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.**

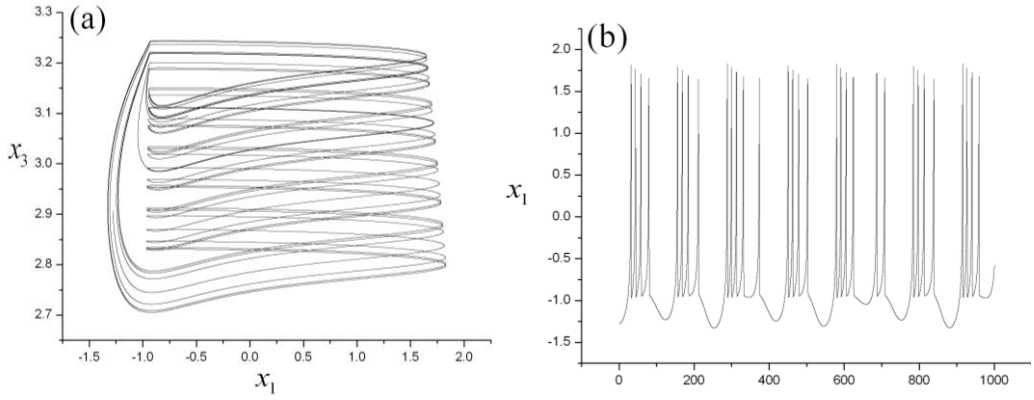

Fig.1. Chaotic bursting of system (1) when I_{ext} = 3.1 (a) Phase portrait. (b)Time series

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

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

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

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

For suitable values of $\hat{k}_1$, $\hat{k}_2$, $\hat{k}_3$, λ, β, it can be available that $\beta - \frac{\lambda}{2}$ is positive and matrix P is positive definite. It means that $\dot{V} < 0$ can be obtained. Therefore, it comes to a conclusion that bursting synchronization between systems (1) and (2) can be reached.

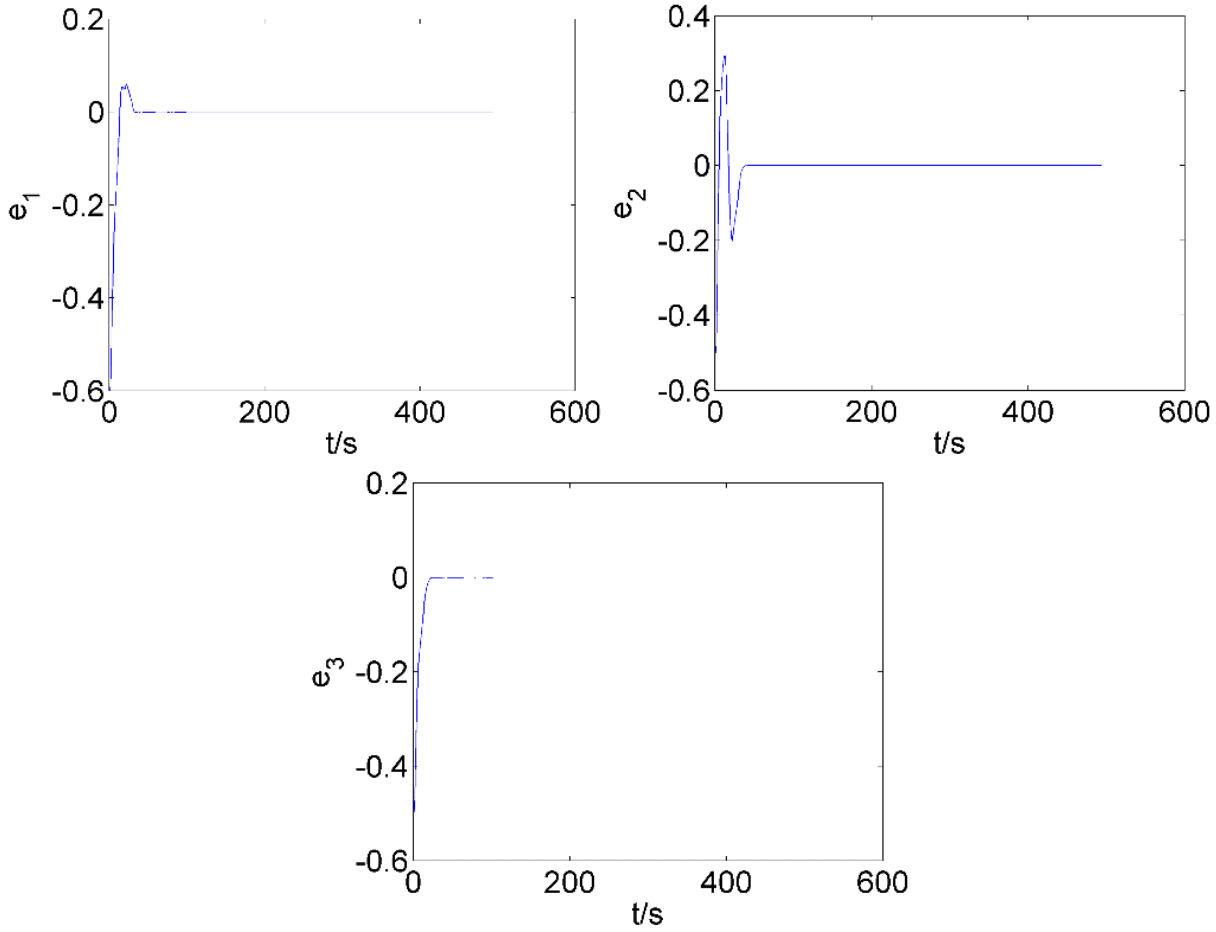

Fig.2 Dynamics of error system (4) with controllers in (3)

When a =3.0, b =1.0, c =1.0, d =5.0, r =0.006, S =4.0, k =1.6, I_{ext} =3.1, $\tau = 1$, and initial values of systems (1) and (2) are set to be (0.3, 0.2, 0.1) and (0.6, 0.7, 0.3), respectively. Fig.2 gives the time evolution of the error system (4) with controllers in (3), from which it is easy to see that bursting synchronization of time-delay neuron systems can be achieved.

Theoretical analysis and simulation results mean that, there is a certain moment t_0, after which trajectories of systems (1) and (2) are identical. But the identical trajectories are relevant to the initial value of the systems and time-delay.

3. Image encryption algorithm

In this section, according to the sequences of state variables produced in section2, an image encryption method is put forward, which includes two main processes of substitution and diffusion. Lena is selected as example to implement the proposed method. Without loss of generality, the size of the Lena image is assumed as $M \times N$ and the pixels' value is from 0 to 255. The steps of encryption are as follows.

Step 1. Read the Lena plain image and obtain its size $M \times N$.

Step 2. Generate Pseudo-random sequence.

Set initial values of systems (1) and (2), the time-delay, realize the bursting synchronization, throw away the groups before synchronization and take remaining groups $S = (x_j, y_j, z_j)$ $(j = 1, 2, \cdots)$.

Step 3. Permutation stage

Image pixels are generally permutated in the light of the logistic map [12]

$$x_{n+1} = \mu x_n (1 - x_n) \tag{6}$$

and formula

$$\begin{cases} x_{i+1} = (x_i + y_i + abs(\,fix(z_j)) + abs(\,fix(z_{j+k}))) \bmod M. \\ y_{i+1} = (y_i + abs(\,fix(z_{j+k})) + K\sin(\frac{2\pi x_{i+1}}{N})) \bmod N. \end{cases} \tag{7}$$

In map (6), μ $(3.5699456 < \mu \le 4)$ is the control parameter, x_n is independent variable. In formula (7), K is a constant, $abs(x)$ returns to the absolute value of x, $fix(x)$ rounds the element of x toward zero resulting in an integer, (x_i, y_i) and (x_{i+1}, y_{i+1}) are the locations before and after permutation, respectively, f is positive integer indicating value interval between r_x and r_y. The extraction of z_j is in light of the logistic map (6).

Step 3. Diffusion

Pixel values are modified sequentially according to

$$v = p \oplus (c \times x_i + d \times y_i) \bmod L \tag{8}$$

based on diffusion parameters, where p and v are the pixels' values before and after the replacement, respectively, (x_i, y_i) means the location information, L is the grayscale of pixels.

c and d are diffusion parameters in view of

$$\begin{cases} c = abs(10^l x_j - round(10^l x_j)) \times 10^3. \\ d = abs(10^l y_j - round(10^l y_j)) \times 10^3. \end{cases} \tag{9}$$

Decryption of image is the inverse of the encryption process including pixel recovery and position recovery. Firstly, restore the pixel value for each pixel and then each pixel will be restored to its original position according to the inverse process of (7) and (8), respectively.

4. Simulations

Set initial values of systems (1) and (2) as $(x_1(0), x_2(0), x_3(0)) = (0.2, 0.4, 0.5)$, $(y_1(0), y_2(0), y_3(0)) = (0.8, 0.9, 1.0)$, time-delay $\tau = 1$, synchronization between systems (1) and (2) is achieved. At this time, get rid of the groups before synchronization and take remaining groups $S = (x_j, y_j, z_j)(j = 1, 2, \cdots)$. Other parameters are chosen as $\mu = 3.99$, $K = 5$, $l = 3$, $f = 20$. The typical image of Lena is chosen to be simulated in Fig.3, from which we know that Lena image can be encrypted and the encrypted image can be fully restored.

To effectively deal with brute force attacks, the key space should be large enough. The proposed algorithm above contains eleven keys, which provide enough key space. On the other hand, image histogram is an important analysis standard for image encryption. To resist statistical attack, a good encryption method is required to obtain an image with uniform histogram significantly different from that of the plain image. That is to say, encrypted images should be provided with random properties. To demonstrate the robustness of our cryptosystem, we have performed statistical analysis by computing the histograms (Fig.4). From Fig.4, it is easy to know that the histogram of the encrypted image is more uniformly distributed and quite different from that of the plain image, which implies that the redundancy of the plain image is successfully hidden after the encryption and consequently does not provide any clue to apply statistical attacks.

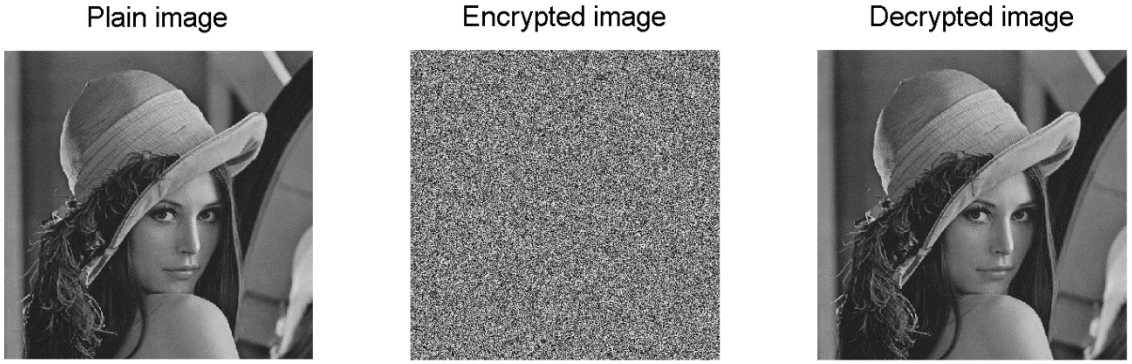

Fig .3 The encryption and decryption results of Lena image

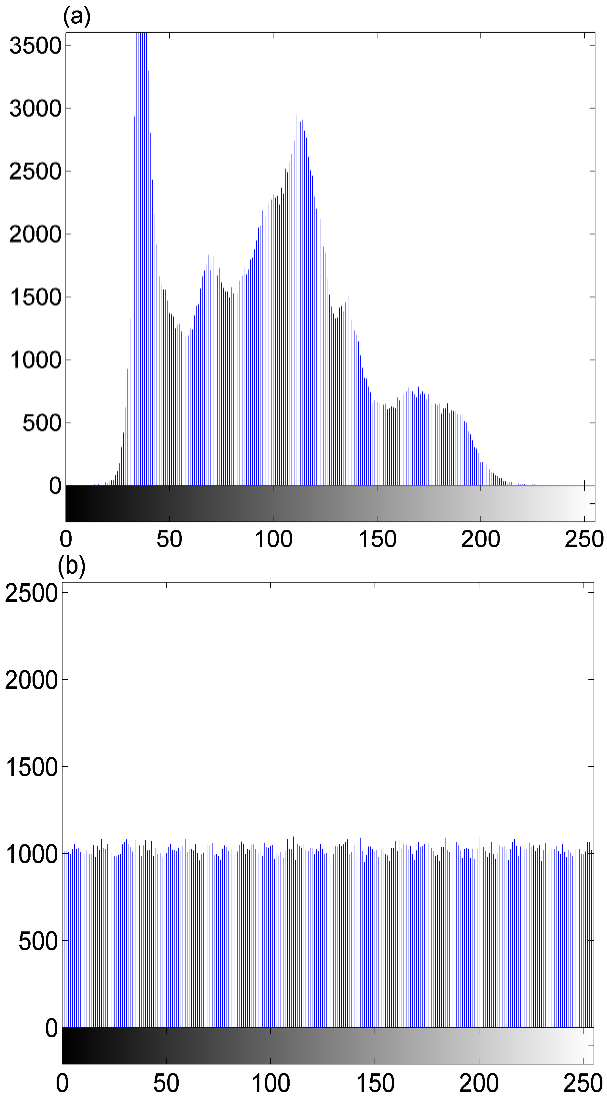

Fig.4 Histograms of Lena image (a) Plain image. (b) Encrypted image

5. Conclusion

In this paper, an image encryption is proposed based on the bursting synchronization of time-delay neural system. In this method, the encrypted image not only can be fully restored, but also has good resistance to statistical attack in image transferring because of the large key space with eleven keys. Histogram of the plain image has significant features while the histogram of encrypted image has more uniformly distributed feature. It suggests that the proposed method is idea and can be used in image encryption.

Acknowledgement

This work is supported by National Natural Science Foundation of China (Grant No. 11472238), the Natural Science Foundation of Xinjiang Uygur Autonomous Region of china (Grant No. 2015211C267) and the Qing Lan Project of the Jiangsu Higher Education Institutions of China.

6. References

[1] L.M. Pecora, T.L. Carroll, Synchronization in chaotic systems, Phys. Rev. Lett. 64 (1990) 821- 824.

[2] X.J. Wu, J.S. Liu, G.R. Chen, Chaos synchronization of Rikitake chaotic attractor using the passive control technique, Nonlinear Dyn. 53 (2007) 45-53.

[3] X.Y. Wang, C.F. Duan, Observer based chaos synchronization and its application to secure communication, J. Chin. Inst. Commun. 26(2005)105-111.

[4] H. Wang, Z.Z. Han, W. Zhang, Q.Y. Xie, Chaotic synchronization and secure communication based on descriptor observer, Nonlinear Dyn. 57 (2009) 69-73.

[5] S.J. Li, G.R. Chen, K.W. Wong, X.Q. Mou, Y.L. Cai, Baptista-type chaotic cryptosystems: problems and countermeasures, Phys. Lett. A 332 (2004) 368-375.

[6] J. Wei, X.F. Liao, K.W. Wong, T. Zhou, Cryptanalysis of a cryptosystem using multiple one- dimensional chaotic maps, Commun. Nonlinear Sci. Numer. Simul. 12 (2007) 814-822.

[7] J. Ahamd, S.O. Hwang, A. Ali, An experimental comparison of chaotic and non-chaotic image encryption schemes, Wirel. Pers. Commun. 84 (2015) 901-918.

[8] A. Souyah, K.M. Faraoun, An image encryption scheme combining chaos-memory cellular automata and weighted histogram, Nonlinear Dyn. (2016)1-15.

[9] S. El Assad, M. Farajallah, A new chaos-based image encryption system, Signal Process. Image Commun. 41 (2016) 144-157.

[10] X. Wang, L. Liu, Y. Zhang, A novel chaotic block image encryption algorithm based on dynamic random growth technique, Opt. Lasers Eng. 66 (2015) 10-18.

[11] J. L. Hindmarsh, R. M. Rose, A model of neuronal bursting using three coupled first order differential equations, Proc.R. Soc. Lond. B Biol. Sci. 221(1984) 87-102.

[12] N.K. Pareek, V. Patidar, K.K. Sud, Image encryption using chaotic logistic map, Image Vision Comput.24 (2006) 926-934.