Chaotic Modeling and Simulation (CMSIM) 1: 199-208, 2013

A Steganography Telecom System using a Chua Circuit Chaotic Noise Generator for data cryptography

Apostolos P. Leros (1,2) and Antonios S. Andreatos (2)

(1) Department of Automation, School of Technological Applications
Technological Educational Institute of Chalkis, 34400 Psachna, Evia, Greece
E-mail: lerosapostolos@gmail.com

(2) Div. of Computer Engineering & Information Science
Hellenic Air Force Academy, Dekeleia Air Force Base
Dekeleia, Attica, TGA-1010, Greece
E-mail: informatics.hafa@haf.gr, aandreatos@gmail.com

Abstract: This paper models an image steganography telecom system based on a Chua circuit chaotic noise generator. An unpredictable chaotic system based on a Master – Slave Chua circuit has been used as a random number generator. The whole system is modeled and simulated in Simulink. A continuous linear controller has been used to synchronize the two Chua circuits, with the same parameters at both the transmitter and the receiver. On the receiver side, usage of the same parameters with the Master circuit produce a similar chaotic signal via the Slave Chua circuit, synchronized to the Master by an analog controller, in order to produce the same noise (random sequence) as that of the Master circuit. After removing the noise from the received ciphertext, the original message is revealed. The proposed system presents advanced security features.
Keywords: Chua circuit, chaotic noise generator, image steganography, Master Chua circuit, Slave Chua circuit, LSB steganography, simulation, continuous linear controller.

1. Introduction

1.1 Random Number Generators

Traditionally, cryptography has been based on the generation of random numbers produced by hardware (true) random or pseudo-Random Number Generators (RNGs). Most pseudo-RNGs (PRNGs) are not suitable for cryptography for several reasons. First, while most pseudo-RNGs outputs appear random to assorted statistical tests, they do not resist determined reverse engineering. Specialized statistical tests that show the random numbers not to be truly random exist. Second, when the state of most PRNGs has been revealed, all past random numbers can be retrodicted, allowing an attacker to read not only future messages, but also, all past ones. This is not possible with a chaotic number generator; thus, Chua circuits resist this type of cryptanalysis. Furthermore, in our approach, even if the configuration circuit is revealed, it is still difficult to reproduce the crypto- signal since this also depends on the initial

Received: 11 March 2012 / Accepted: 8 October 2012
© 2013 CMSIM
ISSN 2241-0503

conditions and the tolerance of the components. The role of the continuous linear controller is to compensate for the component tolerance.

1.2 Steganography

Steganography is a technique for concealing data within pure or often encrypted or even random/ chaotic data. The data to be concealed is first encrypted and then used to overwrite part of a much larger block of encrypted data or random data or different kinds of (usually redundant) data such as images [10, 15, 16].

2. System Overview

In the proposed steganography telecom application, the message to be transmitted is first encrypted using chaotic noise produced by a standard Chua circuit [2, 4]; then, the encrypted sequence is concealed in an image using the LSB's method (Figure 1).

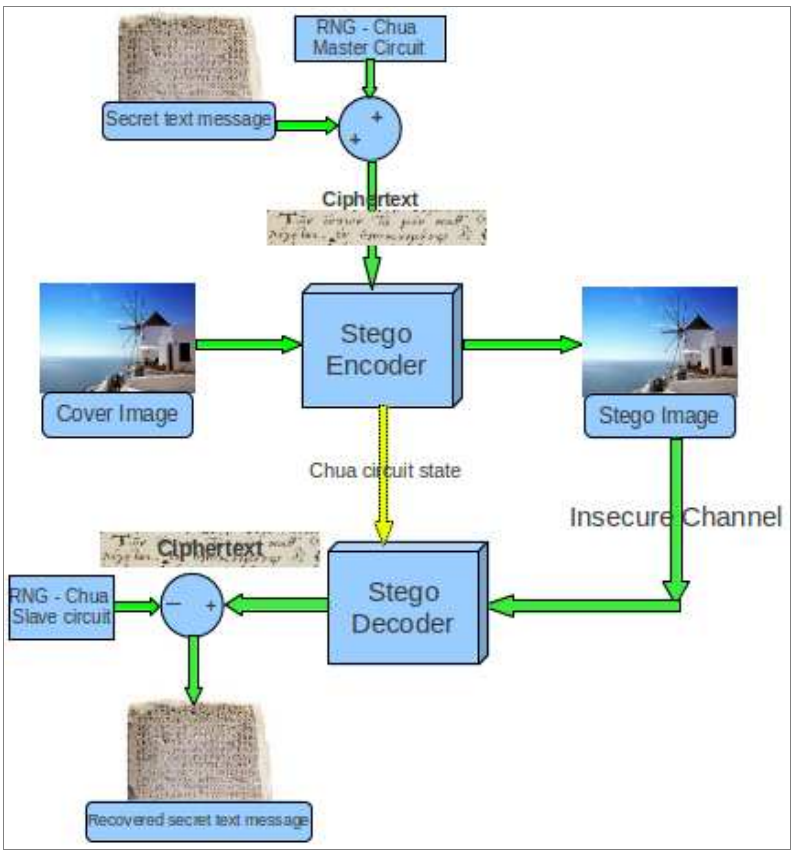

Fig. 1. Proposed steganography telecom application

The input message is in ASCII format; in order to be mixed with the chaotic

noise, it is successively converted from ASCII characters to a binary string. For the sake of simplicity, conversions are not shown in Fig. 1. In the receiver the reverse process takes place, in order to remove the secret text from the image.

3. The Chaotic True Random Number Generator

The Chaotic True Random Number Generator (CTRNG) used by our circuit is based on the Standard Chua's circuit; the latter was invented back in 1983 by Prof. Leon O. Chua in Japan, in his effort to demonstrate chaos in an actual physical model and to prove that the Lorenz double-scroll attractor is chaotic [2, 4]. The electronic circuit suits the study of chaos well because one can precisely control its parameters and observe the results on an oscilloscope. The circuit became popular because it is easy to construct, and many people have built the circuit using off-the-shelf electronic components. In fact, one can model the circuit using only resistors, capacitors, inductors, diodes and op-amps [6].

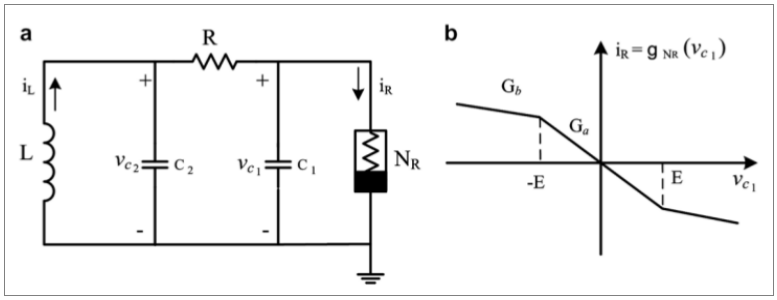

Fig. 2. (a) Standard Chua's circuit; (b) v–i characteristic of the nonlinear device
Source: [4].

In Figure 2 V_{C1} and V_{C2} denote the voltages across the capacitors C_1 and C_2, respectively, i_L is the current through the inductor L, and $gN_R(V_{C1})$ is the nonlinear function which defines the v–i characteristic of the nonlinear device, represented by the piecewise-linear function of Fig. 2b [3]. By solving the above circuit we get the following differential equations (1- 3):

$$C_1 \frac{dV_{C1}}{dt} = \frac{1}{R}(V_{C2} - V_{C1}) - g_{NR}(V_{C1}) \quad (1)$$

$$C_2 \frac{dV_{C2}}{dt} = \frac{1}{R}(V_{C1} - V_{C2}) + i_L \quad (2)$$

$$L \frac{di_L}{dt} = -V_{C2} - R_0 i_L \quad (3)$$

where:

$$g_{NR}(V_{C1}) = G_b V_{C1} + \frac{1}{2}(G_a - G_b)(|V_{C1} + E| - |V_{C1} - E|) \quad (4)$$

4. Simulink implementation

The whole telecom system was successfully implemented in Simulink [8]. In the following an overview of the system will be given; in addition, we shall present the implementation of some critical blocks.

4.1 Simulink implementation of the whole telecom system

The Simulink implementation of the cryptosystem was not as easy; several extra problems had to be solved starting from the input of the carrier image into Simulink; however, all problems were solved and finally the simulation works. The system overview is shown in Figure 3. Next the most important blocks will be briefly presented.

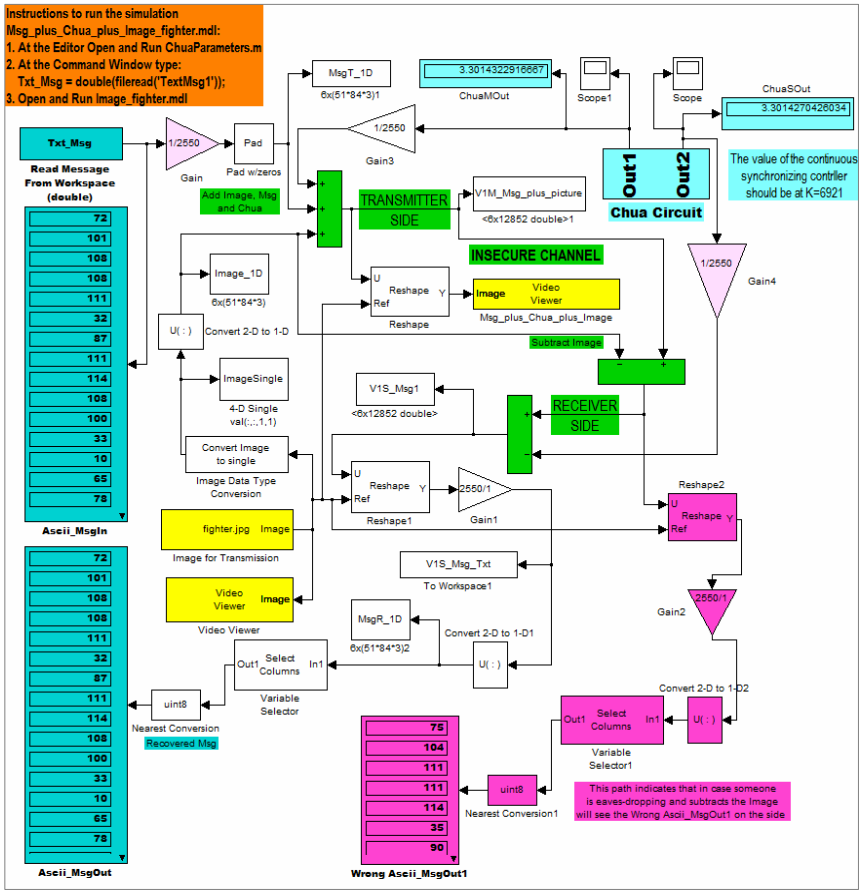

Fig. 3. Stego System overview in Simulink

The message to be encrypted appears on the left side (blue box with the indication Txt_Msg). The cover image for Transmission appears on the left side

in the middle (yellow box named “Image for Transmission”). The Transmitter occupies the top side of the diagram.
The summation element (in green) combines the image, the text message and the Chua chaotic noise, all properly formatted for compatibility. The image with the text message and the Chua chaotic value appears in the yellow box named **Msg_plus_Chua_plus_Image** below the Transmitter Side and it is also inserted into the channel.
The Chua circuits are on the top blue box with the indications Out1 and Out2 for the Master and Slave output values respectively. The value of the continuous linear controller which synchronized the two Chua circuits is **K=6921** as shown in the blue textbox (top right).
The receiver side occupies the bottom side of the diagram. In case an eavesdropper subtracts the image from the received information, he will see an invalid message (bottom right, in magenta).
Finally, at the bottom left side in the blue display with the indication **Ascii_MsgOut** the successfully recovered ASCII message appears.

4.2 Simulink implementation of Chua's circuits Figure 4 presents the Simulink implementation of Chua's circuit, based on the differential equations presented above. The Subsystem (bottom right) represents the nonlinear device.

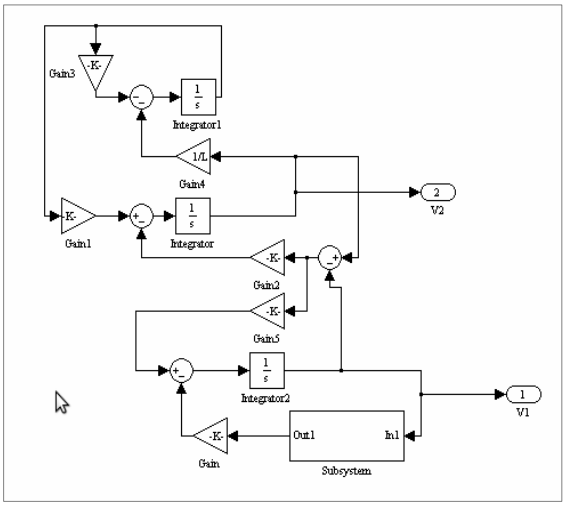

Fig. 4. Simulink implementation of Chua's circuit

4.3 Simulink implementation of the nonlinear device
Figure 5 presents the implementation of the nonlinear device with the v-i characteristic shown in Fig. 2b.

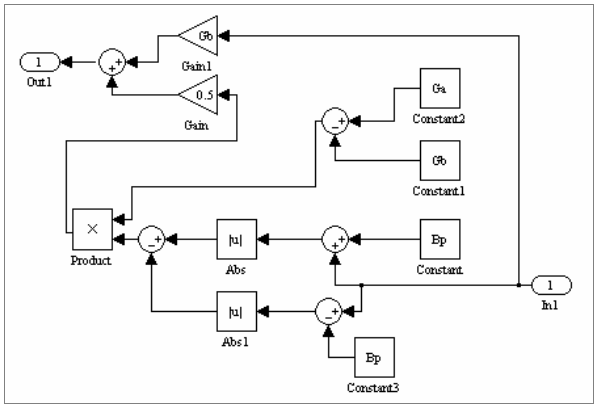

Fig. 5. Simulink implementation of the nonlinear device

5. Synchronization of the Master and Slave Chua circuits

5.1 The need for Master-Slave synchronization

Chaotic systems present an apparently infinite number of states. This characteristic, together with the dependence on the initial conditions as well as the tolerance of the Chua circuit components, make CTRNGs totally unpredictable and non-reproducible, hence ideal for cryptography. However, the receiver must be able to reproduce exactly the same chaotic noise in order to subtract it from the received signal (Figure 1). This becomes possible with synchronization between the two Chua circuits: through the use of specific controllers, we can guide the trajectory of chaotic systems to specific areas producing specific behavior. For this reason, the initial state of the Master Chua circuit [X0, Y0, Z0] has to be transmitted to the Slave Chua circuit via a secure channel (Fig. 6). In our implementation the initial conditions for the Master and Slave Chua circuits are: (Vc1=0, Vc2=1, I_L=0) and (Vc1=0, Vc2=1.1, I_L=0) respectively.

During the last two decades, the chaotic synchronization problem has received a tremendous interest [4]. This property is supposed to have interesting applications in different fields, especially in private and secure communication systems based on cryptography. The broadband and noise-like features of chaotic signals are seen as possibly highly secure media for communication. The cryptographic communication schemes usually consist of a chaotic system as transmitter along with an identical chaotic system as receiver; where the confidential information is embedded into the transmitted chaotic signal by direct modulation, masking, or another technique. At the receiver end, if chaotic synchronization can be achieved, then it is possible to extract the hidden information from the transmitted signal.

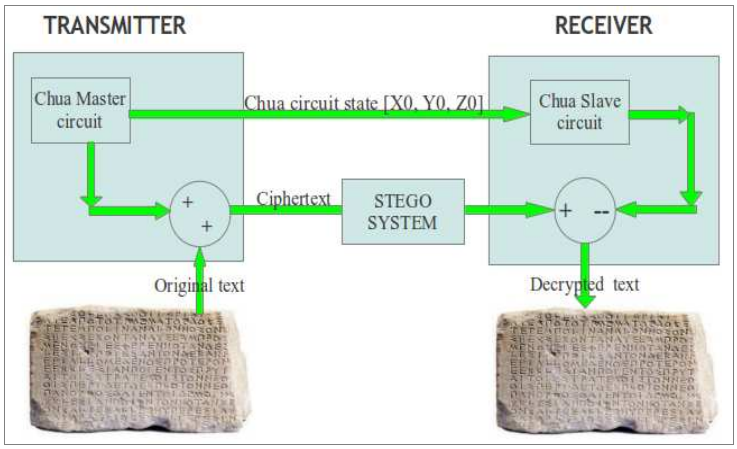

Fig. 6. Synchronization between Master and Slave Chua circuits

5.2 Master-Slave Synchronization circuit

For the synchronization between Master and Slave Chua circuits, Pyragas' continuous control method has been used [1, 3, 5, 7, 9, 11-14]. This method was chosen because it was relatively easy to implement. The synchronization circuit (simplified) is shown in Fig. 7.

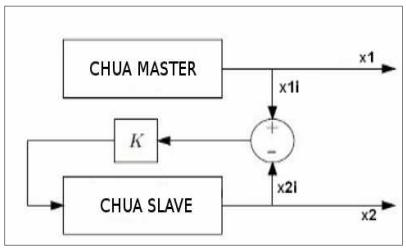

Fig. 7. Master-Slave Synchronization circuit

The Master and Slave Chua's circuits along with the Synchronization device are placed on the top-right side of Figure 4, in a block named Chua circuit. The interior of this block is shown in Figure 8 [6].

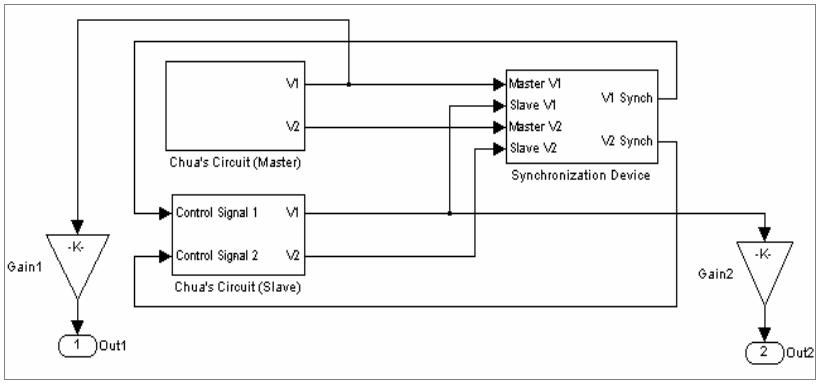

Fig. 8. Chua's circuits along with the synchronization device

6. Simulation results

Initial results show that the system works successfully. Using a small text message and the picture shown in Figure 9 as Cover image, the system produced the stego image of Figure 10.

Fig. 9. Cover image

Figure 10 contains the ciphertext, which is also shown (in ASCII) at the top left column of Figure 3. In this same Figure below we can see the decrypted message at the receiver. An eavesdropper with sufficient information about the image, even connected at a sensitive point of the receiver, won't be able to decode the message correctly, as shown at the bottom of Figure 3.

Fig. 10. Stego image

7. Security features of the proposed stegosystem

The security features of the proposed application are based on:

- ✓ the unknown Chua's circuit topology;
- ✓ the varying tolerance of components (which changes circuit behavior);
- ✓ the unknown initial conditions;
- ✓ the unknown type of the controller / compensator.

8. Conclusion

In this work we have proposed a Steganography Telecom System Based on a Chua Circuit Chaotic Noise Generator with advanced security features. In this system the text message is encrypted using a CTRNG and then the ciphertext is concealed in a cover image using the LSB insertion method. The system has been successfully simulated in Simulink and works with both grayscale and color images.

References

1. S. Boccaletti, C. Grebogi, Y.-C. Lai, H. Mancini, D. Maza, The Control of Chaos Theory and Applications. *Physics Reports*, Elsevier, 2000.
2. Leon O. Chua, Chua's circuit: ten years later. *IEICE Trans. Fundamentals*, vol. E77-A, no. 11, 1811-1822, Nov. 1994.
3. Alexander L. Fradkov and Robin J. Evans, Control of chaos: Methods and applications in engineering, *Annual Reviews in Control*, Elsevier B. V., 2005.
4. L. Gámez-Guzmán, C. Cruz-Hernández, R.M. López-Gutiérrez, E.E. García-Guerrero, Synchronization of Chua's circuits with multi-scroll attractors: Application to

communication, *Commun. Nonlinear Sci. Numer. Simulat.* 14, 2765–2775, 2009.

5. J. Gonzalez, Synchronization and Control of Chaos, *An Introduction for Scientists and Engineers*. Covent Garden, London: Imperial College Press, 2004.
6. Nicholaos N. Grigoropoulos, *Chaotic Systems, Analysis and applications of Chua's circuit*. Diploma Thesis. Supervisor: Prof. A. P. Leros, Technological Institute of Chalkis, School of Technological Applications, 34400 Psachna, Evia, Greece, 2009.
7. T. Kapitaniak, *Controlling Chaos Theoretical and Practical Methods in non-linear Dynamics*. Elsevier Ltd., 1996.
8. Steven T. Karris, *Introduction to Simulink with Engineering Applications*. Orchard Publications, 2006.
9. F. L. Lewis, *Chaos in Automated Control*. Boca Raton, FL: Taylor & Francis Group, 2006.
10. T. Morkel, J.H.P. Eloff and M.S. Olivier, An Overview of Image Steganography, in *Proceedings of the Fifth Annual Information Security South Africa Conference* (ISSA2005), Sandton, South Africa, June/July 2005.
11. Louis M. Pecora, Thomas L. Carroll, Gregg A. Johnson, and Douglas J. Mar, Fundamentals of synchronization in chaotic systems, concepts, and applications. *American Institute of Physics*, 1997.
12. A. Pikovsky, Synchronization, *A universal concept in nonlinear sciences*. New York: Cambridge University Press, 2001.
13. K. Pyragas, Continuous Control of Chaos by Self Controling Feedback. *Physics Letters A*, 1992.
14. E. Schöll, *Handbook of Chaos Control*, 2nd Ed. Weinheim: Verlag GmbH & Co., 2008.
15. Mohit Kr. Srivastava, Sharad Kr. Gupta, Sushil Kushwaha and Brishket S. Tripathi, *Steganalysis of LSB Insertion Method in Uncommpressed Images Using Matlab*. Available online from: http://www.tutorialspoint.com/white-papers/124.pdf
16. Dr Ekta Walia and Payal Jain, An Analysis of LSB & DCT based Steganography, *Global Journal of Computer Science and Technology*, Vol. 10 Issue 1, 4-8, 2010.