Nonlinear Dynamics and Systems Theory, **8**(3) (2008) 221–236

Synchronization of Different Hyperchaotic Maps for Encryption

A.Y. Aguilar–Bustos [1,2], C. Cruz–Hernández [2*],
R.M. López–Gutiérrez [3] and C. Posadas–Castillo [3]

[1] *Ensenada Technological Institute (ITE),*
Blvd. Tecnológico 150, Ex-Ejido Chapultepec, 22780 Ensenada, B.C., México.
[2] *Electronics and Telecommunications Department,*
Scientific Research and Advanced Studies of Ensenada (CICESE),
Km. 107, Carretera Tijuana-Ensenada, 22860 Ensenada, B.C., México.
[3] *Baja California Autonomous University (UABC),*
Km. 103, Carretera Tijuana-Ensenada, 22860 Ensenada, B.C., México.

Received: June 26, 2008; Revised: July 24, 2008

Abstract: In this paper, the synchronization problem of different hyperchaotic maps is presented. In particular, we appeal to model-matching approach from nonlinear control theory to synchronize the otputs of the coupled Rössler and Hénon hyperchaotic maps. An application to secure communication of confidential information is also given. By using a hyperchaotic encryption scheme, we show that output synchronization of different hyperchaotic maps is indeed suitable for encryption, transmission, and decryption of confidential information which can be implemented for use in computer communication.

Keywords: *Synchronization; hyperchaotic maps; model-matching problem; secure communication.*

Mathematics Subject Classification (2000): 37N35, 65P20, 68P25, 70K99, 93D20, 94A99.

* Corresponding author: ccruz@cicese.mx

1 Introduction

In modern communication systems, data secury is a requirement of central importance. As a result, with the rapid development of the different communication systems, there exits a great demand of cryptography algorithms to protect the confidential information, see e.g. [1, 2]. In particular, nowadays most communication is through computers and even real-time communication systems are digital. Recently, by using chaotic dynamics to address the secure communication problem has received a great interest. In several articles is reported the extreme relationship between chaotic dynamics and conventional cryptography, some common properties are:

- a small variation in the input originates a large change at the output,
- the output preserves the same distribution for any input,
- a small variation in the local area originates a large variation in the whole space,
- a simple process has a very high complexity, and
- a deterministic system originates a pseudorandom dynamics.

During last decades, the problem of chaos synchronization has received a lot attention, see e.g. [3, 4, 5, 6, 7, 8, 9, 37] and references therein. This interest increases by practical reasons, mainly to design secure communication systems. Chaos synchronization can be used in different ways for encryption of confidential information in secure communication systems, see e.g. [7, 11, 12, 13, 14, 15, 26, 28, 29, 33, 35, 36, 37]. However, in subsequent works, see e.g. [16, 17] it has been shown that encrypted information by means of comparatively "simple" chaos with only one positive Lyapunov exponent, does not ensure a sufficient security level. For higher security purpose, *hyperchaotic dynamics* characterized by more than one positive Lyapunov exponents are advantageous over simple chaotic dynamics.

On the basis of these considerations, one way to enhance the level of encryption security is by applying conventional *cryptographic techniques* to the information in *combination with chaotic encryption schemes* [18, 19]. Another way is to encode information by using systems generated of *high dimensional chaotic attractors,* or *hyperchaotic attractors*. In this case, one generally encounters *multiple positive Lyapunov exponents*. However, hyperchaos synchronization is a much more difficult problem, see e.g. [9, 21, 22, 23, 24, 25, 27, 34, 37]. The level of security is also enhanced by using *chaos modeled by delay differential equations*, such systems have an infinite-dimensional state space, and produce hyperchaotic dynamics with an *arbitrarily large number of positive Lyapunov exponents* [26, 27, 28, 29].

The aim of this paper is to present a communication scheme to transmit encrypted audio and image information, which is based on synchronized different hyperchaotic discrete-time systems; in particular, we use the generalized Rössler and Hénon maps. This objective is achieved by appealing to nonlinear control theory, in particular, we use the model-matching approach given in [37]. We enumerate several advantages over the existing synchronization methods reported in the current literature:

- It enables synchronization be achieved in a systematic way and clarifies the issue of deciding on the nature of the coupling signal to be transmitted.
- It can be successfully applied to many chaotic and hyperchaotic systems (in continuous-time, or discrete-time).
- It can be applied to identical and nonidentical systems in continuous-time [7] and in discrete-time [37].
- It does not require the computation of any Lyapunov exponent.
- It does not require initial conditions belonging to the same basin of attraction.

In addition, we use output synchronization for encoding, transmission, and decoding of confidential information.

The organization of the sections of this paper is as follows: In Section 2, the proposed hyperchaotic encryption scheme is described. In Section 3, a review on output synchronization of hyperchaotic maps via model matching is provided. By using computer simulations, the approach used is explained by means of the hyperchaotic generalized Rössler and Hénon maps in Section 4. An application of output synchronization to secure communication systems is illustrated in Section 5. The paper is concluded with some remarks in Section 6.

2 Hyperchaotic Encryption Scheme

In this section, a cryptosystem based on synchronized hyperchaotic (three-dimensional) maps is described. The aim is to transmit encrypted information from side A to side B (the so-called *authorized* communicating remote parts) as is illustrated in Figure 2.1. A confidential *information* m is to be transmitted over an *insecure* communication channel. To avoid any *unauthorized* part (intruder) located at the mentioned channel; m is encrypted prior to transmission to generate an *encrypted* information s,

$$s = f(m, k),$$

by using hyperchaotic dynamics generated by the map f on side A.

The encrypted information s is sent to remote side B, where m is *recovered* as $\hat{m}$ from the hyperchaotic decryption. g, as

$$\hat{m} = g(s, k).$$

If f and g have used the same *key* k, then at remote side B it is possible to obtain the recovered information $\hat{m} = m$. A *secure* channel (dashed line) is used for transmission of the keys. Generally, this secure communication channel is a courier and is too slow for the transmission of the confidential information m. Our hyperchaotic cryptosystem is reliable, if it preserves the security of m, i.e. if $m\prime \neq m$ for even the best *cryptanalytic* function h, given by

$$m\prime = h(s).$$

To achieve the proposed hyperchaotic encryption scheme, we appeal to three-dimensional hyperchaotic *generalized Rössler and Hénon maps* for encryption/decryption

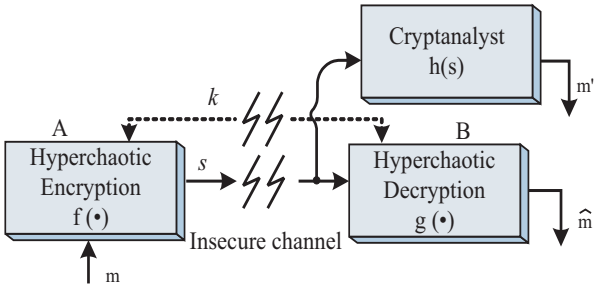

Figure 2.1: Secure hyperchaotic cryptosystem.

purposes (f and g, respectively), as will be shown in Section 5. The hyperchaotic Rössler and Hénon maps have a number of parameters determining their dynamics; such parameters and initial conditions are the coding "keys", k. We expect that it can perform the objective of the secure communication and the transmitting information can be recovered at the receiver. In order to guarantee the encryption and decryption, the generalized hyperchaotic Rössler and Hénon maps have to achieve the so-called *synchronization* on both remote sides A and B. For such reason, our first problem to solve is to design a control law u for hyperchaotic synchronization, which will be shown in next sections.

3 Output Synchronization of Different Hyperchaotic Maps

Consider a nonlinear discrete-time system, defined by

$$P : \begin{cases} x(k+1) &= f(x(k), u(k)), \\ y(k) &= h(x(k)), \end{cases} \tag{1}$$

where the state vector $x \in X$ (an open set in $\mathbb{R}^n$), the input u is inside an open set U in $\mathbb{R}$, and the output y belongs to an open set Y in $\mathbb{R}$. The mappings $f : X \times U \to X$ and $h : X \to Y$ are analytic. In addition, consider the following nonlinear discrete-time system, described by

$$M : \begin{cases} x_M(k+1) &= f_M(x_M(k), u_M(k)), \\ y_M(k) &= h_M(x_M(k)), \end{cases} \tag{2}$$

where the state vector $x_M \in X_M$ (an open set in $\mathbb{R}^{n_M}$), the input $u_M \in U_M$ (an open set in $\mathbb{R}$), and the output y_M belongs to an open set Y_M in $\mathbb{R}$. Also, the mappings $f_M : X_M \times U_M \to X_M$ and $h_M : X_M \to Y_M$ are analytic. Assume that for certain parameter values, the uncontrolled discrete-time dynamical systems (1) and (2), i.e. for $u(k) = u_M(k) = 0$, exhibit *hyperchaotic behavior*; that is, the dynamical systems have *multiple positive Lyapunov exponents*. The synchronization problem addressed here is defined as follows.

Definition 3.1 (Output Synchronization Problem, OSP) [30] The output $y(k)$ of the hyperchaotic discrete-time system (1) **synchronizes** with the output $y_M(k)$ of the hyperchaotic discrete-time system (2), if

$$\lim_{k\to\infty} |y(k) - y_M(k)| = 0, \tag{3}$$

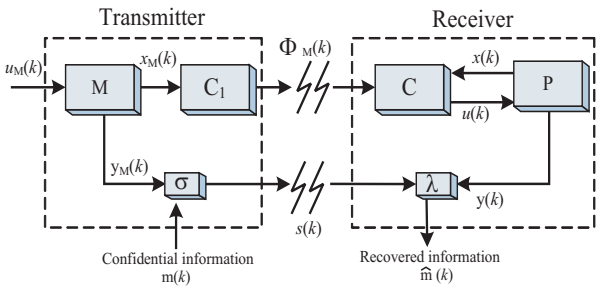

Figure 3.1: Output synchronization scheme based on model matching approach.

no matter which initial conditions $x(0)$ and $x_M(0)$ have, and for suitable input signals $u(k)$ and $u_M(k)$.

Notice that, we are considering *partial synchronization* between hyperchaotic maps (1) and (2), which is a substantial difference with other approaches based on complete synchronization.

Figure 3.1 shows the *output synchronization scheme* by using model-matching approach: the **master** system is the hyperchaotic map M with state x_M, input u_M, and output y_M. The nonlinear function $\phi_M(k) = \phi_M(x_M, u_M)$ is the coupling signal, which is transmitted through a public channel to the slave system, and is used to synchronize the master and slave systems to satisfy the condition (3). The **slave** consists of the hyperchaotic map P and a compensator C. The **compensator** C is utilized to control P with inputs ϕ_M and x, and output u. If the compensator C yields properly the control signal u, then the *output error synchronization* $e(k) = y_E(k) = y(k) - y_M(k)$ *asymptotically converges to zero*.

For secure communications based on previous output synchronization scheme between maps (1) and (2): at the hyperchaotic transmitter, the confidential information is encrypted (by direct modulation, additive masking, or another technique) and sent to the hyperchaotic receiver via a insecure channel. Finally, the original information is decrypted at the receiver end by using output synchronization $e(k) = y_E(k)$. For this purpose, we will use a communication scheme based on *hyperchaotic encryption*, to send encrypted audio and image information.

3.1 Model-matching problem

Considering the hyperchaotic maps (1) and (2), we assume that P evolves in a neighborhood of an equilibrium point x^0; that is, around $(x^0, u^0) \in X \times U$ such that $f(x^0, u^0) = x^0$, with $\{u(k) = u^0 : k \geq 0\}$ being a (constant) input sequence. For this sequence there exists another (constant) output sequence $\{y(k) = h(x^0) = y^0 : k \geq 0\}$. In the same way, let the equilibrium point of model M be denoted by x_M^0 around $(x_M^0, u_M^0) \in X_M \times U_M$. According to Figure 3.1 we are interested in to design a control u for P which, irrespectively of the initial conditions of P and M, makes the output $y(k)$ of P asymptotically converges to the output $y_M(k)$ produced by M under an arbitrary

input $u_M(k)$. This problem is the so-called *discrete-time asymptotic model-matching problem (DAMMP)* from nonlinear control theory which coincides with the OSP, see [7, 37]. Similar to [37] we adopt the following approach: where the DAMMP is reduced into a problem of decoupling the output of a suitable auxiliary system from the input u_M to the model M. In this way, we define an *output error* $y_E(k) = y(k) - y_M(k)$, and we choose the control law $u(k)$ such that the output $y_E(k)$ is decoupled from $u_M(k)$ for all $k \geq 0$, and converges asymptotically to zero. The *auxiliary system* is defined as follows

$$E : \left\{ \begin{array}{rcl} x_E(k+1) & = & f_E(x_E(k), u_E(k), w_E(k)), \\ y_E(k) & = & h_E(x_E(k)), \end{array} \right. \tag{4}$$

with *auxiliary state* $x_E = (x, x_M)^T \in \mathbb{R}^{n+n_M}$, and *auxiliary inputs* $u_E = u$ and $w_E = u_M$, where

$$f_E(x_E, u_E, w_E) = \left(\begin{array}{c} f(x,u) \\ f_M(x_M, u_M) \end{array} \right), \quad h_E(x_E) = h(x) - h_M(x_M).$$

Given this system, together with an equilibrium point $x_E^0 = \left(x^0, x_M^0\right)$ it is known that, if the disturbance-decoupling problem with measurement disturbance w_E associated with the system E has a solution on Ω_0^E, an open and dense subset of $X \times X_M \times U \times U_M$, defined around the equilibrium point $\left(x^0, x_M^0, u^0, u_M^0\right)$, then there exists an analytic mapping γ^E defined on Ω_0^E with the property that the control law

$$u(k) = \gamma^E(x_E(k), w_E(k)) = \gamma^E(x_E(k), u_M(k)) \tag{5}$$

decouples the output y_E of the closed-loop system (4)-(5) from the disturbance w_E for every initial state of x_E in an open and dense subset of $X \times X_M$ contained in Ω_0^E.

The DAMMP is treated in terms of a *relative degree* associated with the outputs y and y_M. Thus, the following definitions are introduced. Let f_0, f_{M_0}, and f_{E_0} be the undriven state dynamics $f(\cdot, 0)$, $f_M(\cdot, 0)$, and $f_E(\cdot, 0, 0)$, respectively, and f_0^j, $f_{M_0}^j$, and $f_{E_0}^j$ the j-times iterated compositions of f_0, f_{M_0}, and f_{E_0} with $f_0^0(x) = x$, $f_{M_0}^0(x_M) = x_M$, and $f_{E_0}^0(x_E) = x_E$.

Definition 3.2 (Relative degree) [31] The output y of the plant Eq. (1) is said to have a relative degree d in an open and dense subset O of $X \times U$ containing the equilibrium point $\left(x^0, u^0\right)$, if

$$\frac{\partial}{\partial u}\left[h \circ f_0^l(f(x,u))\right] \equiv 0$$

for all $0 \leq l \leq d-1$, for all $(x,u) \in O$, and

$$\frac{\partial}{\partial u}\left[h \circ f_0^d(f(x,u))\right] \neq 0$$

for all $(x,u) \in O$.

A similar definition can be given for the relative degree of the model M Eq. (2), d_M, in an open and dense subset O_M, of $X_M \times U_M$ containing the equilibrium point $\left(x_M^0, u_M^0\right)$.

The following theorem gives necessary and sufficient conditions for the local solvability of the OSP for hyperchaotic maps.

Theorem 3.1 *[37] Consider the hyperchaotic maps P Eq. (1) and M Eq. (2) around, respectively, their equilibria $\left(x^0, u^0\right)$ and $\left(x_M^0, u_M^0\right)$. Suppose that the outputs y of P and y_M of M have finite relative degree d and d_M, respectively defined on O and O_M. Assume that for all $x_E = (x, x_M)^T \in X \times X_M$ and $u_M \in U_M$,*

$$0 \in Im\left\{h_E \circ f_{E_0}^d \left(f_E\left(x_E, \cdot, u_M\right)\right)\right\},$$

holds, where $Im\{\varphi\}$ denotes the image of φ. Then the OSP is locally solvable on Ω_0^E if and only if

$$d \leq d_M. \tag{6}$$

If the condition (6) holds, then from definition of relative degrees d and d_M we have that there exists an analytic mapping $\gamma^E : \mathbb{R}^{n+n_M} \times \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ such that

$$y_E(k+d+1) = h_E \circ f_{E_0}^d \circ f_E\left(x_E(k), \gamma^E\left(x_E(k), u_M(k), v(k)\right)\right) = v(k),$$

with $v \in \mathbb{R}$ an external control, or equivalently,

$$S\left(x(k), \gamma^E\left(x_E(k), u_M(k), v(k)\right)\right) =$$

$$v(k) - h \circ f_0^d \circ f(x(k)) + h_M \circ f_{M_0}^l \circ f_M\left(x_M(k), u_M(k)\right).$$

The analytic mapping $\gamma^E\left(x_E, u_M, v\right)$ is the inverse of $S(x, \cdot)$, that is

$$\gamma^E\left(x_E(k), u_M(k), v(k)\right) =$$

$$S^{-1}\left(x(k),\ v(k) - h \circ f_0^d \circ f(x(k)) + h_M \circ f_{M_0}^l \circ f_M\left(x_M(k), u_M(k)\right)\right), \tag{7}$$

where the external control is given by

$$v(k) = -\sum_{l=0}^{d} \alpha_l \left[h \circ f_0^l(x(k)) - h_M \circ f_{M_0}^l\left(x_M(k)\right)\right]. \tag{8}$$

Under the new coordinates

$$\left(\zeta\left(x_E\right), x_M\right) = \phi\left(x_E\right) = \phi\left(x, x_M\right),$$

where $\zeta\left(x_E\right) = \left(\zeta_1\left(x_E\right), ..., \zeta_{d+1}\left(x_E\right)\right)^T$ and $\zeta_i\left(x_E\right) = h_{E_i} \circ f_{E_0}^{i-1}\left(x_E\right) = \xi_i(x) - h_{M_i} \circ f_{M_0}^{i-1}\left(x_M\right)$ for all $i = 1, 2, \ldots, d+1$. The closed-loop auxiliary system E, by using the control law $u = \gamma^E\left(x_E, u_M\right)$ Eqs. (7)-(8), takes the form

$$\begin{aligned}
\zeta_i(k+1) &= \zeta_{i+1}(k), \qquad i = 1, ..., d, \\
\zeta_{d+1}(k+1) &= -\alpha_0 \zeta_1(k) - \ ... \ - \alpha_d\ \zeta_{d+1}(k) = v(k), \\
x_M(k+1) &= f_M\left(x_M(k), u_M(k)\right), \\
y_E(k) &= \zeta_1(k).
\end{aligned} \tag{9}$$

From Eq. (9) we see that the output $y(k)$ of the closed-loop slave system P differs from the output y_M of the model M by a signal $y_E(k)$ obeying the linear difference equation

$$y_E(k+d+1) + \alpha_d\ y_E(k+d) + \ldots + \alpha_1 y_E(k+1) + \alpha_0\ y_E(k) = 0,$$

where $\alpha_0, \ldots, \alpha_d$ are constant real coefficients. A proper location of the roots of the polynomial

$$\lambda^{d+1} + \alpha_d \lambda^d + \ldots + \alpha_1 \lambda + \alpha_0$$

entails the desired asymptotic behavior $y_E(k) = 0$, i.e. $y(k)$ converges to $y_M(k)$ as $k \to \infty$, and therefore the output synchronization condition (3) holds. We can identify two subsystems in the closed-loop system (9), as follows:

1. The subsystem is described by

$$x_M(k+1) = f_M(x_M(k), u_M(k)),$$

which represents the dynamics of the model M, and

2. The subsystem is described by

$$\zeta(k+1) = A\zeta(k),$$

where

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -\alpha_0 & -\alpha_1 & -\alpha_2 & \cdots & -\alpha_d \end{pmatrix},$$

which represents the dynamics of the signal $y_E(k)$.

The dynamics of model M is stable by assumption and, if we choose u Eqs. (7)–(8) such that the eigenvalues of matrix A have magnitude strictly less than one, then the closed-loop system (9) will be exponentially stable, and the output synchronization condition (3) holds.

3.2 Output synchronization procedure

From Eq. (5) we can express the control law u in the following form

$$u(k) = \gamma^E(x(k), x_M(k), u_M(k)) = \gamma^E(x(k), \phi_M(x_M(k), u_M(k))), \tag{10}$$

where the nonlinear function $\phi_M(x_M, u_M)$ is the coupling signal to be transmitted from the master M to construct the control law u in C, which solves the OSP, see Figure 3.1. In the context of synchronization, a key observation, provided by the special form of the control law u in (10), is that the nonlinear function $\phi_M(x_M, u_M)$ fixes the coupling signal to be transmitted to the slave system. We rewrite the following procedure to achieve output synchronization between hyperchaotic maps P and M proposed in [37]:

Step 1. Given two hyperchaotic maps $x(k+1) = f(x(k))$ and $x_M(k+1) = f_M(x(k))$ we write it in the forms P Eq. (1) and M Eq. (2) by adding the control inputs $u(k)$ and $u_M(k)$, respectively.

Step 2. We define properly the outputs y and y_M for maps P and M, respectively; such that the OSP has a solution, that is the condition $d \leq d_M$ holds.

Step 3. We obtain the control law u according to Eqs. (7)-(8).

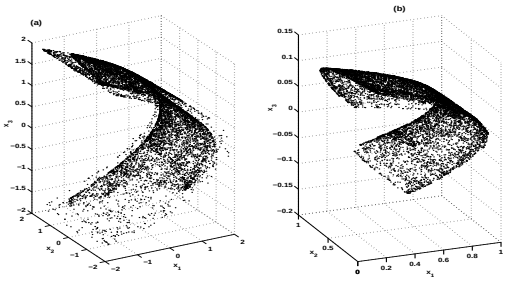

Figure 4.1: Hyperchaotic attractors generated by the uncontrolled: (a) Hénon and (b) Rössler maps.

Step 4. From $u = \gamma^E(x_E, u_M)$, we proceed to identify the nonlinear coupling signal $\phi_M(x_M, u_M)$.

Step 5. Once the coupling signal $\phi_M = \phi_M(x_M, u_M)$ has been decided, then the output y of slave P can track arbitrary the reference signal y_M of model M in the sense of condition (3).

In next section, we will appeal to the above procedure to synchronize the outputs of the hyperchaotic generalized Hénon and Rössler maps, which is a necessary condition in secure communications for encryption and decryption of confidential information.

4 Output Synchronization of Hyperchaotic Hénon and Rössler Maps

Consider the following hyperchaotic generalized **Hénon map** described by the third order difference equations [38]:

$$\begin{cases} x_1(k+1) &= 1.76 - x_2^2(k) - 0.1x_3(k), \\ x_2(k+1) &= x_1(k), \\ x_3(k+1) &= x_2(k), \end{cases} \tag{11}$$

In addition, consider the **Rössler map** defined by [34]:

$$\begin{cases} x_1(k+1) &= \alpha x_1(k)(1-x_1(k)) - \beta(x_3(k)+\gamma)(1-2x_2(k)), \\ x_2(k+1) &= \delta x_2(k)(1-x_2(k)) + \varsigma x_3(k), \\ x_3(k+1) &= \eta((x_3(k)+\gamma)(1-2x_2(k))-1)(1-\theta x_1(k)), \end{cases} \tag{12}$$

for parameter set: $\alpha = 3.8$, $\beta = 0.05$, $\gamma = 0.35$, $\delta = 3.78$, $\varsigma = 0.2$, $\eta = 0.1$, and $\theta = 1.9$; the uncontrolled generalized Hénon and Rössler maps exhibit hyperchaotic dynamics. Figures 4.1(a) and 4.1(b) show the hyperchaotic attractors projected onto three-dimensional space generated by the generalized Hénon and Rössler maps, respectively (when we have used 10 000 iterations). Following the Step 1, we add the control inputs $u(k)$ and $u_M(k)$ to Hénon and Rössler maps, respectively. In addition for Step 2, we define the outputs $y(k) = x_2(k)$ and $y_M(k) = x_{M2}(k)$ in (11) and (12), respectively. In this way, we have the generalized Hénon map P for the *slave system* (in the form of Eq. (1)), as follows

$$P:\begin{cases} x_1(k+1) &= 1.76 - x_2^2(k) - 0.1x_3(k), \\ x_2(k+1) &= x_1(k), \\ x_3(k+1) &= x_2(k) + u(k), \\ y(k) &= x_2(k) \end{cases} \tag{13}$$

and the Rössler map M for the *master system* (in the form of Eq. (2)), described by

$$M:\begin{cases} x_{M1}(k+1) &= \alpha x_{M1}(k)(1 - x_{M1}(k)) - \beta(x_{M3}(k) + \gamma)(1 - 2x_{M2}(k)) + u_M(k), \\ x_{M2}(k+1) &= \delta x_{M2}(k)(1 - x_{M2}(k)) + \varsigma x_{M3}(k), \\ x_{M3}(k+1) &= \eta((x_{M3}(k) + \gamma)(1 - 2x_{M2}(k)) - 1)(1 - \theta x_{M1}(k)), \\ y_M(k) &= x_{M2}(k), \end{cases} \tag{14}$$

the relative degrees are $d = d_M = 2$, with this the OSP has a solution. In order to obtain the particular solution u (Step 3) to control to P, we define $\zeta_1 = y_E = x_2 - x_{M2}$, in this way, the auxiliary system in new coordinates is described by

$$\begin{aligned} \zeta_1(k+1) &= \zeta_2(k), \\ \zeta_2(k+1) &= \zeta_3(k), \\ \zeta_3(k+1) &= -\alpha_2\zeta_3(k) - \alpha_1\zeta_2(k) - \alpha_0\zeta_1(k) = v\,(k)\,. \end{aligned}$$

The control law u is given by

$$u\,(k) = 10\left(1.76 - x_1^2\,(k) - 0.1x_2\,(k)\right) - a - \phi_M\left(x_M\,(k)\,, u_M\,(k)\right)), \tag{15}$$

where

$$a = -\alpha_2\left(1.76 - x_2^2\,(k) - 0.1x_3\,(k)\right) - \alpha_1 x_1\,(k) - \alpha_0 x_2\,(k)\,.$$

Step 4, from Eq. (15) the coupling function $\phi_M\,(x_M, u_M)$ is given by

$$\phi_M\left(x_M\,(k)\,, u_M\,(k)\right) = -\left(-\alpha_2\rho_1 - \alpha_1\rho_2 - \alpha_0 x_{M2}\,(k)\right) + \rho_4, \tag{16}$$

where

$$\begin{aligned} \rho_1 &= \delta\rho_2\,(1 - \rho_2) + \varsigma\rho_3, \\ \rho_2 &= \delta x_{M2}\,(k)\,(1 - x_{M2}\,(k)) + \varsigma x_{M3}\,(k)\,, \\ \rho_3 &= \eta\left(((x_{M3}\,(k) + \gamma)\,(1 - 2x_{M2}\,(k))) - 1\right)(1 - \theta x_{M1}\,(k))\,, \\ \rho_4 &= \delta\left(\delta\rho_2\,(1 - \rho_2) + \varsigma\rho_3\right)(1 - (\delta\rho_2(1 - \rho_2) + \varsigma\rho_3) + \rho_5, \\ \rho_5 &= \varsigma(\eta(((\rho_3 + \gamma)(1 - 2\rho_2)) - 1)(1 - \theta\rho_6), \\ \rho_6 &= \alpha x_{M1}\,(k)\,(1 - x_{M1}\,(k)) - \beta\,(x_{M3}\,(k) + \gamma)\,(1 - 2x_{M2}\,(k)) + u_M\,(k)\,. \end{aligned}$$

In the following, we carry out some numerical simulations by using the initial conditions $x\,(0) = (0.3, 0, 0.05)$ and $x_M\,(0) = (0.1, 0.2, -0.1)$ with the selection $\alpha_i = 0.1$, $i = 0, 1, 2$. In this case, we use $u_M\,(k) = 0$ to keep the master system M Eq. (14) with hyperchaotic dynamics. With the above selection, Step 5 is achieved.

Figure 4.2 shows the matching between the output signals $y\,(k) = x_2\,(k)$ and $y_M\,(k) = x_{M_2}\,(k)$ (top of figure); in addition, the output synchronization error $e_2\,(k) = x_2\,(k) - x_{M2}\,(k)$ is shown (top of figure). Meanwhile, Figure 4.3 illustrates the synchronization errors $e_1\,(k) = x_1\,(k) - x_{M1}\,(k)$ and $e_3\,(k) = x_3\,(k) - x_{M3}\,(k)$. In this case, notice that

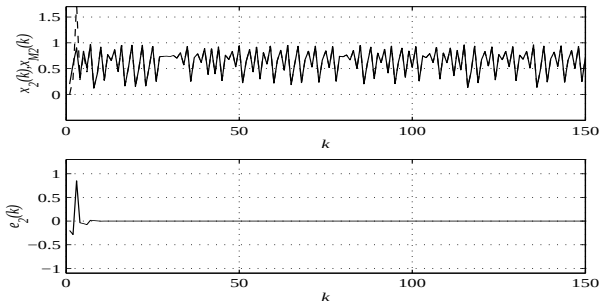

Figure 4.2: Matching between output signals $y(k) = x_2(k)$ and $y_M(k) = x_{M_2}(k)$ (top of figure). Output synchronization error $e_2(k) = x_2(k) - x_{M2}(k)$ (bottom of figure).

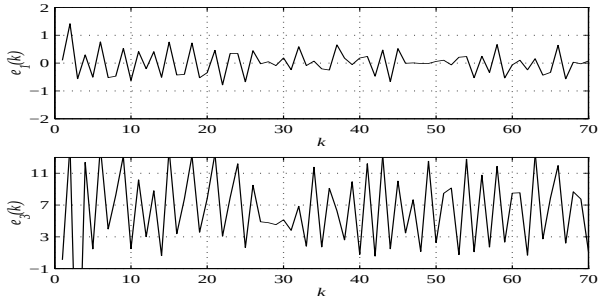

Figure 4.3: Output synchronization errors $e_1(k) = x_1(k) - x_{M1}(k)$ and $e_3(k) = x_3(k) - x_{M3}(k)$.

remaining output synchronization errors $e_1(k)$ and $e_3(k)$ are different from zero; also, notice that there exist big magnitudes of the synchronization errors $e_1(k)$ and $e_3(k)$ which can be estimated by the enormous difference between the hyperchaotic attractors generated by the hyperchaotic Rössler and Hénon maps, which is depicted in Figure 4.4: hyperchaotic attractors generated by the controlled hyperchaotic Hénon and Rössler maps, i.e. after we have achieved output synchronization, when we have used 50 000 iterations.

5 Secure Hyperchaotic Encryption

In this section, we show how output synchronization of the hyperchaotic Hénon and Rössler maps is used in a secure communication scheme to send confidential information. In particular, we propose a communication scheme to transmit encrypted audio and image information.

The communication scheme to send confidential information is shown in Figure 5.1. This cryptosystem uses two transmission channels, in one the complex coupling sequence $\phi_M(k) = \phi_M(x_M(k), u_M(k))$ is transmitted to achieve output synchronization between hyperchaotic transmitter and receiver. The signal $\phi_M(k)$ is only used for fast synchronization and does not contain any information of the confidential information $m(k)$.

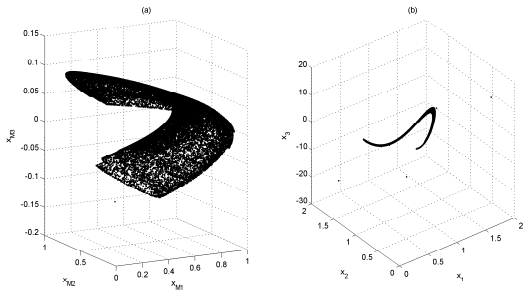

Figure 4.4: Hyperchaotic attractors generated by the controlled (after output synchronization): (a) Rössler and (b) Hénon maps.

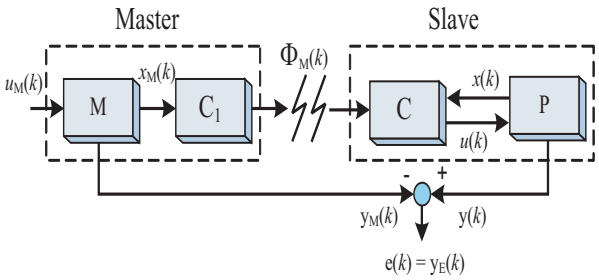

Figure 5.1: Secure communication scheme for transmission of encrypted audio and image information.

While, in the second channel, we send the encrypted confidential information $m\,(k)$, here the nonlinear function $\sigma(\cdot,\cdot)$ encrypts both the information $m\,(k)$ and chaotic output $y_M\,(k)$ in the transmitter. The encrypted message $s\,(k)$ is transmitted to the receiver end. The nonlinear function for encryption is proposed as follows

$$\sigma\,(y_M, m) = s = g_1\,(y_M) + g_2\,(y_M)\,m,$$

and the nonlinear function for decryption is given by

$$\lambda\,(y, s) = \frac{-g_1\,(y)}{g_2\,(y)} + \frac{s}{g_2\,(y)}.$$

In particular, the *encryption function* installed in the transmitter computer is given by

$$\sigma\,(y_M, m) = y_M^3 + \left(1 + y_M^3\right) m = s, \tag{17}$$

and the decryption function installed into the remote receiver computer is defined by

$$\lambda\,(y, s) = \frac{-y^3}{1 + y^3} + \frac{s}{1 + y^3}\ . \tag{18}$$

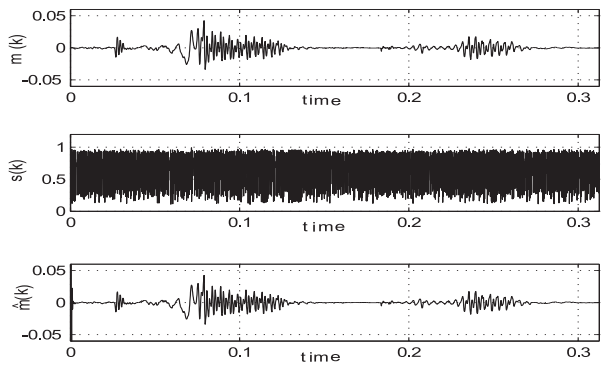

Figure 5.2: Original voice information to be encrypted, m (middle of figure). The transmitted signal with the hidden information. The recovered information $\hat{m}$, at the reciver end (bottom of figure).

5.1 Communicating encrypted audio information signals

Firstly, we use like confidential information $m\,(k)$ a *voice message*, the transmitted signal with the hidden the information is $s\,(k)$, and at the receiver end, the recovered information $\hat{m}\,(k)$ is given by Figure 5.2 shows the encrypted transmission and recovery when the confidential information $m\,(k)$ (top of figure) is a voice signal, in this case the word "*cuatro*" that means *four* in Spanish. The transmitted hyperchaotic signal $s(k)$ (middle of figure), and recovered information signal $\hat{m}$ (bottom of figure). We can see after brief transient time that information is recovered faithfully.

5.2 Communicating encrypted images

Figure 5.3 shows the transmission and recovering of an image message by using hyperchaotic encryption, which is based on output synchronization of Hénon and Rössler maps. The original image to be encrypted and transmitted is shown in Figure 5.3(a). While Figure 5.3(b) shows the transmitted encrypted image to the remote receiver via an insecure channel. Finally, the recovered image at the receiver end is depicted in Figure 5.3(c).

Remark 5.1 In our 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, the hyperchaotic communication scheme with two transmission channels gives faster synchronization and high security, see [35].

6 Conclusions

In this paper, we have presented a scheme to achieve output synchronization of different discrete-time hyperchaotic maps via model-matching approach. This method is inspired from nonlinear control theory. We have showed by computer simulations, that this

(a) (b) (c)

Figure 5.3: (a) Original jpg image information to be send for thransmitter, (b) hyperchaotic encrypted image through insecure channel, and (c) recovered jpg information at the receiver end.

approach is indeed suitable to synchronize hyperchaotic generalized Hénon and Rössler maps, in a master-slave coupled configuration.

We have applied output synchronization in secure communication based on hyperchaos. In particular, we have presented a hyperchaotic communication scheme to transmit encrypted confidential (audio and image) information. As well as, the intrinsic advantages for the encryption presented by the mentioned schemes (σ and λ function for exception/decryption, respectively), we have increased the security by using complex hyperchaotic transmitted signals.

Acknowledgments

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

References

[1] Schneier, B. *Applied cryptography: protocols, algorithms, and source code in C.* Wiley & Sons, Inc., 1996.

[2] Menezes, A.J., van Oorschot, P.C. and Vanstone, S.A. *Handbook of Applied Cryptography.* CRC Press, 1997

[3] Pecora, L.M. and Carroll, T.L.. Synchronization in chaotic systems. *Phys. Rev. Lett.* **64** (1990) 821–824.

[4] Nijmeijer, H. and Mareels, I.M.Y. An observer looks at synchronization. *IEEE. Trans. Circ. Syst. I* **44**(10) (1997) 882–890.

[5] Cruz-Hernández, C. and Nijmeijer, H. Synchronization through filtering. *Int. J. Bifurc. Chaos* **10**(4) (2000) 763–775.

[6] Sira-Ramírez, H. and Cruz-Hernández, C. Synchronization of chaotic systems: A generalized Hamiltonian systems approach. *Int. J. Bifurc. Chaos* **11**(5) (2001) 1381–1395.

[7] López-Mancilla, D. and Cruz-Hernández, C. Output synchronization of chaotic systems: model-matching approach with application to secure communication. *Nonlinear Dyn. Syst. Theory* **5**(2) (2005) 141–156.

[8] López-Mancilla, D. and Cruz-Hernández, C. Output synchronization of chaotic systems under nonvanishing perturbations. *Chaos, Solitons & Fractals* **37**(4) (2008) 1172–1186.

[9] Vincent, U.E. Synchronization of identical and non-identical 4-D chaotic systems using control. *Chaos, Solitons & Fractals* in press, doi: 10.1016/j.chaos.2006.10.005.

[10] Yan J.-J., Yang, Y.-S., Chiang, T.-Y., and Chen, C.-Y. Robust synchronization of unified chaotic via sliding mode control. *Chaos, Solitons & Fractals* **34**(3) (2007) 947–954.

[11] Hyun, C.H., Kim, J.H., Kim, E., Park, M. Adaptive fuzzy observer based synchronization design and secure communications of chaotic systems. *Chaos, Solitons & Fractals* **27**(4) (2006) 930–940.

[12] Cuomo, K.M., Oppenheim, A.V., Strogratz, S.H. Synchronization of Lorenz-based chaotic circuits with applications to communications. *IEEE Trans. Circ. Syst. II* **40**(10) (1993) 626–633.

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

[14] Chen, M., Zhou, D. and Shang, Y. A sliding mode observer based secure communication scheme. *Chaos, Solitons & Fractals* **25**(3) (2005) 573–578.

[15] Posadas-Castillo, C., López-Gutiérrez, R.M., Cruz-Hernández, C. Synchronization of chaotic solid-state Nd:YAG lasers: application to secure communication. *Commun. Nonlinear Sci. Numer. Simul.* **13**(8) (2008) 1655–1667.

[16] Short, K.M.and Parker, A.T. Unmasking a hyperchaotic communication scheme. *Phys. Rev. E* **58**(1) (1998) 1159–1162.

[17] Alvarez, G., Montoya, F., Romera, M. and Pastor, G. Breaking parameter modulated chaotic secure communication system. *Chaos, Solitons & Fractals* **21**(4) (2004) 783–787.

[18] Yang, T., Wu, C.W., Chua, L.O. Cryptography based on chaotic systems. *IEEE. Trans. Circ. Syst. I* **44**(5) (1997) 469–472.

[19] Cruz-Hernández, C., Serrano-Guerrero, H. Cryptosystems based on synchronized Chua's circuits. In: *Proceedings of the 16th IFAC World Congress*. Prague, Czech Republic, 2005.

[20] Grassi, G. Observer-based hyperchaos synchronization in cascaded discrete-time systems. *Chaos, Solitons & Fractals* in press, doi:10.1016/j.chaos.2007.08.060.

[21] Yan, Z. and Yu, P. Hyperchaos synchronization and control on a new hyperchaotic attractor. *Chaos, Solitons & Fractals* **35**(2) (2008) 333–345. -

[22] Cruz-Hernández, C., Posadas C. and Sira-Ramírez, H. Synchronization of two hyperchaotic Chua circuits: A generalized Hamiltonian systems approach. In: *Proceedings of the 15th IFAC World Congress*. Barcelona, Spain, 2002.

[23] Gao, T., Chen, Z., Yuan, Z. and Yu, D. Adaptive synchronization of a new hyperchaotic system with uncertain parameters. *Chaos, Solitons and Fractals* **33**(3) (2007) 922–928.

[24] Yang, Y., Ma, X.K. and Zhang, H. Synchronization and parameter identification of high-dimensional discrete chaotic systems via parametric adaptive control. *Chaos, Solitons & Fractals* **28**(1) (2006) 244–251.

[25] Aguilar-Bustos, A.Y. and Cruz-Hernández, C. Synchronization of discrete-time hyperchaotic systems through extended Kalman filtering. *Nonlinear Dyn. Syst. Theory* **6**(4) (2006) 319–336.

[26] Mensour, B., Longtin, A. Synchronization of delay-differential equations with application to private communication. *Phys. Lett. A* **244**(1) (1998) 59–70.

[27] Tamaševičius, A., Čenys, A., Namajūnas, A. and Mykolaitis, G. Synchronising hyperchaos in infinite-dimensional dynamical systems. *Chaos, Solitons & Fractals* **9**(8) (1998) 1403–1408.

[28] Cruz-Hernández, C. Synchronization of time-delay Chua's oscillator with application to secure communication. *Nonlinear Dyn. Syst. Theory* **4**(1) (2004) 1–13.

[29] Cruz-Hernández C, Romero-Haros N. Communicating via synchronized time-delay Chua's circuits. *Commun Nonlinear Sci. Numer. Simul.* **13**(3) (2008) 645–659.

[30] Cruz-Hernández, C. and Martynyuk, A.A. *Advances in chaotic dynamics with applications.* Series on Stability, Oscillations, and Optimization of Systems, Cambridge Scientific Publishers, London, Vol. 4, 2008 in press.

[31] Monaco, S. and Normand-Cyrot, D. Minimum phase nonlinear discrete-time systems and feedback stabilization. *Proceedings of the 26th Conference on Decision and Control*, Los Angeles, CA, USA, 1987:979-86.

[32] Chen, L.Q. An open plus closed loop control for discrete chaos and hyperchaos. *Phys. Lett. A* **281**(5) (2001) 327–333.

[33] Cruz-Hernández, C., López-Mancilla, D., García, V., Serrano, H. and Núñez R. Experimental realization of binary signal transmission using chaos. *J. Circ. Syst. Comput.* **14**(3) (2005) 453–468.

[34] Itoh, M., Yang, T. and Chua, L.O. Conditions for impulsive synchronization of chaotic and hyperchaotic systems. *Int. J. Bifurc. Chaos* **11**(2) (2001) 551–560.

[35] Zhong-Ping, J.A. A note on chaotic on chaotic secure communication systems. *IEEE. Trans. Circ. Syst. I* **49**(1) (2002) 92–96.

[36] López-Mancilla, D. and Cruz-Hernández, C. A note on chaos-based communication schemes. *Revista Mexicana de Física* **51**(3) (2005) 265–269.

[37] Aguilar-Bustos, A.Y. and Cruz-Hernández, C. Synchronization of discrete-time hyperchaotic systems: an application in communications. *Chaos, Solitons & Fractals* in press, doi: 10.1016/j.chaos.2008.05.012.

[38] Baier, G. and Klein, M. Maximum hyperchaos in generalized Hénon maps. *Phys. Lett. A* **51**(6-7) (1990) 281–284.