A Simple Deterministic Lorenz Chaotic-Based Methodology to Cipher and Decipher Information[1]

Metodología Basada en el Modelo Discreto del Sistema de Lorenz Para Cifrar y Descifrar Información

Miguel S. Suárez Castañón[1], Carlos Aguilar Ibañez[2] and Juan C. Martínez García[3]

[1] Escuela Superior de Cómputo del I.P.N.
Av. Juan de Dios Bátiz S/N esq. Manuel Othón de Mendizabal 07738 México, D.F., México
Tel. +(52)-55-57296000, ext. 52028, sasuarez@prodigy.net.mx
[2] Centro de Investigación en Computación del I.P.N.
Av. Juan de Dios Bátiz S/N esq. Manuel Othón de Mendizabal 07738 México, D.F., México
Tel. +(52)-55-57296000, ext. 56568, caguilar@pollux.cic.ipn.mx
[3] Departamento de Control Automático CINVESTAV-IPN
07300 México, D.F., México
martinez@ctrl.cinvestav.mx

Article received on June 24, 2006; accepted on October 01, 2007

Abstract
We present a secure deterministic cipher and decipher mechanism based on the well-known Lorenz dynamic system. The ciphering process is performed by the combination of the message to be ciphered and the states of the Lorenz dynamic system, which act as the ciphering key. The deciphering process is implemented by the reconstruction of the key, which is generated using a Lorenz system state observer. The observed key is then used in the decipher process in order to recover the ciphered message.
Keywords: Cipher/Decipher, Chaotic System, State Observer, Discrete Lorenz System

Resumen
En este artículo presentamos un mecanismo seguro de cifrado y descifrado determinístico basado en el muy conocido sistema dinámico de Lorenz. El proceso de cifrado se lleva a cabo mediante la combinación del mensaje a ser cifrado y los estados del sistema de Lorenz, el cual actúa como llave de cifrado. El proceso de descifrado se realiza mediante la reconstrucción de la llave, que es generada usando un observador de estado del sistema de Lorenz. La llave observada es usada en el proceso de descifrado con el objeto de recuperar el mensaje cifrado
Palabras Clave: Cifrador/Decifrador, Sistema Caótico, Observador de Estado, Sistema de Lorenz

Introduction

Oscillatory chaotic systems have been of great impact in Physics, Biology, Communications Engineering, Control Theory and Atmospheric Sciences. As examples, we can mention some of the books published on the subject over the last few decades ([Holden and Muhamad, 1984], [Acheson, 1997], [Holden, 1986], [Alligood *et al*., 1996], [Devaney, 1989] and [Devaney, 1990]), and some books and magazine that focus their attention on the study of chaotic systems and their applications, such as 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]), the study of the behavior of planets, the prediction of population growth and the predictive study of ecosystem adaptability ([Conrad, 1981] and [Conrad, 1983]).

The main issue in this article is the application of the Lorenz system (in its discrete approximation form), to cipher and decipher any kind of information represented digitally. The ciphering process is performed by generating

[1] A first version of this work was presented at the 3° Congreso Internacional en Control, Instrumentación Virtual y Sistemas Digitales, August, 2001, pp. 20-29.

a cipher key which is the same length as the information that will be ciphered; the deciphering process consists of the reconstruction of the cipher key and then use it in the inverse process which was performed to cipher the information. This system creates a set of chaotic states, (x_{1k}, x_{2k}, x_{3k}) where $k = \{1, 2, \ldots, n\}$ is the iteration index. The states $\{x_{2k}, x_{3k}\}$ are mixed with $\{ s_{1k}, s_{2k} \}$, which are the messages or the signals to be ciphered, by means of a simple arithmetic operation $M_k = (x_{1k}, x_{2k}\lambda_1 + s_{1k}, x_{3k}\lambda_2 + s_{2k})$, where M_k is the transmitted vector to the receiver system and, λ_1 and λ_2 are scaling factors, not equal to zero, selected in a way that the chaotic signals $\{ x_{1k}, x_{2k} \}$ will be large enough compared to the messages or signals $\{ s_{1k}, s_{2k} \}$.

The receiver system or decipher is able to reconstruct the ciphered messages $\{ s_{1k}, s_{2k} \}$ almost exactly from the received chaotic signals: $M_k = (m_{1k}, m_{2k}, m_{3k})$, *i.e.,* $\hat{s}_{1k} = (m_{2k} - \hat{x}_{2k}\,\lambda_1)$ and $\hat{s}_{2k} = (m_{3k} - \hat{x}_{3k}\,\lambda_2)$, where $\{\hat{x}_{2k}, \hat{x}_{3k}\}$, are the chaotic signals that the decipher system reconstructs, such that $\left| x_{ik} - \hat{x}_{ik} \right| \le \varepsilon$, $i = 1, 2$, for every $k > k^* > 0$; where ε is a positive constant near to zero and k^* is a constant selected in a way that the previous inequity is true.

This ciphering/deciphering mechanism is based on chaotic circuits synchronization (see [Nijmeijer and Mareels, 1997], [Sira-Ramírez and Cruz-Hernández, 2001], [Carroll and Pecora, 1991], [Cuomo *et al.*, 1993], [Fradkov and Markov, 1997], [Huijberts *et al*., 1998] and [Pecora and Carroll, 1991]). We say that two chaotic systems, the sender and the receiver, are synchronized if, no matter what the initial conditions were, the difference between both systems is equal to zero, as time goes to infinity. On the other hand, synchronizing two systems is a difficult task, because, among other problems, even very small differences between the values of the initial conditions of the sender and the receiver may generate exponential error amplification [Ogozalek, 1993].

Almost every proposed synchronization scheme was made in a theoretical and academic setting. Some of them were done in real time experiments, and the achieved efficiency in the transmitted signal recovery was between 85% and 95% [Cuomo *et al.*, 1993] because it is impossible to build two identical circuits, *i.e.*, there will always be some variation in the parameters, like resistance and inductance. Such performance is good enough for some applications, like voice transmission; however, it is not reliable for use in the ciphering/deciphering information process (see [Gerald and Wheatley, 1994], [Pfleeger, 1996], [Schneier, 1996] and [DeMillo *et al*., 1983]). It is worth mentioning that in [Lopez-Mancilla and Cruz-Hernandez, 2005] the authors present an interesting work which exploits the model-matching approach to synchronize chaotic system, even when these systems are different, with an application to secure communication of audio and binary information signals.

This article is organized in four sections. The first presents a brief introduction on chaos and their multiple applications. In Section 2 a state observer system for the Lorenz chaotic system is covered. Section 3 is devoted to developing a ciphering/deciphering mechanism, based on the chaotic properties of the Lorenz system and its respective state observer. In Section 4 a numerical application to cipher and decipher information is introduced. In the same section the numerical application performance is illustrated by ciphering and deciphering a digital image. The conclusions can be found in the last section.

2 A Simple Lorenz System-Based Observer

Inspired in the previous works of [Sira-Ramírez and Cruz-Hernández, 2001] and [Carroll and Pecora, 1991] we present the theoretical framework of our work.

First of all, we present the well-known three dimensional chaotic Lorenz dynamic system:

$$\begin{aligned}
\dot{x}_1(t) &= \sigma(x_2(t) - x_1(t)),\\
\dot{x}_2(t) &= rx_1(t) - x_2(t) - x_1(t)x_3(t),\\
\dot{x}_3(t) &= x_1(t)x_2(t) - bx_3(t),\\
y(t) &= x_1(t),
\end{aligned} \tag{1}$$

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

We introduce now our Lorenz dynamic state observer:

$$\begin{aligned}
\dot{\hat{x}}_1(t) &= \sigma(\hat{x}_2(t) - \hat{x}_1(t)) - k(x_1(t) - \hat{x}_1(t)),\\
\dot{\hat{x}}_2(t) &= ry(t) - \hat{x}_2(t) - y(t)\hat{x}_3(t),\\
\dot{\hat{x}}_3(t) &= y(t)\hat{x}_2(t) - b\hat{x}_3(t),
\end{aligned} \tag{2}$$

where: $[\hat{x}_1(\cdot), \hat{x}_2(\cdot), \hat{x}_3(\cdot)]^T$ denotes the observed states and *k* is a positive gain constant .

Subtracting the previously defined Lorenz dynamic system (1) and its corresponding state observer (2), we obtain the dynamic error equations:

$$\begin{aligned}
\dot{e}_1(t) &= \sigma e_2(t) - \sigma e_1(t) - ke_1(t)\\
\dot{e}_2(t) &= -e_2(t) - x_1(t)e_3(t),\\
\dot{e}_3(t) &= x_1(t)e_2(t) - be_3(t),
\end{aligned} \tag{3}$$

where $e_i(\cdot) := x_i(\cdot) - \hat{x}_i$, for i $\in$ { 1, 2, 3 }, denotes the *i-th* state observation error.

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

Theorem 1 *Let* $[x_1(\cdot), x_2(\cdot), x_3(\cdot)]^T$ *and* $[\hat{x}_1(\cdot), \hat{x}_2(\cdot), \hat{x}_3(\cdot)]^T$ *be the states of the Lorenz system (1) and the states of the Lorenz observer system (2), respectively. For any constant* $k \geq 0$*,* $[\hat{x}_1(\cdot), \hat{x}_2(\cdot), \hat{x}_3(\cdot)]^T$ *converges asymptotically to* $[x_1(\cdot), x_2(\cdot), x_3(\cdot)]^T$*, i.e., the vector error state* $[e_1(\cdot), e_2(\cdot), e_3(\cdot)]$ *converges to* $[0,0,0]^T$.

Proof. Consider the Lyapunov function

$$V(t) = \frac{1}{2}\left(\frac{1}{\sigma} e_1^2(t) + e_2^2(t) + e_3^2(t) \right) \tag{4}$$

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

$$\frac{d}{dt}V(t) = e_1(t)e_2(t) - (1+\frac{k}{\sigma})e_1^2(t) - e_2^2(t) - be_3^2(t)\,.$$

Since $\left|e_1 e_2\right| \le (e_1^2 + e_2^2)/2$, and $k \ge 0$, we have that:

$$\frac{d}{dt}V(t) \le -\frac{1}{2}e_1^2(t) - \frac{1}{2}e_2^2(t) - \frac{k}{\sigma}e_1^2(t) - be_3^2(t) \le 0\,.$$

That is to say, given the output $y=x_1$ of system (1), the remaining states can be exactly recovered when t is sufficiently large.

Remark 1 *Since the error converges asymptotically and exponentially to zero, the proposed observer is then robust with respect to some small external perturbation characterized by functions which vanish at the origin and which are locally Lipschitz in the state of the observer. Indeed, for this class of perturbation the origin is an exponentially stable equilibrium point of the perturbed system (for the detail see for instance [Khalil, 2002]).*

As is established in **Theorem 1**, the observer (2) always recovers the motion of the Lorenz system (1) (assuming $\gamma \ge 0$ and $\sigma > 0$). This property of the observer will be applied in the sequel to implement a cipher/decipher information mechanism: the set of parameters $\{\sigma, r, b\}$ 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 1, in this section we propose a cipher and decipher mechanism. As was pointed out in the last paragraph, the set of parameters of the Lorenz chaotic system will play the role of the key involved in the cryptography process. The methodology 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 confidential information through its combination with the output of the chaotic system (ciphering process). The combination exploits the finite representation of numerical computations in order to avoid non-allowed recovery of confidential information. The deciphering is implemented through the state observer, *i.e.*, confidential information is recovered by merely separating the observer state-based information from the chaotic signal.

We now proceed to the discretization of both the chaotic system (1) and the state observer (2). We use a well-known Runge-Kutta method (see for instance [Gerald and Wheatley, 1994]).

3.1 Discrete Approximations

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

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

where:

$$F(X(t)) = \begin{bmatrix} \sigma(x_2(t) - x_1(t)) \\ rx_1(t) - x_2(t) - x_1(t)x_3(t) \\ x_1(t)x_2(t) - bx_3(t) \end{bmatrix}; \tag{5}$$

$$G(\hat{X}(t), x_1(t)) = \begin{bmatrix} \sigma(\hat{x}_2(t) - \hat{x}_1(t)) - \gamma(x_1(t) - \hat{x}_1(t)) \\ rx_1(t) - \hat{x}_2(t) - x_1(t)\hat{x}_3(t) \\ x_1(t)\hat{x}_2(t) - b\hat{x}_3(t) \end{bmatrix}. \tag{6}$$

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

$$\begin{Bmatrix} X_{k+1} = X_k + \frac{1}{6}h(C_{1k} + 2C_{2k} + 2C_{3k} + C_{4k}) = F_a(X_k) \\ t_{k+1} = t_k + h \end{Bmatrix} \tag{7}$$

with:

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

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

$$\begin{Bmatrix} \hat{X}_{k+1} = \hat{X}_k + h(\hat{C}_{1k} + 2\hat{C}_{2k} + 2\hat{C}_{3k} + \hat{C}_{4k}) = G_a(\hat{X}_k, x_{1k}), \\ t_{k+1} = t_k + h \end{Bmatrix} \tag{9}$$

with

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

describe the *observer system approximation*.

Remark 2 *To maintain a convenient 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* $\left\| X_k - \hat{X}_k \right\| \le ce^{-\alpha k}$ *where* $\alpha > 0$ *and c is a positive constant greater than zero. This final constant depends on both the initial conditions of the Lorenz system approximation and the initial conditions of the observer system approximation. In fact, if both initial conditions coincide (which is obviously difficult to achieve) c = 0. If possible, it is suitable to have* $\hat{X}_0$ *near to* X_0.

3.2 Ciphering and Deciphering Numerical Algorithm

We present our main result: a ciphering and deciphering numerical algorithm based on the discrete approximations presented above.

Algorithm 1:

1. *The sender ciphers the messages $\{s_{1k}, s_{2k}\}$ using state variables $\{x_{2k}, x_{3k}\}$ of the approximated Lorenz system, respectively, as follows:*

$$\left\{ \begin{aligned} m_{1k} &= x_{2k}\lambda_1 + s_{1k} \\ m_{2k} &= x_{3k}\lambda_2 + s_{2k} \end{aligned} \right\}, for \;\; k > k^*,$$

   where $\{m_{ik}, m_{2k}\}$ are the ciphered messages and the scale factors, λ_1 and λ_2, are constrained to satisfy:

$$\max\left|s_{1k}\right| << \max\left|x_{2k}\lambda_1\right| \;\; and \;\; \max\left|s_{2k}\right| << \max\left|x_{3k}\lambda_2\right|.$$

   Note that in order to minimize the level of misinformation, ciphering must start after a time $t^*=kh$, such that, the approximation error $\left\| X_k - \hat{X}_k \right\|_2 \le ce^{-\lambda kh}$ *is close to zero*[2].

2. *The sender sends the authorized recipient the approximated Lorenz system output (see (7) and (8)), i.e., $y_k=x_{1k}$ and the ciphered messages $\{m_{1k},m_{2k}\}$. The authorized recipient is the person who has the secrete key, that is, the state observer (see (9) and (10)) and some previously agreed information (see Note 1).*
3. *Once the receiver has the approximated Lorenz system output $y_k=x_{1k}$ and the ciphered messages $\{m_{1k},m_{2k}\}$, he uses the state observer system (9) and (10) to compute* $\{\hat{x}_{2k}, \hat{x}_{3k}\}$ *and decipher messages$\{m_{1k},m_{2k}\}$, as follows:*

$$\left\{ \begin{aligned} \hat{s}_{1k} &= (m_{1k} - \hat{x}_{2k}\lambda_1) \\ \hat{s}_{2k} &= (m_{2k} - \hat{x}_{3k}\lambda_2 \end{aligned} \right\}.$$

Figure 1 represents the proposed ciphering/deciphering system scheme:

[2] The time $t^*=kh$ 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 especified, say 10^{-3}, it is compulsory to perform numerical analysis in order to compute the upper time bound of unacceptable misinformation risk.

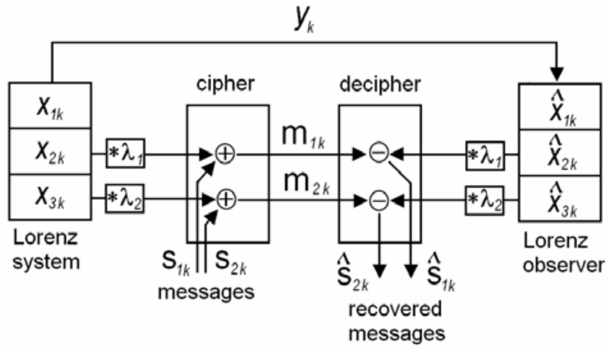

Fig. 1. Ciphering/deciphering scheme

4 Numerical Implementation

In this section we test the ciphering/deciphering algorithm proposed in the previous section. We first designed two numerical experiments: firstly we made some numerical simulations to cipher and decipher two periodical signals. We then implemented the ciphering/deciphering mechanism in programming language C in order to cipher and decipher two digital images; these files were sent via internet to a remote recipient, who recovered the images almost exactly.

4.1 Numerical simulation

We show, by means of a numerical simulation, the ciphering/deciphering algorithm proposed in the last section. We implemented the Lorenz system and its state observer in a discrete manner (see Equations (7), (8), (9) and (10)), with 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 parameters:

$$\sigma = 10, r = 28, c = 20, k = 0, h = 0.001 .$$

Let $s_{1k} = \sin^2(t)$ and $s_{2k} = \cos(t)$; $15 \le t \le 75$ be the messages to be ciphered.

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

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

where $\delta = \{1 \; if \; 15 \le hk \le 75; 0 \; to \; any \; other \; case \}$.

Likewise, we simulate observer system (9) and (10) and estimate the original signals using the decipher mechanism, as follows:

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

Figures 2 and 3 show the errors (e_2, e_3) (see Equations (7), (8), (9), and (10)).

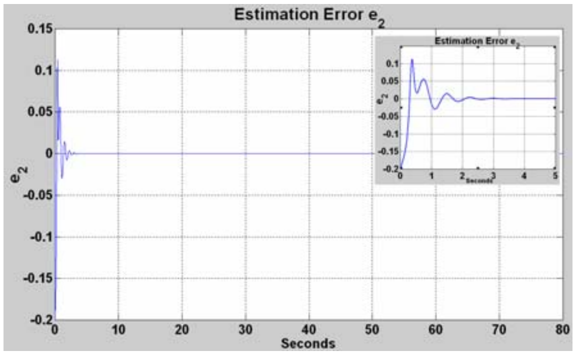

Fig. 2. Error e_2

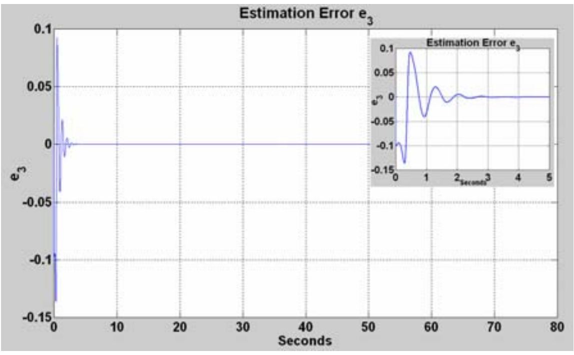

Fig. 3. Error e_3

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

In Figures 4 and 5 the behavior of the first ciphered signal m_{ik} (cipher system), with its respective recovered signal (decipher system), can be seen.

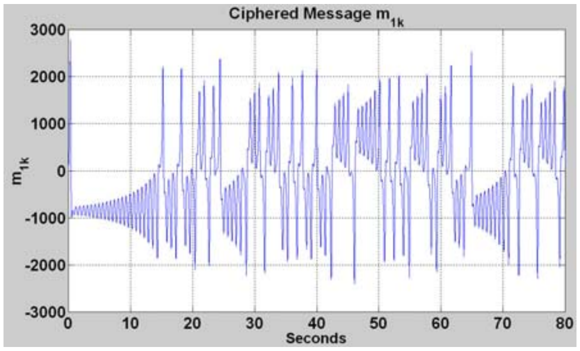

Fig. 4. Ciphered signal m_{1k}.

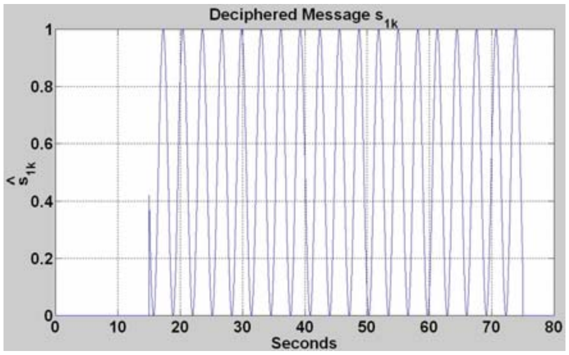

Fig. 5. Deciphered signal $\hat{s}_{1k}$

Figures 6 and 7 show the behavior of the second ciphered signal m_{2k}, with its respective recovered signal.

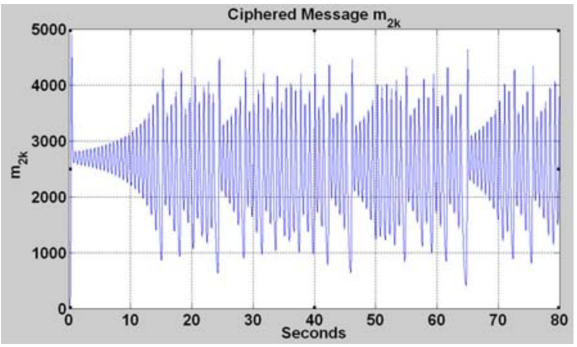

Fig. 6. Ciphered signal m_{2k}

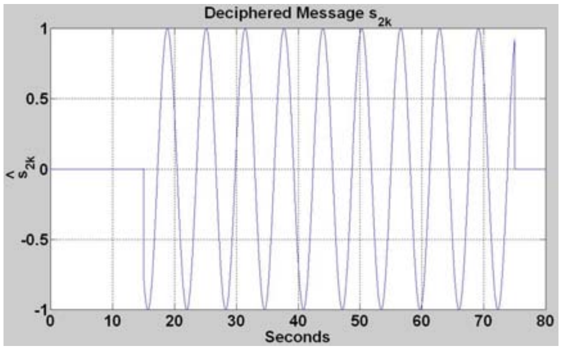

Fig. 7. Deciphered signal $\hat{s}_{2k}$

4.2 Ciphering and Deciphering Information

To perform the ciphering and deciphering algorithm, we implemented, using the C programming language, prototypes of the discretized Lorenz system and the corresponding state observer to test the proposed ciphering and deciphering mechanism. To carry out the tests we ciphered and deciphered a 24 bits BMP image file using simultaneously the second and the third states of the Lorenz system. Having completed the ciphering, we obtained two different ciphered files of the original image. These two files were then deciphered using the second and third estimated states, retrieving in both cases the original image.

We obtain the two ciphered files from the original image, using the operations:

$$\{m_{1k} = s_k + 100x_{2k}, \quad m_{2k} = s_k + 200x_{3k}\} \tag{11}$$

where s_k is the *k-th* byte of the .bmp image[3], x_{2k} and x_{3k} are the second and third Lorenz system states [see Equations (7) and (8)]. The deciphering process was implemented using the operation:

$$s_{1k} = (m_{1k} - 100\hat{x}_{2k}); \; s_{2k} = (m_{2k} - 200\hat{x}_{3k}) \tag{12}$$

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

Note 1: *To be able to use this ciphering/deciphering scheme, the sender and the receiver must agree on the following information: the parameter values assigned to the cipher and the decipher systems* $(\sigma, r, b, k, h, \lambda_1, \lambda_2)$. *We recommend using time t=kh=4 seconds to start the cipher mechanism.*

Let us consider the image in Figure 8:

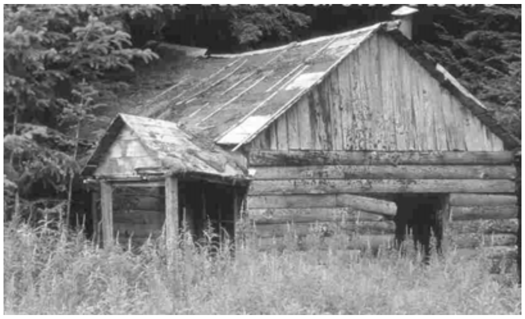

Fig. 8. Image used to cipher and decipher

First, we used the state x_{2k} with a scale factor of 100 to cipher the original image m_{1k} (see (11). Simultaneously, we ciphered the same image using state x_{3k}, with a scale factor of 200; in Figures 9 and 10 we show the ciphered images m_{1k} and m_{2k}, respectively [see (11)].

[3] Recall that a .bmp file uses the first sixty bytes (more or less) to store some data structures containing information about the file itself and the bitmap, such as image size and color. For illustrative purposes we copy these bytes from the original file to the ciphered file. The remaining bytes of the original file are read one by one, ciphered and written, also one by one, in the file that will contain the ciphered image.

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

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

Next, we recovered the original information; Figure 11 shows the deciphered message s_{1k} using the estimated state $\hat{x}_{2k}$ (see (12)). Simultaneously, we deciphered the ciphered image m_{2k}, getting $\hat{s}_{2k}$ using the estimated state $\hat{x}_{3k}$ (see (12)), as be seen in Figure 12.

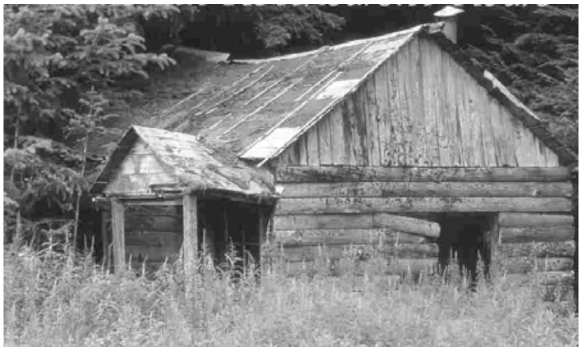

Fig. 11. The deciphered image using $\hat{x}_{2k}$

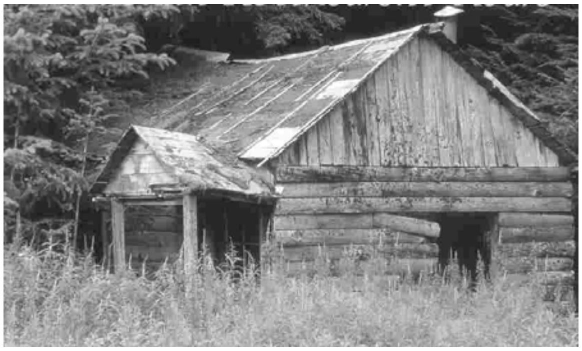

Fig. 12. The deciphered image using $\hat{x}_{3k}$

Figure 13 shows two amplified fragments of each ciphered image, m_{1k} and m_{2k}, respectively, which enable us to observe that they are completely different. This is because the states used in the ciphering process represent, in the original model, different things. Indeed, the Lorenz system gives an approximated description of the convection phenomena when a fluid in a container is heated from below and the states x_{2k} and x_{3k} are proportional to the horizontal and vertical temperature variations, respectively (see for instance [Tsonis, 1992]).

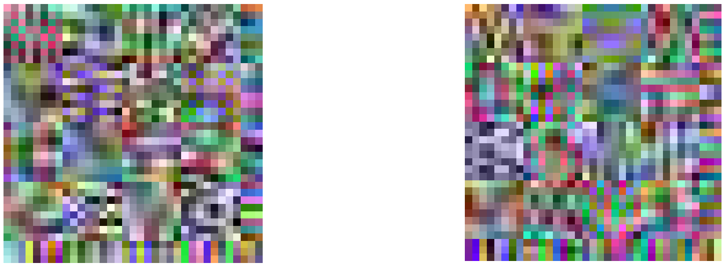

Fig. 13. Amplified corner fragments from the top left hand corner of each ciphered image

The prototype developed to illustrate performance of **Algorithm 1** can be used to cipher and decipher any kind of text. In fact, in order to verify it, we ciphered the source code of a small C program free of syntax errors. Then, we proceeded to decipher and compile it, obtaining the corresponding executable program.

We conclude this section with the observation that the variable state of the Lorenz system used to cipher depends on the user's decision and it makes no difference to the security level provided by the **Algorithm 1**.

5 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 summarized as follows:

The signal to be ciphered is mixed with a chaotic system variable. This variable is chosen 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 used almost immediately, depending on how different the initial conditions between the *sender system* and the *receiver or observer system are*. We recommend that the difference between the initial conditions of the *sender* and the *receiver* be very small, and we recommend starting the cipher process after time $t \geq 4$ seconds.

The deciphering system is based on the use of a state observer, which can be considered as a pseudo-copy of the original system (see Equations (1) and (2)). The convergence to zero of the observation errors is guaranteed via the second Lyapunov method. To do this, first, we chose a Lyapunov function, (see (4)), which is an energy function of the Lorenz system; then we showed that the derivative respect to time of V along the trajectories generated by the observation errors is defined negative, therefore the observation errors exponentially converge to zero.

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

References

1. **Acheson D.**, "From Calculus to Chaos: An introduction to dynamics", Oxford University Press, 280 pages, 1997.
2. **Alligood K. T., Sauer T.** and **Yorke J.A.**, "Chaos: An Introduction to Dynamical System", Springer, 603 pages, 1997.
3. **Tsonis, A. A.**, "Chaos. From Theory to Applications", Plenun Press, New York, 1992.
4. **Carroll T. L.** and **Pecora L.**, "Synchronizing chaotic circuits", IEEE Transactions on Circuits and Systems, vol. 38, (4) (1991), pp. 453-456.
5. **Conrad M.**, "Algorithmic specification as a technique for computing with informal biological models", Biosystems vol. 13 (1981) , pp. 303-320.
6. **Conrad M.**, "Adaptability",. Plenun Press, New York, 1983.
7. **Cuomo. K. M.**, **Oppenheim A. V.** and **Strogatz S. H.**, "Synchronization of Lorenz-Based Chaotic Circuits with Applications to Communications", IEEE Transactions on Circuits and Systems-II: Analog and Digital Signal Processing, vol. 40(10), October 1993, pp. 626-633.
8. **DeMillo R. A.**, **Lynch N. A.** and **Merritt M. J.**, "Applied Cryptology, cryptographic protocols, and computer security models", American Mathematical Society, Proceedings of Symposia in Applied Mathematics, vol. 29, 1983.
9. **Devaney R. L.**, "An Introduction to Chaotic Dynamical System", Addison-Wesley, 1989.
10. **Devaney R. L**, "Chaos, Fractals, and Dynamics: Computer Experiments in Mathematics", Addison-Wesley, 1990.
11. **Fradkov A. L.** and **Markov A. Yu.**, "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. 905-912.
12. **Gerald C. F.** and **Wheatley P. O.**, "Applied Numerical Analysis", Addison-Wesley, Fifth edition, 1994.

13. **Holden A. V.** and **Muhamad M. A.**, "Chaotic activity in neuronal systems", Cybernetics and Systems Research 2, Ed. R. Trappl, Elsevier, Amsterdam, 1984, pp. 245-50.
14. **Holden A.**, "Chaos", Princeton University Press, 1986.
15. **Huijberts H. J. C.**, **Nijmeijer H**. and **Willems R. M. A.**, "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, vol. 2.
16. **Khalil H. K.** "Non-linear Systems", Prentice Hall, 3rd. edition, 2002.
17. **Nijmeijer H.**, and **Mareels M. Y.**, "An Observer Looks at Synchronization", IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, vol. 44(10), 1997, pp. 882-890.
18. **Ogorzalek M.J.**, "Taming Chaos Part I: Synchronization", IEEE T.C.S. Vol. 40, 1993, pp. 693-699.
19. **Pecora L. M.** and **Carroll T. L.**, "Driving systems with chaotic signals", Physical Review A. vol. 44, no.4, 1991, pp. 2374-2383.
20. **Pfleeger C.**, "Security in computing", Prentice-Hall, 1996.
21. **Schneier B.**, "Applied Cryptography", John Wiley & Sons, 1996.
22. **Sira-Ramírez H.** And **Cruz-Hernández C.**, "Synchronization of Chaotic System: A Hamiltonian System Approach", International Journal of Bifurcations and Chaos, vol. 11(5), 2001, pp. 1381-1395.
23. **Special Issue**, Systems and Control Letters, Vol. 31, 1997.
24. **Special Issue**, Chaos Synchronization and Control: Theory and Applications, IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, vol. 40, (1993).
25. **Special Issue**, "Chaos Synchronization and Control: Theory and Applications", IEEE Transactions on Circuits and Systems-I; Fundamental Theory and Applications, vol. 44, (1997).

Miguel Santiago Suárez *was born in Mexico City, Mexico. He received a B.S. degree in Cybernetics and Computer Science from the School of Engineering of the Lasalle University in 1989. From the Research Institute of Applied Mathematics and Systems he received the M.S. degree in Computer Sciences in 2001. In 2005 he received a Ph.D. in Computer Sciences from the CIC-IPN. Since 2007 he is a member of the SNI of México.*

***Carlos F. Aguilar Ibáñez** was born in Tuxpan, Veracruz, Mexico. He graduated in Physics at the Higher School of Physics and Mathematics of the National Polytechnic Institute (IPN), Mexico City 1990. From the Research Center and Advanced Studies of the IPN (Cinvestav-IPN) he received the M.S. degree in Electrical Engineering in 1994, and a Ph.D. in Automatic Control in 1999. Ever since he has been a researcher at the Center of Computing Research of the IPN (CIC-IPN). As of 2000 he belongs to the National System of Researchers (SNI) of Mexico. His research focuses in non-linear systems, mechanical vibrations and chaos theory.*

***Juan Carlos Martínez García** was born in Tlalnepantla, Mexico, in 1964. He is Mechanical and Electrical Engineer from the National Autonomous University of Mexico (1989), and Master of Science in Electrical Engineering from Cinvestav-IPN (1991). He received a Ph.D. in Automatic Control Theory from Ecole Centrale de Nantes, Francia, in 1994. He is with the Department of Automatic Control, Cinvestav-IPN, Mexico City, Mexico. His fields of research include: linear control systems, robotics, failure detection in dynamical systems, evolutionary computing, and robust control. He belongs to the SNI of México.*