Synchronization of multi-scroll chaos generators: application to private communication

L. Gámez-Guzmán and C. Cruz-Hernández*
Electronics and Telecommunications Department,
Scientific Research and Advanced Studies Center of Ensenada (CICESE),
Km. 107, Carretera Tijuana-Ensenada, 22860 Ensenada, B. C., México.

R.M. López-Gutiérrez and E.E. García-Guerrero
Faculty of Engineering, Baja California Autonomous University (UABC),
Km. 103, Carretera Tijuana-Ensenada, 22860 Ensenada, B.C., México.

Recibido el 28 de marzo de 2008; aceptado el 2 de junio de 2008

In this paper, the synchronization problem of coupled 2D-grid scroll attractor families in master-slave configuration is studied numerically. In particular, we consider, for synchronization purposes, the chaos generator model of 3×3-scroll grid attractors by appealing to Generalized Hamiltonian forms and observer design from nonlinear control theory. A potential application to the transmission of encrypted information is also given.

Keywords: Chaos synchronization; multi-scroll chaotic attractor; observer; Generalized Hamiltonian system; chaotic encryption; private communication.

Este trabajo versa sobre la comunicación secreta de información analógica y digital. El encriptado se produce por sincronía de caos, la cual se obtiene de formas hamiltonianas y el diseño de un observador no lineal. En particular, se emplean circuitos caóticos generadores de una familia de atractores con enrollamientos de 3×3 en cuadrícula 2D, como consecuencia produciendose incremento en la seguridad del cifrado en la transmisión de información confidencial.

Descriptores: Sincronización de caos; atractor caótico con enrollamientos de 3×3 en cuadrícula 2D; sistema hamiltoniano generalizado; observador; comunicación secreta.

PACS: 05.45.+b; 43.72.+q; 43.50.+y (89.75.-K; 05.45.Gg)

1. Introduction

Generations of multi-scroll chaotic attractors have received considerable attention for more than a decade; such interest is both theoretical and practical [1-9], because of their potential application to communications, cryptography, and neural networks [8] have also received attention.

On the other hand, in the past decades, chaotic synchronization has received a tremendous increase in interest (see *e.g.* Refs. 10 to 17). This property is supposed to have interesting applications in different fields, particularly in designing secure communication systems [18-27]. Private communication schemes are usually composed of a chaotic system as transmitter with another chaotic system as receiver, where the confidential information is imbedded into the transmitted chaotic signal by direct modulation, masking, or another technique. At the receiver end, if chaotic synchronization is achieved, then it is possible to extract the hidden information from the transmitted signal.

The main goal of this paper is the synchronization of 2D-grid scroll attractor families. In particular, the model 3×3-scroll grid attractor is chosen as chaos generator. This objective is achieved by using the Hamiltonian systems and nonlinear observer approach from nonlinear control theory [14]. In addition, chaos synchronization of multi-scroll attractors is applied to transmit encrypted analog and digital information.

This paper is organized as follows: In Sec. 2, a summary on chaos synchronization via Hamiltonian systems approach is provided. Mathematical models for generating families of scroll grid chaotic attractors are briefly introduced in Sec. 3, while in Sec. 4, we show chaos synchronization of coupled 3×3-grid scroll attractors. In Sec. 5, we carry out a stability analysis of the synchronization error. In Sec. 6, we present an application to chaotic communication, where we transmit encrypted analog and digital confidential information. Finally, some conclusions are given in Sec. 7.

2. Summary of chaos synchronization: Hamiltonian systems approach

Consider the dynamical system

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

where $x \in \mathbb{R}^n$ is the *state vector* and $f : \mathbb{R}^n \to \mathbb{R}^n$ is a nonlinear function.

In Ref. 14, it is reported how system (1) can be written in the following *Generalized Hamiltonian canonical form*:

$$\dot{x} = \mathcal{J}(x)\frac{\partial H}{\partial x} + \mathcal{S}(x)\frac{\partial H}{\partial x} + \mathcal{F}(x), \qquad x \in \mathbb{R}^n, \tag{2}$$

where $H(x)$ denotes a smooth *energy function* which is globally positive definite in $\mathbb{R}^n$. The *gradient vector* of H, denoted by $\partial H/\partial x$, is assumed to exist everywhere. We use

quadratic energy function $H(x) = (1/2)\, x^T \mathcal{M} x$ with $\mathcal{M}$ being a constant, symmetric positive definite matrix. In this case, $\partial H/\partial x = \mathcal{M}x$. The matrices $\mathcal{J}(x)$ and $S(x)$ satisfy, for all $x \in \mathbb{R}^n$, the following properties: $\mathcal{J}(x) + \mathcal{J}^T(x) = 0$ and $\mathcal{S}(x) = \mathcal{S}^T(x)$. The vector field $\mathcal{J}(x)\partial H/\partial x$ exhibits the *conservative* part of the system and it is also referred to as the *workless* part, or *work-less* forces of the system, and $\mathcal{S}(x)$ denotes the *working* or *nonconservative* part of the system. For certain systems, $\mathcal{S}(x)$ is *negative definite* or *negative semidefinite*. Thus, the vector field is referred to as the dissipative part of the system. If, on the other hand, $\mathcal{S}(x)$ is positive definite, positive semidefinite, or indefinite, it clearly represents the global, semi-global, or local *destabilizing* part of the system, respectively. In the last case, we can always (although nonuniquely) decompose such an indefinite symmetric matrix into the sum of a symmetric negative semidefinite matrix $\mathcal{R}(x)$ and a symmetric positive semidefinite matrix $\mathcal{N}(x)$. Finally, $\mathcal{F}(x)$ represents a *locally destabilizing* vector field.

In the context of observer design, we consider a *special class* of Generalized Hamiltonian forms with output $y(t)$, given by

$$\dot{x} = \mathcal{J}(y)\frac{\partial H}{\partial x} + (\mathcal{I} + \mathcal{S})\frac{\partial H}{\partial x} + \mathcal{F}(y), \qquad x \in \mathbb{R}^n, \quad (3)$$
$$y = \mathcal{C}\frac{\partial H}{\partial x}, \qquad y \in \mathbb{R}^m,$$

where $\mathcal{S}$ is a constant symmetric matrix, not necessarily of a definite sign. $\mathcal{I}$ is a constant skew symmetric matrix, and $\mathcal{C}$ is a constant matrix.

We denote the *estimate* of the state $x(t)$ by $\xi(t)$, and consider the Hamiltonian energy function $H(\xi)$ to be the particularization of H in terms of $\xi(t)$. Similarly, we denote by $\eta(t)$ the estimated output, computed in terms of $\xi(t)$. The gradient vector $\partial H(\xi)/\partial\xi$ is, naturally, of the form $\mathcal{M}\xi$ with $\mathcal{M}$ being a constant, symmetric positive definite matrix.

A *nonlinear state observer* for the Generalized Hamiltonian form (3) is given by

$$\dot{\hat{\xi}} = \mathcal{J}(y)\frac{\partial H}{\partial \xi} + (\mathcal{I} + \mathcal{S})\frac{\partial H}{\partial \xi} + \mathcal{F}(y) + K(y - \eta),$$
$$\xi \in \mathbb{R}^n, \quad (4)$$
$$\eta = \mathcal{C}\frac{\partial H}{\partial \xi}, \qquad \eta \in \mathbb{R}^m,$$

where K is the *observer gain*.

The *state estimation error*, defined as $e(t)=x(t)-\xi(t)$, and the output estimation error, defined as $e_y(t)=y(t)-\eta(t)$, are governed by

$$\dot{e} = \mathcal{J}(y)\frac{\partial H}{\partial e} + (\mathcal{I} + \mathcal{S} - K\mathcal{C})\frac{\partial H}{\partial e}, \qquad e \in \mathbb{R}^n, \quad (5)$$
$$e_y = \mathcal{C}\frac{\partial H}{\partial e}, \qquad e_y \in \mathbb{R}^m,$$

where $\partial H/\partial e$ actually stands, with some abuse of notation, for the gradient vector of the *modified* energy function, $\partial H(e)/\partial e = \partial H/\partial x - \partial H/\partial\xi = \mathcal{M}(x - \xi) = \mathcal{M}e$. We set, when needed, $\mathcal{I} + \mathcal{S} = \mathcal{W}$.

Definition 1 *(Chaotic synchronization) [17] The slave system (nonlinear state observer) (4) synchronizes with the chaotic master system in Generalized Hamiltonian form (3), if*

$$\lim_{t\to\infty} \|x(t) - \xi(t)\| = 0, \quad (6)$$

no matter which initial conditions $x(0)$ and $\xi(0)$ have, where the state estimation error $e(t) = x(t) - \xi(t)$ corresponds to the *synchronization error*.

A necessary and sufficient condition for global asymptotic stability to zero of the estimation error (5) is given by the following theorem.

Theorem 1 [14] *The state $x(t)$ of the nonlinear system (3) can be globally, exponentially, asymptotically estimated by the state $\xi(t)$ of the observer (4) if and only if there exists a constant matrix K such that the symmetric matrix*

$$[\mathcal{W} - K\mathcal{C}] + [\mathcal{W} - K\mathcal{C}]^T = [\mathcal{S} - K\mathcal{C}] + [\mathcal{S} - K\mathcal{C}]^T$$
$$= 2\left[\mathcal{S} - \frac{1}{2}\left(K\mathcal{C} + \mathcal{C}^T K^T\right)\right]$$

is negative definite.

3. Families of scroll grid chaotic attractors

Recently, a family of n-scrolls was reported (in Ref. 8) that was more general than the family of n-double scroll attractors, which generates chaos with a simple circuit implementation. The generated chaotic attractors of this family are called *scroll grid attractors*. For these families it is possible to cover the whole state space with scrolls. Such families of multi-scrolls are classified according to the location of their equilibrium points in *1D, 2D,* and *3D-scroll attractor families*. Below, we describe some chaos generator models, which give origin to families of multi-scroll attractors.

3.1. 1D-grid scroll attractor family

In this family, the equilibrium points are located on a straight line, and the generated scrolls originate around that line along the x_1 state variable direction in state space. In addition, the x_1 state is also the variable on which the nonlinearity in the model operates. In the current literature, the so-called 1D-grid scroll attractor family is also known as *n-scroll attractors* [3].

Consider the following chaos generator model [4]:

$$\begin{cases} \dot{x}_1 = x_2, \\ \dot{x}_2 = x_3, \\ \dot{x}_3 = -a\left(x_1 + x_2 + x_3 - f_2(x_1)\right) \end{cases} \quad (7)$$

where

$$f(\zeta) = \begin{cases} 1, & \zeta \geq 0, \\ -1, & \zeta < 0 \end{cases} \tag{8}$$

the state vector $x = (x_1, x_2, x_3)^T \in \mathbb{R}^3$ and $\zeta \in \mathbb{R}$. For this chaos generator model, a double-scroll like attractor for $a = 0.8$ was reported in Ref. 4. Recently, a generalization of the previous model (7)-(8) for generating multi-scroll attractors was reported in Ref. 6, by taking the nonlinearity

$$f_1(x_2) = \sum_{i=1}^{M_{x_2}} g_{\frac{(-2i+1)}{2}}(x_2) + \sum_{i=1}^{N_{x_2}} g_{\frac{(2i+1)}{2}}(x_2), \tag{9}$$

where

$$g_\theta(\zeta) = \begin{cases} 1, & \zeta \geq \theta, \quad \theta > 0, \\ 0, & \zeta < \theta, \quad \theta > 0, \\ 0, & \zeta \geq \theta, \quad \theta < 0, \\ -1 & \zeta < \theta, \quad \theta < 0 \end{cases} \tag{10}$$

where nonlinearity (10) is parameterized in fewer unknowns. A generalization of the chaos generator model (7) can be systematically obtained by introducing additional breakpoints in the nonlinearity, where each breakpoint can be implemented by using (10). For this reason, the nonlinearity (10) is called the *core function*.

Due to the location of the equilibrium points, this strange attractor family is called *1D-grid scroll attractors*. In the attractors generated, the scrolls are located around the equilibrium points. The number of generated scrolls is equal to the number of equilibrium points, which corresponds to $M_{x_1} + N_{x_1} + 1$. For example; 3-scroll, 5-scroll, and 10-scroll attractors are generated by using model (7) with nonlinearity (9)-(10) for $a = 0.4$ and for ($M_{x_1} = N_{x_1} = 1$), ($M_{x_1} = 0$, $N_{x_1} = 4$), and ($M_{x_1} = 4$, $N_{x_1} = 5$), respectively.

3.2. 2D-grid scroll attractor family

In this family, the equilibrium points are located on the x_1 and x_2 state variables. The generated scrolls are located along the x_1 and x_2 state variable directions in state space. The x_1 and x_2 states are the variables on which the nonlinear functions operate. In the current literature, this family is known as the *2D-grid scroll attractor family* [7].

We consider the chaos generator model proposed in Ref. 1, described by

$$\begin{cases} \dot{x}_1 = x_2 - f_1(x_2), \\ \dot{x}_2 = x_3, \\ \dot{x}_3 = -a(x_1 + x_2 + x_3 - f_2(x_1)) \end{cases} \tag{11}$$

with double nonlinear functions:

$$f_1(x_2) = \sum_{i=1}^{M_{x_2}} g_{\frac{(-2i+1)}{2}}(x_2) \sum_{i=1}^{N_{x_2}} g_{\frac{(2i+1)}{2}}(x_2), \tag{12}$$

$$f_2(x_1) = \sum_{i=1}^{m-1} \beta g_{p_i}(x_1) \tag{13}$$

where

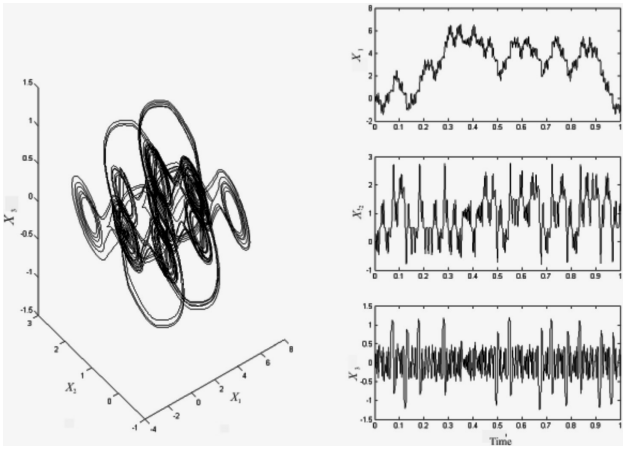

FIGURE 1. (a) 3×3-grid scroll attractor in 2D and (b) time series of chaotic behavior.

$$p_i = M_{x_2} + \frac{1}{2} + (i-1)(M_{x_2} + N_{x_2} + 1),$$
$$i = 1, 2, \ldots, m-1,$$
$$\beta = M_{x_2} + N_{x_2} + 1.$$

In Ref. 7 it is shown that the equilibrium points are located in the (x_1, x_2)-plane, and that this family has $m \times (M_{x_2} + N_{x_2} + 1)$ equilibrium points. For this reason, this chaos generator model has been called *strange attractor family $m \times (M_{x_2} + N_{x_2} + 1)$-scroll grid attractors*. For example, some generated 2D-grid scroll chaotic attractors: 2×2-scroll, 2×3-scroll, 4×4-scroll, and 4×5-scroll grid attractors, and their corresponding nonlinearities are given in [7,8]. Below, we show the family of 3×3-scroll grid chaotic attractor of particular interest to us for synchronization purposes.

3.3. 3×3-grid scroll attractor

For chaos generator model (11) with nonlinear functions (12) and (13), and considering $a = 0.8$, and $M_{x_2} = 0$, $N_{x_2} = 2$, and $m = 3$, we have the particular nonlinear functions:

$$f_1(x_2) = g_{\frac{1}{2}}(x_2) + g_{\frac{3}{2}}(x_2), \tag{14}$$
$$f_2(x_1) = 3\left(g_{\frac{1}{2}}(x_1) + g_{\frac{7}{2}}(x_1)\right),$$

which corresponds to the *family of chaotic attractors with 3×3-grid scroll attractor in 2D* (see Fig. 1). In the next section, we shall synchronize the 2D-grid scroll attractors defined by (11)-(13) with nonlinearities (14), by using the methodology presented in Sec. 2.

4. Synchronization of multi-scroll chaotic attractors

The chaos generator model (11)-(13) in Generalized Hamiltonian form, according to Eq. (3) (as *master model*) is given by

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = \begin{bmatrix} 0 & \frac{1}{2a} & \frac{1}{2} \\ -\frac{1}{2a} & 0 & 1 \\ -\frac{1}{2} & -1 & 0 \end{bmatrix} \frac{\partial H}{\partial x} + \begin{bmatrix} 0 & \frac{1}{2a} & -\frac{1}{2} \\ \frac{1}{2a} & 0 & 0 \\ -\frac{1}{2} & 0 & -a \end{bmatrix} \frac{\partial H}{\partial x} + \begin{bmatrix} -f_1(x_2) \\ 0 \\ a f_2(x_1) \end{bmatrix} \quad (15)$$

with nonlinearities $f_1(x_2)$ and $f_2(x_1)$ given by (14). We take as Hamiltonian energy function

$$H(x) = \frac{1}{2}\left[a x_1^2 + a x_2^2 + x_3^2\right] \quad (16)$$

and as gradient vector

$$\frac{\partial H}{\partial x} = \begin{bmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} a x_1 \\ a x_2 \\ x_3 \end{bmatrix}.$$

The destabilizing vector field calls for x_1 and x_2 signals to be used as the outputs, of the master model (15). We use $y = x_2$ in (15). The matrices $\mathcal{C}$, $\mathcal{S}$, and $\mathcal{I}$ are given by

$$\mathcal{C} = \begin{bmatrix} 0 & \frac{1}{a} & 0 \end{bmatrix},$$

$$\mathcal{S} = \begin{bmatrix} 0 & \frac{1}{2a} & -\frac{1}{2} \\ \frac{1}{2a} & 0 & 0 \\ -\frac{1}{2} & 0 & -a \end{bmatrix}, \quad \mathcal{I} = \begin{bmatrix} 0 & \frac{1}{2a} & \frac{1}{2} \\ -\frac{1}{2a} & 0 & 1 \\ -\frac{1}{2} & -1 & 0 \end{bmatrix}.$$

The pair $(\mathcal{C}, \mathcal{S})$ is observable. Therefore, the nonlinear state observer for (15), to be used as the *slave model*, is designed according to Eq. (4) as

$$\begin{bmatrix} \dot{\xi}_1 \\ \dot{\xi}_2 \\ \dot{\xi}_3 \end{bmatrix} = \begin{bmatrix} 0 & \frac{1}{2a} & \frac{1}{2} \\ -\frac{1}{2a} & 0 & 1 \\ -\frac{1}{2} & -1 & 0 \end{bmatrix} \frac{\partial H}{\partial \xi} + \begin{bmatrix} 0 & \frac{1}{2a} & -\frac{1}{2} \\ \frac{1}{2a} & 0 & 0 \\ -\frac{1}{2} & 0 & -a \end{bmatrix} \frac{\partial H}{\partial \xi} + \begin{bmatrix} -f_1(y) \\ 0 \\ a f_2(\xi_1) \end{bmatrix} + \begin{bmatrix} k_1 \\ k_2 \\ k_3, \end{bmatrix} e_y. \quad (17)$$

With gain k_i, $i = 1, 2, 3$ to be selected in order to guarantee asymptotic exponential stability to zero of the state reconstruction error trajectories (*i.e.*, synchronization error $e(t)$). From Eqs. (15) and (17) we have that the synchronization error dynamics is governed by

$$\begin{bmatrix} \dot{e}_1 \\ \dot{e}_2 \\ \dot{e}_3 \end{bmatrix} = \begin{bmatrix} 0 & \frac{1}{2a} & \frac{1}{2} \\ -\frac{1}{2a} & 0 & 1 \\ -\frac{1}{2} & -1 & 0 \end{bmatrix} \frac{\partial H}{\partial e} + \begin{bmatrix} 0 & \frac{1}{2a} & -\frac{1}{2} \\ \frac{1}{2a} & 0 & 0 \\ -\frac{1}{2} & 0 & -a \end{bmatrix} \frac{\partial H}{\partial e} + \begin{bmatrix} k_1 \\ k_2 \\ k_3 \end{bmatrix} e_y. \quad (18)$$

5. Stability of the synchronization error

In this section, we examine the stability of the synchronization error (18) between the master model (15) described in Hamiltonian form and the slave model (17), corresponding to the designed nonlinear observer. According to the above-mentioned Theorem 1, for this particular case, we have the stability condition

$$2\left[\mathcal{S} - \frac{1}{2}\left(K\mathcal{C} + \mathcal{C}^T K^T\right)\right] < 0$$

that is,

$$2\begin{bmatrix} 0 & \frac{1-k_1}{2a} & -\frac{1}{2} \\ \frac{1-k_1}{2a} & -\frac{k_2}{a} & -\frac{k_3}{2a} \\ -\frac{1}{2} & -\frac{k_3}{2a} & -a \end{bmatrix} 0 < 0. \quad (19)$$

By applying the Sylvester's Criterion -which provides a test for negative definite matrices, we have that the above 3×3-matrix will be negative definite , if we choose k_1, k_2, and k_3 such that the condition (19) holds, *i.e.*:

$$k_1 \neq 1, \quad (20)$$

$$k_3 < -\frac{a\left[k_2 + (1-k_1)^2\right]}{1-k_1}.$$

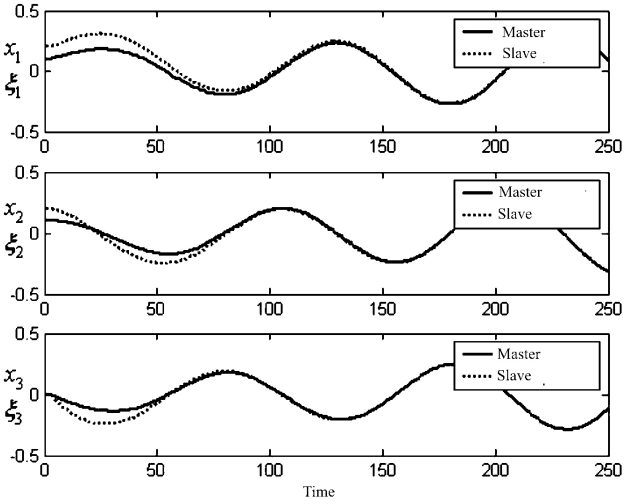

FIGURE 2. Synchronization between state trajectories of master (15) and slave (17) models.

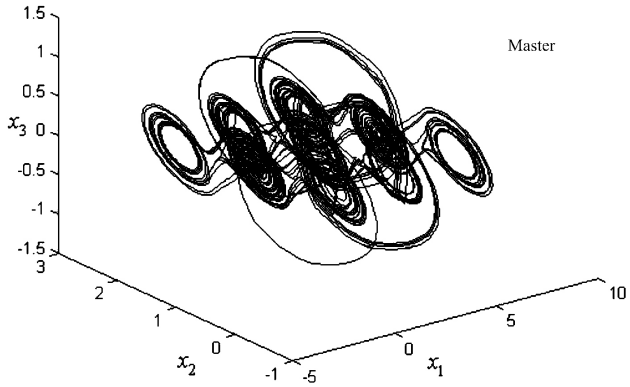

FIGURE 3. 3×3-grid scroll attractor, generated by master model (15).

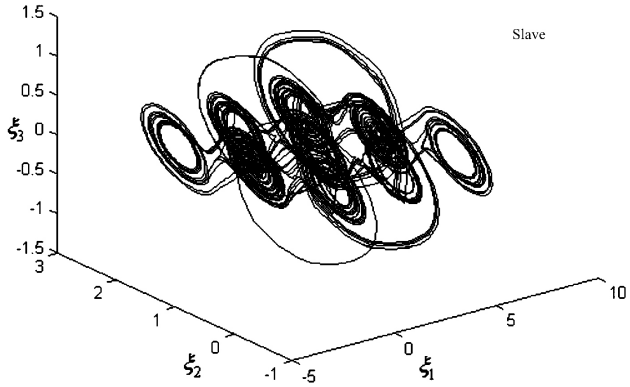

FIGURE 4. 3×3-grid scroll attractor, generated by slave model (17).

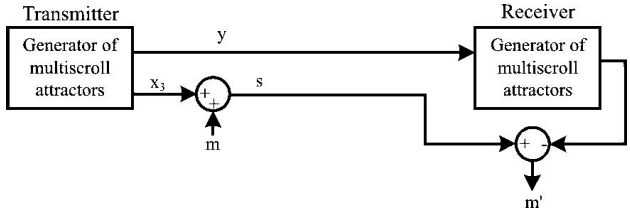

FIGURE 5. Chaotic communication scheme using two transmission channels.

When we have selected $K=(k_1,k_2,k_3)^T$ with k_1=k_2=k_3=2, which satisfies (20), and considering the initial condition $x(0)=(0.1,0.1,0)$, $\xi(0)=(0.2,0.2,0)$, for $a=0.8$ and $M_{x_2}=0$, $N_{x_2}=2$, $m=3$, we carry out the following numerical simulations by using a fourth-order Runge-Kutta integration algorithm with time step 0.01. Nevertheless, it is interesting to note that multistep algorithms can be more efficient for the data computation, as is shown in Ref. 28. Figure 2 shows the state trajectories between the master and slave models (15) and (17), respectively, and their synchronization. Figures 3 and 4 show the 3×3-grid scroll chaotic attractors generated by the master (15) and slave (17) models, respectively, and their synchronization.

Remark 1. We do not take the output $y=x_1$, given that this selection cannot satisfy the condition of Theorem 1.

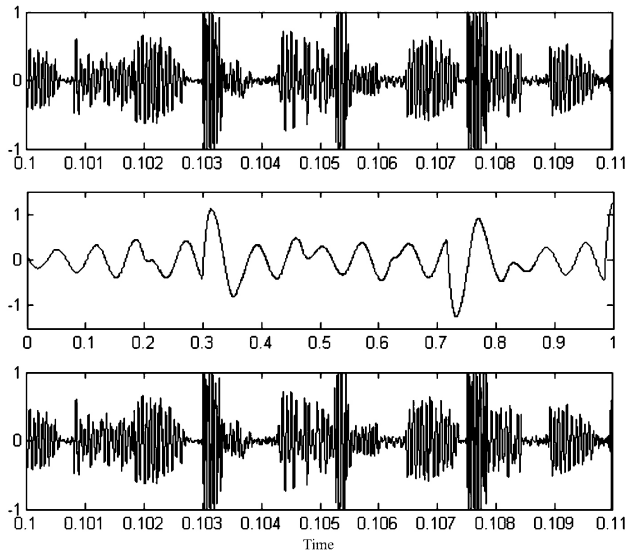

FIGURE 6. Secret communication process of an audio message: original audio message (top of figure), transmitted chaotic signal (middle of figure), and recovered audio message at the receiver end.

6. Secret communication

In this final part, we apply the synchronization of two models generating multi-scroll attractors to private communication of confidential information. In particular, we transmit encrypted analog and digital information.

6.1. Chaotic encoding by using two transmission channels

We resort to a communication scheme for chaotic masking by using two transmission channels. It is well-known that, with this scheme, we achieve faster synchronization and privacy; one channel is used to synchronize master and slave chaos generator models (15) and (17) via coupling signal $y(t)=x_2(t)$. Meanwhile, the other channel is used to transmit hidden audio message $m(t)$, which is recovered at the receiver end, by means of the comparison between signals $s(t)=x_3(t)+m(t)$ and $\xi_3(t)$ (see Fig. 5). On the other hand, Fig. 6 illustrates the secret communication process of an audio message: the private audio message $m(t)$ to be hidden and transmitted (top of figure), the transmitted chaotic signal $s(t)=x_3(t)+m(t)$ (middle of figure), and the recovered audio message $m\prime(t)$ at the receiver end (bottom of figure). The confidential audio message used is a fragment of the song "Billie Jean".

Remark 2. In this cryptosystem, the processes of encryption and synchronization are completely separated with no interference between them. So, encrypted information does not interfere with synchronization, therefore not increasing the sensitivity of synchronization to external errors. As a result, this cryptosystem gives faster synchronization (by the observer gain selected) and security (due to the complex signal used $s(t)$). For greater security, it is possible to incorpo-

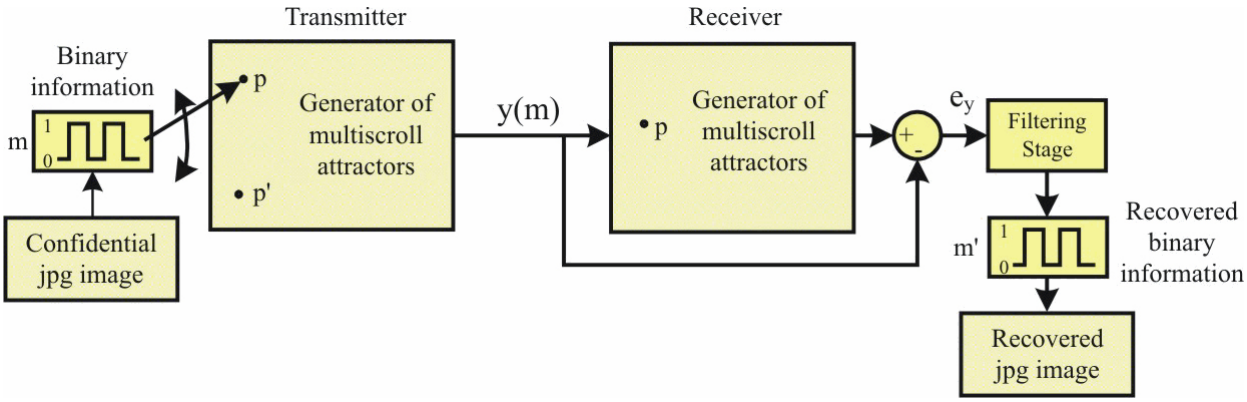

FIGURE 7. Digital communication scheme.

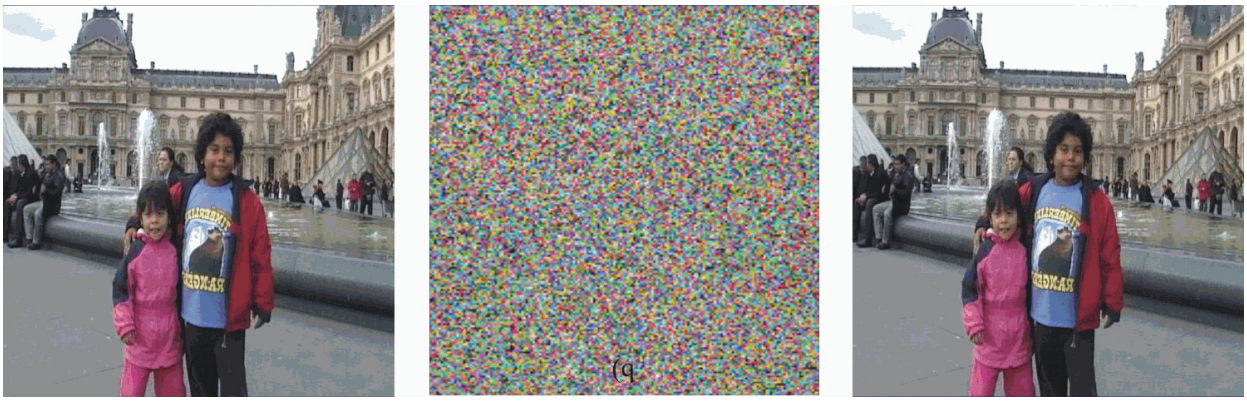

FIGURE 8. (a) Confidential jpg image message to be hidden and transmitted. (b) Chaotic encrypted image through a public channel. (c) Recovered jpg image message at the receiver end.

rate a complex encryption function similar to the technique reported in Ref. 20.

6.2. Chaotic encoding for jpg image transmission

The chaotic communication scheme to transmit hidden jpg images is shown in Fig. 7. The private transmission is achieved by using the chaotic switching technique. A binary signal $m(t)$ is used to modulate one parameter of the transmitter. According to the value of $m(t)$, at any given time t, the transmitter has either the parameter value p or $p\prime$. For example, if it is a '0' bit, then the transmitter has the parameter value p, otherwise the parameter value is $p\prime$. So, $m(t)$ controls a switch whose action changes the parameter values between p and $p\prime$ in the transmitter, while the receiver always has the parameter value p. The synchronization error $e_y(t) = x_2(m(t)) - \xi_2(t)$ determines if the received signal $y(m(t))$ corresponds to a '0' or '1' bit. Thus, when transmitter and receiver synchronize, it can be interpreted as a '0' bit, and when transmitter and receiver do not synchronize, it will be interpreted as a '1' bit.

In our case, to transmit an encrypted jpg image via chaotic switching, let a be the parameter to be modulated in the transmitter (15). The binary information $m(t)$ is added to a as follows: $a(t) = a + r \cdot m(t)$, where $r = 0.001$. Previously, in the encryption process, the jpg image message is converted to a binary sequence of numbers, to obtain $m(t)$. Let us consider the jpg image shown in Fig. 8a as the confidential message to be transmitted. Figure 8b illustrates the chaotic encrypted jpg image transmission through a public channel, when the parameter a in the transmitter is switched between $a(1) = 0.8$ and $a(0) = 0.801$. Meanwhile, at the receiver end, the synchronization error detection $e_y(t) = x_2(m(t)) - \xi_2(t)$ is achieved for the recovered binary sequence $m\prime(t)$ after a filtering stage. Finally, from $m\prime(t)$, the recovered jpg image message is shown in Fig. 8c. The rule for obtaining the binary sequence $m\prime(t)$ is based on $e_y(t)$ for each bit period to assign a '0' or '1' bit, as follows: when $e_y(t) \neq 0$, the it is a '1' bit and when $e_y(t) = 0$, then it is a '0' bit. Note that an eavesdropper will obtain the encrypted image shown in Fig. 8b from the chaotic signal $x_2(m(t))$.

Remark 3. It is a secure cryptosystem, where the hidden information $m(t)$ in the transmitted signal $y(m(t))$ cannot be reconstructed by means of the techniques reported in the literature, *e.g.* [29,30]. Nevertheless, if we wish to increase the encryption security even more, then we can appeal to multi-

step parameter modulation as reported in Ref. 20. A complete analysis of such issues will appear elsewhere.

7. Concluding remarks

In this paper, we have presented synchronization between two chaos generator models of the 3×3-scroll chaotic attractor in 2D. By means of computer simulations, we have illustrated the chaotic synchronization of the mentioned models coupled in master-slave configuration. The approach can be easily implemented in the experimental setup, and shows great potential for actual communication systems in which the encoding is required to be secure.

In a forthcoming article we shall be concerned with the physical implementation of the synchronization of chaos models generating multi-scroll chaotic attractors. Of course, an important issue will show (by means of a complete analysis) that the proposed cryptosystems are secure in the sense of the attacks reported in Refs. 29 and 30.

Acknowledgments

This work was supported by the CONACYT, México under Research Grant No. J49593-Y and P50051-Y, and by the UABC, México, under Research Grant No. 0465.

∗. Corresponding author: CICESE, Electronics and Telecommunications Department, P.O. Box 434944, San Diego, CA 92143-4944, USA, Phone: +52.646.1750500, Fax: +52.646.1750554, e-mail: ccruz@cicese.mx

1. J.A.K. Suykens and J. Vandewalle, *IEEE Proceedings-G* **138**(1991) 595.
2. J.A.K. Suykens and J. Vandewalle, *IEEE Trans. Circuits Syst. I* **40** (1993) 861.
3. J.A.K. Suykens, A. Huang, and L.O. Chua, *Archiv fur Ekektronik und Uberttragungstechnik* **51** (1997) 131.
4. A.S. Elwakil and M.P. Kennedy, *IEEE Trans. Circuits Syst. I* **47**(2000) 76.
5. W.K.S. Tang, G.Q. Zhong, G. Chen, and K.F. Man, *IEEE Trans. Circuit. Syst. I* **48** (2001) 1369.
6. M.E. Yalçin, S. Ozoğuz, J.A.K. Suykens, and J. Vandewalle, *Electronics Letters* **37** (2001) 147.
7. M.E. Yalçin, J.A.K. Suykens, J.P.L. Vandewalle, and S. Özoğuz, *Int. J. Bifurc. Chaos* **12** (2002) 23.
8. M.E. Yalçin, J.A.K. Suykens, and J.P.L. Vandewalle, *Cellular neural networks, multi-scroll chaos and synchronization*. World Scientific Series on Nonlinear Science, Series A, Vol. 50, World Scientific Publishing Co. Pte. Ltd., Singapore, 2005.
9. J. Lü, S. Yu, H. Leung, and G. Chen, *IEEE Trans. Circuits Syst. I* **53** (2006) 149.
10. L.M. Pecora and T.L. Carroll, *Phys. Rev. Lett.* **64** (1990) 821.
11. H. Nijmeijer and I.M.Y. Mareels, *IEEE Trans. Circuits Syst. I* **44** (1997) 882.
12. Special Issue on Control and synchronization of chaos. *Int. J. Bifurc. Chaos* **10**(3-4) (2000).
13. C. Cruz-Hernández and H. Nijmeijer, *Int. J. Bifurc. Chaos* **10** (2000) 763.
14. H. Sira-Ramírez and C. Cruz-Hernández, *Int. J. Bifurc. Chaos* **11** (2001) 1381.
15. A.Y. Aguilar-Bustos and C. Cruz-Hernández, *Nonlinear Dynamics and Systems Theory* **6** (2006) 319.
16. D. López-Mancilla and C. Cruz-Hernández, *Chaos, Solitons and Fractals* **37** (2008) 1172.
17. C. Cruz-Hernández and A.A. Martynyuk *Advances in chaotic dynamics with applications* (Cambridge Scientific Publishers Ltd., 2008) Vol. 4.
18. K.M. Cuomo and A.V. Oppenheim, *Phys. Rev. Lett*. **71** (1993) 65.
19. K. Murali, *Int. J. Bifurc. Chaos* **10** (2000) 2489.
20. J. Zhong-Ping, *IEEE Trans. Circ. Syst. I* **49** (2002) 92.
21. P. Palaniyandi and M. Lakshmanan, *Int. J. Bifurc. Chaos* **11** (2001) 2031.
22. C. Cruz-Hernández, *Nonlinear Dynamics and Systems Theory* **4** (2004) 1.
23. D. López-Mancilla and C. Cruz-Hernández, *Nonlinear Dynamics and Systems Theory* **5** (2005) 141.
24. C. Cruz-Hernández, D. López-Mancilla, V. García, H. Serrano, and R. Núñez, *J. Circuits, Syst. Computers* **14** (2005) 453.
25. D. López-Mancilla and C. Cruz-Hernández, *Rev. Mex. Fís.* **51** (2005) 265.
26. C. Cruz-Hernández and N. Romero-Haros, *Communications in Nonlinear Science and Numerical Simulation* **13** (2008) 645.
27. C. Posadas-Castillo, R.M. López-Gutiérrez, and C. Cruz-Hernández, *Communications in Nonlinear Science and Numerical Simulation* **13** (2008) 1655.
28. E. Tlelo-Cuautle, J.M. Muñoz-Pacheco, and J. Martínez-Carballido, *Applied Mathematics and Computation* **194** (2007) 486.
29. G. Pérez and H.A. Cerdeira, *Phys. Rev. Lett*. **74** (1995) 821.
30. G. Alvarez, F. Montoya, M. Romera, and G. Pastor, *Chaos, Solitons and Fractals* **21** (2004) 783.