[Applied Computing and Informatics 14 (2018) 177–185](http://dx.doi.org/10.1016/j.aci.2017.07.002)



Contents lists available at [ScienceDirect](http://www.sciencedirect.com/science/journal/22108327)

Applied Computing and Informatics

journal homepage: [www.sciencedirect.com](http://www.sciencedirect.com/)

Original Article

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



Zeyu Liu [⇑](#_bookmark0), Tiecheng Xia

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

# a r t i c l e i n f o

*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

# a b s t r a c t

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.

© 2017 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University. This is an

open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

1. Introduction

In the past decade, the discrete dynamic behavior and its appli- cations has been given a lot of attention in various applied areas owing to its potential applications in secure communication field [[1,2]](#_bookmark48). On the basis of the time scale theory [[3]](#_bookmark56), Atici et al. has pro- posed the discrete fractional calculus (DFC) [[4–6]](#_bookmark36) 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); ... ; *x*(*n* — 1). There are many methods designed for the frac-

tional difference models to prove that the DFC is an efficient tool to discretize the chaotic systems with a memory effect [[10–12]](#_bookmark36). Wu and Baleanu [[13–15]](#_bookmark36) focus on applications of the discrete frac- tional 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]](#_bookmark36) and uti- lize the theories of delta difference equations to expose the dis-

\* Corresponding author.

*E-mail addresses:* [liuzeyu\_90@163.com](mailto:liuzeyu_90@163.com) (Z. Liu), [xiatc@t.shu.edu.cn](mailto:xiatc@t.shu.edu.cn) (T. Xia).

Peer review under responsibility of King Saud University.

**Production and hosting by Elsevier**

crete chaos behaviors of the fractionalized map. Some others refer to the applications of fractional fourier transform and frac- tional differential equations [[7–9]](#_bookmark36).

Public key cryptography (asymmetric cryptography) is a famous techniques for many years [[16]](#_bookmark37). 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 cryp- tosystems. 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]](#_bookmark38). Menezes Vanstone Elliptic Curve Cryptosystem (MVECC) was one of the famous techniques that used ECC and gave security for the data [[18]](#_bookmark39). We take use of this technique in our paper and make it more adapted to image encryp- tion and security.

There are many encryption methods proposed recently, such as [[19–24]](#_bookmark40). Some others make use of fractional differential equation, like fractional logistic maps [[25]](#_bookmark46), fractional-order chaos systems

[[26]](#_bookmark47) and fractional form of hyperchaotic system[[27]](#_bookmark49). In [[28]](#_bookmark50), 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 chao- tic 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](#_bookmark1), the definitions and the properties of the DFC are

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

2210-8327/© 2017 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University.

This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

introduced. In Section [3](#_bookmark2), 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](#_bookmark4). 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 differ- ence orders and the initial points are changed. In Section [6](#_bookmark10), we dis- play the applications of fractional 2D-TFCDM with the Menezes- Vanstone Elliptic Curve Cryptosystem in the image encryption. In Section [7](#_bookmark20), the results of applications in part VI are analyzed. At last, some conclusions are given.

1. Preliminaries
2. Introduction to elliptic curve

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

*E* : *y*2 Ξ *x*3 + *ax* + *b*(*mod p*) (7)

where *a*; *b* ∈ *Fp*; *p* – 2; 3 for which 4*a*3 + 27*b*2 – 0. The elliptic curve group *E*(*Fp*) denotes the set of points (*x*; *y*) that satisfy the elliptic curve Eq. [(10)](#_bookmark3) together with a special point *O* at infinity [[31]](#_bookmark53).

* 1. *Elliptic curve operations*

Assume *P* = (*x*1; *y*1); *Q* = (*x*2; *y*2) ∈ *E*(*P* – *Q* ); *E* is defined in Eq.

[(10)](#_bookmark3). Then *R* = (*x*3; *y*3) = *P* + *Q* ∈ *E* is defined as follows [[16,31]](#_bookmark37):

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 N*a* denotes the isolated time scale and

N*a* = {*a*; *a* + 1; *a* + 2; .. .} (*a* ∈ R fixed). The difference operator D

is defined as D*f* (*n*)= *f* (*n* + 1)— *f* (*n*).

*P* + *Q* = *R* = (*x*3; *y*3 ); *P* – — *Q* ;

*O*; *x*1 = *x*2(*mod p*); *y*1 + *y*2 = 0(*mod p*).

where

*x*3 Ξ (*k*2 — 2*x*1)(*mod p*);

(8)

*y* Ξ (*k*(*x*

(9)

— *x* )— *y* )(*mod p*).

Definition 2.1 (*See* [*[4]*](#_bookmark36)). Let *u* : N*a*R and 0 < *m* be given. Then the fractional sum of *m* order is defined by

8>>< ; – ;

3

and

1 3 1

*t*—*m*

(*y*2 — *y*1) *P Q*

(*x*2 — *x*1)

D—*mu*(*t*) := 1 X(*t* — *s* — 1)*m*—1*u*(*s*); *t* ∈ N*a m*; (1)

*a*

>

1

+

*k* = 3*x*2 + *a*

## (10)

C(*m*) *s*=*a*

where *a* is the starting point, *t*(*m*) is the falling function defined as

>: 2*y*1

; *P* = *Q* .

*t*(*m*) = C(*t* + 1) . (2)

If *k* ∈ Z and *P* = (*x*; *y*) ∈ *E*. The scalar multiplication can be

defined by

C(*t* + 1 — *m*)

Definition 2.2 (*See* [*[29]*](#_bookmark51)). For 0 *m m*

<

;

and *u t*

R N

( )

defined on ,

N*a*

*kP* = *P* + *P* +· · · + *P*

## |ﬄﬄﬄﬄﬄﬄﬄﬄ*k*ﬄﬄ—ﬄﬄ{*ti*z*m*ﬄ*e*ﬄﬄ*s*ﬄﬄﬄﬄﬄﬄﬄﬄﬄ}

Let *P* = (*x*; *y*), then the negative of the point *P* is *Q* = —*P* = (*x*; —*y*)

(11)

the Caputo-like delta difference is defined by

*C* D*mu*(*t*) := D—(*m*—*m*)D*mu*(*t*)

1 X*t*—(*m*—*m*)

*a a*

= (*t* — *s* — 1)(*m*—*m*—1)D*mu*(*s*);

C(*m* — *m*)

*s*=*a*

*t* ∈ N*a*+*m*—*m*; *m* = [*m*]+ 1; (3)

where *m* is the difference order.

Theorem 2.3 (*See* [*[30]*](#_bookmark52)). *For the delta fractional difference equation*

*C* D*mu*(*t*)= *f* (*t* + *m* — 1; *u*(*t* + *m* — 1)); D*ku*(*a*)= *uk*;

*a*

## *m* = [*m*]+ 1; *k* = 0; .. . ; *m* — 1 (4)

where *P* + *Q* = *O* [[16,31]](#_bookmark37).

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]](#_bookmark53).

Definition 3.3. Let *P* be an element of the elliptic curve group *E*(*Fp*), then *P* is a generator point if *ord*(*P*) = #*E* [[31]](#_bookmark53) (*ord*(*P*) is the smallest positive integer *n* such that *nP* = *O*).

1. Menezes-Vanstone Elliptic Curve Cryptosystem (MVECC)

When user A wants to send a message *x* = (*x*1; *x*2) ∈ Z\* × Z\* to

*p p*

*the equivalent discrete integral equation can be obtained as*

*t*—*m*

1 X

*x*(*n*)= *u*0(*t*)+ (*t* — *s* — 1)(*m*—1)

C(*m*) *s*=*a*+*m*—*m*

× *f* (*s* + *m* — 1; *u*(*s* + *m* — 1)); *t* ∈ N*a*+*m*; (5)

*where the initial iteration reads*

user *B*, they need firstly to reach an agreement in the elliptic curve *E*(*Fp*) and the base point *a*. Every party should choose a private key randomly, *d* for user *A* and *k* for user *B* (05*d*; *k* < *ord*(*a*)), and com- putes their public key *b* = *d* · *a* and *y*0 = *k* · *a*. User *A* computes the secret key (*c*1 · *c*2) by formula [(15)](#_bookmark6)

(*c*1 · *c*2)= *d* · *y*0 = *d* · *k* · *a* = *k* · *b* (12)

Then the ciphered message is calculated by

*m*—1 (*k*)

*k*=0

*k*!

*u*0(*t*)= X (*t* — *a*) D*ku*(*a*). (6)

*y*1 = *x*1 \* *c*1*mod p*

*y*2 = *x*2 \* *c*2*mod p*

## (13)

*The complex difference equation with long-term memory is obtained. Set the difference order m = 1, it can reduce to the classical one, but the integer one doesn’t hold the discrete memory. The domain is chan-*

*ged from* N*a*+*m*—*m to* N*a*+*m in Eqs.* [(6)–(8)](#_bookmark5)*, and the function u*(*t*) *is pre-*

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* · *b* = *k* · *d* · *a* = (*c*1; *c*2), then computes the following

*x*1 = *y*1 \* *c*—1*mod p*

*served to define on the isolated time scale* N*a in the fractional sums.*

1

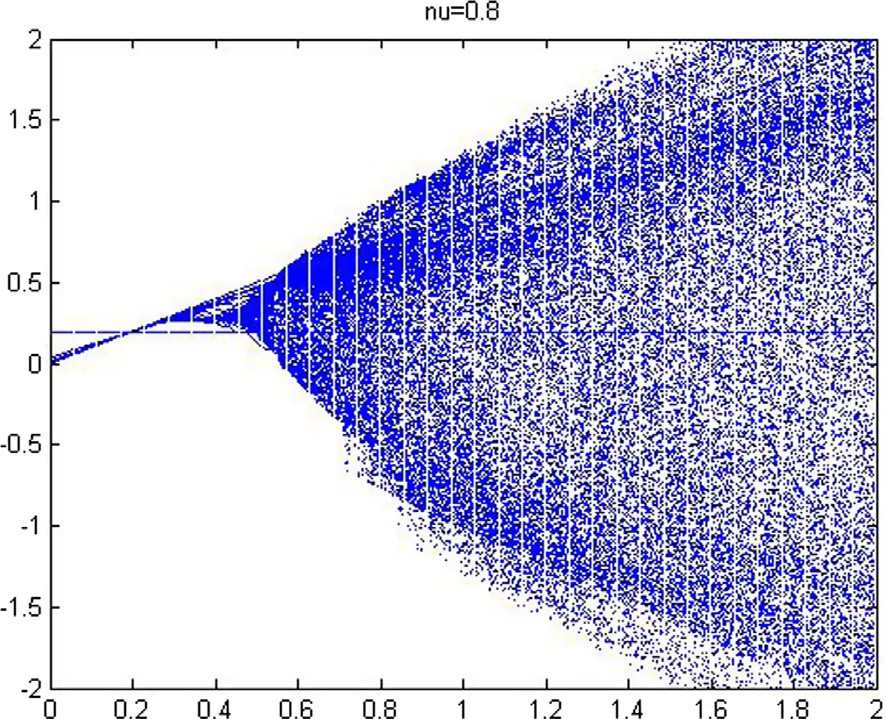
*x*2 = *y*2 \* *c*—1*mod p*

## (14)

*Obviously, the discrete fractional calculus is a crucial tool in the initial- ization of the fractional difference equations.*

2

to get the original message *x* = (*x*1; *x*2) [[18]](#_bookmark39).

Any adversary who knows *b* and *y*0 only without the private keys *d* and *k* is very difficult to solve the ECDLP and get the mes- sage *x*. Moreover, if #*E* have only one big prime divisor, solving the ECDLP is more difficult [[31]](#_bookmark53). So, MVECC is an efficient and

secure technique.

1. Fractional 2D-TFCDM

From the fractional calculus, we notice the application of the DFC to fractional generalizations of the discrete maps [[13]](#_bookmark36). In recent paper [[32]](#_bookmark54), Li introduce the following 1st 2D-TFCDM

*xn*+1 = *acos*(*yn* ), *a* = 1.4,

*yn*+1 = *bxnsin*(*yn*), *b* = 4.

## (15)

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

( *C* D*mx*(*t*)= *acos*(*y*(*t* + *m*)) — *x*(*t* + *m*), 0 < *m* < 1, *t*

*a*

∈ *Na*+1—*m*,

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

*m* = 0.8.

*yn*+1 = *bxnsin*(*yn*), *b* = 4.

## (16)

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

## 8><

>:

*x*(*n*)= *x*(0)+ C1

X*j*=1

C(*n*—*j*+*m*) [*a* cos(*y*(*j* — 1)) — *x*(*j* — 1)],

C(*n*—*j*+1)

## (17)

*y*(*n*)= *bx*(*n* — 1) sin(*y*(*n* — 1)), *b* = 4.

(*m*)

*n*

Let *m* = 1, *x*(0) = 0.19, *y*(0)= 0.06, *n* = 200, we plot the bifurca- tion diagram of [Fig. 1](#_bookmark11), where the step size of the a is set as 0.005. [Fig. 2](#_bookmark7) is the bifurcation diagram while the difference order is *m* = 0.8. We can observe that the chaotic zones are clearly depen-

dent on the changing difference order *m*. In [Fig. 3](#_bookmark9), for *m* = 1, we

get the largest lyapunov exponent using the Jacobian matrix algo- rithm. In somewhere, the largest lyapunov exponent LE1 is posi- tive. It is corresponds to chaotic areas in [Fig. 1](#_bookmark11).

We can also have the numerical formula for the variable *b*

(*a* = 1.4):

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

derived. Then the cases with the fractional difference order *m* = 0.8

8><

*y*(*n*)= *y*(0)+ C X

*n*

1

(*m*)

*j*=1

C(*n* — *j* + *m*)

C(*n* — *j* + 1) [*bx*(*j* — 1)*sin*(*y*(*j* — 1)) — *y*(*j* — 1)],

and *m* = 0.6 are considered in [Figs. 5 and 6](#_bookmark13), respectively.

*x*(*n*)= *a* cos(*y*(*n* — 1)), *a* = 1.4.

>:

(18)

Choose 401 different initial values and plot the *y*(*n*) versus the

*x*(*n*) in one figure. In [Fig. 4](#_bookmark12), the phase portraits of the integer map is

1. Applications

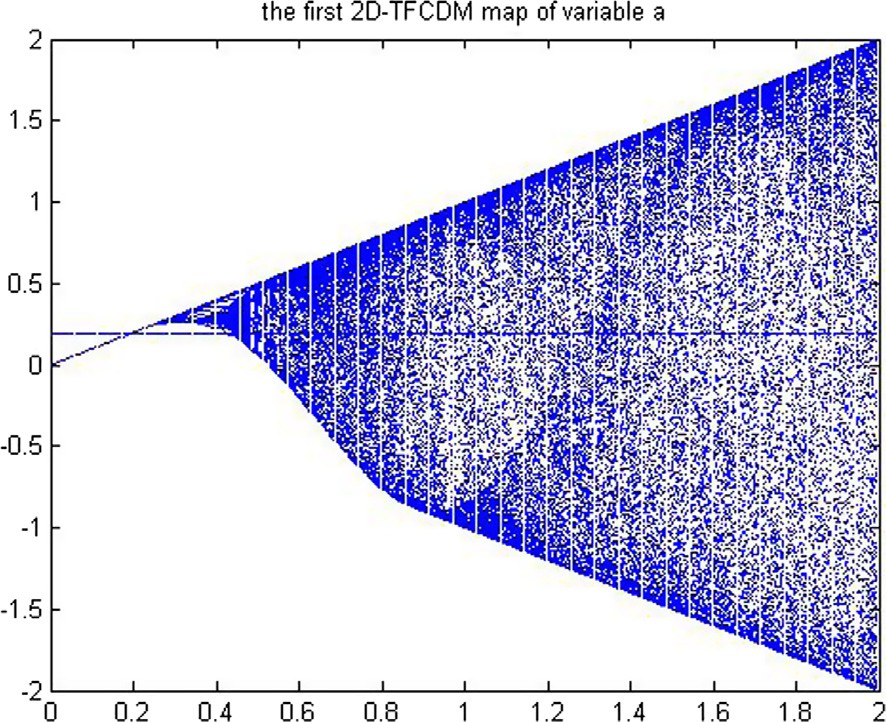
The fractionalized standard map can also be applied in informa- tion security fields. We make use of formula [(17)](#_bookmark8) as a algorithm and set the initial values *x*0, *y*0, the order *m* and the coefficients

*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.

* 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)](#_bookmark2). Since #*E* = 100, 829 is a prime, According to [[31]](#_bookmark53), it is a safe elliptic curve. set *x* = (*x*1, *x*2)= (95, 364, 5113), *a* = (2, 4), *d* = 91, 338, then *da* = (54, 157, 1425) = *b*, the secret key *k* = 63, 236, (*c*1, *c*2) = *kb* = (84, 416, 20, 597)= *dc*, *c* = *ka* = (20, 607, 18, 966). *m* = 9.536405113

' = *c*1 \* *m*01 *mod p* = 84, 416 · 95, 364*mod*100, 927 = 7123*mod*100, 927,

*m*

01

' = *c*2 \* *m*02 *mod p* = 20, 597 · 5113*mod*100, 927 = 45, 600*mod*100, 927.

*m*

02

(19)

Then, the ciphertext is ((20, 369, 92, 263), 7123, 45, 600),

' *m*' *m*'

*m* = 10

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

109

01

,000

+ 02 = 0.7123456 as the key of next step encryption.

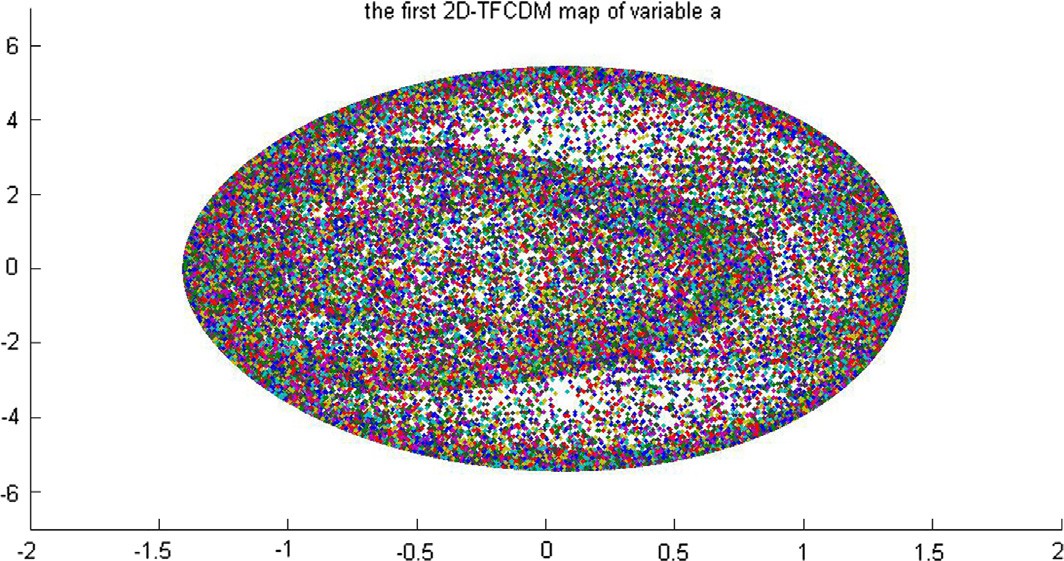


Fig. 4. The phase portraits of the first 2D-TFCDM for a = 1.4, b = 4 and *m* = 1.

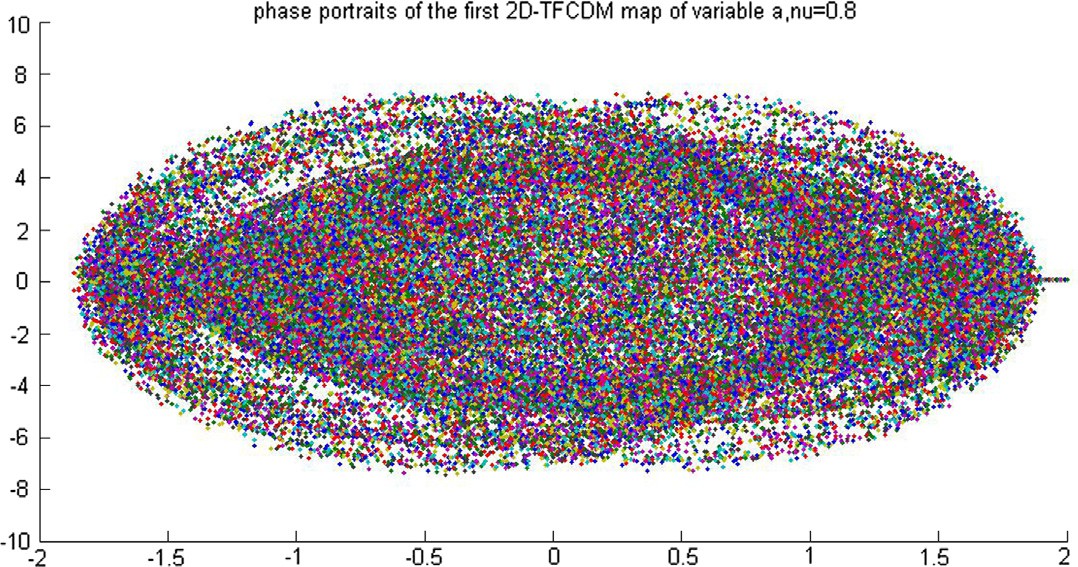


Fig. 5. The phase portraits of the first 2D-TFCDM for a = 1.4, b = 4 and *m* = 0.8.

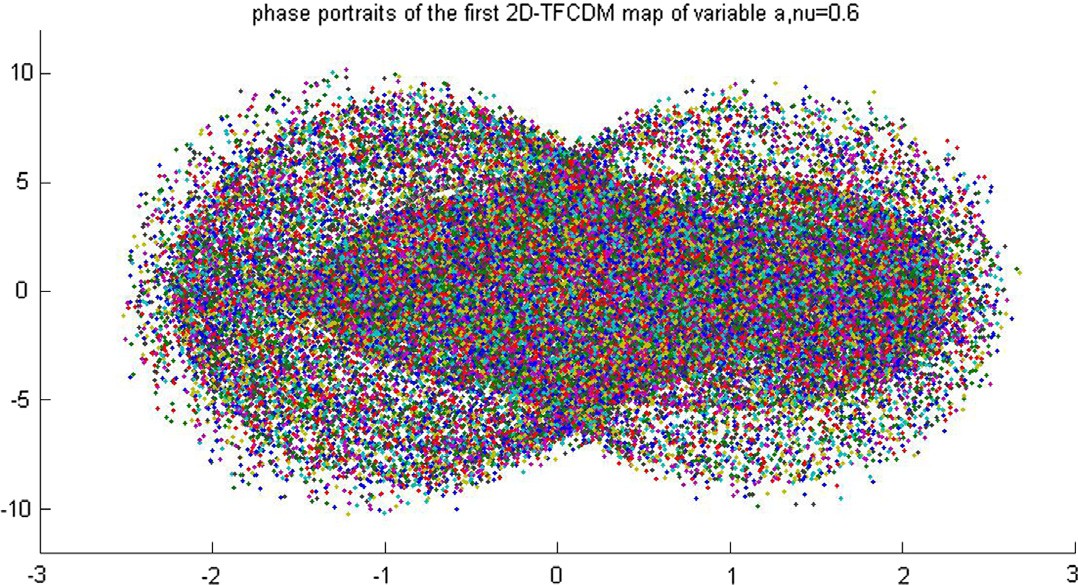


Fig. 6. The phase portraits of the first 2D-TFCDM for a = 1.4, b = 4 and *m* = 0.6.

*x*0 = 4.0301, *y*0 = 2.7955, *k*1 = 6.8541, *k*2 = 8.0623, set *x*01 =

set *x*' = *x*'

= 0.19, *y* = 01

= 0.06, *k* = 01

= 1.4, *k* = 02

= 4, as

*x* 4 4 4 4

01

' *y*'

' *k*'

' *k*'

0 104

0 104

1 104

2 104

0 × 10 , *y*01 = *y*0 × 10 , *k*01 = *k*1 × 10 , *k*02 = *k*2 × 10 , then

the keys of next step encryption.

## ' = *c*1 · *x*01*mod*100, 927 = 84, 416 · 40, 301*mod*100, 927 = 1900*mod*100, 927,

*x*

01

' = *c*2 · *y*01*mod*100, 927 = 20, 597 · 27, 955*mod*100, 927 = 600*mod*100, 927,

*y*

01

'

*k*

= *c*

01 1

· *k*01

*mod*100, 927 = 84, 416 · 68, 541*mod*100, 927 = 14, 000*mod*100, 927,

(20)

' = *c*2 · *k*02*mod*100, 927 = 20, 597 · 80, 623*mod*100, 927 = 40, 000*mod*100, 927.

*k*

02

* 1. *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)](#_bookmark8), 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, ... , *MN*.

1. Reorder *x*(*k*) by the bubble sort, then get *x*'(*k*) and record the change of the subscript of *x*(*k*) as *z*(*k*).
2. Change *M* × *N* original picture *V* into 1 × *MN* sequence *v*(*k*), here *k* = *N*(*m* — 1)+ *n*, (*m* = 1, 2 ... , *M*, *n* = 1, 2 ... , *N*), reorder *v*(*k*) similarly to *x*(*k*) according to *z*(*k*) and get *v*'(*k*).
3. Change *v*'(*k*) into *m* × *n* figure as *V* ', where *V* ' is the encrypted figure we needed.

Reverse this process, we can get the original figure.

* 1. *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](#_bookmark15). Change *M* × *N* original pic- ture *V* ' into 1 × *MN* sequence *u*(*i*), here *i* = *N*(*m* — 1)+ *n*, (*m* =

1, 2 ... , *M*, *n* = 1, 2 ... , *N*). Another *M* × *N* image is used as a

key or cover image (K-image). Also change the K-image into 1 × *MN* sequence *w*(*i*).

1. Set *i* = 0.
2. Retain only the integer part of *x*(*i*)× 108 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). (21)

1. Consider the following formula:

*u*'(*i*)= *u*(*i*)⊕ *mod*(*w*(*i*)+ *x*2(*i*), 256). (22)

where *⊕* is the xor operation, and *u*'(*i*) is the encrypted pixel value.

The inverse form of [(22)](#_bookmark16) is

*u*(*i*)= *u*'(*i*)⊕ *mod*(*w*(*i*)+ *x*2(*i*), 256). (23)

1. Compute the number *k* according to the following formula:

*k*(*i*)= 1 + *mod*(*u*'(*i*), 256). (24)

then, iterate the formula [(20)](#_bookmark14) for *k*(*i*) times, to get the new

*x*(*i* + 1), return to step 3, until *i* = *MN*.

1. Change *u*'(*i*) into *M* × *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)](#_bookmark16) is changed to use formula [(23)](#_bookmark17).
2. Reverse the procedure in Section [6.2](#_bookmark15) to remove the permutation effect.

[Fig. 7](#_bookmark19) display the process of encryption of proposed algorithm, the working principle of S box is illustrated in [Fig. 8](#_bookmark18).

The original, encryption and decryption of a image are shown in [Fig. 9](#_bookmark21)(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](#_bookmark15), 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.

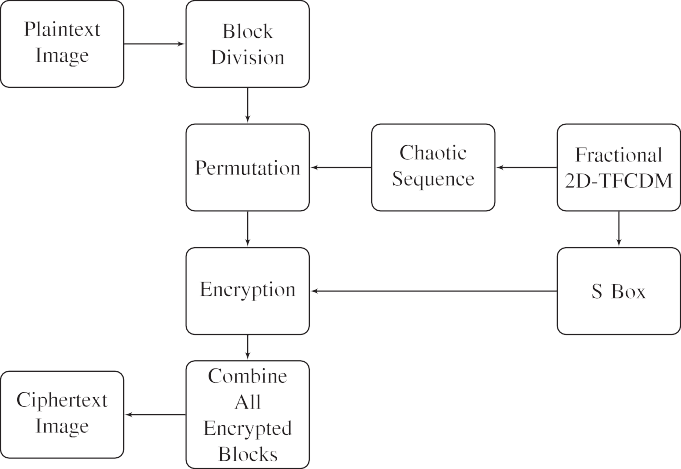


Fig. 7. The proposed encryption method.

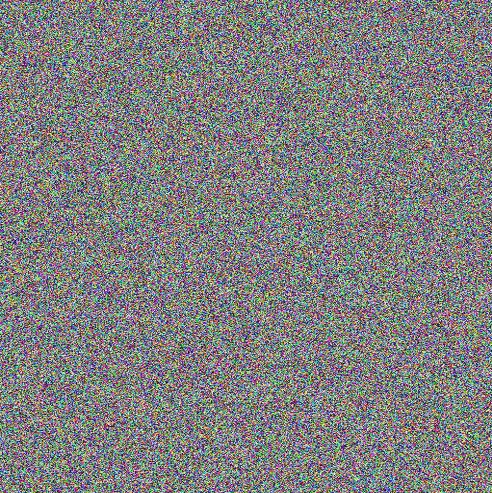
  



Fig. 9. Lena.

1. Analysis of results in applications
   1. *Key sensitivity*

In this algorithm, the order, the initial values and the coefficients of chaotic system can be utilized as the secret keys,

adjacent pixels nearly equal to zero. The correlation coefficients are calculated in vertical, horizontal and diagonal directions by Eq. [(25)](#_bookmark22), then the results are displayed in [Table 1](#_bookmark23). The correlation in the original figure and the encrypted figure of Lena along the x directions are shown in [Fig. 10](#_bookmark24).

implying that there are five secret keys (*x*0, *y*0 , *m*, *k*1, *k*2). If the precision of *x* is 2 × 10—17, the precision of *y* , *m*, *k* and *k* are

*N*

0

0

1

2

|*cov*(*x*, *y*)|

## p*D*ﬃﬃﬃﬃ(ﬃﬃ*x*ﬃﬃ)ﬃﬃp*D*ﬃﬃﬃﬃ(ﬃﬃ*y*ﬃﬃ)ﬃﬃ

*rxy* = (

25)

4 × 10—18, 6 × 10—17, 1.2 × 10—16 and 5 × 10—16, respectively, then

the secret key’s space is (2 × 10—17 × 4 × 10—18 × 6 × 10—17

×1.2 × 10—16 × 5 × 10—16)—1 ≈ 3.47 × 1081 ≈ 0.92 × 2271. If the size

( )= 1 X *i* ( )

of original image is 512 × 512, the key space of K-image is

*cov*(*x*, *y*)= 1 X(*xi* — *E*(*x*))(*y* — *E*(*y*)) (26)

*i*=1

512 × 512 × 28

*N*

*i*

= 226

. The total key space is 0.92 × 2297.

*N*

*E x x* 27

*N i*=1

* 1. *Statistics analysis*

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

* + 1. *Correlation of the plain and cipher images*

In an ordinary image, the correlation coefficient of adjacent pix- els is always high for the reason that the adjacent pixels values are close. A good encryption algorithm should make the correlation of

Table 1

The results of correlation coefficients of image.

*N*

*D x x E x* 2 28

( )= 1 X( *i* — ( ))) ( )

*N i*=1

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](#_bookmark23) 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.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Image |  |  | Original image |  |  |  | Encrypted image |  |  |
|  |  | Horizontal | Vertical | Diagonal |  | Horizontal | Vertical | Diagonal |
|  |  | R | 0.9387 | 0.9556 | 0.9168 |  | 0.0083 | 0.0063 | —0.0037 |  |
| Lena |  | 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 |  |

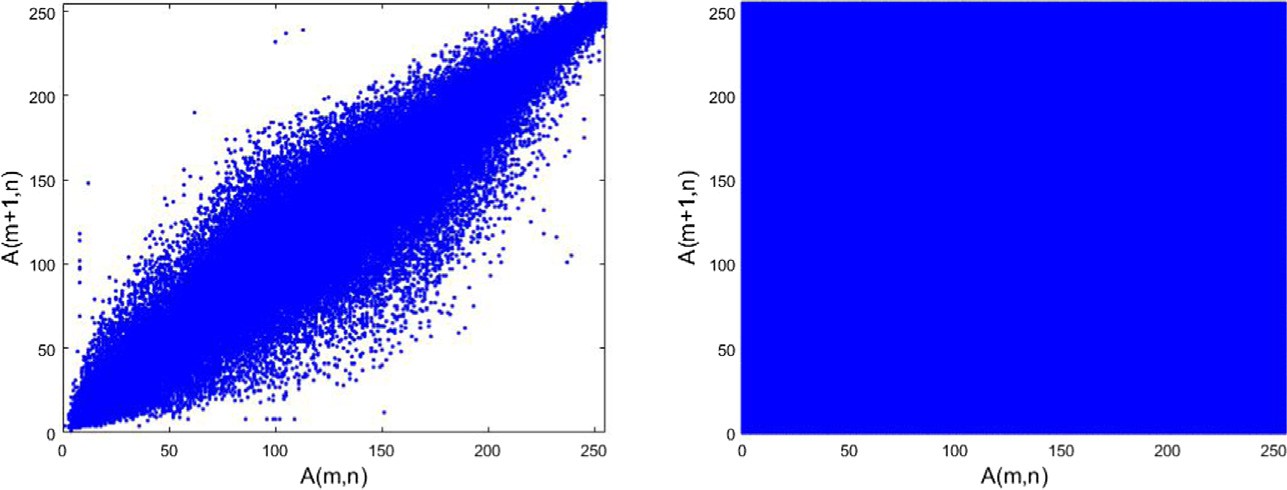


Fig. 10. Analysis of the correlations of Lena.

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]](#_bookmark40) | Lena | 0.9503 | 0.9755 | 0.9275 |  | —0.0226 | 0.0041 | 0.0368 |  |
| [[20]](#_bookmark41) | Lena | 0.927970 | 0.926331 | 0.839072 |  | —0.010889 | —0.018110 | —0.006104 |  |
| [[23]](#_bookmark44) | 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]](#_bookmark45) | 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](#_bookmark25), it can be observed from the statistical data that the proposed scheme are better than the encryption method proposed in other references.

* + 1. *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 dis- tributed with a good image encryption method. [Fig. 11](#_bookmark30) shows the histogram of Airplane in original, encrypted and decrypted 3 stages.

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

* + 1. *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:

2*n*—1

Table 3

The results of information entropy.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | Information entropy |  |  |
|  | Image |  | Original image | Encrypted image |
|  |  | R | 7.2531 | 7.9993 |  |
|  | Lena | 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]](#_bookmark40) | Lena | 7.2072 | 7.9973 |
| [[22]](#_bookmark43) | Lena | Undefined | 7.9972 |
| [[25]](#_bookmark46) | Lena | Undefined | 7.987918 |
| [[26]](#_bookmark47) | Lena | 7.447144 | 7.988847 |

* 1. *Sensitivity analysis*

There are two different criteria for measuring the range between two images: Number of pixels change rate (NPCR) and

*H*(*m*)= 1 X*p*(*mi*)*log*

*N i*=0

## 1

2 *p*(*mi*)

## (29)

unified average changing intensity (UACI), as defined by Eqs. [(31)](#_bookmark29) [and (32)](#_bookmark29).

where *p*(*mi*) expresses the probability of symbol *m*. For the pixels, values of the image are between 0 ~ 255. According to Eq. [(29)](#_bookmark28), the ideal information entropy is 8 bits for an ideally random image.

*D*(*i*, *j*)= 0, *T*1(*i*, *j*)= *T*2(*i*, *j*)

1, *T*1(*i*, *j*) – *T*2(*i*, *j*).

## (30)

Therefore, the closer to 8 bits the information entropy, the better

P*W* P*H*

*D*(*i*, *j*)

the encryption scheme. The information entropy of the encrypted images are shown in [Table 3](#_bookmark26).

*NPCR* = *i*=1 *j*=1 × 100% (31)

*W* × *H*

[Table 4](#_bookmark27) gives the comparison of information entropy. In con-

× 100% (32)

trast with other algorithms, the result implies that the encrypted images of proposed algorithm are closer to the random images.

P*W* P*H*

*UACI* =

*i*=1

|*T*1(*i*, *j*)— *T*2(*i*, *j*)|

All the above is enough to prove that the proposed encryption method has the ability to resist statistical attack.

*j*=1

255*W* × *H*

where *W* and *H* represent the width and the height of the image, respectively. *T*1 and *T*2 represent two analyzed images.

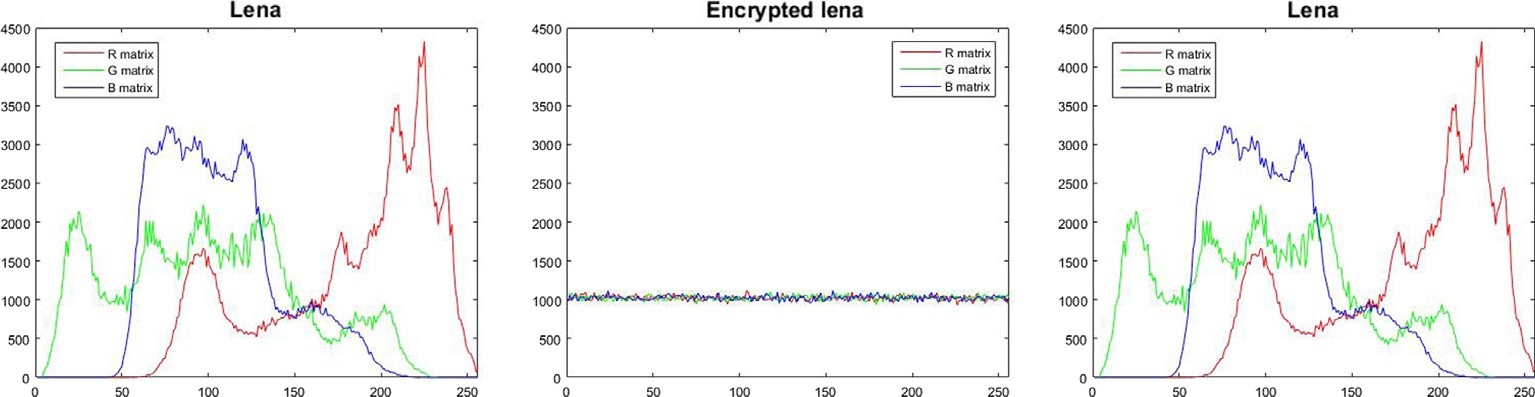


Fig. 11. The histogram of Lena.

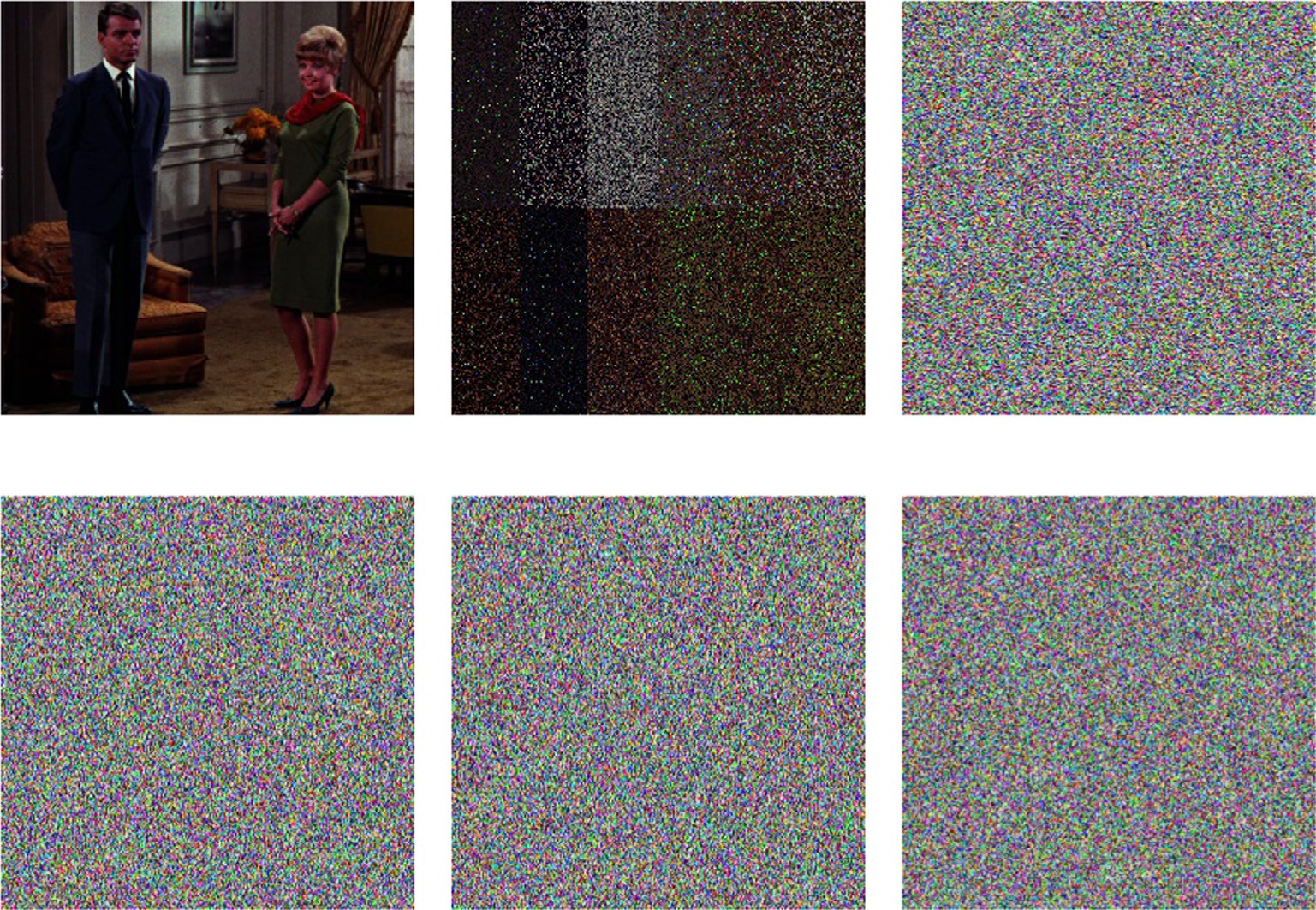


Fig. 12. The test of key sensitivity.

* + 1. *Key sensitivity*

We encrypt the image by using the keys *x*0 = 0.19, *y*0 = 0.06, *m* = 0.7123456, *k*1 = 1.4 and *k*2 = 4. [Fig. 12](#_bookmark31)(a) represents the decrypted image by the correct keys. [Fig. 12](#_bookmark31)(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 origi- nal image. Similarly, the secret keys *y*0 , *m*, *k*1, *k*2 are added 4 × 10—18, 6 × 10—17, 1.2 × 10—16 and 5 × 10—16 and shown in

[Fig. 12](#_bookmark31)(c)–(f), respectively. The NPCR and UACI between [Fig. 12](#_bookmark31)

(a) and (b)–(f) are calculated in [Table 6](#_bookmark32), separately.

Table 5

Comparison of key spaces.

Algorithm Proposed [[20]](#_bookmark41) [[22]](#_bookmark43) [[24]](#_bookmark45)

Key spaces 2.33 × 1089(0.92 × 2297) 2128 ≈ 2273 2276

Table 6

NPCR and UACI between [Fig. 12](#_bookmark31)(a) and (b)–(f).

Compared with other algorithms, the encryption method has the ability to resist exhaustive attack. [Table 5](#_bookmark33) present the result of comparison of key spaces. In [Table 6](#_bookmark32), 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](#_bookmark31)(b)–(f), therefore the encryption method is sensitive to the secret keys.

* + 1. *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]](#_bookmark40) Lena 99.61 33.53

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | NPCR and UACI |  | [[20]](#_bookmark41)  [[21]](#_bookmark42) | Lena  Lena | 99.6429  99.6304 | 33.3935  33.5989 |
| Image | NPCR(%) | UACI(%) | [[23]](#_bookmark44) | Lena | 99.932 | 39.520 |
| [12](#_bookmark31)(b) | 96.10 | 11.19 |  | Lake | 99.85 | 40.303 |
| [12](#_bookmark31)(c) | 99.49 | 40.23 | [[25]](#_bookmark46) | Lena | 75.62561 | 34.84288 |
| [12](#_bookmark31)(d) | 99.57 | 40.17 | [[26]](#_bookmark47) | Lena | 99.6091 | 33.5038 |
| [12](#_bookmark31)(e) | 99.60 | 40.12 | [[27]](#_bookmark49) | Lena | 99.6330 | 34.1319 |
| [12](#_bookmark31)(f) | 99.57 | 40.28 |  |  |  |  |

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](#_bookmark21)(a) (30, 30) | 98.24 | 33.04 | 99.61 | 33.46 |  |
|  | [Fig. 9](#_bookmark21)(a) (50, 50) | 94.09 | 31.62 | 99.60 | 33.50 |  |
|  | [Fig. 9](#_bookmark21)(a) (80, 80) | 94.86 | 31.93 | 99.62 | 33.48 |  |
|  | [Fig. 9](#_bookmark21)(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](#_bookmark35), [Fig. 9](#_bookmark21)(a) (*x*, *y*) indicates that

the pixel value of coordinate (*x*, *y*) is changed in [Fig. 9](#_bookmark21)(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)](#_bookmark29).

From [Table 7](#_bookmark35), 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](#_bookmark34) 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.

* 1. *Resistance to known-plaintext and chosen-plaintext attacks*

In Section [6.3](#_bookmark15), the last round encrypted image pixel can deter- mine the iteration times of the next round. In Eq. [(22)](#_bookmark16), *x*2(*i*), pro- duced 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 pro- posed in Refs. [[33–35]](#_bookmark55) become ineffective on this new scheme. The proposed scheme can primely resist the known-plaintext and the chosen-plaintext attacks.

1. Conclusion

Fractional 2D-TFCDM is obtained from the 2D-TFCDM. Then, new chaotic dynamics behaviors is found with the map. Further- more, 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 frac- tional 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 frac- tional 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,](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0005) [Image Vis. Comput. 24 (9) (2006) 926–934](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0005).
2. [S. Behnia, A. Akhshani, H. Mahmodi, A. Akhavan, A novel algorithm for image](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0010) [encryption based on mixture of chaotic maps, Chaos Soliton Fract. 35 (2)](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0010) [(2008) 408–419](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0010).
3. [M. Bohner, A. Peterson, Dynamic Equations on Time Scales: An Introduction](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0015) [with Applications, Springer Science & Business Media, 2012](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0015).
4. [F.M. Atici, P.W. Eloe, A transform method in discrete fractional calculus, Int. J.](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0020) [Diff. Eqs. 2 (2) (2007) 165–176](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0020).
5. [F.M. Atici, P.W. Eloe, Initial value problems in discrete fractional calculus, Proc.](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0025) [Am. Math. Soc. 137 (3) (2009) 981–989](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0025).
6. [F.M. Atici, S. Sengul, Modeling with fractional difference equations, J. Math.](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0030) [Anal. Appl.. 369 (1) (2010) 1–9](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0030).
7. [Y.D. Zhang, S.H. Wang, G. Liu, J. Yang, Computer-aided diagnosis of abnormal](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0035) [breasts in mammogram images by weighted-type fractional Fourier transform,](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0035) [Adv. Mech. Eng. 8 (2) (2016), 1687814016634243](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0035).
8. [X.J. Yang, H.M. Srivastava, D.F. Torres, Y. Zhang, Non-differentiable solutions](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0040) [for local fractional nonlinear Riccati differential equations, Fundam. Inform.](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0040) [151 (1–4) (2017) 409–417](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0040).
9. [S. Wang, M. Yang, J. Li, X. Wu, H. Wang, B. Liu, Z. Dong, Y. Zhang, Texture](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0045) [analysis method based on fractional Fourier entropy and fitness-scaling](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0045) [adaptive genetic algorithm for detecting left-sided and right-sided](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0045) [sensorineural hearing loss, Fundam. Inform. 151 (1–4) (2017) 505–521](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0045).
10. [T. Abdeljawad, D. Baleanu, Fractional differences and integration by parts, J.](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0050) [Comput. Anal. Appl. 13 (3) (2011)](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0050).
11. [M.T. Holm, The Laplace transform in discrete fractional calculus, Comput.](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0055) [Math. Appl. 62 (3) (2011) 1591–1601](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0055).
12. [C.S. Goodrich, Existence of a positive solution to a system of discrete fractional](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0060) [boundary value problems, Appl. Math. Comput. 217 (9) (2011) 4740–4753](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0060).
13. [G.C. Wu, D. Baleanu, S.D. Zeng, Discrete chaos in fractional sine and standard](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0065) [maps, Phys. Lett. A 378 (5) (2014) 484–487](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0065).
14. [G.C. Wu, D. Baleanu, Discrete chaos in fractional delayed logistic maps,](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0070) [Nonlinear Dynam. 80 (4) (2015) 1697–1703](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0070).
15. [G.C. Wu, D. Baleanu, Discrete fractional logistic map and its chaos, Nonlinear](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0075) [Dynam. 75 (1–2) (2014) 283–287](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0075).
16. [C.X. Xu, Modern Cryptography,](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0080) [Tsinghua University Press, 2015](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0080).
17. [M.F. Fu, C. Wei, Elliptic curve cryptosystem ElGamal encryption and](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0085) [transmission scheme, in: 2010 International Conference on Computer](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0085) [Application and System Modeling (ICCASM 2010),](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0085) [IEEE, 2010, 6: V6-51-V6-53](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0085).
18. [C.G. Ma, Modern Cryptography,](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0090) [National Defense Industry Press, 2014](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0090).
19. [L. Xu, X. Gou, Z. Li, J. Li, A novel chaotic image encryption algorithm using block](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0095) [scrambling and dynamic index based diffusion, Opt. Lasers Eng. 91 (2017) 41–](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0095) [52](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0095).
20. [L. Teng, X. Wang, J. Meng, A chaotic color image encryption using integrated](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0100) [bit-level permutation, Multimedia Tools Appl. (2017) 1–14](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0100).
21. [R. Enayatifar, A.H. Abdullah, I.F. Isnin, A. Altameem, M. Lee, Image encryption](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0105) [using a synchronous permutation-diffusion technique, Opt. Lasers Eng. 90](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0105) [(2017) 146–154](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0105).
22. [Y. Li, C. Wang, H. Chen, A hyper-chaos-based image encryption algorithm](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0110) [using pixel-level permutation and bit-level permutation, Opt. Lasers Eng. 90](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0110) [(2017) 238–246](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0110).
23. [S. Chakraborty, A. Seal, M. Roy, K. Mali, A novel lossless image encryption](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0115) [method using DNA substitution and chaotic logistic map, Int. J. Secur. Appl. 10](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0115)

[(2) (2016) 205–216](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0115).

1. [N. Zhou, S. Pan, S. Cheng, Z. Zhou, Image compression – encryption scheme](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0120) [based on hyper-chaotic system and 2D compressive sensing, Opt. Laser](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0120) [Technol. 82 (2016) 121–133](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0120).
2. [S.M. Ismail, L.A. Said, A.A. Rezk, A.G. Radwan, A.H. Madian, M.F. Abu-ElYazeed,](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0125)

[A.M. Soliman, Biomedical image encryption based on double-humped and](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0125) [fractional logistic maps, in: 2017 6th International Conference on Modern](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0125) [Circuits and Systems Technologies (MOCAST),](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0125) [IEEE, May 2017, pp. 1–4](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0125).

1. [J.F. Zhao, S.Y. Wang, L.T. Zhang, X.Y. Wang, Image encryption algorithm based](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0130) [on a novel improper fractional-order attractor and a wavelet function map, J.](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0130) [Electr. Comput. Eng. 2017 (2017)](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0130).
2. [P. Muthukumar, P. Balasubramaniam, K. Ratnavelu, A novel cascade](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0135) [encryption algorithm for digital images based on anti-synchronized](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0135) [fractional order dynamical systems, Multimedia Tools Appl. (2016) 1–22](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0135).
3. [G.C. Wu, D. Baleanu, Z.X. Lin, Image encryption technique based on fractional](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0140) [chaotic time series, J. Vib. Contr. 22 (8) (2016) 2092–2099](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0140).
4. [T. Abdeljawad, On Riemann and Caputo fractional differences, Comput. Math.](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0145) [Appl. 62 (3) (2011) 1602–1611](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0145).
5. [F. Chen, X. Luo, Y. Zhou, Existence results for nonlinear fractional difference](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0150) [equation, Adv. Diff. Eq. 2011 (2011)](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0150).
6. [Y.A. Xiao, Research on Elliptic Curve Cryptography,](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0155) [Huazhong University of](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0155) [Science and Technology Press, 2006](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0155).
7. [P. Li, L. Min, Y. Hu, G. Zhao, X. Li, Novel two dimensional discrete chaotic maps](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0160) [and simulations, in: 2012 IEEE 6th International Conference on Information](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0160) [and Automation for Sustainability,](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0160) [2012](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0160).
8. [D. Xiao, X. Liao, P. Wei, Analysis and improvement of a chaos-based image](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0165) [encryption algorithm, Chaos Soliton Fract. 40 (5) (2009) 2191–2199](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0165).
9. [C. Li, S. Li, G. Chen, W.A. Halang, Cryptanalysis of an image encryption scheme](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0170) [based on a compound chaotic sequence, Image Vis. Comput. 27 (8) (2009)](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0170) [1035–1039](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0170).
10. [R. Rhouma, E. Solak, S. Belghith, Cryptanalysis of a new substitution – diffusion](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0175) [based image cipher, Commun. Nonlinear Sci. Numer. Simul. 15 (7) (2010)](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0175) [1887–1892](http://refhub.elsevier.com/S2210-8327(17)30161-8/h0175).