IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 1, Ver. II (Jan - Feb. 2015), PP 32-35
www.iosrjournals.org

Evaluating the Synchronization of a Chaotic Encryption Scheme Using Different Channel Parameters

Joan Jani[1], Partizan Malkaj[2]
[1,2] *(Department of Engineering Physics, Polytechnic University of Tirana, Albania)*

Abstract: *In this paper we perform a quality control over an chaotic masking encryption scheme. We simulate a nonlinear system based on Chua's chaotic oscillator. Simulations were carried out using Multisim, which is widely accepted as the circuit simulation software that provides for an interface adequately close to real implementation. In order the circuit to be used in chaotic encryption schemes we have implemented a master slave chaotic synchronization scheme. We investigate the robustness of the simulation with respect to the resistance of the line which connect the two systems. For our results we have figure out that the synchronization could be achieved if the line has a total resistance below 3.5kΩ.*
Keywords: *chaotic circuit, chaotic encryption, nonlinear circuits, Chua's circuit.*

I. Introduction

In recent year there have been proposed many circuit based on chaotic operation [1], [2], [3]. The Chua's chaotic circuit it was the first nonlinear circuit to reveal the presence of chaos. Sample circuits with a simplify topology with a transistor operated in reverse active region [4]. In addition the presence of chaos could be seen and in a differential amplifier topology [5]. The presence of chaos in these circuits has been verified using the nonlinear time series analysis[6]. One of the great achievements of the chaos theory is the application in secure communications.[7].

The goal of the article is to present the performance of a chaotic encryption scheme, simulating the path loss over a chaotic masking system. This is very important in order the chaotic encrypted signal to be decrypted at the receiver.

The paper is structured as follow. After a short introduction, a short presentation of Chua's chaotic circuit follows. We achieve the synchronization of two Chua's circuit using simulation. The evaluation of the system is performed changing the path loses between the receiver and transmitter. At the end the conclusion of the paper are given

II. The Chua's Circuit

In this section we present the Chua's chaotic oscillator. The circuit is simple circuit which exhibits a variety of bifurcation and chaos. The ability to synchronize remote systems through the use of a common drive signal provides the potential for coherent communication over deferent channels.[8]

It consists of simple electronic components resistors, inductor, capacitors and operational amplifiers. The L_1 inductor and C_2 capacitor build a resonant circuit (fig. 1), whereas their values determine the basic oscillation frequency[9].

The use of mathematical tools is necessary for a more detailed analysis of chaotic circuits. The circuit must be described by a suitable mathematical model – by corresponding differential equations [10]. The equations bellow describes the behavior of the Chua's circuit:

$$\begin{aligned} C_1\frac{dv_1}{dt} &= \frac{v_2 - v_1}{R} - h(v_1) \\ C_2\frac{dv_2}{dt} &= \frac{v_1 - v_2}{R} + i_L \\ L\frac{di_L}{dt} &= -v_2 \end{aligned} \tag{1}$$

Where v_1 implies the voltage over the capacitor C_1, v_2 the voltage over the capacitor C_2, i_L the current through the inductance, C_1 and C_2 the capacitance of the capacitor C_1 and C_2 respectively. In addition it is needed to mention that $h(v_1)$ is the nonlinear resistor of the circuit. The current versus voltage characteristic of this resistor could be written as:

$$h(v_1) = G_b v_1 + \frac{1}{2}(G_a - G_b)(|v_1 + E| - |v_1 - E|) \tag{2}$$

where G_a and G_b are the slopes of conductance in the inner and outer regions, which in our case are negative, and E denote the breakpoints [10]. As it easy to be seen, the nonlinear oscillator is coming from a typical RLC oscillator.

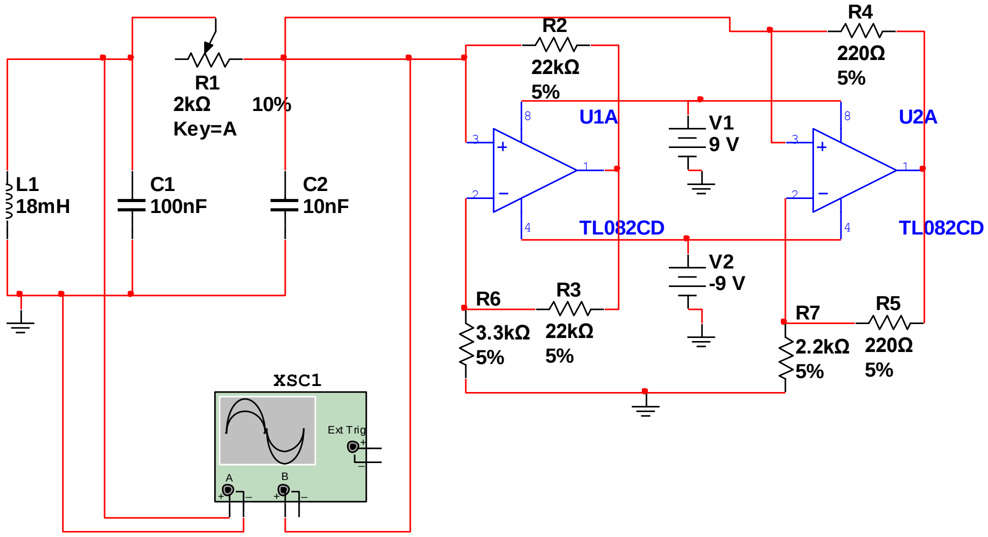

Figure 1: The schematic of the Chua's circuit.

The realization of the circuit is presented in fig. 1. We have used two TL082CD operational amplifier, for realization the nonlinear resistor which is the key factor for the circuit to behave in a chaotic order.

III. The Problem Of Synchronization

The synchronization of a master slave chaotic scheme could be achieved connection the capacitor C_1 of the master circuit with the capacitor C_2 of the slave circuit [11]. The realization of this synchronization technique is presented at fig. 2.

In fig. 2 from the right hand side is presented the master circuit (transmitter), the circuit is operating in a chaotic behavior giving a double scrolled attractor as it can be seen in (fig. 3). The receiver which is presented in the left hand side, it is identical with the transmitter ones.

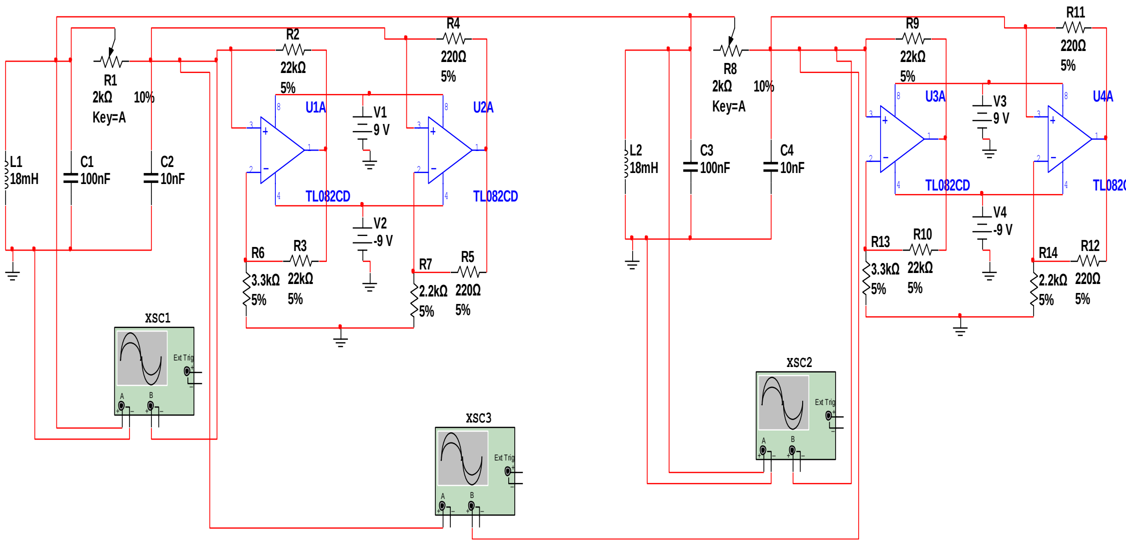

Figure 2. The synchronization of two couple chaotic oschilators.

There we have a pair of the Chua's circuit presented in fig. 1. We have connected the capacitors with a resistance free line. As it is expected form theory and verified from the simulation (fig. 3) we can achieve a perfect synchronization. Here the $v_2(t)$ at the transmitter is identical with $v_2^*(t)$ at the receiver. As a result in the scope we see a y=x line. In fig. 3 the attractor presented in the right figure is presenting the double scroll attractor of the receiver.

Increasing the resistance of the line at 3.5KΩ we can see a partial synchronization. According to our simulation at the begging we can notice a partial synchronization. This could be explained from the difference between the transmitted signal and the received one. After a couple of second we receive a perfect synchronization which could last for a long time. In fig. 4 at the right hand side is presented the $v_2(t)$ at the transmitter versus the $v_2^*(t)$ at the receiver and at the left hide side is presented the chaotic attractor.

Comparing the chaotic attractors generated at this deferent condition we do not notice any deference in the characteristics of the chaotic attractor. In figures bellow the results from the simulation are presented. We have changed the resistance from zero ohm to 3.5kΩ, and finally to 10kΩ.

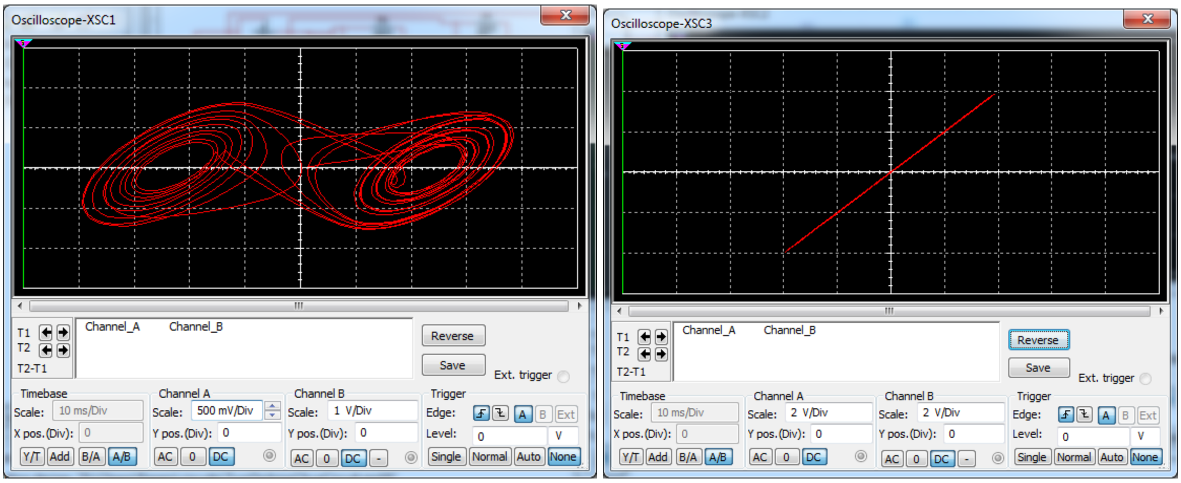

Figure 3. There is no resistance which between the connecting line of master and slave (transmitter - receiver). Form the left is the attractor and from the right the scope in XY mode were in X represent the voltage of C1 and C2 the voltage over C2.

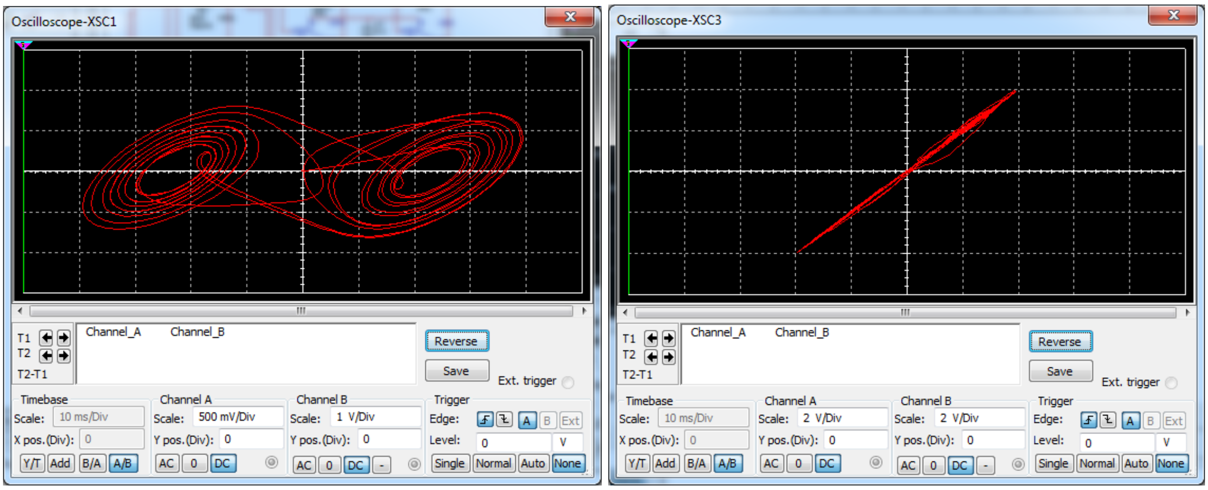

Figure 4. The resistance which connect the master-slave oscillator is R=3.5 kΩ. As it can been seen there is synchronization.

IV. Conclusion

In this paper we have presented an implementation of synchronization of Chua's chaotic circuit. The motivation for synchronization of a chaotic circuit is from the fact that this circuit could be used for encryption. Chaotic circuits and their digital models, respectively, can be included in any sort of cryptosystems [12]. We have used the Multisim, an electronic circuit simulation software, well known for its close to real results.

After simulating a master – slave coupled chaotic transition scheme we figured out that increasing the resistance of the synchronization line more than 3.5kΩ we are not able to have a synchronized system. This could reduce the distance between the transmitter and receiver, since the larger the distance the bigger the resistance. In the design of a chaotic encryption scheme this problem could be solved with the use of amplifications through the line.

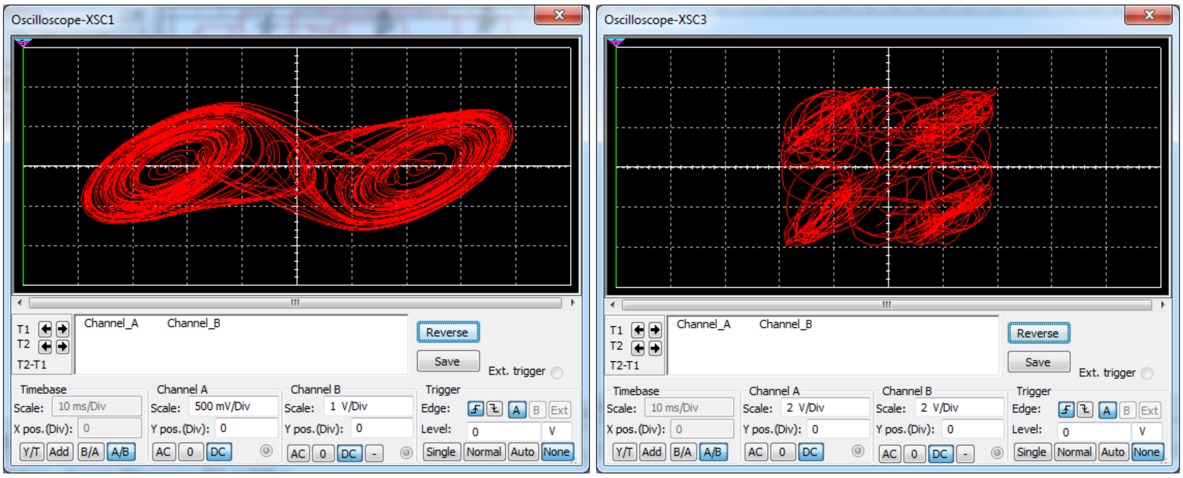

Figure 5. The resistance which connect the master-slave oscillator is R=10kΩ. As it can been seen there is no synchronization.

Acknowledgements

I gratefully acknowledge the support and generosity of Polytechnic University of Tirana and especially the rector of UPT Jorgaq Kacani for their support and contribution all, without which the present study could not have been completed.

References

[1]. L. Chua, The genesis of Chua's circuit, vol. 46. 1992, pp. 250–257.
[2]. M. P. Hanias, Z. Avgerinos, and G. S. Tombras, "Period doubling, Feigenbaum constant and time series prediction in an experimental chaotic RLD circuit," Chaos, Solitons & Fractals, vol. 40, no. 3, pp. 1050–1059, May 2009.
[3]. M. P. Hanias and G. S. Tombras, "Time series analysis in a single transistor chaotic circuit," Chaos, Solitons & Fractals, vol. 40, no. 1, pp. 246–256, Apr. 2009.
[4]. M. P. Hanias, I. L. Giannis, and G. S. Tombras, "Chaotic operation by a single transistor circuit in the reverse active region.," Chaos, vol. 20, no. 1, p. 013105, Mar. 2010.
[5]. J. Jani and P. Malkaj, "Simulation and implementation fo the Chua's chaotic oscilator," in Conference International Conference Research and Education In Natural Sciences, 2013, pp. 164–168.
[6]. R. Hegger, H. Kantz, and T. Schreiber, "Practical implementation of nonlinear time series methods: The TISEAN package.," Chaos, vol. 9, no. 2, pp. 413–435, Jun. 1999.
[7]. B. Aimone and S. Larson, "Chaotic Circuits and Encryption," Neurophysics Lab, 2006.
[8]. T. Matsumoto, L. Chua, and S. Tanaka, "Simplest chaotic nonautonomous circuit," Phys. Rev. A, 1984.
[9]. M. Kennedy, "Three steps to chaos. II. A Chua's circuit primer," Circuits Syst. I Fundam. Theory …, vol. 40, no. 9211603, 1993.
[10]. M. Kennedy, "Three steps to chaos. I. Evolution," Circuits Syst. I Fundam. Theory …, 1993.
[11]. L. Pecora and T. Carroll, "Synchronization in chaotic systems," Phys. Rev. Lett., vol. 64, pp. 821–824, 1990.
[12]. L. Kocarev and S. Lian, Eds., Chaos-Based Cryptography, vol. 354. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011.