HYPERCHAOTIC CIRCUITS FOR SECURE COMMUNICATIONS: AN EFFICIENT SYNCHRONIZATION TECHNIQUE

Michele BRUCOLI, Donato CAFAGNA, Leonarda CARNIMEO, Giuseppe GRASSI †

Dipartimento di Elettrotecnica ed Elettronica - Politecnico di Bari
Via E. Orabona, 4 - 70125 Bari (Italy) - E-Mail: brucoli@poliba.it

† *Dipartimento di Matematica - Università di Lecce - 73100 Lecce (Italy)*

***Abstract* - In this paper an efficient method is illustrated to obtain a secure communication system by means of the synchronization of hyperchaotic circuits. The approach consists in driving the receiver with a proper number of transmitted signals, each of them constituted by a chaotic masking waveform added of an information-bearing signal, and by keeping the transmitting system equivalent to the receiving one by means of a feedback technique. The suggested method assures a recovery of the information signals without degradation, and enhances the security of the communication scheme, since the utilization of several driving signals makes more difficult for an undesirable listener to synchronize with the transmitter. Simulation results are reported to confirm the capability of the proposed approach.**

1. INTRODUCTION

In recent years several methodologies for synchronizing chaotic circuits in secure communications have been developed [1-5]. These techniques are based on a chaotic masking scheme. In fact, since chaotic signals are broadband noiselike waveforms, very difficult to predict, they represent an attractive tool for masking information-bearing signals. The receiver, after synchronizing with the transmitter, recovers the information signal. By analyzing the different methods that have been developed for synchronizing chaotic circuits in secure communications, the techniques proposed by Wu and Chua [3] and by Milanovic and Zaghloul [5] reveal particularly interesting. Namely, to overcome the problem deriving from the inherent sensitivity of chaotic systems to perturbations, in [3] and [5] each transmitter is kept equivalent to its corresponding receiver by feeding the transmitted signal back to the transmitter. In this way, a perfect synchronization between transmitter and receiver is achieved. It should be observed that, since the systems adopted in [1-5] are characterized by only one positive Lyapunov exponent and by a dynamics of a limited complexity, this feature can represent a restriction in the field of secure communication applications [2, 6]. Following these considerations, the idea underlying this paper consists in improving the technique developed in [3, 5] by exploiting the more complex dynamics of hyperchaotic circuits. In fact, in this case, a further possibility of signal masking is provided due to the availability of more than one chaotic signal [7]. Namely, a circuit exhibiting a hyperchaotic behaviour (transmitter) is duplicated to generate a receiver, driven by a proper number of transmitted signals, each of them constituted by a chaotic masking waveform added of an information-bearing signal. The transmitter is kept equivalent to the receiver by using the above mentioned feedback technique. The information signals are completely recovered without degradation, as the suggested method provides a linear, autonomous, globally asymptotically stable error dynamics. It should be observed that hyperchaotic synchronization, instead of chaotic one, enhances the security of the communication scheme, as the utilization of several drive signals makes more difficult for an undesirable listener to synchronize with the transmitter.

The suggested approach is applied to a pair of bidirectionally coupled Chua's circuits. Simulation results are reported to confirm the validity of the proposed approach.

2. SECURE COMMUNICATIONS VIA SYNCHRONIZATION OF HYPERCHAOTIC CIRCUITS

A method is illustrated to obtain a secure communication system by means of the synchronization between all the state variables of hyperchaotic circuits. To this purpose, an n-dimensional circuit exhibiting a hyperchaotic behaviour is considered, the dynamics of which is described by the following system of equations:

$$\dot{x} = h(x) \qquad (1)$$

where $x(t) = [x_1, x_2, \ldots, x_n]^T \in \mathbb{R}^n$ is the state vector and $h = [h_1(x), h_2(x), \ldots, h_n(x)]^T \in \mathbb{R}^n$. Following the considerations reported in [3], it is assumed that system (1) can be rewritten as

$$\dot{x} = Ax + g(x_d) \qquad (2)$$

where the matrix $A \in \mathbb{R}^{nxn}$ has all its eigenvalues in the open left half plane, and $x_d \in \mathbb{R}^d$ is a subvector of x representing the vector of the chaotic signals to be used as driving variables. Note that $x_d = Nx$, where $N \in \mathbb{R}^{dxn}$ is a proper matrix. By introducing the concept of master and slave systems characterized by the same functional form [3], the following drive-response system is derived:

$$\dot{x} = Ax + g(x_d) \qquad (3a)$$

$$\dot{x}' = Ax' + g(x_d) \qquad (3b)$$

where x and x' are the state vectors of the master and slave systems, respectively.

By defining the vector of the synchronization errors as

$$e = x - x' \qquad (4)$$

and, taking into account eqns.(3), the following equation is obtained [3]:

$$\dot{e} = Ae \qquad (5)$$

Eqn.(5) highlights that the error dynamics is linear and autonomous. Since A has all its eigenvalues in the open left half plane, system (5) is globally asymptotically stable, and, for this reason, $e \to 0$ as $t \to \infty$.

This result can be exploited for the design of secure communication systems. At first, by considering $x_d(t)$ as the vector of the noiselike masking chaotic carriers and by indicating with $s(t) \in \mathbb{R}^d$ the vector of the information-bearing waveforms, the vector of the transmitted signals is

$$w(t) = x_d(t) + s(t) \qquad (6)$$

Now, the equations of the transmitter and the receiver, become, respectively:

$$\dot{x} = Ax + g(w) \qquad (7a)$$

$$\dot{x}' = Ax' + g(w) \qquad (7b)$$

As in [5], the transmitter given by eqn.(7a) is kept equivalent with the receiver given by eqn.(7b) by feeding the transmitted signal $w(t)$ back to the transmitter. A block diagram illustrating the proposed approach is reported in Fig.1.

It should be noted that, with the suggested approach, any perturbation which could desynchronize the circuits is avoided. In fact, the error dynamics assures that the information signal can be completely recovered without any degradation.

3. APPLICATION TO A PAIR OF COUPLED CHUA'S CIRCUITS

The transmitter considered in this work is formed by a pair of bidirectionally coupled Chua's circuits (see Fig.2). This network is, in fact, characterized by the existence of a rich variety of dynamical behaviours [8]. In particular, depending on the choice of circuit parameters, this system can exhibit different types of hyperchaotic attractors as well as chaos-hyperchaos intermittency. The state equations for two bidirectionally coupled Chua's circuits can be expressed as [3]:

$$\dot{x}_c = Ax_c + g(x_d) \qquad (8)$$

where $x_c = [x_1, x_2, \ldots, x_6]^T \in \mathbb{R}^6$, $x_d = [x_1, x_4]^T \in \mathbb{R}^2$ and $g(x_d) = [-f(x_1), 0, 0, -f(x_4), 0, 0]^T \in \mathbb{R}^6$, with

$$A = \begin{bmatrix} -\alpha & \alpha & 0 & 0 & 0 & 0 \\ 1 & (-1-K) & 1 & 0 & K & 0 \\ 0 & -\beta & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -\alpha & \alpha & 0 \\ 0 & M & 0 & 1 & (-1-M) & 0 \\ 0 & 0 & 0 & 0 & -\beta & 0 \end{bmatrix}$$

where, as in [8]:

$$f(x_1) = bx_1 + (a - b)(|x_1+1| - |x_1-1|)/2$$

$$f(x_4) = bx_4 + (a - b)(|x_4+1| - |x_4-1|)/2$$

and α, β, a and b are constants. The parameters K and M individualize the bidirectional coupling between the two Chua's circuits.

Following the method illustrated in Sec.2, eqn.(7a) of the transmitter can be rewritten as:

$$\dot{\boldsymbol{x}}_c = \boldsymbol{A}\boldsymbol{x}_c + \boldsymbol{g}(w) \qquad (9)$$

where $\boldsymbol{g}(w)=[-f(w_1), 0, 0, -f(w_2), 0, 0]^T \in \mathbb{R}^6$. Note that the transmitted signals $w_1(t)$ and $w_2(t)$ are constituted by the chaotic masking signals $x_1(t)$ and $x_4(t)$ added of the information-bearing signals $s_1(t)$ and $s_2(t)$, respectively. Analogous equations hold for the receiver. By choosing $K = M = 0.02$, $\alpha = 10$, $\beta = 14.87$, $a = -1.27$ and $b = -0.68$, the following eigenvalues of the matrix A have been calculated:

$\lambda_1 = -10.89$; $\lambda_2 = -10.88$;

$\lambda_{3/4} = -0.074 \pm j3.69$; $\lambda_{5/6} = -0.055 \pm j3.69$

As all eigenvalues have negative real parts, the error dynamics is globally asymptotically stable, and therefore the synchronization between the transmitter and the receiver is guaranteed.

Numerical computations have been performed using the software Insite [9] and by choosing the following initial conditions: $x_1(0) = 0.010$, $x_4(0)= 0.011$, $x_2(0) = x_3(0) = x_5(0) = x_6(0) = 0$ for the transmitter and $x_1'(0) = 0.011$, $x_4'(0)= 0.012$, $x_2'(0) = x_3'(0) = x_5'(0) = x_6'(0) = 0$ for the receiver. Two sinusoidal waveforms of amplitudes $A_1 = 2.5\text{x}10^{-5}$ and $A_2 = 0.5\text{x}10^{-5}$ and frequencies $f_1 = 15$ Hz and $f_2 = 20$ Hz, respectively, have been used as information-bearing signals. Fig.3 shows the power spectra of the chaotic signal x_1, of the transmitted signal w_1 and of the recovered signal s_{r1}, respectively, whereas the power spectra of x_4, w_2 and s_{r2}, respectively, are reported in Fig.4. It should be noted that identical spectra of x_1 and w_1, and x_4 and w_2, respectively, are obtained and that Figs. 3(b) and 4(b) show that the frequencies of the information signals are fairly good hidden in the transmitted broadband signal. The capability of the proposed technique to recover the original messages is highlighted in Fig. 5. Finally, Fig. 6 shows the time waveforms of the synchronization errors $e_1(t)$ and $e_4(t)$.

4.CONCLUSIONS

In this paper an efficient method has been illustrated to obtain a secure communication system via synchronization of hyperchaotic circuits. The suggested approach, which enhances the security of communication schemes by utilizing more than one driving signal, has been successfully applied to a pair of bidirectionally coupled Chua's circuits. The capability of the proposed method has been illustrated by means of simulation results.

REFERENCES

[1] L. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, and U. Parlitz, "Experimental demonstration of secure communications via chaotic synchronization", *Int. J. of Bifurcation and Chaos* , vol.2, no.3, pp. 709-713, 1992.

[2] K. S. Halle, C. W. Wu, M. Itoh, L. O. Chua, "Spread spectrum communication through modulation of chaos", *Int. J. of Bifurcation and Chaos*, vol.3, no.2, pp.469-477, 1993.

[3] C. W. Wu, and L. O Chua, "A simple way to synchronize chaotic systems with applications to secure communication systems", *Int. J. of Bifurcation and Chaos*, vol.3, no.6, pp.1619-1627, 1993.

[4] R. Lozi, and L. O. Chua, "Secure communications via chaotic synchronization II: noise reduction by cascading two identical receivers", *Int. J. of Bifurcation and Chaos*, vol.3, no.5, pp.1319-1325, 1993.

[5] V. Milanovic, and M. E. Zaghloul, "Improved masking algorithm for chaotic communications systems", *Electronics Letters*, vol.32, no.1, pp.11-12, 1996.

[6] K. M. Cuomo, "Synthesizing self-synchronizing chaotic arrays", *Int. J. of Bifurcation and Chaos*, vol.4, no.3, pp.727-736, 1994.

[7] M. Brucoli, L. Carnimeo, G. Grassi, "A method for the synchronization of hyperchaotic circuits", *Int. J. of Bifurcation and Chaos*, in press.

[8] V. S. Anishchenko, T. Kapitaniak, M. A. Safonova, and O. V. Sosnovzeva, "Birth of double-double scroll attractor in coupled Chua circuits", *Phys. Lett. A* vol.192, pp.207-214, 1994.

[9] T. S. Parker, and L. O. Chua, *Practical numerical algorithms for chaotic systems*, Springer-Verlag, Berlin, 1989.

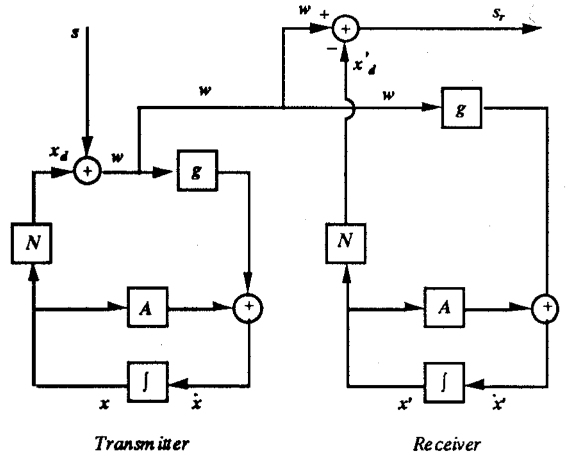

Fig.1. Block diagram illustrating the proposed secure communication system

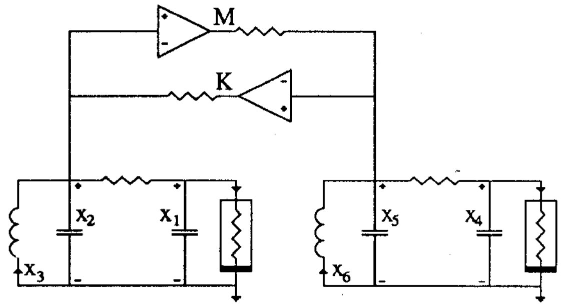

Fig.2. Bidirectionally coupled Chua's circuits

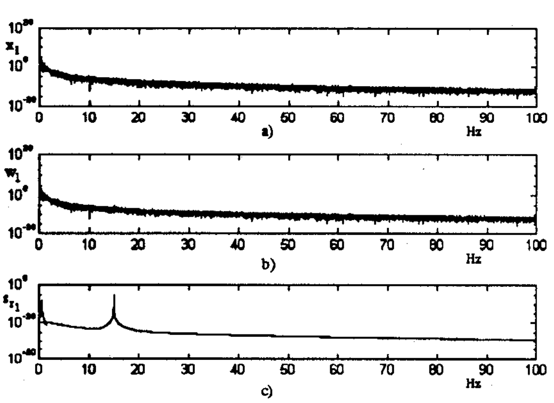

Fig.3. Power spectra:
(a) chaotic signal x_1;
(b) transmitted signal w_1;
(c) recovered signal s_{r1}.

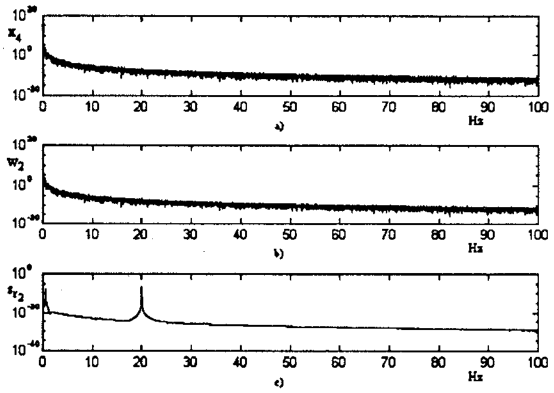

Fig.4. Power spectra:
(a) chaotic signal x_4;
(b) transmitted signal w_2;
(c) recovered signal s_{r2}.

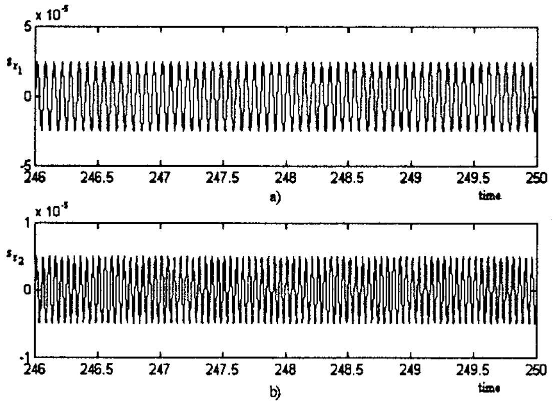

Fig.5. Time waveforms of the recovered signals:(a) s_{r1}; (b) s_{r2}.

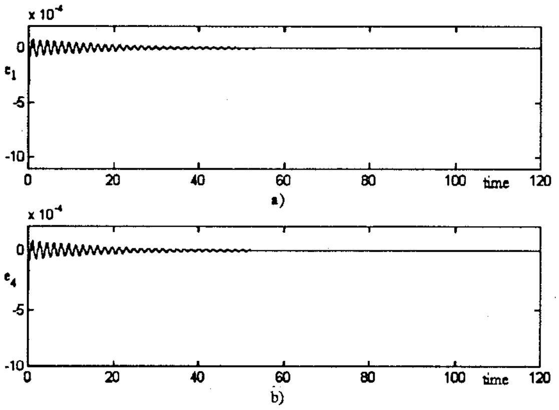

Fig.6. Time waveforms of the synchronization errors:
(a)e_1; (b)e_4.