Proceedings of the 1998 IEEE
International Conference on Control Applications
Trieste, Italy 1-4 September 1998

TP06

Observers for hyperchaos synchronization with application to secure communications

Saverio Mascolo, Member, IEEE
Dipartimento di Elettrotecnica ed Elettronica
Politecnico di Bari
Via Orabona 4, 70125 Bari, Italy
mascolo@poliba.it

Giuseppe Grassi, Member, IEEE
Dipartimento di Matematica
Università di Lecce
73100 Lecce, Italy
grassi@ingle01.unile.it

Abstract

In this paper hyperchaos synchronization is restated as a nonlinear observer design issue. This approach leads to a systematic tool, which guarantees synchronization of a wide class of hyperchaotic systems via a *scalar* signal. By exploiting this result, we propose to combine conventional *cryptographic* methods and *synchronization* of chaotic circuits to design hyperchaos-based cryptosystems. This makes a new contribution to the development of communication systems with higher security.

1. Introduction

In the last few years several researchers have focused their attention on the problems related to the synchronization of chaotic systems [1]-[7]. Since chaos is characterized by a sensitive dependence on initial conditions, one could conclude that synchronization is not obtainable. This because even infinitesimal change will eventually result in divergence of nearby starting orbits [1]. In order to overcome this drawback, different methods have been proposed [1]-[3]. In particular, the scheme suggested by Carroll and Pecora [2] consists in taking a chaotic system, duplicating some subsystem and driving the duplicate and the original subsystem with signals from the unduplicated part. When all the Lyapunov exponents of the driven subsystem (response system) are less than zero, the response system synchronizes with the drive system if both systems start in the same basin of attraction [2]. However, most of the developed methods concern with the synchronization of low dimensional systems characterized by only one positive Lyapunov exponent. Since this feature limits the complexity of the chaotic dynamics, the adoption of higher dimensional chaotic systems has been proposed for secure communications [4]. In fact, the presence of more than one positive Lyapunov exponent clearly improves security by generating more complex dynamics [8].

However, the utilization of more complex dynamics raises the question of whether synchronization can still be achieved by transmitting a scalar signal [4]. Referring to this topic, a method has been developed in [6], which enables hyperchaos synchronization to be achieved in a systematic way by using a scalar signal. The technique proposed in [6] is based on nonlinear observer design and has several advantages over the existing methods. In particular, it can be successfully applied to a wide class of hyperchaotic systems and it does not require the computation of any Lyapunov exponent in order to verify synchronization.

In this paper, the synchronization approach illustrated in [6] is applied to design secure communications systems. In particular, by exploiting the recent result proposed in [9], the idea is to combine conventional cryptographic methods and synchronization of chaotic systems to design hyperchaos-based cryptosystems. This objective is achieved by designing the decrypter as a nonlinear observer for the state of the encrypter. The message signal is recovered at the decrypter by exploiting the synchronization properties of the proposed method. The advantage of the approach developed herein is that the effectiveness of the communication scheme is enhanced, since both the adoption of hyperchaotic systems and the increased complexity of the transmitted signal enable to overcome the low-security objections against low-dimensional chaos-based schemes [8], [9].

2. Observer design for hyperchaos synchronization

Given two hyperchaotic systems, the dynamics of which are described by the following two sets of differential equations:

$$\dot{x} = Ax + b\,f(x) + c \tag{1}$$

$$\dot{y} = Ay + b\,f(y) + c \tag{2}$$

0-7803-4104-X/98/$10.00 ©1998 IEEE

where $x \in \Re^n$, $y \in \Re^n$, $A \in \Re^{n \times n}$, $b \in \Re^n$, $c \in \Re^n$ and $f : \Re^n \to \Re$ is a nonlinear vector field, systems (1) and (2) are said to be synchronized if $e(t) = (y(t) - x(t)) \to 0$ as $t \to \infty$ where e represents the synchronization error [1]. It is worth noting that equation (1) represents a wide class of hyperchaotic systems [6]. In particular, this class includes Rössler's system [6], Matsumoto-Chua-Kobayashi circuit [10], the oscillators reported in [11]-[13] and the n-dimensional Chua's circuit in [14].
In order to obtain synchronization, system (2) has to receive a proper synchronizing signal from system (1). This signal is assumed to be scalar when secure communications systems have to be designed [4], [8]. From a control theory point of view, the synchronizing signal can be considered as an observed quantity feeding a nonlinear observer for the state x of the system (1) [6]-[7]. More precisely, given the dynamic system (1) with the scalar output $z = s(x) \in \Re$, the dynamic system

$$\dot{y} = Ay + b\, f(y) + c + g(z - s(y)) \tag{3}$$

is said to be a nonlinear observer of system (1) if $(y-x) \to 0$ as $t \to \infty$, where $g : \Re \to \Re^n$ is a suitably chosen nonlinear function [12]. Moreover, system (3) is said to be a *global* observer of system (1) if $(y-x) \to 0$ as $t \to \infty$ for any initial condition $y(0)$, $x(0)$ [6]. This means that the error system derived from (3) and (1) has a globally asymptotically stable equilibrium point for $e=0$.

Proposition 1: Given the dynamic system (3), let

$$z = s(x) = f(x) + kx \tag{4}$$

be the scalar synchronizing signal with

$$k = [k_1, k_2, \ldots k_n] \in \Re^{1 \times n}$$

and let

$$g(s(x) - s(y)) = b \cdot (s(x) - s(y)) \tag{5}$$

be the function g.
Then the error system derived from (3) and (1) is linear time-invariant and can be expressed as:

$$\dot{e} = Ae - bke = Ae + bu \tag{6}$$

where $u = -ke$ plays the role of a state feedback.

Proof: From (3) and (1) it follows that:

$$\begin{aligned} \dot{e} &= Ay + bf(y) + c + b(s(x) - s(y)) - (Ax + bf(x) + c) \\ &= Ae + b(f(y) - f(x)) + b(f(x) + kx - f(y) - ky) \\ &= Ae - bke = Ae + bu. \end{aligned}$$

Now, by exploiting linear control theory [6], [15], the following result can be stated.

Proposition 2: A necessary and sufficient condition for the existence of a feedback gain vector k such that system (3) becomes a global observer of system (1) is that all the uncontrollable eigenvalues of the error system (6), if any, have negative real parts.

Proof: For system (6) a coordinate transformation $e = [T_1 \;\; T_2]\bar{e}$ can be found, so that the Kalman controllable canonical form is obtained [15]:

$$\begin{aligned} \begin{bmatrix} \dot{\bar{e}}_c \\ \dot{\bar{e}}_{nc} \end{bmatrix} &= \begin{bmatrix} T_1^T A T_1 & T_1^T A T_2 \\ 0 & T_2^T A T_2 \end{bmatrix} \begin{bmatrix} \bar{e}_c \\ \bar{e}_{nc} \end{bmatrix} + \begin{bmatrix} T_1^T b \\ 0 \end{bmatrix} u \\ &= \begin{bmatrix} \bar{A}_c & \bar{A}_{12} \\ 0 & \bar{A}_{nc} \end{bmatrix} \begin{bmatrix} \bar{e}_c \\ \bar{e}_{nc} \end{bmatrix} + \begin{bmatrix} \bar{b}_c \\ 0 \end{bmatrix} u \end{aligned} \tag{7}$$

where the eigenvalues of $\bar{A}_c$ can be placed anywhere by $u = -ke$, whereas the eigenvalues of $\bar{A}_{nc}$ are not affected by the introduction of any state feedback. Therefore a necessary and sufficient condition to globally asymptotically stabilize system (6) is that the eigenvalues of $\bar{A}_{nc}$ lie in the left half plane [6], [15]. Since $\bar{e} \to 0$ implies $e \to 0$, this completes the proof.

3. Application to secure communications

The synchronization approach illustrated in Section 2 can be applied to design secure communications systems. Referring to the idea proposed in [8]-[9], it is possible to combine conventional cryptographic methods and synchronization of chaotic systems to design hyperchaos-based cryptosystems. A block diagram illustrating the proposed approach is reported in Fig. 1. The encrypter consists of a chaotic system and an encryption function $e_{en}(p(t), K(t))$, which is used to encrypt the message signal $p(t)$ by means of the chaotic key $K(t)=K(x(t))$ [9]. The encrypted signal is fed back to the chaotic system as follows

$$\dot{x} = Ax + b\left(f(x) + e_{en}(t)\right) + c$$

whereas the transmitted signal is

$$z(t) = f(\mathbf{x}) + \sum_{i=1}^{n} k_i x_i + e_{en}(t)$$

The decrypter consists of a chaotic system and a decryption function, which is able to recover the message signal by means of the reconstructed chaotic key $\tilde{K}(t)$. When the decrypter and the encrypter are synchronized, that is $\mathbf{x}(t) \to y(t)$, it results

$$\left(\tilde{K}(t) = K(y(t))\right) \to \left(K(\mathbf{x}(t)) = K(t)\right)$$

$$\left(z(t) - f(y) - \sum_{i=1}^{n} k_i y_i\right) = \tilde{e}_{en}(t) \to e_{en}(t).$$

As a consequence, the decryption function d enables to recover the message signal $p(t)$ since

$$\left(d(\tilde{e}_{en}(t), \tilde{K}(t)) = \tilde{p}(t)\right) \to \left(d(e_{en}(t), K(t)) = p(t)\right).$$

In order to implement the proposed secure communication system, the Matsumoto-Chua-Kobayashi circuit [10] is used (see Fig. 2). This circuit has been the first experimental observation of hyperchaos from a real physical system. By considering the parameters and the equations reported in [13], the dynamics of the circuit can be written as

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \end{bmatrix} = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0.7 & 0 & 0 \\ 0 & 0 & 0 & -10 \\ 0 & 0 & 1.5 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} + \begin{bmatrix} -1 \\ 0 \\ 10 \\ 0 \end{bmatrix} g(x_1, x_3) \tag{8}$$

where

$$g(x_1, x_3) = \begin{cases} -0.2 + 3(x_1 - x_3 + 1) & x_1 - x_3 < -1, \\ -0.2(x_1 - x_3) & -1 \le x_1 - x_3 \le 1, \\ -0.2 + 3(x_1 - x_3 - 1) & x_1 - x_3 > 1. \end{cases}$$

In order to encrypt the message signal $p(t) = \sin t$, an n-shift cipher [9] is chosen

$$e_{en}(t) = f_1(\cdots f_1(f_1(p(t), K(t)), K(t)), \cdots, K(t)) \tag{9}$$

where the following nonlinear function

$$f_1(x, K) = \begin{cases} (x + K) + 2h & -2h \le (x + K) \le -h, \\ (x + K) & -h < (x + K) < h, \\ (x + K) - 2h & h \le (x + K) \le 2h. \end{cases} \tag{10}$$

is recursively used for the encryption, with h=3, n=30 and $K(t) = x_4(t)$.

By exploiting the proposed synchronization approach, encrypter and decrypter must be designed as follows

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \end{bmatrix} = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0.7 & 0 & 0 \\ 0 & 0 & 0 & -10 \\ 0 & 0 & 1.5 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} + \begin{bmatrix} -1 \\ 0 \\ 10 \\ 0 \end{bmatrix} \left(g(x_1, x_3) + e_{en}(t)\right) \tag{11}$$

$$\begin{bmatrix} \dot{y}_1 \\ \dot{y}_2 \\ \dot{y}_3 \\ \dot{y}_4 \end{bmatrix} = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0.7 & 0 & 0 \\ 0 & 0 & 0 & -10 \\ 0 & 0 & 1.5 & 0 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} + \begin{bmatrix} -1 \\ 0 \\ 10 \\ 0 \end{bmatrix} g(y_1, y_3) + \begin{bmatrix} -1 \\ 0 \\ 10 \\ 0 \end{bmatrix} \left(z - g(y_1, y_3) - \sum_{i=1}^{4} k_i y_i\right) \tag{12}$$

where the hyperchaotic transmitted signal

$$z(t) = g(x_1, x_3) + \sum_{i=1}^{4} k_i x_i + e_{en}(t) \tag{13}$$

hides the encrypted signal $e_{en}(t)$, which in turn hides the message signal $p(t)$. From (12) and (11) it is easy to derive the following linear time-invariant error system

$$\begin{bmatrix} \dot{e}_1 \\ \dot{e}_2 \\ \dot{e}_3 \\ \dot{e}_4 \end{bmatrix} = \left(\begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0.7 & 0 & 0 \\ 0 & 0 & 0 & -10 \\ 0 & 0 & 1.5 & 0 \end{bmatrix} - \begin{bmatrix} -1 \\ 0 \\ 10 \\ 0 \end{bmatrix} \begin{bmatrix} k_1 & k_2 & k_3 & k_4 \end{bmatrix} \right) \begin{bmatrix} e_1 \\ e_2 \\ e_3 \\ e_4 \end{bmatrix} \tag{14}$$

Since the controllability matrix of (14) is full rank, the decrypter (12) becomes a global observer of the encrypter (11) by a suitable choice of the vector $\mathbf{k}$. For instance, the choice $k_1 = -0.3764$, $k_2 = 0.2384$, $k_3 = 0.4324$ $k_4 = -0.4314$ places the eigenvalues of (14) in -1. As a consequence, synchronization is

achieved and the method succeeds in generating the desired cryptosystem.
By considering the encrypted signal recovered by the decrypter

$$\tilde{e}_{en}(t) = z - g(y_1, y_3) - \sum_{i=1}^{4} k_i y_i \qquad (15)$$

and by using the recovered key $\tilde{K}(t) = y_4(t)$, the following message signal is retrieved

$$\tilde{p}(t) = f_1\left(\cdots f_1\left(f_1\left(\tilde{e}_{en}(t), -\tilde{K}(t)\right), -\tilde{K}(t)\right), \cdots, -\tilde{K}(t)\right) \qquad (16)$$

where the decryption rule is the same as the encryption one [9]. Since the encrypter and the decrypter are synchronized, it results $y_4(t) \to x_4(t)$, that is, $\tilde{K}(t) \to K(t)$. Moreover, from (13) and (15) it follows that $\tilde{e}_{en}(t) \to e_{en}(t)$, which assures the desired condition

$$\tilde{p}(t) \to p(t).$$

The validity of the proposed secure communications scheme is confirmed by simulation results. In particular, the hyperchaotic transmitted signal (13) is reported in Fig. 3, whereas the recovered message signal (16) is shown in Fig. 4.

4. Conclusions

In this paper conventional cryptographic methods and synchronization of chaotic circuits have been combined in order to design hyperchaos-based secure communications systems. The proposed design technique is systematic and exploits observer design theory. It allows us to design cryptosystems with more complex dynamics, making a further contribution to the development of communication systems with higher security.

5. References

[1] M. Ogorzalek, "Taming chaos-Part I: Synchronization", IEEE Trans. on CAS, part I, vol. 40, no. 10, pp. 693-699, 1993.

[2] T. L. Carroll and L. M. Pecora, "Synchronizing chaotic circuits", IEEE Trans. on CAS, vol. 38, no. 4, pp. 453-456, 1991.

[3] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, "Synchronization of Lorenz-based chaotic circuits with applications to communications", IEEE Trans. on CAS, part II, vol. 40, no. 10, pp. 626-633, 1993.

[4] J. H. Peng, E. J. Ding, M. Ding, and W. Yang, "Synchronizing hyperchaos with a scalar transmitted signal", Physical Review Letters, vol. 76. no. 6, pp. 904-907, 1996.

[5] H. Nijmeijer, "Control of chaos and synchronization", Systems & Control Letters, vol. 31, pp. 259-262, 1997.

[6] G. Grassi and S. Mascolo, "Nonlinear observer design to synchronize hyperchaotic systems via a scalar signal", IEEE Trans. on CAS, part I, Special issue on "Chaos Synchronization, Control and Applications", vol. 44, no. 10, 1997.

[7] H. Nijmeijer and I. M. Y. Mareels, "An observer looks at synchronization", IEEE Trans. on CAS, part I, Special Issue on Chaos Synchronization, Control and Applications, vol. 44, no. 10, pp. 882-890, 1997.

[8] T. Yang and L. O. Chua, "Impulsive control and synchronization of nonlinear dynamical systems and application to secure communication", Int. J. Bifurcation Chaos, vol. 7, no.3, pp. 645-664, 1997.

[9] T. Yang, C. W. Wu and L. O. Chua, "Cryptography based on chaotic systems", IEEE Trans. on CAS, part I, vol. 44, no. 5, pp. 469-472, 1997.

[10] T. Matsumoto, L. O. Chua, and K.Kobayashi, "Hyperchaos: laboratory experiment and numerical confirmation", IEEE Trans. on CAS, vol. 33, no. 11, pp. 1143-1147, 1986.

[11] A. Tamasevicius, A. Namajunas, and A. Cenys, "Simple 4D chaotic oscillator", IEE Electronics Letters, vol. 32, no. 11, pp. 957-958, 1996.

[12] A. Tamasevicius, A. Cenys, G. Mykolaitis, A. Namajunas and E. Lindberg, "Hyperchaotic oscillators with gyrators", IEE Electronics Letters, vol. 33, no. 7, pp. 542-544, 1997.

[13] A. Tamasevicius, "Hyperchaotic circuits: state of the art", Proc. Fifth Int. Workshop on Nonlinear Dynamics of Electronic Systems (NDES '97), Moscow, Russia, pp. 97-102, 1997.

[14] M. Gotz, U. Feldmann, and W. Schwarz, "Synthesis of higher dimensional Chua circuits", IEEE Trans. on CAS, part I, vol. 40, no. 11, pp. 854-860, 1993.

[15] C. T. Chen, "Linear system theory and design", Holt, Rinehart and Winston, 1984.

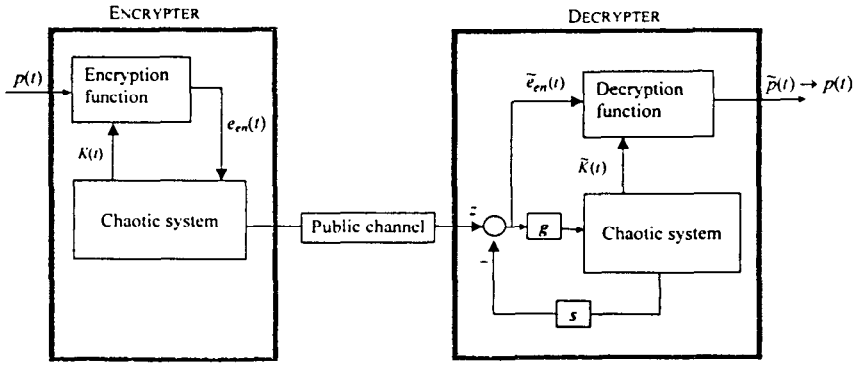

Fig. 1 A block diagram illustrating the proposed secure communications scheme.

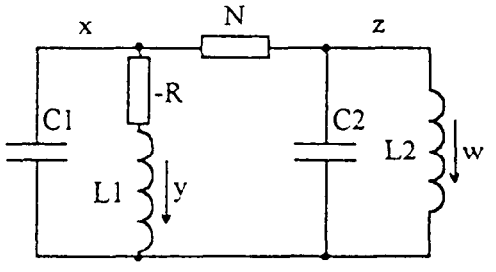

Fig. 2 The Matsumoto-Chua-Kobayashi circuit.

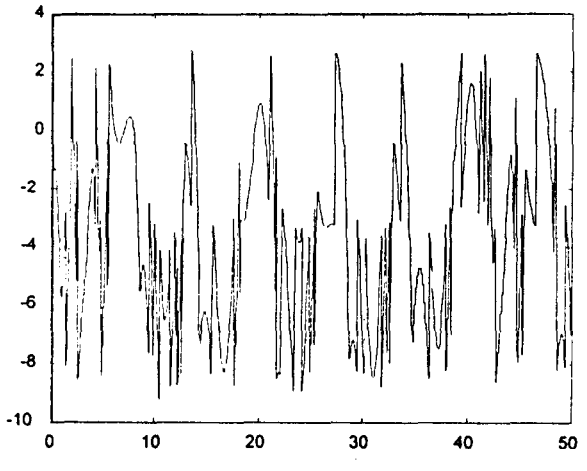

Fig. 3 Time waveform of the transmitted signal (13).

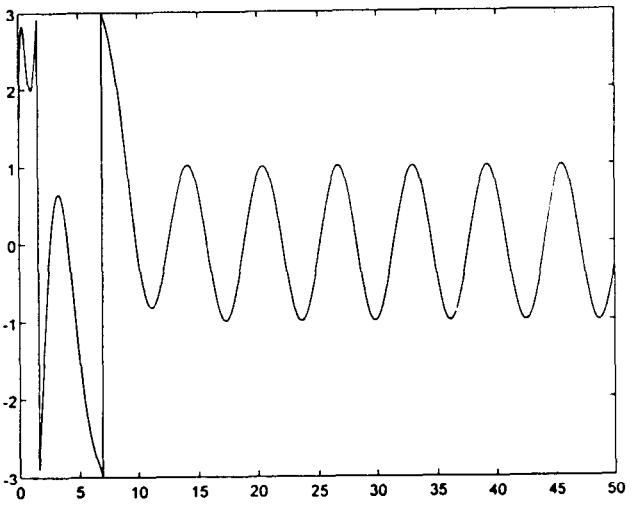

Fig. 4 Time waveform of the message signal (16)