Nonlinear Dynamics and Systems Theory, 5(2) (2005) 141–156

Output Synchronization of Chaotic Systems: Model-Matching Approach with Application to Secure Communication

D. López-Mancilla[1] and C. Cruz-Hernández[2]*

[1] *Electronics & Telecomunications Department, Scientific Research and Advanced Studies of Ensenada (CICESE), Km. 107 Carretera Tijuana-Ensenada, 22860 Ensenada, B. C., México*
[2] *Telematics Direction, Scientific Research and Advanced Studies of Ensenada (CICESE), P.O.Box 434944, San Diego, CA 92143-4944, USA*

Received: October 10, 2004; Revised: March 2, 2005

Abstract: In this paper, a method for synchronizing chaotic systems in continuous-time is presented. The approach, which exploits the model-matching problem from nonlinear control theory, is advantageously applied to achieve complete synchronization and output synchronization of identical and nonidentical chaotic systems, respectively. Some potential applications to secure communication for audio and binary information signals are also given.

Keywords: *Chaos synchronization; model-matching problem; encryption; secure communication.*

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

1 Introduction

Undoubtedly, data security has been an issue of increasing importance in communications as the Internet and personal communication systems are being made accessible world-wide. Recently, increasing efforts have been made to use chaotic systems for enhancing some features of communication systems. In particular, chaotic synchronization to design secure communication systems. Chaos and cryptography have some common features, the most prominent being extremely sensitivity to parameter changes. Chaos has already been used to design cryptography systems [9]. One common feature of most existing chaos-based secure communication schemes is that a chaotic signal is used for

*Corresponding author: ccruz@cicese.mx

transmitting the message. More precisely, by a proper modulation of the chaotic transmitter dynamics, the private message is hidden and sent to the chaotic receiver dynamics. At the receiving side, a synchronous chaotic system is built to synchronize with the transmitter to recover the original message. Different approaches for chaos synchronization have been proposed to synchronize identical systems, see e.g., [3 – 5,7,8,11,13,16,17,19,24–26, 30] and references inside. Although synchronization of identical chaotic systems is useful to transmit private information, some researchers have proposed different methods to synchronize nonidentical chaotic systems, which has been suggested to several potential applications. Adaptive control has been used to synchronize nonidentical chaotic systems in [2, 31]. Feedback linearization and adaptive feedback linearization has been proposed in [28]. A method to get an equivalence between two nonidentical chaotic attractors was presented in [12]. Synchronization of nonidentical chaotic systems is useful in many cases of practical interest, and significantly when it occurs in living systems, like synchronization of the activity of groups of neurons located in different brain areas [20, 27] or, in the synchronization between heart and respiratory rates [15] or, the coupling of biological oscillators [29]. However, the synchronization of nonidentical chaotic systems is a much more difficult problem. The aim of this paper is to illustrate an effective method for synchronizing chaotic systems in continuous-time. This objective is achieved by using results from nonlinear control theory; in particular, we use the model-matching problem [6, 10]. This synchronization method presents the following advantages:

- It is systematic.
- It is useful to synchronize identical and nonidentical chaotic systems.
- It uses unidirectional coupling, that let the coupling signal requires less transmission channels, because of the model/master does not need to know any information from the plant/slave.

Moreover, with this methodology chaotic synchronization has applications on transmission of private information schemes. To this purpose, the attention is at first focused on Rössler–Rössler and Lorenz–Rössler synchronization. Finally, we give an application to private/secure communication for transmission and recovering of audio and binary messages (i.e., analog and digital signals) using different chaotic communication schemes.

The paper is organized as follows: Section 2 states the problem formulation. Briefly, the model-matching problem from nonlinear control theory is reviewed in Section 3. In Section 4, we apply this approach to synchronize identical and nonidentical chaotic systems based on Lorenz and Rössler systems. In Section 5, we propose three private/secure communication schemes based on chaotic synchronization for transmission and recovering of audio and binary messages. Finally, Section 6 summarizes the concluding remarks.

2 Problem Statement

Consider a dynamical system described by state equations of the form

$$P\colon \quad \begin{cases} \dfrac{dx}{dt} = f(x) + g(x)u, \\ y = h(x), \end{cases} \tag{1}$$

where the state $x(t) \in R^n$, the input $u(t) \in R$, and the output $y(t) \in R$, being $f(x)$ and $g(x)$ smooth and analytical functions. In addition, consider another nonlinear system described by

$$M\colon \quad \begin{cases} \frac{dx_M}{dt} = f_M(x_M) + g_M(x_M)u_M, \\ y_M = h_M(x_M), \end{cases} \tag{2}$$

where the state $x_M(t) \in R^{n_M}$, the input $u_M(t) \in R$, and the output $y_M(t) \in R$, being $f_M(x_M)$ and $g_M(x_M)$ smooth and analytical functions too. We assume that x° is an equilibrium point of system (1), i.e., $f(x^\circ) = 0$. Similarly, x_M° is an equilibrium point of system (2). Assume that dynamical systems (1) and (2) under certain conditions have *chaotic* behavior. Then, the chaotic system (1) *synchronizes* with the chaotic system (2), if

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

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

Note that, we are only considering *output synchronization problem* between chaotic systems (1) and (2). Moreover, no matter if the chaotic systems (1) and (2) are identical or nonidentical. In the next section, we will describe how to satisfy the output synchronization condition (3) from the perspective of the model-matching problem.

On the other hand, in the context of secure/private communications based on the chaotic synchronization between systems (1) and (2); in the chaotic transmitter system, the private message is hidden/encrypted and sent to the chaotic receiver system via public channel. Finally, the original message is retrieved/decrypted at the receiver end. For this purpose, we will use the chaotic masking and chaotic switching techniques.

3 Model-Matching Problem

Now, consider the dynamical systems (1) and (2) like a *plant* P and *model* M, respectively. We want to design a feedback control law $u(t)$ for the plant P which, irrespectively of the initial states of P and M, makes the output $y(t)$ asymptotically converges to the output $y_M(t)$ produced by M under an arbitrary input $u_M(t)$. This problem is the so-called asymptotic *model-matching problem* from nonlinear control theory. It is also well-known that different approaches to solve the model-matching problem have been proposed in the literature, see e.g. [6, 10]. In this work, we adopt the following solution: the model-matching problem is reduced into a problem of decoupling the output of a suitable auxiliary system from the input $u_M(t)$ to the model M. To this purpose the *auxiliary system* is defined as follows

$$E\colon \quad \begin{cases} \dfrac{dx_E}{dt} = f_E(x_E) + \hat{g}(x_E)u + \hat{g}_M(x_E)u_M, \\ y_E = h_E(x_E), \end{cases} \tag{4}$$

with state $x_E = (x, x_M)^T \in R^{n+n_M}$, inputs $u(t)$ and $u_M(t)$, and

$$f_E(x_E) = \begin{pmatrix} f(x) \\ f_M(x_M) \end{pmatrix}, \qquad \hat{g}(x_E) = \begin{pmatrix} g(x) \\ 0 \end{pmatrix},$$

$$\hat{g}_M(x_E) = \begin{pmatrix} 0 \\ g_M(x_M) \end{pmatrix}, \qquad h_E(x_E) = h(x) - h_M(x_M).$$

That corresponds to a system having as "output" the difference between the output of P and the output of M. We consider $u_M(t)$ as a "disturbance" acting on the auxiliary system (4), and we want to decouple it from the output $y_E(t)$. We are allowed to use disturbance "measurements" because $u_M(t)$ is the input of M, and thus we may use a control law of the form

$$u = \alpha(x_E) + \gamma(x_E)u_M + \beta(x_E)v, \tag{5}$$

with $v(t)$ an additional input signal to obtain asymptotic stability in the closed-loop auxiliary system, which corresponds to the convergence rate of output synchronization.

The control objective of the model-matching problem is contained in the following definition.

Definition 1 (Model-matching problem) Given the plant P and the model M around their respective equilibrium points x° and x_M°, and a point x_E°. The model-matching problem consists in finding a feedback control law $u(t) \in R$ for auxiliary system E equation (4) such that, the output $y_E(t)$ of system E (feedback by $u(t)$ of the form (5)), $y_E(t) \to 0$ as $t \to \infty$.

In the sequel, the model matching problem will be treated in terms of a relative degree associated with the output $y(t)$ of P and the output $y_M(t)$ of M.

Definition 2 (Relative degree [10]) The single-input single-output nonlinear system (1), is said to have *relative degree* r at a point x° if

(1) $L_g L_f^k h(x) = 0$ for all x in a neighborhood of x° and for all $k < r-1$;

(2) $L_g L_f^{r-1} h(x^\circ) \neq 0$.

In Definition 2, $L_f h(x) = \dfrac{\partial h(x)}{\partial x} f(x)$ and $L_g L_f^k h(x) = \dfrac{\partial (L_f^k h(x))}{\partial x} g(x)$. A similar definition can be given for the relative degree of model (2), r_M near x_M°. Suppose that the output $y(t)$ of P and the output $y_M(t)$ of M have a finite relative degree r and r_M, respectively. It is well-known that the model matching problem is locally solvable if, and only if [10],

$$r \leq r_M. \tag{6}$$

Now, we show the auxiliary system E equation (4) feedback by (5) in terms of P and M in a different coordinate frame. In this work, we restrict our results on output synchronization to fully linearizable plants P, i.e., for $r = n$. From definition of relative degrees r and r_M; $h(x), \dots, L_f^{n-1}h(x)$, and $h_M(x_M), \dots, L_{f_M}^{n-1}h_M(x_M)$ are sets of independent functions from P and M, and can be chosen as new coordinates $\xi_i(x) = L_f^{i-1}h(x)$ and $\xi_{Mi}(x_M) = L_{f_M}^{i-1}h_M(x_M)$ with $i = 1, \dots, n$, around x° and x_M°, respectively. Let us now consider the auxiliary system E and the new coordinates [10]

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

where $\zeta(x_E) = (\zeta_1(x_E), \dots, \zeta_n(x_E))^{\mathrm{T}}$, and $\zeta_i(x_E) = L_{f_E}^{i-1}h_E(x_E) = \xi_i(x) - \xi_{Mi}(x_M)$, $i = 1, \dots, n$.

Thus, the closed-loop auxiliary system E, using the following feedback control law

$$u = \frac{1}{L_g L_f^{n-1}h(x)}(v - L_f^n h(x) + L_{f_M}^n h_M(x_M) + L_{g_M} L_{f_M}^{n-1} h_M(x_M) u_M), \tag{7}$$

takes the form

$$\begin{aligned}\frac{d\zeta_i}{dt} &= \zeta_{i+1}, \quad i = 1, \dots , n-1, \\ \frac{d\zeta_n}{dt} &= v = -c_0\,\zeta_1 - \dots - c_{n-1}\,\zeta_n, \\ \frac{dx_M}{dt} &= f_M(x_M) + g_M(x_M)u_M, \\ y_E &= \zeta_1.\end{aligned} \tag{8}$$

From (8) we see that the output $y(t)$ of the closed-loop system P differs from the output $y_M(t)$ of the model M by a signal $y_E(t)$ obeying the linear differential equation

$$y_E^{(n)} + c_{n-1}y_E^{(n-1)} + \ldots + c_1 y_E^{(1)} + c_0 y_E = 0,$$

where $c_0, \dots , c_{n-1}$ are constant real coefficients, thus allowing us to make the output $y(t)$ converges to $y_M(t)$. We can also identify two subsystems in the closed-loop system (8), namely:

1. The subsystem described by

$$\frac{dx_M}{dt} = f_M(x_M) + g_M(x_M)u_M,$$

   which represents the dynamics of M, and
2. The subsystem described by

$$\frac{d\zeta}{dt} = A^*\zeta$$

   with

$$A^* = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -c_0 & -c_1 & -c_2 & \cdots & -c_{n-1} \end{pmatrix},$$

   which represents the dynamics of $y_E(t)$.

The model M is stable by assumption, and if we choose the control law $u(t)$ so that the eigenvalues of matrix A^* have real part negative, then the closed-loop system will be exponentially stable, and the output synchronization condition (3) holds.

Remark 1 Since $y_E(t) = \zeta_1(t) = \xi_1(x) - \xi_{M_1}(x_M) \to 0$ as $t \to \infty$, notice that $\xi(x)$ and $\xi_M(x_M)$ are diffeomorphisms. Then, if P and M are *identical* chaotic systems, $\xi(x) \to \xi_M(x_M)$ and, if the mappings have the same structure and tends to be equals, then the arguments too, i.e., $x(t) \to x_M(t)$. Moreover, from the control law (7) we can see that, $u(t) \to u_M(t)$, with the purpose to decouple the input $u_M(t)$ from the auxiliary system E. Thus, for identical chaotic systems, *complete synchronization* is achieved, i.e., the condition

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

holds. However, for *nonidentical* chaotic systems only *output synchronization* is guaranteed, i.e., the condition (3) holds.

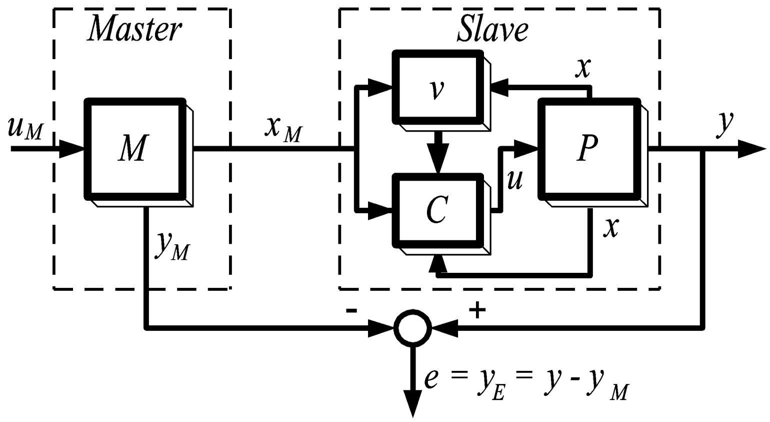

Figure 4.1. Block diagram of chaotic synchronization through model-matching approach.

4 Chaotic Synchronization through Model-Matching Approach

In this section, we use the previous material to show how synchronization of two chaotic systems can be achieved. We consider two cases of study using identical and nonidentical chaotic systems. Figure 4.1 shows the block diagram of chaotic synchronization through model-matching approach. Controller C has like input signals to $x(t)$, $x_M(t)$ and $v(t)$. It has like output signal to $u(t)$ that is the input signal of the plant P. And $e(t) = y_E(t) = y(t) - y_M(t)$ is the *output synchronization error* between the output signals of P and M.

Rössler and Lorenz systems are used to illustrate chaotic synchronization, although the proposed approach can be applied to any chaotic system that holds (6) and for all plant P with a strong relative degree.

4.1 Rössler–Rössler synchronization

Consider the Rössler system given by [21]

$$\begin{aligned}
\frac{dx_1}{dt} &= -(x_2 + x_3), \\
\frac{dx_2}{dt} &= x_1 + \widehat{\alpha} x_2, \\
\frac{dx_3}{dt} &= \widehat{\alpha} + x_3(x_1 - \mu).
\end{aligned} \tag{9}$$

With the parameter values $\widehat{\alpha} = 0.2$ and $\mu = 7$, the Rössler system (9) exhibits chaotic dynamics. We can write it in the form (1) by means of adding a control law $u(t)$ into some equation, we choose rewrite it as follows

$$P\colon \quad \begin{cases} \begin{pmatrix} \dfrac{dx_1}{dt} \\ \dfrac{dx_2}{dt} \\ \dfrac{dx_3}{dt} \end{pmatrix} = \begin{pmatrix} -(x_2 + x_3) \\ x_1 + \widehat{\alpha} x_2 \\ \widehat{\alpha} + x_3(x_1 - \mu) \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} u, \\ y = x_2. \end{cases} \tag{10}$$

The system (10) will be considered *the plant* P. The relative degree of P is $r = 3$. Let us propose a reference model M for P, using another Rössler system writing it in the form (2) and taking the same relative degree $r_M = 3$. Notice that, if both systems have the same relative degree, $r = r_M$, that is, if (6) holds, then, there exists solution to model-matching problem, and so we can achieve synchronization between systems (10) and (11), i.e., the condition (3) is satisfied. So, we have

$$M\colon \quad \begin{cases} \begin{pmatrix} \dfrac{dx_{M_1}}{dt} \\ \dfrac{dx_{M_2}}{dt} \\ \dfrac{dx_{M_3}}{dt} \end{pmatrix} = \begin{pmatrix} -(x_{M_2} + x_{M_3}) \\ x_{M_1} + \widehat{\alpha} x_{M_2} \\ \widehat{\alpha} + x_{M_3}(x_{M_1} - \mu) \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} u_M, \\ y_M = x_{M_2}. \end{cases} \tag{11}$$

We consider the same parameter values in P and M. To solve the model-matching problem, and with this, the original output synchronization problem, we have to take an auxiliary system (4) and thus we reduce the problem described before to disturbance decoupling problem. Then we take $u_M(t)$ like a " disturbance" signal and we seek the control law (7) for system E that is given by

$$\begin{aligned} u = -v &+ (\widehat{\alpha}^2 - 1)(x_1 - x_{M_1}) + \widehat{\alpha}(\widehat{\alpha}^2 - 2)(x_2 - x_{M_2}) + \widehat{\alpha}(x_3 - x_{M_3}) \\ &+ x_3(x_1 - \mu) - x_{M_3}(x_{M_1} - \mu) + u_M. \end{aligned} \tag{12}$$

The auxiliary system (4), after a change of coordinates $\zeta_1 = x_2 - x_{M_2}$, $\zeta_2 = x_1 - x_{M_1} + \widehat{\alpha}(x_2 - x_{M_2})$, and $\zeta_3 = \widehat{\alpha}(x_1 - x_{M_1}) + (\widehat{\alpha}^2 - 1)(x_2 - x_{M_2}) - (x_3 - x_{M_3})$, takes the form (8), with $v = -C\zeta$, or,

$$v = -c_0\,\zeta_1 - c_1\,\zeta_2 - c_2\,\zeta_3.$$

Choosing the poles in -3, we have $C = (27 \quad 27 \quad 9)$. We can consider that the synchronization between both outputs is given too when $u_M(t) = 0$, but in this case we used $u_M(t) = 0.3\,\sin(t)$. And thus we keep the model with chaotic dynamics but in the presence of a disturbance signal. Some numerical simulations were done. The initial conditions $x(0)$ and $x_M(0)$ were $(1, 1, 1)$ and $(2, -2, 2)$, respectively. Figure 4.2 shows the output of the plant, $y(t) = x_2(t)$ following the output of the model $y_M(t) = x_{M_2}(t)$ (top of figure), the error signal $e(t) = y_E(t) = y(t) - y_M(t)$ (middle of figure), and the typical phase plot confirming synchronization between the outputs $y(t)$ and $y_M(t)$ (bottom of figure). The control law $u(t)$ takes action after 20 seconds.

Here, we obtain complete synchronization, i.e., all states of P and M synchronize, because we considered identical chaotic systems.

4.2 Lorenz–Rössler synchronization

Now consider the coupling between two nonidentical chaotic systems as plant and model; for example, a Lorenz system [14] like a model with relative degree $r_M = 3$ (for all x_M

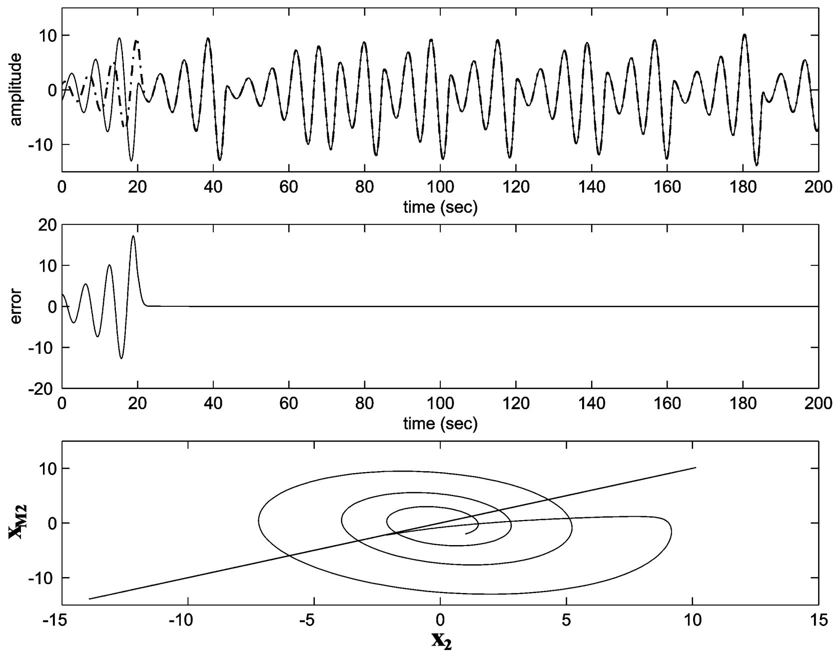

Figure 4.2. Rössler–Rössler synchronization. Solid line $y_M = x_{M_2}$, dashed line $y = x_2$ (top of figure). Error signal $e = y_E = y - y_M$ (middle of figure). Output synchronization between x_{M_2} and x_2 (bottom of figure). Control u takes action when $t = 20$ sec.

such that $x_{M_1} \neq 0$) as follows:

$$M\colon \quad \begin{cases} \begin{pmatrix} \dfrac{dx_{M_1}}{dt} \\ \dfrac{dx_{M_2}}{dt} \\ \dfrac{dx_{M_3}}{dt} \end{pmatrix} = \begin{pmatrix} \sigma(x_{M_2} - x_{M_1}) \\ \hat{r}x_{M_1} - x_{M_2} - x_{M_1}x_{M_3} \\ x_{M_1}x_{M_2} - bx_{M_3} \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} u_M, \\ y_M = x_{M_1}. \end{cases} \tag{13}$$

Let us to consider again the same plant described by equation (10). Thus, the control law $u(t)$ for output synchronization between (10) and (14) is given by

$$\begin{aligned} u = -\{v - [(\widehat{\alpha}^2 - 1)x_1 - \widehat{\alpha}(\widehat{\alpha}^2 - 2)x_2 - -\widehat{\alpha}x_3 - \widehat{\alpha} - x_3(x_1 - \mu)] \\ + \sigma[\sigma(\sigma + \hat{r} - x_{M_3})(x_{M_2} - x_{M_1}) - (\sigma + 1)(\hat{r}x_{M_1} - x_{M_2} - x_{M_1}x_{M_3}) \\ - x_{M_1}(x_{M_1}x_{M_2} - bx_{M_3})] - \sigma x_{M_1}u_M\}. \end{aligned} \tag{14}$$

The results are illustrated by means of some numerical simulations. The initial conditions for plant and model are $x(0) = (3, 1, 1)$ and $x_M(0) = (1, 1.5, 0.1)$, respectively. The parameter values are $\sigma = 10$, $\hat{r} = 28$, $b = 8/3$, $\widehat{\alpha} = 0.2$ and $\mu = 7$.

Figure 4.3 shows how the output of the plant $y(t) = x_2(t)$ follows $y_M(t) = x_{M_1}(t)$ for Lorenz–Rössler output synchronization: a) output of Lorenz/model $y_M(t) = x_{M_1}(t)$,

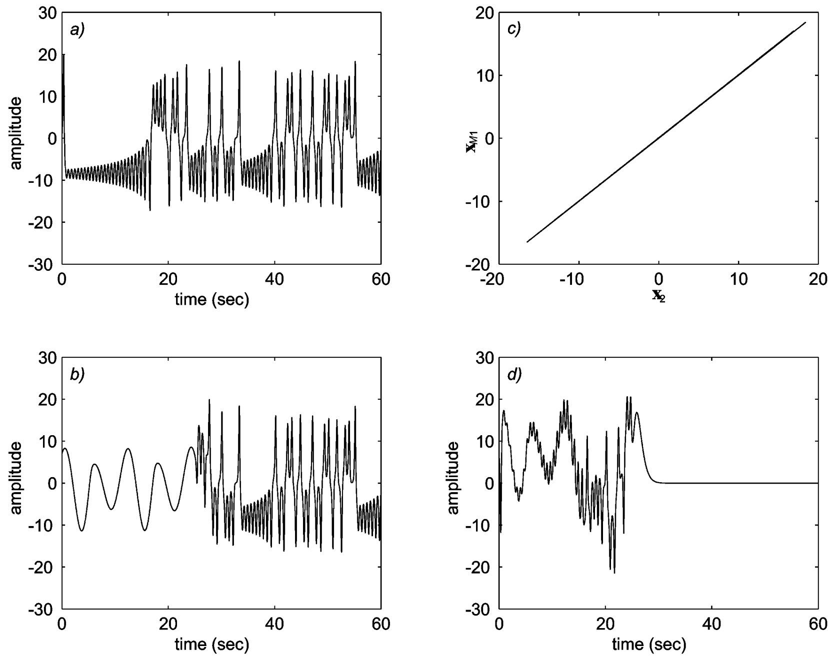

Figure 4.3. Lorenz–Rössler output synchronization: a) $y_M = x_{M_1}$, b) $y = x_2$ following $y_M = x_{M_1}$ after 25 seconds when control law takes action, c) x_2 versus x_{M_1}, and d) error signal $e = y_E = y - y_M$.

b) output of Rössler/plant $y(t) = x_2(t)$ following the output $y_M(t) = x_{M_1}(t)$ of Lorenz/model, c) $x_2(t)$ versus $x_{M_1}(t)$, and d) error signal $e(t) = y_E(t) = y(t) - y_M(t)$.

Remark 2 In this case, unlike the previous one, synchronization between the outputs of both systems was only obtained. No other state of the plant synchronizes with those of the model.

5 Private/Secure Communication Systems

This section does not pretend to propose secure chaos-based communication systems. It tries to illustrate the flexibility of the model-matching approach for chaotic communication. Nevertheless, certain properties of security are found.

5.1 Chaotic communication using two channels

In order to illustrate the proposed approach to transmit private information signals, a chaotic communication scheme using two transmission channels is now designed. It is based on the output synchronization between identical and nonidentical chaotic systems. To this purpose, consider that $u(t)$ equation (5) can be separated in the following form

$$\begin{aligned} u &= \alpha(x, x_M) + \beta(x, x_M)v + \gamma(x, x_M)u_M \\ &= \gamma_2(x)\{[\alpha_1(x_M) + \beta_1(x_M)v_1(x_M) + \gamma_1(x_M)u_M] + [\alpha_2(x) + \beta_2(x)v_2(x)]\} \\ &= \gamma_2(x)[u_1(x_M) + u_2(x)], \end{aligned}$$

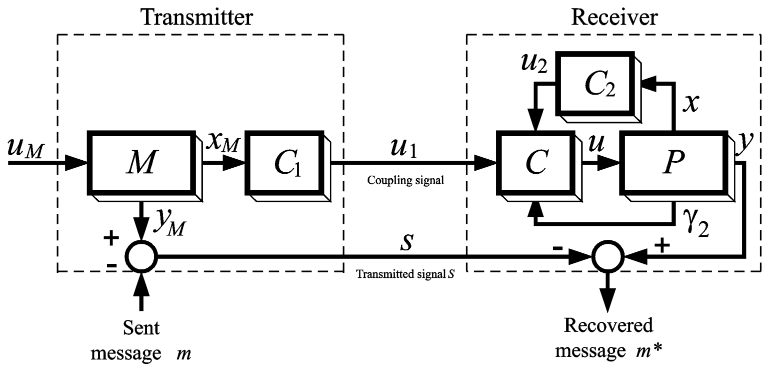

Figure 5.1. Analog communication system using two transmission channels.

with

$$
\begin{aligned}
u_1(x_M) &= v_1(x_M) + L^n_{f_M} h_M(x_M) + L_{g_M} L^{n-1}_{f_M} h_M(x_M) u_M, \\
u_2(x) &= v_2(x) - L^n_f h(x), \\
\gamma_2(x) &= \frac{1}{L_g L_f^{n-1} h(x)}, \\
v_1(x_M) &= c_0 \xi_{M_1}(x_M) + \cdots + c_{n-1} \xi_{Mn}(x_M), \\
v_2(x) &= -c_0 \xi_1(x) - \cdots - c_{n-1} \xi_n(x),
\end{aligned}
$$

like we can see from (7).

This let us to propose the following coupling scheme shown in Figure 5.1, in which $u_1(x_M, u_M)$ is the output from a new control block C_1, $u_2(x)$ is the output of C_2 and $u(x, x_M, u_M)$ or, simply $u(t)$ is the output of controller C. This scheme has two transmission channels, one channel is used to send $u_1(x_M, u_M)$ for output synchronization only, with no connection to the private message. The other channel is used to transmit the hidden message $m(t)$ through $s(t) = y_M(t) - m(t)$. This message is recovered by comparison between the output $y(t)$ and the signal $s(t)$ at the receiver end, i.e., $m^*(t) = y(t) - s(t)$. Some numerical simulations that illustrate the transmission of private message using this scheme were done.

Figure 5.2 shows an audio signal like the private message (top of figure), the transmitted chaotic signal including the hidden message (middle of figure), and the recovered message using Rössler–Rössler output synchronization (bottom of figure). The transmission of the message is through the output of the model $x_{M_2}(t)$.

A remarkable feature is that, in the proposed scheme, the signal that is sent in order to obtain output synchronization is a nonlinear function of the state $x_M(t)$, but is not the own state. So, with this scheme we obtain high privacy because it is possible to hide a message through the coupling signal $u_s(t) = u_1(t) + m(t)$, and with this to increase the security of cryptography, because now $s(t) = y_M(t)$ does not contain any message. So, a third person cannot recover the hidden message with the reported methods in [22, 23]. Figure 5.3 shows a binary signal obtained from a picture like the private message (top of figure), the transmitted chaotic coupling signal including the hidden binary message (middle of figure), and the recovered message at the receiver end (bottom of figure), using Lorenz–Rössler output synchronization.

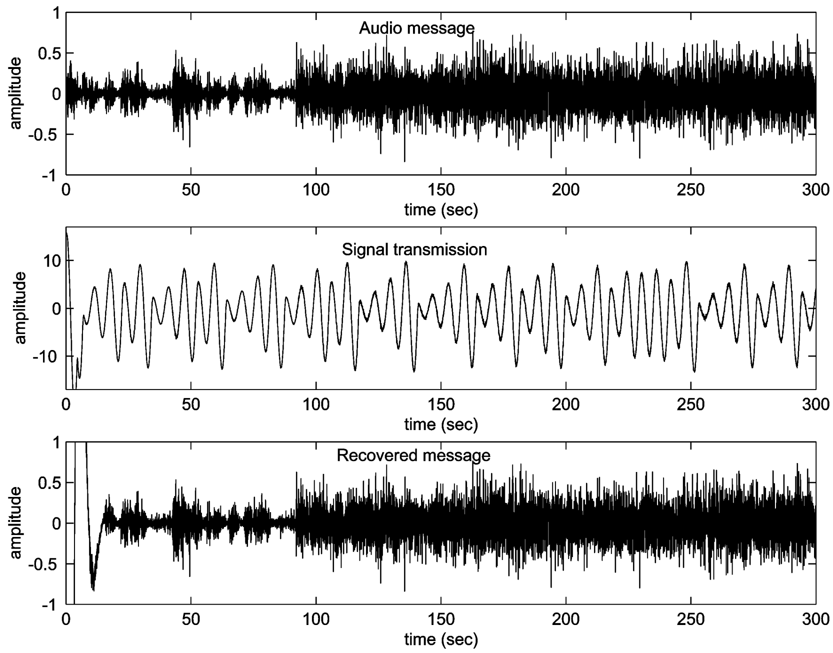

Figure 5.2. Transmission and recovering of an audio message using Rössler–Rössler output synchronization.

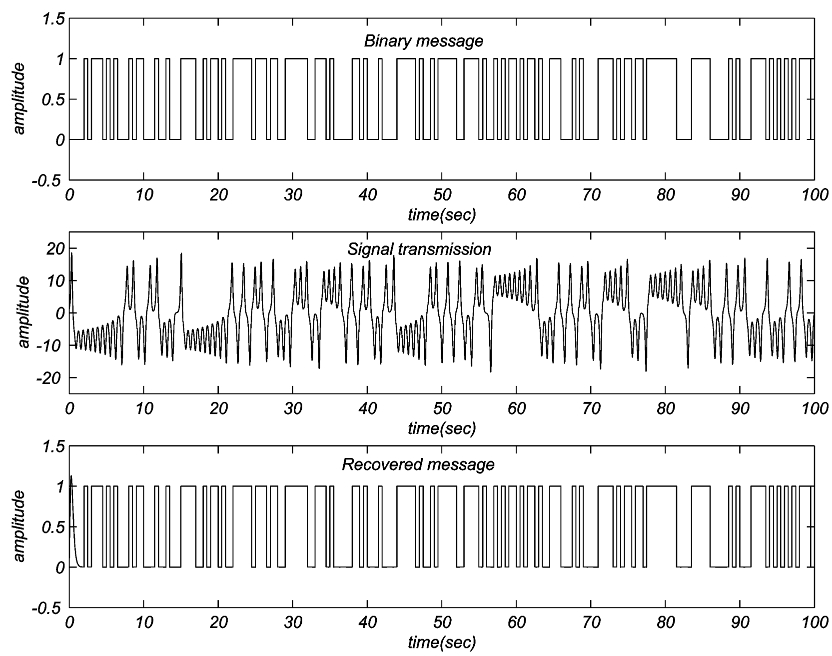

Figure 5.3. Transmission and recovering of a binary message obtained from a digital image using Lorenz–Rössler output synchronization.

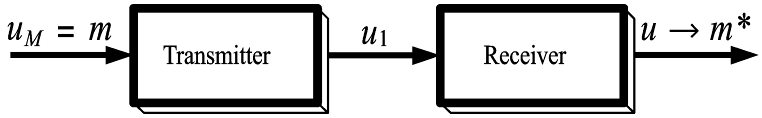

Figure 5.4. Analog communication system using a single transmission channel.

5.2 Chaotic communication using a single channel

Another scheme of transmission that can be used in the case of the synchronization of only identical chaotic systems by model-matching approach is using a single transmission channel to obtain synchronization and to transmit private information signals. This scheme is shown in Figure 5.4. The message $m(t)$ is injected into the transmitter through the input signal $u_M(t)$. The output signal of the transmitter is a nonlinear function $u_1(x_M, u_M)$ whereas it is possible to take like output of receiver to $u(t)$, which, when synchronization is achieved between the outputs of P and M, then $u(t) \to u_M(t) = m(t)$, and thus we obtain the recovered message $m^*(t)$. This scheme is only useful for identical systems because in this case all states of P synchronizes with those of M and $u(t)$ has not to compensate any asynchronous states, so that $u(t) \to u_M(t)$. Figure 5.5 samples numerically the transmission through a single transmission channel using Rössler–Rössler synchronization, in which, control $u(t)$ takes action after 20 seconds and the private message is sent after 40 seconds, when complete synchronization has been achieved.

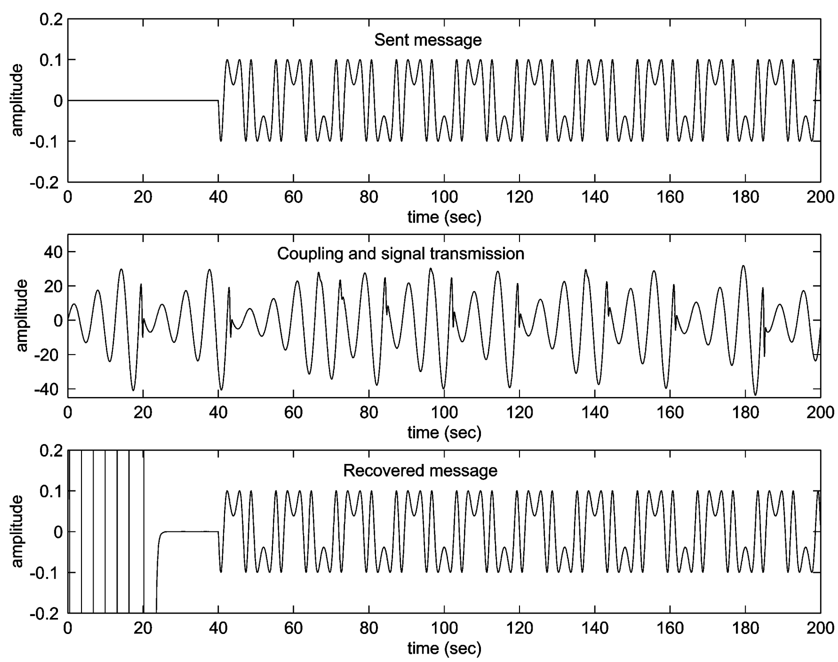

Figure 5.5. Transmission of private information using a single channel.

Since, this scheme does not send any single chaotic signal, but it sends the nonlinear

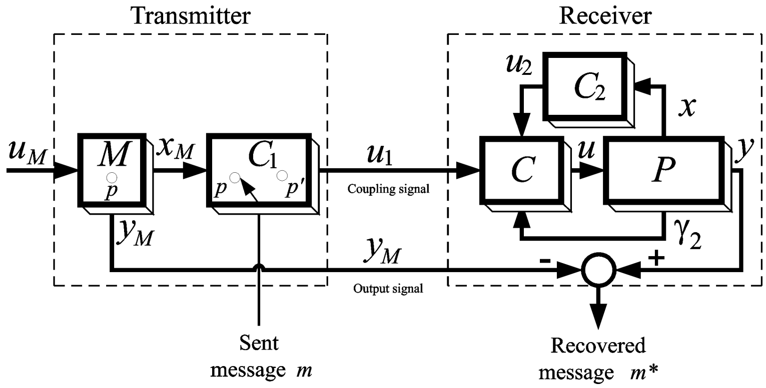

Figure 5.6. Digital communication system of private information by chaotic switching.

function $u_1(t)$, any chaotic attractor can be reconstructed in order to extract the hidden message by means of the reported existing methods in [22, 23].

5.3 Chaotic switching

In the following scheme that is shown in Figure 5.6, we have proposed p like the parameters of P. The same way, p and p' have been proposed like the parameters for controller C_1. During both P and C_1 are on p then there exists synchronization or, at least, output synchronization and during C_1 is on p' there exists an error different from zero. This scheme commonly is known like chaotic switching or chaos shift keying.

Figure 5.7 shows how varying a parameter in the model (transmitter) it is possible to send binary information and to recover it in the plant (receiver) using nonidentical systems: Lorenz–Rössler output synchronization. To make this possible consider that $e_2(t) \to 0$ when $m = 0$ and $e_2(t) \nrightarrow 0$ when $m = 1$, interpreting $e(t) = 0$ like "0" logical and $e(t) \neq 0$ like "1" logical. In this example, the parameter $\hat{r}$ of Lorenz system (13) is switching in C_1 between two values: $p = \hat{r} = 28$ when $m = 0$ and $p' = \hat{r}' = 29$ when $m = 1$ in accordance with $p^* = \hat{r} + m$, with $p^* = (p, p')$. The message is recovered faithfully after a brief iterative signal processing.

Since, this scheme does not switch between two chaotic attractors of identical systems, but it switches a controller parameter, it is a secure cryptography system, where the hidden message through the coupling signal cannot be reconstructed by means of the reported existing methods in literature (see e.g. [18, 23]).

6 Concluding Remarks

In this work we have presented a systematic method to synchronize chaotic systems in continuous-time. In particular, we used the model-matching problem from the nonlinear control theory (see [1] for the discrete-time context). We have obtained *complete synchronization* of Rössler/plant and Rössler/model, and *output synchronization* of Rössler/plant and Lorenz/model. In addition, we have proposed some communication schemes based on complete and output synchronization: using two transmission channels, using a single transmission channel, and using chaotic switching. The advantages over

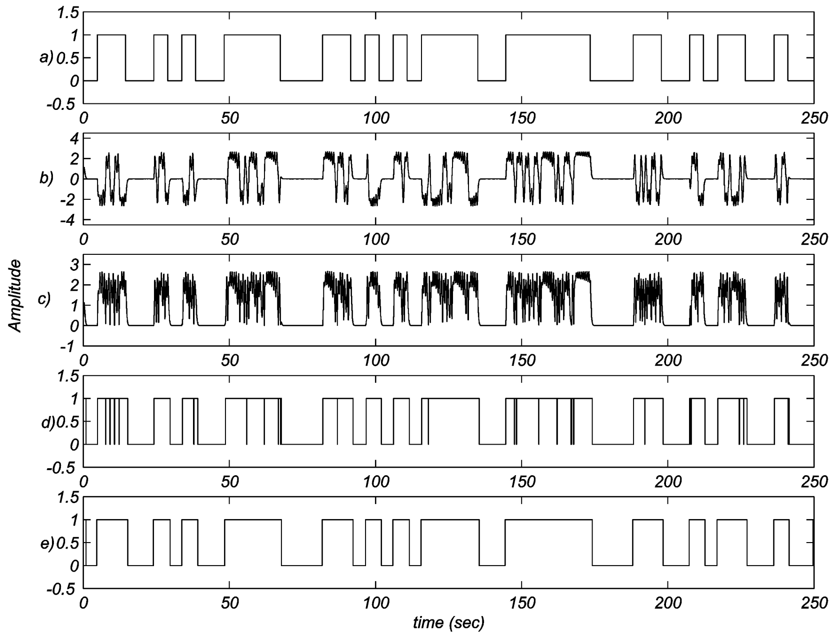

Figure 5.7. Transmission of a binary signal by chaotic switching using Lorenz–Rössler output synchronization: a) original message, b) recovered message at the receiver by output synchronization error detection, c) absolute magnitude of the error signal, d) rounding and iterative signal processing, and e) recovered binary message.

the other cited approaches to synchronize nonidentical chaotic systems are the following: This approach is systematic, it uses unidirectionally coupled systems, gains for controller are small and synchronization is obtained after a short transient behavior. Moreover, this methodology is useful to transmit private information through only one transmission channel (only for identical systems). In addition, this transmission scheme is secure because the coupling signal, including the private message, is a nonlinear function of the state, which is not useful to recover any chaotic attractor and thus it is a difficult if not impossible task that some third person can recover the private message.

Acknowledgment

This work was supported by the CONACYT, México under Research Grant No. 31874-A.

References

[1] Aguilar, A. and Cruz-Hernández, C. Synchronization of two hyperchaotic Rössler systems: Model-matching approach. *WSEAS Trans. on Systems* **1**(2) (2002) 198–203.
[2] Bragard, J., Boccaletti, S. and Arecchi, F.T. Control and synchronization of space extended dynamical systems. *Int. J. Bifurc. Chaos* **11**(11) (2001) 2715–2729.
[3] Chen, G. and Dong, X. *From Chaos To Order*. World Scientific, Singapore, 1998.

[4] Cruz-Hernández, C. and Nijmeijer, H. Synchronization through extended Kalman filtering. In: *New Trends in Nonlinear Observer Design.* (Eds.: H. Nijmeijer and T.I. Fossen). Lecture Notes in Control and Information Science 244; Springer-Verlag, 1999, P.469–490.

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

[6] Di Benedetto, M.D. and Grizzle, J.W. Asymptotic model matching for nonlinear systems. *IEEE Trans. Automatic Control* **39**(8) (1994) 1539–1549.

[7] Feldmann, U., Hasler, M. and Schwarz, W. Communication by chaotic signals: the inverse system approach. *Int. J. Circuits Theory and Appl.* **24** (1996) 551–579.

[8] Fradkov, A.L. and Progromsky, A.Yu. *Introduction to Control of Oscillation and Chaos*. World Scientific Publishing, 1998.

[9] Grassi, G. and Mascolo, S. A system theory approach for designing cryptosystems based on hyperchaos. *IEEE Trans. Circuits Syst. I* **46**(9) (1999) 1135–1138.

[10] Isidori, A. *Nonlinear Control Systems.* Springer, 1995.

[11] Kocarev, L., Halle, K.S., Eckert, K. and Chua L.O. Experimental demonstration of secure communications via chaotic synchronization. *Int. J. Bifurc. Chaos* **2**(3) (1992) 709–713.

[12] Kocarev, L., Shang, A. and Chua, L.O. Transitions in dynamical regimes by driving: a unified method of control and synchronization of chaos. *Int. J. Bifurc. Chaos* **3**(2) (1993) 479–483.

[13] López-Mancilla, D. and Cruz-Hernández, C. An analysis of robustness on the synchronization of chaotic systems under nonvanishing perturbations using sliding modes. *WSEAS Trans. on Math.* **3**(2) (2004) 364–269.

[14] Lorenz, E.N. Deterministic nonperiodic flow. *J. Atmosph. Sci.* **20** (1963) 130–141.

[15] Lotric, M.B. and Stefanovska, A. Synchronization and modulation in the human cardiorespiratory system. *Physica* **A283**(3–4) (2000) 451–461.

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

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

[18] Pérez, G. and Cerdeira, H.A. Extracting messages masked by chaos. *Phys. Rev. Lett.* **74**(11) (1995) 1970–1973.

[19] Pikovsky, A., Rosenblum, M. and Kurths, J. *Synchronization: A Universal Concept in Nonlinear Sciences.* Cambridge University Press, 2001.

[20] Rabinovich, M.I., Varona, P. and Abarbanel, H.D.I. Nonlinear cooperative dynamics of living neurons. *Int. J. Bifurc. Chaos* **10**(5) (2000) 913–933.

[21] Rössler, O.E. An equation for continuous chaos. *Phys. Lett.* **A**57 (1976) 397–398.

[22] Short, K.M. Steps toward unmasking secure communications. *Int. J. Bifurc. Chaos* **4** (1994) 959–977.

[23] Short, K.M. Unmasking a modulated chaotic communications scheme. *Int. J. Bifurc. Chaos* **6**(2) (1996) 367–375.

[24] 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. And in *Procs. of American Control Conference (ACC' 2000)*, Chicago, USA, 2001, P.769–773.

[25] Special Issue on Chaos synchronization and control: Theory and applications. *IEEE Trans. Circuits Syst. I* **44**(10) (1997).

[26] Special Issue on Control and synchronization of chaos. *Int. J. Bifurc. Chaos* **10**(3–4) (2000).

[27] Tass, P., Rosenblum, M.G., Weule, J., Kurths, J., Pikovsky, A., Volkmmann, J., Schnitzler, A. and Freund, H.J. Detection of $n : m$ phase locking from noisy data: Application to magnetoencephalography. *Phys. Rev. Lett.* **81**(15) (1998) 3291–3294.

[28] Wagg, D.J. Partial synchronization of nonidentical chaotic systems via adaptive control, with applications to modeling coupled nonlinear systems. *Int. J. Bifurc. Chaos* **12**(3) (2002) 561–570.

[29] Winfree, A.T. Biological rhythms and the behavior of populations of coupled oscillators. *J. Theor. Biol.* **16** (1967) 15–42.

[30] Wu, C.W. and Chua, L.O. A simple way to synchronize chaotic systems with applications to secure communication systems. *Int. J. Bifurc. Chaos* **3**(6) (1993) 1619–1627.

[31] Wu, C.W., Yang, T. and Chua, L.O. On adaptive synchronization and control of nonlinear dynamical systems. *Int. J. Bifurc. Chaos* **6**(3) (1996) 455–471.

[32] Yang, T. Recovery of digital signals from chaotic switching. *Int. J. Circ. Theory Appl.* [**14**] (1995) 611–615.