Egyptian Informatics Journal 20 (2019) 45–54

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Full length article

A novel image encryption scheme based on 3D bit matrix and chaotic map with Markov properties☆

Meng Ge, Ruisong Ye *

Department of Mathematics, Shantou University, Shantou, Guangdong 515063, PR China

ARTICLE INFO

Article history:
Received 22 June 2017
Accepted 7 October 2018
Available online 17 October 2018

Keywords:
Image encryption
Chaotic map
Markov property
Lorenz system
Logistic map

ABSTRACT

Based on 3D cat map, reverse 3D cat map and an improved class of chaotic maps with Markov properties, an effective bit-level image encryption scheme is proposed. Firstly, we convert the plain-image into binary matrix, and use the sum of all bits in the binary matrix as a part of secret keys to resist chosen-plaintext attack and known-plaintext attack. Secondly, we design a mapping which maps a random bit position to another random bit position rather than using traditional sequential visiting the plain-image. Thirdly, a chaotic map with Markov properties is used in the diffuse process. This kind of chaotic map has good chaotic natures than the Logistic map, which keeps the uniformity and low autocorrelation. The results of simulation and security analysis show that the proposed image encryption scheme is able to resist various attacks and has excellent encryption performance.

1. Introduction

Along with the rapid development of multimedia processing and Internet, more and more images are transmitted, shared and stored on the Internet. The information security has been a serious problem in the practical digital world. The cryptography techniques like DES, AES, IDEA, etc. are good algorithms for text encryption, but they are unsuitable for image encryption [1,2]. Due to the properties of ergodicity, unpredictability, and high sensitivity to initial conditions and system parameters that can be employed in encryption algorithm with satisfied efficiency and security, chaotic systems have been extensively researched for digital image encryption [3]. In 1998, Fridrich firstly proposed a chaos-based image encryption algorithm composing of two stages: permutation and diffusion [4]. The permutation stage is used to rearrange the positions of pixels in the image. It will change the image structure and weaken the correlation of adjacent pixels. The diffusion stage is used to change the image pixel values to random values. The design of image encryption algorithms almost always followed this model nowadays [5,6]. However, the image encryption algorithm in [4] was broken by Ercan Solak et al. in 2010 [7]. The drawbacks of the typical Fridrich's algorithm include several aspects. 1) The permutation and diffusion are independent with each other; 2) The diffusion function may be too simple to break; 3) The key streams are not related to the plain-image. Some chaos-based image encryption algorithms with a permutation-diffusion structure are practically weak to resist common cryptanalysis [8]. To overcome these drawbacks in the existing chaos-based image encryption schemes, many researchers turn to design improved chaos-based cryptosystems with large key spaces and efficient permutation-diffusion mechanisms.

Ye proposed an image encryption scheme with an efficient permutation-diffusion mechanism, which shows good performance, including huge key space, efficient resistance against statistical attack, differential attack, known-plaintext as well as chosen-plaintext attack [9]. In both the permutation and diffusion stages, generalized Arnold maps with real number control parameters are applied to generate pseudo-random sequences and therefore enlarge the key space greatly. Meanwhile, a two-way diffusion operation is executed to improve the security of the diffusion function. Chen et al. proposed a novel chaos-based image encryption algorithm with a dynamic state variables selection mechanism in [10]. This cryptosystem can satisfy the security

* Corresponding author.
E-mail address: rsye@stu.edu.cn (R. Ye).

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

Production and hosting by Elsevier

☆ This research is supported by National Natural Science Foundation of China (No. 11771265).

https://doi.org/10.1016/j.eij.2018.10.001
1110-8665/

requirements suggested in [3]. Wei Zhang et al. put forward a nonlinear traverse on the plain-image using dependent diffusion and reverse cat map to replace the traditional linear traverse performed in the confusion phase [11]. And the confusion and diffusion phases are mixedly performed, so the drawback of the conventional permutation-diffusion architecture is overcome. A class chaotic maps with Markov properties were studied and the related image encryption algorithm was also proposed [12]. Such a kind of chaos has higher complexity than the Logistic map and Sine map, which keeps the uniformity and low autocorrelation. Because the bit-level permutation can change the position and value of a pixel simultaneously, a variety of bit-level image encryption system had been proposed as well [14–17]. Bit level permutation (BLP) [15] is a new approach that is employed at the confusion stage of image encryption. In [16], a new 3D permutation algorithm based on a coupled Chen system and a 3D chaotic map is introduced. [17] introduces a novel bit-level image encryption scheme that is based on cyclic shift, swapping and PWLCM chaotic maps. In this algorithm the bits in one bit group can be permuted into the other bit groups.

In this paper, we proposed an effective bit-level image encryption algorithm based on 3D cat map, reverse 3D cat map and an improved class of chaotic maps with Markov properties. In the permutation stage, we use Lorenz system to generate the parameters of 3D cat map. To resist the exhaustive and differential attack, we use the sum t of all the bits as a part of the 3D cat map's parameters. The reverse 3D cat map and the 3D cat map govern the permutation stage. In this process, not only the bit position but also the pixels values can be modified simultaneously. In the diffusion phase, an improved class of chaotic maps with Markov properties is used. It can be proved that the map generates a uniformly distributed sequence whose autocorrelation function is δ-like. It has no fixed point which can weaken the weak-key's affect. Compared to the Logistic map, tent map, and sine map, it is more complex. As the key streams generated are related to the plain-image content, the proposed image encryption algorithm show robust resistance against chosen-plaintex attack as well as known-plaintext attacks.

The rest of the paper is organized as follows. In Section 2, Lorenz system, 3D cat map, and an improved class of chaotic maps with Markov properties are introduced. The proposed encryption and decryption algorithms are illustrated in Section 3. Experimental results and performance analysis are presented in Section 4. Then, the conclusions are drawn in the last section.

2. Preparatory work

2.1. Lorenz system

The Lorenz system of differential equations is one of the most famous models of nonlinear dynamics which exhibit chaotic properties for certain initial values and system parameters [18,19]. It is described by Eq. (2.1).

$$\begin{aligned}\dot{x} &= a(y-x),\\ \dot{y} &= bx - xz - y,\\ \dot{z} &= xy - cz,\end{aligned} \tag{2.1}$$

where a, b, c are the parameters. In this paper, we let $a = 10, b = 28, c = 8/3$. It is chaotic then. The initial values x_0, y_0, z_0 are treated as secret keys.

2.2. Cat map

The generalized 2D cat map is defined by

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & 1+ab \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod M, \tag{2.2}$$

where a, b are control parameters, M is the width or height of the image. In our paper, we use a 3D version cat map to realize the bit-level permutation stage. The 2D cat map is generalized to its 3D version defined by

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} 1+a_xa_zb_y & a_z & a_y+a_xa_z+a_xa_ya_zb_y \\ b_z+a_xb_y+a_xa_zb_yb_z & a_zb_z+1 & a_yb_z+a_xa_yb_yb_z+a_xa_zb_z+a_x \\ a_xb_xb_y+b_y & b_x & a_xa_yb_xb_y+a_xb_x+a_yb_y+1 \end{pmatrix} \times \begin{pmatrix} x \\ y \\ z \end{pmatrix} \bmod M, \tag{2.3}$$

where $a_x, a_y, a_z, b_x, b_y, b_z$ are all positive integers. (x, y, z) and (x', y', z') are the plain and permuted image pixel positions. And M is the width or height or length of the 3D matrix.

2.3. An improved class of chaotic map with Markov properties

The improved chaotic map with Markov properties is expressed by [20]:

$$K(x,p,\sigma) = \begin{cases} \sigma x + \frac{(i+1)-i\sigma}{p} \bmod 1,\ x \in \left[\frac{i}{p}, \frac{i+1}{p}\right), & i = 0,2,4\ldots p-3, \\ -\sigma x + \frac{i+1+\sigma(i+1)}{p} \bmod 1,\ x \in \left[\frac{i}{p}, \frac{i+1}{p}\right), & i = 1,3,5\ldots p-2, \\ \sigma x + \frac{p-\sigma(p-1)}{p} \bmod 1,\ x \in \left[\frac{p-1}{p}, 1\right]. \end{cases} \tag{2.4}$$

We divides the x-domain into p parts equally, and then every small interval goes into the other intervals after one iteration. which can construct a certain graph. The diagram of the map is shown in Fig. 1. Moreover, $p$is a prime number $p \geqslant 7$ and σ is a positive integer, and $2 \leqslant \sigma \leqslant p-1$. Then this is a class of chaotic map with Markov properties. When $p$changed, its transition graph would change, too. In this paper, one example of transition graph is shown in Fig. 2. Next, some good properties are introduced.

Proposition 1. *The map $K(x,p,\sigma)$ is a piecewise linear map with Markov partition.*

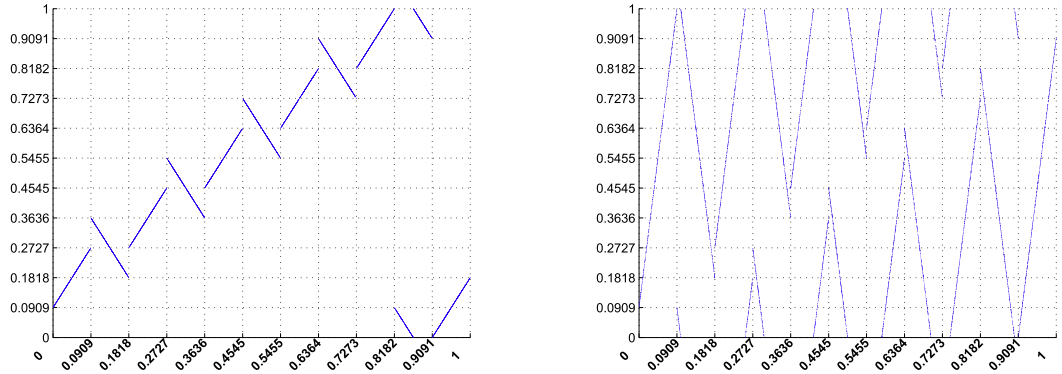
Proof. Let $A_{i+1} = [i/p, (i+1)/p]$ be the i^{th} closed interval, $i = 0, 1, 2, \ldots, p-1$. From the partition, we can see that $int(A_1), \ldots, int(A_p)$ is a collection of intervals that have disjoint interiors, i.e., $int(A_i) \cap int(A_j) = \varnothing$, for $i \neq j$. It follows from formula (2.4) and Fig. 1 that for each $i, \overline{K(A_i)} = \bigcup_{j=1}^{\sigma} A_{i+j}, i = 1, 2, \cdots p$, while $A_{i+j} = A_{i+j \bmod p}$ and if $(i+j) \bmod p = 0, A_{i+j} = A_p$. That is, if $K(\mathrm{int}(A_j)) \cap \mathrm{int}(A_i) \neq \varnothing$, then $K(A_j) \supset A_i$. According to the definition of Markov partition, Kwill be a piecewise linear map with Markov partition [13]. □

Proposition 2. *$K(x,p,\sigma)$ is sensitive dependence on initial condition.*

Proof. $K(x,p,\sigma)$ is a piecewise linear map. Let the set Bbe the jump discontinuity of the map function, while the limits on the left and right of $K(x,p,\sigma)$ exist,

$$B = \left\{ x : \lim_{x \to x^+} K(x,p,\sigma) \neq \lim_{x \to x^-} K(x,p,\sigma) \right\}.$$

If $x \notin A$, then $|K'(x)| = \sigma$. Let $l(x,K)$ be the Lyapunov exponent. It follows from the definition of Lyapunov exponent that



(a) $\sigma = 2, p = 11$ (b) $\sigma = 10, p = 11$

Fig. 1. The iteration diagram of different parameters.

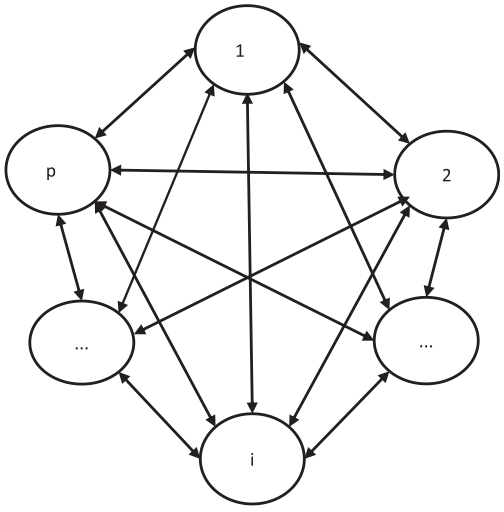


Fig. 2. transition graph with $\sigma = p - 1$.

$$l(x,K) = \lim_{n\to\infty} \frac{\sum_{j=0}^{n-1} \ln(|K'(x_j)|)}{n} = \lim_{n\to\infty} \frac{n\ln\sigma}{n} = \ln\sigma \geqslant \ln 2 > 0,$$

if $x_j = f^j(x_0) \notin A$.

The Lyapunov exponent is positive, which indicates the system has sensitive dependence. □

Proposition 3. *The chaotic map has no fixed points.*

Proof. According to the Fig. 1 and Fig. 2, the period of $K(x,p,\sigma)$ is obvious. While $\sigma = 1, p$, the period $T = \left[\frac{p}{\sigma}\right]$. Otherwise, $T = \left[\frac{p}{\sigma}\right] + 1$. In our paper, $2 \leqslant \sigma \leqslant p-1$, so $T = \left[\frac{p}{\sigma}\right] + 1 \geqslant \left[\frac{p}{p-1}\right] + 1 = 2$, which means the chaotic map have no fixed points. □

Proposition 4. *The limit distribution of $K(x,p,\sigma)$ is a uniform distribution.*

Proof. The chaotic map has Markov properties so that the Markov process constitutes a Markov chain. By calculating the transition probability, the transition probability matrix is shown as (2.5):

$$F = \begin{pmatrix} 0 & 1/\sigma & 1/\sigma & 1/\sigma & \cdots & 0 & 0 \\ 0 & 0 & 1/\sigma & 1/\sigma & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1/\sigma & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 1/\sigma & 0 & 0 & 0 & \ddots & 1/\sigma & 1/\sigma \\ 1/\sigma & 1/\sigma & 0 & 0 & \ddots & \ddots & 1/\sigma \\ 1/\sigma & 1/\sigma & 1/\sigma & \cdots & \cdots & \cdots & 0 \end{pmatrix}_{p\times p} \tag{2.5}$$

and each row of the matrix meeting $\sum_{j=1}^{p} t_{ij} = 1$ As $Fq = q, F$ is the state transition matrix, $q$is the limit distribution. By solving the equation, the limit distribution is the standardized eigenvector ξ of the state transition matrix which eigenvalue equal to $1, \xi = \left(\frac{1}{\sqrt{p}}, \frac{1}{\sqrt{p}}, \frac{1}{\sqrt{p}}, \cdots, \frac{1}{\sqrt{p}}\ \frac{1}{\sqrt{p}}\right)_{1\times p}$. The sum of each component of the row vector is $\sqrt{p}$, to make the sum be 1, we can obtain the eigenvector as $\xi_F = \left(\frac{1}{p}, \frac{1}{p}, \frac{1}{p}, \cdots, \frac{1}{p}, \frac{1}{p}\right)$. So in every small interval, its density is $\rho_i = \frac{1}{p} \times p = 1$, it means the density function of the chaotic map is denoted as formula (2.6). This means that the limit distribution of $K(x,p,\sigma)$ is a uniform distribution.

$$\rho(x) = \begin{cases} 1, & x \in [0,1] \\ 0, & x \in R, x \notin [0,1] \end{cases} \tag{2.6}$$

□

Proposition 5. *The autocorrelation coefficients of the chaotic map $K(x,p,\sigma)$ are δ like.*

Proof. Correlation coefficients are used in statistics to measure how strong a relationship is between two variables. They also range from −1.00 to 1.00, with the weaker the relationship the closer the coefficient is to zero. We plot the autocorrelation coefficients in Fig. 3 and in the figure, we can see that every points are close to zero except the original point and they are δ like. □

3. The proposed image encryption scheme

This paper still adopts the fundamental Fridrich's permutation-diffusion model. The architecture of the proposed encryption scheme is shown in Fig. 4. For a gray image I sized $M \times N$ with 256 Gray scale levels, each pixel can by represented by an 8-bit binary sequence. So the gray scale image can be regarded as a 3D

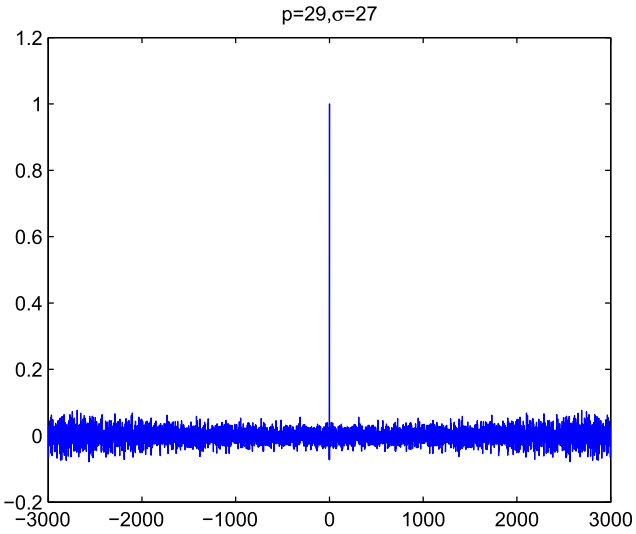


Fig. 3. The autocorrelation coefficients of the chaotic map.

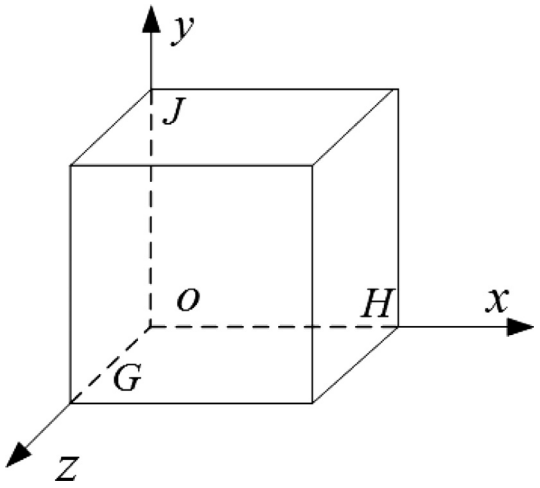


Fig. 5. diagrammatic drawing of the 3D matrix.

bit matrix with size $M \times N \times 8$. Under this circumstance, G, H, J in Fig. 5 must be satisfied the equation: $M * N * 8 = G * H * J$. In the simulation, we suppose that $M = N = 512$ and $G = H = J = 128$.

3.1. Permutation stage

There are two criteria for an effective bit-level permutation algorithm [16]: (1) the confused image should be devoid of any repeat patterns; (2) the histogram of the permuted image should be uniformly distributed. Ordinary permutation algorithms are not capable of fulfilling these two requirements. The permutation process of the proposed scheme based on double random positions mapping with reverse 3D cat map and 3D cat map can fulfill the two criteria.

It is well known that the standard 3D cat map defines a mapping rule from a regular position to a random place. By using the map in reverse, we can obtain a mapping from a random place to a regular one. Then the permutation operation has been separated into three parts. Firstly, we use the reverse 3D cat map to get the random bit position (x_r, y_r, z_r) from the sequential bit position (x, y, z) in the plain image. Secondly, the standard 3D cat map which has the different parameters compared with the reverse 3D cat map is used to obtain the random bit position (x'_r, y'_r, z'_r). At last, the confusion can be regarded as a mapping from a bit random position to another pseudo-random bit position, according to (3.1).

$$(x'_r, y'_r, z'_r) \leftarrow (x_r, y_r, z_r). \tag{3.1}$$

With I representing the plain image, we first adopt binary bitplane decomposition(BBD) [14] in our scheme. BBD can divided the plain image into 8 bitplanes, and then combine these 8 bitplanes together. The matrix obtained above is named bit_I. The operation procedures of permutation is depicted as shown in Fig. 4.

Step 1. Iterate Lorenz system by an Euler algorithm with a step size of $\delta = 0.001$ for $N0$ times with the initial values

$$x0 = 0.34567890126782, y0 = 0.78236459012032,$$
$$z0 = 0.12345678903452, N0 = 200.$$

Step 2. To increase the security against differential attack and ensure that if the plain image changes only a subtle extent, the key will change sufficiently, the value of t is calculated by (3.2)

$$t = \sum_i \sum_j \sum_k bit\_I(i, j, k). \tag{3.2}$$

Step 3. Perform the reverse 3D cat map to get a random bit position (x_r, y_r, z_r) and the first part of confusion's six parameters $a_x, a_y, a_z, b_x, b_y, b_z$ are given by (3.3).

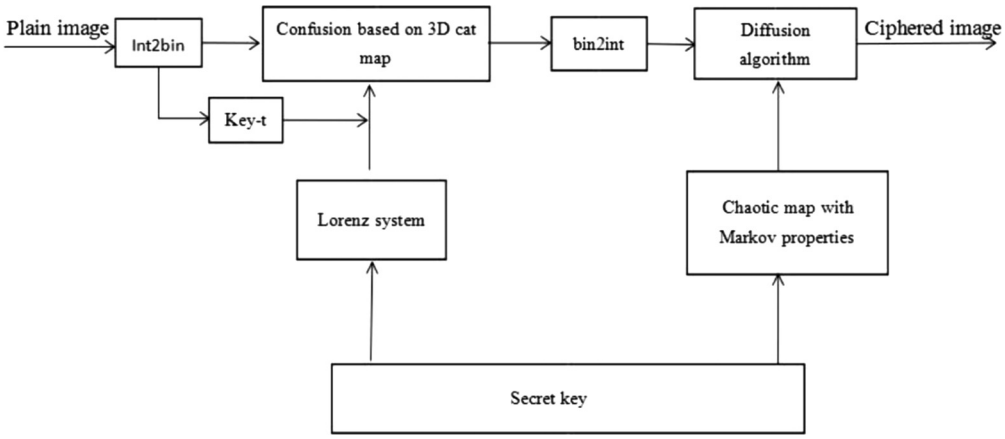


Fig. 4. the flowchart of encryption scheme.

$$\begin{aligned}
a_x &= floor\left(X(100) * 10^{12}\right) + t1 \bmod 128,\\
a_y &= floor\left(Y(100) * 10^{12}\right) + t1 \bmod 128,\\
a_z &= floor\left(Z(100) * 10^{12}\right) + t1 \bmod 128,\\
b_x &= floor\left(X(110) * 10^{12}\right) + t1 \bmod 128,\\
b_y &= floor\left(Y(110) * 10^{12}\right) + t1 \bmod 128,\\
b_z &= floor\left(Z(110) * 10^{12}\right) + t1 \bmod 128,
\end{aligned} \tag{3.3}$$

where $X(i), Y(i), Z(i)$ are generated by Lorenz system, function $floor(x)$ returns the largest integer not larger than x, function x *mod* y returns the remainder after x divided by y.

Step 4. Execute the 3D cat map (2.3) to generate another random bit position (x'_r, y'_r, z'_r) with the cat map's parameters:

$$\begin{aligned}
a'_x &= floor\left(X(150) * 10^{12}\right) + t1 \bmod 128,\\
a'_y &= floor\left(Y(150) * 10^{12}\right) + t1 \bmod 128,\\
a'_z &= floor\left(Z(150) * 10^{12}\right) + t1 \bmod 128,\\
b'_x &= floor\left(X(151) * 10^{12}\right) + t1 \bmod 128,\\
b'_y &= floor\left(Y(151) * 10^{12}\right) + t1 \bmod 128,\\
b'_z &= floor\left(Z(151) * 10^{12}\right) + t1 \bmod 128.
\end{aligned} \tag{3.4}$$

Step 5. It defines a new mapping rule from a random bit position to another random bit position shown as (3.1).

The schematic diagram of the permutation stage is illustrated in Fig. 6. From Fig. 6(b)–(a), the 3*D* cat map is used and from Fig. 6(b)–(c) the reverse 3*D* cat map is employed. And (b) does not really exist during the permutation procedure, it just has played an important role in the mediation.

3.2. Diffusion stage

As we known that a permutation-only cryptosystem is vulnerable to plaintext attacks [21], the diffusion phase has played an important role in a encryption scheme. Based on bit-level permutation, the position of each pixel is exchanged and the values of the pixels are altered as well. In our diffusion phase, we first transform the 3D permuted matrix into 2D matrix, and then all the pixels are selected horizontally from the upper left corner to the lower right corner to form a sequence.

In the proposed diffusion phase, a chaotic map with Markov properties Eq. (2.4) is employed. Eq.(3.5) is applied to govern the diffusion phase. we set the initial value of *temp* to be $temp = mod\left(3.99999 * key0 * (1 - key0) * 10^6, 256\right)$, and $key0 = 0.12345432667893$.

$$\begin{cases} Cipher(i) = Per(i) \oplus f\_Markov(temp), \\ temp = Cipher(i), \end{cases} \tag{3.5}$$

where $cipher(i), Per(i)$ are the resulted pixel's gray values of the cipher-image pixel and the permuted image respectively. f_Markov is gained by Eq.(3.6) where $f\_Markov1$ is generated by a chaotic map with Markov properties with $p = 29, \sigma = 27$ and initial value $u0 = 0.12345678901267$. At the generation procedure, if the value of f_Markov repeats, we discard it and continue to iterate the chaotic map until all the integers between 0 and 255 have been obtained. Therefore one can see that f_Markov is one vector of length 256 whose elements are different from each other and belong to [0, 255].

$$f\_Markov = mod\left(round\left(f\_Markov1 * 10^6\right), 256\right). \tag{3.6}$$

The diffused 1*D* array is transformed into 2*D* matrix and the ciphered image is yielded. The receivers obtain the encrypted image *C* in an insecure channel while the secret keys in a secure channel. The decryption process is the reverse process of the encryption scheme. The flowchart of the decryption process is shown as Fig. 7. However the only part need to be focused on is the calculation about the value of *t*.

4. Experimental results and performance analysis

4.1. Experimental results

The proposed encryption algorithm is performed using MATLAB 7.10.0 that runs on a personal computer with 2 GB memory, and Windows 7, 32 bit OS. The experiments are simulated on 512×512 test images such as Lena, cameraman, and so on. Fig. 8 shows the experimental results for the encrypted and decrypted image. Fig. 8(a), (d) shows the original images, Fig. 8(b), (e) shows the cipher images and Fig. 8(c), (f) shows the decrypted image with correct secret keys. All these validate that the encryption scheme is feasible and satisfactory.

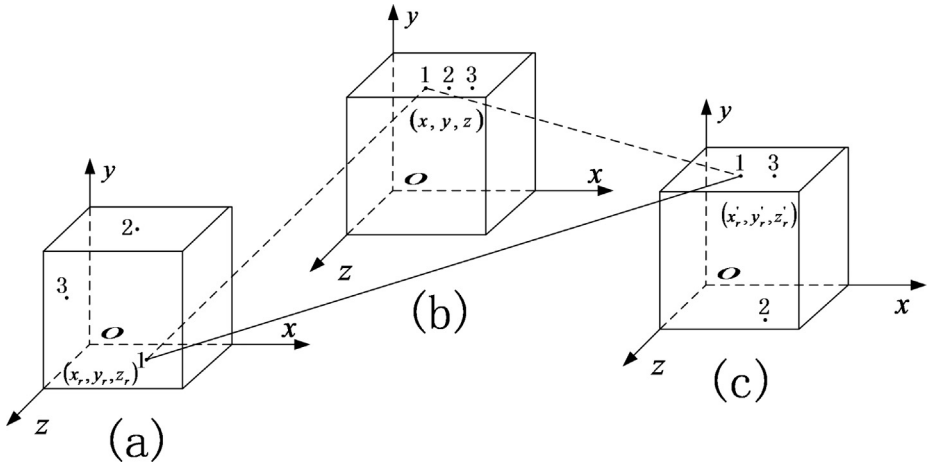


Fig. 6. double random positions confusion in 3D matrices.

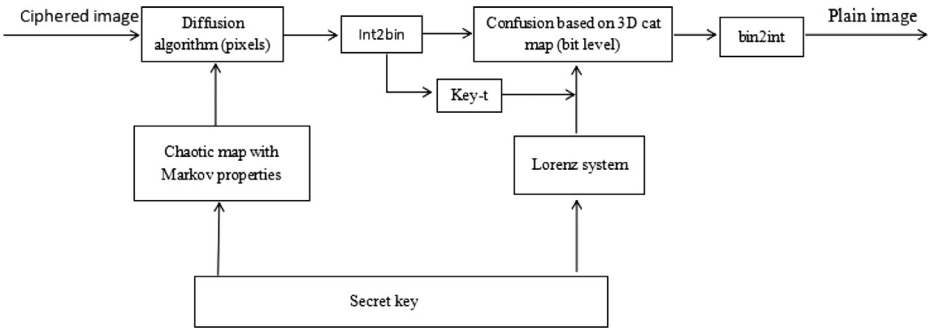
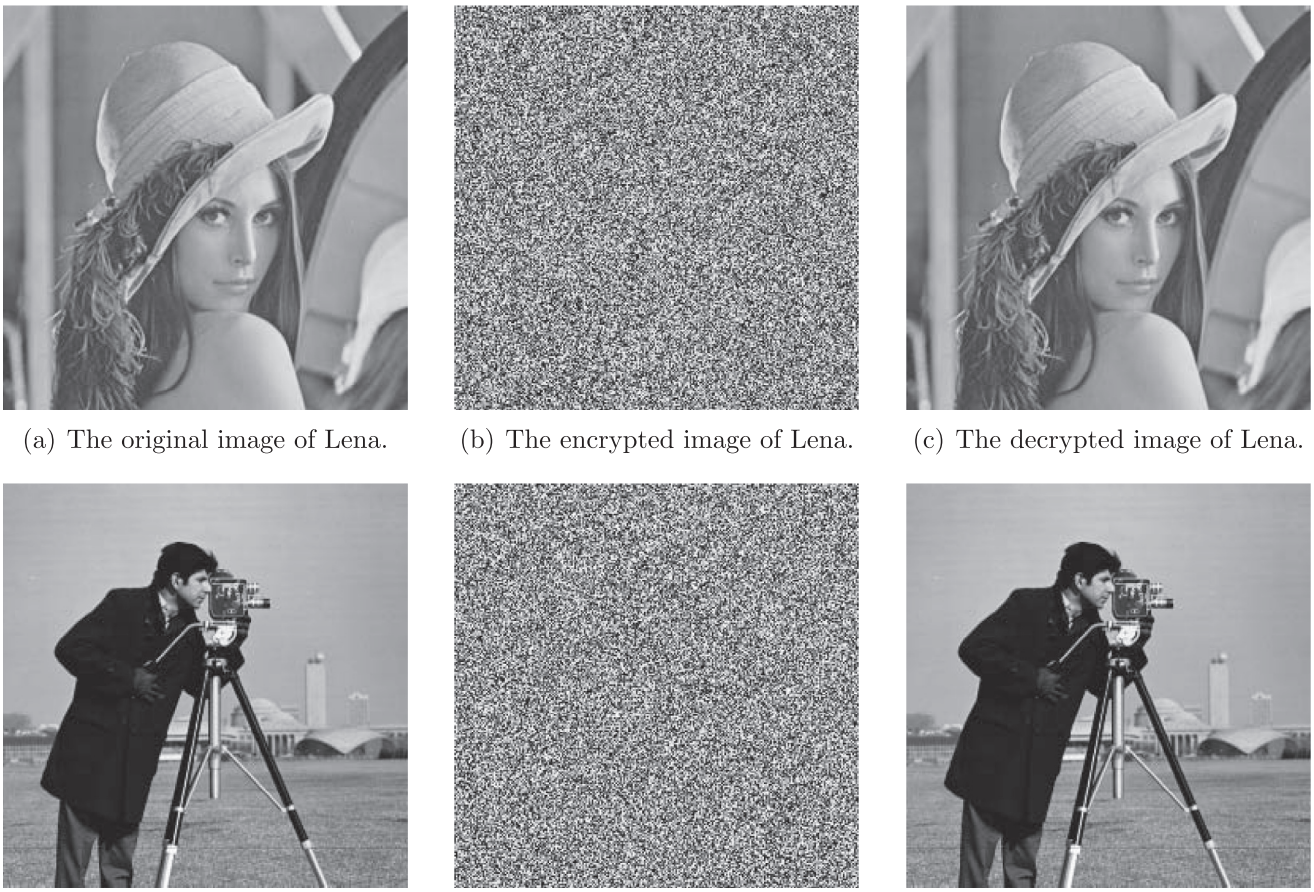


Fig. 7. decryption flowchart of the decryption algorithm.



(a) The original image of Lena. (b) The encrypted image of Lena. (c) The decrypted image of Lena.

(d) The original image of cameraman. (e) The encrypted image of cameraman. (f) The decrypted image of cameraman.

Fig. 8. plain images and cipher images.

4.2. Performance analysis

An idea good encryption algorithm should have strong resistance to any kinds of attacks, such as differential attack, known plaintext attack, chosen plaintext attack and so on [22]. In this section, performance analysis for the proposed algorithm with different images and some comparable algorithms are provided.

4.2.1. Key space analysis

A large key space is very important to an encryption cryptosystem as it is able to resist brute-force attack. We know that the key space size is the total number of entirely different keys that can be used in a cryptosystem. We fix key parameters $p = 29$, $\delta = 0.001, \sigma = 27$ and just consider the other key parameters to be the cipher keys. Then the proposed algorithm consists of six keys $x0, y0, z0, N0, u0, key0$. The IEEE floating-point standard suggests the computational precision for a 64-bit double precision number as 10^{-15} [23]. The different choices for $x0, y0, z0, u0, key0$ are all 10^{15}. The integer key $N0$ is set to belong to [1] and then $N0$ has 10^3 different choices. So the key space size of the proposed algorithm is approximately as large as $key\text{—}space = 10^{75} \times 10^3 = 10^{78}$, which is large enough to resist exhaustive attack [19].

A robust encryption algorithm should be high sensitivity to the change of secret keys. It means that a tiny change of the secert key

will lead to a completely different cipher image, and the ciphered image can't convert into the correct original image with a small change of the secret keys. In this paper, $x0, y0, z0$ are the initial values of Lorenz system, so they are very sensitive thanks to the chaotic natures of the system. In order to test key sensitivity, some experiments have been done. We use the keys introduced in Section 3 as $K1$ to encrypt the original image shown in Fig. 9(a) to obtain the encrypted image shown in Fig. 9(b), and then we use $K2$, obtained by modifying $K1$ as $x0 + 10^{-15}$ to obtain the encrypted image shown in Fig. 9(c), the difference of the two cipher images is shown in Fig. 9(d). Fig. 9(e) shows the decrypted image C1 with the correct keys $K1$, Fig. 9(f) shows the decrypted image C1 with $K2$, Fig. 9(g) shows the decrypted image C2 with $K1$, and Fig. 9(h) shows the decrypted image C2 with $K2$. The other secret keys can be tested similarly and strongly sensitivity can be found as well.

4.2.2. Histogram analysis

The histogram of the image before and after encryption are compared to analyze the statistical performance. The histogram of the cipher image can give information of the original image If it is not uniform enough, a mass of information may be analyzed by the statistic attack. In this paper, the original histogram, the confused histogram, and the ciphered histogram of Lena are shown in Fig. 10; and the original histogram, the confused histogram, and the ciphered histogram of cameraman are shown in Fig. 10. From the simulation results, one can find the histograms of the permuted images have been modified and greatly different from those of the plain images. Furthermore, the histograms of the cipher images are all uniform which means the proposed algorithm is considered robust against histogram analysis attack.

4.2.3. Correlation analysis

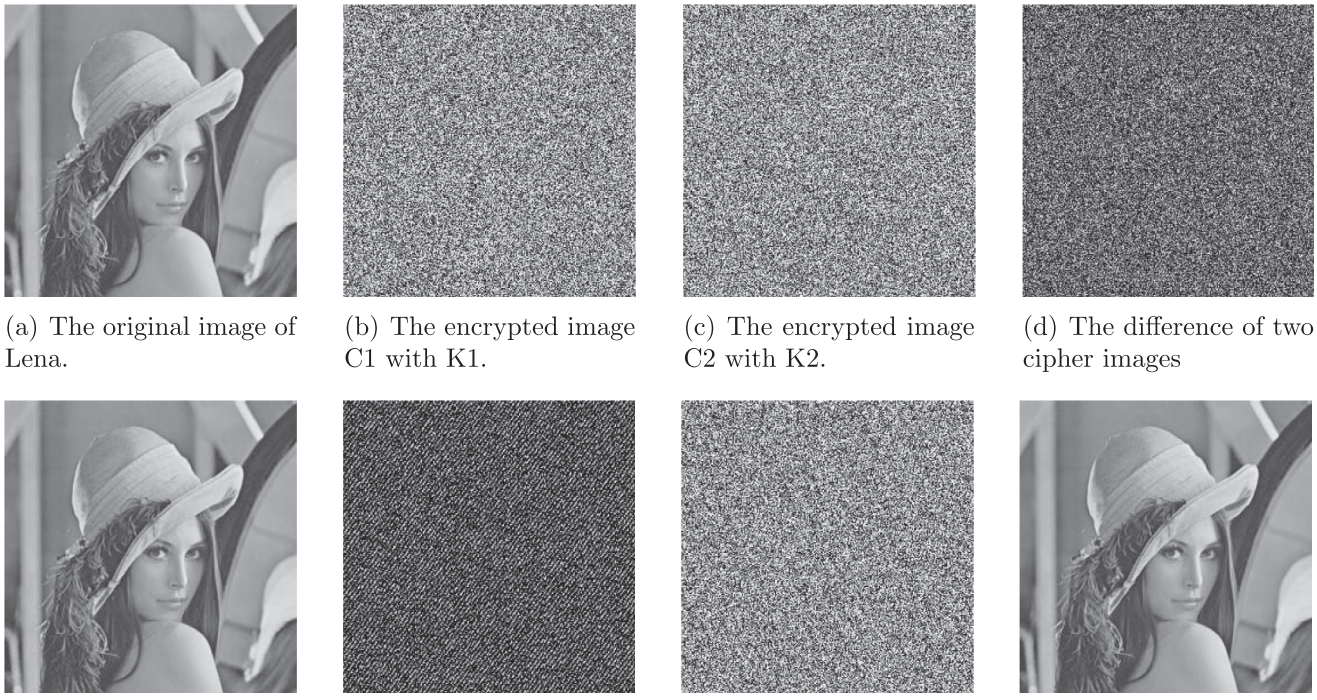
One notable feature for natural image with meaningful visual perception is redundancy [24]. The correlation between adjacent pixels is usually high in the plain image. An effective encryption system should reduce the correlation between adjacent pixels greatly to resist the statistical attack. Zero correlation is the best result for an ideal crytosystem. 3000 pairs of adjacent pixels at the horizontal, vertical and diagonal directions are selected from the plain image and ciphered image randomly to calculate the correlation coefficients by (4.1).

$$
\begin{aligned}
r_{xy} &= \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \\
E(x) &= \frac{1}{N}\sum_{i=1}^{N} x_i, D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2, \\
\mathrm{cov}(x,y) &= \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)).
\end{aligned}
\tag{4.1}
$$

where x, y are the gray values of two adjacent pixels, $E(x)$ is the mean, $D(x)$ is the variance, and $cov(x,y)$ is the covariance. The correlations of the adjacent pixels for original and ciphered image are shown in Fig. 11. Fig. 11(a)–(c) show the correlation distribution of the original image, while Fig. 11(d)–(f) show the correlation distribution of the ciphered image. The correlation coefficients of adjacent pixels in the plain image and its cipher image are listed in Table 1. Table 1 shows that the correlation coefficients of the original images are very high, while those of the encrypted imaged are nearly zero along all three directions. Table 2 shows the analysis of the correlation between adjacent pixels in comparison with Ref. [11], and Ref. [16]. The results can demonstrate that the proposed image encryption system has good permutation and diffusion properties.

4.2.4. Information entropy

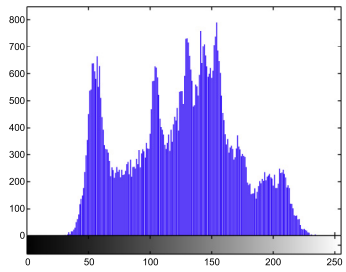
The information entropy is another criterion used to measure the degree of uncertainties of the system [27]. It can be used for evaluating the randomness of an image. Let m be the information



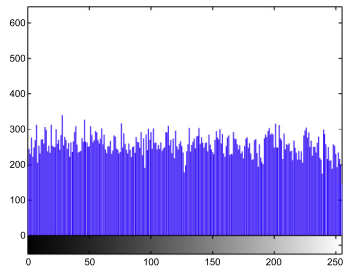
(a) The original image of Lena. (b) The encrypted image C1 with K1. (c) The encrypted image C2 with K2. (d) The difference of two cipher images

(e) The decrypted image C1 with K1 . (f) The decrypted image C1 with K2 . (g) The decrypted image C2 with K1 . (h) The decrypted image C2 with K2 .

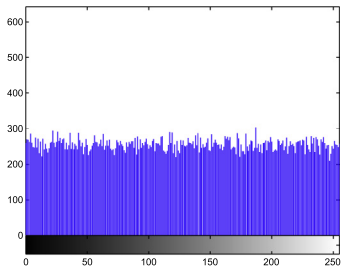
Fig. 9. The key sensitivity of the encryption and decryption process.



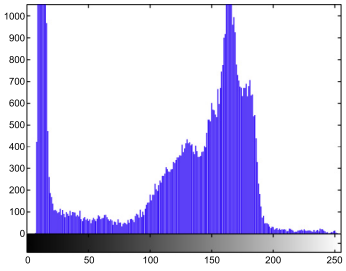
(a) The histogram of original Lena.



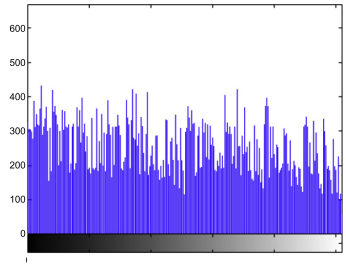
(b) The histogram of confused Lena.



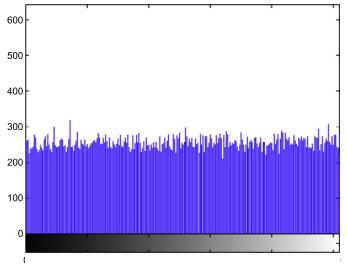
(c) "The histogram of encrypted Lena"



(d) The histogram of original cameraman.

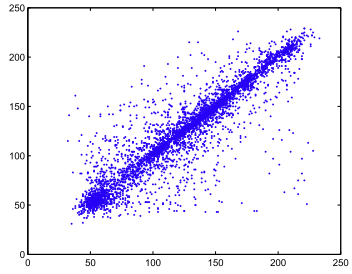


(e) The histogram of confused cameraman.

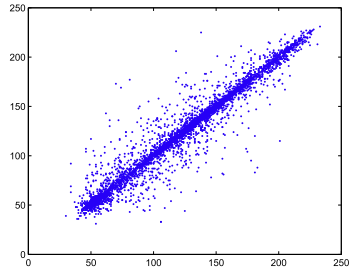


(f) The histogram of encrypted cameraman.

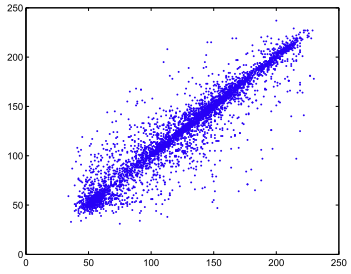
Fig. 10. The histograms of original images and cipher images.



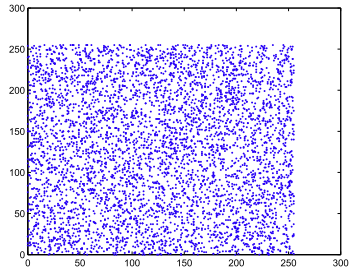
(a) The diagonal correlation of plain image.



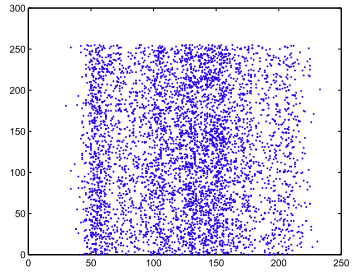
(b) The vertical correlation of plain image .



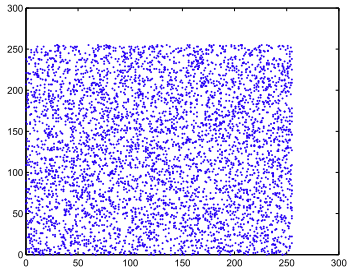
(c) The horizontal correlation of plain image .



(d) The diagonal correlation of ciphered image.



(e) The vertical correlation of ciphered image.



(f) The horizontal correlation of ciphered image.

Fig. 11. The correlation of the adjacent pixels for original and ciphered image.

Table 1
Correlation coefficients of two adjacent pixels in the plain and cipher images.

Figure name	Plain image			Cipher image		
	Horizontal	Diagonal	Vertical	Horizontal	Diagonal	Vertical
Lena	0.9427	0.9164	0.9700	0.0220	−0.0029	−0.0083
Cameraman	0.9311	0.9132	0.9624	−0.0069	0.0083	−0.0013
Clock	0.9572	0.9355	0.9759	−0.0076	−0.0104	−0.0032

Table 2
Correlation coefficients of adjacent pixels of Lena by different algorithms.

Algorithm	Cipher image		
	Horizontal	Diagonal	Vertical
Proposed algorithm	0.0020	−0.0029	−0.0083
Ref. [11]	−0.0022	−0.0228	−0.0062
Ref. [16]	0.0035	−0.0185	0.0148

Table 3
Information entropy of different algorithms.

Algorithm	Cipher image
Proposed algorithm	7.9972
Ref. [28]	7.9970
Ref. [29]	7.9874

source, the mathematical formula for the entropy of a message source is calculated by (4.2).

$$HH(m) = -\sum_{i=0}^{2^R-1} P(m_i)\log_2 P(m_i), \tag{4.2}$$

where R is the number of bits to represent the symbol m_i, and $P(m_i)$ is the emergence probability of the symbol m_i, so $\sum_{i=0}^{2^R-1} P(m_i) = 1$. For an ideally random image, the value of information entropy is 8. An effective encryption system[25] should be closed to 8. In fact, the information entropy resulting from encryption system may be smaller than 8. The greater information entropy is, the less possible for the algorithm to reval the information about plain-image. In Table 3, other two algorithms have been compared with the proposed system. The result shows that our system has good random distributions.

4.2.5. Differential attack

The differential attack, i.e. the chosen plaintext attack, is well-known and effective means to break a ciphered image. In order to resist the differential attack, the cryptosystem should make sure that any tiny modification in the plain image will lead to a completely different ciphered image. The NPCR (number of pixels change rate) and UACI (unified average changing intensity) are usually used for differential attack analysis [26]. Mathematically, the NPCR and UACI are defined by Eqs. (4.3), (4.4) and (4.5):

$$NPCR(C_1, C_2) = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \times 100\%, \tag{4.3}$$

Table 4
NPCR and UACI results of different algorithm.

Algorithm	NPCR	UACI
Proposed algorithm	99.61	33.49
Ref. [11]	40.65	13.64
Ref. [16]	0.517	0.174

$$UACI(C_1, C_2) = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%, \tag{4.4}$$

$$D(i,j) = \begin{cases} 0, \text{if } C_1(i,j) = C_2(i,j) \\ 1, \text{if } C_1(i,j) \neq C_2(i,j) \end{cases} \tag{4.5}$$

where $C1$ is the ciphered image by Lena, and $C2$ is obtained by ciphering the image which only has a slight difference, eg. one bit. Several tests have been performed on three different algorithms for round 1. The results are shown in Table 4.

The expect values of NPCR and UACI are 99.6094%, 33.4635% respectively [30]. From Table 4, the NPCR and UACI values of the proposed image encryption algorithm are all close to their expect values, and they are better than those results stated in [11,16]. This finding shows that the proposed algorithm can resist any type of differential attacks effectively.

5. Conclusion

An effective bit-level image encryption scheme based on 3D cat map, reverse 3D cat map and an improved chaotic map with Markov properties is proposed in this paper. In the proposed algorithm, we transform the plain-image into 3D binary matrix, and use the sum of the elements in the 3D binary matrix to alter the secret keys. This makes a slight modification of the plain image can give a completely different ciphered image, and therefore the proposed image encryption algorithm can strongly resist differential attack, chosen-plaintext attack and known-plaintext attack. An effective diffusion process is also presented to change the gray values of the whole image pixels. Experimental results and performance analysis including key space analysis, histogram analysis, correlation analysis, information entroy and differential attack have been discussed to demonstrate the security and validity of the image encryption algorithm.

References

[1] Chen G, Mao Y, Chui Charles K. A symmetric image encryption scheme based on 3d chaotic cat maps. Chaos Solitons Fractals 2004;21:749–61.
[2] Zeghid M, Machhout M, Khriji L, Baganne A, Tourki R. A modified aes based algorithm for image encryption. Int J Comput Sci Eng 2007;3:526–31.
[3] Alvarez G, Li S. Some basic cryptographic requirements for A modified aes based algorithm for image encryption cryptosystem. Int J Bifurc Chaos 2006;16:2129–51.
[4] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurcation Chaos 1998;8:1259–84.
[5] Chen Jun-xin, Zhu Zhi-liang, Chong Fu, Hai Yu, Zhang Yushu. Reusing the permutation matrix dynamically for efficient image cryptographic algorithm. Signal Process 2015;111:294–307.
[6] Kanso A, Gheble M. A novel image encryption algorithm based on a 3D chaotic map. Commun Nonlinear Sci Numer Simulat 2012;17:2943–59.
[7] Ercan S, Cahit C. OLCAY TY, Cryptanalysis of Fridrich's chaotic image encryption. Int J Bifurcation Chaos 2010;20:1405–13.
[8] Wang Y, Wong KW, Liao XF, Xiang T, Chen GR. A chaos-based image encryption algorithm with variable control parameters. Chaos, Solitons Fractals 2009;41:1773–83.
[9] Ye R. A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism. Optics Commun 2011;284:5290–8.
[10] Chen Jun-xin, Zhu Zhi-liang, Chong Fu, Hai Yu, Zhang Li-bo. A fast chaos-based image encryption scheme with a dynam icstate variables selection mechanism. Commun Nonlinear Sci Numer Simulat 2015;20:846–60.

[11] Zhang Wei, Wong Kwok-wo, Hai Yu, Zhu Zhi-liang. An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion reverse cat map. Commun Nonlinear Sci Numer Simul 2013;18:2066–80.
[12] Liu Quan, Li Pei-yue, Zhang Ming-chao, Sui Yong-xin, Yang Huai-jiang. A novel image encryption algorithm based on chaos maps with Markov properties. Commun Nonlinear Sci Numer Simulat 2015;20:506–15.
[13] Robinson RC. An introduction to dynamical systems: continuous and discrete. Prentice Hall Press; 2004.
[14] Zhou YC, Cao WJ, Chen CLP. Image encryption using binary bitplane. Singal Process 2014;100:197–201.
[15] Zhu Zhi-liang, Zhang Wei, Wong Kwok-wo, Hai Yu. A chaos-based symmetric image encryption scheme using a bit-level permutation. Inf Sci 2011;181:1171–86.
[16] Zhang Wei, Hai Yu, Zhao Yu-li, Zhu Zhi-liang. Image encryption based on three-dimensional bit matrix permutation. Signal Process 2016;118:36–50.
[17] Lu Xu, Li Zhi, Li Jian, Hua Wei. A novel bit-level image encryption algorithm based on chaotic maps. Opt Lasers Eng 2016;78:17–25.
[18] Mirzaei D, Yaghoobi M, Irani H. A new image encryption method: parallel sub-image encryption with hyper chaos. Nonlinear Dyn 2012;67:557–66.
[19] Wang X-Y, Yang L, Liu R. A chaotic image encryption algorithm based on perceptron model. Nonlinear Dyn 2010;62:615–21.
[20] Liu Q, Li PY, Zhang MC, Sui YX, Yang HJ. Construction of a class of chaos systems with Markov properties. Acta Phys Sin 2013;62(17):1–8. 170505.
[21] Li S, Li C, Chen G, Bourbakis NG, Lo KT. A general quantitative cryptanalysis of permutation-only multimedia ciphers against plain-text. Singal Process: Image Commun 2008;23:212–23.
[22] Lian SG, Sun J, Wang Z. Security analysis of a chaos-based image encryption algorithm. Phys A 2005;351:645–61.
[23] IEEE Computer Society, IEEE Standard for Binary Floating-Point Arithmetic, ANSI/IEEE Std. 1985. p. 754.
[24] Zhou Y, Bao L, Chen CLP. A new 1D chaotic system for image encryption. Signal Process 2014;97:172–82.
[25] Guan ZH, Huang F, Guan W. Chaos-based image encryption algorithm. Phys Lett A 2005;346:153–7.
[26] Mao YB, Chen GR, Lian SG. A novel fast image encryption scheme based on 3D chaotic baker maps. Int J Bifurc Chaos 2004;14:3613–24.
[27] Shannon CE. A mathematical theory of communication. Bell Sys Tech J 1949;1:623–56.
[28] Wang XY, Zhang YQ, Bao XM. A novel chaotic image encryption scheme using DNA sequence operations. Opt Lasers Eng 2015;73:53–61.
[29] Liu LJ, Wang XY, Kadir A. Image encryption using DNA complementary rule and chaotic maps. Appl Soft Comput 2012;12:1457–66.
[30] Wu Y, Noonan JP, Agaian S. Npcr and uaci randomness tests for image encryption. Cyber J: Multidiscip J Sci Technol J Sel Are Telecommun (JSAT) 2011;0:31–8.