Output Feedback Synchronization of A Novel Chaotic System And Its Application in Secure Communication

Arian Azarang
Department of electrical and computer engineering Tarbiat Modares University Tehran, Iran

Javad Ranjbar
Department of electrical and computer engineering Yazd University Yazd, Iran

Hamid Mohseni
Department of electrical and computer engineering Islamic Azad University, South Tehran Branch Tehran, Iran

Mohammad Ahi Andy
Department of electrical and computer engineering Tarbiat Modares University Tehran, Iran

Abstract
Chaotic signals have different properties in engineering applications which are the main of interests and many researchers concentrate on them. One of the important applications of chaotic signals is chaotic communications. In this paper, a novel chaotic system is used to communicate audio signals through wired channel. In order to use chaotic signals to communicate, the master and slave systems should be synchronized before any data transmission. In this correspondence, a novel output feedback controller is designed to synchronize the master and slave systems using only one state. After synchronization, analog audio signals are masked with one of the state of chaotic system to improve its privacy. Simulation results are provided to see the effectiveness of the chaotic masking in increasing data security. In order to make our proposed scheme practical, whole system is implemented using analog circuits and claims are demonstrated in practice.

Keywords
Chaotic signals; Output feedback controller; Chaos masking; Analog implementation.

1. Introduction

Chaotic signals have a variety of inherent features such as random-like, sensitive to initial conditions and hard to prediction. When Lorenz in 1963 introduced the first chaotic system [1], deep researches in applications of this field has been started. Although chaos theory and fractals has a large history in mathematics over 300 years, its applications in engineering and environment has a hot topic in the three past decades. Chaotic signals have a great potential to be applied in communication applications. One of the most important problem in chaos-based communications is synchronization of master and slave systems [2]. Furthermore, in practical applications the existence of random signal (such as noise) makes the synchronization goal of chaotic systems even more complex. For the purpose of synchronization, various types of methods are proposed. These methods can be categorized into two general groups: full-state synchronization [3, 4] and output feedback controller [5, 6]. In the full state scheme, all the state variables should be used to achieve the synchronization goal. On the other hand, output feedback controller methods only use the information of one state to synchronize the master and slave systems.

Chaotic signals have a variety of applications in engineering such as mechanical [7], biological [8], electronics [9] and optoelectronics systems [10]. Study of the chaos is an interesting subject because of its importance in detecting and controlling the dynamic behavior of the abovementioned systems [11]. On the other hand, chaotic signals have great potential for secure communication and image encryption. In this correspondence, an implementation and performance evaluation of an improved chaotic image encryption approach proposed by Suri et al. which scrutinized chaotic encryption techniques [12]. Ozkaynak et al. give a general attack scenario in order to conduct security analyses of chaos based cryptosystems [13]. An improvement color image encryption algorithm based on DNA operations and real and complex chaotic systems is proposed by Li et al. with one-time pad [14].

Chaos communications can be divided into three main group: Chaos Masking, Chaos Shift Keying and Chaos Modulation. Chaotic masking for the first time was proposed by Kocarev et al. in 1992 [15], in which the analog signal a(t) is added to one of the state of chaotic system, x(t). Chaos shift keying was presented by Parlitz et al. [16] and Dedieu et al. [17]. Chaos shift keying is mainly used to transmit digital signals. At the transmitter,

Manuscript received April 5, 2017
Manuscript revised April 20, 2017

two different chaotic systems are used for 0-bits and 1-bits of the information signal, respectively. That is, the employed chaotic system is switched from time to time by the information signal. At the receiver side, only one of the two chaotic systems is needed, and the information bits are recovered according to whether or not the response system can achieve chaos synchronization with the drive system. Chaos modulation was proposed in 1993 [18]. Different from chaos masking and chaos switching schemes, in a chaos modulation scheme the message signal m(t) is injected into the sender system so that its dynamics is changed according to the message signal continuously.

In this paper, we employ novel attractors in the field of chaos masking application. For this purpose, a novel output feedback controller is designed to synchronize the master and slave systems only with one state. After synchronization goal, the audio signal masks with one the state of chaotic system at the transmitter. After passing the signal through wired channel, the desired signal from the received signal should be recovered to achieve the transmitted audio signal.

This paper is organized as follows: Section II describes basic properties of the chaotic system and application of the chaotic systems in chaos masking. Section III provide simulation and implementation results of the proposed scheme. Finally, we conclude in section IV.

2. Chaos control and masking

A. Basic porpeties of the chaotic system

The integer order of chaotic system is proposed in [19] and defined as follows:

$$\begin{cases} \dot{x} = -10x + 10y + 1.5z + 3yz \\ \dot{y} = 70x - y \\ \dot{z} = -0.5x^2 - 0.5y^2 + 0.5xy - 5z \end{cases} \quad (1)$$

Where x, y and z are state variables. Due to wide range of variables, we use an "scaled-form" of the system where state variables are normalized as: $X = 1/5\,x$, $Y = 1/10\,y$, and $Z = 1/5\,z$ which the dynamic of (1) reduces to :

$$\begin{cases} \dot{X} = -10X + 20Y + 1.5Z + 30YZ, \\ \dot{Y} = 35X - Y, \\ \dot{Z} = -2.5X^2 - 10Y^2 + 5XY - 5Z. \end{cases} \quad (2)$$

Corresponding phase portraits with initial conditions [0.1, -0.1, 0.1] are shown in Fig. 1. It should be mentioned that Lyapunov exponents of the system (1) are $L_1 = 2.46$, $L_2 = -0.01$ and $L_3 = -18.43$

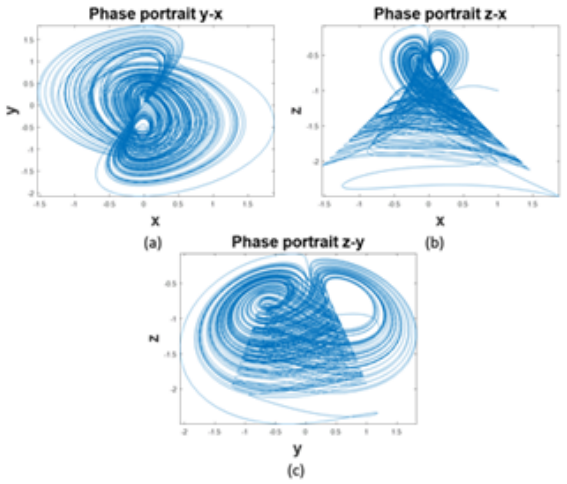

Fig. 1. Phase portraits of system (3), (a) Y-X space, (b) Z-X space and (c) Z-Y space.

A. Output feedback controller Design

In this sub-section, we design an output feedback controller which uses only one state to synchronize the master and slave systems. An important property of this scheme is that other states of the systems can be used to send and receive data and under certain conditions [20] the received signal can be recovered completely. We define state errors as: $e_1(t) = x_s(t) - x_m(t)$ $e_2(t) = y_s(t) - y_m(t)$ and $e_3(t) = z_s(t) - z_m(t)$

Consider the master system as follows:

$$\begin{cases} \dot{x}_m = -10x_m + 20y_m + 1.5z_m + 30y_m z_m \\ \dot{y}_m = 35x_m - y_m \\ \dot{z}_m = -2.5x_m^2 - 10y_m^2 + 5x_m y_m - 5z_m \end{cases} \quad (3)$$

And the slave system is defined as:

$$\begin{cases} \dot{x}_s = -10x_s + 20y_s + 1.5z_s + 30y_s z_s \\ \dot{y}_s = 35x_s - y_s + u(t) \\ \dot{z}_s = -2.5x_s^2 - 10y_s^2 + 5x_s y_s - 5z_s \end{cases} \quad (4)$$

Where lower indices m and s corresponds to master and slave systems , $u(t) = k(e_2(t))$ and K is the controller gain which should be designed. We construct the error system as follows:

$$\begin{cases} \dot{e}_1 = -10e_1 + e_2(20 + 30z_s) + e_3(1.5 + y_m) \\ \dot{e}_2 = 35e_1 - e_2 + ke_2 \\ \dot{e}_3 = e_1(-2.5(x_s + x_m) + 5y_s + 5x_m) + e_2(-10(y_s + y_m)) - 5e_3 \end{cases} \quad (5)$$

In this paper, we use the Lyapunov function to obtain the synchronization of master and slave systems. The Lyapunov candidate function of system (2) is defined as:

$$V = ae_1^2 + be_2^2 + ce_3^2 \quad (6)$$

Where a, b and c are positive constants. Taking the derivative of Eq. (6) with respect to time yields

$$V = 2ae_1e_1 + 2be_2e_2 + 2ce_3e_3 \quad (7)$$

By substituting (5) into (7), we have:

$$\begin{aligned} V &= -20ae_1^2 + (40a + 60az_s + 70b)e_1e_2 + (3a + 60ay_m - 5c(x_s + x_m) + 10cy_s + 10cx_m)e_1e_3 + (2bk - 2b)e_2^2 \\ &+ (-20c(y_s + y_m))e_2e_3 - 10ce_3^2 \le (-20a)e_1^2 + (40a + 70b + 60a|z_s|)|e_1||e_2| + (3a + 60a|y_m| + 20c|x_m| + 10c|y_m|)|e_1||e_3| \\ &+ (2bk - 2b)e_2^2 + (40c|y_m|)|e_2||e_3| - 10ce_3^2 \le (-20a)e_1^2 + (40a + 70b + 60aZ)|e_1||e_2| \\ &+ (3a + 60aY + 20cX + 10cY)|e_1||e_3| + (2bk - 2b)e_2^2 + (40cY)|e_2||e_3| - 10ce_3^2 = e^TAe \end{aligned} \quad (8)$$

Where X, Y, Z are the upper bounds of the state variables, $e = (|e_1| \; |e_2| \; |e_3|)^T$ and

$$A = \begin{bmatrix} -20a & 40a + 70b + 60aZ & 3a + 60aY + 20cX + 10cY \\ * & 2bk - b & 40cY \\ * & * & -10c \end{bmatrix}. \quad (9)$$

In order to ensure that the state errors converge to zero, matrix A should be negative definite. In this paper, we solve the abovementioned problem with MATLAB' LMI Control Toolbox.

A. Chaos Masking

Due to inherent properties of chaotic signal in hiding information, they are used in secure communications. In this paper, we briefly describe the chaotic masking scheme. In [20], the authors demonstrate that under certain conditions the received chaotic signal can be recovered completely. First, before any data transmission, the two systems should be synchronized with each other using abovementioned controller. After passing certain amount of time Ts (the time when error of the synchronization become negligible), we use the state z(t) to mask the data with it. Therefore, we have:

$$m(t) = z_m(t) + i(t) \quad (10)$$

Where i(t) corresponds to the audio input signal and m(t) is the result of masking. The signal m(t) is transmitted to the receiver with the effect of Gaussian white noise. At the receiver, the received signal subtracted from synchronized state zs(t). We have:

$$r(t) = \hat{m}(t) - z_s(t) = z_m(t) + i(t) + n(t) - z_s(t) \quad (11)$$

Where r(t) is the received signal, n(t) corresponds to additive Gaussian noise. As we describe above, after time Ts, the error of the system is negligible and therefore the term zm(t)-zs(t) approximately is zero. There are some key points which should be mentioned. As depicted above, the chaos masking adds the audio input information to one of the states of chaotic system. So, if the amplitude of the audio data becomes larger and dominates the amplitude of the system state, the dynamical behavior of the slave system changes and no desired data will be available at the receiver. It is vital that the amplitude of the audio should be in the order of chaotic signals for successful data transmission. Another important thing is that data transmission is done in a noisy environment and the power of noise is infinite. If the amplitude of noise is considerable in comparison with chaos masked data, the data will be lost.

3. Impementations and Results

In this section, we implement the chaos masking communications step by step. First, the original chaotic system (corresponds to Eq. 2) should be implemented. The result is shown in Fig. 2. In this implementation, the components consist of low cost and quad Op-Amp (TL084), analog multiplier (AD633) and metal film resistors and capacitors. The slave system exactly has the same implementation except in the adding controller according to Eq. 4. The design of controller is done in two steps: the first step is the controller term of the Eq. 4. As depicted in Fig. 3(a). In the second step,

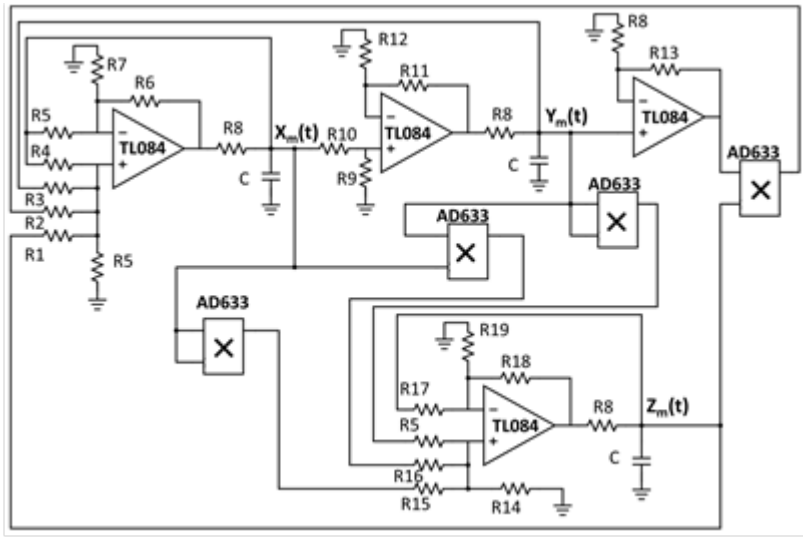

Fig. 2. Circuit diagram for equations (3). AD633: Analog multiplier, TL084 low cost quad op-amps. R1 = 100kΩ, R2 = 5kΩ, R3 = 7.5kΩ, R4 = 25kΩ, R5 = 10kΩ, R6 = 150kΩ, R7 = 10kΩ (potentiometer), R8=1kΩ, R9 = 1.2kΩ, R10 = 1.6kΩ, R11 = 56kΩ, R12 = 680Ω, R13 = 9kΩ, R14 = 12kΩ, R15 = 40kΩ, R16 = 20kΩ, R17 = 250kΩ, R18 = 1MΩ, R19 = 3kΩ, and C = 200nF. In all circuits we have used supply voltages V+ = +9V and V- = -9V.

the controller term should be injected in the construction of the second state of slave system as a new input according to Fig. 3(b).

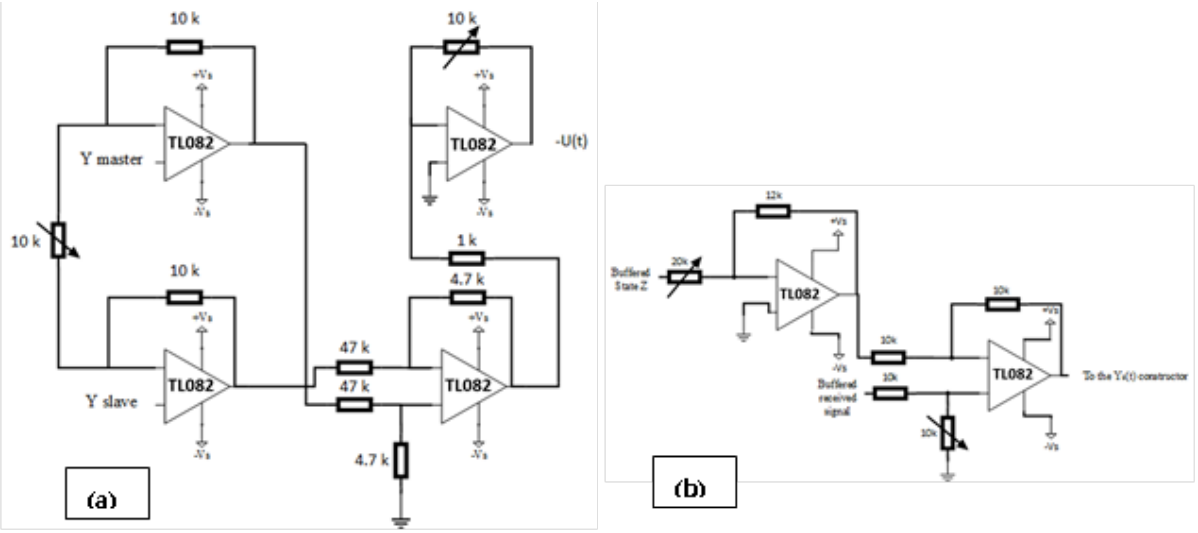

Fig. 3. Controller part. (a) The designed controller corresponds to Eq. 4. (b) Injection of the designed controller to reconstruct the second slave state. In all circuits we have used supply voltages V+ = +9V and V- = -9V.

The practical results of the controlled master and slave system with each other are reported in Fig. 4 for designing gain K=2.15. As depicted before, Synchronization of the master and slave systems is a crucial issue in the application of chaos masking. In the synchronization phase, we used the second state of master and slave systems. So, the first and third states can be used for data transmission. There is a key point which should be mentioned. Due to synchronization time and physical limitations, before any data transmission we should wait until the master and slave systems has been synchronized completely. The result of implementation of the controller at the receiver are provided in the Fig. 4. As it is clear in Fig. 4, the designed output feedback controller can successfully synchronize the master and slave systems.

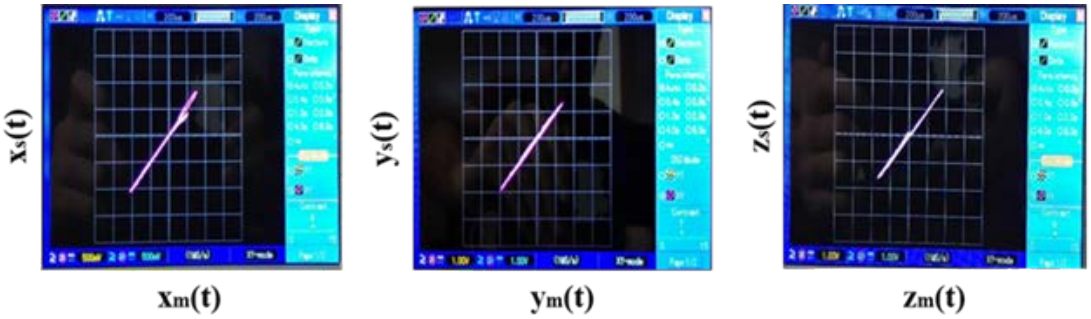

Fig. 4. Result of applying controller to the slave system. (Left to right) (a) Xs(t) vs. Xm(t), (b) Ys(t) vs. Ym(t) and (c) Zs(t) vs. Zm(t).

For the chaos masking part, we can use any audio input device for out experiment. We decide to use a limited song as input. Note that the audio which is came from the audio input device has small amplitude. In order to magnify the amplitude, we design an audio amplifier using LM396. This part is the first step in the chaos masking scheme which is shown in Fig. 5. At the second step, in order to eliminate loading effect of the previous stages, the magnified audio data and third system state (Zm(t)) are buffered. The obtained waveforms are added to each other to form chaos masked signal and transmitted to the receiver side through wired noisy channel. At the receiver, the masked signal is received with a small delay transmission in noisy situation.

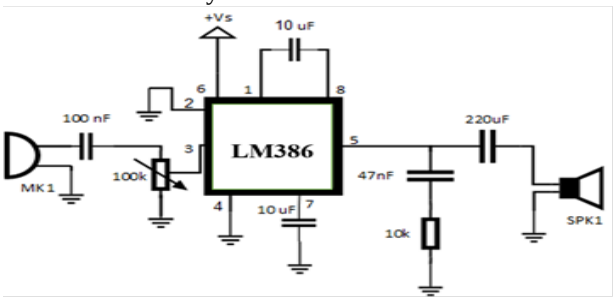

Fig. 5. Audio amplifier part for the chaos masking. In all circuits we have used supply voltages V+ = +9V.

It should be again mentioned that the master and slave systems have been synchronized before any data transmission. So, the received signal is subtracted from the third state of the slave system. As theoretically described above, the obtained signal should be noisy version of the original audio data.

We employ a low pass filter at this stage to decrease the power of the noise. In Fig. 6 the original audio data are shown for a limit time (16 seconds).

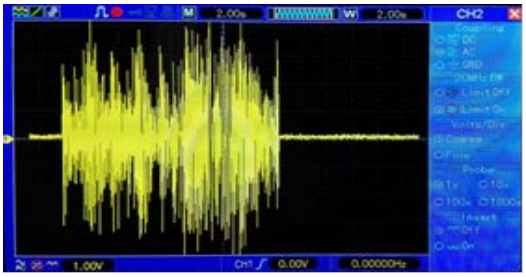

Fig. 6. Original audio data for the application of chaos masking.

Then, the magnified audio input is buffered and added to the third state of the master system (Zm(t)). The obtained signal called chaos masked signal which is like a noise rather than a desired signal and is shown in Fig. 7. The received signal at the receiver should be recovered in order to obtain the desired signal. For this purpose, we first implement a subtraction circuit as depicted in Fig. 8.

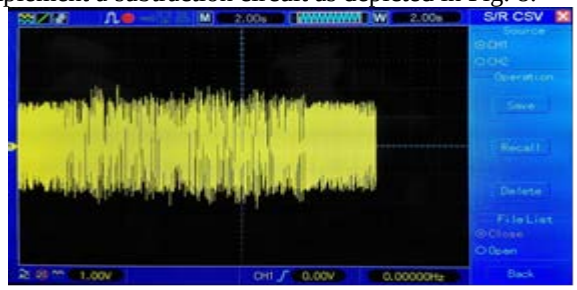

Fig. 7. Chaos masked of the original input data.

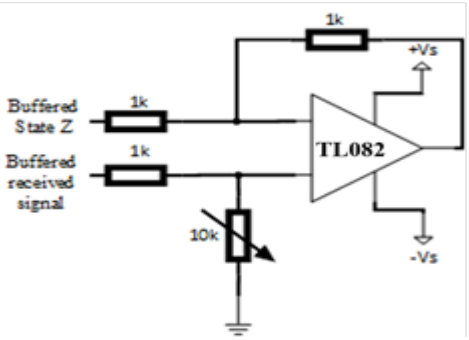

Fig. 8. Subtraction circuit to recover the original audio data.

Due to eliminate the loading effect of the previous stages, the inputs should be buffered. At the final stage, the extracted audio data should be filtered to decrease the power of the noise and better recovery. The final result is provided in Fig. 9.

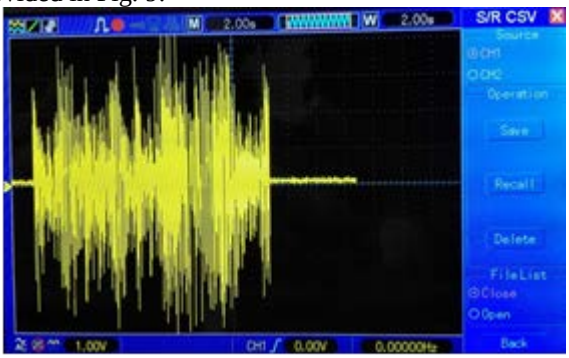

Fig. 9. The recovered audio data at the receiver side.

4. Conclusion

In this paper, we concentrate on applications of chaotic systems in secure communications. In this correspondence, a novel integer order chaotic system is used for the chaos masking. In order to synchronize the master and slave system, a new output feedback controller is designed using LMI toolbox and implemented by analog circuits. To achieve practical results, the chaos masking communication scheme is implemented by utilizing analog circuits. We show that the master and slave systems can synchronize only with one state and audio data can be recovered successfully at the receiver side.

References

[1] Lorenz, E. N. Deterministic nonperiodic flow. J. Atmos. Sci., 20, (1963) 130-141.

[2] Chua, Leon O., et al. "Chaos synchronization in Chua's circuit." Journal of Circuits, Systems, and Computers 3.01 (1993) 93-108.

[3] Wen, Guilin, and Daolin Xu. "Nonlinear observer control for full-state projective synchronization in chaotic continuous-time systems." Chaos, Solitons & Fractals 26.1 (2005) 71-77.

[4] Ouannas, Adel. "On full-state hybrid projective synchronization of general discrete chaotic systems." Journal of Nonlinear Dynamics 2014 (2014) 1-6.

[5] Hou, Yi-You, Teh-Lu Liao, and Jun-Juh Yan. "H∞ synchronization of chaotic systems using output feedback control design." Physica A: Statistical Mechanics and Its Applications 379.1 (2007) 81-89.

[6] Hong, Yiguang, Huashu Qin, and Gunarong Chen. "Adaptive synchronization of chaotic systems via state or output feedback control." International Journal of Bifurcation and Chaos 11.04 (2001) 1149-1158.

[7] Awrejccewicz, J., Kudra, G., Wasilewski, G. Chaotic zones in triple pendulum dynamics observed experimentally and numerically. Applied Mechanics and Materials, 9, (2008) 1-17.

[8] Carlen, E.; Chatelin, R., Degond, P., Wennberg, B. Kinetic hierarchy and propagation of chaos in biological swarm models. Physica D: Nonlinear Phenomena, 260, (2013) 90-111.

[9] Caponetto, R., Di Bernardo, G., Di Cola, E., Occhpinti, L. A new chaotic system for the authentication and electronic certification procedures. In: Proceedings of the 6th IEEE International Conference on Electronics, Circuits and Systems (ICECS'99), Paphos, Cyprus, (1999) 1235-1238.

[10] Callan, K. L., Illing, L., Gao, Z., Gauthier, D. J.; Schöll, E. Broadband chaos generated by an optoelectronic oscillator. Phys. Rev. Lett., 104, (2010) 113901-1:4.

[11] Li, Chun-Lai, et al. "Stabilization for a class of chaotic and hyperchaotic systems with constant switch control strategy." Optik-International Journal for Light and Electron Optics 127.5 (2016): 3109-3111.

[12] Suri, Shelza, and Ritu Vijay. "An implementation and performance evaluation of an improved chaotic image encryption approach." Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on. IEEE, 2016.

[13] Özkaynak, Fatih, and Ahmet Bedri Özer. "Cryptanalysis of a new image encryption algorithm based on chaos." Optik-International Journal for Light and Electron Optics 127.13 (2016) 5190-5192.

[14] Li, Xiang, et al. "An improvement color image encryption algorithm based on DNA operations and real and complex chaotic systems." Optik-International Journal for Light and Electron Optics 127.5 (2016) 2558-2565.

[15] Kocarev, Lj, et al. "Experimental demonstration of secure communications via chaotic synchronization." International Journal of Bifurcation and Chaos 2.03 (1992) 709-713.

[16] Parlitz, Ulrich, et al. "Transmission of digital signals by chaotic synchronization." International Journal of Bifurcation and Chaos 2.04 (1992) 973-977.

[17] Dedieu, Herve, Michael Peter Kennedy, and Martin Hasler. "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits." IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing 40.10 (1993) 634-642.

[18] Halle, K. Sean, et al. "Spread spectrum communication through modulation of chaos." International Journal of Bifurcation and Chaos 3.02 (1993) 469-477.

[19] Azarang, Arian, et al. "A new fractional-order chaotic system and its synchronization via Lyapunov and improved Laplacian-based method." Optik-International Journal for Light and Electron Optics 127.24 (2016): 11717-11731.

[20] Cuomo, Kevin M., Alan V. Oppenheim, and Steven H. Strogatz. "Robustness and signal recovery in a synchronized chaotic system." International Journal of Bifurcation and Chaos 3.06 (1993) 1629-1638.