SINCRONIZACIÓN DE SISTEMAS CAÓTICOS DIFERENTES CON APLICACIÓN A LA TRANSMISIÓN PRIVADA DE INFORMACIÓN BINARIA*

DIDIER LOPEZ-MANCILLA† y CESAR CRUZ-HERNANDEZ‡
Departamento de Electrónica y Telecomunicaciones,
Centro de Investigación Científica y de Educación Superior de Ensenada (CICESE),
Km. 107 Carretera Tijuana-Ensenada, 22860 Ensenada, Baja California, México.

Resumen: En este artículo se presenta una metodología para sincronizar sistemas caóticos diferentes en tiempo continuo. La técnica explota el problema de acoplamiento a modelos tomado de la teoría del control no lineal, es aplicada a la sincronización de salida de dos sistemas diferentes Lorenz-Rössler. En este análisis, se limitan los resultados a plantas completamente linealizables. Se presenta una aplicación a las comunicaciones privadas para mensajes binarios utilizando conmutación caótica.

Palabras clave: Sincronización de salida, caos, problema de acoplamiento a modelos, comunicaciones privadas.

1 Introducción

Indudablemente, la seguridad en el envío de información ha sido un tema de importancia, que ha ido en aumento en las comunicaciones, pues el Internet y los sistemas de comunicación personales se están haciendo mundialmente accesibles. Recientemente, se han incrementado los esfuerzos en utilizar sistemas caóticos para mejorar algunas características de los sistemas de comunicación. En particular, emplear la sincronía de sistemas caóticos para diseñar sistemas de comunicación donde se transmita de manera segura, cualquier tipo de información privada. El caos ya ha sido utilizado para diseñar sistemas de comunicación en combinación con la criptografía [1]. Una característica común de los esquemas seguros existentes de la comunicación basados en caos, es que una señal caótica puede ser utilizada para transmitir un mensaje. Más precisamente, mediante una modulación apropiada de la dinámica caótica del transmisor, el mensaje privado se oculta y se envía a la dinámica caótica del receptor. En el receptor, un sistema caótico se construye para sincronizar con el transmisor con el fin de desencriptar el mensaje original. Diversas metodologías para la sincronización del caos se han propuesto, considere por ejemplo, [2]-[16] y las referencias contenidas en ellos.

El propósito de este trabajo es ilustrar una metodología para sincronizar las salidas de sistemas caóticos diferentes en tiempo continuo. Este objetivo es logrado usando algunos resultados de la teoría del control no lineal; en particular, se usa la metodología de acoplamiento a modelos [17], [18]. Con fines de ilustración, se enfoca la atención en la sincronización de las salidas de los sistemas Lorenz y Rössler. Finalmente, se propone una aplicación en comunicaciones seguras/privadas para la transmisión y desencriptamiento de mensajes binarios utilizando conmutación caótica.

Este artículo está organizado de la siguiente manera: la Sección 2 establece el planteamiento del problema. El problema de acoplamiento a modelos es presentado brevemente en la Sección 3. En la Sección 4, se aplica esta metodología para sincronizar las salidas de dos sistemas caóti-

*Este trabajo fue financiado por el CONACYT, México bajo el proyecto de investigación No. 31874-A.

†**Correspondencia a:** Didier López-Mancilla, CICESE, Electronics & Telecom. Dept., P.O. Box 434944, San Diego, CA 92143-4944, USA, Phone: +52.646.1750500, Fax: +52.646.1750554, E-mail: dlopez@cicese.mx

‡E-mail: ccruz@cicese.mx

cos diferentes: los sistemas de Lorenz y Rössler. En la Sección 5, se propone un esquema de trasmisión para mensajes privados, basado en la sincronización de sistemas caóticos. Finalmente, en la Sección 6 se presentan algunas conclusiones.

2 Planteamiento del Problema

Considere un sistema no lineal descrito por ecuaciones de la forma

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

donde el estado $x(t) \in \mathbb{R}^n$, la entrada $u(t) \in \mathbb{R}$, y la salida $y(t) \in \mathbb{R}$, siendo $f(x)$ y $g(x)$ funciones suaves y analíticas. Además, considere otro sistema no lineal descrito por

$$M : \begin{cases} \dot{x}_M = f_M(x_M) + g_M(x_M)\,u_M, \\ y_M = h_M(x_M), \end{cases} \tag{2}$$

donde el estado $x_M(t) \in \mathbb{R}^{n_M}$, la entrada $u_M(t) \in \mathbb{R}$, y la salida $y_M(t) \in \mathbb{R}$, siendo también $f_M(x_M)$ y $g_M(x_M)$ funciones suaves y analíticas. Asúmase que x° es un punto de equilibrio de (1), es decir, $f(x^\circ) = 0$. Similarmente, x_M° es un punto de equilibrio de (2). Asúmase que los sistemas (1) y (2), bajo ciertas condiciones, presentan comportamiento caótico. Entonces, decimos que el sistema caótico (1) **sincroniza** con el sistema caótico (2), si

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

sin importar sus condiciones iniciales $x(0)$ y $x_M(0)$, y para adecuadas señales de entrada $u(t)$ y $u_M(t)$.

Note que, solamente estamos considerando el **problema de sincronización de salida** entre los sistemas caóticos (1) y (2). En la siguiente sección describiremos cómo satisfacer la condición (3) desde la pespectiva del problema de acoplamiento a modelos tomado de la teoría del control no lineal.

Como aplicación de la sincronía de los sistemas caóticos (1) y (2), en el contexto de comunicaciones privadas/seguras; en el sistema transmisor, el mensaje privado es encriptado y enviado al receptor utilizando un canal público. Finalmente, el mensaje original es desencriptado en el receptor. Para este propósito, utilizaremos la técnica de conmutación entre atractores caóticos.

3 El Problema de Acoplamiento a Modelos

Ahora, considere el sistema dinámico (1) y (2) como una *planta* P y un *modelo* M, respectivamente. Con la intención de diseñar un control $u(t)$ para la planta P, el cual, independientemente de las condiciones iniciales de los estados de P y M, logre que la salida $y(t)$ converja asintóticamente a la salida $y_M(t)$ producida por M bajo la influencia de una entrada arbitraria $u_M(t)$. Este problema es conocido en la literatura como *el problema de acoplamiento a modelos* de la teoría del control no lineal [17], [18]. Este problema se resolverá reduciéndolo al problema de desacoplar la salida de un adecuado sistema auxiliar, de la entrada $u_M(t)$ del modelo. Para este propósito el *sistema auxiliar* es definido como

$$E : \begin{cases} \dot{x}_E = f_E(x_E) + \hat{g}(x_E)\,u + \hat{g}_M(x_E)\,u_M, \\ y_E = h_E(x_E), \end{cases} \tag{4}$$

con estado $x_E = (x, x_M)^T \in \mathbb{R}^{n+n_M}$, entradas $u(t)$ y $u_M(t)$, y

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

Esto corresponde a un sistema teniendo como "salida", a la diferencia entre las salidas de P y M. Se considera a $u_M(t)$ como una "perturbación" actuando sobre el sistema auxiliar (4) y se desea desacoplarla de la salida $y_E(t)$. Es perfectamente válido que se usen "mediciones" de la perturbación porque $u_M(t)$ es una entrada conocida de M y así, se puede proponer un control en la forma

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

con $v(t)$ como una señal de entrada adicional con la finalidad de obtener estabilidad en el sistema auxiliar, lo que corresponde a la razón de convergencia para la sincronización.

El objetivo del problema de acoplamiento a modelos está contenido en la siguiente definición.

Definición 1 (Problema de acoplamiento a modelos): *Dados la planta P y el modelo M al rededor de sus respectivos puntos de equilibrio x° y x_M° y un punto x_E°, el problema de acoplamiento a modelos consiste en encontrar $u(t) \in \mathbb{R}$ para E tal que, la salida del sistema auxiliar E retroalimentado por $u(t)$ en la forma (5), $y_E(t) \to 0$ a medida que $t \to \infty$.*

En adelante el problema de acoplamiento a modelos, será tratado en términos de un grado relativo asociado con las salidas $y(t)$ y $y_M(t)$.

Definición 2 (Grado relativo [17]): *El sistema no lineal de una-entrada y una-salida (1), tiene* **grado relativo** *r en un punto x° si*

1. $L_g L_f^k h(x) = 0$

   para toda x en una vecindad de x° y $k < r-1$.

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

Definición similar se puede dar para el grado relativo del modelo (2), r_M en una vecindad de x_M°. Suponga que la salida $y(t)$ de P y la salida $y_M(t)$ de M tienen grado relativo finito r y r_M, respectivamente. Es bien sabido que el problema de acoplamiento a modelos tiene solución local si, y sólo si [17],

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

Ahora, se mostrará una representación del sistema auxiliar E Ec. (4) retroalimentado por (5) en términos de la planta P y el modelo M en un marco de coordenadas diferente. Supóngase que la planta P es completamente linealizable, i.e., $r = n$. De la definición de r; $h(x), \ldots, L_f^{n-1} h(x)$, es un conjunto de funciones independientes de P, y pueden ser elegidas como nuevas coordenadas $\xi_i(x) = L_f^{i-1} h(x)$ y $\xi_{Mi}(x_M) = L_{f_M}^{i-1} h_M(x_M)$ en forma similar para el sistema M, con $i = 1, \ldots, n$, alrededor de x° y x_M°, respectivamente. Permítase considerar el sistema auxiliar E y las nuevas coordenadas [17]:

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

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

Así, el sistema auxiliar en lazo cerrado, usando la ley de control

$$\begin{aligned} u &= \frac{1}{L_g L_f^{n-1} h(x)} \left(v - L_f^n h(x) + L_{f_M}^n h_M(x_M) \right. \\ &\quad \left. + L_{g_M} L_{f_M}^{n-1} h_M(x_M) u_M \right), \end{aligned} \tag{7}$$

toma la forma

$$\begin{aligned} \dot{\zeta}_i &= \zeta_{i+1}, \quad i = 1, \ldots, n-1, \\ \dot{\zeta}_n &= v = -c_0 \zeta_1 - \ldots - c_{n-1} \zeta_n, \\ \dot{x}_M &= f_M(x_M) + g_M(x_M) u_M, \\ y_E &= \zeta_1. \end{aligned} \tag{8}$$

De (8) se observa que la salida $y(t)$ de la planta P en lazo cerrado, difiere de la salida $y_M(t)$ del modelo M por una señal $y_E(t)$, que obedece a la ecuación diferencial lineal

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

donde $c_0, \ldots, c_{n-1}$ son coeficientes reales constantes, permitiendo así que la salida $y(t)$ converja a $y_M(t)$. Se puede también identificar dos subsistemas en el sistema en lazo cerrado (8), que son:

1. El subsistema descrito por

   $$\dot{x}_M = f_M(x_M) + g_M(x_M) u_M,$$

   el cual representa las dinámicas de M, y

2. El subsistema descrito por

   $$\dot{\zeta} = A^* \zeta$$

   con

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

   el cual representa la dinámica de $y_E(t)$. El modelo M es estable por suposición y si se elige una ley de control $u(t)$ tal que los valores propios de A^* tengan parte real negativa, entonces el sistema en lazo cerrado será exponencialmente estable y la condición de sincronización de salida (3) se cumple.

4 Sincronización de Sistemas Caóticos por Acoplamiento a Modelos

Se emplea el resultado previo, para ilustrar cómo se puede lograr la sincronización de las salidas entre dos sistemas caóticos diferentes.

4.1 Sincronización de Lorenz y Rössler

Considere el acoplamiento entre dos sistemas caóticos diferentes, como planta y modelo; por ejemplo, un sistema de Rössler [19] para la planta P en la forma (1) con grado relativo $r = 3$:

$$P: \begin{cases} \begin{pmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{pmatrix} = \begin{pmatrix} -(x_2 + x_3) \\ x_1 - \widehat{\alpha} x_2 \\ \widehat{\alpha} + x_3 (x_1 - \mu) \end{pmatrix} \\ \qquad\qquad + \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} u \\ y = x_2. \end{cases} \tag{9}$$

Permítase proponer un modelo de referencia M para P, usando un sistema de Lorenz [20], reescribiéndolo en la forma (2) y proponiendo una salida $y_M(t)$ y ubicando un control $u_M(t)$ de tal forma que tenga el mismo grado relativo $r_M = 3$ (para toda x_M tal que $x_{M1} \neq 0$). Note que, si P y M tienen el mismo grado relativo, $r = r_M$, es decir, si (6) se cumple, entonces existe solución al problema de acoplamiento a modelos y así se puede lograr sincronización de salida entre (9) y (10), i.e. la condición (3) se satisface. De este modo, se tiene

$$M: \begin{cases} \begin{pmatrix} \dot{x}_{M1} \\ \dot{x}_{M2} \\ \dot{x}_{M3} \end{pmatrix} = \begin{pmatrix} \sigma (x_{M2} - x_{M1}) \\ \hat{r} x_{M1} - x_{M2} - x_{M1} x_{M3} \\ x_{M1} x_{M2} - b x_{M3} \end{pmatrix} \\ \qquad\qquad + \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} u_M, \\ y_M = x_{M1}. \end{cases} \tag{10}$$

Se logra sincronización de salida entre (9) y (10) mediante la ley de control

$$\begin{aligned} u = -\{ & v - [\widehat{\alpha} \dot{x}_1 + (\widehat{\alpha}^2 - 1) \dot{x}_2 - \widehat{\alpha} \\ & - x_3 (x_1 - \mu)] + \sigma [(\sigma + \hat{r} - x_{M3}) \dot{x}_{M1} \\ & - (\sigma + 1) \dot{x}_{M2} - x_{M1} \dot{x}_{M3}] \}. \end{aligned} \tag{11}$$

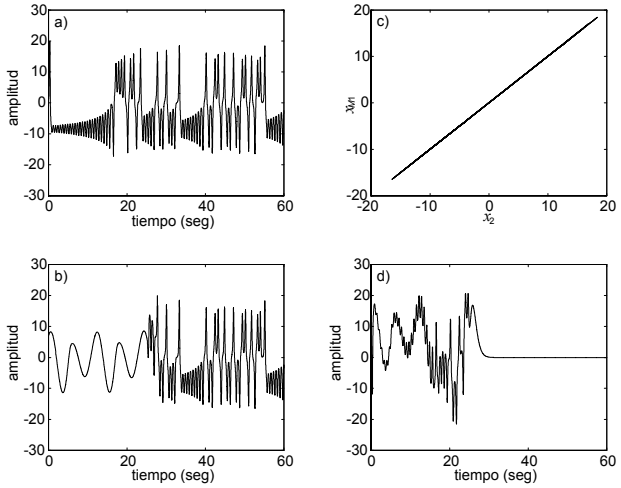

Figura 1: Sincronización de Lorenz y Rössler. a) $y_M = x_{M1}$. b) $y = x_2$. c) Sincronía entre x_{M1} y x_2. d) Error de salida e. El control u entra en acción después de 25 segundos.

Las condiciones iniciales para P y M son $x(0) = (3, 1, 1)$ y $x_M(0) = (1, 1.5, 0.1)$, respectivamente. Los valores de los parámetros son $\sigma = 10$, $\hat{r} = 28$, $b = 8/3$, $\widehat{\alpha} = 0.2$ y $\mu = 7$. Es bien sabido que con estos valores, ambos sistemas exhiben dinámica caótica. La Fig. 1 muestra: a) la salida de M: $y_M(t) = x_{M1}(t)$, b) la salida de P: $y(t) = x_2(t)$, c) la sincronización entre los estados $x_2(t)$ y $x_{M1}(t)$ de los sistemas Rössler y Lorenz para $t > 30$ segundos y, d) la señal de error $e(t) = y_E(t) = x_2(t) - x_{M1}(t)$. El control $u(t)$ entra en acción intencionalemente después de 25 segundos con el fin de hacer más ilustrativas las dinámicas individuales y su comportamiento después del acoplamiento.

Observación 1 *Sólo se logra sincronización entre las salidas de P y M. Ninguno de los otros estados de P sincroniza con los de M.*

Observación 2 *Note que, si se elige adecuadamente $v(t)$ en (5), se puede obtener un breve período transitorio en la sincronización. Esta es una característica apreciable para el diseño de esquemas de comunicación segura/privada basadas en sincronización de caos, ya que es posible evitar con esto, que parte del mensaje privado se pierda durante el comportamiento transitorio.*

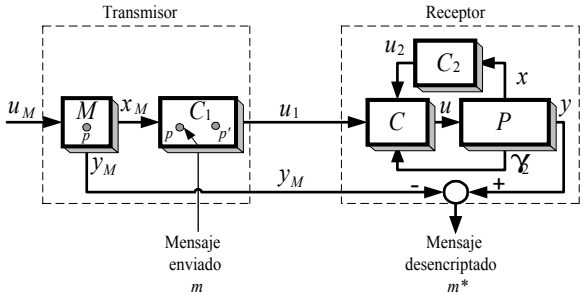

Figura 2: Esquema de transmisión usando conmutación caótica.

5 Comunicación Privada por Conmutación caótica

Para ilustrar la metodología propuesta, se ha diseñado un sistema de comunicación usando dos canales de transmisión. Este está basado en la sincronización de salida entre los sistemas de Lorenz y Rössler. Para este propósito, considere que $u(t)$ Ec. (5) puede ser separado en la siguiente forma

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

Con este esquema se obtiene sincronización de salida y alta privacidad: un canal se usa para enviar $u_1(x_M)$ con el único propósito de lograr sincronización. El otro canal se usa para comparar las salidas $y(t)$ y $y_M(t)$, con el fin de recuperar el mensaje enviado. En este esquema, que se muestra en la Fig. 2, se ha propuesto p como los parámetros de P. De la misma manera, p y p' se han propuesto como los parámetros usados en el controlador C_1. Mientras P y C_1 operen con p existirá sincronización de salida y cuando C_1 opere con p' existirá un error diferente de cero. Este esquema es diseñado para la transmisión de información de manera binaria privada.

La Fig. 3 muestra cómo variando un parámetro en el transmisor es posible enviar información binaria y recobrarla en el receptor usando *sistemas caóticos diferentes* mediante la sincronización de salida de Lorenz y Rössler. Para que esto sea posible considere que $e_2(t) \to 0$ cuando $m = 0$ y

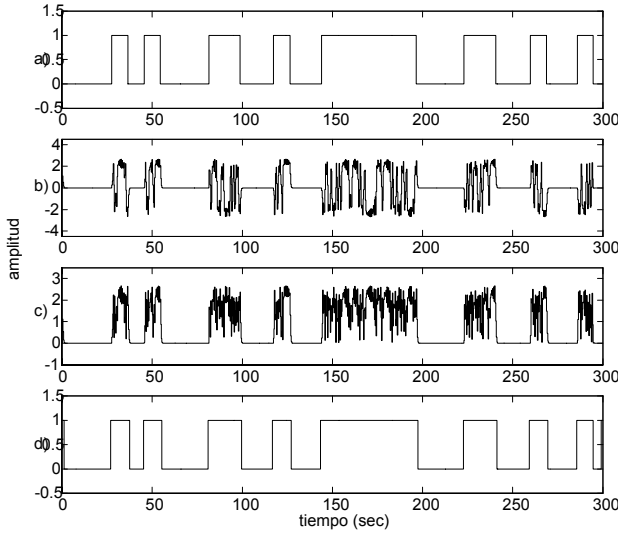

Figura 3: Transmisión y recobrado de un mensaje binario: a) mensaje binario enviado, b) señal recuperada en el receptor, c) proceso iterativo de la señal y, d) mensaje recuperado.

$e_2(t) \nrightarrow 0$ cuando $m = 1$, interpretando $e(t) = 0$ como un "0" y $e(t) \neq 0$ como un "1". En este ejemplo, el parámetro $\hat{r}$ del sistema de Lorenz (10) está conmutando en C_1 entre dos valores: $p = \hat{r} = 28$ cuando $m = 0$ y $p' = \hat{r}' = 29$ cuando $m = 1$ en acuerdo con $p^* = \hat{r} + m$, donde $p^* = (p, p')$. El mensaje es fielmente recuperado después de un breve y adecuado proceso iterativo de la señal del error.

6 Conclusiones

En este trabajo se ha presentado una metodología para sincronizar sistemas caóticos diferentes en tiempo continuo. En particular, se ha usado el problema de acoplamiento a modelos tomada de la teoría del control no lineal (ver [15] en el contexto de tiempo discreto). Se ha ilustrado la sincronización de salida de Rössler (planta) y Lorenz (modelo). Además, se ha propuesto un esquema de comunicación usando dos canales de transmisión para información binaria.

En trabajo futuro se considerará el caso de perturbaciones paramétricas y externas para esta metodología, tomando en cuenta cómo afectan a la sincronización y, por consecuencia, cómo afectan estas perturbaciones a la transmisión de mensajes privados.

Referencias

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

[2] L.M. Pecora y T.L. Carroll. "Synchronization in chaotic systems," *Phys. Rev. Lett.* **64**, 1990, 821-824.

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

[4] U. Feldmann, M. Hasler y W. Schwarz, "Communication by chaotic signals: the inverse system approach," *Int. J. Circuits Theory and Applications*, **24**, 1996, 551-579.

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

[6] Número especial en "Chaos synchronization and control: Theory and applications," *IEEE Trans. Circuits Syst. I*, **44**(10), 1997.

[7] Número especial en "Control and synchronization of chaos," *Int. J. Bifurc. Chaos*, **10**(3-4), 2000.

[8] H. Nijmeijer y I.M.Y. Mareels, "An observer looks at synchronization," *IEEE Trans. Circuits Syst. I* **44**(10), 1997, 882-890.

[9] G. Chen y X. Dong, *From Chaos To Order*, World Scientific, Singapore. 1998.

[10] C. Cruz y H. Nijmeijer, "Synchronization through extended Kalman filtering," *New Trends in Nonlinear Observer Design,* eds. H. Nijmeijer and T. I. Fossen, Lecture Notes in Control and Information Science 244, Springer-Verlag, 1999, 469-490.

[11] C. Cruz y H. Nijmeijer, "Synchronization through filtering," *Int. J. Bifurc. Chaos,* **10**(4), 2000, 763-775.

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

[13] H. Sira-Ramírez y C. Cruz, "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, 769-773.

[14] A.L. Fradkov y A.Yu. Progromsky, *Introduction to control of oscillation and chaos*, World Scientific Publishing, 1998.

[15] A. Aguilar y C. Cruz, "Synchronization of two hyperchaotic Rössler systems: Model-matching approach," *WSEAS Transactions on Systems* **1**(2), 2002, 198-203.

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

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

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

[19] O.E. Rössler, "An equation for continuous chaos," *Phys. Lett.* **A**57, 1976, 397.

[20] E.N. Lorenz, "Deterministic nonperiodic flow," *J. Atmosph. Sci.* **20,** 1963, 130-141.