Letters

International Journal of Bifurcation and Chaos, Vol. 9, No. 10 (1999) 2027–2037

DESIGN OF A HYPERCHAOTIC CRYPTOSYSTEM BASED ON IDENTICAL AND GENERALIZED SYNCHRONIZATION

MICHELE BRUCOLI*, DONATO CAFAGNA and LEONARDA CARNIMEO
Dipartimento di Elettrotecnica ed Elettronica,
Politecnico di Bari Via E. Orabona,
4 – 70124 Bari, Italy

GIUSEPPE GRASSI
Dipartimento di Matematica,
Università di Lecce, 70123 Lecce, Italy

Received July 8, 1998; Revised March 19, 1999

In this paper identical and generalized synchronization and the complex dynamics of hyperchaotic circuits are exploited for designing reliable cryptosystems. Since chaotic additive masking, chaotic switching and chaotic parameter modulation methods can have a low degree of security, an attempt to overcome this drawback is made by utilizing hyperchaotic circuits which make available several chaotic signals. Some of these signals are used to properly synchronize the encrypter and the decrypter in an identical and generalized way. Other chaotic signals are considered for encrypting and decrypting the information messages by means of a multishift cipher scheme. The approach is applied to a communication system constituted by an encrypter and a decrypter each consisting of two coupled Chua's circuits, unidirectionally coupled with two coupled Chua's oscillators. Simulation results are reported to show the performance of the suggested cryptosystem.

1. Introduction

In recent years the synchronization of chaotic circuits has been a topic of great interest. Important contributions can be found in the field of secure communications. In particular, several methods, such as chaotic additive masking [Cuomo *et al.*, 1993], chaotic switching [Parlitz *et al.*, 1992; Dedieu *et al.*, 1993] and chaotic parameter modulation methods [Yang & Chua, 1996a] have been developed. However, recent results have shown that most of these techniques have a low degree of security [Yang *et al.*, 1997; Short, 1996]. In order to overcome this drawback, an interesting method has been developed in [Yang *et al.*, 1997], where a chaos-based cryptosystem is proposed. This approach is different from the traditional cryptographic techniques [Stinson, 1995], in which both the encrypted waveforms and the key signals are transmitted to the receiver. Namely, in [Yang *et al.*, 1997] two chaotic signals, originated by the same system, are considered. One of these signals is used to encrypt the information signal by means of a multishift cipher scheme, the other one is used to synchronize the encrypter and the decrypter.

A further contribution to enhance the level of security of chaos-based communication systems is proposed in this work. More in detail, the limits related to low-dimensional chaotic circuits are overcome by exploiting the potentials of hyperchaotic

*E-mail: brucoli@poliba.it

ones. Moreover, supplementary hyperchaotic subsystems are inserted both at the encrypter and at the decrypter to generate additional and independent key signals. Namely, the state variables to be used as key signals are originated by a subsystem which is different from the one that generates the chaotic variables to be transmitted or received. Figure 1 shows the architecture illustrating the proposed cryptosystem scheme. The presence of supplementary subsystems requires a suitable synchronization between the subsystems within the encrypter and within the decrypter, respectively. To this purpose, the suggested approach exploits the recent concept of generalized synchronization (GS) [Rulkov *et al.*, 1995; Abarbanel *et al.*, 1996; Kocarev & Parlitz, 1996; Yang & Chua, 1996b; Parlitz *et al.*, 1997] between the subsystems which constitute the encrypter and the decrypter, respectively, whereas the more traditional identical synchronization (IS) is adopted between the whole encrypting system and the whole decrypting one. The utilization of the above mentioned supplementary subsystems and the exploitation of generalized synchronization, enhance the level of security of the communication scheme [Parlitz *et al.*, 1997; Short, 1994]. The suggested approach is developed by considering an encrypter and a decrypter, each consisting of two coupled Chua's circuits (the hyperchaotic subsystem) unidirectionally coupled with two coupled Chua's oscillators (the supplementary hyperchaotic subsystem). Numerical examples are presented to show the validity of the proposed technique.

2. A Hyperchaotic Cryptosystem Based on Identical and Generalized Synchronization

2.1. *Hyperchaotic cryptosystem model*

An n-dimensional hyperchaotic circuit is considered, the dynamics of which is described by the following equation:

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}) \tag{1}$$

where $\mathbf{x} = [x_1, \ldots, x_n]^T \in \mathbb{R}^n$ and $\mathbf{f}(\mathbf{x}) = [f_1(\mathbf{x}), \ldots, f_n(\mathbf{x})]^T \in \mathbb{R}^n$.

Taking into account that many physical systems can be described by mathematical models in which the linear and nonlinear parts are separated [Wu & Chua, 1993], Eq. (1) can be written as:

$$\dot{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{g}(\mathbf{x}) \tag{2}$$

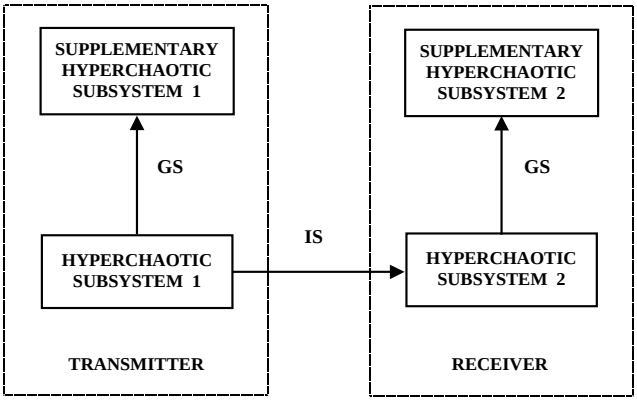


Fig. 1. Architecture of the proposed cryptosystem.

where the nonlinear function $\mathbf{g} : \mathbb{R}^n \to \mathbb{R}^n$ is arranged in such a way that all the eigenvalues of the matrix $A \in \mathbb{R}^{n\times n}$ lie in the open left half-plane.

In order to develop a secure communication system which exploits the synchronization of hyperchaotic circuits, a master–slave system configuration is introduced [Wu & Chua, 1993]:

$$\dot{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{g}(\mathbf{x}) \tag{3a}$$

$$\dot{\mathbf{y}} = \mathbf{A}\mathbf{y} + \mathbf{g}(\mathbf{x}) \tag{3b}$$

where the state vector $\mathbf{x}$ represents the driving signal vector for the response system (3b).

Now, by considering an information signal vector $\mathbf{s}(t) = [s_1(t), \ldots, s_n(t)]^T \in \mathbb{R}^n$ to be transmitted, the vector of the driving signals becomes:

$$\mathbf{w}(t) = \mathbf{x}(t) + \mathbf{s}(t) \tag{4}$$

As a consequence, Eqs. (3) can be rewritten as:

$$\dot{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{g}(\mathbf{w}) \tag{5a}$$

$$\dot{\mathbf{y}} = \mathbf{A}\mathbf{y} + \mathbf{g}(\mathbf{w}) \tag{5b}$$

where Eq. (5b), which represents the receiver, has been kept equivalent to Eq. (5a), by feeding the information signal vector back to the transmitter.

It should be noted that the above illustrated masking technique has a low degree of security as shown by recent results [Yang *et al.*, 1997; Short, 1996]. A way to enhance the level of security of the communication system can consist in applying proper cryptographic techniques to the information signal. To this purpose, basic cryptographic terminology has to be introduced [Stinson, 1995]. The information signal $s_i(t)$ is called *plaintext*, whereas the operation of encoding $s_i(t)$ to hide its

information content is defined *encryption*. The plaintext, coded via an encryption function $c(\cdot, \cdot)$, is named *ciphertext*. The process of retrieving the plaintext from the ciphertext is carried out by means of a decryption function $d(\cdot, \cdot)$. Encryption and decryption are based on the use of the same key function $k(t)$, and a technique of encryption and decryption is called a *cipher method*.

A well known μ-shift cipher technique is defined as [Stinson, 1995]:

$$\mathbf{c}(\mathbf{s}(t), \mathbf{k}(t)) = \mathbf{q}(\ldots \mathbf{q}(\mathbf{q}(\mathbf{s}(t), \mathbf{k}(t)), \mathbf{k}(t)), \ldots, \mathbf{k}(t)) \quad (6)$$

where the vector $\mathbf{q}(\cdot, \cdot)$ is formed by nonlinear functions such as (see Fig. 2):

$$q(z, r) = \begin{cases} (z + r) + 2h_i & -2h_i \le z + r \le -h_i \\ z + r & -h_i < z + r < h_i \\ (z + r) - 2h_i & h_i \le z + r \le 2h_i \end{cases}$$

where z and r are generic time-dependent variables and $h_i (i = 1, \ldots, 6)$ is a real number chosen such that they lie within $(-h_i, h_i)$.

Accordingly, the information signal vector can be recovered by using a decryption function as:

$$\mathbf{s}_r(t) = \mathbf{d}(\mathbf{c}(\mathbf{s}(t), \mathbf{k}(t)) = \mathbf{q}(\ldots \mathbf{q}(\mathbf{q}(\mathbf{c}(\mathbf{s}(t), \mathbf{k}(t)), -\tilde{\mathbf{k}}(t)), -\tilde{\mathbf{k}}(t)), \ldots, -\tilde{\mathbf{k}}(t)) \quad (7)$$

2.2. *Identical and generalized synchronization*

In order to improve the security of the communication scheme the key signals are originated by the state variables of a supplementary system, which is synchronized in the generalized way with the other subsystem within the encrypter. More in detail, GS is considered and, as reported in [Abarbanel *et al.*, 1996] and in [Yang & Chua, 1996b], is applied to the following class of unidirectionally coupled systems:

$$\dot{\mathbf{x}} = \mathbf{h}(\mathbf{x}) \quad (8a)$$

$$\dot{\mathbf{x}}' = \mathbf{h}'(\mathbf{x}', \mathbf{u}(\mathbf{x})) \quad (8b)$$

where $\mathbf{x} \in \mathbb{R}^n$, $\mathbf{x}' \in \mathbb{R}^n$ and the function $\mathbf{u} : \mathbb{R}^n \to \mathbb{R}^m$.

System (8a) is said to be characterized by a generalized synchronization with the system (8b) if there exists a subset $B = (B_x \times B_{x'}) \subset (\mathbb{R}^n \times \mathbb{R}^m)$, a transformation $\tilde{\mathbf{F}}$: $\mathbb{R}^n \to \mathbb{R}^m$ and a manifold $T = \{(\mathbf{x}, \mathbf{x}') : \mathbf{x}' = \tilde{\mathbf{F}}(x)\}$, with $T \subset B$, such that all trajectories of (8a) and (8b), with initial conditions in the basin B, approach T as time goes to infinity [Kocarev & Parlitz, 1996]. If $\tilde{\mathbf{F}}$ equals the identity transformation, GS coincides with the IS.

Now, taking into account Eqs. (8), the encrypter originally represented by Eq. (5a), is modified by introducing a supplementary subsystem characterized by a transformation $\tilde{\mathbf{F}}(\mathbf{x}) = \mathbf{F}(\mathbf{x}, \mathbf{x}')$ for $\mathbf{x}' \in B_{x'}$. As a consequence, the encrypter equations can be written as:

$$\dot{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{g}(\mathbf{w}) \quad (9a)$$

$$\dot{\mathbf{x}}' = \mathbf{A}\mathbf{x}' + \mathbf{g}'(\mathbf{x}') + \mathbf{F}(\mathbf{x}, \mathbf{x}') \quad (9b)$$

In the same way the decrypter, originally represented by Eq. (5b), is now expressed by the equations:

$$\dot{\mathbf{y}} = \mathbf{A}\mathbf{y} + \mathbf{g}(\mathbf{w}) \quad (10a)$$

$$\dot{\mathbf{y}}' = \mathbf{A}'\mathbf{y}' + \mathbf{g}'(\mathbf{y}') + \mathbf{F}(\mathbf{y}, \mathbf{y}') \quad (10b)$$

It should be noted that the transformations $\mathbf{F}(\mathbf{x}, \mathbf{x}')$ and $\mathbf{F}(\mathbf{y}, \mathbf{y}')$ have to be properly chosen in order to assure GS between (9a) and (9b) in the encrypter and between (10a) and (10b) in the decrypter, respectively.

The implementation of the secure communication system requires that the whole receiving system be in IS with the whole transmitting system.

Now, it is very difficult to determine general criteria to assure IS between two generic encrypter

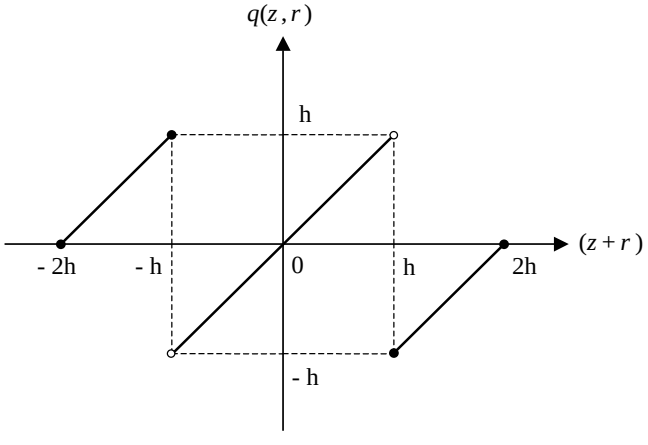


Fig. 2. Nonlinear function used for encryption.

and decrypter. The solution of this problem can be more easily found if a particular cryptosystem is chosen. To this purpose, in the next section a test cryptosystem is considered and the conditions which guarantee both GS between subsystems (9a) and (9b), GS between subsystems (10a) and (10b) and IS between its encrypter and its decrypter will rigorously be derived.

3. A Hyperchaotic Cryptosystem Based on Chua's Circuits and Oscillators

The block diagram of the proposed cryptosystem is shown in Fig. 3. In particular, a pair of bidirectionally coupled Chua's circuits is used to implement the hyperchaotic subsystems both at the encrypter and at the decrypter. Analogously, the supplementary hyperchaotic subsystems are constituted by two bidirectionally coupled Chua's oscillators both at the encrypter and at the decrypter. As is well known, these circuits are characterized by a rich variety of dynamical behaviors, such as chaotic and hyperchaotic attractors, as well as chaos–hyperchaos intermittency [Anishchenko *et al.*, 1994].

The state equations of the encrypter can be written in dimensionless form as [Brucoli *et al.*, 1997]:

$$\dot{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{g}(\mathbf{w}) \tag{11a}$$

$$\dot{\mathbf{x}}' = \mathbf{A}'\mathbf{x}' + \mathbf{g}(\mathbf{x}') + \mathbf{F}(\mathbf{x}, \mathbf{x}') \tag{11b}$$

where $\mathbf{x} = [x_1, \ldots, x_6]^T$ is the state vector of the coupled Chua's circuits, $\mathbf{x}' = [x'_1, \ldots, x'_6]^T$ is the state vector of the coupled Chua's oscillators, $\mathbf{w} = [w_1, 0, 0, w_4, 0, 0]^T$ is the transmitted signal vector. The matrices $\mathbf{A}$ and $\mathbf{A}'$ have the following structures:

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

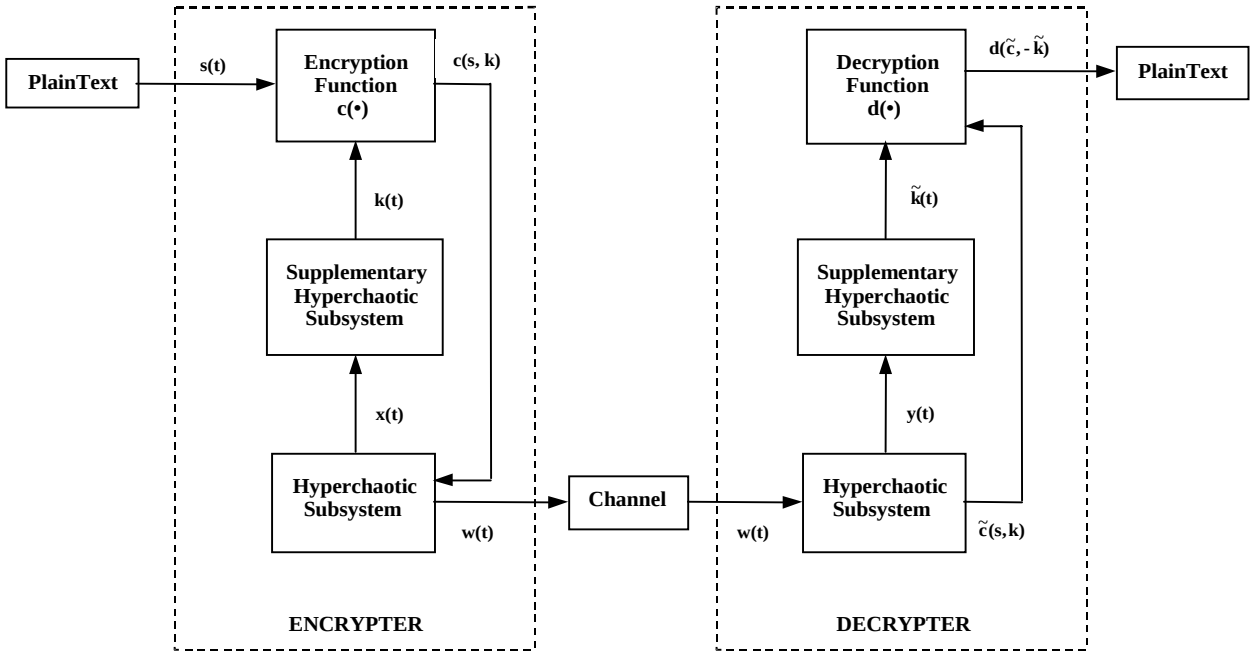


Fig. 3. Block diagram of the proposed hyperchaotic crytosystem.

$$\mathbf{A}' = \begin{bmatrix} -\alpha' & \alpha' & 0 & 0 & 0 & 0 \\ 1 & -1-K' & 1 & 0 & K' & 0 \\ 0 & -\beta' & -\gamma' & 0 & 0 & 0 \\ 0 & 0 & 0 & -\alpha' & \alpha' & 0 \\ 0 & K' & 0 & 1 & -1-K' & 1 \\ 0 & 0 & 0 & 0 & -\beta' & -\gamma' \end{bmatrix}$$

Each function vector $\mathbf{g}(\cdot)$ is formed by six piecewise-linear characteristics whose generic expression is given by:

$$g(z) = bz + (a-b)(|z+1| - |z-1|)/2 \quad (11c)$$

The parameters K and K' take into account the bidirectional coupling between the pairs of Chua's circuits and Chua's oscillators, respectively.

The expressions of the transmitted signals w_1 and w_4 are:

$$w_1(t) = x_1(t) + c(s_1(t),\, k_1(t)) \quad (12a)$$

$$w_4(t) = x_4(t) + c(s_4(t),\, k_4(t)) \quad (12b)$$

where $s_1(t)$ and $s_4(t)$ are the information signals, $k_1(t)$ and $k_4(t)$ are the key signals and $c(\cdot,\, \cdot)$ is the encryption function [Yang *et al.*, 1997].

The function vector $\mathbf{F}(\mathbf{x},\, \mathbf{x}')$ is used to assure the GS [Kocarev & Parlitz, 1996] between the subsystems of the encrypter unidirectionally coupled by means of a proper linear feedback action. This action is characterized by the difference between selected state variables of subsystems (11a) and (11b) and by a feedback gain M. More in detail:

$$\mathbf{F}(\mathbf{x},\, \mathbf{x}') = [M(x_1 + x_4 - x_1'),\, 0,\, 0,\, M(x_1 + x_4 - x_1' - x_4'),\, 0,\, 0]^T \quad (13)$$

The state equations of the decrypting system are

$$\dot{\mathbf{y}} = \mathbf{A}\mathbf{y} + \mathbf{g}(\mathbf{w}) \quad (14a)$$

$$\dot{\mathbf{y}}' = \mathbf{A}'\mathbf{y}' + \mathbf{g}(\mathbf{y}') + \mathbf{F}(\mathbf{y},\, \mathbf{y}') \quad (14b)$$

where

$$y = [y_1, \ldots,\, y_6]^T; \quad y' = [y_1', \ldots,\, y_6']^T$$

and

$$\mathbf{F}(\mathbf{y},\, \mathbf{y}') = [M(y_1 + y_4 - y_1'),\, 0,\, 0,\, M(y_1 + y_4 - y_1' - y_4'),\, 0,\, 0]^T$$

Now, a theorem can be stated to guarantee GS between the subsystems (11a) and (11b) at the encrypter on the basis of the approach developed in [Abarbanel *et al.*, 1996] and [Kocarev & Parlitz, 1996].

Theorem 1. *Generalized synchronization occurs between the unidirectionally coupled subsystems (11a) and (11b) if and only if for all initial conditions* $(\mathbf{x}_0,\, \mathbf{x}_0') \in B$ *the driven system (11b) is asymptotically stable, that is*:

$$\lim_{t\to\infty} \|\mathbf{x}'(t,\, \mathbf{x}_0,\, \mathbf{x}_{10}') - \mathbf{x}'(t,\, \mathbf{x}_0,\, \mathbf{x}_{20}')\| = 0$$

for all $\mathbf{x}'_{10},\, \mathbf{x}'_{20} \in B_{x'}$.

The proof can be found in [Kocarev *et al.*, 1996].

An analogous theorem can be stated for assuring GS between the unidirectionally coupled subsystems (14a) and (14b) at the decrypter.

A specific application of Theorem 1 has been developed in Appendix A to determine the range of values of the coupling parameter M which guarantees GS both between the encrypter subsystems and between the decrypter ones. This application has been developed by using the Auxiliary System Approach [Abarbanel *et al.*, 1996]. The main result is that GS is assured if the coupling parameter M satisfies the following condition:

$$M > \frac{\alpha'}{K'+1} + \alpha'(\max\{|\alpha|,\, |b|\} - 1) \quad (15)$$

Then to guarantee IS between the encrypter and the decrypter, the condition deriving from the following theorem has to be applied.

Theorem 2. *Identical synchronization between the encrypter and the decrypter occurs if condition (15) is satisfied.*

Proof. See Appendix B. ■

Concerning the encryption of the signals to be transmitted

$$w_1(t) = x_1(t) + q(\dots q(q(s_1(t),\, k_1(t)),\, k_1(t)),\, \dots,\, k_1(t)) \tag{16a}$$

$$w_4(t) = x_4(t) + q(\dots q(q(s_4(t),\, k_4(t)),\, k_4(t)),\, \dots,\, k_4(t)) \tag{16b}$$

the keys which have been repeatedly inserted in (16a) and (16b) are:

$$k_1 = a_1 x_1' + a_2 x_2' + a_3 x_3' \tag{17a}$$

$$k_4 = a_4 x_4' + a_5 x_5' + a_6 x_6' \tag{17b}$$

The coefficients a_i $(i = 1, \dots, 6)$ have to be chosen such that k_1 and k_4 lie within $(-h_1,\, h_1)$ and $(-h_4,\, h_4)$, respectively.

After guaranteeing IS between the transmitting and the receiving systems, the plaintext signals can be recovered as:

$$s_i(t) \cong s_{r_i}(t) = q(\dots q(q((w_i(t) - y_i(t)),\, -\tilde{k}_i(t)),\, -\tilde{k}_i(t)) \dots,\, -\tilde{k}_i(t)),\quad i = 1,\, 4 \tag{18}$$

where

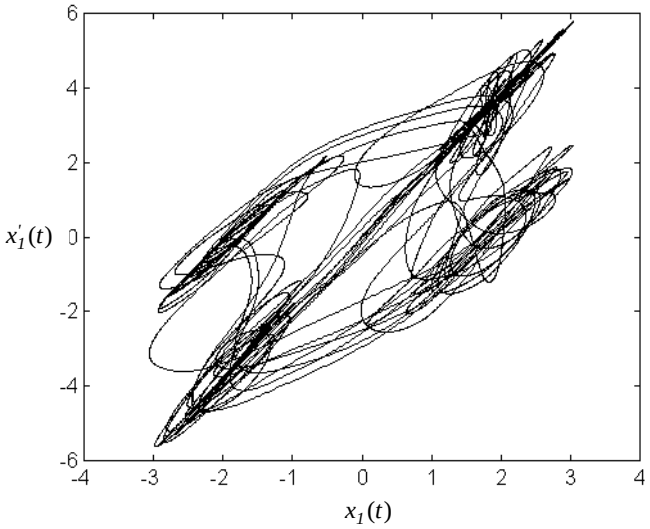
$$\tilde{k}_1 = a_1 y_1' + a_2 y_2' + a_3 y_3' \tag{19a}$$

$$\tilde{k}_4 = a_4 y_4' + a_5 y_5' + a_6 y_6' \tag{19b}$$

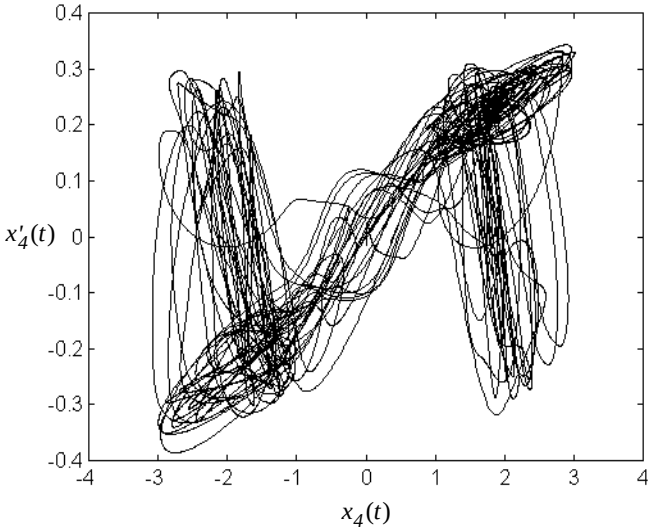
It should be noted that $\tilde{k}_i \to k_i$ as $t \to \infty (i = 1,\, 4)$ due to the IS property between the encrypting system and the decrypting one.

4. Simulation Results

The transmitter and the receiver are both characterized by the following parameters: $\alpha = 10.00$, $\beta = 14.87$, $\alpha' = 12.00$, $\beta' = 17.00$, $\gamma' = 0.04$, $a = -1.27$, $b = -0.68$, $K = 0.25$, $K' = 0.27$ and by the following non-null initial conditions: $x_1(0) = 0.01$, $x_4(0) = 0.011$, $x_1'(0) = 0.1$, $x_3'(0) = -0.1$, $x_5'(0) = 0.1$, $y_1(0) = 0.011$, $y_4(0) = 0.012$, $y_1'(0) = 0.11$, $y_3'(0) = -0.12$, $y_5'(0) = 0.09$. These values assure the existence of the system hyperchaotic behavior. Following the procedure illustrated in Sec. 3, the value of the unidirectional coupling feedback gain has been chosen as $M = 30$, thus guaranteeing GS between the subsystems both at the encrypter and at the decrypter. The following eigenvalues of the matrix **A** have been found: $\lambda_1 = -10.931$, $\lambda_2 = -10.890$, $\lambda_{3/4} = -0.056 \pm j3.695$, $\lambda_{5/6} = -0.286 \pm j3.678$, which, together with the choice of $M = 30$, assure IS between



(a)



(b)

Fig. 4. Generalized synchronization at the encrypter: (a) x_1' versus x_1; (b) x_4' versus x_4.

the encrypting system and the decrypting one. Moreover, a 50-shift cipher scheme has been used together with two key signals characterized by the parameters $a_i = 0.002$, $i = 1, 2, 3$ and $a_i = 0.02$, $i = 4, 5, 6$ with $h_1 = 0.035$ and $h_4 = 0.04$. Finally, the sinusoidal waveforms $s_1(t) = A_1 \sin(2\pi f_1 t)$ and $s_4(t) = A_4 \sin(2\pi f_4 t)$ with $A_1 = 0.03$, $A_4 = 0.04$, $f_1 = 25$ Hz and $f_4 = 30$ Hz have been considered as information bearing signals.

Figure 4 shows selected projections of the attractor generated by the encrypter subsystems (11a) and (11b) on the planes (x_1, x_1') and (x_4, x_4'). Analogously, Fig. 5 shows selected projections of the attractor generated by the decrypter subsystems (14a) and (14b) on the planes (y_3, y_3') and (y_6, y_6'). Both these figures confirm the existence of GS between the subsystems at the encrypter and between the subsystems at the decrypter. Figures 6 and 7 show the time behaviors of the synchronization errors $e_i(t)$ and $e_i'(t)$, $i = 1, \ldots, 6$ respectively. Figures 6 and 7 clearly indicate that the encrypter and the decrypter are identically synchronized. The time waveforms of the encrypted signals $c(s_1(t), k_1(t))$ and $c(s_4(t), k_4(t))$ have been reported in Fig. 8. Analogously, the time waveforms of the transmitted signals $w_1(t)$ and $w_4(t)$ have been reported in Fig. 9. From these figures it can be argued that the information signals are fairly well hidden in the transmitted signals. Finally, the time behaviors of the recovered signals $s_{r1}(t)$ and $s_{r4}(t)$ are shown in Fig. 10, which highlights the capability of the proposed technique to recover the original messages.

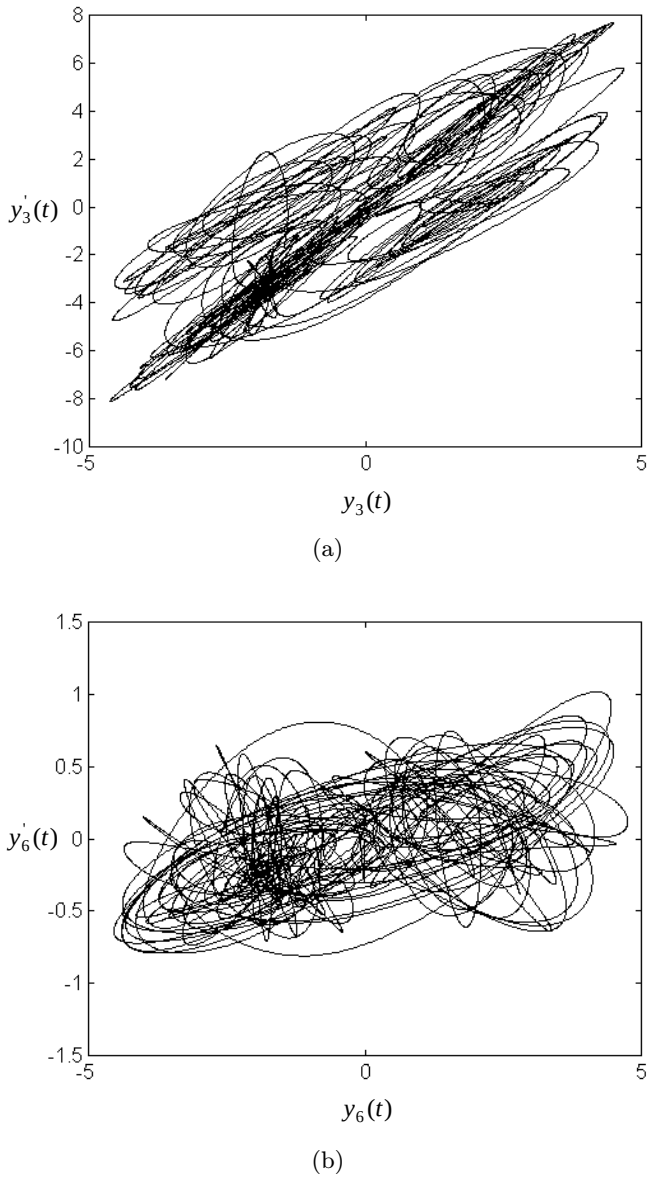


Fig. 5. Generalized synchronization at the decrypter: (a) y_3' versus y_3; (b) y_6' versus y_6.

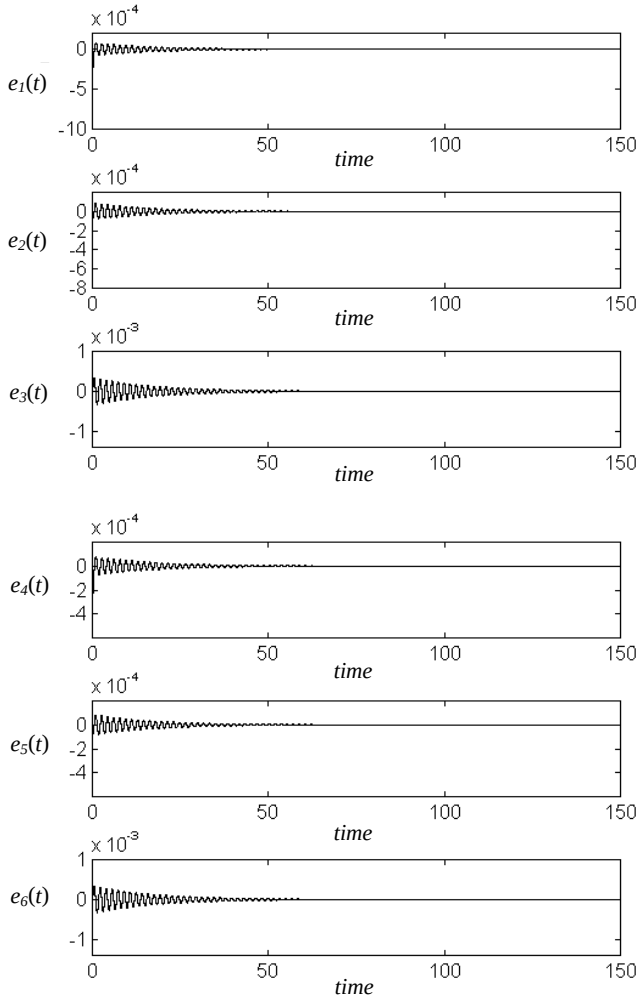


Fig. 6. Time behavior of the synchronization errors $e_i(t)$, $i = 1, \ldots, 6$.

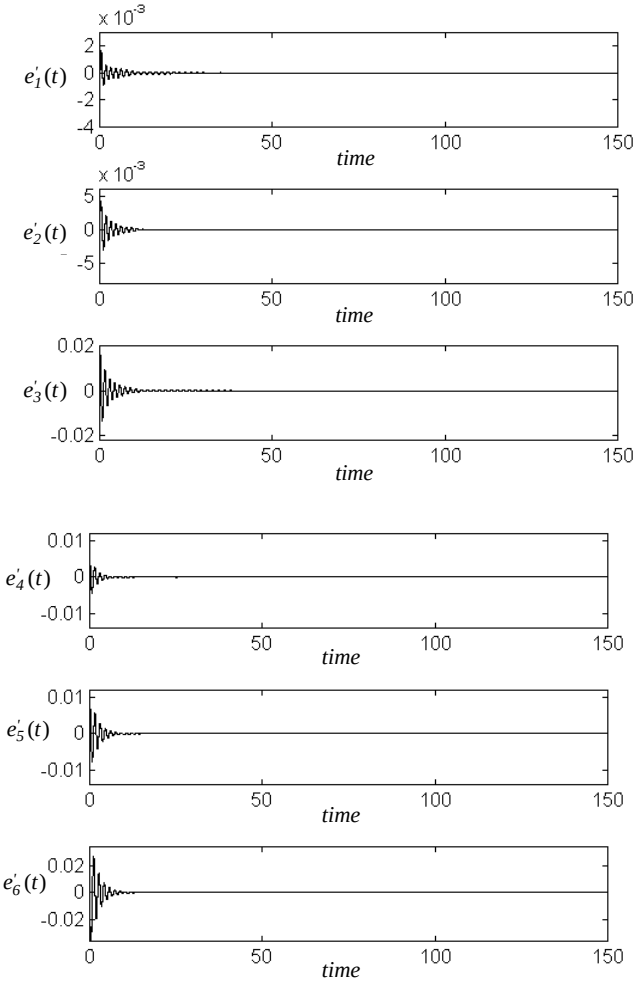


Fig. 7. Time behavior of the synchronization errors $e_i'(t)$, $i = 1, \ldots, 6$.

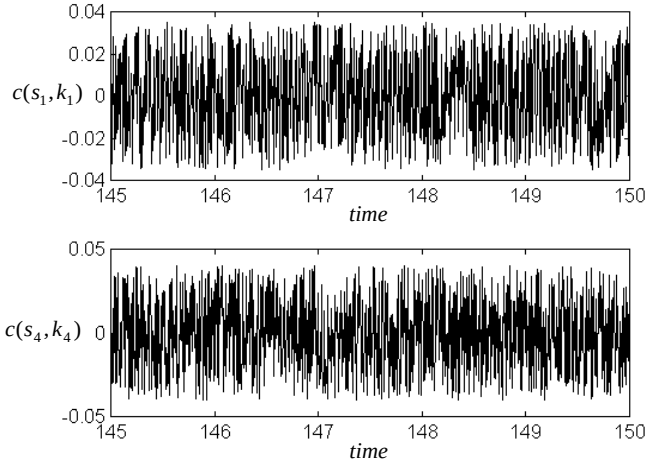


Fig. 8. Time waveforms of the encrypted signals $c(s_1, k_1)$ and $c(s_4, k_4)$.

5. Conclusions

In this paper identical and generalized synchronization have been applied to design a hyper-

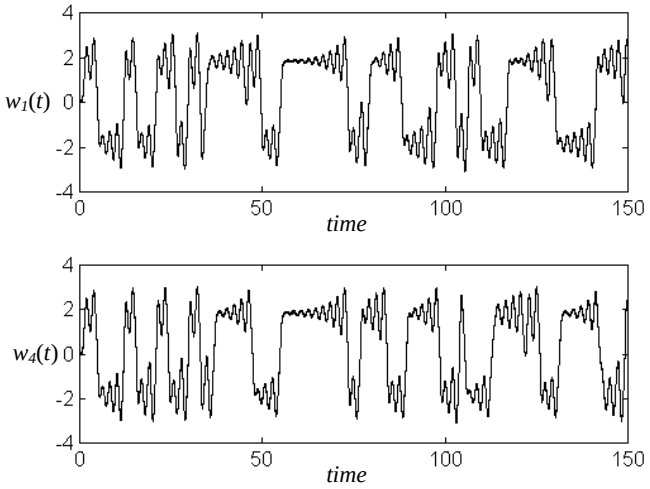


Fig. 9. Time waveforms of the transmitted signals $w_1(t)$ and $w_4(t)$.

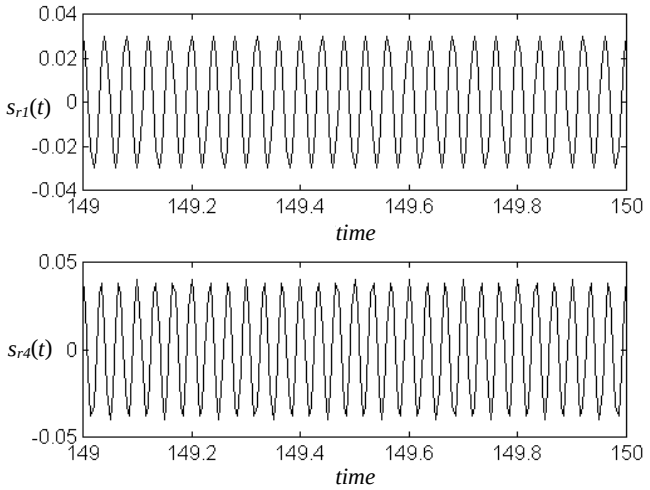


Fig. 10. Time waveforms of the recovered signals $S_{r1}(t)$ and $S_{r4}(t)$.

chaotic cryptosystem. In the proposed scheme, some chaotic signals have been used to encrypt the information messages by means of a μ-shift cipher scheme and proper chaotic signals have been chosen to synchronize the encrypter and the decrypter. An applicative example has been developed and satisfying results have been obtained.

References

Abarbanel, H. D. I., Rulkov, N. F. & Sushchik, M. M. [1996] "Generalized synchronization of chaos: The auxiliary system approach," *Phys. Rev.* **E53**(5), 4528–4535.

Anishchenko, V. S., Kapitaniak, T., Safonova, M. A. & Sosnovzeva, O. V. [1994] "Birth of double–double

scroll attractor in coupled Chua circuits," *Phys. Lett.* **A192**, 207–214.

Brucoli, M., Cafagna, D., Carnimeo, L. & Grassi, G. [1997] "An efficient technique for signal masking using synchronized hyperchaotic circuits," *Proc. 5th Int. Workshop on Nonlinear Dynamics of Electronic Systems* (*NDES '97*), Moscow, Russia, June 26–27, pp. 229–232.

Brucoli, M., Cafagna, D., Carnimeo, L. & Grassi, G. [1998] "Synchronization of hyperchaotic circuits via continuous feedback control with application to secure communications," *Int. J. Bifurcation and Chaos* **8**(10), 2031–2040.

Cuomo, K., Oppenheim, A. & Strogatz, S. [1993] "Synchronization of Lorenz-based chaotic circuits with application to communication," *IEEE Trans. CAS I* **40**(10), 626–633.

Dedieu, H., Kennedy, M. & Hasler, M. [1993] "Chaotic shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits," *IEEE Trans. CAS II* **40**(10), 634–642.

Kocarev, L. & Parlitz, U. [1996] "Generalized synchronization, predictability and equivalence of unidirectionally coupled dynamical systems," *Phys. Rev. Lett.* **76**(11), 1816–1819.

Parlitz, U., Chua, L. O., Kocarev, L., Halle, K. & Shang, A. [1992] "Transmission of digital signals by chaotic synchronization," *Int. J. Bifurcation and Chaos* **2**(4), 973–978.

Parlitz, U., Junge, L. & Kocarev, L. [1997] "Subharmonic entrainment of unstable periodic orbits and generalized synchronization," *Phys. Rev. Lett.* **79**(17), 3158–3161.

Rulkov, N. F., Sushchik, M. M., Tsimring, L. S. & Abarbanel, H. D. [1995] "Generalized synchronization of chaos in directionally coupled chaotic systems," *Phys. Rev.* **E51**(2), 980–994.

Short, K. [1994] "Steps toward unmasking secure communications," *Int. J. Bifurcation and Chaos* **4**(4), 959–977.

Short, K. [1996] "Unmasking a modulated chaotic communication scheme," *Int. J. Bifurcation and Chaos* **6**(2), 367–375.

Slotine, J. J. & Li, W. [1991] *Applied Nonlinear Control* (Prentice-Hall, NJ).

Stinson, D. [1995] *Cryptography: Theory and Practice* (CRC Press, Boca Raton, FL).

Suykens, J. A. K., Curran, P. F. & Chua, L. O. [1997] "Master–slave synchronization using dynamic output feedback," *Int. J. Bifurcation and Chaos* **7**(3), 671–679.

Wu, C. W. & Chua, L. O. [1993] "A simple way to synchronize chaotic systems with applications to secure communications," *Int. J. Bifurcation and Chaos* **3**(6), 1619–1628.

Yang, T. & Chua, L. O. [1996] "Secure communication via chaotic parameter modulation," *IEEE Trans. CAS I* **43**(9), 817–819.

Yang, T. & Chua, L. O. [1996] "Channel-independent chaotic secure communication," *Int. J. Bifurcation and Chaos* **6**(12B), 2653–2660.

Yang, T., Wu, C. W. & Chua, L. O. [1997] "Cryptography based on chaotic system," *IEEE Trans. CAS I* **44**(5), 469–472.

Appendix A

Determination of the coupling parameter M

The Auxiliary System Approach [Abarbanel *et al.*, 1996] is applied here to determine the range of values of the coupling parameter M which assures GS between the Chua's circuits and Chua's oscillators constituting the transmitting subsystems. To this purpose the response system

$$\dot{\mathbf{x}}' = \mathbf{A}'\mathbf{x}' + \mathbf{g}(\mathbf{x}') + \mathbf{F}(\mathbf{x}, \mathbf{x}') \tag{A.1}$$

is duplicated as:

$$\dot{\mathbf{x}}'' = \mathbf{A}'\mathbf{x}'' + \mathbf{g}(\mathbf{x}'') + \mathbf{F}(\mathbf{x}, \mathbf{x}'') \tag{A.2}$$

It should be noted that subsystem (A.1) and the auxiliary subsystem (A.2), which coincide with subsystem (11b), have different initial conditions. Following the auxiliary system approach, the time evolution of the differences

$$d_i = x_i' - x_i'', \quad i = 1, \ldots, 6$$

are described by the equations

$$\begin{aligned}
\dot{d}_1 &= \alpha'(d_2 - d_1) - \alpha'[g(x_1') - g(x_1'')] - Md_1 \\
\dot{d}_2 &= d_1 - d_2 + d_3 + K'(d_5 - d_2) \\
\dot{d}_3 &= -\beta' d_2 - \gamma' d_3 \\
\dot{d}_4 &= \alpha'(d_5 - d_4) - \alpha'[g(x_4') - g(x_4'')] - Md_1 - Md_4 \\
\dot{d}_5 &= d_4 - d_5 + d_6 + K'(d_2 - d_5) \\
\dot{d}_6 &= -\beta' d_5 - \gamma' d_6
\end{aligned} \tag{A.3}$$

The asymptotical stability of the response system (11b) occurs if the dynamical system (A.3) possesses a stable fixed point at the origin $\mathbf{d} = 0$, where $\mathbf{d} = [d_1, d_2, d_3, d_4, d_5, d_6]^T$.

After choosing the following positive definite Lyapunov function as [Brucoli *et al.*, 1997]:

$$V(\mathbf{d}) = d_1^2 + \alpha' d_2^2 + \frac{\alpha'}{\beta'} d_3^2 + d_4^2 + \alpha' d_5^2 + \frac{\alpha'}{\beta'} d_6^2 \tag{A.4}$$

the value of the feedback gain M has to be obtained by imposing that the time derivative $\dot{V}(\mathbf{d})$ be strictly negative.

Now, taking into account Eq. (11c), it results

$$-[g(x_1') - g(x_1'')] \leq d_1 \max\{|a|, |b|\}$$

$$-[g(x_4') - g(x_4'')] \leq d_4 \max\{|a|, |b|\}$$

Thus the derivative of $V(\mathbf{d})$ along the system trajectory can be expressed as:

$$\begin{aligned} \dot{V}(\mathbf{d}) \leq\ & (-\alpha' - M + \alpha' \max\{|a|, |b|\}) d_1^2 \\ & + 2\alpha' d_1 d_2 - \alpha' d_2^2 - \gamma' \frac{\alpha'}{\beta'} d_3^2 \\ & + (-\alpha' - M + \alpha' \max\{|a|, |b|\}) d_2^4 \\ & + 2\alpha' d_4 d_5 - \alpha' d_5^2 - \gamma' \frac{\alpha'}{\beta'} d_6^2 - M d_1 d_4 \\ & - (\alpha' K' d_2^2 - 2\alpha' K' d_2 d_5 + \alpha' K' d_5^2) \end{aligned} \tag{A.5}$$

By considering the worst case, Eq. (A.5) can be written as a quadratic form [Suykens *et al.*, 1997]:

$$\dot{V}(\mathbf{d}) = \mathbf{d}^T \boldsymbol{\Psi} \mathbf{d} \tag{A.6}$$

where $\Psi \in \mathbb{R}^{6\times 6}$ is a symmetric matrix given by:

$$\boldsymbol{\Psi} = \begin{bmatrix} M-p & -\alpha' & 0 & 0 & 0 & 0 \\ -\alpha' & \alpha'(K'+1) & 0 & 0 & -\alpha' K' & 0 \\ 0 & 0 & -\gamma' \dfrac{\alpha'}{\beta'} & 0 & 0 & 0 \\ M & 0 & 0 & M-p & -\alpha' & 0 \\ 0 & -\alpha' K' & 0 & -\alpha' & \alpha'(K'+1) & 0 \\ 0 & 0 & 0 & 0 & 0 & -\gamma' \dfrac{\alpha'}{\beta'} \end{bmatrix}$$

with $p = -\alpha' + \alpha' \max\{|a|, |b|\}$. For the considered configuration it can be easily shown that the parameter p is positive.

Equation (A.6) can be rewritten as:

$$\dot{V}(\mathbf{d}) = -\mathbf{d}_r^T \boldsymbol{\Psi}^1 \mathbf{d}_r - \gamma' \frac{\alpha'}{\beta'} d_3^2 - \gamma' \frac{\alpha'}{\beta'} d_6^2$$

where $\mathbf{d}_r = [d_1, d_2, d_4, d_5]^T$ is a reduced difference vector and $\boldsymbol{\Psi}^1 \in \mathbb{R}^{4\times 4}$ is the symmetric submatrix obtained from $\boldsymbol{\Psi}$ by deleting the third and the sixth rows and the third and the sixth columns, respectively.

By imposing that the matrix $\boldsymbol{\Psi}^1$ be positive definite, i.e. that all principal minors be strictly positive [Slotine, 1991], the parameter M can be derived. To this purpose, by indicating with $\boldsymbol{\Psi}_j^1$ the generic principal minor of $\boldsymbol{\Psi}^1$, it must be imposed that $\boldsymbol{\Psi}_j^1 > 0$, $j = 1, \ldots, 4$. In particular, the synthesis procedure is carried out in four steps [Brucoli *et al.*, 1997]; each step is based on the results of the previous one. Namely, for $j = 1$ it results

$$M > p \tag{A.7}$$

For $j = 2$, the following condition is obtained:

$$M > \frac{\alpha'}{K'+1} + P \tag{A.8}$$

It should be noted that (A.8) includes (A.7).

For $j = 3$, the following condition is obtained:

$$\boldsymbol{\Psi}_3^1 = (M-p)[\alpha'(M-p)(K'+1) - \alpha'^2] > 0 \tag{A.9}$$

The condition (A.9) is satisfied if condition (A.8) holds.

Finally, by imposing $\boldsymbol{\Psi}_4^1 > 0$ it can be shown that this inequality is satisfied for every $M \in \mathbb{R}$ provided that

$$K' > \frac{4(\alpha' + p)}{\alpha' - 8p}$$

It should be noted that this last condition is verified within the range of parameter values for the considered circuit configuration.

It can be concluded that $\dot{V}(\mathbf{d})$ is strictly negative for every $d_i (i = 1, \ldots, 6)$ when

$$M > \frac{\alpha'}{\mathbf{K}' + 1} + \alpha'(\max\{|a|, |b|\} - 1)\,. \qquad \text{(A.10)}$$

Appendix B

Proof of Theorem 2

Identical synchronization can firstly be demonstrated referring to subsystems (11a) and (14a). Namely, by defining the vector of synchronization errors as:

$$\mathbf{e}(t) = \mathbf{x}(t) - \mathbf{y}(t) \qquad \text{(B.1)}$$

the following equation describing the error dynamics can be derived:

$$\dot{\mathbf{e}}(t) = \mathbf{A}\mathbf{e}(t) \qquad \text{(B.2)}$$

Since the error dynamics is linear and autonomous and the eigenvalues of matrix $\mathbf{A}$ have negative real parts, system (B.2) is globally asymptotically stable, i.e. $\mathbf{e}(t) \to 0$ as $t \to \infty$. This implies that $y_1 \to x_1$ and $y_4 \to x_4$ for $t \to \infty$, that is $(y_1 + y_4) \to (x_1 + x_4)$ for $t \to \infty$. Moreover, the error system between (11b) and (14b) is:

$$\dot{\mathbf{e}}'(t) = \mathbf{A}'\mathbf{e}'(t) \qquad \text{(B.3)}$$

where $\mathbf{e}' = [e'_1, e'_2, \ldots, e'_6]^T$, with $e'_i = x'_i - y'_i (i = 1, \ldots, 6)$.

Following the procedure reported in Appendix A and taking into account condition (15), it can be easily proved that the subsystems (11b) and (14b) are identically synchronized. This completes the proof. ■