IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 1, 2019, accepted March 15, 2019, date of publication March 19, 2019, date of current version April 5, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2906052

An Image Encryption Method Based on Elliptic Curve Elgamal Encryption and Chaotic Systems

YULING LUO[1], XUE OUYANG[1], JUNXIU LIU[1], (Member, IEEE), AND LVCHEN CAO[2]
[1]School of Electronic Engineering, Guangxi Normal University, Guilin 541004, China
[2]School of Information and Electronics, Beijing Institute of Technology, Beijing 100081, China

Corresponding author: Junxiu Liu (j.liu@ieee.org)

This work was supported in part by the National Natural Science Foundation of China under Grant 61801131 and Grant 61661008, in part by the Guangxi Natural Science Foundation under Grant 2017GXNSFAA198180 and Grant 2016GXNSFCA380017, in part by the funding of Overseas 100 Talents Program of Guangxi Higher Education under Grant F-KA16035, in part by the Science and Technology Major Project of Guangxi under Grant AA18118004, and in part by the Innovation Project of Guangxi Graduate Education under Grant XYCSZ2019071.

ABSTRACT Due to the potential security problem about key management and distribution for the symmetric image encryption schemes, a novel asymmetric image encryption method is proposed in this paper, which is based on the elliptic curve ElGamal (EC-ElGamal) cryptography and chaotic theory. Specifically, the SHA-512 hash is first adopted to generate the initial values of a chaotic system, and a crossover permutation in terms of chaotic index sequence is used to scramble the plain-image. Furthermore, the generated scrambled image is embedded into the elliptic curve for the encrypted by EC-ElGamal which can not only improve the security but also can help solve the key management problems. Finally, the diffusion combined chaos game with DNA sequence is executed to get the cipher image. The experimental analysis and performance comparisons demonstrate that the proposed method has high security, good efficiency, and strong robustness against the chosen-plaintext attack which make it have potential applications for the image secure communications.

INDEX TERMS SHA-512 hash, elliptic curve ElGamal encryption, chaos game, crossover permutation.

I. INTRODUCTION

Recently, various methods have been presented to meet the challenges of image data security requirements [1]–[5]. According to different types of key distribution, the cryptosystems are mainly divided into two categories, which are symmetric and asymmetric encryptions [6]. In the symmetric encryption, the encryption key is same as decryption key or it is easy to calculate the other key based on one known key. The advantages of symmetric encryption algorithms are low computational complexity, fast speed [7]–[11]. But one of the most significant problems in symmetric encryption is the management and distribution of key. In other words, when users employ symmetric encryption algorithm multiple times, the number of keys will increase dramatically. Moreover, the key may suffer from the risk of attacker interception in the key distribution process. Thus, no matter how the key is managed and distributed, it is slow and expensive, which becomes a burden on secure communication.

The associate editor coordinating the review of this manuscript and approving it for publication was Di He.

In order to solve this problem, the asymmetric encryption requires that the encryption key should be different from the decryption key, and the decryption key cannot be calculated from the encryption key. The asymmetric encryption achieves the secure communication among multiple users, and distributing key on the unsecure channel can also be avoided. Two different types of keys namely the public key and the private key are required in asymmetric encryption. The public key can be made public, which is available for everyone while the private key can only be kept by receiver. The theory of asymmetric encryption is shown in Fig. 1. The key pair is firstly kept by receiver, and the public key is sent to transmitter. Then, transmitter encrypt the information with public key, where the public key can be sent in any way because the cipher information can be only decrypted successfully with the private key. Finally, the cipher information is sent to the receiver and decrypted with the private key. In the asymmetric encryption, the private key is only kept by receiver, which can greatly facilitate key management and distribution.

Elliptic Curve Cryptography (ECC), as an significant asymmetric encryption technology, is proposed in [12]. The

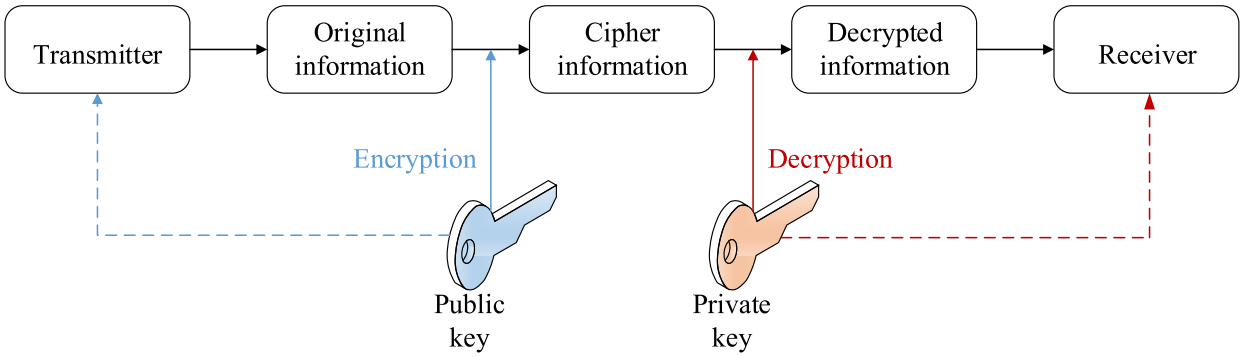

FIGURE 1. The theory of asymmetric encryption.

theory of ECC is based on elliptic curve mathematics, which is the difficulty to calculate the discrete logarithm of the ellipse curve on the Abelian group by using rational points [13]. The ECC has relative high security, short keys, and it is faster than the classical counterparts such as Ron Rives Adi Shamir Leonard Adleman (RSA) and Digital Signature Algorithm (DSA) [14]. Therefore, ECC has bring extensive attention in the fields of authentication [15], digital signature [16], secure communication [17] and signal processing [18] etc. Many methods of image encryption based on the characteristics of ECC are proposed. For example, a color image encryption method is proposed in [19], which utilizes the combination of discrete chaotic map (2D-TFCDM) and Menezes-Vanstone ECC (MVECC). In this method, the keys and parameters are generated by the MVECC, and fractional 2D-TFCDM is used to scramble and diffuse the image. The experiment results demonstrate that this method can resist various attacks. In [20], a method based on DNA encoding and elliptic curve Diffie-Hellman encryption (ECDHE) is introduced, in which the plain image is transformed into DNA matrix by DNA encoding. DNA addition operation is performed on each component, and the cipher image is obtained by ECDHE. Results show that this method has large key space and it can defend common attacks effectively. Based on the ECC and the public key cryptosystem, Elliptic Curve ElGamal (EC-ElGamal) cryptosystem is introduced in [21], which is widely applied in the field of image encryption. In approach of [22], a method of color image encryption based on chaotic systems and EC-ElGamal is presented. Firstly, the plain image is compressed for the purpose of grayscale expansion, and then the compressed image is encrypted by the improved four-dimensional cat map. Finally, the EC-ElGamal encryption algorithm is used for global expansion to obtain the cipher image. This method performs well in statistical analysis and differential attacks, which shows better security compared with other algorithms. Similarly, EC-ElGamal-based method of image encryption is proposed in [23], where a new additive homomorphism in the EC-ElGamal cryptosystem is employed. Furthermore, a medical image encryption method using improved ElGamal encryption technique is presented in [24], in which the operation of embedding plaintext pixels into elliptic curve is discarded. This method can encrypt multiple pixels at the same time, and the results show that it has fast encryption speed.

As an excellent candidate for the key generation of cryptosystem, chaotic systems have characteristics of ergodicity, sensitivity to initial conditions, and long-term unpredictability, which are applied in different fields [25]–[30]. A plenty of chaos-based image encryption methods have been proposed, which include the intertwining Logistic map [31], the Chebyshev map [32], the Arnold cat map [33] the Tent map [1], the Lorenz system [34], the spatiotemporal chaotic system [3], the hyper-chaotic system [35], the memristive chaotic system [36], etc. Chaos-based design patterns are developed to make the encryption process more complicated, which have better encryption performance and capability in resisting different attacks [37], [38]. Furthermore, in [39], the concept of chaos game is proposed in the field of fractal. This is a fast-statistical method for analyzing the internal structure of DNA sequences. It uses a simple Iterative Function System (IFS) to generate fractal graphics in a two-dimensional plane. This method has been widely applied in many research areas such as biotechnology [40] and signal processing [41].

Based on the aforementioned analysis, a novel image encryption method based on EC-ElGamal encryption and chaotic systems is proposed in this paper. The main contributions of this paper include (a) In order to improve the security in existing architecture of permutation-diffusion, a novel encryption structure that permutation-EC-ElGamal encryption-diffusion is designed, which makes separate attacks become more difficult; (b) A method of crossover permutation based on coupled Logistic-Tent map (LTM) and coupled Tent-Sine map (TSM) is introduced, in which the initial values of LTM and TSM are generated by SHA-512 hash. This design not only can resist the known-plaintext attack and chosen-plaintext attack, but also improves the randomness of the pixel distribution; (c) A method of image pixels embedding into elliptic curve is proposed, then the EC-ElGamal encryption is performed. This method is simple for operating, and the EC-ElGamal encryption can greatly improves the

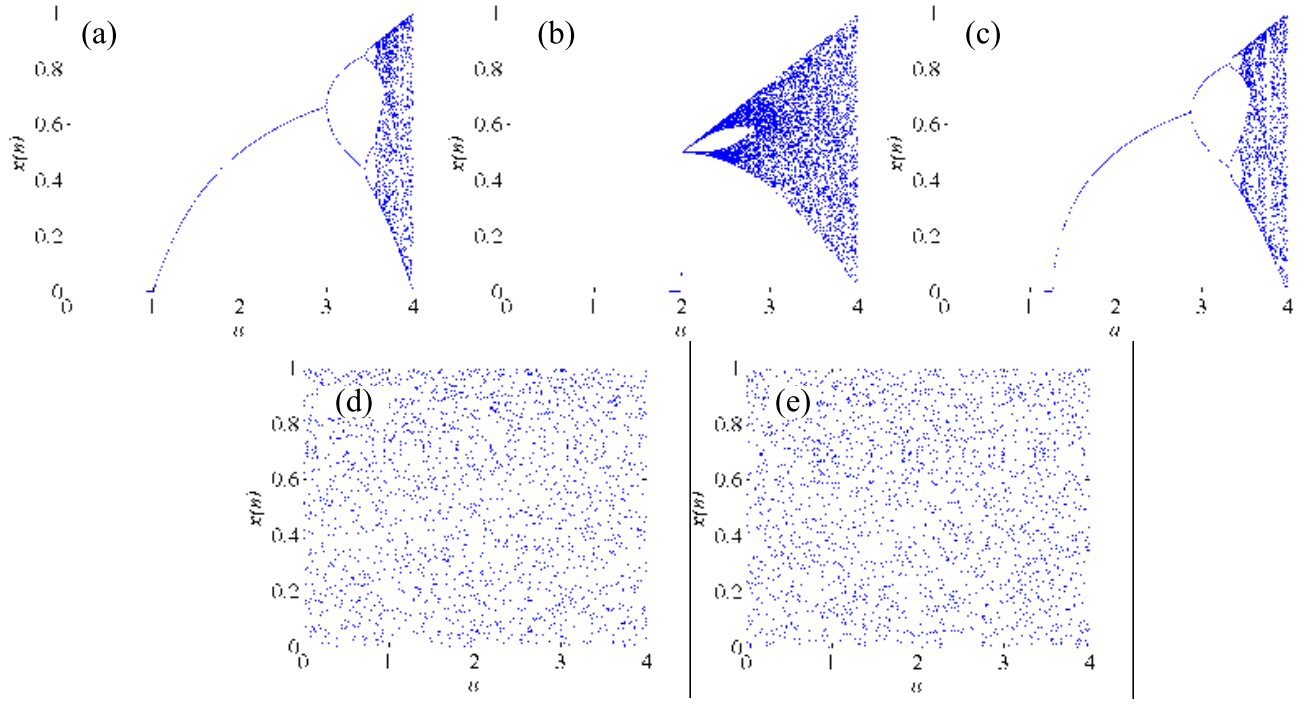

FIGURE 2. Bifurcation diagrams of the (a) Logistic map; (b) Tent map; (c) Sine map; (d) LTS map; (e) TSM map.

encryption performance; (d) A method of diffusion based on chaos game is presented, in which DNA sequence is introduced as the keys, and two sequences of chaos game are generated to diffuse the image. This method achieves good effect in diffusion, which can resist the differential attack effectively.

The rest parts of the paper are arranged as follows. In Section II, the preliminary studies in the proposed method are introduced. The frameworks of encryption and decryption are detailed in section Section III. In Section IV, the simulation results and analyses the security performance are reported. Section V concludes this paper.

II. PRELIMINARIES

A. COUPLED LOGISTIC-TENT MAP (LTM) AND COUPLED TENT-SINE MAP (TSM)

Coupled chaotic map is a combination of two one-dimensional chaotic maps, which is given in [42]

$$F(x_{n+1}) = mod(f(x_n) + g(x_n), 1), \tag{1}$$

where $f(x_n)$ and $g(x_n)$ are different one-dimensional chaotic maps, $mod(x, y)$ is modulo operation which returns the remainder of x divided by y. The range of iteration values of coupled chaotic map is (0, 1) due to modulo operation.

In addition, the Logistic map, Tent map and Sine map are the three widely used one-dimensional chaotic maps, which are described as Eq.2, Eq.3 and Eq.4, respectively.

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

$$x_{n+1} = \begin{cases} \mu x_n, & if\ x_n < 0.5 \\ \mu 1 - x_n, & if\ x_n \geq 0.5, \end{cases} \tag{3}$$

$$x_{n+1} = \frac{a}{4}\sin(\pi x_n). \tag{4}$$

The coupled Logistic-Tent map (LTM) and coupled Tent-Sine map (TSM) based on Eq.1 are introduced in [42], in which LTM is combined with Logistic map and Tent map, and TSM is combined with Tent map and Sine map. They are given by

$$\mathrm{F}_{\mathrm{LTM}}(x_{n+1}) = \begin{cases} mod(\mu x_n(1 - x_n) + \dfrac{(4-\mu)x_n}{2}, 1), & if\ x_n < 0.5 \\ mod(\mu x_n(1 - x_n) + \dfrac{(4-\mu)(1-x_n)}{2}, 1), & if\ x_n \geq 0.5, \end{cases} \tag{5}$$

and

$$\mathrm{F}_{\mathrm{TSM}}(x_{n+1}) = \begin{cases} mod(\dfrac{\mu x_n}{2} + \dfrac{(4-\mu)\sin(\pi x_n)}{4}, 1), & if\ x_n < 0.5 \\ mod(\dfrac{\mu(1-x_n)}{2} + \dfrac{(4-\mu)\sin(\pi x_n)}{4}, 1), & if\ x_n \geq 0.5, \end{cases} \tag{6}$$

where $\mu \in (0, 4]$. The bifurcation diagrams of Logistic map, Tent map, Sine map, LTM and TSM are shown in Fig. 2. The outputs of LTM and TSM evenly distribute in $(0, 4]$, which have larger range than Logistic map, Tent map and Sine map.

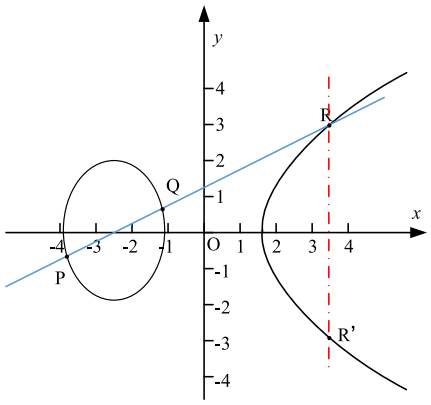

FIGURE 3. The theory of asymmetric encryption.

B. ELLIPTIC CURVE ELGAMAL (EC-ELGAMAL)

The elliptic curve is a set of points that satisfy the Weierstrass equation in the projective plane [22]. Let E_p be an elliptic curve equation over a finite field, and it is given as

$$y^2 = x^3 + ax + b \ (mod\ p), \tag{7}$$

where a and b are two constants which satisfy $4\,a^3 + 27\,b^2 \neq 0$, p is a prime [12]. Specially, the coordinates on the elliptic curve follow the additive Abelian property [13].

Definition 1: Addition on elliptic curve. Suppose P, Q, R, O are four points on elliptic curve E_p (O is an infinite point):

(1). $O + P = P + O = P$;

(2). $-O = O$;

(3). If $P(x, y) \neq 0$, then $-P = (x, -y)$;

(4). If $Q = -P$, then $P + Q = O$;

(5). If $P \neq Q$, $Q \neq O$, $Q \neq -P$, R denotes another intersection of straight line PQ (if $P \neq Q$) or E_p at the intersection point of P (if $P = Q$) with another point of elliptic curve E_p, then $P + Q =$ âĹ′R.

As shown in Fig.3, $P\,(x_1, y_1)$ and $Q\,(x_2, y_2)$ are taken on the elliptic curve randomly, and a straight line is made at another point R on the elliptic curve. Then, cross the parallel line of the y-axis over R to R', and define $P\,(x_1, y_1) + Q\,(x_2, y_2) = R'\,(x_3, y_3)$, $R' = -R = (x_3, -y_3)$. Therefore, the result of point addition $R'\,(x_3, y_3)$ is given by

$$\begin{cases} x_3 = \tau^2 - x_1 - x_2 \\ y_3 = \tau(x_1 - x_3) - y_1, \end{cases} \tag{8}$$

where τ is slope, and it is defined as

$$\tau = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & if\ P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1}, & if\ P = Q, \end{cases} \tag{9}$$

Through the above analysis, it can be concluded that the result of point addition is all on the elliptic curve [23].

Furthermore, combining the law of addition on elliptic curve and discrete logarithm operations, a cryptosystem based on elliptic curves can be established. Elliptic Curve Discrete Logarithm Problem (ECDLP) is an asymmetric cryptosystem, which can establish a security cryptosystem based on elliptic curve cryptosystem.

Definition 2: Suppose p is a prime and E_p is an elliptic curve. For the two points P and Q on the elliptic curve, they satisfy $Q = kP$. It can be proved that it is easier to calculate Q from k and P. However, it is difficult to calculate k from Q and P [22].

Because of irreversible solution on the ECDLP, ElGamal cryptosystem is introduced and known as EC-ElGamal [21], which can provide a faster speed and a smaller key length. Moreover, the security of EC-ElGamal is higher than the other classical counterparts [12]. The specific encryption and decryption processes of EC-ElGamal are performed as follows

Step 1: Generation of keys for receiver:

(i). The elliptic curve equation $E_p : y^2 = x^3 + ax + b$, prime p and basic point L are selected.

(ii). Private key d is set by receiver, then Q is calculated by $Q = dL$.

(iii). Keys E_p, p, L, Q are exposed.

Step 2: Encryption processes of transmitter:

(i). The plaintext is known as U, and it is converted to point U' on the elliptic curve filed.

(i). Private key k is set by transmitter, then $C_1 = kL$ and $C_2 = U' \otimes kQ$, where "$\otimes$" denotes addition operation on elliptic curve.

(iii). Transmit encrypted data C_1, C_2 to receiver.

Step 3: Decryption processes of receiver:

(i). According to the private key d of receiver, U' is given by

$$\begin{aligned} U' &= C_2 \oslash dC_1 \\ &= (U' \otimes kQ) \oslash d(kL) \\ &= U' \otimes (k \cdot dL \oslash d \cdot kL) = U', \end{aligned} \tag{10}$$

where "$\oslash$" is the inverse addition operation on elliptic curve.

(iii). Restore U' to U from the plaintext.

C. DNA SEQUENCE REPRESENTATION BASED ON CHAOS GAME

Deoxyribonucleic acid (DNA) is a biological macromolecule, which is composed of genetic instructions and life functioning. DNA is consisted of four types of bases: Adenine (A), Thymidine (T), Cytosine (C) and Guanine (G). Thus, there are eight kinds of encoding rules [43] which are listed in Table 1. In addition, the Chaos Game Representation (CGR) of DNA sequences based on iterative function is a statistical method for DNA sequence analysis. It can be expressed as the distribution of a certain length of base in DNA sequences [39].

In the DNA-based chaos game, four DNA bases (A, T, C, G) are input into the chaos game. The processes of DNA-based chaos game include two main steps. The coordinates of four bases C(0,0), A(1,0), T(0,1) and G(1,1) are firstly determined. Then, a seed point M(x_0, y_0) is set. If the

TABLE 1. DNA encoding rules [43].

Rule	1	2	3	4	5	6	7	8
00	A	A	T	T	G	G	C	C
01	G	C	G	C	A	T	A	T
10	C	G	C	G	T	A	T	A
11	T	T	A	A	C	C	G	G

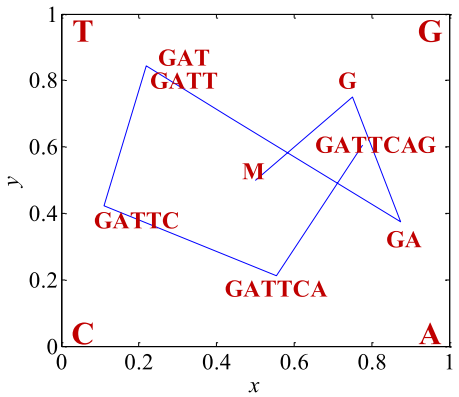

FIGURE 4. Route of chaos game when the DNA sequence is "GATTCAG".

base of DNA sequence is A, the midpoint between M and A is taken as the new starting point. In the same way, the position of each base can be expressed as

$$\begin{cases} x_{i+1} = 0.5(x_i + X_i) \\ y_{i+1} = 0.5(y_i + Y_i), \end{cases} \tag{11}$$

where x_i and y_i are the x and y coordinates of chaos game points, X_i and Y_i represent the corresponding coordinates of four bases.

For instance, a DNA sequence is "GATTCAG". Based on the coordinates of four bases, sequences X_i and Y_i are the corresponding coordinates of the four bases, i.e., $X_i = \{1, 1, 0, 0, 0, 1, 1\}$ and $Y_i = \{1, 0, 1, 1, 0, 0, 1\}$, seed point $M(x_0, y_0) = (0.5, 0.5)$. Thus, the positions of chaos game are iterated by Eq.11, and Fig.4 shows the routes of x_{i+1} and y_{i+1}.

D. CROSSOVER OPERATOR

Genetic algorithm is a computational model that simulates Darwin's theory of natural selection and the process of natural biological evolution. Genetic algorithm consists of three basic genetic operators: selection, crossover and mutation [44]. In general, the selection operator plays the role of selecting the best individuals from the group, the crossover operator is used to reorganize the selected individuals, and the new individuals can be generated by the mutation operator.

There are several methods in crossover algorithm, which are single-point crossover, multiple-point crossover and uniform crossover etc. In single-point crossover, single point is selected in the individual string randomly, and the two individuals at that point are swapped. Similarly, multiple crossover points are selected randomly in the individual string in multiple-point crossover, and perform the same

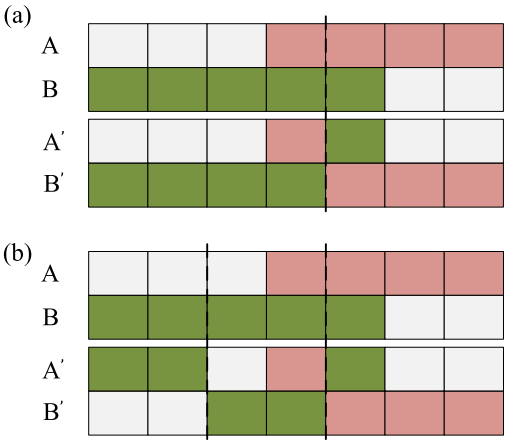

FIGURE 5. The processes of (a). single-point crossover; (b). multiple-point crossover (point=2).

operations [45]. Fig.5 shows the processes of single-point crossover and multiple-point crossover, in which A and B are two individuals, A′ and B′ are the new individuals obtained by crossover operation. In this paper, the multiple-point crossover is used to scramble the plain image.

III. THE PROCESS OF ENCRYPTION AND DECRYPTION

There are two main processes in traditional image encryption, which are permutation and diffusion [46]. In the permutation phase, the correlation of adjacent pixels are reduced and the information entropy is increased. However, the tonal distribution of scrambled image is same as plain image, which is vulnerable to statistical attacks. In order to improve the security of the proposed method, the EC-ElGamal encryption is employed before diffusion operation. That is, there is no connection between permutation and diffusion, which makes separate attacks become more difficult, and only one round of encryption can achieve good performance.

Suppose the size of the plain image $\mathbf{I}$ is M $\times$ N. The flowchart of the proposed images encryption method is shown in Fig.6. There are three main processes in the proposed encryption method, which include the crossover permutation, EC-ElGamal encryption and diffusion. Specially, EC-ElGamal is asymmetric encryption, so that the encryption keys and the decryption keys are different.

A. THE PROCESS OF ENCRYPTION

(1). Generation of the chaotic sequences

In this paper, SHA-512 is employed to generate the initial values of chaotic maps. When two images only have one pixel difference, their hash values are completely different [47]. Thus, SHA-512 can achieve the randomness of the key and the security of the encryption method.

Firstly, the 512-bit secret key H generated from SHA-512 is divided into 128 blocks, and the length of each block is 4-bit. H can be described as

$$\mathrm{H} = h_1, h_2, h_3, \ldots, h_{127}, h_{128}. \tag{12}$$

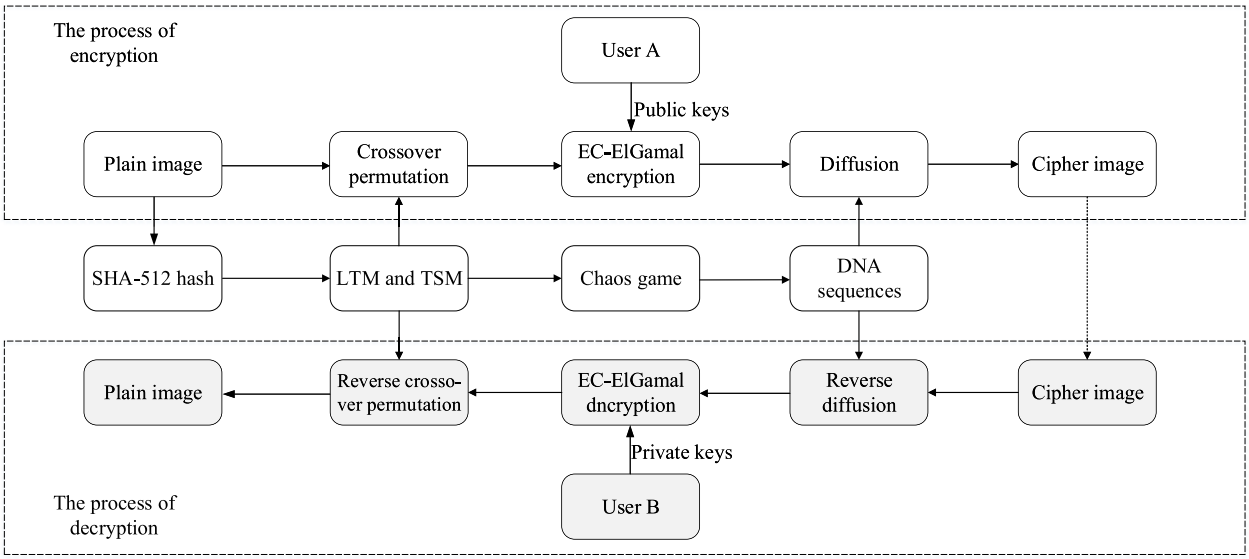

FIGURE 6. The block diagram of the proposed encryption method.

The intermediate parameters A, B, C and D are given by

$$\begin{cases} A = h_1 + h_2 + \cdots + h_{32} \\ B = h_{33} + h_{34} + \cdots + h_{64} \\ C = h_{65} + h_{66} + \cdots + h_{96} \\ D = h_{97} + h_{98} + \cdots + h_{128}. \end{cases} \tag{13}$$

The initial values $x_1, x_2, x_3, x_4, x_5, x_6$ of the chaotic system are obtained by: if $A > B$, B/A is the initial value of x_1; otherwise, A/B is the initial value. Similarly, the initial values x_2, x_3, x_4, x_5, x_6 are obtained based on B and C, C and D, A and C, A and D, B and D, respectively.

Then, four chaotic sequences $\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3, \mathbf{X}_4$ are generated from x_1, x_2, x_3, x_4 by using LTM (Eq.5) and TSM (Eq.6), where $\mathbf{X}_1$, $\mathbf{X}_2$ are generated from x_1, x_2 by LTM, and $\mathbf{X}_3$, $\mathbf{X}_4$ are generated from x_3, x_4 by TSM. For each element of $\overline{\mathbf{X}}_1, \overline{\mathbf{X}}_2, \overline{\mathbf{X}}_3$ and $\overline{\mathbf{X}}_4$, the quantization operations are performed according to

$$\begin{cases} \overline{\mathbf{X}}_1 = floor(mod(\mathbf{X}_1 \times 10^{14}, \mathrm{M})) + 1 \\ \overline{\mathbf{X}}_2 = floor(mod(\mathbf{X}_2 \times 10^{14}, \mathrm{N})) + 1 \\ \overline{\mathbf{X}}_3 = floor(mod(\mathbf{X}_3 \times 10^{14}, \mathrm{M} \times \mathrm{N})) + 1 \\ \overline{\mathbf{X}}_4 = floor(mod(\mathbf{X}_4 \times 10^{14}, 255)) + 1. \end{cases} \tag{14}$$

Delete the repeated values in $\overline{\mathbf{X}}_1$, $\overline{\mathbf{X}}_2$, $\overline{\mathbf{X}}_3$, and three index sequences for crossover permutation $\overline{\mathbf{X}}'_1, \overline{\mathbf{X}}'_2, \overline{\mathbf{X}}'_3$ are obtained.

$$\begin{cases} \overline{\mathbf{X}}'_1 = [\overline{\mathbf{X}}'_1(1), \overline{\mathbf{X}}'_1(2), \ldots, \overline{\mathbf{X}}'_1(\mathrm{M})] \\ \overline{\mathbf{X}}'_2 = [\overline{\mathbf{X}}'_2(1), \overline{\mathbf{X}}'_2(2), \ldots, \overline{\mathbf{X}}'_2(\mathrm{N})] \\ \overline{\mathbf{X}}'_3 = [\overline{\mathbf{X}}'_3(1), \overline{\mathbf{X}}'_3(2), \ldots, \overline{\mathbf{X}}'_3(\mathrm{M} \times \mathrm{N})]. \end{cases} \tag{15}$$

In addition, the DNA sequence $\mathbf{W}$ is generated by $\overline{\mathbf{X}}_4$, which is used for generating the chaos game sequences. The DNA encoding rule is ra, it is given by

$$ra = mod(\mathrm{sum}(\mathrm{H}), 8) + 1. \tag{16}$$

The sequences of chaos game $\mathbf{S}_x$ and $\mathbf{S}_y$ are iterated by Eq.11 for $(\mathrm{M} \times \mathrm{N} - 1)$ times, in which seed point $\mathrm{M}(x_0, y_0) = (0.5, 0.5)$, $\mathbf{S}_x(1)$ and $\mathbf{S}_y(1)$ are x_5 and x_6, respectively. Then, the quantization operations are performed according to

$$\begin{cases} \overline{\mathbf{S}}_x = floor(mod(\mathbf{S}_x \times 10^{14} \\ \qquad + \mathbf{S}_y \times 10^{14}), 256) \oplus t \\ \overline{\mathbf{S}}_y = floor(mod(\mathbf{S}_x \times 10^{14} \\ \qquad - round(\mathbf{S}_y \times 10^{14})), 256) \oplus t, \end{cases} \tag{17}$$

where

$$t = floor(\mathrm{sum}(\mathbf{I})/(\mathrm{M} \times \mathrm{N})). \tag{18}$$

Finally, two chaotic sequences for diffusion $\overline{\mathbf{S}}_x$ and $\overline{\mathbf{S}}_y$ are obtained.

$$\begin{cases} \overline{\mathbf{S}}_x = [\overline{\mathbf{S}}_x(1), \overline{\mathbf{S}}_x(2), \ldots, \overline{\mathbf{S}}_x(\mathrm{M} \times \mathrm{N})] \\ \overline{\mathbf{S}}_y = [\overline{\mathbf{S}}_y(1), \overline{\mathbf{S}}_y(2), \ldots, \overline{\mathbf{S}}_y(\mathrm{M} \times \mathrm{N})]. \end{cases} \tag{19}$$

(2). Image encryption

There are three main operations in the proposed method, which includes crossover permutation, EC-ElGamal encryption and diffusion. These steps are presented as follows in detail.

- *Step 1.* Crossover permutation. Based on the index sequences $\overline{\mathbf{X}}'_1, \overline{\mathbf{X}}'_2, \overline{\mathbf{X}}'_3$, the crossover permutation is performed on the plain image, in which the multiple-point crossover is used to scramble the plain image. The pseudo code of crossover permutation is given in Algorithm 1, and Fig.7 shows the process of crossover permutation when the size of image is 3×3. First, the ith row and $\overline{\mathbf{X}}'_1(i)$th row are crossed, and $\overline{\mathbf{X}}'_1(i)$th row and $(i+1)$th row are crossed. In this process, i, $(i+1)$ and $\overline{\mathbf{X}}'_1(i))$ are the crossover points to get the row scrambled image (see Line 1-3). Then, the column scrambled image

Algorithm 1 Process of Crossover Permutation

Input: Plain image $\mathbf{I}$, index sequences $\overline{\mathbf{X}}_1'$, $\overline{\mathbf{X}}_2'$, $\overline{\mathbf{X}}_3'$.
Output: Scrambled matrix $\bar{\mathbf{I}}$

1: **for** each $i \in [1, \mathrm{M}-1]$ **do**
2: $\quad \mathbf{I}([i\ \ \overline{\mathbf{X}}_1'(i)], :) = \mathbf{I}([\overline{\mathbf{X}}_1'(i)\ \ i+1], :)$
3: **end for**
4: **for** each $i \in [1, \mathrm{N}-1]$ **do**
5: $\quad \mathbf{I}(:, [i\ \ \overline{\mathbf{X}}_2'(i)]) = \mathbf{I}(:, [\overline{\mathbf{X}}_2'(i)\ \ i+1])$
6: **end for**
7: $\mathbf{I_1} \leftarrow$ reshape($\mathbf{I}$,1,M $\times$ N)
8: **for** each $i \in [1, \mathrm{M} \times \mathrm{N}]$ **do**
9: $\quad \mathbf{I_1}(:, [1\ \ \overline{\mathbf{X}}_3'(i)]) = \mathbf{I_1}(:, [\overline{\mathbf{X}}_3'(i)\ \ 1])$
10: **end for**
11: **return** $\bar{\mathbf{I}} \leftarrow \mathbf{I_1}$

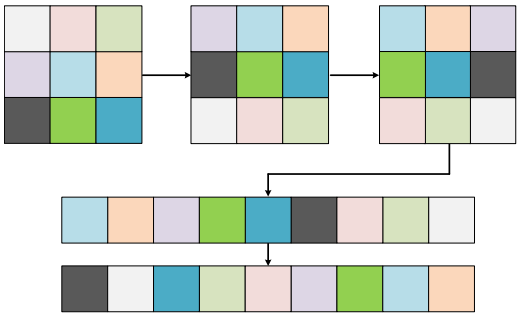

FIGURE 7. The process of crossover permutation when the size of image is 3 × 3.

is generated by using i, $(i+1)$ and $\overline{\mathbf{X}}_2'(i)$, i.e. crossover ith column and $\overline{\mathbf{X}}_2'(i)$ column, and crossover $\overline{\mathbf{X}}_2'(i)$th column and $(i+1)$th column (see Line 4-6). Similarly, in order to achieve a better performance of permutation, the column scrambled image is reshaped to one-dimensional vector $\mathbf{I_1}$, and crossover the elements of i and $\overline{\mathbf{X}}_3'(i)$ to obtain the scrambled matrix $\bar{\mathbf{I}}$, as shown by Line 7-10 of Algorithm 1.

- *Step 2.* EC-ElGamal encryption. Firstly, the coordinates of the elliptic curve are generated by the scrambled matrix. That is, the pixels of $\bar{\mathbf{I}}$ are embedding into elliptic curve, and the parameters p, a and b are selected. Then, if there is a solution quadratic congruence of pixel k in scrambled matrix $\bar{\mathbf{I}}$, i.e. $[y(k)]^2 = \left\{[x(k)]^3 + ax(k) + b\right\} \bmod p$ has solution of quadratic congruence, the coordinate of elliptic curve is obtained. Otherwise, since the results of point addition are all on the elliptic curve, the coordinates of the remaining points can be gotten by the point addition on the elliptic curve. Finally, the corresponding coordinates of the elliptic curve $\mathbf{G}(k) = \left(\mathbf{G}_x(k), \mathbf{G}_y(k)\right)$ can be generated by the pixel values of scrambled matrix $\bar{\mathbf{I}}$.
  Moreover, the parameters of the basic point L, private keys d, k and Q are selected. Then, EC-ElGamal encryption is performed, and two pair of keys $\mathbf{C}_1 = \left(\mathbf{C}_1^x, \mathbf{C}_1^y\right)$ and $\mathbf{C}_2 = \left(\mathbf{C}_2^x, \mathbf{C}_2^y\right)$ are described by $\mathbf{C}_1 = kL$ and $\mathbf{C}_2 = \mathbf{G} \otimes kQ$, which detailed illustration can be seen in the Section II-B.

$$\begin{cases} \mathbf{C}_1 = [(\mathbf{C}_1^x(1), \mathbf{C}_1^y(1)), (\mathbf{C}_1^x(2), \mathbf{C}_1^y(2)), \\ \qquad \ldots, (\mathbf{C}_1^x(\mathrm{M} \times \mathrm{N}), \mathbf{C}_1^y(\mathrm{M} \times \mathrm{N}))] \\ \mathbf{C}_2 = [(\mathbf{C}_2^x(1), \mathbf{C}_2^y(1)), (\mathbf{C}_2^x(2), \mathbf{C}_2^y(2)), \\ \qquad \ldots, (\mathbf{C}_2^x(\mathrm{M} \times \mathrm{N}), \mathbf{C}_2^y(\mathrm{M} \times \mathrm{N}))]. \end{cases} \tag{20}$$

- *Step 3.* Diffusion operation. The cipher matrix $\mathbf{E}'$ is obtained by diffusion, in which all the values on x coordinates are encrypted by $\mathbf{C}_2$, i.e. each pixel in $\mathbf{C}_2^x$ is encrypted and their corresponding cipher values are given by

$$\mathbf{E}'(i+1) = mod(\mathbf{C}_2^x(i) + \bar{\mathbf{S}}_x(i), 256) \oplus \bar{\mathbf{S}}_y(i) \oplus \mathbf{E}'(i). \tag{21}$$

The first value of cipher image $\mathbf{E}'(1)$ is obtained from t (in Eq.18), which is given by

$$\mathbf{E}'(1) = 255 - t, \tag{22}$$

where $i = 1, 2, \ldots, \mathrm{M} \times \mathrm{N} - 1$. Finally, the one-dimensional vector $\mathbf{E}'$ is reshaped with size of M × N to obtain the cipher image $\mathbf{E}$.

B. THE PROCESS OF DECRYPTION

In the decryption process, the following steps need to attention after the receiver receives the cipher image $\mathbf{E}$ and keys. Firstly, the one-dimensional vector $\mathbf{E}'$ is reshaped from the cipher image $\mathbf{E}$, and chaotic sequences $\bar{\mathbf{S}}_x(i)$ and $\bar{\mathbf{S}}_y(i)$ are generated by using the parameters and keys. Then, the inverse diffusion is given by

$$\mathbf{C}_2^x(i) = mod(\mathbf{E}'(i+1) \oplus \mathbf{E}'(i) \oplus \bar{\mathbf{S}}_y(i) - \bar{\mathbf{S}}_x(i), 256), \tag{23}$$

where $i = 1, 2, \ldots, \mathrm{M} \times \mathrm{N} - 1$.

Moreover, coordinate sequence $\mathbf{G}$ is constructed, and $\mathbf{C}_2$ is calculated by $\mathbf{C}_2 = \mathbf{G} \otimes kQ$. According to the keys of d and $\mathbf{C}_1$, scrambled matrix $\bar{\mathbf{I}}$ is given by $\bar{\mathbf{I}} = \mathbf{C}_2 \oslash d\mathbf{C}_1$. Finally, based on the index sequences $\overline{\mathbf{X}}_1'$, $\overline{\mathbf{X}}_2'$, $\overline{\mathbf{X}}_3'$, the plain image $\mathbf{I}$ can be obtained by the inverse operation of crossover permutation, which is described in Algorithm 1.

IV. SIMULATION AND SECURITY ANALYSIS

The simulation and performance analysis are provided in this section. As shown in Fig.8(a)-(e), the images of "Lena", "Barbara", "Peppers", "Baboon"and "Car" with the size of 512 × 512 are selected for the test, and the keys and parameters are set as $\mu = 2.5$, $p = 257$, $a = 1$, $b = 1$, $L = (254, 75)$, $d = 64$, $k = 86$. The scrambled images are shown in Fig.8(f)-(j), Fig.8(k)-(o) denote the corresponding cipher images, and the recovered images are displayed in Fig.8(p)-(t), respectively.

A. KEY SPACE ANALYSIS

The key space is the total set of keys during the process of image encryption. There are two assessments for key space analysis which include the number of keys and the key sensitivity.

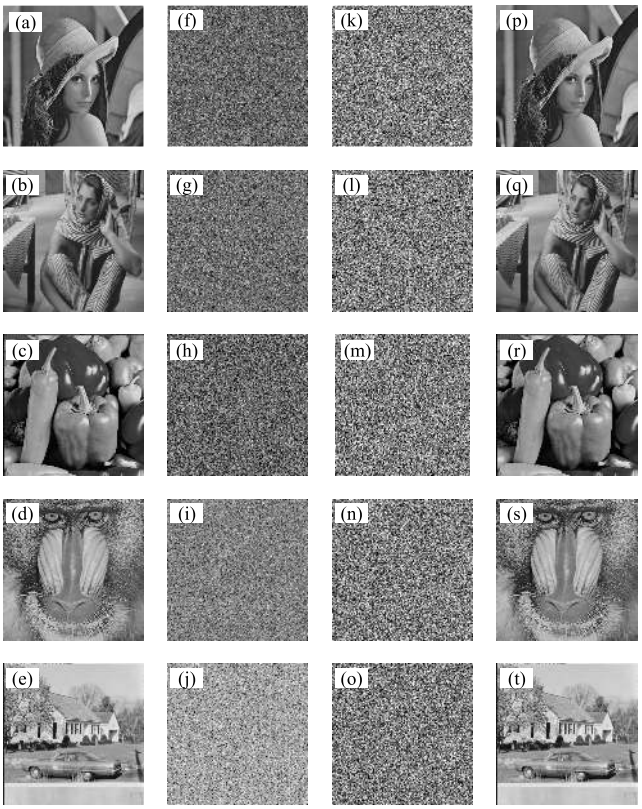

FIGURE 8. Simulation results. (a)-(e) the original images; (f)-(j) the corresponding scrambled images; (k)-(o) the corresponding cipher images; (p)-(t) the corresponding decrypted images.

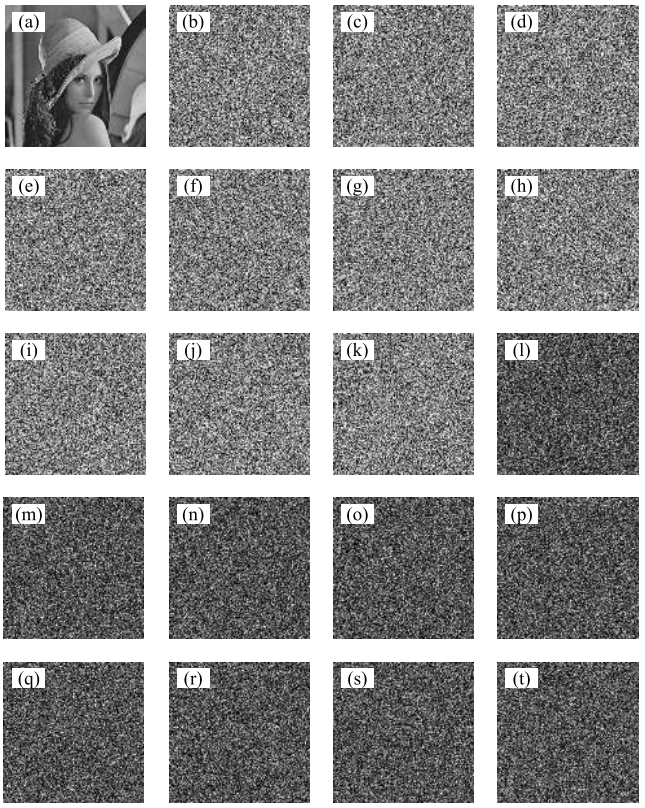

FIGURE 9. The key sensitivity analysis. (a) original "Lena" image; (b) cipher image with original keys; (c)-(k) the cipher images with modified keys. (l)-(t) the differences between (b) and (c)-(k).

1) THE NUMBER OF KEYS ANALYSIS

A large key space can prevent the attacker from getting the correct keys and improve the ability of resisting the brute force attack [1]. The key space includes all the keys that participate in the encryption process, and the key space is generally required to be 2^{100} [48].

In the proposed method, initial values are generated by SHA-512 hash, and the control parameters of chaotic maps is μ. If the computation precision is around 2^{52} [49], the key space is 2^{564}. Other keys in elliptic curve ElGamal encryption are: p, a, b, d, k, t, L $\left(\mathrm{L}_x\mathrm{L}_y\right)$. Therefore, the total key space is sufficient larger than 2^{100}, which can resist the brute force attack effectively.

2) KEY SENSITIVITY ANALYSIS

An excellent cryptosystem should be sensitive to all keys. There are two ways to evaluate the key sensitivity of image encryption. One is changing key slightly, and a completely different cipher image should be obtained. The other is that the plain image cannot be recovered even the decryption key change slightly [2].

In this test, ''Lena'' image in Fig.9(a) is firstly encrypted with the correct keys, and its cipher image with original keys is shown in Fig.9(b). Then, the SHA-512 hash value H (3cfe8e450192b18…079ffd4731c3b4367dbd) is modified to H_1 (3cfe8e450192b18…079ffd4731c3b4367dbe), and the new cipher image are shown in Fig.9(c).

Moreover, the other modified keys are listed in Table 2, and the new cipher images are shown in Fig.9(d)-(k). In addition, the differences between cipher image with original keys and modified keys are displayed in Fig.9(l)-(t). From these results, it can be learned that there are huge differences among the cipher images, which means that the proposed method is highly sensitive to the initial keys, i.e. when the key has tiny change, the cipher images are totally different. Therefore, the proposed method can effectively defend the brute force and statistical attacks.

B. STATISTICAL ANALYSIS

The ability of resisting statistical attack in terms of encryption performance can be assessed by the statistical analysis [50]. Two ways of measurements which include the analysis of histogram and correlation coefficient are applied for the statistical analysis.

1) THE HISTOGRAM ANALYSIS

The tonal distribution is reflected in the histogram, which can intuitively display the amount of each gray level. Therefore, histogram is one of the basic criteria to evaluate the performance of encryption method. A uniform histogram distribution can resist the statistical attack since the information

TABLE 2. Summary of key sensitivity analysis.

Proposed method	Correct key	Modified key	Figure of modified key
Parameters of chaotic system	μ	$\mu + 10^{-14}$	Fig.9(d)
Parameters of elliptic curve encryption	p	$p+1$	Fig.9(e)
	a	$a+1$	Fig.9(f)
	b	$b+1$	Fig.9(g)
	L_x	L_x+1	Fig.9(h)
	L_y	L_x+1	Fig.9(i)
	k	$k+1$	Fig.9(j)
Parameter of diffusion step	t	$t+1$	Fig.9(k)

TABLE 3. The results of variance.

Image	Lena		Barbara		Peppers		Baboon		Car	
	Plain	Cipher	Plain	Cipher	Plain	Cipher	Plain	Cipher	Plain	Cipher
Variance	630730	980.8	433040	1013.2	448850	950.9	627520	1008.3	1229000	958.8

of image can be hided completely. The original ''Lena'', ''Barbara'', ''Peppers'', ''Baboon''and ''Car'', and their corresponding histograms of original and cipher images are shown in Fig.10. It can be observed that the histograms of cipher images are totally different from their plain images, and the histograms distribution of cipher images are uniform.

Additionally, the uniformness of the histogram distribution can be measured by the variance. In other words, variance represents the degree of dispersion between histogram and its average values. The variance of image is defined as

$$\mathrm{Var}(Z) = \frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{1}{2}(z(i)-z(j))^2, \tag{24}$$

where $Z = [z_0, z_1, \ldots, z_{255}]$ is vector of the histogram values, $z(i)$ and $z(j)$ are the pixel values of the gray value i and j, respectively. If the variance of the image is small, it means the histogram of the image is uniform. The variances of ''Lena'', ''Barbara'', ''Peppers'', ''Baboon''and ''Car'' with size of are listed in Table 3. From the Table reftable:variance, the variances of cipher images are much less than the plain images. Furthermore, the variances of cipher image ''Lena'' are compared with other related methods, and the results are given in Table 4. The variance of the proposed method is less than other methods, which demonstrates that the proposed method has better ability of resisting the statistical attack effectively.

TABLE 4. The variances of "Lena" (512 × 512) by using different methods.

Ours	Ref. [51]	Ref. [11]	Ref. [52]	Ref. [53]	Ref. [54]
980.8	1154.7	3485.1953	1209.4	1027.593	1510.3

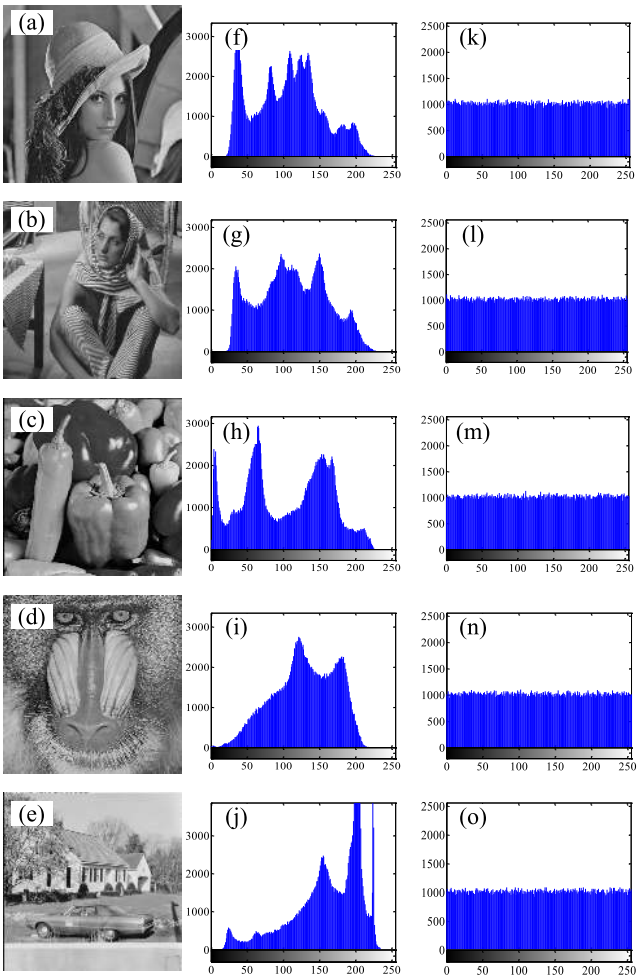

FIGURE 10. The corresponding histograms of the Fig.9(l)-(t).

2) CORRELATION COEFFICIENT ANALYSIS

In the plain image, one pixel is usually highly correlated with adjacent pixels in horizontal, vertical and diagonal directions (usually close to 1). Thus, an effective image encryption method can decrease this correlation [55]. In other words, the correlation of the cipher image is expected to be close to 0.

TABLE 5. Correlation coefficients of plain images and cipher images.

Method	Image	Correlation coefficient in					
		Horizontal		Vertical		Diagonal	
		Plain	Cipher	Plain	Cipher	Plain	Cipher
Ours	Lena	0.9858	0.0019	0.9801	-0.0024	0.9669	0.0011
	Barbara	0.9689	-0.0024	0.8956	0.0031	0.8536	-0.0013
	Peppers	0.9807	-0.0028	0.9752	0.0039	0.9636	-0.0024
	Baboon	0.7251	0.0024	0.8558	0.0011	0.6920	-0.0008
	Car	0.8942	-0.0003	0.8936	0.0014	0.8401	0.0024
Ref. [19]	Lena	0.9325	0.0074	0.9139	-0.0094	0.9469	-0.0054
Ref. [56]	Lena	0.9771	0.0925	0.9631	0.0430	0.9490	0.0533
Ref. [57]	Lena	0.9503	-0.0226	0.9755	0.0041	0.9275	0.0368
Ref. [58]	Peppers	0.9295	0.0048	0.9294	0.0062	0.8771	0.0031
Ref. [59]	Baboon	0.7508	-0.0061	0.8562	0.0130	0.7153	0.0017

TABLE 6. The results of information entropy.

Image	Lena		Barbara		Peppers		Baboon		Car	
	Plain	Cipher	Plain	Cipher	Plain	Cipher	Plain	Cipher	Plain	Cipher
Entropy	7.3871	7.9993	7.4664	7.9993	7.5715	7.9994	7.3579	7.9993	7.2334	7.9993

The correlation coefficient is defined by

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)D(y)}}, \tag{25}$$

$$\mathrm{cov}(x, y) = E\{[x - E(x)][y - E(y)]\}, \tag{26}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{27}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} [x_i - E(x)]^2, \tag{28}$$

where r_{xy} is the correlation coefficient, x and y are two adjacent pixels, N is the total number of pixels, and $E(x)$ and $E(y)$ are the corresponding average values of x_i and y_i. In this experiment, the correlation between adjacent pixels on three directions (horizontal, vertical and diagonal directions) of ''Lena'' and its cipher image are displayed in Fig.11. Additionally, the correlation coefficients of different images and comparison with other methods are given in Table 5. From the results, it can be seen that the values of two adjacent pixels are similar in the plain images. However, the values of two adjacent pixels in the cipher images are very different, and the correlation coefficients of the proposed method are more close to 0 than the other works. It indicates that the proposed method can effectively reduce the correlation of adjacent pixels in cipher image.

3) INFORMATION ENTROPY

Information entropy is intimately bound up with measurement of randomness. According to Shannon's theory, the entropy H(m) of a message source m can be given by

$$\mathrm{H}(m) = \sum_{i=0}^{2^N-1} p(m_i) \log \frac{1}{p(m_i)}, \tag{29}$$

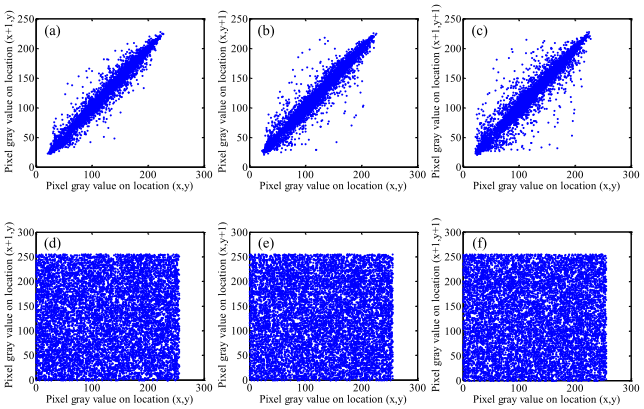

FIGURE 11. Distributions of two adjacent pixels in the original "Lena" image and its cipher image. (a)-(c) the horizontal, vertical, diagonal correlation distributions of original "Lena" image; (d)-(f) the horizontal, vertical, diagonal correlation distributions of cipher "Lena" image.

where $p(m_i)$ is the probability of symbol m_i, N is the number of bits for each symbol m_i. In the ideal case, the information entropy of cipher image with 256 level grayscale is 8 when pixels of the image are distributed randomly [5]. In this experiment, the entropies of ''Lena'', ''Barbara'', ''Peppers'', ''Baboon'' and ''Car'' are listed in Table 6, in which the information entropies of cipher images are very close to the theoretical value 8. Moreover, the entropies of cipher ''Lena'' by different methods are given in Table 7. It is noted that the proposed method obtains the highest entropy compared with other methods, which means the cipher image of proposed method has a random pixel value distribution.

C. PERFORMANCE OF DIFFUSION ANALYSIS

An effective encryption method should have a good diffusion performance [50]. The diffusion means that the pixels of cipher image should depend on the pixels of plain image in

TABLE 7. Information entropies of cipher "Lena" by using different methods.

Ours	Ref. [19]	Ref. [35]	Ref. [60]	Ref. [61]	Ref. [62]
7.9993	7.9992	7.9992	7.9992	7.9991	7.9991

a very complicated way. Differential attack and avalanche effect are commonly used to assess the diffusion performance.

1) DIFFERENTIAL ATTACK ANALYSIS

Differential attack is a type of chosen-plaintext attack [63]. The ability of resisting differential attack is measured by comparing the differences between two cipher images, i.e. when changing one bit of the plain image, the cipher images should be completely different. The sensitivity can be quantitatively evaluated by the number of pixels change rate (NPCR) and unified average changing intensity (UACI). The NPCR represents how many pixels are different between two cipher images by using the same key, it is described as percentage. The UACI represents the average intensity difference between two cipher images by using the same key, i.e. the differences of pixel values of the two cipher images [64].

The NPCR and UACI values are calculated as

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{\mathrm{M} \times \mathrm{N}} \times 100\%, \tag{30}$$

$$\mathrm{UACI} = \frac{1}{\mathrm{M} \times \mathrm{N}} \left[\sum_{i,j} \frac{|E_1(i,j) - E_2(i,j)|}{255} \right] \times 100\%, \tag{31}$$

where M and N are the width and height of the cipher image, $E_1(i,j)$ and $E_2(i,j)$ are the cipher images generated by two plain images with only one-pixel difference, and $D(i,j)$ is difference array, it can be calculated by

$$D(i,j) = \begin{cases} 1, & if\ E_1(i,j) = E_2(i,j) \\ 0, & if\ E_1(i,j) \neq E_2(i,j). \end{cases} \tag{32}$$

Additionally, the expected value of NPCR and UACI are

$$\mathrm{NPCR}_E = \frac{\mathrm{M} \times \mathrm{N} \times [0 \times p_0 + 1 \times p_1]}{\mathrm{M} \times \mathrm{N}} = 1 - \frac{1}{2^n}, \tag{33}$$

and

$$\mathrm{UACI}_E = \frac{1}{\mathrm{M} \times \mathrm{N}} E \left[\sum_{i,j} \frac{|E_1(i,j) - E_2(i,j)|}{2^n - 1} \right]. \tag{34}$$

Since a pixel is composed of eight bits in binary, the expected values of NPCR_E and UACI_E are 99.6094% and 33.4635%, respectively [1]. In this test, the images of "Lena", "Barbara", "Peppers", "Baboon" and "Car" are selected, and the average values of NPCR and UACI with only one bit difference in plain image are given in Table 8. Fig.12 shows the distribution of NPCR and UACI values based on image "Lena", in which 100 pixels with different locations are selected randomly for the test. In addition, 25 pixels are selected in "Baboon" (512 × 512), and the

TABLE 8. The NPCR and UACI of different images.

Image	Lena	Baboon	Barbara	Peppers	Car
NPCR(%)	99.6113	99.6112	99.5796	99.6109	99.6292
UACI(%)	33.4682	33.4919	33.4296	33.4836	33.5039

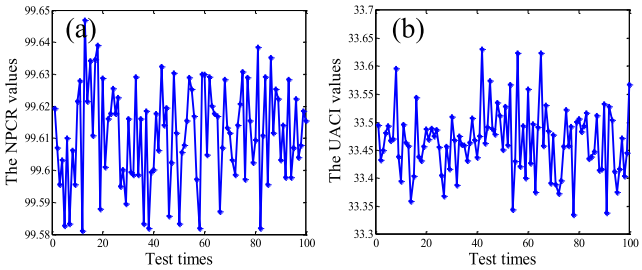

FIGURE 12. The results of (a) NPCR for "Lena"; (b) UACI for "Lena".

corresponding results of NPCR and UACI is given in Table 9. The comparisons of NPCR and UACI values based on the image "Lena" are listed in Table 10. It is observed that the average values of the NPCR and UACI are very close to the expected values no matter where the tested pixel is selected. What's more, the proposed method has lager NPCR and UACI compared with other methods, which shows better robustness in resisting the differential attack.

2) AVALANCHE EFFECT ANALYSIS

It is learned that a tiny change in keys or plain image may cause significant change in the cipher image. This property is known as avalanche effect [65], which can be described by

$$\mathrm{Avalanche} = \frac{\text{Number of changed bits}}{\text{Total of bits}} \times 100\%. \tag{35}$$

The standard of avalanche effect is that if one bit of the plain image is modified, the rate of changing bits in cipher image is not less than 50% [66]. Additionally, the mean square error (MSE) is the squared error accumulated between two images, it can be used for measuring the avalanche effects [65]. MSE can be given by

$$\mathrm{MSE} = \frac{1}{\mathrm{M} \times \mathrm{N}} \sum_{i=0}^{\mathrm{N}-1} \sum_{j=0}^{\mathrm{M}-1} |\mathrm{E}_1(i,j) - \mathrm{E}_2(i,j)|^2, \tag{36}$$

where $\mathrm{M} \times \mathrm{N}$ is the image size, and E_1 and E_2 are two cipher images whose plain images have only one bit difference. Generally, when MSE $\geq$ 30 dB, the differences between the two cipher images is obvious [67]. In this test, the modified bit should be selected from both the plain image and keys. Table 11 shows the results of avalanche effect and MSE by changing one bit in each plain image and key. It is clear that the values of avalanche and MSE of proposed method are larger than the standard no matter by changing the bit of plain image or keys, which proves that the proposed method has a good avalanche effect.

TABLE 9. Results of NPCR and UACI at different locations in "Baboon" image.

Location	(1,1)	(1,128)	(1,256)	(1,384)	(1,512)
Pixel value change	145 → 144	199→ 198	112→ 111	95→ 94	177→ 173
NPCR(%)	99.6010	99.6223	99.6307	99.6132	99.6109
UACI(%)	33.4841	33.5319	33.5287	33.5666	33.5079
Location	(128,1)	(128,128)	(128,256)	(128,384)	(128,512)
Pixel value change	60 → 59	145 → 144	136 → 135	80 → 79	168 → 167
NPCR(%)	99.6185	99.6353	99.6124	99.6170	99.6109
UACI(%)	33.4066	33.4033	33.3996	33.5538	33.4205
Location	(256,1)	(256,128)	(256,256)	(256,384)	(256,512)
Pixel value change	161 → 160	17 → 16	190 → 180	66 → 65	87 → 86
NPCR(%)	99.5956	99.5926	99.6063	99.6132	99.6147
UACI(%)	33.4620	33.3883	33.4705	33.4827	33.5634
Location	(384,1)	(384,128)	(384,256)	(384,384)	(384,512)
Pixel value change	184 → 183	162 → 161	138 → 137	77 → 76	128 → 127
NPCR(%)	99.6072	99.5819	99.6056	99.6017	99.6246
UACI(%)	33.5832	33.4487	33.5728	33.4617	33.4920
Location	(512,1)	(512,128)	(512,256)	(512,384)	(512,512)
Pixel value change	10 → 9	15 → 14	5 → 4	16 → 15	4 → 3
NPCR(%)	99.5972	99.6094	99.6195	99.6109	99.6262
UACI(%)	33.4912	33.3822	33.5885	33.4752	33.5777

TABLE 10. NRCR and UACI values of "Lena" by different encryption methods.

Method	Ours	Ref. [62]	Ref. [68]	Ref. [69]	Ref. [70]
NPCR(%)	99.6113	99.61	99.59	99.60	99.6094
UACI(%)	33.4682	33.32	33.41	33.44	33.4635

TABLE 11. The avalanche and MSE values of different plain images.

Image	One bit change in image		One bit change in key	
	Avalanche (%)	MSE(dB)	Avalanche (%)	MSE(dB)
Lena	50.0334	40.3882	50.0226	40.3910
Barbara	50.0334	40.4003	50.0015	40.3902
Peppers	50.0186	40.3972	50.0267	40.3084
Baboon	50.0411	40.3986	50.0381	40.3850
Car	50.0533	40.3969	50.0267	40.3084

D. SCRAMBLING PERFORMANCE ANALYSIS

The purpose of image scrambling is to prevent the attacker from recognizing the information of the image. If the scrambled image completely fails to recognize its plain image, it indicates that the scrambling method is effective. Based on the scrambling degree evaluation method [71], an 512 × 512 all-white image with 50 × 50 black block is scrambled by using the proposed crossover permutation. The scrambling result is shown in Fig.13, in which the pixels of the black block are dispersed all over the image after crossover permutation.

Besides, another measurement for scrambling degree based on the signal noise ratio (SNR) is presented in [72]. According to the block size R and number of blocks T, the plain image $\mathbf{I}$ and scrambled image $\bar{\mathbf{I}}$ are processed by the optimal block processing and then the SNR of each block is calculated. The degree of scrambling is described by

$$SNR_i = \frac{\sum_{x=0}^{R-1}\sum_{y=0}^{R-1}\mathbf{I}^2(x,y)}{\sum_{x=0}^{R-1}\sum_{y=0}^{R-1}(\mathbf{I}-\bar{\mathbf{I}})^2(x,y)}, \tag{37}$$

$$SNR_{\text{aver}} = \sum_{i=1}^{T}\frac{SNR_i}{T}, \tag{38}$$

$$\eta = \frac{1}{SNR_{aver}}, \tag{39}$$

where $SNR_i (i \in [1, T])$ is the SNR values of each block of $\mathbf{I}$ and $\bar{\mathbf{I}}$, SNR_{aver} is the average SNR values, and η is scrambling degree. In this experiment, the images of "Lena", "Barbara", "Peppers", "Baboon" and "Car" with the size of 512 × 512 are selected for the test, where the block size is R = 8, and the number of blocks is T = 64. Table 12 shows the scrambling degree based on different plain images. From the results, it can be concluded that the scrambling degree of

TABLE 12. The scrambling degree of different plain images.

Image	Lena	Barbara	Peppers	Baboon	Car
Scrambling degree	0.3229	0.3727	0.3735	0.3578	0.3728

TABLE 13. Entropies and correlation coefficients of all black and all white images.

Image		Entropy	Correlation coefficient		
			Horizontal	Vertical	Diagonal
All black	Plain	0	-	-	-
	Cipher	7.9993	0.0023	-0.0075	0.0059
All white	Plain	0	-	-	-
	Cipher	7.9994	-0.0024	-0.0046	0.0019

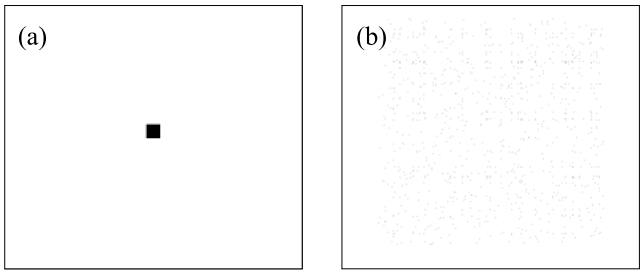

FIGURE 13. Scrambling results. (a) original image; (b) scrambled image.

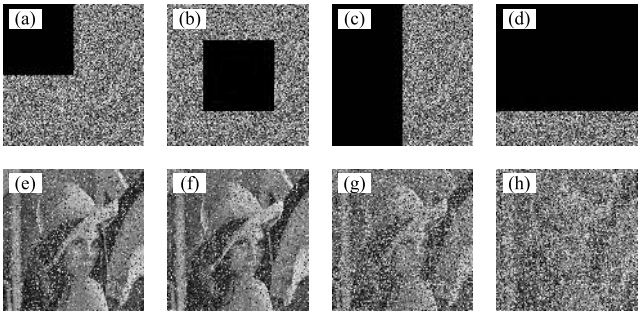

FIGURE 14. The decryption images under occlusion attacks. (a)-(b) the cipher images with 25% occlusion in upper left and middle portions; (c)-(d) the cipher images with 50% and 75% occlusion in the vertical and horizontal; (e)-(h) the corresponding decrypted images of (a)-(d).

the proposed method is basically the same as that of human vision.

E. OCCLUSION AND NOISE ATTACK ANALYSIS

The cipher image may be cropped or jammed by noise during the process of transmission, which may lead to the loss of essential information. Therefore, the ability of resisting cropping and noise attacks should be taken into account [73]. That is, whether the damaged cipher image can be successfully decrypted is used to evaluate the ability of resisting cropping and noise attacks.

In this test, the cropping attack is first tested, in which the cropped part of cipher image is set to ''0'' and then the incomplete image is decrypted. The cipher ''Lena'' image with different cropped part are shown in Fig.14. It can be observed that even if the cipher image loses large amounts of data in different portions or directions, the recovered images can still be recognized. It demonstrates that the proposed method can resist the occlusion attack effectively.

Moreover, the ability of defending the noise attacks is measured by adding different types of noise. In this test, the salt and pepper noise are added in cipher image of ''Lena'' with the density of 10%, 20% and 30%, which are given in Fig.15. The Gaussian noise influences the cipher image with the intensity of 0.0003, 0.0005 and 0.0007 are shown in Fig.16. From the Fig.15 and Fig.16, it is concluded that the proposed method has strong robustness to defend the noise attacks. It is demonstrates the proposed method can still succeeds in recovering the image when the cipher image subjects to different degrees of noise attacks.

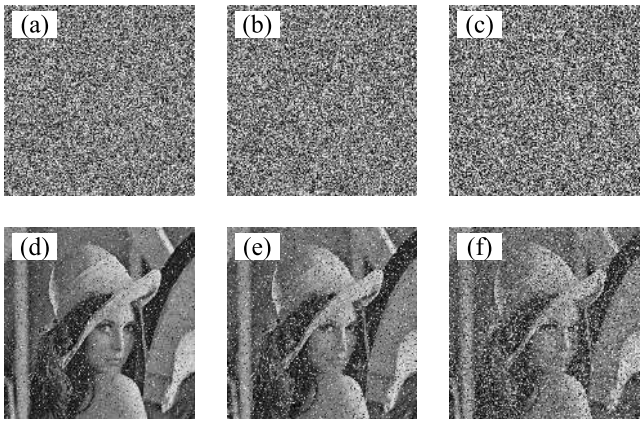

FIGURE 15. (a)-(c) cipher images under salt and pepper noise with the density of 10%, 20%, and 30%; (d)-(f) the corresponding decrypted images of (a)-(c).

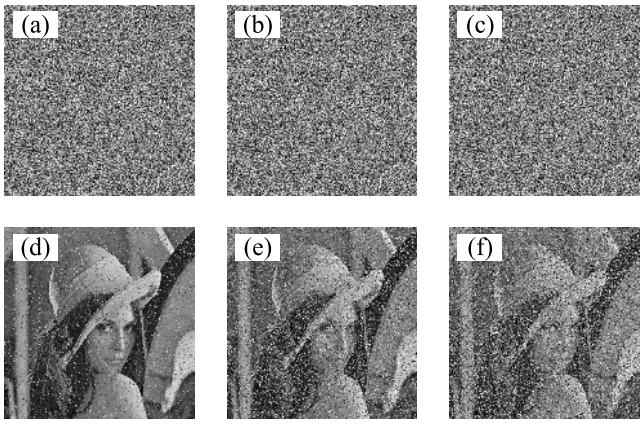

FIGURE 16. (a)-(c) cipher images under Gaussian noise with the degree of Mean=0, Variance=0.0003; Mean=0, Variance=0.0005, and Mean=0, Variance=0.0007; (d)-(f) the corresponding decrypted images of (a)-(c).

F. KNOWN-PLAINTEXT ATTACK AND CHOSEN-PLAINTEXT ATTACK ANALYSIS

Traditional cryptanalysis attacks include: ciphertext-only attack, known-plaintext attack, chosen-plaintext attack, and chosen-ciphertext attack. In these four attacks, chosen-plaintext attack is the most powerful attack [74]. Therefore, it is assumed that if an image encryption method can resist the chosen-plaintext attack, it also can resist the other three attacks [10], [75]–[77].

In the proposed method, the initial values of LTM, TSM and chaos game are generated by SHA-512 hash based on the plain image, which is an important composition in permutation and diffusion process. In other words, the cipher image strongly depends on the plain image, which can withstand the known-plaintext attack and chosen-plaintext attack.

Generally, the attacker can encrypt a special image and try to find the secret key based on the chosen-plaintext attack [1].

TABLE 14. Processing time of the proposed method.

Process	Crossover permutation	EC-ElGamal encryption	Diffusion	Others	Total
Time [unit: sec]	1.19178	1.812777	0.202427	1.526906	4.73389
Percentage	25%	39%	46%	32%	100%

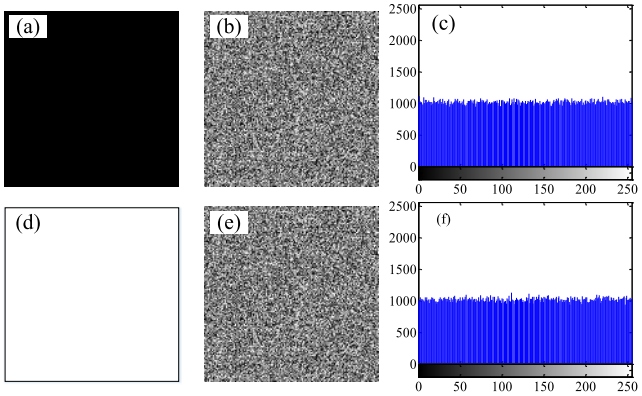

FIGURE 17. (a) all black image; (b) cipher image of (a); (c) the histogram of (b); (d) all white image; (e) cipher image of (d); (f) the histogram of (e).

In this test, two special images are selected in this test, which are all black and all white image with size of 512 × 512. Then, the two images are encrypted and their histograms of cipher images are obtained. The results are shown in Fig.17. Furthermore, the corresponding entropies and correlation coefficients are listed in Table 13. From the results, it can be seen that the histograms of cipher images are uniform, the entropies are close to 8, and the correlation coefficients of the cipher images come close to 0, which means any useful information cannot be obtained in the cipher images. It is indicated that the cryptosystem is suitable for special images, and the attacker cannot decrypt other cipher images by using the same keys. Therefore, the proposed method can resist the known-plaintext attack and chosen-plaintext attack.

G. TIME COMPLEXITY ANALYSIS

A good encryption method not only requires high security performance but also demand fast speed [63]. In this test, the experimental environment is MATLAB R2014a with Intel(R) HD Graphics 630, 3.90GHz Core processor, and 4.0G RAM. The 512 × 512 "Lena" image is encrypted by the proposed method, and the total time consuming and the percentage of each operation are listed in Table 14. From the Table 14, the crossover permutation, EC-ElGamal encryption and diffusion take 25%, 39% and 4% of the total encryption, respectively. Other operations including key generation and the iteration of chaotic systems etc. consume 32%.

Furthermore, the time comparisons of different size images with other related works are listed in Table 15, in which the approaches of [78]–[82] are symmetric encryption, and the approach of [83] is asymmetric encryption method based on elliptic curve. From the Table 15, it can be seen that the execution time of the proposed method is slightly slower than [78]–[80], but it is faster than [81]–[83]. Therefore, the proposed method can achieve a faster encryption speed and secure system performance. In addition, the time consumption of proposed method may be further improved by using high performance devices or parallel computing.

TABLE 15. Time consumption comparisons with other methods [unit: sec].

Image size	128×128	256×256	512×512
Our	0.351779	1.170844	4.73389
Ref. [78]	0.2934	1.4483	-
Ref. [79]	0.06	0.22	0.85
Ref. [80]	0.379602	0.498021	0.938217
Ref. [81]	3.254312	5.556790	8.974393
Ref. [82]	2.17	7.73	31.59
Ref. [83]	-	1.2615	-

V. CONCLUSIONS

In this study, a novel image encryption method based on elliptic curve ElGamal and chaotic theory is proposed. Specifically, the SHA-512 hash is used to generate the initial values of the LTM, TSM and chaos game which reduces the strong correlations between adjacent pixels in plain image as well as resists the known-plaintext attack and chosen-plaintext attack. Then, the proposed scrambled method is used to permutate the plain-image, which is then embedded into elliptic curve to be further encrypted by EC-ElGamal cryptosystem. Moreover, the diffusion based on chaos game and DNA code is executed to get the final cipher, which can improve the randomness of the pixel distribution in advance. The comprehensive performance analysis demonstrates that the proposed method has high security and good efficiency. In the future work, we will focus on the optimization of time consumption, which aims to better satisfy the requirement of real-time communications.

REFERENCES

[1] Y. Luo, L. Cao, S. Qiu, L. Hui, J. Harkin, and J. Liu, "A chaotic map-control-based and the plain image-related cryptosystem," *Nonlinear Dyn.*, vol. 83, no. 4, pp. 2293–2310, Mar. 2016.
[2] Y. Luo and M. Du, "A self-adapting image encryption algorithm based on spatiotemporal chaos and ergodic matrix," *Chin. Phys. Rev. B*, vol. 22, no. 8, pp. 316–324, 2013.
[3] Y. Luo, M. Du, and J. Liu, "A symmetrical image encryption scheme in wavelet and time domain," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 20, no. 2, pp. 447–460, Feb. 2015.
[4] Y. Luo, R. Zhou, J. Liu, C. Yi, and X. Ding, "A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map," *Nonlinear Dyn.*, vol. 93, no. 3, pp. 1165–1181, Aug. 2018.
[5] Y. Luo, R. Zhou, J. Liu, S. Qiu, and C. Yi, "An efficient and self-adapting colour-image encryption algorithm based on chaos and interactions among multiple layers," *Multimedia Tools Appl.*, vol. 77, no. 20, pp. 26191–26217, Oct. 2018.

[6] G. J. Simmons, "Symmetric and asymmetric encryption," *ACM Comput. Surv.*, vol. 11, no. 4, pp. 305–330, 1979.

[7] L. Huang, S. Cai, X. Xiong, and M. Xiao, "On symmetric color image encryption system with permutation-diffusion simultaneous operation," *Opt. Lasers Eng.*, vol. 115, pp. 7–20, Apr. 2019.

[8] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci.*, vol. 480, no. 1, pp. 403–419, Apr. 2019.

[9] Y. Luo, S. Tang, X. Qin, L. Cao, F. Jiang, and J. Liu, "A double-image encryption scheme based on amplitude-phase encoding and discrete complex random transformation," *IEEE Access*, vol. 6, pp. 77740–77753, 2018.

[10] Y. Luo, R. Zhou, J. Liu, S.-H. Qiu, and Y. Cao, "A novel image encryption scheme based on kepler's third law and random Hadamard transform," *Chin. Phys. B*, vol. 26, no. 12, pp. 146–159, 2017.

[11] C. Zhu and K. Sun, "Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps," *IEEE Access*, vol. 6, pp. 18759–18770, 2018.

[12] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.

[13] N. Koblitz, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography," *Designs, Codes Cryptogr.*, vol. 19, nos. 2–3, pp. 173–193, Mar. 2000.

[14] S. S. Tyagi, M. Rana, N. Aggarwal, and P. Bhadana, "A comparative study of public key cryptosystem based on ECC and RSA," *Int. J. Comput. Sci. Eng.*, vol. 3, no. 5, pp. 1904–1909, May 2011.

[15] C. Li, T. Wu, C. Chen, C. Lee, and C. Chen, "An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system," *Sensors*, vol. 17, no. 7, p. 1482, Jun. 2017.

[16] F. Amounas, "Elliptic curve digital signature algorithm using Boolean permutation based ECC," *Int. J. Inf. Netw. Secur.*, vol. 1, no. 3, pp. 216–222, Jul. 2012.

[17] F. H. Hsiao, "Applying elliptic curve cryptography to a chaotic synchronisation system: Neural-network-based approach," *Int. J. Syst. Sci.*, vol. 48, no. 14, pp. 3044–3059, Aug. 2017.

[18] L. Tawalbeh, M. Mowafi, and W. Aljoby, "Use of elliptic curve cryptography for multimedia encryption," *IET Inf. Secur.*, vol. 7, no. 2, pp. 67–74, 2013.

[19] Z. Liu, T. Xia, and J. Wang, "Image encryption technique based on new two-dimensional fractional-order discrete chaotic map and Menezes-Vanstone elliptic curve cryptosystem," *Chin. Phys. B*, vol. 27, no. 3, pp. 1–16, 2018.

[20] M. Kumar, A. Iqbal, and P. Kumar, "A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie-Hellman cryptography," *Signal Process.*, vol. 125, pp. 187–202, Aug. 2016.

[21] N. Koblitz, *A Course Number Theory Cryptography*. New York, NY, USA: Springer, 1987.

[22] J. Wu, X. Liao, and B. Yang, "Color image encryption based on chaotic systems and elliptic curve ElGamal scheme," *Signal Process.*, vol. 141, pp. 109–124, Dec. 2017.

[23] L. Li, A. A. A. El-Latif, and X. Niu, "Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images," *Signal Process.*, vol. 92, no. 4, pp. 1069–1078, Apr. 2012.

[24] L. D. Singh and K. M. Singh, "Medical image encryption based on improved ElGamal encryption technique," *Optik*, vol. 147, pp. 88–102, Oct. 2017.

[25] Q. Wang, S. Yu, C. Li, J. Lü, X. Fang, C. Guyeux, and J. M. Bahi, "Theoretical design and FPGA-based implementation of higher-dimensional digital chaotic systems," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 63, no. 3, pp. 401–412, May 2015.

[26] J. Lü, S. Yu, H. Leung, and G. Chen, "Experimental verification of multidirectional multiscroll chaotic attractors," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 53, no. 1, pp. 149–165, Jan. 2006.

[27] S. Yu, J. Lü, X. Yu, and G. Chen, "Design and implementation of grid multiwing hyperchaotic lorenz system family via switching control and constructing super-heteroclinic loops," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 59, no. 5, pp. 1015–1028, May 2012.

[28] C. Li, D. Lin, J. Lü, and F. Hao, "Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography," *IEEE MultiMediaMag.*, vol. 25, no. 4, pp. 46–56, Oct./Dec. 2018.

[29] S. Yu, J. Lü, H. Leung, and G. Chen, "N-scroll chaotic attractors from a general jerk circuit," in *Proc. Int. Symp. Circuits Syst.*, vol. 2, May 2005, pp. 1473–1476.

[30] I. Sushko, L. Gardini, and K. Matsuyama, "Coupled chaotic fluctuations in a model of international trade and innovation: Some preliminary results," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 58, pp. 287–302, May 2018.

[31] H. Huang and S. Yang, "Colour image encryption based on logistic mapping and double random-phase encoding," *IET Image Process.*, vol. 11, no. 4, pp. 211–216, Apr. 2017.

[32] X. Huang, "Image encryption algorithm using chaotic Chebyshev generator," *Nonlinear Dyn.*, vol. 67, no. 4, pp. 2411–2417, 2012.

[33] G. Ye and K.-W. Wong, "An efficient chaotic image encryption algorithm based on a generalized Arnold map," *Nonlinear Dyn.*, vol. 69, no. 4, pp. 2079–2087, Sep. 2012.

[34] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dyn.*, vol. 62, no. 3, pp. 615–621, 2010.

[35] X. Wang and H.-L. Zhang, "A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems," *Nonlinear Dyn.*, vol. 83, nos. 1–2, pp. 333–346, 2016.

[36] X. Chai, Z. H. Gan, L. Yang, M.-H. Zhang, and Y.-R. Chen, "A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system," *Chin. Phys. B*, vol. 25, no. 10, pp. 76–88, Aug. 2016.

[37] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A novel chaotic image encryption scheme using DNA sequence operations," *Opt. Lasers Eng.*, vol. 73, pp. 53–61, Oct. 2015.

[38] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, "An image encryption algorithm based on chaotic system and compressive sensing," *Signal Process.*, vol. 148, pp. 124–144, Jul. 2018.

[39] H. J. Jeffrey, "Chaos game representation of gene structure," *Nucleic Acids Res.*, vol. 18, no. 8, pp. 2163–2170, Apr. 1990.

[40] M. Jampour, R. Ebrahimzadeh, M. Yaghoobi, and A. Soleimani-Nezhad, "Towards a fast method for iris identification with fractal and chaos game theory," *Int. J. Pattern Recognit. Artif. Intell.*, vol. 26, no. 4, May 2012, Art. no. 1256011.

[41] B. Sulistyo, B. Rahardjo, D. Mahayana, and C. Machbub, "New methodology of block cipher analysis using chaos game," *J. ICT Res. Appl.*, vol. 5, no. 2, pp. 105–124, 2011.

[42] Y. Zhou, L. Bao, and C. P. Chen, "A new 1D chaotic system for image encryption," *Signal Process.*, vol. 97, no. 11, pp. 172–182, 2014.

[43] W. Liu, K. Sun, Y. He, and M. Yu, "Color image encryption using three-dimensional sine ICMIC modulation map and DNA sequence operations," *Int. J. Bifurcation Chaos*, vol. 27, no. 11, Oct. 2017, Art. no. 1750171.

[44] H. Nematzadeh, R. Enayatifar, H. Motameni, F. G. Guimarães, and V. N. Coelho, "Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices," *Opt. Lasers Eng.*, vol. 110, pp. 24–32, Nov. 2018.

[45] X. Wang and D. Xu, "Image encryption using genetic operators and intertwining logistic map," *Nonlinear Dyn.*, vol. 78, no. 4, pp. 2975–2984, Dec. 2014.

[46] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.

[47] X. Wang and C. Liu, "A novel and effective image encryption algorithm based on chaos and DNA encoding," *Multimedia Tools Appl.*, vol. 76, no. 5, pp. 6229–6245, Mar. 2017.

[48] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.

[49] D. Lambic, "Cryptanalyzing a novel pseudorandom number generator based on pseudorandomly enhanced logistic map," *Nonlinear Dyn.*, vol. 89, no. 3, pp. 2255–2257, Aug. 2017.

[50] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[51] M. Dridi, M. A. Hajjaji, B. Bouallegue, and A. Mtibaa, "Cryptography of medical images based on a combination between chaotic and neural network," *IET Image Process.*, vol. 10, no. 11, pp. 830–839, 2016.

[52] X. Chai, K. Yang, and Z. Gan, "A new chaos-based image encryption algorithm with dynamic key selection mechanisms," *Multimedia Tools Appl.*, vol. 76, no. 7, pp. 9907–9927, Apr. 2017.

[53] J. Wu, X. Liao, and Y. Bo, "Image encryption using 2D Hénon-sine map and DNA approach," *Signal Process.*, vol. 153, pp. 11–23, Dec. 2018.

[54] X. Chai, "An image encryption algorithm based on bit level Brownian motion and new chaotic systems," *Multimedia Tools Appl.*, vol. 76, no. 1, pp. 1159–1175, 2017.

[55] M. J. Rostami, A. Shahba, S. Saryazdi, and H. Nezamabadi-Pour, "A novel parallel image encryption with chaotic windows based on logistic map," *Comput. Electr. Eng.*, vol. 62, pp. 384–400, Aug. 2017.
[56] G.-D. Ye, X.-L. Huang, L. Y. Zhang, and Z.-X. Wang, "A self-cited pixel summation based image encryption algorithm," *Chin. Phys. B*, vol. 26, no. 1, pp. 131–138, 2017.
[57] X. Lu, G. Xu, L. Zhi, and L. Jian, "A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion," *Opt. Lasers Eng.*, vol. 91, pp. 41–52, Apr. 2017.
[58] D.-D. Liu, W. Zhang, H. Yu, and Z.-L. Zhu, "An image encryption scheme using self-adaptive selective permutation and inter-intra-block feedback diffusion," *Signal Process.*, vol. 151, pp. 130–143, Oct. 2018.
[59] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, "An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations," *Signal Process., Image Commun.*, vol. 52, pp. 6–19, Mar. 2017.
[60] D. S. Laiphrakpam and M. S. Khumanthem, "A robust image encryption scheme based on chaotic system and elliptic curve over finite field," *Multimedia Tools Appl.*, vol. 77, no. 7, pp. 8629–8652, Apr. 2018.
[61] W. K. Lee, C. W. Phan, W. S. Yap, and B. M. Goi, "Spring: A novel parallel chaos-based image encryption scheme," *Nonlinear Dyn.*, vol. 92, no. 2, pp. 575–593, Apr. 2018.
[62] S. Sun, "Chaotic image encryption scheme using two-by-two deoxyribonucleic acid complementary rules," *Opt. Eng.*, vol. 56, no. 11, 2017, Art. no. 116117.
[63] X. Wang, X. Zhu, X. Wu, and Y. Zhang, "Image encryption algorithm based on multiple mixed hash functions and cyclic shift," *Opt. Lasers Eng.*, vol. 107, no. 1, pp. 370–379, Aug. 2017.
[64] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, and R. M. Lopez-Gutiérrez, "A RGB image encryption algorithm based on total plain image characteristics and chaos," *Signal Process.*, vol. 109, pp. 119–131, Apr. 2015.
[65] A. Jawad and A. Fawad, "Efficiency analysis and security evaluation of image encryption schemes," *Int. J. Video Image Process. Netw. Secur.*, vol. 12, no. 4, pp. 18–31, 2012.
[66] X.-J. Tong, M. Zhang, Z. Wang, and J. Ma, "A joint color image encryption and compression scheme based on hyper-chaotic system," *Nonlinear Dyn.*, vol. 84, no. 4, pp. 2333–2356, Dec. 2016.
[67] L. Zhu, W. Li, L. Liao, and H. Li, "A novel image scrambling algorithm for digital watermarking based on chaotic sequences," *Int. J. Comput. Sci. Netw. Secur.*, vol. 6, no. 8B, pp. 125–130, Aug. 2006.
[68] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using dna sequence operations," *Opt. Lasers Eng.*, vol. 88, pp. 197–213, Jan. 2017.
[69] G. Ye, "A block image encryption algorithm based on wave transmission and chaotic systems," *Nonlinear Dyn.*, vol. 75, no. 3, pp. 417–427, Feb. 2014.
[70] Z. Yong, "The unified image encryption algorithm based on chaos and cubic S-Box," *Inf. Sci.*, vol. 450, pp. 361–377, Jun. 2018.
[71] S. S. Maniccam and N. G. Bourbakis, "Image and video encryption using SCAN patterns," *Pattern Recognit.*, vol. 37, no. 4, pp. 725–737, Apr. 2004.
[72] Z. Li, Y. Chen, and S. Zhang, "Digital image scrambling degree evaluation method based on SNR," *J. Xiamen Univ.*, vol. 45, no. 4, pp. 484–487, 2006.
[73] Y. Zheng and J. Jin, "A novel image encryption scheme based on Hénon map and compound spatiotemporal chaos," *Multimedia Tools Appl.*, vol. 74, no. 18, pp. 7803–7820, Sep. 2015.
[74] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Process.*, vol. 92, no. 4, pp. 1101–1108, Apr. 2012.
[75] C. Zhu, G. Wang, and K. Sun, "Improved cryptanalysis and enhancements of an image encryption scheme using combined 1D chaotic maps," *Entropy*, vol. 20, no. 11, p. 843, Nov. 2018.
[76] C. Li, D. Lin, B. Feng, J. Lü, and F. Hao, "Cryptanalysis of a chaotic image encryption algorithm based on information entropy," *IEEE Access*, vol. 6, pp. 75834–75842, 2018.
[77] C. Zhu, G. Wang, and K. Sun, "Cryptanalysis and improvement on an image encryption algorithm design using a novel chaos based s-box," *Symmetry*, vol. 10, no. 9, p. 399, 2018.
[78] S. Zhu and C. Zhu, "Image encryption algorithm with an avalanche effect based on a six-dimensional discrete chaotic system," *Multimedia Tools Appl.*, vol. 77, no. 21, pp. 29119–29142, Nov. 2018.
[79] S. Zhu, C. Zhu, and W. Wang, "A new image encryption algorithm based on chaos and secure hash SHA-256," *Entropy*, vol. 20, no. 9, p. 716, Sep. 2018.
[80] S. Zhu, C. Zhu, and W. Wang, "A novel image compression-encryption scheme based on chaos and compression sensing," *IEEE Access*, vol. 6, pp. 67095–67107, 2018.
[81] J. Chen, Z. Yu, Q. Lin, F. Chong, and L. Xu, "Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression," *Opt. Laser Technol.*, vol. 99, pp. 238–248, Feb. 2017.
[82] A. U. Rehman, X. Liao, A. Kulsoom, and S. A. Abbas, "Selective encryption for gray images based on chaos and DNA complementary rules," *Multimedia Tools Appl.*, vol. 74, no. 13, pp. 4655–4677, Jul. 2015.
[83] Z. E. Dawahdeh, S. N. Yaakob, and R. R. B. Othman, "A new image encryption technique combining elliptic curve cryptosystem with hill cipher," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 30, no. 3, pp. 349–355, Jul. 2018.

YULING LUO received the Ph.D. degree in information and communication engineering from the South China University of Technology, Guangzhou, China. She is currently an Associate Professor with the School of Electronic Engineering, Guangxi Normal University, Guilin, China. Her research interest includes information security, image processing, chaos theory, and embedded system implementations.

XUE OUYANG received the B.E. degree from the Institute of Information Technology, Guilin University of Electronic Technology, China, in 2017. She is currently pursuing the master's degree with the School of Electronic Engineering, Guangxi Normal University. Her research interests include information security, and image encryption and its application.

JUNXIU LIU, photograph and biography not available at the time of publication.

LVCHEN CAO received the B.Eng. degree in electronic and information engineering from the Zhongyuan University of Technology, Zhengzhou, China, in 2013, and the M.S. degree in electronic science and technology from Guangxi Normal University, Guilin, China, in 2016. He is currently pursuing the Ph.D. degree with the Beijing Institute of Technology. He was an Algorithm Engineer with ALi Corporation, Zhuhai, China, from 2016 to 2017. His current research interests include pattern recognition, machine learning, and chaotic cryptography.