ISSN 1392–124X (print), ISSN 2335–884X (online) INFORMATION TECHNOLOGY AND CONTROL, 2015, T. 44, Nr. 3

A Novel Chaotic System for Secure Communication Applications

Ali Durdu, Ahmet Turan Özcerit

Department of Computer Engineering, Faculty of Computer and Information Science,
Sakarya University, 54187 Serdivan, Sakarya, Turkey,
email: {adurdu,aozcerit}@sakarya.edu.tr

Yılmaz Uyaroğlu

Department of Electrical & Electronics Engineering, Engineering Faculty
Sakarya University, 54187 Serdivan, Sakarya, Turkey
email: uyaroglu@sakarya.edu.tr

crossref http://dx.doi.org/10.5755/j01.itc.44.3.7720

Abstract. The secure communication using synchronization between identical chaotic systems have been introduced in literature for a long time. A well-known practical application of chaotic synchronized systems is the Pecora and Carroll (P-C) secure communication method. In this paper, the P-C secure communication algorithm is applied to a novel three dimensional, autonomous chaotic attractor. Having a 45° slope between sub-driver and sub-receiver circuits of a novel chaotic attractor clearly demonstrates that it can be used for the purpose of secure communications.

Keywords: chaotic systems, synchronization, secure communication.

1. Introduction

Chaos is non-linear, irregular patterned and most complex steady-state behavior. In earlier periods, chaotic systems were considered inappropriate for synchronizing purposes since they are very sensitive to initial conditions and system parameters, Pecora and Carroll proved that chaotic systems could be synchronized by starting different initial conditions in 1990 [1, 2]. In this study, a new chaotic system has been presented and its synchronization conditions has been verified by the P-C method. The synchronized chaotic system accompanied by secure communication applications have been implemented in Matlab Simulink ™ environment. The experimental results show that the chaotic system designed can be used in secure communication.

Pecora and Carroll introduced an original chaotic system and then separated it into two individual subsystems: the driver and the responder. Once creating an identical responder sub-system in the receiver module and driving it with the original driver, chaotic synchronization can be achieved, and this fact can be demonstrated both theoretically and experimentally. Since then, the P-C method was used in many synchronization and secure communication applications. For example, Endo and Chua have presented two phased-locked loops derived from a known phase locked loop, which is driven by chaotic signals [3]. Gonzalez-Miranda has presented secure communications application examples through one-way binding of low-dimensional systems by unidirectional coupling [4]. Liao and Tsai have proposed a solution for adaptive synchronization problem in driver-oriented chaotic systems in which signals are conducted in scalar [5]. Pehlivan and Uyaroglu have implemented an example of diffusionless Lorenz application which is a one-parameter chaos model designed for secure communication purposes and they have verified the effectiveness of the system with numeric and PSpice model simulations. In addition to simulations, the study has been implemented in hardware manner [6]. Qingli et al. have presented the synchronization of two chaotic systems for chaotic secure communication system based on Particle Swarm Optimization-BP neural network which uses chaos masking technology [7]. Zhang and Zhao have proposed a two-stage driver system by employing the PC method on Lorenz chaos model for the field of secure communication [8]. Cheng and Cheng have suggested a robust and regular synchronization system for two different chaotic systems, exposing to a bounded noise [9]. Zhang and Zhang have proposed a new method of complete dislocated general hybrid projective synchronization model in which the unpredictability of the scaling factor in projective synchronization is used to increase the security of the communication [10]. Wang et al. [11] and Tang et al. [12] have adapted Chen system by applying to secure communication field. Zaher [13] and Zapateiro et al. [14] have presented Duffing system applied to secure communication. Yang, Zhu [15], Pisarchik and Ruiz-Oliveras [16], Al-Hussaibi [17], and Zhao [18] have presented secure communication for different areas. Further, the synchronized chaotic systems have been used in many secure communications applications [19-23]. Kocamaz and Uyaroglu have proposed non-identical synchronization, anti-synchronization and control of chaotic single-machine infinite-bus power system via active control method [24]. They have introduced a new chaotic model and proved that it meets the secure communication requirements with chaotic-rich behaviors.

The rest of the paper is organized as follows. In Section 2, a new chaotic system and its numeric model are introduced. This section also elaborates on Lyapunov exponentials, Kaplan-Yorke dimension, equilibrium points and Jacobian matrix of the proposed chaotic system. In Section 3, Simulink synchronization model of the chaotic system is presented. The Section 4 shows the proposed chaotic secure communication system in Matlab-Simulink model. The results are discussed and concluded in the last section.

2. Proposed Chaotic System

In this study, a new chaotic system has been developed, which is in autonomy nonlinear first-degree mode, as a result of a set of numerical models and associated simulations. The proposed chaotic system has been modeled under Matlab-Simulink environment as given in Fig. 1. It is very important that the rich behavior of the chaotic system can obfuscate the communication data for higher security requirements. The phase portraits of the chaotic system presented have been obtained by using system parameters (a=4, b=6, c=10, d=5) and initial conditions (X_0=1, Y_0=1, Z_0=0) as shown in Fig. 2. In addition, the nonlinear equations of the proposed chaotic system are given in Eqs. (1):

$$\begin{aligned} \dot{X} &= aX - bYZ \\ \dot{Y} &= -cY + XZ \\ \dot{Z} &= X - dZ + XY \end{aligned} \quad (1/).$$

Lyapunov exponent λ is calculated as shown in Eq. (2):

$$\lambda = \frac{1}{t_N - t_0} \sum_{k=1}^{N} \log_2 \frac{d(t_k)}{d(t_{k-1})}. \quad (2)$$

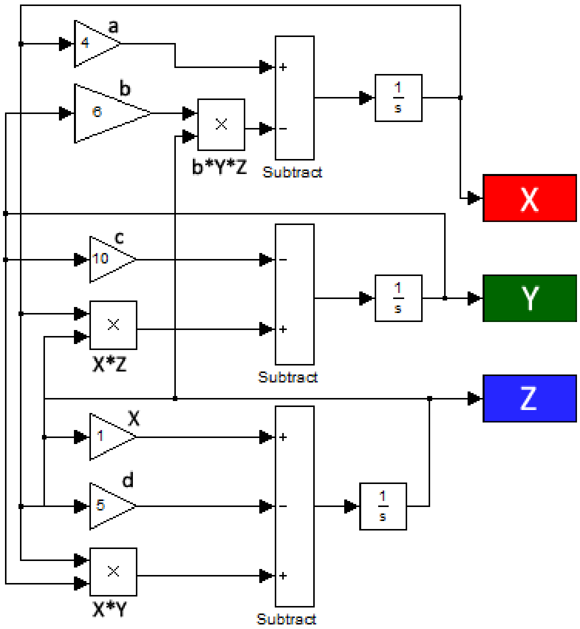


Figure 1. Matlab-Simulink model of proposed chaotic system

Kaplan and Yorke presented an interesting conjecture of the chaotic attractor to Lyapunov spectrum [25] as given in Eq. (3).

$$D_L = j - \frac{\sum_{i=1}^{j} \lambda_i}{\lambda_j + 1}. \quad (3)$$

We have found Lyapunov exponents as λ_1 = 3.38212, λ_2 = 0.831839, and λ_3 = -15.214. These three exponents found have proved that the behavior of the proposed system is chaotic. The graph of each calculated exponent is drawn in Fig. 3 to be a proof for the chaotic behavior of the proposed system. Having substituted Lyapunov exponents in the formula given below, Kaplan-Yorke dimension of the proposed chaotic system can be calculated:

$$D_L = 3 - \frac{3.38212}{15.214} = 2.7776. \quad (4)$$

This chaotic system has five equilibrium points: E_1(0, 0, 0), E_2(5.3949, 1.393, 2.582), E_3(9.2679, -2.393, -2.582), E_4(-9.2679, -2.393, 2.582) and E_5(-5.3949, 1.393, -2.582).

The Jacobian matrix has been obtained by linearizing the system at the equilibrium points:

$$J = \begin{bmatrix} a & -bZ & -bY \\ Z & -c & X \\ Y+1 & X & -d \end{bmatrix} = \begin{bmatrix} 4 & 0 & 0 \\ 0 & -10 & 0 \\ 1 & 0 & -5 \end{bmatrix}. \quad (5)$$

Characteristic equation has been obtained by providing following condition, |λI − J| = 0. Eigenvalues are determined as λ_1=4, λ_2=-5, and λ_3=-10.

Fig. 4 shows the bifurcation diagram with parameter c, demonstrating a period-doubling route to chaos.

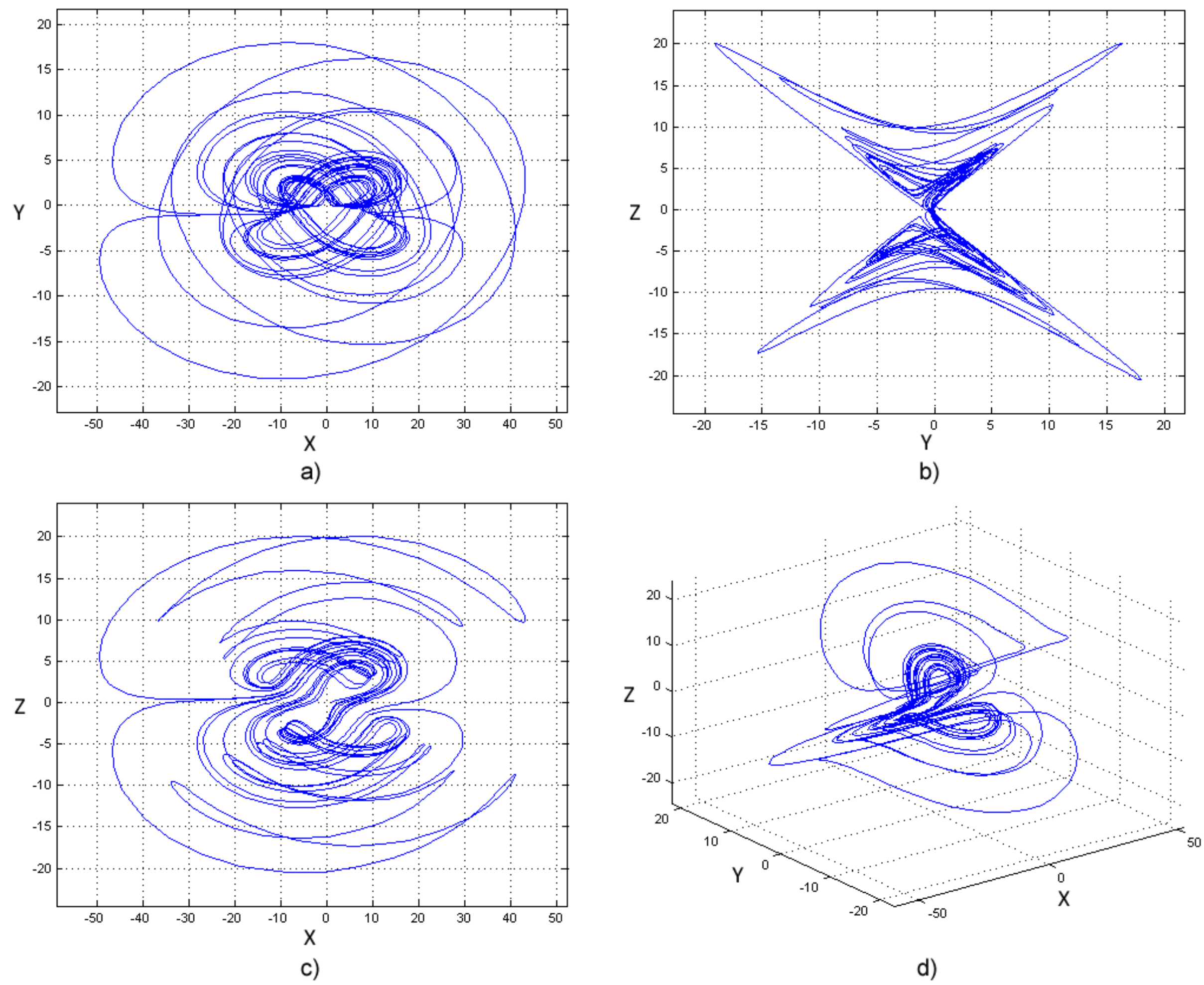


Figure 2. Phase portraits of proposed chaotic system: (a) *X-Y*, (b) *Y-Z*, (c) *X-Z*, (d) *X-Y-Z*

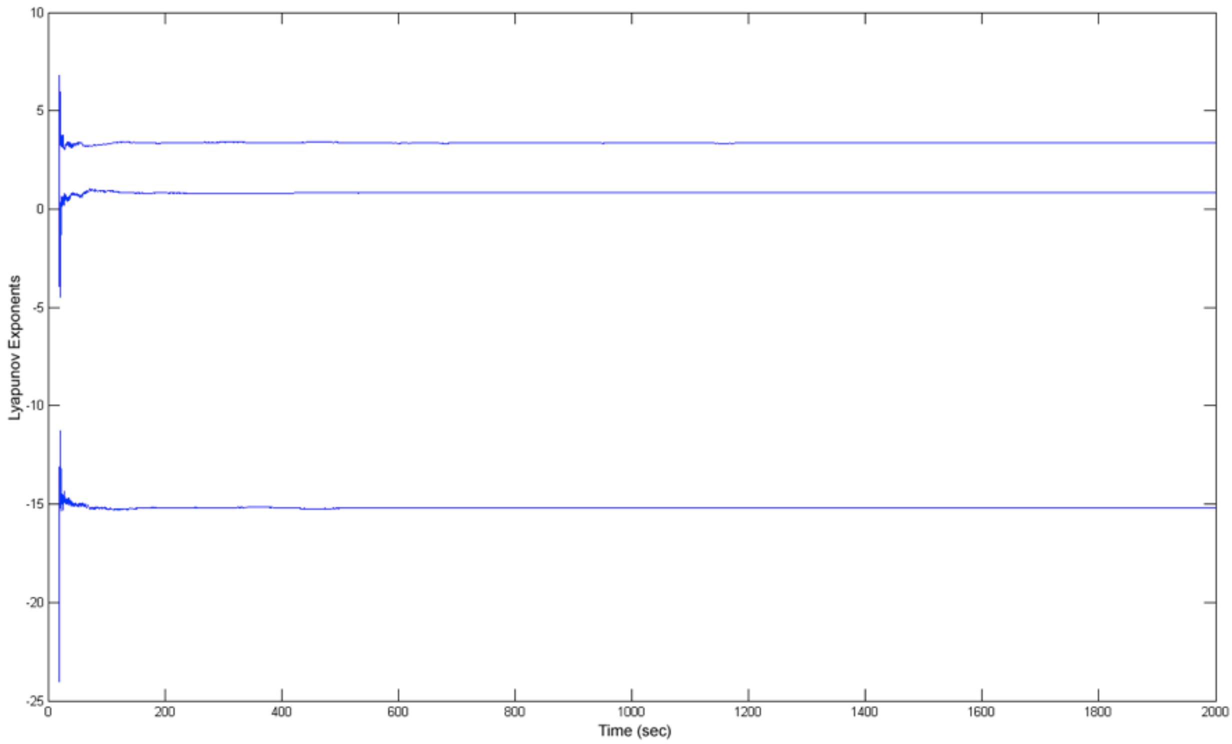


Figure 3. Lyapunov exponents of proposed chaotic system

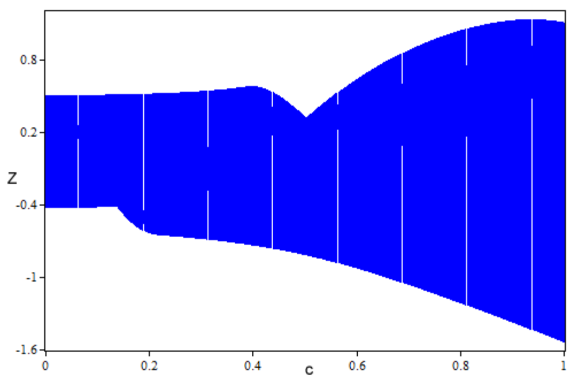


Figure 4. Bifurcation diagram to illustrate chaos in Z against parameter c

3. Synchronization of the Chaotic System

By applying the P-C method to the dynamic equations of the proposed system, the synchronization diagram has been obtained as seen in Fig. 5.

X, Y and Z variables stimulate to the sub systems directly as seen in Fig. 5.

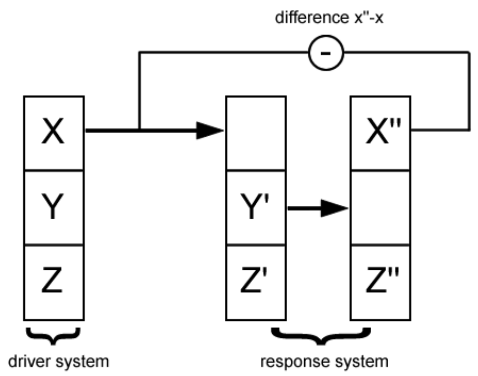


Figure 5. The block diagram of P-C Synchronization [1]

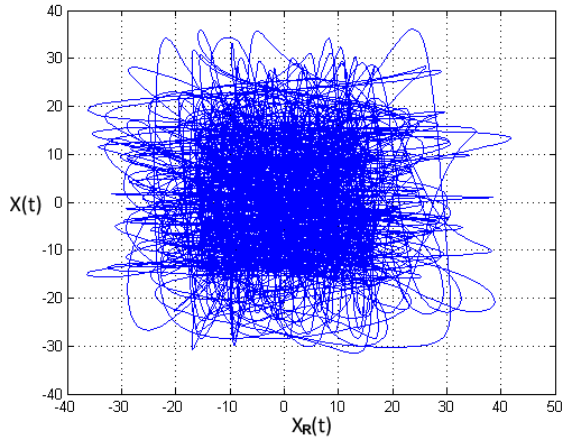
Transmitter circuit equations of the designed system are given in Eqs. (1). As seen in Eqs. (6), $\dot{Y}$ and $\dot{Z}$ can be written in first-order stable response-subsystem as follows:

$$\begin{aligned}\dot{Y} &= -c\dot{Y} + X\dot{Z} \\ \dot{Z} &= X - d\dot{Z} + X\dot{Y}\end{aligned} \quad . \tag{6}$$

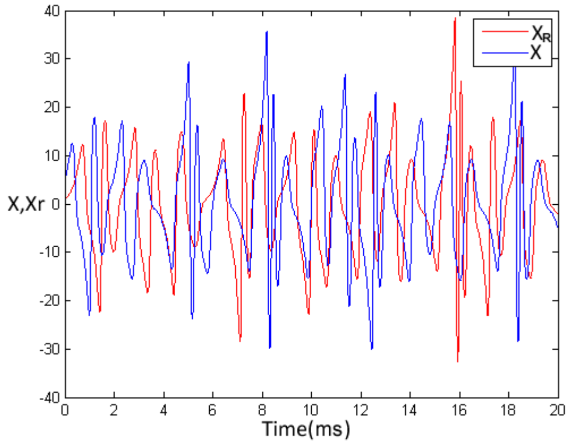
And as seen in Eqs.(7), $\ddot{X}$ and $\ddot{Z}$ can be written in the second order stable response-subsystem as follows [5, 26]:

$$\begin{aligned}\ddot{X} &= a\ddot{X} - b\dot{Y}\ddot{Z} \\ \ddot{Z} &= \ddot{X} - d\ddot{Z} + \ddot{X}\dot{Y}\end{aligned} \quad . \tag{7}$$

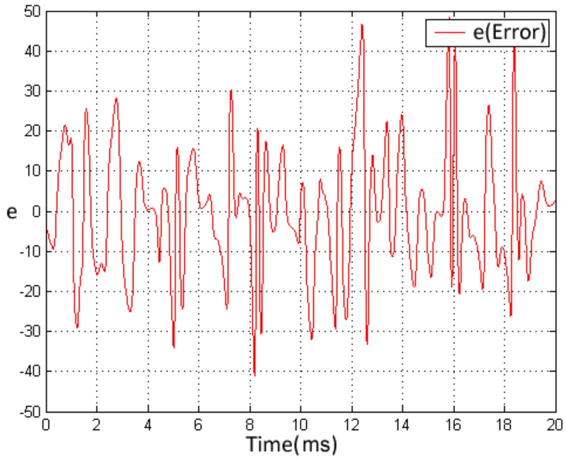
X_R, Y_R, and Z_R are used as $\ddot{X}$, $\dot{Y}$ and $\ddot{Z}$ in the system, respectively. In this study, we have utilized the synchronization between X and X_R. Parameter values have been chosen for two systems as (X_0, Y_0, Z_0) = {1, 1, 0} and (X_{R0}, Y_{R0}, Z_{R0}) = {5, 2, 1}, respectively and the parameter a is selected as 2.028. Once the simulation runs with distinct initial conditions, X-state variables along with time domain signals and variation of these signals in respect to each other have been obtained as shown in Fig. 6. The signal varies within a few milliseconds, and it proves that chaotic system is very sensitive to initial conditions.



a)



b)



c)

Figure 6. Pre-synchronization behavior: (a) time series driving (X), response (X_R), (b) X / X_R phase, (c) sync (e = error signal)

Having determined the initial conditions for the synchronization, both driver and response systems have been created in Matlab-Simulink environment as shown in Fig. 7.

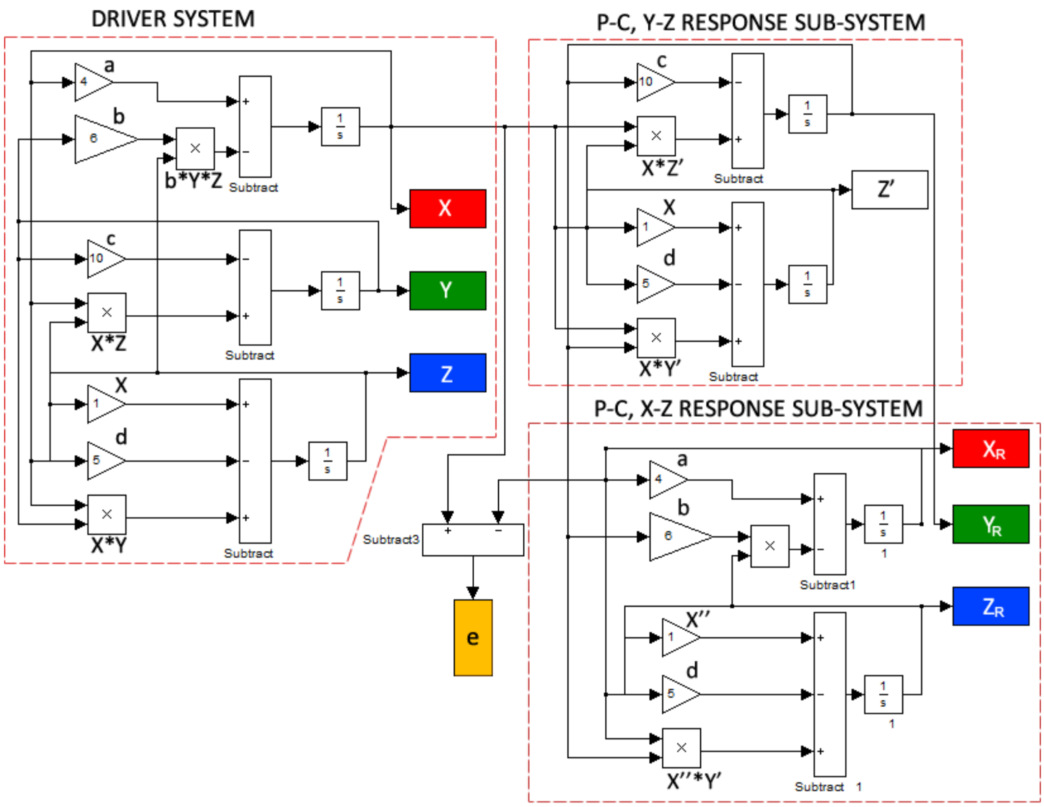
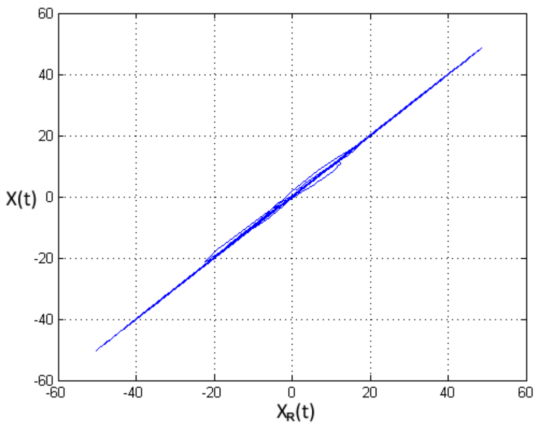
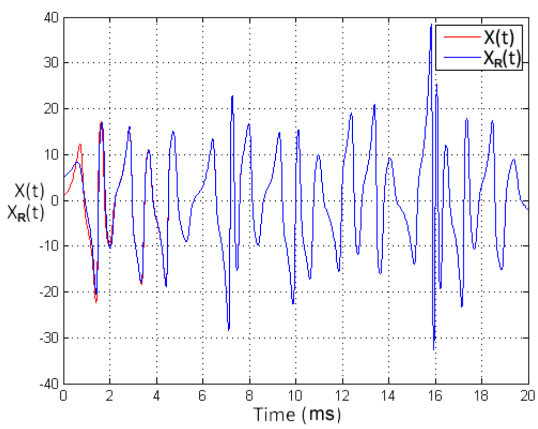


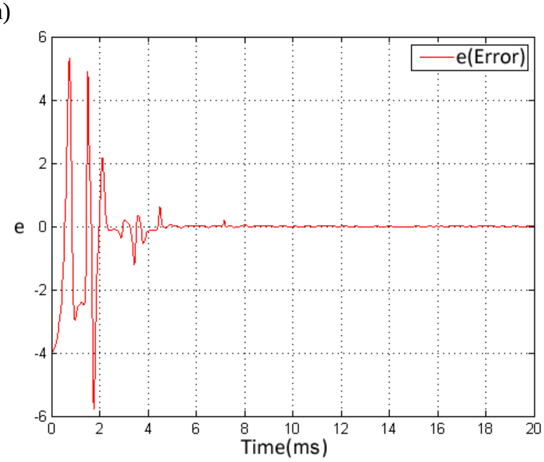
Figure 7. Simulink P-C synchronization modeling of proposed system



a)



b)



c)

Figure 8. Post-synchronization (a) X and X_R time, (b) X and X_R phase, (c) Sync e = error signal

As seen in Fig. 8a, once the simulation is started, it is observed that the drive signal X and response signal X_R become synchronized within a very short amount of time. These two signals change relative to each other as shown in Fig. 8b, and note that, after a short time, the ratio of signals are seemed to be 1.

The difference (e = error) signal is obtained by subtracting X from X_R. As seen in Fig. 8c, after approximately five milliseconds, the signals are synchronized and the error signal equals zero. Hence, the transmitter and receiver circuitry are synchronized in a sufficient amount of time, i.e. 3-5ms.

4. Chaotic Secure Communication Modeling of the Chaotic System

A novel chaotic system as the chaotic method of hiding the transmitter circuitry for secure communication has been established and related equations are given in Eqs. (1). The equations of the transmitter circuit are as follows:

$$\begin{aligned} \dot{X}_R &= aS(t) - bY_R Z_R \\ \dot{Y}_R &= -cY_R + S(t)Z_R \\ \dot{Z}_R &= S(t) - dZ_R + S(t)Y_R \end{aligned} \qquad (8)$$

Principle scheme for chaotic information hiding communication method is given in Fig. 9. Information is represented by a signal of sinus having value of 0.04V. Information signal $I(t)$, is summed with the chaotic signal $X(t)$ and it is then transferred into the transmission medium. Transmitted signal $S(t)$, is the sum of both signals. According to the P-C method at the receiver side, chaotic signal $X(t)$ is synchronized with chaotic signal $X_R(t)$ is subtracted from $S(t)$ thereby, signal $Ic(t)$ is obtained. Chaotic communication using a novel chaotic system supported by P-C synchronization has been simulated under Matlab-Simulink environment. The functional model of the system is presented in Fig. 10.

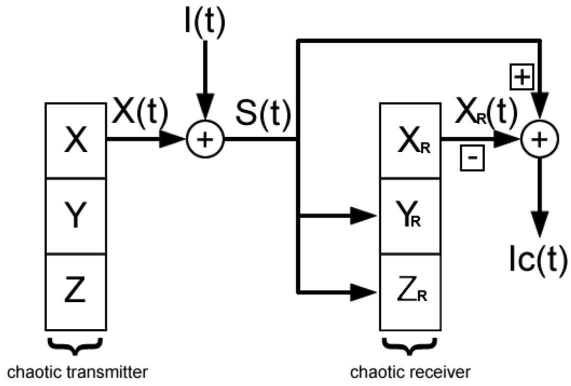


Figure 9. Principle scheme for chaotic secure communication [6]

The output signals of the block diagram given in Fig. 10 are obtained using numeric simulation tools. The signals of I(t), $S(t)$, $Ic(t)$-$I(t)$ and error rate are presented in Fig. 11 which proves that transmitted signal $I(t)$ and received signal $Ic(t)$ are virtually identical. In addition, the error rates in each case are almost zero as shown in Fig. 11c.

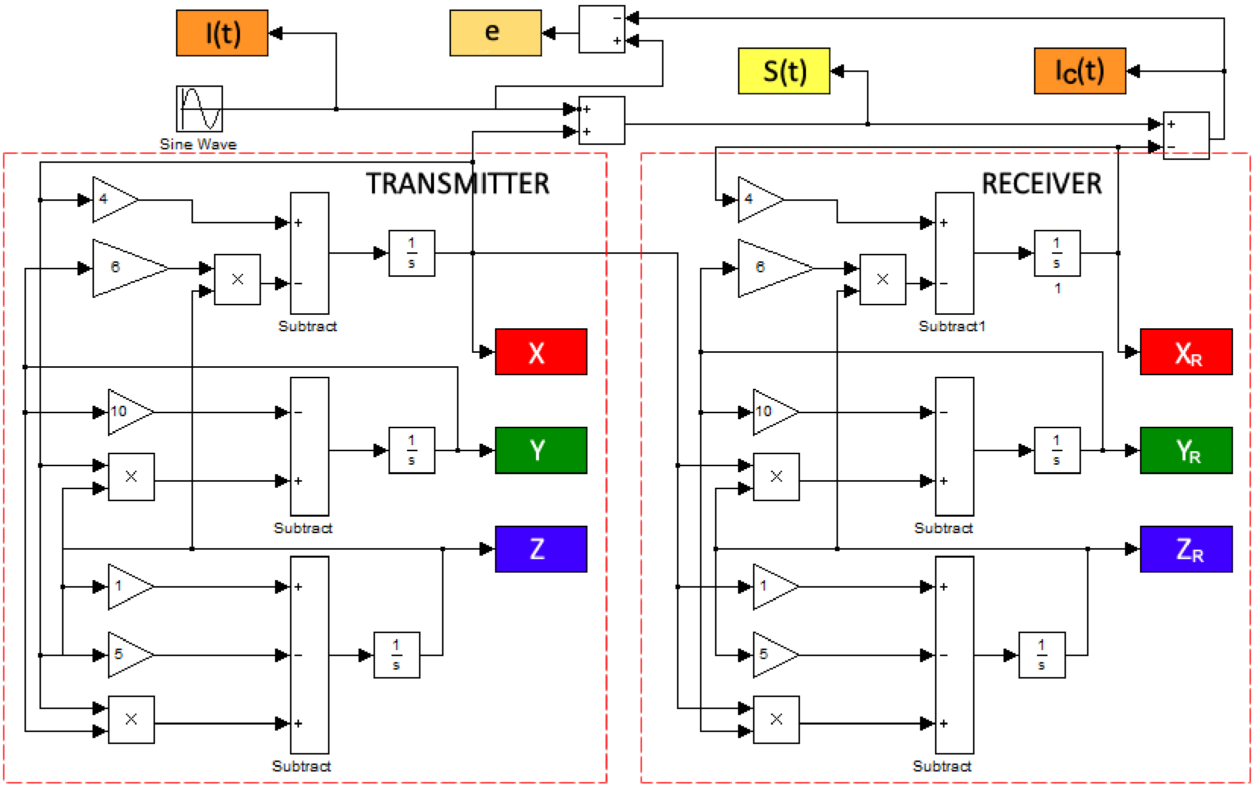


Figure 10. Matlab modeling of chaotic secure communication

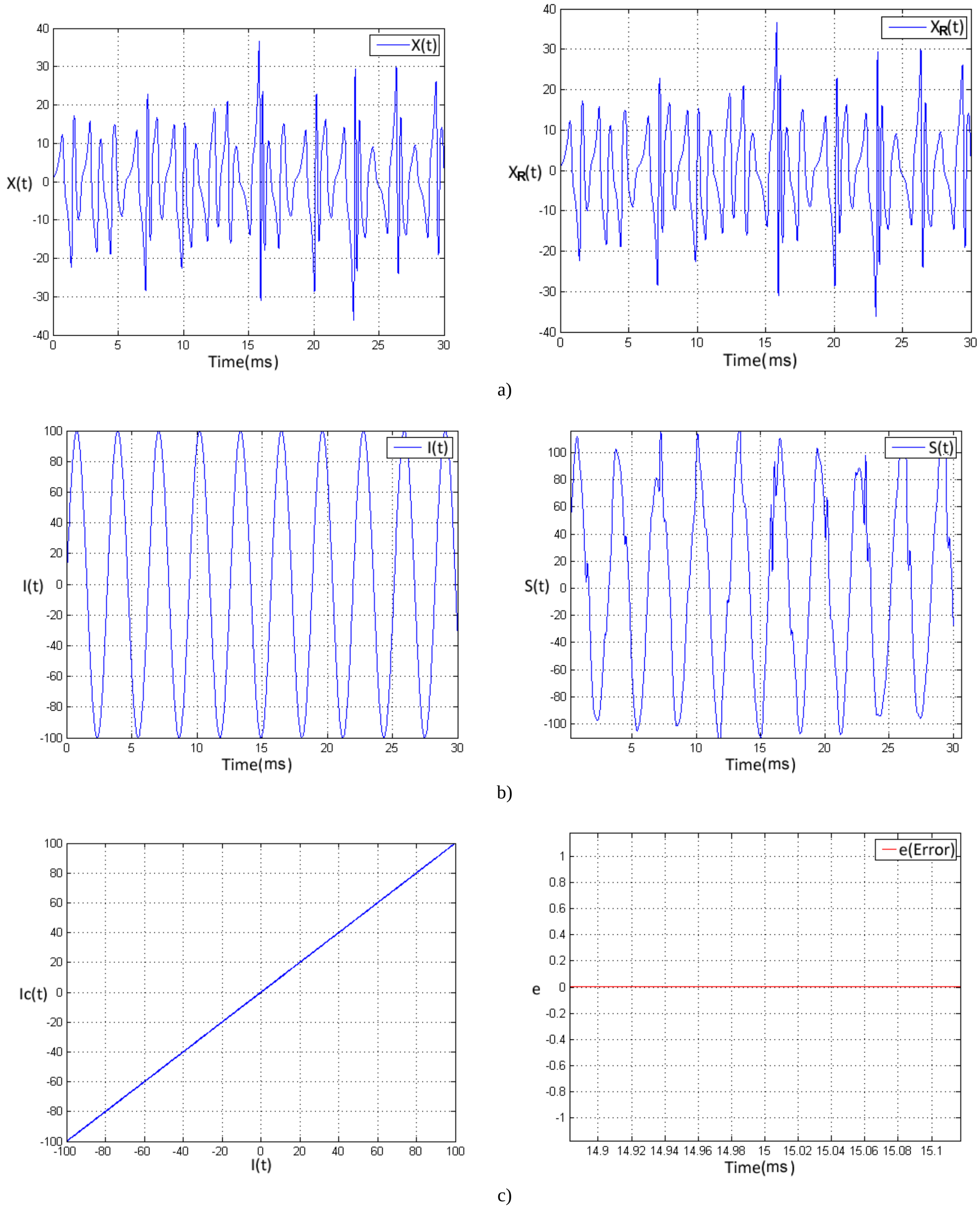


Figure 11. The results of chaotic hiding communication method by using modelling of a new chaotic system simulated under Matlab-Simulink environment (a) $X(t)$ transmitter signal / $X_R(t)$ receiver system signal, (b) $I(t)$ information signal / $S(t)=X(t)+I(t)$ transmitted signal, (c) Difference $I_C(t)$ / $I(t)$ and $e(t)=I(t)-I_C(t)$ communication error signal

5. Conclusion

In this article, the identical synchronization of a novel chaotic attractor has been tested for secure communication applications. The P-C identical cascading synchronization method has been employed for this purpose. According to results obtained from the simulation tool, the chaotic system designed can be used in secure communication applications, as transmitted and received signals are identical and the error rates are almost zero at all times.

References

[1] **L. M. Pecora, T. L. Carroll.** Synchronization in Chaotic Systems. *Physical Review Letters*, 1990, Vol. 64, No. 8, 821-830.

[2] **L. M. Pecora, T. L. Carroll.** Driving Systems with Chaotic Signals. *Physical Review A*, 1991, Vol. 44, No. 4, 2374-2385.

[3] **T. Endo, L. O. Chua.** Synchronization of chaos in phase-locked loops. *In Circuits and Systems, IEEE Transactions on*, 1991, Vol. 38, No. 12, 1580-1588.

[4] **J. M. González-Miranda.** Communications by synchronization of spatially symmetric chaotic systems. *Physics Letters A*, 1999, Vol. 251, No. 2, 115-120.

[5] **T. L. Liao, S. H. Tsai.** Adaptive synchronization of chaotic systems and its application to secure communications. *Chaos, Solitons & Fractals*, 2000, Vol. 11, No. 9, 1387–1396.

[6] **I. Pehlivan, Y. Uyaroğlu.** Simplified chaotic diffusionless Lorentz attractor and its application to secure communication systems. *Communications, IET*, 2007, Vol. 1, No. 5, 1015–1022.

[7] **O. Qingli, Z. Pingrong, Q. Zhaoliang.** Chaotic secure communication system based on PSO-BP network. In: *2nd International Conference on Applied Robotics for the Power Industry (CARPI)*, 2012, pp. 792–795.

[8] **Y. Zhang, Y, H. Zhao, L. Zhang.** Synchronization of chaotic system and its application in secure communication. In: *International Conference on Computer Application and System Modeling (ICCASM)*, 2010, Vol. 14, pp. 94-97.

[9] **C. Cheng, C. Cheng.** Robust Synchronization of Chaotic Systems Subject to Noise and Its Application to Secure Communication. In: *International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN)*, 2012, pp. 206-210.

[10] **L. Zhang, X. An, J. Zhang.** A new chaos synchronization scheme and its application to secure communications. *Nonlinear Dynamics, 2013,* Vol. 73, No. 1-2, 705-722.

[11] **X. Wang, X. Wu, Y. He, G. Aniwar.** Chaos synchronization of Chen system and its application to secure communication. *International Journal of Modern Physics B*, 2008, Vol. 22, No. 21, 3709-3720.

[12] **J. Tang, C. Zou, L. Zhao.** Chaos synchronization of fractional order time-delay Chen system and its application in secure communication. *Journal of Convergence Information Technology,* 2012, Vol. 7, No. 2, pp. 124-131.

[13] **A. A. Zaher.** Secure communication using Duffing oscillators. In: *IEEE International Conference On Signal and Image Processing Applications (ICSIPA),* 2011, pp. 563-568

[14] **M. Zapateiro, Y. Vidal, L. Acho.** A secure communication scheme based on chaotic Duffing oscillators and frequency estimation for the transmission of binary-coded messages. *Communications in Nonlinear Science And Numerical Simulation*, 2014, Vol. 19, No. 4, 991-1003.

[15] **J. Yang, F. Zhu.** Synchronization for chaotic systems and chaos-based secure communications via both reduced-order and step-by-step sliding mode observers. *Communications in Nonlinear Science and Numerical Simulation,* 2013, Vol. 18, No. 4, 926-937.

[16] **A. N. Pisarchik, F. R. Ruiz-Oliveras.** Optical secure communication system based on chaos synchronization. In: *Proceedings of the International Conference on Optical Communication Systems (OPTICS)*, 2010, pp. 149-153.

[17] **W. A. Al-Hussaibi.** Impact of filtering chaotic signals on secure wireless communication systems based Chua's circuit. In: *International Conference on Innovations in Information Technology (IIT),* 2013, pp. 89-94.

[18] **Y. Zhao, G. Xia, J. Wu, Z. Wu.** Investigation of bidirectional dual-channel long-distance chaos secure communication based on 1550nm vertical cavity surface-emitting lasers. *Wuli Xuebao/Acta Physica Sinica*, 2013, Vol. 62, No. 21, 214206-214214.

[19] **I. Pehlivan, Y. Uyaroglu.** Rikitake Attractor and Its Synchronization Application for Secure Communication Systems. *Journal of Applied Sciences,* 2007, Vol. 7, No. 2, 232-236.

[20] **C. Chin Yi, X. Daolin.** Secure digital communication using controlled projective synchronisation of chaos. *Chaos, Solitons and Fractals,* 2005, Vol. 23, No. 3, 1063-1070.

[21] **T. Liangrui, Z. Lin, Y. Xue.** Chaos synchronization based on observer and its application in speech secure communication. In: *IEEE International Conference on Network Infrastructure and Digital Content*, 2010, pp. 773-777.

[22] **A. Zaher, A. Abu-Rezq.** On the design of chaos-based secure communication systems. *Communications in Nonlinear Science and Numerical Simulation*, 2011, Vol. 16 No. 9, 3721-3737.

[23] **A. Ali.** Synchronization and secure communication of uncertain chaotic systems based on full-order and reduced-order output-affine observers. *Applied Mathematics and Computation,* 2013, Vol. 219, No. 19, 10000-10011.

[24] **U. E. Kocamaz, Y. Uyaroglu.** Non-identical synchronization, anti-synchronization and control of single-machine infinite-bus power system via active control. *Information Technology and Control*, 2014, Vol. 43, No. 2, 166-174.

[25] **J. L. Kaplan, J. A. Yorke.** In Functional Differential Equations and Approximations of Fixed Points: *Proceedings, Bonn, July 1978 (Ed. H.-O. Peitgen and H.-O. Walther). Berlin: Springer-Verlag,* 1979, pp. 204-220.

[26] **C. Huang, S. Tsay, Y. Wu.** Implementation of chaotic secure communication systems based on OPA circuits. *Chaos Solitons and Fractals*, 2005, Vol. 23, No. 2, 589-600.

Received August 2014.