Signal Encryption Using Chua's Chaotic Circuits

Ovidiu Vasilovici, Stefan A. Irimiciuc, and Dan G. Dimitriu*
[1] *Faculty of Physics, "Alexandru Ioan Cuza" University of Iasi, 11 Carol I Blvd., RO-700506 Iasi, Romania*

***Abstract* — Experimental results are presented on the building and testing of an encryption system for secure communications based on chaotic Chua's circuits. These results prove that the proposed encryption system works very well, the decrypted signals being very similar with the original ones.**

***Keywords* — chaos, Chua's circuit, encryption, secure communication**

I. Introduction

Chua's circuit represents the cornerstone of the nonlinear circuit theory [1]. This type of circuit was developed by Leon Ong Chua in 1983 [2, 3]. The fact that an electronic device could manifest a chaotic behavior which is dictated by a preexistent nonlinear system of equations solved two fundamental problems. The first one was the proving that the Lorenz attractor or any other chaotic attractor which can be obtained by numerical simulations is in fact chaotic in a strict mathematical sense. The second problem was to develop a device which can be described by a system of non-linear equations, achieving that chaos is a physical phenomenon not a "hoax" produced by the errors from a numerical simulation.

One of the most important applications of the Chua's circuits is the chaotic encryption of the signals in order to ensure a secured communication [4,5]. In this case, the signal from a chaotic Chua's circuit is used as a carrier for the actual information. The encrypted signal is decoded with the help of a second Chua's circuit, which has to be synchronized with the first one.

Here we report on preliminary experimental results related with our attempt to create an encryption system based on chaotic Chua's circuits. Our system was first tested with simple classical signals, like sine-type or square-type signals. Further, the encryption system was used for more complex signals, like conversation or music. The obtained results prove that our encryption system works very well, the decrypted signal being very similar with the original one.

II. SC-CNN Type Chaotic Circuits

One of the most important characteristics of Chua's circuit is its simplicity. It contains minimum five elements, of which four are linear: a coil, a resistor and two capacitors. The fifth element is the most important one, because it is responsible for the non-linear behavior of the circuit [4]. This element is called Chua diode and it is characterized by an *I-V* characteristic which has a negative slope at least in one domain. *I-V* characteristics are described by:

$$g\left(v\right)=\begin{cases} m_1 v + m_1 - m_0\,, & for\ v \le 1 \\ m_0 v\,, & for -1 \le v \le 1\,, \\ m_1 v + m_0 - m_1\,, & for\ v \ge 1 \end{cases} \tag{1}$$

where the coordinates of the symmetry breaking points have been normalized to $v = \pm 1$, m_0 and m_1 being two constant values which describe the negative differential resistance.

Developing such a circuit has one major setback. Because we are dealing with chaotic systems, the initial conditions have a big influence on the results. If we want to make the experiment easy to be reproduced we have to make sure that the initial condition of our system can be reproduced. In this case we have to find a new design for the chaotic circuit which will be more complicated but will use simpler circuit elements. The point is to have a chaotic circuit without a coil (developing a coil at some pre-established values can be difficult under laboratory conditions). One can develop a circuit still having all the characteristics and the design of a classical Chua circuit but the coil is replaced by an equivalent circuit.

State Controlled – Cellular Neural Network (SC-CNN) circuits are based on the Chua's chaotic circuit but are not using coils. Actually they are based on the mathematical system of equations used to describe a classical Chua circuit. That being said, this type of circuit is a cell based circuit. Every cell respects one equation corresponding to one dimension of the system.

As it is shown in Fig. 1, the nonlinear part of this type of circuit is still provided by an operational amplifier. In all the applications of Chua's circuit this type of circuit which has only resistors, capacitors and some operational amplifiers are used. The most important characteristic of SC-CNN circuits

Manuscript received October 28, 2013.
*Corresponding author (*dimitriu@uaic.ro*)

is that they behave exactly as a classical Chua circuit.

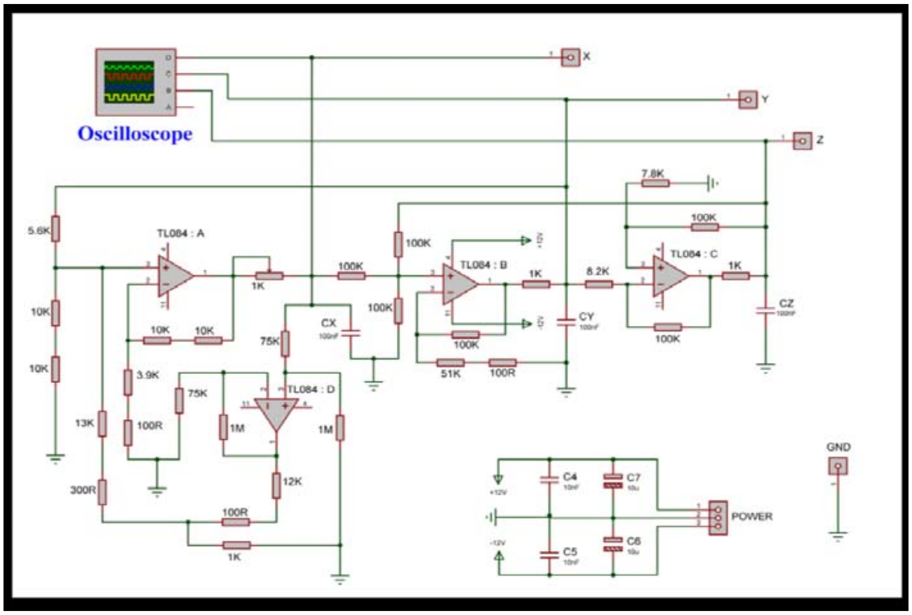

Fig. 1. Typical electronic scheme for a cell based SC-CNN chaotic circuit.

So, we used such type of circuits for our investigation.

III. Signal Encryption

The scheme used by us for the encryption, transmission and decryption of the signals is shown in Fig. 2. It contains two SC-CNN circuits which are synchronized as described in [6]. The synchronization is made by closing the switch K_1. The signal which we want to be securely transmitted (S in Fig. 2) is mixed with the chaotic signal from the master SC-CNN circuit and transmitted to the slave SC-CNN circuit by closing the switch K_2. Here, the useful signal (S' in Fig. 2) is extracted from the encrypted signal.

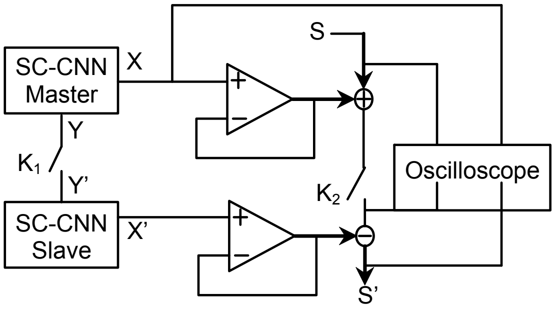

Fig. 2. Secure transmission scheme with two SC-CNN chaotic circuits.

For testing the encryption scheme, we first used simple common signals, like sine and square signals. The obtained results are shown in Fig. 3: the original signal, the chaotic signal used for encryption, the encrypted signal and the decrypted signal, respectively. One can observe that, excepting some noise, the original and the decrypted signals are very similar. Further, we used the encryption system for the secured transmission of more complex signals: conversation and music. The obtained results are shown in Fig. 4, demonstrating the functionality of the system.

Now, we have shown that this specific encryption scheme can be used with great success, but however we have to take into account that it has some limitations. The first limitation is given by the quality of the synchronization. If the two chaotic circuits are poorly synchronized, the decrypted signal will be affected by noise, and consequently the quality of the decrypted signal will suffer. Another limitation is due to the ratio between the original signal and chaotic signal. If this ratio is higher than 30%, again the quality of the decrypted signal will be poor.

IV. Conclusions

The Chua's circuits and also the equivalent SC-CNN circuits are used for secured communications. In this particular application, the signal from chaotic circuits is used as a carrier for the actual information. The two chaotic circuits must be previously synchronized.

Very good results were obtained by using both simple (sine and square) and complex (conversation and music) signals.

The limitations of the proposed encryption scheme were discussed.

References

[1] A. Adamatzky and G. Chen (Eds.), *Chaos, CNN, Memristors and Beyond – A Festschrift for Leon Chua*, Singapore: World Scientific, 2013.

[2] T. Matsumoto, L. O. Chua and S. Tanaka, “Simplest chaotic nonautonomous circuit”, *Phys. Rev. A*, 30, 1984, pp. 1155-1157, DOI: 10.1103/PhysRevA.30.1155.

[3] L. O. Chua, “The genesis of Chua's circuit”, *Archiv für Elektronik und Übertragungstechnik*, 46, 1992, pp. 250-257.

[4] L. Fortuna, M. Frasca and M. G. Xibilia, *Chua's Circuit Implementations – Yesterday, Today and Tomorrow*, Singapore: World Scientific, 2009.

[5] S. Banerjee (Ed.), *Chaos Synchronization and Cryptography for Secure Communications – Applications for Encryption*, Hershey: IGI Global, 2010.

[6] S. A. Irimiciuc, O. Vasilovici and D. G. Dimitriu, "Synchronization of two chaotic systems", *Rev. St. "V. Adamachi"*, to be published.

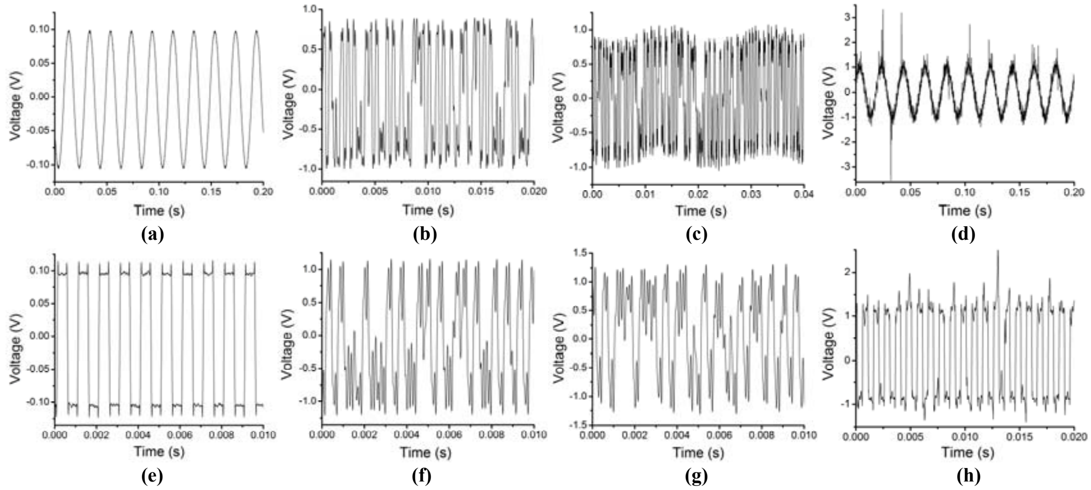

Fig. 3. Encryption and decryption of sine (a) and square (e) signals, respectively (chaotic signals used for encryption (b and f), encrypted (and also transmitted) signals (c and g), decrypted signals (d and h)).

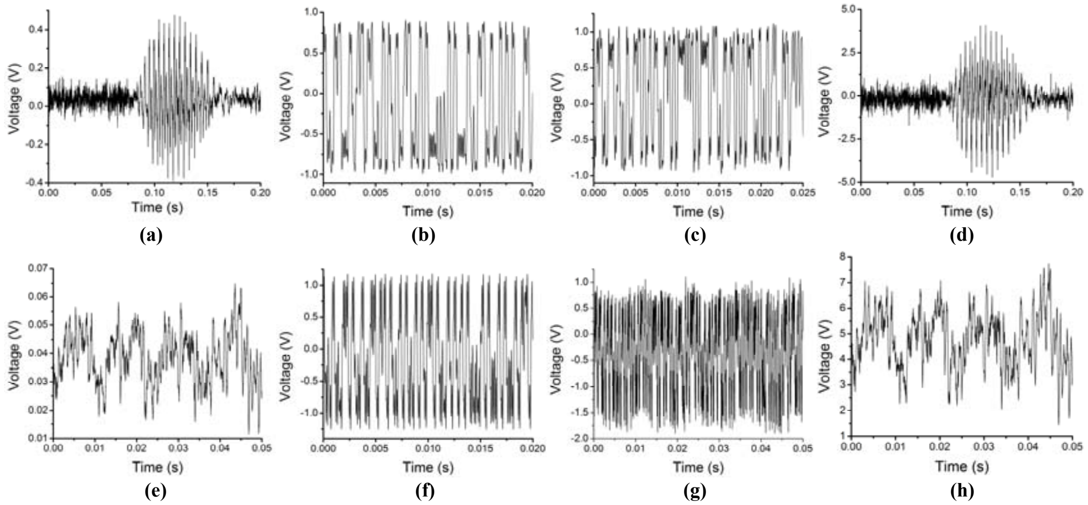

Fig. 4. Encryption and decryption of complex signals, namely conversation (a) and music (e), respectively (chaotic signals used for encryption (b and f), encrypted (and also transmitted) signals (c and g), decrypted signals (d and h)).