Secure Communication via a Chaotic Jerk System

Nicolas Marguet[1], Leonardo Acho Zuppa[2] and Julio César Rolón Garrido[2]
[1]Visiting student at CITEDI*
from École Supérieure de Chimie Physique Electronique (CPE Lyon), France
[2]CITEDI-IPN, 2498 Roll Dr. #757, Otay Mesa, San Diego, CA, 92154, USA

Abstract

Using a chaotic Jerk system and with an appropriate state space representation, it was possible to solve the synchronization problem and produce a secure communication system where the information signal is added to the dynamic of the chaotic Jerk system. From simulation experiments, our propose allows us to use information signal beyond the “slow time varying signal” used in other masking systems where adaptive tools are employed. Moreover, numerical simulations of encrypting-decrypting grey level images are shown.

1 Introduction

Design of masking systems, or secure communication systems, via chaotic signals, has been studied, for instance, in [2], [3], and [7]. In [3] and [7], decryption of the encrypted signal is done through the adaptive identification approach, where the information signal is assumed to be “slow time varying”. This approach is used because the information signal is immersed into the dynamic of the chaotic oscillator transmitter, like in our propose, but we will not use this approach here. The “slow time varying” requirement in the information signal restricts the set of information signal to be transmitted. Probably, one way to face this difficulty is to introduce a time scaling allowing the chaotic dynamics to be faster than the information signal, but this approach can saturate the bandwidth of the communication channel. In this way, it is required to use other chaotic oscillators that can face this difficulty. In [9], many chaotic Jerk systems are introduced. We use one of them, with an appropriate state space representation, to produce a secure communication system. From simulation experiments, we realized that, with this new method, the information signal can be beyond of the type of “slow time varying”. Also, we carried out experiment simulations to encrypt-decrypt gray level images.

2 Synchronization design

Consider the next chaotic Jerk system [9]:

$$\dddot{x} = -0.6\,\ddot{x} - \dot{x} + |x| - 1 + u(t) \qquad (1)$$

where $u(t)$ was added and represents the information signal to be encrypted.

To obtain a state space representation, first we selected

$$\dot{z} = |x| - 1 + u(t), \qquad (2)$$

[*] Mexican Research Center located in Tijuana, B.C., México

which makes (1) become

$$\dddot{x} = -0.6\,\ddot{x} - \dot{x} + \dot{z}\ .$$

Integration of this last expression produces

$$\ddot{x} = -0.6\,\dot{x} - x + z. \tag{3}$$

Using

$$\dot{y} = -x + z \tag{4}$$

in (3), and integrating again, we obtain

$$\dot{x} = -0.6x + y. \tag{5}$$

Then, from (5), (4) and (2), we reach the following state representation of (1):

$$\begin{aligned} \dot{x} &= -0.6x + y \\ \dot{y} &= -x + z \\ \dot{z} &= |x| - 1 + u(t), \end{aligned}$$

which can be rewritten as

$$\dot{\mathbf{X}} = \mathbf{A}\mathbf{X} + \mathbf{B}u(t) + \mathbf{f}(x), \tag{6}$$

where

$$\mathbf{X} = \begin{bmatrix} x \\ y \\ z \end{bmatrix}, \mathbf{A} = \begin{bmatrix} -0.6 & 1 & 0 \\ -1 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix},$$

$$\mathbf{B} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

and

$$f(x) = \begin{bmatrix} 0 \\ 0 \\ |x| - 1 \end{bmatrix}.$$

The strange attractor of (6) is shown in figure 1. Hereafter, it is assumed that the chaotic Jerk system preserves chaotic motion for $|u| < u_m$. This kind of assumption is done, for example, in [7].

We propose the next receiver:

$$\dot{\mathbf{X}}_r = \mathbf{A}\mathbf{X}_r + \mathbf{H}(x - x_r) + \mathbf{f}(x) \tag{7}$$

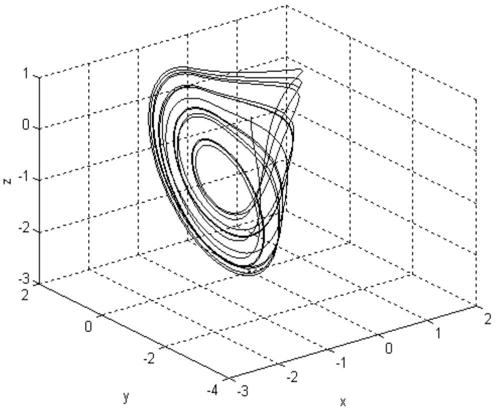

Figure 1: Transmitter's strange attractor.

where $x(t)$ is the only one transmitted signal from (6), and $\mathbf{H} = \begin{bmatrix} h_1 \\ h_2 \\ h_3 \end{bmatrix}$ is a vector that we will compute later. Then, the error dynamics yields

$$\begin{aligned} \dot{\mathbf{X}} - \dot{\mathbf{X}}_r &= \mathbf{A}\mathbf{X} + \mathbf{B}u - \mathbf{A}\mathbf{X}_r - \mathbf{H}(x - x_r) \\ &= \mathbf{A}(\mathbf{X} - \mathbf{X}_r) - \mathbf{H}(x - x_r) + \mathbf{B}u. \end{aligned}$$

Posing $\mathbf{C} = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}$ so that $x(t) = \mathbf{C}\mathbf{X}$, and $\mathbf{E} = \mathbf{X} - \mathbf{X}_r$, we obtain a linear error system

$$\dot{\mathbf{E}} = (\mathbf{A} - \mathbf{H}\mathbf{C})\mathbf{E} + \mathbf{B}u(t) \tag{8}$$

where

$$\tilde{\mathbf{A}} = (\mathbf{A} - \mathbf{H}\mathbf{C}) = \begin{bmatrix} -0.6 - h_1 & 1 & 0 \\ -1 - h_2 & 0 & 1 \\ -h_3 & 0 & 0 \end{bmatrix}$$

determines its stability: vector $\mathbf{H}$ is calculated such that $\tilde{\mathbf{A}}$ be a Hurwitz matrix. Observe that if $u(t) \equiv 0$ with $\tilde{\mathbf{A}}$ a Hurwitz matrix in (8), the error dynamic $\dot{\mathbf{E}}= \tilde{\mathbf{A}}\mathbf{E}$ is asymptotic stable. It follows that if $u(t) \in L_2$, then $E(t) \in L_2$, or if $u(t) \in L_\infty$, then $E(t) \in L_\infty$. The main idea is to find $\mathbf{H}$ such that the eigenvalues of $\tilde{\mathbf{A}}$ are appropriate located and the system $\dot{\mathbf{E}}= \tilde{\mathbf{A}}\mathbf{E}$ reaches the equilibrium in some fashion.

The characteristic polynomial of $\tilde{\mathbf{A}}$ is

$$P(\lambda) = \lambda^3+(0.6 + h_1)\,\lambda^2+(h_2 + 1)\,\lambda+h_3 \quad (9)$$

Now let's say that we want $\tilde{\mathbf{A}}$ to have complex eigenvalues $(\lambda_1, \lambda_2, \lambda_3)$. Then its characteristic polynomial would be

$$\begin{aligned} P(\lambda) &= (\lambda - \lambda_1)(\lambda - \lambda_2)(\lambda - \lambda_3) \\ &= \lambda^3 + (-\lambda_1 - \lambda_2 - \lambda_3)\,\lambda^2 \qquad (10) \\ &\quad + (\lambda_1\lambda_2 + \lambda_3\lambda_1 + \lambda_3\lambda_2)\,\lambda - \lambda_1\lambda_2\lambda_3. \end{aligned}$$

By matching (9) and (10), we obtain the desired vector $\mathbf{H}$:

$$\mathbf{H} = \begin{bmatrix} -\lambda_1 - \lambda_2 - \lambda_3 - 0.6 \\ \lambda_1\lambda_2 + \lambda_3\lambda_1 + \lambda_3\lambda_2 - 1 \\ -\lambda_1\lambda_2\lambda_3 \end{bmatrix}$$

Remark 1 $\mathbf{H}$ *is always real because, if* λ_i *is complex, then their exists* $\lambda_j = conj(\lambda_i), (i \neq j)$ *which means that* $(\lambda_i + \lambda_j) \in \Re$ *and* $\lambda_i\lambda_j \in \Re$.

The synchronization problem consists of finding a receiver system such that, if $u(t) \equiv 0$, we have

$$\lim_{t\to\infty} E(t) = 0$$

In resume, we have the following result.

Theorem 1 *The synchronization problem for (6) is solved with (7) if* $\tilde{\mathbf{A}}$ *is a Hurwitz matrix.*

3 Recovering the sent signal

Observe that from (8), the third extracted equation is

$$\dot{z} - \dot{z_r}= -h_3(x - x_r) + u$$

where h_3 is $-\lambda_1\lambda_2\lambda_3$. If $|h_3|$ is sufficiently high, we can neglect $(\dot{z} - \dot{z_r})$, then $u_r(t)$, the estimation of $u(t)$, could be

$$u_r(t) = h_3(x - x_r) \qquad (11)$$

Assume that $u(t) \in L_2$, and $u(t)$, $\dot{u}(t) \in L_\infty$, then, from Barbalat's lemma, we have that $u(t) \to 0$ as $t \to \infty$. In this way, $u_r(t)$ needs to be able to converge to zero too. Because $\tilde{\mathbf{A}}$ is Hurwitz by construction and if $u(t) \in L_2$, and $u(t)$, $\dot{u}(t) \in L_\infty$, then, from (8), follows that $E(t) \in L_2$ and $E(t) \in L_\infty$, and from (11), it follows that $u_r(t) \in L_2$ and $u_r(t) \in L_\infty$. The time derivative of (11) yields

$$\begin{aligned} \dot{u}_r(t) &= h_3(\dot{x} - \dot{x}_r) \\ &= -(0.6 + h_1)h_3(x - x_r) + h_3(y - y_r) \end{aligned}$$

which means that $\dot{u}_r(t) \in L_\infty$. From Barbalat's lemma, we concluded that $u_r(t) \to 0$ as $t \to \infty$. In resume, if the information signal $u(t)$ goes to zero, the estimation $u_r(t)$ goes to zero too. This motivates us to think that this recovery system can follow some kind of signals (similar thinking is done in the adaptive approach).

4 Simulation results

Choosing $\lambda_1 = \lambda_2 = \lambda_3 = -85$, we found

$$\mathbf{H} = \begin{bmatrix} 254.4 \\ 21674 \\ 614125 \end{bmatrix}.$$

Using null initial conditions for the transmitter, and $x_r(0) = -10$, $y_r(0) = 10$, $z_r(0) = -10$ for the receiver, and Euler approximation with step integration of 0.01 for discrete implementation of (6) and (7), with $0 \leqslant u(t) \leqslant 0.1$, the simulations results are shown in Figures 2 and 3.

We further made numerical experiments with gray level images, where the information

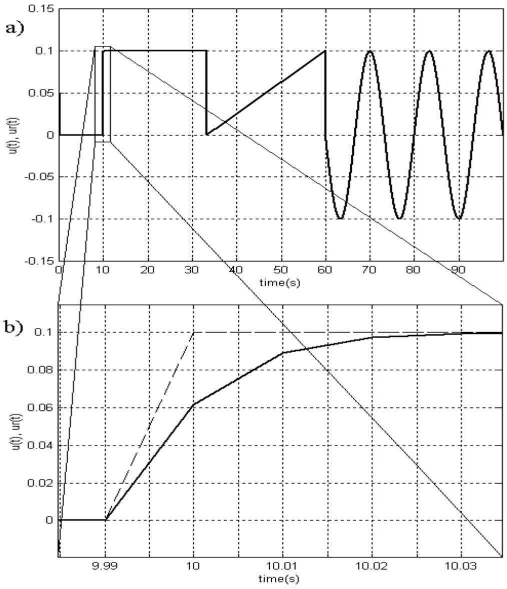

Figure 2: a) Sent $u(t)$ (dashed line) and received $u_r(t)$ (in solid line) signals. b) Zoom around the step: note the time scale.

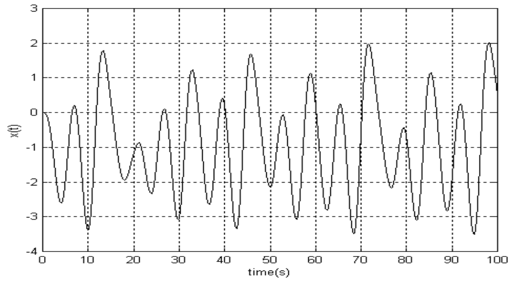

Figure 3: Encrypted signal.

signal $u(t)$ is produced following the intensity variation of the pixels of the images column by column. The encrypted image using image in Fig. 4, is shown in Fig. 5. The decrypted image is illustrated in Fig. 6.

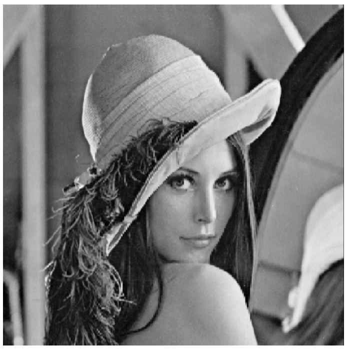

Figure 4: Test gray-level image.

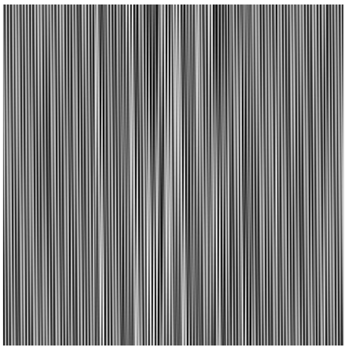

Figure 5: Encrypted image.

The quality of reconstruction can be evaluated by its *MSE* and *PSNR*:

$$MSE \quad = \quad \frac{1}{mn}\sum_{j=0}^{n}\sum_{i=0}^{m}(x_{ij}-\widehat{x_{ij}})^2$$

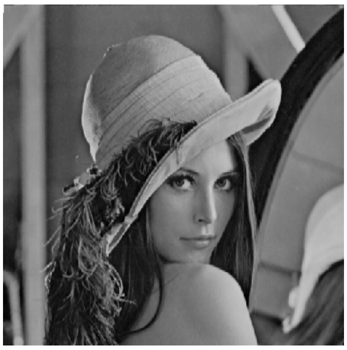

Figure 6: Decrypted image

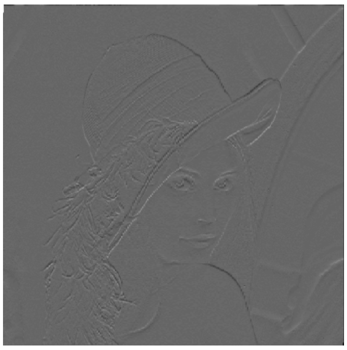

Figure 7: Error image: black means no error

$$PSNR = 10\log\left(\frac{255^2}{MSE}\right)$$

here $MSE = 15$ and $PSNR = 36.4dB$.

To prove robustness with noise in the encrypted image, we contaminated with salt and pepper noise with intensity 0.01 the encrypted image in Fig. 5: result is shown in Fig. 8. The decrypted image is shown in Fig. 9. In this case, $PSNR = 15.9dB$.

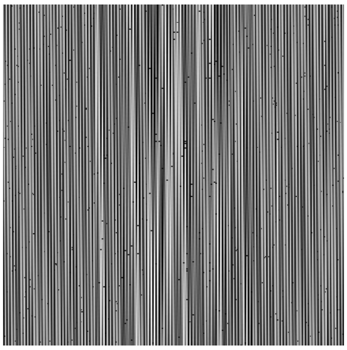

Figure 8: Encrypted image with salt and pepper noise.

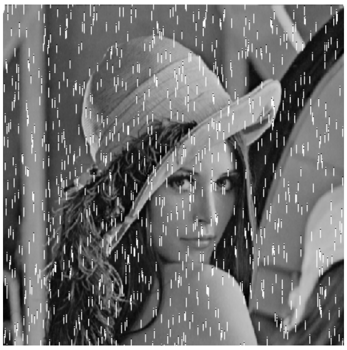

Figure 9: Decrypted image.

5 Conclusion

We have presented a new masking algorithm based on synchronization of chaotic systems. The originality of the method is that its entrance can be a fast varying signal: instead of seeing the emitted signal as ”slow time varying” and using adaptive control theory, we have considered it as ”small valued”. For the synchronization problem, we have used autonomous system theory and applied it on a system introduced in [9]: it proved to be very efficient in synchronization time. In [7] and [3], we can see that synchronizing a step usually lasts seconds, where we obtained times of 1/100s.□□

References

[1] Bai Er-Wei, Lonngren Karl E., and Sprott J.C., “On the synchronization of a class of electronic circuits that exhibit chaos”, *Chaos, Solitons and Fractals,* Vol. 13, pp. 1515-1521, 2002.

[2] Boutayeb M., Darouach M., and Rafaralahy H., “Generalized state-space observers for chaotic synchronization and secure communication”, *IEEE Trans. on Circuits and Systems I*, Vol. 49, pp. 345-349, 2002.

[3] Corron N.J. and Hahs D.W. “A new approach to communications using chaotic signals,”*IEEE Trans. on Circuits and Systems I*, Vol. 44, No. 5, pp. 373-381, 1997.

[4] Cuomo K. M., Oppenheim A.V., and Strogatz S. H. “Synchronization of Lorenz based chaotic circuits with application to communication”, *IEEE Trans. on Circuits and Systems I*, Vol. 40, No. 10, pp. 626-633, 1993.

[5] Domínguez S., Campoy P., Sebastián J.M., and Jímenez A. *Control en el Espacio de Estado.* Prentice Hall, 2002.

[6] Nijmeijer H. and Mareels M.V., ”An observer looks at synchronization, “*IEEE Trans. on Circuits and Systems I”*, Vol. 44, No. 10, pp. 882-890, 1997.

[7] Huijberts H., Nijmeijer H., and Willems R., “System identification in communication with chaotic system”, *IEEE Trans. on Circuits and Systems I,* Vol. 47, No. 6, pp. 800-807, 2000.

[8] Pogromsky A., and Nijmeijer H., “Observer-based robust synchronization of dynamical systems”, *Int. J. of Bifurcation and Chaos*, Vol. 8, No. 11, pp. 2243-2254, 1998.

[9] Sprott J. C., “Simple Chaotic Systems and Circuits” *Am. J. Phys.*, Vol. 68, No. 8, August 2000, pp. 758-763.

[10] Zhong-Ping J., “A note on chaotic secure communication systems”, *IEEE Trans. on Circuits and Systems I,*. Vol. 49, No. 1, pp. 92-96, 2002.