Applied Computing and Informatics xxx (2017) xxx–xxx

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 xxxx

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 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

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

http://dx.doi.org/10.1016/j.aci.2017.07.002
2210-8327/

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

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

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.