Applied Mathematics and Computation 247 (2014) 712–722

Contents lists available at ScienceDirect

Applied Mathematics and Computation

journal homepage: www.elsevier.com/locate/amc

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
[b] Control, Dynamics and Applications Group – CoDAlab, Departament de Matemàtica Aplicada III, Universitat Politècnica de Catalunya-BarcelonaTECH, Comte d'Urgell 187, E08036 Barcelona, Spain

ARTICLE INFO

Keywords:
Chua oscillator
Chaos
Secure communication
Synchronization
Lyapunov methods

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.

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 [21] 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 piece-wise-linear circuit [15]. Thus, a smooth nonlinearity was desirable. A cubic nonlinearity was proposed by [42] 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 [28,36,39]. A new version of the Chua circuit is investigated by [16]. 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 [25]. This discovery aroused interest as a potential means for secure communications [2,22,38]. The idea of synchronization is to use

* Corresponding author.
E-mail addresses: hoz@utfpr.edu.br (M. Zapateiro De la Hoz), leonardo.acho@upc.edu (L. Acho), yolanda.vidal@upc.edu (Y. Vidal).

http://dx.doi.org/10.1016/j.amc.2014.09.031

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. Huang [14] 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. Park [24] 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. Ge and Lee [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. Lan and Li [18] proposed two kinds of synchronization schemes for hyper chaotic systems using adaptive control. The hyper chaotic system they analyzed was presented by [26] and has two large positive and small negative Lyapunov exponents over a large range of parameters which makes it suitable for secure communications applications. Lee and Park [19] 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 [20] 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 [3,6,7,10,17,32,41], 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 [40] 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. Fallalih and Leung [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. Wang and Wang [34] proposed an observer based on parameter modulation theory where the information modulates the parameters of the chaotic system. Yang and Chua [37] 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 Zhon-Ping [43] 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 Fig. 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 [21]:

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

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

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