ISSN 1746-7659, England, UK
Journal of Information and Computing Science
Vol. 14, No. 3, 2019, *pp*.203-210

Image encryption based on fractional-order memristive neuron system and DNA coding technology

Fanqi Meng [1,2], Xiaoqin Zeng[2], Zuolei Wang [1*]

[1]*School of Mathematics and Statistics, Yancheng Teachers University, Yancheng, P.R. China*
[2] *Computer and Information Engineering College, Hohai University, Nanjing, P.R. China*
(Received April 25 2019, accepted June 11 2019)

Abstract. In this paper, we investigate the color image encryption based on fractional-order memristive neuron system and DNA coding technology. The proposed encryption method consists of two stages: permutation and diffusion. Some numerical examples are exploited to demonstrate the feasibility of the encryption algorithm, and the security analysis shows that the algorithm has high security and good resistance to statistical attacks.

Keywords: color image encryption, fractional-order, neuron system, NDA coding

1 Introduction

In the 1980s, researchers found that the inherent randomness, sensitivity to initial values and long-term unpredictability of chaotic systems are just similar to the basic principles of cryptography. They proposed that chaotic theory be applied to cryptography and formed a new cryptography. Fridrich and Pecora et al. [1-2] proposed image pixel scrambling algorithm based on chaotic cryptography theory in the 1990s. Chaotic theory was used to encrypt and decrypt digital images. Then, in the 21st century, more and more chaotic encryption schemes were proposed by researchers to make image encryption technology based on chaotic theory. It has developed rapidly [3-4].

In the field of image encryption, chaotic image encryption by using one-dimensional and multi-dimensional chaotic sequences to scramble image pixel positions are applied in Refs. [5-14]. Recently, researchers have found that DNA sequences can be used to design encryption algorithms. Some image encryption schemes based on NDA sequences are proposed. The main idea is to use operator and DNA sequences to transform the pixel values of the diffused part. The algorithm has the characteristics of less calculation times and low power consumption and can be combined with many chaotic encryption technologies [15-16]. Wu X et al. [17] used DNA coding in combination with 1D chaotic mapping for color image decryption. Wang X et al. [18] proposed that the confusing image will be represented by DNA sequence according to the coding rule, and the extended Hamming distance is calculated to perturb the secret key to generate the key stream related to the initial image; Wei X et al [19] Designing a DNA sequence-based color image encryption algorithm for hyperchaotic systems; Maddodi et al. [20] proposed to first apply DNA sequence permutation and replacement, and then update the parameters in the chaotic neural network to improve the randomness of chaotic sequences to achieve image encryption; Zhao P et al. [21] proposed an image encryption scheme based on high-dimensional chaotic systems and DNA sequences.

Based on the above analysis of motivation, this paper will study the image encryption based on fractional-order memristive neural system and DNA coding technology, it has a great value in practical applications. Finally, some examples are used to numerically simulate the feasibility and security of the encryption algorithm.

The rest of this paper is organized as follows. Section 2 describes some basic definitions and fractional-order neural system. In Sect. 3, an color encryption algorithm based on fractional order neuron system and DNA sequence is designed. The feasibility and security of the encryption algorithm are verified by numerical experiments in Sect. 4. In Sect. 5, some conclusions are proposed.

* Corresponding author. *E-mail address*: wangzuolei1971@163.com.

2 Preliminaries

In this section, we introduce the Caputo fractional order definition and fractional-order HR neuron system with memristor.

2.1 Definitions

Definition 1. [22]**.** The Caputo fractional derivative of order q for function $f(t)$ is defined by

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

where $m \in Z^+,\ t \geq 0,\ \mathrm{m}-1 < q < m$.

Moreover, when $0 < q < 1$,

$$D^q f(t) = \frac{1}{\Gamma(1-q)} \int_0^t f'(\tau)(t-\tau)^{-q}\, d\tau.$$

Definition 2. [22]**.** Mittag-Leffler function is defined by

$$E_q(t) = \sum_{m=0}^{\infty} \frac{t^m}{\Gamma(mq+1)}$$

where $q > 0$ and $z \in C$.

2.2 Fractional-order HR neuron system with memristor

The mathematical HR neuronal model under electromagnetic radiation with four differential equations can be described as follows [23]:

$$\begin{cases} \dot{x}_1 = ax_1^2 - bx_1^3 + x_2 - x_3 + I_{ext} - 0.2W(x_4)x_1, \\ \dot{x}_2 = c - dx_1^2 - x_2, \\ \dot{x}_3 = r(S(x_1+1.6) - x_3), \\ \dot{x}_4 = x_1 - kx_4, \end{cases} \tag{1}$$

where $x_1,\ x_2,\ x_3,\ I_{ext}$ describes the membrane potential, slow current, adaption current, and external input current, respectively. The variable x_4 expresses the magnetic flux which across the membrane of the neuron. $W(x_4)x_1$ calculates memory related the conductance of memristor. When the flux is changed, $W(x_4)x_1$ can estimate the effect of membrane potential, and $W(x_4) = \alpha + 3\beta x_4^2$ [24]. The parameters a, b, c, d, r, S and k are real constants.

Refer to the above model, the new fractional-order HR system with memristor according to (1) is described as

$$\begin{cases} D^q x_1 = ax_1^2 - bx_1^3 + x_2 - x_3 + I_{ext} - 0.2W(x_4)x_1, \\ D^q x_2 = c - dx_1^2 - x_2, \\ D^q x_3 = r(S(x_1+1.6) - x_3), \\ D^q x_4 = x_1 - kx_4\ , \end{cases} \tag{2}$$

Usually, in order to obtain the chaos generation, we set $a = 3,\ b = 1,\ c = 1,\ d = 5,\ \alpha = 0.4,\ \beta = 0.02,\ r = 0.009,\ S = 4,\ k = 0.5, q = 0.9$, than the simulation is done with the initial value (1, -1, 3, -3) to system (2).

To analyse the dynamical characteristics of the system (2), when q is fixed at 0.9. Fig.1 shows the bifurcation diagram, where the function of I_{ext} drawn at the maximum of x_1.