Secure Computer Communication Based on Chaotic Rössler Oscillators

J.H. García-López*[,1], R. Jaimes-Reategui[1], R. Chiu-Zarate[1], D. Lopez-Mancilla[1], R. Ramirez-Jimenez[1] and A.N. Pisarchik[2]

[1]*Universidad de Guadalajara, Centro Universitario de los Lagos, Lagos de Moreno, Jalisco, Mexico*

[2]*Centro de Investigaciones en Optica, Leon, Guanajuato, Mexico*

Abstract: We describe a communication scheme based on chaotic Rössler oscillators for transmission of secure messages *via* computers. The computers are synchronized through one of the channels *via* one of the variables of the Rössler system, while an information signal is transmitted through another channel by adding the message to another system variable. This scheme provides more stable communication because the information signal does not enter to the receiver and hence does not cause an error in synchronization. The method is tested with different types of information signals: audio, text, and image.

INTRODUCTION

One of the great achievements of the chaos theory is its application in secure communications. The chaos communication is based on synchronization of chaotic systems under suitable conditions if any one drives the other of the systems. Since Pecora and Carroll [1-3] have demonstrated that chaotic systems can be synchronized, the research in synchronization of couple chaotic circuits is carried out intensively and some interesting applications such as communication with chaos have come out of that research.

Nowadays there exists a great interest in the use of nonlinear differentials equations, such as the Rössler and other oscillators, for application to secure communication [1-15]. The implementation of coupled chaotic systems to secure communication is based on synchronization of the chaotic signals. Chaos is understood as an irregular motion with no defined frequencies and a broaden Fourier transform spectrum. Deterministic chaotic systems have the property of being sensible to initial conditions. Trajectories of a chaotic system starting from very near initial conditions in phase space tend to diverge exponentially. Nevertheless it was demonstrated that certain chaotic systems can be connected such that their chaotic movements are synchronized [11-13].

The phenomenon of synchronization has been discovered in 1665 by Christian Huygens. Now synchronization is understood as an adjustment of the rhythm of oscillators [11]. Synchronization of coupled Rössler oscillators has been studied by Pecora and Carroll who have demonstrated the possibility for synchronous motion in this system [12]. Recently, synchronization of bistable chaotic Rössler oscillators has been demonstrated [16-18].

In this Letter we describe a scheme for secure communication based on two coupled chaotic Rössler oscillators. First, we analyze separately the dynamics of a single oscillator when a control parameter is varied and then we investigate synchronization of the coupled system. Bifurcation diagrams of the output signal with respect to the control parameter are constructed. We demonstrate how secure communication can be realized by using two channels; the system is synchronized *via* one of the channel and an information signal is sent and recovered *via* another channel. We show that such a scheme improves synchronization of the coupled system.

*Address correspondence to this author at the Universidad de Guadalajara, Centro Universitario de los Lagos, Lagos de Moreno, Jalisco, Mexico; E-mail: hugo@culagos.udg.mx

COMPUTATIONAL MODEL

The computational model used is based on a chaotic Rössler oscillator. The master and slave oscillators can be described by the following model equations

$$\frac{dx_1}{dt} = -x_2 - x_3, \quad (1)$$

$$\frac{dx_2}{dt} = x_1 + A_1 x_2, \quad (2)$$

$$\frac{dx_3}{dt} = A_3 + x_3(x_1 - A_2), \quad (3)$$

$$\frac{dx_1'}{dt} = -x_2 - x_3', \quad (4)$$

$$\frac{dx_2'}{dt} = x_1' + A_1 x_2, \quad (5)$$

$$\frac{dx_3'}{dt} = A_3 + x_3'(x_1' - A_2), \quad (6)$$

where x_1, x_2, x_3 and x_1', x_2', x_3' are the state variables of the master and slave oscillator, respectively, $A_1 = = A_3 = 0.2$ are fixed parameters and A_2 is a control parameter varied from 0 to 10. The system (1)-(6) is solved using a 6th order Runge-Kutta algorithm for different values of A_2.

DYNAMICS BEHAVIOR OF SINGLE OSCILLATOR

The dynamic behavior of the master system exhibits complex behavior defined by the control parameter A_2. Fig. (**1**) shows the bifurcation diagram of the peak values of x_1 of

1874-1290/08

the master oscillator. The diagram represents the well-know cascade of period-doubling bifurcations leading to chaos at $A_2 = 4.2$.

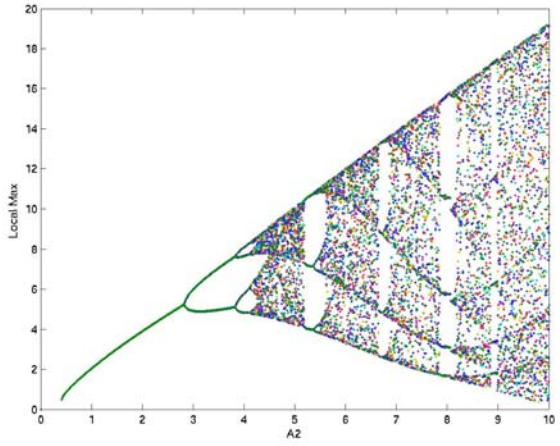

Fig. (1). Bifurcation diagram of master oscillator.

TWO ELECTRONIC CIRCUITS

In this work we apply a novel communication system proposed in [15] for secure computer communications. Master and slave systems are given by the differential equations (1) – (6). The scheme uses two variables x_1 and x_2. x_1 of the master oscillator is used for message transmission and x_1' of the slave oscillator for message recuperation, i.e.

$$x_{1sent} = x_{1master} + S_{Information}, \quad (7)$$

$$S_{Information} = x_{1sent} - x_{1slave}. \quad (8)$$

TWO COUPLED CHAOTIC RÖSSLER OSCILLATORS

Fig. (**2**) shows the time series of the variables x_2 and x_2' of the master and slave oscillators and the phase space plot of x_2 and x_2' where one can see that the chaotic oscillators are completely synchronized.

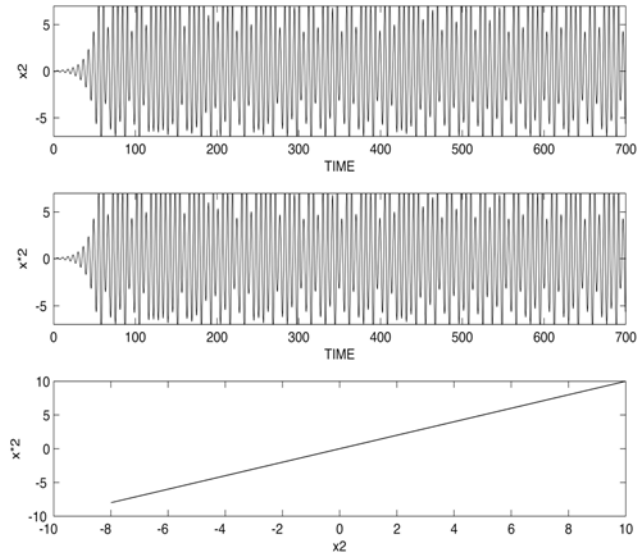

Fig. (2). Chaotic time series of master and slave variables and x_2 versus x_2' demonstrated complete synchronization.

The master and slave oscillators are identical. A small information signal is added to the chaotic signal of the master oscillator. If the oscillators are completely synchronized it becomes possible to recover the message.

When the master and slave systems are completely synchronized, every variable of the slave system follows completely the same trajectory as the corresponding variable of the master system.

SECURE COMMUNICATION WITH A CHAOTIC SYSTEM

In Fig. (**3**) we show a schematic diagram of the message encoding system.

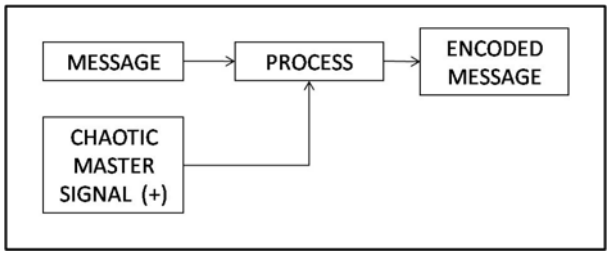

Fig. (3). Diagram of the message encoding process.

The codification process begins from transformation of a message to decimal numbers and then to binary numbers. After this conversion the message is a set of zeros and ones (Fig. **4**). Then this signal of information is added to the chaotic signal of one of the variables of the master system.

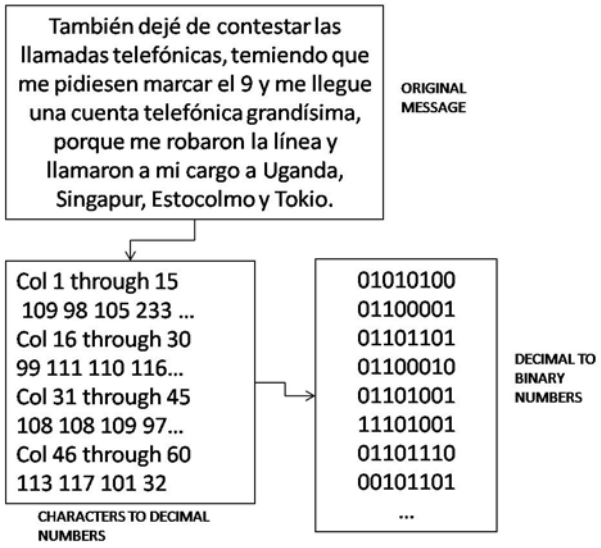

Fig. (4). The message first is encoded to the decimal numbers and then to the binary numbers.

Fig. (**5**) illustrates the information encoding process.

MESSAGE RECOVERING

Fig. (**6**) shows the decoding process. The information signal is the rest of the transmitted signal over variable x_1' of the slave system (8). The procedure shown in Table **1** allows us to obtain the message in the form of binary numbers. These numbers are reordered to the rows of 8 bits, that are equivalent to ASCII characters, and thus the computer interprets each row and sends it to a screen in the form of charac-

ters which can form an electronic mail and can be sent to other computers.

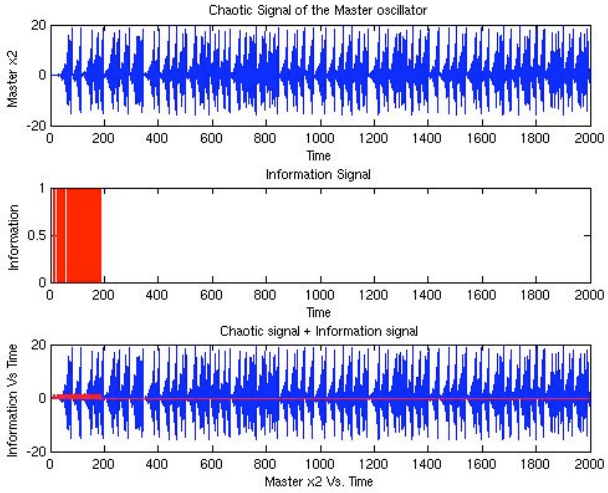

Fig. (5). Chaotic signal of the master oscillator, signal to transmit, and the transmitted signal with information.

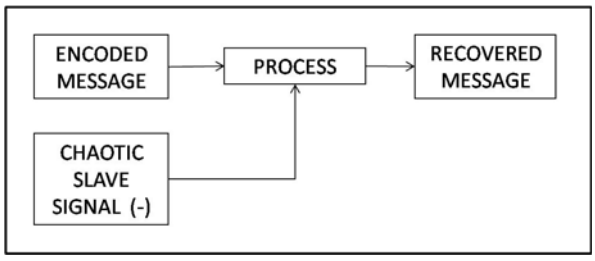

Fig. (6). Diagram of decoding process.

Table 1. Recovered and Reordered Data to form ASCII Code

RECOVERED SIGNAL INFORMATION	VECTOR WHOLE PART	MATRIX ASCII CODE
0.0004	0	01101110
1.0010	1	00101000
1.0015	1	01111001
0.0020	0	00100000
1.0025	1	01001011
1.0030	1	01101110
1.0033	1	00101000
0.0038	0	01111001
0.0041	0	00100000
0.0044	0	01001011
1.0049	1	01111001
0.0049	0	00100000
1.5008	1	01001011
…	…	…

First, we form a vector with three layers in the RGB format which contains the image colors. After that we obtain the encode Image (image + chaotic signal of the master oscillator) and recover the image. The process consists of the subtraction between the encode image and the slave chaotic signal. Then, the layers are separated through the conversion of Double type to Uint8. The last step is to join the three layers in order to form the color image shown in Fig. (**7**).

Fig. (7). Original, encoded, and recovered images.

CONCLUSIONS

In this work we propose the efficient computer communication scheme for secure communications based on synchronization of chaotic Rössler oscillators. The scheme implies the use of two system variables, the one serves for chaos synchronization and the other is used for signal transmission and message recovering. The main advantage of this scheme over the traditional ones is its high stability and very low synchronization error, which can be as small as the noise level.

ACKNOWLEDGMENTS

The authors acknowledge the support from CONACYT project No. 46973-E and from PROMEP-SEP, Mexico.

REFERENCES

[1] L. M. Pecora and T. L. Carroll, “Synchronization in chaotic systems”, *Phys. Rev. Lett*., vol. 64, pp.821-4, 1990.

[2] T. L. Carroll and L. M. Pecora, “Synchronizing chaotic circuits,” *IEEE Trans. Circuits Syst*., vol. 38, pp. 453- 6, April 1991.

[3] T L. M. Pecora and L. Carroll, “A circuit for studying the synchronization of chaotic systems”, *Int. J. Bifurcations Chaos*, vol. 2 (3), pp. 659-67, 1992.

[4] L. O. Chua, L. Kocarev, K. Eckart, and M. Itoh, “Experimental chaos. synchronization in Chua’s circuit,” *Int J. Bifurcations Chaos*, vol. 2 (9), pp. 705-8, 1992.

[5] K. M. Cuomo and A. V. Oppenheim, “Circuit implementation of. synchronized chaos with applications to communications”, *Phys. Rev. Lett*., vol. 71, pp. 65-8, 1993.

[6] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, “Synchronization of Lorenz-based chaotic circuits, with applications to communications”, *IEEE Trans. Circuits Syst. II*, vol. 40 (10), pp. 626-33, 1993.

[7] N. J. Corron and D. W. Hahs, “A new approach to communications using. chaotic signals”, *IEEE Trans. Circuits Syst. I*, vol. 44 (5), pp. 373-82, 1997.

[8] U. Feldmann, M. Hasler, and W. Schwartz, “Communica-. tion by chaotic signals: the inverse system approach”, *Int. J. Circuit Th. Appl*., vol. 24, pp. 551-79, 1996.

[9] C. W. Wu and L. O. Chua, “A simple way to synchronize chaotic systems with applications to secure communication systems”, Int. *J. Bifurcation and Chaos*, vol. 3 (6), pp. 1619-27, 1993.

[10] R. C. Hilborn and N. B. Tufillaro (Eds.), “Chaos and Nonlinear Dynamics”, *American Association of Physics Teachers*, College Park, Maryland, 1999.

[11] J. Kurths, A. Pikovsky, and M. Rosenblum, “Synchronization: A Universal Concept in Nonlinear Sciences”, *Cambridge University Press*, New York, 2001.

[12] T. L. Carroll and L. M. Pecora, “Nonlinear Dynamics in Circuits”, *World Scientific Publishing*, Singapore, 1995.

[13] R. Jaimes-Reátegui, J. H. García-López, A. N. Pisarchik, *et al*. "Experimental demonstration of audio secure communication with Rössler chaotic circuits", *Proc. SPIE*, vol. 6046, p. 60461N, 2006.

[14] A. N. Pisarchik, R. Jaimes-Reátegui, "Homoclinic orbits in a piecewise linear Rössler circuit", *Journal of Physics: Conference Series*, vol. 23, pp. 122-7, 2005.

[15] J. H. García-López, R. Jaimes-Reátegui, A. N. Pisarchik, C. Medina-Gutiérrez, J. C. Jiménez-Godinez, A. U. Murguía-Hernandez, and R. Valdivia, "Novel communication scheme based on chaotic Rössler circuits", *Journal of Physics: Conference Series*, vol. 23, pp. 176-84, 2005.

[16] A. N. Pisarchik, R. Jaimes-Reátegui, J. R. Villalobos-Salazar, J. H. Garcia-Lopez, and S. Boccaletti, "Synchronization of chaotic systems with coexisting attractors", *Phys. Rev. Lett.*, vol. 96, p. 244102, 2006.

[17] A. N. Pisarchik, R. Jaimes-Reátegui, and J. H. García-Lopez, "Synchronization of coupled bistable chaotic systems: Experimental study", *Phil. Trans. Roy. Soc., Ser. A*, vol. 366, pp. 459-473, 2008.

[18] A. N. Pisarchik, R. Jaimes-Reátegui, and J. H. García-Lopez, "Synchronization of multistable systems", *Int. Journal Bif. Chaos* (to be published in June 2008).

Received: December 05, 2007 Revised: February 02, 2008 Accepted: March 07, 2008