SADIO Electronic Journal of Informatics and Operations Research

http://www.dc.uba.ar/sadio/ejs

vol. 4, no. 1, pp. 1-13 (2002)

A simple deterministic Lorenz chaotic-based methodology to cipher and decipher information

M. S. Suárez-Castañón[1] Carlos Aguilar-Ibañez[1] J. C. Martínez-García[2]

[1] Laboratorio de Metrología y Control
Centro de Investigación en Computación del I.P.N.
Av. Juan de Dios Bátiz S/N esquina con Manuel Othon de Mendizabal
Unidad Profesional Adolfo López Mateos
Col. San Pedro Zacatenco, A.P. 75476
07700 México, D.F., México
e-mail: caguilar@pollux.cic.ipn.mx
No. tel. 52-5-7296000, ext. 56568

[2] Departamento de Control Automático
CINVESTAV-IPN
A.P. 14-740
07300 México, D.F., México
e-mail: martinez@ctrl.cinvestav.mx

Abstract

We present in this paper a secure deterministic cipher and decipher mechanism based on the well known Lorenz's dynamic system. The cipher process is performed by the combination of the message to be cipher and the states of the Lorenz's dynamic system, which act as the cipher key. The decipher process is carried out by the reconstruction of the key, which is generated using a Lorenz's system state observer. The observed key is then used in the decipher process in order to recover the ciphered message.

Keywords: : Cryptography, Chaotic System, State Observer

1 Introduction

Oscillatory chaotic systems have been of grate impact in Physics, Biology, Communications Engineering, Control Theory and Atmospherics Science; as examples, we can mention the lots of numbers in magazines and books published in the last decades ([Holden, 1984], [Acheson, 1997], [Holden, 1986], [Alligood, 1996], [Devaney, 1989] and [Devaney, 1990]). Most of this books and magazines focus their attention in the study of chaotic systems and their applications, like chaotic circuits synchronization, used in Communication Engineering and Control ([System and Control Letters, 1997], [Chaos Synchronization and Control, 1993] and [Chaos Synchronization and Control, 1997]), in the study of planets behavior, in prediction of population growth and, in the predictive study of ecosystems adaptability ([Conrad, 1983] and [Conrad, 1981]).

The main issue in this article its the application of Lorenz's systems (*in their discrete approximation form*), to cipher and decipher any kind of information represented in a digital way. The cipher process its carried out generating a cipher key, as long as the information that will be cipher; the decipher process consists in the reconstruction of the cipher key and use it with the inverse process its carried out by a cipher system (*in their discrete approximation form*); this system create a set of chaotic states, (x_{1k}, x_{2k}, x_{3k}) where $k = \{1, 2, \ldots, n\}$, where two of them $\{x_{2k}, x_{3k}\}$, are mixed with the messages or the signals to be send $\{ s_{1k}, s_{2k} \}$, by means of a simple arithmetic operation $M_k = (x_{1k}, x_{2k} l_1 + s_{1k}, x_{3k} l_2 + s_{2k})$. Where M_k is the vector transmitted to the receiver system, $\{ s_{1k}, s_{2k} \}$ are the messages that we want to cipher, l_1 and l_2 are scaling factors, not equal to zero, selected in a way that the chaotic signals $\{ x_{1k}, x_{2k} \}$ will be larger enough comparative with the messages $\{ s_{1k}, s_{2k} \}$.

The receiver circuit or decipher is able to reconstruct the cipher messages $\{ s_{1k}, s_{2k} \}$ almost exactly from the received chaotic signals: $M_k = (m_{1k}, m_{2k}, m_{3k})$, *i.e.* $\hat{s}_{1k} = (m_{2k} - \hat{x}_{2k}\ l_1)$ and $\hat{s}_{2k} = (m_{3k} - \hat{x}_{3k}\ l_2)$, where $\left\{ \hat{x}_{1k}, \hat{x}_{2k} \right\}$, are the reconstructed chaotic signals, by the decipher system, such that $\left| c_{ik} - \hat{c}_{ik} \right| \le e$, $i = 1, 2$, for every $k > k^* > 0$ and e is a positive constant near to zero.
This cipher/decipher mechanism, is based on chaotic circuits synchronization (see [Nijmeijer, 1997],[Sira-Ramírez, 2001], [Carrol, 1991], [Kuomo, 1993], [Fradkov, 1997], [Huijbert, 1998] and [Pecora]). We say that two chaotic systems, sender and receiver, are synchromesh, if not matter what initial conditions start the sender and receiver systems, when time goes to infinity the error between both systems is equal to zero. Synchronize two chaotic systems is not a trivial problem, because it is possible that even very small differences between the initial conditions of both systems may cause an exponential error amplification [Orgozalek, 1993].

Worthy, we mention that almost every proposed synchronization scheme, where made in theoretical and academic frame. Some of them where made in a real time experiment, and achieve an efficiency in the transmitted signal recovery, between 85% to 95% [Kuomo, 1993]. Due to the fact that it is not possible to build two identical circuits, *i.e.*, there will be always some variations in parameters, like resistance and inductance and there. The performance achieved is good enough for some applications, like voice transmission; however, is not reliable to be used in the cipher/decipher information process (see [Gerald, 1994], [Pfleeger, 1996], [Schneier, 1996] and [DeMillo, 1983]).

This article is organized in four sections, the first one where presented as brief introduction on chaos and their diverse applications; the second one propose an state observer system for the Lorenz chaotic circuit; in the third one, we develop a cipher/decipher, mechanism, based on the chaotic properties of the Lorenz chaotic circuit and their respective state observer; in the last section, we implement a numerical application to cipher and decipher information, and show some examples of an image ciphered and deciphered, using this application. Finally, we present the conclusions.

2 A simple Lorenz system-based observer

First of all, let us present the well known three dimensional chaotic Lorenz's dynamical system

Definition 1 *Continuous Lorenz's dynamical system:*

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

where: $[x_1(\cdot) \quad x_2(\cdot) \quad x_3(\cdot)]^T$ *denotes the state vector;* $y(\cdot)$ *denotes the output and* $\{s, r, b\}$ *denotes the real parameters set of the system. We suppose that* $s > 0$.

We introduce now our:

Defnition 2 *Lorenz's dynamical state observer:*

$$\begin{aligned}
&\dot{\hat{x}}_1(t) = s\,(\hat{x}_2(t) - \hat{x}_1(t)) - g\,(x_1(t) - \hat{x}_1(t)),\\
&\dot{\hat{x}}_2(t) = r y(t) - \hat{x}_2(t) - y_1(t)\,\hat{x}_3(t),\\
&\dot{\hat{x}}_3(t) = y(t)\,\hat{x}_2(t) - b\,\hat{x}_3(t),
\end{aligned} \tag{2}$$

where: $\left[\hat{x}_1(\cdot) \quad \hat{x}_2(\cdot) \quad \hat{x}_3(\cdot)\right]^T$ *denotes the observed states. The real parameter* g *is positive.*

Taking into account the previously defined Lorenz's dynamical system and its corresponding state observer, we introduce the following:

Definition 3 *Error system:*

$$\begin{aligned}
&\dot{e}_1(t) = s\,e_2(t) - s\,e_1(t) - g e_1(t)\\
&\dot{e}_2(t) = -e_2(t) - x_1(t)e_3(t),\\
&\dot{e}_3(t) = x_1(t)e_2(t) - b e_3(t),
\end{aligned} \tag{3}$$

Where $e_i(\cdot) \coloneqq x_i(\cdot) - \hat{x}_i$ *, for i Î { 1, 2, 3 }, denotes the i-th state observation error.*

As is established by the following result, the observation error $\{e_1(\cdot), e_2(\cdot), e_3(\cdot)\}$ converges asymptotically to the zero vector $\{0,0,0\}$.

Theorem 4 *Let* $\left[x_1(\cdot)\, x_2(\cdot)\, x_3(\cdot) \right]^T$ *and* $\left[\hat{x}_1(\cdot)\, \hat{x}_2(\cdot)\, \hat{x}_3(\cdot) \right]^T$ *be the states of the Lorenz's system (1), and the states of the Lorenz's observer system, respectively. For any constant* $k \geq 0$, $\left[\hat{x}_1(\cdot)\, \hat{x}_2(\cdot)\, \hat{x}_3(\cdot) \right]^T$ *converges asymptotically to* $\left[x_1(\cdot)\, x_2(\cdot)\, x_3(\cdot) \right]^T$ *i.e., the vector error state* $\left[e_1(\cdot) e_2(\cdot) e_3(\cdot) \right]$ *converges to* $\left[000 \right]^T$.

Proof. Please consider the Lyapunov's function

$$V(t) = \frac{1}{2}\left(\frac{1}{s} e_1^2(t) + e_2^2(t) + e_3^2(t) \right).$$

Clearly $V(\cdot)$ is a positive definitive function. Moreover:

$$\frac{d}{dt} V(t) = e_1(t) e_2(t) - (1 + \frac{g}{s}) e_1^2(t) - e_2^2(t) - b e_3^2(t).$$

Since $\left| e_1 e_2 \right| \leq (e_1^2 + e_2^2)/2$, and because of the assumption $g \geq 0$, we have that:

$$\frac{d}{dt} V(t) \leq -\frac{1}{2} e_1^2(t) - \frac{1}{2} e_2^2(t) - \frac{g}{s} e_1^2(t) - b e_3^2(t) \leq 0,$$

which concludes the proof.

Remark 5 *As is established in Theorem 4, the observer (2) always recovers the motion of the Lorenz's system (1) (assuming* $g \geq 0$ *and* $s > 0$*). This property of the observer will be applied in the sequel to implement a cipher/decipher information mechanism: the set of parameters* $\{s, r, b\}$ *plays the role of the key involved in both the cipher and decipher processes.*

3 Information Cipher and Decipher Mechanism

Taking into account the result introduced by Theorem 4, we propose in this section a cipher and decipher mechanism. As was pointed out in Remark 5, the set of parameters of the Lorenz's chaotic system will play the role of the key involved in the cryptography process. The methodology that we present here requires a discrete approximation of both the chaotic system (1) and the state observer (2). In this section we apply the previous theorem to cipher and decipher digital signals. A numerical algorithm is then implemented to hide the confidential information through its combination with the output of the chaotic system (cipher process). The combination exploits the finite representation of numerical computations, in order to avoid non allowed recovering of the confidential information. The decipher process is implemented through the state observer, *i.e.*, the confidential information is recovered just separating the observer state-based information from the chaotic signal.

We proceed now to the discretization of both the chaotic system (1) and the state observer (1). We use a well-know Runge-Kutta's method (see for instance [Gerald, 1994]).

3.1 Discrete approximations

Let define $X(\cdot)^T = \left[x_1(\cdot)x_2(\cdot)x_3(\cdot) \right]^T$ and $\hat{X}(\cdot)^T = \left[\hat{x}_1(\cdot)\hat{x}_2(\cdot)\hat{x}_3(\cdot) \right]^T$. Thus, (1) and (2) can be rewritten as follows:

$$\frac{d}{dt}X(t) = F(X(t)); \frac{d}{dt}\hat{X}(\cdot) = G(\hat{X}(t), x_1(t)).$$

where:

$$F(X(t)) = \begin{bmatrix} s\,(x_2(t) - x_1(t)) \\ rx_1(t) - x_2(t) - x_1(t)x_3(t) \\ x_1(t)x_2(t) - bx_3(t) \end{bmatrix};$$

$$G(\hat{X}(t), x_1(t)) = \begin{bmatrix} s\,(\hat{x}_2(t) - \hat{x}_1(t)) - g\,(x_1(t) - \hat{x}_1(t)) \\ rx_1(t) - \hat{x}_2(t) - x_1(t)\hat{x}_3(t) \\ x_1(t)\hat{x}_2(t) - b\hat{x}_3(t) \end{bmatrix}.$$

Suppose now that there exist a real number $h > 0$, such that:

$$\left\{ \begin{array}{l} X_{k+1} = X_k + \frac{1}{6}h(C_{1k} + 2C_{2k} + 2C_{3k} + C_{4k}) = F_a(X_k) \\ t_{k+1} = t_k + h \end{array} \right\} \qquad (7)$$

with:

$$\begin{array}{cc} C_{1k} = F(X_k); & C_{2k} = F(X_k + C_{1k}/2); \\ C_{3k} = F(X_k + C_{2k}/2); & C_{4k} = F(X_k + C_{3k}). \end{array} \qquad (8)$$

Then, (7) and (8) describe a Runge-Kutta's discrete approximation to (1) (see for instance ([Acheson, 1997]). In fact, this discrete approximation is just called the *Lorenz's system approximation*. In the same way:

$$\left\{ \begin{array}{l} \hat{X}_{k+1} = \hat{X}_k + h(\hat{C}_{1k} + 2\hat{C}_{2k} + 2\hat{C}_{3k} + \hat{C}_{4k} = G_a = (\hat{X}_k, x_{1k}), \\ t_{k+1} = t_k + h \end{array} \right\} \qquad (9)$$

with

$$\begin{array}{cc} \hat{C}_{1k} = F(\hat{X}_k, x_{1k}); & \hat{C}_{2k} = F(\hat{X}_k + \hat{C}_{1k}/2, x_{1k}); \\ C_{3k} = F(\hat{X}_k + \hat{C}_{2k}/2, x_{1k}); & \hat{C}_{4k} = F(\hat{X}_k + \hat{C}_{3k}, x_{1k}). \end{array} \qquad (10)$$

describe the *observer system approximation*.

Remark 6 *To keep a good discrete system behavior, i.e., near to the continuous system behavior, we take h (the integration step) in the order of* 10^{-4}. *As a result of this choice, we can guarantee that* $\left\| X_k - \hat{X}_k \right\|_2 \leq ce^{-lkh}$, *where* $l > 0$ *and c is a positive constant greater than zero. This final constant depends on both the initial conditions of the Lorenz's system approximation and the initial conditions of the observer system approximation. In fact, if both initial conditions coincides (which is obviously difficult to achieve) c = 0. If possible, it is suitable to have* $\hat{X}_0$ *near to* X_0.

3.2 Cipher and decipher numerical algorithm

We present now our main result: a cipher and decipher numerical algorithm based in the discrete approximations presented above. In the sequel, **DCLCD-Algorithm** will stand for Discrete Chaotic Lorenz Cipher and Decipher Algorithm.

Algorithm ***7 DCLCD-Algorithm.***

1. *We send to the authorized recipient the approximated Lorenz system output (see (7) and (8)), i.e.,* $y_k = x_{1k}$. *The authorized recipient is the one who has the secrete key, i,e,, the state observer (see (9) and (10).*
2. *Once both the Lorenz system approximation and the state observer are working, we start the cipher process. In order to minimize the level of misinformation, the cipher process must start after a time* $t^* = k^* h$ *such that the approximation error* $\left\| X_k - \hat{X}_k \right\|_2 \leq ce^{-lkh}$, *is close to zero*[1]. *If* $\{s_{1k}, s_{2k}\}$ *denotes the messages set, we send to the authorized recipient the chaotic signals:*

$$\left\{ \begin{matrix} m_{1k} = x_{2k} l_1 + s_{1k} \\ m_{2k} = x_{3k} l_2 + s_{2k} \end{matrix} \right\}, \text{ for } k > k^*.$$

The scale factors l_1 *and* l_2 *are constraint to satisfy:*

$$\max|s_{1k}| << \max|x_{2k} l_1| \quad \text{and} \quad \max|s_{2k}| << \max|x_{3k} l_2|.$$[1]

3. *Since the authorized recipient receives the chaotic (11), he (or her) can proceed to perform the decipher process. The observed messages* $\left\{ \hat{s}_{1k}, \hat{s}_{2k} \right\}$ *are then computed as follows:*

$$\left\{ \begin{matrix} \hat{s}_{1k} = (m_{1k} - \hat{x}_{2k}\ l_1) \\ \hat{s}_{2k} = (m_{2k} - \hat{x}_{3k}\ l_2 \end{matrix} \right\}$$

[1] The time $t^* = k^* h$ basically depends on the initial conditions of both the Lorenz system approximation and the state observer approximation. If both initial conditions coincide, $t^* = 0$. If an acceptable approximation error level is previously specified, say 10^{-3}, it is compulsory to perform numerical analisys in order to compute the upper time bound of unacceptable misinformation risk.

The next figure represents in a graphical form the proposed cipher/decipher system:

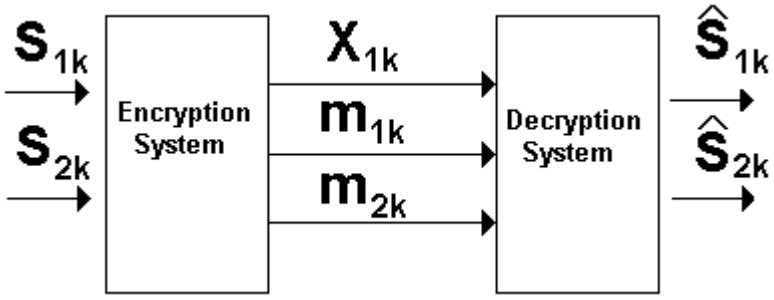

Fig. 1: Cipher/decipher scheme.

4 Numerical Implementation

In this section we test the cipher/decipher algorithm, proposed in the last section. We first designed two numerical experiments: first, we made some numerical simulations to cipher and decipher two periodical signals. We then implement the cipher/decipher mechanism in the programming language C, to cipher and decipher two digital images, and this files were send via internet to another place, and then the original images were recovered almost exactly.

4.1 Numerical simulation

We show by means a numerical simulation the cipher/decipher algorithm, proposed in the last section. We implement the Lorenz's system and their state observer, in a discrete manner (see equations [(7), (8), (9) and (10)]), with the initial conditions:

$$x_{10} = 1, x_{20} = 0.3, x_{30} = 0.0, \hat{x}_{10} = -1.0, \hat{x}_{20} = 0.5, \hat{x}_{30} = 0.1$$

and the parameters:

$$s = 10, r = 28, c = 20, k = 0, h = 0.001$$

Let $s_{1k} = \sin^2(t)$ and $s_{2k} = \cos(t)$; $4 \le t \le 20$ be the messages to be cipher.

Under a numerical simulation environment (SIMNOM™), we simulated the Lorenz's system, described in the equations (7) and (8), and the cipher mechanism, described as follows:

$$m_{1k} = 100x_{2k} + d\sin^2(hk); m_{2k} = 100x_{3k} + d\cos(hk)$$

where $d = \{1 \ if \ 4 \le hk \le 20; \ 0 \ to \ any \ other \ case\}$.

Analogous, we simulate the observer system (9) and (10), and estimate the originals signals using the decipher mechanisms, as follows:

$$\hat{s}_{1k} = (m_{1k} - 100\hat{x}_{2k}); \ \hat{s}_{2k} = (m_{2k} - 100\hat{x}_{3k})$$

The next figures shows graphically the error behavior (e_2, e_3) (see [(7), (8), (9), and (10)]).

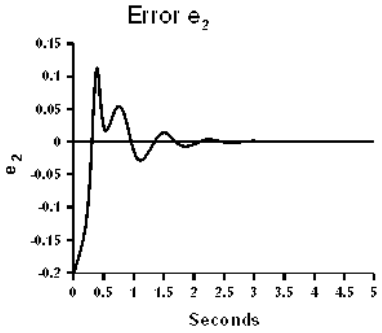

Fig. 2. The error e_2.

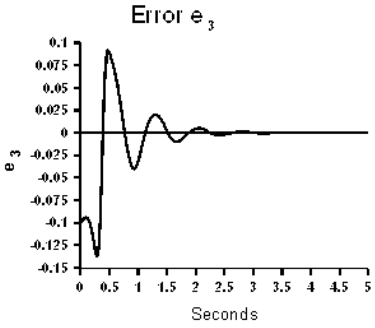

Fig. 3. The error e_3.

note that from $t = 3.8$ seconds, the observation errors are the order of 10^{-3}.

In figures four and five, we see graphically the behavior of the first ciphered signal m_{1k} (cipher system), with their respective recovered signal (decipher system).

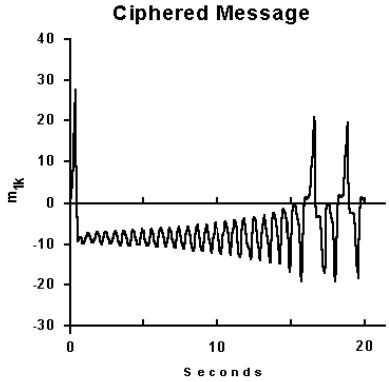

Fig. 4. Ciphered signal m_{1k}.

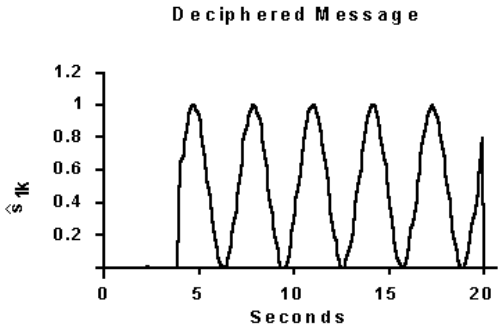

Fig. 5. Deciphered signal $\hat{s}_{1k}$.

The figures six and seven, shows in a graphically form the behavior of the second ciphered signal m_{2k}, with their respective recovered signal.

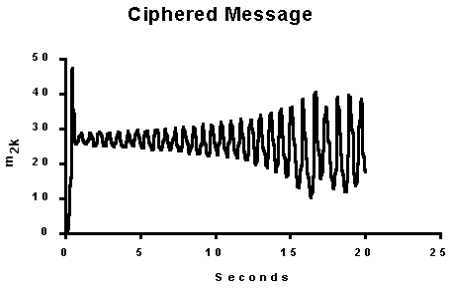

Fig. 6. Ciphered signal m_{2k}.

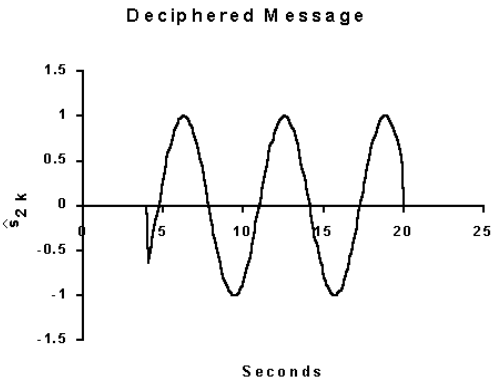

Fig. 7 Deciphered signal $\hat{s}_{2k}$.

4.2 Ciphering and deciphering information

To perform *the Cipher and Decipher algorithm*, we implement a prototype of the discretized Lorenz's system and the corresponding state observer to probe the proposed cipher/decipher mechanism in the programming language C. The tests were made ciphering and deciphering twice an image (a 24 bits BMP file), simultaneously, using the second and the third state of Lorenz's system, respectively.

We deciphered the two ciphered images, using the operation:

$$\left\{ m_{1k} = s_k + 100 x_{2k} \;, m_{2k} = s_k + 200 x_{3k} \right\} \qquad (12)$$

where s_k is the image vector, x_{2k} and x_{3k} are the second and the third Lorenz's system states [see (7) and (8)]. The decipher process was made using the operation:

$$s_{1k} = (m_{1k} - 100 \hat{x}_{2k}); \;\; s_{2k} = (m_{2k} - 200 \hat{x}_{3k}) \qquad (13)$$

where the states $\hat{x}_{2k}$ and $\hat{x}_{3k}$ are the estimated states in the state observer proposed [see (9) and (10)].

Note 2: To be able to use this cipher/decipher schema, it is necessary that the sender and the receiver agree the following information: the parameter values asigned to the cipher and the decipher systems $(s, r, b, k, h, l_1, l_2)$. *We recommend use a time* $t = kh = 4$ sec *., to start the cipher mechanism.*

Let us consider the next image:

Fig. 8. Image used to cipher and decipher.

First, we use the state x_{2k} with a scale factor of 100 to cipher the original image m_{1k} [see (12)]. Simultaneously, we ciphered the same image using the state x_{3k}, with a scale factor of 200; in the figures nine and ten, we show the ciphered images m_{2k} and m_{3k}, respectively [see (12)].

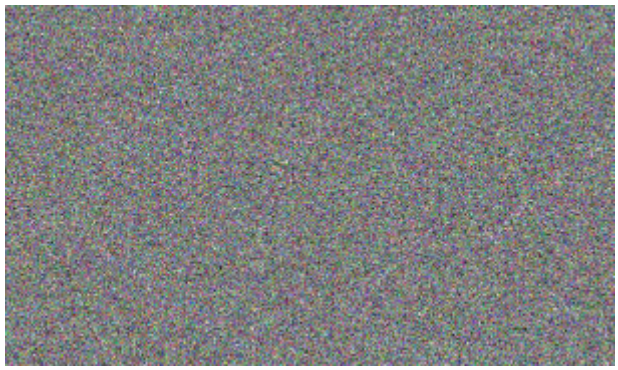

Fig. 9. The ciphered image using x_{2k}.

Fig. 10. The ciphered image using x_{3k}.

Next, we recovered the original information; figure eleven shows the deciphered message s_{1k} using the estimated state $\hat{x}_{2k}$ [see (13)]. Simultaneously, we deciphered the ciphered image m_{2k}, getting $\hat{s}_{2k}$ using the estimated state $\hat{x}_{3k}$ [see (13)], as you can see in figure twelve.

Fig. 11. The deciphered image using $\hat{x}_{2k}$.

Fig. 12. The deciphered image using $\hat{x}_{3k}$

Figure Thirteen, shows two left corner fragments amplified of each ciphered images, m_{1k} and m_{2k}, respectively, that allow to observe that the two are different:

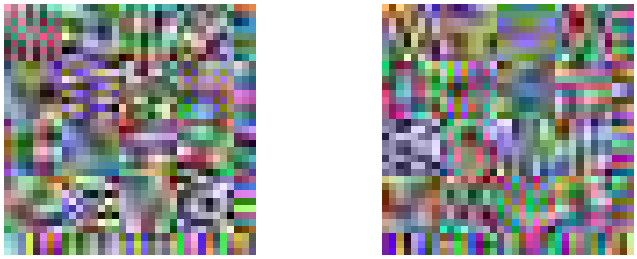

Fig. 13. We show a top left corner fragment amplified
of each ciphered image, it allows to see that both are different

Conclusions

This article presents a very simple methodology to cipher and decipher any kind of information, taking advantage of the chaotic nature of the Lorenz system.

Basically, this algorithm can be resumed as follows:

The signal to be cipher is mixed with a chaotic system variable, this variable is choose in a way that it can be reconstructed by means of one or more outputs of the sender chaotic system. The mechanism to recover the signal, can be made almost immediately, depending on how far are the initial conditions, between the *sender circuit* and the *receiver or observer system*. We recommend that the difference between the initial conditions of the *sender* and the *receiver* be very small, and start the cipher process after at time $t \geq 4$ sec.

The decipher system is based on the use of a state observer, this can be considered as a pseudo-copy of the original system, see equations (1) and (2). The convergence to zero of the observation errors, was made using the second Lyapunov's method, to do this, first, we choose a Lyapunov's function, [see (4)], which is an energy function of the Lorenz's system; after that we show that the derivative respect to time of *V* along the trajectories generated by the observation errors is defined negative, therefore the observation errors is exponentially convergent to zero.

Finally, we developed an algorithm to cipher and decipher any kind of digital information, applying the Lorenz system and their state observer, both expressed in their approximated discrete form, using the Runge-Kutta method (see the discrete equations).

Acknowledge

This work was supported by the Centro de Investigación en Computación of the Instituto Politécnico Nacional (C.I.C.-I.P.N.), of México and the Coordinación General del Posgrado e Investigación (C.G.P.I.-I.P.N. under research project N° 20010267,

References

Acheson D., From Calculus to Chaos, an introduction to dynamics, Edit, Oxford University Press, (1997)

Alligood K. T., Squer T. D., and Yorke J.A., Chaos: An Introduction to Dynamical System, Springer Verlag (1996).

T. L. Carroll, and L. Pecora, Synchronizing chaotic circuits IEEE Transactions on Circuits and Systems, vol. 38, (4) (1991), pp. 453-456.

Conrad M., Adaptability. Plenun Press, New York (1983).

Conrad M., Algorithmic specification as a technique for computing with informal biological models. Biosystems 13, 303-20 (1981)

K. M. Cuomo. A. V. Oppenheim ans S. H. Strogatz, Synchronization of Lorenz-Based Chaotic Circuits with Applications to Communications, IEEE Transactions on Circuits and Systems-II: Analog and Digital Signal Processing, vol. 40, October (1993), pp. 626-633.

DeMillo R, et. al., Applied Cryptology, cryptographic protocols, and computer security models, American Mathematical Society, Proceedings of Symposia in Applied Mathematics, vol. 29, (1983).

Devaney R., An Introduction to Chaotic Dynamical System, Addison-Wesley (1989).

Devaney R., Chaos Fractals and Dynamical System: Computer Experiments in Mathematics, Addison-Wesley (1990).

Fradkov and A. Yu. Markov, Adaptive Synchronization of Chaotic Systems Based on Speed Gradient Method and Passification, IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, vol. 44, (10), (1997), pp. 905-917.

Gerald C. F., Wheatley P. O., Applied Numerical Analysis, Edit. Addison Wesley, Fifth edition (1994).

Holden A., Chaos, Princeton University Press, (1986).

Holden A. V., Muhamad M. A., Chaotic activity in neuronal systems. In Cybernetics and Systems Research 2, ed. R. Trappl, pp. 245-50. Elsevier, Amsterdam (1984).

H. J. C. et. Al., Huijberts, H. Nijmeijer and R. M. A. Willems, A control perspective on communications using chaotic systems, Proceedings 37th IEEE Conference on Decision and Control, Tampa, Florida December 16-18 (1998), pp. 1957-1962.

H. Nijmeijer and M. Y. Mareels, An Observer Looks at Synchronization, IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, vol. 44 (10), October (1997).

Orgozalek M.J. Taming Chaos Part I: Synchronization, IEEE T.C.S. Vol. 40, pp. 693-699, (1993).

L. M. Pecora and T. L. Carroll, Driving systems with chaotic signals, Physical Review A. vol. 44 (4), pp. 2374-2383.

P. Pfleeger C., Security in computing, Edit, Prentice-Hall, (1996).

Schneier B., Applied Cryptography, Edit. John Wiley & sons, (1996).

Sira-Ramírez H. And Cruz-Hernández C., Synchronization of Chaotic System: A Hamiltonian System Approach, International Journal of Bifurcations and Chaos. (to appear)

Special Issue Systems and Control Letters, Vol. 31. (1997).

Special Issue, Chaos synchronization and control: theory and applications, IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, vol. 40, (1993).

Special Issue, Chaos synchronization and control: theory and applications, IEEE Transactions on Circuits and Systems-I; Fundamental Theory and Applications, vol. 44, (1997).