International Journal of Bifurcation and Chaos, Vol. 12, No. 1 (2002) 169–177

EXACT STATE RECONSTRUCTORS IN THE RECOVERY OF MESSAGES ENCRYPTED BY THE STATES OF NONLINEAR DISCRETE-TIME CHAOTIC SYSTEMS*

HEBERTT SIRA-RAMÍREZ
CINVESTAV-IPN, Avenida IPN No. 2508,
Colonia San Pedro Zacatenco, A.P. 14740,
7300 México, D.F., México
hsira@mail.cinvestav.mx

CARLOS AGUILAR IBÁÑEZ† and MIGUEL SUÁREZ-CASTAÑÓN
Laboratorio de Metrología y Control,
Centro de Investigación en Computación del IPN,
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
†*caguilar@pollux.cic.ipn.mx*

Received December 15, 2000; Revised March 20, 2001

In this article we propose the use of nonlinear exact chaotic system state reconstructors for the fast and efficient decoding of multiple discrete-time chaotic encrypted digital messages. Exact state reconstruction features a state estimation error which settles to zero in a finite number of steps. This makes the method specially suitable for chaotic encrypted transmission of digitized files over "noise-free" environments such as the Internet. The method was tested in an actual transmission involving the simultaneous decoding of digitized color images and text files.

1. Introduction

The last decade has witnessed sustained research efforts in the area of chaotic systems synchronization from the work of mathematicians, physicists, computer scientists and control engineers. Many special issues of major scientific journals (see [Special Issues, 1993, 1997a, 1997b, 1999, 2000, 2001]) have been devoted to the problem of chaos, in general, and to synchronization and control of chaotic systems, in particular. Several books exist on the subject (see e.g. [Holden, 1986; Mira, 1987; Afraimovitch *et al.*, 1994; Ott *et al.*, 1994; Chen & Dong, 1998; Fradkov & Pogromsky, 1998; Chen, 1999]). An amazing collection of references on chaotic systems has been gathered by Professor G. Chen in [Chen, 1997] over the years. The interest in the topic of synchronization arises from the possibilities of encoding, or masking, messages using as an analog "carrier" a signal generated as a state, or as an output, of a given chaotic system, called the "transmitter". The effectively random nature of the carrier signal additively, or multiplicatively,

*This research was supported by the Centro de Investigacion y Estudios Avanzados (CINVESTAV-IPN), Mexico, and the Consejo Nacional de Ciencia y Tecnología (CONACYT) under Research Project 32681-A.

nonlinear system with $k \in \{0, 1, 2, \ldots\}$,

$$\begin{aligned} x_{k+1} &= f(x_k), \quad x_k \in R^n, \\ y_k &= h(x_k), \quad y_k \in R \end{aligned} \tag{1}$$

2.1. *Basic assumptions*

(1) We assume that the strings of obtained outputs, prior to $k = 0$, are known from the time $(1-n)$ on. In other words, the output values, y_k for $1 - n < k < 0$ are known, or available for use.

(2) The system (1) is assumed to be locally *observable* around a certain equilibrium point (x_e, y_e). This means that the Jacobian matrix

$$\frac{\partial\{y_k, y_{k+1}, \cdots, y_{k+(n-1)}\}}{\partial x_k} \tag{2}$$

evaluated at the constant equilibrium point (x_e, y_e) has a full column rank n, for all k.

(3) It is assumed that, given a particular equilibrium value, y_e of the output vector, there exists a unique state vector x_e such that the relations, $x_e = f(x_e)$, $y_e = h(x_e)$ are satisfied.

2.2. *Notation*

We use the delay operator δ to express the fact that $\delta\phi_k = \phi_{k-1}$, and, correspondingly, the *advance* operator is denoted by δ^{-1}. The expression, $\delta^{-\mu}\phi_k$, for any positive μ, stands for the identity $\delta^{-\mu}\phi_k = \phi_{k+\mu}$ and, similarly, $\delta^{\mu}\phi_k = \phi_{k-\mu}$. The underlined symbol δ, as in, $\underline{\delta}^{\mu}\phi_k$, stands for the collection: $\{\phi_{k-1}, \phi_{k-2}, \ldots, \phi_{k-\mu}\}$, i.e. $\underline{\delta}^{\mu}\phi_k = \{\delta\phi_k, \ldots, \delta^{\mu}\phi_k\}$. Evidently, $\delta^0 = \underline{\delta}^0 = \mathrm{Id}$ and $\underline{\delta}^1 = \delta$. On the other hand, $\underline{\delta}^{-\mu}\phi_k$ stands for the collection, $\{\phi_k, \phi_{k+1}, \ldots, \phi_{k+\mu}\} = \{\phi_k, \delta^{-1}\phi_k, \ldots, \delta^{-\mu}\phi_k\}$.

Note that the system equation (1) is equivalent to: $x_k = \delta f(x_k) = f(\delta x_k) = f(x_{k-1})$. Since, in turn, one may write $x_{k-1} = f(x_{k-2}) = f(\delta x_{k-1}) = f(\delta^2 x_k)$, it is clear that $x_k = f(f(\delta^2 x_k))$. We denote this last quantity by $f^{(2)}(\delta^2 x_k)$. The expression $f^{(\mu)}(\delta^{\mu} x_k)$, for $\mu > 0$, should be clear from the recursion:

$$\begin{aligned} f^{(i)}(\delta^i x_k) &= f(f^{(i-1)}(\delta^{i-1} x_k)) \\ f^{(1)}(\delta x_k) &= f(\delta x_k) \end{aligned} \tag{3}$$

The operators δ and $\underline{\delta}$ satisfy the following relation

$$\delta^i \underline{\delta}^{-i}\phi_k = \{\phi_k, \underline{\delta}^i \phi_k\} \tag{4}$$

Similar expressions may be defined for the advances of states.

$$\begin{aligned} x_{k+1} &= \delta^{-1} x_k = f(x_k) = f^{[1]}(x_k) \\ x_{k+2} &= \delta^{-2} x_k = f(f(x_k)) = f^{[2]}(x_k) \\ x_{k+3} &= f(f^{[2]}(x_k)) = f^{[3]}(x_k) \\ &\vdots \\ x_{k+i} &= f^{[i]}(x_k) \end{aligned} \tag{5}$$

We set

$$f^{[0]}(x_k) = x_k$$

2.3. *An exact state reconstructor based on delayed output values*

Using the system state equation in (1) in an iterative fashion, one finds:

$$\begin{aligned} x_k &= \delta f(x_k) = f(\delta x_k) \\ x_k &= f(\delta(f(\delta x_k))) = f(f(\delta^2 x_k)) \\ &= f^{(2)}(\delta^2 x_k) \\ &\vdots \\ x_k &= f^{(n-1)}(\delta^{n-1} x_k) \end{aligned} \tag{6}$$

The elements in a finite sequence of advances of the output signal, y_k, are found to be given by,

$$\begin{aligned} y_k &= h(x_k) = h(f^{[0]}(x_k) \\ y_{k+1} &= \delta^{-1} h(x_k) = h(\delta^{-1} x_k) = h(f(x_k)) \\ &= (h \circ f^{[1]})(x_k) \\ y_{k+2} &= \delta^{-1}(h \circ f(x_k)) = h(\delta^{-1} f(x_k)) \\ &= h(f(f(x_k))) \\ &= (h \circ f^{[2]})(x_k) \\ &\vdots \\ y_{k+(n-1)} &= (h \circ f^{[n-1]})(x_k) \end{aligned}$$

The following proposition shows that an observable system is constructible.

Proposition 2.1. *Let the nonlinear chaotic system, $x_{k+1} = f(x_k)$, $y_k = h(x_k)$ be locally observable, and suppose that corresponding to the constant value, y_e, there exists a unique state vector equilibrium value, x_e. Then, the system is* constructible, *i.e. there exists a map $\varphi : R^n \to R^n$*

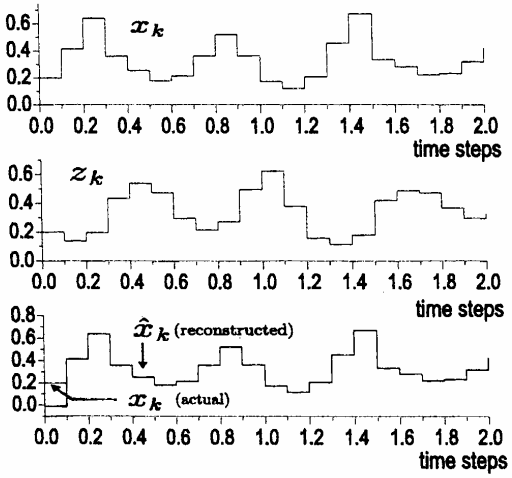

Fig. 1. Exact state reconstruction for the Parasitoid–Host system.

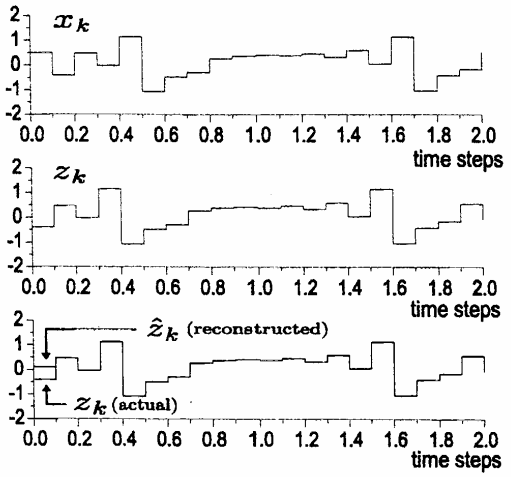

Fig. 2. Exact state reconstruction for the Lozi system.

Figure 1 shows the state evolution of the system and the exactly reconstructed state trajectory for x_k using the, arbitrarily initialized, state reconstructor (18). The initial states of the system were set to be $x_0 = 0.2$ and $z_0 = 0.2$. The parameter a in the system was chosen as: $a = 3.45$. The state reconstructor (18) was arbitrarily initialized with $y_{-1} = z_{-1} = 1$. The time step was set to 0.1.

3.2. *A Lozi system*

Consider the chaotic system, known as the *Lozi* system (see [Chen & Dong, 1993]),

$$\begin{aligned} x_{k+1} &= z_k \\ z_{k+1} &= -P|z_k| + Qx_k + 1 \\ y_k &= x_k \end{aligned} \tag{19}$$

where y_k represents the output measurement making available the state variable x_k.

The Lozi system is known to exhibit chaotic behavior for the following numerical values of the system parameters: $P = 1.8$ and $Q = 0.4$. The system is globally observable from y_k and given a constant value for $y_k = y_e > 0$ there exists a unique equilibrium point for x and z given by $x_e = z_e = 1/(1 + P - Q)$.

An exact reconstructor for the nonmeasured variable z_k may be trivially obtained, since x is a one step delay of z. However, in order to illustrate the proposed method, we follow the general procedure for obtaining the exact state reconstructor, presented in the proof of Proposition 2.1.

Thus, we first rewrite the system in the delayed form:

$$\begin{aligned} x_k &= z_{k-1} \\ z_k &= -P|z_{k-1}| + Qx_{k-1} + 1 \end{aligned} \tag{20}$$

The output y_k and its first advance, y_{k+1}, are given by: $y_k = x_k$, $y_{k+1} = z_k$. From these two expressions it readily follows, by global invertibility that, $x_k = y_k$ and $z_k = y_{k+1}$. Taking one step delay in these two obtained expressions, one has, $x_{k-1} = y_{k-1}$ and $z_{k-1} = y_k$. These new relations, when substituted in the system equations (20), yield an exact state reconstructor expression for the states of the system,

$$\begin{aligned} x_k &= y_k \\ z_k &= -P|y_k| + Qy_{k-1} + 1 \end{aligned} \tag{21}$$

The exact reconstructor (21) requires the knowledge of the delayed output y_k at time $k - 1$. However, observe that if at the initial instant $k = 0$ the output y_{-1} is not known, or available, then the available information, y_0, yields an exact reconstruction of z_k for all $k \geq 1$. Figure 2 shows the state evolution of the system and the exact reconstructed state z_k for an arbitrarily initialized reconstructor. We set $x_0 = 0.5$ and $z_0 = -0.4$. The reconstructor was initialized with $y_{-1} = x_{-1} = 0$. The time step was chosen to be 0.1.

digital computer program, two independent messages. The original messages consisted of a digitized file of Van Gogh's self portrait and a digitized text message containing a biography note on Van Gogh. The encoding of the messages was carried out using the states z, and, w, of the following unobservable, but constructible, Lozi system,

$$\begin{aligned} x_{k+1} &= z_k \\ z_{k+1} &= -P|z_k| + Qx_k + 1 \\ w_{k+1} &= x_k z_k \\ y_k &= x_k \end{aligned} \tag{22}$$

The exact state reconstructor of the system (22), made available at the remote decoding location, was readily derived to be,

$$\begin{aligned} x_k &= y_k \\ z_k &= -P|y_k| + Qy_{k-1} + 1 \\ w_k &= y_{k-1}(-P|y_{k-1}| + Qy_{k-2} + 1) \end{aligned} \tag{23}$$

The image and text files were chaotically encoded in a byte-by-byte fashion after a simple normalization of the carrier chaotic states by an appropriate constant factor. We thus defined

$$\begin{aligned} I_k &= K_1 z_k + i_k\,; \quad T_k = K_2 w_k + t_k \\ i_k &= I_k - K_1 \hat{z}_k\,; \quad t_k = T_k - K_2 \hat{w}_k \end{aligned} \tag{24}$$

where i_k and t_k represent the kth byte of the image and the text files, respectively. I_k and T_k are the corresponding kth bite of the chaotic encrypted image and text. The factors K_1 and K_2 are suitable normalizing parameters, taken to be both equal to 1000. The reconstructed states $\hat{z}$ and $\hat{w}$ exactly coincide with the original states z and w.

We remark at this point that a *secure* communication is not foreign to our proposed scheme. For this, two evident options are possible: (1) The digitized message signal is first encrypted by means of a sufficiently safe encryption procedure (prime number factorization techniques and the like) and then the already encrypted message is further chaotic encrypted and sent over the channel or (2) once the chaotic encrypted digitized message is ready, as previously described, a second encryption process is carried, via the traditional techniques, before establishing communication. The complete decoding processes at the receiving end, in each case, are carried out in the obvious manner.

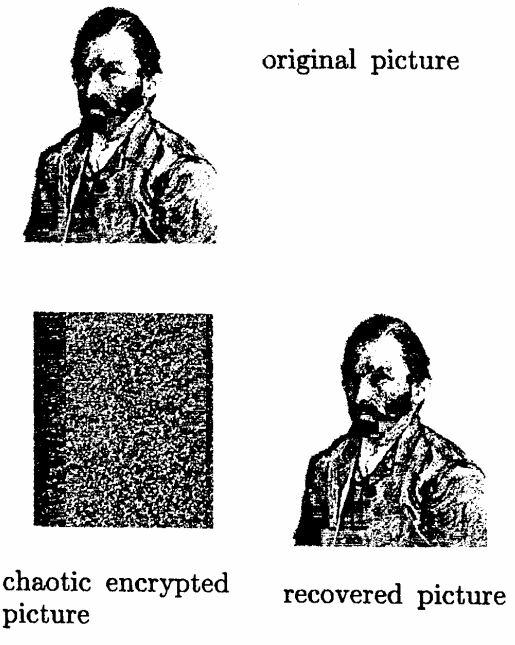

Fig. 4. Original image, chaotic encrypted image and its exact remote reconstruction.

We carried out a computer-based experiment which allowed us to encrypt, transmit, over the internet, and then simultaneously decrypt, at the receiving computer, the digitized image and text files described above. The encryption and decryption programs were written in the C programming language, compiled with Borland C^{++} version 1.01. The encryption program was made to run in a PC equipped with an AMD K6-2-366 Mhz processor. The sizes of the digital image and the text files were of about 120 KB and 1 KB, respectively. The process of encryption was performed in approximately two seconds. We then proceeded to transmit, from our "drive" computer, the signals I_k, T_k along with the chaotic system output signal y_k, through the e-mail facility, to the remote computer, located in a different continent, where the exact state reconstructor program was run. The decoding process also took about two seconds for the two files.

Figure 4 presents the original image, the chaotic encrypted image and the recovered image. Similarly, Fig. 5 depicts a portion of the original text file, the corresponding portion of its chaotic encrypted file and the recovered file.

Chen, G. [1999] *Controlling Chaos and Bifurcations in Engineering Systems* (CRC Press, Boca Raton, FL).

Cuomo, K. M., Oppenheim, A. V. & Strogatz, S. H. [1993] "Synchronization of Lorenz-based chaotic circuits with applications to communications," *IEEE Trans. Circuits Syst. II: Anal. Digit. Sign. Process.* **40**, 626–633.

Fliess, M. [1987] "Quelques Remarques sur les Observateurs non Lineaires," *11*$^{\text{eme}}$ *Colloque GRETSI sur le Traitement du Signal et des Images*, Nice, June 1–5.

Fradkov, A. L. & Markov, A. Yu. [1997] "Adaptive synchronization of chaotic systems based on speed gradient method and passification," *IEEE Trans. Circuit Syst. I: Fundamental Th. Appl.* **44**(10), 905–917.

Fradkov, A. L. & Pogromsky, A. Yu. [1998] *Introduction to Control of Oscillations and Chaos*, World Scientific Series on Nonlinear Science, Series A, Vol. 35 (World Scientific, Singapore).

Holden, A. V. [1986] *Chaos* (Princeton University Press, NJ).

Ląwerier, H. A. [1986] "Two dimensional iterative maps," in *Chaos*, ed. Holden, A. V. (Princeton University Press, NJ), Chapter 4.

Millerioux, G. & Mira, C. [1998] "Coding scheme based on chaos synchronization from non-invertible maps," *Int. J. Bifurcation and Chaos* **10**(10), 2019–2029.

Mira, C. [1987] *Chaotic Dynamics* (World Scientific, Singapore).

Nijmeijer, H. & Mareels, M. Y. [1997] "An observer looks at synchronization," *IEEE Trans. Circuits Syst. I: Fundamental Th. Appl.* **44**(10), 882–890.

Ott, E., Sauer, T. & Yorke, J. A. (eds.) [1994] *Coping with Chaos: Analysis of Chaotic Data and the Exploitation of Chaotic Systems* (Wiley Interscience, NY).

Parker, T. S. & Chua, L. O. [1987] "Chaos: A tutorial for engineers," *Proc. IEEE* **75**, 982–1008.

Pogromsky, A. Yu. [1998] "Passivity-based design of synchronizing systems," *Int. J. Bifurcation and Chaos* **8**(2), 295–319.

Sira-Ramírez, H. & Cruz-Hernández, C. [2000] "Synchronization of chaotic systems: A Hamiltonian systems approach," *Int. J. Bifurcation and Chaos* **11**(5), 1381–1395.

Special Issue [1993] "Chaos synchronization and control: Theory and applications," *IEEE Trans. Circuits Syst. I: Fundamental Th. Appl.* **40**.

Special Issue [1997a] *Syst. Contr. Lett.* **31**.

Special Issue [1997b] "Chaos synchronization and control: Theory and applications," *IEEE Trans. Circuits Syst. I: Fundamental Th. Appl.* **44**(10).

Special Issue [1999] "Communications, information processing and control using chaos," *Int. J. Circuits Th. Appl.* **28**(6).

Special Issue [2000] "Control and synchronization of chaos," *Int. J. Bifurcation and Chaos* **10**(4).

Special Issue [2001] "Application of chaos in modern communication systems," *IEEE. Trans. Circuits Syst.*

Tresser, C. & Worfolk, P. [1997] "Chaotic signal masking with arbitrarily fine recovery," *Appl. Math. Lett.* **10**(5), 103–106.