Hindawi
Discrete Dynamics in Nature and Society
Volume 2018, Article ID 4585083, 24 pages
https://doi.org/10.1155/2018/4585083

Research Article

Image Encryption Technology Based on Fractional Two-Dimensional Triangle Function Combination Discrete Chaotic Map Coupled with Menezes-Vanstone Elliptic Curve Cryptosystem

Zeyu Liu,[1] **Tiecheng Xia**,[1,2] **and Jinbo Wang**[2]

[1] *Department of Mathematics, Shanghai University, Shanghai 200444, China*
[2] *Science and Technology on Communication Security Laboratory, Chengdu, Sichuan 610041, China*

Correspondence should be addressed to Tiecheng Xia; xiatc@shu.edu.cn

Received 7 December 2017; Revised 10 February 2018; Accepted 22 February 2018; Published 23 April 2018

Academic Editor: Youssef N. Raffoul

A new fractional two-dimensional triangle function combination discrete chaotic map (2D-TFCDM) with the discrete fractional difference is proposed. We observe the bifurcation behaviors and draw the bifurcation diagrams, the largest Lyapunov exponent plot, and the phase portraits of the proposed map, respectively. On the application side, we apply the proposed discrete fractional map into image encryption with the secret keys ciphered by Menezes-Vanstone Elliptic Curve Cryptosystem (MVECC). Finally, the image encryption algorithm is analysed in four main aspects that indicate the proposed algorithm is better than others.

1. Introduction

Nowadays, image encryption plays a significant role with the development of security technology in the areas of network, communication, and cloud service. Multifarious chaos-based image encryption algorithms have been developed up to now, such as in [1–6]; however a few of them have referred to the image encryption algorithm based on fractional discrete chaotic map accompanied with Elliptic Curve Cryptography (ECC).

The theory of the fractional difference has been developed for decades [7–13]. Recently, Wu et al. [14–16] made a contribution to the application of the discrete fractional calculus (DFC) on an arbitrary time scale, and the theories of delta difference equations were utilized to reveal the discrete chaos behavior.

ECC is a widely used technology in data security and communication security; it can achieve the same level of security with smaller key sizes and higher computational efficiency [17]. Many famous public-key algorithms, such as Diffie-Hellman, EIGamal, and Schnorr, can be implemented by means of elliptic curves over finite fields. MVECC is one of the popular elliptic curve public-key cryptosystems [18] and we adopt it in our cryptosystem.

Many encryption methods based on fractional derivatives have been proposed in recent time, like fractional logistic maps [19], fractional-order chaos systems [20], and fractional form of hyperchaotic system [21].

In [22], a new image encryption algorithm based on one-dimensional fractional chaotic time series within fractional-order difference has been proposed; however, the two-dimensional discrete chaotic map has seldom been used in image encryption except [23, 24].

Our main purpose is to introduce a new two-dimensional discrete chaotic map based on fractional-order difference and apply it in image encryption. The rest of this paper is organized as follows. In Section 2, the definitions and the properties of the DFC are introduced. After that, the definitions and operation of ECC are given. Then, the working principle of MVECC is described in the next section. In Section 5, we give the fractional 2D-TFCDM on time scales from the discrete integral expression. The bifurcation diagrams and the phase portraits of the map are presented while the difference orders and the coefficients are changing; the largest Lyapunov exponent plots are also displayed. Afterwards, we apply the proposed map into image encryption and show several examples. In Section 7, the performance of the proposed image encryption method is analysed systematically. Finally, we have come to some conclusions.

2. Preliminaries

The definitions of the fractional sum and difference are given as follows. Let $\mathbb{N}_a$ denote the isolated time scale and $\mathbb{N}_a = \{a, a+1, a+2, \ldots\}$ ($a \in \mathbb{R}$ fixed). Within the DFC, the function $f(t)$ is changed as a sequence $f(n)$. The difference operator Δ is defined as $\Delta f(n) = f(n+1) - f(n)$.

Definition 1 (see [25]). Let u: $\mathbb{N}_a \to \mathbb{R}$ and $0 < \nu$ be given. The νth fractional sum is defined by

$$\Delta_a^{-\nu} u(t) := \frac{1}{\Gamma(\nu)} \sum_{s=a}^{t-\nu} (t-s-1)^{\nu-1} u(s), \quad t \in \mathbb{N}_{a+\nu}. \tag{1}$$

Note that a is the starting point; $t^{(\nu)}$ is the falling function defined as

$$t^{(\nu)} = \frac{\Gamma(t+1)}{\Gamma(t+1-\nu)}. \tag{2}$$

Definition 2 (see [26]). For $0 < \nu$, $\nu \notin \mathbb{N}$, and $u(t)$ defined on $\mathbb{N}_a$, the ν-order Caputo fractional difference is defined by

$$\begin{aligned} {}^{C}\Delta_a^{\nu} u(t) &:= \Delta_a^{-(m-\nu)} \Delta^m u(t) \\ &= \frac{1}{\Gamma(m-\nu)} \sum_{s=a}^{t-(m-\nu)} (t-s-1)^{(m-\nu-1)} \Delta^m u(s), \\ &\qquad t \in \mathbb{N}_{a+m-\nu}, \ m = [\nu] + 1. \end{aligned} \tag{3}$$

Theorem 3 (see [27]). *For the delta fractional difference equation*

$$\begin{aligned} {}^{C}\Delta_a^{\nu} u(t) &= f(t+\nu-1, u(t+\nu-1)), \\ \Delta^k u(a) &= u_k, \quad m = [\nu] + 1, \ k = 0, \ldots, m-1 \end{aligned} \tag{4}$$

the equivalent discrete integral equation is

$$\begin{aligned} x(n) = u_0(t) &+ \frac{1}{\Gamma(\nu)} \sum_{s=a+m-\nu}^{t-\nu} (t-s-1)^{(\nu-1)} \\ &\times f(s+\nu-1, u(s+\nu-1)), \quad t \in \mathbb{N}_{a+m}, \end{aligned} \tag{5}$$

where

$$u_0(t) = \sum_{k=0}^{m-1} \frac{(t-a)^{(k)}}{k!} \Delta^k u(a). \tag{6}$$

The complex difference equation with long-term memory is obtained here. It can reduce to the integer order one with the difference order $\nu = 1$ but the integer one does not hold the discrete memory. From (3) to (5), the domain is shifted from $\mathbb{N}_{a+m-\nu}$ to $\mathbb{N}_{a+m}$ and the function $u(t)$ is preserved to be defined on the isolated time scale $\mathbb{N}_a$ in the fractional sums.

3. Introduction to Elliptic Curve

Definition 4. An elliptic curve (EC) E over a prime field F_p denoted by $E(F_p)$ refers to the set of all points (x, y) that satisfy the equation

$$E : y^2 \equiv x^3 + ax + b \pmod{p}, \tag{7}$$

together with a special point O at infinity, where $a, b \in F_p$, $p \neq 2, 3$ and $4a^3 + 27b^2 \neq 0$ [28, 29].

3.1. Elliptic Curve Operations.

If $P = (x_1, y_1)$, $Q = (x_2, y_2) \in E(F_p)$; then if $x_1 = x_2$ but $y_1 \neq y_2$, $P + Q = O$; that is, $Q = -P = (x_1, -y_1)$ [29].

$$P + Q = \begin{cases} R = (x_3, y_3), & P \neq -Q, \\ O, & P = -Q, \end{cases} \tag{8}$$

where

$$\begin{aligned} x_3 &\equiv (\lambda^2 - 2x_1) \pmod{p}, \\ y_3 &\equiv (\lambda(x_1 - x_3) - y_1) \pmod{p}, \\ \lambda &= \begin{cases} \dfrac{(y_2 - y_1)}{(x_2 - x_1)}, & P \neq Q, \\ \dfrac{3x_1^2 + a}{2y_1}, & P = Q. \end{cases} \end{aligned} \tag{9}$$

The scalar multiplication over $E(F_p)$ is defined by

$$kP = \underbrace{P + P + \cdots + P}_{k \text{ times}}, \tag{10}$$

where k is an integer.

Definition 5. The order of an EC is defined by the number of points that lie on the EC denoted by $\#E$ [29].

Definition 6. Set $P \in E(F_p)$, and then P is called a generator point if $\text{ord}(P) = \#E$ ($\text{ord}(P)$ is the smallest positive integer n that makes $nP = O$) [29].

4. Menezes-Vanstone Elliptic Curve Cryptosystem (MVECC)

MVECC is one of most significant extensions of ECC; the working principle of MVECC is as follows.

If Andy wants to encrypt and send the message M to Bob, they should do the step as mentioned hereunder:

(1) Andy and Bob make an agreement on an elliptic curve $E(F_p)$ and the base point α.

(2) Bob firstly selects a private key k to compute the public key $\gamma = k \cdot \alpha$ ($0 \leqq k < \text{ord}(\alpha)$).

(3) If Andy wants to send a message $M = (x_1, x_2) \in Z_p^* \times Z_p^*$ to Bob, he firstly chooses a random private key d ($0 \leqq d < \text{ord}(\alpha)$) and then computes his public key $\beta = d \cdot \alpha$. On the other hand, Andy calculates the secret key (c_1, c_2) by

$$(c_1, c_2) = d \cdot \gamma = d \cdot k \cdot \alpha = k \cdot \beta. \tag{11}$$

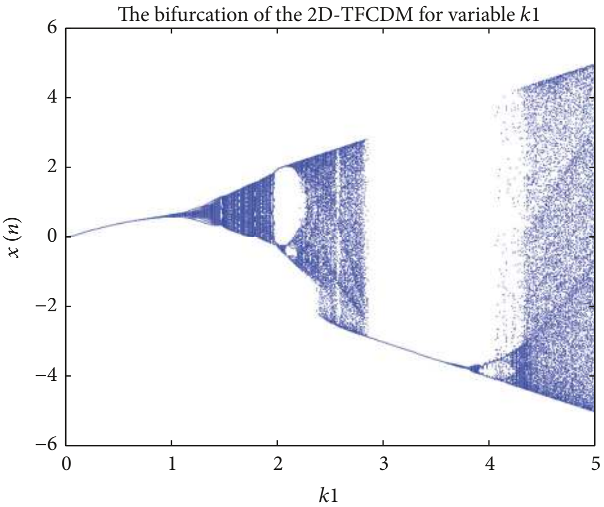


Figure 1: The bifurcation diagram of the 2D-TFCDM of variable k_1 for $\nu = 1$.

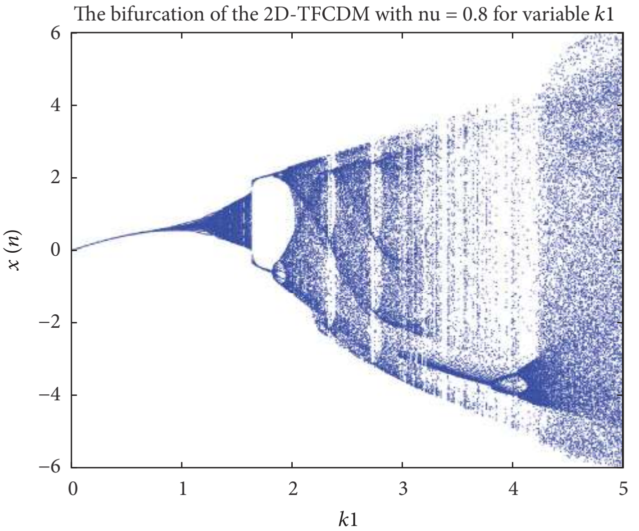


Figure 2: The bifurcation diagram of the fractional 2D-TFCDM of variable k_1 for $\nu = 0.8$.

He should compute the ciphered message afterwards by

$$y_1 = x_1 * c_1 \mod p, \qquad y_2 = x_2 * c_2 \mod p. \tag{12}$$

(4) Then the ciphertext $\{\gamma, (y_1, y_2)\}$ is sent to Bob. When Bob wants to get the plaintext (x_1, x_2), firstly, he computes the secret key $(c_1, c_2) = k \cdot \beta = k \cdot d \cdot \alpha$, and then he computes $M = (x_1, x_2)$ by

$$x_1 = y_1 * c_1^{-1} \mod p, \qquad x_2 = y_2 * c_2^{-1} \mod p, \tag{13}$$

to get the plaintext [18].

Any adversary that only has β and γ without the private keys d and k very difficultly breaks the MVECC to get the plaintext M. What is more, if $\#E$ have only one big prime divisor, the EC is called a safe EC [29]; then, the MVECC can become an more efficient and secure cryptosystem.

5. Fractional 2D-TFCDM

From [14–16], we notice the application of the DFC in fractional generalizations of the discrete chaotic maps. Recently [30], the following 2D-TFCDM was proposed:

$$x_{n+1} = k_1 \cos(x_n + y_n), \quad k_1 = 8, \qquad y_{n+1} = k_2 \sin(x_n - y_n), \quad k_2 = 0.5. \tag{14}$$

Now, consider the fractional generalization of $x(n)$; the map was also studied in [31]:

$$^{C}\Delta_{\alpha}^{\nu} x(t) = k_1 \cos(x(t+\nu) + y(t+\nu)) - x(t+\nu), \quad 0 < \nu < 1, \ t \in N_{a+1-\nu}, \tag{15}$$
$$y_{n+1} = k_2 \sin(x_n - y_n), \quad k_2 = 0.5.$$

From Theorem 3, we have the following equivalent discrete numerical formula for the variable k_1: ($k_2 = 0.5$) with $0 < \nu < 1$:

$$x(n) = x(0) + \frac{1}{\Gamma(\nu)} \sum_{j=1}^{n} \frac{\Gamma(n-j+\nu)}{\Gamma(n-j+1)} \cdot [k_1 \cos(x(j-1) + y(j-1)) - x(j-1)], \qquad y(n) = k_2 \sin(x(n-1) - y(n-1)), \quad k_2 = 0.5. \tag{16}$$

Let $\nu = 1$, $x(0) = 0.19$, $y(0) = 0.06$, $n = 200$, and k_1 be fixed. In what follows, Figure 1 is the bifurcation diagram where the step size of k_1 is 0.002. Figure 2 is the same bifurcation diagram except for $\nu = 0.8$.

In Figures 3 and 4, the largest Lyapunov exponent plots are drawn by use of the Jacobian matrix algorithm proposed in [32]. The largest Lyapunov exponent LE is positive somewhere; it is corresponding to the chaotic intervals in Figures 1 and 2.

By choosing 101 different initial values we can plot $y(n)$ versus $x(n)$ in one figure. The phase portraits of the integer map are derived from Figure 5. The cases of $\nu = 0.8$ and $\nu = 0.6$ are plotted in Figures 6 and 7, respectively.

6. Applications

The fractionalized chaotic map can be applied in image encryption. Exploit (16) into an algorithm, and set the initial values x_0, y_0, the order ν, and the coefficients k_1, k_2 of chaotic system as keys. In this paper, we propose the encryption algorithm and divide it into 3 parts.

6.1. Generation of New Keys Based on Elliptic Curve in a Finite Field. Setting $a = 1$, $b = 6$, and $p = 9996887$ in (7), we can get $E(F_{9996887})$. Since $\#E = 10000721$ is a prime number, according to [29], $E(F_{9996887})$ is a safe EC. Let $\alpha = (2, 4)$, randomly select $d = 9134417$, $k = 1269960 \in [1, \#E]$; then $\beta = d\alpha = (6020909, 7282175)$, $\gamma = k\alpha = (7495358, 7052635)$, and $(c_1, c_2) = k\beta = (3049362, 3915118) = d\gamma$. The initial key $\nu = 0.6026331$, $x_0 = 4.107532$, $\nu_{01} = \nu \times 10^7 = 6026331$, and $x_{01} = x_0 \times 10^6 = 4107532$.

Calculate

$$\begin{aligned} \nu'_{01} &= c_1 * \nu_{01} \mod p = 3049362 \cdot 6026331 \mod 9996887 = 7123456 \mod 9996887, \\ x'_{01} &= c_2 \cdot x_{01} \mod p = 3915118 \cdot 4107532 \mod 9996887 = 190000 \mod 9996887. \end{aligned} \tag{17}$$

Then, the ciphertext is $((7495358, 7052635), 7123456, 190000)$, the enciphered key is $\nu' = \nu'_{01}/10^7 = 0.7123456$, and $x'_0 = x'_{01}/10^6 = 0.19$.

Make $y_0 = 3.650991$, $k_1 = 0.897029$, and $k_2 = 0.434264$, and compute $y_{01} = y_0 \times 10^6$, $k_{01} = k_1 \times 10^6$, and $k_{02} = k_2 \times 10^6$; then

$$\begin{aligned} y'_{01} &= c_1 \cdot y_{01} \mod p = 3049362 \cdot 3650991 \mod 9996887 = 60000 \mod 9996887, \\ k'_{01} &= c_2 \cdot k_{01} \mod p = 3915118 \cdot 897029 \mod 9996887 = 8000000 \mod 9996887, \\ k'_{02} &= c_1 \cdot k_{02} \mod p = 3049362 \cdot 434264 \mod 9996887 = 500000 \mod 9996887. \end{aligned} \tag{18}$$

Set $y'_0 = y'_{01}/10^6 = 0.06$, $k'_1 = k'_{01}/10^6 = 8$, $k'_2 = k'_{02}/10^6 = 0.5$, and then x'_0, y'_0, ν', k'_1, k'_2 are taken as the keys of Section 6.2.

6.2. Permutation Procedure Based on Fractional 2D-TFCDM. Taking advantage of (16) with the initial values x'_0, y'_0, ν', k'_1, and k'_2 generated in the last section, we can encrypt the image. The next step of encryption is permutation; it is subdivided into 4 steps:

(1) Set x'_0 as $x(1)$; iterate (16) for $MN-1$ times to generate the one-dimensional real number chaotic sequence $x(i)$, $i = 1, 2, \ldots, MN$; here M and N denote the length and width of the original image V, respectively.

(2) Reorder $x(k)$ by the bubble sort and get $x'(k)$, and record the change of the subscript of $x(k)$ as $z(k)$.

(3) Change $M \times N$ original image V into $1 \times MN$ sequence $v(k)$, and rearrange $v(k)$ according to $z(k)$ to get the new sequence $v'(k)$.

(4) Reshape $v'(k)$ into $M \times N$ image as V'; V' is the permutated image we needed.

Reversing the above 4 steps, we can remove the effect of permutation to get the original image.

6.3. Encryption Method Based on Fractional 2D-TFCDM. (1) In Section 6.2 we get the chaotic sequence $x(i)$ and image V'. Reshape $M \times N$ image V' into $1 \times MN$ sequence $u(i)$; that is $i = N(m-1) + n$, $(m = 1, 2, \ldots, M, n = 1, 2, \ldots, N)$. Another $M \times N$ image is used as a key image (K-image). Change the K-image also into $1 \times MN$ sequence $w(i)$.

(2) Set $i = 0$.

(3) Round $x(i) \times 10^8$ as $x_1(i)$, do modulus operation to $x_1(i)$ in (19), and get $x_2(i)$:

$$x_2(i) = \operatorname{mod}(x_1(i), 256). \tag{19}$$

(4) Do the following operation and get $u'(i)$:

$$u'(i) = u(i) \oplus \operatorname{mod}(w(i) + x_2(i), 256), \tag{20}$$

where $\oplus$ refers to the Xor operation, and $u'(i)$ is the encrypted pixel value.

The inverse form of (20) is

$$u(i) = u'(i) \oplus \operatorname{mod}(w(i) + x_2(i), 256). \tag{21}$$

(5) Compute the iteration times $k(i)$ according to

$$k(i) = 1 + \operatorname{mod}(u'(i), 256). \tag{22}$$

Then, iterate (16) for $k(i)$ times to get $x(i+1)$, circle from step (3) to step (5), until getting $x(MN)$.

(6) Change $u'(i)$ into $M \times N$ image as V'', which is the finally encrypted figure we need.

The decryption procedure is including 2 parts:

(1) Do all steps in encryption process except (20) which is replaced by (21).

(2) Reverse the procedure in Section 6.2. Then the decryption procedure is done.

Figure 8 shows the encryption process described in Sections 6.2 and 6.3 in a flow chart, and Figure 9 illustrates the iteration procedure of S box.

The original, encrypted, and decrypted images are shown in Figures 10–18. The proposed algorithm can encrypt any rectangular image.

The adopted cryptosystem in Section 6.1 is asymmetric; however, the ones in Sections 6.2 and 6.3 are symmetric.

7. Analysis of Results in Applications

7.1. Key Space. In the proposed algorithm, the initial values x_0, y_0, the order ν, and the coefficients k_1, k_2 are taken as the

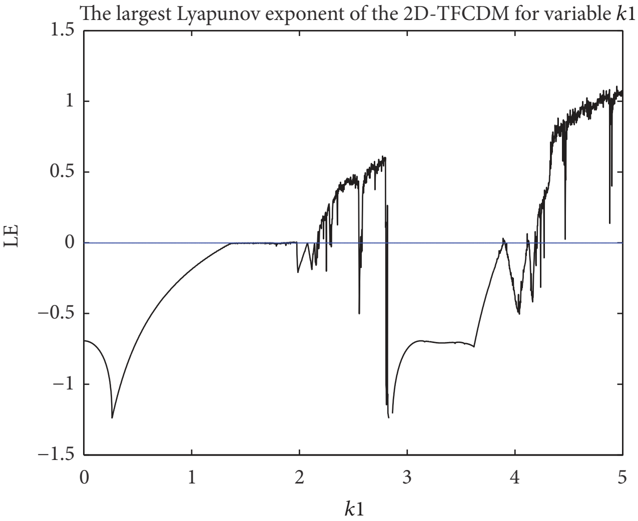


FIGURE 3: The largest Lyapunov exponent of the 2D-TFCDM of the variable k_1.

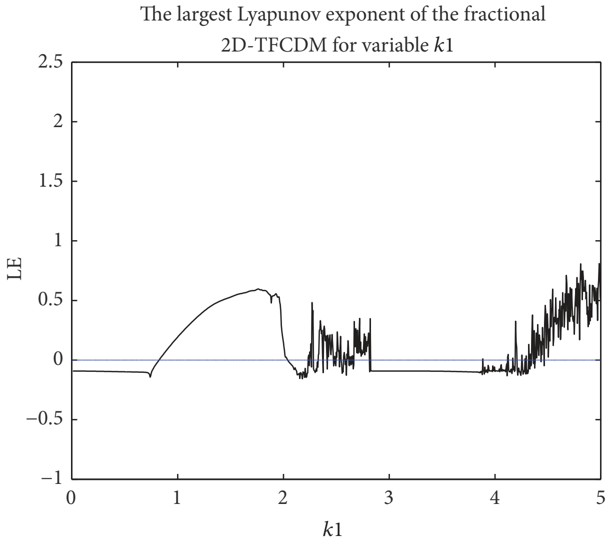


FIGURE 4: The largest Lyapunov exponent of the fractional 2D-TFCDM of the variable k_1.

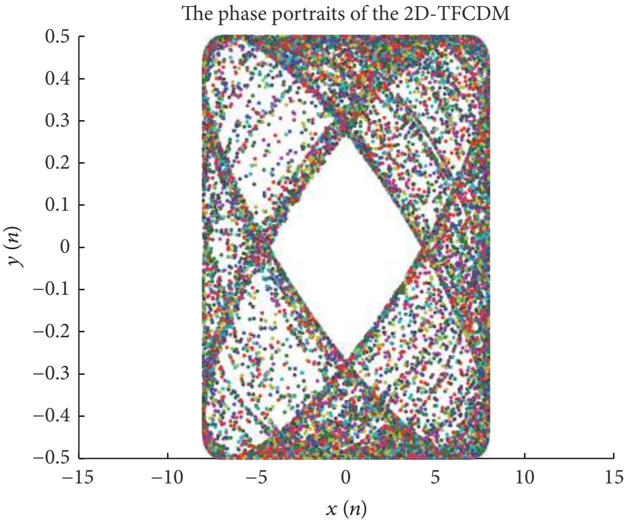


FIGURE 5: The phase portraits of the 2D-TFCDM for $k_1 = 8$, $k_2 = 0.5$, and $\nu = 1$.

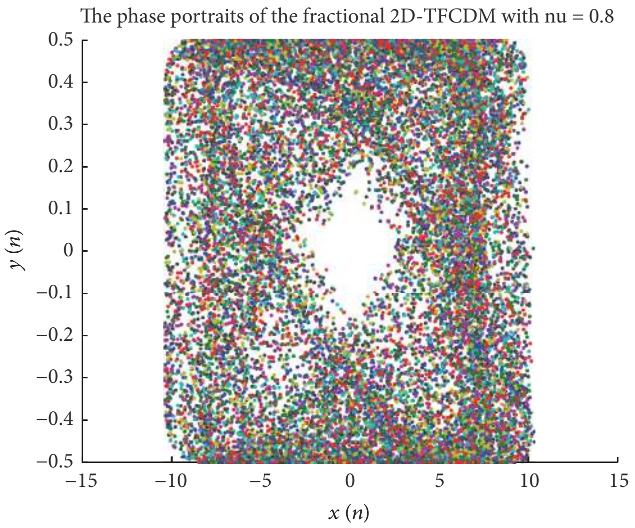


FIGURE 6: The phase portraits of the fractional 2D-TFCDM for $k_1 = 8$, $k_2 = 0.5$, and $\nu = 0.8$.

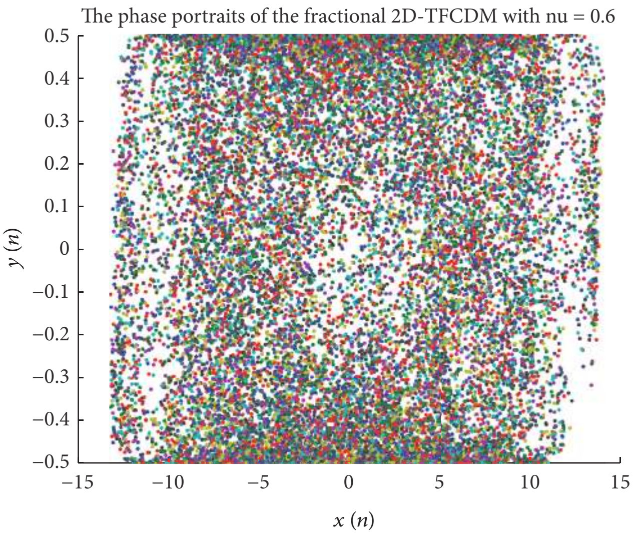


FIGURE 7: The phase portraits of the fractional 2D-TFCDM for $k_1 = 8$, $k_2 = 0.5$, and $\nu = 0.6$.

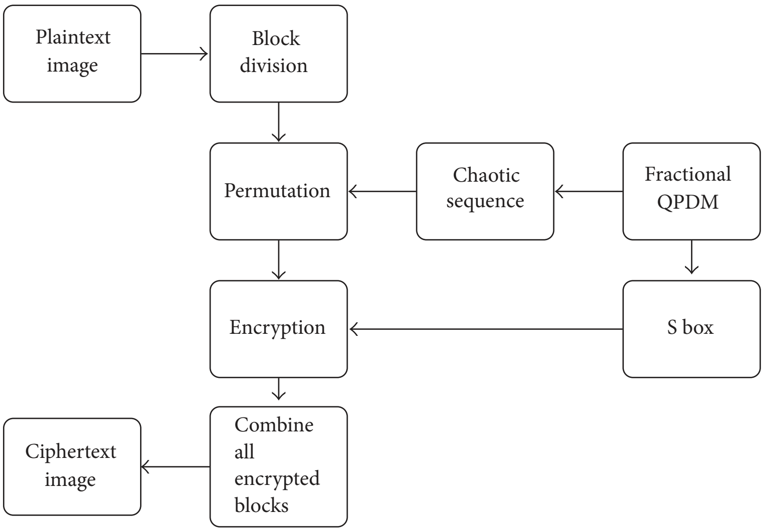


FIGURE 8: The proposed encryption method.

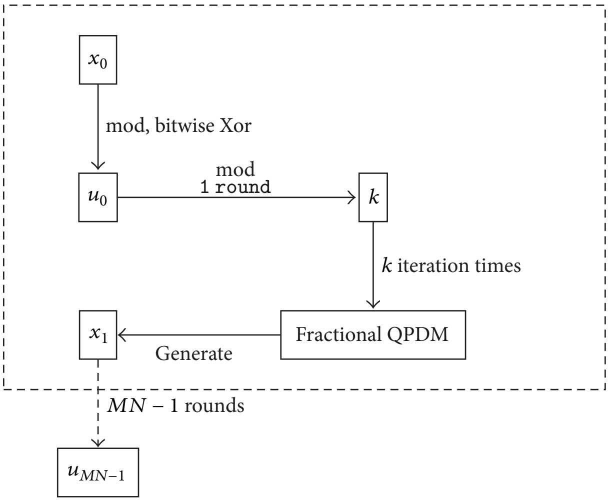
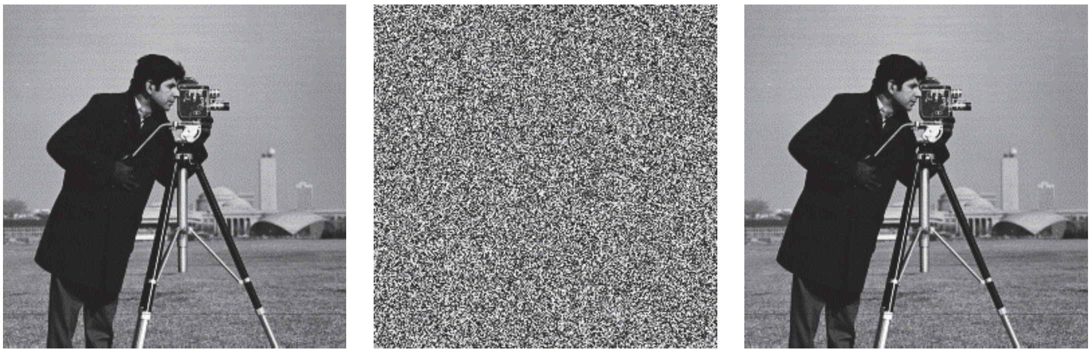


Figure 9: The S box.

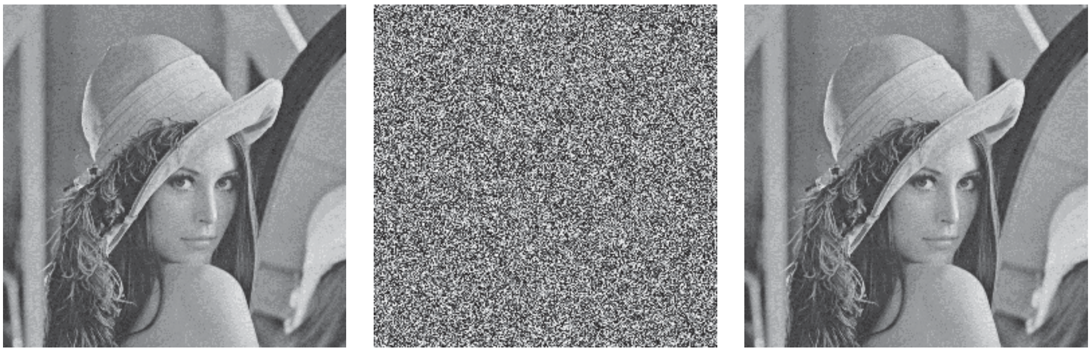


(a) The original figure

(b) The encrypted figure

(c) The decrypted figure

Figure 10: Cameraman.



(a) The original figure

(b) The encrypted figure

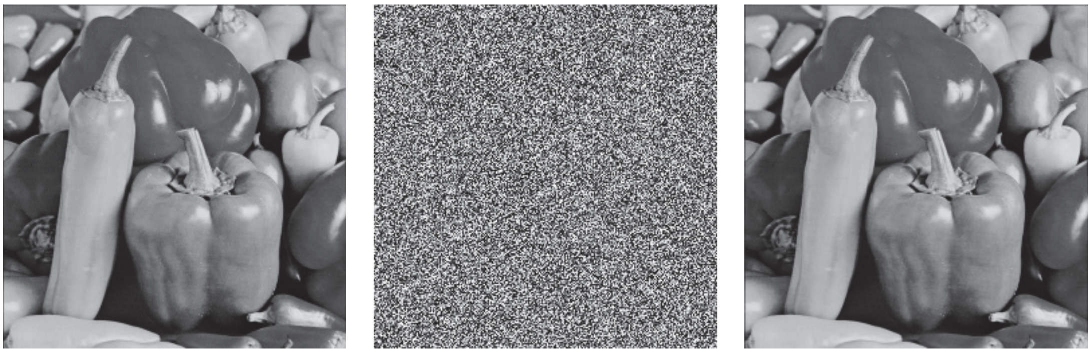
(c) The decrypted figure

Figure 11: Lena.

secret keys; consequently there are 5 keys. Assume the precision of x_0, y_0, ν, k_1, and k_2 are $10^{-16}, 3 \times 10^{-17}, 10^{-16}, 10^{-15}$, and 10^{-16}, respectively; then the key's space is $1/3 \times 10^{80} \approx 1.12 \times 2^{264}$. If the size of the plaintext is 512×512, then the key space of K-image is also $512 \times 512 \times 2^{8} = 2^{26}$. The total key space of the proposed algorithm is 1.12 $\times 2^{290}$.

7.2. Statistics Analysis. The quality against any statistical attack is important for a well-designed encryption method; it include 3 aspects as follows.

7.2.1. Correlation of the Plain- and Cipher-Images. In an ordinary image, the adjacent pixels are related; therefore the correlation coefficient of adjacent pixels is usually high. A good

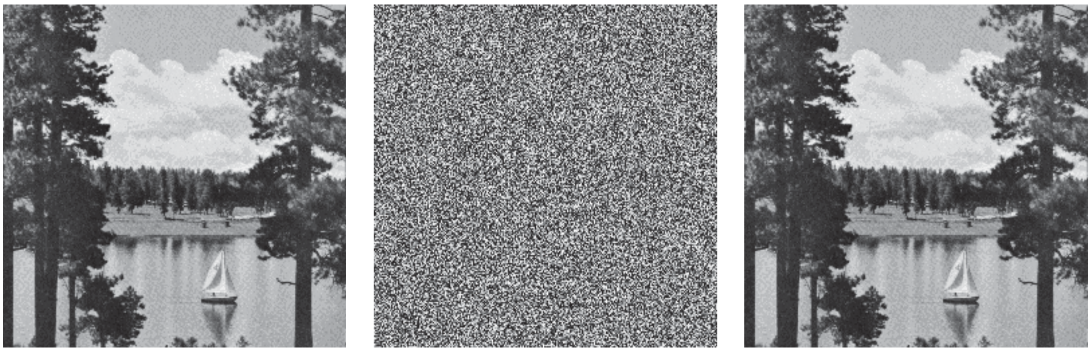


(a) The original figure

(b) The encrypted figure

(c) The decrypted figure

Figure 12: Peppers.

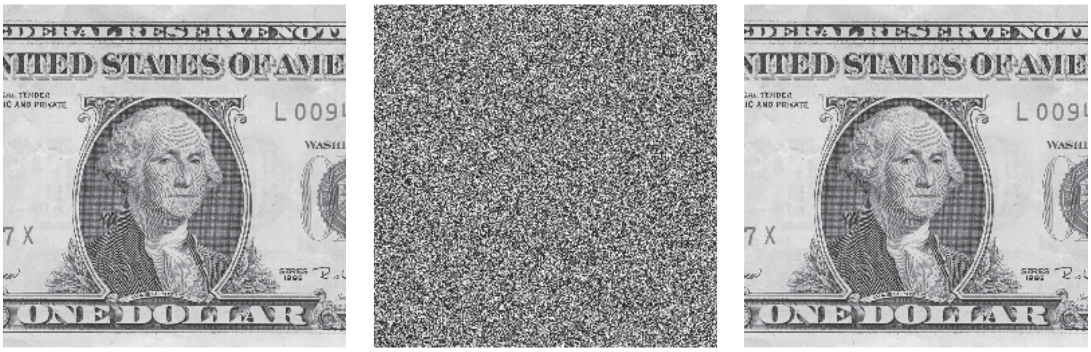


(a) The original figure

(b) The encrypted figure

(c) The decrypted figure

Figure 13: Lake.

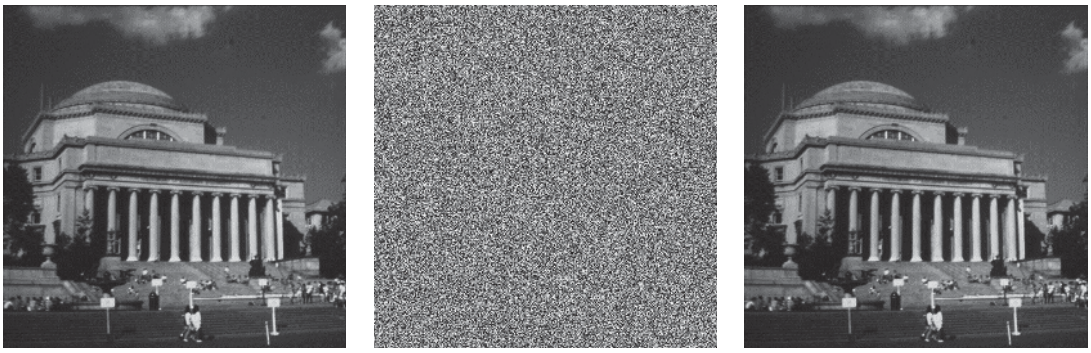


(a) The original figure

(b) The encrypted figure

(c) The decrypted figure

Figure 14: Dollar.

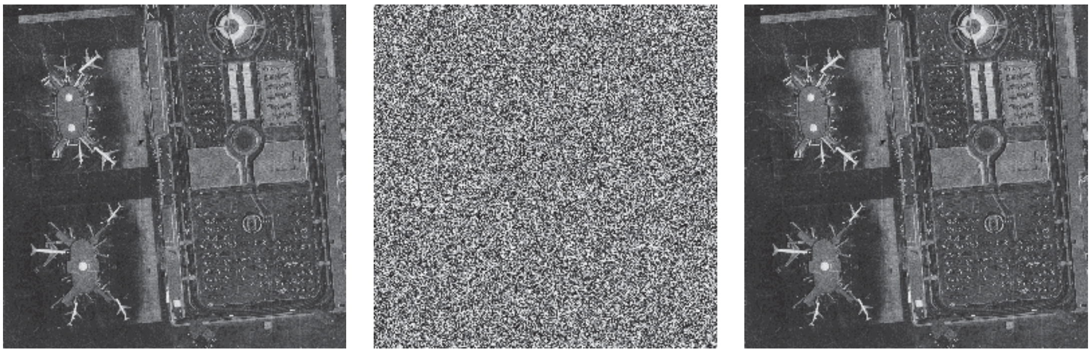


(a) The original figure

(b) The encrypted figure

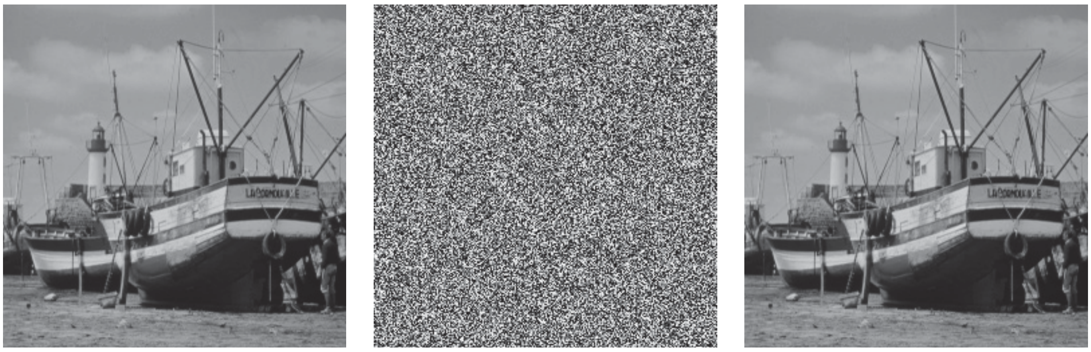
(c) The decrypted figure

Figure 15: Columbia.



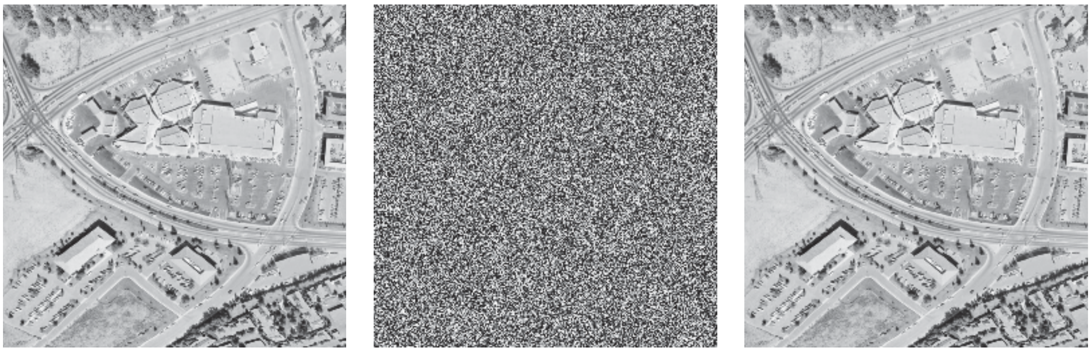
(a) The original figure (b) The encrypted figure (c) The decrypted figure

Figure 16: Lax.



(a) The original figure (b) The encrypted figure (c) The decrypted figure

Figure 17: Boat.



(a) The original figure (b) The encrypted figure (c) The decrypted figure

Figure 18: Aerial.

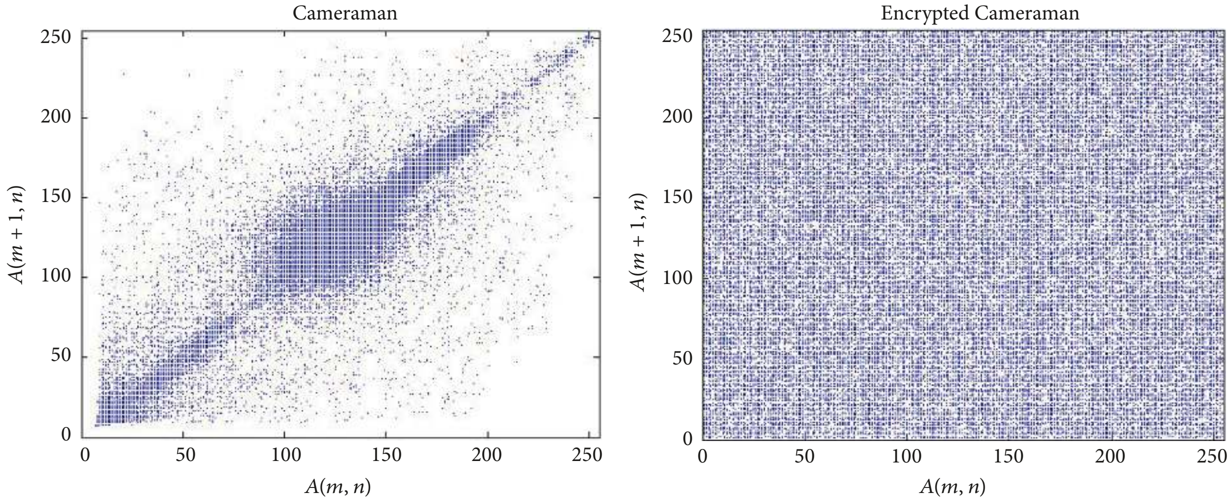
encryption algorithm should make the correlation coefficients of encrypted image nearly equal to zero. The closer to zero the correlation coefficients is, the better the encryption algorithm is. Formulas (23) calculate the correlation coefficient. The correlations along the x direction of both original and encrypted images are displayed in Figures 19–27 from Cameraman to Aerial. The correlation coefficients are displayed in Table 1.

$$r_{xy} = \frac{\left|\operatorname{cov}(x, y)\right|}{\sqrt{D(x)}\sqrt{D(y)}}$$

$$\operatorname{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right)$$

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

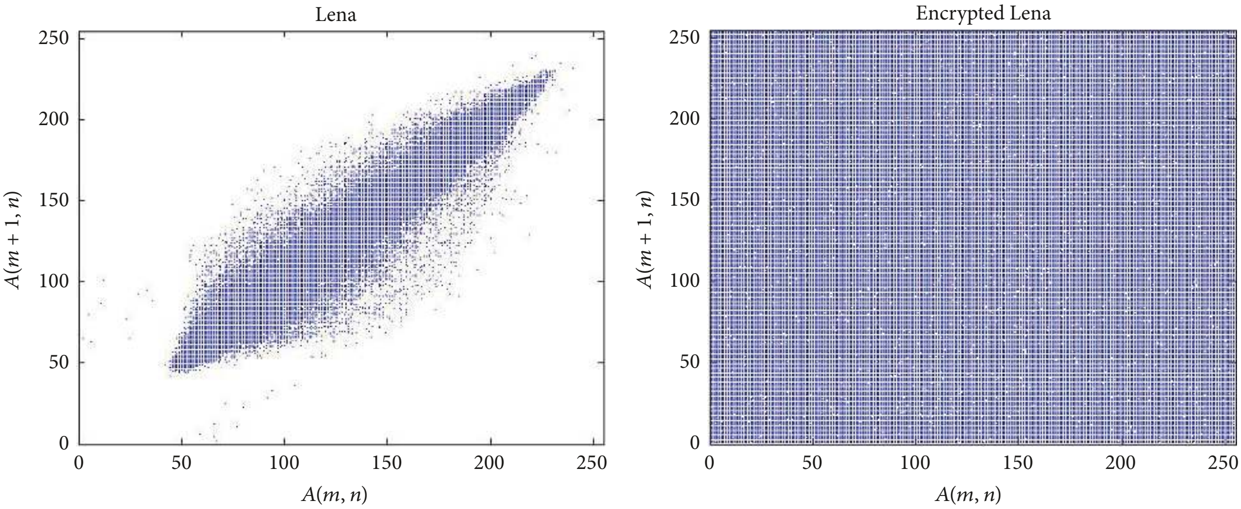
$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)^2. \tag{23}$$



(a) The original figure

(b) The encrypted figure

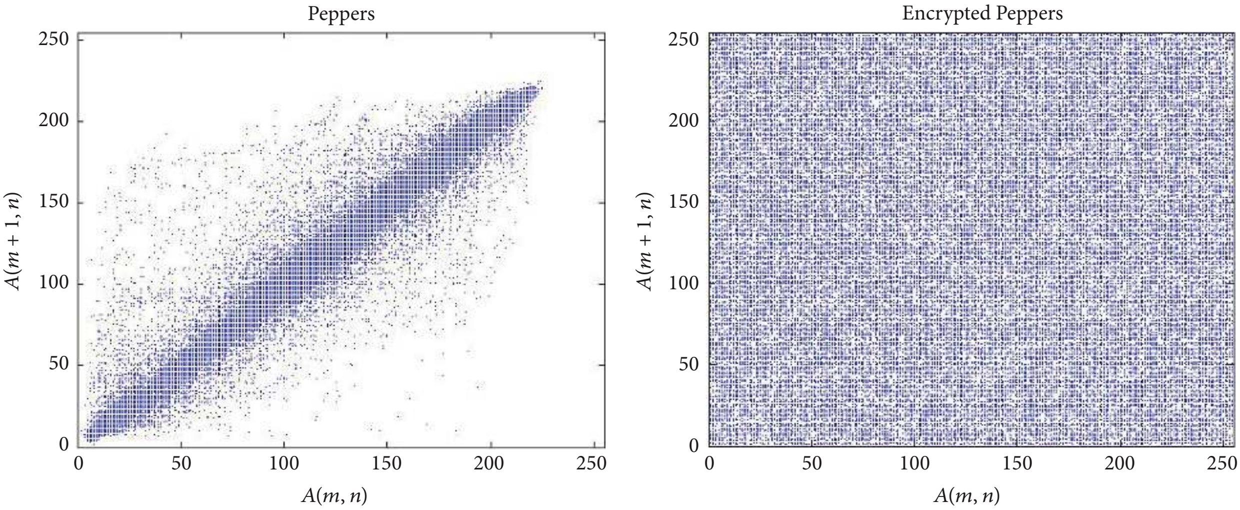
Figure 19: Cameraman.



(a) The original figure

(b) The encrypted figure

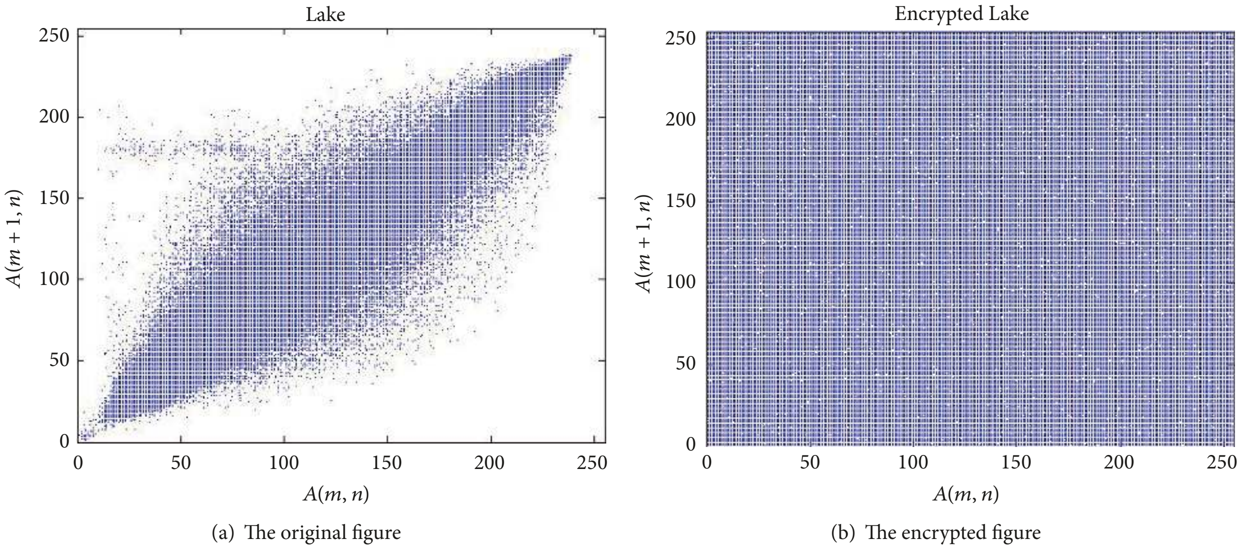
Figure 20: Lena.



(a) The original figure

(b) The encrypted figure

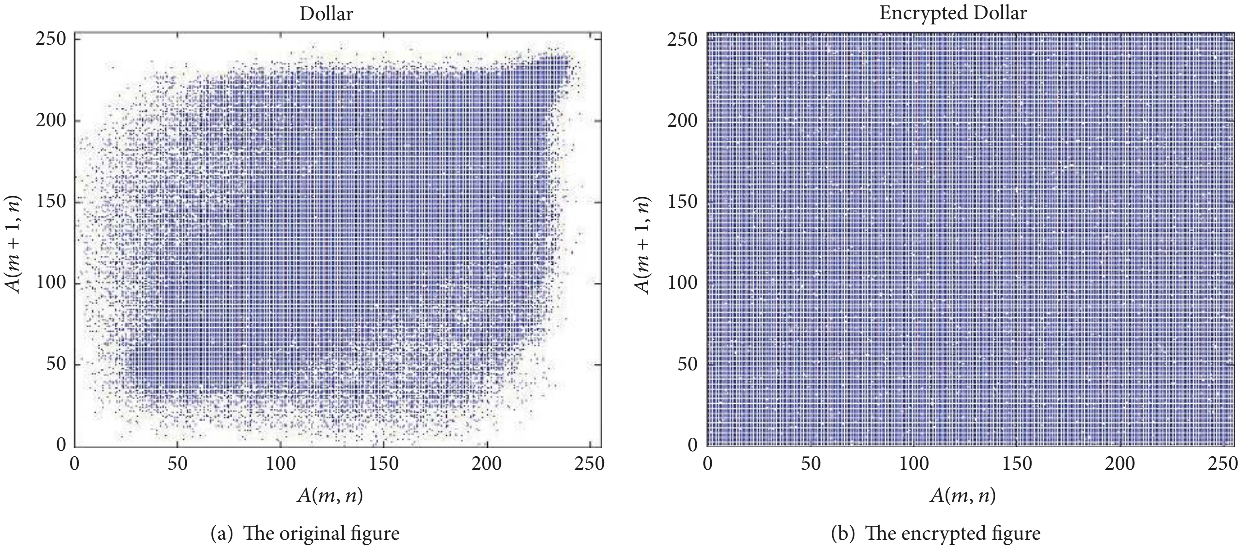
Figure 21: Peppers.



(a) The original figure

(b) The encrypted figure

Figure 22: Lake.



(a) The original figure

(b) The encrypted figure

Figure 23: Dollar.

With the sharp contrast of data between original image and encrypted image, Table 1 indicates that the encryption process make pixels of the encrypted image almost independent with each other. Consequently, the encryption algorithm is good at pixel value randomization.

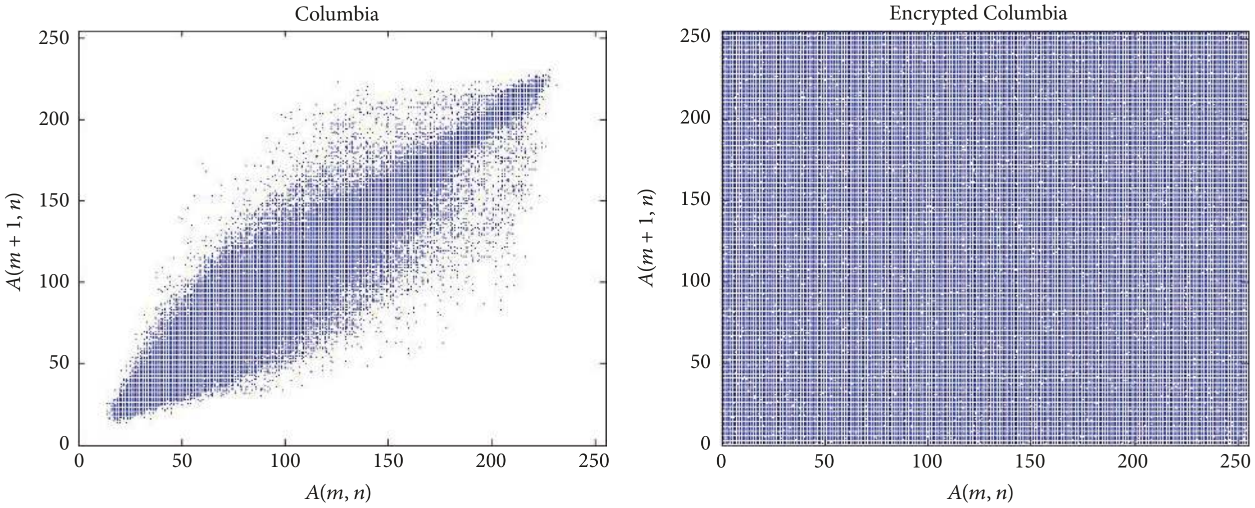
Compared with other algorithm, we can observe that most correlation coefficients of encrypted image are nearer to 0 in Table 2. As a consequence of this, the proposed encryption algorithm is superior to others.

7.2.2. Histogram. Histogram reflects the distribution of colors inside the image. The adversary can get some effective information from the regularity of histogram. Therefore, a well-designed image encryption method should make the pixel value of encrypted image distribute uniformly. Figure 28 shows the histogram of Cameraman. Similarly, the histograms of the other 8 cases are drawn in Figures 29–36. It is illustrated that the proposed encryption method has a good effect on pixel value distribution uniformization.

7.2.3. Information Entropy. Information entropy defines the randomness and the unpredictability of information in an image. It is defined by

$$H(m) = \sum_{i=0}^{2^n-1} p(m_i)\log_2 \frac{1}{p(m_i)}. \quad (24)$$

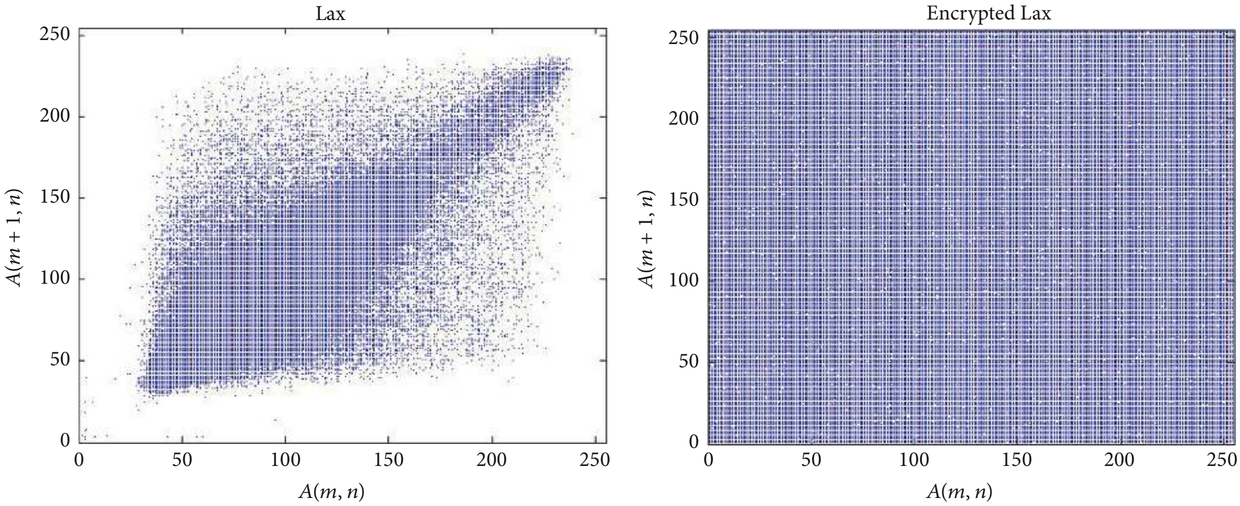
Here $p(m_i)$ is the probability of m_i; n is the number of bits that is required to represent the symbol m_i. For the pixels values of the image are 0~255, according to (24) the information entropy is 8 bits for an ideally random image. Therefore, the closer to 8 bits the information entropy is, the better



(a) The original figure

(b) The encrypted figure

Figure 24: Columbia.



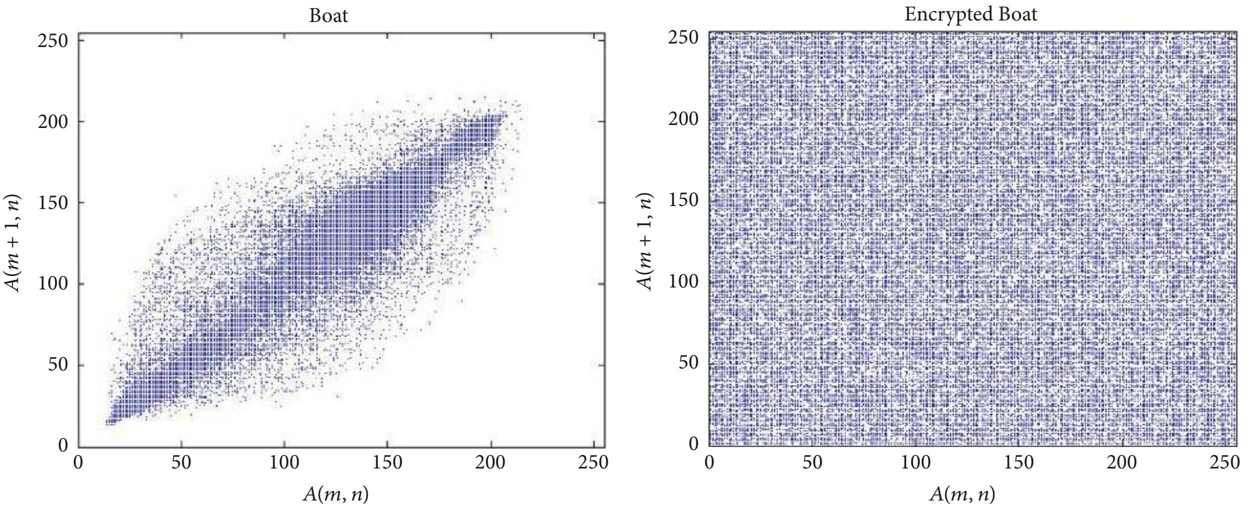
(a) The original figure

(b) The encrypted figure

Figure 25: Lax.

Table 1: Correlation coefficients of image.

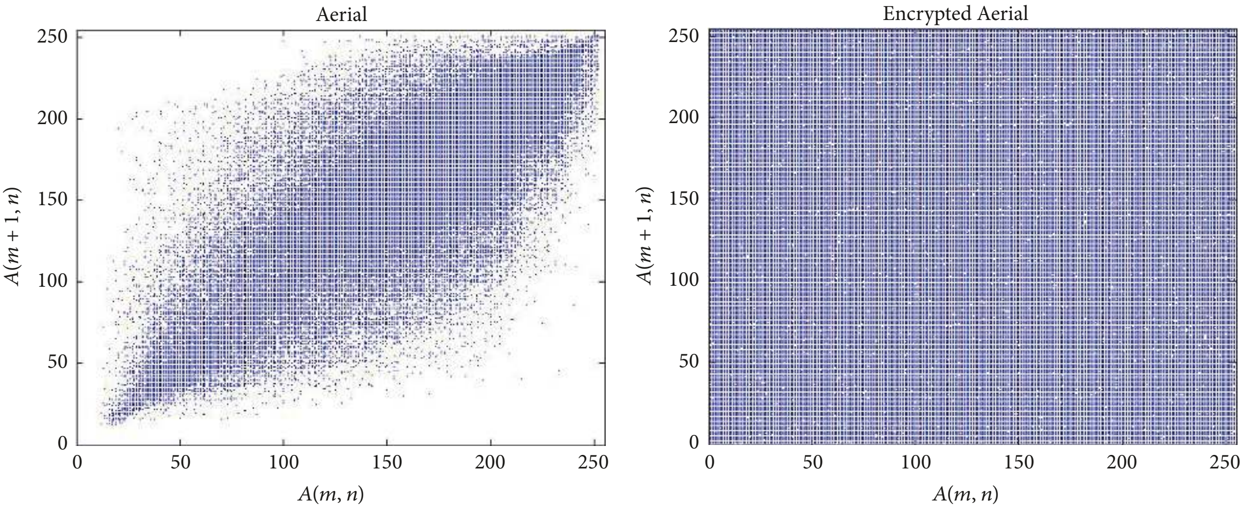
Image	Original image			Encrypted image		
	Horizontal	Diagonal	Vertical	Horizontal	Diagonal	Vertical
Cameraman	0.9276	0.9120	0.9597	0.0119	−0.0021	−0.0025
Lena	0.9722	0.9527	0.9860	−0.0140	−0.0086	−0.0034
Peppers	0.9667	0.9382	0.9694	−0.0088	0.0080	−0.0054
Lake	0.9768	0.9544	0.9748	−0.0155	0.0101	−0.0088
Dollar	0.8035	0.6952	0.6938	0.0131	−0.0183	0.0263
Columbia	0.9727	0.9403	0.9705	0.0060	−0.0104	−0.0093
Lax	0.7889	0.7151	0.8483	−0.0107	0.0147	0.0107
Boat	0.9407	0.9158	0.9545	0.0169	−0.0074	−0.0077
Aerial	0.9135	0.7952	0.8677	0.0084	−0.0123	−0.0133



(a) The original figure

(b) The encrypted figure

Figure 26: Boat.



(a) The original figure

(b) The encrypted figure

Figure 27: Aerial.

the encryption algorithm is. The information entropy of the 9 cases is gotten in Table 3; it indicates that the encrypted images are very close to the random images.

From Table 4, we can observe that the information entropy of proposed algorithm is nearer to 8 bits than other algorithms.

7.3. Sensitivity Analysis. The different range between two images is measured by two criteria: number of pixels change rate (NPCR) and unified average changing intensity (UACI). They are defined as follows:

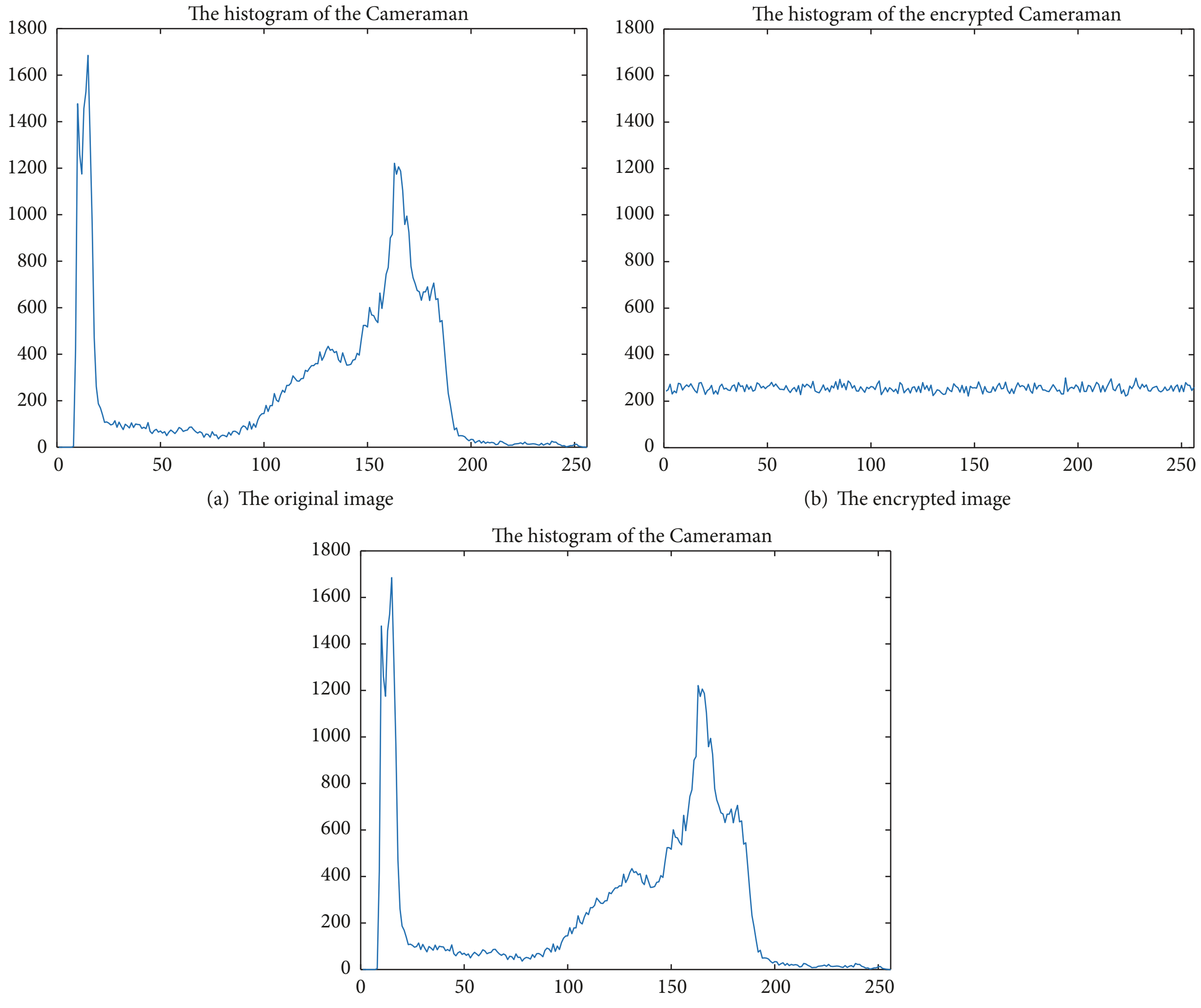
$$D(i,j) = \begin{cases} 0, & T_1(i,j) = T_2(i,j), \\ 1, & T_1(i,j) \neq T_2(i,j), \end{cases}$$

$$\text{NPCR} = \frac{\sum_{i=1}^{W} \sum_{j=1}^{H} D(i,j)}{W \times H} \times 100\%$$

$$\text{UACI} = \frac{\sum_{i=1}^{W} \sum_{j=1}^{H} \left| T_1(i,j) - T_2(i,j) \right|}{255W \times H} \times 100\%. \tag{25}$$

Here W and H are the width and the height of T_1 and T_2.

7.3.1. Key Sensitivity. We encrypt the image by the keys $x_0 = 0.19$, $y_0 = 0.06$, $\nu = 0.7123456$, $k_1 = 8$, and $k_2 = 0.5$. Figure 37(a) is the decrypted image with the correct keys. Figure 37(b) represents the decrypted image under 10^{-16} adding to x_0 with other keys unchanged. Similarly, the secret



(a) The original image

(b) The encrypted image

(c) The decrypted image

Figure 28: Cameraman.

Table 2: Comparison of correlation coefficients of image.

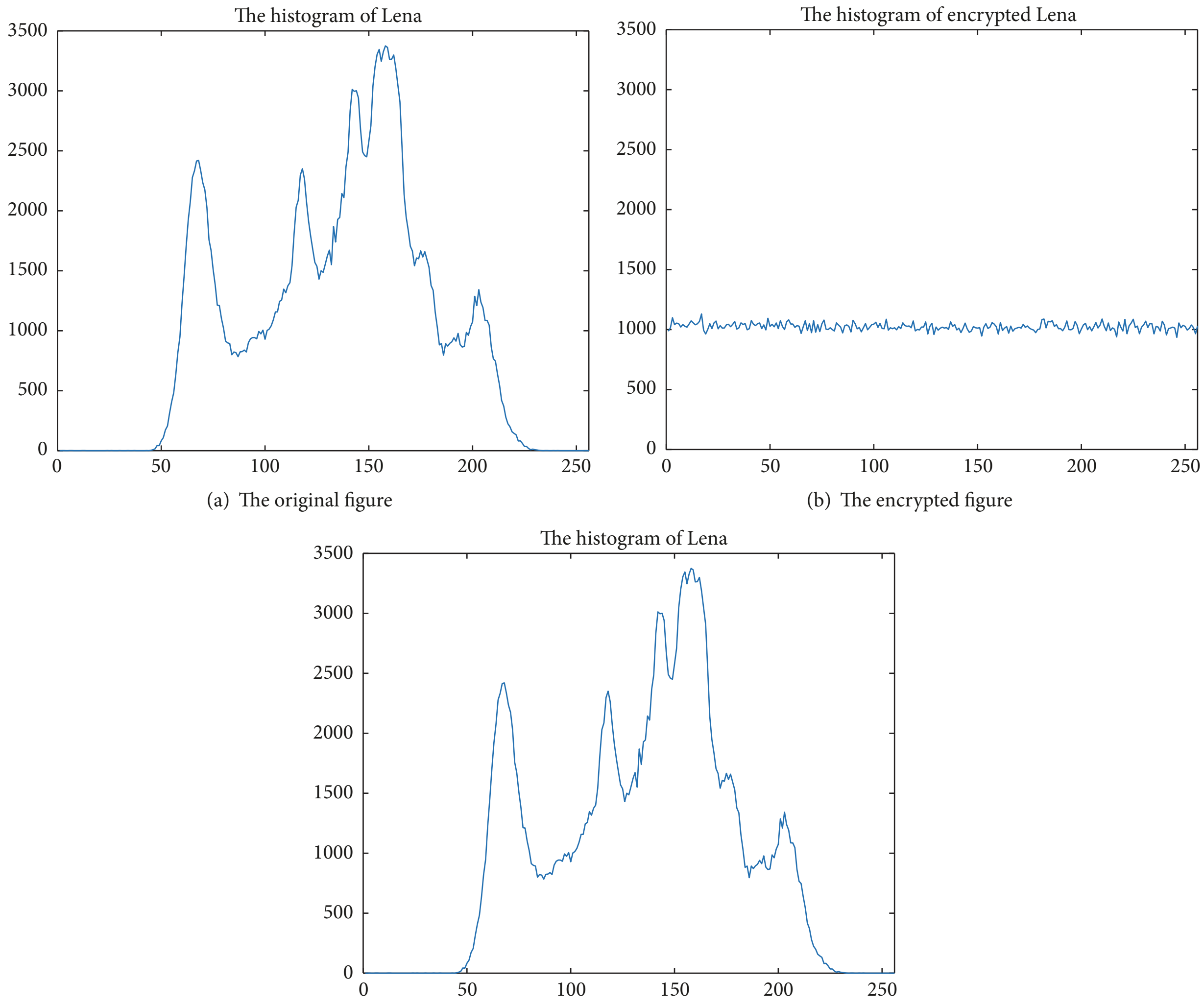
Algorithm	Image	Original image			Encrypted image		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Proposed	Lena	0.9722	0.9527	0.9860	−0.0140	−0.0086	−0.0034
[1]	Lena	0.9503	0.9755	0.9275	−0.0226	0.0041	0.0368
[2]	Lena	0.927970	0.926331	0.839072	−0.010889	−0.018110	−0.006104
[5]	Lena	0.946	0.973	0.921	−0.0055	−0.0075	0.0026
[6]	Lena	0.9569	0.9236	0.9019	0.0042	−0.0043	0.0163

keys y_0, v, k_1, k_2 are added as $3 \times 10^{-17}, 10^{-16}, 10^{-15}$ and 10^{-16} to decrypt the images separately with other keys unchanged. The results are shown in Figures 37(c)–37(f). The comparison of key space is shown in Table 5 and the NPCR and UACI between Figures 37(a) and 37(b)–37(f) are calculated in Table 6.

In contrast with other algorithm, the key space of proposed algorithm is larger than others.

Most NPCR are near to 99.61% and most of UACI are higher than 30% in Table 6. We cannot recognize the man inside from Figures 37(b)–37(f); therefore the encryption method is sensitive to the keys.

7.3.2. Plaintext Sensitivity. By encrypting two same images with only one pixel difference, the attackers can obtain effective information by comparing the two encrypted



(a) The original figure

(b) The encrypted figure

(c) The decrypted figure

Figure 29: Lena.

Table 3: Information entropy.

Image	Original image	Encrypted image
Cameraman	7.0097	7.9974
Peppers	7.5739	7.9976
Dollar	6.9785	7.9992
Lax	6.8272	7.9993
Aerial	6.9940	7.9992
Lena	7.2185	7.9993
Lake	7.4845	7.9993
Columbia	7.2736	7.9992
Boat	6.9391	7.9972

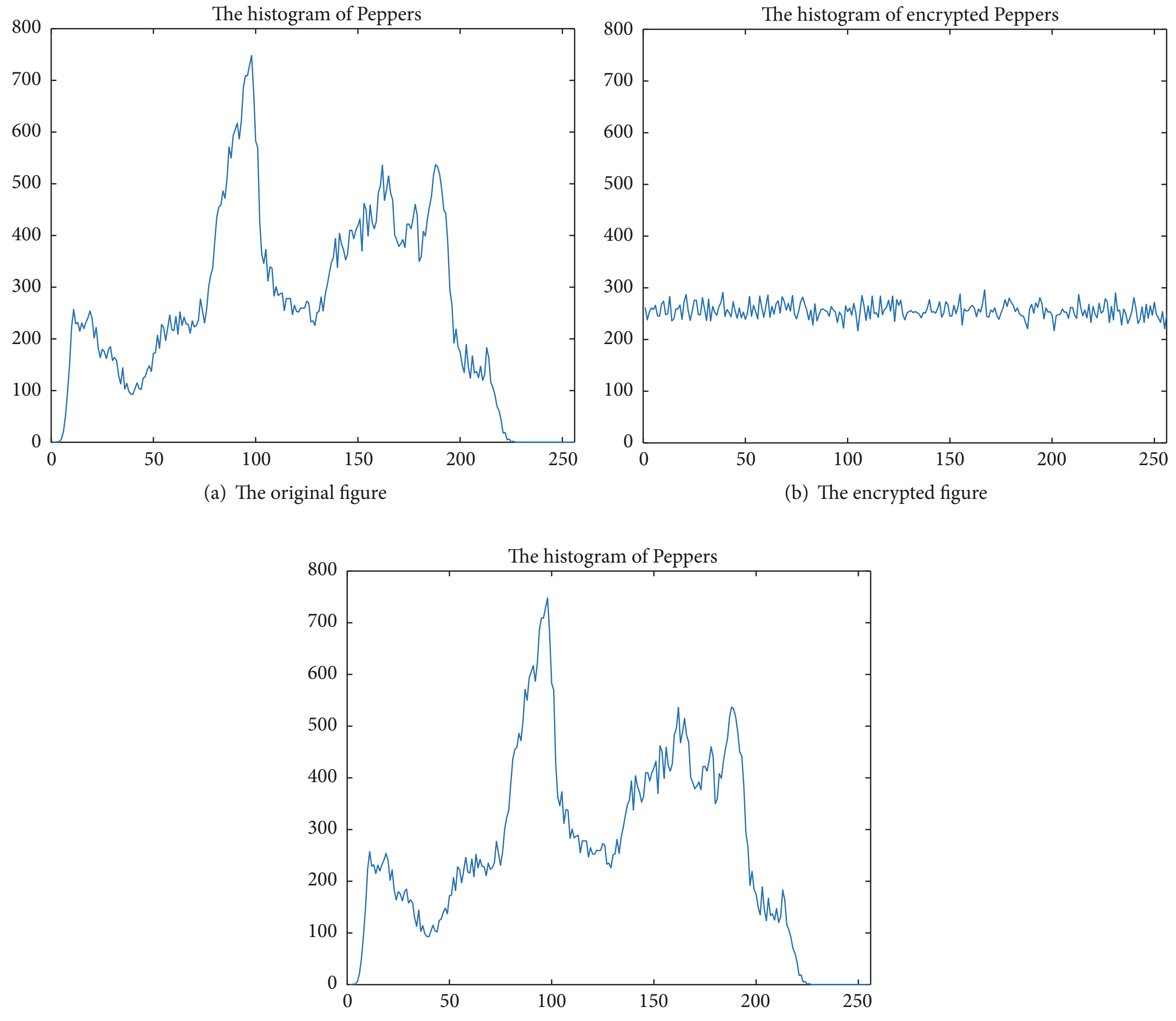
Table 4: Comparison of information entropy.

Algorithm	Image	Original image	Encrypted image
Proposed	Lena	7.2185	7.9993
[1]	Lena	7.2072	7.9973
[4]	Lena	Undefined	7.9972
[19]	Lena	Undefined	7.987918
[20]	Lena	7.447144	7.988847

Table 5: Comparison of key spaces.

Algorithm	Proposed	[2]	[4]	[6]
Key spaces	$2.23 \times 10^{87} (1.12 \times 2^{290})$	2^{128}	$\approx 2^{273}$	2^{276}

images. Therefore an encryption method designed against differential attack should ensure that the two encrypted images are completely different even if there is only a pixel difference in the original image.



(a) The original figure

(b) The encrypted figure

(c) The decrypted figure

Figure 30: Peppers.

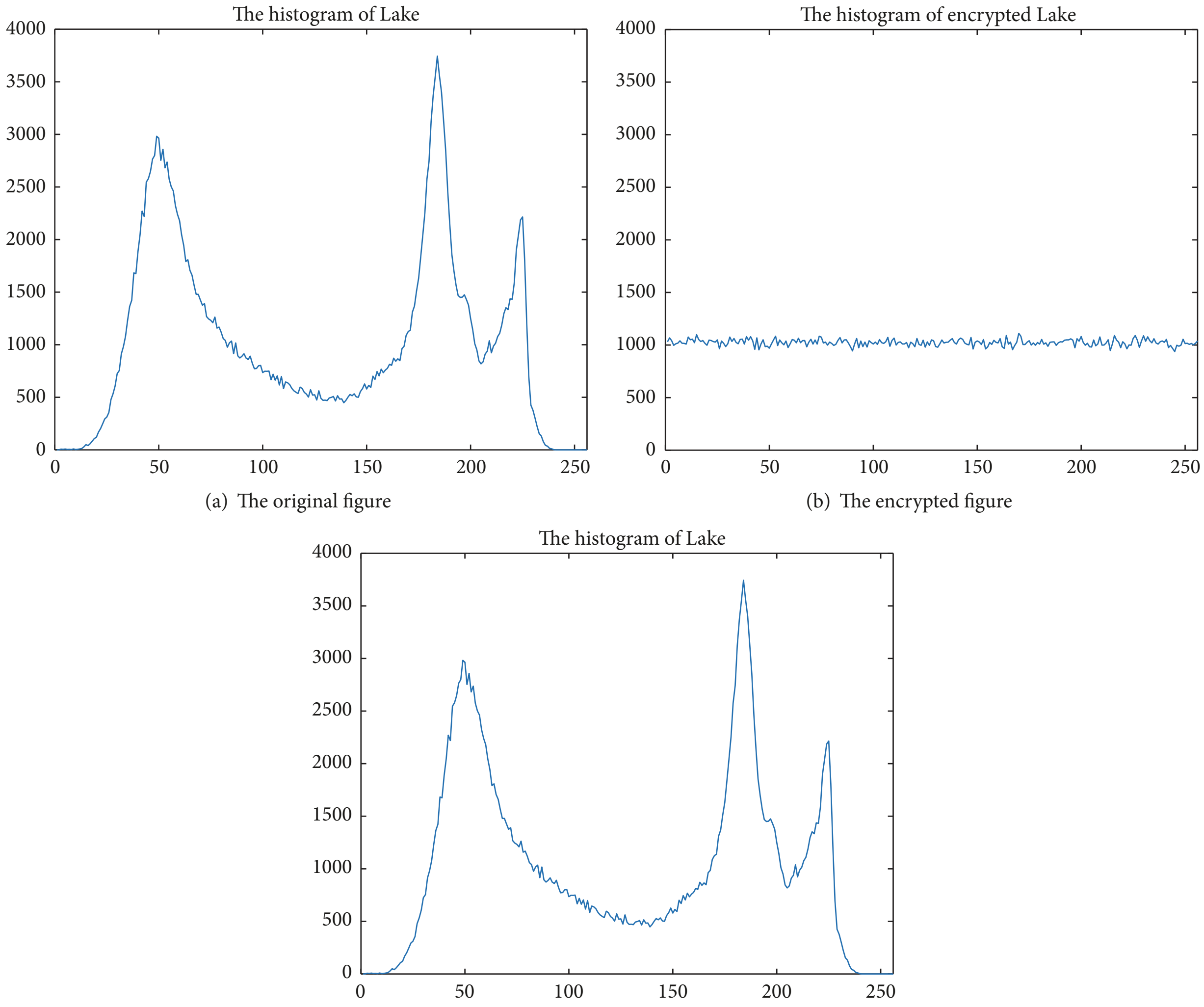
Table 6: NPCR and UACI between Figures 37(a) and 37(b)–37(f).

Image	NPCR and UACI	
	NPCR (%)	UACI (%)
Figure 37(b)	99.61	31.26
Figure 37(c)	97.02	30.23
Figure 37(d)	99.60	31.03
Figure 37(e)	99.61	31.01
Figure 37(f)	99.62	31.27

In Table 7, Figure 10(a)(x, y) is the same as Figure 10(a) except for a pixel locating (x, y). After that, the 2 images are encrypted with the same keys and the NPCR and UACI between the 2 ciphertext images are calculated. Similarly, the data of other 8 cases are obtained in Tables 8–15.

From Table 16, the NPCR and UACI of proposed algorithm after 2-round encryption are nearer to the ideal values 99.61% and 33.46% [33] than others. Therefore the proposed method is better.

7.4. Resistance to Known-Plaintext and Chosen-Plaintext Attacks. In Section 6.3, the iteration times of the next round are decided by the encrypted pixel value of present round. In (20), $x_2(i)$, generated from the fractional 2D-TFCDM, is dependent on $k(i-1)$ and determines $k(i)$. Therefore, the corresponding keystream is different when different plaintext is encrypted. For the resultant information is related to the chosen-images, the attacker cannot get useful information after encrypting some special images. As a result, the attacks proposed in [34–41] become ineffective for our scheme. In a word, the proposed scheme can primely resist the known-plaintext and the chosen-plaintext attacks.



(a) The original figure

(b) The encrypted figure

(c) The decrypted figure

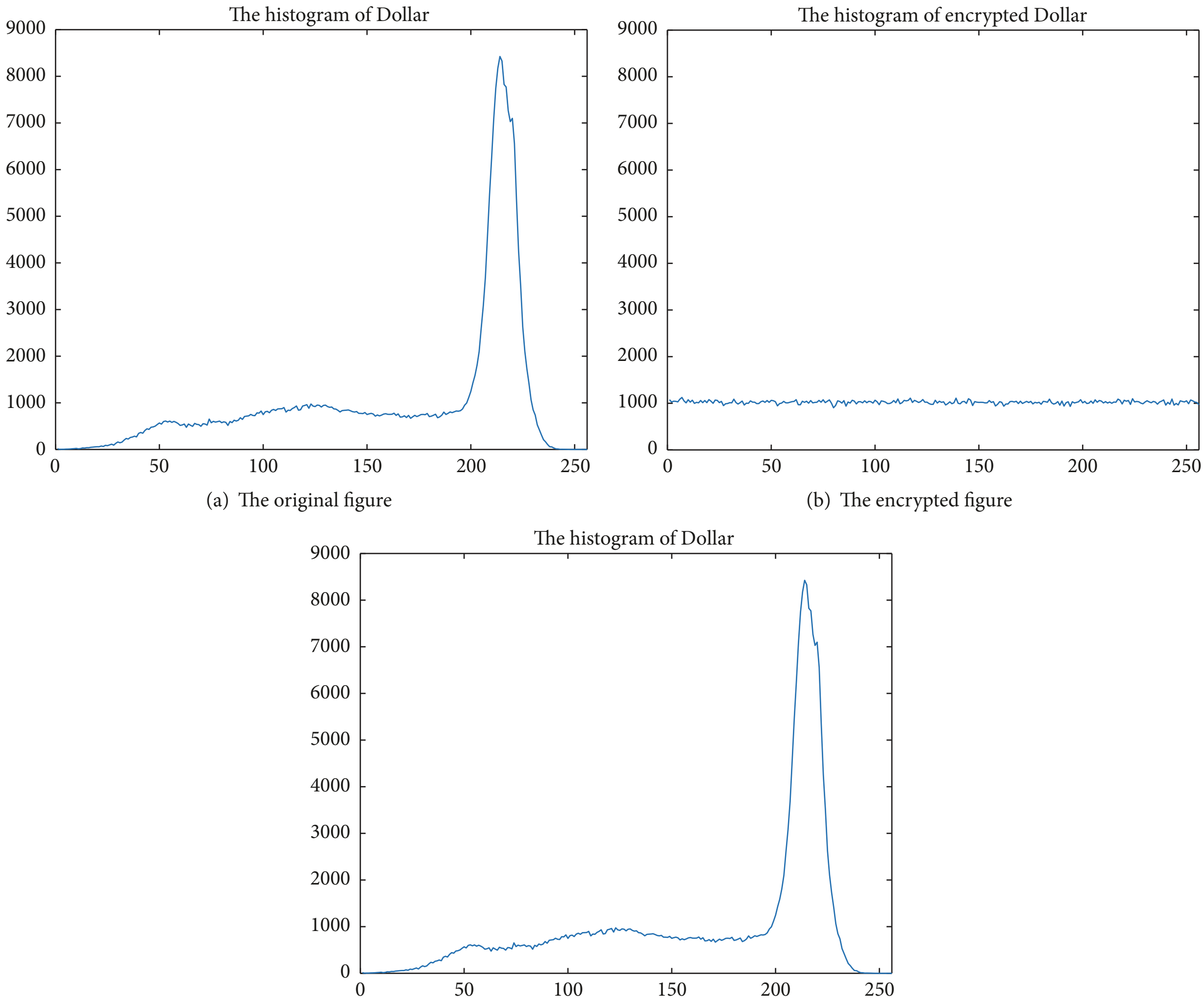
Figure 31: Lake.

Table 7: NPCR and UACI between cipher-images with slightly different plain-images.

Image	NPCR and UACI of Cameraman			
	NPCR (1-round %)	UACI (1-round %)	NPCR (2-round %)	UACI (2-round %)
Figure 10(a)(30, 30)	4.84	1.64	99.57	33.61
Figure 10(a)(50, 50)	81.43	27.39	99.62	33.56
Figure 10(a)(80, 80)	80.87	27.19	99.59	33.51
Figure 10(a)(100, 100)	6.82	2.28	99.59	33.46

Table 8: NPCR and UACI between cipher-images with slightly different plain-images.

Image	NPCR and UACI of Lena			
	NPCR (1-round %)	UACI (1-round %)	NPCR (2-round %)	UACI (2-round %)
Figure 11(a)(30, 30)	1.21	0.41	99.59	33.39
Figure 11(a)(50, 50)	95.06	31.93	99.59	33.53
Figure 11(a)(80, 80)	94.90	31.93	99.60	33.48
Figure 11(a)(100, 100)	1.71	0.58	99.63	33.40



(a) The original figure

(b) The encrypted figure

(c) The decrypted figure

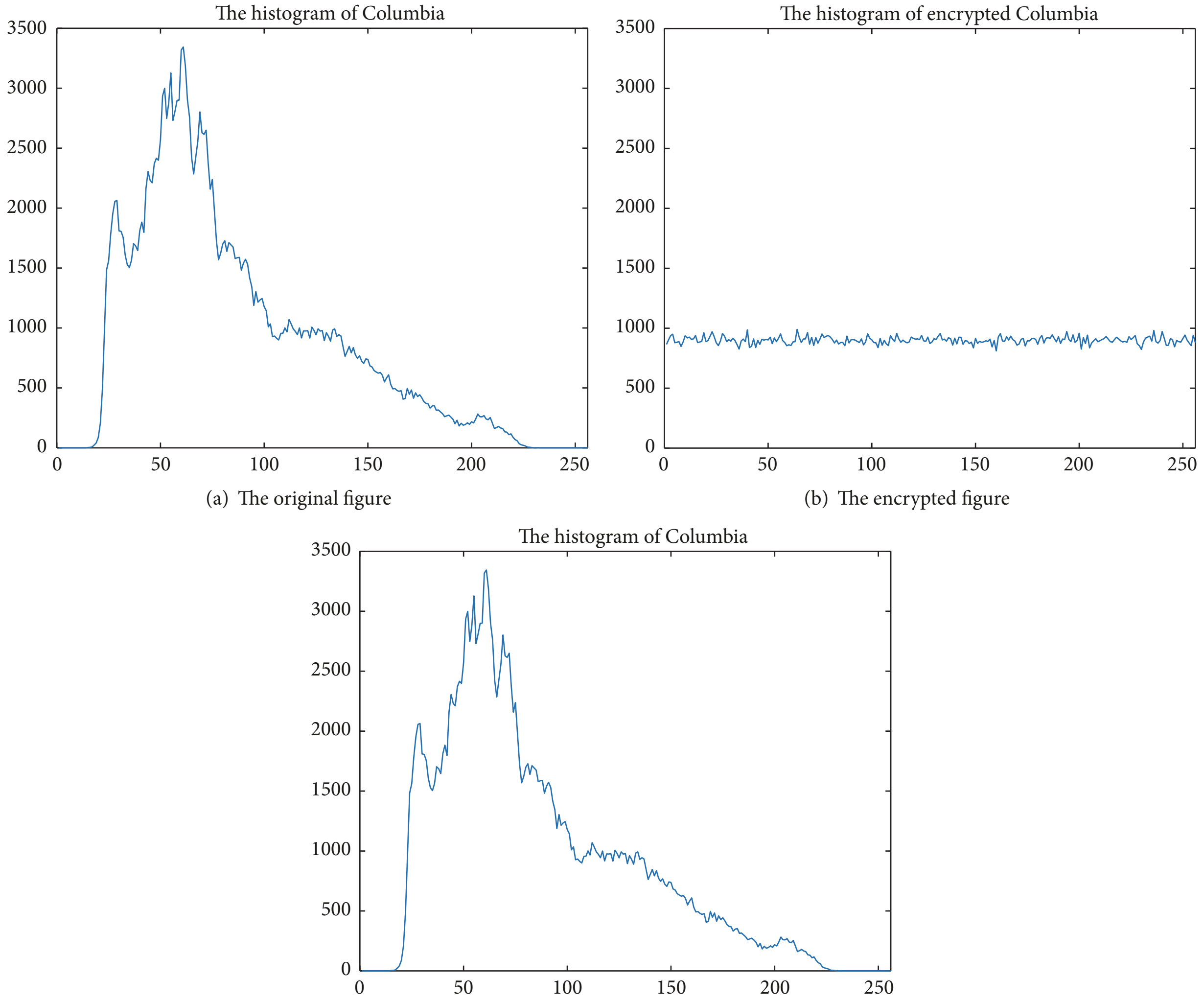
Figure 32: Dollar.

Table 9: NPCR and UACI between cipher-images with slightly different plain-images.

Image	NPCR and UACI of Peppers			
	NPCR (1-round %)	UACI (1-round %)	NPCR (2-round %)	UACI (2-round %)
Figure 12(a)(30, 30)	4.83	1.64	99.56	33.44
Figure 12(a)(50, 50)	81.44	27.35	99.62	33.50
Figure 12(a)(80, 80)	6.12	2.03	99.57	33.42
Figure 12(a)(100, 100)	6.83	2.32	99.60	33.50

Table 10: NPCR and UACI between cipher-images with slightly different plain-images.

Image	NPCR and UACI of Lake			
	NPCR (1-round %)	UACI (1-round %)	NPCR (2-round %)	UACI (2-round %)
Figure 13(a)(30, 30)	1.21	0.41	99.61	33.46
Figure 13(a)(50, 50)	95.09	31.88	99.61	33.42
Figure 13(a)(80, 80)	94.92	31.89	99.60	33.46
Figure 13(a)(100, 100)	1.71	0.58	99.59	33.47



(a) The original figure

(b) The encrypted figure

(c) The decrypted figure

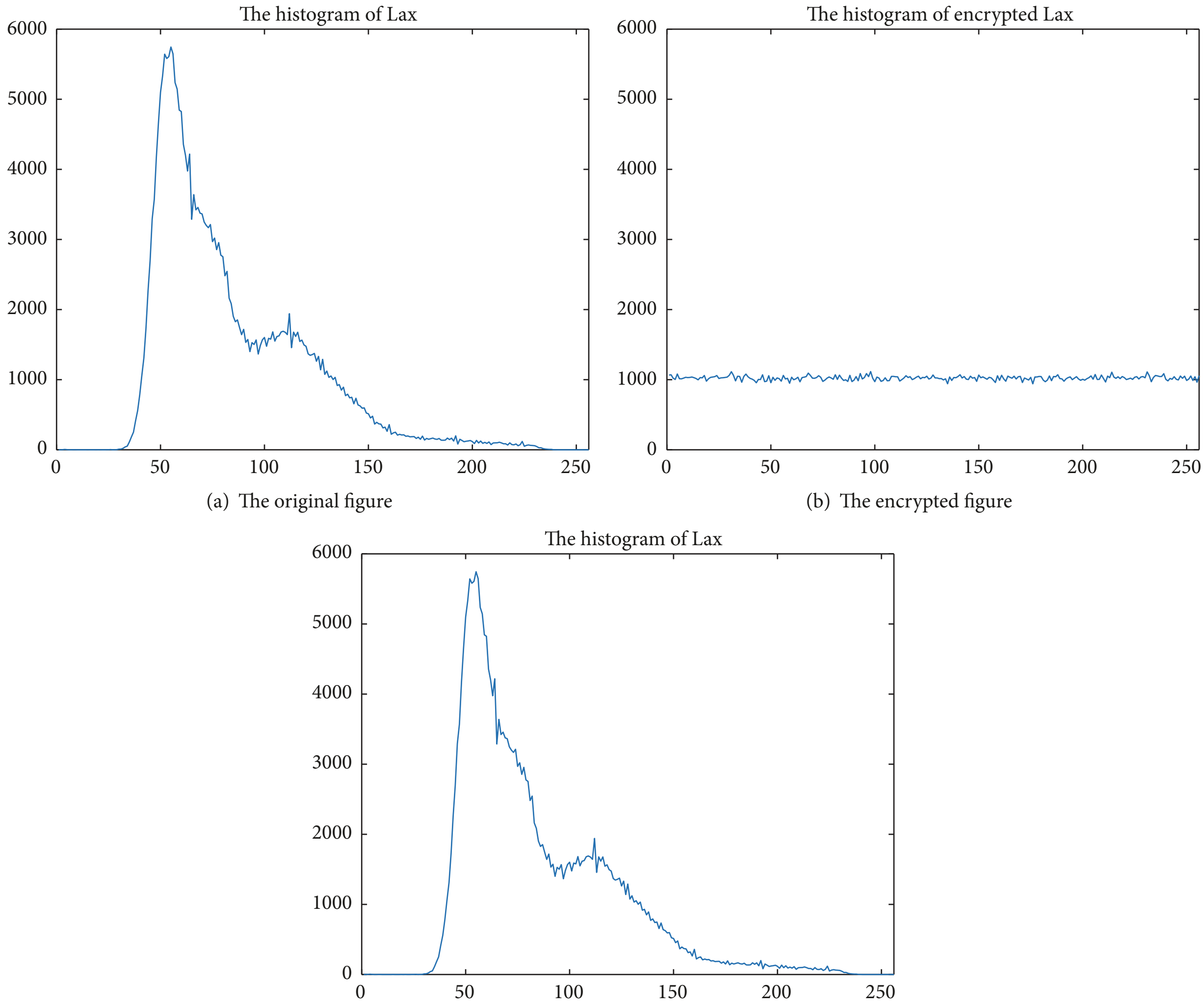
Figure 33: Columbia.

Table 11: NPCR and UACI between cipher-images with slightly different plain-images.

Image	NPCR and UACI of Dollar			
	NPCR (1-round %)	UACI (1-round %)	NPCR (2-round %)	UACI (2-round %)
Figure 14(a)(30, 30)	1.21	0.41	99.64	33.42
Figure 14(a)(50, 50)	95.08	32.00	99.60	33.49
Figure 14(a)(80, 80)	94.90	31.93	99.61	33.48
Figure 14(a)(100, 100)	1.71	0.57	99.61	33.41

Table 12: NPCR and UACI between cipher-images with slightly different plain-images.

Image	NPCR and UACI of Columbia			
	NPCR (1-round %)	UACI (1-round %)	NPCR (2-round %)	UACI (2-round %)
Figure 15(a)(30, 30)	94.83	31.96	99.61	33.47
Figure 15(a)(50, 50)	93.48	31.40	99.48	33.36
Figure 15(a)(80, 80)	0.96	0.32	99.60	33.45
Figure 15(a)(100, 100)	1.11	0.38	99.61	33.51



(a) The original figure

(b) The encrypted figure

(c) The decrypted figure

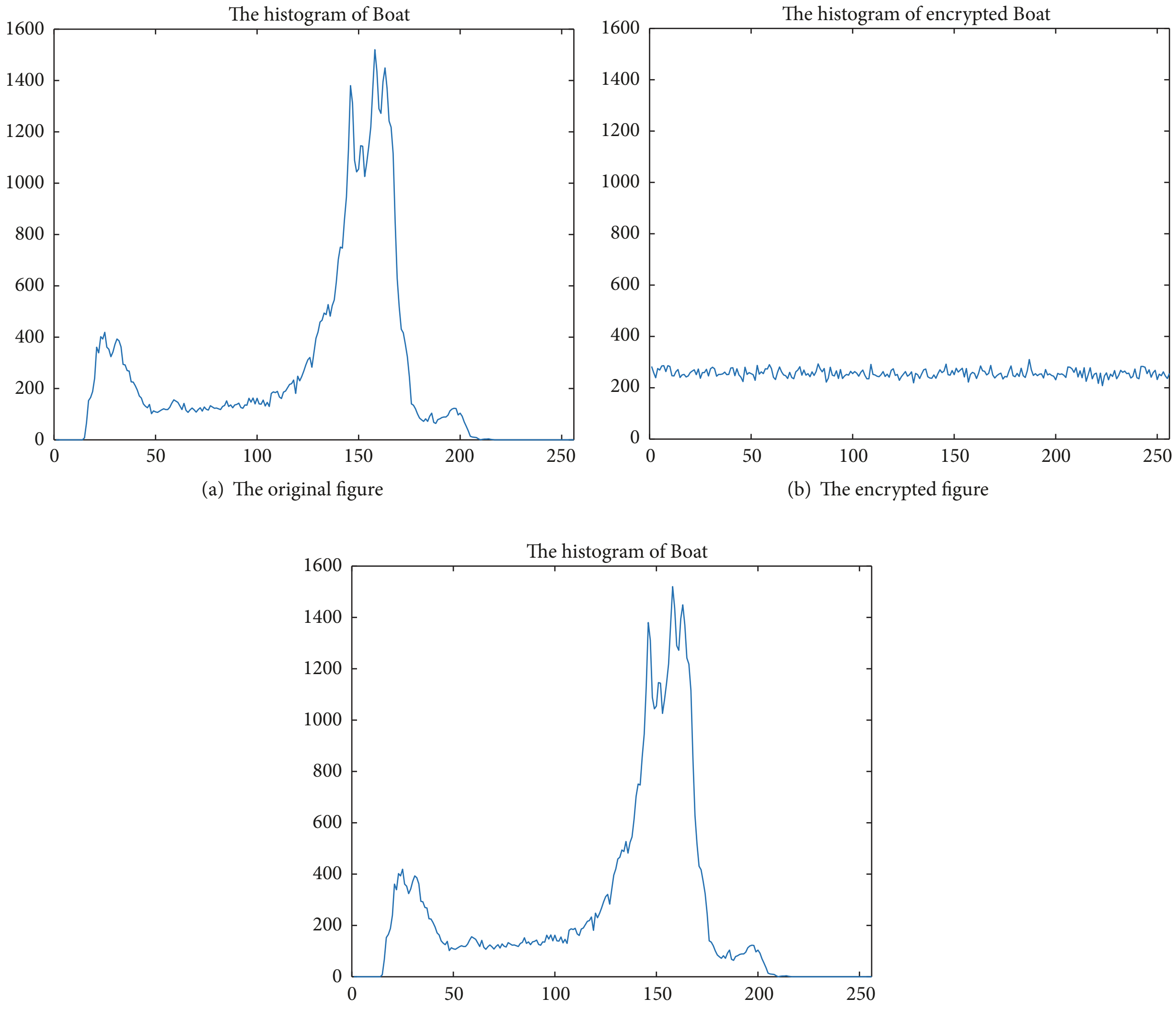
Figure 34: Lax.

Table 13: NPCR and UACI between cipher-images with slightly different plain-images.

Image	NPCR and UACI of Lax			
	NPCR (1-round %)	UACI (1-round %)	NPCR (2-round %)	UACI (2-round %)
Figure 16(a)(30, 30)	1.21	0.40	99.62	33.39
Figure 16(a)(50, 50)	95.06	31.99	99.61	33.49
Figure 16(a)(80, 80)	94.92	31.87	99.58	33.41
Figure 16(a)(100, 100)	1.70	0.58	99.62	33.48

Table 14: NPCR and UACI between cipher-images with slightly different plain-images.

Image	NPCR and UACI of Boat			
	NPCR (1-round %)	UACI (1-round %)	NPCR (2-round %)	UACI (2-round %)
Figure 17(a)(30, 30)	4.83	1.60	99.59	33.47
Figure 17(a)(50, 50)	81.46	27.45	99.62	33.59
Figure 17(a)(80, 80)	80.82	27.24	99.58	33.48
Figure 17(a)(100, 100)	6.82	2.32	99.62	33.61



(a) The original figure

(b) The encrypted figure

(c) The decrypted figure

Figure 35: Boat.

Table 15: NPCR and UACI between cipher-images with slightly different plain-images.

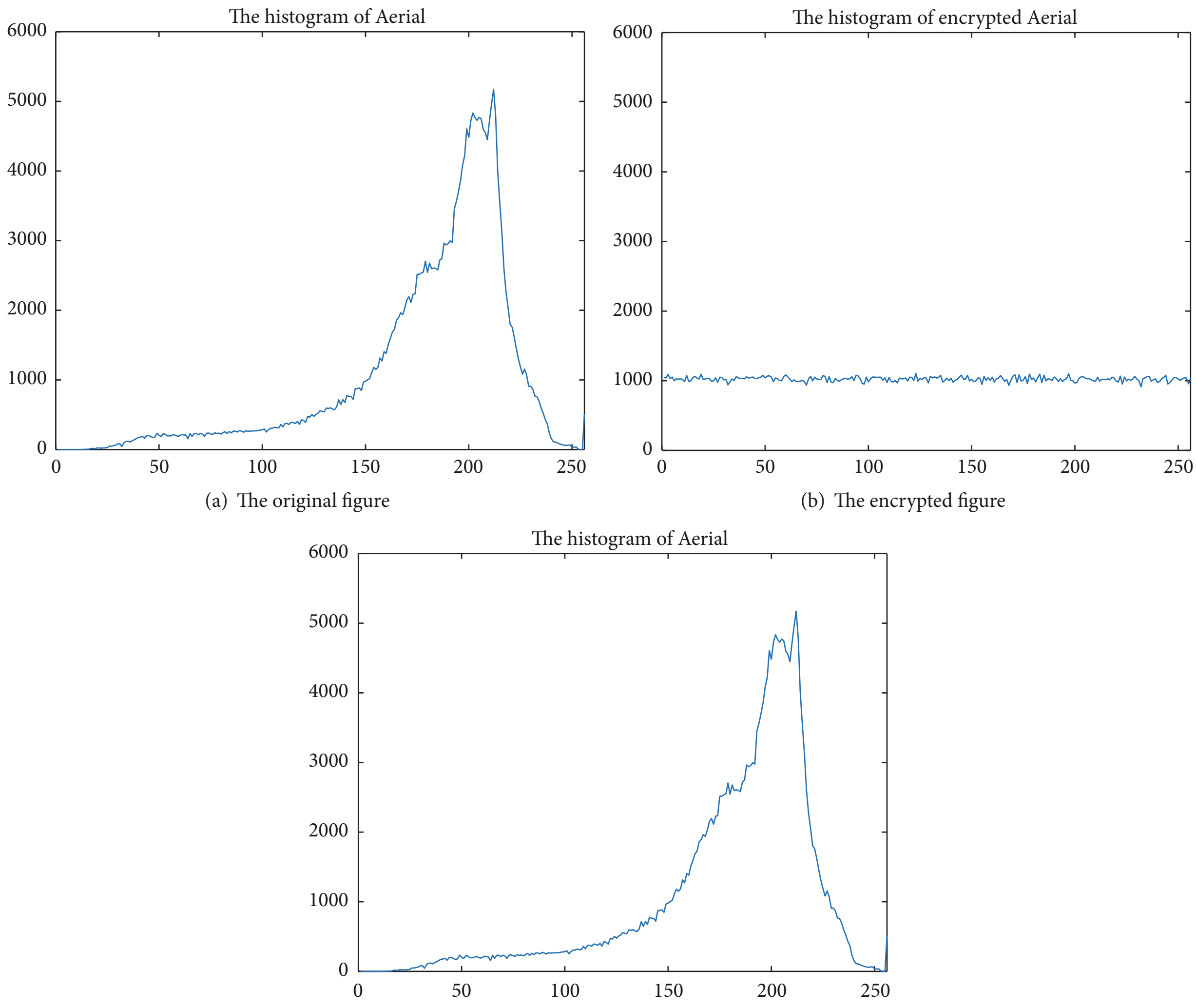
Image	NPCR and UACI of Aerial			
	NPCR (1-round %)	UACI (1-round %)	NPCR (2-round %)	UACI (2-round %)
Figure 18(a)(30, 30)	1.21	0.41	99.61	33.49
Figure 18(a)(50, 50)	95.06	31.93	99.62	33.43
Figure 18(a)(80, 80)	94.91	31.88	99.61	33.53
Figure 18(a)(100, 100)	1.71	0.57	99.61	33.52

8. Conclusions

Fractional 2D-TFCDM is obtained from the 2D-TFCDM. After that, we found new chaotic dynamics behaviors from the fractionalized map. Moreover, the map can be converted into image encryption algorithm as an application. Finally, the encryption effect is analysed in 4 main aspects; we find the proposed scheme is superior to others almost anywhere in comparison. As far as we know, the proposed image encryption algorithm has never been reported before.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

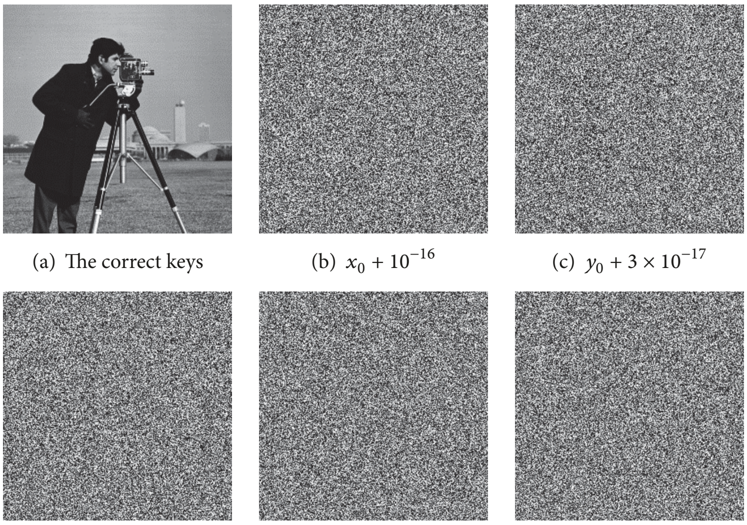


(a) The original figure

(b) The encrypted figure

(c) The decrypted figure

Figure 36: Aerial.



(a) The correct keys

(b) $x_0 + 10^{-16}$

(c) $y_0 + 3 \times 10^{-17}$

(d) $v + 10^{-16}$

(e) $k_1 + 10^{-15}$

(f) $k_2 + 10^{-16}$

Figure 37: The test of key sensitivity.

Table 16: Comparison of NPCR and UACI of image.

Algorithm	Image	NPCR (%)	UACI (%)
Proposed	Lena	99.60	33.48
[1]	Lena	99.61	33.53
[2]	Lena	99.6429	33.3935
[3]	Lena	99.6304	33.5989
[5]	Lena	99.932	39.520
[19]	Lena	75.62561	34.84288
[20]	Lena	99.6091	33.5038
[21]	Lena	99.6330	34.1319

Acknowledgments

The project was supported by the National Natural Science Foundation of China (Grant nos. 61072147, 11271008).

References

[1] L. Xu, X. Gou, Z. Li, and J. Li, "A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion," *Optics and Lasers in Engineering*, vol. 91, pp. 41–52, 2017.

[2] L. Teng, X. Wang, and J. Meng, "A chaotic color image encryption using integrated bit-level permutation," *Multimedia Tools and Applications*, pp. 1–14, 2017.

[3] R. Enayatifar, A. H. Abdullah, I. F. Isnin, A. Altameem, and M. Lee, "Image encryption using a synchronous permutation-diffusion technique," *Optics and Lasers in Engineering*, vol. 90, pp. 146–154, 2017.

[4] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Optics and Lasers in Engineering*, vol. 90, pp. 238–246, 2017.

[5] S. Chakraborty, A. Seal, M. Roy, and K. Mali, "A novel lossless image encryption method using DNA substitution and chaotic logistic map," *International Journal of Security and Its Applications*, vol. 10, no. 2, pp. 205–216, 2016.

[6] N. Zhou, S. Pan, S. Cheng, and Z. Zhou, "Image compressionï¿¡Cencryption scheme based on hyper-chaotic system and 2D compressive sensing," *Optics & Laser Technology*, vol. 82, pp. 121–133, 2016.

[7] K. S. Miller and B. Ross, "Fractional difference calculus," in *Univalent functions, fractional calculus, and their applications (Kōriyama, 1988)*, Ellis Horwood Ser. Math. Appl., pp. 139–152, Horwood, Chichester, 1989.

[8] M. Bohner and A. Peterson, *Dynamic Equations on Time Scales: An Introduction with Applications*, Birkhauser, Boston, Mass, USA, 2001.

[9] F. M. Atıcı and P. W. Eloe, "Initial value problems in discrete fractional calculus," *Proceedings of the American Mathematical Society*, vol. 137, no. 3, pp. 981–989, 2009.

[10] F. M. Atici and S. Sengul, "Modeling with fractional difference equations," *Journal of Mathematical Analysis and Applications*, vol. 369, no. 1, pp. 1–9, 2010.

[11] M. T. Holm, "The Laplace transform in discrete fractional calculus," *Computers & Mathematics with Applications*, vol. 62, no. 3, pp. 1591–1601, 2011.

[12] M. D. Ortigueira, "Introduction to fractional linear systems. Part 2: discrete-time case," *IEE Proceedings Vision, Image and Signal Processing*, vol. 147, no. 1, pp. 71–78, 2000.

[13] M. D. Ortigueira, F. J. V. Coito, and J. J. Trujillo, "A new look into the discrete-time fractional calculus: Derivatives and exponentials," in *Proceedings of the 6th Workshop on Fractional Differentiation and Its Applications, FDA 2013*, pp. 629–634, France, February 2013.

[14] G.-C. Wu and D. Baleanu, "Discrete chaos in fractional delayed logistic maps," *Nonlinear Dynamics*, vol. 80, no. 4, pp. 1697–1703, 2015.

[15] G.-C. Wu and D. Baleanu, "Discrete fractional logistic map and its chaos," *Nonlinear Dynamics*, vol. 75, no. 1-2, pp. 283–287, 2014.

[16] G.-C. Wu, D. Baleanu, and S.-D. Zeng, "Discrete chaos in fractional sine and standard maps," *Physics Letters A*, vol. 378, no. 5-6, pp. 484–487, 2014.

[17] K. Araki, T. Satoh, and S. Miura, "Overview of elliptic curve cryptography," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface*, vol. 1431, pp. 29–49, 1998.

[18] C. Ma, *Modern Cryptography*, National Defense Industry Press, 2014.

[19] S. M. Ismail, L. A. Said, A. A. Rezk et al., "Biomedical image encryption based on double-humped and fractional logistic maps," in *Proceedings of the 6th International Conference on Modern Circuits and Systems Technologies, MOCAST 2017*, Greece, May 2017.

[20] J.-F. Zhao, S.-Y. Wang, L.-T. Zhang, and X.-Y. Wang, "Image encryption algorithm based on a novel improper fractional-order attractor and a wavelet function map," *Journal of Electrical and Computer Engineering*, vol. 2017, Article ID 8672716, 2017.

[21] P. Muthukumar, P. Balasubramaniam, and K. Ratnavelu, "A novel cascade encryption algorithm for digital images based on anti-synchronized fractional order dynamical systems," *Multimedia Tools and Applications*, pp. 1–22, 2016.

[22] G.-C. Wu, D. Baleanu, and Z.-X. Lin, "Image encryption technique based on fractional chaotic time series," *Journal of Vibration and Control*, vol. 22, no. 8, pp. 2092–2099, 2016.

[23] Z. Liu and T. Xia, "Novel two dimensional fractional-order discrete chaotic map and its application to image encryption," *Applied Computing and Informatics*, 2017.

[24] Z. Liu, T. Xia, and J. Wang, "Fractional two-dimensional discrete chaotic map and its applications to the information security with elliptic-curve public key cryptography," *Journal of Vibration and Control*, p. 107754631773471, 2017.

[25] F. M. Atici and P. W. Eloe, "A transform method in discrete fractional calculus," *International Journal of Difference Equations*, vol. 2, no. 2, pp. 165–176, 2007.

[26] T. Abdeljawad and D. Baleanu, "Fractional differences and integration by parts," *Journal of Computational Analysis and Applications*, vol. 13, no. 3, pp. 574–582, 2011.

[27] Y. Zhou, F. Chen, and X. Luo, "Existence results for nonlinear fractional difference equation," *Advances in Difference Equations*, vol. 2011, Article ID 713201, 2011.

[28] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

[29] Y. Xiao, *Research on Elliptic Curve Cryptography*, Huazhong University of Science and Technology Press, 2006.

[30] P. Li, L. Min, Y. Hu, G. Zhao, and X. Li, "Novel two dimensional discrete chaotic maps and simulations," in *Proceedings of the*

2012 IEEE 6th International Conference on Information and Automation for Sustainability, ICIAFS 2012, pp. 159–162, China, September 2012.

[31] M. M. Liu, T. C. Xia, and J. B. Wang, "A two dimensional fractional discrete chaos combined with triangle function," *Journal of Shanghai University (Natural Science Edition)*, 2017, pre-printed.

[32] G.-C. Wu and D. Baleanu, "Jacobian matrix algorithm for Lyapunov exponents of the discrete fractional maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 22, no. 1-3, pp. 95–100, 2015.

[33] F. M. Guo and L. Tu, *The Application of Chaotic Theory in Cryptography*, Beijing Institute of Technology Press, Beijing, China, 2015.

[34] D. Xiao, X. Liao, and P. Wei, "Analysis and improvement of a chaos-based image encryption algorithm," *Chaos, Solitons & Fractals*, vol. 40, no. 5, pp. 2191–2199, 2009.

[35] C. Li, S. Li, G. Chen, and W. A. Halang, "Cryptanalysis of an image encryption scheme based on a compound chaotic sequence," *Image and Vision Computing*, vol. 27, no. 8, pp. 1035–1039, 2009.

[36] R. Rhouma, E. Solak, and S. Belghith, "Cryptanalysis of a new substitution-diffusion based image cipher," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 7, pp. 1887–1892, 2010.

[37] Y. Zhang, D. Xiao, W. Wen, and M. Li, "Cryptanalyzing a novel image cipher based on mixed transformed logistic maps," *Multimedia Tools and Applications*, vol. 73, no. 3, pp. 1885–1896, 2014.

[38] C. Li, L. Y. Zhang, R. Ou, K.-W. Wong, and S. Shu, "Breaking a novel colour image encryption algorithm based on chaos," *Nonlinear Dynamics*, vol. 70, no. 4, pp. 2383–2388, 2012.

[39] Y. Zhang, D. Xiao, W. Wen, and H. Nan, "Cryptanalysis of image scrambling based on chaotic sequences and Vigenère cipher," *Nonlinear Dynamics*, vol. 78, no. 1, pp. 235–240, 2014.

[40] Y. Zhang, D. Xiao, W. Wen, and M. Li, "Breaking an image encryption algorithm based on hyper-chaotic system with only one round diffusion process," *Nonlinear Dynamics*, vol. 76, no. 3, pp. 1645–1650, 2014.

[41] L. Y. Zhang, C. Li, K.-W. Wong, S. Shu, and G. Chen, "Cryptanalyzing a chaos-based image encryption algorithm using alternate structure," *The Journal of Systems and Software*, vol. 85, no. 9, pp. 2077–2085, 2012.