with the size 256 × 256 pixels is used for this experiment.

The results of the encryption are presented in Figure 5(b). As can be seen from the encrypted image Figure 5(b), there are no patterns or shadows visible in the corresponding cipher image. The result of the decryption is presented in Figure 5(c). As can be seen from the decrypted image Figure 5(c), it is not different from the original image.

The color image Lenna with the size $512 \times 512 \times 3$ pixels is used for this experiment. The Figure 6(a) is the color image of Lenna, Figure 6(b) is the encrypted color image of Lenna, and Figure 6(c) shows the decrypted color image of Lenna from Figure 6(b).

The result of the decryption using wrong key is presented in Figure 5(f). As can be seen from the Figure 5(f), there are no patterns or shadows visible in the corresponding ciphered image.

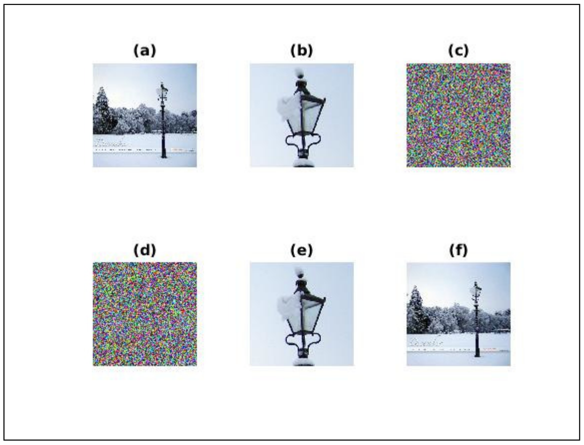

Figure 7: (a) The original image ($1024 \times 1024 \times 3$); (b) The preview region image ($256 \times 256 \times 3$); (c) The encrypted preview region image; (d) The integrated encrypted image; (e) The decrypted preview region image; (f) The decrypted original image.

4.2 Experimental Results of The Image Encryption Preview Scheme

The efficiency of the proposed image encryption preview scheme is shown in the following experimental results. The color images with different sizes are used in this experiment.

The color image with the size $1024 \times 1024 \times 3$ is used in this experiment. The Figure 7(a) is the color image of street lamp in snow ($1024 \times 1024 \times 3$), Figure 7(b) is the preview region image ($256 \times 256 \times 3$), which is a party selected from Figure 7(a), Figure 7(c) shows the encryption of Figure 7(b), Figure 7(d) shows the integrated encrypted image (include the encryption of the preview region image and the entire encrypted original image), Figure 7(e) shows the preview of the encryption image, Figure 7(f) shows the decrypted color image of street lamp in snow.

We have also done another experiments using the color image with the size $2048 \times 2048 \times 3$, as shown in Figure 8.

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.

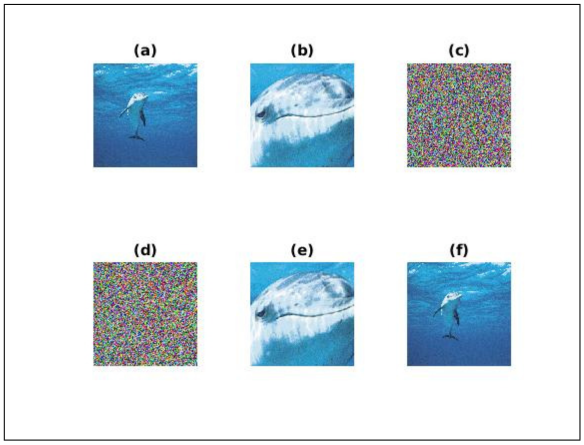

Figure 8: (a) The original image (2048×2048×3); (b) The preview region image (256 × 256 × 3); (c) The encrypted preview region image; (d) The integrated encrypted image; (e) The decrypted preview region image; (f) The decrypted original image.

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:

$$T(\mu, x_0, y_0) = \theta(\mu \times x_0 \times y_0),$$

where $x_0 \in [0, 1]$, $y_0 \in [0, 1]$, $\mu \geq 0.6$, the each precision of x_0, y_0 and μ is 10^{-16}, namely, the size of key space is 2^{160} $(((10^{16})^3))$. This key space is big enough for brute-force attacks [32]. In this scheme, we take the key to the original as follows: $x_0 = 0.100001$, $y_0 = 0.100003$, $\mu = 0.9000000001$. When taking the wrong key: the difference between wrong and right key is 10^{-16}. For example, using $\mu = 0.9000000001000001$ as the wrong key to decrypt the encryption image, we get a wrong decrypted image shown in Figure 5(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 Lenna image (its size is 256 × 256) as the original image. Histogram of the original Lenna image and the corresponding ciphered Lenna image are shown in Figures 5(d) and 5(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 [44]. We analyze the correlation between adjacent pixels in original and ciphered Lenna image. We calculate the correlation coefficient in the horizontal, vertical and diagonally, the following relation is used [5]:

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

Direction	Original image	Ciphered image
Horizontal	0.9302	0.0057
Vertical	0.8367	0.0041
Diagonal	0.8623	0.0032

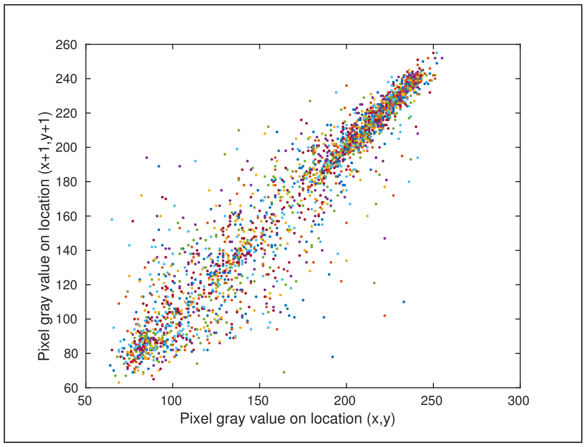

Figure 9: Correlation analysis of original image

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

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 9 and 10.

5.4 Information Entropy

Information theory is a mathematical theory founded in 1949 by Shannon [36]. 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:

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

where $P(s_i)$ represents the probability of symbol s_i and the entropy is expressed in bits. The ideal entropy value

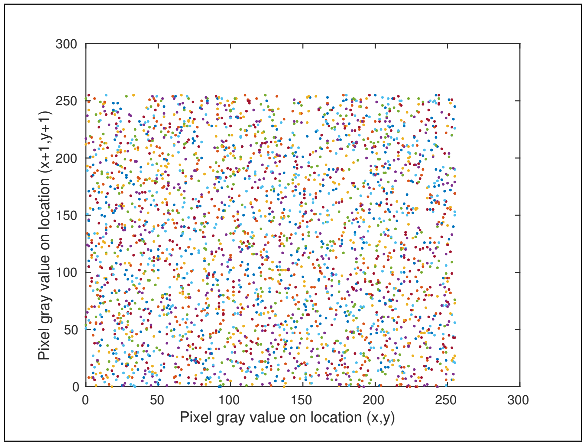

Figure 10: Correlation analysis of encrypted image

for an encrypted image should be 8. The calculation of entropy for the ciphered image (Figure 5(b)) is presented below:

$$H(s) = \sum_{i=0}^{255} P(s_i)\log_2 \frac{1}{P(s_i)} = 7.9986387.$$

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 [44]. 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 $UACI$ [14]. $NPCR$ 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 [35]:

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

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 $x_0 = 0.1000010000000001$,$y_0 = 0.100003$ to $y_0 = 0.1000030000000001$) $NPCR$ is calculated. We obtained $NPCR = 0.00351$ $(1 - NPCR = 0.99649)$ and $UACI = 0.367$. 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 [3]. 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 ($\mu = 0.9000000001$ versus $\mu = 0.9000000000000001$). The calculated value of $NPCR$ for the proposed algorithm is 0.003169 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 [15].

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. The average time of the image encryption preview scheme taken by the algorithm for different-sized images is shown in the Table 3.

6 Conclusion

In this paper we concentrate on the field of image encryption. The image encryption and decryption preview schemes have been given. In this scheme, we presented a method to preview the encrypted image before entire decryption. Using the scheme can save a lot of unnecessary decryption time. Experimental results show that

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

Images size(pixels)	Bits/pixels	Ciphered time(s)
$256 \times 256 \times 3$	24	0.53-0.68
$512 \times 512 \times 3$	24	2.92-3.06
$1024 \times 1024 \times 3$	24	10.57-13.23
$2048 \times 2048 \times 3$	24	33.80-39.75

Table 3: Average ciphering preview time taking of a few different size images

Images size(pixels)	Bits/pixels	Ciphered time(s)
$256 \times 256 \times 3$	24	0.53-0.68
$512 \times 512 \times 3$	24	0.55-0.71
$1024 \times 1024 \times 3$	24	0.63-0.76
$2048 \times 2048 \times 3$	24	0.67-0.82

the scheme is efficient and usable for the preview of the image encryption. To the best of our knowledge, this is the first attempt to present such a scheme in the field of image encryption. The advantage of this scheme is that it is possible to know whether the encrypted image is the image we need. The disadvantage is that the encrypted preview image also takes up more storage spaces. Following up, we will try to solve this defect. One possible solution is that we use the encrypted preview image to replace the corresponding part of the original encrypted image.

Acknowledgments

This work is supported by the foundation of science and technology department of Sichuan province NO.2016GZ0077 and NO.2017JY0007.

References

[1] E. Aghajari and G. D. Chandrashekhar, "Self-organizing map based extended fuzzy c-means (seefc) algorithm for image segmentation," *Applied Soft Computing*, vol. 54, pp. 347–363, 2017.

[2] A. Akgul, H. Calgan, I. Koyuncu, I. Pehlivan, and A. Istanbullu, "Chaos-based engineering applications with a 3d chaotic system without equilibrium points," *Nonlinear Dynamics*, vol. 84, no. 2, pp. 481–495, 2015.

[3] 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.

[4] A. Akhavan, A. Samsudin, and A. Akhshani, "A novel parallel hash function based on 3d chaotic map," *EURASIP Journal on Advances in Signal Processing*, vol. 2013, no. 1, pp. 126, 2013.

[5] A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel block cipher based on hierarchy of one-dimensional composition chaotic maps," in *IEEE International Conference on Image Processing*, pp. 1993–1996, 2006.

[6] M. Amin, O. S. Faragallah, and A. A. A. El-Latif, "A chaotic block cipher algorithm for image cryptosystems," *Communications in Nonlinear Science & Numerical Simulation*, vol. 15, no. 11, pp. 3484–3497, 2010.

[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] A. Belazi, A. A. A. El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, 2016.

[9] 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.

[10] Y. Boykov and G. Funkalea, "Graph cuts and efficient n-d image segmentation," *International Journal of Computer Vision*, vol. 70, no. 2, pp. 109–131, 2006.

[11] L. Caponetti and G. Castellano, *Image Segmentation*, Springer International Publishing, 2017.

[12] C. C. Chang, M. S. Hwang, and T. S. Chen, "A new encryption algorithm for image cryptosystems," *Journal of Systems & Software*, vol. 58, no. 2, pp. 83–91, 2001.

[13] G. Chen, Y. 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.

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

[15] A. A. A. El-Latif, L. Li, and X. Niu, "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.

[16] J. Gleick, "Chaos: Making a new science," *The Quarterly Review of Biology*, vol. 56, no. 64, pp. 1053–1054, 1989.

[17] L. Grady, "Random walks for image segmentation," *IEEE Transactions on Pattern Analysis & Machine Intelligence*, vol. 28, no. 11, pp. 1768, 2006.

[18] M. F. Haroun 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.

[19] H. I. Hsiao and J. Lee, "Color image encryption using chaotic nonlinear adaptive filter," *Signal Processing*, vol. 117, no. C, pp. 281–309, 2015.

[20] H. I. Hsiao and J. Lee, "Fingerprint image cryptography based on multiple chaotic systems," *Signal Processing*, vol. 113, pp. 169–181, 2015.

[21] 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.

[22] M. S. Hwang, C. C. Chang, K. F. Hwang, "Digital watermarking of images using neural networks", *Journal of Electronic Imaging*, vol. 9, no. 4, pp. 548–556, Jan. 2000.

[23] K. Ikeda, H. Daido, and O. Akimoto, "Optical turbulence: Chaotic behavior of transmitted light from a ring cavity," *Physical Review Letters*, vol. 45, no. 9, pp. 709–712, 1980.

[24] K. Ikeda, "Multiple-valued stationary state and its instability of the transmitted light by a ring cavity system," *Optics Communications*, vol. 30, no. 2, pp. 257–261, 1979.

[25] L. M. Jawad and G. Sulong, "Chaotic map-embedded blowfish algorithm for security enhancement of colour image encryption," *Nonlinear Dynamics*, pp. 1–15, 2015.

[26] M. Kumar, A. Iqbal, and P. Kumar, "A new RGB image encryption algorithm based on dna encoding and elliptic curve diffieVhellman cryptography," *Signal Processing*, vol. 125, pp. 187–202, 2016.

[27] L. Larger, J. P. Goedgebuer, and V. Udaltsov, "Ikeda-based nonlinear delayed dynamics for application to secure optical transmission systems using chaos," *Comptes rendus - Physique*, vol. 5, no. 6, pp. 669–681, 2004.

[28] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 127–133, 2017.

[29] L. H. Liu and Z. J. Cao, "Analysis of two confidentiality-preserving image search schemes based on additive homomorphic encryption," *International Journal of Electronics & Information Engineering*, vol. 5, 2016.

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

[31] O. Mirzaei, M. Yaghoobi, and H. Irani, "A new image encryption method: parallel sub-image encryption with hyper chaos," *Nonlinear Dynamics*, vol. 67, no. 67, pp. 557–566, 2012.

[32] 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.

[33] V. Patidar, N. K. Pareek, and K. K. Sud, "A new substitutionVdiffusion based image cipher using chaotic standard and logistic maps," *Communications in Nonlinear Science & Numerical Simulation*, vol. 14, no. 7, pp. 3056–3075, 2009.

[34] 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*, vol. 19, no. 1, pp. 47-59, 2016.

[35] P. Schneier, Bruce/Sutherland, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Wiley, 1995.

[36] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[37] J. Shi and C. Qi, "From local geometry to global structure: Learning latent subspace for low-resolution face image recognition," *IEEE Signal Processing Letters*, vol. 22, no. 5, pp. 554–558, 2015.

[38] 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.

[39] J. C. Sprott, *Chaos and Time-Series Analysis*, Oxford University Press, 2003.

[40] X. J. Tong, Z. Wang, M. Zhang, and Y. Liu, "A new algorithm of the combination of image compression and encryption technology based on cross chaotic map," *Nonlinear Dynamics*, vol. 72, no. 1-2, pp. 229–241, 2013.

[41] N. Tsuruta, R. I. Taniguchi, and M. Amamiya, "Hypercolumn model: A combination model of hierarchical self?organizing maps and neocognitron for image recognition," *Systems and Computers in Japan*, vol. 31, no. 2, pp. 49–61, 2015.

[42] L. A. Vese and T. F. Chan, "A multiphase level set framework for image segmentation using the mumford and shah model," *International Journal of Computer Vision*, vol. 50, no. 3, pp. 271–293, 2002.

[43] X. Wang and H. L. Zhang, "A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems," *Nonlinear Dynamics*, vol. 83, no. 1-2, pp. 333–346, 2016.

[44] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, "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.

[45] 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.

[46] R. Wu, S. Yan, Y. Shan, Q. Dang, and Gang Sun, "Deep image: Scaling up image recognition," *Computer Science*, 2015. DOI: 10.1038/nature0693.

[47] G. Ye, H. Zhao, and H. Chai, "Chaotic image encryption algorithm using wave-line permutation and block diffusion," *Nonlinear Dynamics*, vol. 83, no. 4, pp. 1–11, 2015.

[48] J. Zang, Z. Xie, and Y. Zhang, "Optical image encryption with spatially incoherent illumination," *Optics Letters*, vol. 38, no. 8, pp. 1289, 2013.

[49] H. Zhu, X. Zhang, H. Yu, C. Zhao, and Z. Zhu, "An image encryption algorithm based on compound homogeneous hyper-chaotic system," *Nonlinear Dynamics*, pp. 1–19, 2017.

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.