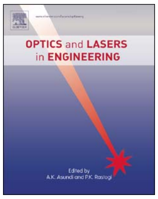
Optics and Lasers in Engineering 88 (2017) 65–74

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

journal homepage: www.elsevier.com/locate/optlaseng



Application of coupled map lattice with parameter q in image encryption

Zhang Hao, Wang Xing-yuan*, Wang Si-wei, Guo Kang, Lin Xiao-hui

Faculty of Electronic Information & Electrical Engineering, Dalian University of Technology, Dalian, 116024 China

ARTICLE INFO

Article history:
Received 4 July 2015
Received in revised form
13 July 2016
Accepted 13 July 2016

Keywords:
Image encryption
Coupled map lattice
Bifurcation
Predictor–corrector
Fractional calculus

ABSTRACT

In this paper, a novel coupled map lattice (CML) with parameter q is applied to image encryption to get higher security. The CML with parameter q is provided with Euler method and Adams–Bashforth–Moulton predictor–corrector method. In the new CML, dynamical properties are improved because the coupled strength can decrease the periodic dynamical behaviors which are caused by finite-precision. What's more, the CML changes system parameters from one-dimensional to two-dimensional. Two-dimensional parameters and coupling strengths provide researchers a possibility to improve the performance in image encryption. Finally, from numerical simulation results, it can be found that the CML improves the effectiveness and security.

1. Introduction

In 1990, the OGY method [1] was proposed by Ott, Grebogi and Yorke to control chaotic system. At the same year, the synchronization of two coupled synchronized chaotic systems was achieved by Pecora and Carroll [2]. Since then, chaos has been widely used in a variety of fields such as biological system, chemical reaction, secure communication and image encryption [3–5]. In chaos study, chaotic map is an important field. It refers to discrete variables updated iteratively and it has potential applications in image encryption. Generally, classical chaotic maps can be classified into Logistic map, Hénon map and Tent map [6,7]. Especially, the Logistic map is always chosen as chaotic model to encrypt image.

At the same time, with the deep study of low-dimensional classical maps, it is easy to infer their properties. On the other hand, compared with low-dimensional chaotic maps, properties of high-dimensional coupled maps are more complex [8–10]. So CML model can improve the dynamical properties of chaotic map effectively [11–16]. What's more, in CML with traditional Logistic map, the one-dimensional system parameter and limited parameter range also weaken the security of image encryption. As a result, a local map with two-dimensional parameter control need to be applied in the CML model to overcome this disadvantage.

Image encryption has become an emergency research in recent years [17–26]. Because of its property of bulky data and strong correlations among adjacent pixels, the traditional algorithms such as Rivest–Shamir–Adleman (RSA) [27], data encryption algorithm (DES) [28] are not suitable for images' encryption. Chaos is a definitive and similar random procedure which appears in a nonlinear system [29]. Since the chaos-based encryption algorithm was first proposed in 1989 [30], many cryptographic protocols have emerged in the scientific literature [31,32]. Chaos has many important properties, such as aperiodicity, topological transitivity, sensitive dependence on initial conditions and random-like behaviors, etc. [33,34], so chaos-based encryption algorithms have proved to be superior for encrypting images [35].

Motivated by above discussions, this paper studies the CML with parameter q and apply the CML model to image encryption. Compared with previous studies, the novel CML with parameter q extend the parameter range from one-dimensional to two-dimensional. The new parameter combination leads to complex dynamics and higher security. It should be noticed that this promotion is just for local Logistic map in CML. With bifurcation diagrams and largest Lyapunov exponent diagrams, the security and robustness of the novel CML are studied. In addition, the parameter range is provided and the CML is applied to image encryption. To the best of our knowledge, for this respect, there is no result in the literature so far. So the study is still opening and challenging.

The rest paper is organized as follows. Section 2 is the introduction of the basic model and theoretical analysis. Section 3 presents dynamical analysis of the CML model with parameter q.

* Corresponding author.
E-mail addresses: zhangh545@126.com (Z. Hao), wangxy@dlut.edu.cn (W. Xing-yuan).

http://dx.doi.org/10.1016/j.optlaseng.2016.07.004

The application and image encryption are given in Section 4. Finally, some concluding remarks are given in Section 5.

2. The CML model and theoretical analysis

In this section, the coupled map lattices with parameter q are provided and the theoretical analysis based on the special map model is given. Because the parameter q is related to fractional calculus. Then the following fractional derivative from Caputo's paper is presented.

Definition [36] The Caputo fractional calculus definition is described by:

$$D^q f(t) = \frac{1}{\Gamma(\varphi - q)} \int_0^t (t-\tau)^{-q+\varphi-1} f^{(\varphi)}(\tau) d\tau, \ (q > 0),$$

where $\varphi = \lceil q \rceil$ is smallest integer which greater than q. D^q is the q-order Caputo differential operator and Γ stands for Gamma function.

In this paper, the CML is chosen as adjacent coupled map lattices model which can be depicted as

$$z_{i,n+1} = (1-\varepsilon) f(z_{i,n}) + \frac{\varepsilon}{2} f(z_{i+1,n}) + \frac{\varepsilon}{2} f(z_{i-1,n}), \qquad i = 2, 3, \cdots, \ M-1, \tag{1}$$

where z_i is the state variable in ith lattice, ε is the coupled strength, i is the lattice index and M is the number of lattices. $n = 0, 1, \cdots, N-1$ is the iteration time and N is the iteration length. Boundary conditions are periodic chosen as

$$\begin{cases} z_{1,n+1} = (1-\varepsilon) f(z_{1,n}) + \frac{\varepsilon}{2} f(z_{2,n}) + \frac{\varepsilon}{2} f(z_{M,n}) \\ z_{M,n+1} = (1-\varepsilon) f(z_{M,n}) + \frac{\varepsilon}{2} f(z_{1,n}) + \frac{\varepsilon}{2} f(z_{M-1,n}) \end{cases}, \tag{2}$$

and $f(\bullet)$ is the local map. In many studies of image encryption, the local map is chosen as the Logistic map which can be represented as $f(a) = \mu a(1-a)$ and μ ranges in (3.57, 4). The one-dimensional parameter and the limited range weaken the security to a certain extent. In order to overcome this disadvantage, in this paper, we will take a two dimensional local map as the new local map [37]. It is not a fractional system but has similar modeling process as the fractional chaotic system. The CML with boundary conditions can be described as

$$z_{i,n+1} = z_{i,n} + h\{((1-\varepsilon)\mu z_{i,n}(1-z_{i,n}) + \frac{\varepsilon}{2}\mu z_{i+1,n}(1-z_{i+1,n}) + \frac{\varepsilon}{2}\mu z_{i-1,n}(1-z_{i-1,n}))/h\}. \tag{3}$$

Where $h = T/N$, T is the iteration time. The corresponding continuous form with appropriate h to Eq. (3) is

$$\dot{z}_i = ((1-\varepsilon)\mu z_i(1-z_i) + \frac{\varepsilon}{2}\mu z_{i+1}(1-z_{i+1}) + \frac{\varepsilon}{2}\mu z_{i-1}(1-z_{i-1}))/h. \tag{4}$$

According to the fractional calculus definition, the q-order derivative corresponding to Eq. (4) is defined as

$$\begin{cases} D^q z_i = ((1-\varepsilon)\mu z_i(1-z_i) + \frac{\varepsilon}{2}\mu z_{i+1}(1-z_{i+1}) + \frac{\varepsilon}{2}\mu z_{i-1}(1-z_{i-1}))/h \\ z_i^{(k)}(0) = z_{i,0}^{(k)}, \quad k = 0, 1, \cdots, \lceil q \rceil - 1 \end{cases}, \quad (i = 2, 3, \cdots, M-1). \tag{5}$$

Set $D^q w = g(t, w)$. Based on the Adams–Bashforth–Moulton predictor–corrector method, in order to get the corrector formula, one can firstly get the equivalent Volterra integral equation of Eq. (5) as

$$z_i(t) = \sum_{k=0}^{\lceil q \rceil - 1} z_{i,0}^{(k)} \frac{t^k}{k!} + \frac{1}{\Gamma(q)} \int_0^t \frac{g(\tau, z_i(t))}{(t-\tau)^{1-q}} d\tau. \tag{6}$$

From the defination of rectangular formula, the approximate calculation of partial Eq. (6) can be

$$\int_0^{t_{n+1}} \frac{g(\tau, z_i(t_{n+1}))}{(t_{n+1}-\tau)^{1-q}} d\tau \approx \sum_{j=0}^{n} \frac{h^q}{q} [(k+1-j)^q - (k-j)^q] g(t_j, z_i(t_j)), \tag{7}$$

where $t_j = jh$, $j = 1, 2, \cdots, N$. For any h, the error is an infinitesimal number $\max\limits_{i=1,2,\cdots,N} |x(t_i) - x_i| = o(h^\alpha)$ and $\alpha = \min(1+q, 2)$. Define $b_{j,k+1} = (k+1-j)^q - (k-j)^q$ and substitute Eq. (7) into Eq. (6), one has

$$z_i^p(t_{n+1}) = \sum_{k=0}^{\lceil q \rceil - 1} z_{i,0}^{(k)} \frac{t_{n+1}^k}{k!} + \frac{h^q}{q\Gamma(q)} \sum_{j=0}^{n} b_{j,k+1} g(t_j, z_i(t_j)). \tag{8}$$

Eq. (8) is the predictor operator. In a similar way, with the trapezoidal formula, one has

$$\int_0^{t_{n+1}} \frac{g(\tau, z_i(t_{n+1}))}{(t_{n+1}-\tau)^{1-q}} d\tau \approx \sum_{j=0}^{n} \frac{h^q}{q(q+1)} a_{j,n+1} g(t_j, z_i(t_j)), \tag{9}$$

where

$$a_{j,n+1} = \begin{cases} n^{q+1} - (n-q)(n+1)^q, j = 0 \\ (n-j+2)^{q+1} + (n-j)^{q+1} - 2(n-j+1)^{q+1}, 1 \le j \le n. \\ 1\ , j = n+1 \end{cases}$$

From above, one has that for lattice i, state variables $z_i(t_j)$, $j = 1, 2, \cdots, n$ are known and the predictor operator (8) can be calculated. Then one can get the fractional formula

$$z_i(t_{n+1}) = \sum_{k=0}^{\lceil q \rceil - 1} z_{i,0}^{(k)} \frac{t_{n+1}^k}{k!} + \frac{h^q}{\Gamma(q+2)} g(t_{n+1}, z_i^p(t_{n+1})) + \frac{h^q}{\Gamma(q+2)} \sum_{j=0}^{n} a_{j,n+1} g(t_j, z_i(t_j)). \tag{10}$$

3. Dynamical analysis of the CML model

To analyze dynamical properties of the proposed model, in this section, the spatio-temporal evolution, chaos bifurcation and Lyapunov exponents are studied. Concrete analysis is as follows.

3.1. Coupled parameter ε and its influence on system

n order to analyze dynamical properties with ε, fix parameters μ and q with appropriate values and define $\varepsilon = 0$ (any lattice has no relationship with each other). Choose a lattice to observe. When $q = 0.99$, the bifurcation diagram and the largest Lyapunov exponent diagram are illustrated by Fig. 1. In Fig. 1(a), a periodic window appears when $\mu = 2.63$ and excellent chaotic properties can be achieved when μ ranges from 2.8 to 3. Corresponding Largest lyapunov exponent diagram Fig. 1(b) leads to similar results.