A modified Chua chaotic oscillator and its application to secure communications

Mauricio Zapateiro De la Hoz[a], Leonardo Acho[b], Yolanda Vidal[b]

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

[b] *Control, Dynamics and Applications Group - CoDAlab, Departament de Matemàtica Aplicada III, Universitat Politècnica de Catalunya-BarcelonaTECH, Comte d'Urgell 187, E08036 Barcelona, Spain. E-mails: leonardo.acho@upc.edu, yolanda.vidal@upc.edu*

Abstract

In this paper, a new modified Chua oscillator is introduced. The original Chua oscillator is well known for its simple implementation and mathematical modeling. A modification of the oscillator is proposed in order to facilitate the synchronization and the encryption and decryption scheme. The modification consists in changing the nonlinear term of the original oscillator to a smooth and bounded nonlinear function. A bifurcation diagram, a Poincaré map and the Lyapunov exponents are presented as proofs of chaoticity of the newly modified oscillator. An application to secure communications is proposed in which two channels are used. Numerical simulations are performed in order to analyze the communication system.

Keywords: Chua oscillator, chaos, secure communication, synchronization, Lyapunov methods

1. Introduction

The Chua oscillator is a well known system characterized by its simplicity and chaotic behavior. It contains a nonlinear term originally represented by a piecewise-linear function [22] and displays very rich and typical bifurcation and chaos phenomena such as double scroll and dual double scroll [13]. Some researchers have investigated the way to modify the original system. One of the reasons for doing this was the fact the numerical simulations revealed that not all features of a real circuit were correctly captured by the piecewise-linear circuit [16]. Thus, a smooth nonlinearity was desirable. A cubic

nonlinearity was proposed by [43] as an appropriate modification, physically realizable, that preserved the chaotic characteristics of the oscillator. This nonlinearity has a shape similar to that of the original function but with the advantage that smoothness is gained avoiding analysis difficulties due to the discontinuities of the original function. Some other proposals in which this variation is employed are found in the works by [29], [37] and [40]. A new version of the Chua circuit is investigated by [17]. The objective of the work was to perform an experimental study about the impulsive synchronization of the modified Chua circuits. A simple and flexible modification scheme was presented in which some circuit connections were broken and passive elements were inserted. The resulting circuit was a higher dimensional system that exhibits the original dynamics of the Chua circuit.

The Chua oscillator, as well as other chaotic maps and systems, has been investigated in applications to secure communications. This field became an important research line in the latest years due to the possibility of encrypting information using chaotic systems. The synchronization of two coupled chaotic systems was proven to be feasible as shown by [26]. This discovery aroused interest as a potential means for secure communications [2, 23, 39]. The idea of synchronization is to use the output of the driving system to control the response system in such a way that they both oscillate in a synchronized manner. A wide variety of synchronization schemes have been developed since then, from those that assume perfect knowledge of the system to those that account for uncertainties. For instance, in [1] the synchronization of chaotic systems by means of active control was demonstrated. The authors worked with two systems: one of them composed of two identical Rössler systems and the other one composed of two identical Chen systems. [15] investigates the chaos synchronization between the Lorenz-Stenflo (LS) system and a novel dynamical system called CYQY, as well as the synchronization between an LS system and a hyper chaotic system. This is done by means of adaptive control techniques. [25] investigates chaos synchronization between two different chaotic systems by means of nonlinear control laws. He demonstrates that the two different systems could be controlled using nonlinear control techniques and proved the closed-loop stability by means of linear control theory. [11] studied the synchronization of a two-degree of freedom heavy symmetric gyroscope using the Lyapunov theory with control terms, adaptive control and random optimization. [19] proposed two kinds of synchronization schemes for hyper chaotic systems using adaptive control. The hyper chaotic system they analyzed was presented by [27] and has two

large positive and small negative Lyapunov exponents over a large range of parameters which makes it suitable for secure communications applications. [20] also investigated the synchronization of two hyper chaotic systems. In this case, the authors worked on a Rössler hyper chaotic system with four unknown parameters and applied an adaptive control scheme for functional lag synchronization. In [21] the problem of synchronizing uncertain dynamic systems in the presence of missing data is further investigated. Other examples can be found in the works by [3], [6], [7], [10], [18], [33] and [42], to name a few.

Such a wide variety of synchronization schemes opened the possibility of using the signals generated by chaotic systems as carriers for analog and digital communications. For instance, in [41] a chaotic communication system in which a binary signal is encrypted in the frequency of the sinusoidal term of a chaotic Duffing oscillator is designed. Two chaotic signals of the oscillator are further encrypted with a Delta modulator before they are sent through the channel. In the receiver, a Lyapunov-based observer uses the chaotic signals for retrieving the sinusoidal term that contains the message. A novel frequency estimator is then used to obtain the binary signal. The numerical simulations demonstrated the high accuracy of the proposed scheme and its robustness in noisy environments. [9] developed a chaotic communication system based on multiplication modulation. The transmitter consists of a chaotic system and a chaos multiplication modulator that encrypts the signal. The chaotic signal is generated by using the Gnesio-Tesi chaotic system. The synchronization of the chaotic signals in the recover is achieved by means of an Extended Kalman Filter that estimates the states of the oscillator in the presence of noise. This scheme does not require the knowledge of the initial conditions of the transmitter. The authors also prove that the system security could not be broken with the existing methods at that time. [35] proposed an observer based on parameter modulation theory where the information modulates the parameters of the chaotic system. [38] presented different schemes of chaotic parameter modulation. The objective was to modulate one parameter of the transmitter Chua oscillator while keeping the other at a fixed value. In the receiver, an adaptive controller was implemented in order to determine the corresponding changing parameter.

The objective of this paper is twofold. First, we introduce a new modification of the Chua oscillator and second, a communication scheme is proposed as an application based on it. The modification consists in changing the nonlinear term to a smooth nonlinear function that is also bounded. We present

different proofs of chaoticity of this newly modified system. Thus, a bifurcation diagram, a Poincaré map and the Lyapunov exponents are presented in order to show how the modified oscillator features chaotic behavior when the appropriate parameters values are chosen. The modified Chua oscillator is used to encrypt/decrypt a message signal based on the scheme proposed by [44] in which a highly nonlinear function is used along with 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 paper is as follows. A brief introduction to the Chua oscillator and the details of the proposed modification are given in Section 2. The application to secure communications is then presented. The details of the transmitter and receiver as well as the encryption/decryption blocks are explained in Section 3. Then, the numerical results corresponding the secure communications application are presented in Section 4. Finally, conclusions are outlined in Section 5.

2. Modified Chua oscillator

The Chua oscillator, as shown in Figure 1(a), is the physical realization of an oscillator developed by Leon Chua during his visit to Waseda University (Tokyo, Japan) in 1983 - 1984. The circuit is well known for its simplicity and the fact that its dynamic becomes chaotic when the appropriate devices are selected. Hence the interest it has raised since it was published and that is patent in several works found in literature. The dynamic of the circuit is given by the following set of equations [22]:

$$C_1 \frac{dv_{C_1}}{dt} = G(v_{C_2} - v_{C_1}) - g(v_{C_1}), \tag{1}$$

$$C_2 \frac{dv_{C_2}}{dt} = G(v_{C_1} - v_{C_2}) + i_L, \tag{2}$$

$$L \frac{di_L}{dt} = -v_{C_2}. \tag{3}$$

where v_{C_1}, v_{C_2} denote the voltage across the capacitors C_1 and C_2, respectively and i_L is the current through the inductor L; G is the electric conductance of the resistor. The function $g(v_{C_1})$ is a piecewise linear function that can be graphically represented as in Figure 1(b) and is given by:

$$g(v_{C_1}) = m_0 v_{C_1} + \frac{1}{2}(m_1 - m_0)|v_{C_1} + B_p| + \frac{1}{2}(m_0 - m_1)|v_{C_1} - B_p|. \tag{4}$$

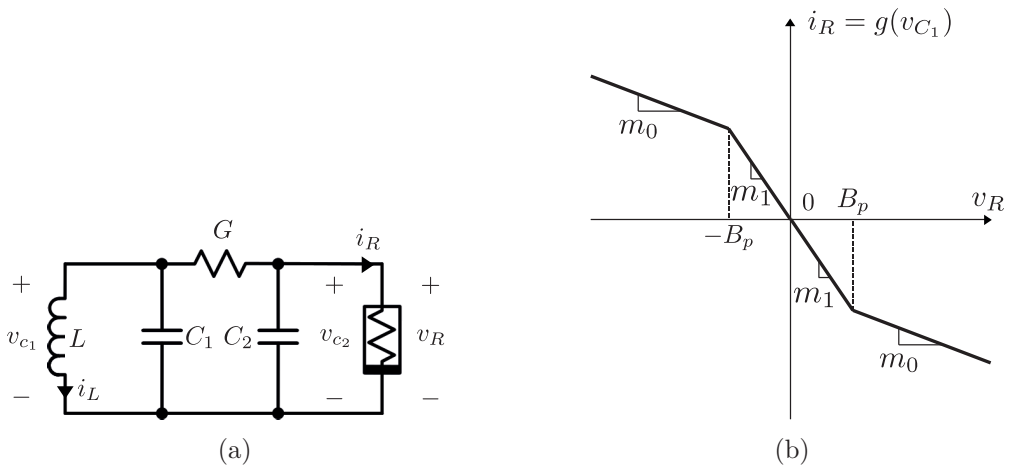

Figure 1: The Chua circuit. (a) Electric diagram. (b) Graphic of the nonlinear function $g(v_{C_1})$.

where m_0 and m_1 are parameters with units of Ω^{-1} and B_p has units of V.

Chaos in the circuit occurs when $1/C_1 = 9$, $1/C_2 = 1$, $1/L = 7$, $G = 0.7$, $m_0 = -0.5$, $m_1 = -0.8$ and $B_p = 1$ [22]. In that paper, the authors physically proved the existence of a chaotic attractor using this circuit but it was not until 1986 that Chua, Matsumoto and Komuro provided a rigorous mathematical demonstration of the chaoticity of this system [5].

The dynamic equations derived form the electric circuit analysis can be transformed into a dimensionless form. Thus the following set of equations is frequently used for studying the Chua chaotic oscillator [5]:

$$\dot{x}_1 = \alpha\left(x_2 - f(x_1)\right), \tag{5}$$

$$\dot{x}_2 = x_1 - x_2 + x_3, \tag{6}$$

$$\dot{x}_3 = -\beta x_2, \tag{7}$$

$$f(x_1) = m_1 x_1 + \frac{1}{2}(m_0 - m_1)(|x_1 + 1| - |x_1 - 1|). \tag{8}$$

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 to obtain chaotic behavior. The function $f(x_1)$ is the canonical piecewise-linear function describing an odd-symmeric three-segment piecewise-linear curve having a breakpoint at $x_1 = -1$ and at $x_1 = 1$, a slope equal to $m_0 = a+1 < 0$ at the inner segment and $m_1 = b+1 > 0$ at the outer segments, respectively.

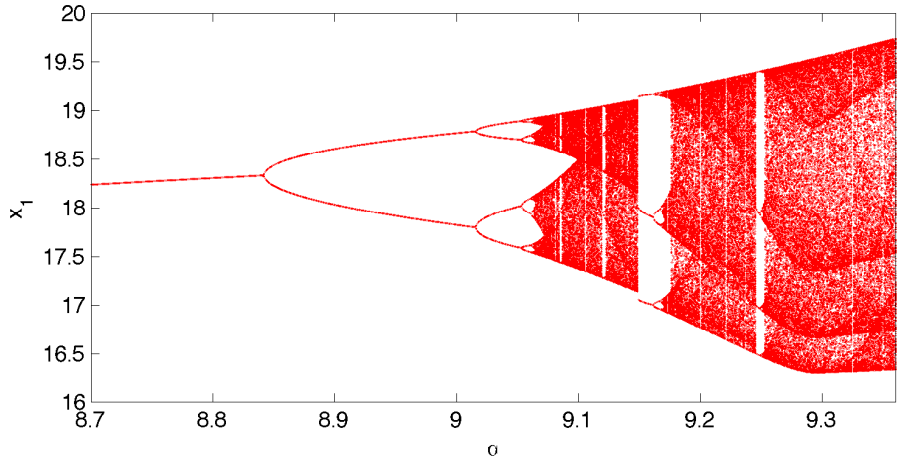

Figure 2: Bifurcation diagram of the modified Chua oscillator.

In the next subsection of this paper, we will give the details of the modification of the Chua oscillator that we propose.

2.1. Proposed modification

We modified the original oscillator given by Equations 5 - 8 by choosing the following characteristic function $f(x_1)$:

$$f(x_1) = -\sin x_1 \cdot e^{-0.1|x_1|}. \tag{9}$$

Note that, unlike Equation 8, Equation 9 is a bounded smooth function such that $|f(x_1)| \leq 1$. The new system has infinite equilibrium points located at $(x_1, x_2, x_3) = (-k\pi, 0, k\pi)$, $k \in \mathbb{Z}$, and it is possible to show that all of them are unstable. Figure 2 is a bifurcation diagram of the modified Chua oscillator. It depicts the route to chaos of the oscillator variable x_1 when the parameter α is varied form 8.7 to 9.36 and the parameter β is set at a fixed value equal to 14.35. Period doubling occurs at $\alpha = 8.84$, 9.01 and 9.05 approximately, and then, as α increases, the dynamics becomes more and more complex until it reaches chaos at $\alpha = 9.065$ approximately. Figure 3 illustrates the limit cycles of the oscillator for different values of α, namely 8.50, 8.90, 9.05, 9.10, 9.15 and 9.35 with $\beta = 14.35$.

According to the bifurcation diagram, the system of Equations 5-7 and 9 is chaotic when $\alpha = 9.35$ and $\beta = 14.35$. The sensibility of this oscillator to small changes in the initial conditions can be observed in Figure 4. This figure

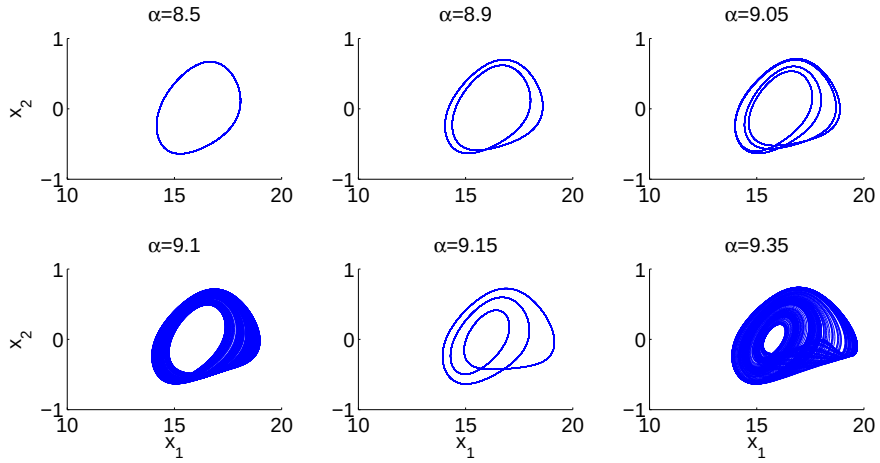

Figure 3: Limit cycles of the modified Chua oscillator for different values of α.

shows a comparison of the oscillator trajectories with three different sets of initial conditions: IC1=[15, 0, -15], IC2=[15, 0.01, -15] and IC3=[15.01, 0, -15].

2.2. Poincaré map and Lyapunov exponents

Further proofs of chaoticity of the modified Chua oscillator are given in this subsection. We begin by plotting a Poincaré map of the modified oscillator. It is well known that the Poincaré map is a useful graphical tool that helps determining if a system is periodic, non-periodic, chaotic or random [34]. It is created by plotting the points where the trajectories of the system intersect a particular plane. If the Poincaré map consists neither of a finite number of points nor of points filling up a closed curve but nevertheless appear ordered, then it is a strong indicator of chaos [34].

Figure 6 depicts the Poincaré map of the modified Chua oscillator with $\alpha = 9.35$ and $\beta = 14.35$, generated when the trajectories intersect the plane $x+y+z+1 = 0$ as it is depicted in Figure 5. The map of Figure 6 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.

Finally, the Lyapunov exponents of the system are calculated and provided as another proof of chaoticity. The Lyapunov exponents are the average exponential rates of convergence or divergence of nearby orbits in phase space

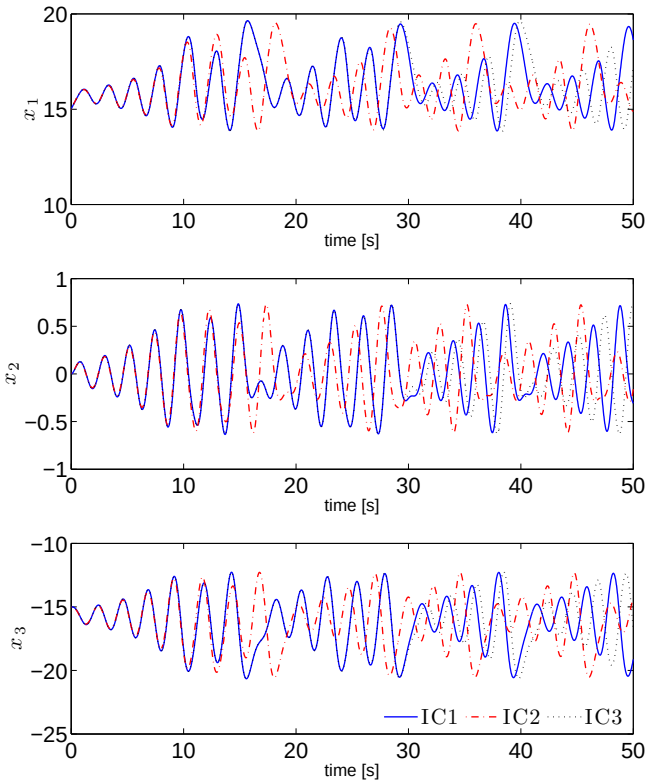

Figure 4: Oscillator dynamics subject to different initial conditions.

[28]. When the system is chaotic, the trajectories diverge, on average, at an exponential rate characterized by the largest Lyapunov exponent. 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 [36]. A positive exponent gives an indication of the rate at which the ability to predict the system response is lost [24]. Several algorithms have been developed to calculate both the largest Lyapunov exponent or all of them for a given system (see for instance [24], [31], [28], [36] to name a few). In order to calculate the maximum Lyapunov exponent, λ, we applied the numerical algorithm detailed in [34]. The algorithm was implemented in Matlab/Simulink. The simulation was run for a long time enough to let the system trajectories converge. Figure 7 shows how λ evolves until it reaches stability. From these

data, it could be found that the maximum Lyapunov exponent of our modified oscillator is $\lambda \approx 0.0025$ which confirms the chaoticity of the system. We have also calculated all the Lyapunov exponents following the algorithms described in [36] using the Matlab program developed by [12]. The resulting exponents were $\lambda_1 = 0.192222$, $\lambda_2 = 0.003675$ and $\lambda_3 = -1.807019$. The Lyapunov dimension was also calculated. It was done following the Kaplan-Yorke definition which establishes a conjecture about the fractal dimension of the attractor and the Lyapunov spectrum [30]. It can be defined as the fractional dimension in which a cluster of initial conditions will neither expand nor contract as it evolves in time [4]. The Lyapunov dimension D_L can be calculated according to [30]:

$$D_L = j + \frac{\sum_{i=1}^{j} \lambda_i}{|\lambda_{j+1}|}$$

where j is the largest integer such that $\lambda_1 + \lambda_2 + ... + \lambda_j > 0$. Then, the Lyapunov dimension of the system is $D_L = 2.1084$ which is consistent with that of a third order chaotic system. Figure 8 illustrates the evolution of the Lyapunov exponents when the initial conditions are IC= $[15, 0, -15]$. Finally the results obtained with the Matlab program developed by [32] which is based on the algorithms by [8] and [36] are: $\lambda_1 = 0.22037$, $\lambda_2 = -0.005839$ and $\lambda_3 = -1.82700$ with $D_L = 2.1174$ and IC= $[15, 0, -15]$.

In the remaining of the paper, we present an application to secure communications using this oscillator. In order to gain higher flexibility in the implementation of the communication system, let $t = \mu\tau$, $\mu > 0$. This time scaling allows for the use of higher frequency message signals without

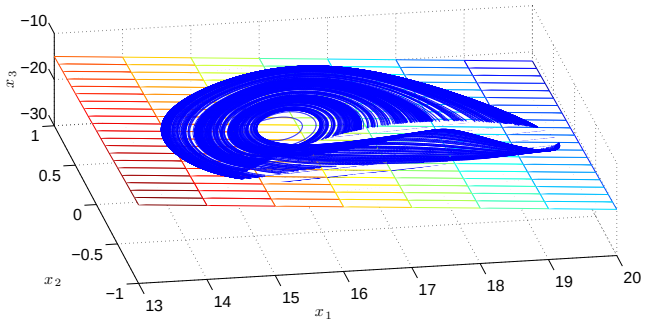

Figure 5: Trajectories of the modified Chua oscillator intersecting the plane $x+y+z+1 = 0$.

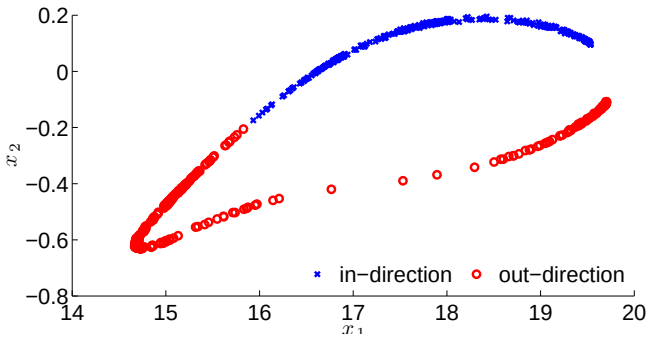

Figure 6: Poincaré map of the oscillator as seen in the XY plane perspective.

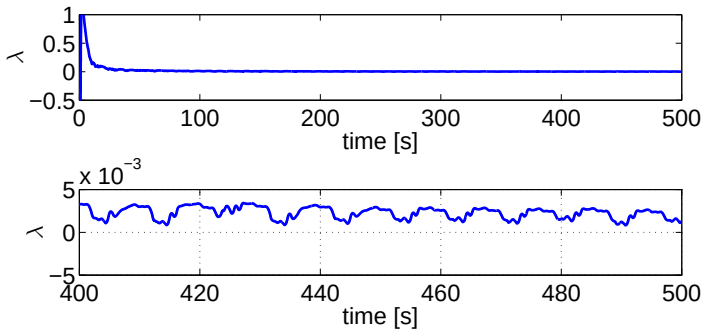

Figure 7: Top: evolution of the maximum Lyapunov exponent. Bottom: zoom of the upper figure.

compromising the chaotic behavior of the oscillator. Thus $dt = \mu d\tau$ and the following state space realization of the modified Chua oscillator can be obtained:

$$\dot{x}_1 = \mu\alpha\left(x_2 - f(x_1)\right), \tag{10}$$

$$\dot{x}_2 = \mu\left(x_1 - x_2 + x_3\right), \tag{11}$$

$$\dot{x}_3 = -\mu\beta x_2, \tag{12}$$

$$f(x_1) = -\sin x_1 \cdot e^{-0.1|x_1|}. \tag{13}$$

3. Application to secure communications

In this section, we present the scheme of a secure communication system based on the modified Chua oscillator. The diagram of the proposed scheme

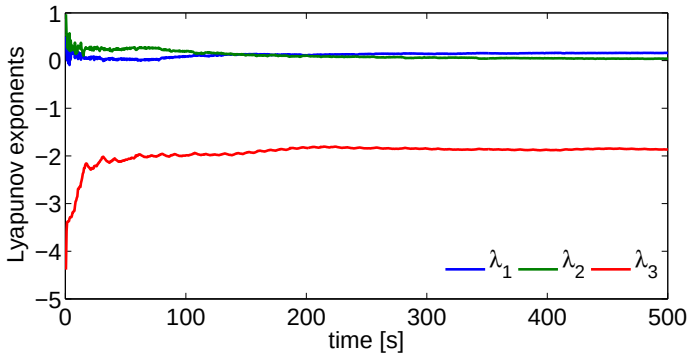

Figure 8: Evolution of the Lyapunov exponents.

is shown in Figure 9. It consists of the following elements:

1) *Chaotic oscillator*: It is the modified Chua oscillator presented in Section 2.1 that generates three signals (x_1, x_2 and x_3). The signal x_1 is sent through the first channel for synchronization purposes.

2) *Encryption block*: The message $m(t)$ is encrypted using a nonlinear function $m_e(t) = \phi(\mathbf{x}(t), m(t))$, $\mathbf{x}(t) = [x_1, x_2, x_3]$. This signal is sent through the second channel.

3) *Channels*: Two channels transmit the chaotic signal and the encrypted message. Channel noise $n_d(t)$ is added to the signals $x_1(t)$ and $m_e(t)$ converting them into $x_{1n}(t)$ and $m_{en}(t)$ respectively. 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*: A synchronization system is implemented in order to retrieve the chaotic signals. It works by using the chaotic signal $x_{1f}(t)$ only.

5) *Decryption block*: The message signal is decrypted by using a nonlinear function $m_d(t) = \psi(\mathbf{y}(t), m_{ef}(t))$, $\mathbf{y}(t) = [y_1, y_2, y_3]$. In this case, $\mathbf{y}(t)$ is the estimation of the chaotic signals $\mathbf{x}(t)$ generated by the synchronization block.

6) *Retrieving block*: In this stage, a decision algorithm is implemented in the case that the transmitted message corresponds to a digital signal.

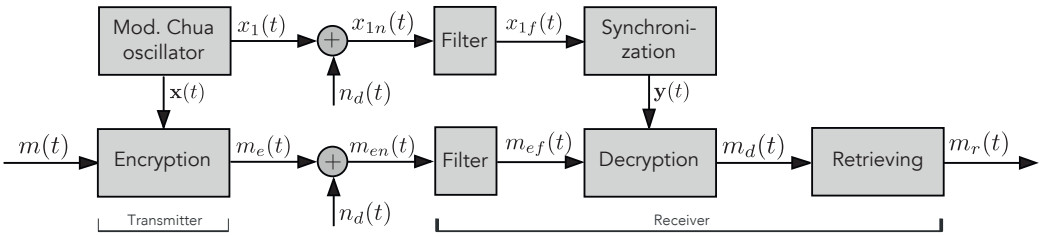

Figure 9: Block diagram of the proposed communication system.

The details of the main blocks of the communication system are given in Sections 2 - 3.2

3.1. Encryption and decryption

We use the encryption/decryption scheme proposed by [44] in his work about chaotic secure communication systems. We have modified the encryption and decryption functions as well as the chaotic oscillator. In this scheme, there are two channels in order to make the synchronization process faster. We now summarize the encryption/decryption mechanism:

- *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 $\mathbf{x} \in \mathbb{R}^3$ and satisfies the following property: for every fixed pair of $(\mathbf{x}, m) \in \mathbb{R}^3 \times \mathbb{R}$, there exists a unique function $\psi : \mathbb{R}^3 \to \mathbb{R}$ that is continuous in its first argument $\mathbf{x} \in \mathbb{R}^3$ and is such that $\psi(\mathbf{x}, \phi(\mathbf{x}, m)) = m$. 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*: In the receiver side of the communication system, a synchronization block is implemented in order to retrieve the chaotic oscillator signals and get the necessary information for the decryption. Recall that the oscillator signal x_1 is sent though one of the channels for synchronization purposes. This signal is sufficient to generate the signals y_1, y_2 and y_3 that are estimations of the master oscillator signals x_1, x_2 and x_3, respectively. Retrieving this signal is necessary in order to decrypt the message that is received on the second channel. The details of the synchronizer will be provided in Section 3.2

- *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 $m(t)$.

3.2. Synchronization

The synchronization block is implemented in the receiver side of the communication system in order to retrieve the oscillator signals. It consists of a dynamic system that takes the signal x_1 sent through the first communication channel producing the signals y_1, y_2 and y_3 that are estimations of the oscillator signals x_1, x_2 and x_3, respectively. The following theorem is the base of the synchronization system.

Theorem 1. *Consider the modified Chua oscillator given by Equations 10 - 12 and 13 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:*

$$\dot{y}_1 = \mu k \cdot \mathtt{sgn}(x_1 - y_1), \tag{14}$$

$$\dot{y}_2 = \mu \left(x_1 - y_2 + y_3\right), \tag{15}$$

$$\dot{y}_3 = -\mu\beta y_2, \tag{16}$$

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

i) $\lim\limits_{t \to T_s} y_1(t) = x_1(t)$, *for a given* $T_s \in \mathbb{R}^+$.

ii) $\lim\limits_{t \to \infty} y_2(t) = x_2(t)$.

iii) $\lim\limits_{t \to \infty} y_3(t) = x_3(t)$.

Proof 1. *Let the system of Equations 10 - 12 be the master and the system of Equations 14 - 16 be the slave. The function $f(x_1)$ in 13 is such that $|f(x_1)| \leq 1$, $\forall t \geq 0$. Since the system 10 - 12 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:*

$$e_1 = x_1 - y_1, \ \dot{e}_1 = \dot{x}_1 - \dot{y}_1. \tag{17}$$

Consider the terms $\dot{x}_1$ and $\dot{y}_1$ from Equations 5 and 14, respectively. Substitution of these terms into Equation 17 yields:

$$\dot{e}_1 = \mu\alpha(x_2 - f(x_1)) - \mu k \texttt{sgn}(x_1 - y_1). \tag{18}$$

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

$$\begin{aligned}
\dot{V}_1 = e_1\dot{e}_1 &= e_1\mu\alpha x_2 - e_1\mu\alpha f(x_1) - \mu k e_1 \texttt{sgn}(e_1) \\
&= -\mu k|e_1| + \mu\alpha x_2 e_1 - \mu\alpha f(x_1)e_1 \\
&\leq -\mu k|e_1| + \mu\alpha x_2 e_1 + |\mu\alpha f(x_1)e_1| \\
&\leq -\mu k|e_1| + \mu\alpha x_2 e_1 + |\mu\alpha| \cdot 1 \cdot |e_1| \\
&= -\mu k|e_1| + \mu\alpha x_2 e_1 + \mu\alpha|e_1|.
\end{aligned}$$

Recall that $\alpha > 0$ and $|x_2(t)| < \rho$. Thus we can write:

$$\begin{aligned}
\dot{V}_1 &\leq -\mu k|e_1| + \mu\alpha\rho|e_1| + \mu\alpha|e_1| \\
&= -\mu|e_1|\left(k - \alpha(\rho + 1)\right).
\end{aligned}$$

$\dot{V}_1$ 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 15 and 16. 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 6 and 15 we have that

$$\begin{aligned}
\dot{e}_2 &= \mu\left(x_1 - x_2 + x_3 - x_1 + y_2 - y_3\right) \\
&= \mu\left(-x_2 + x_3 + y_2 - y_3\right) \\
&= \mu\left(-e_2 + e_3\right).
\end{aligned}$$

From Equations 7 and 16 we have that

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

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

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

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

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

4. Numerical results

The communication system of Section 3 was implemented in Matlab/ Simulink for performance analysis. The transmitter is the implementation of Equations 10 - 13 with $\alpha = 9.35$ and $\beta = 14.35$. The receiver is the implementation of Equations 14 - 15 with $k = 1000$. For simulation purposes, noise was added to each signal and thus, a bank of filters was implemented at the input of the receiver to clean the signals before their processing. The filters implemented in the system are of the Butterworth type with cutoff frequencies of 40 rad/s and 100 rad/s. They have the following transfer functions:

i) Channel 1 (Synchronization signal): $H_1(s) = \dfrac{1600}{s^2 + 56.6s + 1600}$.

ii) Channel 2 (Encrypted message): $H_2(s) = \dfrac{10000}{s^2 + 141s + 10000}$.

The following simulations were performed with the following initial conditions: $x_1(0) = 15$, $x_2(0) = 0$, $x_3(0) = -15$, $y_1(0) = 14$, $y_2(0) = 1$ and $y_3(0) = -14$. Figure 10 illustrates the synchronization of the chaotic signals in the receiver. It is observed that signal y_1 synchronizes first, at $t = 0.2$

seconds approximately, while signals y_2 and y_3 take longer (5 seconds, approximately). 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 initially, during the transient response, when decrypting 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.

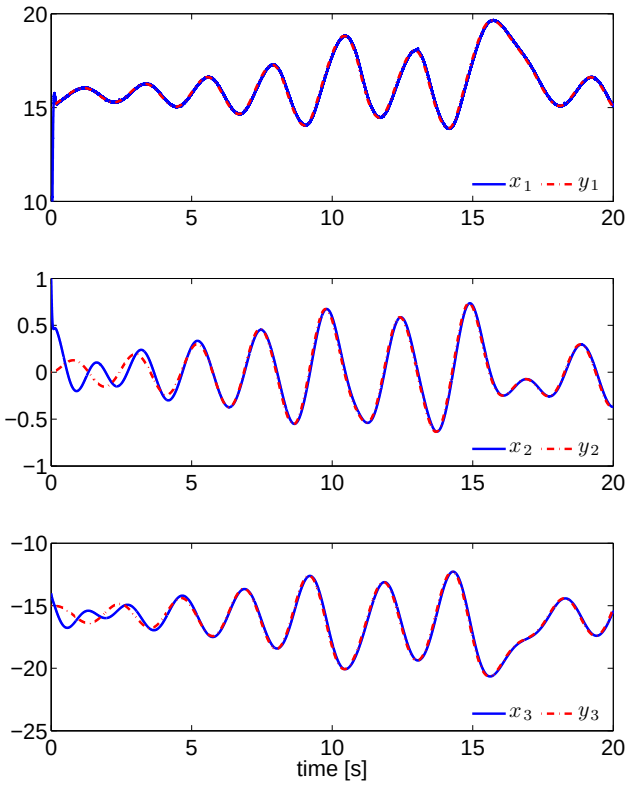

Figure 10: Oscillator signals synchronization and their estimations.

In the first simulation, the message $m(t)$ is composed of a sequence of sine waves with frequencies $\omega = \pi$, 2π and 3π rad/s and $\mu = 1$. The encryption and decryption functions were chosen as:

$$\textit{Encryption:} \quad \phi: \; m_e(t) = |x_3|^{\frac{2}{3}} - 6.5 + (x_2^2 + 0.1)\, m(t).$$

$$\textit{Decryption:} \quad \psi : m_d(t) = \frac{m_e(t) + 6.5 - |y_3|^{\frac{2}{3}}}{y_2^2 + 0.1}.$$

Figure 11 shows the simulation results of the 50-second transmission. The top subfigure compares the encrypted message signal as it travels through the channel. Thus, this subfigure depicts the signals $m_e(t)$ (generated by the master oscillator), $m_{en}(t)$ (the noisy $m_e(t)$ signal) and $m_{en}(t)$ (the filtered version of the noisy signal). The bottom subfigure shows the original message sent, $m(t)$, compared to the decrypted version $m_d(t)$. As explained earlier, during the first five seconds of transmission the estimation is not good because the slave oscillator signals have not synchronized yet. Once synchronization is achieved, the message is estimated correctly as can be observed in the figure.

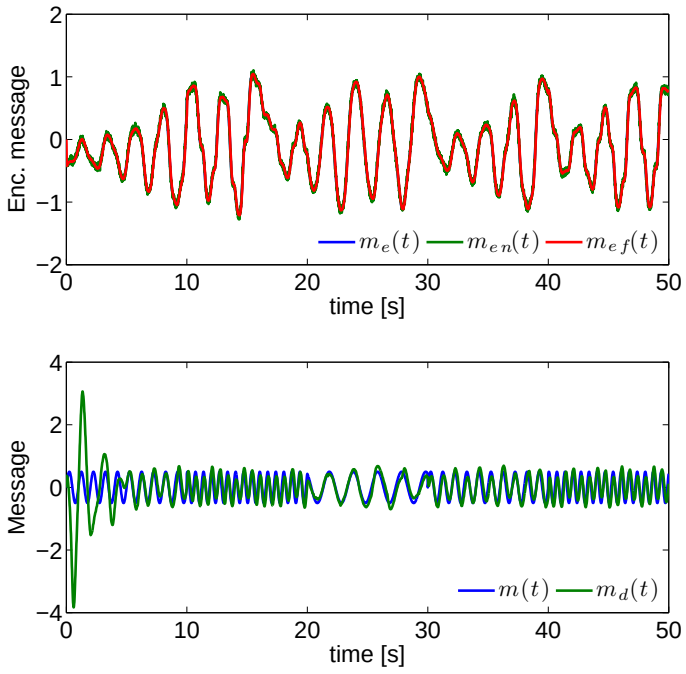

Figure 11: Sinusoidal message signal. Top: encrypted message (original, noisy and filtered). Bottom: original and retrieved message.

In the second test, a digital message $m(t)$ is sent through the channel. The digital message signal consists of a binary signal with the following values:

-0.5 and +0.5. The message is sent at a rate of T_b bits/second. For this simulation, we set $\mu = 5$ and $T_b = 0.5$. The encryption and decryption functions were chosen as:

$$\textit{Encryption:} \quad \phi : \; m_e(t) = \mathtt{sgn}(x_2)m(t).$$

$$\textit{Decryption:} \quad \psi : \; m_r(t) = \mathtt{sgn}(y_2)m_e(t).$$

Figure 12 shows the first ten 10 seconds of transmission of the digital message. The top subfigure compares the encrypted message (original, noisy and filtered). The bottom subfigure compares the original digital message $m(t)$ to the decrypted message in the receiver $m_d(t)$. Recall that $m(t)$ is a digital signal and thus a decision algorithm must be implemented before obtaining the actual message. The decision algorithm implemented in this case is as follows: at an instant $t = t_k$, $k = 1, 2, ..., n$, compare the value of $m_d(t_k)$ to a threshold equal to zero. If $m_d(t_k) \geq 0$ then $m_r(t_k) = +0.5$, otherwise, $m_r(t_k) = -0.5$. Figure 13 (top) shows the results. As explained earlier, some dummy information is sent before the actual message in order to let the slave oscillator synchronize and avoid errors in retrieving the message. The error is defined as $e_m(t_k) = |m(t_k) - m_r(t_k)|$. In this case, 2 seconds of dummy information were introduced followed by the true message which was correctly retrieved (Figure 13, bottom). The time to synchronize the signals is less than in the previous case because the time has been scaled by the factor $\mu = 5$.

5. Conclusion

In this paper we introduced a modified Chua chaotic oscillator. The nonlinear term of the original oscillator was changed to a smooth and bounded function that allows for easier analysis and synchronization with another oscillators. The diagram of bifurcation, the Poincaré map and the Lyapunov exponents were presented as proofs of the chaotic dynamics of the proposed oscillator. An application to secure communications using the modified oscillator was developed and its performance evaluated by numerical simulations.

Acknowledgments

Mauricio Zapateiro is supported by the fellowship from CAPES/Programa Nacional de Pos-Doutorado from Brazil. This work has been partially funded

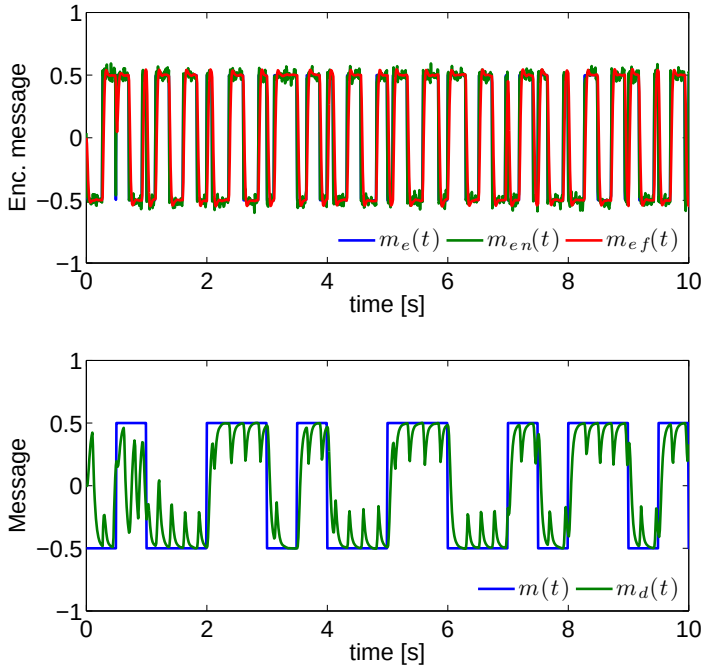

Figure 12: Digital message signal. Top: encrypted message (original, noisy and filtered). Bottom: original and estimated message.

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 2014SGR859.

References

[1] H.N. Agiza, M.T. Yassen. Synchronization of Rossler and Chen chaotic dynamical systems using active control, *Physics Letters A* 278, pp. 191–197 (2001).

[2] B. Andrievsky. Adaptive synchronization methods for signal transmission on chaotic carriers, *Mathematics and Computers in Simulation* 58 (46), 285 –293 (2002).

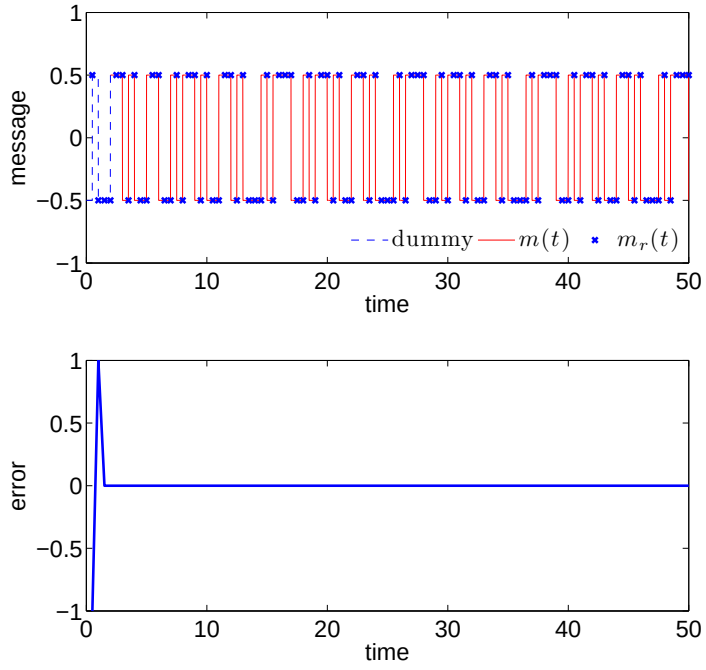

Figure 13: Digital message signal. Top: retrieved message. Bottom: retrieval error.

[3] S. Benítez, L. Acho. Impulsive synchronization for a new chaotic oscillator, *International Journal of Bifurcation and Chaos* 17, 617–623 (2007).

[4] K.E. Chlouverakis, J.C. Sprott. A comparison of correlation and Lyapunov dimensions, *Physica D* 200(1-2), pp. 156–164 (2005).

[5] L.O. Chua, M. Komuro, T. Matsumoto. The double scroll family, *IEEE Transactions on Circuits and Systems* 33(11), pp. 1073-1118 (1986).

[6] L.O. Chua, M. Itoh, L. Kocarev, K. Eckert. Chaos synchronization in Chua's circuit, *Journal of Circuits, Systems and Computers* 3, pp. 93–108 (1993).

[7] C.F. Chuang, Y.J. Sun, W.J. Wang. A novel synchronization scheme with a simple linear control and guaranteed convergence time for generalized Lorenz chaotic systems *Chaos* 22, http://dx.doi: 10.1063/1.4761818 (2012).

[8] J.P. Eckmann, D. Ruelle. Ergodic theory of chaos and strange attractors, *Reviews of Modern Physics* 57(3), pp. 617–656 (1985).

[9] K. Fallalih, H. Leung. A chaos secure communication scheme based on multiplication modulation. *Communications in Nonlinear Science and Numerical Simulation* 15, pp. 368–383 (2010).

[10] M. Feki. An adaptive chaos synchronization scheme applied to secure communication, *Chaos, Solitons and Fractals* 18, 141–148 (2003).

[11] Z.M. Ge, J.K. Lee. Chaos synchronization and parameter identification for gyroscope system, *Applied Mathematics and Computation* 163, pp. 667-682 (2005).

[12] V.N. Govorukhin. Lyapunov exponent calculation for ODE-system, MATLAB code, 2004.

[13] W. Guo, D. Liu. Adaptive control in Chua's circuit. *Mathematical Problems in Engineering* 2011, doi:10.1155/2011/620946 (2011).

[14] T.T. Hartley. The Duffing double scroll, *Proc. of the American Control Conference*, Pittsburgh, PA, USA, pp. 419–423 (1989).

[15] J. Huang. Adaptive synchronization between different hyper chaotic systems with fully uncertain parameters, *Physics Letters A* 372, pp. 4799–4804 (2008).

[16] A.I. Khibnik, D. Roose, L.O. Chua. On periodic orbits and homoclinic bifurcations in Chua's circuit with a smooth nonlinearity, *International Journal of Bifurcation and Chaos*, 3, pp. 363–384 (1993).

[17] R. Kiliç. Experimental study on impulsive synchronization between two modified Chua's circuits, *Nonlinear Analysis: Real World Applications* 7, pp. 1298–1303 (2006).

[18] H.R. Koofigar, F. Sheikholeslam, S. Hosseinnia. Robust adaptive synchronization for a general class of uncertain chaotic systems with application to Chua's circuit. *Chaos* 21, doi:10.1063/1.367169 (2011).

[19] Y. Lan, Q. Li. Chaos synchronization of a new hyper chaotic system, *Applied Mathematics and Computation* 217, pp. 2125–2132 (2010).

[20] T.H. Lee, J.H. Park. Adaptive functional projective lag synchronization of a hyperchaotic Rössler system, *Chinese Physics Letters* 26(9), pp. 90507-1–4 (2009).

[21] T.H. Lee, J.H. Park, S.M. Lee, O.M. Kwon. Robust sampled-data control with random missing data scenario, *International Journal of Control* 87(9), pp. 1957–1969 (2014).

[22] T. Matsumoto, L.O. Chua, M. Komuro. The double scroll, *IEEE Transactions on Circuits and Systems* 32, pp. 797–818 (1985).

[23] O. Morgul, M. Feki. A chaotic masking scheme by using synchronized chaotic systems, *Physics Letters A* 251 (3), 169 – 176 (1999).

[24] P.C. Müller. Calculation of Lyapunov exponents for dynamic systems with discontinuities, *Chaos, Solitons and Fractals* 5(9), pp.1671-1681 (1995).

[25] J.H. Park. Chaos synchronization between two different chaotic dynamical systems, *Chaos, Solitons and Fractals 27*, pp. 549–554 (2006).

[26] Pecora, L.M., Carroll, T.L., Feb 1990. Synchronization in chaotic systems. Phys. Rev. Lett. 64, 821–824.
URL http://link.aps.org/doi/10.1103/PhysRevLett.64.821

[27] G.Y. Qi, M.A. van Wyk, B.J. van Wyk, G. Chen. On a new hyperchaotic system, *Physics Letters A* 372, pp. 124–136 (2008).

[28] M.T. Rosenstein, J.J. Collins, C.J. de Luca. A practical method for calculating largest Lyapunov exponents from small data sets, *Physica D* 65, pp. 117–134 (1993).

[29] H. Salarieh, A. Alasty. Adaptive chaos synchronization in Chua's systems with noisy parameters, *Mathematics and Computer in Simulation* 79, pp. 233–241 (2008).

[30] M. Sandri. Numerical calculation of Lyapunov exponents, *The Mathematica Journal* 6(3), pp. 78–84 (1996).

[31] M. Sano, Y. Sawada. Measurement of the Lyapunov spectrum from a chaotic time series, *Physical Review Letters* 55(10), pp. 1082-1085 (1985).

[32] W.K. Steve. Lyapunov Exponents Toolbox for MATLAB, 1998.

[33] J. Tang. Synchronization of different fractional order time-delay chaotic systems using active control, *Mathematical problems in Engineering* 2014, doi:10.1155/2014/262151 (2014).

[34] J.J.Thomsen. Vibrations and Stability : Advanced Theory, Analysis, and Tools, Springer (2003).

[35] X.Y. Wang, M.J. Wang. A chaotic secure communication scheme based on observer, *Communications in Nonlinear Science and Numerical Simulation* 14, pp. 1502–1508 (2009).

[36] 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).

[37] T. Wu, M.S. Chen. Chaos control of the modified Chua's circuit system, *Physica D* 164, pp. 53–58 (2002).

[38] T. Yang and L.O. Chua. Secure communication via chaotic parameter modulation, *IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications* 43, pp. 817–819 (1996).

[39] T. Yang. A survey of chaotic secure communication systems, *International Journal Computational Cognition* 2, pp. 81–130 (2004).

[40] M.T Yassen. Adaptive control and synchronization of a modified Chua's circuit system, *Applied Mathematics and Computation* 135, pp. 113–128 (2003).

[41] 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).

[42] H. Zhang, W. Huang, Z. Wang, T. Chai. Adaptive synchronization between two different chaotic systems with unknown parameters, *Physics Letters A* 350, pp. 363–366 (2006).

[43] G.Q. Zhong. Implementation of Chua's circuit with a cubic nonlinearity, *IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications* 41, pp 934–941 (1994).

[44] 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).