M. Kunz, and K. Vogelsang, Eds. Leipzig, Germany: Verlag im Wissenschaftszentrum Leipzig, 1996, pp. 91–132.
[30] V. E. Katsnelson, "The mean-periodic continuation method in sampling theory for functions with multi-band spectrum," in *Pro. 1997 Workshop on Sampling Theory Applications (SampTA-97)*, Aveiro, Portugal, June 1997, pp. 457–462.
[31] W. Stepanoff, "Sur quelques généralizations des fonctions presque périodiques," *C. R. Acad. Sci., Paris, Séer. I*, vol. 181, pp. 90–94, 1925.

# Synchronizing Hyperchaotic Systems by Observer Design

Giuseppe Grassi and Saverio Mascolo

***Abstract*— In this brief, a technique for synchronizing hyperchaotic systems is presented. The basic idea is to make the driven system a linear observer for the state of the drive system. By developing this approach, a linear time-invariant synchronization error system is obtained, for which a necessary and sufficient condition is given in order to asymptotically stabilize its dynamics at the origin. The suggested tool proves to be effective and systematic in achieving global synchronization. It does not require either the computation of the Lyapunov exponents, or the initial conditions belonging to the same basin of attraction. Moreover, it guarantees synchronization of a wide class of hyperchaotic systems via a *scalar signal*. Finally, the proposed tool is utilized to design a secure communications scheme, which combines conventional cryptographic methods and synchronization of hyperchaotic systems. The utilization of both *cryptography* and hyperchaos seems to make a contribution to the development of communication systems with higher security.**

***Index Terms*—Chaotic encryption, hyperchaotic circuits and systems, synchronization theory.**

## I. Introduction

At first thought, chaotic phenomena generated by nonlinear systems would seem singularly unsuited for engineering applications. In reality, the broad-band frequency spectrum makes chaotic signals a natural way of sending and receiving private communications. For this reason, chaotic dynamics, synchronization of coupled dynamic systems, and secure communications have been the topics of many papers over the last few years [1]–[7].

Referring to synchronization, Carroll and Pecora [2] have theoretically and experimentally shown that the dynamics of a drive system and of a driven subsystem (response system) become synchronized if the Lyapunov exponents of the response system are less then zero, assuming that both the systems start in the same basin of attraction. However, most of the methods concern the synchronization of low dimensional systems, characterized by only one positive Lyapunov exponent [2]–[4]. Since this feature limits the complexity of the chaotic dynamics, it is believed that the adoption of higher dimensional chaotic systems, with more than one positive Lyapunov exponent, enhances the security of the communication scheme. Therefore, hyperchaotic systems and hyperchaos synchronization have recently become fields of active research [5]–[7]. In particular, in [5] the synchronization between hyperchaotic systems is achieved by exploiting linear and nonlinear feedback functions, although the attention is not focused on the number of the synchronizing signals. In [6], a linear combination of the original state variables (i.e., a scalar signal) is used to synchronize hyperchaos in Rössler's systems. However, the approach in [6] cannot be considered a systematic technique for synchronization, since the coefficients of the linear combination are somewhat arbitrary. An interesting result has been recently reported in [7], where a parameter control method is proposed to achieve hyperchaos synchronization. In any case, the computation of the Lyapunov exponents is still required in order to verify the synchronization.

Manuscript received September 19, 1997; revised September 14, 1998. This paper was recommended by Associate Editor P. Thiran.

G. Grassi is with the Dipartimento di Matematica, Universitá di Lecce, 73100 Lecce, Italy.

S. Mascolo is with the Dipartimento di Elettrotecnica ed Elettronica, Politecnico di Bari, 70125 Bari, Italy.

Publisher Item Identifier S 1057-7130(99)02364-2.

This brief makes a contribution in the context of hyperchaos synchronization. Furthermore, an application to hyperchaos-based cryptography is presented. The key idea is to make the response system a linear observer for the state of the drive system. This approach guarantees synchronization, because an observer has the property that its state converges to the state of the plant; that is, the state of the driven system converges to the state of the drive one. The proposed technique has several advantages over the existing methods. It proves to be simple and rigorous. It does not require either the computation of the Lyapunov exponents or initial conditions belonging to the same basin of attraction. Moreover, global synchronization is achievable in a systematic way for several examples of hyperchaotic systems reported in literature.

The paper is organized as follows. In Section II, a general class of hyperchaotic systems is defined and the well-known concept of linear observer is introduced to formalize the problem of hyperchaos synchronization. Following this approach, a linear time-invariant synchronization error system is derived, along with a necessary and sufficient condition for its asymptotic stabilization. This technique guarantees synchronization of Rössler's system [6], the Matsumoto–Chua–Kobayashi (MCK) circuit [8] and its modified version [9], two oscillators recently reported in literature [10], [11], and a circuit with hysteretic nonlinearity [12]. A major advantage is that all of these systems are synchronized using a *scalar* signal. In order to show the effectiveness of the developed technique, numerical simulations are carried out in Section III, whereas in Section IV, a secure communications scheme is designed, which combines conventional *cryptographic* methods and synchronization of hyperchaotic systems. In Section V, some concluding remarks are given.

## II. Hyperchaos Synchronization Using Linear Observer

The goal of synchronization is to design a coupling between two chaotic systems, called drive system and response system, so that their dynamics become identical after a transient time. The coupling is implemented via a synchronizing signal, which is generated by the drive system. In this brief, the attention is focused on the following class of dynamic systems.

*Definition 1:* A hyperchaotic system belongs to the class $C_m$ if its state and output equations can be written, respectively, as

$$\dot{x}(t) = Ax(t) + Bf(x(t)) + c \tag{1}$$

$$y(t) = h(x(t)) \tag{2}$$

where $A \in \Re^{n\times n}$, $B \in \Re^{n\times m}$, $f = (f_1(x), f_2(x), \cdots, f_m(x))^T \in \Re^{m\times 1}$ with $f_i \neq f_j$ for $i \neq j$, $m \leq n$, $c \in \Re^{n\times 1}$ and $y = (h_1(x), h_2(x), \cdots, h_m(x))^T \in \Re^{m\times 1}$.

Each class $C_m$ represents a partition of the set $C$ of all hyperchaotic systems described by ordinary differential equations. More precisely, it results $C = \bigcup_{i=1}^{n} C_i$ with $C_i \bigcap C_j = \emptyset$. Note that the classes considered herein do not include hyperchaotic systems described by partial differential equations or delay differential equations. From a practical point of view, a system belonging to the class $C_m$ is characterized by $m$ independent nonlinear elements. The class characterized by a *single* nonlinear element includes several chaotic and hyperchaotic systems. Chua's circuit [1], higher-dimensional Chua circuits [14], and Chua's oscillator [1] are well-known examples of chaotic systems belonging to class $C_1$. Regarding hyperchaos, Rössler's system [6], the MCK circuit [8] and its modified version [9], the oscillators in [10] and [11], and the circuit with hysteretic nonlinearity in [12] all belong to the class $C_1$. Regarding higher classes, the Lorenz system [15], Rössler's system [16], the coupled Chua's circuit in [17], and the circuit proposed by Carroll and Pecora in [18] belong to the class $C_2$, whereas the coupled Lorenz systems in [15] and the coupled Chua's circuits forming a ring in [19] belong to the classes $C_4$ and $C_5$, respectively.

Given the drive system (1), most of the synchronization schemes proposed in the literature do not give a systematic procedure to determine the response system and the drive signal (2). Hence, most of these schemes are closely related to the given drive system and could not be easily generalized to a class of chaotic systems. The proposed approach overcomes this drawback by exploiting known results from linear control theory. In particular, the response system is chosen in the *observer* form [13], and the drive signal is designed so that a linear time-invariant synchronization error system is obtained.

*Definition 2:* Given system (1) and (2), the linear dynamic system

$$\dot{\hat{x}}(t) = A\hat{x}(t) + B(y(t) - \hat{y}(t)) + c \tag{3}$$

$$\hat{y}(t) = K\,\hat{x}(t) \tag{4}$$

where $K \in \Re^{m\times n}$ is a matrix to be determined, is said to be an *observer* for the state of system (1) and (2), if the synchronization error system has an asymptotically stable equilibrium point for $e = 0$, with $e(t) = (\hat{x}(t) - x(t))$ . Furthermore, system (3) and (4) is said to be a *global* observer of systems (1) and (2), if $e(t) \to 0$ as $t \to \infty$ for any initial condition $\hat{x}(0),\, x(0)$ [4], [13].

The synchronizing signal (2) can be viewed as an artificial output, which is properly designed to feed the response system (3) and (4). By taking

$$y(t) = f(x(t)) + Kx(t) \tag{5}$$

it can be easily shown that the error system is linear time-invariant

$$\dot{e}(t) = (A - BK)\,e(t) = Ae(t) + Bu(t) \tag{6}$$

where $u(t) = -Ke(t) \in \Re^{m\times 1}$ plays the role of a state feedback. Namely, by substituting (5) in (3), the error system is

$$\begin{aligned}\dot{e} &= A\hat{x} + B(y(t) - \hat{y}(t)) + c - (Ax + Bf(x) + c)\\ &= Ae + B(f(x) + Kx - K\hat{x}) - Bf(x)\\ &= Ae - BKe = Ae + Bu.\end{aligned}$$

Now the aim is to make the response system (3) and (4) an observer for the state of the drive system (1) and (2). This objective is achieved if system (6) is globally asymptotically stabilized at the origin. Referring to this concept, a result from linear control theory is briefly summarized [13]. Namely, the $n$-dimensional linear time-invariant, multivariable dynamic system $\dot{x} = Ax + Bu$ is controllable if the controllability matrix $\begin{bmatrix} B & AB & A^2B & \cdots & A^{n-1}B\end{bmatrix}$ is full rank. In this case, all the eigenvalues are controllable, i.e., they can be arbitrarily assigned by the introduction of state feedback. Thus, a theorem for hyperchaos synchronization can be stated.

*Theorem:* Consider a dynamic system belonging to the class $C_m$ and a response system described by (3) and (4). Let (5) be the synchronizing signal. Then, a necessary and sufficient condition for the existence of a feedback gain matrix $K,$ such that system (3) and (4) becomes global observer of system (1) and (2) is that the uncontrollable eigenvalues of system (6), if any, have negative real parts.

*Proof:* System (6) can be transformed to the Kalman controllable canonical form [13] by means of a coordinate transformation $e = T\overline{e} = [T_1 \quad T_2]\overline{e}$, with the property that $T^{-1} = t^T$

$$\begin{aligned}\begin{bmatrix}\dot{\overline{e}}_c\\ \dot{\overline{e}}_{nc}\end{bmatrix} &= \begin{bmatrix} T_1^T A T_1 & T_1^T A T_2\\ 0 & t_2^T A T_2\end{bmatrix}\begin{bmatrix}\overline{e}_c\\ \overline{e}_{nc}\end{bmatrix} + \begin{bmatrix} T_1^T B\\ 0\end{bmatrix} u\\ &= \begin{bmatrix}\overline{A}_c & \overline{A}_{12}\\ 0 & \overline{A}_{nc}\end{bmatrix}\begin{bmatrix}\overline{e}_c\\ \overline{e}_{nc}\end{bmatrix} + \begin{bmatrix}\overline{B}_c\\ 0\end{bmatrix} u\end{aligned} \tag{7}$$

where the eigenvalues of $\overline{A}_c$ are controllable (i.e., they can be placed anywhere by state feedback $u = -Ke$), whereas the eigenvalues of $\overline{A}_{nc}$ are uncontrollable (i.e., they 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 $\overline{A}_{nc}$ lie in the left-half plane. Since $\overline{e} \to 0$ implies $e \to 0$, it follows that $\hat{x} \to x$ as $t \to \infty$. As a consequence, system (3) and (4) becomes global observer of state equation (1) with output (5). This completes the proof.

*Remark 1:* The dynamic system described by (3) and (4) is a particular implementation of the Luenberger observer [13]. Namely, the external excitation in (3) is only the output signal (5), whereas in the standard structure the excitation is composed of both the input and the output of the plant.

## III. Synchronization Examples

### A. Systems Belonging to the Class $C_1$

$C_1$ represents an important class of hyperchaotic systems. In fact, a remarkable feature is that systems belonging to this class can be synchronized using a *scalar* signal.

*1) Simplified MCK Circuit:* In 1986, the MCK circuit led to the first experimental observation of hyperchaos from a real physical system [8]. Recently, a simplified MCK circuit has been proposed [9]. In particular, the three-segment piecewise-linear resistor implemented in [8] has been replaced with a diode, whereas the remaining circuit elements have not been modified. All of these elements are linear and passive, except an active resistor, which has negative resistance. By considering the parameters reported in [9], the state equations of the simplified MCK circuit are given by

$$\begin{bmatrix}\dot{x}_1\\ \dot{x}_2\\ \dot{x}_3\\ \dot{x}_4\end{bmatrix} = \begin{bmatrix}0 & -1 & 0 & 0\\ 1 & 0.5 & 0 & 0\\ 0 & 0 & 0 & -10\\ 0 & 0 & 1.5 & 0\end{bmatrix}\begin{bmatrix}x_1\\ x_2\\ x_3\\ x_4\end{bmatrix} + \begin{bmatrix}-1\\ 0\\ 10\\ 0\end{bmatrix} g(x_1,\, x_3) \tag{8}$$

where $g(\cdot)$ is the diode characteristic

$$g(x_1,\, x_3) = \begin{cases} 0, & \text{if } x_1 - x_3 \le 1\\ 3(x_1 - x_3 - 1), & \text{if } x_1 - x_3 > 1.\end{cases}$$

Let

$$y(t) = g(x_1,\, x_3) + \sum_{i=1}^{4} K_i x_i \tag{9}$$

be the scalar output. Clearly, system (8) and (9) belongs to the class $C_1$. By applying the proposed method, the linear response system is

$$\begin{bmatrix}\dot{\hat{x}}_1\\ \dot{\hat{x}}_2\\ \dot{\hat{x}}_3\\ \dot{\hat{x}}_4\end{bmatrix} = \begin{bmatrix}0 & -1 & 0 & 0\\ 1 & 0.5 & 0 & 0\\ 0 & 0 & 0 & -10\\ 0 & 0 & 1.5 & 0\end{bmatrix}\begin{bmatrix}\hat{x}_1\\ \hat{x}_2\\ \hat{x}_3\\ \hat{x}_4\end{bmatrix} + \begin{bmatrix}-1\\ 0\\ 10\\ 0\end{bmatrix}\left(y(t) - \sum_{i=1}^{4} K_i \hat{x}_i\right). \tag{10}$$

Since the controllability matrix of the error system

$$\begin{bmatrix}\dot{e}_1\\ \dot{e}_2\\ \dot{e}_3\\ \dot{e}_4\end{bmatrix} = \left(\begin{bmatrix}0 & -1 & 0 & 0\\ 1 & 0.5 & 0 & 0\\ 0 & 0 & 0 & -10\\ 0 & 0 & 1.5 & 0\end{bmatrix} - \begin{bmatrix}-1\\ 0\\ 10\\ 0\end{bmatrix}[K_1 K_2 K_3 K_4]\right)\begin{bmatrix}e_1\\ e_2\\ e_3\\ e_4\end{bmatrix} \tag{11}$$

is full rank, its eigenvalues can be moved anywhere. By placing them in $-2$, it results in $K = [-2.6302 \quad -0.6054 \quad 0.5870 \quad 0.7763]$, and system (10) becomes a global observer of system (8). This means that $\hat{x} \to x$, as $t \to \infty$ for each initial state $\hat{x}(0)$ of the response system (10).

*Remark 2:* The proposed approach does not require initial conditions of drive and response systems belonging to the same basin of attraction. This means that, in some sense, the technique developed herein overcomes the drawback related to the sensitive dependence on the initial condition of the chaotic systems to be synchronized [2]. Furthermore, since system (11) is controllable and all its modes can be arbitrarily assigned, synchronization can be achieved according to any specified design features.

*2) Hysteresis Chaos Generator:* The four-dimensional autonomous circuit reported in [12] contains one inductor, two capacitors, one negative conductor, a current-controlled nonlinear resistor, and one small inductor serially connected with it. The circuit dynamics can be written in dimensionless form as

$$\begin{bmatrix}\dot{x}_1\\ \dot{x}_2\\ \dot{x}_3\\ \dot{x}_4\end{bmatrix} = \begin{bmatrix}0 & 0 & -1 & -1\\ 0 & 2\gamma\delta & \gamma & 0\\ \rho & -\rho & 0 & 0\\ 1/\varepsilon & 0 & 0 & 0\end{bmatrix}\begin{bmatrix}x_1\\ x_2\\ x_3\\ x_4\end{bmatrix} + \begin{bmatrix}0\\ 0\\ 0\\ -(1/\varepsilon)\end{bmatrix} f(x_4) \tag{12}$$

where the nonlinear resistor is described by

$$f(x_4) = \begin{cases} x_4 + (1+\eta), & \text{if } x_4 \le -\eta\\ -(1/\eta)x_4, & \text{if } -\eta < x_4 < \eta\\ x_4 - (1+\eta), & \text{if } x_4 \ge \eta. \end{cases} \tag{13}$$

If $\varepsilon \to 0$, (12) is simplified into a constrained system that brings on hysteretic switching [12]. In this case, all motions in the phase space can, in fact, be divided into fast and slow ones. These motions highlight that the three-segment piecewise-linear resistor (13) behaves as a device with hysteretic nonlinearity [12]. In particular, for $\gamma = 1$, $\delta = 0.95$, $\rho = 14$, and $\eta = 1$, laboratory experiments and numerical computations have confirmed the generation of hyperchaos and related phenomena.

Let $y(t) = f(x_4) + \sum_{i=1}^{4} K_i x_i$ be the *scalar* output of (12), and let

$$\begin{bmatrix}\dot{\hat{x}}_1\\ \dot{\hat{x}}_2\\ \dot{\hat{x}}_3\\ \dot{\hat{x}}_4\end{bmatrix} = \begin{bmatrix}0 & 0 & -1 & -1\\ 0 & 2\gamma\delta & \gamma & 0\\ \rho & -\rho & 0 & 0\\ 1/\varepsilon & 0 & 0 & 0\end{bmatrix}\begin{bmatrix}\hat{x}_1\\ \hat{x}_2\\ \hat{x}_3\\ \hat{x}_4\end{bmatrix} + \begin{bmatrix}0\\ 0\\ 0\\ -(1/\varepsilon)\end{bmatrix}\left(y(t) - \sum_{i=1}^{4} K_i \hat{x}_i\right) \tag{14}$$

be the linear response system in the observer form. Since the controllability matrix of the error system is full rank, the eigenvalues can be placed, for instance, in $-3$ for $K = [-0.9516 \quad -0.0403 \quad -0.0123 \quad -0.0136]$. It can be concluded that global synchronization is achieved between the hysteresis hyperchaos generators described by (12) and (14).

*Remark 3:* It is easy to show that the proposed approach can be applied to other examples of hyperchaotic systems belonging to the class $C_1$, such as Rössler's system [6], the MCK circuit proposed in 1986 [8], and the oscillator with gyrators, illustrated in [11].

## *B. Systems Belonging to Higher Classes*

In this section, an example of a high-dimensional chaotic system is synchronized. In particular, a 15-dimensional dynamic system belonging to the class $C_5$ is considered, for which experimental observation of hyperchaos have been reported in [19]. The system consists of five identical coupled Chua's circuits forming a ring. Each Chua's circuit contains a linear resistor, three linear energy-storage elements, and a single nonlinear resistor with a three-segment linear characteristic. In this case, (1) and (3)–(5) give

$$A = \begin{bmatrix}A_1 & A_2 & 0 & 0 & 0\\ 0 & A_1 & A_2 & 0 & 0\\ 0 & 0 & A_1 & A_2 & 0\\ 0 & 0 & 0 & A_1 & A_2\\ A_2 & 0 & 0 & 0 & A_1\end{bmatrix}$$

$$A_1 = \begin{bmatrix}-3.2 & 10 & 0\\ 1 & -1.01 & 1\\ 0 & -14.87 & 0\end{bmatrix}$$

$$A_2 = \begin{bmatrix}0 & 0 & 0\\ 0 & 0.01 & 0\\ 0 & 0 & 0\end{bmatrix}, \qquad 0 \in \Re^{3\times 3}$$

$$b = \begin{bmatrix}b & 0 & 0 & 0 & 0\\ 0 & b & 0 & 0 & 0\\ 0 & 0 & b & 0 & 0\\ 0 & 0 & 0 & b & 0\\ 0 & 0 & 0 & 0 & b\end{bmatrix}$$

$$b = \begin{bmatrix}2.95\\ 0\\ 0\end{bmatrix}, \qquad 0 \in \Re^{3\times 1}, \qquad c = 0 \in \Re^{15\times 1}$$

$$f(x) = [f(x_1) \quad f(x_4) \quad f(x_7) \quad f(x_{10}) \quad f(x_{13})]^T$$

$$f(x_i) = |x_i + 1| - |x_i - 1|.$$

Since the controllability matrix $[B \quad AB \quad A^2B \quad \cdots \quad A^{14}B]$ of the error system (6) is full rank, the proposed Theorem assures the existence of a feedback matrix $K \in \Re^{5\times 15}$ such that $\hat{x} \to x$ as $t \to \infty$ for any initial state. For

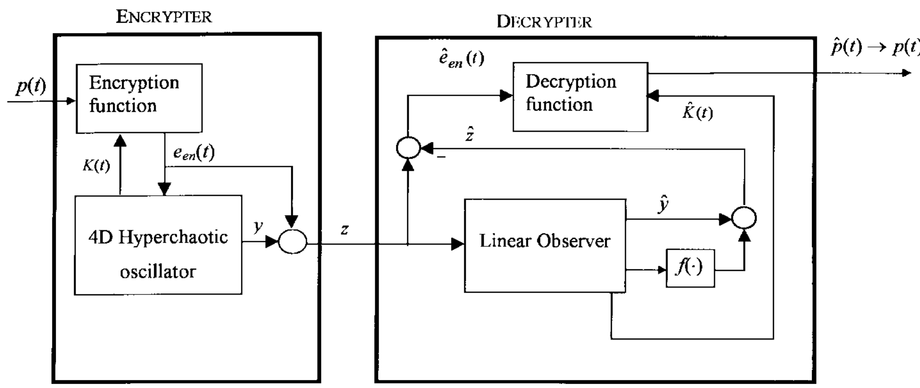


Fig. 1. A block diagram illustrating the proposed secure communications approach.

instance, the set of the error system eigenvalues becomes $\{-1, -1, -1, -1, -1, -2, -2, -2, -2, -2, -3, -3, -3, -3 -3\}$ for

$$K = \begin{bmatrix} K_1 & K_2 & 0 & 0 & 0 \\ 0 & K_1 & K_2 & 0 & 0 \\ 0 & 0 & K_1 & K_2 & 0 \\ 0 & 0 & 0 & K_1 & K_2 \\ K_2 & 0 & 0 & 0 & K_1 \end{bmatrix}$$

where

$$K_1 = [0.6068 \quad 0.3695 \quad 1.5547]$$
$$K_2 = [0.0034 \quad 0.0135 \quad 0.0034], \qquad 0 \in \Re^{1\times 3}.$$

Again, global synchronization is achieved between drive and response systems.

## IV. Application to Cryptography

The synchronization approach illustrated in Section II can be applied to design secure communications systems. By exploiting the idea proposed in [20] and [21], 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 hyperchaotic system and an encryption function, which is used to encrypt the message signal by means of the chaotic key [20]. The decrypter, which basically consists of a linear observer and a decryption function, enables the message signal to be retrieved when synchronization is achieved between the transmitting and receiving systems. Herein a four-dimensional (4-D) hyperchaotic oscillator belonging to the class $C_1$ is considered [10]. Its hyperchaotic behavior has been confirmed by both laboratory experiment and numerical simulation. The dynamics of the circuit can be written in dimensionless form as [10]

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \end{bmatrix} = \begin{bmatrix} 0.7 & -1 & -1 & 0 \\ 1 & 0 & 0 & 0 \\ 3 & 0 & 0 & -3 \\ 0 & 0 & 3 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ -1 \end{bmatrix} 30(x_4 - 1)\, H(x_4 - 1) \tag{15}$$

where $H$ is the Heaviside function (i.e., $H(u) = 0$, if $u < 0$; $H(u) = 1$, if $u \geq 0$). In order to encrypt the message signal $p(t) = 0.5 \sin t$, an $n$-shift cipher [20] is chosen

$$e_{en}(t) = f_1(\cdots f_1(f_1(p(t), K(t)), K(t)), \cdots, K(t)) \tag{16}$$

where the following nonlinear function

$$f_1(x, K) = \begin{cases} (x+K) + 2h, & -2h \leq (x+K) \leq -h \\ (x+K), & -h < (x+K) < h \\ (x+K) - 2h, & h \leq (x+K) \leq 2h \end{cases} \tag{17}$$

is recursively used for the encryption, with $h = 4$, $n = 30$, and $K(t) = x_2(t)$. The encrypted signal is fed back to the chaotic system as follows [3], [20]

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \end{bmatrix} = \begin{bmatrix} 0.7 & -1 & -1 & 0 \\ 1 & 0 & 0 & 0 \\ 3 & 0 & 0 & -3 \\ 0 & 0 & 3 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ -1 \end{bmatrix} 30(x_4 - 1)\, H(x_4 - 1) + \begin{bmatrix} 0 \\ 0 \\ 0 \\ -1 \end{bmatrix} e_{en}(t) \tag{18}$$

whereas the output is given by

$$y(t) = 30(x_4 - 1)\, H(x_4 - 1) + \sum_{i=1}^{4} K_i x_i. \tag{19}$$

By considering the *scalar* transmitted signal

$$z(t) = y(t) + e_{en}(t) \tag{20}$$

and by applying the proposed technique, the dynamics of the decrypter can be written as

$$\begin{bmatrix} \dot{\hat{x}}_1 \\ \dot{\hat{x}}_2 \\ \dot{\hat{x}}_3 \\ \dot{\hat{x}}_4 \end{bmatrix} = \begin{bmatrix} 0.7 & -1 & -1 & 0 \\ 1 & 0 & 0 & 0 \\ 3 & 0 & 0 & -3 \\ 0 & 0 & 3 & 0 \end{bmatrix} \begin{bmatrix} \hat{x}_1 \\ \hat{x}_2 \\ \hat{x}_3 \\ \hat{x}_4 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ -1 \end{bmatrix} (z(t) - \hat{y}(t)) \tag{21}$$

where

$$\hat{y}(t) = \sum_{i=1}^{4} K_i \hat{x}_i. \tag{22}$$

It is worth noting that $y(t)$ masks the encrypted signal $e_{en}(t)$, which in turn hides the message signal $p(t)$. Taking into account the considerations reported in [21], it can be stated that both the increased complexity of the transmitted signal and the adoption of a hyperchaotic system enable to overcome the low-security objections against low-dimensional chaos-based schemes.

Since the error system between (21) and (18) is linear time-invariant and its controllability matrix is full rank, the decrypter (21) becomes a global observer of the encrypter (18) by a suitable choice of $K$. For instance, by choosing the set of the error system

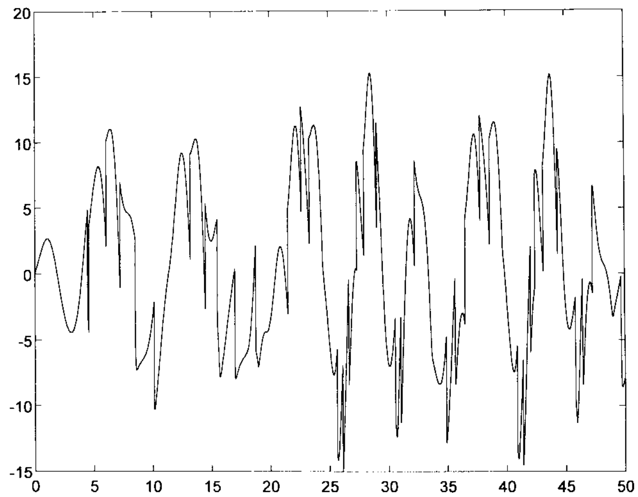

Fig. 2. Time waveform of the transmitted signal in (20).

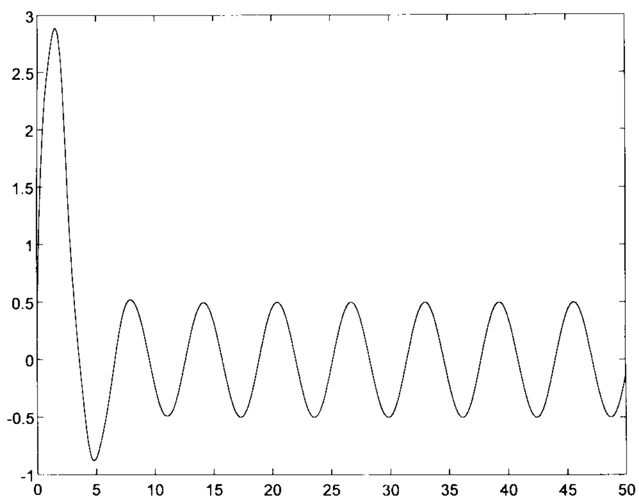

Fig. 3. Time waveform of the recovered signal in (25).

eigenvalues as $\{-0.5 \mp 3.486j, \quad -0.5 \mp 0.8222j\}$, it results $K_1 = -3.6937$, $K_2 = 0.2445$, $K_3 = 1.0727$ and $K_4 = -2.7000$.

The encrypted signal recovered by the decrypter is

$$\hat{e}_{en}(t) = z(t) - \hat{z}(t) \tag{23}$$

where

$$\hat{z}(t) = 30(\hat{x}_4 - 1)\, H(\hat{x}_4 - 1) + \hat{y}(t). \tag{24}$$

By using the key $\hat{K}(t) = \hat{x}_2(t)$ generated by the decrypter, the following message signal is retrieved:

$$\hat{p}(t) = f_1\Big(\cdots f_1\Big(f_1\Big(\hat{e}_{en}(t), -\hat{K}(t)\Big), -\hat{K}(t)\Big), \cdots, -\hat{K}(t)\Big) \tag{25}$$

where the decryption rule is the same as the encryption one [20]. Since encrypter and decrypter are synchronized, it results $\hat{x}(t) \to x(t)$, that is, $\hat{K}(t) \to K(t)$ and $\hat{e}_{en}(t) \to e_{en}(t)$. As a consequence, from (16) and (25) it follows that $\hat{p}(t) \to p(t)$.

The validity of the proposed secure communications scheme is confirmed by simulation results. In particular, the hyperchaotic transmitted signal (20) is reported in Fig. 2, whereas the recovered message signal (25) is shown in Fig. 3. This figure clearly highlights that $\hat{p}(t) \to p(t)$.

## V. Discussion

An interesting approach to *chaos* synchronization, based on the concept of observer design, has been proposed in [4]. In particular, synchronization is achieved by considering a linear output for the drive system, whereas for the response one, a Luenberger observer is chosen. This leads to a nonlinear and nonautonomous synchronization error system for which it is not easy to obtain the stability properties of the origin. Thus, the conclusion of the analysis developed in [4] is that local synchronization is possible under relatively mild conditions, whereas global synchronization can be achieved only if the system can be transformed to Brunowsky canonical form. On the other hand, the technique developed herein chooses a nonlinear output for the drive system, so that global synchronization is achievable if the linear error dynamics is stabilized at the origin.

In [3], the attention is focused on synchronization of *chaotic* systems. When dealing with hyperchaos, the hypothesis in [3] (that is, eigenvalues of $A$ be in the open left-half plane) seems hard to be satisfied. In fact, by examining the matrix $A$ for each system in Section III, it results that $A$ always has eigenvalues with positive real part. As a consequence, the approach in [3] cannot be exploited for synchronizing the systems considered herein.

Some considerations have to be made with regard to the more general case of hyperchaos synchronization illustrated in Section III-B. To this purpose, it should be noted that the results obtained in this case prove to be not so good as those illustrated in Section III-A. This is because the ring of Chua's circuits can be synchronized only by transmitting as many signals as the number of nonlinear elements. Therefore, if one wants to use just a scalar signal to synchronize systems with more than one independent nonlinear terms, the computation of the Lyapunov exponents is still an effective approach. Nevertheless, the technique illustrated in Section III-B can be considered a simple and systematic way to synchronize high-dimensional complex systems in the form (1) and (2), especially when the attention is not focused on the adoption of a scalar synchronizing signal.

The advantages and the shortcomings of the proposed secure communications scheme are now discussed. By using a *scalar* signal, the suggested approach exploits hyperchaos and cryptography to enhance the level of security of the communications scheme. In fact, several researchers believe that both the increased complexity of the transmitted signal and the adoption of hyperchaotic systems enable to overcome the low-security objections against low-dimensional chaos-based schemes [6], [20], [21]. However, it should be pointed out that this is a conjecture, the truthfulness of which needs to be further investigated. As a consequence, it is not easy at present to assess the level of security of a communications scheme. Lastly, it should be pointed out that some features of the proposed scheme might hamper the security level. For instance, each variation of any of the parameters will change the spectrum or total power of the transmitted signal.

## VI. Conclusion

By considering a linear observer and by designing a suitable synchronizing signal, the technique developed in this brief generates a linear time-invariant synchronization error system between the drive and the response systems. In this way, global synchronization is obtainable if the uncontrollable eigenvalues of the error system, if any, have negative real parts. It should be emphasized that synchronization can be achieved via a scalar signal for a wide class of hyperchaotic systems, which includes the MCK circuit, its modified version, a circuit with hysteretic nonlinearity, Rössler's system, and an oscillator with gyrators. Furthermore, the tool developed herein has been utilized to design a secure communications system based on a 4-D hyperchaotic oscillator. The scheme, by combining cryptography and hyperchaos synchronization, seems to make a contribution to the development of communication systems with higher security. Simulation results have confirmed the effectiveness and the simplicity of the approach developed herein.


## Acknowledgment

The authors would like to express their sincere gratitude to Associate Editor P. Thiran, for handling the process of reviewing the paper, as well as to the reviewers who carefully reviewed the manuscript.


## References


[1] R. N. Madan, Ed., *Chua's Circuit: A Paradigm for Chaos*. Singapore: World Scientific, 1993.

[2] T. L. Carroll and L. M. Pecora, "Synchronizing chaotic circuits," *IEEE Trans. Circuits Syst.,* vol. 38, pp. 453–456, Apr. 1991.

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

[4] Ö. Morgül and E. Solak, "Observed based synchronization of chaotic systems," *Phys. Rev. E,* vol. 54, no. 5, pp. 4803–4811, 1996.

[5] M. K. Ali and J. Q. Fang, "Synchronization of chaos and hyperchaos using linear and nonlinear feedback functions," *Phys. Rev. E,* vol. 55, no. 5, pp. 5285–5290, 1997.

[6] J. H. Peng, E. J. Ding, M. Ding, and W. Yang, "Synchronizing hyperchaos with a scalar transmitted signal," *Phys. Rev. Lett.,* vol. 76, no. 6, pp. 904–907, 1996.

[7] C. K. Duan and S. S. Yang, "Synchronizing hyperchaos with a scalar signal by parameter controlling," *Phys. Lett. A,* vol. 229, pp. 151–155, 1997.

[8] T. Matsumoto, L. O. Chua, and K. Kobayashi, "Hyperchaos: Laboratory experiment and numerical confirmation," *IEEE Trans. Circuits Syst.,* vol. CAS-33, pp. 1143–1147, Nov. 1986.

[9] A. Tamasevicius, "Hyperchaotic circuits: State of the art," in *Proc. 5th Int. Workshop Nonlinear Dynamics Electronic Systems (NDES'97),* Moscow, Russia, 1997, pp. 97–102.

[10] A. Tamasevicius, A. Namajunas, and A. Cenys, "Simple 4D chaotic oscillator," *Electron. Lett.,* vol. 32, no. 11, pp. 957–958, 1996.

[11] A. Tamasevicius, A. Cenys, G. Mykolaitis, A. Namajunas, and E. Lindberg, "Hyperchaotic oscillators with gyrators," *Electron. Lett.,* vol. 33, no. 7, pp. 542–544, 1997.

[12] T. Saito, "An approach toward higher dimensional hysteresis chaos generators," *IEEE Trans. Circuits Syst.,* vol. 37, pp. 399–409, Mar. 1990.

[13] T. Kailath, *Linear Systems.* Englewood Cliffs, NJ: Prentice-Hall, 1980.

[14] M. Gotz, U. Feldmann, and W. Schwarz, "Synthesis of higher dimensional Chua circuits," *IEEE Trans. Circuits Syst. I,* vol. 40, pp. 854–860, Nov. 1993.

[15] A. Stefanski, T. Kapitaniak, and J. Brindley, "Dynamics of coupled Lorenz systems and its geophysical implications," *Physica D,* vol. 98, pp. 594–598, 1996.

[16] O. E. Rössler, "An equation for continuous chaos," *Phys. Lett.,* vol. 57A, no. 5, pp. 397–398, 1976.

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

[18] T. L. Carroll and L. M. Pecora, "A circuit for studying the synchronization of chaotic systems," *Int. J. Bifurcation Chaos,* vol. 2, no. 3, pp. 659–667, 1992.

[19] T. Kapitaniak, L. O. Chua, and G. Q. Zhong, "Experimental hyperchaos in coupled Chua's circuits," *IEEE Trans. Circuits Syst. I,* vol. 41, pp. 499–503, July 1994.

[20] T. Yang, C. W. Wu, and L. O. Chua, "Cryptography based on chaotic systems," *IEEE Trans. Circuits Syst. I,* vol. 44, pp. 469–472, May 1997.

[21] 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.


# Comments on "Linear Circuit Fault Diagnosis Using Neuromorphic Analyzers"

Giulio Fedi, Stefano Manetti, and Maria Cristina Piccirilli

***Abstract*—In a recent paper, Spina and Upadhyaya presented a method for the fault diagnosis of analog linear circuits. The method, which is based on a white noise generator and an artificial neural network for response analysis, has been applied to circuits of reasonable dimensions, taking into account the effect of the component tolerances. However, the proposed method does not take into account the testability analysis of the circuit under test. Research on testability analysis of linear circuits has been developed by several authors in the last 20 years, and algorithms and programs for testability evaluation have been presented in several publications. It is our opinion that the testability analysis concept could be useful in the approach proposed by Spina and Upadhyaya to improve the quality of the results even further. In this brief, we discuss this possibility.**

***Index Terms*— Analog system fault diagnosis, analog system testing, fault location.**

## I. Testability and Canonical Ambiguity Groups

In the above paper,[1] Spina and Upadhyaya presented a method for the fault diagnosis of analog linear circuits. In the analog fault diagnosis field, an essential point is constituted by the concept of testability which, independently of the method which will be effectively used in fault location, gives theoretical and rigorous upper limits to the degree of solvability of the problem once the test point set has been chosen.

The testability is strictly tied to the concept of network-element-value-solvability, which was first introduced by Berkowitz [1]. Successively, a very useful testability measure was introduced by Saeks *et al.* [2]–[4]. Other definitions have been presented in subsequent years [5], [6], but, at present, there is no universal definition of analog testability. In this brief, we adopt the Saeks definition because it provides a well-defined quantitative measure of testability. In fact, this definition of testability gives a measure of solvability to the fault diagnosis equations, nonlinear with respect to the component values, and indicates the ambiguity which will result from an attempt to solve such equations in a neighborhood of almost any failure. Algorithms for evaluating this kind of testability measure have been developed by the authors, at first using a numerical approach [7], [8]. These methods were suitable only for networks of moderate size because of the inevitable roundoff errors introduced by numerical algorithms. This limitation has been overcome with the introduction of the symbolic approach [9]–[11] through an efficient manipulation of algebraic expressions [12], [13].

Another concept which is strictly related to that of testability and is extremely useful, particularly in case of low-testability value, is that of a canonical ambiguity group. Roughly speaking, an ambiguity group is a set of components that, if considered as potentially faulty, do not give unique solution in the phase of fault location. A canonical ambiguity group is simply an ambiguity group which does not contain other ambiguity groups. The knowledge of the canonical ambiguity

Manuscript received July 1, 1997; revised October 14, 1998. This paper was recommended by Associate Editor W. Kao.

The authors are with the Dipartimento di Ingegneria Electtronica, Università degli astudi di Firenze, 50139 Florence, Italy.

Publisher Item Identifier S 1057-7130(99)02358-7.

[1] R. Spina and S. Upadhyaya, *IEEE Trans. Circuits Syst.,* vol. 44, pp. 188–196, Mar. 1997.