ISSN 1746-7659, England, UK
Journal of Information and Computing Science
Vol. 11, No. 3, 2016, *pp*.235-240

Image encryption based on the bursting synchronization of time-delay neural system

Xuerong Shi[1,2]*, Lixin Han[1], Zuolei Wang[2]
[1] Computer and Information Engineering College, Hohai University, Nanjing 210098, China
[2] School of Mathematics and Statistics, Yancheng Teachers University, Yancheng 224002, China

(*Received January 13, 2016, accepted May 20, 2016)*

Abstract. In this paper, an image encryption is raised based on bursting synchronization of time-delay neuron system. The proposed method consists of two stages: permutation and diffusion. Security analysis illuminated the high security and the good resistance to statistical attacks.

Keywords: Image encryption, bursting synchronization, time-delay neural system

1. Introduction

With the development of society, security of multimedia data received more and more attention because of its wide use in various areas, such as military, telemedicine, e-commerce, broadcasting and financial transaction, image encryption, and so on. In the past decade, chaos has become a topic research. It has been applied to many fields, for instance, physics, biology, electrical engineering, communication theory, etc. [1-4]. The usage of chaos for image encryption has also received intensive attention [5, 6]. Existing result [7] suggests that encryption of image is quite different from that of textual information. Due to inherent features of images, like large data size, bulk data capacity, high redundancy and strong correlation among adjacent pixels, it would take large computational time. For this, several image encryption schemes based on chaos are proposed [8-10]. With further study of the image encryption, people found that the key space has great impact on the security level of the image. The larger the cryptosystem's key space is, the more difficultly the image is to be attacked.

Motivated by above, in this paper, we propose an image encryption scheme based on bursting synchronization of time-delay neural system. Section 2 gives the time-delay neural system and its synchronization scheme. In section 3, Image encryption algorithm is depicted. Simulation results are carried out in section 4. Section 5 draws some conclusions.

2. Bursting synchronization of time-delay neural system

In this section, time-delay Hindmarsh-Rose neuron model [11] is considered to obtain the pseudo-random sequence, which can be written as following (1)

$$\begin{cases} \dot{x}_1 = ax_1^2 - bx_1^3 + x_2 - x_3(t-\tau) + I_{ext} \\ \dot{x}_2 = c - dx_1^2 - x_2 \\ \dot{x}_3 = r(S(x_1+k) - x_3) \end{cases}, \tag{1}$$

where $\tau > 0$ is the time delay. x_1, x_2, x_3 are state variables. $a, b, c, d, r, S, k, I_{ext}$ are real constants. When $a = 3.0$, $b = 1.0$, $c = 1.0$, $d = 5.0$, $r = 0.006$, $S = 4.0$, $k = 1.6$, system (1) has chaotic bursting for $I_{ext} = 3.1$ (Fig.1). To obtain the bursting synchronization, system (1) is considered as the drive system and the response system is taken as following (2)

$$\begin{cases} \dot{y}_1 = ay_1^2 - by_1^3 + y_2 - y_3(t-\tau) + I_{ext} + u_1 \\ \dot{y}_2 = c - dy_1^2 - y_2 + u_2 \\ \dot{y}_3 = r(S(y_1+k) - y_3) + u_3 \end{cases}, \tag{2}$$

where u_1, u_2, u_3 are controllers to be designed. Due to the boundedness of chaotic system, there is a positive constant M satisfying $|x_i| < M$, $|y_i| < M$ ($i = 1, 2, 3$).

Let $e_1 = y_1 - x_1$, $e_2 = y_2 - x_2$, $e_3 = y_3 - x_3$, and we can get **Theorem 1.**

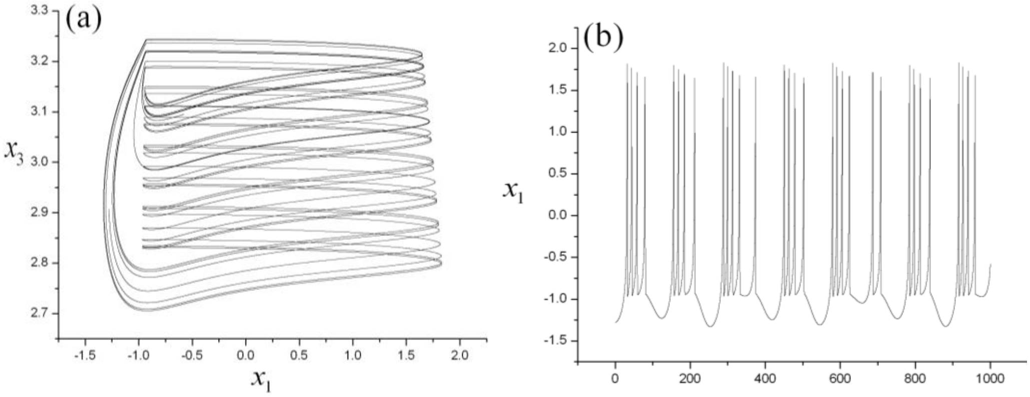

Fig.1. Chaotic bursting of system (1) when I_{ext} = 3.1 (a) Phase portrait. (b)Time series

Theorem 1 If the controllers are taken as following linear feedback controller with parameter update laws

$$\begin{cases} u_1 = -k_1 e_1, & \dot{k}_1 = g_1 e_1^2, \\ u_2 = -k_2 e_2, & \dot{k}_2 = g_2 e_2^2, \\ u_3 = -k_3 e_3, & \dot{k}_3 = g_3 e_3^2, \end{cases} \tag{3}$$

where $g_1,\ g_2,\ g_3 > 0$ are arbitrary constants, then response system (2) can bursting synchronize the drive system (1).

Proof: From system (1) and (2), the error system can be gotten as

$$\begin{cases} \dot{e}_1 = a(y_1^2 - x_1^2) - b(y_1^3 - x_1^3) + e_2 - e_3(t-\tau) + u_1, \\ \dot{e}_2 = -d(y_1^2 - x_1^2) - e_2 + u_2, \\ \dot{e}_3 = rSe_1 - re_3 + u_3, \end{cases} \tag{4}$$

Lyapunov function is chosen as

$$V = \frac{1}{2}[e_1^2 + e_2^2 + e_3^2 + (k_1 - \hat{k}_1)^2 / g_1 + (k_2 - \hat{k}_2)^2 / g_2 + (k_3 - \hat{k}_3)^2 / g_3] + \beta \int_{t-\tau}^{t} e_3^2 dt\,, \tag{5}$$

where $\hat{k}_1$, $\hat{k}_2$, $\hat{k}_3$ are constants to be determined. Obviously, V is positive definite.

Differentiate V with error system (4), and we can deduce that

$$\begin{aligned} \dot{V} &\le -(\hat{k}_1 - 2aM - 3bM^2 - \frac{1}{2\lambda})e_1^2 - (1 + \hat{k}_2)e_2^2 - (r + \hat{k}_3 - \beta)e_3^2 + (1 + 2dM)e_1 e_2 \\ &\quad + rSe_1 e_3 - (\beta - \frac{\lambda}{2})e_3^2(t-\tau) \\ &= -(|e_1|, |e_2|, |e_3|)P(|e_1|, |e_2|, |e_3|)^T - (\beta - \frac{\lambda}{2})e_3^2(t-\tau)\,, \end{aligned}$$

where $a_{11} = -2aM - 3bM^2$, $a_{12} = -(1 + 2dM)/2$, $a_{13} = -rS/2$ and

$$P = \begin{pmatrix} \hat{k}_1 - \frac{1}{2\lambda} + a_{11} & a_{12} & a_{13} \\ a_{12} & 1 + \hat{k}_2 & 0 \\ a_{13} & 0 & r + \hat{k}_3 - \beta \end{pmatrix}.$$