UNIVERSIDAD
NACIONAL
DE COLOMBIA
SEDE MEDELLÍN
FACULTAD DE MINAS

DYNA
http://dyna.medellin.unal.edu.co/

Secure point-to-point communication using chaos

Maricela Jiménez-Rodríguez [a], María Guadalupe González-Novoa [a], Juan Carlos Estrada-Gutiérrez [a], Cuauhtemoc Acosta-Lúa[a] & Octavio Flores-Siordia [a]

[a] *Departamento de Ciencias Tecnológicas, Centro Universitario de la Ciénega, Universidad de Guadalajara, Ocotlán, Jalisco, México.*
m_jimenez_r@yahoo.com, gleznogpe@hotmail.com, jcarlosredes@gmail.com, temo09@gmail.com, o_flores@live.com.mx

Received: October 9th, de 2015. Received in revised form: Mach 1rd, 2016. Accepted: Mach 15th, 2016

Abstract
This article presents an alternative for resolving the existing vulnerability of systems that implement masking by means of chaotic synchronization. This system avoids detection of the parameters used as the cipher key by an attacker on implementing encryption by means of synchronized chaotic-phase masks of the Rössler oscillator, for encoding and establishing synchronization among transmitter-receiver devices. In addition, it employs two ciphering keys: the first, with a recommended length of 2,048 characters, and the second, which is used as an initial value. Both keys are employed for continual modification of one of the oscillator's parameters. This strengthens the security system and avoiding an attacker from obtaining the oscillator's parametric values by calculating the least average synchronization error. The use of the system developed provides a cipher, which is resistant to statistical attacks. In addition, our system validates the data of the transmitter device (username, password, etc.) in order to authorize transmission.

Keywords: authentication; data encryption; security; integrity; chaos.

Comunicación punto a punto segura usando caos

Resumen
Este artículo presenta una alternativa para resolver la vulnerabilidad existente en los sistemas que implementan el enmascaramiento mediante la sincronización caótica, este sistema evita que los parámetros utilizados como clave de cifrado puedan ser detectados por un atacante al implementar el modelo matemático caótico del oscilador de Rössler para codificar y establecer la sincronización entre los dispositivos transmisor-receptor; además usa dos llaves de cifrado: la primera con una longitud recomendable de 2048 caracteres y la segunda se utiliza como un valor inicial. Ambas llaves se emplean para modificar continuamente uno de los parámetros del oscilador, esto fortalece la seguridad del sistema y evita que un atacante obtenga los valores del parámetro del oscilador calculando el error de sincronización promedio menor. El uso del sistema desarrollado proporciona un cifrado resistente a ataques estadísticos, además valida datos del dispositivo transmisor (nombre de usuario, password, etc.) para autorizar la transmisión hacia el destino.

Palabras clave: autenticación; encriptación de datos; seguridad; integridad; caos.

1. Introduction

The role of chaotic systems is an excellent alternative for information security and privacy. This is due to such systems' great properties, such as high sensitivity to the initial conditions and to the parameters. Another interesting characteristic is that chaos uses frequencies that render it resistant to the customary filtering techniques to separate information superimposed on a signal [1]. In other words, a message transmitted through a network can be encoded by chaos, using previously cited characteristics. Once transmitted, the information would be very difficult to decode, unless the receptor possesses the inverse-way method, considering the exact values of the parameters, in order to recover and be able to extract the original message with certainty. Some discreet chaotic systems have been used to cipher information, such as the technique implemented by Ranjan and Saumitr, in which the authors compress and

How to cite: Jiménez-Rodríguez, M., González-Novoa, M.G., Estrada-Gutiérrez, J.C., Acosta-Lúa, C. and Flores-Siordia, O., Secure point-to-point communication using chaos. DYNA 83(197), pp. 181-187, 2016

DYNA 83 (197), pp. 180-186. June, 2016 Medellín. ISSN 0012-7353 Printed, ISSN 2346-2183 Online
DOI: http://dx.doi.org/10.15446/dyna.v83n197.53506

encode text using chaotic Logistic Map system. The authors employ an insecure channel to transmit the encoded data and another, secure channel to send the key [2]. Pareek et al. developed a symmetrical key algorithm for ciphering, in which they used multiple one-dimensional chaotic maps and an external key of 128 bits. Plain text is encoded sequentially using a set of chaotic maps in random fashion [3]. In addition, Pisarchik and Carmona elaborated chaotic map network-based algorithms to encrypt images in color. These authors used the Logistic Map, and as ciphered keys, they used the parameters, the number of iterations, the number of cycles, and the size of the image [4]. Hossam et al. proposed a cryptosystem for encrypting color images or videos that employs a mechanism of iterative encryption, in which each of the image's pixels depends on a secret key, of the logistic map exit and of the previously encrypted pixel [5]. Chaos is also used in the world of medicine. Barbara et al. proposes a transmission method allowing electrocardiogram (ECG) signals obtained from a patient to be combined with algorithms generating chaotic signals, based on the Lorenz equation system [6]. Another very important technique employed in secure communications is the synchronization of chaotic systems [7-13]. Tao and Len used the Chua circuit to modulate a signal in a parameter in a transmitter; subsequently, the authors used an adaptive controller in the receiver to maintain the synchronization and to recover the signal [14]. They developed an Image Encryption Algorithm where logistic map and iterative equation are used, and they switch the position and the pixels values [15]. The authors also employed two different chaotic cryptography techniques in which they employed the logistic map to apply the diffusion technique, and the chaotic synchronization of two, coupled Rössler oscillators to apply the confusion [16]. Zanin and colleagues carried out a systems cryptanalysis that uses synchronization for encryption through message masking, and the authors demonstrated how to detect the parameters used as encrypted keys, calculating the least synchronization error [17]. Thus, in this work, we implemented a method to strengthen the security of systems that use chaotic masking, avoiding the detection of parameters used as the encrypted key. In other studies, the authors have recommended prior encryption of the information before employing synchronization, in order to avoid detection of the parameters, but this approach implies more time to encode and decode [16,17]. A security analysis was carried out on different Wireless Local Area Networks (WLAN), where it was determined that one of the risks comprises the absence of mechanisms of authentication [18]. The method recommended in this work varies the parameter according to the way in which the mathematical system used for synchronizing conducts solving. Therefore, no extra time is required for previous ciphering. The identification of users who transmit information provides greater security. Thus, in this work, in addition to encoding, a technique is performed to validate users who attempt to transmit. The remainder of this article is organized as follows: in Section 2, the methodology for developing the system used is clearly explained, and in Section 3, we show how the communication channels for transmitting encrypted information in a point-to-point network using chaos are implemented. Later, in Section 4, we show the results of using tests to evaluate the system's functionality; we have also included a statistical analysis and the conclusions obtained.

2. Methodology

2.1. Chaotic synchronization

Pecora and Carroll demonstrated unidirectional coupled chaotic systems [19], an excellent tool used in the area of secure communication. In this investigation, the Rössler oscillator is implemented to transmit encrypted information employing chaotic synchronization where the Master $m(t)$ oscillator is described in an eq. (1) system [20], in which x, y, z, are the system's state variables, and the system's parameters are rendered by: $\mathrm{a}1,\ \mathrm{a}2,\ \mathrm{a}3$.

$$\begin{aligned}\frac{dx}{dt} &= -(y+z)\\ \frac{dy}{dt} &= (x+(a1)y)\\ \frac{dz}{dt} &= a3+z\,(x+a2)\end{aligned} \tag{1}$$

The Slave oscillator $s(t)$ is defined by the eq. (2) system, where $x^{\prime}$, $y^{\prime}$, z' are state variables and the system's parameters are: $a1,\ a2,\ a3$.

$$\begin{aligned}\frac{dx'}{dt} &= -(y+z'\ )\\ \frac{dy'}{dt} &= (x'\ +(a1)y)\\ \frac{dz'}{dt} &= a3+z'\ \ (x'\ +a2)\end{aligned} \tag{2}$$

Complete synchronization is an entity between the trajectories of two Master-Slave systems [19, 21], which can be determined by the synchronization error $\mathrm{e(t)}$, that is $\lim_{t\to\infty} \mathrm{e(t)} = 0$, where $\mathrm{e(t)} \equiv ||\ \mathrm{m(t)}\text{-}\mathrm{s(t)}|| = 0$ [21].
In this study, chaotic synchronization is implemented using the Rössler oscillator for point-to-point communication in a secure manner, where the Master $\mathrm{m(t)}$ system is used to encrypt in the transmitter and the Slave $\mathrm{s(t)}$ in order to decrypt in the receptor; however, prior to this, these should be synchronized using variable y for coupling [19]. That is, the exit $\mathrm{y_{master}}$ is coupled with the entry $\mathrm{y_{slave}}$ to ensure synchronization. Functioning is exhibited in Fig. 1.

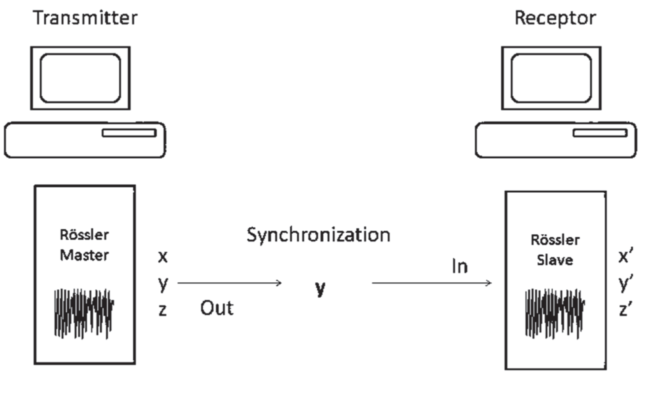


Figure 1. Master-Slave synchronization method.
Source: Authors.

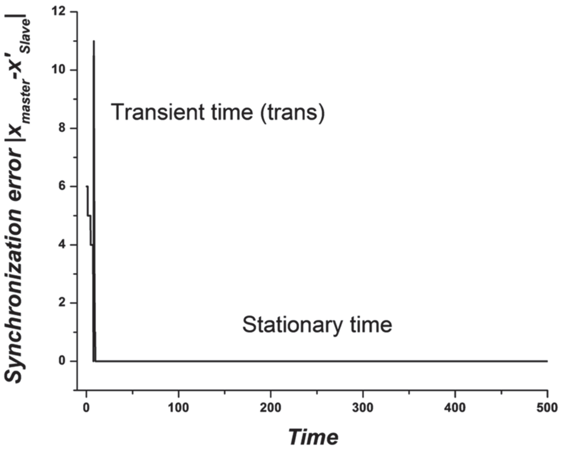


Figure 2. Transitory (trans) and stationary time determined by the synchronization error.
Source: Authors.

Prior to the synchronization, a transitory time trans should pass, during which the Master-Slave systems yield different results until the stationary time, which is when the exit variables x, y, z of the Master system are identical to those of the exit variables x', y', z' of the Slave system. Thus, the synchronization error $e(t) = 0$ and the synchronization itself is complete, as depicted in Fig. 2.

When the encrypted transmitter and the receptor are completely synchronized, the receptor can decipher without any problem because both the transmitter and the receptor generate the same values of the variables. This technique is used for encoding information because it is very interesting that two irregular behaviors are based on a sole behavior, generating a chaotic orbit that is similar to noise that is very difficult to predict. This represents an important application in secure communications and cryptography. It is for this reason that this work was implemented.

3. System functioning

The system allows for point-to-point communication establishing channels to encrypt and transmit information with greater security through the network. In addition, the system is more robust because the transmitter should authenticate it in order to permit it to send information. Next, chaotic synchronization is implemented by means of the Rössler Master oscillator, equation system (1) to encrypt the final decrypted outcome using equation system (2). Below are the steps to follow:

1. The transmitter sends the name and password of the user to the receptor.
2. The receptor authenticates the user's data and the IP and MAC electronic addresses of the transmitter. If the latter are not correct, the transmission is cancelled.
3. If it is an allowed user, the authorization is sent.
4. The transmitter uses the algorithm to encrypt what is explained in Section 3.2.
5. The information is sent.
6. The receptor uses an algorithm of Section 3.2 for deciphering.

This process is illustrated in Fig. 3.

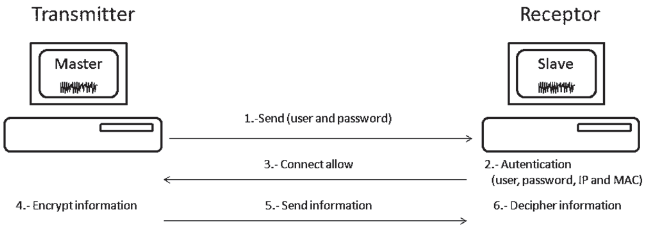


Figure 3. Master-Slave synchronization method.
Source: Authors.

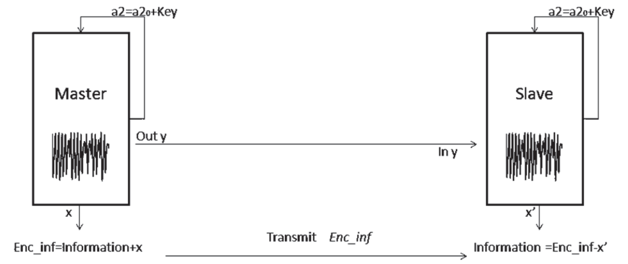


Figure 4. Data encryption and transmission.
Source: Authors.

3.1. Encryption with parameter variation

The transmitter solves equation system (1), modifying the value of parameter a_2 that is used as the encrypting key $(a2 = a2_0 + key)$, to avoid detection by an attacker. Once the transitory time $(trans)$ has passed and complete synchronization is initiated, the transmitter encrypts the information by adding up $Enc\_inf = Information + x_{master}$. After encrypting it together with the coupling variable $\mathrm{y}_{\mathrm{master}}$ so that the receptor can synchronize itself, solving equation system (2), modifying the parameter. After this, it deciphers, subtracting $\mathrm{Information} = \mathrm{Enc\_inf\text{-}x'}_{\mathrm{slave}}$. This procedure is shown in Fig. 4.

3.2. Algorithms

In this section, we describe the functioning of the algorithms for encrypting and deciphering an archive of text, but any type of information can be encrypted by dividing it into bytes.

Nomenclature:

- C: Original information, with values between 0 and 255.
- n: Length of original information.
- trans: Number if iterations necessary to achieve synchronization (transitory time).
- l: Length of the key k.
- Encrypting keys:
  a) k: External key used to modify parameter a2 and to encrypt the information.
  b) $a2_0$: Initial value of parameter a2 in the chaotic regime.

3.2.1. Algorithm for encryption

Step 1. Convert each character of the text file into its American Standard (ASCII) value.

$$Information = [C_1, C_2, C_3, \dots, C_n]$$

Step 2. Divide each element that contains the Information vector by 255 to obtain values between 0 and 1.

$$Information = [C_1, C_2, C_3, \dots, C_n]\,/255$$

Step 3. Convert the key k into its ASCII value and store it in the vector.

$$key = [k_1, k_2, k_3, \dots, k_l]$$

Step 4. Divide each element of the key k by 255 to obtain values between 0 and 1.

$$key = [k_1, k_2, k_3, \dots, k_l]/255$$

To vary parameter a2

Step 5. Calculate the value of $a2$ by adding $a2_0$ plus an element of the vector key and solve equation system (1). In the case of all of the elements of key having been already used, initiate the re-run of the vector key form the first position.

$$a2 = a2_0 + key_{1\dots l}$$

Step 6. After solving the system trans times, encrypt the information by adding $Information + x_{master}$ and storing the result in vector Enc_inf. Observe the functioning in Fig. 5.

Step 7. Store y_{master} in vector $y\_sync = [y_1, y_2, y_3, \dots, y_{trans+n}]$

Step 8. Repeat steps 5 through 7 trans + n times.

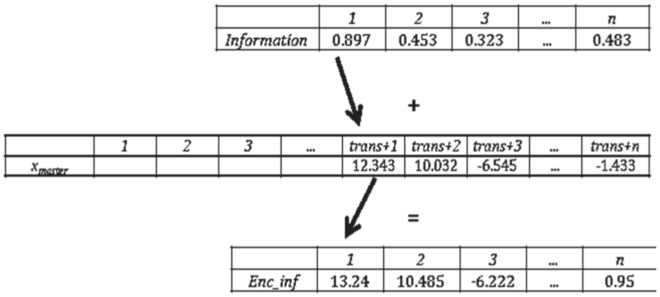
3.2.2. Algorithm for deciphering

It is necessary to possess the encrypted information Enc_inf, the values of y_sync for synchronization of the Slave and the encrypted keys key, $a2_0$.

Step 1. Perform Steps 3 and 4 of the algorithm to encrypt.

Step 2. Calculate the value a_2 by adding $a2_0$ plus one element of the vector key and solve equation system (2). In the case that all of the elements of the key have already been used, initiate the re-run from the first position.

$$a2 = a2_0 + key_{1\dots l}$$



	1	2	3	...	n
Information	0.897	0.453	0.323	...	0.483

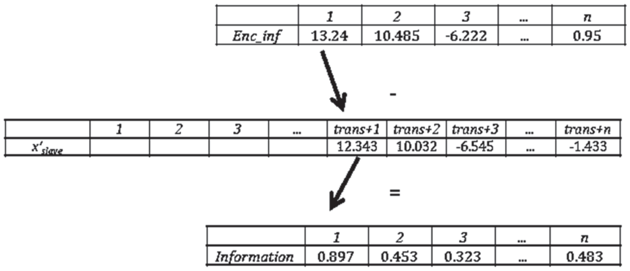
+

	1	2	3	...	trans+1	trans+2	trans+3	...	trans+n
x_{master}					12.343	10.032	-6.545	...	-1.433

=

	1	2	3	...	n
Enc_inf	13.24	10.485	-6.222	...	0.95

Figure 5. Encryption process using Step 6.
Source: Authors.



	1	2	3	...	n
Enc_inf	13.24	10.485	-6.222	...	0.95

-

	1	2	3	...	trans+1	trans+2	trans+3	...	trans+n
x'_{slave}					12.343	10.032	-6.545	...	-1.433

=

	1	2	3	...	n
Information	0.897	0.453	0.323	...	0.483

Figure 6. Deciphering information according to Step 3.
Source: Authors.

Step 3. After solving the trans times system, decipher the remaining information Enc_inf-x'_{slave} and store the result in the vector Information. Observe the functioning in Fig. 6.

Step 4. Perform Steps 2 and 3 trans + n times to decipher all of the information.

Step 5. Multiply each element of the vector information by 255 to obtain the original information.

$$Information = [C_1, C_2, C_3, \dots, C_n] * 255$$

4. Results and Conclusions

The results obtained in the statistical tests employed to determine the system's robustness on encrypting and sending a text message are shown below.

4.1. Correlation diagram

These allow us to demonstrate graphically the relationship between two variables and in addition how to obtain the correlation coefficient, which can fall within the range of -1 and 1, indicating that the nearer the two they are to each other, the stronger the linear association will be. In the case of its nearing a 0, this indicates a weak or null association if this is 0.

The correlation diagram (Fig. 7) depicts the values of the deciphered information in the horizontal axis, and the values of the original information in the vertical axis. We can observe that the correlation coefficient is 1. Thus, the original information and the information that was deciphered is identical; that is, the system manages excellent data integrity, therefore, there is no information deformation at the moment of encrypting and deciphering.

In the correlation diagram (Fig. 8), the original vs. encrypted information is shown, and it yields a correlation coefficient of 0.000032329, which indicates that the relationship between encrypted and original information is nearly null. This is very favorable because some attackers study the relationship that exists between these two variables in order to attempt to determine the encryption key that has been employed.

4.2. Histograms

These are used to represent the distribution of the message, where the horizontal axis is shown with vertical bars and the data that are being transmitted. The height of each bar corresponds the number of frequencies of the data.

In Fig. 9, the data that are being transmitted (the original information) are between 0.1 and 1, with the majority of data being between 0.375 and 0.475.

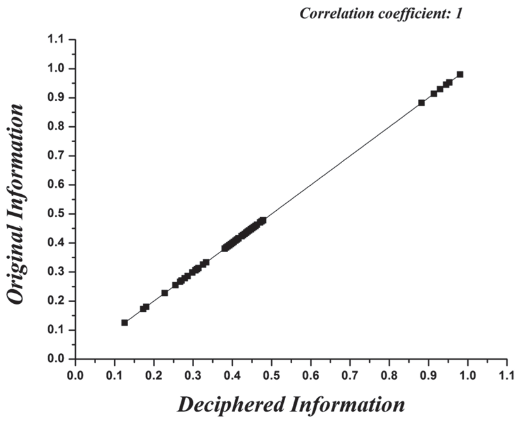


Figure 7. Correlation diagram: original vs. deciphered information.
Source: Authors.

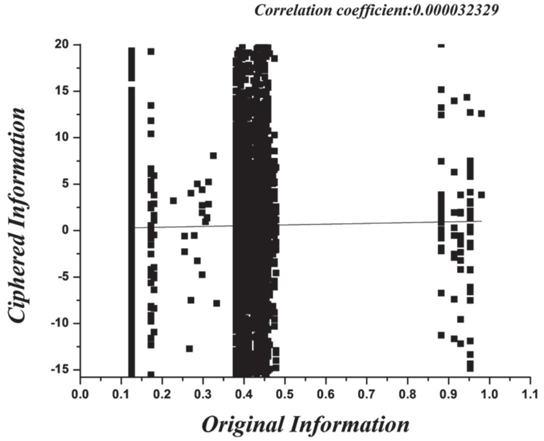


Figure 8. Correlation diagram of encrypted vs. original information.
Source: Authors.

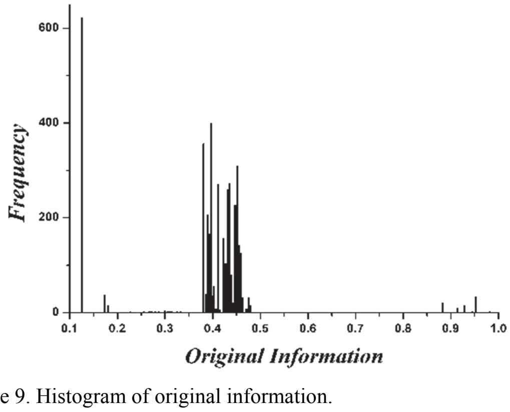


Figure 9. Histogram of original information.
Source: Authors.

Fig. 10 shows the histogram of the encrypted information, where it is clear that the encrypted data are found within the range of –15.25 and 20. If Figs. 9 and 10 are compared, we can observe that there is no relationship between the number of frequencies and the range of values of the graphs' horizontal axis. This helps to make it more difficult for an attacker to find a relationship between original and encrypted information.

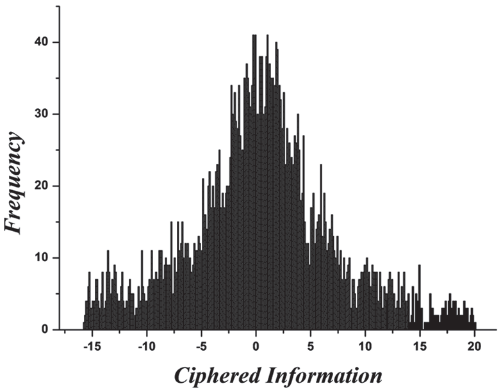


Figure 10. Histogram of ciphered information.
Source: Authors.

4.3. Conclusions

The communications system developed truncates the orbit or trajectory by constantly changing one of the chaotic mathematical model's parameters; this speeds up the encoding time in comparison with other cryptographic systems that employ various orbits. Thus, more computer processing is necessary. Our system guarantees confidentiality because only the receiver, which possesses the keys used for encoding, can calculate the parameter's different values, in order to reconstruct the orbit; thus, decoding the information received. The constant change of the parameter employed avoids an attacker from detecting the parameter by using the least average synchronization error.

To verify the robustness of the system developed, the original information (plaintext) is compared to the ciphered text (ciphertext), using the correlation diagram depicted in Fig. 8, in which a coefficient near the value of 0 is exhibited. This indicates that the linear association is nearly null. With the latter, it is proven that the system is resistant to statistical attacks, such as those based on clear text (differential and linear), in which an attempt was made to determine the key on searching for some relationship between the ciphertext and the plaintext. Another of the tests conducted is illustrated in the histograms shown in Figs. 9 and 10, in which there are very different ranges of values and frequencies. This renders the system sufficiently robust for avoiding an attack in which the frequencies or repeat chains are analyzed in order to attempt to find correspondence between ciphered and deciphered information.

To evaluate the integrity of the data transmitted vs. the data received once the encoding and decoding process was accomplished, the correlation diagram in Fig. 7 provides a coefficient with a value of 1. This indicates that the information is not altered on passing through the ciphering and communications process.

The system employed within this investigation protects the communication point-to-point, combining authentication and encoding techniques, in order to safeguard the information transmitted from one point to another. In this way, it complies with integrity, confidentiality, and security services. Additionally, the technique used for varying the parameter contributes robustness to the communications system.

Acknowledgment

The authors acknowledge the support from PRODEP-SEP (Convocatoria de Fortalecimiento de Cuerpos académicos) (Mexico).

References

[1] Hilborn, R.C., Chaos and Nonlinear Dynamics. New York: Oxford University Press, 2000.

[2] Ranjan, B. and Sumitr, P., A novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system. IEEE Transactions on Circuits and System-I, 53(4), pp. 848-857, 2006. DOI: 10.1109/TCSI.2005.859617.

[3] Pareek, N., Patidar, V. and Sud, K., Cryptography using multiple one-dimensional chaotic maps. Communications in Nonlinear Science and Numerical Simulation, 10(7), pp. 715-723, 2005. DOI: 10.1016/j.cnsns.2004.03.006

[4] Alexander, P. and Flores, N., Computer algorithms for direct encryption and decryption of digital images for secure communication. Proceedings of the 6th WSEAS International Conference on Applied Computer Science, (Tenerife, Canary Islands, Spain), pp. 29-34, 2006.

[5] Hossam, E., Ahmed, H., Haamdy, K. and Osama, F., An Efficient chaos-based feedback stream cipher (ECBFSC) for image encryption and decryption. Informatica, 31, pp. 121-129, 2007.

[6] Barbara, E., Alba, E. and Rodríguez, O., Modulating electrocardiographic signals with chaotic algorithms. Ingeniería e Investigación, 32(2), pp. 46-50, 2012.

[7] Sundar, S. and Minai, A., Synchronization of randomly multiplexed chaotic systems with application to communication. Physical Review Letters, 85(25), pp. 5456-5459, 2000. DOI: 10.1103/PhysRevLett.85.5456

[8] Parlitz, U., Kocarev, L., Stonjanovski, T. and Preckel. H., Encoding messages using chaotic synchronization. Physical Review E, 53(5), pp. 4351-4361, 1996. DOI: 10.1103/PhysRevE.53.4351

[9] Partlitz, U., Chua, L., Kocarev, Lj., Halle, K. and Shang. A., Transmission of digital signals by chaotic synchronization. International Journal of Bifurcation and Chaos, 2(4), pp. 973-977, 1992. DOI: 10.1142/S0218127492000562

[10] Annovazzi, V., Donati, S. and Sciré, A., Synchronization of chaotic lasers by optical feedback for cryptographic applications. IEEE Journal of Quantum Electronics, 33(9), pp. 1449-1454, 1997. DOI: 10.1109/3.622622

[11] Kocarev, L. and Parlitz, U., General approach for chaotic synchronization with applications to communication. Physical Review Letters, 74(25), pp. 5028-5031, 1995. DOI: 10.1103/PhysRevLett.74.5028

[12] Zhao, Y., Experimental demonstration of chaotic synchronization in the modified Chua's oscillators. International Journal of Bifurcation and Chaos, 7(6), pp. 1401-1410, 1997. DOI: 10.1142/S0218127497001126

[13] Cuomo, K., Oppenheim, A. and Strogatz, S., Synchronization of Lorenz-based chaotic circuits with applications to communications, IEEE Transactions on Circuits and Systems- II: Analog and Digital Design Processing, 40(10), pp. 626-633, 1993. DOI: 10.1109/82.246163

[14] Yang, T. and Chua, L.O., Secure communication via chaotic parameter modulation. IEEE Transactions on Circuits and Systems - I: Fundamental Theory and Applications, 43(9), pp. 817-819, 1996. DOI: 10.1109/81.536758

[15] Zhang, J. and Zhang, Y., An image encryption algorithm based on balanced pixel and chaotic map. Hindawi Publishing Corporation: Mathematical Problems in Engineering, 2014, pp. 1-7, 2014. DOI: 10.1155/2014/216048

[16] Jiménez, M., Rider, J. and Alexander, P., Secure communication based on chaotic cipher and chaos synchronization. Discontinuity, Nonlinearity and Complexity, 1, pp. 57-68, 2012. DOI: 10.5890/DNC.2012.02.003

[17] Zanin, M., Sevilla, J., Jaimes, R., García, J., Huerta, G. and Pisarchik, A.N., Synchronization attack to chaotic communication systems. Discontinuity, Nonlinearity, and Complexity, 2(4), pp. 333-343, 2013. DOI: 10.5890/DNC.2013.11.003.

[18] Julián, M., Fredy, A. and Fabián, Ch., Security analysis of a WLAN network sample in Tunja, Boyacá, Colombia. DYNA, pp. 226-232, 2015. DOI: 10.15446/dyna.v82n189.43259

[19] Carroll, T.L. and Pecora, L.M., Synchronizing chaotic circuits. IEEE Transactions on Circuits and Systems, pp. 453-456, 1991. DOI: 10.1109/31.75404

[20] Ramírez, C.A., Masking information through synchronized chaotic systems, MSc. Thesis, Department of Mathematics, Universidad Nacional de Colombia, Bogotá, Colombia, 2011.

[21] Schuster, H.G., Handbook of chaos control. New York: Wiley-VCH, 1999.

M. Jiménez-Rodríguez, has an BSc. degree in Computation Engineering, from the UdeG in 1999, a MSc. degree in Applied Computation in 2003, Universidad Central Martha Abreu, Cuba. In 2005, she obtained a Cisco Certified Network Associate certification, and in 2007, a Cisco Certified Academy Instructor certification. She was awarded a Dr. degree in Science and Technology at the Centro Universitario de los Lagos (CULagos), UdeG, in 2012. Currently, she is a professor in the Department of Technological Sciences at the Centro Universitario de la Ciénega (CUCIénega) and conducts investigation in the areas of Security Systems and Communications and Systems Elaboration, in addition to Applied Mathematics in Systems Development.
ORCID: orcid.org/0000-0002-4935-2731

M.G. González-Novoa, is a full-time professor, working at the Department of Basic Sciences of the UdeG, Ciénega. She has a MSc. degree in Applied Communications with a specialty in databases, awarded in 2005. Her area of specialization is object-oriented programming and software development, distributed systems, the application of algorithms, and data structure. She Participates in diverse investigation projects, is the author of various international and national publications, books and peer-review articles, all with reference to the line of investigation with which she collaborates: Elaboration of Security Systems and Communications. Currently she is working on the development of applications with technology for networks and security.
ORCID: orcid.org/0000-0002-1170-1238

J.C. Estrada-Gutiérrez, has an BSc. degree in Computational Engineering 2001, a MSc. degree in Applied Computation from the UdeG, in 2005, a PhD in Sciences from the UdeG in 2014, awarded in 2005 by Cisco CCNA (Cisco Certified Network Associate), and in 2007 received a certification as a Cisco Certified Academy Instructor. He is also a Candidate to be a National Instructor in the Mexican National System of National Investigators (SNICONACYT) 2014-2016. He is a professor at the Department of Technological Sciences, CUCiénega, and carries out research in the areas of Telecommunications, Applied Physics, and Biomedical Engineering.
ORCID: orcid.org/0000-0002-6727-3500

C. Acosta-Lúa, obtained his BSc.in Electronic Engineering from the Technological Institute of Morelia in 2001. He completed his MSc.degree in 2003 and Ph.D. in 2007 in Science in Electrical Engineering at CINVESTAV Guadalajara Unit. He participated in stays at INSA Lyon, France and DEWS Research Center in L'Aquila Italy. He carried out his Postdoctoral studies at DEWS Research Center in L' Aquila, Italy and the Centre for Research and Implementation of the Ford Motor Company. Since 2009, he has been an Associate Professor of Automatic Control at the University of Guadalajara. He is currently engaged in the development of nonlinear techniques for vehicle control and observers for nonlinear subsystems thereof.
ORCID: orcid.org/0000-0002-7398-2629.

O. Flores-Siordia, is a full-time professor in the Department of Technological Sciences at CUCiénega, UdeG. He has an BSc. degree in Chemical Engineering, a MSc. degree in Chemical Engineering, and a PhD in the Teaching Methodology. His areas of specialization include applied mathematics. He participates in the following lines of investigation: Elaboration of Security Systems and Communications, and collaborates in diverse research projects, and has various international and national publications, books and peer-reviewed articles, in reference to the development of applications with technology for networks and security.
ORCID: orcid.org/0000-0003-3611-4512