RIIT Vol.X. No.1. 2009 21-27, ISSN1405-7743 FI-UNAM
(artículo arbitrado)

Estudios e Investigaciones Recientes

Secure Communication System Using Chaotic Signals

Sistema de comunicación seguro usando señales caóticas

I. Campos-Cantón
Facultad de Ciencias
Universidad Autónoma de San Luis Potosí, México
E-mail: icamposu@galia.fc.aslp.mx

E. Campos-Cantón
Departamento de Físico Matemáticas, CIEP-FI
Universidad Autónoma de San Luis Potosí, México
E-mail: ecamp@uaslp.mx

J.S. Murguía-Ibarra
Departamento de Físico Matemáticas
Universidad Autónoma de San Luis Potosí, México
E-mail: ondeleto@uaslp.mx

M.E. Chavira-Rodríguez
Departamento de Físico Matemáticas
Universidad Autónoma de San Luis Potosí, México
E-mail: mchavira@uaslp.mx

(Recibido: agosto de 2006: aceptado: enero de 2008)

Abstract

We present experimental results of a chaotic communication system that employs direct modulation, with the Chua's chaotic oscillator as a core of the transmitter block. The main result is that its possible to recover the information signal if we modulate over one state of oscillator and transmit a different state, avoiding a correlation between the information signal and the chaotic carrier.

Keywords: *Chaotic communication, chaotic carrier, chaos synchronization, transmitter block, receiver block.*

Resumen

Se presentan resultados experimentales de un sistema de comunicación caótico que emplea modulación directa, con el oscilador caótico de Chua como corazón del bloque transmisor. El principal objetivo es que es posible recuperar la señal de información al modular un estado del oscilador y transmitir un estado diferente, evitando una correlación entre la señal de información y la portadora caótica.

Descriptores: Comunicación caótica, portadora caótica, sincronización de caos, bloque transmisor, bloque receptor.

Introduction

Despite the fact that there exist several conventional communication systems, one main interest is to warrant privacy of the information. In this aspect the chaotic communication systems have been contributed to the secure communication area. Research in the last two decades (Itho *et al.*, 1995; Sushchik *et al*., 2000; Maybhate A. *et al.*, 2003) indicates that chaotic behavior has several characteristics that makes it attractive for use in communication systems as carrier signals. To mention some basic

techniques, we can consider chaotic mask, direct modulation, and binary modulation. a) *Chaotic mask* (Cuomo *et al*., 1993; Kocarev *et al*., 1992), where the information signal is added to the chaotic carrier in the transmitter block, and the receiver block just takes the chaotic carrier away from the receiver signal in order to recover the information signal. b) For *direct modulation* (Halle *et al*., 1993; Urías, 1999; Volkovskii *et al*., 1993), we refer to the action of adding the information signal to the dynamics of the chaotic oscillator in the transmitter block, whereas an inverse operation is carried out on the receiver block to recover the information signal. c) In *binary modulation* (Dedieu *et al*., 1993; Parlitz *et al*., 1992), the information signal is codified by two distinct chaotic systems, and it is recovered by detecting synchronization with similar corresponding systems in the receiver block. One target is to improve or propose new schemes (Dmitriev A.S. *et al*., 2003; Larson *et al.*, 2006) of this kind of communication systems.

However, some problems have been presented when chaotic oscillators are used to modulate information signals. For instance, for a certain range of amplitudes and frequencies of the information signal there exist a high correlation between the chaotic carrier signal and the information signal, as long as destruction of chaotic behavior is presented, respectively. These two problems avoid the main purpose of "masking" information signal using chaos.

In this work, we propose a procedure to avoid correlation between information signal and chaotic carrier signal, and the possibility to recover the information signal. The physical implementation of this communication system is based on Chua's circuit under the same spirit that in (Corron *et al*., 1997).

The structure of this paper is as follows. The section called chaotic communication system describes the general theory of this communication system. The following section contains the physical implementation of such communication system. Finally, the experimental results and conclusions are presented.

Chaotic Communication System

Figure 1 shows the basic functional blocks of our chaotic communication system. The main blocks are the transmitter and the receiver, respectively. It is possible to consider a communication system with the following characteristics:

a) In the transmitter, we modulate one state of the system with the information signal and use a different state as a chaotic carrier. With this, we mask the information signal and avoid correlation between these signals.
b) In the receiver, we reconstruct others states that were not transmitted using a convergence strategy; furthermore, we use a non-lineal filters to reconstruct the information signal.

The components of our chaotic communication system are described below.

The Transmitter

Basically, the transmitter couples the information signal to the communication channel. It is comprised of a chaotic oscillator, which is modulated by the information signal using direct modulation. Considering a third order oscillator, the transmitter has the form

$$\begin{aligned} \dot{x} &= u_0(x,y,z) \quad (t)u_1(x,y,z), \\ \dot{y} &= v(x,y,z), \\ \dot{z} &= w(w,y,z). \end{aligned} \tag{1}$$

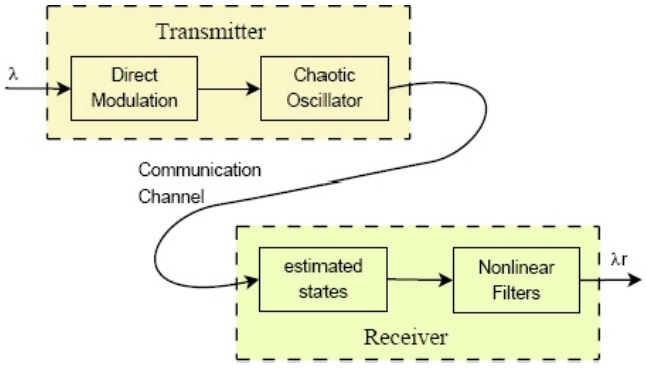

Figure 1. Block diagram of the chaotic communication system using direct modulation

The parameter (*t*) is a prescribed function of time that represents the information to be communicated. The set of equations 1, which represents the transmitter, has to satisfy the following requirements.

1. To make use of one state to modulate and the other one as a carrier. In our case is the state modulated, whereas the *y* state is transmitted.
2. The acceptable values of (*t*) need to satisfy the condition | (*t*)| . The constant is selected such that the oscillator in always operates in a chaotic regime.

In our approach, the carrier is *y*(*t*), in contrast to (Corron *et al*., 1997), where the carrier was *x*(*t*) and the subsystem formed by (*y*,*z*) is independent of the parameter .

The Receiver

It is well known that the main function of the receiver is to extract the information signal from the degraded version of the transmitted signal coming from the channel. From figure 1, the receiver consists of two blocks, where the first one is useful to reconstruct the states that were not transmitted. The way to reconstruct states depends strongly of the chaotic oscillator employed. In the next section is presented the approach to estimate the non-transmitted states using the Chua's oscillator. The original signals *x* and *z* are reconstructed from signal, as long as x_r and z_r by means of chaotic synchronization at the receiving end. The second block is utilized to estimate the information signal. The naive approach to recover (*t*) would be to use the estimation

$$_r \quad \frac{\dot{x}_r \quad u_0(x_r, y, z_r)}{u_1(x_r, y, z_r)}. \tag{2}$$

However, if we use equation (2) to implement the demodulator, singularities are encountered whenever $u_1 \quad (x_r, y, z_r) \quad 0$. In order to avoid this situation we use a low pass filter.

Alternatively to estimate equation (2), we used the uncoupled pair of first order filters

$$\dot{p}_0 \quad u_0(x_r, y, z_r) \quad \frac{(x \quad p_0)}{k}, \tag{3}$$

$$\dot{p}_1 \quad u_1(x_r, y, z_r) \quad \frac{p_1}{k}. \tag{4}$$

In the filters (3)-(4), the constant $k \quad 0$ works as a tuning parameter. Its main functionality is to reduce residues of the carrier in the output of the receiver. Consequently, the information signal is estimated as $\hat{}_r \quad (x \quad p_0)/p_1$, where the parameters p_0 and p_1 are the outputs of the filters (3)-(4). This signal $_r$ is further passed through the low-pass filter

$$\dot{} \quad \hat{} \quad . \tag{5}$$

Summarizing, the receiver block consists of a subsystem to estimate the variable states x_r and z_r, that is driven by the incoming carrier *y*, which was generated by the transmitter and followed by the filters (3)-(5). The demodulated signal is $_f$, and the quantities *k* and $_f$ are tuning parameters of the receiver.

Physical Implementation

The physical implementation of this communication system is based on a chaotic electric circuit that does not involve analog multiplication, and it is a very handy and cheap electric system. It uses only resistors, capacitors, diodes and operational amplifiers as we will see.

The Transmitter

Figure 2 shows the electronic circuit of the transmitter block. It is worth to note that the Chua's oscillator is the core of the transmitter, where the component values employed for its construction are setting to have a chaotic behavior, and the value of potentiometer was fixed at 1.8k . For more information of Chua's circuit see (Chua *et al*., 1992).

The mathematic model of the transmitter block is described by the following set of equations:

$$\dot{V}_1 \quad \frac{(G_m \quad G)}{C_1} V_1 \quad \frac{G}{C_1} V_2 \quad \frac{G_m}{C_1} V_m \quad \frac{1}{C_1} I_x, \tag{6}$$

$$\dot{V}_2 \quad \frac{G}{C_2} V_1 \quad \frac{G}{C_2} V_2 \quad \frac{1}{C_2} I_L, \tag{7}$$

$$\dot{I}_L \quad \frac{1}{L} V_2, \tag{8}$$

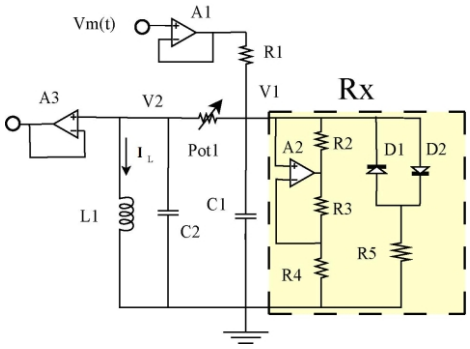

Figure 2. The electronic circuit of the transmitter block. The component values employed are R_1 10k , R_2 R_3 220 , R_4 750 , R_5 1.2 , $Pot1$ 5k , C_1 10nF, C_2 100nF, L_1 18mH. The diodes D_1 and D_2 are 1N914, and the operational amplifiers are TL-082.

where V_1 , V_2 , and I_L are the corresponding states, and , G_m 1/R_1 , G 1/$Potl$, C_1 , C_2 and L are parameters of the system. According to our model (1), x V_1 , y V_2 and z I_L . Here, the direct modulation is applied to the node V_1 , the information signal V_m is injected to the oscillator by the resistor R_1 , and is transmitted the state V_2 . With this will avoid correlation between the information signal V_m and the chaotic carrier V_2 .

The Receiver

In the receiver block, the problem is how we can estimate the non-transmitted states using just one state. As we said, the V_2 state is the chaotic carrier and it is employed to estimate the states V_1 and I_L . To achieve the estimation of the non-transmitted states V_1 and I_L , we use equations $V_1^{'}$ and $I_L^{'}$ to obtain the estimated states and as follow

$$V_1^{'} \quad \frac{C_2}{G}\dot{V}_2 \quad V_2 \quad \frac{1}{G}I_L^{'}, \tag{9}$$

$$I_L^{'} \quad \frac{1}{L} \quad V_2 d \ . \tag{10}$$

Figure 3 shows the estimator block to estimate states $V_1^{'}$ and $I_L^{'}$. This estimator is the realization of equations 9 and 10.

In figure 4 is shown the electrical circuit diagram to implement the estimator block. This subsystem is formed for one integrator, one differentiator and one adder circuits. The values adjusted of the potentiometers were Pot2 = 390 , Pot3 = 4.4 k , Pot4 = 390 , Pot5 = 3.9 k and Pot6 = 3.6 k . These values of the potentiometers were tuning to work properly with the frequency of the chaotic carrier signal.

In order to recover the information signal, we need to use the equation. Therefore, the information signal can be recovered as follows

$$V_m \quad \frac{C_1}{G_m}\dot{V}_1 \quad \frac{(G_m \quad G)}{G_m}V_1 \quad \frac{G}{G_m}V_2 \quad \frac{1}{G_m}I_x . \tag{11}$$

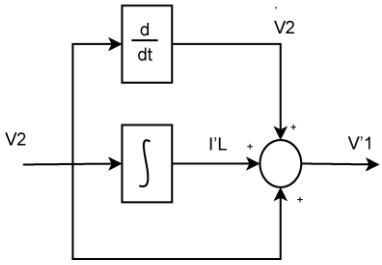

Figure 3. Block diagram of the circuit to estimate the states V_1 and I_L.

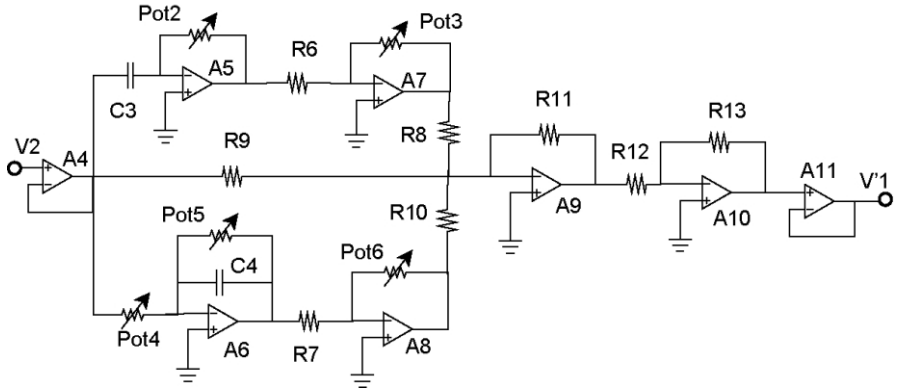

Figure 4. The electronic circuit of the estimator block

This circuit estimates the state V_1' using the state V^2. The component values employed are

R_1 10 k ,
R_6 R_7 1k ,
R_8 R_9 R_{10} R_{11} R_{12} R_{13} 10 ,
$Pot2,3,4,6$ 10 k ,
$Pot5$ 100 k .
C_3 C_4 100 nF and the operational amplifiers are TL-082.

In figure 5 is shown the recover information block. The device labeled as Rx is a negative nonlinear resistive and is shown in the transmitter block, see figure 2. The values of the potentiometers and were adjusted to 1.9 k and 1.71 k , respectively.

The element labeled as Rx is an identical Chua's diode, which is showed in the transmitter circuit (figure 2). The component values employed to implement the non-linear of the receiver block

R_{24} R_{25} R_{26} R_{31} R_{32} 12 k ,
R_{33} R_{34} R_{35} 10 ,
$Pot8,9$ 10 k ,
C_6 C_7 10 nF and the operational amplifiers are TL-082.

Results and Conclusions

Three different signals were considered as information signal V_m, and we use couple wire transmission to transmit all signals. The first information signal was a simple sine function V_m $A\sin t$, with amplitude A $0.5V$ and angular frequency w $2 f (f$ $3 kHz)$. This signal is shown in figure 6 (top signal). Following our approach, in the receiver block we have three states (V_1', V_2', I_L'). Figure 7 shows the projection on the (V_1, V_1') plane, the receiver variable V_1' against its transmitter counterpart V_1. This graph indicates synchronization between these two signals, despite the fact that both circuits are running chaotically. The recovered information signal is shown in figure 6 (bottom signal). The attenuation and delay of the reconstructed signal are introduced by the filters used for its reconstruction.

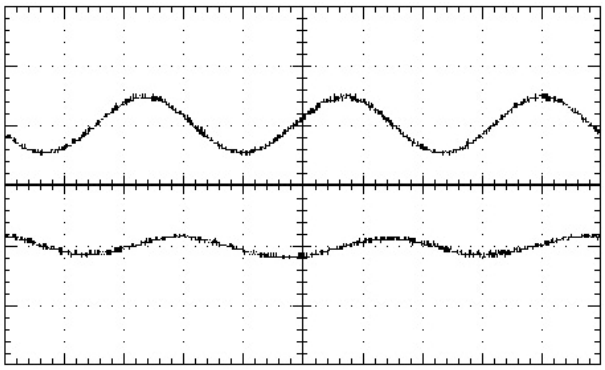

Figure 6. The top signal is the first information signal and the bottom signal is the recovered information signal V_m'

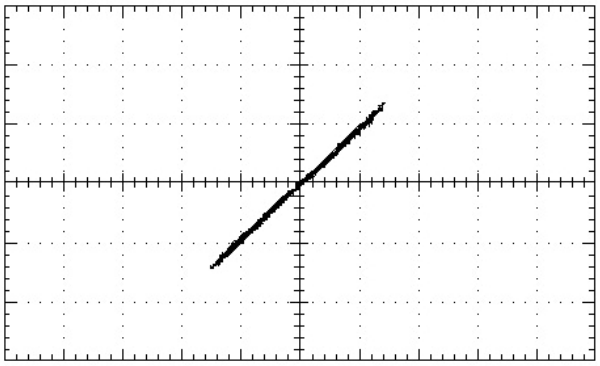

Figure 7. Projection on the (V_1, V_1') plane. The horizontal axis represents the state V_1, whereas the vertical axis represents the state V_1'

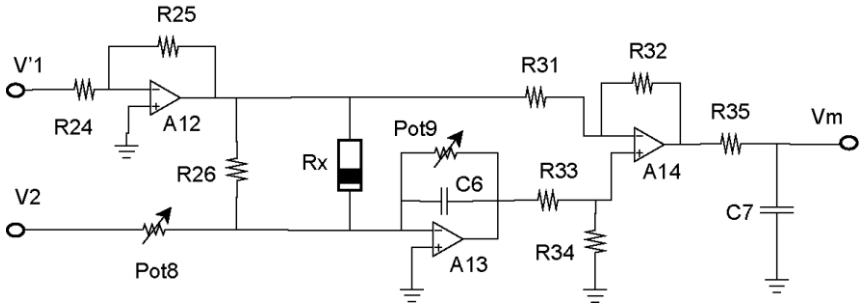

Figure 5. Nonlinear filter to recover the information signal

The results of correlation between the information signal and the chaotic carrier are shown in figure 8. Figure 8 shows the information signal (A), the modulated state V_1 (B), and the chaotic carrier V_2 (C), respectively. We can observe that there is no correlation between the signals of figure 8 (A) and (C), whereas in signals of figure 10 (A) and (B) is evident a correlation.

The second information signal analyzed was a square signal with amplitude equals to 1 Vpp, and a frequency of 100 Hz. The results obtained with this signal are shown in Figure 9; the top signal is V_m, whereas the bottom signal is the recovered information signal V_m'. The smoothening of the transitions in the demodulated signal is introduced by the filters.

Finally, we consider as an information signal V_m a music signal, obtained from the sound card of the PC. Figure 10 shows a segment of this signal (top), and the corresponding demodulated signal (bottom). The music was recovered very well.

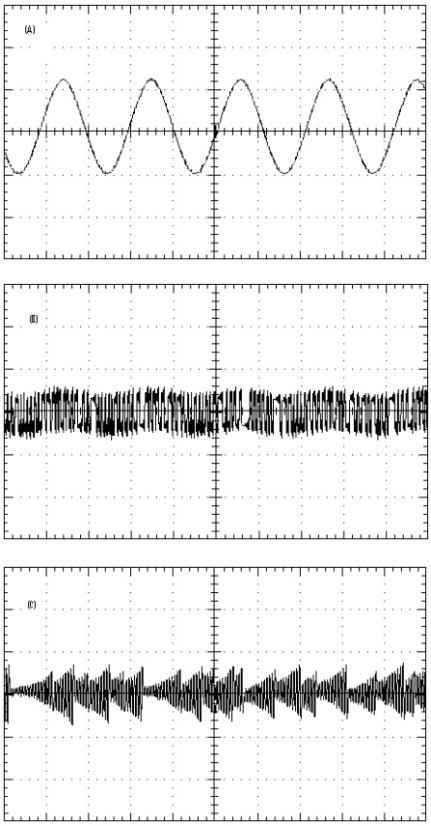

Figure 8. (A) The first information signal V_m $A\sin$ t, where $A=1$ Vpp and $2f(f$ $15Hz)$. (B) The modulated state V_1 state. (C) The chaotic carrier, V_2.

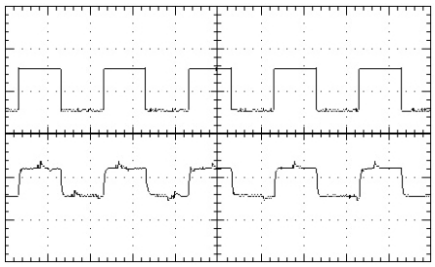

Figure 9. A square signal as an information signal V_m, with amplitude equals to 1 Vpp and a frequency of 100Hz, (top signal), and recovered information signal V_m' (bottom signal).

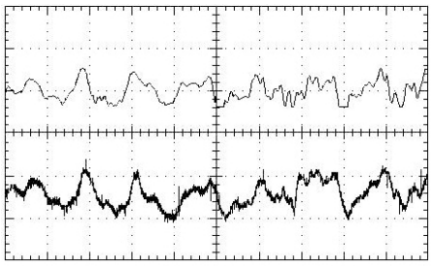

Figure 10. The last information signal V_m (top, music signal), and recovered information signal V_m' (bottom signal).

In conclusion, a method of chaotic communication using direct modulation was proposed here, and a practical experimental implementation of this communication system was realized. We could recover the information signal using this method, where correlation between the information signal and the chaotic carrier was avoided. It is clear that Chua's chaotic oscillator allowed making a practical evaluation of the direct modulation approach to secure communications.

Finally, despite we do not consider the effect of the noise in the experiments, the possibility to consider the noise will be examined in another publication.

Acknowledgments

ECC received financial support from FAI-UASLP under contract C07-FAI-11-38.74, and JSM received financial support from PROMEP and FAI-UASLP.

References

Chua L.O., Kocarev L., Eckert K., Itoh M. Experimental Chaos Synchronization in Chua's Circuit. *Int. J. Bifur. & chaos*, (12):705-708.1992.

Corron N.J., Hahs D.W. A New Approach to Communications Using Chaotic Signals. *IEEE, Trans. Circuits System,* I(44):373-382. 1997.

Cuomo K.M., Oppenheim A.V., Strogatz S.H. Robustness and Signal Recovery in a Synchronized Chaotic System. *Int. J. Bifur. and Chaos*, (3):1629-1638. 1993.

Dedieu H., Kennedy M.P., Hasler M. Chaotic Shift Keying: Modulation and Demodulation of Chaotic Carrier Using Self-Synchronization Chua's Circuit. *IEEE Trans. Circuits Syst.* II(40):634-642.1993.

Dmitriev A.S., Kyarginsky B.Y., Panas A.I., Starkov S.O. Experiments on Ultra Wideband Direct Chaotic Information Transmission in Microwave Band. *Int. J. Bifur. & Chaos*, (13):1495-1507. 2003.

Halle K.S., Wu C.W., Itoh M., Chua L.O. Spread Spectrum Communication Through Modulation of Chaos. *Int. J. of Bifur. and Chaos*, (3):469-477. 1993.

Itho M., Murakami V. New Communication System Via Chaotic Synchronizations and Modulations. *IEICE Trans. Fundament.*, E78A:285-290. 1995.

Larson-Lawrence L.J.M., Tsimring L. *Digital Communications Using Chaos and Nonlinear Dynamics.* Edt. Springer. 2006.

Kocarev V, Halle K.S., Eckert K., Chua L.O., Parlitz V. Experimental Demonstration of Secure Communications Via Chaotic Synchronization. *Int. J. Bifur. and Chaos*, (2):709 713. 1992.

Maybhate A., Amritkar R.E., Kulkarni D.R. Estimation of Initial Conditions and Secure Communication. *Int. J. Bifur. and Chaos*, (13):3079-3084. 2003.

Parlitz V, Chua L.O, Kocarev V, Halle K., Shang A. Transmission of Digital Signals by Chaotic Synchronization. *Int. J. Bifur. and Chaos*, (2):973-977. 1992.

Sushchik M.M., Rulkov N.F., Larsen L., Tsimring L.S., Abarbanel H.D.I., Yan K., Volkovskii A.R. Chaotic Pulse Position Modulation: a Robust Method of Communicating with Chaos. *IEEE Comm. Lett.*, (4):128-130. 2000.

Urías J. Analog Modulation and Demodulation of a Chaotic Oscillator. *Rev. Mex. de Fís.,* (45):331-335. 1999.

Volkovskii A.R., Rulkov N.F. Synchronous Chaotic Response of a Nonlinear Oscillator System as a Principle for the Detection of the Information Component of Chaos. *Tech. Phys. Lett.,* (19):97-99. 1993.

About the authors

Isaac Campos-Cantón. Received the Master's degree in electrical engineering from the School of Engineering, UNAM in 1997, in this moment he is working in his doctorate at IICO, UASLP, his current research is on the electronic circuits with nonlinear behavior and complex networks.*Eric Campos-Cantón*. Es licenciado en electrónica por la Facultad de Ciencias, UASLP, maestro en ingeniería eléctrica por la IICO-Facultad de Ingeniería, UASLP y doctor enciencias aAplicadas por el IICO-Facultad de Ciencias, UASLP.

Eric Campos-Cantón. Received the Master's degree in electrical engineering in 1999 and the Ph. D. degree in Applied Science in 2003 from Universidad Autónoma de San Luis Potosí. Since then, he has been a Professor at the same University. He contributed in the book *Digital Communications using Chaos and Nonlinear Dynamics* (Springer, 2006). His research interests include dynamical systems with nonlinear behavior and its applications to engineering and science.

José Salomé Murguía-Ibarra. Obtained his B.Sc. degree in 1998 in Electronic Engineer with a specialization in Digital Systems from the Autonomous University of San Luis Potosí (AUSLP). He got his M.Sc. degree in Electrical Engineering and his PhD degree in Applied Sciences in the AUSLP, in 1999 and 2003, respectively. Since January 2003, he has been Professor-Researcher of the Physics-Mathematical Department of the AUSLP. He is actually a member of the Researchers National System, and his research interests include signal processing, wavelet analysis and applied mathematics.

Mayra Elizabeth Chavira-Rodríguez. Obtained her Master Engineering degree in 2000, and her Doctorate in Science in 2004 from the Universidad Autónoma de San Luis Potosí. Actually, she works at Departamento Fisico-Matematicas at the Universidad Autónoma de San Luis Potosí; she is a member of Sistema Nacional de Investigadores and her works deal with physics of semiconductors and applications in sciences, including mathematical modeling.