International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:3, No:6, 2009

Encrypter Information Software Using Chaotic Generators

Cardoza-Avendaño L., López-Gutiérrez R.M., Inzunza-González E., Cruz-Hernández C., García-Guerrero E., Spirin V., and Serrano H.

***Abstract*—**This document show a software that show different chaotic generator, as continuous as discrete time. The software give the option for obtain the different signals, using different parameters and initial condition value. The program show then critical parameter for each model. All theses models are capable of encrypter information, this software show it too.

***Keywords*—**cryptography, chaotic attractors, software.

I. Introduction

THE chaos theory describes the behavior of certain dynamical systems that may exhibit dynamics that are highly sensitive to initial conditions, popularly referred to as the butterfly effect. As a result of this sensitivity, the behavior of chaotic systems appears to be random. The future dynamics of these systems are completely defined by their initial conditions. This behavior is known as deterministic chaos, or simply chaos.

Chaotic behavior is also observed in natural systems, such as the weather. This may be explained by a chaos-theoretical analysis of a mathematical model of such a system, embodying the laws of physics that are relevant for the natural system.

The chaotic behavior occurs in many areas of practical engineering, i.e., in communications, the information transmission plays a crucial role, where an ever-growing capacity for communication services is required. Two of the major requirements in communication systems are privacy and security.

The chaotic systems [1]-[9] have been greatly motivated by the possibility of encoding information by using a chaotic carrier.

Hence, we are interesting in software that shows the behavior of different chaotic signal. In this paper we present software for different chaotic attractor, for continuous–time and discrete-time systems.

Cardoza-Avendaño L. is with the Baja California Autonomous University (UABC), Ensenada, B.C. 22860 México; (e-mail: lcardoza@uabc.mx).
R. M. López Gutiérrez is with the Baja California Autonomous University (UABC), Ensenada, B.C. 22860 México (corresponding author to provide phone: +52 646-175-0744; fax: +52 646-174-4333; (e-mail: roslopez@uabc.mx).
C. Cruz Hernández is with the Electronics and Telecommunications Department, Scientific Research and Advanced Studies of Ensenada (CICESE), Ensenada B.C. 22860 México; (e-mail: ccruz@cicese.mx).
E. Inzunza is with the Baja California Autonomous University (UABC), Ensenada, B.C. 22860 México; (e-mail: einzunza@ uabc.mx).
E. E. García Guerrero is with the Baja California Autonomous University (UABC), Ensenada, B.C. 22860 México ; (e-mail: eegarcia@uabc.mx).
V. Spirin is with Scientific Research and Advanced Studies of Ensenada; (e-mail: vaspir@cicese.mx).
H. Serrano is with the Baja California Autonomous University (UABC), Ensenada, B.C. 22860 México; (e-mail: hazael@uabc.mx).

II. Chaotic signal generation

A. Continuous

Different models exist for chaotic dynamics in continuous time. They use differential equations that exhibits chaotic dynamics associated with the fractal properties of the attractor.

1) Lorenz

Lorenz wrote a remarkable article in 1963, he described a three parameter of the nonlinear first-order ordinary differential equation that, when integrated numerically on a computer, appeared to have extremely complicated solutions.

This set of ordinary differential equations that would model some of the unpredictable behavior that we normally associate with the weather [10]. They are

$$\begin{aligned} \dot{x}_1(t) &= \sigma(x_2(t) - x_1(t)), \\ \dot{x}_2(t) &= r x_1(t) - x_2(t) - x_1(t) x_3(t), \\ \dot{x}_3(t) &= x_1(t) x_2(t) - b x_3(t) \end{aligned} \tag{1}$$

Where σ=10, b=8/3, and r=28.

a) *0<r<1. There is only stable equilibrium point at the origin.*
b) *1<r<1.346. Two new stable nodes are born and the origin becomes a saddle with a one-dimensional, unstable manifold.*
c) *1.346<r<13.926. At the lower value the stable nodes become stable spirals.*
d) *13.926<r<24.74. Unstable limit cycles are born near each of the spiral nodes, and the basins of attraction of each of the two fixed points become intertwined. The steady-steady notion is sensitive to initial conditions.*
e) *24.74<r. All three fixed points becomes unstable. Chaotic motions result.*

2) Chua

The second model is Chua's circuit is a simple electronic circuit that exhibits classic chaos theory behavior. It was introduced in 1983 by Leon O. Chua, who was a visitor at Waseda University in Japan at that time [11]. The ease of construction of the circuit has made it a ubiquitous real-world example of a chaotic system, leading some to declare it "a paradigm for chaos [12].

$$\begin{aligned} \dot{x}_1 &= \alpha\left[x_2 - x_1 - h(x_1)\right] \\ \dot{x}_2 &= x_1 - x_2 + x_3, \\ \dot{x}_3 &= -\beta x_2, \end{aligned} \tag{2}$$

Where G=2/R and a three-segment piecewise linear v_{C1}-i characteristics of nonlinear elements is defined by

$$h(x_1) = bx_1 + \frac{1}{2}(a-b)(|x_1+1| - |x_1-1|).$$

For α=10, β=14.87, a=-1.27, and b=-0.Chua's circuit operates on the chaotic double scroll attractors. Chua's circuits exhibits a chaotic attractor.

3) Rossler

The Rössler system is a system of three equations. These equations are a nonlinear ordinary differential equation. Some properties of the Rössler system can be deduced via linear methods such as eingen-vector. The original Rössler paper says the Rössler attractor was intended to behave similarly to the Lorenz attractor, but also be easier to analyze qualitatively. This attractor has some similarities to the Lorenz attractor, but is simpler and has only one mainfold. Otto Rössler designed the Rössler attractor in 1976, but the originally theoretical equations were later found to be useful in modeling equilibrium in chemical reactions. The defining equations are [13]:

$$\begin{aligned} \dot{x}_1(t) &= -x_2(t) - x_3(t), \\ \dot{x}_2(t) &= x_1(t) - ax_2(t), \\ \dot{x}_3(t) &= b + x_3(t)(x_1(t) - c) \end{aligned} \tag{3}$$

Rössler studied the chaotic attractor with a = 0.2, b = 0.2, and c = 5.7.

B. Discrete

1) Hénon map

The Hénon map is a discrete-time dynamical system. It is one of the most studied examples of dynamical systems that exhibit chaotic behavior. The Hénon map takes a point (x_1, x_2) in the plane and maps it to a new point [14]

$$\begin{aligned} x_1(k+1) &= c - ax_2(k) + x_2(k), \\ x_2(k+1) &= bx_1(k) \end{aligned} \tag{4}$$

The map depends on two parameters, *a, b,* and *c*, which for the canonical Hénon map have values of a = 1.4, b = 0.3, and c=1. For the canonical values the Hénon map is chaotic. For other values of a and b the map may be chaotic, intermittent, or converge to a periodic orbit. An overview of the type of behavior of the map at different parameter values may be obtained from its orbit diagram.

2) Logistic map

The logistic map is a polynomial mapping of degree 2, often cited as an archetypal example of how complex, chaotic behavior can arise from very simple nonlinear dynamical equations. The map was popularized in a seminal 1976 paper by the biologist Robert May, in part as a discrete-time demographic model analogous to the logistic equation first created by Pierre François Verhulst [5], the logistic map is written [16]

$$x(k+1) = \alpha x(k) + \beta x^2(k), \tag{5}$$

where:

$\alpha x(k)$ represent a growth or birth effect, whereas $\beta x^2(k)$ accounts for the limits to growth such as availability of energy or food. If β=0, we obtain the equation $x(k+1) = \alpha x(k)$ with explicit solution

$$x(k) = x(0)\alpha^k, \tag{6}$$

This nonlinear difference equation is intended to capture two effects.

- Reproduction where the population will increase at a rate proportional to the current population when the population size is small.
- starvation (density-dependent mortality) where the growth rate will decrease at a rate proportional to the value obtained by taking the theoretical "carrying capacity" of the environment less the current

However, as a demographic model the logistic map has the pathological problem that some initial conditions and parameter values lead to negative population sizes.

III. Simulation

A. Chaotic generator

Firstly, we develop software for resolve and graphic different chaotic generator in the previous section, this program is made in Matlab. The principal screen present two options, continuous and discrete models (see Fig. 1). In the fig.2 show of the three different model for continuous and the Fig.3 two discrete model. In this page it is necessary select the option selected.

The Figure 4 show the Lorenz Model, in this screen show the initial and final time, initial conditions, parameters, and the equation of this model. In this screen is possible to change the values, so, is possible to see the behavior of the x_1, x_2, and x_3.

When finish the calculate, we can graph the variable with time or the phase between two or three variable. The Figure 5 shows a example.

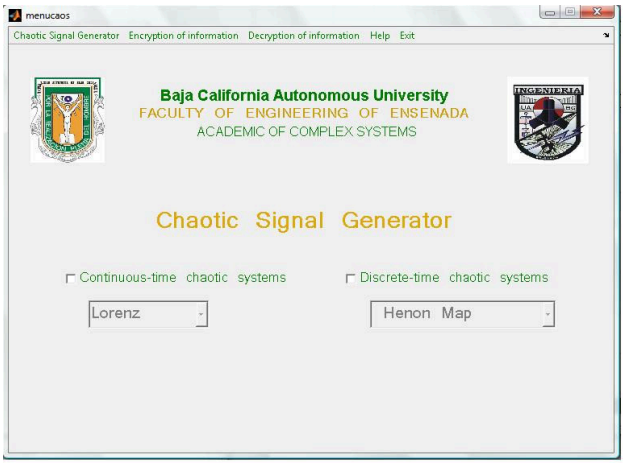


Fig. 1. Principal page.

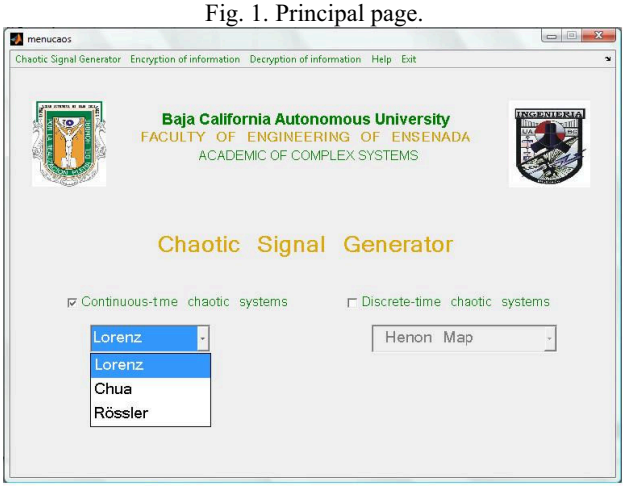


Fig. 2. Continuous chaotic system screen

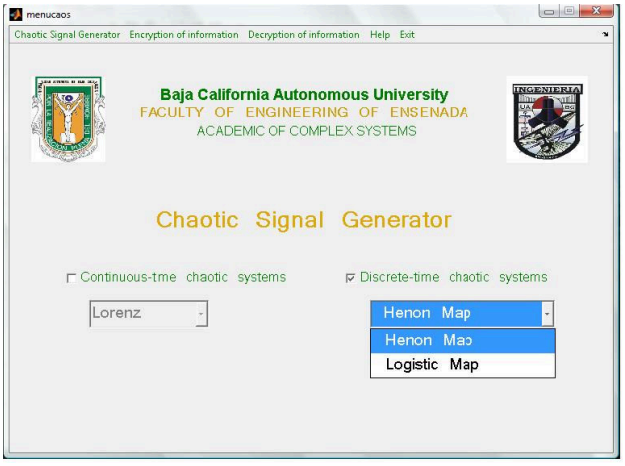


Fig. 3. Discrete chaotic system screen.

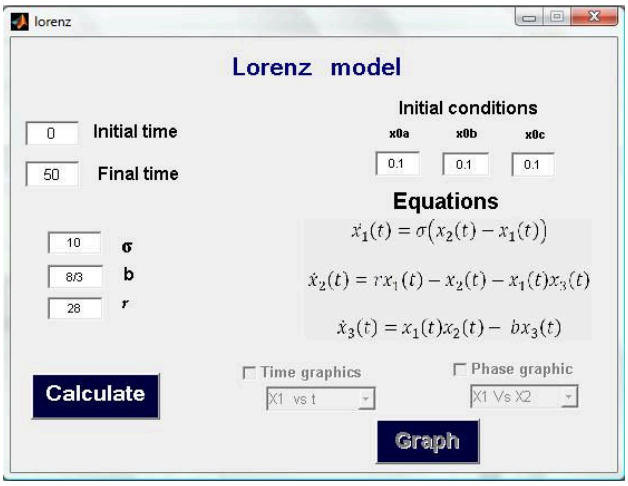


Fig. 4. Screen for model Lorenz.

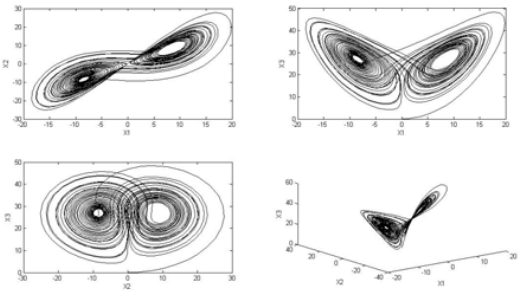


Fig. 5. Lorenz Attractors.

Like the Lorenz model, it is possible call the other five models. In all case we can the change the time, initial condition, parameters, and for each model show the own equations. For illustration only show the Lorenz model.

B. Chaotic generator Application: Secret Communication software

The models presented in previous section have applications to the secret communication. The principal page show the option for encrypts the information for continuous models (Fig. 6).

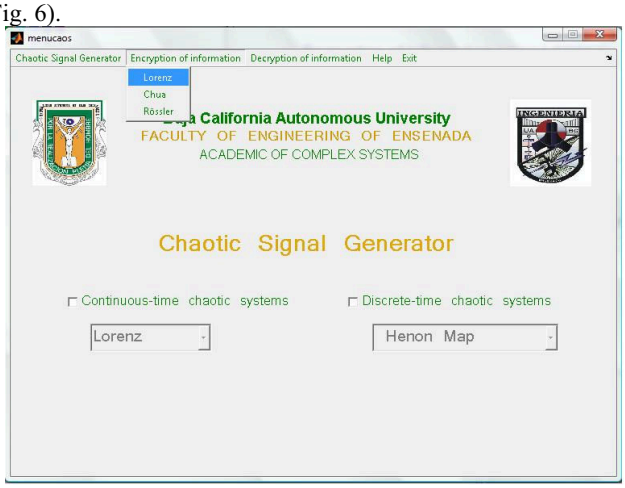


Fig. 6. Encryption information.

For example, we take the Lorenz model for show the …

Then, appear the screen show in the Fig. 7. In this screen we have the option the parameters, time, and message. This message can be sinusoidal or rectangular signal.

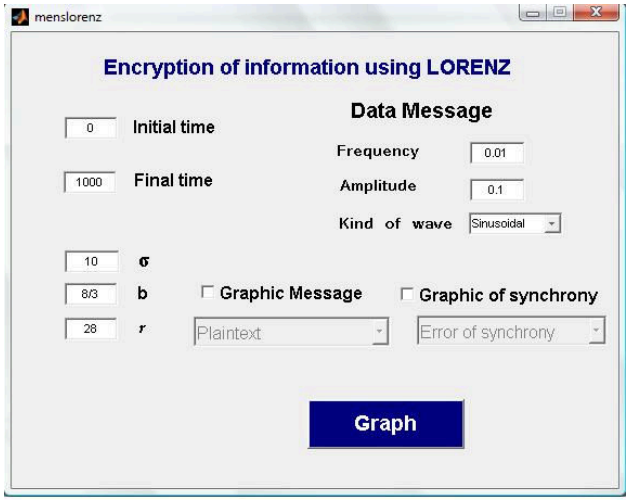
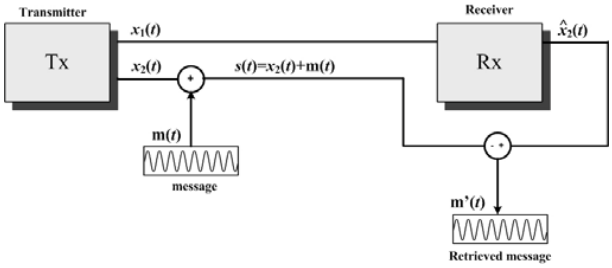


Fig. 7. Encrypt information for Lorenz model.

The schematic for encryption message is shown in the Fig. 8. We use one channel for synchronize transmitter and receiver. A second channel is used to add the message, for illustration we use a sinusoidal message. Finally, we subtract $\hat{x}_2(t) - s(t) = m'(t)$, that is, the recovery message



Finally we can select the desired graph. These can be the original and retrieved message, transmitted signal, and the error between original and retrieved message, Fig. 9. The other option is graph the synchrony error (Fig.10).

Finally, the Figure 11 shows the original message, transmitted signal, retrieval message, and error between original and retrieval message.

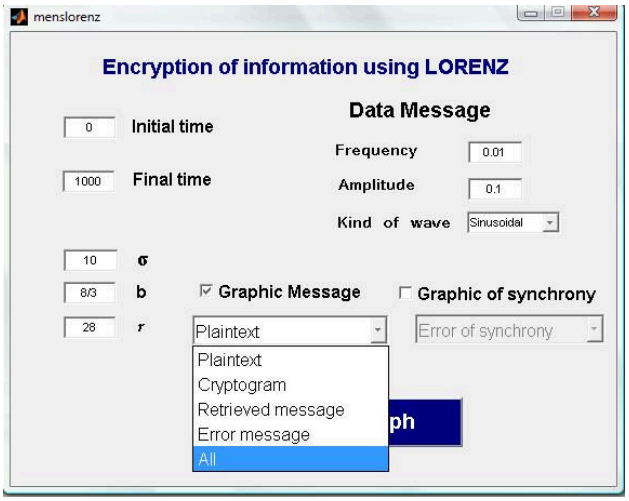


Fig.9. Screen for select message graph.

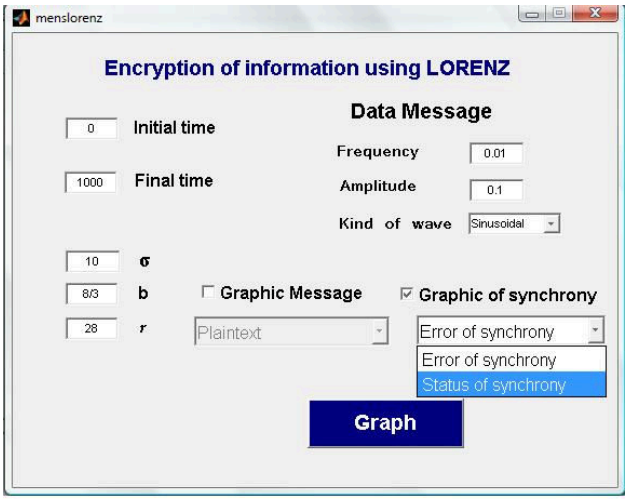


Fig.10. Screen for select synchrony graph.

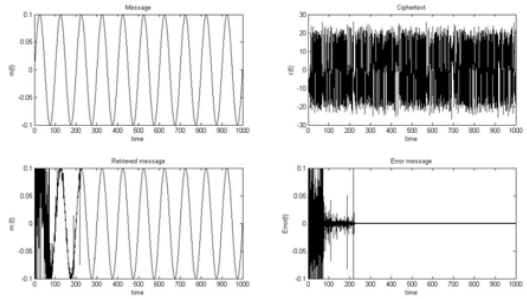


Fig. 11. Message encrypted.

IV. Conclusion

This software is a tool very useful for to show different chaotic generator. In this software is possible appreciate the attractor behavior when are changed the different parameters.

The critical parameters are a option in the software, this parameter show value range for chaotic behavior.

For encrypted message is possible select binary o digital

information. In a future work, we added the option for select the from file or write the message

APPENDIX

Appendixes, if needed, appear before the acknowledgment.

ACKNOWLEDGMENT

The authors would like to thank to CONACYT, México by the support under Research Grants No. J49593-Y and P50051-Y. And to UABC, México, by academic mobility.

REFERENCES

[1] L.M... Pechora and T.L. Carroll, "Synchronization in chaotic systems,"Phys. Rev. Lett. 64, 821-824 (1990).
[2] L. M. Pecora and T. L. Carroll, "Circuit implementation of synchronizedchaos with applications to communications," Phys. Rev. A **44**, (1991).
[3] [3] Special Issue on Chaos synchronization and control: Theory and applications IEEE Trans. Circuits Syst. I, **44**, (1997).
[4] [4] Special Issue on Control and synchronization of chaos, Int. J. Bifurc. Chaos, **10**, (2000).
[5] [5] C. Cruz-Hernández and H. Nijmeijer, "Synchronization through filtering," Int. J. Bifurc. Chaos, **10**, 763-775 (2000). Synchronization through extended Kalman filtering. In: Nijmeijer H, Fossen TI, editors. *New trends in nonlinear observer design*. Lecture notes in control and information sciences, **244** London: Springer; 469–490, (1999).
[6] [6] H. Sira-Ramírez and C. Cruz-Hernández, "Synchronization of chaotic systems: a generalized Hamiltonian systems approach," Int. J. Bifurc. Chaos, **11**, 1381-1395 (2001). And in: Proceedings of the American Control Conference, Chicago, USA, 769–773 (2000).
[7] [7] D. López-Mancilla and C. Cruz-Hernández, "Output synchronization of chaotic systems: model-matching approach with application to secure communication," Nonlinear Dynamics and Systems Theory, **5**, 141-15 (2005).
[8] [8] U. Feldmann, M. Hasler and W. Schwarz, "Communication by chaotic signals: the inverse system approach," Int. J. Circuits Theory and Applications, **24**, 551-579 (1996).
[9] H. Nijmeijer and I. M. Y. Mareels, "An observer looks atsynchronization," IEEE Trans. Circuits Syst. I, **44**, 882-890 (1997).
[10] Lorenz, E. N. , "Deterministic nonperiodic flow". *J. Atmos. Sci.* **20**: 130–141. doi:10.1175/1520-0469(1963)020<0130:DNF>2.0.CO;2., (1963).
[11] Matsumoto, Takashi , "A Chaotic Attractor from Chua's Circuit". *IEEE Transactions on Circuits and Systems* (IEEE) **CAS-31** (12): 1055-1058. (1984).
[12] Madan, Rabinder N., "*Chua's circuit: a paradigm for chaos"*. River Edge, N.J.: World Scientific Publishing Company. ISBN 9810213662, (1993).
[13] O. E. Rössler, "An Equation for Continuous Chaos". *Physics Letters* **57A** (5): 397–398M., (1976).
[14] Hénon, "A two-dimensional mapping with a strange attractor". *Communications in Mathematical Physics* **50**: 69–77. doi:10.1007/BF01608556, (1976).
[15] *Eric W. Weisstein, Logistic Equation at MathWorld.*
[16] R.M. May, "Simple mathematical models with very complicated dynamics". *Nature* **261**: 459. doi:10.1038/261459a0, 1976.

Cardoza-Avendaño L. was born in Ensenada, B.C. México on 1980. She is Professor of Electronics Engineering in Baja California Autonomous University since 2005. She received her Master Engineering degree in Electrical Engineering from Baja California Autonomous University, México, in 2008. Since August 2008, she has been a PhD student. Her research interests involve synchronization of complex systems and Applications.

López-Gutiérrez R. M. was born on 10-11-1972. She is a Professor of Electronics Engineering in Baja California Autonomous University since 2001. She received her Master Science degree and Ph.D. degree in Electronics and Telecommunications from CICESE, Mexico in 1996 and 2003, respectively. Her research interests involve synchronization of complex systems and applications.

Cruz Hernández C. received the M.S. and Ph.D. degrees in electrical engineering from CINVESTAV, México, in 1991 and 1995, respectively. Since 1995, he is with the Department of Electronics and Telecommunications of the Scientific Research and Advanced Studies of Ensenada (CICESE), where, he is current Professor of Automatic Control. His research interests include multimode oscillations of coupled oscillators, nonlinear systems analysis, and synchronization and control of complex dynamical systems.

Inzunza González E. was born in Navolato, Sinaloa México on 1976. Received the Bachelors degree in Electronic Engineer from the Culiacán Institute of technology, in 1999, the M. Sc. degree in electronics and telecommunications from CICESE, México, in 2001. Since August 2008, he where, he is current Professor of Automatic Control. His research interests include multimode oscillations of coupled oscillators, nonlinear systems analysis, and synchronization and control of complex dynamical systems.

Garcia-Guerrero E. E. studied physics engineering at the University Autonomous Metropolitana, Mexico, and received the PhD degree in optical physics from the Scientific Research and Advanced Studies Center of Ensenada, B.C, (CICESE) Mexico. He has been with the Engineering Faculty, Baja California Autonomous University (UABC) Mexico since 2004. His current interests are in the field of Optical Synchronization of Complex Systems.

Serrano Guerrero H. was born in Culiacán, Sinaloa, México. Received the Bachelors degree in electronic engineer from the Technologic Institute of Culiacán in 2000, the M. Sc. degree in instrumentation and control from CICESE, México, in 2002. From March 2003 to August 2006 he worked as Test Engineer in Electrónica Lowrance de México. From August 2006 to August 2008 he was a full time professor in the Faculty of Engineering of the Universidad Autónoma de Baja California, México. Since August 2008, he has been a doctoral student and subject professor in the Faculty of Engineering of the Universidad Autónoma de Baja California, México. His current research interest include control and synchronization of complex dynamical systems, and encrypted transmissions using chaos.