

**CENTRO DE INVESTIGACIÓN CIENTÍFICA Y DE EDUCACIÓN SUPERIOR
DE ENSENADA**



**PROGRAMA DE POSGRADO EN CIENCIAS
EN ELECTRÓNICA Y TELECOMUNICACIONES**

SINCRONIZACIÓN DE OSCILADORES CAÓTICOS DISCRETOS

TESIS

que para cubrir parcialmente los requisitos necesarios para obtener el grado de
DOCTOR EN CIENCIAS

Presenta:

ANA YAVENI AGUILAR BUSTOS

Ensenada, Baja California, México, Septiembre del 2005.

RESUMEN de la tesis de **Ana Yaveni Aguilar Bustos**, presentada como requisito parcial para la obtención del grado de DOCTOR EN CIENCIAS en ELECTRONICA Y TELECOMUNICACIONES. Ensenada, Baja California. Septiembre de 2005.

SINCRONIZACIÓN DE OSCILADORES CAÓTICOS DISCRETOS

Resumen aprobado por:

Dr. César Cruz Hernández
Director de Tesis

El presente trabajo doctoral versa sobre sincronía de sistemas caóticos en tiempo discreto. El interés en el caso discreto radica en las facilidades de implementación que este tipo de sistemas ofrece. Para la sincronía de estos osciladores, se considera un escenario de acoplamiento unidireccional (maestro y esclavo) y se recurre a técnicas conocidas en teoría de control no lineal, como *acoplamiento a modelos* que garantiza sincronía de salida para maestro y esclavo no idénticos y, sincronía completa cuando maestro y esclavo son idénticos. Para el caso de ruido presente en las dinámicas y en la señal de acoplamiento entre los osciladores, se propone como esclavo a un *filtro extendido de Kalman* lográndose sincronía aproximada. Las metodologías propuestas se aplican exitosamente en la sincronización de sistemas hipercaóticos discretos. Se presenta el empleo de sincronización de tales dinámicas a la transmisión de información encriptada en hipercaos.

Palabras Clave: Sincronización de caos, sistemas discretos, acoplamiento a modelos, filtro extendido de Kalman, comunicaciones privadas/seguras, control.

ABSTRACT of the thesis by **Ana Yaveni Aguilar Bustos** as a partial requeriment to obtain the **DOCTOR OF SCIENCE** degree in **ELECTRONICS AND TELECOMUNICATIONS**. Ensenada, Baja California. September 2005.

SYNCHRONIZATION OF DISCRETE-TIME CHAOTIC OSCILLATORS

This theses deals about synchronization of discrete-time chaotic systems. The use of discrete-time systems is important due the implementation facilities that this kind of systems offers. To achieve the synchronization are used two known control tools like model matching approach with the advantage that gives the synchrony in a systematical way; and for a noisy scheme in the dynamic and in the coupling signal is used an extended Kalman filter giving conditions for the approximate synchronization. The two methodologies presented are applied in the synchronization of discrete-time hyperchaotic systems in order to contribute to the increase of the confiability in communications. Shown numeric simulations using the two methodologies. An application to secure/private communication of confidential information is also given using the model matching approach with three different schemes.

Keywords: Synchronization; discrete-time systems; hyperchaos; secure/private communication.

Agradecimientos

*Al Dr. Cesar Cruz Hernández por la atinada dirección de este trabajo de tesis, por su confianza, enseñanzas, dedicación y sobre todo por saberme guiar en el difícil camino de la investigación científica.
Gracias infinitas!*

A los doctores Rafael Kelly, Yuri Orlov y Hebbert Sira-Ramírez por sus atinados comentarios y su apoyo durante todo este tiempo.

El mas profundo agradecimiento al Instituto Tecnológico de Ensenada por todas las facilidades prestadas para la buena conclusión de este trabajo de tesis. En particular a toda la academia de Ingeniería Electrónica, al Ing. Cervantes y al M.S. Domingo Trujillo.

A Ricardo Núñez

A mi madre y a mi suegra por su valiosa ayuda.

Al CICESE.

Al Consejo Nacional de Ciencia y Tecnología.

A Dirección General de Institutos Tecnológicos.

Dedicatoria

A mis padres por confiar siempre en mí y por estar siempre a cualquier hora, en cualquier lugar junto a mí apoyándome incondicionalmente. Mil gracias, los quiero!

A mis hermanos Gilberto y Luis Tupak.

A mi esposo Eusebio por su espera, comprensión y amor.

A mi razón de vida: Yutsil y Ehinea.

Contenido

	Página
I Introducción	1
I.1 Motivación	7
I.2 Planteamiento del problema	12
I.3 Objetivos	15
I.4 Organización del manuscrito	16
II Preliminares	18
II.1 Mapas	18
II.2 Caos	20
II.3 Exponentes de Lyapunov	23
II.4 Hipercaos	26
II.5 Sincronía	27
II.5.1 Escenarios de acoplamiento	27
II.5.2 Sincronización completa	29
II.5.3 Sincronización aproximada	29
II.5.4 Sincronización parcial	31
II.5.5 Sincronización y control de caos	32
III Sincronización de Sistemas Hipercaóticos Utilizando Filtro Extendido de Kalman	34
III.1 Filtro de Kalman	35
III.1.1 Filtro Extendido de Kalman	38
III.2 Sincronización de sistemas hipercaóticos discretos	39

Contenido (Continuación)	Página
III.2.1 Convergencia del error de estimación (sincronización)	43
III.3 Ejemplos	56
III.3.1 Ejemplo 1. Sistema caótico de segundo orden.	56
III.3.2 Ejemplo 2: Sincronización del sistema discreto hipercaótico de Rössler	62
III.4 Resumen	66
IV Sincronización de Sistemas Hipercaóticos por Acoplamiento a Mode- los	68
IV.1 Descripción del problema de estudio	69
IV.2 Problema de acoplamiento a modelos	71
IV.2.1 Acoplamiento asintótico a modelos	72
IV.2.2 Metodología de solución al PDAAMN	73
IV.3 Sincronización de sistemas hipercaóticos mediante acoplamiento a modelos	81
IV.4 Ejemplos	84
IV.5 Sincronización de sistemas no idénticos	97
IV.6 Caso perturbado	101
IV.6.1 Variaciones paramétricas	101
IV.7 Resumen	105
V Aplicación a Comunicaciones Privadas	107
V.1 Comunicación por conmutación entre dos atractores caóticos	108
V.1.1 Caso particular	112
V.2 Encriptamiento aditivo	117
V.3 Encriptamiento por Modulación	120
V.4 Resumen	123
VI Conclusiones generales	125
VI.1 Problemas abiertos	127
Literatura Citada	128
Apéndice A	133

Lista de Figuras

Figura		Página
1	Estados $x_1(t)$, $x_2(t)$ y plano x_1 vs x_2 del circuito de Chua. (a) Comportamiento periódico, (b) Comportamiento caótico.	4
2	Osciladores sin acoplamiento (figura superior) y acoplados mediante la señal $\varphi(x_M)$ (figura inferior).	13
3	Espectro de frecuencias típico de una señal caótica.	21
4	Divergencia de las trayectorias en un sistema caótico comenzando bajo condiciones iniciales muy cercanas.	22
5	Evolución en el tiempo de uno de los estados del circuito caótico de Chua inicializado bajo condiciones muy semejantes.	23
6	Atractor del circuito caótico de Chua (tiempo continuo).	24
7	Atractor del mapa caótico de Hénon (tiempo discreto).	24
8	Atractor del circuito hipercaótico de Chua.	26
9	Escenarios de acoplamiento: (a) Configuración unidireccional (Maestro y Esclavo), (b) Configuración bidireccional (mutuo).	28
10	Plano x_1 vs \hat{x}_1 : (a) Osciladores no sincronizados, (b) Osciladores sincronizados.	30
11	Diagrama de bloques que muestra el sistema a estimar, la salida medida y el filtro de Kalman discreto.	38
12	Atractor caótico del sistema (35).	57
13	Evolución temporal de los errores de sincronía $e_1(k)$ y $e_2(k)$, $\tau = 0$ para $\rho = 0.06$	59
14	Evolución temporal de los errores de sincronía $e_1(k)$ y $e_2(k)$, $\tau = 7$ para $\rho = 0.06$	59
15	Estados $x_1(k)$, $x_2(k)$ y $x_3(k)$ del sistema hipercaótico de Rössler. . . .	63

Lista de Figuras (Continuación)

Figura	Página
16 Atractores del sistema discreto hipercaótico de Rössler.	64
17 Evolución temporal de los errores en la estimación de los estados del sistema de Rössler.	65
18 Esquema de sincronización empleando acoplamiento a modelos.	83
19 Evoluciones en el tiempo de los estados hipercaóticos del sistema (57).	85
20 Atractor hipercaótico desplegado por el sistema (57).	85
21 Acoplamiento entre $x_{M1}(k)$ (línea continua) y $x_1(k)$ (línea segmentada) y acoplamiento (sincronía) entre la salida del modelo $y_M(k) = x_{M2}(k)$ (línea continua) y la salida de la planta $y(k) = x_2(k)$ (línea segmentada) cuando la ley de control actúa en el tiempo $k = 20$	89
22 Control $u(k)$ actuando en $k = 20$. Señal acoplante $\phi_M(x_M(k), u_M(k))$ enviada por el modelo M (maestro) hacia la planta P (esclavo) para lograr sincronía.	89
23 Evolución temporal de los errores de sincronía: $e_i(k) = x_i(k) - x_{Mi}(k)$, $i = 1, 2$	90
24 Evoluciones en el tiempo de los estados hipercaóticos del sistema (63) cuando $x(0) = (0.1, 0.2, -0.1)$	91
25 Atractores del sistema hipercaótico (63), x_1 vs x_2 , x_1 vs x_3 y x_2 vs x_3	91
26 Sincronía (acoplamiento) entre $y(k) = x_2(k)$ (línea punteada) e $y_M(k) = x_{M2}(k)$ (línea continua) y error de sincronía $e_2(k) = x_2(k) - x_{M2}(k)$	96
27 Evolución temporal de los errores de sincronía restantes $e_1(k) = x_1(k) - x_{M1}(k)$ y $e_3(k) = x_3(k) - x_{M3}(k)$	96
28 Sincronía (acoplamiento) entre $y(k) = x_2(k)$ e $y_M(k) = x_{M2}(k)$ y la evolución temporal del error de sincronía $e_2(k) = x_2(k) - x_{M2}(k)$ cuando $\alpha_i = 0.75$	97
29 Sincronía (acoplamiento) entre $y(k) = x_2(k)$ (línea punteada) e $y_M(k) = x_{M2}(k)$ (línea continua) y error de sincronía $e_2(k) = x_2(k) - x_{M2}(k)$	101
30 Evolución temporal de los errores de sincronía restantes $e_1(k) = x_1(k) - x_{M1}(k)$ y $e_3(k) = x_3(k) - x_{M3}(k)$	102
31 Errores de sincronía $e_1(k) = x_1(k) - x_{M1}(k)$ y $e_2(k) = x_2(k) - x_{M2}(k)$ cuando los parámetros del maestro son $a = 1.95$ y $b = 1$ y en el esclavo son $a = 2$ y $b = 1.1$	103

Lista de Figuras (Continuación)

Figura	Página
32 Errores de sincronía $e_i(k) = x_i(k) - x_{M_i}(k)$, $i = 1, 2, 3$ cuando el parámetro γ del maestro es 0.35 y en el esclavo es $\gamma = 0.45$	104
33 Errores de sincronía $e_1(k) = x_1(k) - x_{M_1}(k)$, $e_2(k) = x_2(k) - x_{M_2}(k)$ y $e_3(k) = x_3(k) - x_{M_3}(k)$ cuando el parámetro γ del maestro es 0.35 y en el esclavo es $\gamma = 0.75$	105
34 Errores de sincronía $e_1(k) = x_1(k) - x_{M_1}(k)$, $i = 1, 2, 3$ cuando el parámetro ζ del maestro es 0.2 y en el esclavo es $\zeta = 0.3$	106
35 Esquema de comunicación privada empleando sincronía de salida por acoplamiento a modelos.	109
36 Transmisión de una señal binaria por medio de conmutación entre atractores hipercaóticos. Parámetro $a_0(k)$ (mensaje binario), Señal transmitida $\phi_M(k)$ y señal de error $e(k) = y(k) - y_M(k)$ (mensaje recuperado).	111
37 Transmisión de una señal binaria por medio de conmutación entre atractores hipercaóticos. Parámetro $\gamma(k)$ (mensaje binario), Señal transmitida $\phi_M(k)$ y señal de error $e(k) = y(k) - y_M(k)$ (mensaje recuperado).	111
38 Esquema de comunicación privada empleando una línea de transmisión.	112
39 Transmisión de una señal binaria por medio de conmutación entre atractores hipercaóticos. Parámetro $a(k)$ (mensaje binario), Señal transmitida $\phi_M(k)$ y señal de error $e(k) = \phi_M(k) - \phi(k)$ (mensaje recuperado).	114
40 Parámetro $\gamma(k)$, señal transmitida $\phi_M(k)$ y error $e(k) = \phi_M(x_M(k), p, p') - \phi(x(k), p)$	116
41 Encriptamiento aditivo empleando dos líneas de transmisión.	118
42 Mensaje original $m(k)$, señal de transmisión $s(k) = y_M(k) + m(k)$ y mensaje recuperado $\hat{m}(k) = s(k) - y(k)$	119
43 Mensaje original $m(k)$, señal de transmisión $s(k) = y_M(k) + m(k)$ y mensaje recuperado $\hat{m}(k) = s(k) - y(k)$	119
44 Esquema de comunicación con una línea de transmisión.	121
45 Mensaje $m(k)$, señal transmitida $\phi_M(k)$ y mensaje recuperado.	122
46 Mensaje $m(k)$ (señal de audio), señal transmitida $\phi_M(k)$ y mensaje recuperado.	123

Lista de Tablas

Tabla		Página
I	Error cuadrático medio de Monte Carlo $(SSE_i)_{MC}$, error cuadrático medio truncado $(TMSE_i)_{MC}$ de Monte Carlo y tiempo de sincronía (39) para el ejemplo 1 con $P_0 = 5 \times 10^{-6}$	61
II	Error cuadrático medio $(SSE_i)_{MC}$ de Monte Carlo y tiempo de sincronía (39) para el ejemplo 2 con $P_0 = 1$, $R = 5 \times 10^{-8}$, $\rho = 0.05$ y $N = 100$. . .	66
III	Error cuadrático medio truncado de Monte Carlo y tiempo de sincronía (39) para el ejemplo 2 con $P_0 = 1$, $q_i = 1 \times 10^{-6}$, $i = 1, 2, 3$, $R = 5 \times 10^{-8}$, $\rho = 0.05$ y $N = 100$	66

Capítulo I

Introducción

El presente trabajo doctoral versa sobre **sincronización de sistemas caóticos en tiempo discreto**, por tanto, se considera propicio iniciar por describir aunque breve y de manera informal, los conceptos de *sincronía* y *caos*.

La palabra **sincronía** proviene de los vocablos griegos $\chi\rho\acute{o}\nu\omicron\varsigma$ (**cronos**, que significa **tiempo**) y $\sigma\acute{o}\nu$ (**sin**, que significa **lo mismo, común, coincidencia**), en una traducción directa, "sincronía" significa "sucesos ocurriendo al mismo tiempo". Ahora, según el diccionario de la Real Academia Española, **sincronizar** significa: "*Hacer que coincidan en el tiempo dos o más movimientos o fenómenos*". O también, se define en Cruz-Hernández, (2006) que **sincronización** puede verse como la propiedad que presenta un conjunto de "objetos" de naturaleza distinta (o no) de manifestar un ritmo uniforme de coexistencia, generalmente distinto a sus ritmos individuales, debido a la presencia de una conexión o de un medio físico de acoplamiento entre ellos, el cual, en

la mayoría de los casos, es extremadamente débil.

La propiedad de sincronía puede observarse en actividades tan sencillas y cotidianas, como la de un niño brincando una cuerda, donde cada salto del niño coincide con el paso de la cuerda sobre el piso, en el vuelo de las aves. Un grupo de personas bailando acorde con el ritmo de la música, en el nado sincronizado, en general, en el comportamiento colectivo de los humanos, ya sea voluntaria o involuntariamente. También, puede observarse esta propiedad en hechos más complejos como en el movimiento que describen los cuerpos celestes.

La primera observación formal de este fenómeno de sincronía se remonta al siglo XVII y se atribuye al científico holandés Christian Huygens, quien observó y trató de explicar la sincronía ocurrida entre dos péndulos de relojes colgados de una misma plataforma. En sus experimentos, Huygens observó que los movimientos de los péndulos siempre sincronizaban, es decir, al cabo de cierto tiempo ambos péndulos terminaban su recorrido en algún sentido (derecha o izquierda) al mismo tiempo, y si el movimiento de alguno de ellos era perturbado de manera intencional, los movimientos de los péndulos volvía a entrar en sincronía después de transcurrir breve tiempo. Huygens encontró la explicación a este fenómeno en el *acoplamiento* que existía entre los dos relojes por medio de la plataforma a la que estaban colgados. Desde entonces, el fenómeno de sincronía de osciladores se emplea con provecho en muchas áreas de las ciencias e ingenierías y su aplicación recae en campos tan diversos como dispositivos eléctricos, sistemas de radiocomunicación, máquinas vibratorias, encriptado de información, en

neurociencias y medicina, por mencionar algunas. A continuación se mencionan algunos ejemplos particulares en nuestra área de interés Cruz-Hernández, (2006):

- Sincronización de generadores cuánticos de radio frecuencia ("massers"),
- Sincronización de osciladores exhibiendo comportamiento periódico, cuasiperiódico o caótico con aplicación en comunicaciones privadas y seguras de información confidencial.
- Sincronización de robots para realizar una tarea común.
- Sincronización de oscilaciones eléctricas y electromagnéticas en electrónica y radio.
- Sincronización modal en láseres que permite generar pulsos de luz muy potentes.

Otro concepto importante en este trabajo de investigación es el **caos**, aunque la palabra misma, invita a pensar en desorden. Desde el punto de vista científico, el caos se refiere a un comportamiento dinámico complejo, que puede modelarse por ecuaciones no lineales, el cual, posee características muy particulares como ser sensible a condiciones iniciales, generar atractores "extraños", tener al menos un exponente de Lyapunov positivo, entre otras que se describirán con detalle posteriormente. A manera de ilustración, en la figura 1 se muestran simulaciones de un sistema que presenta este comportamiento (circuito de Chua). El sistema bajo ciertas condiciones paramétricas presenta un comportamiento *periódico*, como puede observarse en la figura 1(a),

sin embargo, al modificar sus parámetros el sistema puede exhibir un comportamiento *caótico*. La figura 1(b) presenta este caso en el que es evidente que genera una dinámica más compleja. Hoy en día, los sistemas caóticos son utilizados en distintas ramas de la ciencia como por ejemplo en meteorología, en un intento por modelar la atmósfera y su comportamiento, en biología en los estudios de población cambiante en colonias de animales o en la propagación de epidemias, en física dentro de la teoría de partículas elementales y los desplazamientos de electrones en el átomo, etc.

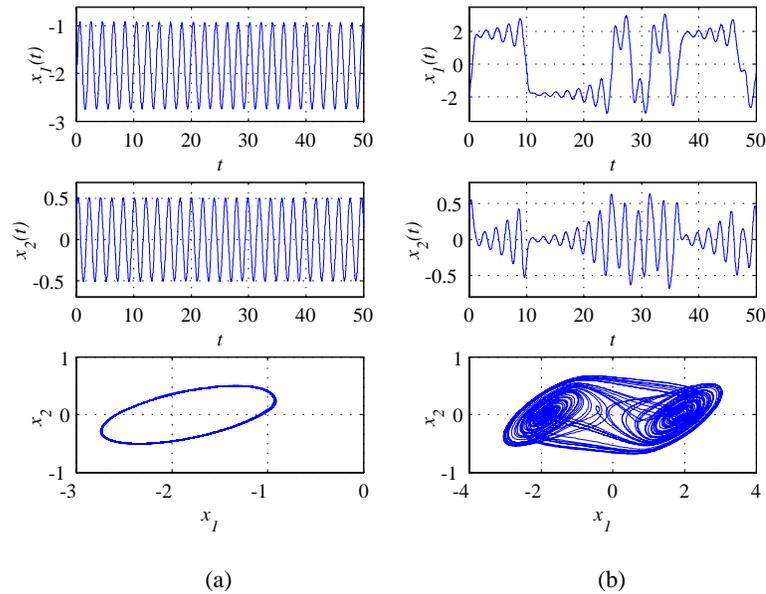


Figura 1: Estados $x_1(t)$, $x_2(t)$ y plano x_1 vs x_2 del circuito de Chua. (a) Comportamiento periódico, (b) Comportamiento caótico.

Sincronizar sistemas con dinámicas complejas como los sistemas caóticos, es decir, hacer que coincidan en tiempo y forma con alguna dinámica de interés ha generado diversas líneas de investigación, principalmente por el gran potencial de aplicaciones que tiene en el área de comunicaciones seguras. Básicamente, el **problema de sin-**

cronización de caos, en un escenario de acoplamiento unidireccional, puede formularse como sigue (Cruz-Hernández, 2006): "Dado un sistema caótico, considerado como maestro y otro sistema como esclavo, el objetivo es forzar el comportamiento del esclavo a converger a la dinámica impuesta por el maestro, independientemente de las condiciones iniciales". Entre los trabajos pioneros sobre sincronización de osciladores caóticos figuran Fujisaka y Yamada, (1983); Pikovsky, (1984); Afraimovich *et al.*, (1986); Pecora y Carroll, (1990), que expusieron los primeros ejemplos de sincronización de osciladores caóticos con acoplamiento unidireccional (donde la información fluye en un sólo sentido).

En particular, el trabajo de Pecora y Carroll en 1990 tuvo fuerte impacto en la comunidad científica y estimuló muchas investigaciones posteriores sobre sincronización de caos y tópicos relacionados, como por ejemplo los trabajos reportados en congresos y revistas Kocarev *et al.*, (1992); Ogorzalek, (1993); Wu y Chua, (1993); Ding y Ott, (1994); Nijmeijer y Mareels, (1997); Sira-Ramírez y Cruz-Hernández, (2001); Número especial en IEEE Transactions on Circuit and Systems I, (1997) y en System and Control Letters, (1997) y en los libros Chen y Dong, (1998; 2000); Fradkov y Progronsky, (1998) y Pikovsky, (2001) por mencionar algunos. Estos trabajos están ubicados en un escenario ideal, sin embargo, en una situación real es necesario sincronizar sistemas ante perturbaciones o ruido en la señal acoplante y en las dinámicas de los osciladores [Sobiski, 1998; Cruz-Hernández y Nijmeijer, 1999; 2000] o bien, sincronización de sistemas no idénticos [Wagg, 2002; López Mancilla y Cruz-Hernández, 2004; 2005a; 2005b;

López Mancilla, 2005].

Por otra parte, la mayoría de trabajos reportados en la literatura relacionados con este tópico, abordan el caso de osciladores caóticos en tiempo continuo. En cambio, sobre sincronización de osciladores caóticos en **tiempo discreto** son escasos los trabajos realizados. Sin embargo, el interés en el caso discreto es de considerable importancia, debido a las facilidades de implementación que este tipo de sistemas ofrece, al emplear por ejemplo computadoras digitales, resulta en una motivación más para estudiar el caso discreto. Aunque la mayoría de los sistemas reales son de tiempo continuo, frecuentemente es deseable obtener modelos discretos, los cuales, representen fielmente las dinámicas de tales sistemas, algunas razones se deben a:

- En la práctica, las mediciones comunmente se realizan a determinados intervalos de tiempo,
- El procesamiento digital de señales y en el control, se encuentran constantemente favorecidos,
- Simulaciones digitales pueden efectuarse fácil y rápidamente.

Algunos trabajos sobre sincronización de osciladores en tiempo discreto son Feldmann *et al.*, (1996); Huijberts *et al.* (1999); Cruz-Hernández y Nijmeijer, (1999; 2000); Sira-Ramírez *et al.*, (2002); Hai y Jiandong, (1997).

I.1 Motivación

El cifrado de información confidencial con base en sincronía de caos, fue reportado en los albores de la década de los 90s [Pecora y Carroll, 1990; Ott *et al.*, 1990] como alternativa prometedora para la codificación, que difiere sustancialmente de los métodos criptográficos convencionales, los cuales, emplean algoritmos numéricos como claves de encriptamiento. Una *señal caótica es intrínsecamente apropiada para el encriptamiento*. Se mencionan por el momento, dos razones poderosas para afirmar lo anterior; primeramente, la dinámica caótica es similar a la del ruido blanco y de este modo, puede emplearse para ocultar información y proteger en la comunicación a ésta de algún intruso. En segundo lugar, los sistemas caóticos son determinísticos y en algunos casos, sus dinámicas complejas son gobernadas por simples ecuaciones diferenciales o en diferencias no lineales. De manera general, el **esquema de un sistema encriptador de información con base en caos**, consiste en un transmisor compuesto por dos elementos principales, un generador de caos (maestro) y un algoritmo (o medio) de encriptamiento para codificar la información en el caos. Un receptor, también formado por dos elementos principales, un sistema esclavo, el cuál, tiene la consigna de reproducir el comportamiento caótico generado en el transmisor (usualmente se diseña con los mismos elementos empleados en el transmisor para generar caos) y un algoritmo (o medio) de desencriptamiento, cuya función es extraer la información original escondida dentro de señales caóticas transmitidas.

Muchos trabajos se han dedicado al diseño de sistemas de encriptado de informa-

ción con base en caos. Por ejemplo en Pecora y Carroll, (1990) se reportó un sistema en el cual, el generador de caos está formado por dos subsistemas, uno estable y otro inestable. Una replica del subsistema estable se emplea en el receptor para obtener sincronía caótica con el transmisor, el cual, de este modo se pueda restar de la señal caótica de transmisión para reconstruir la información. Otro método consiste en codificar la información dentro de órbitas periódicas inestables adjuntas al caos en su espacio de fase [Ott *et al.*, 1990]. Este método de encriptado supone, que cada órbita periódica inestable puede ser dirigida separadamente por la señal de información. Esto es posible mediante el método conocido por OGY (Ott, Gregori y Yorke) el cual, dirige a las oscilaciones caóticas a cualquiera de sus órbitas periódicas inestables. La decodificación se obtiene por un procedimiento inverso. El método OGY es potencialmente atractivo pero requiere un tiempo de procesamiento relativamente grande para inducir las pequeñas perturbaciones requeridas para guiar cada una de las trayectorias. Métodos analógicos y más rápidos fueron también estudiados, empleando retroalimentación en el lazo del oscilador caótico [Hunt, 1991; Pyragas, 1992]. Desde entonces diferentes métodos se han propuesto para transmitir información oculta en dinámicas caóticas: **encriptamiento caótico aditivo** [Cuomo *et al.*, 1993], **encriptamiento por conmutación entre dos atractores caóticos** [Cuomo *et al.*, 1993; Parlitz *et al.*, 1992; Dedieu *et al.*, 1993], **encriptamiento por modulación paramétrica** [Yang y Chua, 1996], etc. Sin embargo, trabajos posteriores mostraron que en algunos casos particulares, la *información cifrada por caos* (con tan solo un exponente de Lyapunov positivo), se puede *reconstruir (descifrar) con algún receptor intruso*, ya sea empleando técnicas

de procesamiento de señales o bien mapas de reconstrucción [Short, 1994; 1996; Pérez y Cerdeira, 1995], conocidas por técnicas de "**ataque**".

Quedando demostrado con lo anterior, dos factores relevantes en la seguridad de estos sistemas, que son:

- La dimensión del atractor caótico y
- El esfuerzo requerido para obtener la igualdad en los valores de los parámetros en transmisor y receptor.

A partir de entonces, la comunidad científica interesada en este tópico, se dió a la tarea de hacerle frente a estos ataques criptoanalíticos a la comunicación confidencial con base en sincronía de caos. A continuación, se mencionan las principales aportaciones en esta dirección, algunos **procedimientos para incrementar la seguridad en la comunicación caótica** son:

- Aplicar algoritmos criptográficos convencionales a la información y mezclarla posteriormente con el caos [Yang y Chua, 1997; Serrano y Cruz-Hernández, 2002; 2005].
- Aumentar la dimensión del atractor, generando con esto atractores hipercaóticos [Anishchenko *et al.*, 1994; Meranza y Cruz-Hernández, 2002; Cruz *et al.*, 2004].
- Sincronizar osciladores con retardo de tiempo [Pyragas, 1998; Cruz-Hernández, 2003; 2004], ya que tales osciladores cuentan con un espacio de estados de dimen-

sión infinita y despliegan atractores hipercaóticos con un número arbitrariamente grande de exponentes de Lyapunov positivos.

- Sincronizar sistemas no idénticos [López y Cruz-Hernández, 2004a; 2004b; López, 2005].
- Emplear osciladores con atractores caóticos de enrollamientos múltiples [Chen y Ueta, 2002; Díaz *et al.*, 2003; Gámez *et al.*, 2004].

Por tanto, un **asunto fundamental** y relevante en la construcción de sistemas de encriptado, tanto analógicos como digitales basados en dinámicas caóticas, **es la selección del generador de caos** [Kolumban *et al.*, 1997].

De ahí que, se haya planteado como objetivo a alcanzar con este trabajo doctoral, la sincronización de sistemas caóticos en tiempo discreto, empleando acoplamiento a modelos y para un escenario ruidoso en las dinámicas y en la señal de acoplamiento, emplear un filtro extendido de Kalman. Con la consecuencia de aplicar estos resultados en el diseño de sistemas de encriptamiento de información confidencial. Por el tipo de sistemas empleados en maestro y esclavo con dinámicas extremadamente complejas, se pretende contribuir al incremento de la "confiabilidad" en la codificación. Además, proponer específicamente para el acoplamiento a modelos, algunas modificaciones a técnicas conocidas y empleadas de encriptamiento caótico, con el propósito de dificultar más la decodificación de la información confidencial, por un receptor no autorizado.

En los últimos años ha surgido el interés por sincronizar **sistemas hipercaóticos**

[Peng *et al.*, 1996, Brucoli *et al.*, 1998, Pecora *et al.*, 1997, Zhang *et al.*, 1998; Cruz-Hernández *et al.*, 2002; Cruz-Hernández, 2004], los cuales, manifiestan una dinámica más compleja que los sistemas caóticos. También para estos sistemas, nuevamente la mayoría de los trabajos realizados se refieren al caso continuo. Sin embargo, aunque pocos, existen trabajos en el contexto discreto que reportan resultados satisfactorios, aunque muchas veces en un escenario ideal o bien considerando sólo sistemas caóticos con una estructura particular.

De lo anterior, es que surge una de las principales motivaciones del presente trabajo de tesis doctoral por estudiar la sincronización de osciladores hipercaóticos discretos con la intención de contribuir a la solución de este problema, empleando como metodología de trabajo, herramientas matemáticas conocidas de teoría de control no lineal, como el acoplamiento a modelos, la cual, presenta las siguientes ventajas con relación a otras metodologías de sincronización:

- La sincronía se obtiene de manera sistemática y permite conocer la señal de acoplamiento apropiada.
- Puede aplicarse a muchos sistemas caóticos e hipercaóticos, tanto en el contexto continuo como discreto.
- Puede aplicarse a sistemas idénticos y no idénticos [López y Cruz-Hernández, 2005a; 2005b; López, 2005].
- No es necesario el cálculo de ningún exponente de Lyapunov.

- No requiere que las condiciones iniciales pertenezcan a la misma región de atracción.

En cuanto al empleo de un filtro extendido de Kalman como sistema esclavo, presenta las siguientes ventajas sobre otras metodologías de sincronía:

- El filtro extendido de Kalman posee algunas propiedades naturales de robustez a ruido gaussiano aditivo en la señal de acoplamiento [Cuomo *et al.*, 1993].
- El filtro extendido de Kalman es de fácil implementación.
- Flexibilidad en aplicaciones, dado que no es necesario una descomposición en subsistemas en el sentido de Pecora y Carroll.

Se describe a continuación el problema de estudio.

I.2 Planteamiento del problema

Considere el siguiente par de osciladores hipercaóticos definidos por ecuaciones de la forma

$$x_M(k+1) = f_M(x_M(k)), \quad x_M(k) \in \mathbb{R}^n, \quad (1)$$

$$x(k+1) = f(x(k)), \quad x(k) \in \mathbb{R}^n, \quad (2)$$

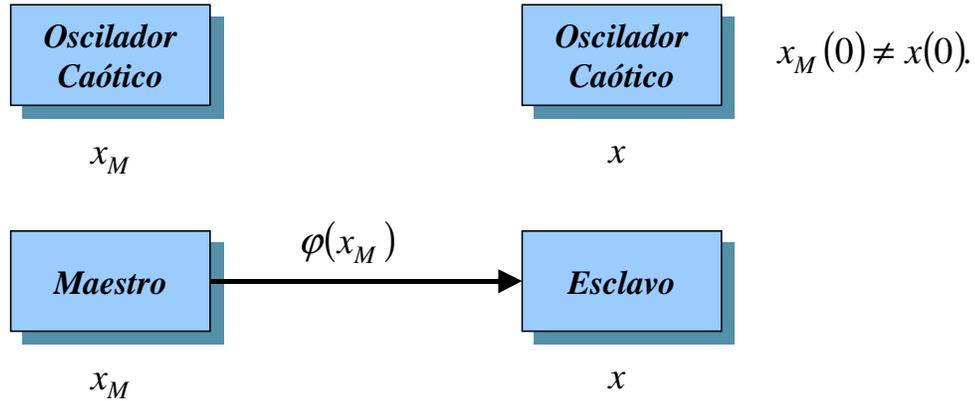


Figura 2: Osciladores sin acoplamiento (figura superior) y acoplados mediante la señal $\varphi(x_M)$ (figura inferior).

Se considera que los osciladores están inicialmente desacoplados y presentan dinámicas totalmente diferentes ($x_M(0) \neq x(0)$). Aplicando el escenario de acoplamiento maestro-esclavo (unidireccional) entre (1) y (2) mediante una señal de acoplamiento $\varphi(x_M)$ como se muestra en la figura 2 quedando entonces el sistema maestro representado por

$$x_M(k+1) = f_M(x_M(k)), \quad x_M(k) \in \mathbb{R}^n,$$

y el sistema esclavo queda

$$x(k+1) = f(x(k), u(k)), \quad x(k) \in \mathbb{R}^n,$$

siendo $u(k)$ la entrada al esclavo.

El objetivo de control es que los osciladores caóticos cumplan con:

$$\lim_{k \rightarrow \infty} \|x_M(k) - x(k)\| \equiv 0,$$

para toda señal acoplante apropiada generada por los osciladores e independientemente de las condiciones iniciales $x_M(0)$ y $x(0)$, lo anterior se conoce en la literatura como sincronización completa. El vector de error de sincronía se define por la expresión

$$e(k) = x_M(k) - x(k).$$

En particular para el empleo del filtro extendido de Kalman las ecuaciones del maestro y del esclavo quedan expresadas de la siguiente manera:

$$M : \begin{cases} x_M(k+1) = f_M(x_M(k)) + w(k) \\ y_M(k) = h_M = h_M(x_M(k)) + v(k) \end{cases}$$

$$E : \begin{cases} x(k+1) = f(x(k), y_M(k)) \\ y(k) = h(x(k)). \end{cases}$$

y el problema de control consiste en diseñar un filtro extendido de Kalman tal que

$$\lim_{k \rightarrow \infty} \|E[x_M(k) - x(k)]\| \leq \rho,$$

independientemente de las condiciones iniciales, lo anterior se conoce como sincronización

aproximada.

Para el caso del empleo de acoplamiento a modelos, maestro y esclavo quedan expresados de la siguiente forma

$$\begin{aligned}
 M & : \begin{cases} x_M(k+1) = f_M(x_M(k), u_M(k)) \\ y_M(k) = h_M(x_M(k)), \end{cases} \\
 E & : \begin{cases} x(k+1) = f(x(k), u(k)) \\ y(k) = h(x(k)). \end{cases}
 \end{aligned}$$

el problema de control en este caso consiste en el diseño de una ley de control $u(k)$ apropiada, tal que se cumpla con la sincronización de salida:

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

independientemente de las condiciones iniciales (sincronización parcial).

Se mencionan a continuación los objetivos que conforman el presente trabajo de tesis doctoral.

I.3 Objetivos

Dado que hasta el momento no existe solución general al problema de sincronización de osciladores hipercaóticos y dada la escasa formalización de resultados reportados sobre el tema en la literatura, más específicamente tratándose de sistemas discretos,

con la realización de este trabajo se plantea alcanzar el siguiente **objetivo general**:

Contribuir a la solución de problemas abiertos en sincronización de sistemas hipercaóticos discretos empleando la configuración unidireccional de acoplamiento.

Los problemas particulares que serán abordados son los siguientes:

1. *Sincronización de sistemas hipercaóticos discretos por acoplamiento a modelos.*
2. *Sincronización de sistemas hipercaóticos discretos contaminados por ruido, mediante un filtro extendido de Kalman.*
3. *Sincronización de sistemas hipercaóticos discretos en presencia de perturbaciones.*
4. *Aplicaciones en sistemas seguros/privados de comunicación en la codificación de información confidencial.*

I.4 Organización del manuscrito

La presente memoria de tesis se organiza en seis capítulos y un apéndice. En el **primer capítulo**, se presenta una introducción al trabajo desarrollado y se plantean los objetivos del mismo. Para una mejor comprensión del trabajo que aquí se presenta se facilitan en el **capítulo dos**, algunas definiciones básicas sobre los principales términos que se emplearán a lo largo de esta memoria. En el **tercer capítulo** se expone la teoría del filtro de Kalman para posteriormente utilizar el filtro extendido de Kalman en la sincronización de sistemas hipercaóticos discretos mostrándose simulaciones numéri-

cas para dos ejemplos particulares. En el **capítulo cuatro**, se aborda el tema de acoplamiento a modelos describiendo brevemente en que consiste dicho problema, para luego utilizar dicha técnica en la sincronización parcial y completa de sistemas hipercaóticos discretos, complementando lo anterior con simulaciones numéricas realizadas a dos ejemplos particulares. En el **quinto capítulo**, se muestra la aplicación en el área de comunicaciones privadas de los resultados obtenidos en el capítulo cuatro utilizando simulaciones. Finalmente, en el **capítulo seis** se presentan las conclusiones más importantes del trabajo doctoral y se mencionan las posibilidades de trabajos futuros en esta dirección.

Capítulo II

Preliminares

En este capítulo, se presenta un conjunto de definiciones básicas de algunos términos que se utilizarán a través de esta memoria, así como un panorama general de la sincronización de sistemas caóticos, todo esto con el propósito de ayudar a una mejor comprensión de este trabajo de tesis.

II.1 Mapas

El tipo de sistemas que involucra este trabajo de tesis son **sistemas discretos**, los cuales, son sistemas dinámicos, cuyo comportamiento está formulado directa o indirectamente, mediante iteraciones o mapas. Por formulación **directa** se refiere a aquellos modelos matemáticos provenientes de sistemas dinámicos cuya naturaleza propia es discreta y por formulación **indirecta**, se entiende aquel que proviene de la discretización

aplicada a un sistema continuo.

Un sistema discreto esta definido por ecuaciones en diferencias de la forma

$$x(k+1) = f(x(k)), \quad x(0) = x_0, \quad k \in \mathbb{Z} \quad (3)$$

donde el vector de estado x es de dimensión n , k es el índice de iteración (que puede representar tiempo) y f es una función no lineal tal que, para todos los elementos $x(k) \in \mathbb{R}^n$ asigna un elemento único $f(x(k))$, esto es, $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$ para toda $k \geq 0$. Un sistema discreto siempre tiene solución derecha (para $k > 0$). Sin embargo, a menos que f sea invertible, no tendrá solución izquierda ($k < 0$). En particular, la solución del sistema (3) esta dada por $x(k) = f^k(x_0)$ con $x(0) = x_0$. A continuación se mencionan algunas características básicas de los sistemas discretos:

- En el sistema (3), si f no depende explícitamente del tiempo discreto k entonces el mapeo se denomina **autónomo**. En contraparte, en los sistemas **no autónomos** la función f depende explícitamente de k , es decir $x(k+1) = f(x(k), k)$. El término **mapa** se reserva generalmente a sistemas autónomos.
- Un **punto de equilibrio** $x_e \in \mathbb{R}^n$ del sistema (3) es una solución del mismo que satisface $x_e = f(x_e)$ para toda $k \geq 0$.
- Cuando f es una función continua para toda k y continuamente diferenciable en x y si f^{-1} existe y es única en el dominio de f , entonces el mapa f es un **mapa invertible** llamado **difeomorfismo**. Cuando f no es continuamente diferenciable

se llama simplemente mapa invertible. Cuando f es tal que f^{-1} pudiera ser multivaluada o pudiera no existir, entonces se dice que el mapa es **no invertible**.

- Sea f un mapa C^1 . Un punto de equilibrio $\bar{x} \in \mathbb{R}^n$ de f es **asintóticamente estable** si $|f'(\bar{x})| < 1$, e **inestable** si $|f'(\bar{x})| > 1$.

II.2 Caos

Al escuchar la palabra “**caos**”, generalmente se piensa en desorden. Sin embargo, en la literatura técnica, el término caos se refiere a una secuencia que parece azarosa y desordenada, pero que en realidad es de naturaleza determinística. En este sentido, el concepto de caos se conoce desde mucho tiempo atrás, sin embargo, no ha sido sino hasta en las últimas tres décadas que comenzó a crecer el interés por conocer este fenómeno a fondo, debido a la gran variedad de aplicaciones en que se puede emplear, por ejemplo, en la estabilización de láseres, en la codificación de información confidencial en comunicaciones privadas, en el control de arritmias y en casos de epilepsia en el cerebro humano, los fluidos en régimen turbulento, la dinámica de la atmósfera, las reacciones químicas, la propagación de enfermedades infecciosas, los procesos metabólicos de las células, el mercado financiero mundial, los movimientos de grupos animales (cardúmenes o enjambres), etc.

En la actualidad no existe una definición rigurosa y universalmente aceptada de caos, aunque de manera general, se puede definir un sistema caótico como un sistema

determinístico, regido por ecuaciones diferenciales o en diferencias no lineales, que presenta un comportamiento dinámico aparentemente aleatorio y sensible a condiciones iniciales. A continuación se presentan algunas **características** principales **que identifican a los sistemas caóticos**:

- **Dinámica no lineal.** El caos es un fenómeno exclusivo de los sistemas dinámicos **no lineales**. Un sistema lineal, no importa el orden que tenga, no puede presentar este comportamiento [Álvarez Gallegos, 2001].
- **Múltiples órbitas periódicas.** La presencia de varias órbitas periódicas origina que los sistemas caóticos presenten un espectro frecuencial característico, similar a la de una señal aleatoria (ruido). La figura 3 muestra un espectro de frecuencias típico de una señal caótica.

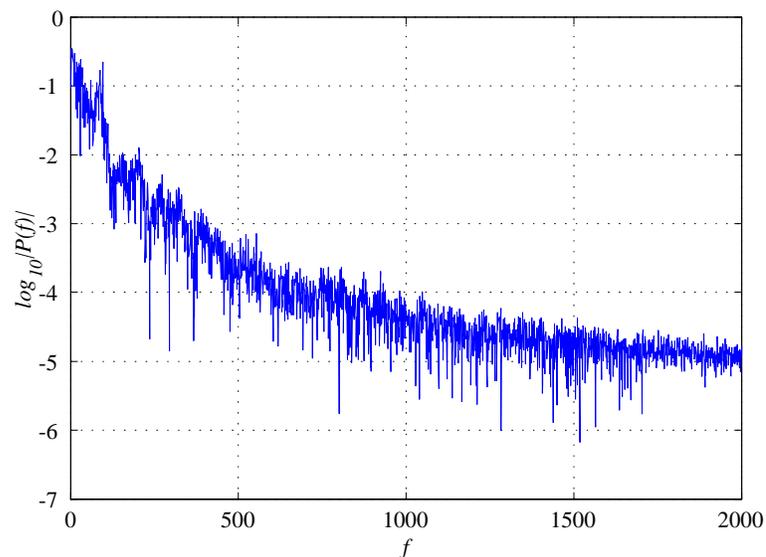


Figura 3: Espectro de frecuencias típico de una señal caótica.

- **Sensibilidad a condiciones iniciales.** A partir de condiciones iniciales diferentes, aunque muy cercanas una de las otras, las trayectorias correspondientes que se producen tienden a ser distintas o a diverger exponencialmente conforme el tiempo transcurre, sin existir correlación alguna entre dichas trayectorias. Esto se ilustra en las figuras 4 y 5 donde se observa que la diferencia entre trayectorias crece de manera que no es posible predecir a largo plazo la evolución del sistema, aún cuando la diferencia inicial sea arbitrariamente pequeña.

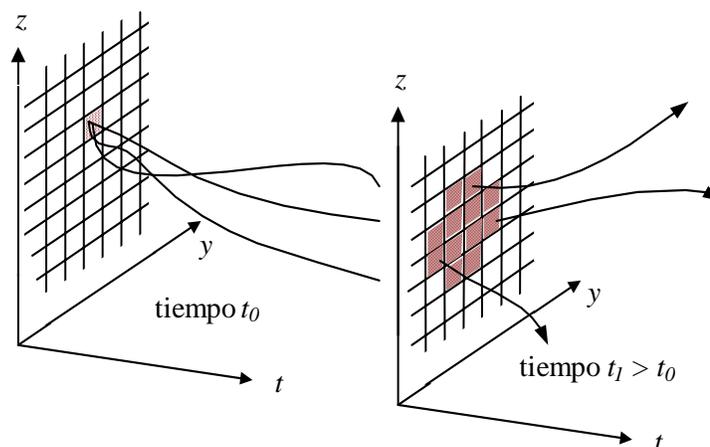


Figura 4: Divergencia de las trayectorias en un sistema caótico comenzando bajo condiciones iniciales muy cercanas.

- **Presencia de “atractores extraños”.** Otra característica propia de los sistemas caóticos es la aparición, en su diagrama de fase, de estructuras geométricas con formas poco usuales y sin ningún parecido a objetos geométricos clásicos, son los llamados “atractores extraños”, nombre dado a las estructuras asintóticas hacia donde evolucionan las órbitas de un sistema caótico. En las figuras 6 y 7

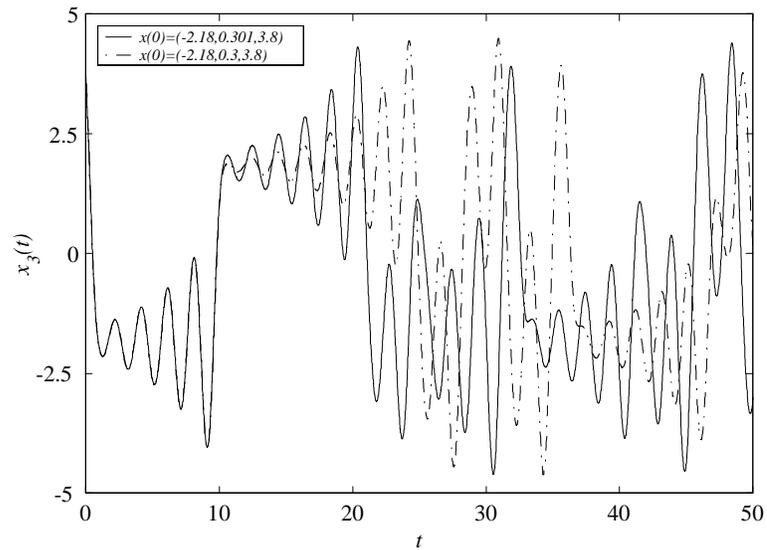


Figura 5: Evolución en el tiempo de uno de los estados del circuito caótico de Chua inicializado bajo condiciones muy semejantes.

se presenta el atractor para dos sistemas, uno continuo y otro discreto respectivamente, que presentan comportamiento caótico. los sistemas caóticos también poseen otras características como la dimensión fractal, propiedad de mezcla, etc. pudiendo consultar para más detalle Moon, .

II.3 Exponentes de Lyapunov

Entre otras (como las que se mencionaron anteriormente), un atractor caótico tiene las siguientes dos características:

- Atrae puntos vecinos al atractor y
- Las órbitas de puntos vecinos entre sí divergen.

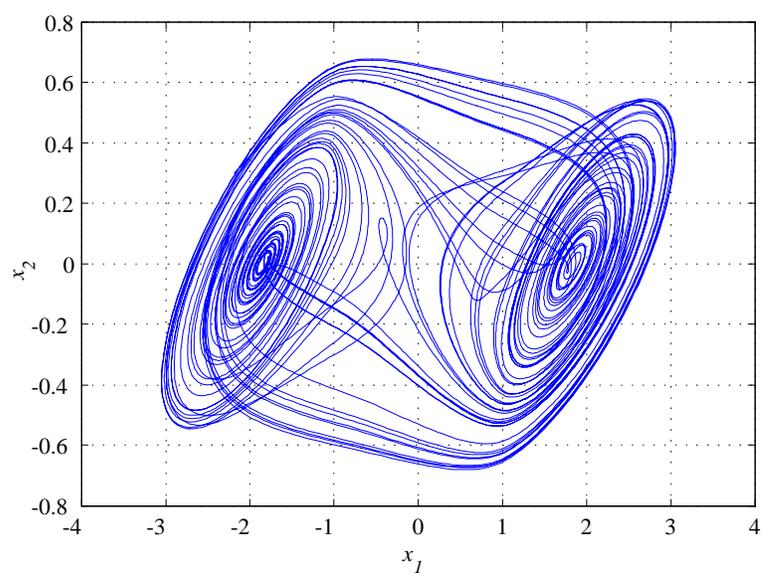


Figura 6: Atractor del circuito caótico de Chua (tiempo continuo).

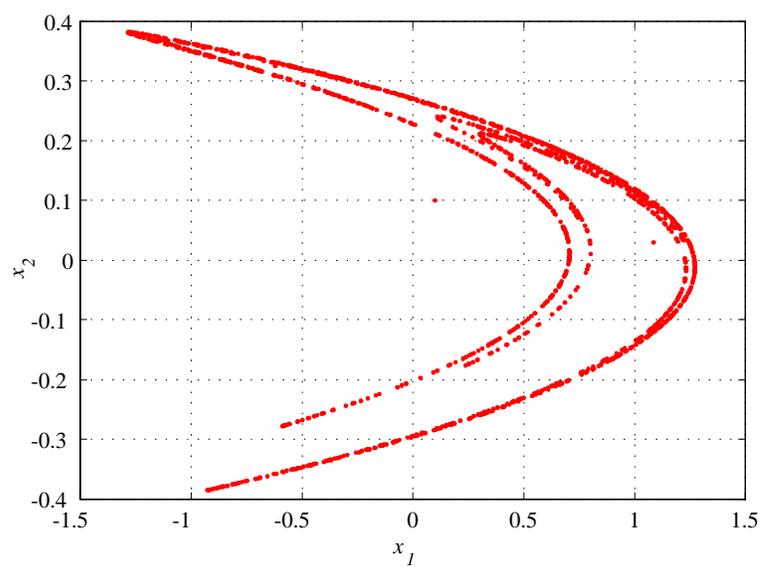


Figura 7: Atractor del mapa caótico de Hénon (tiempo discreto).

Los exponentes de Lyapunov se utilizan para cuantificar dicha expansión y contracción de trayectorias vecinas en un sistema dinámico, es decir, dan una medida de la proporción exponencial, en la cual, órbitas cercanas se van apartando o acercando. En algún sentido, determinan la complejidad de un sistema no lineal.

Los exponentes de Lyapunov son una generalización de lo que son los valores propios en un sistema lineal. Matemáticamente, los exponentes de Lyapunov de un sistema se definen en términos de la solución de la ecuación,

$$\lambda = \lim_{k \rightarrow \infty} \frac{1}{k} \ln \left| \frac{d f^k(x_0)}{dx_0} \right| \quad (4)$$

si el límite existe, siendo λ el **exponente de Lyapunov** de la trayectoria $x(k) = f^k(x_0)$, o bien del mapa f iniciando en el punto x_0 [Chen y Dong, 1998].

La *convergencia* de trayectorias a lo largo de una dirección en el espacio de estados, corresponde a un exponente de Lyapunov negativo. Mientras que la *divergencia* de trayectorias se caracteriza por un exponente de Lyapunov positivo. Una dirección neutra, *sin converger ni diverger*, corresponde a un exponente de Lyapunov con valor cero. El valor absoluto de estos exponentes cuantifica la velocidad de convergencia de las trayectorias. Por tanto, **si un sistema tiene un exponente de Lyapunov positivo** se dice que el sistema **es caótico** (condición necesaria).

II.4 Hipercaos

Cuando un sistema dinámico tiene solución acotada con **dos o más exponentes de Lyapunov positivos**, se dice que el sistema es **hipercaótico**, es decir, presenta un comportamiento más complejo que el caos. Físicamente, esta cantidad representa una mayor velocidad de divergencia de las trayectorias. Este tipo de sistemas se presentan tanto en el contexto continuo como en el discreto, y se pueden encontrar en diversos fenómenos naturales o bien se pueden construir, utilizando por ejemplo, dos sistemas caóticos acoplados. En la figura 8 se muestra el atractor del circuito hipercaótico de Chua, formado al acoplar dos circuitos caóticos de Chua. Obsérvese que presenta un comportamiento más complejo que el mostrado en la figura 6.

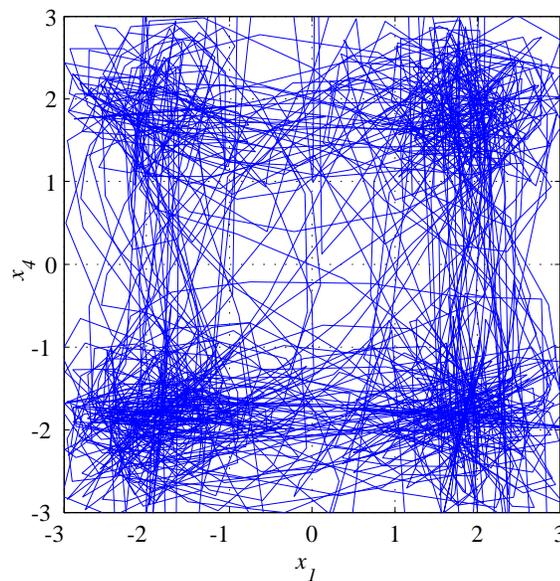


Figura 8: Atractor del circuito hipercaótico de Chua.

II.5 Sincronía

De manera general, **sincronización** se puede definir como la propiedad que posee un conjunto de objetos materiales de naturaleza muy distinta, de adoptar un mismo ritmo de coexistencia pese a sus diferentes ritmos individuales y a menudo, interactuando mediante conexiones extremadamente “débiles”.

Históricamente, la sincronía está ligada generalmente al movimiento periódico; en particular, en este trabajo de tesis el interés radica en la sincronización de sistemas caóticos e hipercaóticos. Dos señales periódicas sincronizan si sus periodos son idénticos, para el caso de señales caóticas es diferente, en este caso, se requiere que las señales sean idénticas por lo menos de manera asintótica para decir que están sincronizadas. Se dice que dos osciladores caóticos están sincronizados, si finalmente transcurrido el transitorio (pudiendo ser un lapso de tiempo largo o corto), las oscilaciones coinciden exactamente, a pesar de comenzar ambos osciladores en condiciones distintas.

II.5.1 Escenarios de acoplamiento

La sincronización es frecuentemente categorizada con base al mecanismo físico de acoplamiento que existe entre los osciladores, el cual, permite su interacción. Este acoplamiento puede ser **unidireccional** [Parlitz y Kokarev, 1998; Hasler, 1995] o **bidireccional** [Schuster, 1995]. Al acoplamiento unidireccional se le conoce también como configuración **maestro y esclavo** [Pecora y Carroll, 1990]. En este tipo de configu-

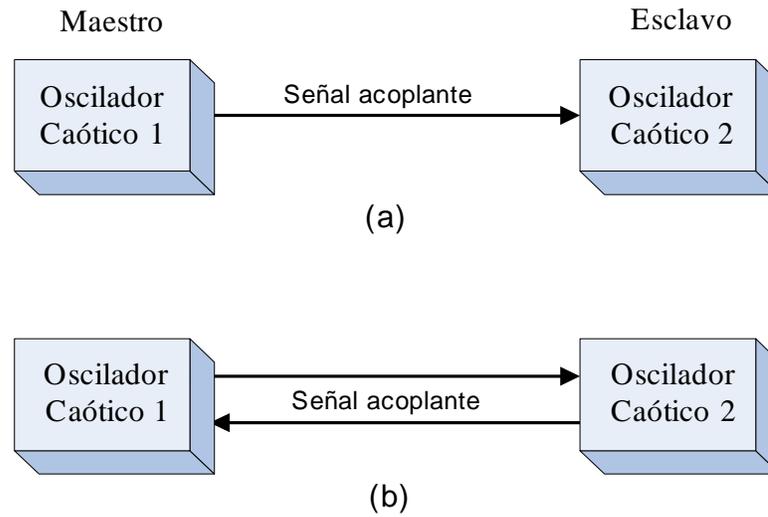


Figura 9: Escenarios de acoplamiento: (a) Configuración unidireccional (Maestro y Esclavo), (b) Configuración bidireccional (mutuo).

ración el sistema maestro controla al sistema esclavo por medio de una señal acoplante, con el propósito de obligarlo a adoptar sus dinámicas (incluyendo el comportamiento caótico). En general, el sistema esclavo se construye de forma muy semejante en estructura al sistema maestro, con la diferencia de que éste tiene una entrada adicional, la cual, proviene del sistema maestro. La señal caótica que se transmite del maestro al esclavo, tiene el efecto de forzar a este sistema a copiar su comportamiento. En la figura 9 se muestran los dos tipos de escenarios de acoplamiento.

A continuación se presentan de manera formal algunos conceptos relacionados con la sincronización de osciladores caóticos.

II.5.2 Sincronización completa

Considerando los escenarios de acoplamiento de sistemas ilustrados en la figura 9. Se dice que los osciladores caóticos 1 y 2 de dimensión n , con vector de estados $x(k)$ y $\hat{x}(k)$, respectivamente; **sincronizan completamente** sí

$$\lim_{k \rightarrow \infty} \|x(k) - \hat{x}(k)\| \equiv 0, \quad (5)$$

para toda señal acoplante apropiada generada por los osciladores, e independientemente de las condiciones iniciales $x(0)$ y $\hat{x}(0)$. El vector de **error de sincronía** se define por la expresión

$$e(k) = x(k) - \hat{x}(k), \quad x, \hat{x} \in \mathbb{R}^n.$$

En la figura 10 se muestran para el primer estado del sistema caótico de los n estados, la gráfica de sincronía de dos osciladores no sincronizados (a) y sincronizados (b). Puede notarse que cuando existe sincronía exacta se forma una recta con pendiente de 45 grados. Esta situación ocurre para el resto de los $n - 1$ estados de los osciladores 1 y 2.

II.5.3 Sincronización aproximada

En una situación real, es necesario sincronizar osciladores (idénticos o no idénticos) ante perturbaciones más comunes o ruido. En esta situación, no se puede esperar que el error de sincronía tienda a cero, sino que en el mejor de los casos, permanezca

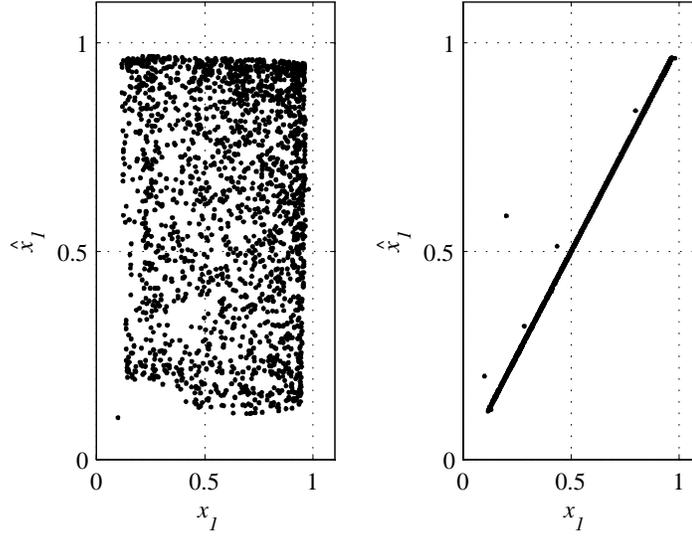


Figura 10: Plano x_1 vs \hat{x}_1 : (a) Osciladores no sincronizados, (b) Osciladores sincronizados.

uniformemente acotado por un valor positivo $\rho \in \mathbb{R}$.

Para esa situación, se recurre a una condición más relajada para establecer solo **sincronización aproximada** en el contexto ruidoso, perturbado en la señal acoplante, con diferencias en los valores de los parámetros, etc., como sigue,

$$\lim_{k \rightarrow \infty} \|x(k) - \hat{x}(k)\| \leq \rho, \quad (6)$$

independientemente de las condiciones iniciales $x(0)$ y $\hat{x}(0)$. Si para algún $\rho > 0$ dado, existe un instante de tiempo $\tau > 0$, llamado, τ **tiempo de sincronía aproximada** tal que la condición (6) se cumple, entonces el oscilador 1 y el oscilador 2 están aproximadamente sincronizados. Se define para los errores $e_i(k) = x_i(k) - \hat{x}_i(k)$, $i = 1, 2, \dots, n$ los

siguientes tiempos de sincronía para cada uno de los estados

$$\tau_i(\rho) = \min \tau \{ |e_i(k)| < \rho, \quad k = \tau, \tau + 1, \dots \},$$

y el **tiempo de sincronía aproximada** será entonces

$$\tau(\rho) = \max(\tau_i(\rho)), \quad i = 1, 2, \dots, n.$$

Observación: En la condición para sincronía aproximada, nótese que existe un compromiso entre las cantidades ρ y τ , dado que si ρ se incrementa, entonces τ decrece y viceversa.

II.5.4 Sincronización parcial

En este manuscrito, se aceptará como **sincronización completa**, cuando la condición (5) o bien (6) se cumple para todos los estados de los osciladores 1 y 2, $x_i(k)$, $\hat{x}_i(k)$ respectivamente, para toda $i = 1, 2, \dots, n$. Y se define como **sincronización parcial** a la situación particular, en la cual, la condición (5) o bien (6) se cumple sólo para una parte de los estados pero no para todos, es decir

$$x_i(k) = \hat{x}_i(k), \quad i = 1, 2, \dots, m, \quad m < n.$$

II.5.5 Sincronización y control de caos

Los trabajos de Ott, Grebogi y Yorke y de Pecora y Carroll publicados en 1990 abrieron amplio panorama a las aplicaciones del caos. Ambos documentos recibieron gran atención y establecieron dos áreas muy activas de investigación: el **control** y la **sincronización de sistemas caóticos**, respectivamente. La sincronización, muchas veces se relaciona con el control, puesto que el problema de sincronización, puede considerarse como un tipo particular del problema genérico de control, en el cual, el objetivo de control es seguir una trayectoria caótica deseada [Fradkov y Pogromsky, 1998]. O bien, de manera natural el problema de sincronización puede formularse como un problema de diseño de observadores no lineales de estado [Nijmeijer y Mareels, 1997].

Al controlar el caos, se pretende que el sistema adquiera un comportamiento regular o bien, un comportamiento más caótico. En otras palabras, dado un sistema no lineal, el problema consiste en eliminar el caos si lo hay (control de arritmias cardíacas. maquinas con vibración,etc.) o generar caos donde no exista (para tratar casos de epilepsia o trastornos mentales). En la *sincronización* se desea que un conjunto de sistemas, por medio de un acoplamiento apropiado adquieran el mismo comportamiento, este puede ser regular o complejo. Por otra parte, se sabe que el inicio de las técnicas para controlar el caos tienen su origen en la teoría de control y por otro lado, trabajos reportados sobre el problema de sincronización del caos le dan a éste un giro en dirección también de la teoría de control. Ésto finalmente une el estudio de control de caos y de sincronización de caos en un mismo marco, como es la **teoría de control no**

lineal. Reconociendo esta importancia, este trabajo de tesis toma de la teoría de control no lineal, la metodología de acoplamiento a modelos con el objetivo de sincronizar osciladores con dinámicas extremadamente complejas, es decir, caos e hipercaos.

En el siguiente capítulo se aplicará la técnica del filtro extendido de Kalman, herramienta muy conocida dentro de la teoría de control para sincronizar sistemas hipercaóticos Sobiski y Thorp, (1998) para el caso continuo y Cruz-Hernández y Nijmeijer, (1999; 2000) para el caso discreto.

Capítulo III

Sincronización de Sistemas

Hipercaóticos Utilizando Filtro

Extendido de Kalman

La teoría del *filtro de Kalman* es una de las herramientas matemáticas más poderosas con que se cuenta actualmente, debido al empleo de ideas estadísticas a problemas de filtrado, ayudando con esto, a resolver diversos problemas de filtrado de ruido en imágenes, seguimiento de trayectorias, estimación de parámetros, etc. De ahí, que se origine la idea de emplearlo para resolver el **problema de sincronización** considerando ruido en las dinámicas de los sistemas y en la señal acoplante entre los sistemas.

El empleo del filtro de Kalman y el filtro extendido de Kalman en la sincronización de sistemas caóticos, se presentó con éxito, tanto en el contexto continuo como en el

discreto en los trabajos Sobiski y Thorp, (1998); Cruz-Hernández y Nijmeijer, (1999; 2000); Lian *et al.*, (2000). Por otra parte, la sincronización de sistemas hipercaóticos se ha obtenido también mediante diversas técnicas, por ejemplo, utilizando observadores no lineales [Grassi y Mascolo, 1998], mediante control por retroalimentación [Brucoli *et al.*, 1998] donde se dan condiciones de robustez ante perturbaciones paramétricas y mediante división en subsistemas [Peng *et al.*, 1996] para el caso continuo.

En este capítulo se mostrará el empleo del **filtro extendido de Kalman** para la **sincronización de sistemas hipercaóticos discretos** considerando ruido en los sistemas a sincronizar, tanto en sus dinámicas como en la señal acoplante. El escenario de acoplamiento natural para el filtro extendido de Kalman, en el problema de sincronización, es la configuración maestro y esclavo, siendo por supuesto, considerado a él como sistema esclavo.

III.1 Filtro de Kalman

El **filtro de Kalman** es un estimador de los estados de un sistema lineal contaminado por ruido blanco gaussiano; el estimador que resulta es estadísticamente óptimo con respecto a cualquier función cuadrática del error estimado. Es decir, dado un modelo lineal estocástico, el objetivo del filtro de Kalman es producir una estimación $\hat{x}(k)$ del estado del modelo $x(k)$, utilizando mediciones ruidosas hasta el tiempo k para minimizar el error cuadrático medio entre la estimación y el estado real.

La dinámica del sistema lineal a estimar está modelada por

$$\begin{aligned}x(k+1) &= F(k)x(k) + w(k), \\y(k) &= H(k)x(k) + v(k),\end{aligned}$$

donde el estado $x(k)$ es un vector de dimensión n , la salida $y(k)$ es un vector de dimensión ℓ . Las señales de ruido $v(k)$ y $w(k)$ se suponen procesos independientes y secuencias gaussianas de media cero y $E[w(k)w(l)^T] = Q(k)\delta(k-l)$ y $E[v(k)v(l)^T] = R(k)\delta(k-l)$, respectivamente, donde $Q(k)$ es la matriz de covarianza del ruido en el proceso y $R(k)$ es la matriz de covarianza del ruido en la salida. Se supone además, que la condición inicial x_0 es de naturaleza gaussiana con media conocida \bar{x}_0 y covarianza conocida P_0 independientes de $v(k)$ y $w(k)$. El problema del filtro de Kalman consiste en obtener una estimación del estado $x(k)$ representado por $\hat{x}(k)$, tal que se minimice el error cuadrático medio.

En el proceso de estimación del filtro de Kalman se pueden observar dos etapas:

- **Etapas de predicción.** En esta etapa se pretende predecir el nuevo valor de la cantidad que se desea estimar. Para ello, la estimación del estado anterior $\hat{x}(k)$ y su matriz de covarianza $P(k)$ son extrapoladas para formar el vector de estado

predicho $\hat{x}(k+1/k)$ y su matriz de covarianza $P(k+1/k)$

$$\hat{x}(k+1/k) = F(k)\hat{x}(k),$$

$$P(k+1/k) = F(k)P(k)F(k)^T + Q(k).$$

- **Etapa de actualización.** En esta etapa se calcula el nuevo vector de estado $\hat{x}(k)$ y su matriz de covarianza $P(k)$. Para ello, se utiliza la covarianza predicha para calcular la ganancia de Kalman $K(k)$, escalando ésta por el valor del residuo de medición $y(k) - H(k)\hat{x}(k/k-1)$, es decir, por la estimación del error cometido en la predicción y sumándose al vector de estado predicho $\hat{x}(k/k-1)$ para calcular el nuevo vector de estado $\hat{x}(k)$

$$\hat{x}(k) = \hat{x}(k/k-1) + K(k)[y(k) - H(k)\hat{x}(k/k-1)],$$

$$P(k) = [I - K(k)H(k)]P(k/k-1),$$

donde

$$K(k) = P(k/k-1)H(k)^T [H(k)P(k/k-1)H(k)^T + R(k)]^{-1},$$

siendo

$$\hat{x}(k/k-1) = E[x(k) | y(k-1)].$$

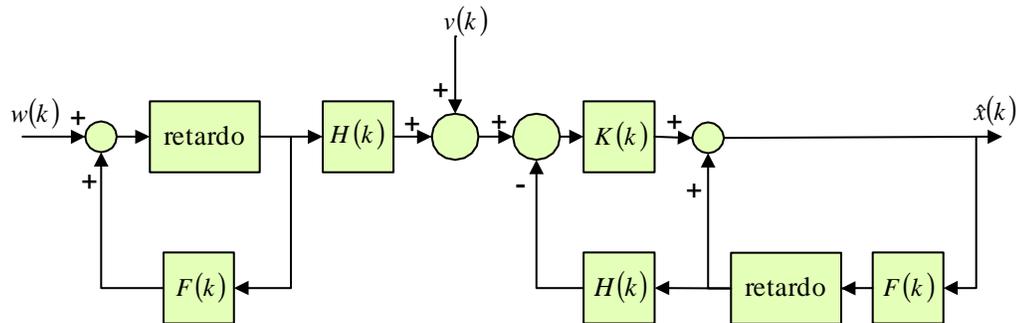


Figura 11: Diagrama de bloques que muestra el sistema a estimar, la salida medida y el filtro de Kalman discreto.

y

$$\hat{x}(k) = \hat{x}(k/k) = E[x(k) | y(k)]$$

La figura 11 muestra en bloques el modelo a estimar y el filtro de Kalman.

III.1.1 Filtro Extendido de Kalman

En numerosos problemas de tipo práctico, el modelo lineal no representa de forma adecuada la dinámica del fenómeno objeto de estudio, siendo preciso recurrir a modelos no lineales, lo que supone una mayor complejidad en el cálculo matemático asociado. Uno de los procedimientos más simples para el tratamiento de un sistema no lineal, consiste en intentar obtener un sistema lineal que se aproxime a él, manteniendo al menos las propiedades estocásticas básicas. Una de tales aproximaciones se denomina *filtro extendido de Kalman*. Esta aproximación no garantiza producir una *estimación óptima*. Este filtro consiste en linealizar el sistema no lineal empleando la mejor estimación de los estados como valores de referencia para usarlos en cada etapa de la

linealización. Es decir, el filtro extendido de Kalman consiste en utilizar las ecuaciones clásicas del filtro de Kalman para la aproximación de primer orden del sistema no lineal con respecto a la última estimación. El filtro resultante, obviamente ya no es ni lineal, ni óptimo, este filtro es pues considerado un *filtro subóptimo*. Sin embargo, su empleo ha proporcionado excelentes resultados en diversas aplicaciones. Ahora bien, en el problema de sincronización, algunas ventajas de utilizar un filtro extendido de Kalman como *sistema esclavo* para sincronizar con el sistema maestro, son que éste posee robustez natural ante ruido aditivo gaussiano, es fácil de implementar y es flexible; de ahí pues, el interés de aplicarlo a la sincronización de sistemas hipercaóticos, motivados también por los resultados obtenidos en Cruz-Hernández y Nijmeijer, (1999; 2000). A continuación se presentará el planteamiento del problema de sincronización empleando las ecuaciones del filtro extendido de Kalman para resolver dicho problema.

III.2 Sincronización de sistemas hipercaóticos discretos

Considere el siguiente sistema no lineal discreto como **sistema maestro**

$$x(k+1) = f(x(k)) + w(k), \quad x(0) = x_0, \quad (7)$$

con salida o señal acoplante

$$y(k) = h(x(k)) + v(k) \quad (8)$$

donde $x(k) \in \mathbb{R}^n$ es el estado maestro, $w(k)$ representa el ruido en la dinámica del sistema maestro, el cual, se asume que posee las características de tener media cero con $E[w(k)w(l)^T] = Q\delta(k-l) > 0$, siendo $\delta(k)$ la función delta de Kronecker, $v(k)$ es también una señal de ruido de media cero y $E[v(k)v(l)^T] = R\delta(k-l) > 0$; se asume además, que $w(k)$ y $v(k)$ son procesos gaussianos independientes.

La dinámica del **sistema esclavo** es precisamente el **filtro extendido de Kalman**, que producirá una estimación del estado maestro $x(k)$ a partir de las mediciones $y(k)$. Si el filtro logra estimar en "buena forma" al estado del sistema maestro, entonces se podrá considerar a los sistemas como sincronizados. Las ecuaciones del filtro extendido de Kalman utilizado como **sistema esclavo** se describen a continuación [Anderson y Moore, 1979]:

- Ecuaciones que *estiman* el estado maestro actual

$$\hat{x}(k) = \hat{x}(k/k-1) + K(k)[y(k) - h(\hat{x}(k/k-1))], \quad (9)$$

el vector $\hat{x}(k)$ es la estimación hecha por el filtro del estado $x(k)$. La covarianza

del error en $\hat{x}(k)$ está dada por

$$P(k) = [I - K(k)H(k)]P(k/k-1).$$

- Ecuaciones que *predicen* el estado maestro actual

$$\hat{x}(k+1/k) = f(\hat{x}(k)),$$

la matriz de covarianza del error de predicción es definida mediante

$$P(k+1/k) = F(k)P(k)F^T(k) + Q,$$

donde

$$K(k) = P(k/k-1)H^T(k)[H(k)P(k/k-1)H^T(k) + R]^{-1} \quad (10)$$

que se conoce como la matriz de *ganancias de Kalman* y

$$F(k) = \left. \frac{\partial f(x(k))}{\partial x(k)} \right|_{x(k)=\hat{x}(k)}, \quad H(k) = \left. \frac{\partial h(x(k))}{\partial x(k)} \right|_{x(k)=\hat{x}(k/k-1)}.$$

Observación: En la práctica puede en ocasiones ser imposible determinar las condiciones iniciales $x(0)$ exactamente. En este caso, $x(0)$ se asume como una variable aleatoria gaussiana de media conocida $E[x(0)] = \bar{x}(0)$ y covarianza conocida

$E \left\{ [x(0) - \bar{x}(0)] [x(0) - \bar{x}(0)]^T \right\} = P(0)$, además se considera independiente de las señales de ruido $w(k)$ y $v(k)$.

El filtro se inicializa en $\hat{x}(0) = \bar{x}_0$ y $P(0) = P_0 = P_0^T > 0$. De esta manera, $x(0)$ es dada y se selecciona arbitrariamente a \bar{x}_0 y $P(0) = P_0 = P_0^T > 0$.

Para el problema de sincronización de sistemas con ruido en las dinámicas y en la señal acoplante, considerando en esta situación al filtro extendido de Kalman como esclavo, éste alcanzará tan solo *sincronía aproximada*, es decir cumpliendo con la condición (6). Sin embargo, para este caso particular, la constante de error de sincronía ρ debe estar relacionada con Q y R .

Observación: Se puede también considerar como una adecuada condición para sincronización aproximada en el contexto ruidoso [Cruz-Hernández y Nijmeijer, 2000] a

$$\lim_{k \rightarrow \infty} \|E[x(k) - \hat{x}(k)]\| \leq \rho.$$

Con el fin de mostrar convergencia del error de sincronía, en la siguiente sección se hará uso de la metodología presentada en Reif *et al.*, (1999), para establecer condiciones de convergencia del filtro extendido de Kalman cuando se emplea como esclavo de un sistema discreto estocástico no lineal considerando un mapeo lineal de salida, es decir de la forma,

$$y(k) = Hx(k) + v(k). \quad (11)$$

III.2.1 Convergencia del error de estimación (sincronización)

Definiendo el error de estimación como

$$e(k) = x(k) - \hat{x}(k), \quad (12)$$

y el error entre el estado y la predicción de la estimación se define como

$$e(k/k-1) = x(k) - \hat{x}(k/k-1).$$

Suponiendo que f y h en (7) y (8), respectivamente son funciones C^1 , entonces éstas se pueden expandir de la siguiente manera

$$f(x) = f(\hat{x}) + F(k)[x(k) - \hat{x}(k)] + \varphi(x(k), \hat{x}(k)) \quad (13)$$

La dinámica del error entre el estado maestro y la predicción está gobernada por la ecuación

$$\begin{aligned} e(k+1/k) &= x(k+1) - \hat{x}(k+1/k) = f(x(k)) + w(k) - f(\hat{x}(k)), \\ &= F(k)e(k) + \varphi(x(k), \hat{x}(k)) + w(k) \end{aligned}$$

y la dinámica del error está dada por

$$\begin{aligned}
e(k+1) &= x(k+1) - \hat{x}(k+1) \\
&= f(x(k)) + w(k) - f(\hat{x}(k)) - K(k+1)[y(k+1) - H\hat{x}(k+1/k)] \\
&= [I - K(k+1)H]F(k)e(k) + [I - K(k+1)H]\varphi(x(k), \hat{x}(k)) \\
&\quad + [I - K(k+1)H]w(k) - K(k+1)v(k+1) \\
e(k+1) &= [I - K(k+1)H]F(k)e(k) + r(k) + s(k) \tag{14}
\end{aligned}$$

con

$$\begin{aligned}
r(k) &= [I - K(k+1)H]\varphi(x(k), \hat{x}(k)), \\
s(k) &= [I - K(k+1)H]w(k) - K(k+1)v(k+1).
\end{aligned}$$

Antes de continuar analizando la estabilidad de la ecuación (14), se enlistan una serie de hipótesis que serán de utilidad para dicho análisis.

(H1). *Existen números reales positivos \bar{f} , \bar{h} , p_1 , p_2 tales que las siguientes cotas se*

verifican para toda $k \geq 0$:

$$\|F(k)\| \leq \bar{f}, \quad (15)$$

$$\|H(k)\| \leq \bar{h}, \quad (16)$$

$$p_1 I \leq P(k) \leq p_2 I, \quad (17)$$

$$qI \leq Q, \quad (18)$$

$$rI \leq R. \quad (19)$$

(H2). $f \in C^2$ y $F(k)$ es no singular para toda $k \geq 0$.

(H3). Existen números reales positivos ϵ y κ tales que la función

$\varphi(x(k), \hat{x}(k))$ en (13) está acotada por

$$\|\varphi(x(k), \hat{x}(k))\| \leq \kappa \|x(k) - \hat{x}(k)\|^2,$$

para $x(k), \hat{x}(k) \in \mathbb{R}^n$ con $\|x(k) - \hat{x}(k)\| \leq \epsilon$.

Nota: La desigualdad (17) está muy ligada a la propiedad de observabilidad del sistema linealizado por lo que en el apéndice A se mencionan brevemente algunos conceptos relacionados.

Primero se presentarán los siguientes lemas necesarios

Lema 1 *Bajo las condiciones de acotamiento (15)-(19) existe un número real*

$0 < \alpha < 1$ tal que $P^{-1}(k)$ satisface la desigualdad

$$F^T(k) [I - K(k+1)H]^T P^{-1}(k+1) [I - K(k+1)H] F(k) \leq (1 - \alpha) P^{-1}(k) \quad (20)$$

para toda $k \geq 0$.

Prueba El término $P(k+1) = [I - K(k+1)H] [F(k)P(k)F^T(k) + Q]$ se puede reescribir de la siguiente manera,

$$\begin{aligned} P(k+1) &= [I - K(k+1)H] F(k) P(k) F^T(k) [I - K(k+1)H]^T \quad (21) \\ &+ [I - K(k+1)H] Q [I - K(k+1)H]^T \\ &+ [I - K(k+1)H] [Q + F(k)P(k)F^T(k)] H^T K^T(k+1), \end{aligned}$$

donde

$$[I - K(k+1)H] [Q + F(k)P(k)F^T(k)]$$

es una matriz simétrica. Utilizando el lema de la inversión de una matriz se tiene que

$$\begin{aligned} [I - K(k+1)H] [Q + F(k)P(k)F^T(k)] &= \\ [(Q + F(k)P(k)F^T(k))^{-1} + H^T R^{-1}H]^{-1} &> 0, \quad (22) \end{aligned}$$

con base (22) se obtiene que

$$[I - K(k+1)H] [Q + F(k)P(k)F^T(k)] H^T K^T(k+1) \geq 0, \quad (23)$$

utilizando la condición (23) y eliminando ese término de (21), la siguiente desigualdad se cumple

$$P(k+1) \geq [I - K(k+1)H]F(k)P(k)F^T(k)[I - K(k+1)H]^T \\ + [I - K(k+1)H]Q[I - K(k+1)H]^T,$$

lo anterior se puede reescribir de la siguiente manera,

$$P(k+1) \geq [I - K(k+1)H]F(k)[P(k) + F^{-1}(k)QF^{-T}(k)]F^T(k)[I - K(k+1)H]^T,$$

utilizando las condiciones (15), (17) y (18) se llega a lo siguiente

$$P(k+1) \geq [I - K(k+1)H]F(k) \left(I + \frac{qI}{\bar{f}^2 p_2} \right) P(k)F^T(k)[I - K(k+1)H]^T, \quad (24)$$

tomando la inversa en ambos lados de (24) y multiplicando por $F^T(k)[I - K(k+1)H]^T$ y $[I - K(k+1)H]F(k)$ se tiene,

$$F^T(k)[I - K(k+1)H]^T P^{-1}(k+1)[I - K(k+1)H]F(k) \leq \left(1 + \frac{q}{p_2 \bar{f}^2} \right)^{-1} P^{-1}(k)$$

con $(1 - \alpha) = \left(1 + \frac{q}{p_2 \bar{f}^2} \right)^{-1}$. Demostrándose que la desigualdad (20) se cumple. ■

Lema 2 Dado que las condiciones (15)-(19) se cumplen. Entonces existen núme-

ros reales positivos ϵ y k_{nom} , tales que

$$r^T(k) P^{-1}(k) \{2[I - K(k+1)H]F(k)e(k) + r(k)\} \leq k_{nom} \|e(k)\|^3 \quad (25)$$

se cumple para todo $\|e(k)\| \leq \epsilon$.

Prueba Siendo $r(k) = [I - K(k+1)H]\varphi(x(k), \hat{x}(k))$, por las condiciones dadas se tiene que

$$\|\varphi(x(k), \hat{x}(k))\| \leq \kappa \|e(k)\|^2$$

además, considerando que $Q \leq \delta_1 I$ se tiene lo siguiente

$$\begin{aligned} \|K(k+1)\| &\leq \left\| [F(k)P(k)F^T(k) + Q] H^T [H[F(k)P(k)F^T(k) + Q]H^T + R]^{-1} \right\| \\ &\leq \left\| [F(k)P(k)F^T(k) + Q] \right\| \|H^T\| \left\| [H[F(k)P(k)F^T(k) + Q]H^T + R]^{-1} \right\| \\ &\leq (\bar{f}^2 p_2 + \delta_1) \frac{\bar{h}}{r} \end{aligned}$$

el término $\|K(k+1)\|$ se puede expresar como $\|K(k+1)\| \leq \rho_1 + \rho_2 \delta_1$ con $\rho_1 = \frac{\bar{f}^2 p_2 \bar{h}}{r}$

y $\rho_2 = \frac{\bar{h}}{r}$. Por tanto, se llega a

$$\begin{aligned} \|r(k)\| &\leq \|I - K(k+1)H\| \|\varphi(x, \hat{x})\| \\ &\leq [\|I\| + \|K(k+1)H\|] \kappa \|e(k)\|^2 \\ &\leq [1 + \|K(k+1)\| \|H\|] \kappa \|e(k)\|^2 \\ &\leq (1 + \rho_1 \bar{h} + \rho_2 \bar{h} \delta_1) \kappa \|e(k)\|^2 \end{aligned} \quad (26)$$

utilizando la expresión (26) se tiene entonces que

$$\begin{aligned}
& r^T(k) P^{-1}(k) \{2[I - K(k+1)H]F(k)e(k) + r(k)\} \\
\leq & \left\| r^T(k) P^{-1}(k) \{2[I - K(k+1)H]F(k)e(k) + r(k)\} \right\| \\
\leq & \left\| r^T(k) \right\| \left\| P^{-1}(k) \right\| \left\| \{2[I - K(k+1)H]F(k)e(k) + r(k)\} \right\| \\
\leq & (1 + \rho_1 \bar{h} + \rho_2 \bar{h} \delta_1) \kappa \|e(k)\|^2 \left(\frac{1}{p_1} \right) \\
& \times [2(1 + \rho_1 \bar{h} + \rho_2 \bar{h} \delta_1) \bar{f} \|e(k)\| + (1 + \rho_1 \bar{h} + \rho_2 \bar{h} \delta_1) \kappa \|e(k)\|^2] \\
\leq & (1 + \rho_1 \bar{h} + \rho_2 \bar{h} \delta_1)^2 \kappa \left(\frac{1}{p_1} \right) (2\bar{f} + \kappa \epsilon) \|e(k)\|^3 \\
\leq & k_{nom} \|e(k)\|^3
\end{aligned}$$

con

$$k_{nom} = (1 + \rho_1 \bar{h} + \rho_2 \bar{h} \delta)^2 \kappa \left(\frac{1}{p_1} \right) (2\bar{f} + \kappa \epsilon) \quad \text{y} \quad \delta = \delta_1.$$

por lo que la desigualdad (25) se cumple. ■

Lema 3 Bajo las condiciones (15)-(19). Existen números reales positivos ρ_3, ρ_4, ρ_5 independientes de δ , tales que

$$E [s^T(k) P^{-1}(k+1) s(k)] \leq \rho_3 \delta^3 + \rho_4 \delta^2 + \rho_5 \delta$$

se cumple para alguna $\delta > 0$.

Prueba

$$\begin{aligned}
s^T(k) P^{-1}(k+1) s(k) &= w^T(k) [I - K(k+1) H]^T P^{-1}(k+1) [I - K(k+1) H] w(k) \\
&\quad - w^T(k) [I - K(k+1) H] P^{-1}(k+1) K(k+1) v(k) \\
&\quad - v^T(k) K^T(k+1) P^{-1}(k+1) [I - K(k+1) H] w(k) \\
&\quad + v^T(k) K^T(k+1) P^{-1}(k+1) K(k+1) v(k), \tag{27}
\end{aligned}$$

como $w(k)$ y $v(k)$ son señales no correlacionadas, la expresión (27) queda como sigue,

$$\begin{aligned}
s^T(k) P^{-1}(k+1) s(k) &= w^T(k) [I - K(k+1) H]^T P^{-1}(k+1) [I - K(k+1) H] w(k) \\
&\quad + v^T(k) K^T(k+1) P^{-1}(k+1) K(k+1) v(k).
\end{aligned}$$

Del lema anterior se obtuvo que $\|K(k+1)\| \leq \rho_1 + \rho_2 \delta_1$ con $\rho_1 = \frac{\bar{f}^2 p_2 \bar{h}}{r}$ y $\rho_2 = \frac{\bar{h}}{r}$ y,

considerando nuevamente que $Q \leq \delta_1 I$ y $R \leq \delta_2 I$, se tiene

$$\begin{aligned}
s^T(k) P^{-1}(k+1) s(k) &\leq (1 + \rho_1 \bar{h} + \rho_2 \bar{h} \delta_1)^2 \frac{1}{p_1} w^T(k) w(k) \\
&\quad + (\rho_1 + \rho_2 \delta_1)^2 \frac{1}{p_1} v^T(k) v(k) \\
&\leq (1 + \rho_1 \bar{h} + \rho_2 \bar{h} \delta_1)^2 \frac{1}{p_1} \delta_2 + (\rho_1 + \rho_2 \delta_1)^2 \frac{1}{p_1} \delta_1 \tag{28}
\end{aligned}$$

considerando $\delta_1 = \delta_2 = \delta$ se puede reescribir lo anterior como sigue,

$$s^T(k) P^{-1}(k+1) s(k) \leq \rho_3 \delta^3 + \rho_4 \delta^2 + \rho_5 \delta$$

con

$$\rho_3 = \frac{\rho_2^2 (1 + \bar{h}^2)}{p_1}, \quad \rho_4 = \frac{2\rho_2 (\bar{h} + \rho_1 \bar{h}^2 + \rho_1)}{p_1}, \quad \rho_5 = \frac{1 + 2\rho_1 \bar{h} + \rho_1^2 \bar{h}^2 + \rho_1^2}{p_1}.$$

■

Lema 4 (Reif et al., 1999). Suponga que $V(e(k))$ es un proceso estocástico y que existen números reales $v_1, v_2, \mu > 0$ y $0 < \alpha' \leq 1$ tales que:

$$v_1 \|e(k)\|^2 \leq V(e(k)) \leq v_2 \|e(k)\|^2$$

y

$$E[V(e(k+1)) | e(k)] - V(e(k)) \leq \mu - \alpha' V(e(k))$$

se cumplen para toda solución de (14). Entonces el proceso estocástico es exponencialmente acotado de la siguiente manera

$$E[\|e(k)\|^2] \leq \frac{v_2}{v_1} E[\|e(0)\|^2] (1 - \alpha)^k + \frac{\mu}{v_1 \alpha'}. \quad (29)$$

Prueba Para la demostración de este lema puede consultarse Reif *et al.*, (1999). ■

Con los resultados expuestos anteriormente, se llega al siguiente teorema.

Teorema. Considere un sistema estocástico no lineal descrito por (7) y (11) junto con un filtro extendido de Kalman (9) y (10). Supongase que las hipótesis (H1)-(H3)

se cumplen. Entonces, los sistemas (7) y (9) sincronizan aproximadamente si el error estimado inicial satisface

$$\|e(0)\| = \|x(0) - \hat{x}(0)\| \leq \varepsilon,$$

y las matrices de covarianzas para las señales de ruido en (7) y (11) están acotadas por

$$Q \leq \delta_1 I$$

$$R \leq \delta_2 I$$

para algún $\delta_1, \delta_2, \varepsilon > 0$.

Prueba Considere la siguiente función candidata de Lyapunov

$$V(e(k)) = e^T(k) P^{-1}(k) e(k), \quad (30)$$

debido a que $P(k)$ es definida positiva entonces $P^{-1}(k)$ también lo es y por tanto $V(e(k))$ es definida positiva, comprobándose que (30) es función candidata de Lyapunov. Conforme (17) se puede obtener que

$$\frac{\|e(k)\|^2}{p_2} \leq V(e(k)) \leq \frac{\|e(k)\|^2}{p_1},$$

iterando (30) se tiene

$$\begin{aligned}
V(e(k+1)) &= e(k+1)^T P^{-1}(k+1) e(k+1) \\
&= e(k)^T F^T(k) [I - K(k+1)H]^T P^{-1}(k+1) [I - K(k+1)H] F(k) e(k) \\
&\quad + r^T(k) P^{-1}(k+1) \{2[I - K(k+1)H]F(k) e(k) + r(k)\} \\
&\quad + 2s^T(k) P^{-1}(k+1) \{[I - K(k+1)H]F(k) e(k) + r(k)\} \\
&\quad + s^T(k) P^{-1}(k+1) s(k).
\end{aligned}$$

aplicando el lema 1 se llega a

$$\begin{aligned}
V(e(k+1)) &\leq (1 - \alpha) V(e(k)) \\
&\quad + r^T(k) P^{-1}(k+1) \{2[I - K(k+1)H]F(k) e(k) + r(k)\} \\
&\quad + 2s^T(k) P^{-1}(k+1) \{[I - K(k+1)H]F(k) e(k) + r(k)\} \\
&\quad + s^T(k) P^{-1}(k+1) s(k).
\end{aligned}$$

Tomando la esperanza $E[V(e(k+1)) | e(k)]$ y considerando las propiedades del ruido blanco gaussiano, se puede ver que el término

$$E[2s^T(k) P^{-1}(k+1) [[I - K(k+1)H]F(k) e(k) + r(k)] | e(k)]$$

se desvanece [Reif *et al.*, 1999]. Quedando entonces que

$$E[V(e(k+1))|e(k)] \leq (1-\alpha)V(e(k)) + s^T(k)P^{-1}(k+1)s(k) \\ + r^T(k)P^{-1}(k+1)\{2[I-K(k+1)H]F(k)e(k) + r(k)\}.$$

Invocando los lemas 2 y 3 se llega a

$$E[V(e(k+1))|e(k)] \leq V(e(k)) - \alpha V(e(k)) + \rho_3\delta^3 + \rho_4\delta^2 + \rho_5\delta \quad (31) \\ + k_{nom} \|e(k)\|^3,$$

reacomodando términos

$$E[V(e(k+1))|e(k)] - V(e(k)) \leq -\frac{\alpha}{p_2} \|e(k)\|^2 + \rho_3\delta^3 + \rho_4\delta^2 + \rho_5\delta \quad (32) \\ + k_{nom} \|e(k)\|^3.$$

La desigualdad (32) será semidefinida negativa si se cumple que:

i)

$$k_{nom} \|e(k)\| \leq \frac{\alpha}{2p_2}, \quad (33)$$

ii)

$$\rho_3\delta^3 + \rho_4\delta^2 + \rho_5\delta \leq \frac{\alpha}{2p_2} \|e(k)\|^2. \quad (34)$$

la expresión (34) se puede sustituir por

$$(1 + \rho_1 \bar{h} + \rho_2 \bar{h} \delta_1)^2 \frac{1}{p_1} \delta_2 + (\rho_1 + \rho_2 \delta_1)^2 \frac{1}{p_1} \delta_1 \leq \frac{\alpha}{2p_2} \|e(k)\|^2,$$

en caso de no considerar $\delta_1 = \delta_2 = \delta$.

Definiendo $\varepsilon = \min\left(\varepsilon, \frac{\alpha}{2p_2 k_{nom}}\right)$ y utilizándolo en (32), la siguiente desigualdad se cumple

$$E[V(e(k+1)) | e(k)] - V(e(k)) \leq -\frac{\alpha}{2} V(e(k)) + \rho_3 \delta^3 + \rho_4 \delta^2 + \rho_5 \delta$$

para todo $\|e(k)\| \leq \varepsilon$. Y recurriendo al lema 4 con $\|e(0)\| \leq \varepsilon$, $v_1 = \frac{1}{p_2}$, $v_2 = \frac{1}{p_1}$, $\alpha' = \frac{\alpha}{2}$ y $\mu = \rho_3 \delta^3 + \rho_4 \delta^2 + \rho_5 \delta$ se puede cuantificar el error $e(k)$.

Con las desigualdades (33) y (34) se pueden obtener los valores de δ_1 y δ_2 tal que se cumplan dichas desigualdades y con la desigualdad (29) dado un valor ε se puede obtener una cota para el error inicial tal que la convergencia del error se cumpla. ■

Lo anterior muestra que la estabilidad del error depende de la naturaleza de las no linealidades y del tamaño del ruido en el proceso, así como del acotamiento del error inicial. Por tanto, estos resultados pueden emplearse para diseñar filtros no lineales estables.

A continuación se presentan dos ejemplos que ilustran los resultados anteriores.

III.3 Ejemplos

III.3.1 Ejemplo 1. Sistema caótico de segundo orden.

Considere el siguiente sistema discreto

$$\begin{aligned}x_1(k+1) &= x_2(k) + ax_1(k), \\x_2(k+1) &= x_1(k)^2 + b,\end{aligned}\tag{35}$$

se sabe que el sistema (35) para ciertos valores de parámetros exhibe dinámica caótica [Itoh *et al.*, 2001]. En las simulaciones numéricas realizadas se consideraron los valores paramétricos: $a = -0.1$ y $b = -1.7$. La figura 12 muestra el atractor caótico del sistema (35) en el espacio de estados.

Siguiendo el material presentado en la sección anterior, a continuación se muestra la sincronización de dos sistemas caóticos (35), utilizando un filtro extendido de Kalman como sistema esclavo, el cual, tratará de adquirir la dinámica del *sistema maestro* corrompido por ruido, descrito por las ecuaciones

$$\begin{aligned}x_1(k+1) &= x_2(k) + ax_1(k) + w_1(k), \\x_2(k+1) &= x_1(k)^2 + b + w_2(k),\end{aligned}\tag{36}$$

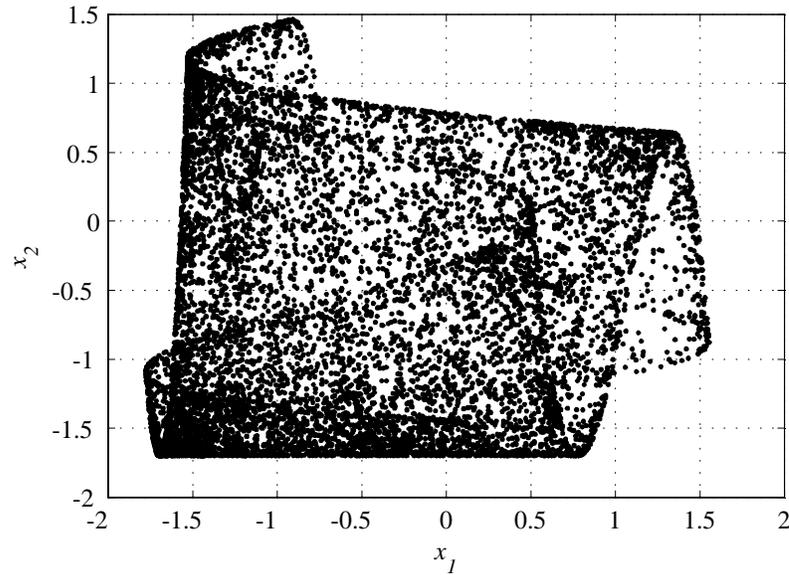


Figura 12: Atractor caótico del sistema (35).

con salida corrompida por ruido, de la forma

$$y(k) = x_1(k) + v(k).$$

Con dicha salida el sistema cumple la condición de observabilidad. El filtro extendido de Kalman generará un estado estimado $\hat{x}_i(k)$, $i = 1, 2$ para cada una de las señales maestras $x_i(k)$. Las ecuaciones dinámicas del *filtro extendido de Kalman* para el *sistema esclavo*, se describen a continuación

$$\hat{x}_1(k) = \hat{x}_1(k/k-1) + K_1(k) [y(k) - \hat{x}_1(k/k-1)], \quad (37)$$

$$\hat{x}_2(k) = \hat{x}_2(k/k-1) + K_2(k) [y(k) - \hat{x}_1(k/k-1)],$$

donde el vector de ganancias $(K_1(k), K_2(k))^T$ está dado por (10).

Para el sistema (36) con los parámetros mencionados, se obtienen los siguientes valores: $\bar{h} = 1$, $\bar{f} = 4$, $p_1 = 4.52 \times 10^{-6}$, $p_2 = 5.52 \times 10^{-6}$, $\kappa = 2$. Por simulación se tiene $\delta_1 = 0.0005$ con el propósito de que el sistema conserve la dinámica caótica. Se proponen además, los siguientes valores para q y r , $q = r = \frac{\delta_1}{100}$. Con los datos anteriores y utilizando las ecuaciones (33) y (34) se obtienen los siguientes valores $\delta_2 = 0.0001$ y $\|e(0)\| \leq 0.22$ que satisfacen dichas condiciones. A continuación se muestran resultados de simulaciones.

En las simulaciones se consideró a $x(0) = (0.1, 0.1)$, $P_0 = \text{diag}\{p_0\}$, $p_0 = 5 \times 10^{-6}$. Las figuras 13 y 14 muestran la evolución temporal de los errores de sincronía entre los estados $x(k)$ y $\hat{x}(k)$ para $\hat{x}(0) = (0.13, 0.13)$ y $\hat{x}(0) = (0.31, 0.31)$, respectivamente, para una realización del ruido. En este ejemplo, $e_i(k) = x_i(k) - \hat{x}_i(k)$, $i = 1, 2$ y se ha considerado un $\rho = 0.06$, obteniéndose $\tau = 7$.

Para evaluar el desempeño del filtro extendido de Kalman desde un punto de vista de la sensibilidad al error inicial y al ruido, se generaron 20 corridas de Monte Carlo con el fin de obtener estadísticas sobre el error cuadrático medio. Los resultados se resumen en la tabla I, donde SSE_i es la suma de los errores al cuadrado de cada corrida dado un cierto ruido

$$SSE_i = \sum_{k=0}^N (x_i(k) - \hat{x}_i(k))^2, \quad i = 1, 2, \dots, n$$

donde $x_i(k)$ y $\hat{x}_i(k)$ son el valor real y estimado, respectivamente, N es el número de iteraciones realizadas. Con lo anterior, la media del error al cuadrado (MSE_i) está

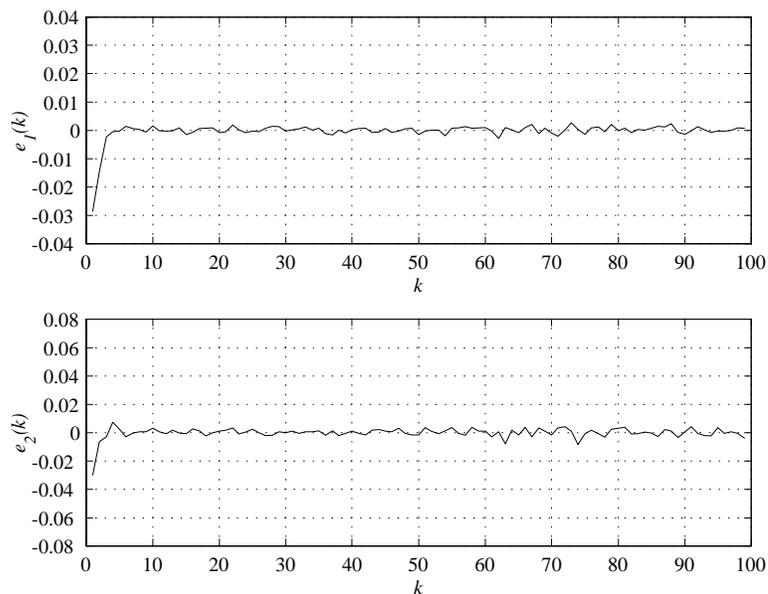


Figura 13: Evolución temporal de los errores de sincronía $e_1(k)$ y $e_2(k)$, $\tau = 0$ para $\rho = 0.06$.

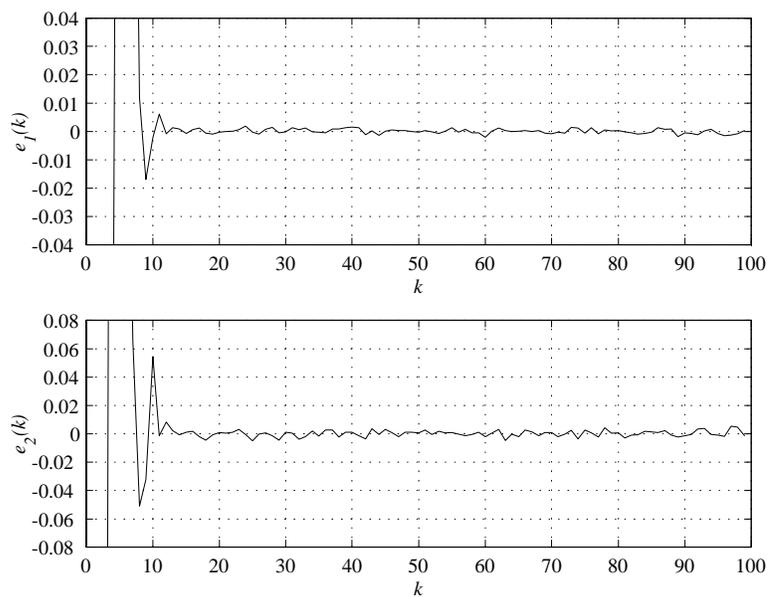


Figura 14: Evolución temporal de los errores de sincronía $e_1(k)$ y $e_2(k)$, $\tau = 7$ para $\rho = 0.06$.

dada por $\frac{1}{N+1} (SSE_i)$. Por tanto, la suma de Monte Carlo de los errores al cuadrado $(SSE_i)_{MC}$ está dada por

$$(SSE_i)_{MC} = \frac{1}{20} \sum_{j=1}^{20} (SSE_i)_j, \quad i = 1, 2, \dots, n. \quad (38)$$

Con el propósito de conocer las mismas estadísticas una vez transcurrido el transitorio, se define el error cuadrático medio truncado $(TMSE_i)$ como

$$TMSE_i = \frac{1}{N+1-\tau} \sum_{k=\tau}^N (x_i(k) - \hat{x}_i(k))^2, \quad i = 1, 2, \dots, n$$

por lo que el error cuadrático medio truncado de Monte Carlo será

$$(TMSE_i)_{MC} = \frac{1}{20} \sum_{j=1}^{20} (TMSE_i)_j, \quad i = 1, 2, \dots, n \quad (39)$$

y el tiempo de sincronía de Monte Carlo τ_{MC} es

$$\tau_{MC} = \frac{1}{20} \sum_{j=1}^{20} \max(\tau_i(\rho))_j, \quad i = 1, 2, \dots, n$$

donde $\max(\tau_i(\rho))$ se definió en el capítulo anterior. Los resultados se resumen en la tabla I para $Q = R = 0.00005$.

Tabla I: Error cuadrático medio de Monte Carlo $(SSE_i)_{MC}$, error cuadrático medio truncado $(TMSE_i)_{MC}$ de Monte Carlo y tiempo de sincronía (39) para el ejemplo 1 con $P_0 = 5 \times 10^{-6}$.

$e(0)$	$(SSE_1)_{MC}$	$(SSE_2)_{MC}$	$(TMSE_1)_{MC}$	$(TMSE_2)_{MC}$	τ_{MC}
(0.2, 0.2)	0.0043	0.0595	0.0035	0.0203	2
(0.05, 0.05)	0.0065	0.0235	0.0064	0.0228	0
(0.01, 0.01)	0.0040	0.0219	0.0042	0.0210	1
(-0.01, -0.01)	0.0038	0.0204	0.0042	0.0213	0
(-0.05, -0.05)	0.0065	0.0243	0.0064	0.0262	0
(-0.1, -0.1)	0.0141	0.0319	0.0055	0.0216	2
(-0.2, -0.2)	0.0450	0.0721	0.0042	0.0229	4
(-0.5, -0.5)	0.2676	0.4756	0.0040	0.0214	6
(-1, -1)	1.1183	3.09	0.0052	0.0230	7
(-5, -5)	30.37	544.12	0.0038	0.0194	10

De la tabla I se observa cómo el filtro extendido de Kalman logra de manera satisfactoria la sincronía aproximada, cumpliendo con las condiciones de $e(0) < \varepsilon$ y R y Q menores a un δ_1 y δ_2 , respectivamente. En los tres últimos ejemplos de la tabla I se toman valores de $e(0) > \varepsilon$ y aún así se observa que con el filtro extendido de Kalman se sigue obteniendo sincronía aproximada, lo que habla de que las cotas obtenidas son conservadoras.

III.3.2 Ejemplo 2: Sincronización del sistema discreto hipercaótico de Rössler

Considere el siguiente sistema discreto de Rössler

$$x_1(k+1) = \alpha x_1(k)(1-x_1(k)) - \beta(x_3(k) + \gamma)(1-2x_2(k)), \quad (40)$$

$$x_2(k+1) = \delta x_2(k)(1-x_2(k)) + \zeta x_3(k),$$

$$x_3(k+1) = \eta((x_3(k) + \gamma)(1-2x_2(k)) - 1)(1 - \theta x_1(k)),$$

se sabe que el sistema (40) para ciertos valores de parámetros exhibe dinámica hipercaótica [Itoh *et al.*, 2001]. En las simulaciones realizadas se consideraron los siguientes valores de parámetros: $\alpha = 3.8$, $\beta = 0.05$, $\gamma = 0.35$, $\delta = 3.78$, $\zeta = 0.2$, $\eta = 0.1$, $\theta = 1.9$. En la figura 15 se muestra la evolución temporal de los estados del sistema hipercaótico de Rössler, mientras que en la figura 16 se muestran los planos de fase del sistema hipercaótico (40). Se sincronizarán dos sistemas hipercaóticos de Rössler utilizando un filtro extendido de Kalman como sistema esclavo, el cual, tratará de estimar la dinámica del *sistema maestro* corrompido por ruido, definido por las ecuaciones

$$x_1(k+1) = \alpha x_1(k)(1-x_1(k)) - \beta(x_3(k) + \gamma)(1-2x_2(k)) + w_1(k), \quad (41)$$

$$x_2(k+1) = \delta x_2(k)(1-x_2(k)) + \zeta x_3(k) + w_2(k),$$

$$x_3(k+1) = \eta((x_3(k) + \gamma)(1-2x_2(k)) - 1)(1 - \theta x_1(k)) + w_3(k),$$

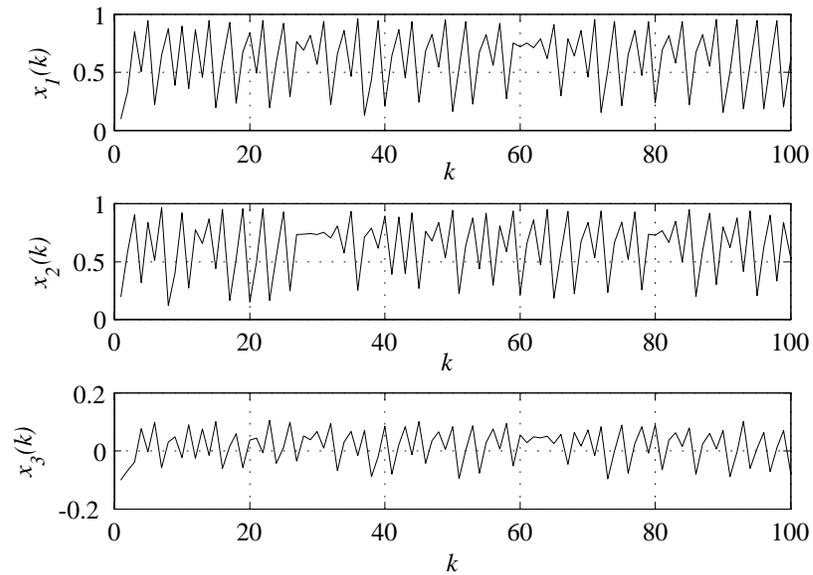


Figura 15: Estados $x_1(k)$, $x_2(k)$ y $x_3(k)$ del sistema hipercaótico de Rössler.

con salida ruidosa, de la forma

$$y(k) = x_1(k) + v(k).$$

El filtro extendido de Kalman generará un estado estimado $\hat{x}_i(k)$, $i = 1, 2, 3$ para cada una de las señales maestras $x_i(k)$. Las ecuaciones del filtro extendido de Kalman

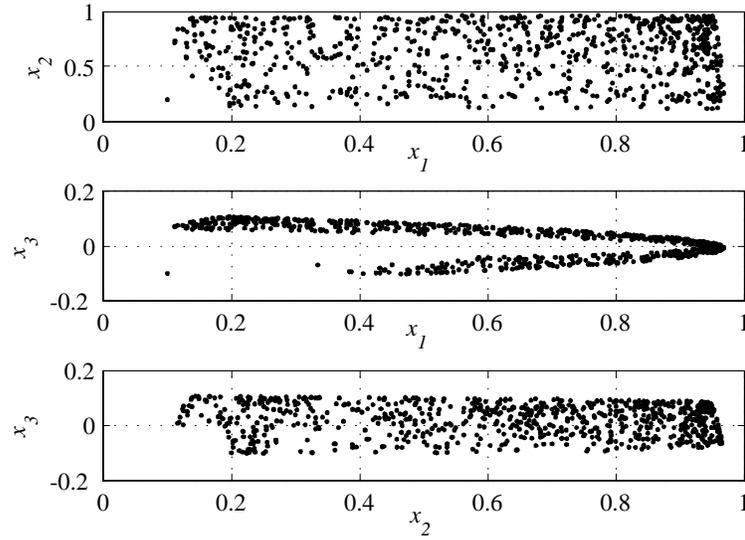


Figura 16: Atractores del sistema discreto hipercaótico de Rössler.

que representa al *sistema esclavo* se describen a continuación

$$\begin{aligned}
 \hat{x}_1(k) &= \hat{x}_1(k/k - 1) + K_1(k) [y(k) - \hat{x}_1(k/k - 1)], \\
 \hat{x}_2(k) &= \hat{x}_2(k/k - 1) + K_2(k) [y(k) - \hat{x}_1(k/k - 1)], \\
 \hat{x}_3(k) &= \hat{x}_3(k/k - 1) + K_3(k) [y(k) - \hat{x}_1(k/k - 1)],
 \end{aligned} \tag{42}$$

el vector de ganancias $(K_1(k), K_2(k), K_3(k))^T$ está dado por (10).

Para el sistema (41) con los parámetros anteriormente mencionados se tienen los siguientes datos: $\bar{h} = 1$, $\bar{f} = 3.84$, $p_1 = 5.5 \times 10^{-3}$, $p_2 = 248$, $\kappa = 7.6$. Por simulación se tiene $\delta_1 = 0.00005$ para que el sistema conserve la condición de dinámica hipercaótica. Proponiendo los siguientes valores para q y r , $q = r = \frac{\delta_1}{1000}$ y utilizando las ecuaciones

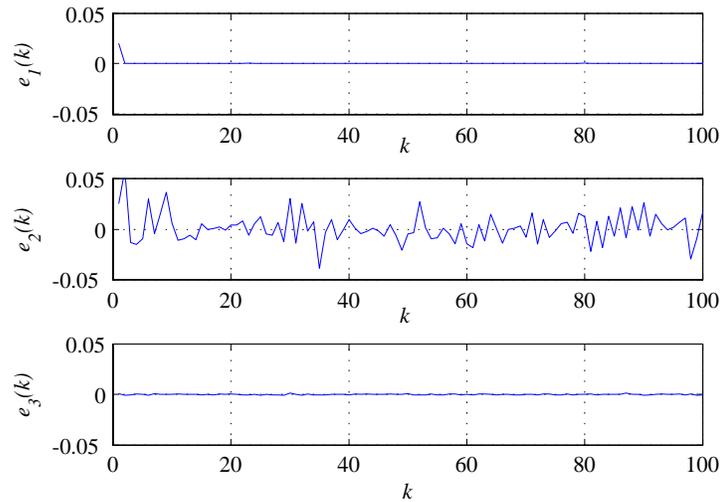


Figura 17: Evolución temporal de los errores en la estimación de los estados del sistema de Rössler.

(33) y (34), se obtienen los siguientes valores $\delta_2 = 1 \times 10^{-7}$ y $\|e(0)\| \leq 0.03$ que satisfacen dichas condiciones.

A continuación se muestran resultados de simulaciones realizadas.

En las simulaciones se consideró $x(0) = (0.95, 0.9, 0)$, $P_0 = \text{diag}\{p_{0i}\}$, $p_{0i} = 500$, $i = 1, 2, 3$. En la figura 17 se observa la evolución temporal de los errores $e_i(k) = x_i(k) - \hat{x}_i(k)$, $i = 1, 2, 3$ en la estimación de los estados del sistema de Rössler proporcionados por el filtro extendido de Kalman. De la propia figura puede verse que se alcanza sincronía aproximada en $\tau = 3$ s, para un $\rho = 0.07$. Se muestra a continuación tablas que resumen el estudio estadístico para las corridas de Monte Carlo.

En las tablas presentadas se puede ver el buen funcionamiento del filtro extendido

Tabla II: Error cuadrático medio $(SSE_i)_{MC}$ de Monte Carlo y tiempo de sincronía (39) para el ejemplo 2 con $P_0 = 1$, $R = 5 \times 10^{-8}$, $\rho = 0.05$ y $N = 100$.

$e(0)$	$(SSE_1)_{MC}$	$(SSE_2)_{MC}$	$(SSE_3)_{MC}$	τ_{MC}
(0.1, 0.1, 0.1)	0.0100	0.1066	0.0110	6
(0.05, 0.05, 0.05)	0.0025	0.0532	0.0035	5
(0.01, 0.01, 0.01)	1.0095×10^{-4}	0.0142	0.0010	4
(-0.01, -0.01, -0.01)	1.0100×10^{-4}	0.0176	0.0011	3

Tabla III: Error cuadrático medio truncado de Monte Carlo y tiempo de sincronía (39) para el ejemplo 2 con $P_0 = 1$, $q_i = 1 \times 10^{-6}$, $i = 1, 2, 3$. $R = 5 \times 10^{-8}$, $\rho = 0.05$ y $N = 100$.

$e(0)$	$(TMSE_1)_{MC}$	$(TMSE_2)_{MC}$	$(TMSE_3)_{MC}$	τ_{MC}
(0.1, 0.1, 0.1)	1.0205×10^{-6}	0.0131	9.7194×10^{-4}	6
(0.05, 0.05, 0.05)	9.6606×10^{-7}	0.0128	9.7529×10^{-4}	5
(0.01, 0.01, 0.01)	8.5910×10^{-5}	0.0117	9.8750×10^{-4}	4
(-0.01, -0.01, -0.01)	9.5976×10^{-5}	0.0148	0.0011	3

de Kalman (como esclavo) cuando se cumplen las condiciones del error inicial y de los valores de Q y R . Comparando este ejemplo con el anterior se puede observar que las cotas obtenidas para este último son mucho más reducidas que para el ejemplo anterior, esto debido a la condición de hipercaos que se presenta en este ejemplo.

III.4 Resumen

En este capítulo se consideró el problema de sincronizar sistemas hipercaóticos discretos, en un ambiente ruidoso tanto en las dinámicas del sistema maestro como en la señal acoplante. Para el problema considerado, se propuso un filtro extendido de Kalman a manera de sistema esclavo, con el propósito de estimar los estados de un sis-

tema maestro ruidoso. Se obtuvo sincronía aproximada entre los estados de maestro y esclavo. Además, de manera analítica, se establecieron condiciones para el error inicial y el ruido que garantizan la convergencia del error de estimación (sincronía) $e(k)$.

Capítulo IV

Sincronización de Sistemas

Hipercaóticos por Acoplamiento a

Modelos

Es común observar el empleo de diversas herramientas de control conocidas en la sincronización de osciladores caóticos. En este capítulo, se presenta la metodología de acoplamiento a modelos para alcanzar este objetivo. Esta metodología fue sugerida en DiBenedetto e Isidori, (1986) empleando conceptos de geometría diferencial, mientras en Moog, *et al.* (1991) se propuso una solución con base en el álgebra diferencial, para el caso continuo y en Kotta, (1989) para el caso discreto. En este trabajo se optará por la propuesta presentada en Cruz-Hernández y Alvarez, (1995); Cruz-Hernández *et al.*, (1999) y se empleará dicha metodología para resolver el problema de sincronización de

sistemas hipercaóticos discretos.

IV.1 Descripción del problema de estudio

Considere el sistema no lineal discreto en el tiempo P , definido por

$$P : \begin{cases} x(k+1) = f(x(k), u(k)), \\ y(k) = h(x(k)), \end{cases} \quad (43)$$

donde el vector de estados $x(k) \in X$, siendo X un conjunto abierto en \mathbb{R}^n , la entrada $u(k)$ pertenece a un conjunto abierto U en \mathbb{R} y la salida $y(k)$ pertenece a un conjunto abierto Y en \mathbb{R} . Los mapeos $f : X \times U \rightarrow X$ y $h : X \rightarrow Y$ son analíticos.

Considere además, otro sistema no lineal discreto en el tiempo M , descrito por

$$M : \begin{cases} x_M(k+1) = f_M(x_M(k), u_M(k)), \\ y_M(k) = h_M(x_M(k)), \end{cases} \quad (44)$$

donde el vector de estados del modelo $x_M(k) \in X_M$, X_M siendo un conjunto abierto en \mathbb{R}^{n_M} , la entrada al modelo $u_M(k) \in U_M$, U_M es un conjunto abierto en \mathbb{R} y la salida del modelo $y_M(k)$ pertenece a un conjunto abierto Y_M en \mathbb{R} . También los mapeos $f_M : X_M \times U_M \rightarrow X_M$ y $h_M : X_M \rightarrow Y_M$ son analíticos. Para el resto del capítulo, se asume que para ciertos valores en los parámetros, los sistemas dinámicos P y M sin control, es decir, cuando $u(k) = u_M(k) = 0$ exhiben comportamientos **hipercaóticos**.

Esto es, los sistemas en consideración cuentan con *múltiples exponentes de Lyapunov positivos*. El problema particular de sincronización considerado en este trabajo, se define a continuación.

Definición (Problema de Sincronización de Salida): *Se dice que el sistema hipercaótico en tiempo discreto (43) sincroniza con el sistema hipercaótico en tiempo discreto (44) si*

$$\lim_{k \rightarrow \infty} \|y_M(k) - y(k)\| = 0, \quad (45)$$

independientemente de las condiciones iniciales $x(0)$ y $x_M(0)$ y para apropiadas señales de entrada $u(k)$ y $u_M(k)$.

Nótese, que se está considerando el problema de **sincronización parcial** entre P y M . Además, no importa si las dinámicas hipercaóticas de P y M son producidas por sistemas idénticos o sistemas diferentes. En trabajos muy recientes [López-Mancilla y Cruz-Hernández, 2005a; 2005b] fueron estudiados ambos casos para sistemas en tiempo continuo. En la siguiente sección se describirá cómo satisfacer la condición de sincronización de salida (45) desde una perspectiva de control, en particular, recurriendo al problema de acoplamiento a modelos.

IV.2 Problema de acoplamiento a modelos

Considere que la planta P evoluciona en una vecindad de un punto de equilibrio x^0 ; que es, alrededor de $(x^0, u^0) \in X \times U$ tal que $f(x^0, u^0) = x^0$ con $\{u(k) = u^0 : k \geq 0\}$ una secuencia constante de entrada. Para esta secuencia, existe otra secuencia constante de salida $\{y(k) = h(x^0) = y^0 : k \geq 0\}$. En forma similar, sea x_M^0 un punto de equilibrio de M , alrededor de $(x_M^0, u_M^0) \in X_M \times U_M$. Dada la planta P (43) y el modelo de referencia M (44), se está interesado en diseñar una ley de control $u(k)$ para la planta P , la cual, independientemente de las condiciones iniciales de P y M , produzca que la salida de la planta retroalimentada $y(k)$, converga asintóticamente a la salida del modelo M bajo una arbitraria entrada $u_M(k)$. Este problema es bien conocido en teoría de control de sistemas no lineales como **problema de acoplamiento a modelos (PAM)**. En otras palabras, el efecto del control $u(k)$, es el de producir un comportamiento entrada-salida en la planta compensada igual al que presenta el modelo preestablecido.

Cuando se considera que las condiciones iniciales del modelo y de la planta son las mismas ($x(0) = x_M(0)$) se conoce como **problema de acoplamiento fuerte a modelos (PAFM)**. En este caso, desde el primer instante de tiempo, la salida de la planta compensada es igual a la salida del modelo. En cambio, cuando las condiciones iniciales de la planta y del modelo son distintas ($x(0) \neq x_M(0)$), se le conoce como **problema de acoplamiento asintótico a modelos (PAAM)**; en este caso las salidas de la planta compensada y del modelo son distintas en un principio ($k = 0$), pero a medida

que transcurre el tiempo ($k \rightarrow \infty$), la salida de la planta compensada converge a la salida del modelo. En este trabajo de tesis, se tiene interés particular en el problema de acoplamiento asintótico a modelos que a continuación se describe brevemente y donde el análisis que se presenta, está dado para el caso particular de sistemas de **una entrada** y **una salida** únicamente, por considerarlo apropiado para las aplicaciones propuestas en un capítulo posterior.

IV.2.1 Acoplamiento asintótico a modelos

El objetivo de control del problema de acoplamiento asintótico a modelos consiste en encontrar una ley de control $u(k)$ para la planta P que logre, para cualesquiera de los estados iniciales de P y M , que la salida $y(k)$ de P converja asintóticamente a la salida $y_M(k)$ producida por M bajo una entrada arbitraria $u_M(k)$. En la literatura correspondiente, se encuentran reportados muchos trabajos donde se han propuestos diferentes maneras de resolver el problema de acoplamiento a modelos en tiempo discreto [Nijmeijer y van der Schaft, 1990; Kotta, 1995; Cruz-Hernández *et al.*, 1999]. En particular, en este trabajo de tesis se adoptará la metodología propuesta en [Cruz-Hernández y Alvarez, 1995; Cruz-Hernández *et al.*, 1999]: *donde el PAAM se transforma en un problema de desacoplar la salida de un sistema auxiliar de la entrada al modelo $u_M(k)$.*

Expuesto lo anterior, se está en condiciones de definir formalmente el problema de acoplamiento asintótico a modelos.

Definición 1: Problema discreto de acoplamiento asintótico a modelos

no lineales (PDAAMN) [Cruz y Alvarez, 1995]. Dada la planta P (43) y el modelo M (44) definidos alrededor de sus respectivos puntos de equilibrio (x^0, u^0) y (x_M^0, u_M^0) , y un punto $(x(0), x_M(0)) \in X^0 \times X_M^0 \subset X \times X_M$. El PDAAMN consiste en encontrar un entero ν y una ley de control $u(k)$, tal que la salida de la planta compensada $y_{P \circ C}(k)$ converja asintóticamente a la salida $y_M(k)$ producida por una entrada $u_M(k)$ del modelo M .

IV.2.2 Metodología de solución al PDAAMN

Una forma de resolver el PDAAMN¹ [Cruz-Hernández, 1995; Cruz-Hernández y Alvarez, 1995; Cruz-Hernández *et al.*, 1999] consiste en definir un error $y_E(k) = y(k) - y_M(k)$ entre las salidas de la planta P y del modelo M y diseñar una ley de control $u(k)$, tal que este error reúna las siguientes propiedades:

- i)* Esté desacoplado de la entrada del modelo $u_M(k)$ para toda $k \geq 0$ y
- ii)* Converja asintóticamente a cero.

El primer punto es equivalente a transformar el PDAAMN en un problema de desacoplamiento a perturbaciones de un sistema auxiliar (compuesto por planta y modelo). Al resolver el problema en esta forma, se obtiene no sólo convergencia de la salida de la planta a la salida del modelo, sino también, una convergencia del error que es independiente de la entrada al modelo $u_M(k)$. De esta manera, el error de salida $y_E(k)$

¹Para el caso continuo, es propuesta por Di Benedetto e Isidori, 1986.

depende sólo de las condiciones iniciales $x(0)$ y $x_M(0)$. Con este propósito, se define dicho **sistema auxiliar** como sigue

$$E : \begin{cases} x_E(k+1) = f_E(x_E(k), u_E(k), w_E(k)), \\ y_E(k) = h_E(x_E(k)), \end{cases} \quad (46)$$

con vector de estado auxiliar $x_E(k) = (x(k), x_M(k))^T \in \mathbb{R}^{n+n_M}$ y entradas $u_E(k) = u(k)$ y $w_E(k) = u_M(k)$, donde

$$\begin{aligned} f_E(x_E, u_E, w_E) &= \begin{pmatrix} f(x, u) \\ f_M(x_M, u_M) \end{pmatrix}, \\ h_E(x_E) &= h(x) - h_M(x_M). \end{aligned}$$

Nótese que en este sistema auxiliar la señal $u_M(k)$ se considera una *perturbación* y siendo ésta una señal conocida en todo tiempo (ya que es la entrada a M), se puede tratar el problema anterior como un problema de desacoplamiento a perturbaciones con medición de perturbaciones.

En los casos de plantas en tiempo continuo [Di Benedetto e Isidori, 1986] y plantas en tiempo discreto [Alvarez *et al.*, 1992] se puede probar que: *un problema de acoplamiento a modelos no lineales tiene solución, si existe solución al problema de desacoplamiento a perturbaciones con medición de perturbaciones, asociado al sistema auxiliar (46)*. A continuación el PDAAMN se tratará en términos del **grado relativo** asociado a las salidas $y(k)$ e $y_M(k)$ para lo cual se presenta la siguiente definición:

Considere f_0 , f_{M_0} y f_{E_0} las dinámicas sin entradas $f(\cdot, 0)$, $f_M(\cdot, 0)$ y $f_E(\cdot, 0, 0)$, respectivamente. f_0^j , $f_{M_0}^j$ y $f_{E_0}^j$ la j -ésima composición de f_0 , f_{M_0} y f_{E_0} con $f_0^0(x(k)) = x(k)$, $f_{M_0}^0(x_M(k)) = x_M(k)$ y $f_{E_0}^0(x_E(k)) = x_E(k)$.

Definición 2: Grado relativo [Monaco y Normand-Cyrot, 1987]. La salida $y(k)$ de la planta (43) se dice que tiene grado relativo d en un subconjunto abierto y denso O de $X \times U$ conteniendo al punto de equilibrio (x^0, u^0) , si

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

para toda $0 \leq l \leq d - 1$, para todo $(x, u) \in O$ y

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

para todo $(x, u) \in O$.

Una definición similar puede formularse para el grado relativo d_M del modelo (44), en un subconjunto abierto y denso O_M , de $X_M \times U_M$ conteniendo al punto de equilibrio (x_M^0, u_M^0) .

Para resolver el PAAM, la siguiente hipótesis es requerida:

(H4) Para todo $x_E = (x, x_M)^T \in X \times X_M$ y toda $u_M \in U_M$,

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

donde $\Im m \{ \varphi \}$ indica la imagen del mapa φ y “ \circ ” es la operación de composición.

De este modo, el siguiente teorema da condiciones necesarias y suficientes para la solución local del PAAM.

Teorema. (Cruz-Hernández, 1995; Cruz-Hernández et al., 1999). Considere la planta P (43) y el modelo M (44) definidos alrededor de sus respectivos puntos de equilibrio (x^0, u^0) y (x_M^0, u_M^0) . Supóngase que la salida de la planta y del modelo tienen grados relativos finitos d y d_M , respectivamente. Asumase que la suposición (H4) se cumple. Entonces el PAAM tiene solución local en Ω_o^E , si y sólo si

$$d \leq d_M. \quad (47)$$

Si la condición (47) se cumple, entonces a partir de la definición de grado relativo d y d_M , se tiene que

$$\begin{aligned} y_E(k+l) &= h_E \circ f_{E_0}^l(x_E(k)) \\ &= h \circ f_0^l(x(k)) - h_M \circ f_{M_0}^l(x_M(k)), \quad l = 0, 1, \dots, d, \end{aligned}$$

además,

$$\begin{aligned} y_E(k+d+1) &= h \circ f_0^d \circ f(x(k), u(k)) - h_M \circ f_{M_0}^l \circ f_M(x_M(k), u_M(k)) \\ &= h \circ f_0^{d+1}(x(k)) + S(x(k), u(k)) - h_M \circ f_{M_0}^l \circ f_M(x_M(k), u_M(k)), \end{aligned}$$

con $S(x(k), 0) = 0$ y

$$\frac{\partial S(x(k), u(k))}{\partial u(k)} = \frac{\partial y_E(k+d+1)}{\partial u(k)} \neq 0. \quad (48)$$

Considerando (48) y la suposición (H4), se sigue a partir del teorema de la función implícita que existe un mapa analítico $\gamma^E : \mathbb{R}^{n+n_M} \times \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ tal que

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

con $v \in \mathbb{R}$ un control externo, o equivalentemente,

$$\begin{aligned} S(x(k), \gamma^E(x_E(k), u_M(k), v(k))) &= v(k) \\ &\quad - h \circ f_0^d \circ f(x(k)) \\ &\quad + h_M \circ f_{M_0}^l \circ f_M(x_M(k), u_M(k)). \end{aligned}$$

El mapeo analítico $\gamma^E(x_E, u_M, v)$ es el inverso de $S(x, \cdot)$, es decir

$$\gamma^E(x_E(k), u_M(k), v(k)) = S^{-1}(x(k), v - h \circ f_0^d \circ f(x) + h_M \circ f_{M_0}^l \circ f_M(x_M(k), u_M(k))), \quad (49)$$

donde el control externo es dado por

$$v(k) = - \sum_{l=0}^d \alpha_l [h \circ f_0^l(x(k)) - h_M \circ f_{M_0}^l(x_M(k))]. \quad (50)$$

Finalmente, se muestra al sistema auxiliar E (46) retroalimentado por la ley de control (49)-(50) en términos de la planta P y del modelo M en un marco de coordenadas diferentes. En este trabajo, se restringen los resultados sobre sincronización de salida a:

(A5) *Plantas completamente linealizables, es decir, para $d + 1 = n$.*

A partir de la definición de grado relativo d , se tiene que: $h(x), \dots, h \circ f_0^d(x)$ son funciones independientes [Nijmeijer, 1987] y pueden ser elegidas como nuevas coordenadas con $\xi_i(x) = h \circ f_0^{i-1}(x)$ para $i = 1, 2, \dots, d + 1$ definidas en el subconjunto O alrededor de x^0 . Permítase considerar al sistema auxiliar E (46) y las nuevas coordenadas

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

donde $\zeta(x_E) = [\zeta_1(x_E), \dots, \zeta_{d+1}(x_E)]^T$ y $\zeta_i(x_E) = h_{E_i} \circ f_{E_0}^{i-1}(x_E) = \xi_i(x) - h_{M_0} \circ f_{M_0}(x_M)$ para $i = 1, 2, \dots, d + 1$. De este modo, el sistema auxiliar (46) en lazo cerrado

en el nuevo marco de coordenadas toma la forma

$$\begin{aligned}
 \zeta_i(k+1) &= \zeta_{i+1}(k), & i = 1, \dots, d, \\
 \zeta_{d+1}(k+1) &= v(k) = -\alpha_0\zeta_1(k) - \dots - \alpha_d\zeta_{d+1}(k), \\
 x_M(k+1) &= f_M(x_M(k), u_M(k)), \\
 y_E(k) &= \zeta_1(k).
 \end{aligned} \tag{51}$$

De la descripción del sistema (51), se puede ver que la salida $y(k)$ de la planta retroalimentada, difiere de la salida $y_M(k)$ del modelo por una señal de error $y_E(k)$, gobernada por la ecuación lineal en diferencias

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

donde $\alpha_0, \dots, \alpha_d$ son coeficientes reales constantes, lográndose que la salida $y(k)$ converja a $y_M(k)$. Es decir, $y_E(k) = 0$ después de algún tiempo, lográndose por tanto, que la condición de sincronización de salida (45) se cumpla.

Del sistema en lazo cerrado (51), se pueden distinguir dos subsistemas, que son:

1. El sistema descrito por la ecuación

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

que representa la dinámica del modelo de referencia M .

2. El subsistema lineal definido por la ecuación

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

con

$$A^* = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -\alpha_0 & -\alpha_1 & -\alpha_2 & \cdots & -\alpha_d \end{bmatrix}$$

asociada a la dinámica de la señal de error $y_E(k)$.

Como el subsistema M puede asumirse estable, si se elige una ley de control tal que la matriz A^* tenga todos sus valores propios con magnitud estrictamente menor que 1, entonces el sistema en lazo cerrado será exponencialmente estable. Como consecuencia de lo anterior, se cumple también con la condición de sincronía de salida (45).

Observación: Dado que $y_E(k) = \zeta_1(k) = \xi_1(x(k)) - h_{M1}(x_M(k)) \rightarrow 0$ a medida que $k \rightarrow \infty$, notese que $\xi_i(x)$ y $h_{M_i} \circ f_{M_0}^{i-1}(x_M)$, $i = 1, 2, \dots, d+1$ son difeomorfismos. Entonces, si la planta P y el modelo M son sistemas hipercaóticos discretos **idénticos**, $\xi_i(x) \rightarrow h_{M_i} \circ f_{M_0}^{i-1}(x_M)$, $i = 1, 2, \dots, d+1$ y, si los mapeos tienen la misma estructura y tienden a ser iguales, entonces los argumentos también, es decir $x(k) \rightarrow x_M(k)$ a medida que $k \rightarrow \infty$. Además, de la ley de control (49)-(50) se puede ver que, $u(k) \rightarrow u_M(k)$ a medida que $k \rightarrow \infty$, con el propósito de desacoplar la entrada $u_M(k)$

en el sistema auxiliar E (46). Por tanto, para sistemas hipercaóticos idénticos, se obtiene **sincronización completa**, es decir la condición

$$\lim_{k \rightarrow \infty} \|x_M(k) - x(k)\| = 0, \quad (52)$$

se cumple. Sin embargo, para sistemas hipercaóticos discretos no idénticos únicamente se garantiza sincronización en la salida, i.e. la condición (45) se cumple.

IV.3 Sincronización de sistemas hipercaóticos mediante acoplamiento a modelos

Con la información presentada en la sección anterior se puede establecer lo siguiente:

- Dados dos sistemas P y M definidos alrededor de sus puntos de equilibrio (x^0, u^0) y (x_M^0, u_M^0) por (43) y (44), respectivamente. Suponga que P y M tienen grados relativos finitos d y d_M respectivamente y que la hipótesis **H4** se cumple. Entonces, es posible encontrar una ley de control $u(k)$ tal que, la salida de P sincronice con la salida del modelo M , si y sólo si

$$d \leq d_M. \quad (53)$$

- Para el caso particular de que planta y modelo esten representados por sistemas

idénticos (y por tanto $d = d_M$) con P completamente linealizable, además de **sincronía de salida**, se obtiene **sincronía completa**.

En tanto que la ley de control que resuelve el $PDAAMN$ se obtiene de la expresión

$$y_E(k+d+1) + \alpha_d y_E(k+d) + \dots + \alpha_1 y_E(k+1) + \alpha_0 y_E(k) = 0 \quad (54)$$

que puede expresarse de la siguiente forma

$$u(k) = \gamma(x_E(k), u_M(k)) \quad (55)$$

$$= \gamma(x(k), x_M(k), u_M(k))$$

$$= \gamma(x(k), \phi_M(x_M(k), u_M(k))), \quad (56)$$

donde $\phi_M(x_M(k), u_M(k))$ (obtenida al despejar $u(k)$ de (54)) es la señal que deberá enviarse por el modelo al esclavo como señal acoplante, con el propósito de construir la ley de control $u(k)$ que resuelve el $PDAAMN$, y con ésto el problema de sincronización de salida. La figura 18 muestra un diagrama a bloques que representa lo anterior; con esta configuración se garantiza sincronización en la salida, significando que la condición (45) se cumple.

Observación: Hay que mencionar que la función no lineal $\phi_M(x_M(k), u_M(k))$ que proviene del modelo, depende también de las constantes α_i , $i = 0, 1, \dots, d$ que aparecen tanto en maestro como esclavo. Esto implica que se tendrá que conocer dichos valores previamente y ser iguales en ambos sistemas. Si dichos valores difieren entre el maestro

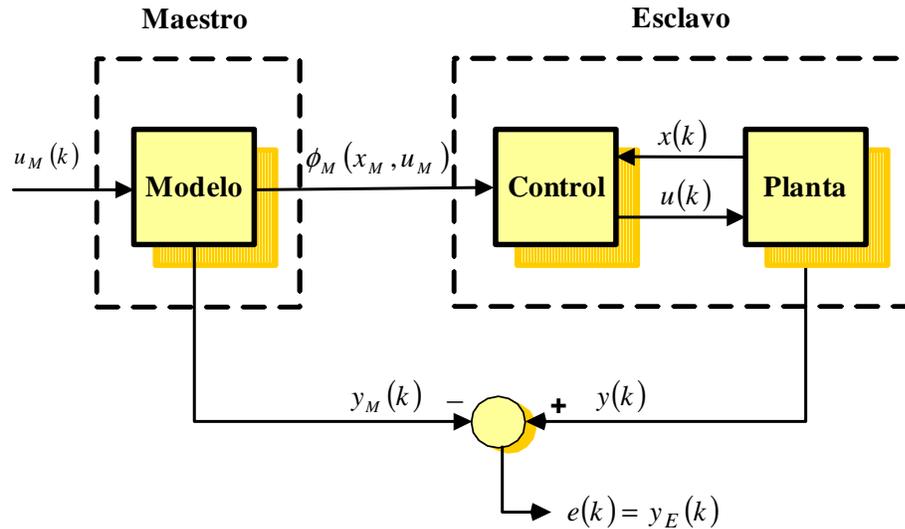


Figura 18: Esquema de sincronización empleando acoplamiento a modelos.

y el esclavo, la sincronía no se obtiene. Esta característica se puede explotar en el contexto de comunicación de información privada.

A continuación se resume la metodología presentada anteriormente en un breve método sistemático.

Sincronización de salida:

Metodo sistemático: (Sistemas completamente linealizables)

1. Dado un sistema hipercaótico discreto en el tiempo $x(k+1) = f(x(k))$, se escribe en la forma P (43) y M (44) agregando una entrada de control $u(k)$ y $u_M(k)$, respectivamente.
2. Se definen propiamente las salidas $y(k)$ e $y_M(k)$ para P y M , respectivamente, tal

que la condición para la solución del PAAMN se cumpla $d \leq d_M$. (Si los sistemas son idénticos, dicha condición siempre se cumple).

3. De la ecuación (54) se obtiene la ley de control $u(k)$ (que resuelve el PAAMN asignando valores apropiados a α_i en P y M).
4. De $u(k)$ (55) se identifica la señal de acoplamiento que se transmite al sistema esclavo P para lograr la sincronía en la salida.

A continuación se presenta un par de ejemplos que ilustran la metodología expresada en la sección anterior.

IV.4 Ejemplos

Ejemplo 1. Considere el siguiente sistema discreto de segundo orden

$$\begin{aligned} x_1(k+1) &= 1 - a(x_1^2(k) + x_2^2(k)), \\ x_2(k+1) &= -2abx_1(k)x_2(k), \end{aligned} \tag{57}$$

con los valores en los parámetros $a = 1.95$ y $b = 1$, el sistema presenta comportamiento hipercaótico (Chen, 2001). En la figura 19 se observa el comportamiento temporal de los estados del sistema (57) cuando parten de la condición $x(0) = (0.025, 0.97)$. Mientras que en la figura 20 se muestra en el espacio de estados el atractor hipercaótico del sistema sobre el plano x_1 vs x_2 .

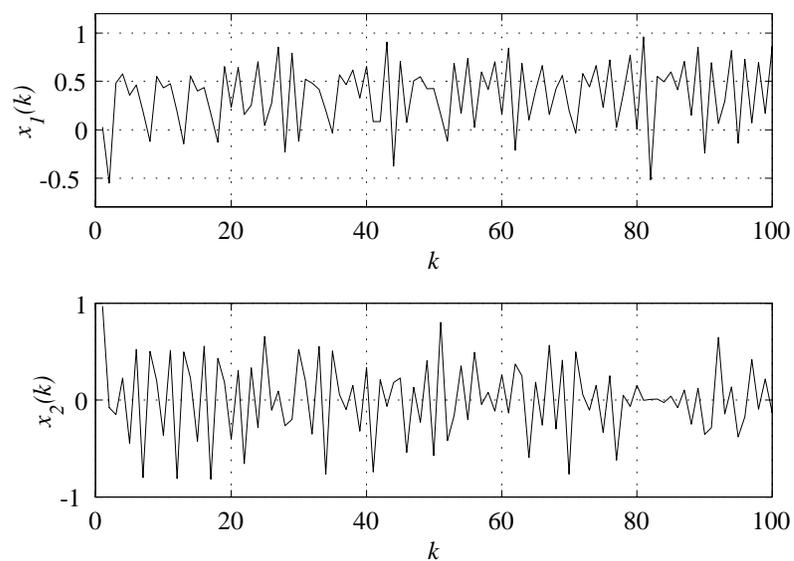


Figura 19: Evoluciones en el tiempo de los estados hipercaóticos del sistema (57).

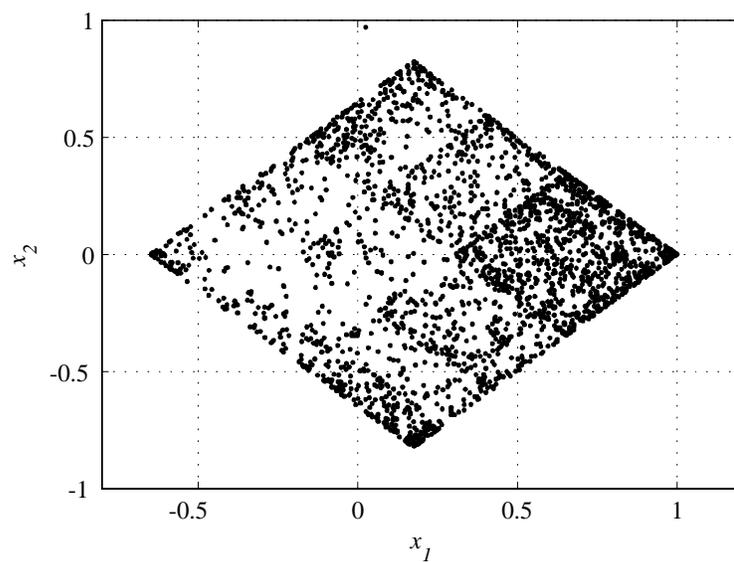


Figura 20: Atractor hipercaótico desplegado por el sistema (57).

Con base en el sistema anterior, considere el siguiente sistema como esclavo (planta),

$$P : \begin{cases} x_1(k+1) = 1 - a(x_1^2(k) + x_2^2(k)) + u(k), \\ x_2(k+1) = -2abx_1(k)x_2(k), \\ y(k) = x_2(k), \end{cases} \quad (58)$$

además, considere el siguiente sistema como maestro (modelo de referencia),

$$M : \begin{cases} x_{M1}(k+1) = 1 - a(x_{M1}^2(k) + x_{M2}^2(k)) + u_M(k), \\ x_{M2}(k+1) = -2abx_{M1}(k)x_{M2}(k), \\ y_M(k) = x_{M2}(k), \end{cases} \quad (59)$$

con esto, el grado relativo tanto del esclavo (58) como del maestro (59) es $d = d_M = 1$, garantizando solución al problema de acoplamiento a modelos y por tanto, al problema equivalente de sincronización de salida, condición (45).

Para encontrar la solución a este problema siguiendo nuestra metodología, se define un sistema auxiliar como en (46), cuya salida es la diferencia entre la salida del esclavo y del maestro:

$$y_E(k) = y(k) - y_M(k) = x_2(k) - x_{M2}(k).$$

Definiendo $\zeta_1(k) = y_E(k)$ se expresan los sistemas (58) y (59) en nuevas coorde-

nadas:

$$\zeta_1(k+1) = y_E(k+1) = \zeta_2(k), \quad (60)$$

$$\zeta_2(k+1) = y_E(k+2) = v(k) = -\alpha_1\zeta_2(k) - \alpha_0\zeta_1(k).$$

Del sistema anterior (60), se observa que en este caso el sistema auxiliar en las nuevas coordenadas, está completamente linealizado. La selección apropiada de los valores de α_i , $i = 0, 1$ garantiza convergencia del error a cero, es decir $\zeta_1(k) = 0$.

Se obtiene la siguiente ley de control que logra el acoplamiento entre la salida del maestro y del esclavo

$$u(k) = \left(\frac{v(k) + \epsilon(k)}{4a^2b^2x_1(k)x_2(k)} \right) - 1 + a(x_1^2(k) + x_2^2(k)), \quad (61)$$

donde

$$\epsilon(k) = -2ab [1 - a(x_{M1}^2(k) + x_{M2}^2(k)) + u_M(k)] (-2abx_{M1}(k)x_{M2}(k)),$$

$$\begin{aligned} v(k) &= -\alpha_1\zeta_2(k) - \alpha_0\zeta_1(k) \\ &= -\alpha_1(-2abx_1(k)x_2(k) + 2abx_{M1}(k)x_{M2}(k)) - \alpha_0(x_2(k) - x_{M2}(k)) \\ &= 2\alpha_1abx_1(k)x_2(k) - \alpha_0x_2(k) + \alpha_0x_{M2}(k) - 2\alpha_1abx_{M1}(k)x_{M2}(k). \end{aligned}$$

De este modo, la función no lineal $\phi_M(x_M, u_M)$ está definida por

$$\begin{aligned} \phi_M(x_M(k), u_M(k)) &= \alpha_0 x_{M2}(k) - 2\alpha_1 ab x_{M1}(k) x_{M2}(k) \\ &\quad - 2ab [1 - a (x_{M1}^2(k) + x_{M2}^2(k)) + u_M(k)] \times \\ &\quad (-2ab x_{M1}(k) x_{M2}(k)). \end{aligned} \quad (62)$$

Utilizando la ley de control (61) y el esquema mostrado en la figura 18, se realizaron las siguientes simulaciones numéricas.

Se emplearon los mismos valores de parámetros tanto en maestro como en esclavo ($a = 1.95$ y $b = 1$). Se optó por $u_M(k) = 0$ para garantizar el comportamiento hipercaótico del maestro, se fijaron condiciones iniciales $x(0) = (0.1, 0.1)$ para el esclavo y $x_M(0) = (0.025, 0.025)$ para el maestro y se seleccionó $\alpha_i = 0.2$, $i = 0, 1$. El control se activó en el tiempo $k = 20$ para apreciar mejor el efecto de sincronía.

En la figura 21 se observa la evolución temporal de los estados $x_1(k)$ y $x_{M1}(k)$ además de los estados $x_2(k)$ y $x_{M2}(k)$; puede apreciarse como después de un transitorio, los estados se acoplan (sincronizan). Es decir, para este ejemplo, donde se construye maestro y esclavo con sistemas idénticos, se obtiene sincronía completa. La figura 22 muestra la señal de control $u(k)$ y la señal transmitida por el maestro $\phi_M(x_M(k), u_M(k))$ hacia el esclavo. Finalmente, la figura 23 muestra la evolución temporal de los errores entre los estados del maestro y del esclavo, $e_i(k) = x_i(k) - x_{M_i}(k)$, $i = 1, 2$.

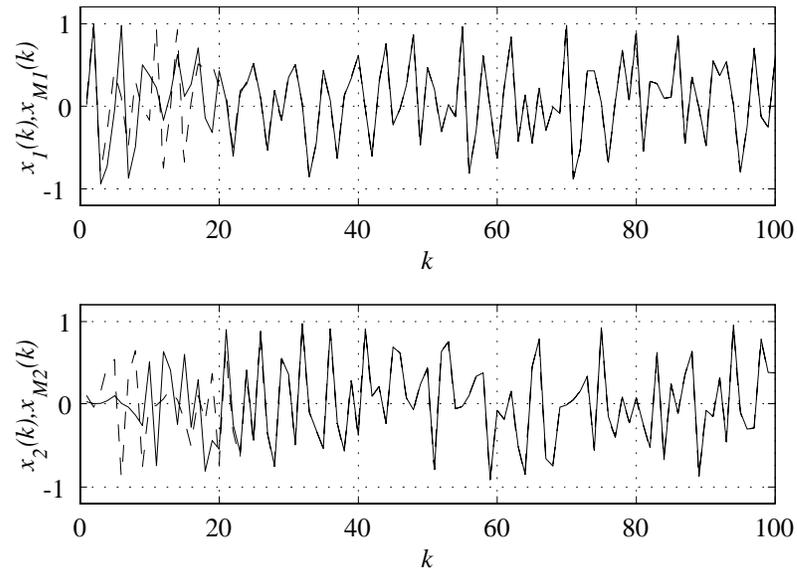


Figura 21: Acoplamiento entre $x_{M1}(k)$ (línea continua) y $x_1(k)$ (línea segmentada) y acoplamiento (sincronía) entre la salida del modelo $y_M(k) = x_{M2}(k)$ (línea continua) y la salida de la planta $y(k) = x_2(k)$ (línea segmentada) cuando la ley de control actúa en el tiempo $k = 20$.

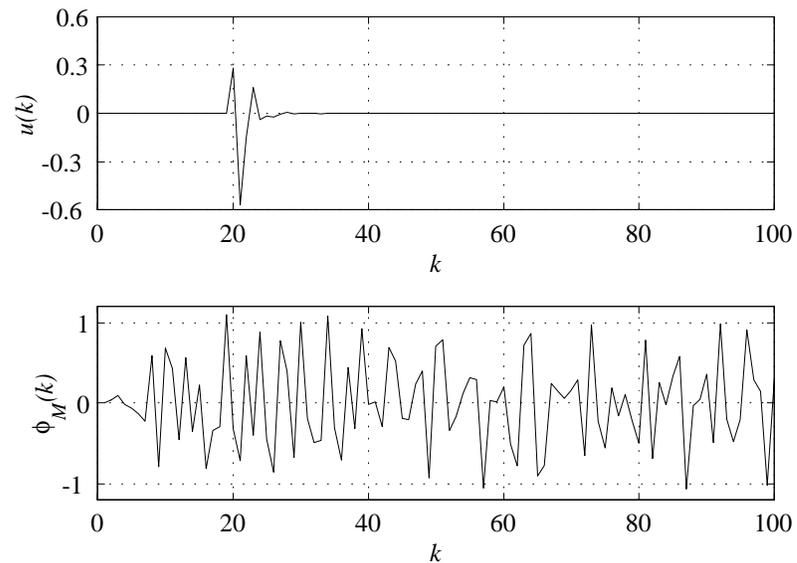


Figura 22: Control $u(k)$ actuando en $k = 20$. Señal acoplante $\phi_M(x_M(k), u_M(k))$ enviada por el modelo M (maestro) hacia la planta P (esclavo) para lograr sincronía.

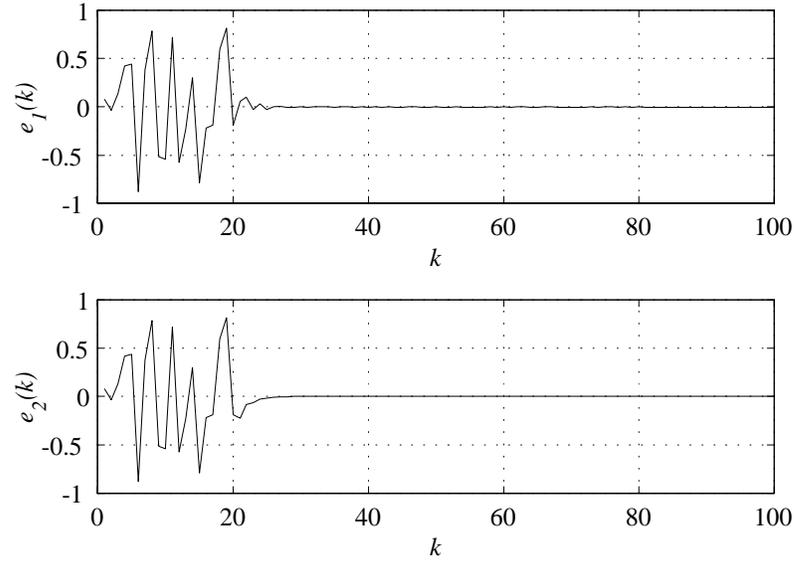


Figura 23: Evolución temporal de los errores de sincronía: $e_i(k) = x_i(k) - x_{M_i}(k)$, $i = 1, 2$.

Ejemplo 2. Considere el siguiente sistema discreto de Rössler

$$x_1(k+1) = \alpha x_1(k)(1 - x_1(k)) - \beta(x_3(k) + \gamma)(1 - 2x_2(k)), \quad (63)$$

$$x_2(k+1) = \delta x_2(k)(1 - x_2(k)) + \varsigma x_3(k),$$

$$x_3(k+1) = \eta((x_3(k) + \gamma)(1 - 2x_2(k)) - 1)(1 - \theta x_1(k)).$$

Para el conjunto de valores paramétricos: $\alpha = 3.8$, $\beta = 0.05$, $\gamma = 0.35$, $\delta = 3.78$, $\varsigma = 0.2$, $\eta = 0.1$, $\theta = 1.9$, el sistema de Rössler (63) presenta comportamiento hipercaótico (Itoh, *et al*, 2001). En la figura 24 se observa el comportamiento temporal de los tres estados. Mientras que en la figura 25 se muestra las proyecciones de los estados sobre el espacio de estados del sistema.

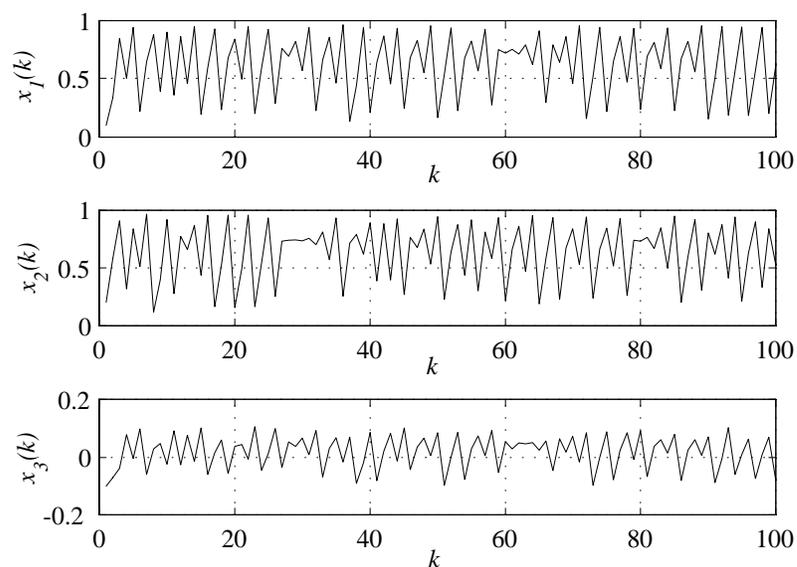


Figura 24: Evoluciones en el tiempo de los estados hipercaóticos del sistema (63) cuando $x(0) = (0.1, 0.2, -0.1)$.

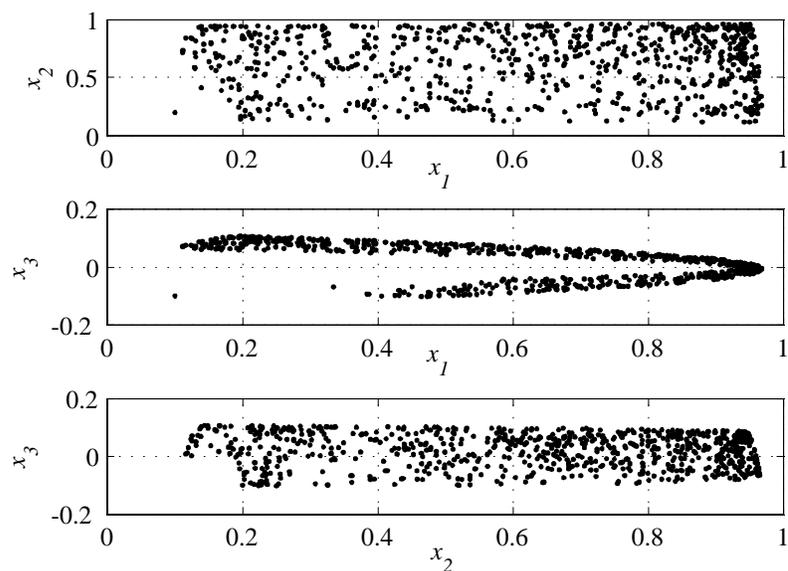


Figura 25: Atractores del sistema hipercaótico (63), x_1 vs x_2 , x_1 vs x_3 y x_2 vs x_3 .

Agregando una entrada de control $u(k)$ en (63) se puede considerar como esclavo (planta) el sistema hipercaótico de Rössler,

$$P : \begin{cases} x_1(k+1) = \alpha x_1(k)(1-x_1(k)) - \beta(x_3(k) + \gamma)(1-2x_2(k)) + u(k), \\ x_2(k+1) = \delta x_2(k)(1-x_2(k)) + \varsigma x_3(k), \\ x_3(k+1) = \eta((x_3(k) + \gamma)(1-2x_2(k)) - 1)(1-\theta x_1(k)), \\ y(k) = x_2(k), \end{cases} \quad (64)$$

además, considere el siguiente sistema hipercaótico de Rössler como maestro (modelo de referencia),

$$M : \begin{cases} x_{M1}(k+1) = \alpha x_{M1}(k)(1-x_{M1}(k)) - \beta(x_{M3}(k) + \gamma)(1-2x_{M2}(k)) + u_M(k), \\ x_{M2}(k+1) = \delta x_{M2}(k)(1-x_{M2}(k)) + \varsigma x_{M3}(k), \\ x_{M3}(k+1) = \eta((x_{M3}(k) + \gamma)(1-2x_{M2}(k)) - 1)(1-\theta x_{M1}(k)), \\ y_M(k) = x_{M2}(k), \end{cases} \quad (65)$$

el grado relativo tanto del esclavo (64) como del maestro (65) es $d = d_M = 2$, con esto se garantiza solución al problema de acoplamiento a modelos y al de sincronía de salida definido en (53) de acuerdo con (45). Para hallar la solución de acuerdo a la metodología propuesta, se construye el sistema auxiliar (46), cuya salida es el error entre la salida del esclavo y del maestro,

$$y_E(k) = y(k) - y_M(k) = x_2(k) - x_{M2}(k).$$

Definiendo $\zeta_1(k) = y_E(k)$, se expresan los sistemas (64) y (65) en nuevas coordenadas como sigue:

$$\zeta_1(k+1) = y_E(k+1) = \zeta_2(k), \quad (66)$$

$$\zeta_2(k+1) = y_E(k+2) = \zeta_3(k),$$

$$\zeta_3(k+1) = y_E(k+3) = v(k) = -\alpha_2\zeta_3(k) - \alpha_1\zeta_2(k) - \alpha_0\zeta_1(k).$$

El sistema (66) se encuentra completamente linealizado y por tanto, con la selección adecuada de los valores de α_i , $i = 0, 1, 2$, se garantiza convergencia del error a cero, es decir, $\zeta_1(k) = 0$.

La ley de control de acuerdo con (56), que logra el acoplamiento entre las salidas del maestro y del esclavo, está dada por

$$u(k) = \frac{1}{\theta} \left(1 - \frac{v+a-b}{c} \right) - (\alpha x_1(1-x_1) - \beta(x_3 + \gamma)(1-2x_2)), \quad (67)$$

donde

$$a = \delta a_1 (1 - a_1) + a_2,$$

$$a_1 = \delta (\delta x_{M2} (1 - x_{M2}) + \varsigma x_{M3}) (1 - (\delta x_{M2} (1 - x_{M2}) + \varsigma x_{M3})) \\ + \varsigma (\eta ((x_{M3} + \gamma) (1 - 2x_{M2}) - 1) (1 - \theta x_{M1})),$$

$$a_2 = \varsigma [\eta ((\eta ((x_{M3} + \gamma) (1 - 2x_{M2}) - 1) (1 - \theta x_{M1})) + \gamma) \\ \times (1 - 2(\delta x_{M2} (1 - x_{M2}) + \varsigma x_{M3}) - 1) \\ \times (1 - \theta (\alpha x_{M1} (1 - x_{M1}) - \beta (x_{M3} + \gamma) (1 - 2x_{M2}) + u_M)],$$

$$b = \delta b_1 (1 - b_1),$$

$$b_1 = \delta (\delta x_2 (1 - x_2) + \varsigma x_3) (1 - (\delta x_2 (1 - x_2) + \varsigma x_3)) \\ + \varsigma (\eta ((x_3 + \gamma) (1 - 2x_2) - 1) (1 - \theta x_1)),$$

$$c = \varsigma \eta (((\eta ((x_3 + \gamma) (1 - 2x_2) - 1) (1 - \theta x_1)) + \gamma) (1 - 2(\delta x_2 (1 - x_2) + \varsigma x_3) - 1)).$$

De ahí que la función no lineal de acoplamiento $\phi_M(x_M, u_M)$ entre maestro y esclavo, adquiere la forma,

$$\phi_M(x_M(k), u_M(k)) = \alpha_0 x_{M2}(k) + \alpha_1 (\delta x_{M2}(k) (1 - x_{M2}(k)) + \varsigma x_{M3}(k)) \\ + \alpha_2 d_1 + a, \tag{68}$$

donde

$$d_1 = \delta (\delta x_{M2}(k) (1 - x_{M2}(k)) + \varsigma x_{M3}(k)) (1 - (\delta x_{M2}(k) (1 - x_{M2}(k)) + \varsigma x_{M3}(k))) \\ + \varsigma (\eta ((x_{M3}(k) + \gamma) (1 - 2x_{M2}(k)) - 1) (1 - \theta x_{M1}(k))).$$

Utilizando la ley de control (67) y el esquema mostrado en la figura 18, se realizaron las simulaciones que a continuación se describen. Nuevamente se seleccionaron los mismos valores de parámetros para el maestro y esclavo: $\alpha = 3.8$, $\beta = 0.05$, $\gamma = 0.35$, $\delta = 3.78$, $\varsigma = 0.2$, $\eta = 0.1$, $\theta = 1.9$. Se eligió $u_M(k) = 0$ para garantizar el comportamiento hipercaótico del modelo y se tomaron condiciones iniciales $x(0) = (-0.3, -0.2, 0.3)$ y $x_M(0) = (0.1, 0.2, -0.1)$. También, se eligieron los coeficientes $\alpha_i = 0.1$, $i = 0, 1, 2$ con estos valores el *tiempo de sincronía* τ fue de 18.

La figura 26 muestra el acoplamiento entre $y(k) = x_2(k)$ e $y_M(k) = x_{M2}(k)$, además muestra la evolución temporal del error de sincronía $e_2(k) = x_2(k) - x_{M2}(k)$ de las salidas de (64) y (65). Aquí nuevamente, se puede apreciar como después de transcurrido un tiempo τ , se obtiene sincronía en la salida. La figura 27 muestra la evolución temporal de los errores de los estados restantes, se observa que nuevamente se obtiene sincronía en todos los estados y no únicamente en la salida.

Para las siguientes simulaciones se incrementaron los valores de α_i , $i = 0, 1, 2$ a 0.75, con esto se observa un aumento en el tiempo de sincronía τ , por lo que cambiando el valor de α_i se modifica también el valor de τ . La figura 28 muestra el acoplamiento entre

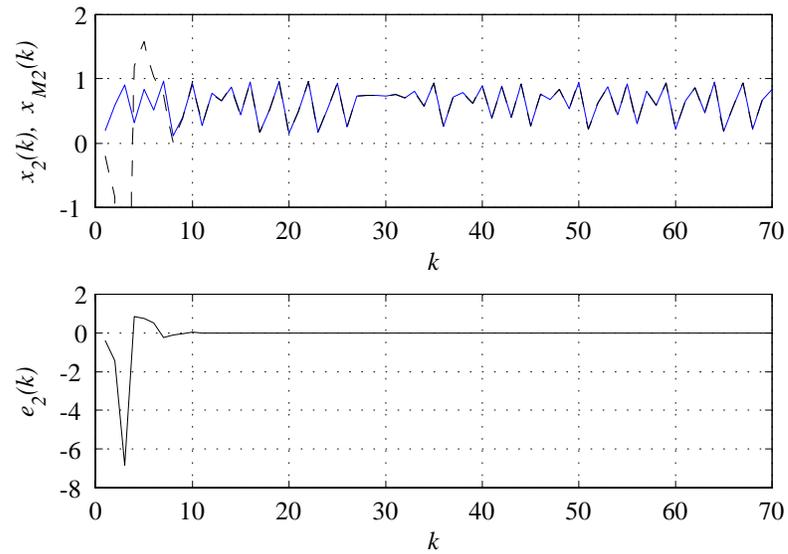


Figura 26: Sincronía (acoplamiento) entre $y(k) = x_2(k)$ (línea punteada) e $y_M(k) = x_{M2}(k)$ (línea continua) y error de sincronía $e_2(k) = x_2(k) - x_{M2}(k)$.

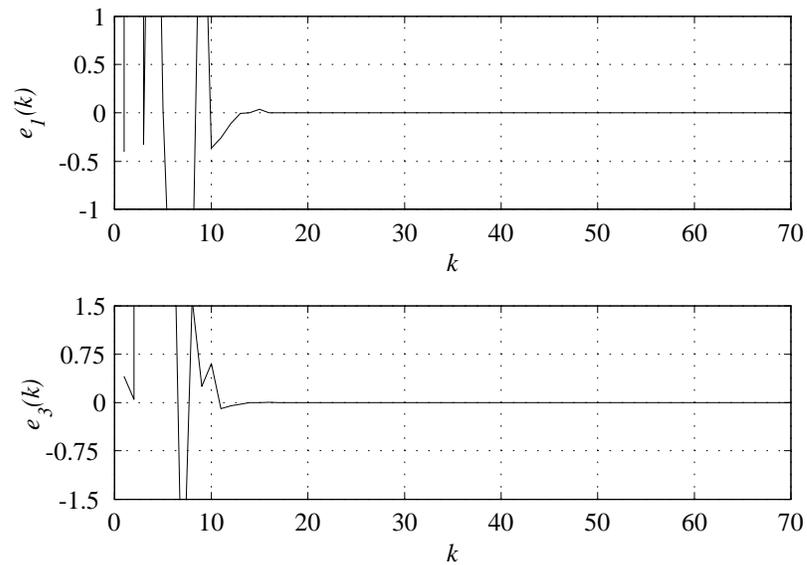


Figura 27: Evolución temporal de los errores de sincronía restantes $e_1(k) = x_1(k) - x_{M1}(k)$ y $e_3(k) = x_3(k) - x_{M3}(k)$.

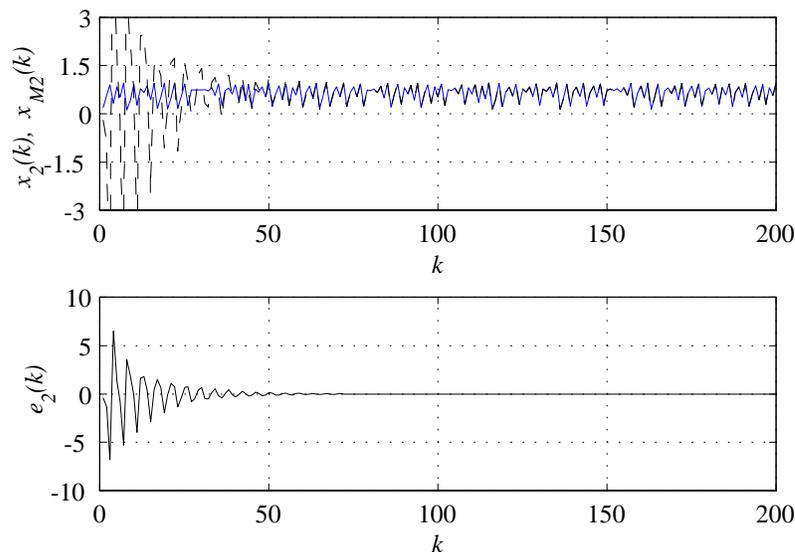


Figura 28: Sincronía (acoplamiento) entre $y(k) = x_2(k)$ e $y_M(k) = x_{M2}(k)$ y la evolución temporal del error de sincronía $e_2(k) = x_2(k) - x_{M2}(k)$ cuando $\alpha_i = 0.75$.

$y(k) = x_2(k)$ e $y_M(k) = x_{M2}(k)$ cuando $\alpha_i = 0.75$ y muestra también, la evolución temporal del error de sincronía $e_2(k) = x_2(k) - x_{M2}(k)$ entre las salidas de (64) y (65); en este caso el tiempo de sincronía fue de $\tau = 91$.

IV.5 Sincronización de sistemas no idénticos

En los ejemplos anteriores se mostró el caso de sincronización de **sistemas idénticos** (maestro y esclavo), para el cual, se obtiene que **sincronización de salida, implica sincronización completa**. El siguiente ejemplo involucra sistemas no idénticos, con el propósito de ilustrar que la metodología adoptada de acoplamiento a modelos, es aplicable exitosamente, aún en este caso de sincronización de salida. Sin embargo,

para este caso, no se obtiene sincronía completa, permaneciendo un error en los demás estados.

Ejemplo 3 (Grassi y Miller, 2002). Considere el siguiente sistema hipercaótico de Hénon como esclavo (planta),

$$P : \begin{cases} x_{M1}(k+1) = 1.76 - x_{M2}^2(k) - 0.1x_{M3}(k), \\ x_{M2}(k+1) = x_{M1}(k), \\ x_{M3}(k+1) = x_{M2}(k) + u_M(k), \\ y_M(k) = x_{M2}(k), \end{cases} \quad (69)$$

además, considere de nuevo el sistema hipercaótico de Rössler del ejemplo 2 como maestro (modelo de referencia),

$$M : \begin{cases} x_1(k+1) = \alpha x_1(k)(1 - x_1(k)) - \beta(x_3(k) + \gamma)(1 - 2x_2(k)) + u(k), \\ x_2(k+1) = \delta x_2(k)(1 - x_2(k)) + \varsigma x_3(k), \\ x_3(k+1) = \eta((x_3(k) + \gamma)(1 - 2x_2(k)) - 1)(1 - \theta x_1(k)), \\ y(k) = x_2(k), \end{cases} \quad (70)$$

el grado relativo tanto del esclavo (69) como del maestro (70) es $d = d_M = 2$, con esto se garantiza que el problema de sincronía definido en (53) se puede resolver de acuerdo con (45). Siguiendo la misma metodología se llega nuevamente a un sistema auxiliar completamente linealizado. Definiendo $\zeta_1(k) = y_E(k) = x_2(k) - x_{M2}(k)$, como nuevas

coordenadas, este sistema en lazo cerrado se expresa

$$\begin{aligned}\zeta_1(k+1) &= y_E(k+1) = \zeta_2(k), \\ \zeta_2(k+1) &= y_E(k+2) = \zeta_3(k), \\ \zeta_3(k+1) &= y_E(k+3) = v(k) = -\alpha_2\zeta_3(k) - \alpha_1\zeta_2(k) - \alpha_0\zeta_1(k).\end{aligned}$$

La ley de control que logra el acoplamiento (sincronía de salida) entre $y(k)$ y $y_M(k)$, está dada por

$$u(k) = 10 \left(1.76 - x_1^2(k) - 0.1(x_2(k)) - a - \phi_M(x_M(k), u_M(k)) \right) \quad (71)$$

donde

$$a = -\alpha_2 \left(1.76 - x_2^2(k) - 0.1x_3(k) \right) - \alpha_1x_1(k) - \alpha_0x_2(k).$$

Por lo que la función no lineal de acoplamiento $\phi_M(x_M, u_M)$ entre maestro y esclavo, es como sigue,

$$\phi_M(x_M(k), u_M(k)) = -(-\alpha_2\rho_1 - \alpha_1\rho_2 - \alpha_0x_{M2}(k)) + \rho_4.$$

donde

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

Y con una adecuada selección de los valores de α_i , se garantiza convergencia del error a cero ($e_2(k) = x_2(k) - x_{M2}(k) \rightarrow 0$). Se realizaron las simulaciones que a continuación se describen.

Se emplearon los siguientes valores para los de parámetros del modelo: $\alpha = 3.8$, $\beta = 0.05$, $\gamma = 0.35$, $\delta = 3.78$, $\varsigma = 0.2$, $\eta = 0.1$, $\theta = 1.9$. Se optó por $u_M(k) = 0$ para garantizar comportamiento hipercaótico del modelo y se tomaron las condiciones iniciales $x(0) = (0.3, 0, 0.05)$ y $x_M(0) = (0.1, 0.2, -0.1)$. También, se eligieron los coeficientes $\alpha_i = 0.1$, $i = 0, 1, 2$.

La figura 29 muestra el acoplamiento entre $y(k) = x_2(k)$ e $y_M(k) = x_{M2}(k)$, además muestra la evolución temporal del error de sincronía de las salidas $e_2(k) = x_2(k) - x_{M2}(k)$ de (64) y (65). Aquí, nuevamente se puede apreciar que trascurrido un tiempo τ se obtiene **sincronía en la salidas**. La figura 30 muestra la evolución

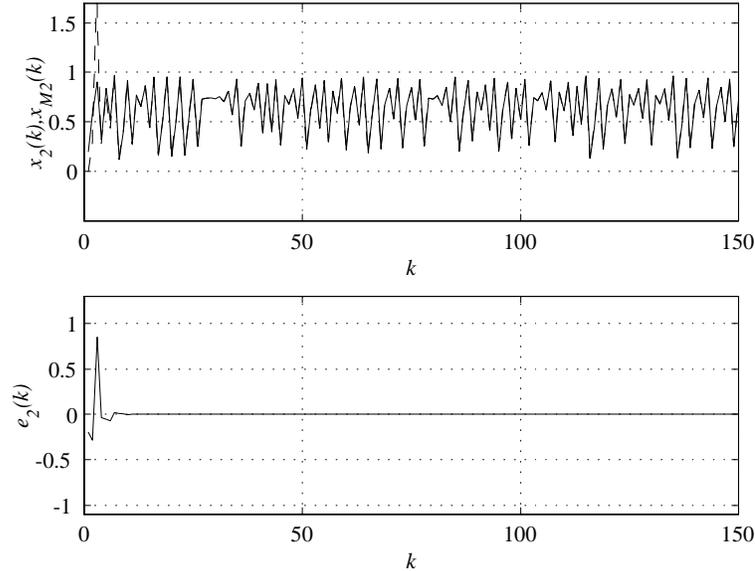


Figura 29: Sincronía (acoplamiento) entre $y(k) = x_2(k)$ (línea punteada) e $y_M(k) = x_{M2}(k)$ (línea continua) y error de sincronía $e_2(k) = x_2(k) - x_{M2}(k)$.

temporal de los errores de los estados restantes $e_1(k) = x_1(k) - x_{M1}(k)$ y $e_3(k) = x_3(k) - x_{M3}(k)$, se observa que dichos errores no convergen a cero, pero permanecen acotados. Es decir, con sistemas maestro y esclavo no idénticos no se tiene **sincronía completa**.

IV.6 Caso perturbado

IV.6.1 Variaciones paramétricas

En los ejemplos mostrados en la sección anterior, los valores de los parámetros tanto del esclavo como del maestro fueron **idénticos**. En esta sección, se presentan resultados

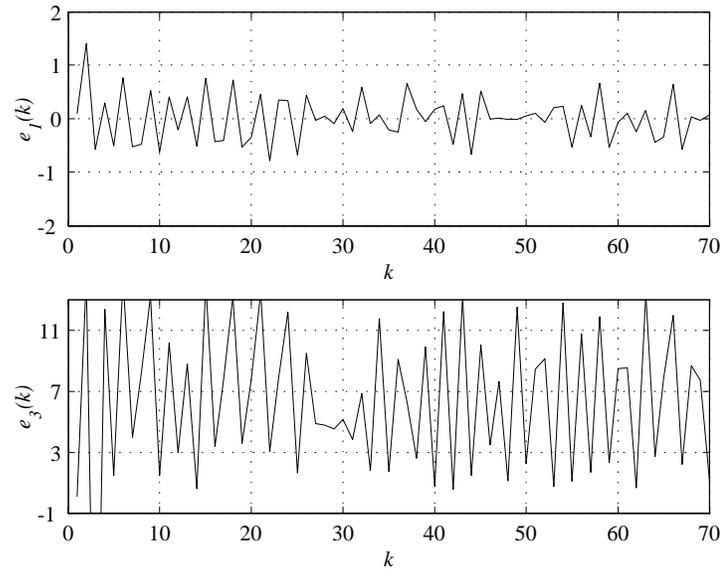


Figura 30: Evolución temporal de los errores de sincronía restantes $e_1(k) = x_1(k) - x_{M1}(k)$ y $e_3(k) = x_3(k) - x_{M3}(k)$.

en simulaciones realizadas cuando los valores de los parámetros en maestro y esclavo son **diferentes**, con el propósito de observar cómo influyen estos cambios en la sincronía de salida.

Para el ejemplo 1, los valores de los parámetros del maestro de referencia se mantienen en $a = 1.95$ y $b = 1$. En el esclavo se cambió el valor a : $a = 2$ y $b = 1.1$. En la figura 31 se observa la evolución temporal de los errores de sincronía $e_1(k) = x_1(k) - x_{M1}(k)$ y $e_2(k) = x_2(k) - x_{M2}(k)$. Se observa que el error de la salida $e_2(k) = x_2(k) - x_{M2}(k)$ converge a cero, es decir, que a pesar de las variaciones paramétricas, **la sincronía en la salida no se pierde**, lo que **se pierde es la sincronía completa**. Si se incrementa la variación paramétrica, aumenta el error $e_1(k)$.

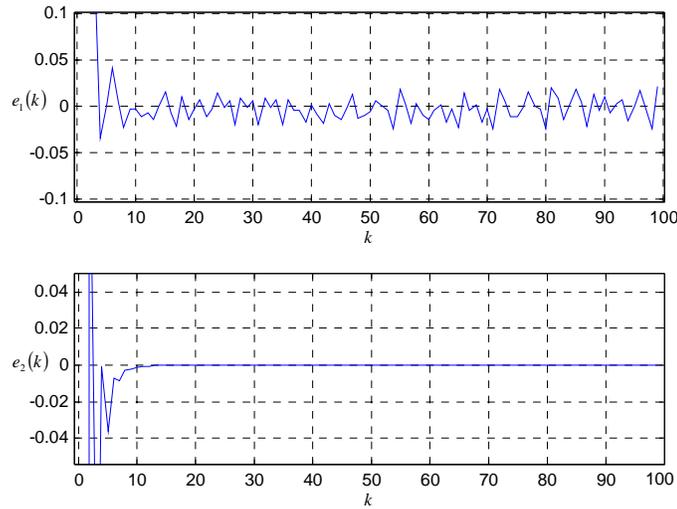


Figura 31: Errores de sincronía $e_1(k) = x_1(k) - x_{M1}(k)$ y $e_2(k) = x_2(k) - x_{M2}(k)$ cuando los parámetros del maestro son $a = 1.95$ y $b = 1$ y en el esclavo son $a = 2$ y $b = 1.1$.

Para el ejemplo 2, valores de los parámetros del maestro se mantienen en: $\alpha = 3.8$, $\beta = 0.05$, $\gamma = 0.35$, $\delta = 3.78$, $\zeta = 0.2$, $\eta = 0.1$, $\theta = 1.9$ y en el esclavo se dejaron los mismos valores y únicamente se modificó el valor del parámetro γ a 0.45. Los resultados se muestran en la figura 32, aquí se observan los errores de sincronía $e_i(k) = x_i(k) - x_{Mi}(k)$, $i = 1, 2, 3$, se puede ver que igual que en el caso anterior, la sincronía en la salida no se pierde, es robusta ante perturbaciones paramétricas. Ocurre lo mismo para $e_3(k)$ y se pierde la sincronía completa con $e_1(k)$ aunque el error permanezca acotado. En la figura 33 se observa que al aumentar la variación en γ a 0.75 también aumenta el error de sincronía $e_1(k)$, sin embargo los errores $e_2(k)$ y $e_3(k)$ continúan convergiendo a cero. Por último, en la figura 34 se modificó el valor del parámetro ζ a 0.3 para el esclavo y se observa como al modificar este parámetro, el

error $e_3(k) = x_3(k) - x_{M3}(k)$ ya no converge a cero, es decir, en este caso se conserva únicamente la sincronía en la salida, la cual, es la única que se garantiza obtener mediante el acoplamiento a modelos.

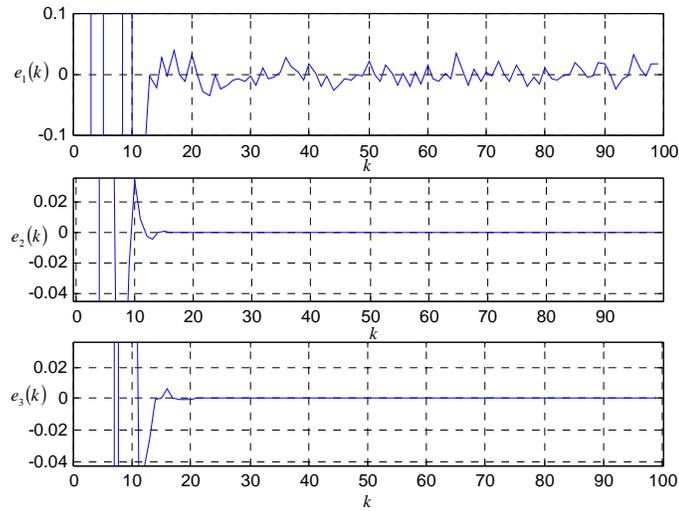


Figura 32: Errores de sincronía $e_i(k) = x_i(k) - x_{Mi}(k)$, $i = 1, 2, 3$ cuando el parámetro γ del maestro es 0.35 y en el esclavo es $\gamma = 0.45$.

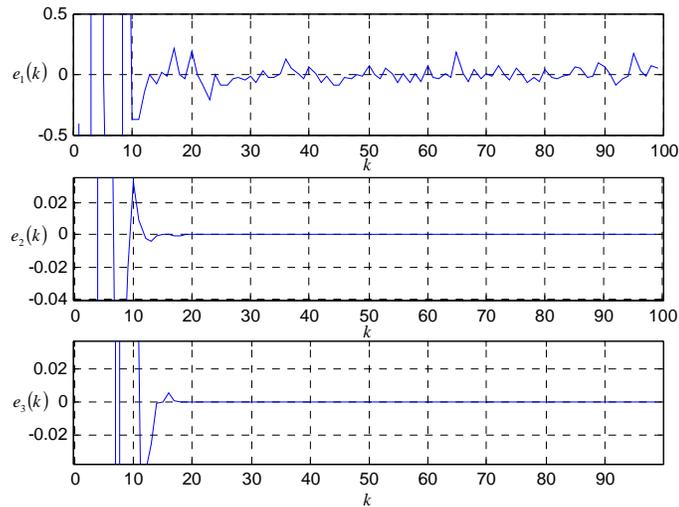


Figura 33: Errores de sincronía $e_1(k) = x_1(k) - x_{M1}(k)$, $e_2(k) = x_2(k) - x_{M2}(k)$ y $e_3(k) = x_3(k) - x_{M3}(k)$ cuando el parámetro γ del maestro es 0.35 y en el esclavo es $\gamma = 0.75$.

IV.7 Resumen

Se empleó la metodología de control de acoplamiento a modelos con el propósito de sincronizar sistemas discretos con dinámicas extremadamente complejas, es decir, sistemas que pueden exhibir comportamiento caótico e hipercaótico. Los resultados obtenidos con respecto a la sincronización principalmente son:

- Para maestro y esclavo idénticos, se obtiene sincronización de salida y sincronización completa.
- Para maestro y esclavo no idénticos, se obtiene sincronización de salida con errores acotados en el resto de los $n - 1$ estados.

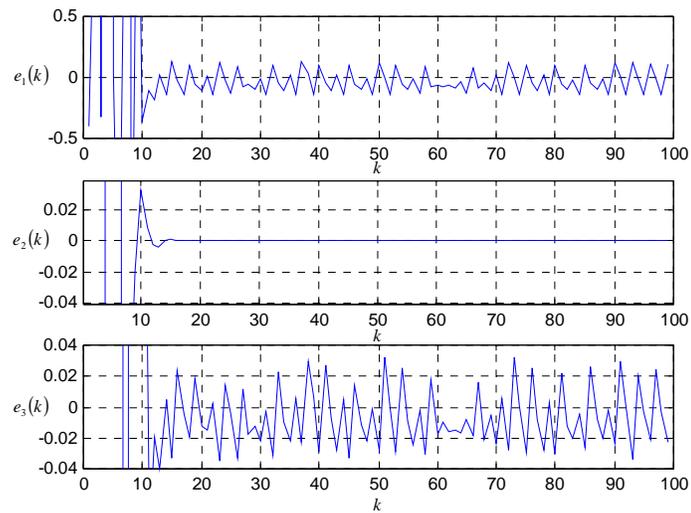


Figura 34: Errores de sincronía $e_i(k) = x_i(k) - x_{M1}(k)$, $i = 1, 2, 3$ cuando el parámetro ς del maestro es 0.2 y en el esclavo es $\varsigma = 0.3$.

- Robustez en la sincronización de salida ante variaciones paramétricas.

En el siguiente capítulo, se mostrará la aplicación de algunos de los resultados obtenidos y empleando los mismos ejemplos, a la codificación de información confidencial en sistemas de comunicaciones.

Capítulo V

Aplicación a Comunicaciones

Privadas

En el mundo de las comunicaciones, las ventajas que el caos puede proporcionar a dicho campo, todavía no han sido explotadas ampliamente, algunas a destacar como la seguridad en la transmisión de datos, conseguida con la transmisión de voz usando señales caóticas y también, el aumento del número de usuarios que pueden emplear un mismo canal, característica que resulta altamente beneficiosa en las comunicaciones móviles y que ha sido estudiada para CDMA (por sus siglas en inglés, esquema de acceso múltiple por división de códigos), donde la generación de códigos para usuarios se hace mediante la codificación de una variable caótica, alcanzando una cantidad de códigos muy superior a las que se obtienen con generadores tradicionales.

Durante los últimos quince años la sincronización de oscilaciones caóticas se convir-

tió en uno de los tópicos más intensamente estudiado en sistemas dinámicos y tópicos afines. Este hecho fue principalmente estimulado por el trabajo realizado en [Pecora y Carroll, 1990]. Una razón del éxito del método propuesto por Pecora y Carroll fue probablemente el hecho de que, por primera vez, se mencionó la posibilidad de emplear la sincronía de osciladores acoplados unidireccionalmente, en sistemas de comunicación privada/segura basados en caos. Lograda la sincronía de una pareja de osciladores caóticos, ésta puede emplearse en diferentes formas para codificar o encriptar información confidencial. Diferentes implementaciones de este principio general se han reportado en la literatura, algunos ejemplos son: **encriptamiento caótico aditivo, conmutación entre atractores caóticos y modulación paramétrica, etc.**

Con el propósito de mostrar algunas aplicaciones de la sincronización de sistemas caóticos, obtenida de acuerdo a la metodología de acoplamiento a modelos, en un escenario de acoplamiento maestro y esclavo, se presenta a continuación su potencial empleo en la codificación de información confidencial para sistemas de comunicaciones privadas/seguras.

V.1 Comunicación por conmutación entre dos atractores caóticos

En este método el mensaje $m(k)$ es una señal binaria, que se utiliza para modular uno o más parámetros del transmisor, es decir, $m(k)$ controla un interruptor cuya

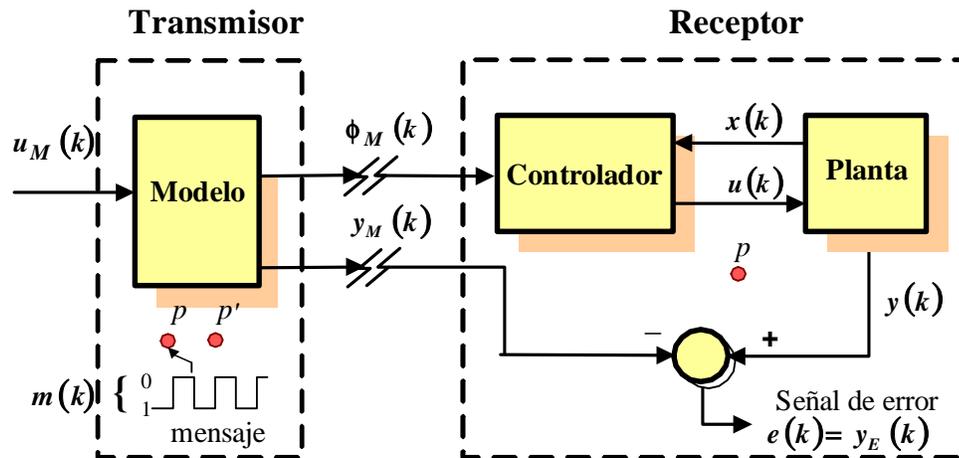


Figura 35: Esquema de comunicación privada empleando sincronía de salida por acoplamiento a modelos.

acción cambia los valores de los parámetros del transmisor. Por lo que, de acuerdo al valor de $m(k)$ en algún tiempo dado k , el transmisor posee un conjunto de valores de parámetros p o un conjunto de valores de parámetros p' .

En el receptor, $m(k)$ es decodificado utilizando el error de sincronía para decidir cuando la señal recibida corresponde a un conjunto de valores de parámetros o a otro (estas acciones pueden interpretarse como la recepción de un "cero" o de un "uno").

La figura 35 muestra la configuración para llevar a cabo la conmutación entre dos atractores caóticos, a continuación se muestra un ejemplo para ilustrar este esquema de comunicación de información cifrada.

Utilizando el ejemplo 3 de sincronización de sistemas no idénticos mostrado en el capítulo anterior, se eligen como parámetros a modificar el valor del parámetro α_0 establecido en el sistema maestro. Recuérdese que α_0 es un "parámetro" de la función

$\phi_M(k)$ generada por el modelo de acuerdo al capítulo anterior y que para obtener sincronía, dichos valores deben ser **iguales** tanto en transmisor como en el receptor. Se conmutó α_0 de 0.1 a 0.2 para codificar y enviar información binaria. La señal $u_M(k) = 0$ para asegurar el comportamiento hipercaótico de la señal transmitida. Además, si esto no fuera así y $u_M(k) \neq 0$, se corre el riesgo de no distinguir el momento en que conmutan los valores en los parámetros (dependiendo de las características de $u_M(k)$).

La figura 36 muestra el parámetro conmutado $a_0(k)$ utilizado para enviar codificada la información binaria. Además, se muestra la señal enviada $\phi_M(x_M(k), p, p')$ del transmisor al receptor, se observa que el mensaje enviado se oculta de manera satisfactoria. También, muestra el mensaje recuperado (error de sincronía) que puede interpretarse como "0" ó "1", dicho error de sincronía está dado por

$$e(k) = y(x(k); \alpha_i) - y_M(x(k); \alpha_i, \alpha'_i).$$

El motivo de no variar parámetros de las ecuaciones del modelo es que como se mostró en el capítulo anterior, la sincronía es **robusta** ante perturbaciones paramétricas, por lo que la sincronía se pierde sólo por instantes pequeños y únicamente se detecta el momento del cambio de parámetro (aunque no siempre es tan claro) pero no surge de manera tan evidente el mensaje. Este caso se ilustra en la figura 37 donde el parámetro a conmutar fue γ de 0.35 a 0.45. Se nota que en el instante $k = 100$ el error es muy pequeño haciendo difícil la detección del mensaje.

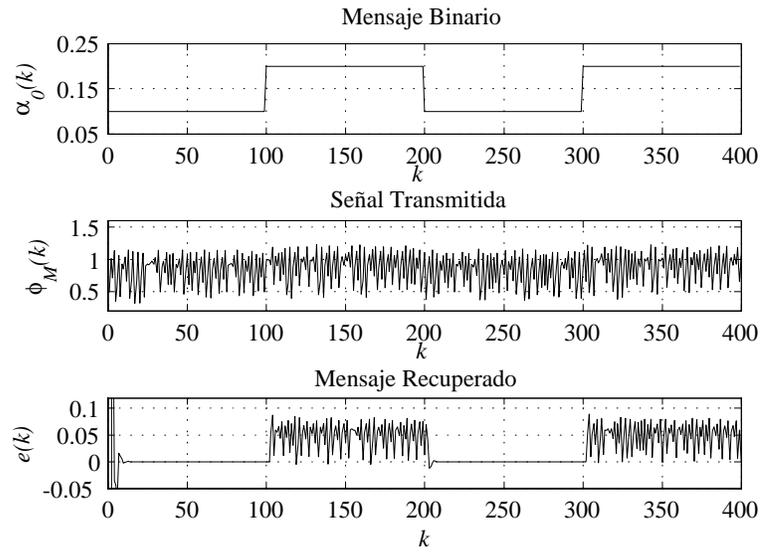


Figura 36: Transmisión de una señal binaria por medio de conmutación entre atractores hipercaóticos. Parámetro $a_0(k)$ (mensaje binario), Señal transmitida $\phi_M(k)$ y señal de error $e(k) = y(k) - y_M(k)$ (mensaje recuperado).

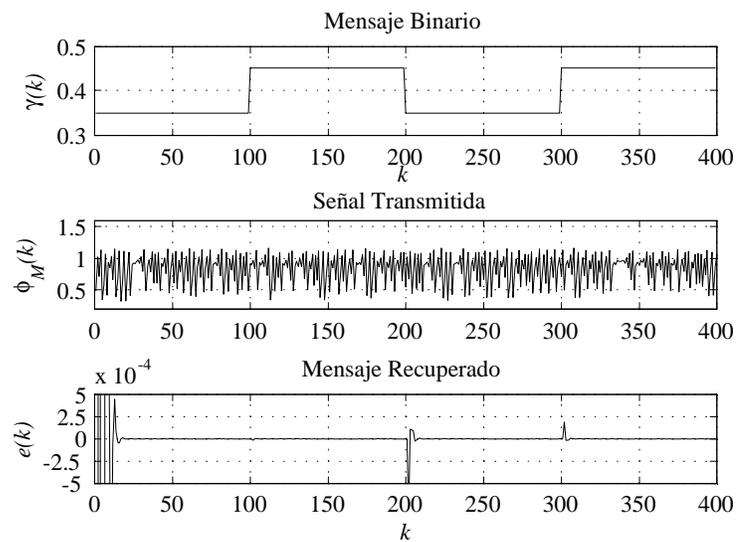


Figura 37: Transmisión de una señal binaria por medio de conmutación entre atractores hipercaóticos. Parámetro $\gamma(k)$ (mensaje binario), Señal transmitida $\phi_M(k)$ y señal de error $e(k) = y(k) - y_M(k)$ (mensaje recuperado).

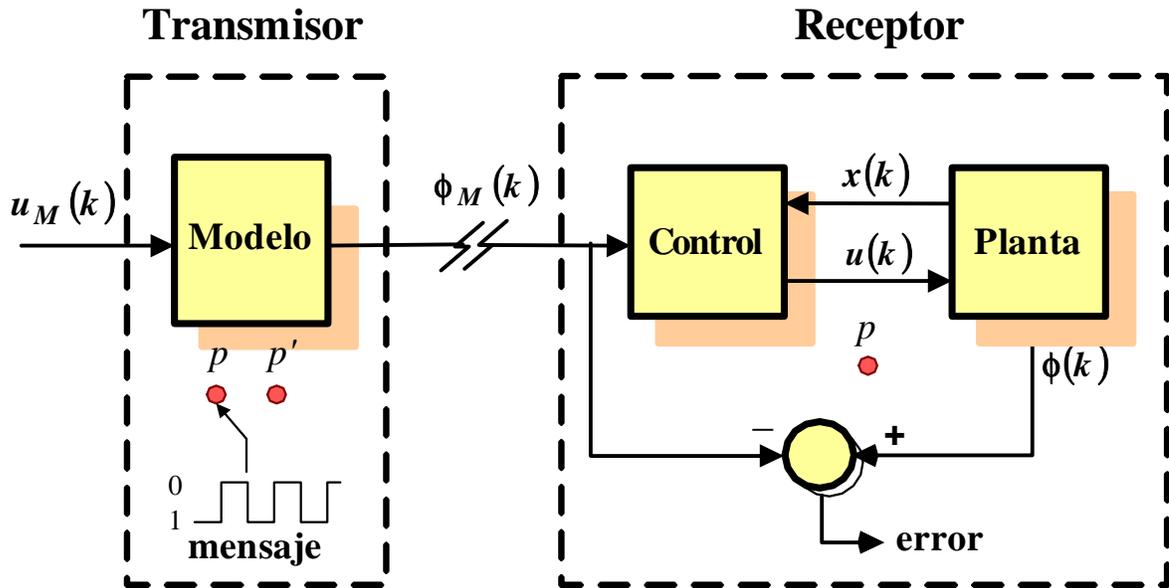


Figura 38: Esquema de comunicación privada empleando una línea de transmisión.

V.1.1 Caso particular

Para el caso particular, en que las siguientes condiciones se cumplan:

- Sistemas hipercaóticos idénticos en transmisor y receptor,
- $u_M(k) = 0$

Se puede utilizar la conmutación paramétrica modificando el esquema anterior por el que se presenta en la figura 38 con la ventaja de que se reduce el número de canales, aquí se observa que el error que se obtiene es la diferencia entre $\phi_M(k)$ y una señal $\phi(x(k), p)$ en el receptor, con

$$\phi(x(k), p) = \phi_M(x_M(k), u_M(k), p)|_{x_M=x},$$

esta señal es necesaria para hacer una comparación con $\phi_M(x_M(k), p, p')$ y obtener un error $e_\phi(k)$ que ayude a detectar el mensaje cuando los valores de los parámetros en el maestro M cambien. Para el ejemplo 1 del capítulo anterior la función no lineal $\phi(x(k), p)$ está dada por

$$\begin{aligned} \phi(x(k), p) = & \alpha_0 x_2(k) - 2\alpha_1 a b x_1(k) x_2(k) \\ & - 2ab [1 - a(x_1^2(k) + x_2^2(k))] (-2ab x_1(k) x_2(k)). \end{aligned}$$

En este caso se utilizaron las mismas condiciones presentadas en el ejemplo 1 del capítulo anterior y el parámetro que se conmutó fue a de 1.95 a 1.85 para codificar y enviar información binaria. La señal $u_M(k) = 0$ para asegurar el comportamiento hipercaótico de la señal transmitida. Además, si esto no fuera así y $u_M(k) \neq 0$ se corre el riesgo de no distinguir el momento en que conmutan los parámetros (dependiendo de las características de $u_M(k)$) o bien, en el receptor se tendría que conocer el valor de la señal $u_M(k)$ para poder recuperar el mensaje, lo cual, implica la necesidad de incrementar el número de canales de transmisión.

La figura 39 muestra el parámetro conmutado $a(k)$ utilizado para enviar información binaria. Además, se muestra la señal enviada $\phi_M(x_M(k), p, p')$ del trasmisor hacia el receptor, se observa que el mensaje enviado se oculta de manera satisfactoria. También, muestra el mensaje recuperado (error de sincronía) que puede interpretarse como "0"

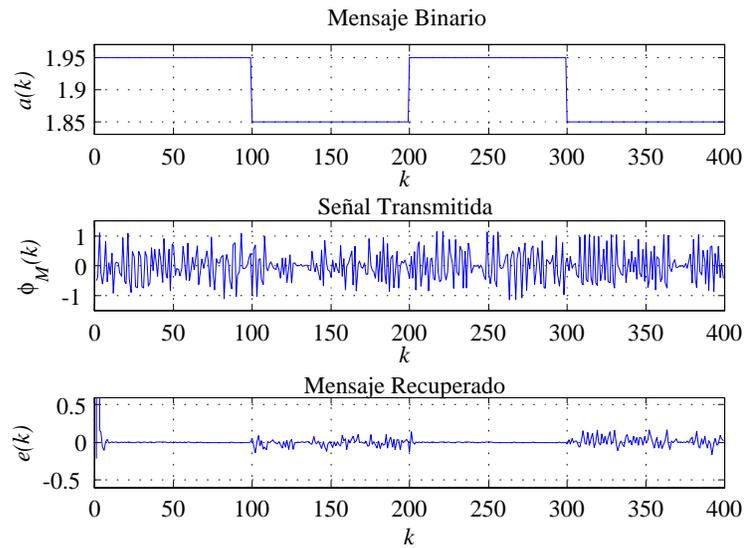


Figura 39: Transmisión de una señal binaria por medio de conmutación entre atractores hipercaóticos. Parametro $a(k)$ (mensaje binario), Señal transmitida $\phi_M(k)$ y señal de error $e(k) = \phi_M(k) - \phi(k)$ (mensaje recuperado).

ó "1", dicho error de sincronía está dado por

$$e_\phi(k) = \phi_M(x_M(k), p, p') - \phi(x(k), p).$$

El mensaje transmitido $m(k)$ y el mensaje recuperado $\hat{m}(k) = e_\phi(k)$ en la figura 39 pueden interpretarse como sigue en el caso particular de esta simulación:

$$m(k) = \begin{cases} 1 & \text{para } a(k) = 1.95, & 0 \leq k < 100 \\ 0 & \text{para } a(k) = 1.85, & 100 \leq k < 200 \\ 1 & \text{para } a(k) = 1.95, & 200 \leq k < 300 \\ 0 & \text{para } a(k) = 1.85, & 300 \leq k < 400 \end{cases}$$

Codificación

y

$$\hat{m}(k) = \begin{cases} e(k) = 0, & 0 \leq k < 100 \rightarrow 1 \\ e(k) \neq 0, & 100 \leq k < 200 \rightarrow 0 \\ e(k) = 0, & 200 \leq k < 300 \rightarrow 1 \\ e(k) \neq 0, & 300 \leq k < 400 \rightarrow 0 \end{cases}$$

Decodificación

Para el ejemplo 2 se utilizó $\alpha_i = 0.2$, $i = 0, 1, 2$ las condiciones iniciales fueron $x_M(0) = (0.1, 0.2, -0.1)$, $x(0) = (0.4, 0.5, -0.4)$ para el maestro y el esclavo, respectivamente. El parámetro conmutado fue γ de 0.35 a 0.45. La figura 40 muestra el mensaje enviado $m(k) = \gamma(k)$, la señal transmitida $\phi_M(x_M(k), p, p')$ y el mensaje recuperado $\hat{m}(k) = e_\phi(k)$. De nuevo, el mensaje enviado $m(k)$ y el mensaje recuperado

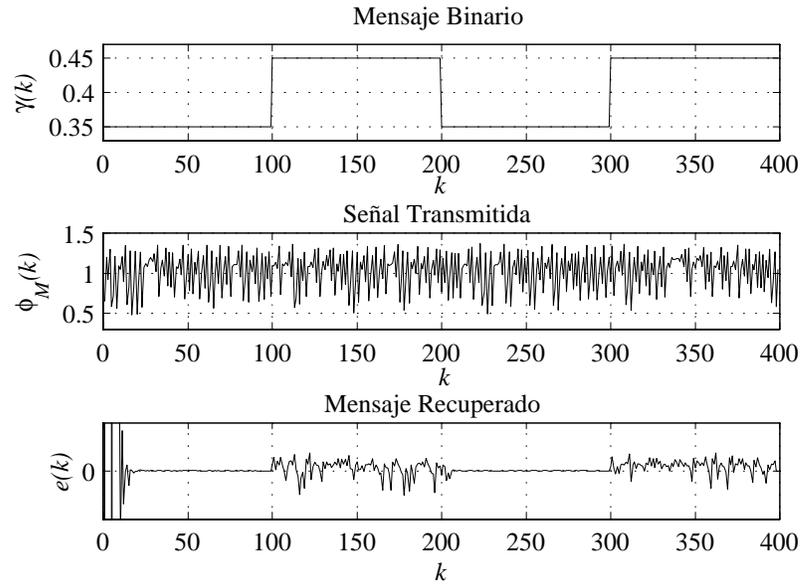


Figura 40: Parámetro $\gamma(k)$, señal transmitida $\phi_M(k)$ y error $e(k) = \phi_M(x_M(k), p, p') - \phi(x(k), p)$.

$\hat{m}(k)$ pueden interpretarse como sigue:

$$m(k) = \begin{cases} 0 & \text{para } \gamma(k) = 0.35, & 0 \leq k < 100 \\ 1 & \text{para } \gamma(k) = 0.45, & 100 \leq k < 200 \\ 0 & \text{para } \gamma(k) = 0.35, & 200 \leq k < 300 \\ 1 & \text{para } \gamma(k) = 0.45, & 300 \leq k < 400 \end{cases}$$

y

$$\hat{m}(k) = \begin{cases} e(k) = 0 & 0 \leq k < 100 \rightarrow 0 \\ e(k) \neq 0 & 100 \leq k < 200 \rightarrow 1 \\ e(k) = 0 & 200 \leq k < 300 \rightarrow 0 \\ e(k) \neq 0 & 300 \leq k < 400 \rightarrow 1 \end{cases}$$

Si bien en esta configuración se observa como ventaja el hecho de utilizar una sólo línea de transmisión, también se tiene que dicha línea está dedicada al envío exclusivo de señales binarias como mensajes. En las siguientes secciones se presentan dos esquemas de comunicación por medio de los cuales pueden enviarse señales de audio entre otras, como mensajes encriptados.

V.2 Encriptamiento aditivo

En esta sección, se presenta una configuración conocida para el envío de mensajes discretos más complejos, este esquema emplea dos canales de transmisión: uno se dedica a enviar la señal para sincronizar transmisor y receptor (en este caso dicha señal es $\phi_M x_M(k), u_M(k)$), mientras que el otro canal, se reserva para el envío del mensaje encriptado (por ejemplo, sumándolo a algún estado o función proporcionada por el transmisor hipercaótico), en este caso se empleó la suma del mensaje con la salida del transmisor como forma de encriptar el mensaje. La figura 41 muestra la configuración para encriptamiento aditivo empleando dos líneas de transmisión con base en sincronía por acoplamiento a modelos.

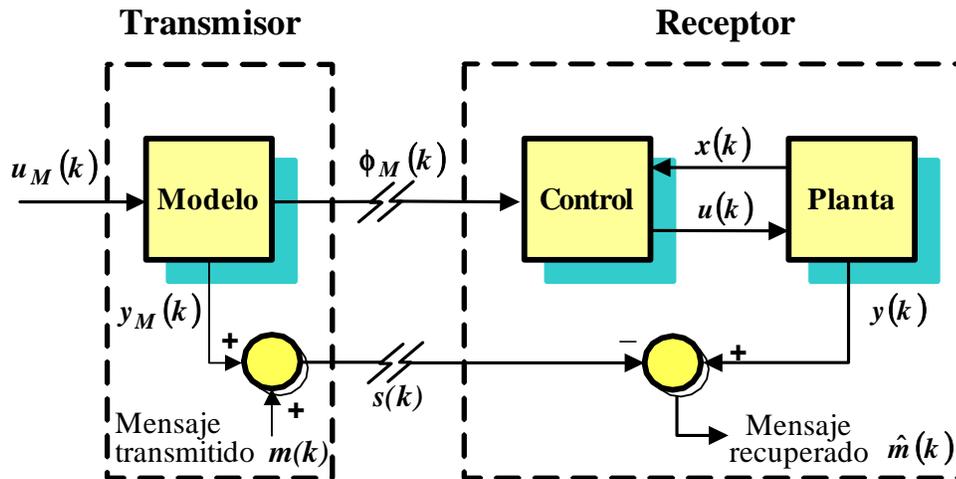


Figura 41: Encriptamiento aditivo empleando dos líneas de transmisión.

Como mensaje transmitido $m(k)$ se seleccionó una señal senoidal $m(k) = 0.07\text{sen}(0.5k) + 0.05\text{sen}(0.3k)$, la señal transmitida que oculta el mensaje está dada por $s(k) = y_M(k) + m(k)$ y el mensaje recuperado $\hat{m}(k)$ se obtiene de la siguiente forma

$$\hat{m}(k) = s(k) - y(k).$$

En la figura 42 se muestra el mensaje $m(k)$, la señal de transmisión $s(k)$ (con mensaje oculto) y el mensaje recuperado del cual se observa que después de un lapso de tiempo τ (tiempo de sincronía) se obtiene excelente recuperación del mensaje. Este lapso de tiempo está dado por τ y puede modificarse cambiando los valores de α_i , $i = 0, 1, 2$ como se comentó en secciones anteriores. La figura 43 muestra los mismos resultados para el ejemplo 2 del capítulo anterior, en este caso, utilizando como mensaje una señal de audio (la palabra "cuatro").

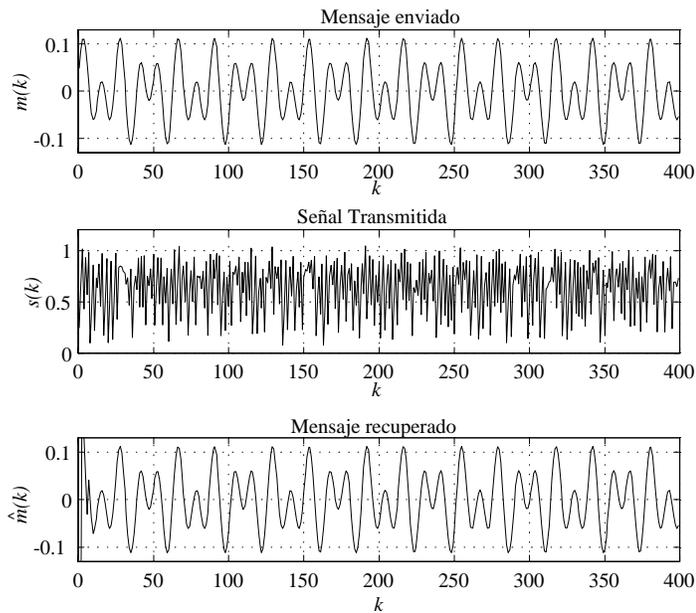


Figura 42: Mensaje original $m(k)$, señal de transmisión $s(k) = y_M(k) + m(k)$ y mensaje recuperado $\hat{m}(k) = s(k) - y(k)$.

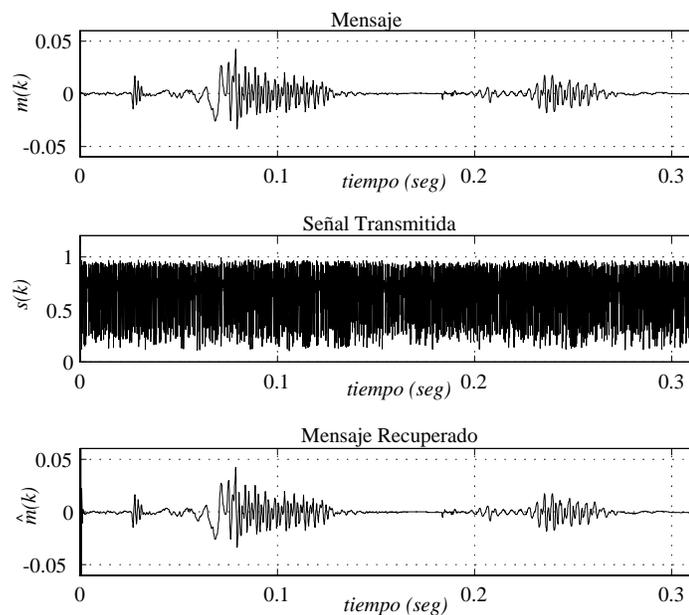


Figura 43: Mensaje original $m(k)$, señal de transmisión $s(k) = y_M(k) + m(k)$ y mensaje recuperado $\hat{m}(k) = s(k) - y(k)$.

En ambos ejemplos se utilizó $u_M(k) = 0$ para hacer más sencillo el tratamiento, sin embargo, en general es necesario cuidar su valor para conservar el comportamiento hipercaótico del transmisor que pudiera llegar a perderse con $u_M(k)$. En la siguiente sección se presenta otro esquema de comunicación empleando una sola línea de transmisión.

V.3 Encriptamiento por Modulación

Otra configuración para el envío de señales discretas más compleja se presenta en la figura 44. Aquí se utiliza únicamente un canal de transmisión, el mensaje se coloca en la señal de entrada del modelo M , es decir,

$$m(k) = u_M(k),$$

de este modo, el mensaje se oculta al ser modulado por la dinámica del modelo.

Se utilizó como mensaje una señal senoidal dada por $m(k) = u_M(k) = 0.01\text{sen}(0.3k)$ para el ejemplo 1 y para el ejemplo 2 el mensaje es una señal de voz con la palabra "cuatro". La señal $\hat{m}(k)$ se reconstruye en el receptor por la expresión dada a continuación

$$\hat{m}(k) = G(x, p) [\phi_M(x_M(k), u_M(k)) - \phi(x(k))],$$

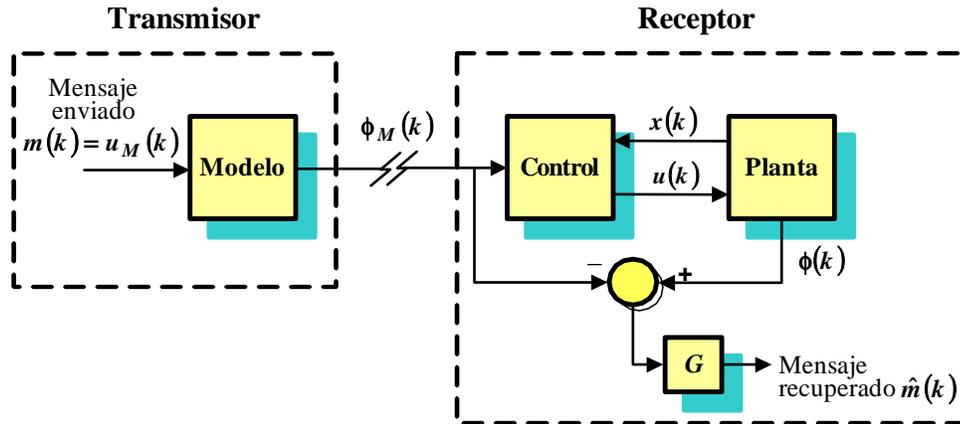


Figura 44: Esquema de comunicación con una línea de transmisión.

donde $\phi_M(x_M(k), u_M(k))$ se definió anteriormente y

$$\phi(x(k)) = \phi_M(x_M(k), u_M(k))|_i G(x, p)$$

es una expresión necesaria para obtener $\hat{m}(k)$ proveniente de la ecuación (56), para el ejemplo 1 la función $G(x, p)$ está dada por

$$G(x, p) = 4a^2b^2x_1(k)x_2(k),$$

y para el ejemplo 2 la expresión está dada por

$$G(x, p) = \theta c,$$

con

$$c = \varsigma \eta \left(\left(\eta \left((x_3 + \gamma) (1 - 2x_2) - 1 \right) (1 - \theta x_1) \right) + \gamma \right) (1 - 2(\delta x_2 (1 - x_2) + \varsigma x_3) - 1) .$$

Las figuras 45 y 46 muestran los resultados obtenidos utilizando esta configuración para los ejemplos 1 y 2, respectivamente. Con este esquema de comunicación, se obtiene nuevamente buena reconstrucción del mensaje $m(k)$ transcurrido el tiempo de sincronía. Sin embargo, se recomienda cuidado en la elección de los mensajes, pues se pudiera perder el comportamiento hipercaótico del transmisor, el cual, es deseable para encriptar la información de manera más confiable.

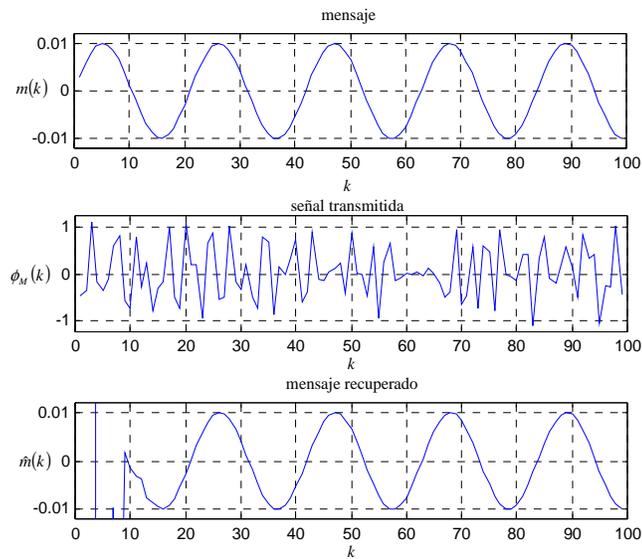


Figura 45: Mensaje $m(k)$, señal transmitida $\phi_M(k)$ y mensaje recuperado.

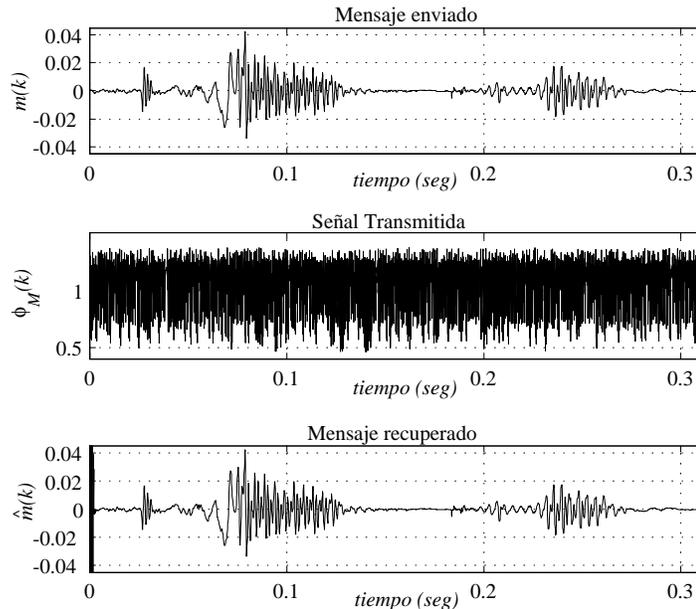


Figura 46: Mensaje $m(k)$ (señal de audio), señal transmitida $\phi_M(k)$ y mensaje recuperado.

V.4 Resumen

Se presentaron tres esquemas para el encriptado de información confidencial, con base en sincronía de salida por acoplamiento a modelos. De los esquemas presentados, el de comunicación por conmutación entre dos atractores hipercaóticos tiene la desventaja de que el envío de información binaria, tiene una velocidad de respuesta a considerar que depende del tiempo de sincronía. Entre los esquemas de encriptamiento por una línea y dos líneas, en los que se pueden enviar señales discretas más complejas, el de una línea tiene la clara ventaja de que utiliza menos canales de transmisión (factor económico), aunque al tener que enviar el mensaje por medio de $u_M(k)$, tiene la desventaja de limitar el tipo de señales que se envían principalmente en magnitud, pues puede perderse el

comportamiento hipercaótico del modelo de referencia en el transmisor.

Con los esquemas de comunicación de codificación presentados, se incrementa la seguridad o al menos la privacidad por el hecho de utilizar dinámicas extremadamente complejas (hipercaos) para el encriptado.

Capítulo VI

Conclusiones generales

En este trabajo de tesis doctoral se presentó la **sincronización aproximada** de sistemas hipercaóticos discretos, empleando como sistema esclavo un **filtro extendido de Kalman**. Se determinaron condiciones para el error inicial y el ruido que garantizan la convergencia de la esperanza del error $e(k)$ a una cota ρ . Esta metodología de trabajo se aplicó satisfactoriamente a dos sistemas discretos particulares, uno caótico y otro hipercaótico.

También se empleó la metodología de control de **acoplamiento a modelos** con el propósito de **sincronizar sistemas discretos caóticos e hipercaóticos** obteniéndose sincronización de salida y, bajo ciertas condiciones también lográndose **sincronización completa**.

Se presentaron tres esquemas para el encriptado de información confidencial, con base en sincronía de salida por acoplamiento a modelos. Logrando codificar tanto

señales binarias como de audio, de manera más segura que empleando los mismos esquemas de transmisión, pero empleando "simple" caos.

Las principales aportaciones que arrojó este trabajo doctoral se resumen a continuación:

- Se propuso una forma de obtener sincronía de sistemas hipercaóticos discretos, basada en el empleo del filtro extendido de Kalman, y se establecieron condiciones para sincronización aproximada.
- Se diseñaron controladores basados en el acoplamiento a modelos para sincronizar la salida de dos sistemas hipercaóticos discretos.
- Bajo ciertas condiciones, se obtuvo la manera sistemática de obtener sincronización completa utilizando acoplamiento a modelos.
- Se obtuvo robustez en la sincronización de salida ante variaciones paramétricas (por acoplamiento a modelos).
- Se aplicó la sincronización de salida de sistemas hipercaóticos (acoplamiento a modelos) en el campo de la comunicación segura/privada, recurriendo a tres esquemas distintos.
- Por el empleo de sistemas hipercaóticos, se incrementó la seguridad en la codificación para la transmisión de información confidencial.

VI.1 Problemas abiertos

A continuación, se menciona brevemente algunos problemas abiertos detectados y que representan posible trabajo a futuro en esta dirección:

- Experimentación de la sincronía con los métodos propuestos (filtro extendido de Kalman y acoplamiento a modelos) para validar los resultados teóricos obtenidos.
- Aplicación de la sincronización mediante el uso del filtro de Kalman a comunicación privada (ruido en el canal de transmisión).
- Empleo de alguna variante del filtro extendido de Kalman con el fin de poder incrementar los valores de las condiciones que aseguren la sincronía de sistemas hipercaóticos.
- Ante escenarios ruidosos, explorar el empleo de otros estimadores probabilísticos (filtros), en la sincronía aproximada.
- Diseño de observadores no lineales para el estado del maestro e incorporarlo al controlador, en la sincronía de salida por acoplamiento a modelos.
- Analizar de manera formal el caso perturbado utilizando el acoplamiento a modelos.
- Realizar criptoanálisis a los sistemas de cifrado propuestos.

Literatura Citada

Afraimovich V.S., Verichev N.N. y Rabinovich M.I. 1986. "Stochastic synchronization of oscillation in dissipative system", *Radiophys. Quantum Electron.* 29, 795-803 p.

Álvarez Gallegos J. 2001. "Sistemas Caóticos. Notas de Curso". CINVESTAV Guadalajara, Jal.

Brucoli M., Cafagna D., Carmineo L. y Grassi G. 1998. "Synchronization of hyperchaotic circuits via continuous feedback control with application to secure communications," *Int. J. Bifurcation and Chaos* 8(10), 2031-2040 p.

Chen G. y Dong X. 1998. "From Chaos to Order—Perspectives, Methodologies, and Applications". World Scientific Pub. Co. Singapore.

Chen L.Q. 2001. "An open plus closed loop control for discrete chaos and hyperchaos" *Physics Letters A*, 281(5), 327-333 p.

Cruz Hernández C. 1995. "Stability of discrete nonlinear systems under regular perturbations", Ph D.Thesis CINVESTAV-IPN, México.

Cruz Hernández C. y Alvarez Gallegos J. 1995. "Stability analysis of nonlinear model matching for a class of perturbed discrete-time systems", *Procs. of NOLCOS'95*, Tahoe City, CA, USA, pp. 422-427 p.

Cruz Hernández C., Alvarez Gallegos J. y Castro R. 1999. "Stability of discrete nonlinear systems under nonvanishing perturbations: application to a nonlinear model matching problem", *IMA J. Math. Control & Information*, 16, 23-41 p.

Cruz Hernández C. y Nijmeijer, H. 1999. "Synchronization through extended Kalman filtering", *New Trends in Nonlinear Observer Design*, eds. Nijmeijer, H. & Fossen, T. I., *Lecture Notes in Control and Information Sciences* 244 (Springer-Verlag), 469-490 pp.

Cruz Hernández C. y Nijmeijer H. 2000. "Synchronization through filtering", *Int. J. Bifurcation and Chaos*, 10(4), 763-775 p.

Cruz Hernandez C., Posadas Castillo C., Sira Ramírez H. 2002. "Synchronization of two hyperchaotic Chua circuits: a Generalized Hamiltonian systems approach", 15th Triennial World Congress of the International Federation of Automatic Control. IFAC.

Cruz C. y Romero N. 2005 "Communicating confidential information via synchronized time-delay Chua's circuits", Procs. of the WSEAS International Conference IMCCAS'05, 11-14 de mayo de 2005, Cancún, México.

Cruz-Hernández C. y Serrano H. 2005 "Cryptosystems based on synchronized chua's circuits", Procs. of the 16th IFAC World Congress, Praga, República Checa.

Cruz Hernández C. 2006. "Synchronization of oscillations: Application to chaotic communications", Cambridge Scientific Publishers Ltd.

Cuomo K.M., Oppenheim y Strogatz S.H. 1993. "Synchronization of Lorenz-based chaotic circuit with applications to communications, " IEEE Trans. Circuits Syst. II 40, 626-633 p.

Dedieu H., Kennedy M.P. y Hasler M. 1993. "Chaotic shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits", IEEE Trans. Circuits Syst. II 40, 634-642 p.

Deyst J. Jr. y Price C., 1968. "Conditions for Asymptotic Stability of the Discrete Minimum-Variance Linear Estimator", IEEE Trans. Aut. Control, 702-705.

Di Benedetto M.D. e Isidori A. 1986. "The matching of nonlinear models via dynamics state feedback", SIAM J. of Control and Optimization, 24, pp. 1063-1075 p.

Ding M. y Ott E. 1994. "Enhancing synchronism of chaotic systems", Physical Review E, 49 (2), 945-948 p.

Díaz E., Gámez L., Ayala P., C. Cruz y Núñez R. 2003 "Sincronización de atractores con múltiples enrollamientos y una aplicación a la comunicación secreta", Memorias del Congreso Nacional de Control Automático de la AMCA2003, 15-17 de octubre, Ensenada B.C., México.

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

Fujisaka H., y Yamada T. 1983. "Stability Theory of Synchronized Motion in Coupled-Oscillator Systems", Prog. Theor. Phys. 69(1), 32-47 p.

Gámez L., C. Cruz y Núñez R. (2004) "Sincronización de atractores con enrollamientos de 3x3 en cuadrícula 2D: aplicación a la comunicación secreta", Memorias del Congreso Latinoamericano de Control Automático, 10-15 de mayo 2004, La Habana, Cuba.

Grassi G. y Mascolo S. 1998. "Synchronization of hyperchaotic oscillators using a scalar signal", IEE Electron. Lett. 34, 424-425 p.

Grewal M. y Andrews A. 1993. "Kalman Filtering, Theory and Practice". Prentice Hall. Primera Edición. New Jersey. 381 pp.

Grizzle J. W. 1985. "Controlled invariance for discrete time nonlinear systems with an application to the disturbance decoupling problem", IEEE Trans. AC, 30, 866-874 p.

Hai W. y Jiandong H. 1997. "Chaotic Spread-Spectrum Communication Using Discrete-Time Synchronization", *J.of China Universities of Posts and Telecommunications*,. 4 (1), 66-69 p.

Hasler M. 1995. "Engineering chaos for encryption and broadband communication", *Phil. Trans. R. Soc. Lon. A*, 353, 115-126.

He R., y Vaidya P.G. 1992. "Analysis and synthesis of synchronous periodic and chaotic systems", *Phys. Rev. A* 46(12), 7387-7392 p.

Huijberts, H. J. C., Nijmeijer, H. y Pogromsky, A. Yu. 1999b. "Discrete time observers and synchronization", *Controlling Chaos and Bifurcations in Engineering Systems*, ed. Chen, G. (CRC Press, Boca Raton).

Hunt E.R. 1991. "Stabilizing high-period orbits in a chaotic system: The diode resonator", *Phys. Rev. Lett.* 67(15), 1953-1955.

Itoh M., Yang T. y Chua L.O.2001. "Conditions for impulsive synchronization of chaotic and hyperchaotic systems", *Int. J. Bifurcation and Chaos*, 11(2), 551-560 p.

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

Kolumban G., Kennedy M.P. y Chua L.O. 1997. "The role of synchronization in digital communications using chaos", *IEEE Trans. Circuits Syst. I* 44(10), 927-935.

Kotta U. 1989. "Matching a nonlinear discrete-time system with a prescribed linear input-output behavior", *Aut. and Rem. Control*, 49, 1286-1292 p.

Kotta U. 1995 "Inversion method in the discrete-time control systems synthesis problems", *Lecture notes in Control and Information Sciences*, Springer-Verlag, Berlin, 205 pp.

La Scala B., Bitmead R. y James M. 1995. "Conditions for Stability of Extended Kalman Filter and Their Application to the Frequency Tracking Problem", *Mathematics of Control, Signals and Systems*, 8, 1-26 p.

Lian K, Chiang T. y Liu P. 2000. "Discrete-time chaotic systems applications in secure communications", *Int. J. Bifurcation and Chaos*, 10(9), 2193-2206 p.

López Mancilla D. y Cruz-Hernández C. 2004. "An analysis of robustness on the synchronization of chaotic systems under nonvanishing perturbations using sliding modes", *WSEAS Transactions on Mathematics*, 3(2), pp. 364-369

López Mancilla D. y Cruz-Hernández C. 2005a. "Output synchronization of chaotic systems: Model-matching approach with application to secure communication," *Non-linear Dynamics & Systems Theory*, 5(2), pp. 141-156.

López Mancilla D. y Cruz-Hernández C. 2005b. "Output synchronization of chaotic oscillators and private communication", *Procs. of the 16th IFAC World Congress*, Praga, República Checa.

López Mancilla D. 2005. "Sincronización de osciladores caóticos perturbados con aplicación a sistemas de comunicaciones", Tesis doctoral, CICESE.

Mascolo S. y Grassi G. 1998. "Observers for hyperchaos synchronization with application to secure communications", Proc. of the IEEE Int. Conf. on Control Appl. 1016-1020 p.

Meranza M. O. y Cruz-Hernández C. [2002 "Estudio experimental de la sincronía de dos circuitos hipercaóticos de Chua," Proceedings of the 2nd International Conference on Automatic Control AUTOMATICA 2002, Julio 17-19, 2002, Santiago de Cuba, Cuba.

Meranza M. O. y C. Cruz 2002, "Estudio experimental sobre comunicación privada usando sincronía de circuitos hipercaóticos de Chua", Memorias del X Congreso Latinoamericano de Control Automático CLCA2002, 3-6 diciembre, 2002, Guadalajara Jal., México.

Monaco S. y Normand-Cyrot D. 1987. "Minimum phase nonlinear discrete-time systems and feedback stabilization", Proceedings of the 26th Conference on Decision and Control, Los Angeles CA, USA, 979-986 p.

Moog C. H., Perdon A. M. y Conte G. 1991. "Model matching and factorization for nonlinear systems" SIAM J. of Control Optimization, 29(4), 769-785 p.

Murali K., y Lakshmanan M. 1994. Phys. Rev. E 49(6), 4882 p.

Nijmeijer H. 1987. "Local (dynamic) input-output decoupling of discrete nonlinear systems". IMA J. Math. Control & Information, 4, 237-250 p.

Nijmeijer H. y V. der Schaft J. 1990. "Nonlinear dynamical control systems", Springer-Verlag.

Nijmeijer H. y Mareels I.M.Y. 1997. "An observer looks at synchronization", IEEE Trans. Circuit Syst. I, 44(10), 882-890 p.

Número especial. 1997 on Chaos synchronization and control: Theory and applications, IEEE Trans. Circuit Syst. I , 44(10).

Número especial. 1997 on Control of chaos and synchronization, Systems Control Letters. I , 31(5).

Número especial. 2000. on Control and synchronization of chaos, Int. J. Bifurcation Chaos , 10(3-4).

Ogorzalek M.J. 1993. "Taming Chaos-Part I: Synchronization", IEEE Trans. on Circuits and Systems-I, 40(10), 693-699 p.

Ott E., Gregori C. y Yorke J.A. 1990. "Controlling chaos," Phys. Rev. Lett. 64, 1196-1199 p.

Parlitz U., Chua L.O., Kocarev Lj., Halle K.S. y Shang A. 1992. "Transmission of digital signals by chaotic synchronization," Int. J. Bifurcation and Chaos 2(4), 973-977 p.

Parlitz U., Kocarev L., Stojanovski T. y Preckel H. 1996a. "Encoding messages using chaotic synchronization", *Phys. Rev. E* 53(5), 4351-4361 p.

Parlitz U., Junge L., Lauterborn W. y Kocarev L. 1996b. "Experimental observation of phase synchronization", *Phys. Rev. E* 54(2), 2115-2117 p.

Parlitz U., Junge L. y Kocarev L. 1996c. "Synchronization based parameter estimation from time series", *Phys. Rev. E* 54(6), 6253-6259 p.

Parlitz U. y Kocarev. 1998 *Handbook of Chaos Control*, Ed. Springer-Verlag.

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

Pecora L.M., Carroll T.L., Johnson G. y Mar D. 1997. "Volume-preserving and volume-expanding synchronized chaotic systems," *Phys. Rev. E.* 56(5), 5090-5100 p.

Peng J. H., Ding E. J., Ding M. y Yang W. 1996. "Synchronizing hyperchaos with a scalar transmitted signal", *Phys. Rev. Lett.* 76(6), 904-907 p.

Pikovsky A.S. 1984. "On the interaction of strange attractors", *Z. Phys. B* 55, 149-154 p.

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

Pyragas K. 1998. "Transmission of signals via synchronization of chaotic time-delay systems," *Int. J. Bifurcation Chaos*, 8(9), 1839-1842.

Reif K., Gunther S., Yaz E. y Unbehauen R. 1999. "Stochastic Stability of the Discrete-Time Extended Kalman Filter", *IEEE Trans. AC*, 44, 714-728 p.

Serrano H. y Cruz-Hernández C. 2002 "Sistema encriptador con base en la sincronía de circuitos de Chua", *Proceedings of the 2nd International Conference on Automatic Control AUTOMATICA 2002*, Julio 17-19, 2002, Santiago de Cuba, Cuba.

Serrano H. y C. Cruz . 2002. "Dos sistemas de encriptamiento con base en la sincronía de circuitos de Chua", *Memorias del X Congreso Latinoamericano de Control Automático CLCA2002*, 3-6 diciembre, 2002, Guadalajara Jal., México.

Short K. 1998. "Unmasking a modulated chaotic communications scheme", *Int. J. Bifurcation Chaos*, 6(2), 367-375 p.

Sira-Ramírez H. y Cruz Hernández C. 2001. "Synchronization of Chaotic Systems: A Generalized Hamiltonian Systems Approach", *Int. J. Bifurcation and Chaos*, 11(5), 1381-1395 p.

Sira-Ramírez H., Aguilar Ibañez C y Suárez Castañón M. 2002. "Exact state reconstructors in the recovery of messages encrypted by the states of nonlinear discrete-time chaotic systems", *Int. J. Bifurcation and Chaos*, 12(1), 169-177 p.

Sobiski, D. J. y Thorp, J. S. 1998. "PDMA-1: Chaotic communication via the extended Kalman lter", *IEEE Trans. Circuit Syst. I* 45(2), 194-197 p.

Wagg D.J. 2002. "Partial synchronization of nonidentical chaotic systems via adaptive control with applicatios to modeling coupled nonlinear systems", *Int. J. Bifurcation Chaos*, 12(3), 561-570.

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

Yang T. y Chua L.O. 1996. "Secure communication via chaotic parameter modulation", *IEEE Trans. Circuit Syst. I* 43, 817-819 p.

Zhang Y., Dai M., Hua Y., Ni W. y Du G. 1998. "Digital communication by active-passive-decomposition synchronization in hyperchaotic systems", *Phys. Rev. E* 58(3), 3022-3027 p.

Apéndice A.

Observabilidad y Controlabilidad Definiendo el gramiano de observabilidad de $[F_z, R^{-1/2}H]$ a lo largo de la trayectoria $\{z(k)\}$ como

$$\mathcal{O}(k, N) = \sum_{i=k-N}^k \Phi(i, k)^T H(i)^T R(i)^{-1} H(i) \Phi(i, k), \quad (72)$$

para algún $N \geq 0$ y para toda $k \geq N$, donde $\Phi(k_2, k_1) = F_z(k_2 - 1) F_z(k_2 - 2) \dots F_z(k_1)$ con $k_2 \geq k_1 \geq 0$ y $F_z(k) = \frac{\partial f}{\partial x}(z(k))$.

Similarmente, se define el gramiano de controlabilidad de $[F_z, Q]$ a lo largo de la trayectoria $\{z(k)\}$ como

$$\mathcal{C}(k, N) = \sum_{i=k-N}^{k-1} \Phi(k, i+1) Q(i) \Phi(k, i+1)^T. \quad (73)$$

Un sistema se dice que es controlable (observable) a lo largo de una trayectoria $\{z(k)\}$ si existe N tal que, para toda $R_x > 0$ exista $0 < \varepsilon_r < R_x$, $a_i(R_x, \varepsilon_r, N)$ y $b_i(R_x, \varepsilon_r, N)$ con $i = 1, 2$ tal que, para alguna secuencia arbitraria $\{\psi(k)\}$, $|\psi(k)| \leq R_x$

y para toda $v(k)$ tal que $|v(k)| \leq \varepsilon_r$,

$$a_1 I \geq \mathcal{C}(k, N) \geq a_2 I, \quad 0 < a_2 \leq a_1 < \infty, \quad (74)$$

$$b_1 I \leq \mathcal{O}(k, N) \leq b_2 I, \quad 0 < b_1 \leq b_2 < \infty. \quad (75)$$

Los gramianos son evaluados a lo largo de la trayectoria $\{z(k)\} = \psi(k) - v(k)$, esto es,

$$F_z(k) = \frac{\partial f}{\partial x} \{z(k)\} = \frac{\partial f}{\partial x} \{\psi(k) - v(k)\}.$$

Con lo anterior y utilizando los resultados reportados en [Deyst y Price, 1968] se obtienen las siguientes cotas

$$q^{-1}I \leq P(k) \leq pI,$$

con

$$p = a_1 + \frac{1}{b_1},$$

$$q = \frac{1}{a_2} + b_2.$$

Este material puede consultarse para mayores detalles en [La Scala *et al.*, 1995 y Reif *et al.*, 1999].