Applied Computing and Informatics 14 (2018) 177–185

Contents lists available at ScienceDirect

Applied Computing and Informatics

journal homepage: www.sciencedirect.com

Original Article

Novel two dimensional fractional-order discrete chaotic map and its application to image encryption

Zeyu Liu *, Tiecheng Xia

Department of Mathematics, Shanghai University, Shangda Road 99, Baoshan District, Shanghai 200444, PR China

ARTICLE INFO

Article history:
Received 11 May 2017
Revised 20 June 2017
Accepted 13 July 2017
Available online 19 July 2017

Keywords:
Chaos
Discrete fractional calculus
Fractional 2D-TFCDM
Image encryption
Elliptic curve in finite field

ABSTRACT

A new fractional two dimensional triangle function combination discrete chaotic map (2D-TFCDM) is proposed by utilizing the discrete fractional calculus. Furthermore, the chaos behaviors are numerically discussed in the fractional-order difference. The bifurcation diagrams, the largest Lyapunov exponent plot and the phase portraits are shown, respectively. With the keys produced by elliptic curve in finite field, the discrete fractional map is converted into algorithm, and applied to color image encryption. The image encryption method is first proposed by us worldwide.

1. Introduction

In the past decade, the discrete dynamic behavior and its applications has been given a lot of attention in various applied areas owing to its potential applications in secure communication field [1,2]. On the basis of the time scale theory [3], Atici et al. has proposed the discrete fractional calculus (DFC) [4–6] to describe the dynamics of the discrete time, some results have been reported. The discrete memory effect of the system indicates that the momentum $x(n)$ depends on the past information $x(0),\ldots,x(n-1)$. There are many methods designed for the fractional difference models to prove that the DFC is an efficient tool to discretize the chaotic systems with a memory effect [10–12]. Wu and Baleanu [13–15] focus on applications of the discrete fractional calculus on an arbitrary time scale and utilized the theories of delta difference equations to reveal the discrete chaos behavior.

In order to understand the background of the discrete dynamics behaviors, our primary objective is to introduce applications of the discrete fractional calculus on an arbitrary time scale [4–6] and utilize the theories of delta difference equations to expose the discrete chaos behaviors of the fractionalized map. Some others refer to the applications of fractional fourier transform and fractional differential equations [7–9].

Public key cryptography (asymmetric cryptography) is a famous techniques for many years [16]. Strong public-key cryptography is often considered to be too computationally expensive for small devices if not accelerated by cryptographic hardware. Elliptic curves are popular settings for building efficient public key cryptosystems. Elliptic curve cryptography (ECC) is an popular effective public key cryptography techniques. ECC has many advantages, such as small storage capacity, faster computations and reduction of the power consumption [17]. Menezes Vanstone Elliptic Curve Cryptosystem (MVECC) was one of the famous techniques that used ECC and gave security for the data [18]. We take use of this technique in our paper and make it more adapted to image encryption and security.

There are many encryption methods proposed recently, such as [19–24]. Some others make use of fractional differential equation, like fractional logistic maps [25], fractional-order chaos systems [26] and fractional form of hyperchaotic system[27]. In [28], fractional-order difference has been proposed to apply in the image encryption based on fractional chaotic time series, while the new encryption method which utilizes two dimensional chaotic map based on fractional-order difference has seldom been proposed.

Our main aim is to introduce a new two dimensional discrete chaotic map on the basis of fractional-order difference and apply the map to information security. The paper is organized as follows: In Section 2, the definitions and the properties of the DFC are

* Corresponding author.
E-mail addresses: liuzeyu_90@163.com (Z. Liu), xiatc@t.shu.edu.cn (T. Xia).

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.aci.2017.07.002

introduced. In Section 3, we provide the introduction of elliptic curve in finite field. The working mechanism of the Menezes-Vanstone Elliptic Curve Cryptosystem is described in Section 4. Then, in the next section, we present fractional 2D-TFCDM and standard map on time scales from the discrete integral expression. The bifurcation diagrams, the largest Lyapunov exponent plot and the phase portraits of the map are also displayed while the difference orders and the initial points are changed. In Section 6, we display the applications of fractional 2D-TFCDM with the Menezes-Vanstone Elliptic Curve Cryptosystem in the image encryption. In Section 7, the results of applications in part VI are analyzed. At last, some conclusions are given.

2. Preliminaries

First, let us briefly revisit the definitions of the fractional sum and difference. Considering the DFC, the function $f(t)$ is changed as a sequence $f(n)$. Let $\mathbb{N}_a$ denotes the isolated time scale and $\mathbb{N}_a = \{a, a+1, a+2, \ldots\}$ ($a \in \mathbb{R}$ fixed). The difference operator Δ is defined as $\Delta f(n) = f(n+1) - f(n)$.

Definition 2.1 (*See [4]*). Let $u : \mathbb{N}_a\mathbb{R}$ and $0 < v$ be given. Then the fractional sum of v order is defined by

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

where a is the starting point, $t^{(v)}$ is the falling function defined as

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

Definition 2.2 (*See [29]*). For $0 < v, v \notin \mathbb{N}$ and $u(t)$ defined on $\mathbb{N}_a$, the Caputo-like delta difference is defined by

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

where v is the difference order.

Theorem 2.3 (*See [30]*). *For the delta fractional difference equation*

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

the equivalent discrete integral equation can be obtained as

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

where the initial iteration reads

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

The complex difference equation with long-term memory is obtained. Set the difference order $v = 1$, it can reduce to the classical one, but the integer one doesn't hold the discrete memory. The domain is changed from $\mathbb{N}_{a+m-v}$ to $\mathbb{N}_{a+m}$ in Eqs. (6)–(8), and the function $u(t)$ is preserved to define on the isolated time scale $\mathbb{N}_a$ in the fractional sums. Obviously, the discrete fractional calculus is a crucial tool in the initialization of the fractional difference equations.

3. Introduction to elliptic curve

Definition 3.1. An elliptic curve E defined over a prime field F_p is

$$E : y^2 \equiv x^3 + ax + b (mod\ p) \tag{7}$$

where $a, b \in F_p, p \neq 2, 3$ for which $4a^3 + 27b^2 \neq 0$. The elliptic curve group $E(F_p)$ denotes the set of points (x, y) that satisfy the elliptic curve Eq. (10) together with a special point O at infinity [31].

3.1. Elliptic curve operations

Assume $P = (x_1, y_1), Q = (x_2, y_2) \in E (P \neq Q), E$ is defined in Eq. (10). Then $R = (x_3, y_3) = P + Q \in E$ is defined as follows [16,31]:

$$P + Q = \begin{cases} R = (x_3, y_3), P \neq -Q, \\ O, x_1 = x_2 (mod\ p), y_1 + y_2 = 0 (mod\ p). \end{cases} \tag{8}$$

where

$$\begin{aligned} x_3 &\equiv (\lambda^2 - 2x_1)(mod\ p), \\ y_3 &\equiv (\lambda(x_1 - x_3) - y_1)(mod\ p). \end{aligned} \tag{9}$$

and

$$\lambda = \begin{cases} \dfrac{(y_2 - y_1)}{(x_2 - x_1)}, & P \neq Q, \\ \dfrac{3x_1^2 + a}{2y_1}, & P = Q. \end{cases} \tag{10}$$

If $k \in \mathbb{Z}$ and $P = (x, y) \in E$. The scalar multiplication can be defined by

$$kP = \underbrace{P + P + \cdots + P}_{k-times} \tag{11}$$

Let $P = (x, y)$, then the negative of the point P is $Q = -P = (x, -y)$ where $P + Q = O$ [16,31].

Definition 3.2. The order of an elliptic curve is defined as the number of points lies on the curve and denoted by $\#E$ [31].

Definition 3.3. Let P be an element of the elliptic curve group $E(F_p)$, then P is a generator point if $ord(P) = \#E$ [31] ($ord(P)$ is the smallest positive integer n such that $nP = O$).

4. Menezes-Vanstone Elliptic Curve Cryptosystem (MVECC)

When user A wants to send a message $x = (x_1, x_2) \in Z_p^* \times Z_p^*$ to user B, they need firstly to reach an agreement in the elliptic curve $E(F_p)$ and the base point α. Every party should choose a private key randomly, d for user A and k for user B ($0 \leqq d, k < ord(\alpha)$), and computes their public key $\beta = d \cdot \alpha$ and $y_0 = k \cdot \alpha$. User A computes the secret key $(c_1 \cdot c_2)$ by formula (15)

$$(c_1 \cdot c_2) = d \cdot y_0 = d \cdot k \cdot \alpha = k \cdot \beta \tag{12}$$

Then the ciphered message is calculated by

$$\begin{aligned} y_1 &= x_1 * c_1 mod\ p \\ y_2 &= x_2 * c_2 mod\ p \end{aligned} \tag{13}$$

And the ciphertext $\{y_0, (y_1, y_2)\}$ is sent to user B. When user B wants to decrypt the ciphertext (y_1, y_2), he needs firstly to compute the secret key by $k \cdot \beta = k \cdot d \cdot \alpha = (c_1, c_2)$, then computes the following

$$\begin{aligned} x_1 &= y_1 * c_1^{-1} mod\ p \\ x_2 &= y_2 * c_2^{-1} mod\ p \end{aligned} \tag{14}$$

to get the original message $x = (x_1, x_2)$ [18].

Any adversary who knows β and y_0 only without the private keys d and k is very difficult to solve the ECDLP and get the message x. Moreover, if $\#E$ have only one big prime divisor, solving the ECDLP is more difficult [31]. So, MVECC is an efficient and secure technique.

5. Fractional 2D-TFCDM

From the fractional calculus, we notice the application of the DFC to fractional generalizations of the discrete maps [13]. In recent paper [32], Li introduce the following 1st 2D-TFCDM

$$\begin{cases} x_{n+1} = a\cos(y_n), & a = 1.4, \\ y_{n+1} = bx_n\sin(y_n), & b = 4. \end{cases} \tag{15}$$

In this paper, considering the fractional generalization of $x(n)$, we modify the 1st 2D-TFCDM as a Caputo-like delta difference form

$$\begin{cases} {}^{C}\Delta_{\alpha}^{v}x(t) = a\cos(y(t+v)) - x(t+v), & 0 < v < 1, t \in N_{a+1-v}, \\ y_{n+1} = bx_n\sin(y_n), & b = 4. \end{cases} \tag{16}$$

From Theorem 2.5, we can get the following equivalent discrete numerical formula with $0 < v < 1$

$$\begin{cases} x(n) = x(0) + \frac{1}{\Gamma(v)}\sum_{j=1}^{n}\frac{\Gamma(n-j+v)}{\Gamma(n-j+1)}[a\cos(y(j-1)) - x(j-1)], \\ y(n) = bx(n-1)\sin(y(n-1)), b = 4. \end{cases} \tag{17}$$

Let $v = 1, x(0) = 0.19, y(0) = 0.06, n = 200$, we plot the bifurcation diagram of Fig. 1, where the step size of the a is set as 0.005. Fig. 2 is the bifurcation diagram while the difference order is $v = 0.8$. We can observe that the chaotic zones are clearly dependent on the changing difference order v. In Fig. 3, for $v = 1$, we get the largest lyapunov exponent using the Jacobian matrix algorithm. In somewhere, the largest lyapunov exponent LE1 is positive. It is corresponds to chaotic areas in Fig. 1.

We can also have the numerical formula for the variable b $(a = 1.4)$:

$$\begin{cases} y(n) = y(0) + \frac{1}{\Gamma(v)}\sum_{j=1}^{n}\frac{\Gamma(n-j+v)}{\Gamma(n-j+1)}[bx(j-1)sin(y(j-1)) - y(j-1)], \\ x(n) = a\cos(y(n-1)), \qquad a = 1.4. \end{cases} \tag{18}$$

Choose 401 different initial values and plot the $y(n)$ versus the $x(n)$ in one figure. In Fig. 4, the phase portraits of the integer map is

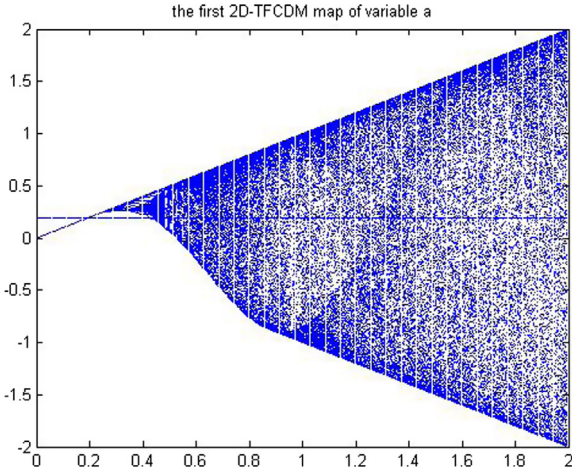


Fig. 1. The bifurcation diagram of the first 2D-TFCDM of the variable a for $v = 1$.

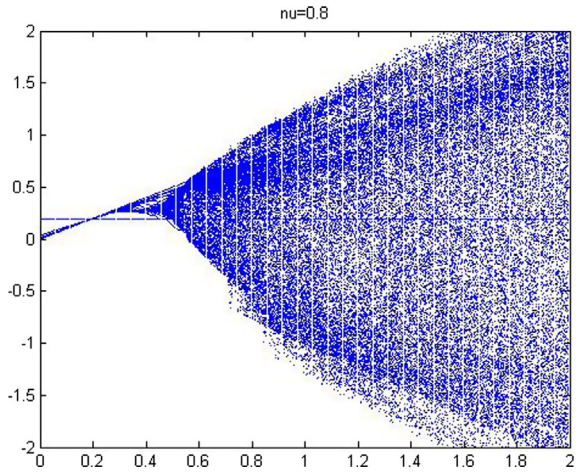


Fig. 2. The bifurcation diagram of the fractional first 2D-TFCDM of the variable a for $v = 0.8$.

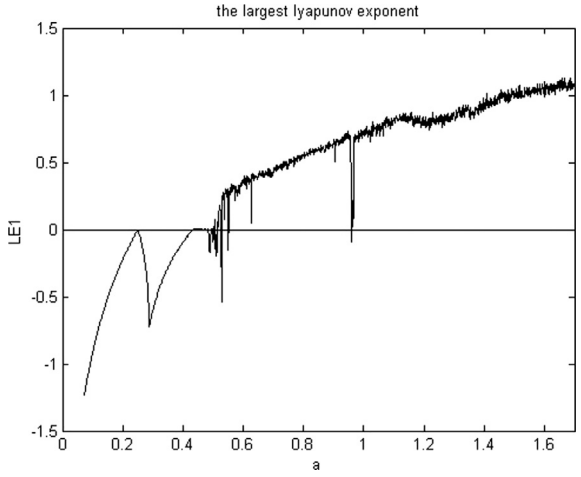


Fig. 3. The largest lyapunov exponent of the first 2D-TFCDM of the variable a.

derived. Then the cases with the fractional difference order $v = 0.8$ and $v = 0.6$ are considered in Figs. 5 and 6, respectively.

6. Applications

The fractionalized standard map can also be applied in information security fields. We make use of formula (17) as a algorithm and set the initial values x_0, y_0, the order v and the coefficients a, b of chaotic system as keys for R, G, B components, respectively, where R, G and B component represent the red, green and blue color matrix of an plain image.

6.1. Generation of new keys based on elliptic curve in a finite field

Let elliptic curve E defined over F_{100927} with parameters $a = 1, b = 6$ in (7). Since $\#E = 100,829$ is a prime, According to [31], it is a safe elliptic curve. set $x = (x_1, x_2) = (95, 364, 5113)$, $\alpha = (2, 4), d = 91,338$, then $d\alpha = (54, 157, 1425) = \beta$, the secret key $k = 63,236, (c_1, c_2) = k\beta = (84, 416, 20, 597) = d\gamma, \gamma = k\alpha = (20, 607, 18, 966)$. $v = 9.536405113$

$$\begin{aligned} v'_{01} &= c_1 * v_{01} mod\ p = 84,416 \cdot 95,364 mod 100,927 = 7123 mod 100,927, \\ v'_{02} &= c_2 * v_{02} mod\ p = 20,597 \cdot 5113 mod 100,927 = 45,600 mod 100,927. \end{aligned} \tag{19}$$

Then, the ciphertext is $((20, 369, 92, 263), 7123, 45, 600)$, $v' = \frac{v'_{01}}{10,000} + \frac{v'_{02}}{10^9} = 0.7123456$ as the key of next step encryption.

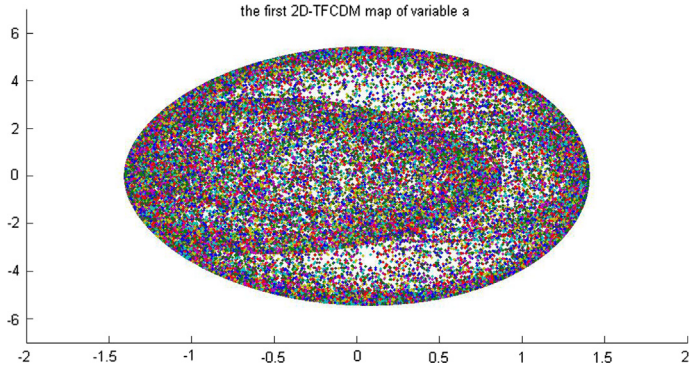


Fig. 4. The phase portraits of the first 2D-TFCDM for a = 1.4, b = 4 and $v = 1$.

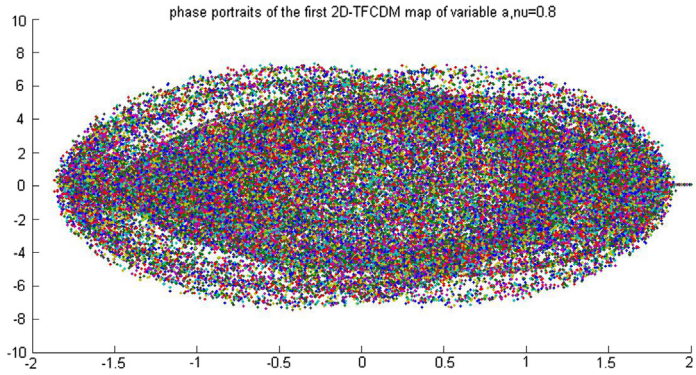


Fig. 5. The phase portraits of the first 2D-TFCDM for a = 1.4, b = 4 and $v = 0.8$.

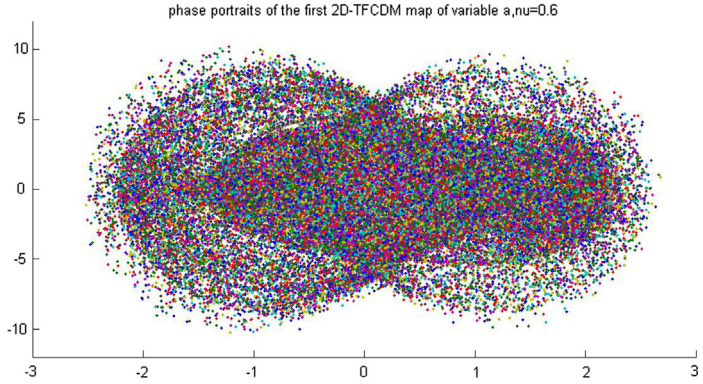


Fig. 6. The phase portraits of the first 2D-TFCDM for a = 1.4, b = 4 and $v = 0.6$.

$x_0 = 4.0301, y_0 = 2.7955, k_1 = 6.8541, k_2 = 8.0623$, set $x_{01} = x_0 \times 10^4, y_{01} = y_0 \times 10^4, k_{01} = k_1 \times 10^4, k_{02} = k_2 \times 10^4$, then

$$\begin{aligned} x'_{01} &= c_1 \cdot x_{01} mod 100,927 = 84,416 \cdot 40,301 mod 100,927 = 1900 mod 100,927, \\ y'_{01} &= c_2 \cdot y_{01} mod 100,927 = 20,597 \cdot 27,955 mod 100,927 = 600 mod 100,927, \\ k'_{01} &= c_1 \cdot k_{01} mod 100,927 = 84,416 \cdot 68,541 mod 100,927 = 14,000 mod 100,927, \\ k'_{02} &= c_2 \cdot k_{02} mod 100,927 = 20,597 \cdot 80,623 mod 100,927 = 40,000 mod 100,927. \end{aligned} \tag{20}$$

set $x'_0 = \frac{x'_{01}}{10^4} = 0.19, y'_0 = \frac{y'_{01}}{10^4} = 0.06, k'_1 = \frac{k'_{01}}{10^4} = 1.4, k'_2 = \frac{k'_{02}}{10^4} = 4$, as the keys of next step encryption.

6.2. Permutation procedure based on fractional 2D-TFCDM

The procedure of permutation can be divided into 4 steps:

1. Set $x(1)$ equal to initial value x_0, do iteration test for $MN-1$ times by utilizing formula (17), here M and N are length and width of the original picture V, respectively. Generate the one dimensional real number chaotic sequences $x(i), i = 1, 2, \ldots, MN$.
2. Reorder $x(k)$ by the bubble sort, then get $x'(k)$ and record the change of the subscript of $x(k)$ as $z(k)$.
3. Change $M \times N$ original picture V into $1 \times MN$ sequence $v(k)$, here $k = N(m-1)+n, (m = 1, 2 \ldots, M, n = 1, 2 \ldots, N)$, reorder $v(k)$ similarly to $x(k)$ according to $z(k)$ and get $v'(k)$.
4. Change $v'(k)$ into $m \times n$ figure as V', where V' is the encrypted figure we needed.

Reverse this process, we can get the original figure.

6.3. Encryption method based on fractional 2D-TFCDM

The procedure of encryption can be divided into 4 steps:

1. Generate chaotic sequence $x(i)$ to permutate the original image V into V' as described in Section 6.2. Change $M \times N$ original picture V' into $1 \times MN$ sequence $u(i)$, here $i = N(m-1)+n, (m = 1, 2 \ldots, M, n = 1, 2 \ldots, N)$. Another $M \times N$ image is used as a key or cover image (K-image). Also change the K-image into $1 \times MN$ sequence $w(i)$.
2. Set $i = 0$.
3. Retain only the integer part of $x(i) \times 10^8$ as $x_1(i)$, do modulus operation mod between $x_1(i)$ and 256, then we get
$$x_2(i) = mod(x_1(i), 256). \tag{21}$$
4. Consider the following formula:
$$u'(i) = u(i) \oplus mod(w(i) + x_2(i), 256). \tag{22}$$
where $\oplus$ is the xor operation, and $u'(i)$ is the encrypted pixel value.
The inverse form of (22) is
$$u(i) = u'(i) \oplus mod(w(i) + x_2(i), 256). \tag{23}$$
5. Compute the number k according to the following formula:
$$k(i) = 1 + mod(u'(i), 256). \tag{24}$$
then, iterate the formula (20) for $k(i)$ times, to get the new $x(i+1)$, return to step 3, until $i = MN$.
6. Change $u'(i)$ into $M \times N$ figure as V'', here V'' is the finally encrypted figure we needed.

The decryption procedure can be divided into the parts as follows:

1. Do the same step as in encryption unless the formula (22) is changed to use formula (23).
2. Reverse the procedure in Section 6.2 to remove the permutation effect.

Fig. 7 display the process of encryption of proposed algorithm, the working principle of S box is illustrated in Fig. 8.

The original, encryption and decryption of a image are shown in Fig. 9(a), (b) and (c) as Lena, the figure size is 512×512. Another 4 cases are displayed in supplementary material.

In the process of encryption and decryption of Section 6.3, the keys are the same. Moreover, owing to the coupling structure of the algorithm, the chaotic sequences depend on each other. These features strengthen the encryption algorithm security, and make the encryption algorithm more robust.

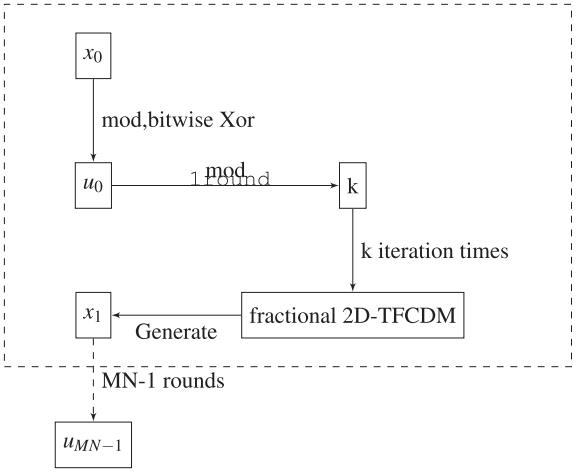


Fig. 8. The S Box.

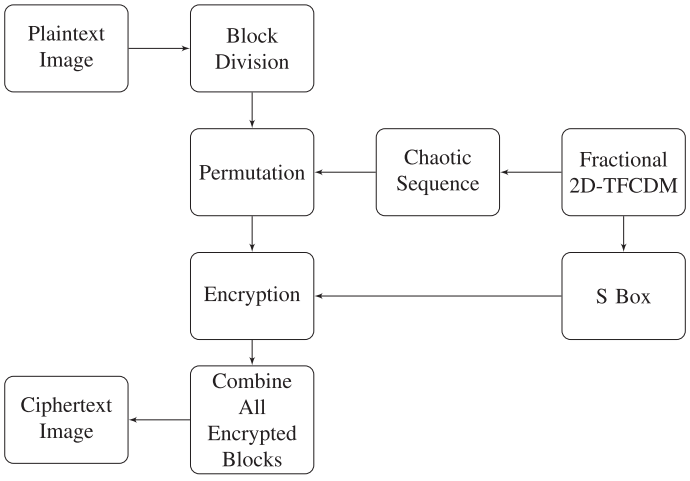
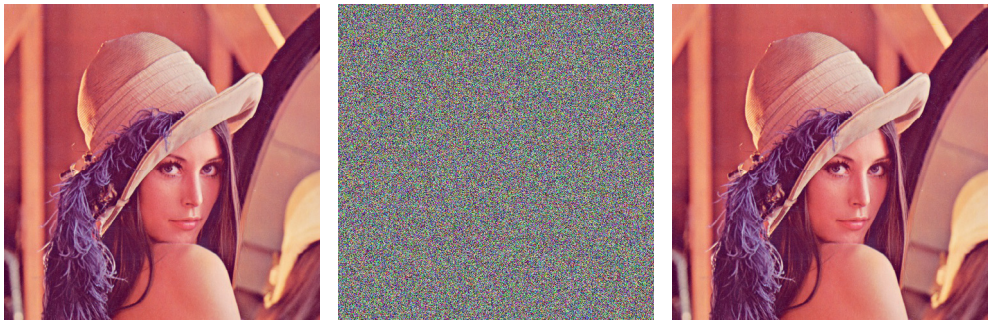


Fig. 7. The proposed encryption method.



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

Fig. 9. Lena.

7. Analysis of results in applications

7.1. Key sensitivity

In this algorithm, the order, the initial values and the coefficients of chaotic system can be utilized as the secret keys, implying that there are five secret keys (x_0, y_0, v, k_1, k_2). If the precision of x_0 is 2×10^{-17}, the precision of y_0, v, k_1 and k_2 are $4 \times 10^{-18}, 6 \times 10^{-17}, 1.2 \times 10^{-16}$ and 5×10^{-16}, respectively, then the secret key's space is $(2 \times 10^{-17} \times 4 \times 10^{-18} \times 6 \times 10^{-17} \times 1.2 \times 10^{-16} \times 5 \times 10^{-16})^{-1} \approx 3.47 \times 10^{81} \approx 0.92 \times 2^{271}$. If the size of original image is 512×512, the key space of K-image is $512 \times 512 \times 2^8 = 2^{26}$. The total key space is 0.92×2^{297}.

7.2. Statistics analysis

The statistical property is significant to an encrypted image and a good encryption method should be robust against any statistical attacks.

7.2.1. Correlation of the plain and cipher images

In an ordinary image, the correlation coefficient of adjacent pixels is always high for the reason that the adjacent pixels values are close. A good encryption algorithm should make the correlation of adjacent pixels nearly equal to zero. The correlation coefficients are calculated in vertical, horizontal and diagonal directions by Eq. (25), then the results are displayed in Table 1. The correlation in the original figure and the encrypted figure of Lena along the x directions are shown in Fig. 10.

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

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{26}$$

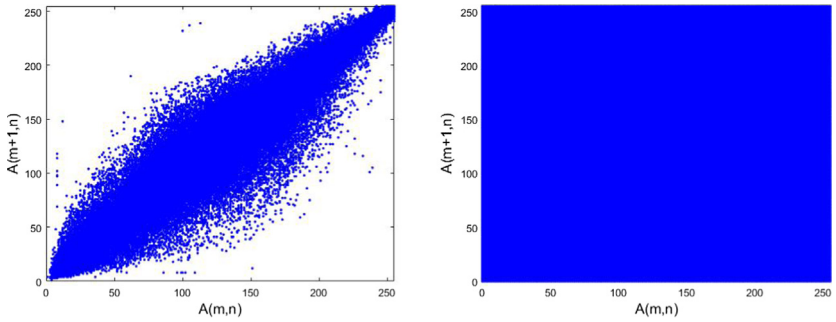
$$E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i \tag{27}$$

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

It is evident to see that the correlation of original image has a linear relationship, while that of the encrypted image is stochastic. Table 1 indicates that the correlation coefficients of encrypted image are nearly 0, compared with the correlation coefficients of original image are all bigger than 0.9, some one is nearly 1. It can be concluded that the encryption process makes the pixels of the image almost independent with each other.

Table 1
The results of correlation coefficients of image.

Image		Original image			Encrypted image		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	R	0.9387	0.9556	0.9168	0.0083	0.0063	−0.0037
	G	0.9325	0.9469	0.9139	−0.0015	−0.0074	0.0053
	B	0.9217	0.9387	0.8873	−0.0019	0.0013	−0.0014



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

Fig. 10. Analysis of the correlations of Lena.

Table 2
Comparison of correlation coefficients of image.

Algorithm	Image	Original Image			Encrypted Image		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Proposed	Lena	0.9792	0.9888	0.9653	−0.0028	0.0081	0.0091
	Lake	0.9657	0.9630	0.9401	0.0071	−0.0080	0.0060
[19]	Lena	0.9503	0.9755	0.9275	−0.0226	0.0041	0.0368
[20]	Lena	0.927970	0.926331	0.839072	−0.010889	−0.018110	−0.006104
[23]	Lena	0.946	0.973	0.921	−0.0055	−0.0075	0.0026
	Lake	0.958	0.958	0.929	−0.0025	0.00977	0.0127
[24]	Lena	0.9569	0.9236	0.9019	0.0042	−0.0043	0.0163
	Lake	0.9377	0.9403	0.9100	0.0231	0.0140	0.0097

In Table 2, it can be observed from the statistical data that the proposed scheme are better than the encryption method proposed in other references.

7.2.2. Histogram

The distribution of colors inside the image is described by the histogram. An ordinary image has the regular histogram and it can provide the attackers with effective information. Consequently, the colors inside the encrypted image should be uniformly distributed with a good image encryption method. Fig. 11 shows the histogram of Airplane in original, encrypted and decrypted 3 stages.

Obviously, the histogram of encrypted image is nearly uniformly distributed compared with the histogram of original image, so that the encryption method can resist statistical attack.

7.2.3. Information entropy

Entropy is a measure of unpredictability of information content. The information entropy is the most important characteristic of randomness and it is used to indicate the degree of uncertainty of a system. It is defined as:

$$H(m) = \frac{1}{N}\sum_{i=0}^{2^n-1} p(m_i) log_2 \frac{1}{p(m_i)} \tag{29}$$

where $p(m_i)$ expresses the probability of symbol m. For the pixels, values of the image are between $0 \sim 255$. According to Eq. (29), the ideal information entropy is 8 bits for an ideally random image. Therefore, the closer to 8 bits the information entropy, the better the encryption scheme. The information entropy of the encrypted images are shown in Table 3.

Table 4 gives the comparison of information entropy. In contrast with other algorithms, the result implies that the encrypted images of proposed algorithm are closer to the random images. All the above is enough to prove that the proposed encryption method has the ability to resist statistical attack.

Table 3
The results of information entropy.

Image		Information entropy	
		Original image	Encrypted image
Lena	R	7.2531	7.9993
	G	7.5952	7.9993
	B	6.9686	7.9992

Table 4
Comparison of information entropy.

Algorithm	Image	Original	Encrypted
Proposed	Lena	7.2531	7.9993
[19]	Lena	7.2072	7.9973
[22]	Lena	Undefined	7.9972
[25]	Lena	Undefined	7.987918
[26]	Lena	7.447144	7.988847

7.3. Sensitivity analysis

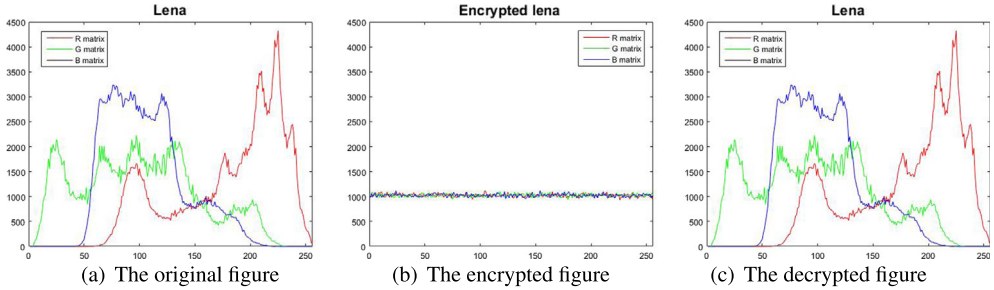
There are two different criteria for measuring the range between two images: Number of pixels change rate (NPCR) and unified average changing intensity (UACI), as defined by Eqs. (31) and (32).

$$D(i,j) = \begin{cases} 0, T_1(i,j) = T_2(i,j) \\ 1, T_1(i,j) \neq T_2(i,j). \end{cases} \tag{30}$$

$$NPCR = \frac{\sum_{i=1}^{W}\sum_{j=1}^{H} D(i,j)}{W \times H} \times 100\% \tag{31}$$

$$UACI = \frac{\sum_{i=1}^{W}\sum_{j=1}^{H} |T_1(i,j) - T_2(i,j)|}{255W \times H} \times 100\% \tag{32}$$

where W and H represent the width and the height of the image, respectively. T_1 and T_2 represent two analyzed images.



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

Fig. 11. The histogram of Lena.

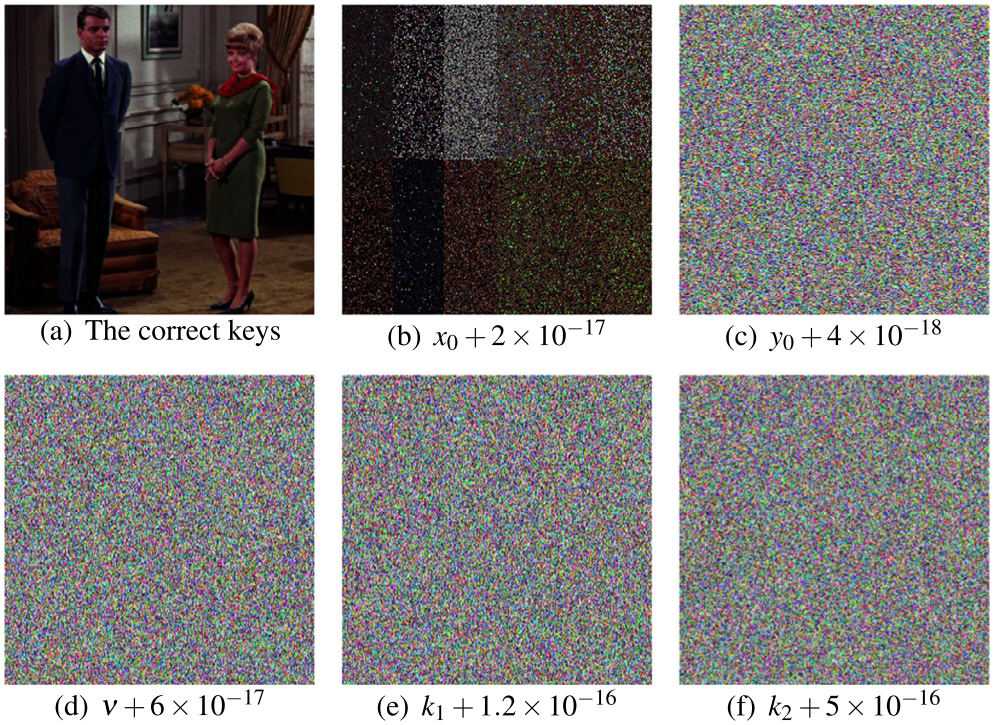


Fig. 12. The test of key sensitivity.

7.3.1. Key sensitivity

We encrypt the image by using the keys $x_0 = 0.19, y_0 = 0.06, v = 0.7123456, k_1 = 1.4$ and $k_2 = 4$. Fig. 12(a) represents the decrypted image by the correct keys. Fig. 12(b) represents the decrypted image under 2×10^{-17} adding in x_0 and other secret keys unchanged. The decrypted image is quite different from the original image. Similarly, the secret keys y_0, v, k_1, k_2 are added $4 \times 10^{-18}, 6 \times 10^{-17}, 1.2 \times 10^{-16}$ and 5×10^{-16} and shown in Fig. 12(c)–(f), respectively. The NPCR and UACI between Fig. 12 (a) and (b)–(f) are calculated in Table 6, separately.

Table 5
Comparison of key spaces.

Algorithm	Proposed	[20]	[22]	[24]
Key spaces	$2.33 \times 10^{89} (0.92 \times 2^{297})$	2^{128}	$\approx 2^{273}$	2^{276}

Table 6
NPCR and UACI between Fig. 12(a) and (b)–(f).

	NPCR and UACI	
Image	NPCR(%)	UACI(%)
12(b)	96.10	11.19
12(c)	99.49	40.23
12(d)	99.57	40.17
12(e)	99.60	40.12
12(f)	99.57	40.28

Compared with other algorithms, the encryption method has the ability to resist exhaustive attack. Table 5 present the result of comparison of key spaces. In Table 6, It can be observed that all NPCR are higher than 95% as well as near to the ideal value 99.61%, most of UACI are near to the ideal value 33.46%. We cannot recognize the object inside Fig. 12(b)–(f), therefore the encryption method is sensitive to the secret keys.

7.3.2. Plaintext sensitivity

A good encryption method should ensure that the two encrypted images are completely different even if the two original figures have only one pixel difference. Because of that the attackers

Table 8
Comparison of NPCR and UACI of image.

Algorithm	Image	NPCR (%)	UACI (%)
Proposed	Lena	99.61	33.47
	Lake	99.61	33.47
[19]	Lena	99.61	33.53
[20]	Lena	99.6429	33.3935
[21]	Lena	99.6304	33.5989
[23]	Lena	99.932	39.520
	Lake	99.85	40.303
[25]	Lena	75.62561	34.84288
[26]	Lena	99.6091	33.5038
[27]	Lena	99.6330	34.1319

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

	NPCR and UACI of Lena			
Image	NPCR (1-round%)	UACI (1-round%)	NPCR (2-round%)	UACI (2-round%)
Fig. 9(a) (30,30)	98.24	33.04	99.61	33.46
Fig. 9(a) (50,50)	94.09	31.62	99.60	33.50
Fig. 9(a) (80,80)	94.86	31.93	99.62	33.48
Fig. 9(a) (100,100)	98.02	32.93	99.60	33.44

can obtain informations by encrypting two original images of one pixel difference and comparing the two encrypted images.

The results are shown in Table 7, Fig. 9(a) (x, y) indicates that the pixel value of coordinate (x, y) is changed in Fig. 9(a) as the original image and then encrypted by the proposed encryption method, the NPCR and UACI are calculated with the formulas (31) and (32).

From Table 7, the NPCR and UACI of encrypted images with 2 round encryption are all near to the ideal value 99.61% and 33.46%, respectively. As a consequence, the encryption method has good property in plaintext sensitivity.

Table 8 compares the proposed encryption method with other methods by computing the NPCR and UACI. It is obvious that our method is more superior than other method.

7.4. Resistance to known-plaintext and chosen-plaintext attacks

In Section 6.3, the last round encrypted image pixel can determine the iteration times of the next round. In Eq. (22), $x_2(i)$, produced from the fractional 2D-TFCDM, dependent on the iteration times $k(i-1)$, determines the iteration times $k(i)$. Therefore, the corresponding keystream is not the same when different plaintext are encrypted. By encrypting some special images, the attacker cannot obtain useful information since the resultant information is related to those chosen-images. In consequence, the attacks proposed in Refs. [33–35] become ineffective on this new scheme. The proposed scheme can primely resist the known-plaintext and the chosen-plaintext attacks.

8. Conclusion

Fractional 2D-TFCDM is obtained from the 2D-TFCDM. Then, new chaotic dynamics behaviors is found with the map. Furthermore, the map can be applied in encryption and decryption of image transmission in information security. The results show that the DFC is an efficient tool for fractional generations of the discrete maps. We believe that the fractional calculus methods and fractional discrete formula will give us a better description of discrete fractional dynamics in future. From our research, we discovered that no paper has been reported on information security of fractional difference.

Acknowledgment

The Project supported by the Natural Science Foundation of China (Grant Nos. 61072147, 11271008).

Appendix A. Supplementary material

Supplementary data associated with this article can be found, in the online version, at http://dx.doi.org/10.1016/j.aci.2017.07.002.

References

[1] N.K. Pareek, V. Patidar, K.K. Sud, Image encryption using chaotic logistic map, Image Vis. Comput. 24 (9) (2006) 926–934.
[2] S. Behnia, A. Akhshani, H. Mahmodi, A. Akhavan, A novel algorithm for image encryption based on mixture of chaotic maps, Chaos Soliton Fract. 35 (2) (2008) 408–419.
[3] M. Bohner, A. Peterson, Dynamic Equations on Time Scales: An Introduction with Applications, Springer Science & Business Media, 2012.
[4] F.M. Atici, P.W. Eloe, A transform method in discrete fractional calculus, Int. J. Diff. Eqs. 2 (2) (2007) 165–176.
[5] F.M. Atici, P.W. Eloe, Initial value problems in discrete fractional calculus, Proc. Am. Math. Soc. 137 (3) (2009) 981–989.
[6] F.M. Atici, S. Sengul, Modeling with fractional difference equations, J. Math. Anal. Appl.. 369 (1) (2010) 1–9.
[7] Y.D. Zhang, S.H. Wang, G. Liu, J. Yang, Computer-aided diagnosis of abnormal breasts in mammogram images by weighted-type fractional Fourier transform, Adv. Mech. Eng. 8 (2) (2016), 1687814016634243.
[8] X.J. Yang, H.M. Srivastava, D.F. Torres, Y. Zhang, Non-differentiable solutions for local fractional nonlinear Riccati differential equations, Fundam. Inform. 151 (1–4) (2017) 409–417.
[9] S. Wang, M. Yang, J. Li, X. Wu, H. Wang, B. Liu, Z. Dong, Y. Zhang, Texture analysis method based on fractional Fourier entropy and fitness-scaling adaptive genetic algorithm for detecting left-sided and right-sided sensorineural hearing loss, Fundam. Inform. 151 (1–4) (2017) 505–521.
[10] T. Abdeljawad, D. Baleanu, Fractional differences and integration by parts, J. Comput. Anal. Appl. 13 (3) (2011).
[11] M.T. Holm, The Laplace transform in discrete fractional calculus, Comput. Math. Appl. 62 (3) (2011) 1591–1601.
[12] C.S. Goodrich, Existence of a positive solution to a system of discrete fractional boundary value problems, Appl. Math. Comput. 217 (9) (2011) 4740–4753.
[13] G.C. Wu, D. Baleanu, S.D. Zeng, Discrete chaos in fractional sine and standard maps, Phys. Lett. A 378 (5) (2014) 484–487.
[14] G.C. Wu, D. Baleanu, Discrete chaos in fractional delayed logistic maps, Nonlinear Dynam. 80 (4) (2015) 1697–1703.
[15] G.C. Wu, D. Baleanu, Discrete fractional logistic map and its chaos, Nonlinear Dynam. 75 (1–2) (2014) 283–287.
[16] C.X. Xu, Modern Cryptography, Tsinghua University Press, 2015.
[17] M.F. Fu, C. Wei, Elliptic curve cryptosystem ElGamal encryption and transmission scheme, in: 2010 International Conference on Computer Application and System Modeling (ICCASM 2010), IEEE, 2010, 6: V6-51-V6-53.
[18] C.G. Ma, Modern Cryptography, National Defense Industry Press, 2014.
[19] L. Xu, X. Gou, Z. Li, J. Li, A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion, Opt. Lasers Eng. 91 (2017) 41–52.
[20] L. Teng, X. Wang, J. Meng, A chaotic color image encryption using integrated bit-level permutation, Multimedia Tools Appl. (2017) 1–14.
[21] R. Enayatifar, A.H. Abdullah, I.F. Isnin, A. Altameem, M. Lee, Image encryption using a synchronous permutation-diffusion technique, Opt. Lasers Eng. 90 (2017) 146–154.
[22] Y. Li, C. Wang, H. Chen, A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation, Opt. Lasers Eng. 90 (2017) 238–246.
[23] S. Chakraborty, A. Seal, M. Roy, K. Mali, A novel lossless image encryption method using DNA substitution and chaotic logistic map, Int. J. Secur. Appl. 10 (2) (2016) 205–216.
[24] N. Zhou, S. Pan, S. Cheng, Z. Zhou, Image compression – encryption scheme based on hyper-chaotic system and 2D compressive sensing, Opt. Laser Technol. 82 (2016) 121–133.
[25] S.M. Ismail, L.A. Said, A.A. Rezk, A.G. Radwan, A.H. Madian, M.F. Abu-ElYazeed, A.M. Soliman, Biomedical image encryption based on double-humped and fractional logistic maps, in: 2017 6th International Conference on Modern Circuits and Systems Technologies (MOCAST), IEEE, May 2017, pp. 1–4.
[26] J.F. Zhao, S.Y. Wang, L.T. Zhang, X.Y. Wang, Image encryption algorithm based on a novel improper fractional-order attractor and a wavelet function map, J. Electr. Comput. Eng. 2017 (2017).
[27] P. Muthukumar, P. Balasubramaniam, K. Ratnavelu, A novel cascade encryption algorithm for digital images based on anti-synchronized fractional order dynamical systems, Multimedia Tools Appl. (2016) 1–22.
[28] G.C. Wu, D. Baleanu, Z.X. Lin, Image encryption technique based on fractional chaotic time series, J. Vib. Contr. 22 (8) (2016) 2092–2099.
[29] T. Abdeljawad, On Riemann and Caputo fractional differences, Comput. Math. Appl. 62 (3) (2011) 1602–1611.
[30] F. Chen, X. Luo, Y. Zhou, Existence results for nonlinear fractional difference equation, Adv. Diff. Eq. 2011 (2011).
[31] Y.A. Xiao, Research on Elliptic Curve Cryptography, Huazhong University of Science and Technology Press, 2006.
[32] P. Li, L. Min, Y. Hu, G. Zhao, X. Li, Novel two dimensional discrete chaotic maps and simulations, in: 2012 IEEE 6th International Conference on Information and Automation for Sustainability, 2012.
[33] D. Xiao, X. Liao, P. Wei, Analysis and improvement of a chaos-based image encryption algorithm, Chaos Soliton Fract. 40 (5) (2009) 2191–2199.
[34] C. Li, S. Li, G. Chen, W.A. Halang, Cryptanalysis of an image encryption scheme based on a compound chaotic sequence, Image Vis. Comput. 27 (8) (2009) 1035–1039.
[35] R. Rhouma, E. Solak, S. Belghith, Cryptanalysis of a new substitution – diffusion based image cipher, Commun. Nonlinear Sci. Numer. Simul. 15 (7) (2010) 1887–1892.