ISSN 1746-7659, England, UK
Journal of Information and Computing Science
Vol. 12, No. 2, 2017, *pp*.123-129

Image encryption based on the tracking control Hindmarsh-Rose system via Genesio-Tesi system

Keming Tang[1], Xuerong Shi [2*], Zuolei Wang [2], Wen Yun[2], Liying Zheng[2]
[1] *Academic Affairs Office, Yancheng Teachers University, Yancheng, 224002, China;*
[2] *School of Mathematics and Statistics, Yancheng Teachers University, Yancheng, 224002, China, E-mail: sxryctc@163.com.*
(Received December 22, 2016, accepted February 15, 2017)

Abstract. According to encryption structure of permutation and diffusion, as well as pseudo-randomness of chaotic synchronization sequences, tracking Hindmarsh-Rose system via Genesio-Tesi system is applied into the process of image encryption. Theoretical analysis and simulations suggest that the proposed encryption algorithm has good security in image transmission.

Keywords: tracking synchronization; Hindmarsh-Rose system; Genesio-Tesi system; image encryption.

1. Introduction

Chaos synchronization is making two chaotic systems identical after transient initial states. Since being proposed by Carroll and Pecora [1], it has been studied and applied in many fields, such as secure communication[2], biological systems[3], robotics[4]. It is found that synchronization is useful and has many potential applications in many domains[2-7], especially, synchronization in physical or biological system is a fascinating subject attracting many renewed attention [5].

In many kinds of synchronizations, one is about the synchronization between non-linear systems with different structures and orders, which can be seen as the variable states of the slave system are tracking the trajectories of the master system [8-12]. This problem can be transformed to a regulation problem with the origin (zero) as the corresponding set point. the trajectories of two systems will follow the same path after some transient. This synchronization needs weaker conditions to be realized than complete synchronization and it is can be regarded as partial synchronization [13, 14], which has been studied by many researchers in the past years[15-18].

In the last decades, due to the strong sensitivity to the initial value, chaos synchronization has been applied into digital image encryption[19-21] and good encryption results have been obtained.

In this paper, changeable gain coefficients are introduced into Lyapunov function to study tracking Hindmarsh-Rose system via Genesio-Tesi system. This tracking synchronization is applied into digital image encryption. Theoretical analysis and numerical simulations are presented to demonstrate the effectiveness of the proposed tracking scheme and the security of the encryption algorithm.

2. System descriptions

2.1. Hindmarsh-Rose system

Hindmarsh-Rose (HR) model, first proposed by Hindmarsh and Rose as a mathematical representation of the firing behavior of neurons, was originally introduced to give a bursting type with long inters pike intervals of real neurons [22], which is given as

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

where a, b, c, d, r, S, k, I_{ext} are real constants.

2.2. Genesio-Tesi system

The Genesio-Tesi system[23] consists of a simple square part and three simple differential equations depending on three positive real parameters. It can be written as

$$\begin{aligned} \dot{y}_1 &= y_2, \\ \dot{y}_2 &= y_3, \\ \dot{y}_3 &= -a_1 y_1 - a_2 y_2 - a_3 y_3 + y_1^2, \end{aligned} \tag{2}$$

where a_1, a_2, a_3 are positive real constants.

Next, tracking synchronization of Hindmarsh-Rose neuron system via Genesio -Tesi system will be discussed via a single controller.

3. Tracking synchronization of Hindmarsh-Rose system via Genesio-Tesi system

In this section, a scheme is proposed to realize the tracking synchronization of Hindmarsh-Rose neuron system via Genesio-Tesi system. This scheme needs only one single controller u, which is added to the second equation of system (2). The controlled Genesio-Tesi system is given as

$$\begin{aligned} \dot{y}_1 &= y_2, \\ \dot{y}_2 &= y_3 + u, \\ \dot{y}_3 &= -a_1 y_1 - a_2 y_2 - a_3 y_3 + y_1^2. \end{aligned} \tag{3}$$

To explore the tracking synchronization of Hindmarsh-Rose neuron system via Genesio-Tesi system, let the error be

$$e = x - y_1, \tag{4}$$

where x is one of the observed states of system (1). Lyapunov function is chosen as

$$V = \alpha e^2 + (\dot{e} + \beta e)^2, \tag{5}$$

where α and β are positive gain coefficients, the over dot denotes the differential variable e over time t. The differential of V is

$$\begin{aligned} \dot{V} &= 2\alpha e\,\dot{e} + 2(\dot{e} + \beta e)(\ddot{e} + \beta\dot{e}) \\ &= -2\beta V + 2\beta V + 2\alpha e\,\dot{e} + 2(\dot{e} + \beta e)(\ddot{e} + \beta\dot{e}) \\ &= -2\beta V + 2\beta[\alpha e^2 + (\dot{e} + \beta e)^2] + 2\alpha e\,\dot{e} + 2(\dot{e} + \beta e)(\ddot{e} + \beta\dot{e}) \\ &= -2\beta V + 2\alpha e\,(\dot{e} + \beta e) + 2\beta(\dot{e} + \beta e)^2 + 2(\dot{e} + \beta e)(\ddot{e} + \beta\dot{e}) \\ &= -2\beta V + 2(\ddot{e} + 2\beta\dot{e} + \alpha e + \beta^2 e)(\dot{e} + \beta e). \end{aligned} \tag{6}$$

When

$$2(\ddot{e} + 2\beta\dot{e} + \alpha e + \beta^2 e)(\dot{e} + \beta e) = 0 \tag{7}$$

is satisfied , we have

$$\frac{dV}{dt} = -2\beta V < 0. \tag{8}$$

It means that the errors of corresponding variables will be stabilized to a certain threshold. That is to say, the observed state x of system (1) and the salve state y_1 of the system (2) with a controller will reach synchronization.

To verify the feasibility of above method, three cases are to be considered and some numerical simulations will be demonstrated. In the numerical simulations, The system parameters are chosen as a = 3.0, b = 1.0, c = 1.0, d = 5.0, r = 0.006, S = 4.0, k = 1.6, I_{ext} = 3.0, a_1 = 6.0, a_2 = 2.88, a_3 =1.2. The initial conditions of the HR system and the Genesio-Tesi system are set as (0.1, 0.9, 0.8) and (0.4, 0.3, 0.2), respectively.

Case 1 Simulating the bursting activity of x_1 using y_1.

In this case, let $e_1 = x_1 - y_1$, the controller u is taken as

$$u_1 = (2ax_1 - 3bx_1^2)(ax_1^2 - bx_1^3 + x_2 - x_3 + I_{ext}) + (c - dx_1^2 - x_2)$$

$$-[r(S(x_1+k)-x_3)]-y_3+2\beta(ax_1^2-bx_1^3+x_2-x_3+I_{ext}-y_2)+(\alpha+\beta^2)(x_1-y_1). \quad (9)$$

The evolutions of the error variable e_1 is given in Fig.1, from which, it is known that e_1 converges to zero at fixed constants $\alpha=\beta$=0.2.

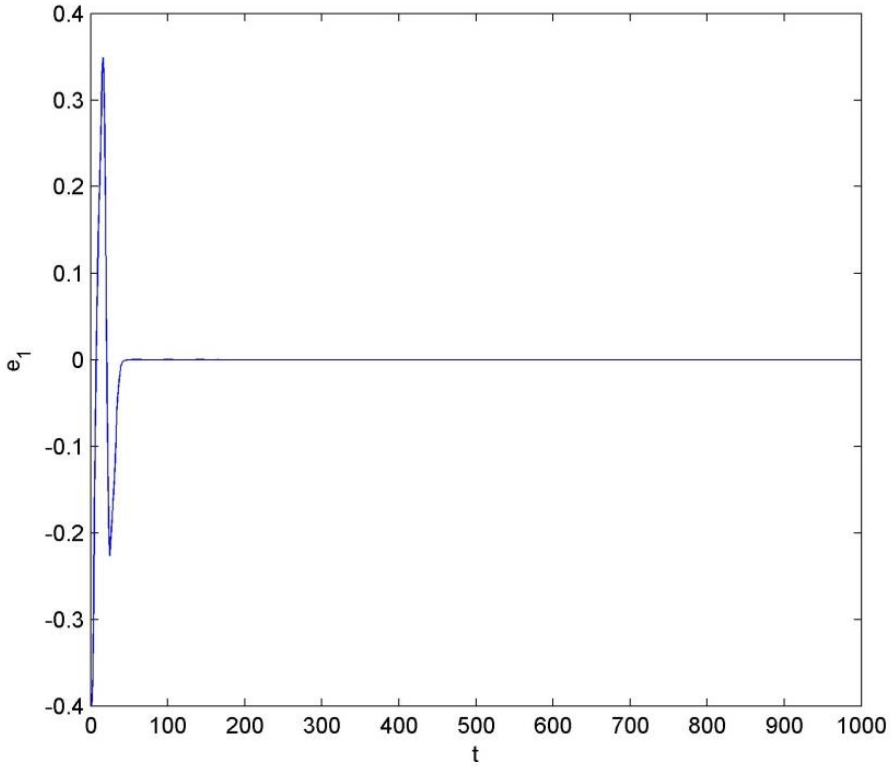

Fig.1. Synchronization error of e_1 at fixed constants ($\alpha=\beta$=0.2).

Case 2 Simulating the bursting activity of x_2 using y_1.

In this case, let $e_2=x_2-y_1$ the controller u is given as

$$u_2=-2dx_1(ax_1^2-bx_1^3+x_2-x_3+I_{ext})-(c-dx_1^2-x_2)$$
$$-y_3+2\beta(c-dx_1^2-x_2-y_2)+(\alpha+\beta^2)(x_2-y_1). \quad (10)$$

The evolutions of e_2 is calculated under $\alpha=\beta$=0.2 and depicted in Fig. 2.

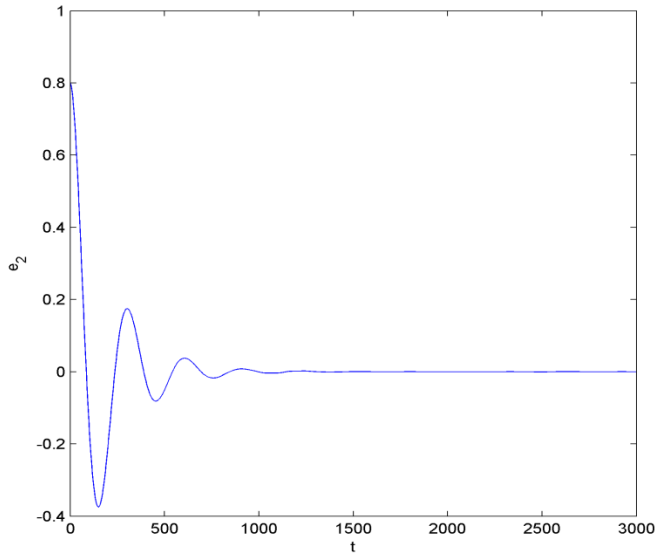

Fig.2. Synchronization error of e_2 at fixed constants ($\alpha=\beta$=0.2).

Case 3 Simulating the bursting activity of x_3 using y_1.

In this case, let $e_3 = x_3 - y_1$, the controller u is given as

$$u_3 = rS(ax_1^2 - bx_1^3 + x_2 - x_3 + I_{ext}) - r^2[S(x_1 + k) - x_3]$$
$$-y_3 + 2\beta[r(S(x_1 + k) - x_3) - y_2] + (\alpha + \beta^2)(x_3 - y_1). \quad (11)$$

The evolutions of e_3 under fixed constants $\alpha = \beta$ =0.2 is shown in Fig. 3.

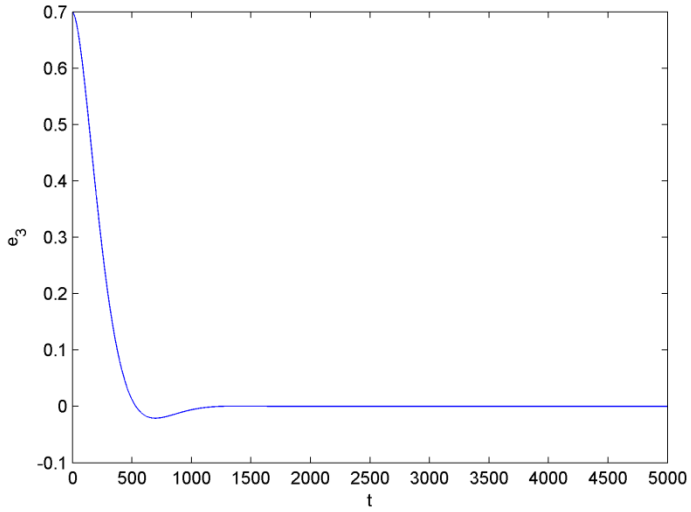

Fig.3. Synchronization error of e_3 at fixed constants ($\alpha = \beta$ =0.2).

From Figs.1-3, it is obvious to see that, state variable y_1 in the slave system can be tracking any state variable of the drive system using suitable single controller.

4. Image encryption based on the tracking synchronization

4.1. Encryption algorithm

In this section, according to the sensitivity to initial conditions of chaos synchronization sequences, tracking synchronization is applied into the image encryption algorithm. Without loss of generality, the size of the image is assumed as $M \times N$ and the pixels' value is from 0 to 255. The specific encryption process is as follows.

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

Step 2. Generate Pseudo-random sequence.

Set initial values of systems (1) and (2), choose suitable controllers, realize the tracking synchronization of x_i $(i = 1,2,3)$ in system (1) via y_1 in system (2), throw away the series before synchronization and take remaining series, which are denoted as $s_1(i)$, $s_2(i)$, $s_3(i)$ $(i = 1,2,3)$.

Step 3. Permutation stage.

Image pixels are permutated in the light of one of the series $s_j(i)$ $(j = 1,2,3)$ and formula

$$\begin{cases} x_{i+1} = (x_i + y_i + abs(fix(z_j)) + abs(fix(z_{j+k}))) \bmod M \\ y_{i+1} = (y_i + abs(fix(z_{j+k})) + K\sin(\frac{2\pi x_{i+1}}{N})) \bmod N \end{cases}, \quad (11)$$

where K is a constant, $abs(\cdot)$ returns to the absolute value, $fix(\cdot)$ rounds the element toward to zero resulting in an integer, (x_i, y_i) and (x_{i+1}, y_{i+1}) are the locations before and after permutation, respectively. k is a positive integer. z_j is in the light of one of the series $s_j(i)$ $(j = 1,2,3)$.

Step 4. Diffusion stage.

Pixel values are modified according to

$$v = p \oplus (c \times x_i + d \times y_i) \bmod L, \quad (12)$$

where p and v are pixels' values before and after diffusion, respectively. L is the gray scale of pixels. c and d are diffusion parameters based on

$$\begin{cases} c = abs(10^l x_j - round(10^l x_j)) \times 10^3 \\ d = abs(10^l y_j - round(10^l y_j)) \times 10^3 \end{cases}. \tag{13}$$

The inverse of the encryption process is the decryption of image.

4.2. Simulations and security analysis

According to tracking synchronization of Hindmarsh-Rose system via Genesio -Tesi system in section 3, typical Lenna image is chosen to be considered. For the encryption algorithm in section 4.1, the number of keys can be eighteen. It is large enough to resist exhaustive attacks. Fig.4 demonstrates the encryption and decryption of Lenna image. From Fig.4, it's obvious to see that the proposed method not only can encrypt Lenna image but also can effectively decrypt the cipher image.

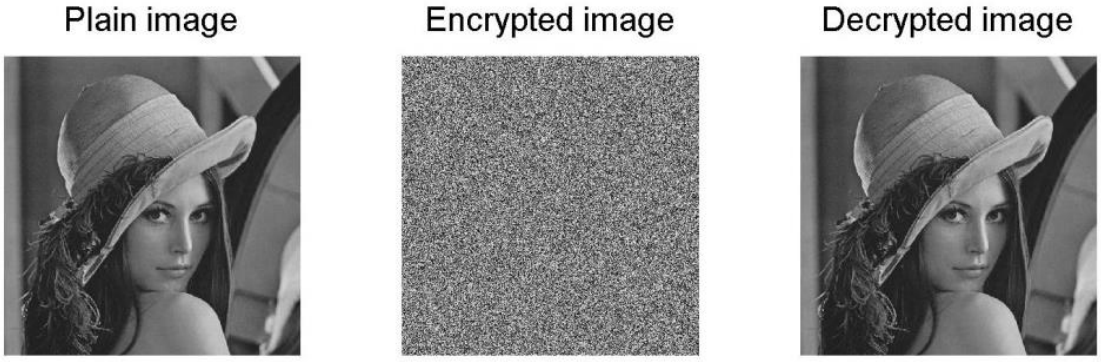

Fig.4. Encryption and decryption of Lenna image.

In security analysis, histogram of image is an important indicator reflecting the advantages and disadvantages of an encryption algorithm. If the histogram of the encrypted image has strong randomness, the encryption algorithm is good. Fig.5 depicts the histograms of plain Lenna image and the encrypted image in Fig.4. From Fig.5, it is easy to see that the histogram of encrypted Lenna image has strong random characteristics. This result suggests that the proposed encryption algorithm based on the tracking synchronization of Hindmarsh-Rose neuron system and Genesio-Tesi system can greatly enhance the randomness of the histogram of the encrypted image and so as to resist the statistical attack. Furthermore, adjacent pixel correlation coefficients in the horizontal direction, vertical direction and diagonal direction can be calculated via following formula

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{14}$$

where $\mathrm{cov}(x, y) = E(x - E(x))(y - E(y))$, $E(x)$ is average gray value of N pixels randomly selected and $\sqrt{D(x)}$ is the mean square error of the gray value of the selected pixel. Selected 2500 pixel and the adjacent pixel correlation coefficients in three directions are calculated using formula (14), which can be seen in Table 1. From Table 1, it's known, compared to the original image, the correlation coefficients of adjacent pixels in the cipher image are greatly reduced, which suggests that this encryption algorithm has strong anti-attack performance.

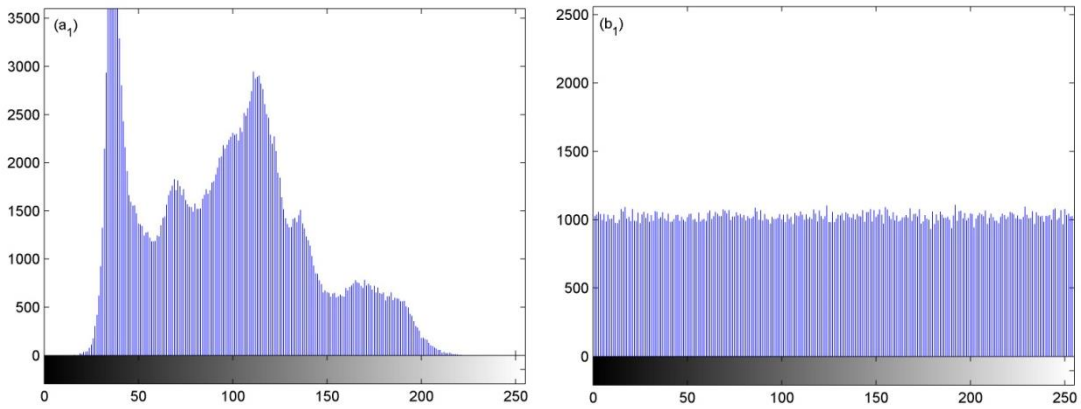

Fig.5. Histogram of Lenna image and the encrypted Lenna image,
(a_1) Histogram of Lenna image, (b_1) Histogram of encrypted Lenna image.

Table 1. Correlation coefficients between adjacent pixels

	Plain Lenna image	Encrypted Lenna image
horizontal direction	0.9336	0.0004
vertical direction	0.9738	-0.0020
diagonal direction	0.9759	0.0015

5. Conclusion

In this paper, an encryption algorithm is proposed based on the tracking synchronization of Hindmarsh-Rose system via Genesio-Tesi system. Lenna image, as an example, is encrypted using the proposed method. Results suggest that this encryption algorithm can fully hide the information of the image and protect the image from being attacked.

6. Acknowledgement

This work is supported by National Natural Science Foundation of China (Grant No. 61379064).

7. References

[1] Carroll T L, Pecora L M, Synchronization in chaotic systems, Physical Review Letters. 64: 821(1990).

[2] Hoang T M, A New Secure Communication model based on synchronization of coupled multidelay feedback systems, International Journal of Computer Systems Science & Engineering. 4: 240-246(2008).

[3] Wang H X, Lu Q S, Wang Q Y, Complete synchronization in coupled chaotic HR neurons with symmetric coupling schemes, Chinese Physics Letters. 22: 2173(2005).

[4] Zhu A L, Cooperation random mobile robots based on chaos synchronization, Mechatronics, ICM 4th IEEE International Conference. 1-5(2007).

[5] Jalan S, Kumar A, Zaikin A, et al. Interplay of degree correlations and cluster synchronization, Physical Review E. 94(6): 062202(2016).

[6] Tchakui M V, Woafo P, Dynamics of three unidirectionally coupled autonomous Duffing oscillators and application to inchworm piezoelectric motors: Effects of the coupling coefficient and delay, Chaos. 26(11): 113108(2016).

[7] Li TT, Li CR, Wang C, et al, Synchronization investigation of the network group constituted by the nearest neighbor networks under inner and outer synchronous couplings, Chinese Physics B. 25(12): 128902(2016).

[8] Feng C, Projective synchronization between two different time-delayed chaotic systems using active control approach. Nonlinear Dynamics. 62: 453-459(2010).

[9] Ma J, Ying HP, Pu ZS, An anti-control scheme for spiral under Lorenz chaotic signal, Chinese Physics Letters. 22: 1065-1068(2005).

[10] Ghosh D, Nonlinear-observer-based synchronization scheme for multiparameter estimation, Europhysics Letters. 84: 40012(2008).

[11] Odibat ZM, Adaptive feedback control and synchronization of non-identical chaotic fractional order systems, Nonlinear Dynamics. 60: 479-487(2010).

[12] Che Y Q, Wang J, Cui S G, et al, Chaos synchronization of coupled neurons via adaptive sliding mode control, Nonlinear Analysis Real World Applications. 12(6):3199-3206(2011).

[13] Hasler M, Maistrenko Y, Popovych O, Simple example of partial synchronization of chaotic systems, Physical Review E Statistical Physics Plasmas Fluids & Related Interdisciplinary Topics. 58(5): 6843-6846(1998).

[14] Yanchuk S, Maistrenko Y, Mosekilde E, Partial synchronization and clustering in a system of diffusively coupled chaotic oscillators, Mathematics & Computers in Simulation. 54(6):491-508(2001).

[15] Vieira M D S, Lichtenberg A J, Nonuniversality of weak synchronization in chaotic systems, Physical Review E Statistical Physics Plasmas Fluids & Related Interdisciplinary Topics. 56(4): R3741-R3744(1997).

[16] Taborov A V, Maistrenko Y L, Mosekilde E, Partial synchronization in a system of coupled logistic maps, International Journal of Bifurcation & Chaos. 10(5):1051-1066(2012).

[17] Novikov N, Gutkin B, Robustness of persistent spiking to partial synchronization in a minimal model of synaptically driven self-sustained activity, Physical Review E. 94(5-1): 052313(2016).

[18] Clusella P, Politi A, Rosenblum M, A minimal model of self-consistent partial synchrony. 18(9): 093037(2016).

[19] Daneshgar A, Khadem B, A self-synchronized chaotic image encryption scheme. Signal Processing Image Communication. 36:106-114(2015).

[20] Liu H, Wan H B, Tse CK, An encryption scheme based on synchronization of two-layered complex dynamical networks, IEEE Transactions On Circuits And Systems I-Regular Papers. 63(11): 2010-2021(2016).

[21] Wang H, Liang H F, Miao Z H, A new color image encryption scheme based on chaos synchronization of time-delay Lorenz system, Advances in Manufacturing. 4(4):1-7(2016).

[22] Hindmarsh J L, Rose R M, A model of the nerve impulse using two first-order differential equations, Nature. 296: 162(1982).

[23] Genesio R, Tesi A, Harmonic balance methods for the analysis of chaotic dynamics in nonlinear systems, Automatica. 28(3):531-548(1992).