16th European Signal Processing Conference (EUSIPCO 2008), Lausanne, Switzerland, August 25-29, 2008, copyright by EURASIP

A NEW SECURE COMMUNICATION TECHNIQUE USING A NOVEL CHAOS-BASED NONLINEAR CRYPTOGRAPHY FUNCTION

Ashraf A. Zaher

Physics Department, Science College, Kuwait University
P. O. Box 5969, Safat 13060, Kuwait
phone: + (965) 498-7241, fax: + (965) 481-9374, email: a.zaher@kuniv.edu
web: physics.kuniv.edu.kw

ABSTRACT

A new secure communication technique is proposed using a novel chaotic encryption method. A chaotic system with a single adjustable parameter, which has a structure that is similar to the Rikitake model, is used to construct the communication link between the receiver and the transmitter. The nonlinear function used for the encryption/decryption of the message utilizes a single time series of the receiver system along with a synchronization-based states observer and an adaptive parameter identifier. A Lyapunov function is used to design the parameter identifier that functions as an embedded secret key. The proposed technique is demonstrated to have improved security as the signal could be efficiently retrieved only if the secret key is known, even when both the receiver and the transmitter are in perfect synchronization. In addition, the proposed technique is shown to be easily implementable using both analog and digital hardware while being capable of transmitting signals with variable bandwidth.

1. INTRODUCTION

In the last two decades, and since the pioneer work of chaos control [1], and chaos synchronization [2], chaos proved to be of effective use for a wide variety of applications. Using chaos for the purpose of secure communication was motivated by the generation of cipher keys for the use of pseudo-chaotic systems in cryptography [3]. For more than a decade, chaos-based secure communication systems have evolved in plenty of forms using different techniques to achieve synchronization between the transmitter and the receiver [4] while encrypting the secret message. The survey of the early work, presented in [5], proved that chaos can indeed be effectively used for secure communication and consequently was an inspiration for developing other methods and techniques in this field. Additive masking, chaos shift keying, chaotic switching, and chaotic modulation are among the most famous techniques in the field of secure communication [6-10].

In the last decade, further research was carried out to improve the security level of chaotic secure communication systems via utilizing chaotic cryptosystems [11]. In these systems nonlinear encryption methods are used to scramble the secure message at the transmitter side, while using an inverse operation at the receiver side that can effectively recover the original message, provided that synchronization is achieved. The degree of complexity of the encryption function and the insertion of ciphers (secret keys) led to having more robust techniques with applications to both analog and digital communication [12]. Recently new techniques, based on impulsive synchronization, are introduced [13]. These systems have the advantage of reducing the information redundancy in the transmitted signal as only synchronization impulses are sent to the driven system. Other methods for enhancing security in chaos-based secure communication system, that are currently reported in the literature, include employing pseudorandom numbers generators for encoding messages [14] and using high-dimension hyperchaotic systems having multiple positive Lyapunov exponents [15]. A recent survey that categories secure communication techniques into subsequent chronological generations is found in [4].

In this paper, it is intended to address the deficiencies in current secure communication systems, reported in [4,16], via proposing an improved security mechanism in which the encryption function, at the transmitter, depends on a novel combination of the chaotic system states and an adjustable secret key that has a random piecewise linear profile. The rest of this paper is organized as follows. In Sec. II, analysis of the proposed technique is introduced, where the design is split into two parts; one for the synchronization mechanism, and the other for implementing the secret key. Simulation results are given in Sec. III, illustrating the effectiveness of the proposed methodology, while highlighting the improvements in the security level when using the secret key. Finally, a discussion is given in Sec. IV to summarize the work done and proposing future extensions to it.

2. THE PROPOSED TECHNIQUE

The basic idea of the proposed improved-security communication system is to rely on a novel nonlinear encryption function that has an additional embedded secret key. This secret key should not be kept constant in order to make it harder for an intruder to break into the communication channel. On the other hand, the receiver should be able to track any changes in the secret key and to use it successfully to decrypt the sent message. To achieve such goal, a chaotic system with a special structure is proposed such that the synchronization process is not affected by changing the secret key. Meanwhile a robust parameter update law is designed to dynamically identify the secret key. A candidate chaotic system that is capable of achieving the required objective is inspired from the famous Rikitake model that is described by:

$$\begin{aligned}\tau\dot{x}_1 &= -x_1 + x_2x_3\\ \tau\dot{x}_2 &= -\alpha x_1 - x_2 + x_1x_3\\ \tau\dot{x}_3 &= 1 - x_1x_2\end{aligned} \tag{1}$$

where α is a constant parameter and τ is a time scaling factor that can be used to adjust the bandwidth of the system. Linear analysis of the chaotic system near equilibrium points reveals that the system has the characteristic equation depicted in Eq. (2)

$$(\lambda+2)\left(\lambda^2+\sqrt{\alpha^2+4}\right)=0 \tag{2}$$

where the equilibrium points are given by

$$X_{eq}=\left[\pm\beta \quad \pm\beta^{-1} \quad \beta^2\right], \beta=\sqrt{\left(\frac{\alpha}{2}\right)+\sqrt{\left(\frac{\alpha}{2}\right)^2+1}} \tag{3}$$

Figure 1 shows the 3D phase plane of the system for $\alpha = 1$.

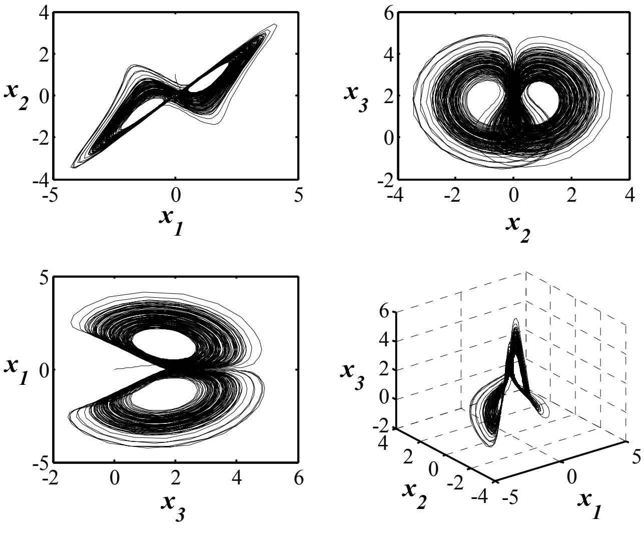

Figure 1 - Chaotic behavior of the system for $\alpha = 1$

Assuming that only the scalar time series for x_2 is accessible, and that the range of α is chosen such that the system is always chaotic, the structure of the dynamic model, described by Eq. (1), allows for decoupling the design of both the synchronization algorithm and the parameter update law for α. This is further explained in the next section.

2.1 Design of the state observer

Synchronization of both the chaotic transmitter and receiver is considered to be a bottleneck in designing chaotic secure communication systems as, by default, chaotic systems defy synchronization [2,17] due to their inherent sensitivity to initial conditions and, as a result, two trajectories emerging from two different closely initial conditions separate exponentially in the course of the time. Never the less, synchronization for two identical, possibly chaotic, dynamical systems can be achieved such that the solution of one always converges to the solution of the other independently of initial conditions using a drive-response mechanism, where there is an interaction between one system and the other, but not vice versa. This drive-response coupling can be used to generate estimates of the states of the drive system when both the systems to be synchronized have a similar structure, i.e. identical synchronization. This kind of synchronization can be achieved provided that all real parts of the Lyapunov exponents of the response system, under the influence of the driver, are negative. In this section, we develop a synchronization-based approach to design a reduced-order state observer. Assuming that only the time series for x_2 is used for the coupling, the dynamics of the reduced order state observer is given by:

$$\begin{aligned}\tau\dot{\hat{x}}_1 &= -\hat{x}_1 + x_2\hat{x}_3\\ \tau\dot{\hat{x}}_3 &= 1 - \hat{x}_1x_2\end{aligned} \tag{4}$$

Introducing the following synchronization errors:

$$e_i = \hat{x}_i - x_i, i = 1,3 \tag{5}$$

and using the following candidate Lyapunov function:

$$L_{13} = 0.5\tau(e_1^2 + e_3^2) \tag{6}$$

the result given in Eq. (7) is obtained, which guarantees that the observed states will asymptotically follow those of the drive system.

$$\dot{L}_{13} = (e_1\dot{e}_1 + e_3\dot{e}_3) = -e_1^2 < 0 \tag{7}$$

The results outlined in Eqs. (4-7) show that the unknown parameter, α, has no effect on the state observer. Thus the two-way coupling between the state observer and the parameter identifier is broken. This result will now be taken an advantage of to design a simple parameter identification algorithm for α.

2.2 Design of the parameter update law

When dealing with chaos, for both control and synchronization applications, it is required to be able to identify unknown/uncertain parameters of the chaotic system [9].This is usually achieved via building parameters update laws for which the degree of complexity depends crucially on many factors; among them the structure and type of nonlinearity of the system at hand, complete or partial availability of the states for direct measurement, and the nature of the application. Different techniques were reported in the literature that rely, some way or another, on the use of local Lyapunov functions to establish the stability and convergence of the parameters identification system [18]. Introducing the following functions:

$$\begin{aligned} \tau\dot{\hat{x}}_2 &= -\hat{\alpha}\hat{x}_1 - \hat{x}_2 + \hat{x}_1\hat{x}_3 \\ e_2 &= \hat{x}_2 - x_2 \\ e_\alpha &= \hat{\alpha} - \alpha \end{aligned} \tag{8}$$

where $\hat{\alpha}$ is the estimate for the unknown parameter α and e_α is its corresponding estimation error, the following augmented Lyapunov function is introduced to test for the stability of the overall system comprising the original chaotic system, the synchronization-based state observer, and the parameter identifier:

$$L = L_{13} + 0.5\tau(e_2^2 + ke_\alpha^2) \tag{9}$$

where k is a constant used to adjust the convergence rate of the parameter identifier. Differentiating Eq. (9) along the solution of Eqs. (4,8) yields:

$$\dot{L} = -e_1^2 - e_2^2 + e_\alpha(k\tau\dot{e}_\alpha - \hat{x}_1 e_2) + e_2[(\hat{x}_3 - \alpha)e_1 + x_1 e_3] \tag{10}$$

Although it is analytically difficult to prove negative definiteness of Eq. (10), incorporating the result of Eq. (7) for which e_1 → 0 and e_3 → 0 as $t \to \infty$, clearly shows that near synchronization the last bracket of Eq. (10) vanishes. Thus the choice of the parameter update law, given in Eq. (11), completes the proof for asymptotic stability.

$$\dot{e}_\alpha = \hat{x}_1 e_2 / k\tau \Rightarrow \dot{\hat{\alpha}} = \hat{x}_1(\hat{x}_2 - x_2)/k\tau \tag{11}$$

The speed of convergence for $\hat{\alpha}$ can be adjusted via decreasing k such that fast convergence of the parameter identifier is obtained once the synchronization errors diminish.

3. SIMULATION RESULTS

Using two communication channels, one for the encrypted message and the other for the synchronizing signal, and following the methodology outlined in [19], the following nonlinear encryption function is proposed:

$$E(X, \alpha, s, t) = x_1^2 + (\alpha^2 + x_1^2)s(t) \tag{12}$$

for which its counterpart decryption function is given by:

$$\hat{s}(t) = D(\hat{X}, \hat{\alpha}, s, t) = (E(X, \alpha, s, t) - \hat{x}_1^2)/(\hat{\alpha}^2 + \hat{x}_1^2) \tag{13}$$

The strategy behind using the special structure of the secure transmission system in Eqs. (12,13) is to make it harder for the intruder to decrypt the transmitted message via using a nonlinear function of both the states and the parameters of the chaotic system. By slowly modifying α at the transmitter, an intruder that manages to synchronize its response system with the transmitter will still be not able to extract the message because of not knowing the exact value of α. This is illustrated by the following example. Using τ = 1 µs in Eq. (1) and assuming that the message to be transmitted is of the form:

$$s(t) = A_s \sin(2\pi f_s t), f_s << f_d \tag{14}$$

where A_s is the amplitude of the message to be securely transmitted, f_s is its frequency, and f_d is the dominant frequency component of the chaotic signal used for the encryption process. Using simulations, it was found that the range $0.5 < \alpha < 1.5$ resulted in an average of f_d = 0.35 MHz with negligible fluctuations and consequently this range was used for performing the encryption. Figure 2 illustrates the contrast between the message and its encryption using A_s = 0.01 and f_s = 50 KHz where it is obvious that the message is effectively scrambled.

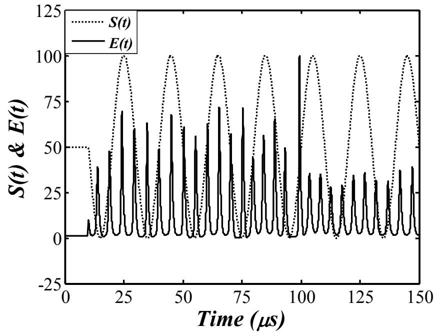

Figure 2 - The normalized-amplitudes of the message before and after encryption

In addition, Fig. (3) shows the effectiveness in recovering the transmitted message illustrating the correlation between the identification error and the mismatch error between both the transmitted and received messages.

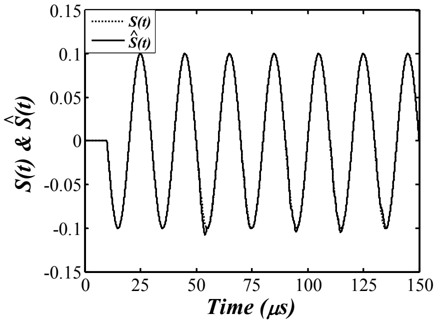

Figure 3 - The recovered signal vs. the original signal

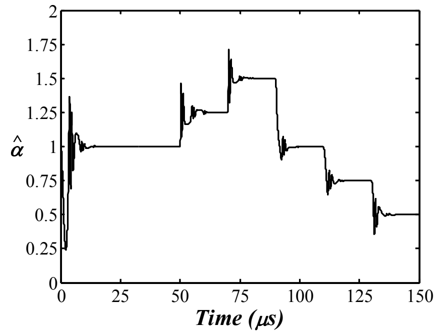

Figure 4 - Tracking of α (the cipher key)

As the synchronization-based state observer is not affected by the mismatch between α and $\hat{\alpha}$ at the transmitter and the receiver respectively, the receiver will lock on the correct estimates of the states x_1 and x_3 regardless of the deliberate frequent changes in α. This has the effect of simplifying the design process as the there is only coupling between the state observer and the parameter identifier, but not vice versa. This result is illustrated in Fig. (5). In addition, the communication error with and without using the parameter update law is illustrated in Figs. (6,7) respectively, where Fig. (6) reflects the negligible error in contrast to the result, shown in Fig. (7), when assuming a nominal value of $\alpha = 1$.

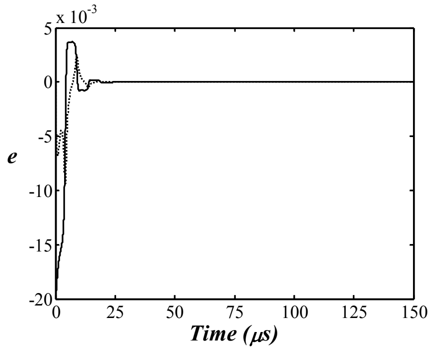

Figure 5 – Synchronization errors of the observed signals

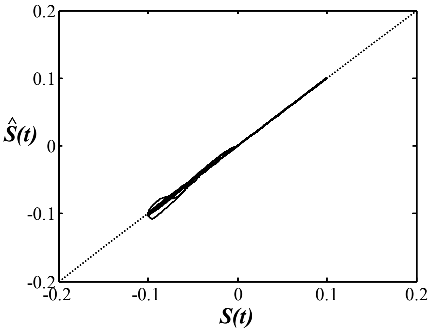

Figure 6 - Communication error using the parameter update law

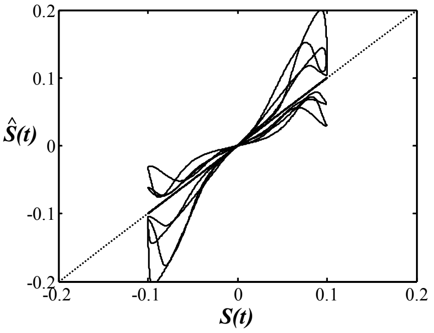

Figure 7 - Communication error without the parameter update law

4. IMPLEMENTATION

The design of the transmitter, the receiver, and the parameter update law can be implemented using both analog and digital hardware. Figure 8 demonstrate one possible implementation where the indicated switch is used to distinguish between the receiver (default position) where x_2 is used as the drive signal, and the transmitter. The time scaling factor of the circuit can be adjusted via adjusting the capacitors values, while manipulating the cipher key can be done via adjusting R_8. The AD633AD was used to implement the analog multipliers while using R_1, R_5, and R_{10} to adjust their gains. As indicated in Fig. (9), other circuit elements could be used as a cipher, e.g. keeping α constant and changing the voltage source connected to R_{11} could be considered as an alternative to the proposed design which verifies its flexibility and versatility. In addition, the complete system can be implemented using SIMULINK, and then the real-time-workshop toolbox is used to generate the corresponding digital signals in MATLAB environment, which can be converted later to their analog counterparts using a proper D/A converter.

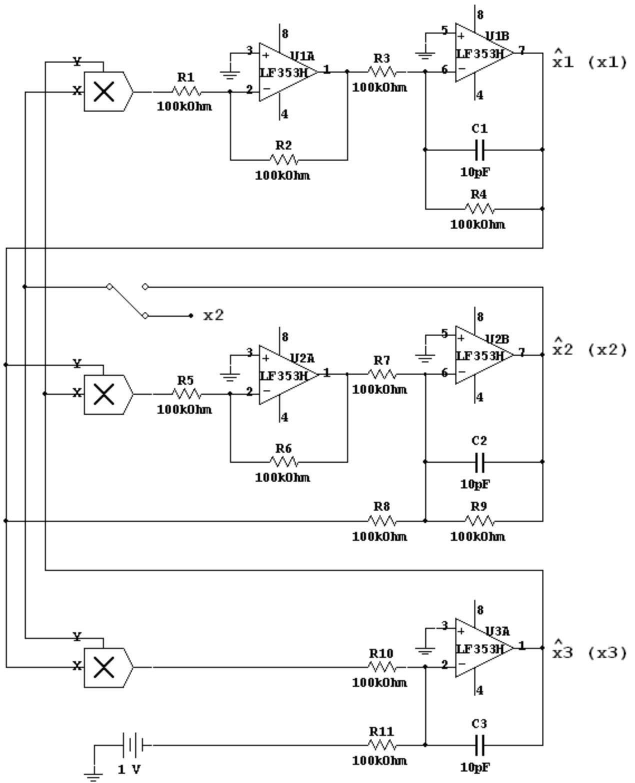

Figure 8 - Analog implementation of the transmitter/Receiver

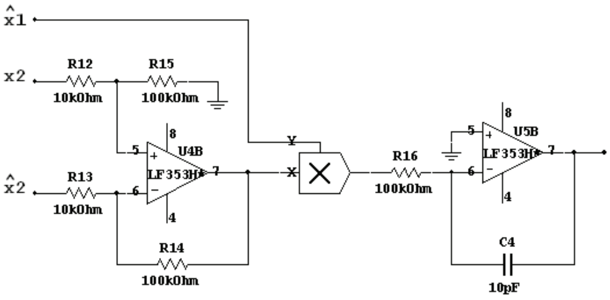

Figure 9 - Analog implementation of the parameter update law

5. DISCUSSION AND CONCLUSION

A chaos-based secure communication system was introduced. This system is designed to have an improved security over those reported in the literature via the use of a novel encryption function at the transmitter side. This function has a special nonlinear form that depends on both the chaotic transmitter states and a single parameter that serves as a secret key (cipher). This secret key is allowed to changed in a random piecewise linear fashion in order to accomplish two tasks; first, to act as a cipher key that makes the scrambling process of the transmitted message more robust, and second, to continuously change the chaotic attractor of the transmitter; thus making it harder for an intruder to break into the communication channel.

The corner stone of the design was the use of a chaotic system with a special structure that allows decoupling the synchronization process from that of identifying the secret key. A Rikitake-like model was chosen to exemplify the design process; however other models satisfying the same characteristics could have been used as well. The models reported in [20] have rich varieties of structures and as a consequence can serve as promising candidates for using some of their parameters as cipher keys while performing the encryption process. Another possible extension to the work done in this paper is to try other parameter identification techniques while performing the synchronization [21] to simplify the design process while maintaining robustness. Another added advantage of the proposed technique was its ability to cope with transmitting different messages having different bandwidths via adjusting a simple parameter that has the effect of controlling the dominant frequency of the chosen chaotic attractor. Finally it should be emphasized that, like many other chaotic oscillators, implementation using both analog and digital hardware is feasible as demonstrated in this paper and similar work, e.g. [22].

REFERENCES

[1] E. Ott, C. Grebogi, and J. Yorke, "Controlling Chaos," *Physical Review Letters*, vol. 64, pp. 1196–1199, 1990.

[2] L. M. Pecora and T. L. Carroll, "Synchronization in Chaotic Systems," *Physical Review Letters*, vol. 64, pp. 821–825, 1990.

[3] D. Stinson, *Cryptography: Theory and Practice, 3rd Ed.* CRC Press, 2005.

[4] T. Yang, "A Survey of Chaotic Secure Communication Systems," *International Journal of Computational Cognition*, vol. 2, pp. 81–130, 2004.

[5] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, "Synchronization of Lorenz-Based Chaotic Circuits with Applications to Communications," *IEEE Transactions on Circuits and Systems II*, vol. 40, pp. 626–633, 1993.

[6] H. Dedieu, M. P. Kennedy, and M. Hasler, "Chaos shift keying - modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits," *IEEE Transactions on Circuits and Systems II*, vol. 40, pp. 634–642, 1993.

[7] T. Yang and L. O. Chua, "Secure Communication via Chaotic Parameter Modulation," *IEEE Transactions on Circuits and Systems I*, vol. 43, pp. 817–819, 1996.

[8] C. Zhou and C. H. Lai, "Decoding information by following parameter modulation with parameter adaptive control," *Physical Review E*, vol. 59, pp. 6629–6636, 1999.

[9] A. d'Anjou, C. Sarasola, F. J. Torrealdea, R. Orduna, and M. Graña, "Parameter-adaptive identical synchronization disclosing Lorenz chaotic masking," *Physical Review E*, vol. 63, pp. 046213:1–5, 2001.

[10] C. W. Wu and L. O. Chua, "A simple way to synchronize chaotic systems with applications to secure communication systems," *International Journal of Bifurcation and Chaos*, vol. 3, pp. 1619–1627, 1994.

[11] T. Yang, C. W. Wu, and L. O. Chua, "Cryptography Based on Chaotic Systems," *IEEE Transactions on Circuits and Systems I*, vol. 44, pp 469–472, 1997.

[12] S. Sundar and A. A. Minai, "Synchronization of Randomly Multiplexed Chaotic Systems with Application to Communication," *Physical Review Letters*, vol. 85, pp. 5456–5459, 2000.

[13] T. Yang and L. O. Chua, "Impulsive stabilization for control and synchronization of chaotic systems - theory and application to secure communication," *IEEE Transactions on Circuits and Systems I*, vol. 44, pp. 976–988, 1997.

[14] Y. Zhang, C. Tao, G. Du, and J. J. Jiang, "Synchronized pseudorandom systems and their application to speech communication," *Physical Review E*, vol. 71, pp. 016217:1–5, 2005.

[15] L. Yaowen, G. Guangming, Z. Hong, and W. Yinghai, "Synchronization of hyperchaotic harmonics in time-delay systems and its application to secure communication," *Physical Review E*, vol. 62, pp. 7898–7904, 2000.

[16] G. Alvarez, L. Hernández, J. Muñóz, F. Montoya, and S. Li, "Security analysis of communication system based on the synchronization of different order chaotic systems," *Physical Letters A*, vol. 345, pp. 245–250, 2005.

[17] S. Boccaletti, J. Kurths, G. Osipov, D. L. Valladares, and C. S. Zhou, "The synchronization of chaotic systems," *Physics Reports*, vol. 366, pp. 1–101, 2002.

[18] U. Parlitz, "Estimating Model Parameters from Time Series by Autosynchronization," *Physical Review Letters*, vol. 76, pp. 1232–1235, 1996.

[19] Z. P. Jiang, "A Note on Chaotic Secure Communication Systems," *IEEE Transactions on Circuits and Systems I*, vol. 49, pp. 92–96, 2002.

[20] J. C. Sprott, "A new class of chaotic circuit," *Physical Letters A*, vol. 266, pp. 19–23, 2000.

[21] Ashraf A. Zaher, "Design of model-based controllers for a class of nonlinear chaotic systems using a single output feedback and state observers," *Physical Review E*, vol. 75, pp 056203:1–9, 2007.

[22] I. Pehlivan and Y. Uyaroğlu, "Rikitake Attractor and It's Synchronization Application for secure Communication Systems," *Journal of Applied Sciences*, vol. 7, pp. 232–236, 2007.