A Secure Communication System Based on a Modified Chaotic Chua Oscillator

Mauricio Zapateiro De la Hoz[1], Leonardo Acho[2], and Yolanda Vidal[2]

[1] Universidade Tecnológica Federal do Paraná, Av. Alberto Carazzai 1640, 86300-000 Cornélio Procópio, Paraná, Brazil
(E-mail: hoz@utfpr.edu.br)

[2] Control, Dynamics and Applications Group - CoDAlab. Departament de Matemàtica Aplicada III. Universitat Politècnica de Catalunya, Comte d'Urgell 187, 08036, Barcelona, Spain
(E-mail: leonardo.acho@upc.edu, yolanda.vidal@upc.edu)

Abstract. In this paper we propose a new scheme for secure communications using a modified Chua oscillator. A modification of the oscillator is proposed in order to facilitate the decryption. The communication system requires two channels for transmitting the message. One of the channels transmits a chaotic signal generated by the oscillator and is used for synchronization. The second channel transmits the message encrypted by a nonlinear function. This function is built in terms of one of the chaotic signals, different from that sent on the first channel. In the receiver side, a synchronizer reconstructs the chaotic oscillator signals, one of which is used for the decryption of the message. The synchronization system is designed via Lyapunov theory and chaoticity proves via Poincaré maps and Lyapunov exponents will be provided in order to demonstrate the feasibility of our system. Numerical simulations will be used to evaluate the performance of the system.

Keywords: Chaos, Secure communication, Chua oscillator.

1 Introduction

The possibility to synchronize two coupled chaotic systems has allowed the development of a variety of communication schemes based on chaotic systems. A wide variety of synchronization schemes have been developed since Pecora and Carroll [5], among others, showed it was possible to do so. In this way the use of signals generated by chaotic systems as carriers for analog and digital communications aroused great interest as a potential means for secure communications [1], [4], [9].

There are several works in the literature about chaotic secure communications. For instance, [8] addressed the problems of the chaos synchronization in a secure communication system when the observer matching condition is not satisfied. Zapateiro, Vidal and Acho [11] designed a chaotic communication system in which a binary signal is encrypted in the frequency of the sinusoidal term of a chaotic Duffing oscillator. Fallahi and Leung [2] developed a chaotic communication system based on multiplication modulation. Further examples can be found in [3], [10] and [12], to name a few.

In this paper, we present a new scheme to securely transmit a message using chaotic oscillators. It is based on a modification of the Chua oscillator

7th CHAOS Conference Proceedings, 7-10 June 2014, Lisbon Portugal
C. H. Skiadas (Ed)

that allows for a simpler synchronization design and stability demonstration. A Poincaré map and the maximum Lyapunov exponent are presented as proofs of chaoticity of the modified oscillator. This scheme requires two channels for transmission. The encryption/decryption process is based on a modification of the scheme proposed by [13] in which a highly nonlinear function is used along with one of the chaotic signals. The advantage of the scheme is that neither the key signals nor the encrypted signals are transmitted over the channels.

The structure of this chapter is as follows. The problem statement is presented in Section 2. The details of the transmitter and receiver as well as the encryption/decryption blocks are given in Sections 3 - 6. Finally, conclusions are outlined in Section 7

2 Communication system scheme

The diagram of the proposed communication scheme is shown in Figure 1. It consists of the following elements:

1) *Chaotic oscillator*: It is a modified Chua oscillator that generates three signals (x_1, x_2, x_3), two of which are used for synchronization and encryption/decryption purposes.
2) *Encryption block*: It encrypts the message $m(t)$ using a nonlinear function $m_e(t) = \phi(x_2(t), m(t))$.
3) *Channels*: Two channels transmit the chaotic signal and the encrypted message. Channel noise $n_d(t)$ is added. In the receiver side, the signals are filtered with a bank of filters, producing signals $x_{1f}(t)$ and $m_{ef}(t)$.
4) *Synchronization block*: It retrieves the chaotic signals using only one signal from the chaotic oscillator ($x_{1f}(t)$).
5) *Decryption block*: It decrypts the message by using a nonlinear function $m_d(t) = \psi(y_2(t), m_{ef}(t))$. In this case, y_2 is the estimation of the chaotic signal x_2 generated by the synchronization block.
6) *Retrieving block*: In this stage, an algorithm is executed for deciding which message value was sent at an instant $t = t_k$, $k = 1, 2, 3, ...$

The details of the main blocks of the communication system are given in Sections 3 - 5

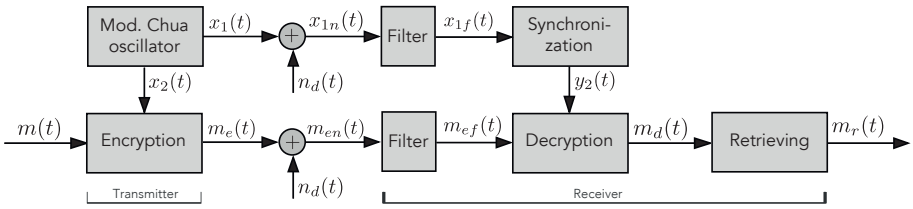


Fig. 1. Block diagram of the proposed communication system.

3 Modified Chua chaotic oscillator

The original Chua oscillator is given by the following set of equations:

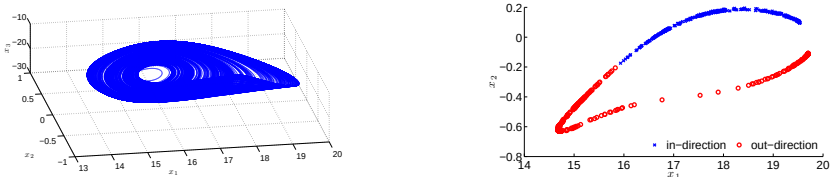
$$\dot{x}_1 = \alpha\,(x_2 - f(x_1))\,, \tag{1}$$
$$\dot{x}_2 = x_1 - x_2 + x_3, \tag{2}$$
$$\dot{x}_3 = -\beta x_2, \tag{3}$$
$$f(x_1) = m_1 x_1 + \frac{1}{2}(m_0 - m_1)(|x_1 + 1| - |x_1 - 1|). \tag{4}$$

where the overdot denotes differentiation with respect to time t; $\alpha > 0$, $\beta > 0$, m_0 and m_1 are parameters that must be chosen appropriately for obtaining chaotic behavior. In this work, we modified the original system by choosing the following characteristic function $f(x_1)$:

$$f(x_1) = -\sin x_1 \cdot e^{-0.1|x_1|}. \tag{5}$$

Note that 5 is a bounded smooth function. The system of Equations 1-3 and 5 is chaotic if $\alpha = 9.35$ and $\beta = 14.35$, as can be seen in Figure 2(a).

Figure 2(b) is the Poincaré map of the modified Chua oscillator generated when the trajectories intersect the plane $x + y + z + 1 = 0$. The map of Figure 2(b) shows the points where the trajectories intersect the plane. The two different markers show if the trajectory goes in one direction or another as it intersects the plane. The map is seen in the XY plane perspective.



(a) (b)

Fig. 2. (a) Dynamics of the modified Chua oscillator. (b) Poincaré map of the oscillator as seen in the XY plane perspective. Trajectories intersecting the plane $x + y + z + 1 = 0$.

Finally, the maximum Lyapunov exponent is calculated as another proof of chaoticity. A positive Lyapunov exponent is a strong indicator of chaos. If a system has at least one positive Lyapunov exponent, then the system is chaotic [7]. In order to determine the maximum Lyapunov exponent λ of the modified Chua oscillator, the algorithm presented in [6] was implemented in Matlab/Simulink. Figure 3 shows how λ evolves until it reaches stability. From these data, it could be found that $\lambda \approx 0.0025$ which confirms the chaoticity of the system.

4 Encryption and decryption

The encryption/decryption scheme proposed by [13] is implemented in our communication system with modified encryption/decryption functions and chaotic oscillator. In this scheme, there are two channels in order to make the synchronization process faster. The encryption/decryption process is as follows [13]:

- *Encryption*: The message $m(t)$ to be sent is encrypted by means of a nonlinear function $\phi : \mathbb{R}^3 \times \mathbb{R} \to \mathbb{R}$ that is continuous in its first argument $x \in \mathbb{R}^3$ and satisfies the following property: for every fixed pair of $(x, m) \in \mathbb{R}^3 \times \mathbb{R}$, theres exists a unique function $\psi : \mathbb{R}^3 \to \mathbb{R}$ that is continuous in its first argument $x \in \mathbb{R}^3$ and is such that $\psi(x, \phi(x, m)) = m$. The encryption function ϕ is built in terms of the chaotic signals. The result is a signal $m_e(t)$ containing the message that is sent through one of the channels.
- *Synchronization*: A synchronization block retrieves the chaotic oscillator signals. It uses only the oscillator signal x_1 from the transmitter oscillator. This signal is sufficient to generate the signals y_1, y_2 and y_3 that are estimations of the oscillator signals x_1, x_2 and x_3, respectively. Retrieving x_2 is necessary for decrypting the message received on the second channel.
- *Decryption*: Once the oscillator signals are retrieved, the decryption function ψ can be used along with the signal $m_{ef}(t)$ in order to get the message $m(t)$.

The functions that we chose in this work to encrypt and decrypt the message are:

$$\phi : \frac{|x_2|}{x_2 + \delta} \cdot m(t) = m_e(t) \tag{6}$$

$$\psi : \frac{y_2 + \delta}{|y_2|} \cdot m_{ef}(t) = m_d(t) \tag{7}$$

where $m_d(t)$ is the decrypted message, as shown in Figure 1 and $\delta > 0$ and small compared to $|x_2|$.

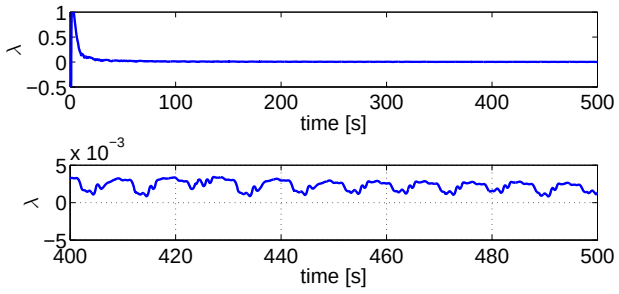


Fig. 3. Top: evolution of the maximum Lyapunov exponent. Bottom: zoom of the upper figure.

5 Synchronization

The synchronization block consists of a dynamic system that takes the signal x_1 and generates the signals y_1, y_2 and y_3 that are estimations of the oscillator signals x_1, x_2 and x_3, respectively.

Theorem 1. *Consider the modified Chua oscillator given by Equations 1 - 3 and 5 with α and β having appropriate positive values that guarantee the chaoticity of the system. Consider also a constant $\rho > 0$ such that $|x_2(t)| < \rho$. Then the system given by:*

$$\dot{y}_1 = k \cdot \mathtt{sgn}(x_1 - y_1), \tag{8}$$
$$\dot{y}_2 = y_1 - y_2 + y_3, \tag{9}$$
$$\dot{y}_3 = -\beta y_2, \tag{10}$$

where k is a design parameter such that $k > \alpha(\rho + 1)$ synchronizes with the modified Chua oscillator and thus:

i) $\lim_{t \to T_s} y_1(t) = x_1(t)$, *for a given* $T_s \in \mathbb{R}^+$.
ii) $\lim_{t \to \infty} y_2(t) = x_2(t)$.
iii) $\lim_{t \to \infty} y_3(t) = x_3(t)$.

Proof. Let the system of Equations 1 - 3 be the master and the system of Equations 8 - 10 be the slave. The function $f(x_1)$ in 5 is such that $|f(x_1)| \leq 1$, $\forall t \geq 0$. Since the system 1 - 3 is chaotic, the signal $x_2(t)$ is bounded and thus, there exists a constant $\rho > 0$ such that $|x_2(t)| \leq \rho \, \forall t \geq 0$. In fact, ρ depends on the initial conditions. However, assuming that $x_2(0)$ lays inside the attractor then ρ can be obtained independently of the initial conditions. The proof begins by defining the following error variable and its derivative:

$$e_1 = x_1 - y_1, \;\; \dot{e}_1 = \dot{x}_1 - \dot{y}_1. \tag{11}$$

Consider the terms $\dot{x}_1$ and $\dot{y}_1$ from Equations 1 and 8, respectively. Substitution of these terms into Equation 11 yields:

$$\dot{e}_1 = \alpha(x_2 - f(x_1))k - \mathtt{sgn}(x_1 - y_1). \tag{12}$$

Let $V_1 = \frac{1}{2}e_1^2$ be a Lyapunov function candidate. Then:

$$\begin{aligned} \dot{V}_1 = e_1\dot{e}_1 &= e_1\alpha x_2 - e_1\alpha f(x_1) - ke_1\mathtt{sgn}(e_1) = -k|e_1| + \alpha x_2 e_1 - \alpha f(x_1)e_1 \\ &\leq -k|e_1| + \alpha x_2 e_1 + \alpha|e_1| \leq -k|e_1| + \alpha\rho|e_1| + \alpha|e_1| \\ &= -|e_1|\left(k - \alpha(\rho + 1)\right). \end{aligned}$$

$\dot{V}_1$ will decrease and converge in finite time if and only if $k > \alpha(\rho + 1)$. Under this condition, there exists a settling time $t = T_s$ such that

$$\lim_{t \to T_s} x_1(t) = y_1(t),$$

and thus $x_1(t) = y_1(t)$, $\forall t \geq T_s$. After $t = T_s$, the synchronization system is completed with the subsystem of Equations 9 and 10. Define two new error variables e_2 and e_3 and their derivatives, as follows:

$$e_2 = x_2 - y_2, \ \dot{e}_2 = \dot{x}_2 - \dot{y}_2,$$

$$e_3 = x_3 - y_3, \ \dot{e}_3 = \dot{x}_3 - \dot{y}_3.$$

From Equations 2 and 9 we have that

$$\dot{e}_2 = x_1 - x_2 + x_3 - x_1 + y_2 - y_3 = -e_2 + e_3.$$

From Equations 3 and 10 we have that

$$\dot{e}_3 = -\beta x_2 + \beta y_2 = -\beta(x_2 - y_2) = -\beta e_2.$$

Rearrange the error variables e_2 and e_3 as a matrix system $\dot{\mathbf{e}} = \mathbf{A}\mathbf{e}$:

$$\begin{bmatrix} \dot{e}_2 \\ \dot{e}_3 \end{bmatrix} = \underbrace{\begin{bmatrix} -1 & 1 \\ -\beta & 0 \end{bmatrix}}_{A} \begin{bmatrix} e_2 \\ e_3 \end{bmatrix}.$$

It is straightforward to show that for all $\beta > 0$, the eigenvalues of matrix $\mathbf{A}$ have negative real parts and thus:

$$\lim_{t\to\infty} y_2(t) = x_2(t), \text{ and } \lim_{t\to\infty} y_3(t) = x_3(t).$$

6 Numerical results

The communication system was implemented in Matlab/Simulink. The transmitter is the implementation of Equations 1 - 3 and 5 with $\alpha = 9.35$ and $\beta = 14.35$. The receiver is the implementation of Equations 8 - 9 with $k = 1000$. The encryption and decryption functions are those of Equations 6 and 7 with $\delta = 0.01$. Noise was added to each signal and thus, a bank of filters was implemented at the input of the receiver so as to clean the signals before their processing. The message signal is assumed to be a two-valued signal that takes the values $m(t) = \{-1, +1\}$. The results to be discussed in what follows were obtained by setting the following initial conditions in the oscillator: $x_1(0) = 15$, $x_2(0) = 0$ and $x_3(0) = -15$. The initial conditions of the synchronizer were: $y_1(0) = 1$, $y_2(0) = 10$ and $y_3(0) = -1$.

Figure 4 compares the signals x_1, x_2 and x_3 of the oscillator in the transmitter side with their estimations y_1, y_2 and y_3 generated by the synchronizer. Figure 4 shows that signals x_1 and y_1 synchronize in a finite time (approximately 0.2 seconds). On the other hand, from Figure 4 we can see that the synchronization of the remaining signals takes around 5 seconds. Given that the signals $y_2(t)$ and $y_3(t)$ have an asymptotic convergence to x_2 and x_3, respectively, it could be expected that some errors might occur when retrieving the message. In order to avoid this problem, we propose sending dummy information in the beginning of the communication so as to avoid losing information.

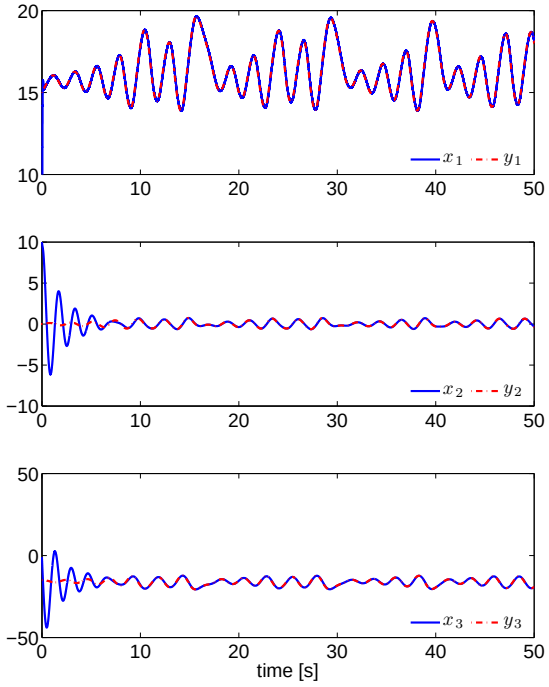


Fig. 4. Comparison of the oscillator signals and their estimations.

Figure 5 is the message that we used for the simulations. For the sake of simplicity, let us call "bit" each possible message value (+1 and −1). Thus, in this test the message $m(t)$ is sent at a rate of $T_b = 1$ bit/second. As can be seen in Figure 5, the dummy information is sent at the beginning of the transmission and afterwards, the true message is sent. Also, the message is passed through a lowpass filter in order to improve the encryption. The filter has the following transfer function:

$$H_e(s) = \frac{1}{s + 100}.$$

In this way we obtain a modified signal $M^*(s) = H_e(s)M(s)$, where $M(s) = \mathscr{L}\{m(t)\}$ and $M^*(s) = \mathscr{L}\{m^*(t)\}$. Figure 6 (top) shows the encrypted message $m_e(t)$, the signal corrupted by channel noise $m_{en}(t)$ and the filtered signal $m_{ef}(t)$. Figure 6 (bottom) shows the message sent in order to observe the differences between the original message and its encryption.

Figure 7 shows the message after the lowpass filter compared to what is obtained after the decryption, i.e. $m_d(t)$. In order to finally retrieve the message, we must determine if the bit corresponds to +1 or −1. This is done at the end of the transmission of every bit, i.e. every T_b^{-1} seconds. In this simulation, we sampled the signal $m_d(t)$ at a rate of $T_r = 0.01$ seconds. So in order to

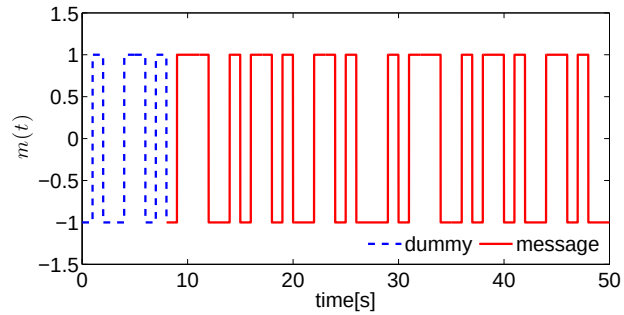


Fig. 5. Message transmitted during the test.

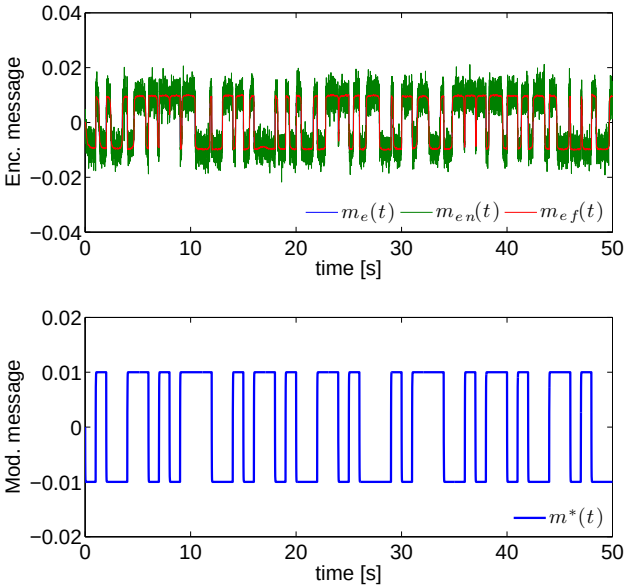


Fig. 6. Top: Encrypted message sent through the channel. Bottom: Original message (filtered).

determine the corresponding bit, we compute the sign of the sample at every instant $t = kT_b^{-1}$, $k = 1, 2, 3, ...$

Figure 8 (top) shows the result of the transmission of the message $m(t)$ which starts at $t = 8$ seconds, after a dummy message, and the retrieved message $m_r(t)$. The blue message is some dummy information sent at the beginning of the transmission in order to avoid incorrect retrieval. The true message is sent from $t = 8$ seconds. The stars in the graphic indicate the retrieved message. Figure 8 (bottom) shows the error between the original message and the retrieved message. Note that all the errors occur in the first 8 seconds of transmission of dummy information.

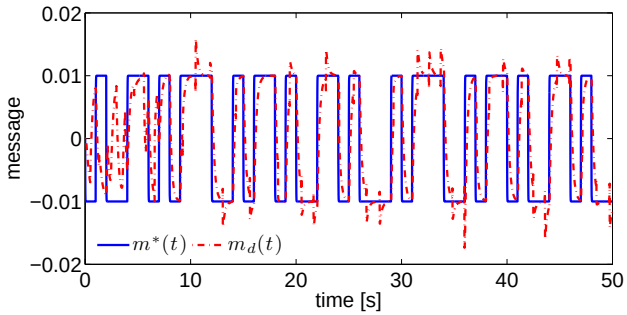


Fig. 7. Comparison between the message sent $m^*(t)$, and the decrypted message $m_d(t)$.

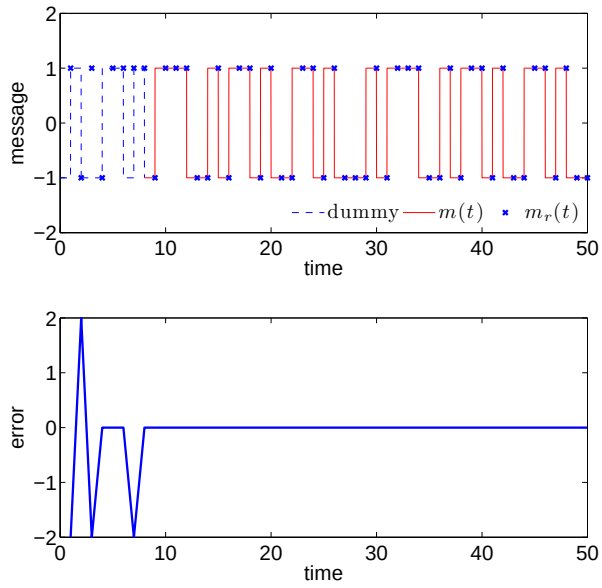


Fig. 8. Top: original and retrieved messages. Bottom: error in retrieved message.

7 Conclusion

In this paper we explored a new secure communication scheme composed of a modified Chua oscillator and an encryption/decryption scheme that makes use of nonlinear functions to encrypt the message. The oscillator characteristic function $f(x)$ was modified to make it bounded. This facilitates the synchronization because only one channel is needed and furthermore, it facilitates the demonstration of the theorem that makes possible the synchronization between the master and the slave. The encryption/decryption scheme used in this work has the advantage that the key signals and encrypted signals do not have to be transmitted over the channel and thus an increase in security is achieved.

Chaoticity proofs of the modified Chua oscillator were provided by means of a Poincaré Map and the maximum Lyapunov Exponent. The feasibility of the system was tested by numerical simulations performed in Matlab/Simulink.

Acknowledgments

Mauricio Zapateiro is supported by the fellowship from CAPES/Programa Nacional de Pos-Doutorado from Brazil. This work has been partially funded by the European Union (European Regional Development Fund) and the Spanish Ministry of Economy and Competitiveness through the research projects DPI2012-32375/FEDER and DPI2011-28033-C03-01 and by the Government of Catalonia (Spain) through 2009SGR1228.

References

1.B. Andrievsky. Adaptive synchronization methods for signal transmission on chaotic carriers, *Mathematics and Computers in Simulation* 58 (46), 285 –293 (2002).
2.K. Fallalih, H. Leung. A chaos secure communication scheme based on multiplication modulation. *Commun. Nonlinear Sci. Numer. Simulat.* 15, pp. 368–383 (2010).
3.C. Hua, B. Yang, G.Ouyang, X. Guan. A new chaotic secure communication scheme *Physics Letters A* 342, pp. 305–308 (2005).
4.O. Morgul, M. Feki. A chaotic masking scheme by using synchronized chaotic systems, *Physics Letters A* 251 (3), 169 – 176 (1999).
5.L. M. Pecora, T. L. Carroll. Synchronization in chaotic systems, *Phys. Rev. Lett.* 64, 821–824 (1990).
6.J. J.Thomsen. Vibrations and Stability : Advanced Theory, Analysis, and Tools, Springer (2003).
7.A. Wolf, J. B. Swift, H. L. Swinney, J. A. Vastano. Determining Lyapunov exponents from a time series, *Physica D* 16, pp. 285–317 (1985).
8.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* 18, pp. 926–937 (2013).
9.T. Yang. A survey of chaotic secure communication systems, *Int. J. Comp. Cognition* 2, pp. 81–130 (2004).
10.T. Yang, L. O. Chua. Impulsive stabilization for control and synchronization of chaotic systems: Theory and application to secure communication, *IEEE Transaction on Circuits and Systems-I: Fundamental Theory and Applications* 44(10), pp. 976–988 (1997).
11.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* 19(4), pp.991-1003 (2014).
12.X. Wang, J. Zhang. Chaotic secure communication based on nonlinear autoregressive filter with changeable parameters, *Physics Letters A* 357, pp. 323–329 (2006).
13.J. Zhon-Ping. A note on Chaotic Secure Communication Systems, *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* 49, pp. 92–96 (2002).