A Snake Encryption Algorithm for Image with Multiple Chaos Fusion

Ye Tao, Wenhua Cui, Jiaming Zhao, Wenyu Zhang, and Zhao Zhang

Abstract—**In this paper, the historical process of chaotic image encryption algorithm is introduced. Classical Logistic chaotic system and piecewise linear chaotic map (PWLCM) are fused to form a novel chaotic system LPW. Based on LPW chaotic system, a snake encryption algorithm for digital image with multiple chaotic fusion is proposed. The algorithm carries out three rounds of image encryption, including forward crawling, reverse crawling and hibernation of snakes. The encryption of the algorithm uses the diffusion algorithm associated with the plain and the single row non-repetitive scrambling algorithm, and performs the scrambling and diffusion processes simultaneously. Experimental results show that the algorithm has high security, fast encryption and decryption speed, larger key space, and can resist common attacks such as differential attack and separate attack of scrambling and diffusion.**

Index Terms—**chaos, image encryption, snake encryption algorithm, scrambling, diffusion**

I. Introduction

IN the era of information explosion, information security has become a topic of discussion. Cryptography is becoming more and more important due to the protection of privacy and important information [1]. Cryptography has become a very hot topic of today. Finding a more secure, more efficient encryption method becomes very important. In the field of information security, most information is expressed as images. As an illustration of the similarity and clarity of objective objects, image is an important information carrier in our lives [2]. At present, the More common image encryption algorithms include image pixel position disorder and pixel value change. However, These image encryption algorithms are particularly vulnerable to statistical analysis and to crack. Moreover, these simple image encryption methods is generally relatively inefficient. As chaotic maps is disordered, they can be combined with image encryption algorithms to improve image security. Chaos based image encryption algorithms have been widely developed in cryptography.

In 1989, British mathematician R.Matthews [3] first proposed the concept of chaos code and a generalized Logistic mapping based. The chaotic mapping generated many pseudorandom numbers for data encryption. This work marked the combination of chaotic systems and cryptography, and set off a hot wave of research on chaotic cryptography. The cryptography algorithm proposed by R.Matthews was mainly for the encryption and decryption of text data. Image cryptography system based on chaotic system was proposed by J.Fridrich [4] in 1998. The largest contribution of J.Fridrich is to propose a method of iterative state values of chaotic systems directly for scrambled image pixels.In 2001, G.Jakimoski and L.Kocarev [5] proposed the block image diffusion algorithm.The algorithm is implemented by bitwise XOR. It are still widely used in image cryptography systems. Logistic map and piecewise linear chaotic map (PWLLCM) are two common functions for generating chaotic sequences. Many scholars have proposed chaotic encryption algorithms based on these two mappings. Liu et al. [6] proposed a chaotic mapping with variable parameters. This chaotic map can compensate for the defect of the traditional one-dimensional Logistic mapping and resist phase space attacks effectively. In 2014, Nasir et al. [7] proposed the bit-level scrambling algorithm for nested PWLCM to improve security of encryption systems. However, it is necessary to generate PWLCM chaotic sequence for many times, which increases the complexity and computational cost of the system.

An image encryption algorithm based on chaotic systems has recently been developed and implemented. The current problems are long encryption and decryption time, can not resist the choice of plain attacks, scrambling and diffusion is easy to be cracked separately, and so on. For example, Diab et al. [8] cracked the scrambling and diffusion of the cryptosystem in [9] respectively using only a small part of the plain image. Tu et al.[10] prepared a particular image for reversing the scrambling process in [11]. This operation cracked the entire encryption system. Liu et al.[12] prepared a particular image cracking the diffusion processing of the encryption algorithm in [13] and cracking the encryption system by the inverse scrambling operation.The following

Manuscript received August 12, 2021; revised July 2, 2022. This work was supported by National Natural Science Foundation of China (U1908218), the Project of State Key Laboratory of Synthetical Automation for Process Industries (PAL-N201801), and the Excellent Talent Training Project of University of Science and Technology Liaoning (2019RC05).

Ye Tao is a Ph.D. student in School of Electronic and Information Engineering, and a lecturer in School of Computer and Software Engineering, University of Science and Technology Liaoning, Anshan, China. (e-mail: taibeijack@163.com).

Wenhua. Cui is a Professor of School of Computer Science and Software Engineering, University of Science and Technology Liaoning, Anshan, China. (corresponding author to provide phone: +86-133-0422-4928; e-mail: taibeijack@126.com).

Jiaming. Zhao is a graduate student of School of Computer Science and Software Engineering, University of Science and Technology Liaoning, Anshan, China.(e-mail: 453131435@qq.com).

Wenyu. Zhang is a Professor of School of Computer Science and Software Engineering, University of Science and Technology Liaoning, Anshan, China. (e-mail: zhangwenyu8518@126.com).

Zhao. Zhang is an associate Professor of School of Computer Science and Software Engineering, University of Science and Technology Liaoning, Anshan, China and a Researcher of State Key Laboratory of Industrial Process Automation (Northeastern University), Shenyang, China. (e-mail: zhangzhao333@hotmail.com).

references also have problems such as long encryption time and inability to resist diffusion and scrambling separate attacks. Wang X et al. [14] described a chaos safe communication method based on variable parameter nonlinear autoregressive digital filters. Meysam et al. [15] described an image encryption algorithm based on polynomial combination of chaotic mappings and dynamic function generation. Y. Chen et al.[16] proposed an image encryption method based on PWLCM and standard mapping. X. Wu et al. [17] described a deoxyribonucleic acid (DNA) based on color image encryption scheme for a sequential operation and a multiply modified one-dimensional (1D) chaotic system.

In order to improve the security of image encryption methods, we propose a snake cryptographic algorithm for images with multiple chaotic fusion. This algorithm confuses the one-dimensional logistic chaos map and piecewise linear chaos mapping (PWLCM) to obtain a novel chaotic system LPW (logistic and PWLCM). The chaotic matrix generated by LPW scrambles and diffuses the plain image, and scrambles and diffuses simultaneously in the process of encryption and decryption. In each row or column, first the diffusion of the plain association, and then the scrambling without repetition. This algorithm makes it impossible for an attacker to attack scrambling and diffusion separately. Furthermore, this algorithm can withstand the attack of the plane association. Finally, we show that the simulation results have high safety and practicality.

II. Introduction to Chaotic Maps

A. Logistic chaotic map

The logistic mapping is a classical model to study the behavior of complex systems such as dynamical systems, chaos and fractals.It is widely used in the field of image encryption, owing to its simple principles and useful calculations.It is defined by equation (1).

$$x(n+1)=\mu x(n)\left[1-x(n)\right] \tag{1}$$

where μ , x are the parameters. $x(n)$ is in a chaotic state when $3.569945627<\mu\le 4$, $0<x<1$.

B. Piecewise linear chaotic map（PWLCM）

PWLCM is a typical chaotic map, and it is easy to be implemented by fixed-point algorithm with finite digital accuracy. Because of its advantages in both implementation and speed, it has attracted the attention of cryptography [18]. PWLCM has a wider range of parameters. Other important features of the PWLCM system include good kinetic behavior, simple hardware and software implementation, efficient implementation, uniform invariant distribution, hybrid properties, accuracy and exponentially damped correlation functions. The definition of PWLCM is shown in Equation (2).

where p is the parameter, $0<p<0.5$. x is the state variable, $0<x<1$. The initial value of the state variable x_0 can’t equal p . When the values of x and p are within the specified range, the piecewise linear map has chaotic characteristics.

$$x_i=f\left(x_{i-1},p\right)=\begin{cases}\dfrac{x_{i-1}}{p}, & 0<x_{i-1}<p\\ \dfrac{x_{i-1}-p}{0.5-p}, & p\le x_{i-1}<0.5\\ f\left(1-x_{i-1},p\right), 0.5\le x_{i-1}<1 & \end{cases} \tag{2}$$

C. LPW chaotic map

There are some problems in PWLCM mapping, for example, the security cannot be guaranteed when the number of segment intervals is small, and the hardware implementation cost is high when the number of segment intervals is large. In this paper, a piecewise linear chaotic map (PWLCM) and a logistic map are combined to obtain a composite chaotic map (LPW). The mapping expands the key space, improves the randomness of the generated chaos matrix, and improves the security of encryption. LPW is defined as shown in Equation (3).

$$x_i=f\left(x_{i-1},p\right)\begin{cases}\dfrac{\mu x_{i-1}(1-x_{i-1})}{p}, 0<x_{i-1}<p\\ \dfrac{\mu x_{i-1}\left(1-x_{i-1}\right)-p}{0.5-p}, p\le x_{i-1}<0.5\\ f\left(1-x_{i-1},p\right), 0.5\le x_{i-1}<1\end{cases} \tag{3}$$

where μ and p are the parameters of the LPW system, x is the state variable of LPW. When $3.569945<\mu\le 4,\ 0<x<0.5$, the system is in a chaotic state.

III. Image encryption and decryption algorithm

A. Chaotic cipher generator

The chaotic cipher generator is used for LPW chaos map to generate three random matrices with the same size as the plain P , denoted as U , V and R , and all sizes are $M\times N$. The steps to generate the three chaotic matrices are as follows:

Step 1: Take the initial value of x is m_0 , in this paper, $m_0=0.7896$, $p=0.5487$, $\mu=3.57$. Substitute the x , p , μ into Equation (3), iterate LPW r_1+r_2 times to skip the transition state, $r_1=69$, $r_2=138$. Then continue iterating $M\times N$ times to get a state sequence of length $M\times N$, remember to $\{m_i\}$, $i=\{1,2,...M\times N\}$, $M=256,\ N=256$.

Step 2: Take the initial value of x is n_0 , in this paper, $n_0=0.3535$, $p=0.6677$, $\mu=3.57$. Substitute the x , p , μ into Equation (3), iterate LPW r_3+r_4 times to skip the transition state, $r_3=91$, $r_4=105$. Then continue iterating $M\times N$ times to get a state sequence of length $M\times N$, remember to $\{n_i\}$, $i=\{1,2,...M\times N\}$, $M=256,\ N=256$.

Step 3: From the vectors $\{m_i\}$ and $\{n_i\}$, $i=\{1,2,...M\times N\}$. According to Equations (4) to (6), matrices *U, V* and *R* are obtained.

$$U(u,v)=floor\left[\left(\frac{r_1+1}{r_1+r_3+2}m_{(u-1)\times N+v}+\frac{r_1+1}{r_1+r_3+2}n_{(u-1)*N+v}\right)\times 10^{14}\right] mod\ 256 \tag{4}$$

$$V(u,v)=floor\left[\left(\frac{r_1+1}{r_1+r_3+2}m_{(u-1)\times N+v}+\frac{r_1+1}{r_1+r_3+2}n_{(u-1)*N+v}\right)\times 10^{13}\right] mod\ 256 \tag{5}$$

$$R(u,v)=floor\left[\left(\frac{r_1+1}{r_1+r_3+2}m_{(u-1)\times N+v}+\frac{r_1+1}{r_1+r_3+2}n_{(u-1)*N+v}\right)\times 10^{12}\right] mod\ 256 \tag{6}$$

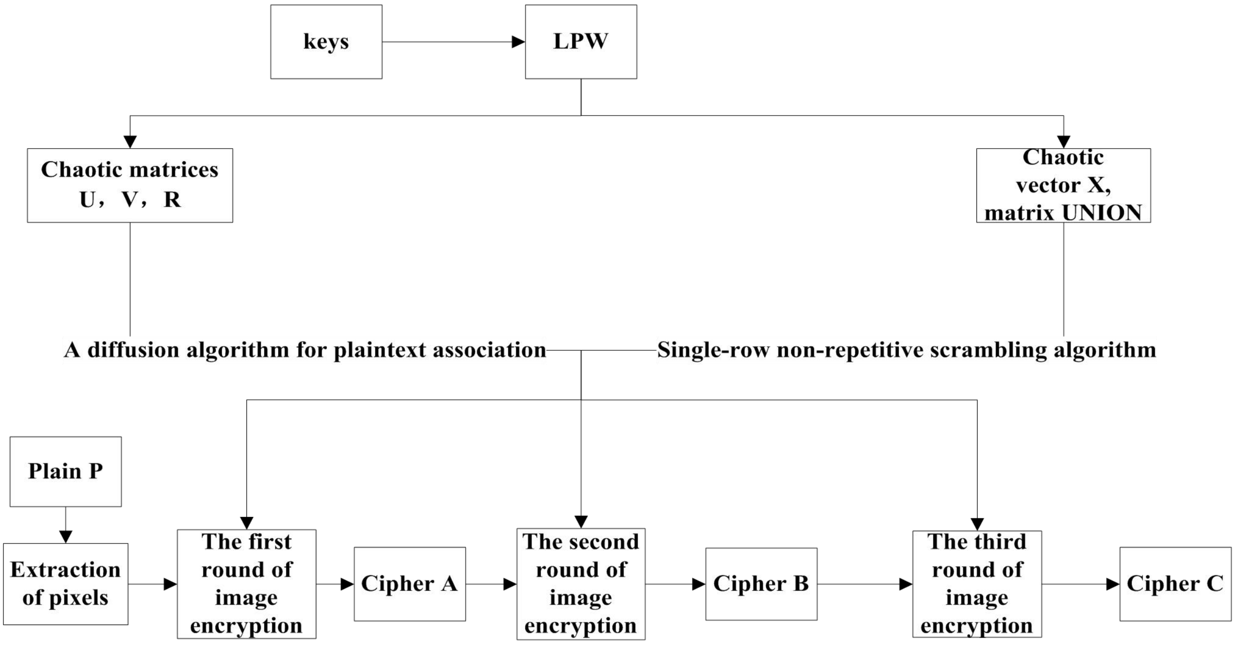

keys
LPW
Chaotic matrices U，V，R
Chaotic vector X, matrix UNION
A diffusion algorithm for plaintext association
Single-row non-repetitive scrambling algorithm
Plain P
Extraction of pixels
The first round of image encryption
Cipher A
The second round of image encryption
Cipher B
The third round of image encryption
Cipher C

Fig. 1. The image encryption process

In equation (4) to (6), $floor(t)$ returns the largest integer less than or equal to t, $u=\{1,2,...,M\}$, $v=\{1,2,...,N\}$. The chaotic matrices generated by the chaotic cipher generator are used in the diffusion process of image encryption algorithm.

Some chaotic vectors and matrices are generated in a single row without repetition for image scrambling. The specific process is as follows. With the help of the chaotic system LPW proposed in this paper, a random number vector of length M are generated, denoted as X, and the same random number is only saved once in X. Find elements that do not appear in the vector X within $\{1,2,...,M\}$ and append these elements to the vector X.This method ensures that each element in X is not repeated. The same method generates a vector Y and generates N different X vector to form matrix $UNION$. $UNION$ is a chaotic matrix with no repeating values in each row.

B. *Image encryption algorithm*

In order to ensure that the image encryption process is fast, effective and secure, a novel encryption algorithm is proposed in this paper, as shown in Fig. 1.

The encryption algorithm consists of three rounds of snake image encryption algorithm. Using the chaotic matrices *U, V, UNION, X, Y* generated by LPW to diffuse and scramble the pixels. The implementation process of the algorithm is explained below.

The first round of image encryption algorithm was performed according to the snake crawling route. The snake crawling route is shown in Fig.2. The specific process of image encryption algorithm is shown in Fig.3. The pixels of each odd row are encrypted from left to right, and the pixels of each even row are encrypted from right to left.

Step 1: Diffuse (1,1) through Equations (7):

$$A(1,1)=\left(P(1,1)+U(1,1)+r_3+r_4\right) mod\ 256 \tag{7}$$

where P is the plain, A is the first round of cipher and U is the chaotic matrix.

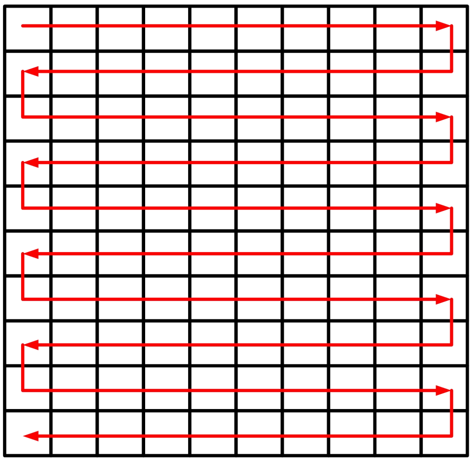


Fig. 2. The snake crawling route

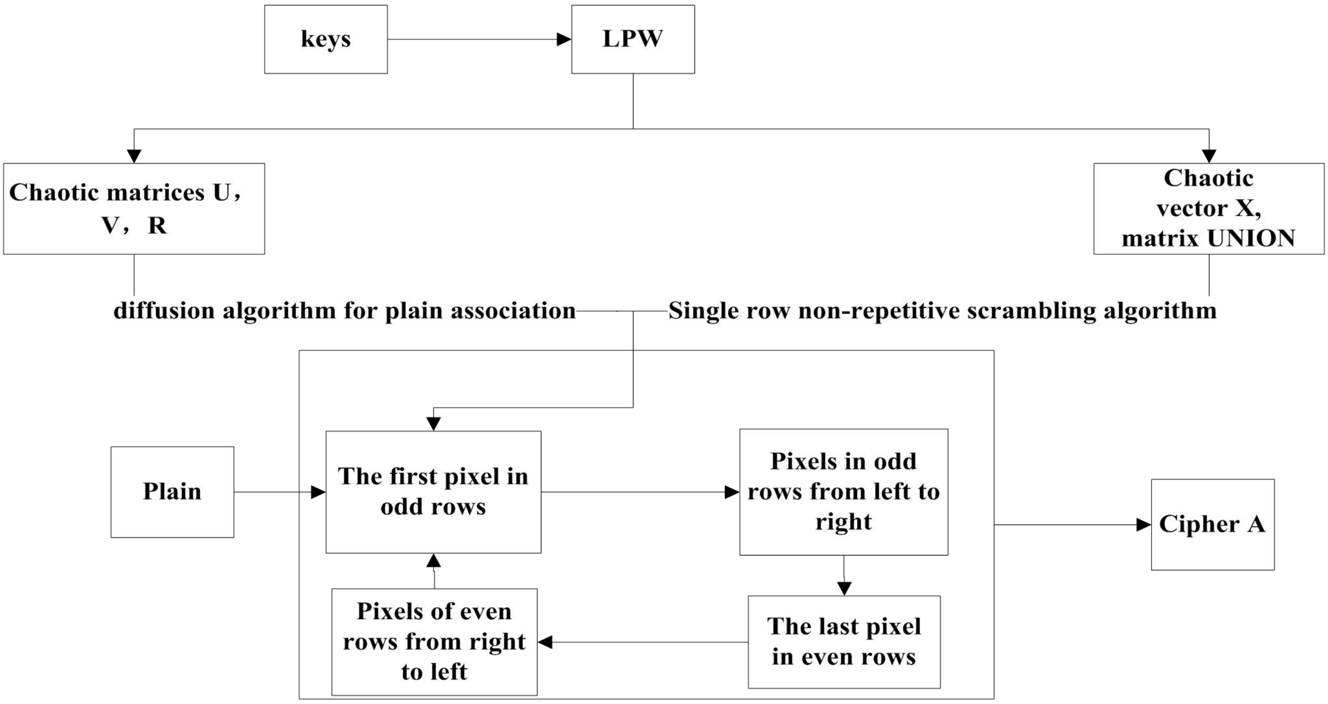

keys
LPW
Chaotic matrices U，V，R
Chaotic vector X, matrix UNION
diffusion algorithm for plain association
Single row non-repetitive scrambling algorithm
Plain
The first pixel in odd rows
Pixels in odd rows from left to right
The last pixel in even rows
Pixels of even rows from right to left
Cipher A

Fig. 3. The first round of the encryption process

Step 2: According to Equation (8), the pixels in the first row of P are diffused from left to right, then the $X(1,j)-th$ pixel and the $X(1,M-j+1)-th$ pixel in the first row of A swap positions. That is, use the value of the X matrix as the position of the pixels in the A matrix and swap the positions of these two pixels.

$$A(1,j)=\left(P(1,j)+A(1,j-1)+R(1,j)\right)mod\ 256 \quad (8)$$

Where j is the number of columns, $j\in(1,256]$. R is the chaotic matrix.

Step 3: Equation (9) is used to diffuse the pixels in the last column of each even row. Equation (10) is used to diffuse the pixels of each even rows from right to left. Then the $UNION(1,j)-th$ pixel and the $UNION(1,M-j+1)-th$ pixel in the each row of A swap positions.

$$A(i,N)=(P(i,N)+A(i-1,1)+A(i-1,N) + A(i-1,52)+R(i,N))mod\ 256 \quad (9)$$

$$A(i,j)=\left(P(i,j)+A(i,j+1)+R(i,j)\right)mod\ 256 \quad (10)$$

Where $A(i-1,52)$ is a random pixel. i is an even number , $i\in[1,256]$, $j\in[1,256]$.

Step 4: Equation (11) is used to diffuse the pixels in the first column of the each odd row. Equation (12) is used to diffuse the pixels of each odd row from left to right. Then the $UNION(i,j)-th$ pixel and $UNION(i,M-j+1)-th$ pixel of A swap positions.

$$A(i,1)=(P(i,1)+A(i-1,1)+A(i-1,N) + A(i-1,36)+R(i,1))mod\ 256 \quad (11)$$

$$A(i,j)=\left(P(i,j)+A(i,j-1)+R(i,j)\right)mod\ 256 \quad (12)$$

Repeat steps 3 and 4 from the second row to the 256th row of the plain, then get cipher A .

The second round of image encryption algorithm is the reverse operation of the first round algorithm. The snake reverse crawling route is shown in Fig.4. Starting from $A(256,1)$, even rows from left to right, odd rows from right to left, overall process from bottom to top, pixels are diffused and scrambled at the same time.Then generate cipher B .

The third round of image encryption mimics the hibernation of snakes. Image encryption process from outer circle to inner circle. The process is shown in Fig. 5.

Specifically, the scrambling process of this algorithm don’ t use any chaotic matrix, and the chaotic matrix (U, V, R) generated by the LPW chaotic system is used for image encryption during diffusion. The specific process is shown in Fig. 6.

Step 1: Equation (13) is used to diffuse the pixel $B(i,i)$. The pixel $B(i,j)$ are diffused from left to right by Equation (14), and the pixels $B(i,j)$ and $B(i,N-j+1)$ are swapped for scrambling, $i\in[1,128]$, $j\in[i+1,N-i+1]$.

$$C(i,i)=\left(B(i,i)+U(i,i)+r_3+r_4\right)mod\ 256 \quad (13)$$

$$C(i,j)=\left(B(i,j)+sum(B(i,i+1\ to\ j-1))+R(i,j)\right) mod\ 256 \quad (14)$$

$sum(\ )$ means the sum of all the pixel values in row i from column $i+1$ to column $j-1$.

Step 2: Diffuse the pixels $B(i+1,N-i+1)$ through Equation (15), $i\in[1,127]$. The pixels $B(k,N-i+1)$ are diffused from top to bottom through Equation (16), and the pixels $B(k,N-i+1)$ and $B(M-k+1,N-i+1)$ are swapped for scrambling, $i\in[1,127]$, $k\in[i+1,M-i]$.

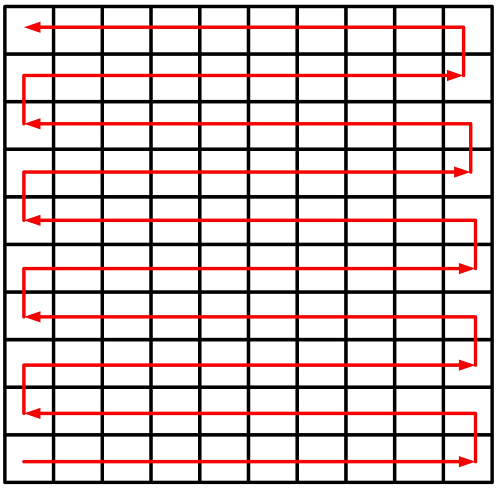


Fig. 4. The snake reverse crawling route

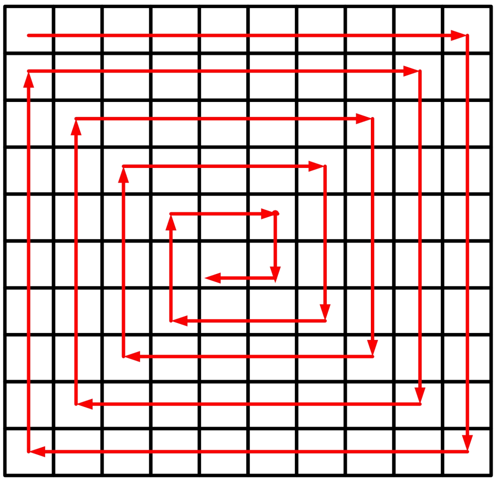
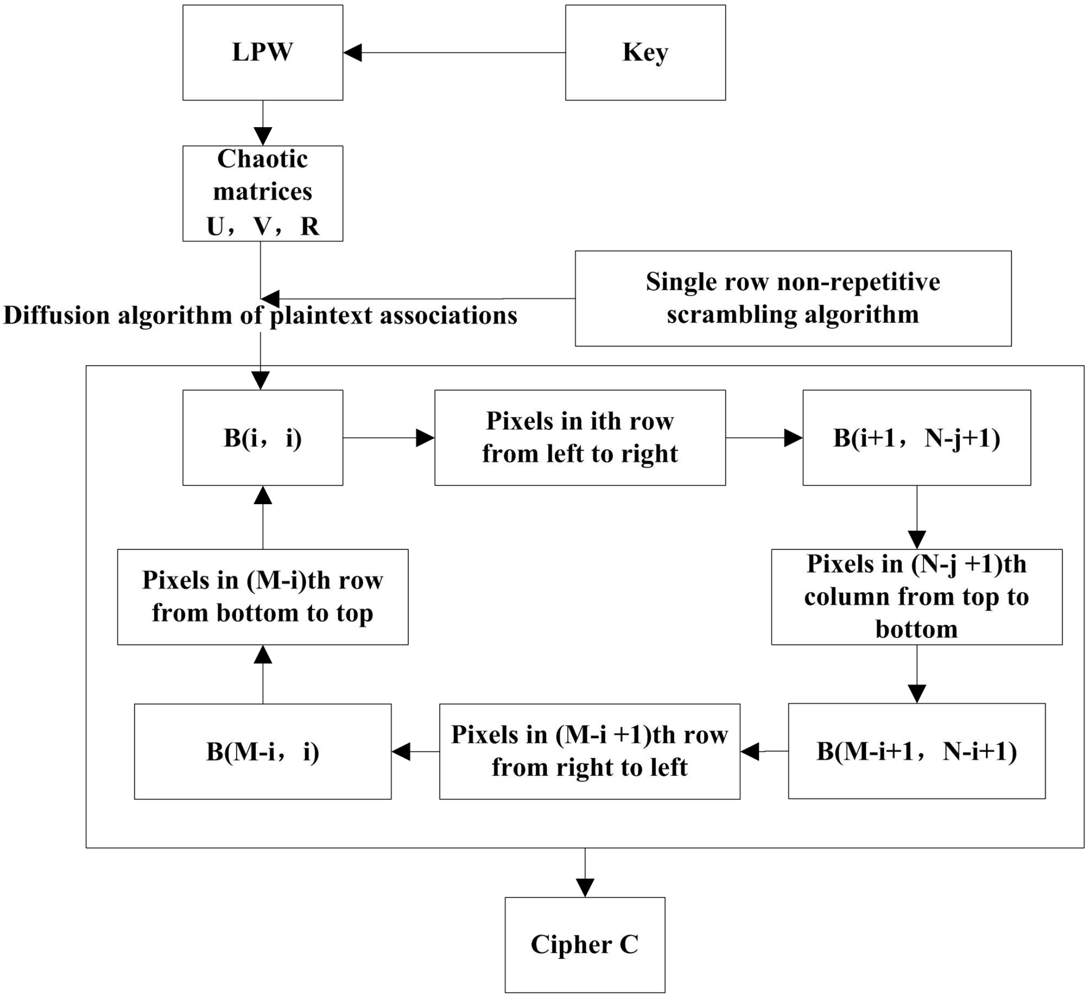


Fig. 5. The hibernation of snakes



LPW
Key
Chaotic matrices U，V，R
Diffusion algorithm of plaintext associations
Single row non-repetitive scrambling algorithm
B(i，i)
Pixels in ith row from left to right
B(i+1，N-j+1)
Pixels in (N-j +1)th column from top to bottom
B(M-i+1，N-i+1)
Pixels in (M-i +1)th row from right to left
B(M-i，i)
Pixels in (M-i)th row from bottom to top
Cipher C

Fig. 6. The third round of the encryption process

$$C(i+1, N-i+1) = (B(M-i+1, N-i+1) + r_3 + U(M-i+1, N-i+1) + r_4) \, mod \; 256 \tag{15}$$

$$C(k, N-i+1) = (B(k, N-i+1) + U(k, N-i+1) + sum(C(i+2 \; to \; k-1, N-i+1))) \, mod \; 256 \tag{16}$$

Step 3: Equation (17) is used to diffuse the pixels $B(M-i+1, N-i+1)$, $i \in [1,128]$. Equation (18) is used to diffuse the pixels $B(M-i+1, j)$ from right to left, $i \in [1,128]$, $j \in [N-i, i]$, swap the pixels $B(i, j)$ and pixels $B(i, N-j+1)$ ·

$$C(M-i+1, N-i+1) = (B(M-i+1, N-i+1) + r_3 + U(M-i+1, N-i+1) + r_4) \bmod 256 \tag{17}$$

$$C(M-i+1, j) = (B(M-i+1, j) + U(M-i+1, j) + sum(C(M-i+1, N-i \; to \; j+1))) \bmod 256 \tag{18}$$

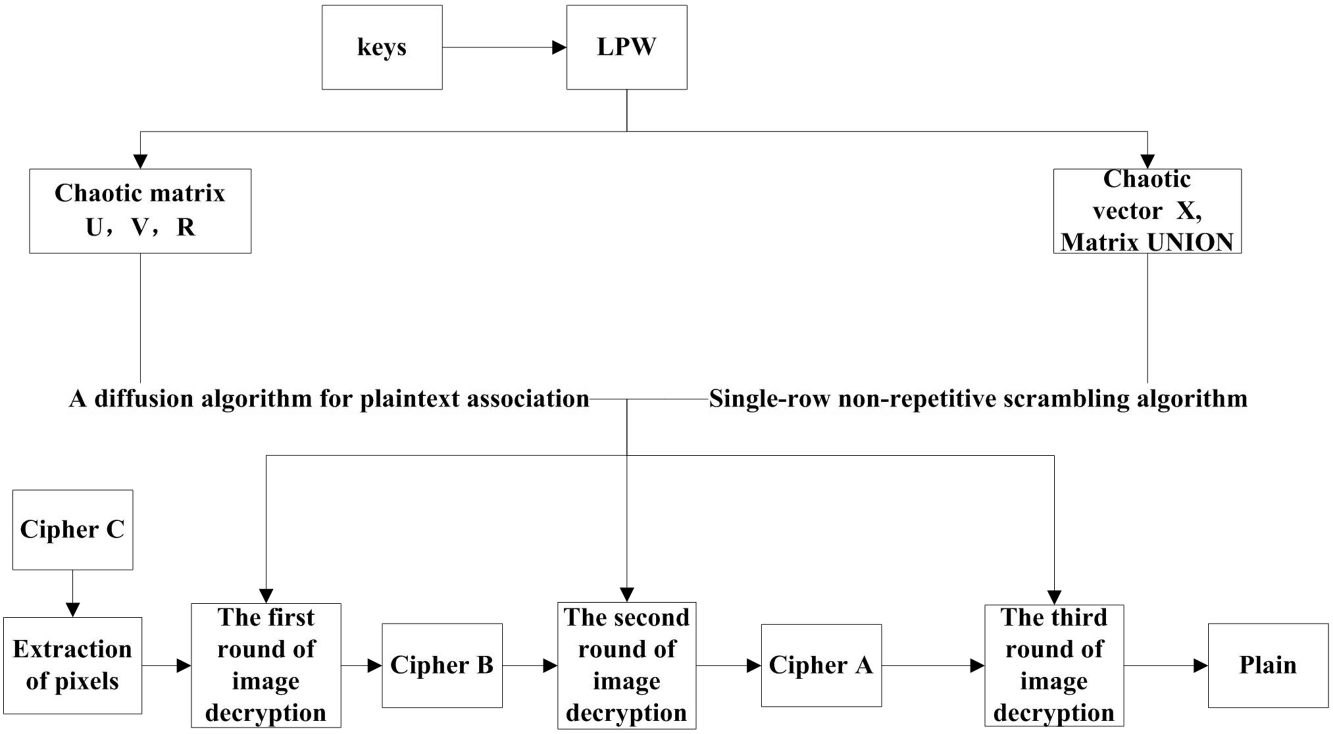

keys
LPW
Chaotic matrix U，V，R
Chaotic vector X, Matrix UNION
A diffusion algorithm for plaintext association
Single-row non-repetitive scrambling algorithm
Cipher C
Extraction of pixels
The first round of image decryption
Cipher B
The second round of image decryption
Cipher A
The third round of image decryption
Plain

Fig. 7. The image decryption algorithm

Step 4: Diffuse the pixels $B(m-i,i)$ through Equation (19), $i\in[1,127]$. Diffuse the pixels $B(m-i+1,j)$ from bottom to top by equation (20), and the pixels $B(k,j)$ and $B(i,n-j+1)$ are swapped for scrambling, $i\in[1,127]$, $k\in[M-i-1,i+1]$.

$$C(M-i,i)=\left(B(M-i,i)+U(M-i,i)+r_3+r_4\right)\bmod 256 \quad (19)$$

$$\begin{aligned} C(k,j)=(&B(K,j)+U(k,j)\\ &+sum(C(M-i-1\ to\ k+1,i)))\bmod 256 \end{aligned} \quad (20)$$

Steps 1 to 4 are cycled M/2 times, and the pixels in each cycle are successively decreased to obtain the cipher C.

The image encryption algorithm designed in this paper has three rounds of encryption process, each round of encryption scrambling and diffusion process are carried out simultaneously, and in the diffusion algorithm added plain elements, so that the encryption algorithm to achieve plain association.

C. Image decryption algorithm

The image decryption algorithm is the inverse operation of the encryption algorithm. Image decryption is performed in three rounds. Diffusion and scrambling are performed simultaneously in each round. The key and chaos matrix used for decryption are the same as those used for encryption, as shown in Fig. 7.

D. The experimental results

The simulation experiment software of the proposed image encryption algorithm is matlabR2018b, and the operating system is Windows 10. 256*256 grayscale images were used. The CPU is Intel Core i5-1135G7 and memory is 16GB.

We encrypt the image using the proposed cipher algorithm and decrypt the cipher image using the decoding algorithm. The experimental results are shown in Fig. 8.

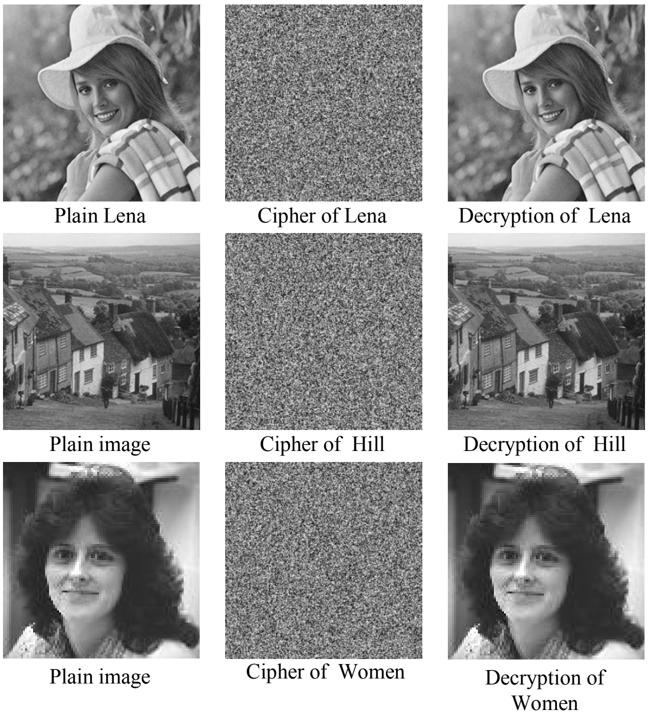

Plain Lena
Cipher of Lena
Decryption of Lena
Plain image
Cipher of Hill
Decryption of Hill
Plain image
Cipher of Women
Decryption of Women

Fig. 8. The experimental results

E. Safety analysis

(1) Encryption and decryption time

In this paper, take eight 256 × 256 images, encrypt and decrypt once with the proposed algorithm and the other five algorithms, and obtain the average value. The encryption and decryption time is shown in Table 1.

Although this algorithm carries out three rounds of image encryption and decoding, it shows that the image encryption and decoding speed are 10% to 80% faster than the other five algorithms.The algorithm has better encryption and decoding efficiency.

TABLE 1
ENCRYPTION AND DECRYPTION TIME

Algorithm	Encryption time (unit:s)	Decryption time (unit:s)
Proposed	0.1756	0.1753
Ref.[13]	1.0900	1.2368
Ref.[15]	0.2409	0.2688
Ref.[16]	0.5829	0.5406
Ref.[17]	0.3645	0.3784
Ref.[18]	0.6765	0.6895

(2)Key space

Key space is the collection of all valid keys in a cryptosystem. In the proposed algorithm in this paper, key $K=\{\mu,m_0,p,n_0,q,r_1,r_2,r_3,r_4\}$, $\mu\in(3.57,4)$, Step for 10^{-14}, m_0, $n_0\in(0,1)$, Step for 10^{-14}, $p,q\in(0,0.5)$, Step for 10^{-14}, r_1,r_2,r_3,r_4 are integers between [0,255], Step for 1, The total key space size of K is about $4.2950*10^{79}$.

For an image encryption system with high encrypting and decrypting speed, the key space should be at least 2^{100}. Since $2^{10}\approx10^{3}$, the key space of this paper is about 2^{260}. The key space proves that the proposed algorithm can effectively defend against the brute force attack.

Table 2 shows the key space of the proposed algorithm and the key space of other algorithms.

TABLE 2
KEY SPACE

Algorithm	Proposed	Ref. [13]	Ref. [15]	Ref. [16]	Ref. [17]	Ref. [18]
Keys space	10^{79}	10^{59}	10^{68}	10^{58}	10^{75}	10^{56}

(2) Cipher statistics

In this paper, the original image is encrypted to the noise cipher image, and the original image histogram is compared with the cryptogram image histogram, and the related characteristic is analyzed, and the statistical characteristic of the cipher image is evaluated.

Fig. 9 shows the original image and cryptographic histograms.The histogram of the original image (plain) rises and falls. This phenomenon shows that the neighboring pixels of the original image have strong correlation.The cryptogram histogram becomes flat. This phenomenon indicates that there is little correlation between neighboring pixels of the cipher.

In this paper, we calculate the correlation coefficients between the plain and cryptography. The correlation becomes weak as the correlation coefficient is close to zero.

Let N pairs of adjacent pixels be selected from Lena image, and their gray values are recorded as (σ_i,τ_i), $i=1,2,...,N.$ The calculation formula of correlation coefficient of vector $\sigma=\{\sigma_i\},\tau=\{\tau_i\}$ is shown in Equation 21.

$$\begin{cases} r_{xy}=\dfrac{\operatorname{cov}(\sigma,\tau)}{\sqrt{D(\sigma)}\sqrt{D(\tau)}} \\ \operatorname{cov}(\sigma,\tau)=\dfrac{1}{N}\sum\left(x_i-E(\sigma)\right)\left(y_i-E(\tau)\right) \\ D(\sigma)=\dfrac{1}{N}\sum\limits_{i=1}^{N}\left(\sigma_i-E(\sigma)\right)^2 \\ E(\sigma)=\dfrac{1}{N}\sum\limits_{i=1}^{N}\sigma_i \end{cases} \tag{21}$$

Set the coordinate of σ_i as (x_i,y_i), and if the coordinate of τ_i is (x_{i+1},y_i), then the correlation coefficient in the horizontal direction is calculated. If the coordinate of τ_i is (x_i,y_{i+1}), then the correlation coefficient in the vertical direction is calculated; If the coordinate of τ_i is (x_{i+1},y_{i+1}), calculate the coefficient in the diagonal direction. Fig. 10 shows the relationship between neighboring pixels in the three directions of plain and cipher of the Lena image. Most of the plain pixels are distributed on the straight line and are shifted straight from the straight line. This phenomenon indicates that the correlation between plain pixels is very strong.The pixels of the cipher are basically uniformly distributed, and there is no relation between adjacent pixels. This phenomenon indicates that the correlation between pixels of the cipher image is weak and can be effectively resistant to the statistical attack.

Table 3 shows the results of calculation of correlation coefficients between adjacent pixels in horizontal, vertical and diagonal directions of the plain and cipher images of Lena.

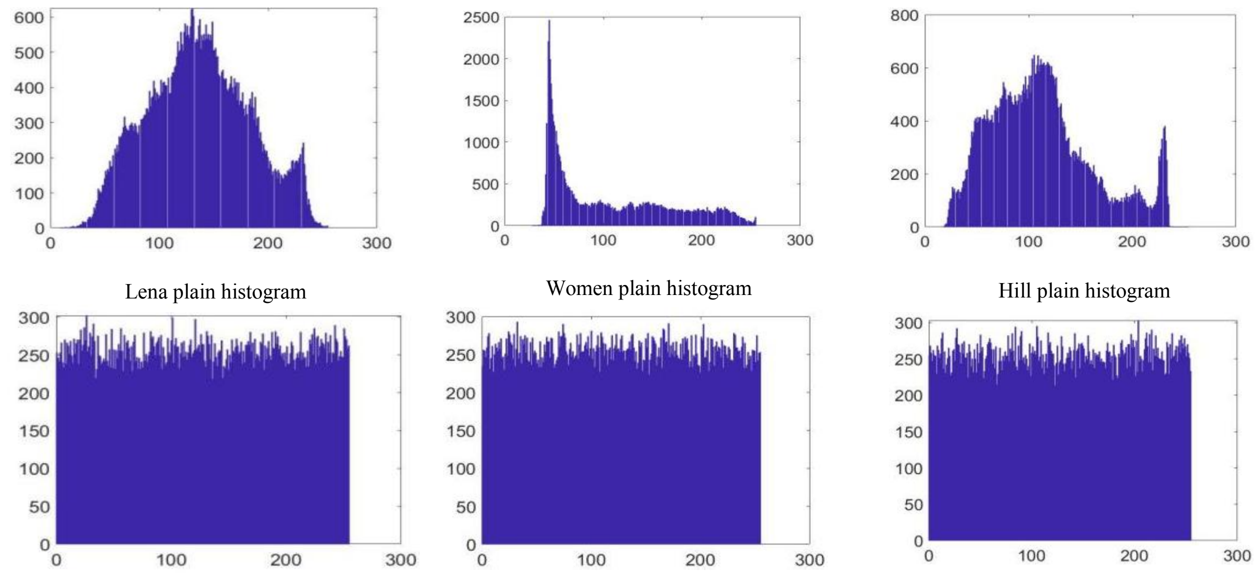
TABLE 3
THE CORRELATION COEFFICIENT

Algorithm	Horizontal direction	Vertical direction	Diagonal direction
Proposed（plain）	0.9882	0.9900	0.9790
Proposed（cipher）	-0.0064	0.0007	-0.0006
Ref.[13]（cipher）	0.0013	0.0008	0.0066
Ref.[15]（cipher）	0.0046	0.0050	0.0080
Ref.[16]（cipher）	0.0076	0.0190	0.0091
Ref.[17]（cipher）	–0.0084	0.0004	−0.0015
Ref.[18]（cipher）	0.0017	0.0023	0.0077

Table 3 shows that the correlation between adjacent pixels of the original image is above 0.9000. Although the value is very strong, the correlation coefficient of adjacent pixels of the cipher image is close to zero, and it is proved that there is little correlation. This reflects the safety and effectiveness of the proposed algorithm.

(3) Key sensitivity analysis

A value in the key K is slightly changed (10^{-14}), and then compare the cipher before the change and the cipher after the change, and analyze the key sensitivity of the algorithm. There are two indicators to measure the difference between two images, *NPCR* and *UACI*. Two images of the same size are denoted as *P1* and *P2*, and the image size is *M*N.*



Lena plain histogram

Women plain histogram

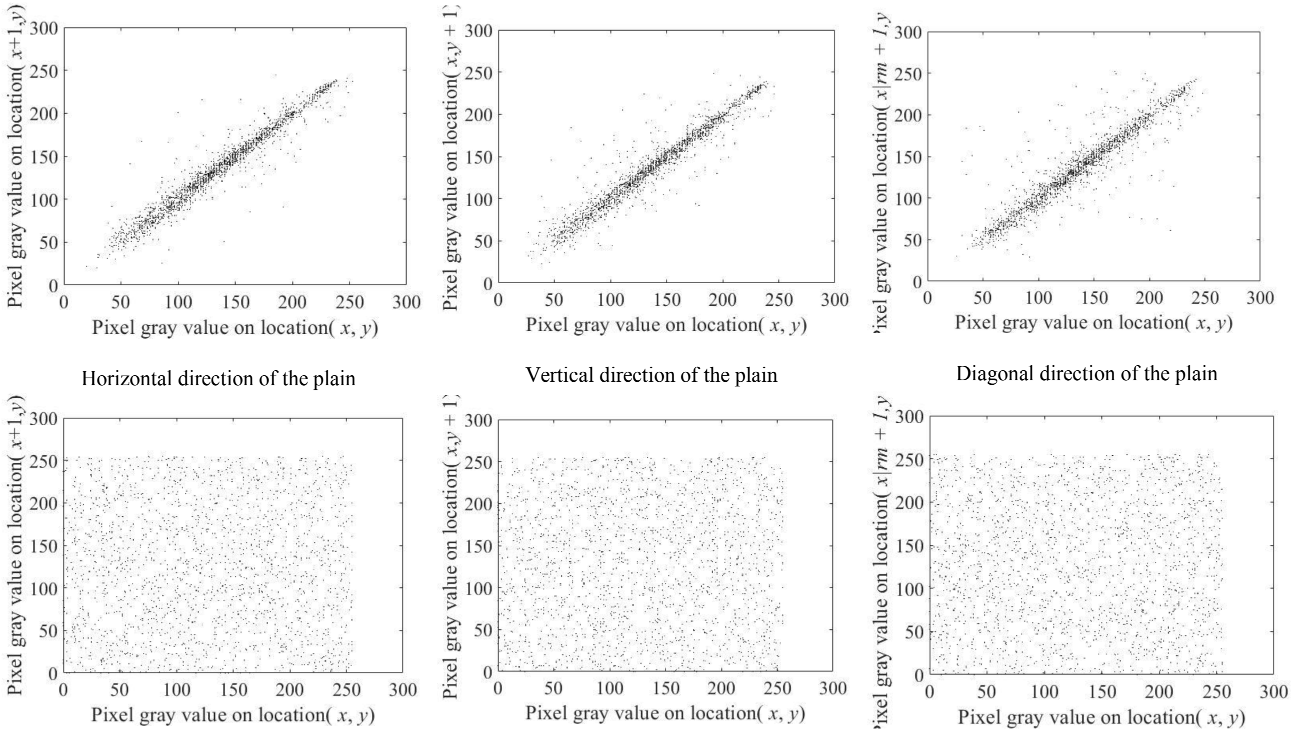
Hill plain histogram

Lena cipher histogram

Women cipher histogram

Hill cipher histogram

Fig. 9. Plain and cipher histograms of Lena, Women, and Hill



Horizontal direction of the plain

Vertical direction of the plain

Diagonal direction of the plain

Horizontal direction of the cipher

Vertical direction of the cipher

Diagonal direction of the cipher

Fig. 10. Correlation distribution of adjacent pixels in a Lena image

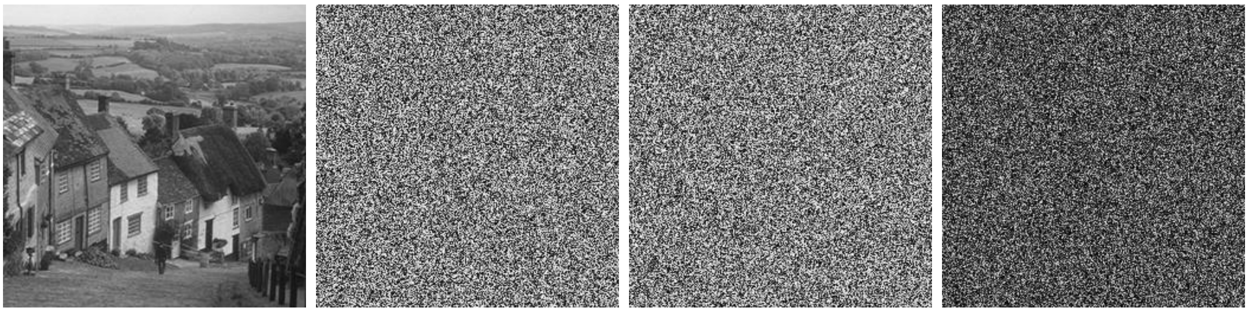
NPCR is the proportion of different pixels in the total pixels in the two images. The theoretical expectation of *NPCR* is 99.6094%.The calculation of *NPCR* is shown in Equation (22).

$$NPCR\left(P1,P2\right)=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|\left(SgnP1\left(i,j\right)-P2\left(i,j\right)\right)\right|\times 100\% \quad (22)$$

The difference between all the pixels at the same position in the two images is calculated, and then the average of the ratio of this difference to the maximum difference (255) is calculated. This average is *UACI*, and its theoretical expected value is 33.4635%. The calculation of *UACI* is shown in Equation (23).

$$UACI\left(P1,P2\right)=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|\frac{\left(P1\left(i,j\right)-P2\left(i,j\right)\right)}{255}\right|\times 100\% \quad (23)$$

In the experiment, a parameter in the key *K* is changed by 10−14 each time, and the difference operation is performed on the two cipher images before and after the key change, and it is concluded that the two cipher images are quite different. The cipher images and their difference images before and after key change encryption are shown in Figure 11, and the result analysis is shown in Table 4. (take the Hill image as an example).



Hill plain image　Hill cipher image 1　Hill cipher image 2　Hill cipher difference image

Fig. 11. Hill plain, cipher before and after changing the key and their image difference

TABLE 4
KEYS SENSITIVITY

Algorithm	NPCR（%）	UACI(%)
Proposed	99.6045	33.4660
Ref.[13]	99.4099	33.3990
Ref.[15]	99.6049	33.4656
Ref.[16]	99.6100	33.4529
Ref.[17]	99.5701	33.4520
Ref.[18]	99.6313	33.5321
Theoretical value	99.6094	33.4635

In the experiment, after changing the key parameters 1000 times, we calculated the values of *NPCR* and *UACI*. According to table 4, the values of the *NPCR* and *UACI* of the algorithm are quite close to the theoretical values, so that this algorithm has good key sensitivity. It can effectively resist discriminatory attacks.

(5) Plain sensitivity analysis

The plain pixel values are slightly changed and compared between plain encrypted ciphers and encrypted ciphers to compute NPCR and UACI to analyze plain sensitivity after comparing plain differences.

In the experiment, a small change (+ 1 or - 1) was carried out for the random pixel value of the Lena plane image. This experiment is performed 1000 times, and the average value of NPCR and UACI is calculated. The experimental results are displayed in Table 5.

TABLE 5
PLAIN SENSITIVITY

Algorithm	NPCR（%）	UACI(%)
Proposed	99.5934	33.5535
Ref.[13]	99.6101	33.4801
Ref.[15]	99.5926	33.3386
Ref.[16]	99.6098	33.4537
Ref.[17]	99.6097	33.4819
Ref.[18]	99.6922	33.3313
Theoretical value	99.6094	33.4635

The proposed algorithm in this paper incorporates plain pixels during the encryption computation. Moreover, in order to resist the separate attacks of diffusion or scrambling, diffusion and scrambling are carried out at the same time, so the index of the algorithm is closer to the theoretical value.

(6) Information entropy

Information entropy shows uncertainty of image information. It is generally considered that the larger the entropy, the larger the uncertainty and the less visible information. The calculation of information entropy is calculated in Equation (24).

$$H = -\sum_{i=0}^{L} p(i)\log_2 p(i) \qquad (24)$$

In Equation 24, L is the gray level of the image and $L=256$, and $p(i)$ is the probability of the occurrence of gray value i.

The information entropy results of the proposed algorithm in this paper are shown in Table 6.

TABLE 6
INFORMATION ENTROPY RESULTS

Algorithm	Information entropy
Proposed（plain）	7.2767
Proposed (cipher)	7.9991
Ref.[13] (cipher)	7.9993
Ref.[15] (cipher)	7.9992
Ref.[16] (cipher)	7.9991
Ref.[17] (cipher)	7.9892
Ref.[18] (cipher)	7.9996
Theoretical value	8

In a 256 * 256 images, the theoretical value of information entropy is 8. According to the values in table 6, the information entropy of the cipher generated by the proposed algorithm is quite close to the theoretical value.

IV. CONCLUSION

In this paper, a multi-chaos fusion digital image snake encryption algorithm is proposed. The classic Logistic algorithm and the PWLCM algorithm are integrated into the LPW algorithm, which expands the key space. Three rounds of image encryption are executed, the first round of execution route is the snake's S-shaped crawling trajectory, the second round of execution route is the snake's reverse S-shaped crawling trajectory, and the third round is the snake's hibernation mode, each round will scramble The diffusion process is carried out at the same time, so that the attacker cannot attack separately in the scrambling and diffusion process, and the speed of encryption and decryption is improved. In the diffusion, plain pixels are added to become a plain associated image encryption algorithm, which increases the security of the algorithm. In the experiment, the keys sensitivity, plain sensitivity, correlation coefficient and information entropy of the algorithm are not lower than other algorithms. The speed of encryption and decryption is improved, the key space is enlarged, and the efficiency, security and feasibility of the algorithm are proved.

REFERENCES

[1] J. ALLEN, “Short term spectral analysis, synthesis, and modification by Discrete Fourier Transform,” IEEE Transactions on Acoustics Speech & Signal Processing. vol. 25, no. 3, pp. 235-238, 1977.

[2] Ye Tao,Wenhua Cui, Zhao Zhang, “Spatiotemporal chaos in multiple dynamically coupled map lattices and its application in a novel image encryption algorithm,” Journal of Information Security and Applications. vol. 55, no.1, pp. 2214-2126, 2020.

[3] R. Matthews, “On the derivation of a “Chaotic encryption algorithm,” Cryptologia. vol. 8, no. 1, pp. 29-41, 1989.

[4] J. Fridrich, “Symmetric ciphers based on two dimensional chaotic maps,” International Journal of Bifurcation and Chaos, vol. 8, no.1, pp.1259-1284, 1998.

[5] G. Jakimoski, L. Kocarev, “Chaos and cryptography: block encryption ciphers based on chaotic maps,” IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, vol. 48, no. 2, pp. 163-169, 2001.

[6] L. Liu, S. Miao, “A new image encryption algorithm based on logistic chaotic map with varying parameter,” Springer Plus, vol. 5, no. 1, pp. 1-12, 2016.

[7] Q. Nasir, H. H. Abdlrudha, “High security nested PWLCM chaotic map bit-level permutation basedimage encryption,” International Journal of Communications Network & System Sciences, vol. 5, no. 9. pp. 548-556, 2014.

[8] Diab, Hossam, El-semary, “Cryptanalysis and Improvement of the Image Cryptosystem Reusing Permutation Matrix Dynamically,” Signal Processing,vol.18, pp.1-31, 2018.

[9] X. Tong, M. Cui, “Image encryption with compound chaotic sequence cipher shifting dynamically,” Image and Vision Computing, vol.26, pp.843-850, 2008.

[10] G. Tu, X. Liao, X. Tao, “Cryptanalysis of a color image encryption algorithm based on chaos,” Optik - International Journal for Light and Electron Optics, vol.124, pp.5411-5415, 2013.

[11] X. Wang, T. Lin, Q. Xue, “A novel color image encryption algorithm based on chaos,” Signal Processing, vol. 92, pp. 1101-1108, 2012.

[12] L. Liu, Z. Zhang, R. Chen, “Cryptanalysis and improvement in a plain-related image encryption scheme based on hyper chaos,” IEEE Access, vol. 7, pp. 126450-126463, 2019.

[13] Z. Li, C. Peng, L. Li, X. Zhu, “A novel plain-related image encryption scheme using hyper-chaotic system,” Nonlinear Dynamics, vol. 94, pp. 1319–1333, 2018.

[14] Wang X , Zhang J . “Chaotic secure communication based on nonlinear autoregressive filter with changeable parameters”. Physics Letters A, vol. 15, pp. 323-329, 2006.

[15] Meysam, Asgari-Chenaghlu, Mohammad-Ali, et al. “A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation,” Signal Processing, vol. 157, pp. 1-13, 2019.

[16] Y. Chen, C. Tang, Z. Yi, “A Novel Image Encryption Scheme Based on PWLCM and Standard Map,”Complexity. vol.15, pp. 23-31, 2020.

[17] X. Wu, H. Kan, Ju, et al. “A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps,”Applied Soft Computing, vol. 37, pp. 24-39, 2015.

[18] X. J. Tong, M. Zhang, Z. Wang, et al, “A fast encryption algorithm of color image based on four-dimensional chaotic system,” Journal of Visual Communication and Image Representation, vol. 33, pp.219-234, 2015.