Commun Nonlinear Sci Numer Simulat 19 (2014) 3735–3744

Contents lists available at ScienceDirect

Commun Nonlinear Sci Numer Simulat

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

Image encryption based on synchronization of fractional chaotic systems

Yong Xu *, Hua Wang, Yongge Li, Bin Pei

Department of Applied Mathematics, Northwestern Polytechnical University, Xi'an 710072, China

ARTICLE INFO

Article history:
Received 9 July 2013
Received in revised form 23 February 2014
Accepted 26 February 2014
Available online 12 March 2014

Keywords:
Fractional-order
Chaotic
Synchronization
Image encryption

ABSTRACT

This paper deals with a synchronization scheme for two fractional chaotic systems which is applied in image encryption. Based on Pecora and Carroll (PC) synchronization, fractional-order Lorenz-like system forms a master–slave configuration, and the sufficient conditions are derived to realize synchronization between these two systems via the Laplace transformation theory. An image encryption algorithm is introduced where the original image is encoded by a nonlinear function of a fractional chaotic state. Simulation results show that the original image is well masked in the cipher texts and recovered successfully through chaotic signals. Further, the cryptanalysis is conducted in detail through histogram, information entropy, key space and sensitivity to verify the high security.

1. Introduction

With the rapid growth of internet and wireless networks, information security becomes more and more important and is a critical issue. In particular, image encryption has received a great deal of increasing interest, due to the fact that most of image data are required to be confidential between the sending side and the receiver end, such as some military images, architectural drawings, medical imaging, and so on. During the last several decades, numerous encryption algorithms have been proposed in the literature based on different principles [1–5]. Among them, chaos based encryption techniques is considered good for practical applications as these techniques provide a good combination of speed, high security, high sensitive, complexity, etc.

Many researchers devoted to the chaotic behaviors and chaotic synchronization of dynamical systems involved the fractional derivative, which is called fractional-order chaotic system [6–11]. What's more, since the synchronization of fractional-order chaotic systems was firstly investigated in [12], it has attracted increasing attention due to its potential applications in secure communication and control processing [13–16]. Such synchronization may be safer than those of the classical chaotic systems in secure communications, by the reason of that the fractional order chaotic dynamic system has more complicated dynamic characteristic than the regular derivatives, and the fractional order of derivatives can be regarded as parameter to hide information.

In recent years, the cryptosystems based on chaos synchronization were mainly applied in encrypting the sine and cosine signal, simple mixed-signal, text message, and so on [17–20]. So far, because the image signal has the distinctive feature compared with general signal, such as strong correlation between adjacent pixels, great capacity of data, etc. There is a few research on image encryption used chaos synchronization, and they often lack of security analysis [21–23]. Motivated

* Corresponding author. Tel./fax: +86 29 88431637.
E-mail address: hsux3@nwpu.edu.cn (Y. Xu).

http://dx.doi.org/10.1016/j.cnsns.2014.02.029

by the above discussions, this paper does some tentative research on image encryption to increase security. We focus on the synchronization of fractional-order Lorenz-like chaotic system via Pecora and Carroll (PC) control method and its application in image encryption. The advantage of using fractional chaotic systems in communication is that the derivative orders can be used as secret keys as well. The main goals of this paper are: (i) to synchronize two fractional order Lorenz-like systems in master–slave configuration; (ii) to propose an image encryption design based on chaos synchronization; (iii) to verify the good effectiveness (security) of the presented scheme.

This paper is organized as follows. In Section 2, we propose the synchronization of fractional-order Lorenz-like system as PC drive-response configuration. In Section 3, based on fractional chaotic synchronization, the image encryption algorithm is given. In Section 4, the availability of the proposed method is verified by numerical simulation, and the cryptanalysis is conducted through histogram, information entropy, key space and sensitivity. Finally, conclusions are presented to close this paper.

2. Proposed systems for synchronization

In this section, based on Laplace transformation theory, we construct synchronization systems via the PC [24] method. Consider the fractional-order Lorenz-like model [25] described by

$$\begin{cases} D^{\alpha_1}x = a(y-x), \\ D^{\alpha_2}y = bx - lxz, \\ D^{\alpha_3}z = -cz + hx^2 + ky^2, \end{cases} \tag{1}$$

where α_i $(i = 1, 2, 3)$ is fractional derivative order, x, y, z are state variables, and a, b, c, l, h, k are parameters of the system. $D^{\alpha}f(t)$ denotes the Caputo fractional derivative of order $\alpha \in R$ defined as [26]

$$D^{\alpha}f(t) = \frac{1}{\Gamma(n-\alpha)} \int_0^t \frac{f^{(n)}(\tau)}{(t-\tau)^{\alpha-n+1}} d\tau, \quad \text{for } n-1 < \alpha < n \tag{2}$$

with $\Gamma(z) = \int_0^{\infty} e^{-t}t^{z-1}dt$ is the Euler's Gamma function.

Actually, system (1) will exhibit chaotic behavior [25] when $\alpha_1 = 0.97$, $\alpha_2 = 0.98$, $\alpha_3 = 0.99$, $a = 10$, $b = 40$, $c = 2.5$, $l = 1$, $h = 2$, $k = 2$, and the chaotic attractor is depicted in Fig. 1.

Let us build a PC drive-response configuration: a drive system given by the fractional order Lorenz-like model system (with three-state variables denoted by the subscript m), and a response system given by the subspace containing the (y,z) variables. One uses the chaotic signal x_m to drive the response subsystem whose variables are denoted by subscripts. The drive system is defined by

$$\begin{cases} D^{\alpha_1}x_m = a(y_m - x_m), \\ D^{\alpha_2}y_m = bx_m - lx_m z_m, \\ D^{\alpha_3}z_m = -cz_m + hx_m^2 + ky_m^2. \end{cases} \tag{3}$$

The response system is given by

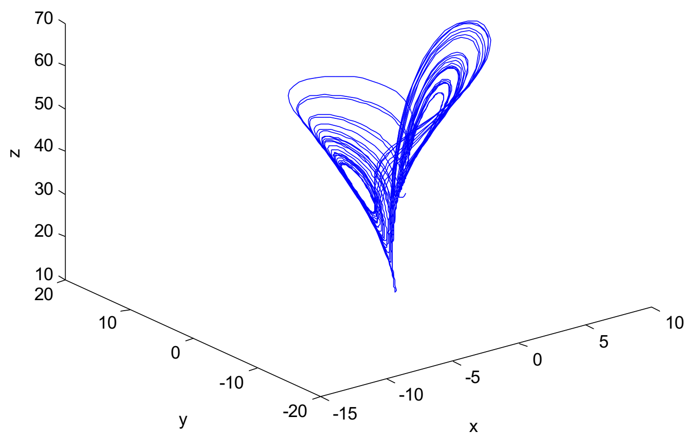

Fig. 1. Attractors of fractional-order Lorenz-like system.