Centro de Investigación Científica y de Educación Superior de Ensenada

SINCRONIZACIÓN DEL CIRCUITO DE CHUA CON RETARDO: APLICACIÓN A LA TRANSMISIÓN SECRETA DE INFORMACIÓN

TESIS
MAESTRIA EN CIENCIAS

NESTOR RUBEN ROMERO HAROS

ENSENADA BAJA CFA, MEXICO FEBRERO DE 2005

TESIS DEFENDIDA POR

Néstor Rubén Romero Haros

Y aprobada por el siguiente comité:

Dr. César Cruz Hernández

Director del Comité

Dr. Iouri Orlov Kuchina

Miembro del Comité

Dr. Oscar Iván Lepe Aldama

Miembro del Comité

M.C. Ricardo Francisco Núñez Pérez

Miembro del Comité

Dr. Arturo Velázquez Ventura

Coordinador del Programa en Electrónica y Telecomunicaciones

Dr. Federico Graef Ziehl

Director de Estudios de Posgrado

Ensenada, B.C., México. 18 de febrero de 2005

CENTRO DE INVESTIGACIÓN CIENTÍFICA Y DE EDUCACIÓN SUPERIOR DE ENSENADA

POSGRADO EN CIENCIAS EN ELECTRÓNICA Y TELECOMUNICACIONES

Sincronización del circuito de Chua con retardo: aplicación a la transmisión secreta de información

TESIS

que para cubrir parcialmente los requisitos necesarios para obtener el grado de

MAESTRO EN CIENCIAS

Presenta:

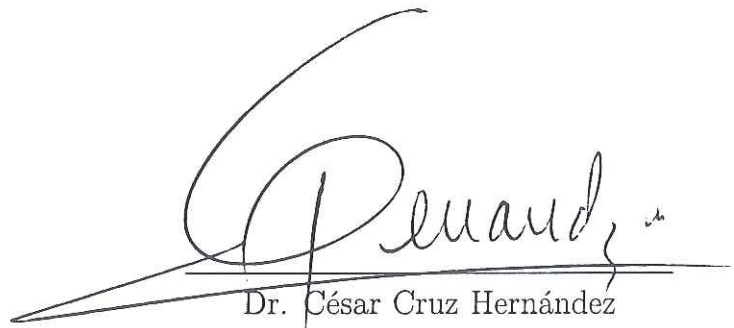
Néstor Rubén Romero Haros

Ensenada, Baja California, febrero de 2005.

RESUMEN de la tesis de **Néstor Rubén Romero Haros**, presentada como requisito parcial para obtener el grado de **MAESTRO EN CIENCIAS** en **ELECTRÓNICA Y TELECOMUNICACIONES**. Ensenada, B.C., México, Febrero de 2005.

Sincronización del circuito de Chua con retardo: aplicación a la transmisión secreta de información

Resumen aprobado por:



Dr. César Cruz Hernández

Director de Tesis

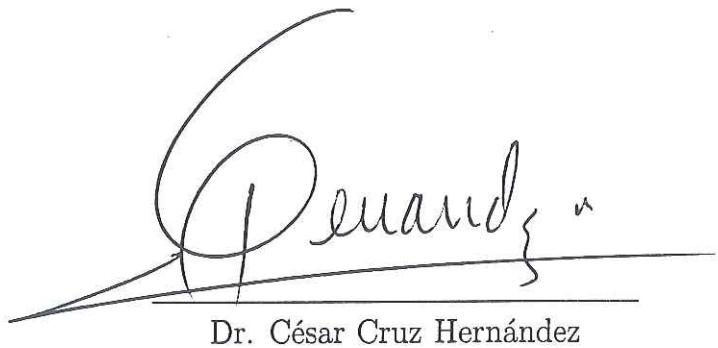
La presente tesis versa sobre el diseño de sistemas de encriptamiento basados en sincronía de caos, que emplean como generador caótico al circuito de Chua con retardo. El propósito que se persigue es incrementar la seguridad en la transmisión de información confidencial. Mediante simulaciones numéricas y la aplicación de técnicas de procesamiento de señales, se determinan los valores de los parámetros para los cuales el circuito de Chua con retardo produce señales caóticas con dinámicas extremadamente complejas. Los sistemas transmisor y receptor se acoplan en configuración maestro y esclavo, empleando como metodología de trabajo, la sincronización por formas hamiltonianas y el diseño de un observador y, se recurre a la teoría de estabilidad de Lyapunov para el análisis de convergencia del error. Se transmiten señales de información analógica ocultas en la señal caótica, por un canal de transmisión, por un canal de transmisión con retroalimentación del mensaje privado y por dos líneas de transmisión. Se oculta información binaria en dos diferentes señales caóticas y se trata la técnica de conmutación entre múltiples atractores caóticos. Se muestra la inmunidad de los sistemas de encriptado caótico diseñados, a los "ataques" reportados en la literatura.

Palabras clave: Encriptamiento, comunicación secreta, sincronización de caos, circuito de Chua con retardo, formas hamiltonianas, observador.

ABSTRACT of the thesis presented by **Néstor Rubén Romero Haros**, as a partial requirement to obtain the **MASTER DEGREE IN SCIENCE** in **ELECTRONICS AND TELECOMMUNICATIONS**. Ensenada, B.C., Mexico, February 2005.

Sinchronization of time-delay Chua's circuit: application to secret transmission of information

Abstract approved by:



Dr. César Cruz Hernández

Thesis advisor

The present dissertation turns on the design of chaotic cryptosystems, in particular, we use as chaos generator to the time-delay Chua's circuit. The objective that is persecuted is to increase the security in the transmission of confidential information. By means of numerical simulations and the application of techniques of signal processing, the values of the parameters are determined for which the time-delay Chua's circuit produces chaotic behavior extremely complex. In particular, we use a Generalized Hamiltonian forms and observer approach to synchronize two unidirectional coupled chaotic systems, the first like a master/transmitter system and the other like a slave/receiver system. Hidden signals of analogical information in the hyperchaotic signal are transmitted, by a communication channel, a communication channel with feedback of the private message and by two lines of communication. Binary information in two different chaotic signals is hidden and the chaotic technique of commutation between manifold treats atractores. The chaotic cryptosystems are immunities to reported "attacks" in literature.

Keywords: Encryption, secure communication, chaos synchronization, time-delay Chua's circuit, Hamiltonian forms, observer.

A mis padres, ***Rubén Romero*** *y* ***Rosa Elvira Haros.***

A ambos, por su cariño, sacrificio, esfuerzo, enseñanzas, orientación y ejemplo. No pudiendo expresar todo lo que siento por ustedes, solo digo GRACIAS, éste trabajo también es de ustedes.

Agradecimientos

A Dios, por el don de la vida, por concederme a terminar un proyecto más, y por darme las fuerzas para seguir adelante en los momentos difíciles.

A ti amor, por todo tu apoyo y confianza. Por ser el aliento que me da ánimo para seguir siempre adelante y por tus consejos. Parte de ti está en éste trabajo, gracias.

A mi hermana, *Denisse Adriana*, por todo el apoyo y cariño que he recibido de ti, sé que siempre puedo contar contigo, te quiero mucho.

A mis sobrinos, *Adrian* y *Marian*, por llenar de alegría nuestros corazones.

A mis amigos, por los buenos y malos momentos, por aguantarme y por escucharme.

Al M.C. Ricardo Núñez, por todo el tiempo que me ha dado, por sus sugerencias e ideas de las que tanto provecho he sacado, por su respaldo y amistad.

Al Dr. César Cruz Hernández, por toda la confianza, motivación y el apoyo brindados durante la realización de esta tesis.

A mi comité de tesis: Dr. César Cruz Hernández, Dr. Iouri Orlov, Dr. Oscar Iván Lepe y M.C. Ricardo Núñez Pérez, por sus valiosas aportaciones para la elaboración de esta tesis.

Al Consejo Nacional de Ciencia y Tecnología (CONACYT) por su apoyo y soporte económico para realizar mis estudios de posgrado.

Y a todas las personas que de una u otra forma, colaboraron o participaron en la realización de este trabajo, por el apoyo y la confianza que me han prestado.

Néstor Romero

Tabla de Contenido

Tabla de Contenido (Continuación)

Capítulo Página

Tabla de Contenido (Continuación)

Lista de Figuras

Lista de Figuras (Continuación)

Lista de Figuras (Continuación)

Lista de Figuras (Continuación)

Lista de Figuras (Continuación)

Lista de Figuras (Continuación)

Lista de Tablas

Capítulo I

Introducción

I.1 Motivación

En el pasado la criptografía se utilizó principalmente en la guerra. Este proposito de la criptografía para mantener segura la información confidencial, y los esfuerzos para descubrir los secretos militares del enemigo, hizo que después de la Segunda Guerra Mundial la criptografía se desarrollara principalmente en agencias gubernamentales que operan de manera secreta. Con la evolución de la tecnología y, especialmente con el avance explosivo de las comunicaciones en estos días, la criptografía se ha convertido en una de las principales herramientas para obtener seguridad en el almacenamiento, procesamiento y transmisión de información en un gran número de campos. Esto ha incrementado la demanda de técnicas de encriptado y el desarrollo de la criptología. En muchas ocasiones, los objetivos de seguridad de la información no se pueden alcanzar solamente con los protocolos usuales de comunicación.

El cifrado de información confidencial empleando sistemas caóticos, fue sugerido por Pecora y Carroll (1990) como alternativa de encriptado. Esta difiere sustancialmente de los métodos convencionales de cifrado; los cuales, se construyen con base en sofisticados algoritmos matemáticos (como factorización en grandes números primos, curvas elípticas, etc.), ver por ejemplo (Menezes *et al.*, 2001). A partir de entonces, diversas técnicas se han propuesto y probado a nivel laboratorio, para transmitir información encriptada con base en sincronía caótica: **encriptamiento aditivo**, **modulación paramétrica**, **conmutación entre atractores caóticos**, entre otras.

Sin embargo, se mostró posteriormente, que en determinados casos, la información oculta en el caos (con sólo un exponente de Lyapunov positivo), se puede extraer por algún receptor intruso, ya sea empleando técnicas de procesamiento de señales o a partir de mapas de reconstrucción (regresión), ver por ejemplo (Short, 1994; 1996; Pérez y Cerdeira, 1995; Yang *et al.*, 1998; Tao y Du, 2003). Quedando demostrado en esos trabajos, dos factores relevantes en la seguridad de estos sistemas criptográficos:

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

Con el propósito de superar esta limitante en el cifrado caótico, las investigaciones actuales unifican esfuerzos para asegurar la confidencialidad de la información, **incrementando la seguridad en el cifrado desde varias perspectivas**. Algunas ideas relevantes en este sentido, se describen brevemente a continuación: una forma de incrementar la seguridad del cifrado empleando sincronía caótica, es aplicar algoritmos criptográficos a la información confidencial y mezclarla posteriormente con el caos, ver por ejemplo (Yang *et al.*, 1997; Serrano-Guerreo, 2002; Serrano-Gerrero y Cruz-Hernández, 2002a; 2002b; Cruz-Hernández y Serrano-Gerrero, 2005). Una mas, consiste en aumentar la dimensión del sistema caótico, dando lugar a atractores hipercaóticos (Anishchenko *et al.*, 1994; Meranza-Castillón , 2002; Meranza-Castillón y Cruz-Hernández, 2002a; 2002b). Otra forma, es empleando sistemas caóticos que generan atractores con múltiples enrollamientos (Díaz-Moreno *et al.*, 2003; Gámez-Guzmán, 2004; Gámez-Guzmán *et al.*, 2004). Otra alternativa, es considerar sistemas caóticos con retardo de tiempo, algunos ejemplos en esta dirección se proponen en (Pyragas, 1998; Cruz-Hernández *et al.*, 2002; Cruz-Hernández, 2003; 2004), semejantes sistemas cuentan con espacio de estados de dimensión infinita y despliegan atractores hipercaóticos con un

número arbitrario de exponentes de Lyapunov positivos.

Independientemente de los enfoques mencionados, para superar los ataques al encriptado caótico, éstos mantienen una característica común, que se establece a continuación. Un asunto fundamental en el diseño y construcción de sistemas encriptadores, tanto analógicos como digitales basados en caos, es por tanto, la **selección del generador de caos** (Kolumbán *et al.*, 1997). El problema se establece como sigue: *incrementar la complejidad de la dinámica caótica, hasta donde sea posible, procurando mantener el modelo matemático (circuito electrónico) tan sencillo como sea posible.*

Por otra parte, es conocido que un simple oscilador de primer orden con un retardo de tiempo, puede producir comportamientos hipercaóticos extremadamente complejos, ver por ejemplo (Farmer, 1982; Lu y He, 1996). Esta propiedad, ha estimulado grandemente el diseño de sistemas de comunicación segura (usando caos), los cuales, son reconocidos por su escasa probabilidad de detección de la información, ver por ejemplo (Mensour y Longtin, 1998; Pyragas, 1998; Cruz-Hernández, 2004).

Motivado por lo expuesto antes, el **presente trabajo de tesis se propone** contribuir a la solución de este problema, es decir, **incrementar la seguridad del encriptado caótico** para la transmisión de información confidencial.

En particular, **para el incremento en la seguridad** de los sistemas encriptadores con base en sincronía de caos, **se empleará el circuito de Chua con retardo de tiempo**, que genera atractores hipercaóticos con un número arbitrario de exponentes de Lyapunov positivos.

I.2 Objetivos

Con la realización de este trabajo de tesis, se pretendió alcanzar el **objetivo general:**

Incrementar la seguridad de los sistemas encriptadores con base en sincronía de caos.

Y alcanzar los siguientes **objetivos particulares:**

- *Sincronizar el circuito de Chua con retardo y obtener resultados numéricos.*
- *Emplear como generador de hipercaos, al circuito de Chua con retardo, en la transmisión de información confidencial.*
- *Construir un sistema encriptador, para transmitir información confidencial (voz, audio, datos, etc.) de manera segura y obtener resultados numéricos.*
- *Diseñar y simular numéricamente la transmisión segura de información.*
- *Estudiar las principales técnicas de ataque a los sistemas de encriptamiento caótico.*
- *Evaluar la seguridad del sistema de encriptamiento propuesto.*

I.3 Metodología adoptada en esta tesis

Para alcanzar los objetivos planteados en este trabajo de tesis, se propuso emplear la **metodología de sincronización de sistemas caóticos por formas hamiltonianas y el diseño de un observador** presentada en (Sira-Ramírez y Cruz-Hernández, 2000; 2001). En particular, para sincronizar el circuito de Chua con retardo y proporcionar una aplicación a la comunicación secreta de información, tanto analógica como digital. A manera de justificación de la metodología adoptada en este trabajo, se mencionan las siguientes *ventajas* sobre otros métodos de sincronización reportados en la literatura:

- *La sincronización se obtiene de manera sistemática,*

- *Se puede aplicar a la mayoría de sistemas caóticos e hipercaóticos,*
- *No requiere el cálculo de ningún exponente de Lyapunov,*
- *No requiere que las condiciones iniciales estén dentro de la misma cuenca de atracción,*
- *Permite conocer la señal acoplante para obtener la sincronía.*

I.4 Organización del manuscrito

El material restante de este trabajo de tesis está organizado como sigue: en el **Capítulo II** se presenta el planteamiento general del problema de estudio, el encriptado de información confidencial. Se mencionan algunos algoritmos de cifrado que se han empleado a través del tiempo, hasta llegar a métodos que se estan aplicando actualmente. También se describe una solución alternativa empleando caos y, finalmente, se establece la propuesta particular de solución de esta tesis.

El **Capítulo III** empieza con algunas definiciones importantes, dando lugar después a una breve introducción a los sistemas caóticos desde el punto de vista de control, se presenta el *circuito de Chua*, uno de los sistemas físicos más estudiados, para el cual, se ha demostrado de manera rigurosa la presencia de caos, y su modelo normalizado con el cual, se obtienen algunos resultados numéricos. Posteriormente, se presenta el sistema caótico empleado en el encriptador, el *circuito de Chua con retardo* y se discuten resultados obtenidos en simulaciones numéricas.

El **Capítulo IV** empieza con breve explicación del problema de sincronía de osciladores; en particular, la sincronización de sistemas caóticos, se mencionan algunos métodos que se han reportado en la literatura correspondiente. Posteriormente, se

presenta la metodología de sincronización de sistemas caóticos por formas hamiltonianas y el diseño de un observador propuesta en (Sira-Ramírez y Cruz-Hernández, 2000; 2001). Por último, se presenta el análisis para la sincronía del *circuito de Chua con retardo* empleando la metodología mencionada, finalmente se ilustran numericamente los resultados analíticos.

El **Capítulo V** está dedicado a los sistemas de comunicación caóticos aplicados a la transmisión de información analógica. Se inicia con una descripción general de los sistemas de comunicación, seguido de una breve introducción a la aplicación del caos a las comunicaciones. Después se explican las diferentes técnicas de encriptamiento caótico aditivo. Se presentan los resultados obtenidos en la transmisión de información analógica confidencial usando estas técnicas.

El **Capítulo VI** trata la comunicación de información digital confidencial con base en caos. Primeramente se estudia la comunicación digital empleando la conmutación entre diferentes atractores caóticos. Se emplea al circuito de Chua y el circuito de Chua con retardo como generadores de caos, para alcanzar el propósito mencionado. Para el diseño del sistema de comunicación seguro, se mostrará la inmunidad de este sistema de encriptado a los "ataques" comunes a estos sistemas reportados en la literatura.

Finalmente, en el **Capítulo VII**, se proporcionan las conclusiones más importantes de este trabajo de tesis, además se mencionan algunos problemas abiertos para trabajo futuro.

Capítulo II

Planteamiento del problema

En este capítulo se presenta el planteamiento general del problema de estudio de este trabajo de tesis, se describen brevemente los sistemas criptográficos clásicos y modernos, con el propósito de ubicar en este contexto, a los sistemas criptográficos caóticos. Para mayor información al respecto, el lector interesado puede consultar (Menezes *et al.*, 2001).

II.1 Problema general

Quizás desde que el hombre empezó a comunicarse, tuvo necesidad de que algunos de sus mensajes fueran comprendidos sólo por personas a quienes estaban destinados. En dirección a satisfacer este requerimiento, nace la **criptografía**, que trata problemas relacionados con la seguridad en el intercambio de información confidencial entre emisor y receptor, a través de un canal de comunicación público, ver ejemplo en la figura 1. El objetivo básico de la criptografía, es mantener privacidad de la información en la comunicación entre comunicantes, alterando el mensaje original del emisor, de modo que sea *"incomprensible"* a toda persona ajena al destinatario. De tal forma que, después de un proceso de transformación, lo que se conoce como **cifrado**, sólo puede ser "entendido" siguiendo un proceso de **descifrado**, ver ejemplo en la figura 2; estos pasos se realizan mediante un conjunto de reglas preestablecidas entre los comunicantes llamadas **claves** o **llaves**. Ahora bien, la criptografía corresponde sólo a una parte de la comunicación secreta. Si se requiere secreto para los mensajes en la comunicación,

es porque existe desconfianza o peligro de que el mensaje confidencial transmitido, sea interceptado por un intruso o curioso. El cual, utilizará los medios a su alcance para descifrar esos mensajes secretos, mediante un conjunto de técnicas y métodos que constituyen una ciencia conocida como **criptoanálisis**. Al conjunto de ambas ciencias, criptografía y criptoanálisis se denomina **criptología**.

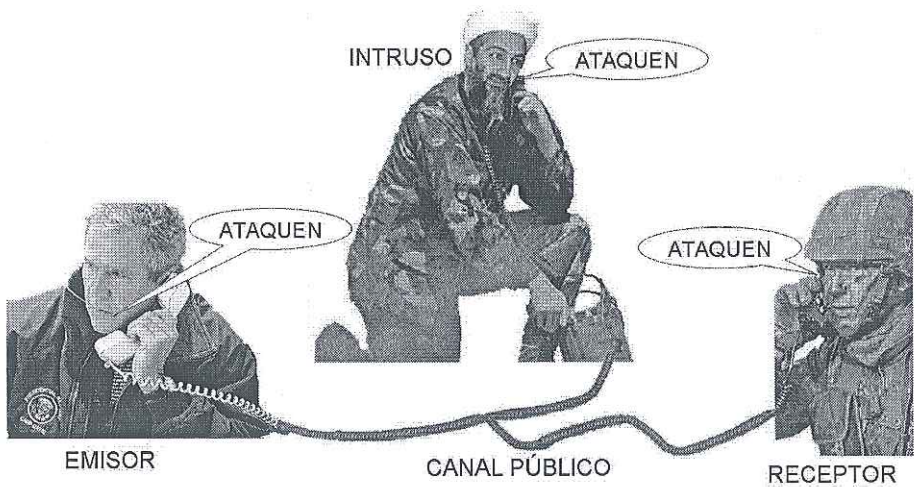


Figura 1: Transmisión de información confidencial a través de un canal público de manera insegura.

En lo sucesivo se centrará la atención en la criptografía mas que en el criptoanálisis, ya que el interés radica, mas que en atacar sistemas de cifrado, conocer cómo funcionan éstos y, contribuir al encriptamiento de información proponiendo un sistema de comunicación seguro basado en la sincronía de caos.

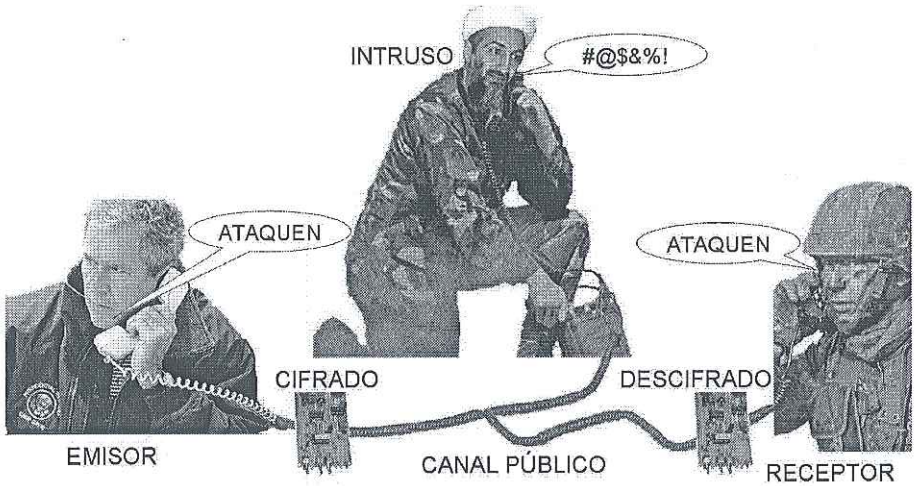


Figura 2: Transmisión de información confidencial a través de un canal público de manera segura.

II.2 Encriptado convencional

II.2.1 Criptografía clásica

El hombre ha usado algoritmos criptográficos desde la antigüedad para ocultar información y así controlar o limitar el acceso a ésta. Se puede decir, que la criptografía es tan antigua como la civilización misma, acciones militares, de estado, religiosas o comerciales impulsaron desde tiempos remotos el uso de escrituras secretas; los antiguos egipcios usaron métodos criptográficos, mientras el pueblo utilizaba la lengua **demótica**, los sacerdotes usaban la escritura **hierática** (jeroglífica) incomprensible para el resto. Los antiguos babilonios también utilizaron métodos criptográficos en su escritura **cuneiforme**.

El primer caso claro del uso de métodos criptográficos que se conoce, se dió durante la guerra entre Atenas y Esparta: la **escitala** de los Lacedemonios (figura 3). El mensaje se escribía sobre una cinta de tela, enrollada cuidadosamente sobre un palo

de madera de un cierto diámetro. Al desenrollar la cinta, el mensaje se perdía entre los pliegues de la tela, volviéndolo ilegible para cualquiera que no supiese cómo había sido escrito. El receptor del mensaje confidencial, tenía que tomar la tela y volver a enrollarla en un palo del mismo diámetro, comenzando por un lugar exacto donde se hacía una marca especial, sólo conocida entre emisor y receptor. En este sistema criptográfico, el "diámetro" del palo se considera la clave que cifraba el mensaje.

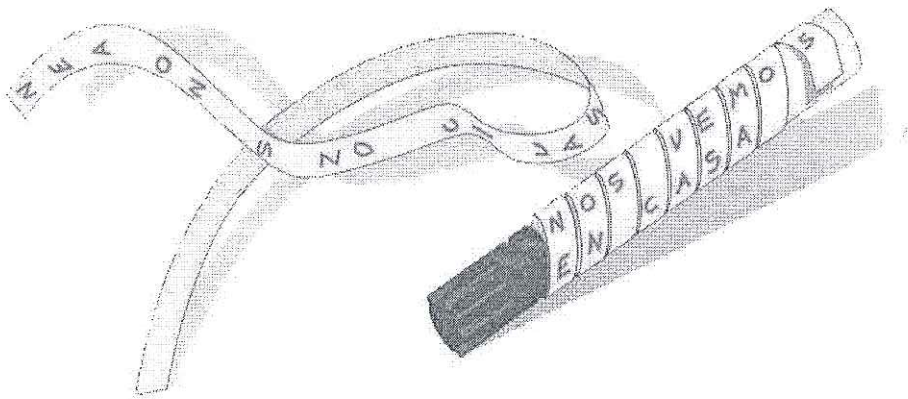


Figura 3: Cifrado antiguo por medio de la escitala.

El método de la escitala era extremadamente sencillo y muy efectivo, como también el método que instituyó Julio César, basado en la sustitución de cada letra del alfabeto por la que ocupa tres lugares más adelante en el alfabeto. Un ejemplo de las equivalencias que se tiene en nuestro alfabeto actual se muestra en la tabla I.

Así pues, el mensaje "ATAQUEN HOY AL ENEMIGO" podría codificarse en "DWDTXHQKRBDOHQHPLJR", con el fin de no ser reconocido por el adversario. Para reconstruir el mensaje original, a partir del texto cifrado, tan sólo hay que recurrir

Tabla I: Sistema de cifrado que utilizó Julio César.

Letra original	A	B	C	D	E	F	.....	R	S	T	U	V	W	X	Y	Z
Letra codificada	D	E	F	G	H	I	.....	U	V	W	X	Y	Z	A	B	C

a un alfabeto e ir sustituyendo cada letra por la que está tres posiciones antes en el mismo (ver tabla I).

Estos métodos se mantuvieron en uso durante algun tiempo. Si bien se mejoraron, especialmente los basados en el cifrado César, ya que la permutación de letras en el mensaje permite un número muy grande de combinaciones.

Todos los procedimientos de cifrado conocidos, a pesar de su diversidad y de su número ilimitado, entran en una de dos categorías siguientes: **transposición** o **sustitución**. La transposición consiste en mezclar, de conformidad con cierta ley, el contenido del mensaje original. Sustitución consiste en reemplazar esos elementos por otras letras, palabras, cifras o signos.

Durante la Segunda Guerra Mundial, los ejércitos combatientes utilizaron máquinas mecánicas, que realizaban complejos procesos de sustitución y transposición. Es bien conocido, el caso de la máquina **"Enigma"** que utilizó el ejército alemán. Esta máquina marca el punto de inflexión entre la criptografía antigua y la moderna; similar a una máquina de escribir, disponía de una serie de rotores interconectados, que codificaban automáticamente cada tecla pulsada según un complejo proceso mecánico.

II.2.2 Criptografía moderna

Con la llegada de las computadoras digitales, se ganó capacidad y velocidad para procesar datos y las nuevas tecnologías electrónicas y digitales se adaptaron a las máquinas criptográficas; por otra parte, los avances en matemáticas permitieron encontrar y definir con claridad sistemas criptográficos seguros.

A partir de estas bases, se dieron los primeros pasos hacia la construcción de los sistemas criptográficos modernos, que se clasifican en distintas categorías, independientemente del nivel de seguridad de cada uno. La categorización más importante reconoce la distinción entre sistemas *simétricos* (*clave secreta*) y *asimétricos* (*clave pública*). Los algoritmos modernos de cifrado simétrico, combinan la trasposición y la permutación, mientras que los de clave pública, se basan mas en complejas operaciones matemáticas.

Sistemas de cifrado simétrico. Estos sistemas de cifrado se caracterizan porque en ellos se utiliza la misma clave para cifrar y descifrar un mensaje. Por tanto, es necesario que las partes que se comunican, se pongan de acuerdo de antemano sobre la clave a usar (esto forma parte del protocolo).

Un buen sistema de cifrado basa toda la seguridad en la clave y nada en el algoritmo, ya que, generalmente, se divulga públicamente. La fortaleza del mismo, dependerá de su complejidad interna, pero sobre todo, de la longitud de la clave empleada.

Dado que toda la seguridad radica en la clave, si ésta cae en manos de terceros, el sistema deja de ser seguro, por lo que habría que desechar dicha llave y generar una nueva. El problema principal con los sistemas de cifrado simétrico, reside en el intercambio y la distribución de las claves. Sus principales desventajas son el peligro de

que muchas personas deban conocer una misma clave y en el caso, en el cual se asigna una clave por usuario, surge la dificultad de almacenar y proteger el gran número de claves cuando hay bastantes usuarios .

Todos los sistemas criptográficos clásicos se pueden considerar simétricos y los principales algoritmos simétricos actuales, se pueden clasificar en dos grandes grupos: los correspondientes a fuentes que generan n-palabras (cifrado en bloque) y los correspondientes a fuentes que generan letras (cifrado en flujo).

Algunos algoritmos de cifrado simétrico más importantes son:

- **DES** (por sus siglas en inglés, Data Encryption Standard - Estándar de Encriptado de Datos) fue desarrollado en 1977 por el Departamento de Comercio y la Oficina Nacional de Estándares de EEUU en colaboración con la empresa IBM. Se creó con objeto de proporcionar al público en general, un algoritmo de cifrado normalizado para redes de computadoras. Está basado en la aplicación de todas las teorías criptográficas existentes hasta el momento.

- **TDES** (Triple DES) el sistema DES se considera en la actualidad poco seguro, debido a la corta longitud de su clave. Para resolver este problema para continuar utilizando el DES, se creó el sistema TDES, basado en tres iteraciones sucesivas del algoritmo DES, con lo que se consigue una longitud de clave de 128 bits y que es compatible con el DES simple.

- **IDEA** (por sus siglas en inglés, International Data Encryption Algorithm - Algoritmo Internacional de Encriptamiento de Datos). Sistema criptográfico simétrico,

creado en 1990 por Lai y Massey, que trabaja con bloques de texto de 64 bits, operando siempre con números de 16 bits usando operaciones como OR-Exclusiva, suma y multiplicación de enteros.

Sistemas de cifrado asimétrico. Estos sistemas de cifrado usan dos claves diferentes. Una es la *clave pública*, que se puede enviar a cualquier persona y otra que se llama *clave privada*, que debe guardarse para que nadie tenga acceso a ella.

Generalmente una de las claves de la pareja, la clave pública, se emplea para cifrar los mensajes confidenciales, mientras que la otra, la privada, se destina para descifrar el mensaje encriptado, ni siquiera el que ha cifrado el mensaje puede volver a descifrarlo. Por ello, se puede dar a conocer perfectamente la clave pública, para que todo aquél, que quiera comunicarse con el destinatario lo pueda hacer.

Las claves pública y privada tienen características matemáticas especiales. Se generan siempre a la vez, estando cada una de ellas ligada intrínsecamente a la otra. Si dos llaves públicas son diferentes, entonces sus llaves privadas asociadas también lo son y viceversa.

Los algoritmos asimétricos están basados en funciones matemáticas fáciles de resolver en un sentido, pero muy complicadas de realizar en sentido inverso, salvo que se conozca la clave privada. Las claves pública y privada están relacionadas matemáticamente, pero esta relación, debe ser suficientemente compleja, que resulte muy difícil obtener una a partir de la otra. Este es el motivo, por el que normalmente estas claves no las elige el usuario, sino que lo hace un algoritmo específico para ello y suelen ser de gran longitud. Mientras que 128 bits se considera suficiente en las claves de cifrado simétrico, y dado

que la tecnología de hoy en día, se encuentra muy avanzada, se recomienda en este caso, que la clave pública tenga un mínimo de 1024 bits.

A continuación, se mencionan algunos sistemas criptográficos de clave pública que han tenido más trascendencia:

- **DH**. Este algoritmo de encriptado debido a Whitfield Diffie y Martin Hellman vió la luz en 1976 y ocasionó verdadera revolución en el campo de la criptografía, ya que fue el punto de partida para los sistemas asimétricos. Matemáticamente se basa en potencias de números y en la función *mod* (módulo discreto).

- **RSA** fue desarrollado en 1977 por Ronald Rivest, Adi Shamir y Leonard Adleman, con longitud de clave de 128 bits y es compatible con el DES. Se basa en el hecho de que no existe forma eficiente de factorizar números que sean productos de dos grandes números primos. Es el más usado en la criptografía asimétrica.

Este tipo de claves (1024 bits de longitud) se consideran seguras al menos hasta el año 2015. Sin embargo, a causa de la magnitud de la clave, estos sistemas tienen la desventaja de no ser eficientes en dispositivos con recursos reducidos de memoria, de procesamiento y de transmisión.

II.3 Solución alternativa de encriptamiento

Dado el comportamiento aparentemente aleatorio de los sistemas caóticos y, a partir que Pecora y Carroll reportaron que oscilaciones caóticas sincronizan (Pecora y Carroll,

1990), surgió una alternativa para sustituir los complicados algoritmos numéricos empleados en los métodos de cifrado convencionales. En la figura 4, se puede apreciar la idea fundamental, que consiste en codificar el mensaje confidencial, por medio de la dinámica compleja de un sistema caótico ubicado en el transmisor. Es posible reconstruir el mensaje original a través de un proceso de descifrado mediante un segundo sistema caótico en el receptor, sincronizado al comportamiento caótico del transmisor.

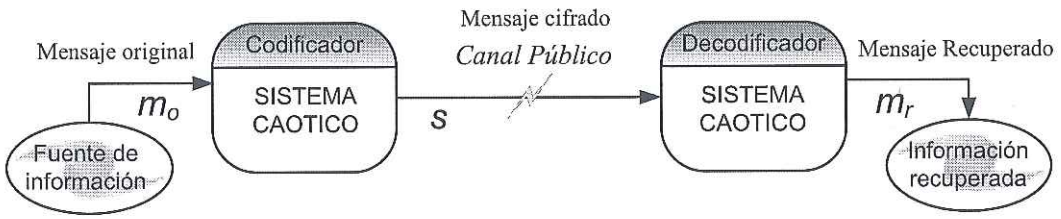


Figura 4: Sistema de cifrado con base en sincronía de sistemas caóticos, m_o: mensaje original por encriptar y transmitir, s: mensaje cifrado, señal caótica transmitida ocultando a m_o y m_r: mensaje descifrado.

II.3.1 Antecedentes de solución

En tiempos recientes, las comunidades científica y tecnológica, manifiestan enorme interés en la transmisión de información confidencial de manera segura, con base en sincronía de sistemas caóticos, Produciéndose continuamente nuevos resultados en esta área de investigación, por ejemplo:

- *Codificación por conmutación entre dos atractores caóticos*, ver por ejemplo (Parlitz *et al.*, 1992; Cuomo *et al.*, 1993; Dedieu *et al.*, 1993; Ogorzalek, 1993).

- *Codificación caótica aditiva*, ver por ejemplo (Cuomo *et al.*, 1993; Ogorzalek, 1993).

- *Codificación por modulación paramétrica*, ver por ejemplo (Kocarev *et al.*, 1992; Halle *et al.*, 1993; Cuomo *et al.*, 1993; Dedieu *et al.*, 1993; Yang y Chua, 1996).

- *Codificación por conmutación entre múltiples atractores caóticos*, ver por ejemplo (Palaniyandi y Lakshmanan, 2001).

Sin embargo, investigaciones posteriores evidenciaron que en algunos sistemas criptográficos y en situaciones muy particulares, no son capaces de proveer alto nivel de seguridad, ya que un intruso, utilizando técnicas de análisis de señales o mapas de reconstrucción (regresión), puede extraer con precisión el mensaje oculto (Short, 1994; 1996; Pérez y Cerdeira, 1995; Yang *et al.*, 1998; Tao y Du, 2003), como se muestra en la figura 5. **Por lo que es necesario incrementar la complejidad de la señal caótica, reemplazando el generador de caos en el transmisor.**

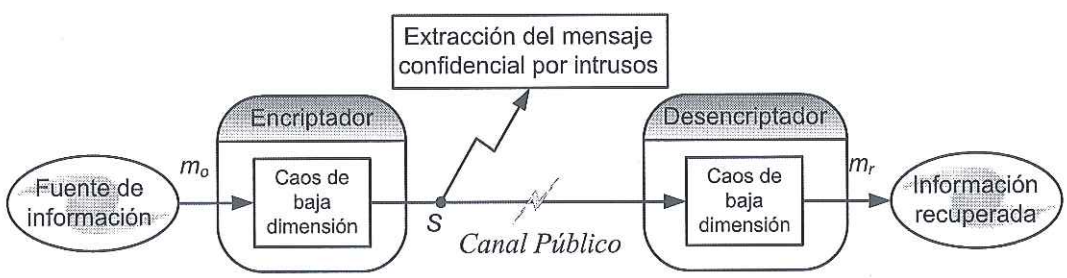


Figura 5: En algunos sistemas criptográficos y en situaciones particulares, un intruso pudo extraer el mensaje oculto en el caos, empleando técnicas de procesamiento de señales o mapas de regresión.

Estos "**ataques**" al encriptado caótico, despertaron el interés por complicar más la dinámica de la señal caótica para cifrar el mensaje; con el propósito de obtener mayor seguridad. Una propuesta es codificar la información confidencial combinando ésta con algoritmos criptográficos convencionales, antes de ocultarla en la señal caótica (Yang *et al.*, 1997; Serrano-Guerreo, 2002; Serrano-Gerrero y Cruz-Hernández, 2002a; 2002b; Cruz-Hernández y Serrano-Gerrero, 2005), ver figura 6. Otra manera de aumentar la seguridad en estos esquemas, es utilizar sistemas generadores de señales hipercaóticas (sistemas con dos o más exponentes de Lyapunov positivos), ver por ejemplo (Anishchenko *et al.*, 1994; Meranza-Castillón , 2002; Meranza-Castillón y Cruz-Hernández, 2002a; 2002b), ver figura 7. Otra, empleando sistemas caóticos que generan atractores con múltiples enrollamientos, reportada en (Díaz-Moreno *et al.*, 2003; Gámez-Guzmán, 2004; Gámez-Guzmán *et al.*, 2004), ver figura 8. Recientemente se ha demostrado que usando sistemas dinámicos gobernados por ecuaciones diferenciales con retardo, se presentan atractores caóticos con un número grande de exponentes positivos de Lyapunov, produciendo como consecuencia señales caóticas extremadamente complejas y de este modo hacen que la identificación de la información oculta en este tipo de señales sea más difícil (Pyragas, 1998, Cruz-Hernández, 2003; 2004).

II.3.2 Alcances de esta tesis

Con la realización de esta tesis de maestría, se pretende diseñar un sistema de encriptado caótico, en particular, empleando el circuito de Chua con retardo de tiempo (como generador de señales caóticas con dinámicas extremadamente complejas), con el propósito de transmitir información confidencial (voz, datos, audio, etc) de manera segura. A partir de sincronizar dos osciladores hipercaóticos (circuitos de Chua con retardo)

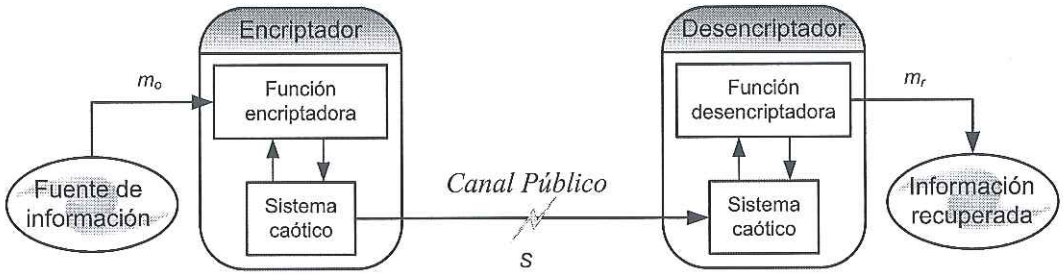


Figura 6: Incrementar la complejidad de la señal s en los sitemas de cifrado con base en caos, se logra al aplicar algoritmos criptográficos convencionales a la información y mezclarla posteriormente con el caos.

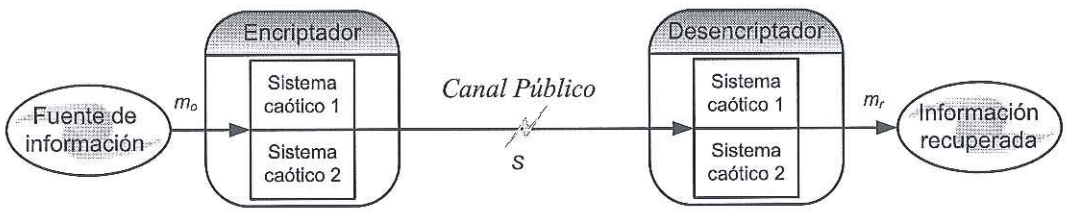


Figura 7: Incrementar la complejidad de la señal s en los sitemas de cifrado con base en caos, se logra al aumentar la dimensión del atractor dando lugar a atractores hipercaóticos.

en configuración maestro y esclavo, empleando como metodología de trabajo, la sincronización por formas hamiltonianas y el diseño de un observador, ver figura 9. Se recurrirá a la teoría de estabilidad de Lyapunov para el análisis de convergencia del error de sincronía. En lo que respecta a la transmisión de información tanto analógica como digital, se hará por distintas técnicas de comunicación caótica reportadas en la literatura. Finalmente, se evaluará el nivel de seguridad de la información encriptada y enviada.

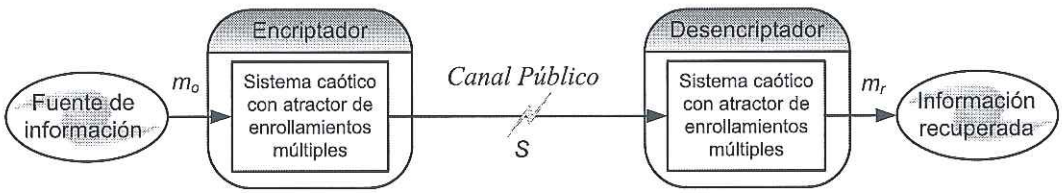


Figura 8: Incrementar la complejidad de la señal s en los sitemas de cifrado con base en caos, se logra al utilizar sistemas caóticos que generan atractores con múltiples enrollamientos.

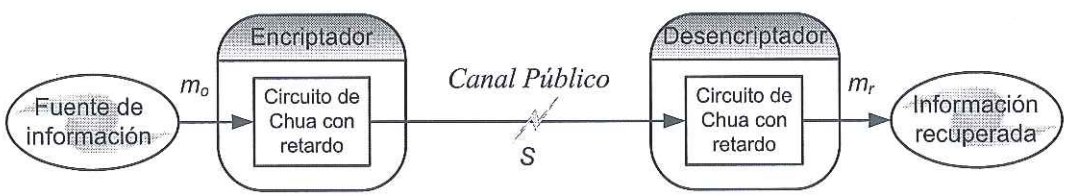


Figura 9: Empleando como generador de caos sistemas modelados por ecuaciones diferenciales con retardo, es una manera de incrementar la complejidad de la señal s en los sistemas de cifrado con base en caos.

Capítulo III

Sistemas caóticos

En este capítulo se presenta el circuito de Chua con retardo. Primeramente, se dan algunas definiciones y principales características de los sistemas caóticos. Se describe el circuito de Chua clásico, su modelo normalizado y se aplican técnicas de procesamiento de señales para conocer su dinámica caótica. Después, se presenta el circuito de Chua con retardo, se describe su característica no lineal, el diagrama esquemático, las ecuaciones de estado que modelan su comportamiento dinámico y las ecuaciones equivalentes al modelo normalizado. Posteriormente, se muestran resultados obtenidos en el estudio numérico del comportamiento dinámico de ambos circuitos. Finalmente, se dan algunas conclusiones al respecto. El lector interesado en profundizar en los tópicos tratados en este capítulo puede recurrir a (Cruz-Hernández y Núñez-Pérez, 2003; Moon, 1992).

III.1 Definiciones básicas

Antes de hablar acerca de los sistemas caóticos, se considera conveniente definir algunos términos básicos, necesarios para la comprensión del material contenido en capítulos posteriores.

Un **sistema** puede entenderse como un grupo de elementos físicos y/o lógicos que actúan juntos y realizan un objetivo determinado. El concepto de sistema se aplica a fenómenos abstractos y dinámicos, como los que se encuentran en sistemas físicos,

biológicos, económicos y similares.

Un **sistema no lineal** es aquel en que sus respuestas no son directamente proporcionales a una variable dada (que puede ser la señal de entrada).

Un **sistema dinámico** es aquel que experimenta cambios en su estado con el transcurso del tiempo. Los modelos de sistemas dinámicos lineales se han utilizado para describir y modelar dinámicas de muchos fenómenos físicos, químicos, etc. Sin embargo, muchos fenómenos pueden presentar dinámicas muy complejas que no pueden aproximarse convenientemente mediante modelos lineales. Hoy en día, los sistemas dinámicos no lineales se utilizan para describir una variedad extensa de fenómenos naturales y de ingeniería.

En general, un sistema dinámico tiene un cierto número de variables de estado independientes, cuyas trayectorias son gobernadas por un conjunto de ecuaciones diferenciales (o en diferencias) que involucran a todas las variables de estado. Para un sistema de orden n, existen n variables de estado y un conjunto de n ecuaciones diferenciales (o en diferencias). Una herramienta muy útil para el estudio de estos sistemas es la simulación numérica, que permite validar modelos matemáticos y confrontarlos con la realidad.

Las **variables de estado** de un sistema dinámico, son las que forman el conjunto más pequeño de variables que determinan el estado del sistema dinámico. Se necesitan al menos, n variables $x_1, x_2, \ldots, x_n$ para describir por completo el comportamiento de un sistema dinámico en $\mathbb{R}^n$, tales n variables son un conjunto de variables de estado.

El espacio de dimensión n cuyos ejes de coordenadas están formados por el eje x_1, el eje $x_2, \ldots$, el eje x_n, se denomina **espacio de estados**. Cualquier estado puede representarse mediante un punto en el espacio de estados.

III.2 Principales características del caos

Se ha observado que el comportamiento de muchos sistemas dinámicos no lineales, no siguen trayectorias simples, ni regulares, ni predecibles de una manera bien definida; sino aleatorias e irregulares, similar al "ruido" (ver figura 10). Este comportamiento se entiende y reconoce como **caos**.

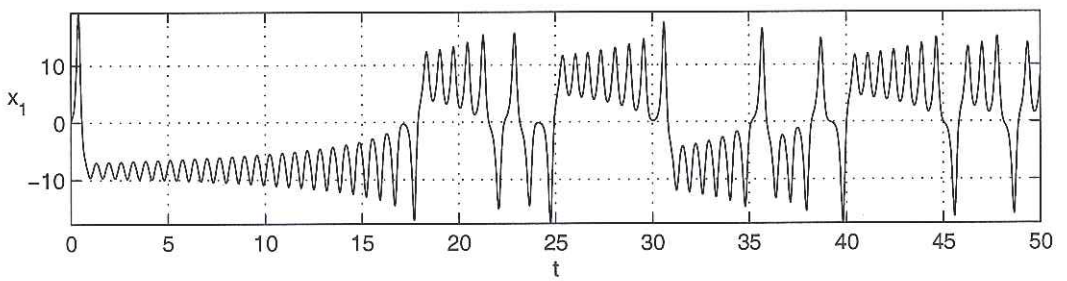


Figura 10: Dinámica temporal del estado caótico $x_1(t)$ del sistema de Lorenz.

A pesar de las dificultades para definirlo, el caos abarca un grupo de conceptos y de características comúnmente aceptadas. Estas características se discuten a continuación.

El comportamiento irregular, no periódico, de los estados de un sistema caótico pareciera reflejar que éstos, se generan mediante un proceso estocástico, o bien, que son generados por un proceso determinístico, sometido a la influencia de perturbaciones de origen estocástico. Sin embargo, este comportamiento aparentemente aleatorio del sistema dinámico es de **naturaleza totalmente determinística**; esto es, se puede

conocer con precisión la secuencia que les da origen, debido a que existe una ecuación determinística que gobierna su conducta y al conocimiento de las condiciones iniciales.

Los sistemas caóticos son sistemas dinámicos cuyas variables de estado se mueven de manera limitada (en un espacio acotado), no periódica y aparentemente aleatoria. Además, son caracterizados por una propiedad especial conocida como **sensibilidad a condiciones iniciales**; la cuál, escencialmente significa que a partir de dos condiciones iniciales "extremadamente cercanas" se producen trayectorias que divergen de manera exponencial al evolucionar el sistema en el tiempo. Esto se puede apreciar en la figura 11.

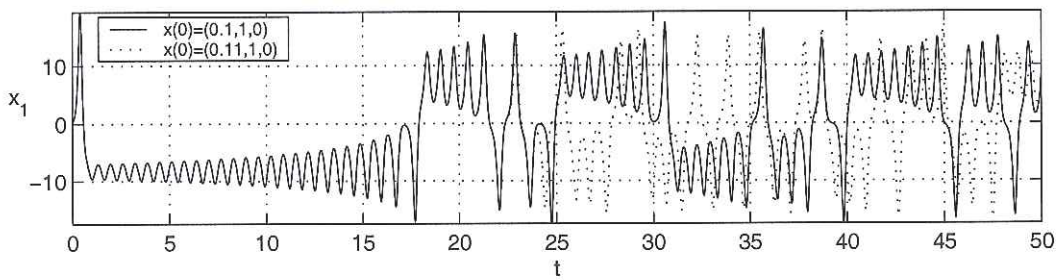


Figura 11: Evolución en el tiempo del estado caótico $x_1(t)$ del sistema de Lorenz para dos condiciones iniciales diferentes $x(0) = (0.1, 1, 0)$ y $x(0) = (0.11, 1, 0)$.

Un **atractor** es una región del espacio de estados hacia la cual convergen las trayectorias posibles de un sistema, en general, los atractores poseen la forma de alguna figura geométrica conocida. El atractor de los sistemas estables es un punto, mientras que el atractor de sistemas periódicos es un ciclo límite. El atractor de un sistema caótico se llama **atractor extraño**, ya que sus trayectorias realizan un recorrido raro o poco usual, formando imagenes de una geometría complicada y con **dimensión fractal**, un ejemplo puede observarse en la figura 12.

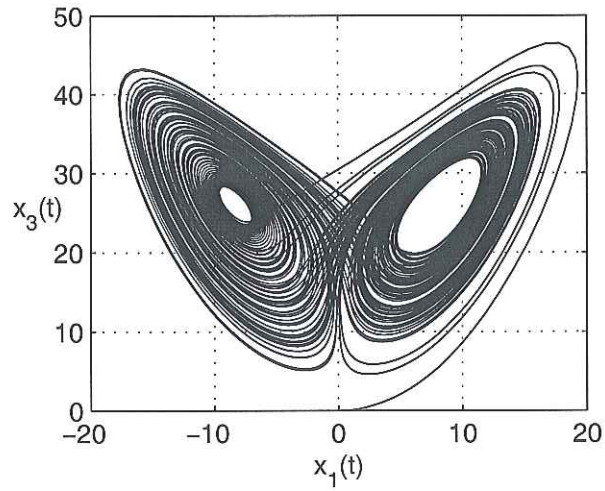


Figura 12: Atractor extraño formado por los estados caóticos $x_3(t)$ y $x_1(t)$ del sistema de Lorenz, conocido como "Mariposa de Lorenz".

Uno de los mejores indicadores de la presencia de caos en un sistema, son los exponentes de Lyapunov, ya que contienen información sobre la tasa de cambio promedio de las trayectorias en un atractor generadas por dos condiciones iniciales cercanas, por lo que, son utilizados para obtener una medida de la dependencia sobre las condiciones iniciales. La "cantidad" de caos dentro del sistema se mide por la cantidad de **exponentes de Lyapunov positivos**, que son proporcionales al orden del sistema. Un exponente de Lyapunov positivo es un indicador de comportamiento caótico.

Una característica esencial de estos sistemas, es que entre "mayor" caos exista, **su función de autocorrelación tiende más rápidamente a cero** (ver figura 13), esto se debe al carácter errático de la historia temporal.

Una característica mas, que presentan los sistemas caóticos, es la apariencia de un **espectro de frecuencias continuo y de banda ancha**, muy parecido al espectro

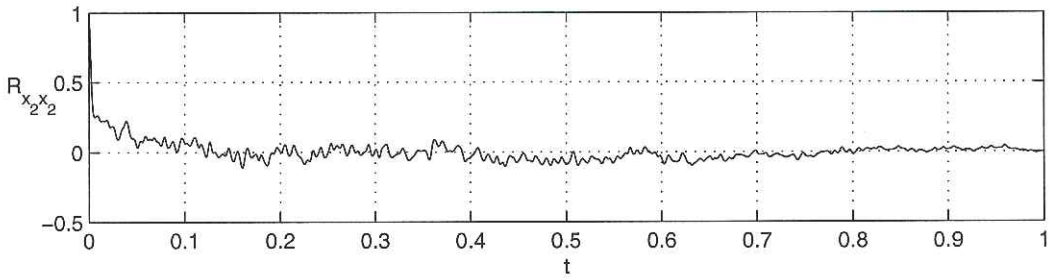


Figura 13: Autocorrelación del estado caótico $x_2(t)$ del sistema de Lorenz.

típico del ruido estocástico, pero con pico en las frecuencias dominantes (ver figura 14). Se puede observar cambios de amplitud o frecuencia en el espectro mientras se varía cierto parámetro.

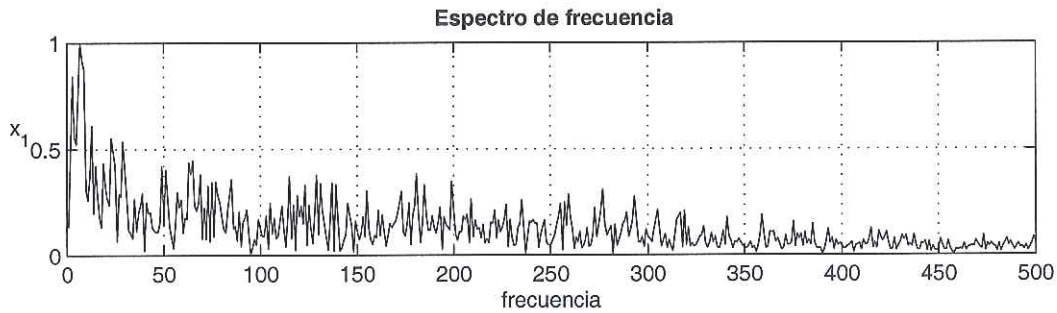


Figura 14: Espectro de frecuencia del estado caótico $x_1(t)$ del sistema de Lorenz.

III.3 Circuito de Chua

Para que pueda existir caos en un circuito eléctrico (sin entradas) construido con resistencias, inductores y capacitores, éste debe contener: *i) al menos un elemento no lineal, ii) mínimo un resistor localmente activo* y *iii) al menos tres elementos almacenadores de energía.* El circuito de Chua, mostrado en la figura 15, es el circuito electrónico más simple que satisface este criterio (Kennedy, 1993). En esta figura, R_0 representa la

resistencia interna del inductor L. Además, el circuito de Chua presenta una variedad de bifurcaciones y diferentes conjuntos límites. Este circuito es un sistema físico muy sencillo, para el cual, se ha demostrado experimentalmente, confirmado numéricamente y probado matemáticamente la existencia de caos (Madan, 1993).

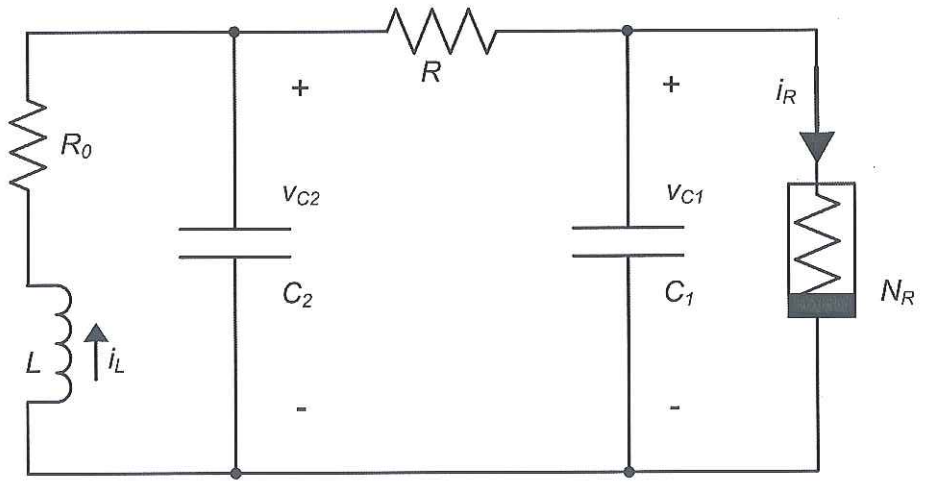


Figura 15: Circuito de Chua, contiene un inductor L, dos capacitores C_1 y C_2, una resistencia R, la resistencia interna del inductor R_0 y un resistor no lineal N_R (diodo de Chua).

La resistencia no lineal N_R, también llamada *diodo de Chua*, tiene una característica $v-i$ que es lineal por secciones, como se observa en la figura 16. Las tres zonas lineales conforman una función no lineal suave.

Empleando análisis de redes, se deducen las ecuaciones de estado, que modelan el comportamiento dinámico del circuito de Chua (Madan, 1993):

$$\begin{aligned} \frac{dv_{C_1}}{dt} &= \frac{1}{RC_1}\left(v_{C_2}-v_{C_1}\right)-\frac{1}{C_1}f\left(v_{C_1}\right), \\ \frac{dv_{C_2}}{dt} &= \frac{1}{RC_2}\left(v_{C_1}-v_{C_2}\right)-\frac{1}{C_2}i_L, \end{aligned} \tag{1}$$

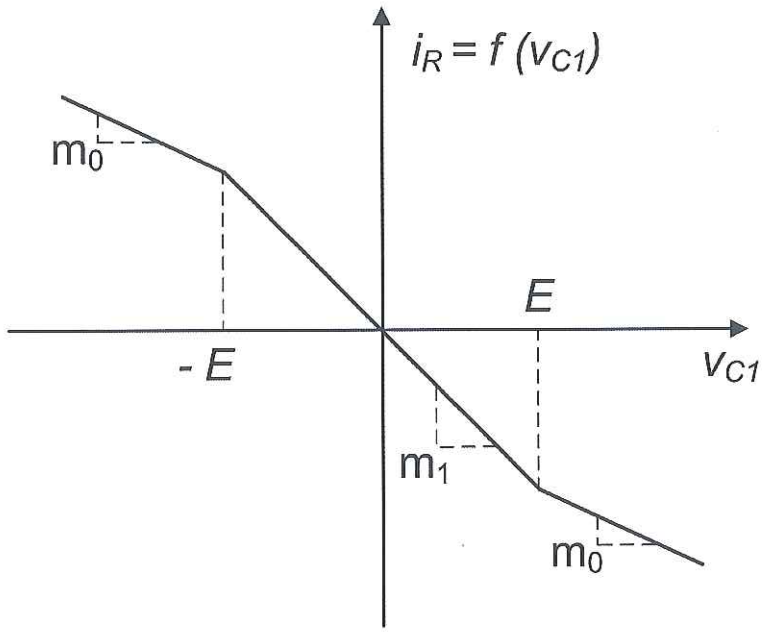


Figura 16: Característica $v - i$ de tres segmentos lineales de la resistencia no lineal N_R del circuito de Chua. Las regiones externas tienen pendiente m_0; la región interna tiene pendiente m_1. Los puntos de quiebre se encuentran dados por $\pm E$.

$$\frac{di_L}{dt} = -\frac{1}{L}v_{C_2} - \frac{R_0 i_L}{L}$$

donde

$$f(v_{C_1}) = m_1 v_{C_1} + \frac{1}{2}(m_0 - m_1)(\mid v_{C_1} + E \mid - \mid v_{C_1} - E \mid) \tag{2}$$

es la característica $v - i$ del diodo de Chua, donde m_0 es la pendiente de las regiones externas y m_1 es la pendiente del segmento interior. $\pm E$ es el voltaje del punto de quiebre en la curva de los segmentos lineales mostrada en la figura 16.

III.3.1 Modelo normalizado

Para realizar el análisis dinámico del circuito de Chua, en cualquiera de sus versiones, es de gran utilidad trabajar con un modelo matemático que tenga menor número de

parámetros y al mismo tiempo, que describa la misma dinámica de los circuitos de Chua. Para este propósito, es posible transformar (1) y (2) en un conjunto de ecuaciones adimensionales (normalizadas) mediante el siguiente cambio de variables:

$$x_1 = \frac{v_{C_1}}{E}, \quad x_2 = \frac{v_{C_2}}{E}, \quad x_3 = i_L\left(\frac{R}{E}\right), \quad \gamma = \frac{RC_2R_0}{L}$$
$$\alpha = \frac{C_2}{C_1}, \quad \beta = \frac{R^2C_2}{L}, \quad a = Rm_0, \quad b = Rm_1$$

donde E representa el voltaje de ruptura de la parte no lineal del diodo de Chua (figura 16), el cual, se fijará en "1" para el resto del documento. Así, las **ecuaciones adimensionales** o **normalizadas** del circuito de Chua son

$$\begin{aligned} \dot{x_1} &= \alpha\left(x_2 - x_1 - f\left(x_1\right)\right), \\ \dot{x_2} &= x_1 - x_2 + x_3, \\ \dot{x_3} &= -\beta x_2 - \gamma x_3, \end{aligned} \tag{3}$$

donde $f\left(x_1\right)$ es la función no lineal y es definida por

$$f\left(x_1\right) = bx_1 + \frac{1}{2}\left(a - b\right)\left[\mid x_1 + 1 \mid - \mid x_1 - 1 \mid\right]. \tag{4}$$

III.3.2 Comportamiento dinámico

Para observar el comportamiento dinámico del circuito de Chua, se realizaron simulaciones numéricas, utilizando el modelo normalizado (3)-(4) con valores de los parámetros:

$$\alpha = 10, \quad \beta = 15.62, \quad a = -8/7, \quad b = -5/7$$

y condiciones iniciales

$$x\,(0) = (x_1(0),\, x_2(0),\, x_3(0)) = (0.1,\ 0.02,\ 0)\,.$$

Estos valores aseguran la existencia de oscilaciones caóticas (Madan, 1993).

En la figura 17a), se presenta la evolución en el tiempo de los estados del circuito de Chua. Al observar la amplitud de la señal con respecto al tiempo, se puede apreciar la primera característica que presenta un sistema caótico; la forma de onda que exhibe no muestra ningún patrón o periodicidad visible, al menos en el tiempo de simulación empleado, que fue suficientemente grande. La siguiente característica, son los atractores extraños formados por las trayectorias caóticas de estos estados, los cuales, se ilustran en las figuras 17a), 17b) y 17c). Cabe mencionar que son los atractores típicos del cicuito de Chua, especificamente el atractor conocido como "doble enrollamiento" (ver figura 17b).

Es de gran provecho emplear técnicas de análisis de señales para determinar el comportamiento dinámico de los estados de un sistema caótico. La función de autocorrelación manifiesta en el tiempo, qué tan parecida es una señal a sí misma, es decir, cuántas componentes periódicas la constituyen. Para este caso, la señal que presente la autocorrelación más pequeña, indicará la que tiene mayor dinámica caótica. En la figura 18, puede apreciarse que la trayectoria que describe la función de autocorrelación de los estados del circuito de Chua, tiene una envolvente que disminuye rápidamente a cero, lo cual, es consistente con el aparente caracter azaroso del sistema. Otra forma de presentar estos resultados es en términos de la frecuencia, una señal caótica presenta espectros con gran cantidad de armónicas excitadas. Los espectros que representan

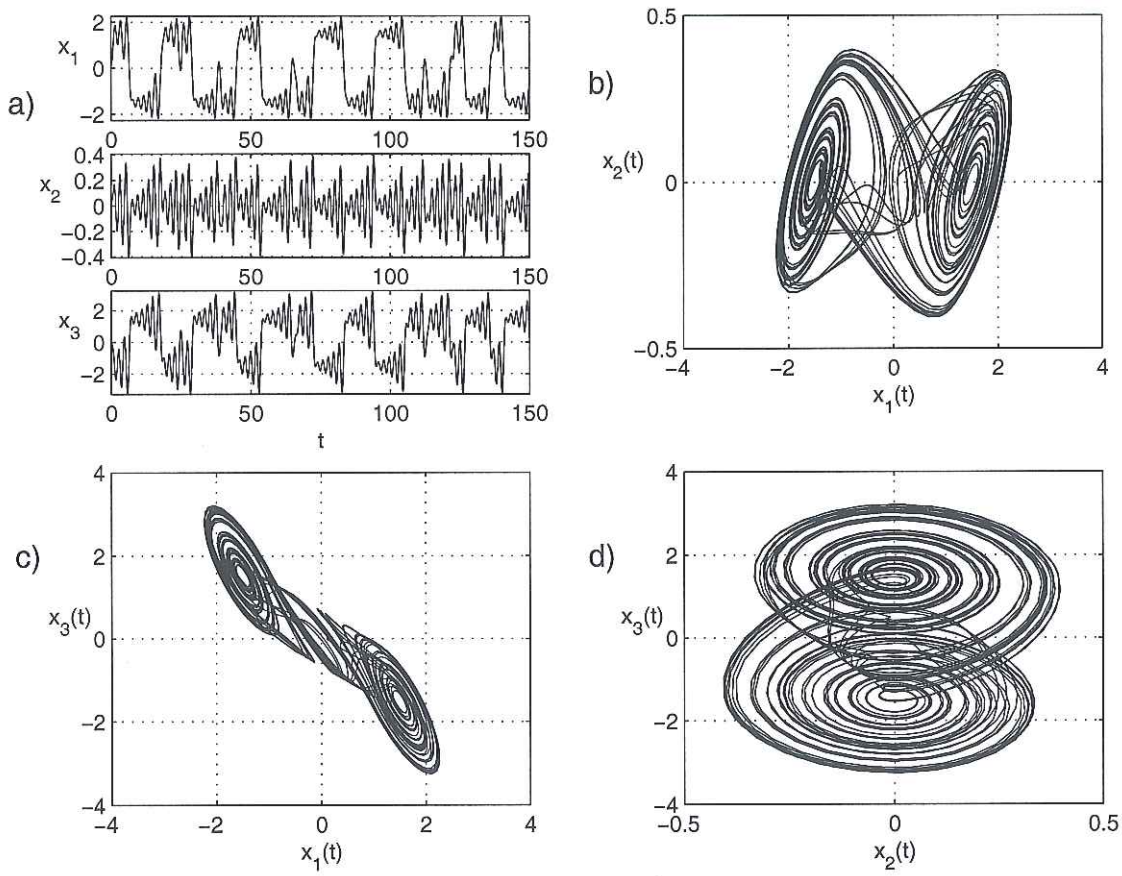


Figura 17: a) Evolución en el tiempo de los estados $x_1(t)$, $x_2(t)$ y $x_3(t)$ del circuito de Chua, b) atractor caótico $x_2(t)$ *vs* $x_1(t)$, c) atractor caótico $x_3(t)$ *vs* $x_1(t)$ y d) atractor caótico $x_3(t)$ *vs* $x_2(t)$. Resultados para valores en los parámetros: $\alpha = 10$, $\beta = 15.62$, $a = -8/7$ y $b = -5/7$.

la dinámica del circuito de Chua se muestran en la figura 18, se observa que de los tres estados $x_2(f)$ tiene mayor cantidad de componentes frecuenciales. Una manera de cuantificar la dinámica es mediante el cálculo de la *riqueza espectral* (Núñez-Pérez, 2003), con esta herramienta se encuentra que el estado $x_2(t)$ presenta mayor caos, con una riqueza espectral del 15.79%.

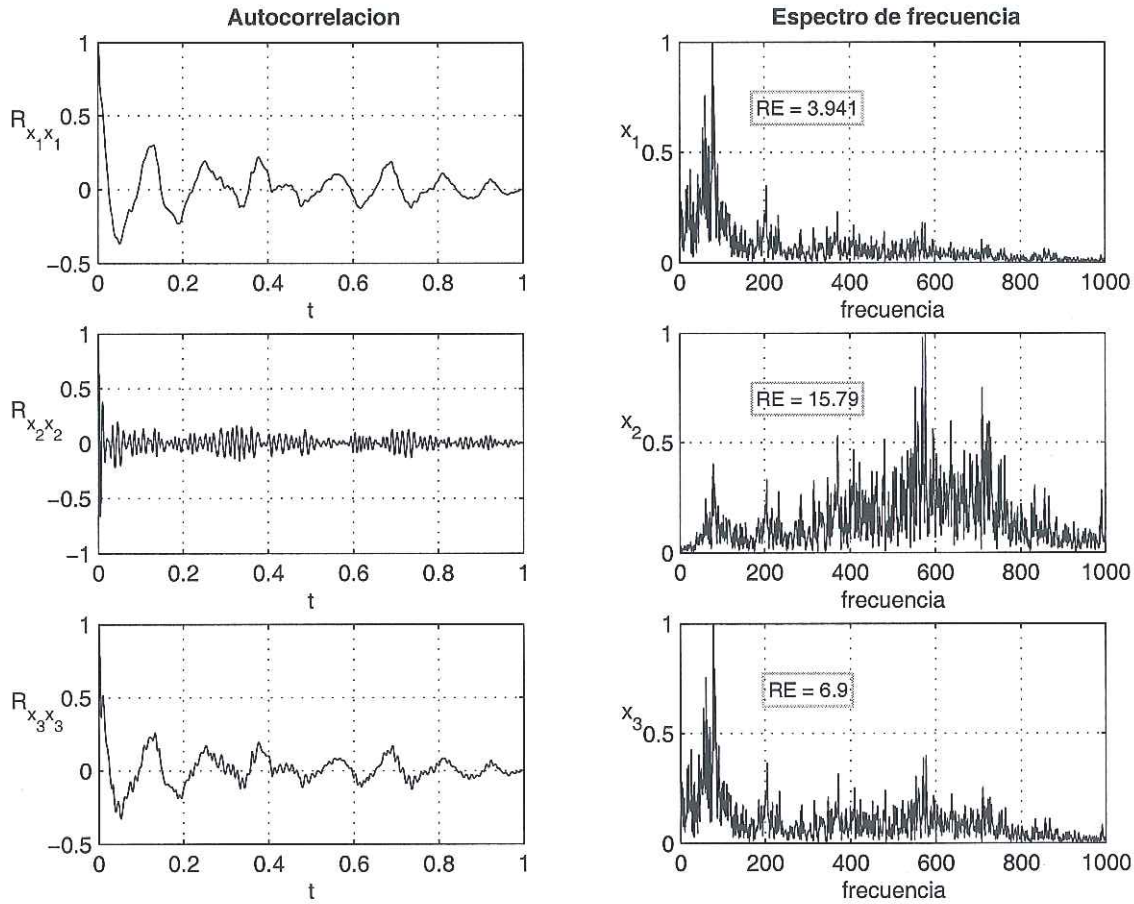


Figura 18: Autocorrelación de las señales temporales $x_1(t)$, $x_2(t)$ y $x_3(t)$ del circuito de Chua para valores de los parámetros: $\alpha = 10$, $\beta = 15.62$, $a = -8/7$ y $b = -5/7$.

III.4 Circuito de Chua con retardo

El circuito de Chua clásico (1)-(2) solamente puede producir caos de baja dimensión con un exponente de Lyapunov positivo.

Agregando al circuito de Chua clásico una retroalimentación de voltaje con un retardo de tiempo de amplitud arbitrariamente dada, como se muestra en la figura 19, es posible alcanzar dinámicas que presentan comportamientos hipercaóticos muy complejos (Wang *et al.*, 2001) con múltiples exponentes de Lyapunov positivos.

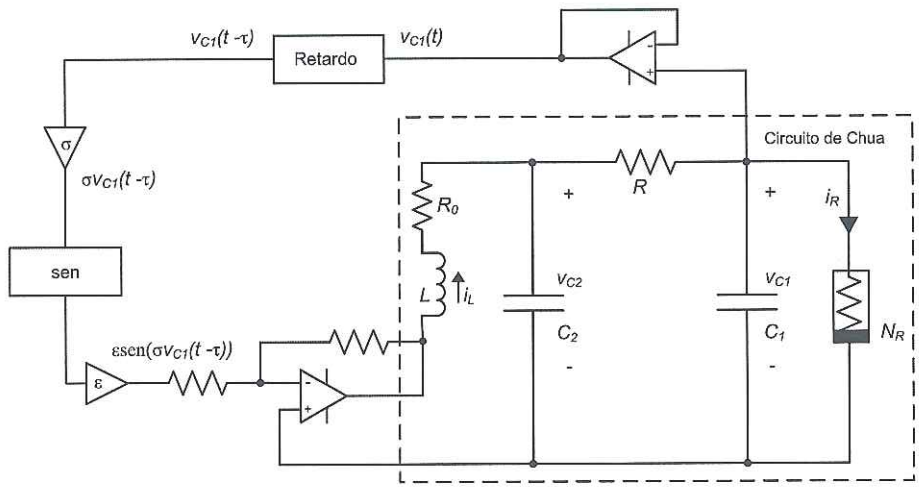


Figura 19: Circuito de Chua con retroalimentación de voltaje con un retardo de tiempo.

El circuito de Chua con retardo resultante e ilustrado en la figura 19, es modelado por el siguiente conjunto de ecuaciones diferenciales:

$$\begin{aligned} C_1\dot{x}_1 &= G(x_2 - x_1) - F(x_1), \\ C_2\dot{x}_2 &= G(x_1 - x_2) + x_3, \\ L\dot{x}_3 &= -x_2 - R_0 x_3 - w(x_1(t-\tau)), \end{aligned} \tag{5}$$

con $F(x_1)$ dada por

$$F(x_1) = bx_1 + \frac{1}{2}(a-b)(|x_1+1| - |x_1-1|), \qquad a,\ b < 0. \tag{6}$$

Y el término del retardo se toma como

$$w(x_1(t-\tau)) = \varepsilon \,\text{sen}(\sigma\, x_1(t-\tau)), \tag{7}$$

donde ε y σ son constantes positivas, τ representa el retardo de tiempo en el circuito. Puede verse que la máxima amplitud del retardo es ε, esto es,

$$|w\left(x_1\left(t-\tau\right)\right)| \leq \varepsilon. \tag{8}$$

Para un $\varepsilon > 0$ arbitrariamente dado, el circuito de Chua con retardo (5)-(6) puede ser hipercaótico para σ y τ suficientemente grandes, incluso si el circuito de Chua clásico correspondiente a (1)-(2) tiene órbitas periódicas estables.

III.4.1 Ecuaciones normalizadas

De manera similar a la sección III.4.1, mediante un cambio apropiado de variables, es posible transformar al modelo (5)-(6) y obtener el sistema de *ecuaciones normalizadas*, que describa el comportamiento dinámico del circuito de Chua con retardo como sigue:

$$\begin{aligned} \dot{x}_1 &= \alpha\left(x_2 - x_1 - f\left(x_1\right)\right), \\ \dot{x}_2 &= x_1 - x_2 + x_3, \\ \dot{x}_3 &= -\beta x_2 - \gamma x_3 - \beta\,\varepsilon\,\mathrm{sen}\left(\sigma x_1\left(t-\tau\right)\right), \end{aligned} \tag{9}$$

la función no lineal esta dada por

$$f\left(x_1\right) = bx_1 + \frac{1}{2}\left(a-b\right)\left(\left|x_1+1\right| - \left|x_1-1\right|\right). \tag{10}$$

Estas son las ecuaciones del circuito de Chua con retardo, que se emplearán para la obtención de los resultados numéricos que aparecen en capítulos posteriores.

III.4.2 Comportamiento dinámico

En (Wang *et al.*, 2001) se demuestra que si el circuito de Chua clásico tiene un punto de equilibrio exponencialmente estable, para valores de ε suficientemente pequeños y condiciones iniciales cercanas al punto de equilibrio, las trayectorias $x_i(t)$ (para $i = 1, 2, 3$) del circuito de Chua con retardo (9)-(10) permanecerán en una vecindad del punto de equilibrio. Además, se demuestra que las trayectorias son caóticas para valores de σ y τ suficientemente grandes.

Para el siguiente estudio numérico de las dinámicas del circuito de Chua con retardo (figura 19), se recurrió al modelo normalizado (9)-(10) y se fijaron los valores de los parámetros que se dan a continuación:

$$\alpha = 10, \quad \beta = 19.53, \quad \gamma = 0.1636, \quad a = -1.4325, \quad b = -0.7831, \quad \tau = 5.23. \qquad (11)$$

Simulación 1.

En la figura 20a), se pueder ver la evolución en el tiempo de los estados $x_1(t)$, $x_2(t)$ y $x_3(t)$ del circuito de Chua con retardo para los valores de los parámetros definidos en (11) y $\varepsilon = 0.07$, $\sigma = 0.4$ con condiciones iniciales $x(0) = (-1, -0.1, 1)$ presentan una forma de onda periódica. En esta misma figura se presentan los retratos de fase que describen estas trayectorias, en los cuales, se puede ver que tienden a un ciclo límite (de periodo uno).

Para obtener mayor información acerca de la dinámica que presenta el circuito de Chua con retardo, se puede recurrir a técnicas de procesamiento de señales. Al aplicar la función de **autocorrelación** a las señales temporales $x_1(t)$, $x_2(t)$ y $x_3(t)$ mostradas en la

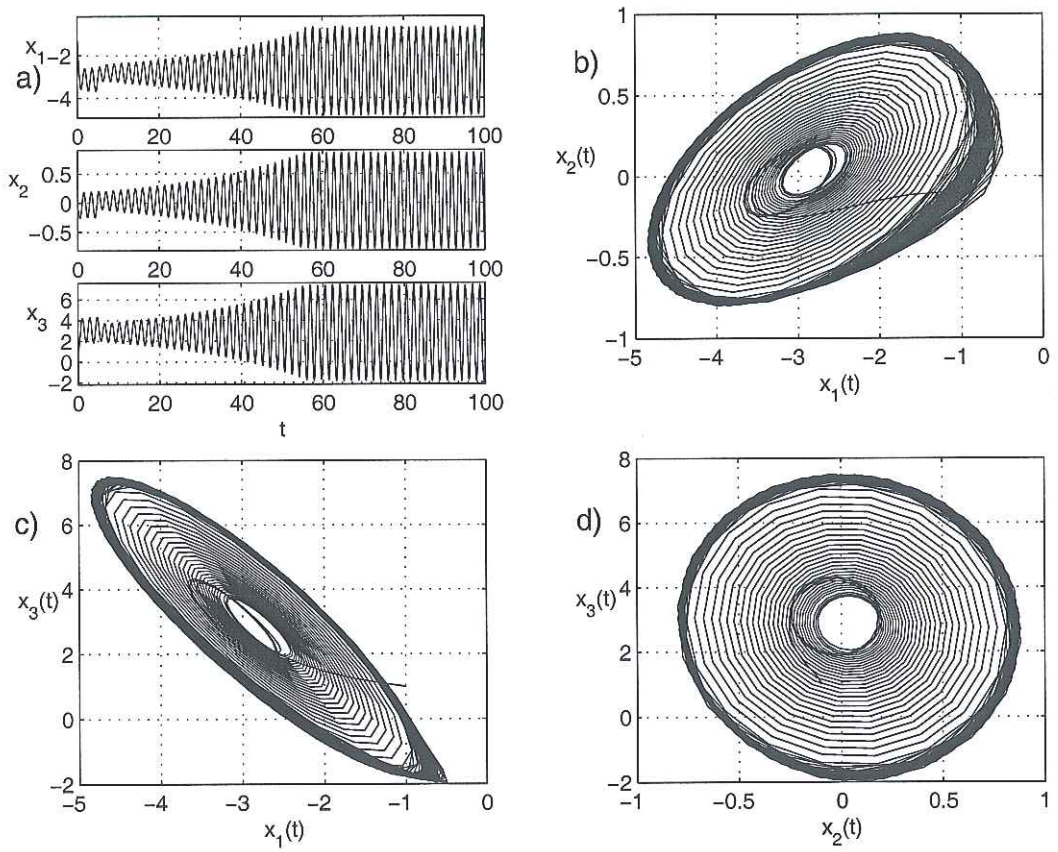


Figura 20: a) Evolución en el tiempo de los estados $x_1(t)$, $x_2(t)$ y $x_3(t)$ del circuito de Chua con retardo, b) retrato de fase $x_1(t)$ *vs* $x_2(t)$, c) retrato de fase $x_3(t)$ *vs* $x_1(t)$ y d) retrato de fase $x_3(t)$ *vs* $x_2(t)$. Resultados para valores de $\varepsilon = 0.07$ y $\sigma = 0.4$.

figura 20a), se obtienen los resultados mostrados en la figura 21, aquí se puede distinguir que los estados presentan periodicidad. Esta periodicidad se puede determinar de mejor manera, al obtener la transformada de Fourier a las señales mostradas en la figura 20a), así al estudiar el **espectro de frecuencia** mostrado en la figura 21 se observa que tienen frecuencias dominantes cerca de los 780Hz.

A partir de los resultados mostrados antes, se concluye que es necesario emplear otros valores para los parámetros ε y σ que generen señales más complejas, ya que por motivos de seguridad en la transmisión, sería fácil identificar la información oculta en

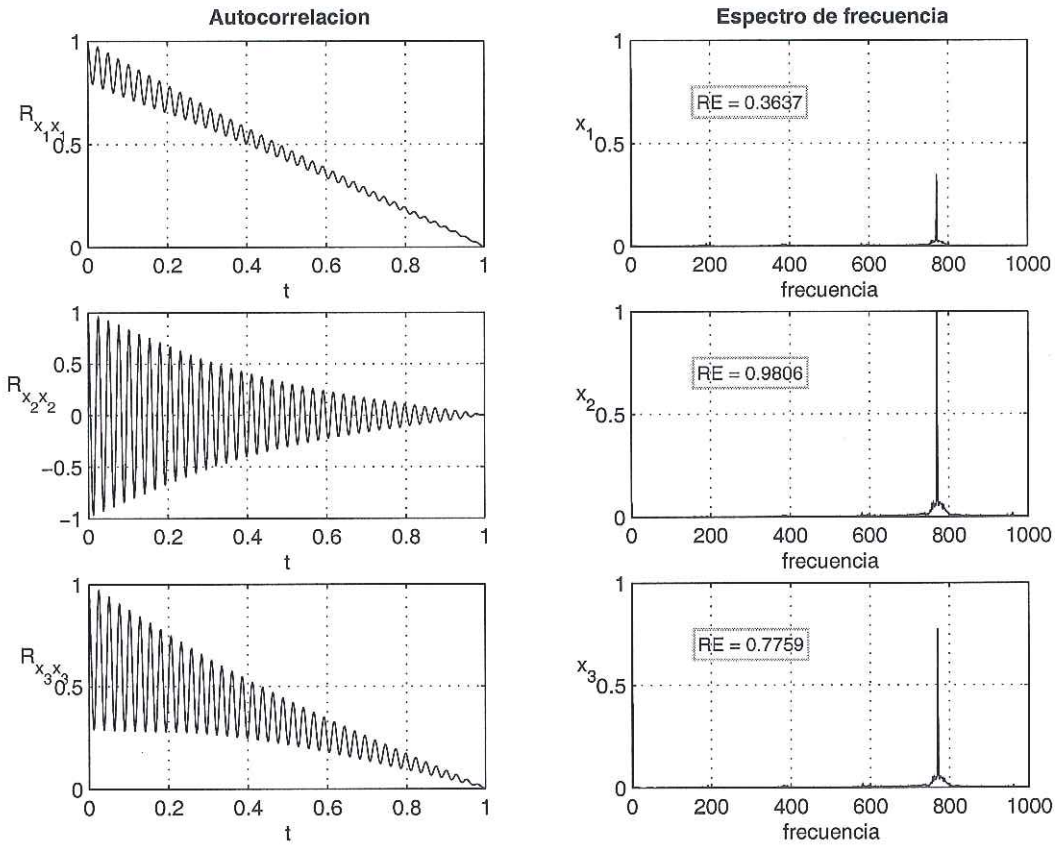


Figura 21: Autocorrelación de las señales temporales $x_1(t)$, $x_2(t)$ y $x_3(t)$ del circuito de Chua con retardo. Espectro de frecuencia correspondiente a las señales caóticas $x_1(f)$, $x_2(f)$ y $x_3(f)$ generadas por el circuito de Chua con retardo. Resultados para valores de $\varepsilon = 0.07$ y $\sigma = 0.4$.

señales periódicas de esta naturaleza.

Simulación 2.

Para los valores de los parámetros dados en (11) y con $\varepsilon = 0.2$, $\sigma = 0.5$ y con condiciones iniciales $x(0) = (-1, -0.1, 1)$, se puede ver en la figura 22 que las trayectorias recorridas por los estados $x_1(t)$, $x_2(t)$ y $x_3(t)$ del circuito de Chua con retardo, obviamente presentan mayor complejidad que las señales periódicas mostradas en la figura 20a). Los retratos de fase, que describen las trayectorias caóticas definidas por estos estados, también son más complejos que los desplegados en la figura 20.

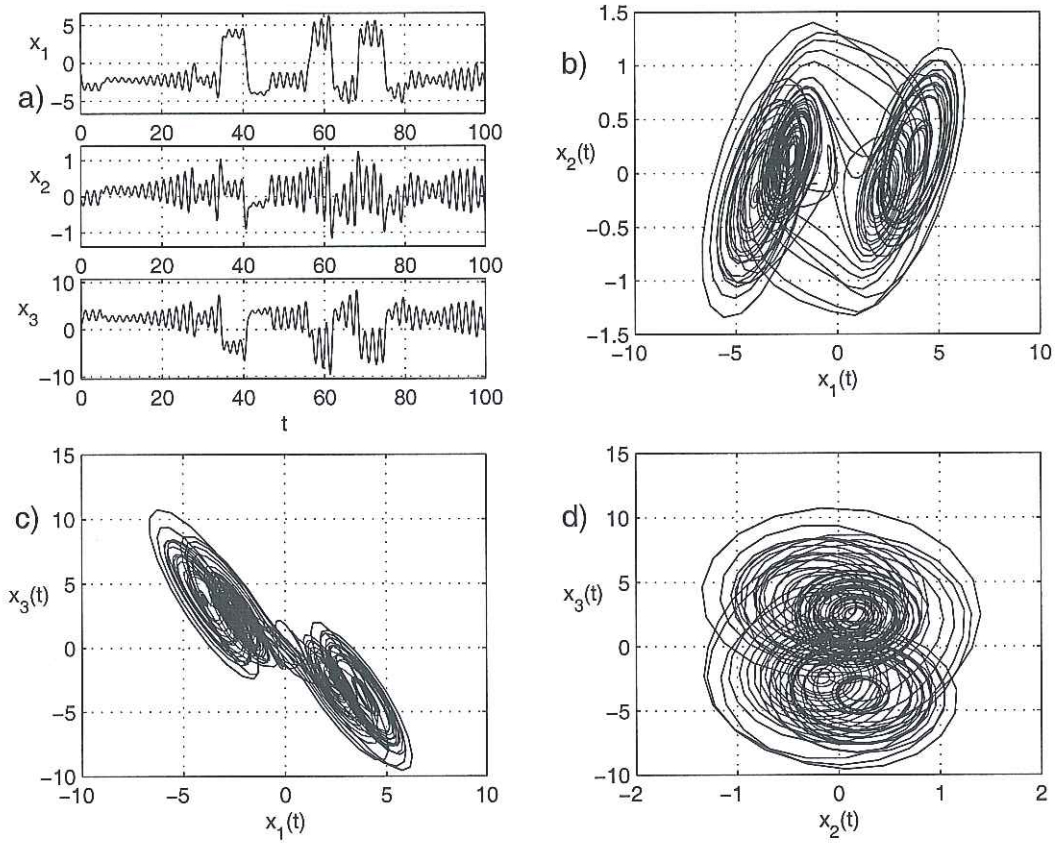


Figura 22: a) Evolución en el tiempo de los estados $x_1(t)$, $x_2(t)$ y $x_3(t)$ del circuito de Chua con retardo, b) atractor caótico $x_1(t)$ *vs* $x_2(t)$, c) atractor caótico $x_3(t)$ *vs* $x_1(t)$ y d) atractor caótico $x_3(t)$ *vs* $x_2(t)$. Resultados para valores de $\varepsilon = 0.2$ y $\sigma = 0.5$.

Al aplicar la función de autocorrelación a las señales temporales $x_i(t)$ $(i = 1,2,3)$ mostradas en la figura 22, se ve en la figura 23 que los resultados exhiben señales sin periodicidad y con una envolvente de menor magnitud. También se presenta el espectro de frecuencias resultante para estos valores de los parámetros, se puede observar que tiene gran cantidad de componentes frecuenciales excitadas.

De la comparación de los resultados obtenidos para el circuito de Chua con retardo, con valores de $\varepsilon = 0.07$ y $\sigma = 0.4$ comparados con los obtenidos para los valores de

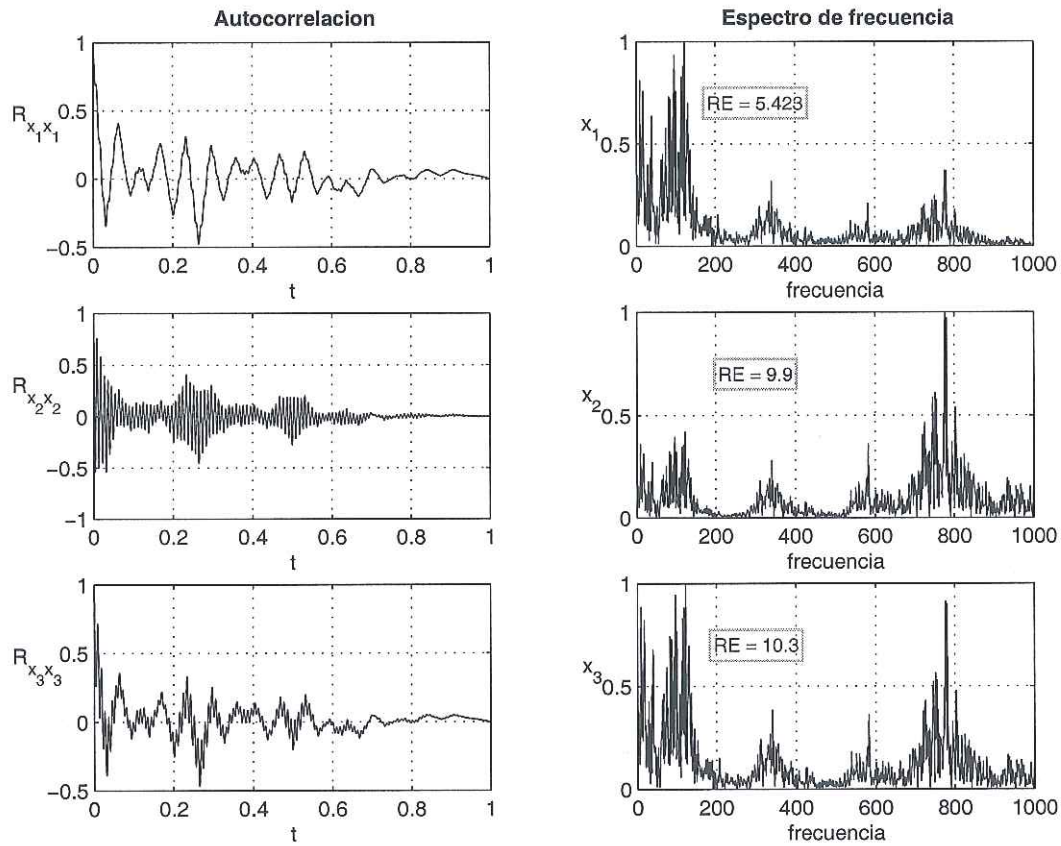


Figura 23: Autocorrelación de las señales temporales $x_1(t)$, $x_2(t)$ y $x_3(t)$ del circuito de Chua con retardo. Espectro de frecuencia correspondiente a las señales caóticas $x_1(f)$, $x_2(f)$ y $x_3(f)$ generadas por el circuito de Chua con retardo. Resultados para valores de $\varepsilon = 0.2$ y $\sigma = 0.5$.

$\varepsilon = 0.2$ y $\sigma = 0.5$, se puede distinguir que ya se tiene una dinámica caótica y, ésta da más posibilidad de encriptar información.

Simulación 3.

Con el objetivo de obtener señales más complejas, a continuación se propone nuevos valores para ε y σ. En la figura 24, se presentan los resultados obtenidos para los valores de los parámetros mostrados en (11) y $\varepsilon = 0.5$, $\sigma = 3$ y condiciones iniciales $x(0) = (-1, -0.1, 1)$. De esta figura resulta difícil decidir si las trayectorias son más complejas que las mostradas en la figura 22, para eso se recurrirá a otra de las

características que se estan empleando para estudiarlo. En la figura 24 también se despliegan los atractores caóticos, pero igualmente sería difícil resolver acerca de la complejidad de las señales.

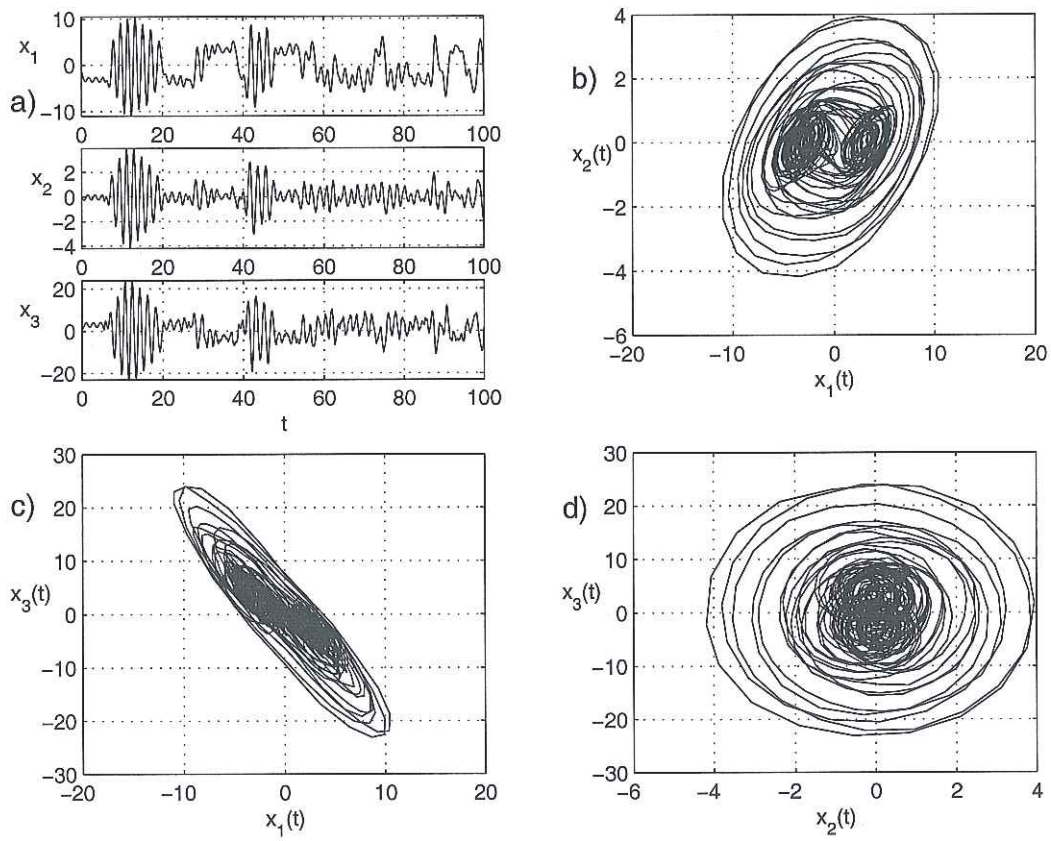


Figura 24: a) Evolución en el tiempo de los estados $x_1(t)$, $x_2(t)$ y $x_3(t)$ del circuito de Chua con retardo, b) atractor caótico $x_1(t)$ *vs* $x_2(t)$, c) atractor caótico $x_3(t)$ *vs* $x_1(t)$ y d) atractor caótico $x_3(t)$ *vs* $x_2(t)$. Resultados para valores de $\varepsilon = 0.5$ y $\sigma = 3$.

Los autocorrelogramas mostrados en la figura 25 presentan señales con envolventes que tienden más rápidamente a cero y de magnitud más pequeña que las mostradas en la figura 23, lo cual, indica que las señales generadas por el circuito de Chua con retardo para los nuevos valores propuestos son más caóticas que las generadas con los valores anteriormente usados, también se considera que los estados $x_1(f)$, $x_2(f)$ y $x_3(f)$

del circuito de Chua con retardo, presentan un espectro de frecuencia más ancho y de mayor magnitud que los analizados en la figura 23.

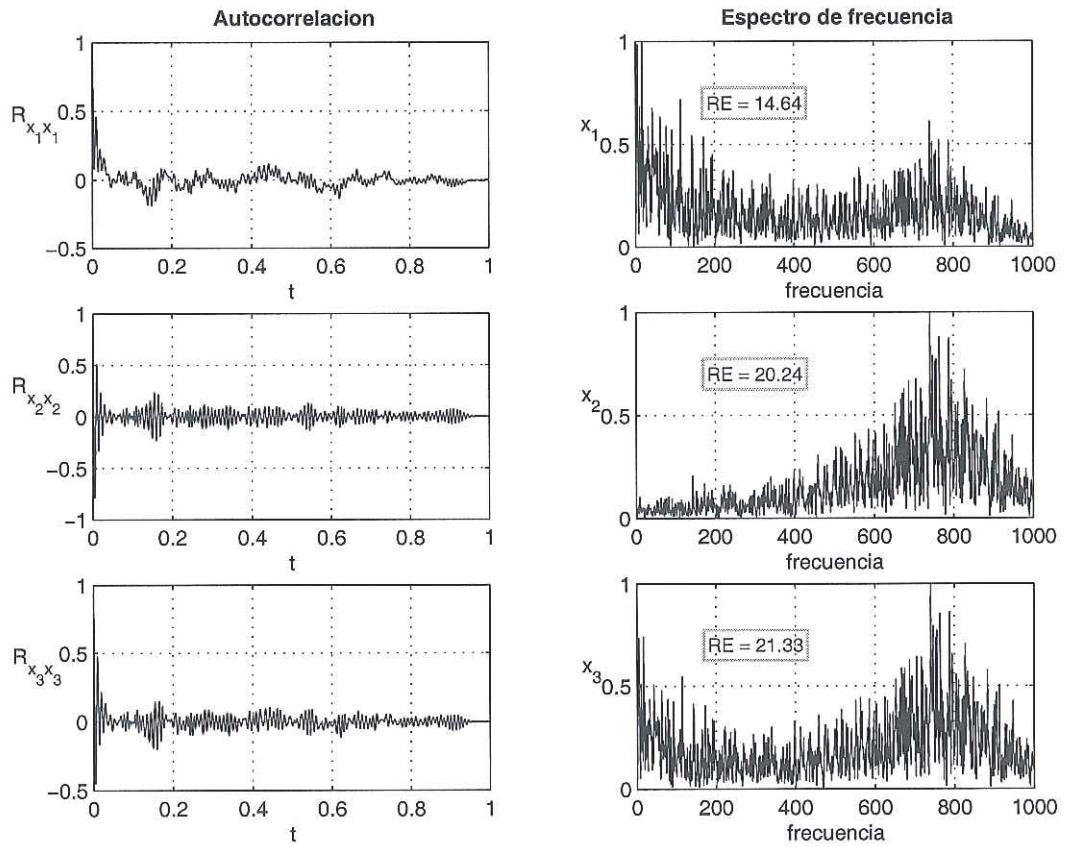


Figura 25: Autocorrelación de las señales temporales $x_1(t)$, $x_2(t)$ y $x_3(t)$ del circuito de Chua con retardo. Resultados para valores de $\varepsilon = 0.5$ y $\sigma = 3$.

De los resultados antes vistos, se puede decir, que para los valores de $\varepsilon = 0.5$ y $\sigma = 3$ el circuito de Chua con retardo genera señales caóticas con dinámica muy compleja.

Simulación 4.

El proponer diferentes valores para los parámetros ε y σ ha dado buenos resultados, por lo que, se considera conveniente analizar resultados para otros valores. En la

figura 26, se muestran la evolución en el tiempo de los estados del circuito de Chua con retardo para los valores de los parámetros en (11) $\varepsilon = 1$, $\sigma = 1$ y condiciones iniciales $x(0) = (-1, -0.1, 1)$, aquí tampoco se puede concluir con precisión acerca de la complejidad de las trayectorias de los estados $x_1(t)$, $x_2(t)$ y $x_3(t)$. En la figura 26, se pueden ver los atractores extraños formados por las trayectorias caóticas $x_1(t)$, $x_2(t)$ y $x_3(t)$ (figura 26 a)), se ve que presentan caos, pero resulta difícil decidir acerca de la complejidad en esta característica.

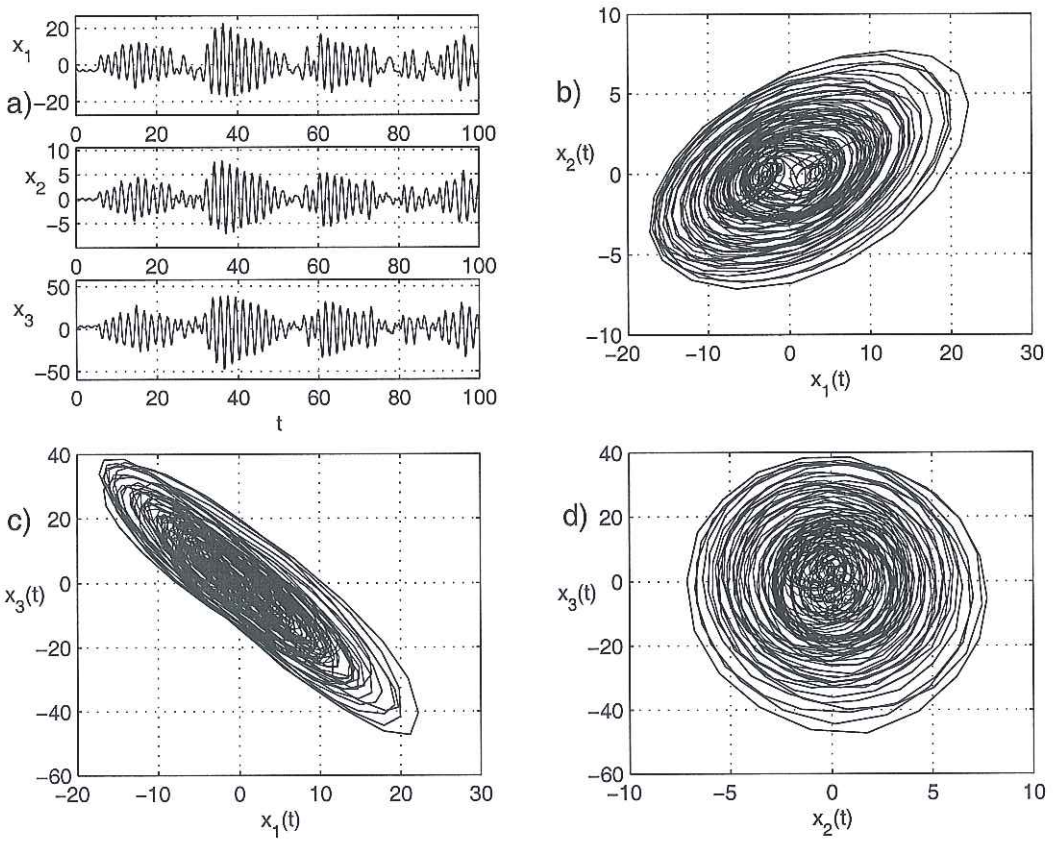


Figura 26: a) Evolución en el tiempo de los estados $x_1(t)$, $x_2(t)$ y $x_3(t)$ del circuito de Chua con retardo, b) atractor caótico $x_1(t)$ *vs* $x_2(t)$, c) atractor caótico $x_3(t)$ *vs* $x_1(t)$ y d) atractor caótico $x_3(t)$ *vs* $x_2(t)$. Resultados para valores de $\varepsilon = 1$ y $\sigma = 1$.

Las funciones de autocorrelación resultante de los estados $x_1(t)$, $x_2(t)$ y $x_3(t)$ se

ilustran en la figura 27, en ésta se puede ver que existen componentes en la señal que presentan periodicidad y su envolvente presenta mayor magnitud, comparada con los resultados obtenidos en la figura 25, por lo que se puede decir que las señales son menos caóticas. Analizando el espectro de frecuencias mostrado en la figura 27, se puede distinguir que existen armónicas dominantes alrededor de 750Hz y presenta una firma espectral más pobre.

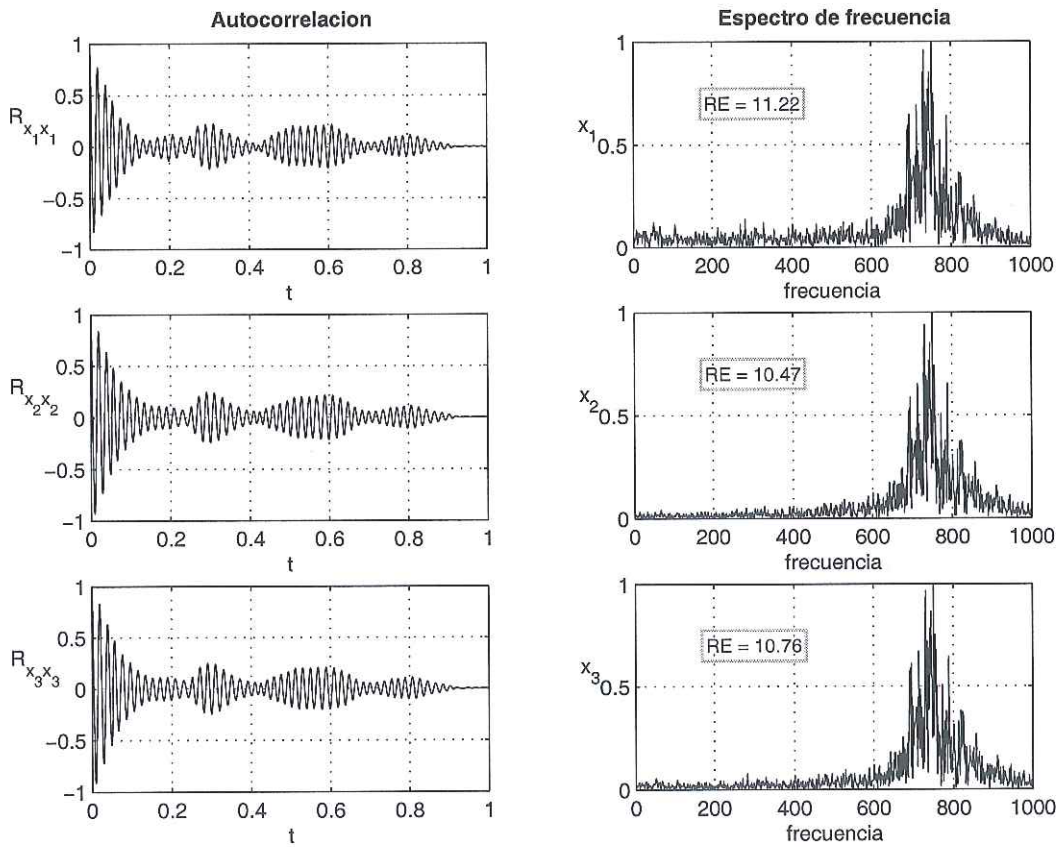


Figura 27: Autocorrelación de las señales temporales $x_1(t)$, $x_2(t)$ y $x_3(t)$ del circuito de Chua con retardo. Espectro de frecuencia correspondiente a las señales caóticas $x_1(f)$, $x_2(f)$ y $x_3(f)$ generadas por el circuito de Chua con retardo. Resultados para valores de $\varepsilon = 1$ y $\sigma = 1$.

De las observaciones realizadas para las señales generadas por el circuito de Chua con retardo, para los distintos valores de ε y σ, se concluye que la mayor dinámica

caótica se encuentra con los valores de $\varepsilon = 0.5$ y $\sigma = 3$.

III.5 Conclusiones

Es bien conocido que el circuito clásico de Chua presenta caos de baja dimensión, el cual, cuenta con un exponente de Lyapunov positivo . Como se mencionó en algunos trabajos (Short, 1994; 1996; Pérez y Cerdeira, 1995; Yang *et al.*, 1998; Tao y Du, 2003), se mostró que codificar información con este tipo de caos, no conduce a un encriptado seguro. Por tanto, habrá que darse a la tarea de sustituir en los sistemas encriptadores, al caos de baja dimensión por caos más "complejo", producido por sistemas con retardo, que generan dinámicas con varios exponentes de Lyapunov positivos. En este sentido, en este capítulo, se empleó el circuito de Chua con retardo a partir del circuito clásico de Chua. Agregando una retroalimentación de un voltaje retardado de pequeña amplitud produce atractores caóticos de alta dimensión. Mediante la aplicación de algunas técnicas de procesamiento de señales y simulaciones numéricas, se conoce e identifica que para valores de los parámetros:

$$\alpha = 10, \quad \beta = 19.53, \quad \gamma = 0.1636, \quad a = -1.4325,$$

$$b = -0.7831, \quad \tau = 5.23, \quad \varepsilon = 0.5 \text{ y } \sigma = 3$$

los estados del circuito de Chua con retardo, presentan gran complejidad en su dinámica caótica. Por tanto, como conclusión principal, se tiene a este circuito como excelente candidato a ser colocado como encriptador de información con el propósito de construir un sistema de encriptado seguro. Este asunto constituye el contenido de los capítulos posteriores.

Capítulo IV

Sincronía

Este capítulo proporciona breve introducción a la sincronía de osciladores periódicos. Posteriormente, se da una definición de sincronía caótica, se presentan los escenarios de acoplamiento más frecuentes. Luego, se mencionan algunos métodos de sincronización en sistemas caóticos. A continuación se explica un método de sincronización de osciladores caóticos con retardo, desde la perspectiva de sistemas hamiltonianos generalizados y el diseño de un observador sugerido en (Sira-Ramírez y Cruz-Hernández, 2000; 2001). Se diseña el sistema esclavo para el oscilador de Chua con retardo. Se exponen los resultados obtenidos de la simulación numérica de la sincronía y finalmente se dan algunas conclusiones al respecto.

IV.1 Sincronía de osciladores

Generalmente, por **sincronización** se entiende la capacidad de acoplar sistemas osciladores con diferentes frecuencias, para adquirir un comportamiento, tal que, de un régimen de oscilaciones independientes pasa ha un régimen común de oscilaciones periódicas, es decir, a oscilaciones de una misma frecuencia. Como resultado de la sincronización, los osciladores cambian sus frecuencias de una manera tal, que dichas frecuencias llegan a ser idénticas o relacionadas por un factor racional. Dependiendo de las características de los osciladores considerados, existen diferentes explicaciones en cuanto a por qué estos osciladores sincronizan. La observación de este fenómeno es muy antigua y se presenta en una amplia variedad de campos de la ciencia y la tecnología.

La sincronización está relacionada de muchas maneras con el control. Los dos problemas de sincronizar y de controlar movimientos caóticos, tienen raíces comunes en el problema de conducir un sistema no lineal para restringir sus movimientos. En cada caso, uno selecciona los regímenes del parámetro o las fuerzas externas para alcanzar un subespacio seleccionado del espacio total. El control de caos, busca cambiar el funcionamiento libre del sistema en movimientos más regulares o más caóticos, variedad de campos de la ciencia y la tecnología. En la naturaleza se encuentran comportamientos de ritmos biológicos acoplados, tales como enjambres de luciérnagas que destellan en sincronía, sincronía de células cardiacas, grupos de mujeres cuyos ciclos menstruales sincronizan, etc. Los ejemplos bien conocidos son la sincronía de los relojes que cuelgan en una pared, la sincronía de la rotación de la luna con su movimiento orbital de tal modo que la luna siempre muestra el mismo lado hacia la tierra. Sincronía también puede observarse entre sistemas de microondas, la energía de muchos dispositivos se puede combinar con la sincronía, de modo que la energía aumente cuadráticamente con el número de osciladores. Necesidades similares se encuentran en generadores de corriente eléctrica alimentando una carga común, láseres acoplados para obtener luz más potente, etc.

La capacidad de sincronizar osciladores no lineales, constituye una base para la explicación de muchos procesos en la naturaleza, por tanto, la sincronía desempeña un papel significativo en la ciencia. En neurociencias, en biología, en el comportamiento colectivo de los humanos, etc. Las numerosas aplicaciones en mecánica, electrónica, comunicaciones privadas/seguras, mediciones y en muchos otros campos, han demostrado que la sincronía es extremadamente importante en ingeniería.

IV.2 Sincronía de sistemas caóticos

Los fenómenos caóticos se presentan en muchos sistemas naturales y en dispositivos artificiales. Muchos trabajos de investigación se han centrado principalmente en el descubrimiento y caracterización del caos. Recientemente, se han propuesto varias ideas y técnicas para utilizar las características del caos para alcanzar ciertos objetivos. La sincronía de caos se ha empleado para incrementar la potencia de láseres, sincronizar circuitos electrónicos, controlar oscilaciones en reacciones químicas, estabilizar el ritmo cardíaco en animales y para seguridad en las comunicaciones mediante la codificación de información. Las aplicaciones del caos en diferentes campos de la ciencia y tecnología tienen su base en dos problemas, que son el **control del caos** y la **sincronización en sistemas caóticos**.

La *sincronización de sistemas caóticos* es el problema que se abordará en este trabajo de tesis; por tanto, se tratará de proporcionar una explicación más detallada del mismo.

La posibilidad de que dos o más sistemas caóticos oscilen de manera coherente y sincronizada no es obvia. Una de las principales características asociadas al comportamiento caótico, es la sensibilidad a condiciones iniciales. De lo anterior se pudiera concluir que la sincronización de sistemas caóticos no es factible, porque en sistemas reales no es posible reproducir exactamente condiciones iniciales idénticas. Así, incluso una desviación infinitesimal en los parámetros o de las condiciones iniciales eventualmente dará lugar a la divergencia de trayectorias. En este contexto, el hecho de alcanzar sincronía de sistemas caóticos, pueden considerarse como un problema fascinante e importante.

Definición 1 (Sincronización caótica). Considérese un sistema caótico modelado

por la ecuación de estado

$$\dot{x} = f(x) \tag{12}$$

y otro por

$$\dot{\xi} = f(\xi) \tag{13}$$

con f un campo vectorial con estados $x(t)$ y $\xi(t)$ definidos en $\mathbb{R}^n$. Se dice que ambos sistemas **sincronizarán completamente** si para cualquier valor de las condiciones iniciales $x(0)$ y $\xi(0)$, se cumple que

$$\lim_{t\to\infty} \|x(t) - \xi(t)\| \equiv 0. \tag{14}$$

Se define la siguiente diferencia como el *error de sincronía*

$$e(t) = x(t) - \xi(t)\,. \tag{15}$$

IV.2.1 Escenarios de acoplamiento

El ambiente, relación, comunicación, etc. necesario para que dos osciladores (caóticos o no) interactuen y entren en sincronía, se llama **escenario de acoplamiento**. Los más frecuentes son el escenario de acoplamiento unidirecional y el bidireccional. De este modo, la sincronización se puede clasificar en **sincronización unidireccional** y **sincronización bidireccional**.

La sincronización unidireccional, también conocida como **sincronización maestro y esclavo**, se presenta cuando un sistema A tiene influencia sobre un sistema B, pero no a la inversa, ver figura 28. En este esquema y como resultado de este acoplamiento, el sistema A (maestro) impone su comportamiento al oscilador B (esclavo).

Figura 28: Escenario de acoplamiento unidireccional (maestro-esclavo).

La sincronización bidireccional, también conocida como **sincronización mutua**, se presenta cuando un sistema A, tiene influencia sobre el sistema B y viceversa, ver figura 29. En este esquema y como resultado de este acoplamiento, las dinámicas de los sistemas A y B coinciden a un nuevo estado.

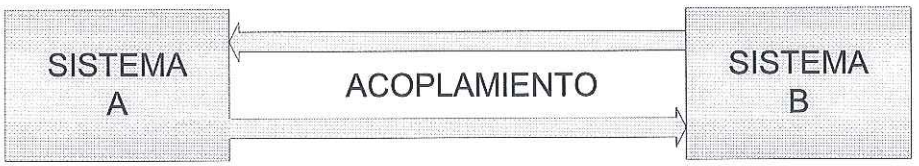


Figura 29: Escenario de acoplamiento bidireccional (mutuo).

IV.2.2 Métodos de sincronización en sistemas caóticos

En el problema de sincronización unidireccional de sistemas caóticos, se tiene un sistema caótico (maestro) con un vector de estados compuesto por n elementos. Se requiere crear un segundo sistema (esclavo) que sea capaz de reproducir el vector de estados completo del maestro con el mínimo de información. Para sincronizar los dos sistemas caóticos, el sistema esclavo debe responder a la señal de acoplamiento de forma tal que, la dinámica del error de sincronía (15) sea cero, al menos asintóticamente. El error al que se hace mención, corresponde a la diferencia entre los estados del sistema maestro y los correspondientes del sistema esclavo. Por tanto, no hay una estructura específica para el sistema esclavo.

El diseño de un modelo matemático para el sistema esclavo, fue tratado primeramente por Pecora y Caroll en (Pecora y Carroll, 1990), en este modelo, el sistema esclavo es una copia de un subsistema estable del sistema maestro. A partir de este modelo han surgido nuevas propuestas; en algunas de ellas, se han empleado sistemas compensados como Schweizer y colaboradores en (Schweizer *et al.*, 1995), donde se emplea una especie de observador y Kapitaniak y colaboradores en (Kapitaniak *et al.*, 1994), mostrándose experimentalmente la sincronización mediante una ley de control. Se ha propuesto también el empleo de observadores completos o reducidos para lograr la sincronización (Nijmeijer y Mareels, 1997; Ushio *et al.*, 1996; Fradkov *et al.*, 1999), sincronización por construcción de un sistema inverso (Kocarev *et al.*, 1992; Halle *et al.*, 1992; Chua *et al.*, 1993; Feldman *et al.*, 1996), por retroalimentación del error (Chen y Dong, 1993a; 1993b), recientemente sincronización mediante formas hamiltonianas y observador (Sira-Ramírez y Cruz-Hernández, 2000; 2001), por modos deslizantes (López-Mancilla y Cruz-Hernández, 2004), otra manera es por acoplamiento a modelos (Aguilar-Bustos y Cruz-Hernández, 2002; 2003; López-Mancilla y Cruz-Hernández, 2005; en proceso), entre otros.

IV.3 Sincronización de osciladores caóticos con retardo de tiempo

Considerese un sistema dinámico descrito de la siguiente forma

$$\dot{x} = f\left(x,\, x\left(t-\tau\right)\right), \qquad x \in \mathbb{R}^n \tag{16}$$

el cual, representa cualquier sistema caótico con retardo de tiempo, donde $x\left(t\right) = \left(x_1(t), \ldots, x_n(t)\right)^T \in \mathbb{R}^n$ es el vector de estados, f es una función no lineal y τ es el

retardo de tiempo. El sistema provee un ejemplo de oscilador de dimensión infinita con *múltiples exponentes de Lyapunov positivos* (es decir, genera señales caóticas extremadamente complejas). A partir de la solución proporcionada en (Sira-Ramírez y Cruz-Hernández, 2000; 2001) y en particular para este sistema (Cruz-Hernández, 2004), el oscilador con retardo de tiempo descrito por la ecuación (16), se puede escribir en la siguiente *forma canónica hamiltoniana generalizada*,

$$\dot{x} = \mathcal{J}(x)\frac{\partial H}{\partial x} + \mathcal{S}(x)\frac{\partial H}{\partial x} + \mathcal{F}(x, x(t-\tau)), \qquad x \in \mathbb{R}^n \tag{17}$$

donde $H(x)$ es una *función de energía suave*, la cual es definida positiva globalmente en $\mathbb{R}^n$. El *vector gradiente* de H, representado por $\partial H/\partial x$, se asume su existencia donde quiera. Se utiliza una *función de energía cuadrática* $H(x) = 1/2\ x^T \mathcal{M}\, x$ con $\mathcal{M}$ siendo una matriz constante, simétrica y definida positiva. Tal que $\frac{\partial H}{\partial x} = \mathcal{M}\, x$. Las matrices cuadradas $\mathcal{J}(x)$ y $\mathcal{S}(x)$ satisfacen, para toda $x \in \mathbb{R}^n$, las siguientes propiedades:

$$\mathcal{J}(x) + \mathcal{J}^T(x) = 0, \qquad \mathcal{S}(x) = \mathcal{S}^T(x). \tag{18}$$

El campo vectorial $\mathcal{J}(x)\frac{\partial H}{\partial x}$ exhibe la parte *conservativa* del sistema y el campo vectorial $\mathcal{S}(x)\frac{\partial H}{\partial x}$ describe la parte *no conservativa* del sistema. En algunos casos, $\mathcal{S}(x)$ es *definida negativa* o *semidefinida negativa*, entonces el campo vectorial $\mathcal{S}(x)\frac{\partial H}{\partial x}$ es la parte *disipativa* del sistema. Por otra parte, si $\mathcal{S}(x)$ es definida positiva, semidefinida positiva o de signo indefinido, representa la parte *desestabilizante* del sistema en forma global, semiglobal o local, respectivamente. En el último caso, siempre se puede (aunque no de forma única) descomponer el campo vectorial $\mathcal{S}(x)$ en la suma de una matriz simétrica semidefinida negativa $\mathcal{R}(x)$ y una matriz simétrica semidefinida positiva $\mathcal{N}(x)$. Por último, $\mathcal{F}(x, x(t-\tau))$ representa el campo vectorial *localmente*

desestabilizante.

IV.3.1 Diseño de observadores no lineales para una clase de sistemas en forma hamiltoniana generalizada

En el contexto de diseño de observadores, se considera una clase especial de sistemas hamiltonianos generalizados con campo vectorial desestabilizante y un mapeo lineal de salida $y(t)$, dado por

$$\begin{aligned} \dot{x} &= \mathcal{J}(y)\frac{\partial H}{\partial x} + (\mathcal{I}+\mathcal{S})\frac{\partial H}{\partial x} + \mathcal{F}(y, y(t-\tau)), \qquad x \in \mathbb{R}^n, \\ y &= \mathcal{C}\frac{\partial H}{\partial x}, \qquad y \in \mathbb{R}^m \end{aligned} \tag{19}$$

donde $\mathcal{S}$ es una matriz simétrica constante, no necesariamente de signo definido e $\mathcal{I}$ es una matriz constante antisimétrica. El vector $y(t)$ se refiere a la salida del sistema y la matriz $\mathcal{C}$ es una matriz constante de dimensiones apropiadas.

Se representa por $\xi(t)$ al **vector estimado** del vector de estado $x(t)$ y se considera la función de energía hamiltoniana $H(\xi)$, como una particularización de H en términos del estado estimado $\xi(t)$. De manera similar, se representa por $\eta(t)$ a la salida estimada y calculada en términos de $\xi(t)$. El vector gradiente $\frac{\partial H(\xi)}{\partial \xi}$ es naturalmente de la forma $\mathcal{M}\xi$ con $\mathcal{M}$ una matriz constante, simétrica y definida positiva.

Un observador no lineal para el sistema hamiltoniano generalizado (20) se describe como sigue

$$\dot{\xi} = \mathcal{J}(y)\frac{\partial H}{\partial \xi} + (\mathcal{I}+\mathcal{S})\frac{\partial H}{\partial \xi} + \mathcal{F}(y, y(t-\tau)) + K(y-\eta), \qquad \xi \in \mathbb{R}^n, \tag{20}$$

$$\eta = \mathcal{C}\frac{\partial H}{\partial \xi}, \qquad \eta \in \mathbb{R}^m$$

donde $K = (k_1, k_2, \ldots, k_n) \in \mathbb{R}^n$ es un vector constante, conocido como **ganancia del observador**. En el contexto de sincronización, el observador (21) desempeñará el papel de oscilador esclavo. Cuya función será estimar (reproducir) las dinámicas completas del maestro (20).

El **error de estimación del estado** se define como $e(t) = x(t) - \xi(t)$ y el error de estimación de la salida por $e_y(t) = y(t) - \eta(t)$, ambos son gobernados por el sistema dinámico siguiente

$$\begin{aligned} \dot{e} &= \mathcal{J}(y)\frac{\partial H}{\partial e} + (\mathcal{I} + \mathcal{S} - K\mathcal{C})\frac{\partial H}{\partial e}, \qquad e \in \mathbb{R}^n, \\ e_y &= \mathcal{C}\frac{\partial H}{\partial e}, \qquad e_y \in \mathbb{R}^m \end{aligned} \tag{21}$$

donde el vector $\frac{\partial H}{\partial e}$ con abusos de notación, es el vector gradiente de la función de energía *modificada*,

$$\frac{\partial H(e)}{\partial e} = \frac{\partial H}{\partial x} - \frac{\partial H}{\partial \xi} = \mathcal{M}(x - \xi) = \mathcal{M}e. \tag{22}$$

Mas adelante, donde sea necesario se escribirá $\mathcal{I} + \mathcal{S} = \mathcal{W}$.

Antes de continuar con la exposición, es importante recordar las definiciones básicas de *detectabilidad* y *observabilidad* en sistemas lineales.

Definición 1 (Detectabilidad y Observabilidad). Dado un par de matrices constantes $(\mathcal{C}, \mathcal{A})$ de dimensión $m \times n$ y $n \times n$ respectivamente, se dice que el par es **detectable** si la matriz

$$\begin{bmatrix} \mathcal{C} \\ s\mathcal{I} - \mathcal{A} \end{bmatrix} \tag{23}$$

es de rango pleno n para todos los valores de s en el semiplano derecho del plano complejo. El sistema se dice que es **observable**, si la matriz (23) es de rango pleno para todos los valores de s en el plano complejo.

Para que el estado del maestro $x(t)$ del sistema no lineal (20) sea global y exponencialmente estimado por el estado $\xi(t)$ del observador no lineal (21), el par de matrices $(\mathcal{C}, \mathcal{S})$ debe ser *observable* o al menos *detectable*, condiciones suficientes reportadas en (Sira-Ramírez y Cruz-Hernández, 2000; 2001). En el caso que resultara que el par de matrices (C, S) es *no observable* o al menos *detectable*, se puede agregar una matriz $\mathcal{I}$ a $\mathcal{S}$ para formar una nueva matriz $\mathcal{W} = \mathcal{I} + \mathcal{S}$.

Ahora, sí el par de matrices $(\mathcal{C}, \mathcal{W})$ es cualquiera, *observable* o *detectable*, es bien conocido de la teoría de sistemas lineales que existe un vector constante K tal que, todos o al menos los *valores propios observables* de la matriz $\mathcal{W} - K\mathcal{C}$, se puedan mover a lugares preestablecidos del semiplano izquierdo del plano complejo. La distinción hecha anteriormente, mencionando *valores propios observables*, significa que algunos valores propios de $(\mathcal{C}, \mathcal{W})$ pueden ser *fijos* y no ser influenciados por algún valor de la ganancia del observador. En el caso de un par *detectable*, aquellos valores propios no observables tienen una parte real negativa, si el par de matrices $(\mathcal{C}, \mathcal{W})$ es *observable*, eso significa que todos los valores propios de $\mathcal{W} - K\mathcal{C}$ pueden ser reubicados en el semiplano izquierdo del plano complejo, con la adecuada selección de la matriz K. Como consecuencia, la matriz $(\mathcal{W} - K\mathcal{C})^T$ también manifiesta valores propios con parte real negativa. Esto, también implica que la suma,

$$[\mathcal{W} - K\mathcal{C}] + [\mathcal{W} - K\mathcal{C}]^T = [\mathcal{S} - K\mathcal{C}] + [\mathcal{S} - K\mathcal{C}]^T = 2\left[\mathcal{S} - \frac{1}{2}\left(K\mathcal{C} + \mathcal{C}^T K^T\right)\right] \quad (24)$$

sea una matriz simétrica con valores propios reales negativos.

Se aprecia que la matriz $\mathcal{W} - K\mathcal{C}$ es una matriz cuadrada, con una estructura nada particular. Se puede reemplazar fácilmente dicha matriz por la siguiente suma,

$$\mathcal{W} - K\mathcal{C} = \left[\mathcal{S} - \frac{1}{2}\left(K\mathcal{C} + \mathcal{C}^T K^T\right)\right] + \left[\mathcal{I} - \frac{1}{2}\left(K\mathcal{C} - \mathcal{C}^T K^T\right)\right]. \tag{25}$$

Los sumandos comprendidos en la primer matriz de la ecuación (25), claramente forman una matriz simétrica definida negativa, mientras que lo sumandos contenidos en la segunda matriz, conforman una matriz simétrica.

El sistema dinámico del error (22) puede escribirse en la siguiente forma

$$\dot{e} = \left[\mathcal{J}(y) + \mathcal{I} - \frac{1}{2}\left(K\mathcal{C} - \mathcal{C}^T K^T\right)\right]\frac{\partial H}{\partial e} + \left[\mathcal{S} - \frac{1}{2}\left(K\mathcal{C} + \mathcal{C}^T K^T\right)\right]\frac{\partial H}{\partial e}. \tag{26}$$

Entonces, tomando como función de energía hamiltoniana modificada, la función definida positiva

$$H(x) = \frac{1}{2}\, x^T \mathcal{M}\, x, \tag{27}$$

se encuentra que la derivada en el tiempo de esta función, a lo largo de las trayectorias del sistema dinámico del error (26), se obtiene que

$$\dot{H}(e) = \frac{\partial H(e)}{\partial e^T}\dot{e} = \frac{\partial H(e)}{\partial e^T}\left[\mathcal{S} - \frac{1}{2}\left(K\mathcal{C} + \mathcal{C}^T K^T\right)\right]\frac{\partial H(e)}{\partial e} \leq 0 \tag{28}$$

con $\dot{H}(e) = 0$ si y sólo si $e(t) = 0$.

IV.3.2 Análisis de estabilidad

En esta subsección se determina la estabilidad del error de sincronía (22) obtenido entre el sistema maestro (20) y el observador no lineal (esclavo) (21).

Teorema 1 (Sira-Ramírez y Cruz-Hernández, 2001). *El estado $x(t)$ del sistema caótico (20) puede ser global, asintótica y exponencialmente estimado por el estado $\xi(t)$ de un observador de la forma (21), si el par de matrices $(\mathcal{C}, \mathcal{W})$ ó $(\mathcal{C}, \mathcal{S})$ son observables o al menos detectables.*

La observabilidad en cualquiera de los pares $(\mathcal{C}, \mathcal{W})$ ó $(\mathcal{C}, \mathcal{S})$ es una condición suficiente, mas no necesaria para la reconstrucción asintótica de los estados del maestro (20). Una condición necesaria y suficiente para estabilidad asintótica global del error de estimación está dada por el siguiente teorema.

Teorema 2 (Sira-Ramírez y Cruz-Hernández, 2001). *El estado $x(t)$ del circuito (20) puede ser global, exponencial y asintóticamente estimado, por el estado $\xi(t)$ del observador (21), si y sólo si, existe una matriz constante K tal que, la matriz simétrica*

$$[\mathcal{W} - K\mathcal{C}] + [\mathcal{W} - K\mathcal{C}]^T = [\mathcal{S} - K\mathcal{C}] + [\mathcal{S} - K\mathcal{C}]^T = 2\left[\mathcal{S} - \frac{1}{2}\left(K\mathcal{C} + \mathcal{C}^T K^T\right)\right] \quad (29)$$

sea definida negativa.

IV.4 Sincronización del oscilador de Chua con retardo por formas hamiltonianas y observador

Para facilitar las simulaciones numéricas se acudió a la versión normalizada del oscilador de Chua con retardo (9)-(10), que por comodidad se repiten a continuación

$$\dot{x}_1 = \alpha\left(x_2 - x_1 - f(x_1)\right),$$

$$\begin{aligned}\dot{x}_2 &= x_1 - x_2 + x_3, \\ \dot{x}_3 &= -\beta x_2 - \gamma x_3 - \beta\,\varepsilon sen\left(\sigma x_1\left(t-\tau\right)\right),\end{aligned}$$

con función no lineal

$$f\left(x_1\right) = bx_1 + \frac{1}{2}\left(a-b\right)\left(\left|x_1+1\right| - \left|x_1-1\right|\right).$$

Tomando como función de energía hamiltoniana a la función escalar

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

y el vector gradiente como

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

Con esto, las ecuaciones de estado del **sistema maestro** que describen el oscilador de Chua con retardo, mostrado en la figura 19, en forma canónica hamiltoniana con un campo vectorial desestabilizante, están dadas por

$$\begin{aligned}\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} &= \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & \beta \\ 0 & -\beta & 0 \end{bmatrix} \frac{\partial H}{\partial x} \\ &+ \begin{bmatrix} -\alpha^2 & \alpha & 0 \\ \alpha & -1 & 0 \\ 0 & 0 & -\gamma\beta \end{bmatrix} \frac{\partial H}{\partial x} + \begin{bmatrix} -\alpha f\left(x_1\right) \\ 0 \\ -\beta sen\left(\sigma x_1\left(t-\tau\right)\right) \end{bmatrix}.\end{aligned} \tag{30}$$

Evidentemente el campo vectorial desestabilizante indica que $x_1\left(t\right)$ se use como salida $y\left(t\right)$, del circuito maestro (30). Las matrices $\mathcal{C}$, $\mathcal{S}$ y $\mathcal{I}$, están dadas por

$$\mathcal{C} = \begin{bmatrix} \alpha & 0 & 0 \end{bmatrix}, \quad \mathcal{S} = \begin{bmatrix} -\alpha^2 & \alpha & 0 \\ \alpha & -1 & 0 \\ 0 & 0 & -\gamma\beta \end{bmatrix}, \quad \mathcal{I} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & \beta \\ 0 & -\beta & 0 \end{bmatrix}.$$

El par $(\mathcal{C}, \mathcal{S})$ no es observable ni detectable. Sin embargo, como el par de matrices $(\mathcal{C}, \mathcal{W})$ *es observable*, de acuerdo al teorema 1, es posible diseñar el observador (sistema esclavo) para el sistema maestro (30) como sigue

$$\begin{bmatrix} \dot{\xi}_1 \\ \dot{\xi}_2 \\ \dot{\xi}_3 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & \beta \\ 0 & -\beta & 0 \end{bmatrix} \frac{\partial H}{\partial \xi} + \begin{bmatrix} -\alpha^2 & \alpha & 0 \\ \alpha & -1 & 0 \\ 0 & 0 & -\gamma\beta \end{bmatrix} \frac{\partial H}{\partial \xi} + \begin{bmatrix} -\alpha F(y) \\ 0 \\ -\beta sen(\sigma y(t-\tau)) \end{bmatrix}, \tag{31}$$

y el error de sincronía esta dado por el sistema asintótico y globalmente estable

$$\begin{bmatrix} \dot{e}_1 \\ \dot{e}_2 \\ \dot{e}_3 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 2\beta \\ 0 & -2\beta & 0 \end{bmatrix} \frac{\partial H}{\partial e} + \begin{bmatrix} -\alpha^2 & \alpha & 0 \\ \alpha & -1 & 0 \\ 0 & 0 & -\gamma\beta \end{bmatrix} \frac{\partial H}{\partial e}. \tag{32}$$

Para garantizar una mayor rapidez de la convergencia a cero de las trayectorias del error (32), se puede utilizar el observador (31), pero ahora incluyendo un término del error de la salida de la reconstrucción del estado. El observador resultante esta dado por

$$\begin{bmatrix} \dot{\xi}_1 \\ \dot{\xi}_2 \\ \dot{\xi}_3 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & \beta \\ 0 & -\beta & 0 \end{bmatrix} \frac{\partial H}{\partial \xi} + \begin{bmatrix} -\alpha^2 & \alpha & 0 \\ \alpha & -1 & 0 \\ 0 & 0 & -\gamma\beta \end{bmatrix} \frac{\partial H}{\partial \xi} \tag{33}$$

$$+\begin{bmatrix} -\alpha F(y) \\ 0 \\ -\beta sen(\sigma y(t-\tau)) \end{bmatrix} + \begin{bmatrix} k_1 \\ k_2 \\ k_3 \end{bmatrix} e_y,$$

donde el vector $K = (k_1, k_2, k_3)^T$ se elige apropiadamente, para garantizar estabilidad exponencial asintótica a cero de la trayectoria del error en la reconstrucción del estado (error de sincronía $e(t)$), que representa la velocidad de reconstrucción de los estados del sistema maestro (30). A partir de los sistemas maestro y esclavo (30) y (33), respectivamente, se obtiene que las dinámicas del error de sincronía son gobernadas por el sistema

$$\begin{bmatrix} \dot{e}_1 \\ \dot{e}_2 \\ \dot{e}_3 \end{bmatrix} = \begin{bmatrix} 0 & \frac{k_2\alpha}{2} & \frac{k_3\alpha}{2} \\ -\frac{k_2\alpha}{2} & 0 & 2\beta \\ -\frac{k_3\alpha}{2} & -2\beta & 0 \end{bmatrix} \frac{\partial H}{\partial e} \tag{34}$$
$$+\begin{bmatrix} -\alpha(\alpha+\frac{k_1}{2}) & \alpha\left(1-\frac{k_2}{2}\right) & -\frac{k_3\alpha}{2} \\ \alpha\left(1-\frac{k_2}{2}\right) & -1 & 0 \\ -\frac{k_3\alpha}{2} & 0 & -\sigma\beta \end{bmatrix} \frac{\partial H}{\partial e}.$$

Para encontar los valores k que garanticen estabilidad asintótica a cero del error de sincronía, se invoca el teorema 2, con base en éste, se tiene que:

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

es decir,

$$\begin{bmatrix} -2(\alpha^2+k_1) & 2\alpha-k_2 & -k_3 \\ 2\alpha-k_2 & -2 & 0 \\ -k_3 & 0 & -2\gamma\beta \end{bmatrix} < 0. \tag{35}$$

K debe tomar valores tal que la condición (35) se satisfaga, para esto, el valor elegido para la ganancia K está limitado por las siguientes restricciónes:

$$\begin{aligned} k_1 &\geq 0, \\ k_2 &< 2\alpha + \left(\frac{1}{\gamma\beta}k_3^2 + 4k_1 + 4\alpha^2\right)^{\frac{1}{2}}, \\ k_3 &< 2\left(\gamma\beta\left(k_1 + \alpha^2\right)\right)^{\frac{1}{2}}. \end{aligned}$$

IV.4.1 Resultados numéricos

En esta parte del manuscrito, se presentan los resultados numéricos obtenidos en la sincronización de los circuitos maestro y esclavo, los cuales, son caracterizados con los siguientes valores de los parámetros:

$$\alpha = 10,\ \beta = 19.53,\ \gamma = 0.1636,\ a = -1.4325,\ b = -0.7831,$$

$$\sigma = 3,\ \varepsilon = 0.5 \text{ y } \tau = 5.23$$

y con condiciones iniciales:

$$x\left(0\right) = \left(x_1(0),\ x_2(0),\ x_3(0)\right) = \left(-1, -0.1, 1\right) \text{ y}$$

$$\xi\left(0\right) = \left(\xi_1(0),\ \xi_2(0),\ \xi_3(0)\right) = \left(0, 0, 0\right).$$

Comparando el error de sincronía para diferentes valores de ganancia del observador no lineal (esclavo), la primera columna de la figura 30 presenta las trayectorias del error para una ganancia $k_1 = k_2 = k_3 = 1$, en la segunda columna se muestra el error de sincronía resultante para una ganancia $k_1 = k_2 = k_3 = 3$ y en la tercera columna se ve el error obtenido para la ganancia $k_1 = k_2 = k_3 = 5$. Los valores elegídos para k_1, k_2

y k_3 satisfacen la condición 35. De los errores observados se aprecia que al aumentar la ganancia del observador el tiempo de sincronía disminuye, para $k_1 = k_2 = k_3 = 5$ se considera suficientemente corto.

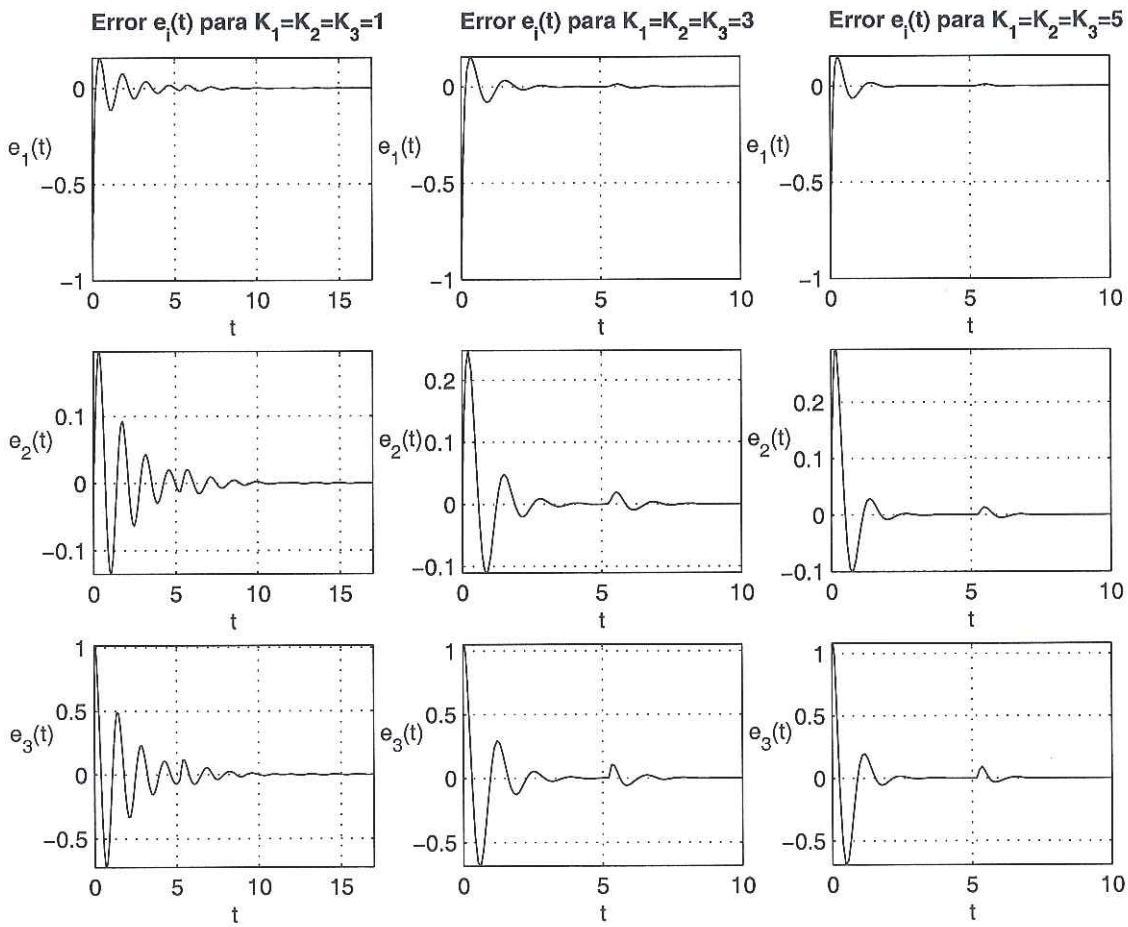


Figura 30: Trayectorias del error de sincronía $e_i(t)$, $i = 1, 2, 3$ para diferentes ganancias del sistema receptor (observador).

A continuación, se describen las simulaciones de las trayectorias correspondientes al oscilador de Chua con retardo y del receptor (observador). La figura 31 muestra las trayectorias del oscilador de Chua con retardo del circuito maestro y las trayectorias generadas por el circuito esclavo (observador). La figura 32 despliega los retratos de

fase de los circuitos maestro y esclavo. La figura 33 ilustra el comportamiento en el tiempo de las trayectorias del error de sincronía entre maestro y esclavo. Mientras que en la figura 34 se aprecia el error de sincronía entre los circuitos maestro y esclavo en el espacio de estado.

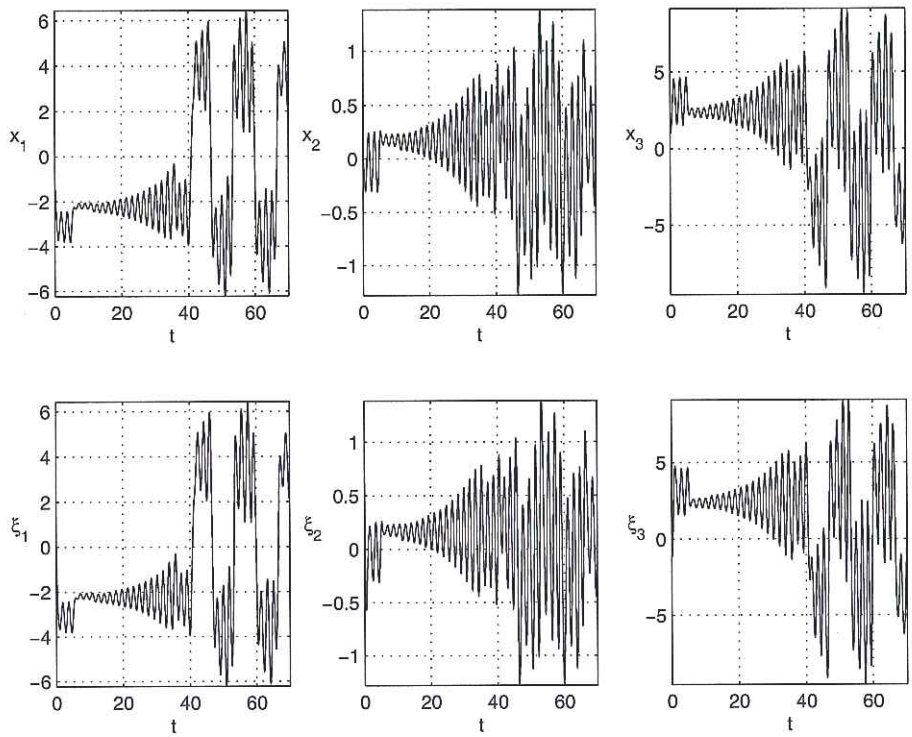


Figura 31: Evolución de los estados en el tiempo de los circuitos de Chua con retardo del sistema maestro y esclavo, $x_i(t)$ y $\xi_i(t)$, $i = 1, 2, 3$, respectivamente.

IV.5 Conclusiones

Se sincronizó el oscilador de Chua con retardo en configuración maestro y esclavo mediante la metodología presentada en (Sira-Ramírez y Cruz-Hernández, 2000; 2001). Primero, se descompuso a dicho circuito en la parte conservativa, la parte disipativa y el vector de campo desestabilizante. De este análisis, se encontró que la señal acoplante

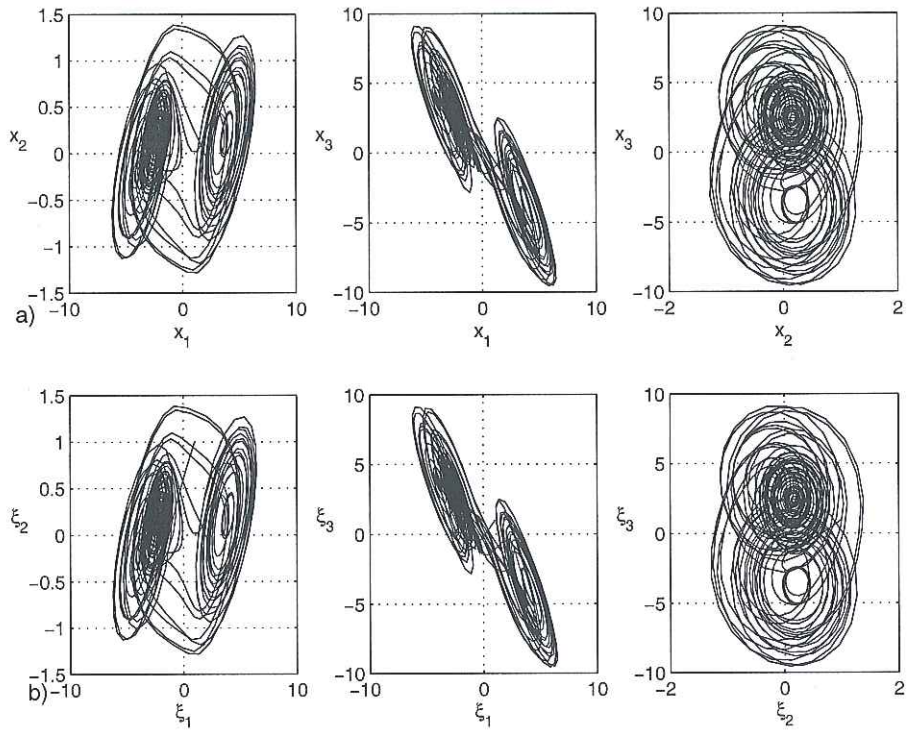


Figura 32: Retratos de fase del oscilador de Chua con retardo (maestro) $x_i(t)$ y retratos de fase del esclavo (sincronizado) correspondiente $\xi_i(t)$, $i = 1, 2, 3$.

para lograr la sincronía es $x_1(t)$. Después de una prueba de observabilidad se diseñó un observador hamiltoniano (esclavo). El análisis y los resultados numéricos presentados manifiestan la efectividad del esclavo diseñado mediante la metodología empleada y una de las grandes ventajas que ofrece este método es que mediante la ganancia K se puede regular el tiempo de sincronía $e(t)$. Finalmente, se concluye que estos sistemas (maestro y esclavo) sincronizados se pueden aplicar en sistemas de encriptamiento caótico, como se mostrará en el capítulo siguiente.

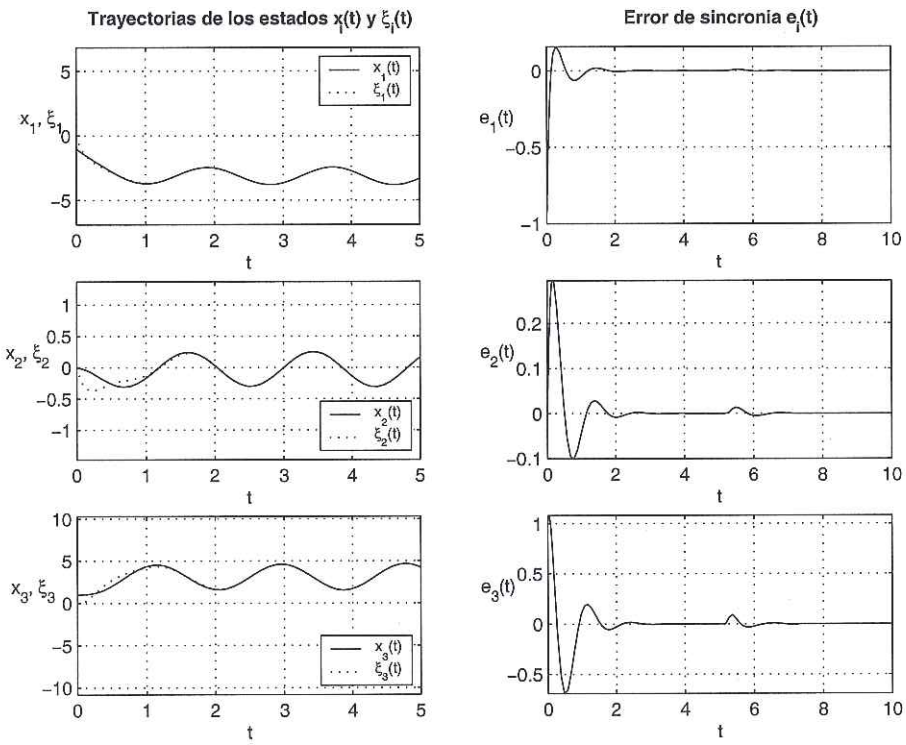


Figura 33: (a) Trayectorias de los estados $x_i(t)$ y $\xi_i(t)$ y el error de sincronía $e_i(t) = x_i(t) - \xi_i(t)$, $i = 1, 2, 3$.

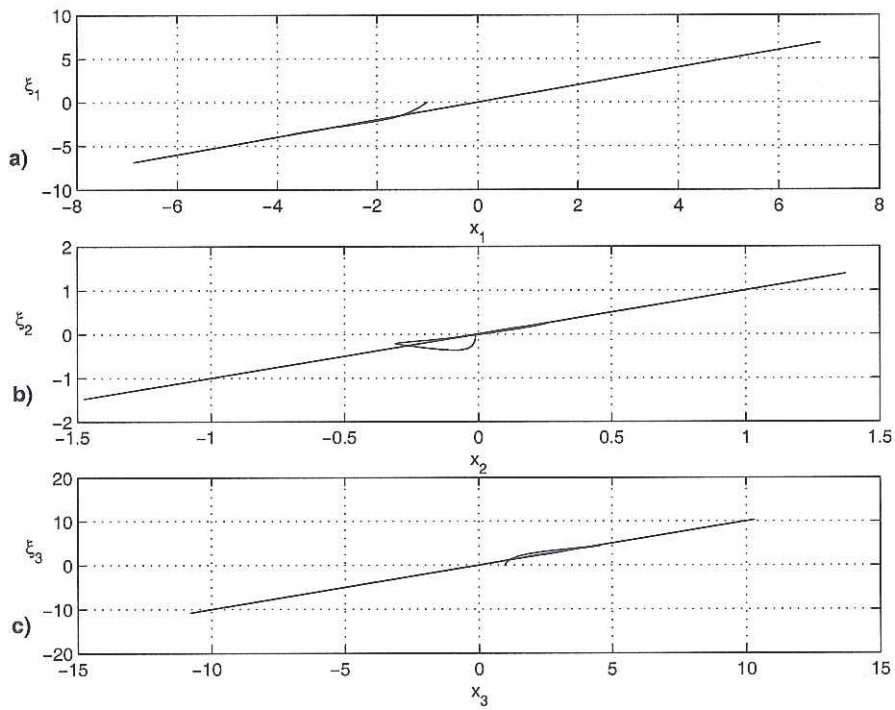


Figura 34: Error de sincronía entre los circuitos maestro y esclavo en el espacio de estado. (a) x_1 vs ξ_1 y (b) x_2 vs ξ_2, (c) x_3 vs ξ_3.

Capítulo V

Comunicaciones analógicas privadas con base en caos

En este capítulo se estudian tres de las principales técnicas de comunicaciones analógicas privadas basadas en caos. La discusión empieza con una descripción de los sistemas de comunicación. Después, se da una breve introducción de la aplicación de caos en las comunicaciones. Primero se describe el esquema de encriptamiento caótico aditivo con una línea de transmisión; en seguida, se explica la modificación propuesta en (López-Mancilla y Cruz-Hernández, en proceso). Luego, se describe la técnica de encriptamiento caótico aditivo utilizando dos líneas de transmisión. Se dan resultados numéricos en la transmisión de un tono y de un mensaje de audio por los diferentes esquemas y al final se mencionan algunas conclusiones.

V.1 Descripción básica de los sistemas de comunicación

Comunicación, es la **transferencia** de información de un lugar a otro. Por otra parte, **información** es un patrón físico no determinístico, al cual, se le asigna un significado comúnmente acordado. El patrón debe ser único, capaz de ser enviado por el transmisor y capaz de ser detectado y entendido por el receptor.

Los sistemas de comunicación, en su forma más sencilla, son sistemas que permiten o mejoran la transmisión de información en diferentes situaciones. El propósito de un

sistema de comunicación es transmitir mensajes de una fuente de información a uno o más destinos. En general, se pueden identificar cuatro componentes básicos en un sistema de comunicación, según lo representado por el diagrama a bloques mostrado en la figura 35, estos son: *fuente de información*, *transmisor*, *canal* y *receptor*.

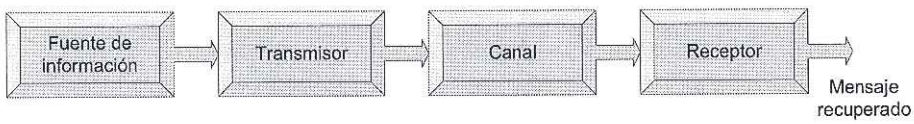


Figura 35: Diagrama a bloques de un sistema simplificado de comunicación.

Fuente de información. Una fuente de información se refiere al origen de la información que necesita ser transmitida. En sistemas de comunicaciones modernos, la información puede codificarse de forma analógica o digital para adecuarla al medio de almacenamiento, procesamiento y transmisión. Por otra parte, la información analógica puede ser convertida a forma digital y viceversa, con fines de almacenamiento, procesamiento y transmisión.

Transmisor. El papel del transmisor es convertir información dada, en una forma apropiada, conveniente para la transmisión a través del canal de comunicación. Para lograr una transmisión eficiente y efectiva, se deben realizar varias operaciones de procesamiento de la señal de información. Por ejemplo, la *modulación*, proceso que se distingue por el acoplamiento de la señal transmitida a las propiedades del canal.

Canal. El canal es el medio físico a través del cual la señal se envía del transmisor al receptor, siendo el puente de unión entre la fuente y el destino de la información. Pueden

identificarse dos tipos básicos de canales, *inalámbricos* (ondas de radio, microondas, infrarojos, etc.) y *alámbricos*, guiados o cableados (fibra óptica, par trenzado, cable coaxial, etc.).

Receptor. En el destino, el mensaje original tiene que ser recuperado. Este es el trabajo del receptor. Por ejemplo, la *demodulación*, el caso inverso del proceso de modulación del transmisor, con lo cual, vuelve la señal de información a su forma original.

V.2 Aplicación de caos a las comunicaciones

Una de las principales aplicaciones de la sincronía de caos se encuentra en el encriptamiento de información en sistemas de comunicación. Las señales caóticas con su característico ancho de banda, son candidatas naturales para codificar información, las señales resultantes son señales con espectros extendidos, tienen grandes anchos de banda y baja densidad de potencia espectral, haciendo más difícil la detección. Por otra parte, es fácil producir gran número de señales con éstas características, como consecuencia de la sensibilidad a las condiciones iniciales y variaciones de los parámetros. Así, el caos provee un bajo costo y una variedad de medios para las comunicaciones de espectro extendido.

Obtenida la sincronización unidireccional de dos sistemas caóticos, puede emplearse de distintas maneras para codificar información confidencial. En este contexto de comunicaciones, el sistema maestro será el **transmisor** y el sistema esclavo el **receptor**. A continuación se describen brevemente dos técnicas de comunicación caótica que se

han estudiado ampliamente.

Encriptamiento caótico aditivo. La idea fundamental del encriptamiento caótico aditivo, es usar una señal portadora producida por un sistema caótico, el mensaje analógico confidencial se suma a la portadora caótica. En el receptor, a partir de la sincronía caótica, se reconstruye la señal caótica original, entonces, el mensaje analógico original es reconstruído restando la señal caótica reproducida de la señal de transmisión.

V.3 Encriptamiento caótico aditivo empleando un canal de transmisión

Usando la propiedad de sincronía de sistemas caóticos, algunos investigadores (Cuomo *et al.*, 1993; Carroll y Pecora, 1991; Kocarev *et al.*, 1992) sugieren la posibilidad de realizar comunicación usando señales caóticas como portadora, con aplicación a la comunicación segura enmascarando la señal de información. En el sistema transmisor se oculta la señal de información dentro de la señal caótica por adición directa; esto es, la señal del mensaje confidencial $m_o(t)$ se suma a la señal caótica acoplante $x_1(t)$ producida por el sistema maestro, generando una señal de transmisión con dinámica muy compleja de la forma $s(t) = x_1(t) + m_o(t)$. Para encriptar, el nivel de potencia de $m_o(t)$ debe ser significativamente más bajo que el de la señal $x_1(t)$. El siguiente paso, es enviar $s(t)$ al sistema receptor. En el extremo del receptor, si el sistema esclavo ha sincronizado con $s(t)$, se produce la señal caótica $\xi_1(t)$, entonces $\xi_1(t) \approx x_1(t)$ por lo que entre la señal acoplante recibida y la señal caótica generada en el receptor, existirá un error de sincronía $e_1(t) = \xi_1(t) - x_1(t)$ distinto a cero y, consecuentemente, la información es recuperada como $m_r(t) = e_1(t)$. En la figura 36, se muestra el esquema de comunicación

empleando una línea de transmisión propuesto por Cuomo y colaboradores en (Cuomo *et al.*, 1993).

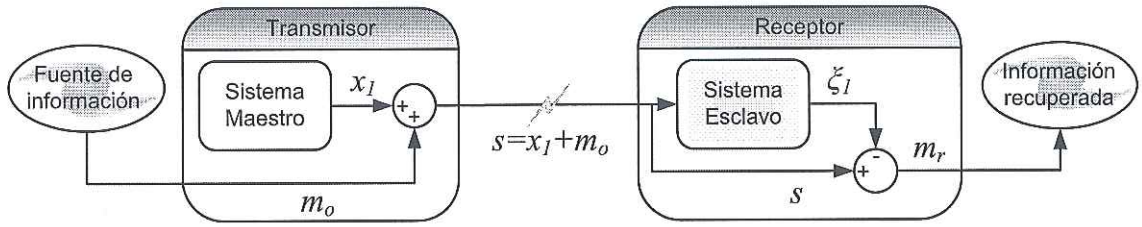


Figura 36: Sistema de encriptamiento caótico aditivo con un canal de transmisión: m_o es el mensaje privado por ser transmitido oculto. x_1 es la señal caótica de sincronía y que se utilizará para enmascarar el mensaje. $s(t) = x_1 + m_o$ es la señal caótica transmitida. m_r, es el mensaje recuperado en el receptor.

V.3.1 Resultados numéricos

Para efectuar las simulaciones numéricas, el circuito de Chua con retardo se utiliza como generador caótico en el sistema transmisor expresado en forma hamiltoniana, mientras que en el sistema receptor va el observador diseñado; de acuerdo al análisis realizado en el Capítulo IV, se emplea como señal acoplante el estado caótico $x_1(t)$, las ganancias del observador $k_1 = k_2 = k_3 = 5$, el circuito se caracteriza con los siguientes valores para los parámetros:

$$\begin{aligned} \alpha &= 10, \ \beta = 19.000, \ \gamma = 0.1636, \ \varepsilon = 0.5, \ \sigma = 3, \\ & a = -1.4325, \ b = -0.7831, \ \tau = 5.23 \end{aligned} \tag{36}$$

y se escogieron las condiciones iniciales:

$$x\,(0) = (-1, -0.1, 1) \ \text{y} \ \xi\,(0) = (0, 0, 0)\,.$$

Transmisión de un tono.

La figura 37 presenta resultados en simulación numérica en la transmisión de un mensaje confidencial analógico, utilizando el esquema de comunicación caótica mostrado en la figura 36. Una onda seno de amplitud 0.1 y de frecuencia 151Hz es utilizada como señal de información privada $m_o(t)$ (figura superior), la cual, estará oculta en la señal caótica $x_1(t)$ (figura central superior). La figura central exhibe la forma de onda de la señal transmitida $s(t) = x_1(t) + m_o(t)$. Mientras que, la figura central inferior describe la forma de onda de la señal recuperada $m_r(t)$ en el sistema receptor. Se puede observar claramente, que la señal $m_r(t)$ no se recupera con fidelidad, sufre de una atenuación de -20dB y es necesario filtrarla, como se puede ver en la figura inferior de la figura 37.

Transmisión de un tono con ruido en el canal de transmisión.

En la figura 38, se muestran los resultados obtenidos al transmitir un mensaje analógico confidencial a través de un canal ruidoso, utilizando el esquema de comunicación mostrado en la figura 36. En la señal caótica $x_1(t)$ (figura central superior), que se usa para sincronizar, se oculta la señal de información privada $m_o(t)$, que consiste de una onda seno de amplitud 0.1 y de frecuencia 151Hz (figura superior). El ruido que se suma al canal de transmisión se muestra en la figura central. Forma de onda de la señal transmitida $s(t) = x_1(t) + m_o(t) + n(t)$ (figura central inferior). El mensaje recuperado $m_r(t)$ se presenta en la figura inferior. En este caso, cuando hay ruido presente en el canal de transmisión, $m_r(t)$ resulta muy afectado.

Transmisión de una señal de audio.

La figura 39 muestra los resultados de la comunicación secreta de un mensaje de audio privado por el esquema de la figura 36. En la figura superior se puede apreciar la forma de onda del mensaje de audio confidencial $m_o(t)$ (fragmento de una canción)

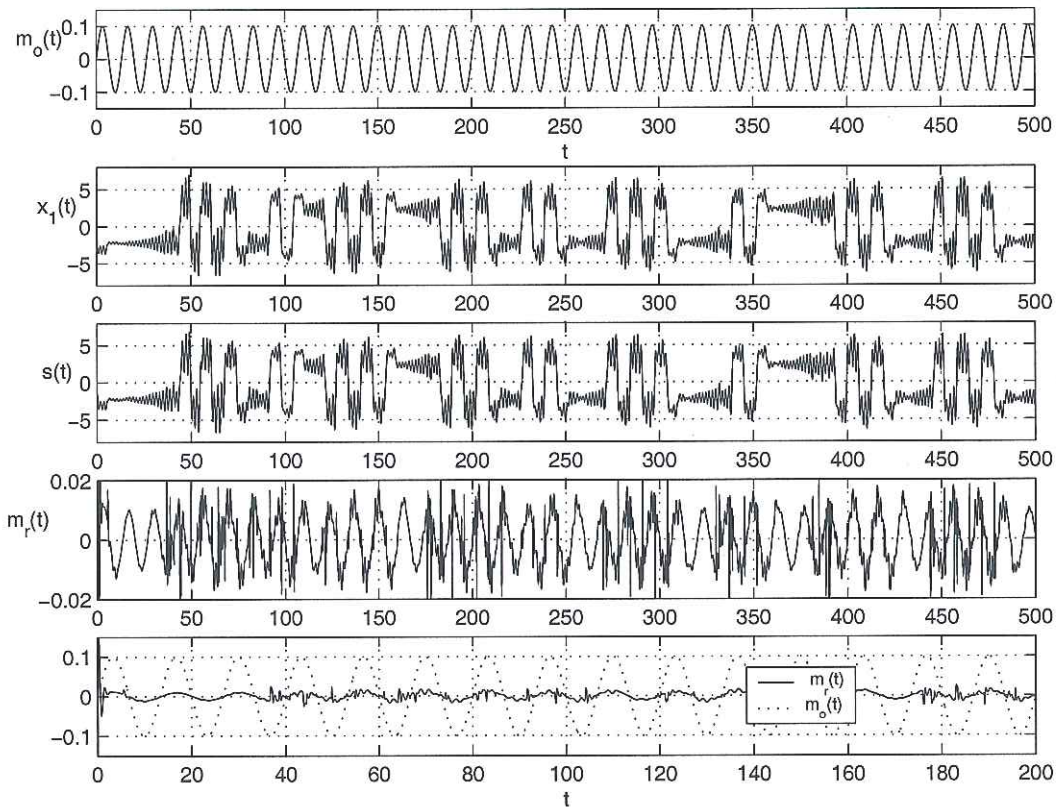


Figura 37: Transmisión de un tono a través del sistema de encriptamiento caótico aditivo con un canal de transmisión: $m_o(t)$ es el mensaje analógico confidencial que se desea ocultar y enviar. $x_1(t)$ corresponde a la señal caótica portadora. $s(t) = x_1(t) + m_o(t)$ es la señal caótica transmitida y $m_r(t)$ es el mensaje confidencial recuperado.

a ser enviado oculto. La siguiente figura presenta la señal caótica portadora $x_1(t)$. $s(t)$ es la señal transmitida con el mensaje oculto (figura del centro). La forma de onda del mensaje de audio recuperado $m_r(t)$ en el lado del receptor se puede ver en la figura inferior.

Transmisión de una señal de audio con ruido en el canal.

La figura 40 muestra los resultados de la comunicación secreta de un mensaje de audio privado transmitido a través de un canal ruidoso, usando el esquema ilustrado en la figura 36. La forma de onda del mensaje de audio confidencial $m_o(t)$ (fragmento

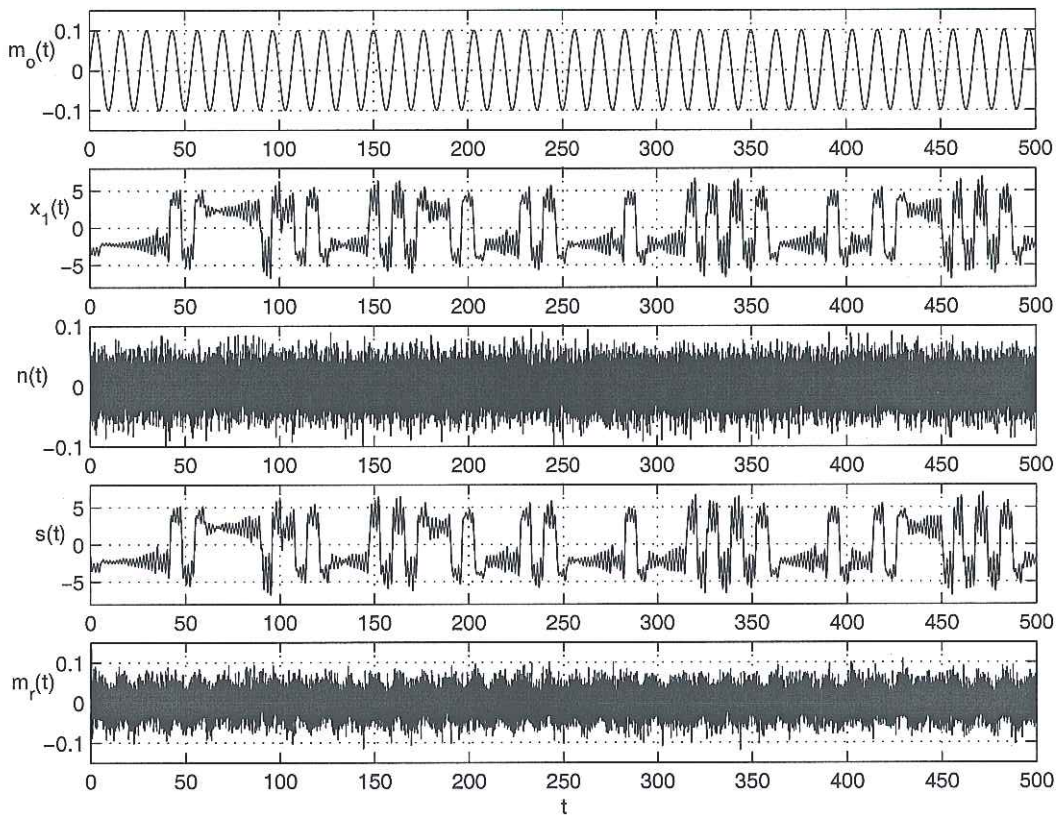


Figura 38: Transmisión de un tono a través de un canal ruidoso empleando el sistema de encriptamiento caótico aditivo mostrado en la figura 36: $m_o(t)$ es el mensaje analógico confidencial que se desea ocultar y enviar; $x_1(t)$ la señal caótica portadora. $s(t) = x_1(t)+m_o(t)$ es la señal caótica transmitida y $m_r(t)$ es el mensaje confidencial recuperado.

de una canción) a ser enviado oculto, se despliega en la figura superior. En la figura central superior aparece la señal caótica portadora $x_1(t)$. Se suma un ruido al canal del orden de -13.98dB con respecto a la señal de información (figura del centro). La señal transmitida $s(t) = x_1(t) + m_o(t)$ se puede ver en la figura central inferior. El mensaje recuperado $m_r(t)$ aparece en la figura inferior.

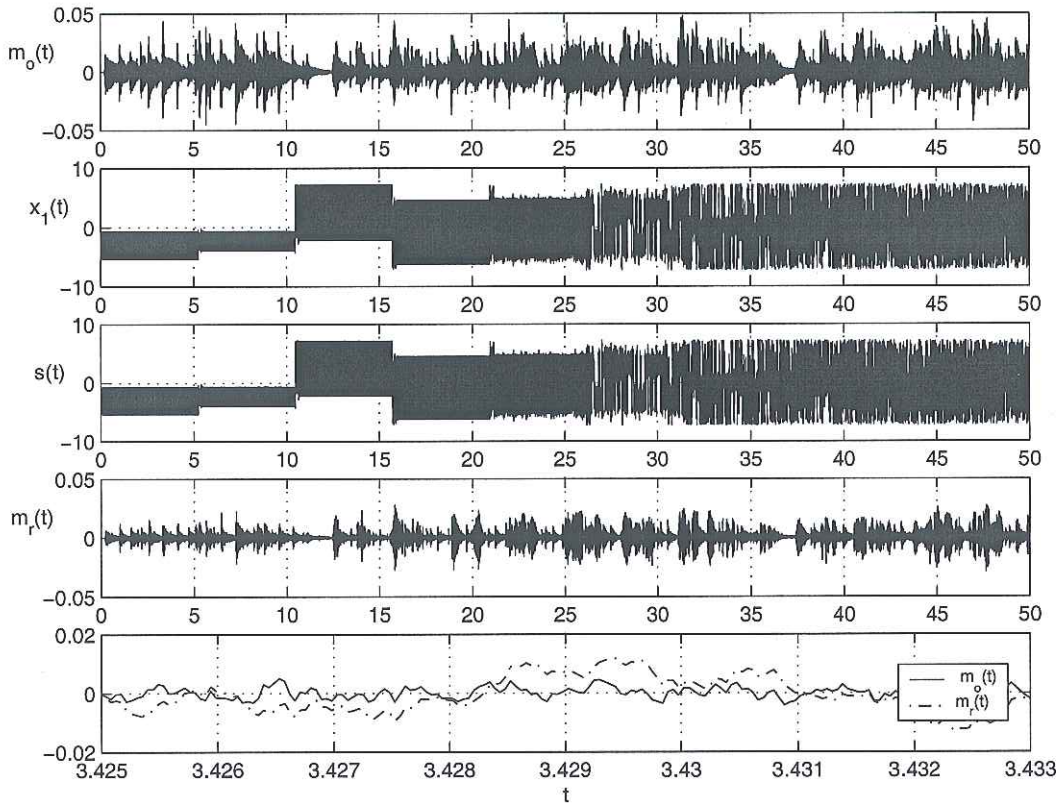


Figura 39: Transmisión de audio a través del sistema de encriptamiento caótico aditivo con un canal de transmisión: $m_o(t)$ es el mensaje de audio (fragmento de una canción confidencial) que se desea ocultar y enviar; $x_1(t)$ la señal caótica portadora; $s(t)$ la señal enviada con el mensaje encriptado y $m_r(t)$ es el mensaje confidencial recuperado.

V.4 Encriptamiento caótico aditivo empleando un canal de transmisión y retroalimentación del mensaje

En el contexto de encriptamiento caótico aditivo por un canal de transmisión, es conocido que, al sumar la señal de información privada a la señal acoplante sufre de ciertas desventajas. La principal desventaja, es cuando el mensaje encriptado se envía a través de la señal acoplante, éste actua como una perturbación y ocasiona que el vector de estados del sistema receptor $\xi(t)$ no sincronice con el vector de estados correspondiente en el sistema transmisor $x(t)$. La consecuencia es que es difícil asegurar

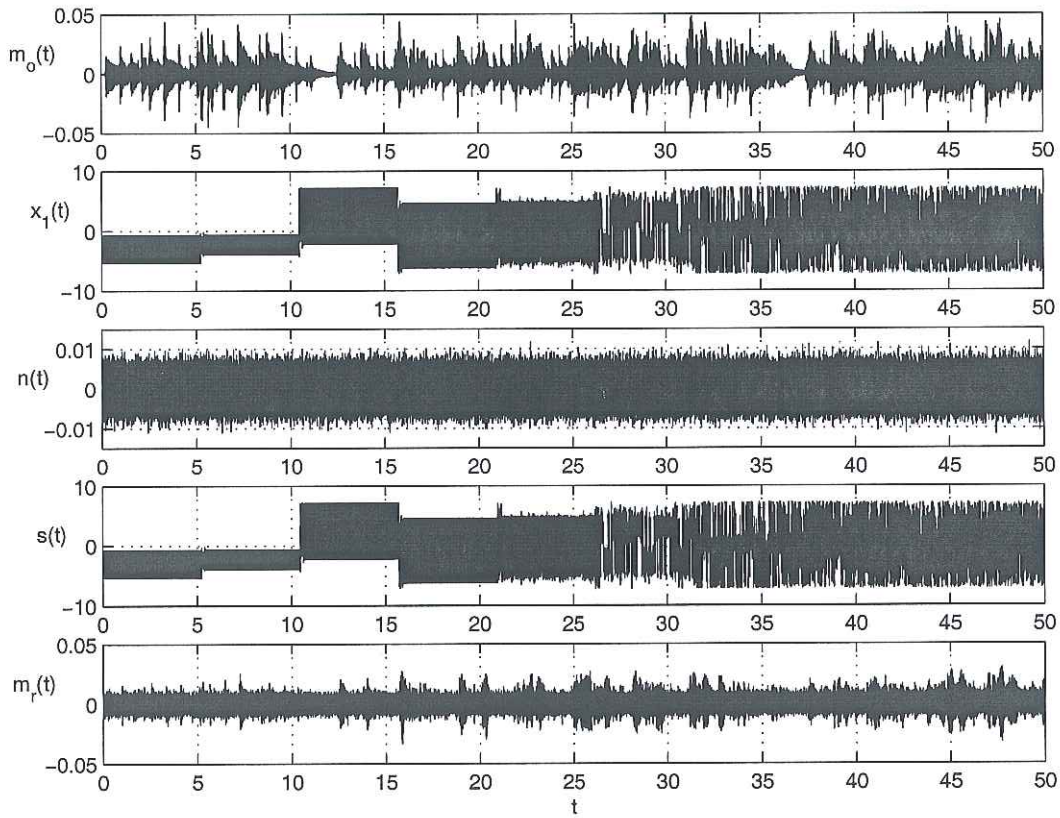


Figura 40: Transmisión de audio a través de un canal ruidoso utilizando el sistema de encriptamiento caótico aditivo con un canal de transmisión: $m_o(t)$ es el mensaje analógico confidencial que se desea ocultar y enviar, $x_1(t)$ la señal caótica portadora, $s(t) = x_1(t) + m_o(t) + n(t)$ la señal transmitida con el mensaje oculto y $m_r(t)$ el mensaje confidencial recuperado.

una reconstrucción exacta del mensaje confidencial, por lo que, es requisito indispensable que el nivel de energía de la señal de información sea muy pequeño con respecto al nivel de energía de la señal caótica portadora. Entre más pequeño sea aquella, habrá más posibilidades de recuperarlo, sin embargo, cuando el nivel de energía del ruido en el canal de transmisión sea igual, o más alto que, la energía de la señal enviada $s(t)$ será muy difícil, si no es que imposible, recuperarlo.

Como se puede observar, el mensaje privado afecta la dinámica del sistema receptor,

resultando en asincronía entre $\xi(t)$ y $x(t)$. Por tanto, es necesario realizar un análisis para ver que sucede con el sistema receptor (López-Mancilla y Cruz-Hernández, en proceso).

Primeramente se recuerda que el sistema **transmisor** tiene la forma especial del sistema hamiltoniano generalizado dada por

$$\begin{aligned} \dot{x} &= \mathcal{J}(y)\frac{\partial H}{\partial x} + (\mathcal{I}+\mathcal{S})\frac{\partial H}{\partial x} + \mathcal{F}(y, y(t-\tau)), \qquad x \in \mathbb{R}^n, \\ y &= \mathcal{C}\frac{\partial H}{\partial x}, \qquad y \in \mathbb{R}^m \end{aligned} \tag{37}$$

y el sistema **receptor**

$$\begin{aligned} \dot{\xi} &= \mathcal{J}(y)\frac{\partial H}{\partial \xi} + (\mathcal{I}+\mathcal{S})\frac{\partial H}{\partial \xi} + \mathcal{F}(y, y(t-\tau)) + K(y-\eta), \qquad \xi \in \mathbb{R}^n \\ \eta &= \mathcal{C}\frac{\partial H}{\partial \xi}, \qquad \eta \in \mathbb{R}^m. \end{aligned} \tag{38}$$

Al sumar $m_o(t)$ a $y(t)$, cambia la forma de la señal acoplante (transmisión),

$$s(t) = m_o(t) + y(t),$$

y al llegar al sistema receptor modifica su estructura, siendo ahora modelado por

$$\begin{aligned} \dot{\xi} &= \mathcal{J}(s)\frac{\partial H}{\partial \xi} + (\mathcal{I}+\mathcal{S})\frac{\partial H}{\partial \xi} + \mathcal{F}(s, s(t-\tau)) + K(s-\eta), \qquad \xi \in \mathbb{R}^n \\ \eta &= \mathcal{C}\frac{\partial H}{\partial \xi}, \qquad \eta \in \mathbb{R}^m. \end{aligned} \tag{39}$$

Se puede observar, que efectivamente, la estructura del sistema receptor se ve afectada cuando se suma la señal $m_o(t)$. Por tanto, es necesario modificar el sistema transmisor. Un esquema más general de esta modificación se presenta en la figura 41, consiste en retroalimentar $m_o(t)$ al sistema maestro, de este modo el mensaje afecta la dinámica de la misma manera que al sistema receptor. Así, la estructura del sistema transmisor es ahora

$$\begin{aligned} \dot{x} &= \mathcal{J}(s)\frac{\partial H}{\partial x} + (\mathcal{I}+\mathcal{S})\frac{\partial H}{\partial x} + \mathcal{F}(s, s(t-\tau)) + K(s-y), \qquad x \in \mathbb{R}^n, \quad (40) \\ y &= \mathcal{C}\frac{\partial H}{\partial x}, \qquad y \in \mathbb{R}^m. \end{aligned}$$

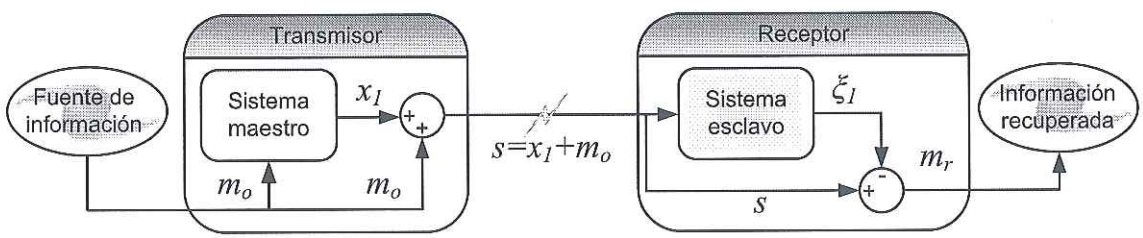


Figura 41: Sistema de encriptamiento caótico aditivo con un canal de transmisión y retroalimentación del mensaje en el transmisor: m_o, es el mensaje privado por ocultarse y transmitirse. x_1 es la señal caótica acoplante, que también se utiliza para enmascarar el mensaje. $s = x_1 + m_o$ es la señal caótica transmitida y m_r es el mensaje recuperado en el receptor.

V.4.1 Resultados numéricos

Empleando el circuito de Chua con retardo como generador caótico y la sincronización por formas hamiltonianas y observador, en la Sección IV.3, se demostró que la salida del sistema maestro es $x_1(t)$, al sumar el mensaje confidencial $m_o(t)$ para ocultarlo, la señal acoplante (transmisión) es

$$s(t) = x_1(t) + m_o(t),$$

con esto, se obtiene que el sistema **transmisor** es modelado por

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & \beta \\ 0 & -\beta & 0 \end{bmatrix} \frac{\partial H}{\partial x} + \begin{bmatrix} -\alpha^2 & \alpha & 0 \\ \alpha & -1 & 0 \\ 0 & 0 & -\gamma\beta \end{bmatrix} \frac{\partial H}{\partial x} + \begin{bmatrix} -\alpha f(s) \\ 0 \\ -\beta sen(\sigma s(t-\tau)) \end{bmatrix} \tag{41}$$

y el sistema **receptor** correspondiente por

$$\begin{bmatrix} \dot{\xi}_1 \\ \dot{\xi}_2 \\ \dot{\xi}_3 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & \beta \\ 0 & -\beta & 0 \end{bmatrix} \frac{\partial H}{\partial \xi} + \begin{bmatrix} -\alpha^2 & \alpha & 0 \\ \alpha & -1 & 0 \\ 0 & 0 & -\gamma\beta \end{bmatrix} \frac{\partial H}{\partial \xi} + \begin{bmatrix} -\alpha F(x_1) \\ 0 \\ -\beta sen(\sigma x_1(t-\tau)) \end{bmatrix} + \begin{bmatrix} k_1 \\ k_2 \\ k_3 \end{bmatrix} e_1. \tag{42}$$

Se emplean ganancias para el observador de $k_1 = k_2 = k_3 = 5$, mientras que los valores de los parámetros son los presentados en (36) y las condiciones iniciales $x(0) = (-1, -0.1, 1)$ y $\xi(0) = (0, 0, 0)$.

Transmisión de un tono.

La figura 42 presenta los resultados de la simulación numérica en la transmisión de un mensaje confidencial analógico, utilizando el esquema de comunicación caótica

mostrado en la figura 41. Una onda seno de amplitud 0.1 y de frecuencia 151Hz es utilizada como señal de información privada $m_o(t)$ (figura superior), la cual, será oculta en la señal caótica $x_1(t)$ (figura central superior). La figura del centro exhibe la forma de onda de la señal transmitida $s(t) = x_1(t) + m_o(t)$. Mientras que la figura central inferior describe la forma de onda de la señal recuperada $m_r(t)$ en el sistema receptor. Se puede observar que la señal $m_r(t)$, después de un comportamiento transitorio son iguales, esto es $e_m(t) = m_o(t) - m_r(t) = 0$.

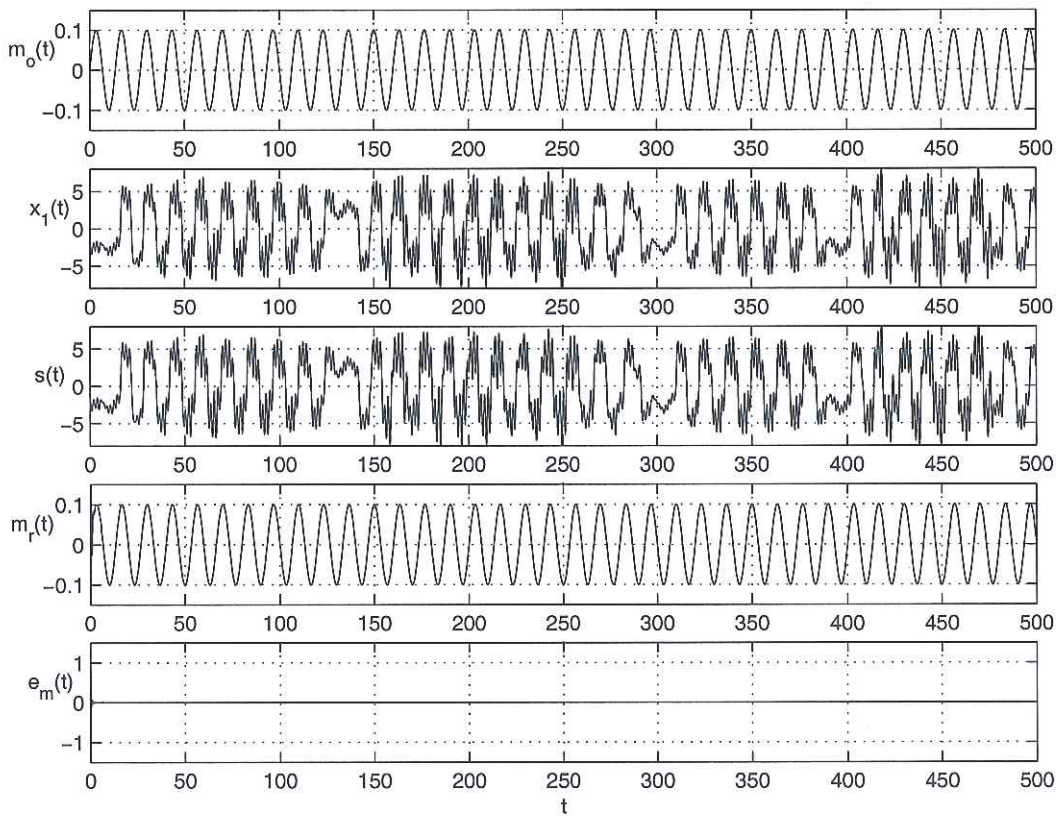


Figura 42: Transmisión de un tono a través del sistema de encriptamiento caótico aditivo con un canal de transmisión y retroalimentación del mensaje: $m_o(t)$ es el mensaje analógico confidencial que se desea ocultar y enviar. $x_1(t)$ corresponde a la señal caótica portadora. $s(t) = x_1(t) + m_o(t)$ es la señal caótica transmitida, $m_r(t)$ es el mensaje confidencial recuperado. $e_m(t) = m_o(t) - m_r(t)$ es el error entre los mensajes original y recuperado.

Transmisión de un tono con ruido en el canal de transmisión.

En la figura 43, se ilustran los resultados obtenidos al transmitir un mensaje analógico confidencial a través de un canal ruidoso, utilizando el esquema de comunicación mostrado en la figura 41. En la señal caótica $x_1(t)$ (figura central superior), que se usa para sincronizar, se oculta la señal de información privada $m_o(t)$, que consiste de una onda seno de amplitud 0.1 y de frecuencia 151Hz (figura superior). El ruido que se suma al canal de transmisión se muestra en la figura del centro. Forma de onda de la señal transmitida $s(t) = x_1(t) + m_o(t) + n(t)$ (figura central inferior). El mensaje recuperado $m_r(t)$ se presenta en la figura inferior.

Transmisión de una señal de audio.

La figura 44 muestra los resultados de la comunicación secreta de un mensaje de audio privado por el esquema de la figura 41. En la figura superior se puede apreciar la forma de onda del mensaje de audio confidencial $m_o(t)$ (fragmento de una canción) a ser enviado oculto. La figura central superior presenta la señal caótica portadora $x_1(t)$. $s(t) = x_1(t) + m_o(t)$ es la señal transmitida con el mensaje oculto (figura del centro). La forma de onda del mensaje de audio recuperado $m_r(t)$ en el extremo del receptor se puede ver en la figura central inferior. El error entre el mensajes original y el mensaje recuperado $e_m(t)$ se presenta en la figura inferior.

En la figura 45 se presenta una amplificación de $e_m(t)$, error que existe entre los mensajes de audio transmitido y recuperado por el esquema de comunicación caótica mostrado en la figura 41.

Transmisión de una señal de audio con ruido en el canal.

La figura 46 muestra los resultados en la comunicación secreta de un mensaje de

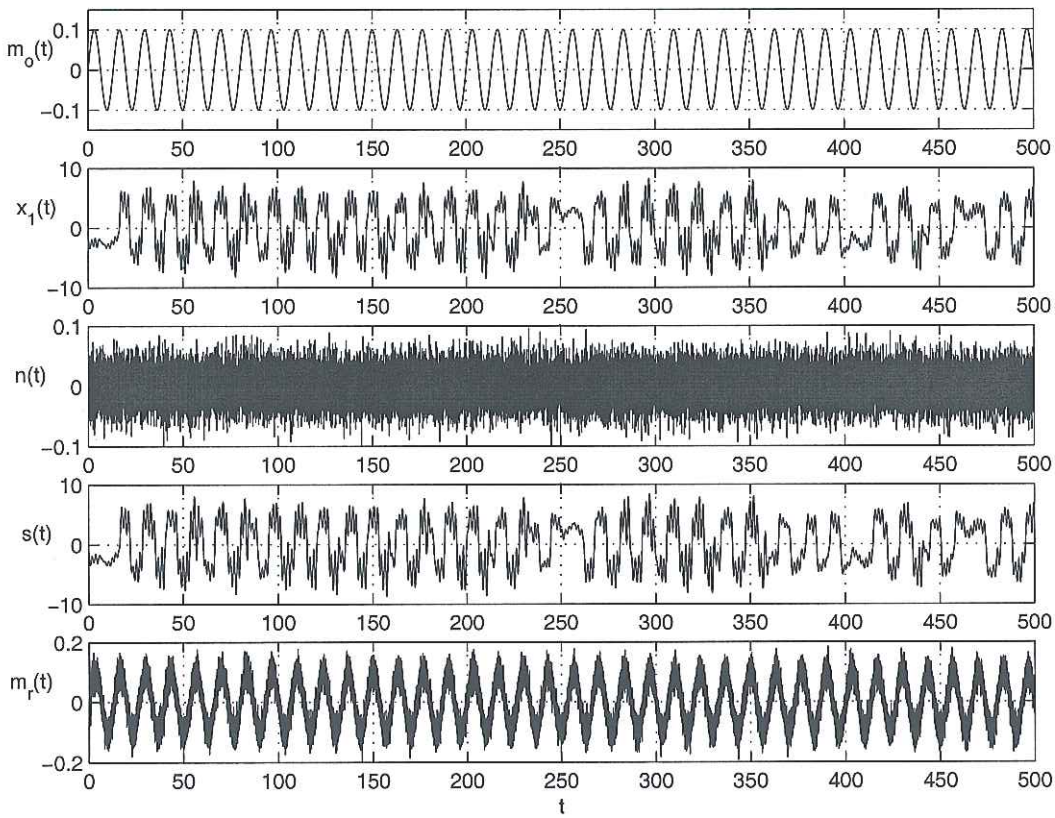


Figura 43: Transmisión de un tono a través de un canal ruidoso empleando el sistema de encriptamiento caótico aditivo seguro mostrado en la figura 41: $m_o(t)$ es el mensaje analógico confidencial que se desea ocultar y enviar; $x_1(t)$ la señal caótica portadora. $s(t) = x_1(t) + m_o(t) + n(t)$ es la señal caótica transmitida y $m_r(t)$ es el mensaje confidencial recuperado.

audio privado, transmitido a través de un canal ruidoso, usando el esquema ilustrado en la figura 41. La forma de onda del mensaje de audio confidencial $m_o(t)$ (fragmento de una canción) a ser enviado oculto, se despliega en la figura central superior. Mientras que, en la figura central superior aparece la señal caótica portadora $x_1(t)$. Se suma un ruido al canal del orden de -13.98dB con respecto a la señal de información privada (figura del centro). La señal transmitida $s(t) = x_1(t) + m_o(t) + n(t)$ se puede ver en la figura central inferior. El mensaje recuperado $m_r(t)$ aparece en la figura inferior.

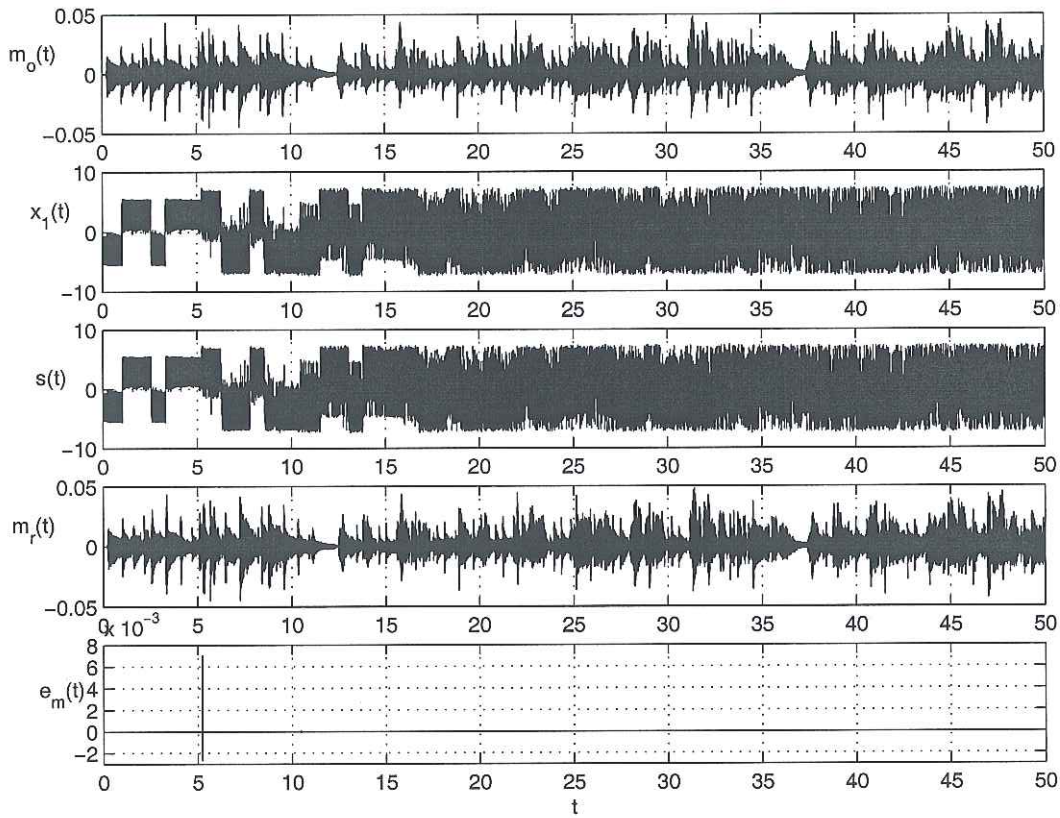


Figura 44: Transmisión de audio a través del sistema de encriptamiento caótico aditivo con un canal de transmisión y retroalimentación del mensaje: $m_o(t)$ es el mensaje de audio confidencial (fragmento de una canción) que se desea ocultar y enviar; $x_1(t)$ la señal caótica portadora; $s(t)$ la señal enviada con el mensaje encriptado; $m_r(t)$ es el mensaje confidencial recuperado; $e_m(t) = m_o(t) - m_r(t)$ es la diferencia entre el mensaje original y el recuperado.

V.5 Encriptamiento caótico aditivo empleando dos canales de transmisión

Otra manera de transmisión segura de información empleando encriptamiento caótico aditivo se logra usando dos canales de comunicación en lugar de uno (Pecora y Carroll, 1990) (ver figura 47). El algoritmo esta compuesto de 3 pasos: 1) *sincronización*, 2) *encriptado* y 3) *decodificación*. En el primer paso se transmite por un canal la señal acoplante, digamos $x_1(t)$ la cual, es uno de los estados del transmisor caótico. Es importante precisar que esta señal se utiliza solamente para lograr una rápida sincronía.

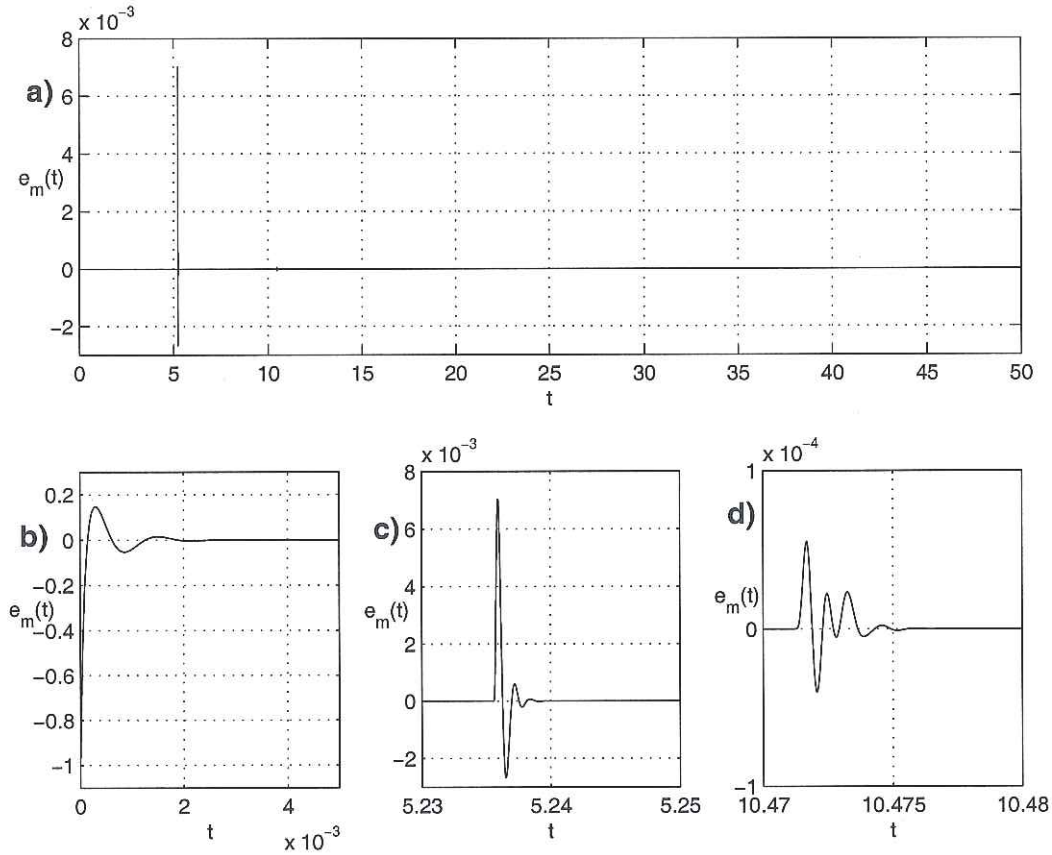


Figura 45: Error entre los mensaje de audio transmitido y recuperado por el esquema de comunicación caótica que se muestra en la figura 41.

En el segundo paso, se selecciona el estado caótico con mayor dinámica, por ejemplo $x_2(t)$, al cual se le suma la señal de información privada $m_o(t)$, formando así la señal encriptada $s(t)$. La señal encriptada es transmitida al receptor por el canal restante. En el tercer paso, el mensaje es recuperado en el extremo del receptor por medio de la comparación entre las señales $s(t)$ y $\xi_2(t)$.

Con este esquema, se obtiene una sincronización más rápida y se aumenta la seguridad. Al hacer esto, el encriptamiento y la sincronía son completamente separados sin interferencia entre ellos; dado que un canal se utiliza para enviar la señal caótica $x_1(t)$

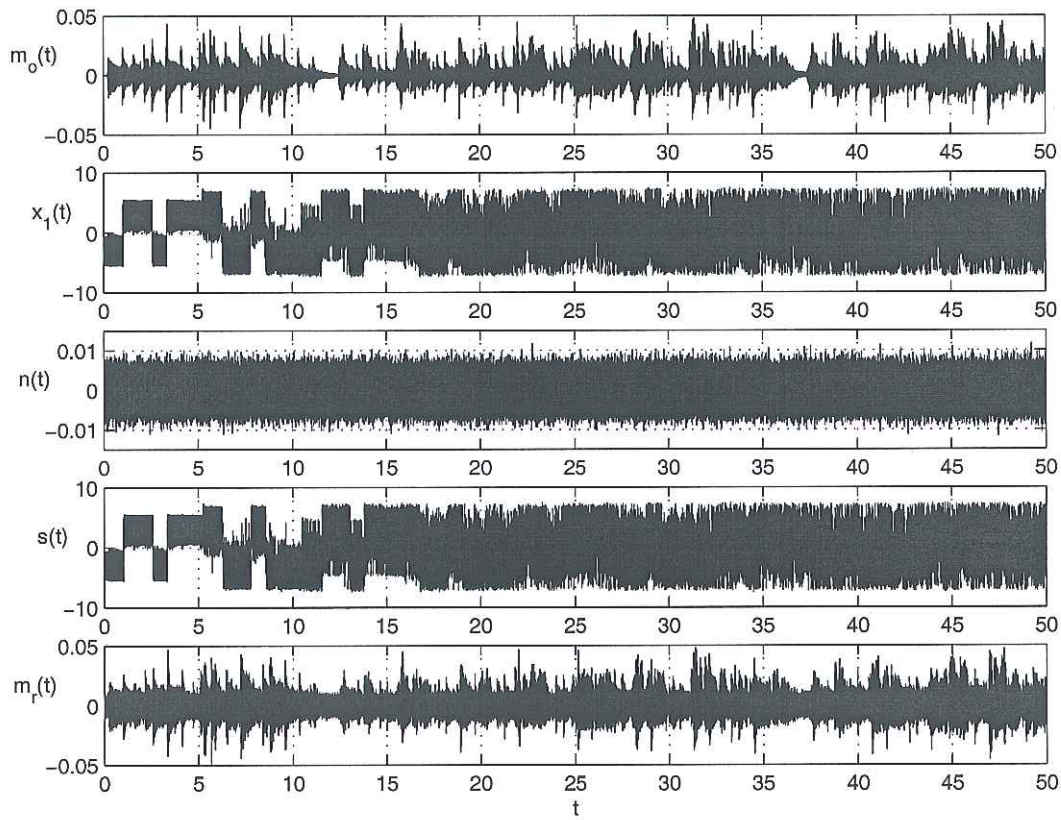


Figura 46: Transmisión de audio a través de un canal ruidoso utilizando el sistema de encriptamiento caótico aditivo con un canal de transmisión y retroalimentación del mensaje: $m_o(t)$ es el mensaje analógico confidencial que se desea ocultar y enviar, $x_1(t)$ la señal caótica portadora, $s(t) = x_1(t) + m_o(t) + n(t)$ la señal transmitida con el mensaje oculto y $m_r(t)$ el mensaje confidencial recuperado.

del transmisor que se usa para sincronizar, sin conexión con el mensaje secreto $m_o(t)$. Mientras que el otro canal se utiliza para transmitir el mensaje oculto $s(t)$.

V.5.1 Resultados numéricos

Para obtener los resultados de las simulaciones numéricas, se utiliza el modelo del circuito de Chua con retardo (41) en el sistema transmisor como generador caótico, sincronizado por formas hamiltonianas con el sistema receptor (42); en el análisis

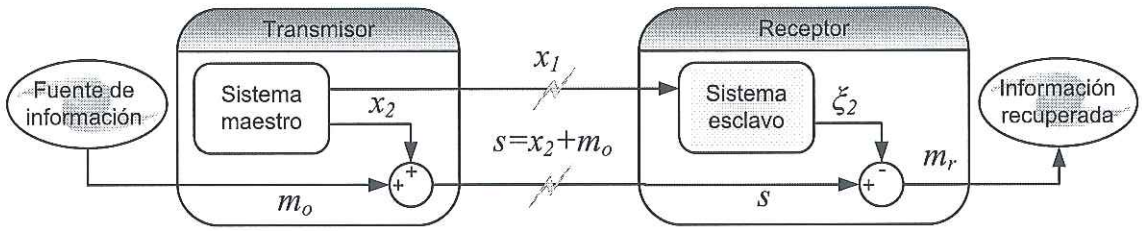


Figura 47: Sistema de encriptamiento caótico aditivo con dos canales de transmisión: m_o es el mensaje privado por ocultarse y transmitirse. x_1 es la señal caótica de sincronía. x_2 es la señal caótica que se utilizará para ocultar y enviar la información. $s = x_2 + m_o$ es la señal caótica transmitida y m_r es el mensaje recuperado.

realizado en el Capítulo IV, se indica que el estado $x_1(t)$ se debe usar como señal acoplante, las ganancias del observador $k_1 = k_2 = k_3 = 5$, el circuito se caracteriza con valores de los parámetros mostrados en (36) y condiciones iniciales:

$$x\,(0) = (-1, -0.1, 1) \text{ y } \xi\,(0) = (0, 0, 0)\,.$$

Transmisión de un tono.

La figura 48 presenta los resultados de la simulación numérica del esquema de comunicación caótica mostrado en la figura 47. Una onda seno de amplitud 0.1 y de frecuencia 151Hz es utilizada como señal de información privada $m_o(t)$ (figura superior), la cual será, ocultada en la señal caótica $x_2(t)$ (figura central superior). La figura del centro exhibe la forma de onda de la señal transmitida $s(t) = x_1(t) + m_o(t)$. Mientras que, la figura central inferior describe la forma de onda de la señal recuperada $m_r(t)$ en el sistema receptor. Se puede observar que la señal $m_r(t)$, después de un comportamiento transitorio son iguales, esto es, $e_m(t) = m_o(t) - m_r(t) = 0$.

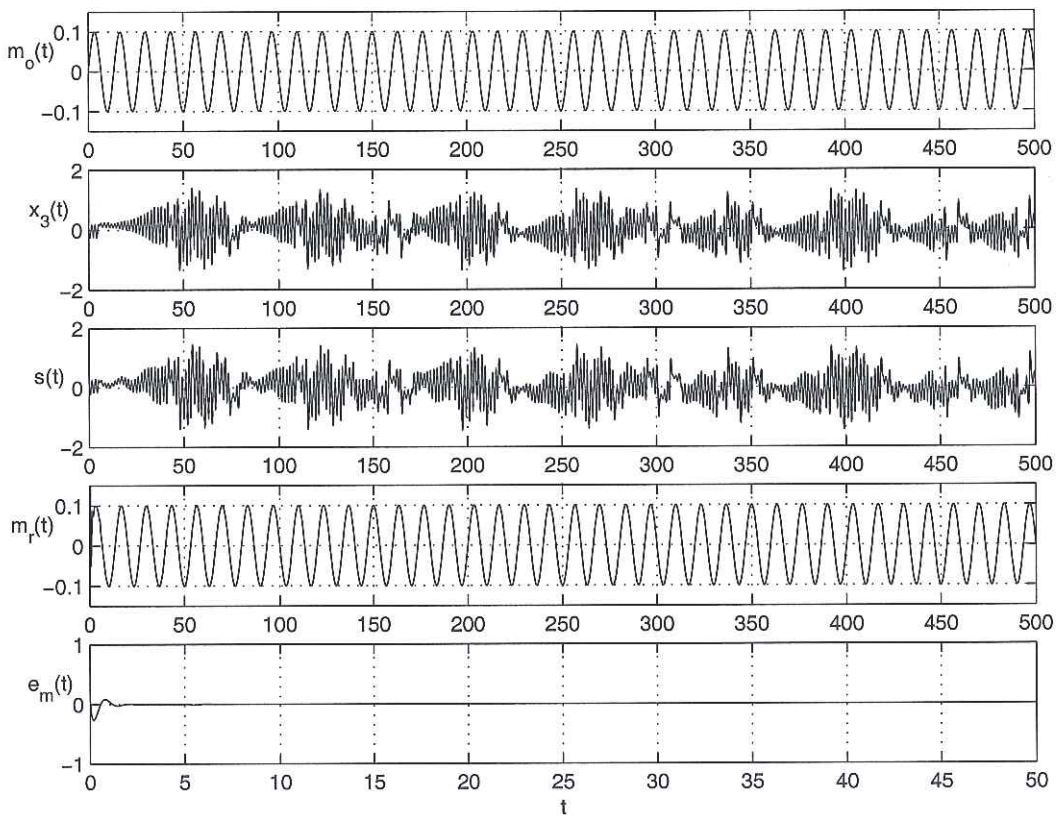


Figura 48: Transmisión de un tono a través del sistema de encriptamiento caótico aditivo con dos canales de transmisión: figura superior: $m_o(t)$ es el mensaje analógico confidencial que se desea ocultar y enviar. $x_2(t)$ corresponde a la señal caótica portadora. $s(t) = x_2(t) + m_o(t)$ es la señal caótica transmitida, $m_r(t)$ es el mensaje confidencial recuperado. $e_m(t) = m_o(t) - m_r(t)$ es el error entre los mensajes original y recuperado.

Transmisión de un tono con ruido en el canal de transmisión.

En la figura 49, se ilustran los resultados obtenidos al transmitir un mensaje analógico confidencial a través de un canal ruidoso, utilizando el esquema de comunicación mostrado en la figura 47. En la señal caótica $x_2(t)$ (figura central superior) se oculta la señal de información privada $m_o(t)$, que consiste de una onda seno de amplitud 0.1 y de frecuencia 151Hz (figura superior). El ruido que se suma al canal de transmisión se muestra en la figura del centro. Forma de onda de la señal transmitida $s(t) = x_2(t) + m_o(t) + n(t)$ (figura central inferior). El mensaje recuperado $m_r(t)$ se presenta en la figura inferior.

Transmisión de una señal de audio.

La figura 50 muestra los resultados de la comunicación secreta de un mensaje de audio privado por el esquema de la figura 47. En la figura superior se puede apreciar la forma de onda del mensaje de audio confidencial $m_o(t)$ (fragmento de una canción) a ser enviado oculto. La siguiente figura presenta la señal caótica portadora $x_2(t)$. $s(t) = x_2(t) + m_o(t)$, es la señal transmitida con el mensaje oculto (figura del centro). La forma de onda del mensaje de audio recuperado $m_r(t)$ en el lado del receptor se puede ver en la figura central inferior. El error entre el mensaje original y el mensaje recuperado $e_m(t)$ se presenta en la figura inferior.

En la figura 51 se presenta una amplificación de $e_m(t)$, error que existe entre los mensaje de audio transmitido y recuperado, por el esquema de comunicación seguro que se muestra en la figura 47.

Transmisión de una señal de audio con ruido en el canal.

La figura 52 muestra los resultados de la comunicación secreta de un mensaje de

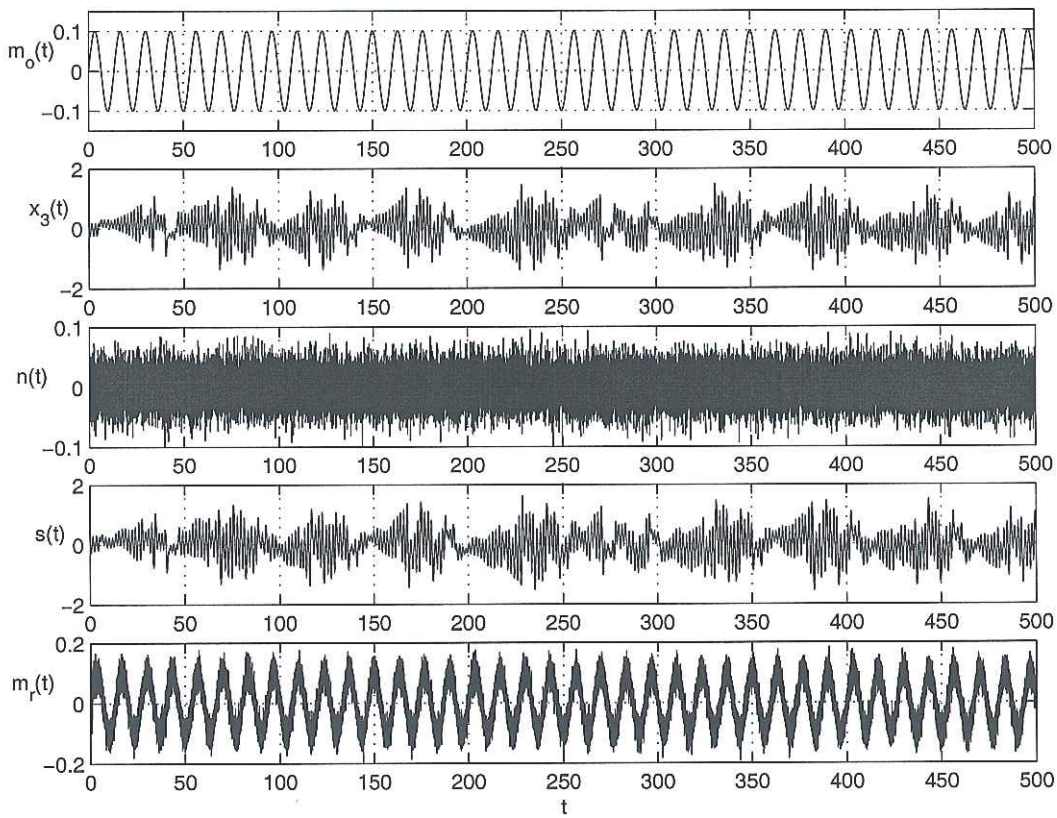


Figura 49: Transmisión de un tono a través de un canal ruidoso empleando el sistema de encriptamiento caótico aditivo mostrado en la figura 47: $m_o(t)$ es el mensaje analógico confidencial que se desea ocultar y enviar; $x_2(t)$ la señal caótica portadora. $s(t) = x_2(t) + m_o(t) + n(t)$ es la señal caótica transmitida y $m_r(t)$ es el mensaje confidencial recuperado.

audio privado transmitido a través de un canal ruidoso, usando el esquema ilustrado en la figura 47. La forma de onda del mensaje de audio confidencial $m_o(t)$ (fragmento de una canción) a ser enviado oculto se despliega en la figura superior. Mientras que, en la figura central superior aparece la señal caótica portadora $x_1(t)$. Se suma ruido al canal del orden de -13.98dB con respecto a la señal de información privada (figura del centro). La señal transmitida $s(t) = x_2(t) + m_o(t) + n(t)$ se puede ver en la figura central inferior. El mensaje recuperado $m_r(t)$ aparece en la figura inferior.

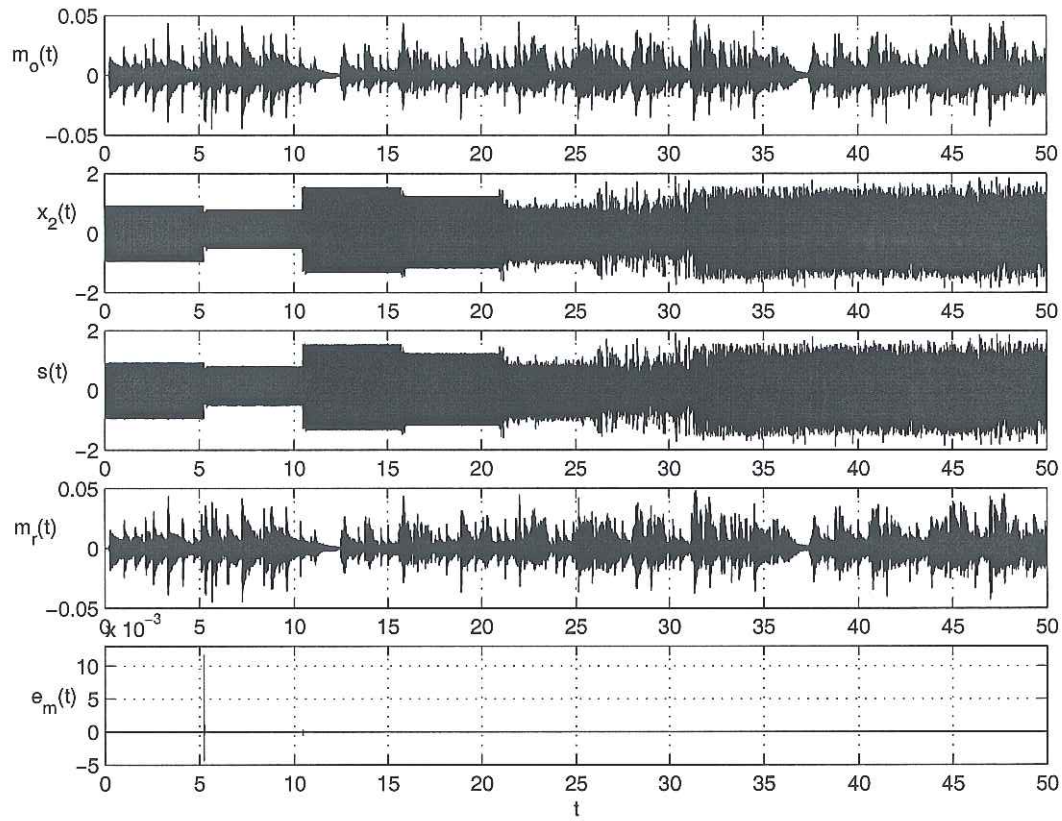


Figura 50: Transmisión de audio a través del sistema de encriptamiento caótico aditivo con dos canales de transmisión: $m_o(t)$ es el mensaje de audio confidencial (fragmento de una canción) que se desea ocultar y enviar; $x_1(t)$ la señal caótica portadora; $s(t)$ la señal enviada con el mensaje encriptado; $m_r(t)$ es el mensaje confidencial recuperado; $e_m(t) = m_o(t) - m_r(t)$ es la diferencia entre el mensaje original y el recuperado.

V.6 Conclusiones

Utilizando la sincronía de dos circuitos de Chua con retardo obtenida en el Capítulo IV, se diseñaron tres diferentes sistemas encriptadores de información analógica. En los resultados numéricos obtenidos se encontró, que al transmitir información privada con el sistema de encriptamiento caótico aditivo con una línea de transmisión, el mensaje recuperado se ve afectado en magnitud y fase, además, contiene armónicos que no forman parte de la señal original, ya que la señal de información es enviada a través de la señal acoplante y el receptor no alcanza una sincronía exacta. Al utilizar el mismo

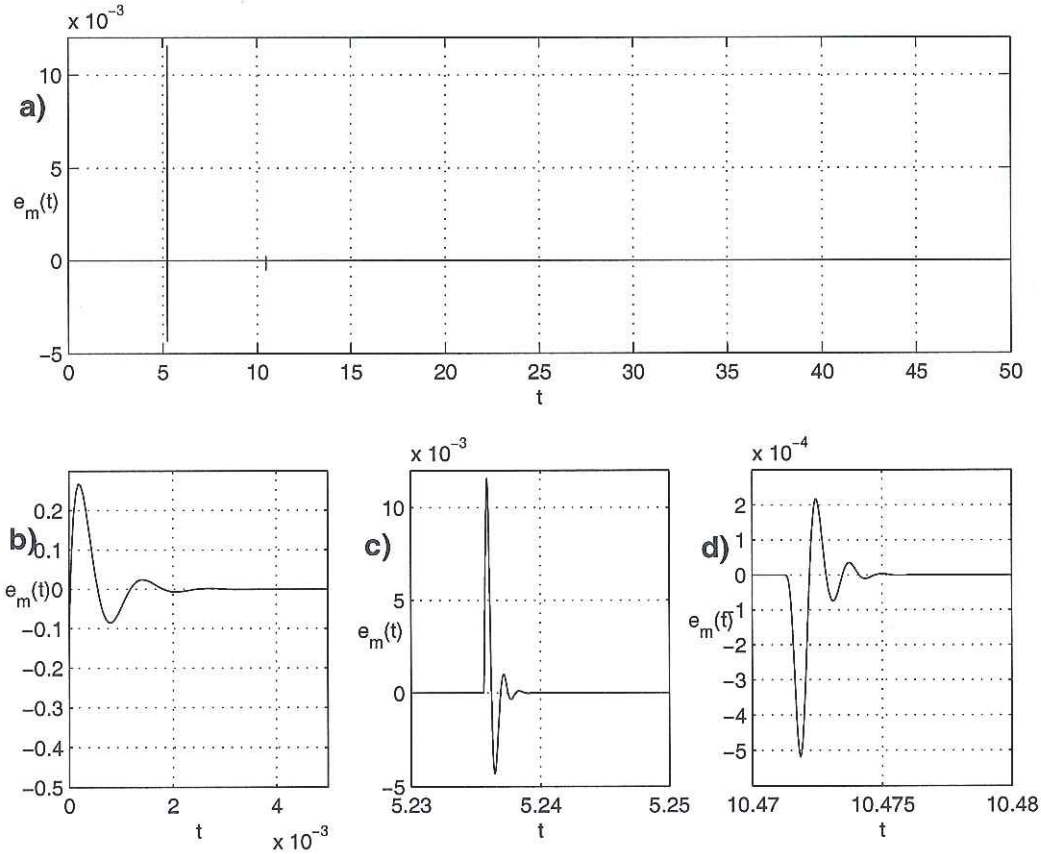


Figura 51: Error entre los mensaje de audio transmitido y recuperado por el esquema de comunicación seguro que se muestra en la figura 47.

esquema pero con retroalimentación del mensaje privado en el sistema transmisor, se logró recuperar el mensaje oculto con precisión y suficiente fidelidad. Los resultados obtenidos en la comunicación privada por dos líneas de transmisión muestran que este esquema ayuda a aumentar la seguridad y no existe problema en la reconstrucción del mensaje confidencial. Se realizaron pruebas añadiendo ruido al canal de transmisión, en este caso, el esquema de comunicación caótico con una línea de transmisión y retroalimentación del mensaje y el esquema con dos líneas son capaces de recobrar el mensaje oculto con gran semejanza al mensaje original, mientras que con el sistema de encriptamiento caótico con una línea de transmisón esto no es posible.

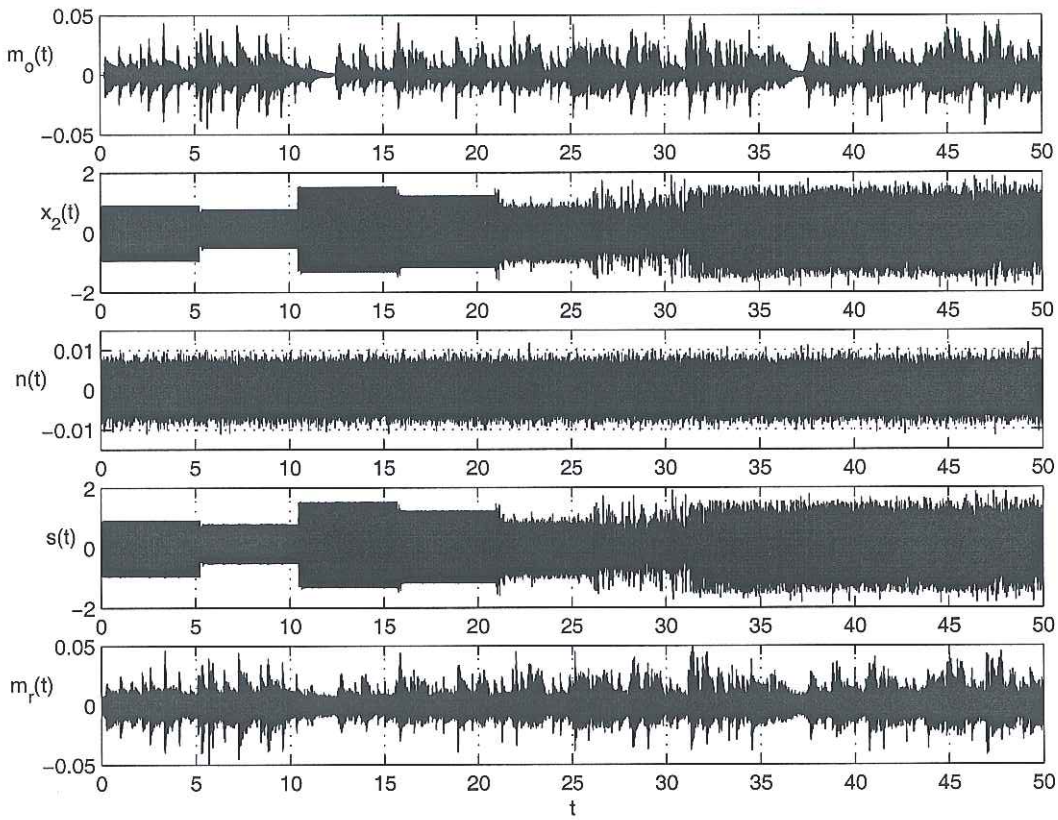


Figura 52: Transmisión de audio a través de un canal ruidoso utilizando el sistema de encriptamiento caótico aditivo con dos canales de transmisión: $m_o(t)$ es el mensaje analógico confidencial que se desea ocultar y enviar, $x_1(t)$ la señal caótica portadora, $s(t) = x_1(t) + m_o(t) + n(t)$ la señal transmitida con el mensaje oculto y $m_r(t)$ el mensaje confidencial recuperado.

Capítulo VI

Comunicaciones digitales privadas con base en caos

En este capítulo comienza la presentación formal de los sistemas de comunicaciones digitales seguros basados en caos. Se empieza con el estudio del esquema propuesto por Parlitz y colaboradores en (Parlitz *et al.*, 1992), que consiste basicamente en ocultar información binaria con dos diferentes señales caóticas. Después, se expone el ataque propuesto por Pérez y Cerdeira en (Pérez y Cerdeira, 1995). Luego, se trata la técnica de comunicación que emplea conmutación entre múltiples atractores caóticos para ocultar información digital confidencial propuesta por Palaniyandi y Lakshmananen (2001) para superar la vulnerabilidad antes mencionada. Al final del capítulo se presentan las conclusiones correspondientes.

VI.1 Conmutación entre dos atractores caóticos

Una pequeña diferencia en los valores paramétricos en los sistemas maestro y esclavo, causará asincronía entre los estados del transmisor y receptor. Usando esta propiedad, surge un método muy sencillo para la transmisión oculta de señales digitales, ver por ejemplo (Parlitz *et al.*, 1992; Cuomo *et al.*, 1993), esta idea se explica a continuación.

En esta técnica, el mensaje binario $m_o(t)$ se utiliza para modular uno o más parámetros del transmisor, es decir, en el transmisor se escoge un parámetro p, para tal propósito. Por ejemplo, el parametro p puede adquirir cualquier valor digamos p_1

ó p_2 (ver figura 53). El valor del parámetro p en el receptor se mantiene en un valor constante p_1, mientras en el transmisor se alterna entre dos valores, p_1 y p_2, cuando la señal de información es "1" y "0", respectivamente. Así, según el valor de $m_o(t)$ en cualquier tiempo dado t, en el transmisor el parámetro tiene el valor p_1 o el valor para el parámetro de p_2. El mensaje digital $m_o(t)$ transmitido, es reconstruido en el receptor, usando la potencia del error de sincronía $[\xi_1(t) - x(t)]^2$. Esta es cero, cuando receptor y transmior están sincronizados, mientras que ésta tiene un valor diferente de cero, cuando no están sincronizados. Así, el receptor sincronizará con el transmisor cuando el parámetro p adquiera el valor de p_1, mientras que habrá asincronía, cuando el parámetro p adquiera tome el valor de p_2 en el transmisor. Esta situación puede ser interpretada en el receptor como un "1" o un "0".

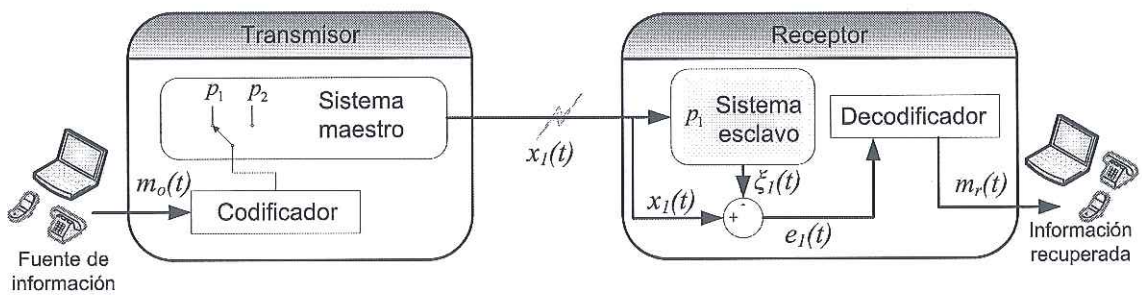


Figura 53: Sistema de comunicación digital empleando conmutación caótica.

VI.1.1 Resultados numéricos empleando el circuito de Chua clásico como generador caótico

En esta parte del manuscrito, se ilustra la transmisión digital confidencial, empleando el sistema de comunicación caótica descrito arriba y mostrado en la figura 53. Se utilizara el circuito de Chua clásico (3)-(4) como generador de caos en este sistema. Se selecciona β como el parámetro a conmutar, el resto de los parámetros se mantienen en valores

fijos. Se utiliza la regla de modulación para modular la información digital $m_o(t)$ como sigue

$$\beta(t) = \beta + r \cdot m_o(t),$$

con $r = 0.001$; el parámetro β cambia en las ecuaciones del transmisor entre el valor de referencia $\beta = \beta(1) = 15.620$ y $\beta = \beta(0) = 15.621$. El parámetro correspondiente en el sistema receptor se mantiene fijo en el valor de referencia, esto se puede apreciar mejor en la figura 54.

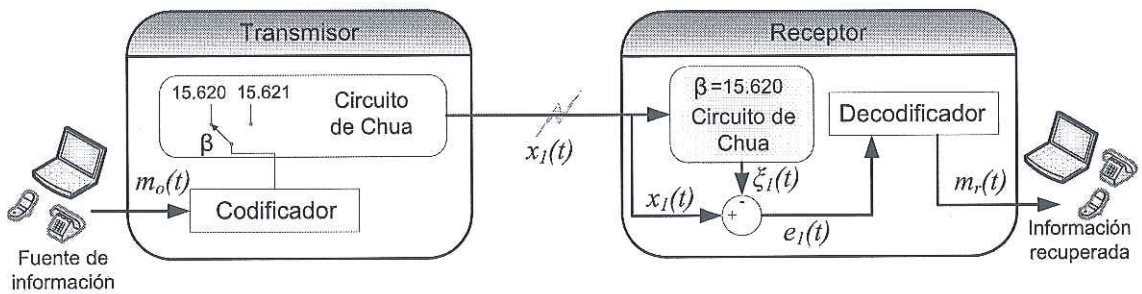


Figura 54: Sistema de comunicación digital empleando conmutación caótica y el circuito de Chua como generador caótico.

En la figura 55 se ilustran los resultados obtenidos en la transmisión y recuperación del mensaje binario secreto

$$m_o(t) = 1\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1 \cdots,$$

el mensaje confidencial $m_o(t)$ se ilustra en la figura superior, mientras que la figura central superior, presenta la señal caótica transmitida $x_1(t)$ y la figura inferior el mensaje binario recuperado en el lado del receptor por la detección del error de sincronía $e_1(t) = x_1(t) - \xi_1(t)$ expuesto en la figura central inferior.

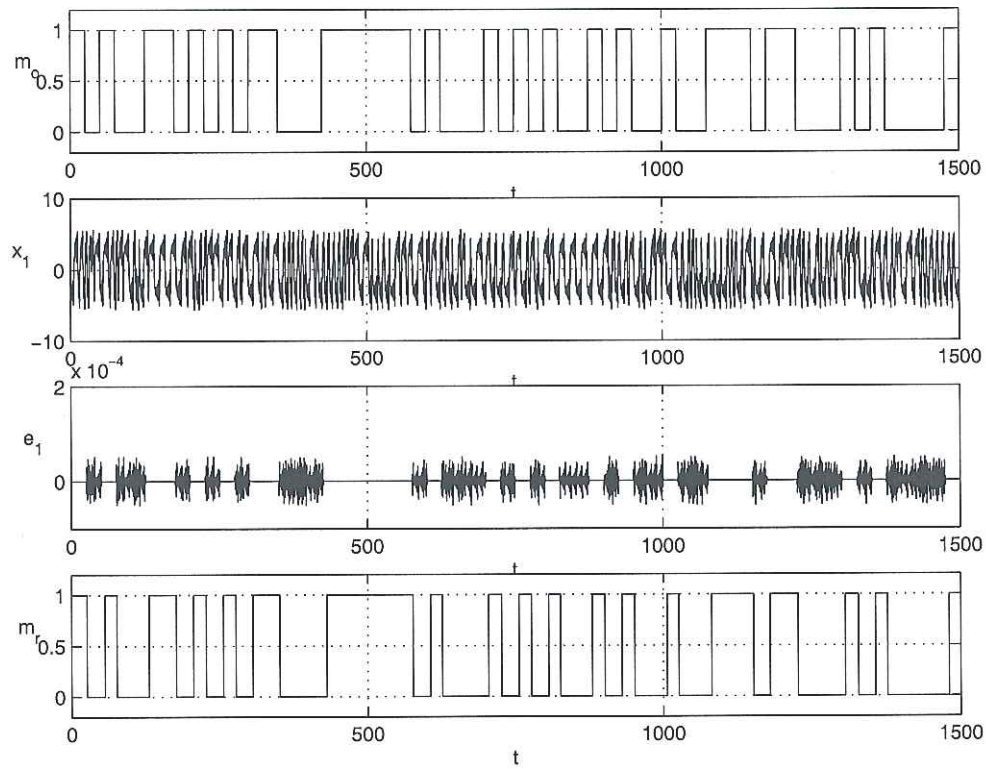


Figura 55: Transmisión y recuperación de un mensaje binario confidencial: figura superior: señal privada a ser ocultada y transmitida $m_o(t)$. Figura central superior: señal caótica transmitida $x_1(t)$. Figura central inferior: error de sincronía en sistema esclavo localizado en el receptor. Figura inferior: $m_r(t)$ mensaje binario recuperado en el receptor por el error de sincronía detectado.

VI.1.2 Vulnerabilidad

Pérez y Cerdeira demostraron en (Pérez y Cerdeira, 1995) que es posible la reconstrucción del mensaje $m_o(t)$ por un receptor intruso, empleando un simple "mapa de regresión (reconstrucción)" formado por los máximos y mínimos de la señal acoplante modulada. En ese trabajo se demuestra también que con cualquier circuito receptor, se puede desenmascarar el mensaje de la señal acoplante modulada, sin necesidad de llevar a cabo en ningún momento la reconstrucción completa de la dinámica del transmisor.

Esta técnica de "ataque" a la transmisión secreta de información digital y que

vulnera la seguridad, se describe a continuación. Empezando de algún punto arbitrario en el tiempo, se define t_n como el tiempo cuando $x_1(t)$ (señal caótica de transmisión), alcanza su n-ésimo máximo local y X_n como el valor de x_1 en ese momento. De manera similar, se define u_m como el tiempo cuando $x_1(t)$ alcanza su m-ésimo mínimo local y Y_m como el valor de x_1 en ese momento. Por ejemplo, para el sistema de Lorenz, empleando $x_1(t)$ como señal de transmisión, se tiene que usando esos valores discretos X_n y Y_n, se puede construir el mapa de regresión $A_n \, vs \, B_n$ que se presenta en la figura 56, donde A_n y B_n son resultado de la combinación lineal

$$A_n = \frac{X_n + Y_n}{2} \qquad \text{y} \qquad B_n = X_n - Y_n.$$

Estos son los valores promedio de un par máximo-mínimo consecutivos y la distancia entre ellos.

Una vez que se realice la transmisión digital, empezará la conmutación entre los dos valores paramétricos, este pequeño cambio, no solamente afectará la sincronía, también existirá un cambio en los segmentos del atractor, aparecerán dos tiras paralelas cercanas donde solamente se encontraba un segmento, mientras que se conserva su forma general. En la figura 57 se ilustra el mapa de regresión donde existen tres segmentos en el atractor y cada uno está dividido en dos tiras. Es obvio que este efecto es debido al cambio en el parámetro del sistema transmisor.

Del mapa de regresión (figura 57), se puede desenmascarar fácilmente el mensaje, del siguiente modo. Se asigna un '0" o un "1" a cada segmento, entonces sólo hay que empezar a clasificar los puntos (A_n, B_n) de acuerdo al segmento en el cual cae en el atractor.

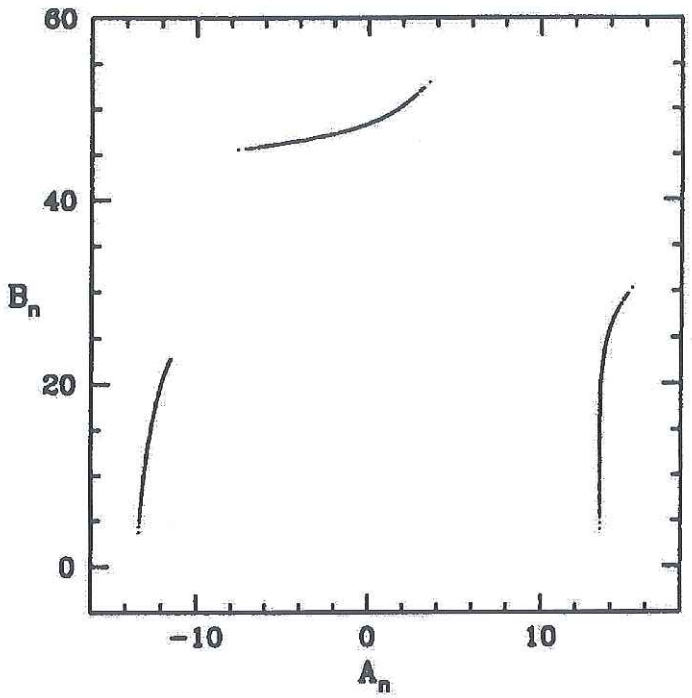


Figura 56: Atractor del mapa de regresión obtenido del máximo y mínimo del estado $x_1(t)$ en el sistema de Lorenz.

VI.1.3 Resultados numéricos empleando el circuito de Chua con retardo como generador caótico

Para superar la vulnerabilidad al ataque antes ilustrado, recientemente muchos autores han sugerido varios métodos, como comunicación privada usando técnicas de señales caóticas mezcladas (Murali y Lakshmanan, 1998), comunicación a través de ruido (Minai y Pandian, 1998), utilizar técnicas de ecuaciones diferenciales con retardo (Mensour y Longtin, 1998; Cruz-Hernández, 2004), entre otros.

Es posible **complicar el mapa** de regresión **utilizando el circuito de Chua con retardo** (9)-(10) como generador caótico para transmitir el mensaje

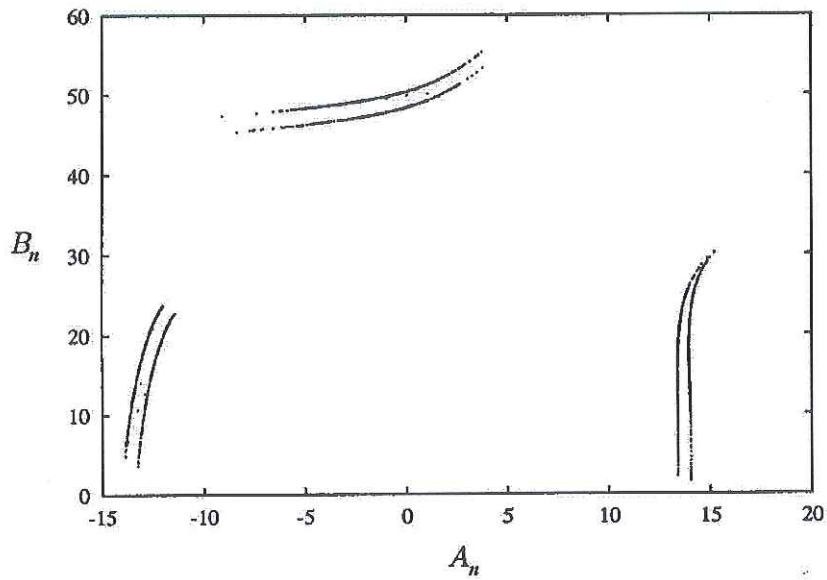


Figura 57: Mapa de regresión entre A_n y B_n en la conmutación entre dos atractores caóticos para el sistema de Lorenz.

$$m_o(t) = 1\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\cdots,$$

se deja β como el parámetro a conmutar, empleando la regla de modulación para modular $m_o(t)$ como sigue

$$\beta(t) = \beta + r \cdot m_o(t),$$

con $r = 0.001$ cuando β es conmutado entre $\beta = \beta(1) = 19.000$ y $\beta = \beta(0) = 19.001$, en el transmisor, en el sistema receptor β se deja fijo en $\beta = 19.000$, el resto de los parámetros se mantienen en valores fijos para ambos sistemas (transmisor y receptor).

La figura 58 muestra el sistema de comunicación binaria seguro por conmutación caótica. Mientras que la figura 59 ilustra los resultados obtenidos en la transmisión y la recuperación del mensaje binario secreto: el mensaje privado $m_o(t)$ (figura superior), la

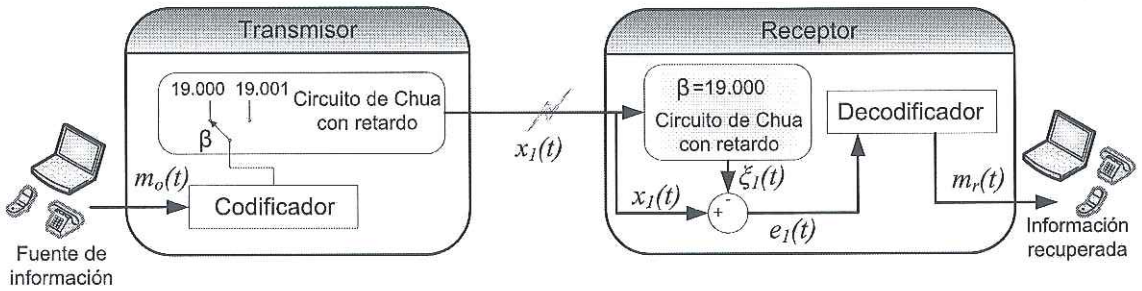


Figura 58: Sistema de comunicación digital empleando conmutación caótica y el circuito de Chua con retardo como generador caótico.

señal hipercaótica transmitida $x_1(t)$ (figura del centro) y el mensaje binario recuperado en el lado del receptor (figura inferior) por la detección del error de sincronía $e_1(t) = x_1(t) - \xi_1(t)$ mostrado en la figura central inferior.

En la figura 60 se presenta el mapa de regresión obtenido de la señal caótica acoplante, generada por el estado $x_1(t)$ del circuito de Chua, como se puede apreciar, de aquí se puede recuperar el mensaje. Sin embargo al emplear como señal acoplante el estado hipercaótico $x_1(t)$ del circuito de Chua con retardo, se obtiene el mapa de regresión mostrado en la figura 61, del cual, resulta más dificil sino que fue imposible la extracción del mensaje.

VI.2 Conmutación entre múltiples atractores caóticos

Una manera mas de superar los ataques sufridos a los sistemas de comunicación empleando conmutación caótica, donde se hizo posible la reconstrucción del mensaje hecha por Pérez y Cerdeira en (Pérez y Cerdeira, 1995), es aumentar el número de maneras por las cuales, el mensaje se puede reconstruir y de tal modo eliminar la posibilidad de identificar el mensaje correcto. A continuación se describe este procedimiento y para

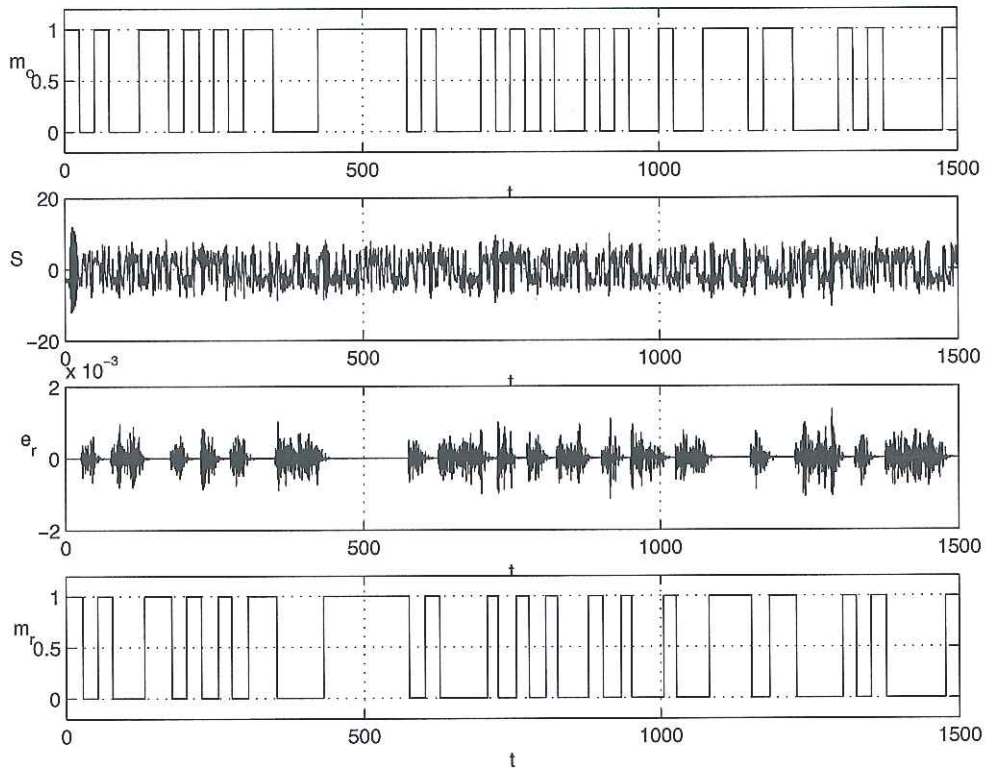


Figura 59: Transmisión y recuperación de un mensaje binario confidencial: figura superior: señal privada a ser ocultada y transmitida $m_o(t)$. Figura central superior: señal hipercaótica transmitida $x_1(t)$. Figura central inferior: $e_1(t)$ error de sincronía que presenta el sistema esclavo localizado en el receptor. Figura inferior: $m_r(t)$ mensaje binario recuperado en el receptor por el error de sincronía detectado.

el cual, se empleará otra vez la versión normalizada del circuito de Chua con retardo (9)-(10).

Palaniyandi y Lakshmanan (2001) proponen una modificación en la manera de transmitir el mensaje digital, cuando se emplea la técnica de conmutación caótica descrita anteriormente, con el propósito de complicar el atractor en el "mapeo de regresión (reconstrucción)". Primeramente, en el sistema transmisor, en lugar de conmutar el valor del parámetro entre dos valores únicamente, se conmuta entre múltiples valores, donde para un estado del mensaje binario (cualquier "1" ó "0"), al parámetro

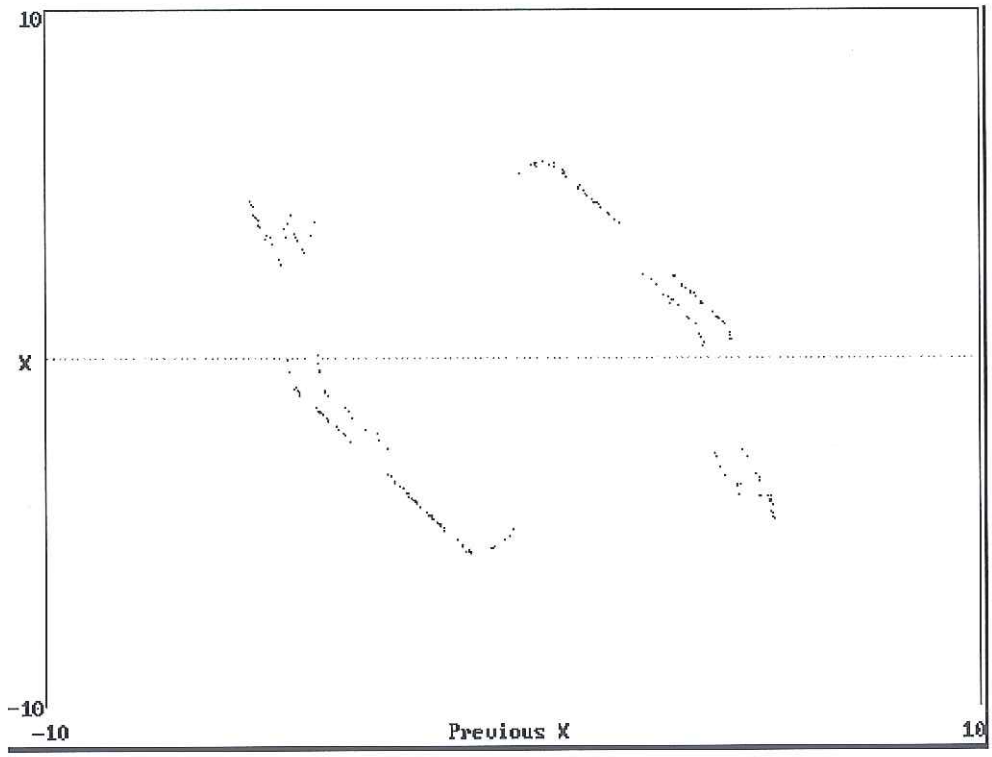


Figura 60: Mapa de regresión entre A_n y B_n en la conmutación entre dos atractores caóticos obtenido de la señal acoplante $x_1(t)$ y modulada por el mensaje. Empleando el circuito de Chua clásico.

selecionado en las ecuaciones del transmisor, se le asigna cualquiera de los "n" valores preasignados y "n" para el otro estado ($n > 1$ y suficientemente grande), mientras en el receptor se usan "n" sistemas esclavos con diferentes valores en el parámetro seleccionado.

El diagrama a bloques del transmisor y el receptor con "n" cambios en el valor del parámetro, se muestra en la figura 62, donde SE_1, SE_2, ..., SE_n son los "n" sistemas esclavos en el receptor. A cada SE_i se le asigna un valor de los "n" valores escogidos para el parámetro, los cuales, se usan para imponer el estado correspondiente del mensaje digital en la señal acoplante. La potencia del error de sincronía a la salida de cada sistema esclavo pasa através de un filtro pasa bajas, por separado. Entonces

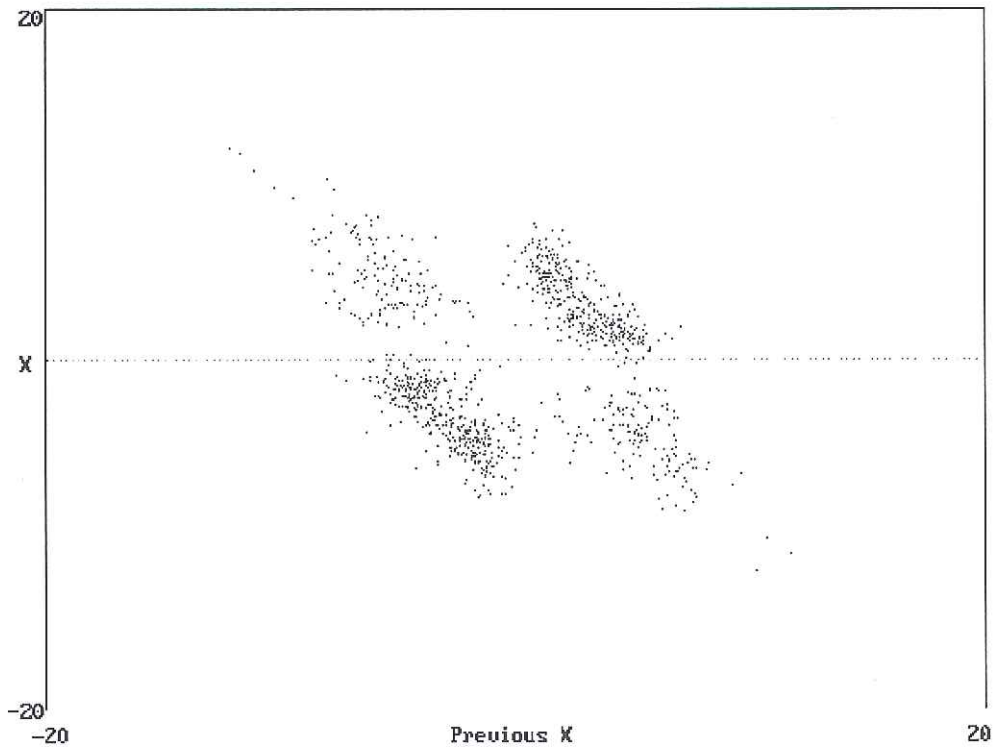


Figura 61: Mapa de regresión entre A_n y B_n en la conmutación entre dos atractores caóticos obtenido de la señal caótica acoplante $x_1(t)$ y modulada por el mensaje. Empleando el circuito de Chua con retardo.

la señal filtrada es convertida a señal digital en el detector de nivel (TD, "threshold detector"). Una compuerta lógica "O" en el receptor combina todas las salidas. Así, cuando el mensaje digital impuesto en la señal acoplante es "1", cualquiera de los sistemas esclavos en el receptor sincronizará en el receptor y la salida de la compuerta lógica "O" será "1". Ningún sistema esclavo sincronizará, si el mensaje digital es "0" y ahora será "0" la salida de la compuerta lógica "O". En la siguiente parte del manuscrito, se recurrirá a este método de transmisión digital, para el circuito de Chua.

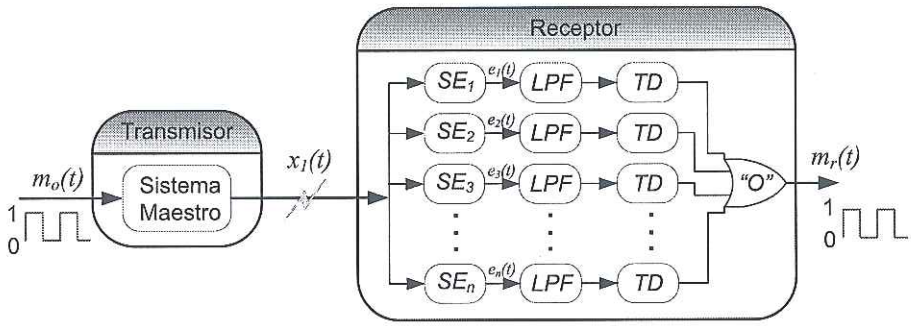


Figura 62: Diagrama a bloques del transmisor y el receptor empleados en la conmutación entre múltiples valores del parámetro con señal acoplante $x_1(t)$ (LPF- filtro pasabajas, TD- detector de niveles, O- Compuerta lógica O).

VI.2.1 Resultados numéricos empleando el circuito de Chua clásico como generador caótico

Empleando este método con el circuito de Chua clásico (3)-(4) como generador caótico, se selecciona a β como el parámetro a conmutar y con $n = 5$, es decir 5 diferentes valores del parámetro escogido para un estado de la señal binaria, 5 valores para el otro estado y 5 sistemas esclavos en el receptor. En la figura 63 se puede observar que β es el parámetro a conmutar en el sistema transmisor, éste permite adquirir cualquiera de los cinco valores de referencia: **15.616, 15.618, 15.620, 15.622 y 15.624** para el **estado alto** de la señal binaria, mientras que adquiere uno de los valores: **15.617, 15.619, 15.621, 15.623 y 15.625** para el **estado bajo** y en el sistema receptor se colocan 5 sistemas esclavos con los valores de referencia fijos en el parámetro β.

El método trabaja de la siguiente manera. Suponiendo que el mensaje confidencial binario empieza con un "1". Entonces, el sistema receptor sincronizará el sistema esclavo que tiene el parámetro β con valor de 15.616. Para el siguiente estado alto que se presente en el mensaje el transmisor conmutará al valor de $\beta = 15.618$ y este proceso continua hasta que el valor de β llega a 15.624. Entonces el valor de β vuelve a comenzar

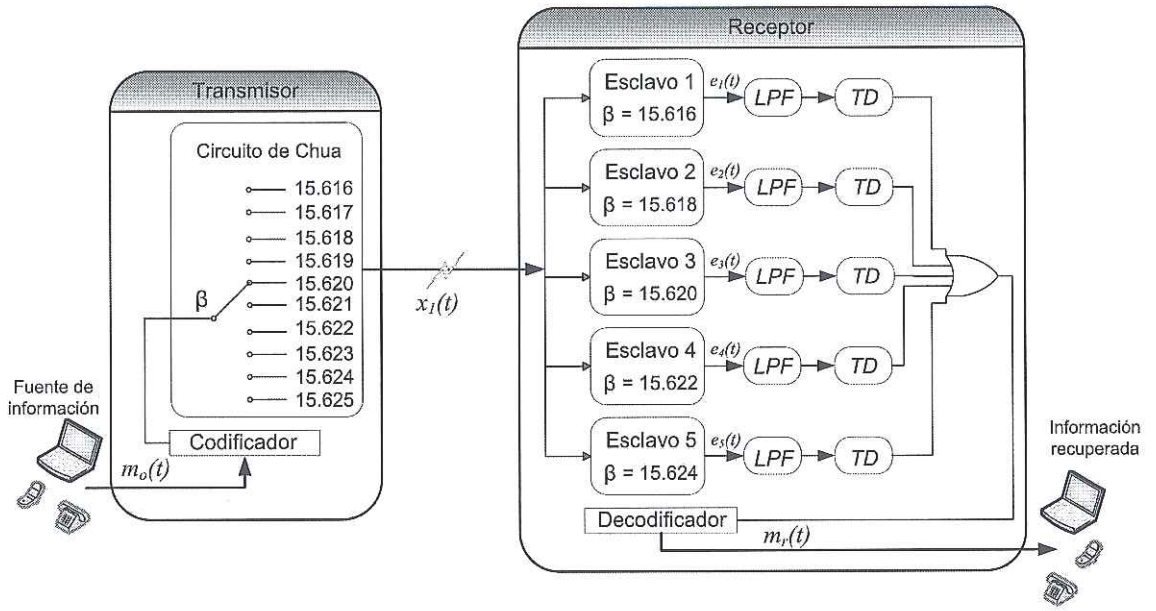


Figura 63: Sistema de comunicación caótico seguro emplendo la técnica de conmutación entre múltiples valores del parámetro, con $n = 5$ y el circuito de Chua clásico como generador caótico.

en 15.616. Este procedimiento también se aplica al estado bajo del mensaje, pero la conmutación del parámetro adquiere los valores 15.617, 15.619, 15.621, 15.623 y 15.6255 en este orden. En el sistema receptor todos los sistemas esclavos Esclavo_1, Esclavo_2, ..., Esclavo_5 son controlados por la misma señal acoplante $x_1(t)$. Sin embargo, los sistemas esclavos sincronizarán sólo para los valores de referencia del parámetro en el transmisor. Cuando algún sistema esclavo sincroniza, el valor absoluto del error será detectado por el TD y entonces el mensaje obtenido del TD será un "1". En cambio se obtendrá un "0" si el sistema esclavo no sincroniza.

Así mismo, si alguno de los sistemas esclavos es sincronizado a la salida de la compuerta lógica "O" se obtiene un "1" y cuando ocurre asincronía en todos los sistemas esclavos se recupera un "0" del mensaje digital.

Para el mensaje binario confidencial

$$m_o(t) = 1\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\cdots,$$

transmitido por este esquema, el error de sincronía resultante en cada sistema esclavo del receptor, se despliega en la figura 64.

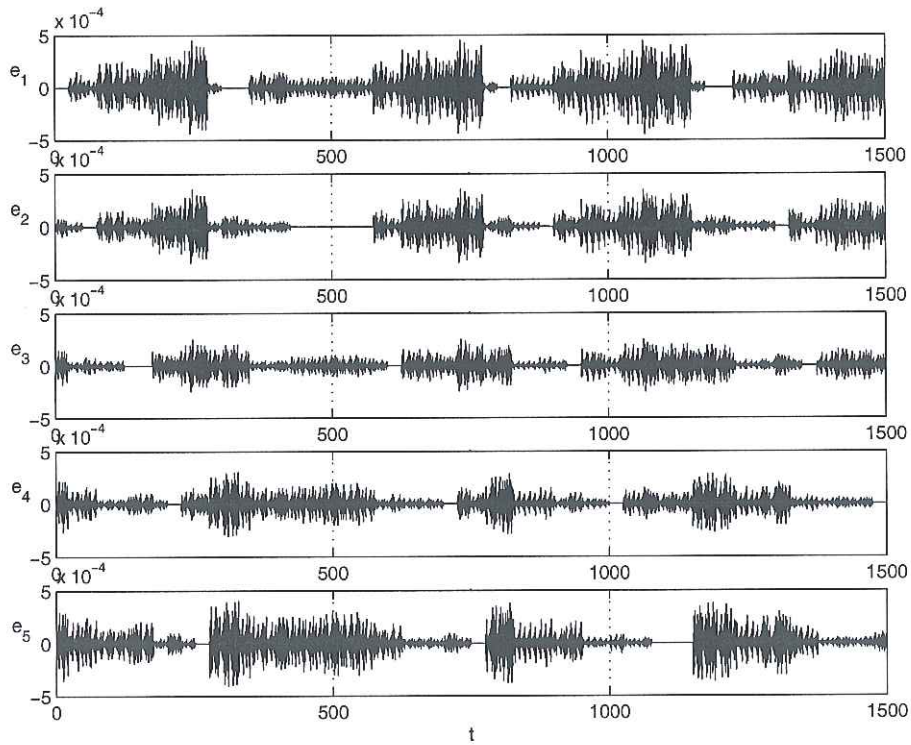


Figura 64: Error de sincronía e_i $(i = 1, 2, \ldots, 5)$ resultante en los sistemas esclavos Esclavo_1, Esclavo_2, Esclavo_3, Esclavo_4 y Esclavo_5 del receptor, en la transmisión del mensaje $m_o(t) = 10100110010110001111\cdots$ empleando el esquema de conmutación entre múltiples atractores caóticos con $n = 5$ (circuito de Chua clásico).

Una vez que la señal de dichos errores son filtrados y posteriormente convertida a una señal digital por el TD se recupera la secuencia binaria mostrada en la tabla II, también se aprecia ahí, que el mensaje obtenido a la salida de la compuerta lógica "O" corresponde al mensaje binario confidencial enviado.

Tabla II: Palabra binaria recuperada por cada sistema esclavo en el receptor.

Esclavo_1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0 ...
Esclavo_2	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1 ...
Esclavo_3	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0 ...
Esclavo_4	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0 ...
Esclavo_5	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0 ...
Salida de la compuerta "O" ($m_r(t)$)	1	0	1	0	0	1	1	0	1	0	1	0	1	1	0	0	0	1 ...

La figura 65 ilustra el mensaje confidencial binario a ocultar $m_o(t)$ (figura superior), la señal caótica transmitida $x_1(t)$ y el mensaje recuperado $m_r(t)$ después de filtrar, pasar a través del detector de nivel y la compuerta lógica "O" el error de sincronía detectado en cada sistema esclavo del sistema receptor y mostrado en la figura 64.

VI.2.2 Resultados numéricos empleando el circuito de Chua con retardo como generador caótico

En lo que sigue se empleará este método con el *circuito de Chua con retardo* como generador caótico, se selecciona a β como el parámetro a conmutar y con $n = 5$, es decir, 5 diferentes valores del parámetro escogido para un estado de la señal binaria, 5 valores para el otro estado y 5 sistemas esclavos en el receptor. Como se demostró antes, el circuito de Chua con retardo presenta una dinámica caótica muy rica cuando el parámetro β toma el valor de 19.000. El parámetro β en el sistema transmisor permite tomar cualquiera de los cinco valores de referencia: **18.996, 18.998, 19.000, 19.002 y 19.004** para el **estado alto** de la señal binaria, mientras que toma uno de

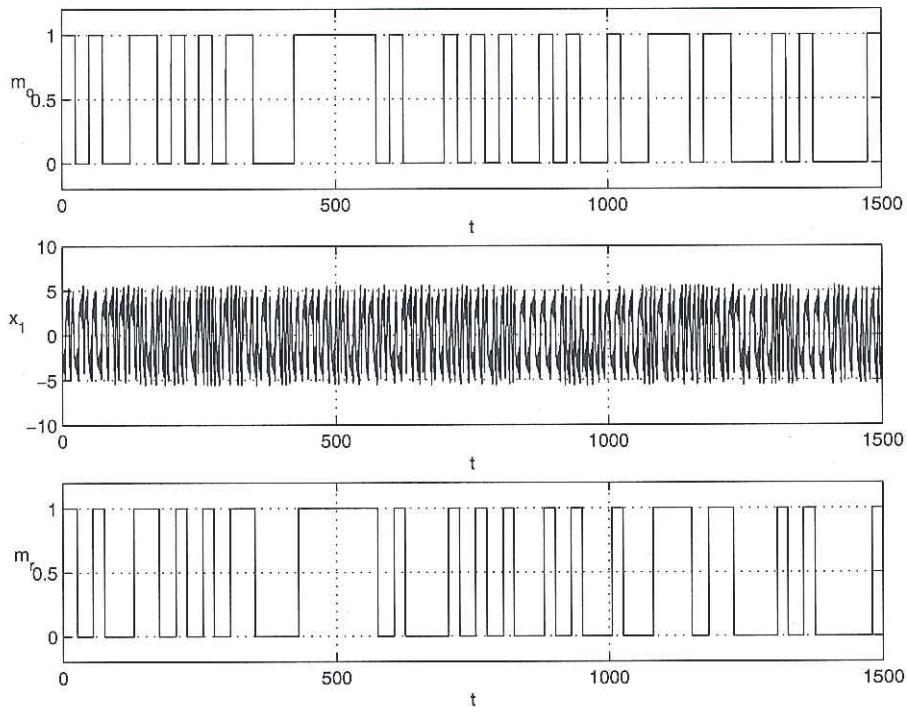


Figura 65: Transmisión y recuperación de un mensaje secreto binario aplicando la técnica de conmutación entre múltiples atractores caóticos: figura superior: señal privada binaria a ser ocultada y transmitida $m_o(t)$. Figura central: señal caótica transmitida $x_1(t)$. Figura inferior: mensaje binario recuperado en el receptor por el error de sincronía detectado $m_r(t)$.

los valores: **18.997, 18.999, 19.001, 19.003 y 19.005** para el **estado bajo**. En el sistema receptor, se usan 5 sistemas esclavos con los valores de referencia fijos en el parámetro β (ver figura 66).

Permítase repetir brevemente cómo trabaja el método de transmisión y recuperación de información digital. Suponiendo que el mensaje confidencial binario empieza con un "1". Entonces, el sistema receptor sincronizará el sistema esclavo que tiene el parámetro β con valor de 18.996. Para el siguiente estado alto que se presente en el mensaje el transmisor conmutará al valor de $\beta = 18.998$ y este proceso continua hasta que el valor de β llega a 19.004. Entonces, el valor de β vuelve a comenzar en 18.996. Este

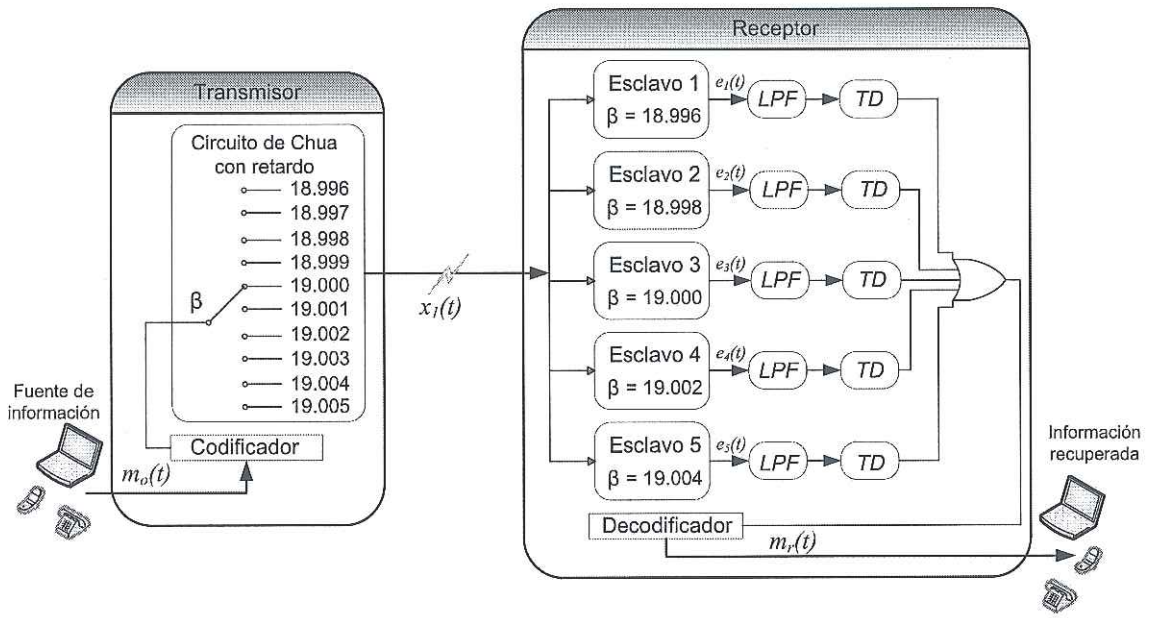


Figura 66: Sistema de comunicación caótico seguro emplendo la técnica de conmutación entre múltiples valores del parámetro, con $n = 5$ y el circuito de Chua con retardo como generador caótico.

procedimiento también se aplica al estado bajo del mensaje, pero la conmutación del parámetro toma los valores 18.997, 18.999, 19.001, 19.003 y 19.005 en este orden. En el sistema receptor todos los sistemas esclavos Esclavo_1, Esclavo_2, ..., Esclavo_5 son controlados por la misma señal hipercaótica acoplante $x_1(t)$. Sin embargo, los sistemas esclavos sincronizarán sólo para los valores del parámetro en transmisor 18.996, 18.998, 19.000, 19.002 y 19.004 respectivamente. Cuando algún sistema esclavo sincroniza, el valor absoluto del error será detectado por el TD y entonces el mensaje obtenido del TD será un "1", en cambio se obtendrá un "0", si el sistema esclavo no sincroniza.

Así mismo, si alguno de los sistemas esclavos es sincronizado a la salida de la compuerta lógica "O" se obtiene un "1" y cuando ocurre asincronía en todos los sistemas esclavos se recupera un "0" del mensaje original.

Para el mensaje binario confidencial

$$m_o(t) = 1\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\cdots,$$

con duración del bit (tb) de $tb = 100$ transmitido por este esquema, el error de sincronía resultante en cada sistema esclavo del receptor, se despliega en la figura 67.

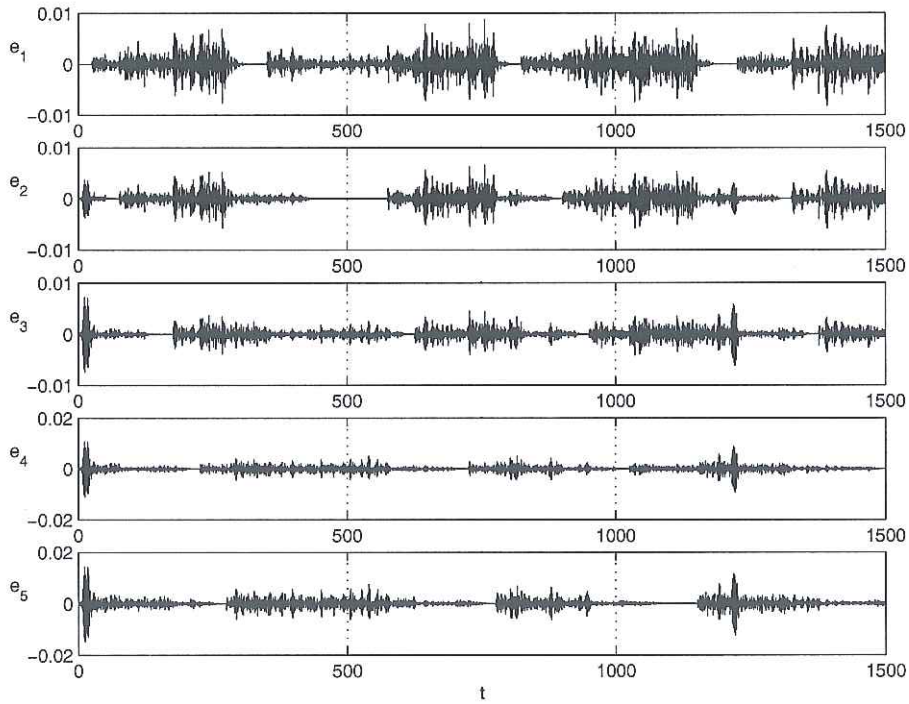


Figura 67: Error de sincronía e_i resultante en los sistemas esclavos Esclavo_1, Esclavo_2, Esclavo_3, Esclavo_4 y Esclavo_5 del sistema receptor, en la transmisión del mensaje $m_o(t) = 10100110010110001111\cdots$ empleando el esquema de conmutación entre múltiples atractores caóticos con $n = 5$ (circuito de Chua con retardo).

Una vez que la señal de dichos errores son filtrados y convertida a una señal digital por el TD, se recupera la palabra binaria mostrada en la tabla III, donde también se aprecia que el mensaje obtenido a la salida de la compuerta lógica "O" corresponde al mensaje binario confidencial enviado.

Tabla III: Palabra binaria recuperada por cada sistema esclavo en el receptor.

Esclavo_1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0 ...
Esclavo_2	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1 ...
Esclavo_3	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0 ...
Esclavo_4	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0 ...
Esclavo_5	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0 ...
Salida de la compuerta "O" ($m_r(t)$)	1	0	1	0	0	1	1	0	1	0	1	0	1	1	0	0	0	1 ...

La figura 68 ilustra el mensaje binario confidencial a ocultar $m_o(t)$ (figura superior), la señal hipercaótica transmitida $x_1(t)$ y el mensaje recuperado $m_r(t)$ después de filtrar, pasar a través del detector de nivel y la compuerta lógica "O" el error de sincronía detectado en cada sistema esclavo del sistema receptor y mostrado en la figura 67.

VI.3 Conclusiones

En este capítulo se presentó el diseño de sistemas de encriptado digital con base en la técnica de conmutación caótica y el circuito de Chua clásico como generador caótico, mediante simulaciones se demuestra que ante el ataque propuesto por Pérez y Cerdeira en (Pérez y Cerdeira, 1995), el sistema resulta ser inseguro. Al emplear la misma técnica de comunicación, pero usando como generador caótico el circuito de Chua con retardo, esta vulnerabilidad es superada. Además, se incrementó la seguridad aumentando el número de atractores caóticos entre los que conmuta la señal transmitida con la información oculta.

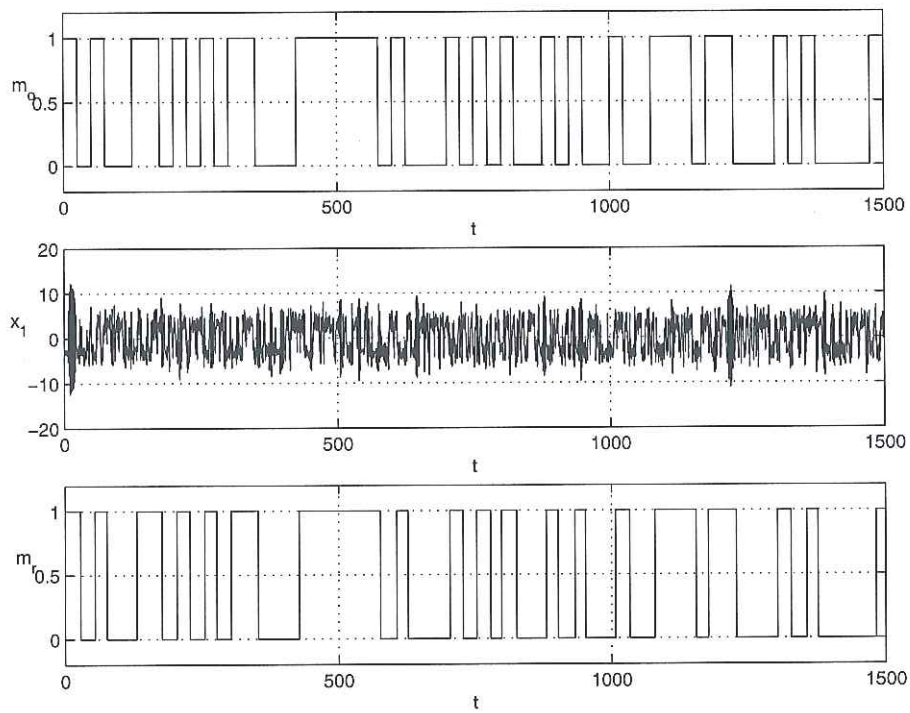


Figura 68: Transmisión y recuperación de un mensaje secreto binario aplicando la técnica de conmutación entre múltiples atractores caóticos (Chua con retardo): figura superior: señal privada binaria a ser ocultada y transmitida $m_o(t)$. Figura central: señal hipercaótica transmitida $x_1(t)$. Figura inferior: $m_r(t)$ mensaje binario recuperado en el receptor por el error de sincronía detectado (circuito de Chua con retardo).

Capítulo VII

Conclusiones

En este trabajo de tesis se presentó la sincronización del circuito de Chua con retardo, empleando la metodología de sincronización de sistemas caóticos por formas hamiltonianas y el diseño de observador, se dió una aplicación en la transmisión de información analógica y digital dentro del ámbito de las comunicaciones privadas/seguras. Obteniendo los siguientes resultados:

- Mediante técnicas de procesamiento de señales se realizó un estudio numérico de la dinámica caótica de los estados del circuito de Chua con retardo y se encontró que para valores de los parámetros $\alpha = 10$, $\beta = 19.53$, $\gamma = 0.1636$, $a = -1.4325$, $b = -0.7831$, $\tau = 5.23$, $\varepsilon = 0.5$ y $\sigma = 3$ es capaz de producir señales extremadamente complejas.

- Los resultados numéricos reportados demostraron sincronización del circuito de Chua con retardo mediante formas hamiltonianas y el diseño de un observador.

- El encriptado de una línea con retroalimentación del mensaje y el de dos líneas son más eficientes en seguridad y robustez.

- La dinámica caótica del circuito de Chua con retardo es suficientemente compleja para superar el ataque por mapas de regresión (en la conmutación entre dos atractores).

- Los sistemas de encriptado caótico con base en el generador de caos (Chua con retardo), presentan ya gran seguridad para el cifrado de información privada.

- Es necesario conocer el ancho de banda de la información por encriptar para cada requerimiento de usuarios.

Trabajo futuro

El área de investigación de sincronización de sistemas caóticos y su aplicación en las comunicaciónes seguras es muy amplia. Por tanto, existe un gran numéro de problemas abiertos en cada una de sus etapas. Entre algunas perspectivas que pueden mencionarse para trabajo futuro y que constituyen problemas abiertos, con relación a esta tesis a nuestro juicio, son:

- En cuanto la sincronía, es recomendable investigar la robustez a variaciones paramétricas y a ruido en la señal acoplante de los sistemas de encriptado.
- Estudiar el encriptado de información digital incorporando ruido en la línea de transmisión.
- Los resultados presentados muestran que se cumple satisfactoriamente con el objetivo planteado, haciendo recomendable una implementación física.
- Estudiar la factibilidad de la tecnología de DSP para llevar a cabo la implementación de los sistemas de encriptado caótico.
- Llevar a cabo trabajos de investigación conjuntos con el área de telecomunicaciones que involucren variables que el mercado comercial demanda. Por ejemplo, disminuir el tiempo de sincronía para hacer factible la conmutación entre atractores caóticos.

Bibliografía

Aguilar A. y Cruz-Hernández, C. (2002), "Synchronization of two hyperchaotic Rossler systems: Model-matching approach", *WSEAS Transactions on Mathematics*, **1**(2): 198-203 p.

Aguilar A. y Cruz-Hernández, C. (2003), "Synchronization of hyperchaotic discrete-time systems: model-matching approach", *Proceedings of the American Control Conference*, Denver, Colorado, junio 2003. 2335-2340 p.

Anishchenko, V. S., Kapitaniak, T., Safonova, M. A. y Sosnovzeva, O. V. (1994), "Birth of double-double scroll attractor in coupled Chua circuits", *Phys. Rev. Lett.* **A192**: 207-214 p.

Carroll, T. L. y Pecora, L. M. (1991), "Synchronization in chaotic circuits", *IEEE Trans. Circuits Syst. I*, **38**(4): 453-456 p.

Chen, G. y Dong, X. (1993a), "Controlling Chua's circuit", *J. Circs. Syst. Computers*, **3**: 139-149 p.

Chen, G. y Dong, X. (1993b), "From chaos to order: perspectives and methodologies in controlling nonlinear chaotic dynamical systems", *Int. J. Bifurc. Chaos*, **3**(6): 1363-1389 p.

Chua, L. O., Kocarev, L. y Eckert, K. (1993), "Chaos synchronization in Chua's circuit", *J. Circs. Syst. Computers*, **3**(1): 93-108 p.

Cruz-Hernández, C., Posadas-Castillo, C. y Sira-Ramírez, H. (2002), "Synchronization of two hyperchaotic Chua circuits: A generalized hamiltonian systems approach", Memorias del *15th IFAC*, Barcelona, España, julio 2002.

Cruz-Hernández, C. (2003), "Synchronization of time-delay Chua's oscillator: A generalized Hamiltonian systems approach", *Procs. of the IASTED on Circuits, Signal, and Systems*, mayo 2003, Cancún México.

Cruz-Hernández, C. (2004), "Synchronization of time-delay Chua's oscillator with application to secure communication", *Nonlinear Dynamics and Systems Theory*, **4**(1): 1-13 p.

Cruz-Hernández, C. y Serrano-Guerrero, H. (2005), "Cryptosystems based on synchronized Chua's circuits", *16th IFAC World Congress*, Praga, República Checa, julio 2005.

Cruz-Hernández, C., Posadas-Castillo, C., Serrano H. y Núñez-Pérez, R. F. (en proceso), "Experimental realization of binary signals transmission using chaos", *J. Circs. Syst. Computers.*

Cruz-Hernández, C. y Núñez-Pérez, R. F. [2003], "Métodos de comunicaciones por señales caóticas", *curso* **ET108**, *Centro de Investigación Científica y de Educación Superior de Ensenada.*

Cuomo, K. M., Oppenheim, A. V. y Strogatz, S. H. (1993), "Synchronization of Lorenz-based chaotic circuits with applications to communications", *IEEE Trans. Circuits Syst. I*, **40**(10): 626-632 p.

Cuomo, K. M., Oppenheim A. V. y Strogatz S.(1993), "Robustness and signal recovery in a synchronized chaotic system", *Int. J. Bifurc. Chaos*, **3**(6): 1629-1638 p.

Cuomo, K. M. y Oppenheim, A. V. (1993), "Circuit implementation of synchronized chaos with application to communication", *Physics Letters*, **70**: 3031-3035 p.

Díaz-Moreno, E., Gámez-Guzmán, L., Ayála-Morales, P., Cruz-Hernández, C. y Núñez-Pérez, R. (2003), "Sincronización de atractores con múltiples enrollamientos y una aplicación a la comunicación secreta", *Memorias del Congreso Nacional de Control Automático C.N.C.A.*, Ensenada, México, octubre 2003.

Dedieu H., Kennedy M.P. y Hasler M. (1993), "Chaos Shift Keying: Modulation and Demodulation of a Chaotic Carrier Using Self-Synchronizing Chua's Circuits", *IEEE Trans. Circuits Syst. II*, **40**(10): 634-642 p.

Ditto, W. L. y Pecora, L. M. (1993), "Mastering chaos", *Scientific American*, **269**(2): 62-68 p.

Farmer, J.D. (1982), "Chaotic attractors of an infinite-dimensional dynamical systems", *Physica D*, 4(2): 366-393 p.

Feldman, U., Hasler, M. y Schwarz, W. (1996), "Communication by chaotic signals: the inverse system approach", *Int. j. Circ. Theory Applic.*, **24**: 551-579 p.

Fradkov, A. L., Nijmeijer, H. y Progromsky, A. Yu. (1999), Adaptive observer based synchronisation. En: Chen, G. (ed.) "Controlling chaos and bifurcations in engineering systems", *CRC Press*, primera edición, Boca Raton, Florida, 405-426 p.

Gámez-Guzmán, L. (2004), "Encriptador de información con base en la sincronía de atractores con enrollamientos múltiples", *tesis de maestría, Centro de Investigación Científica y de Educación Superior de Ensenada (DET-CICESE)*. 156 pp.

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

Halle K.S., Chua, L. O., Anishchenko, V. S. y Safonova, M. A. (1992), "Signal amplification via chaos: experimental evidence", *Int. J. Bifurc. Chaos*, **2**(4): 1011-1020 p.

Halle K.S., Wu C.W., Itoh M. y Chua, L. O. (1993), "Spread spectrum communication through modulation of chaos", *Int. J. Bifurc. Chaos*, **3**(2): 469-477 p.

Cuomo, K. M., Oppenheim A. V. y Strogatz S.(1995), "Engineering chaos for encryption and broadband communication", *Phil. Trans. R. Soc. Lond.*, **A**(353): 115-126 p.

Kapitaniak, T., Chua, L. O. y Zhong, G. Q. (1994), "Experimental synchronization of chaos using continuous control", *Int. J. Bifurc. Chaos*, **4**(2): 483-488 p.

Kennedy, M. P., (1993), "Three steps to chaos part II: A Chuas's circuit", *IEEE Trans. Circuits Syst. I*, **40**(10): 657-674 p.

Kocarev, L., Halle, K. S., Eckert, K., Chua, L. O. y Parlitz, U. (1992), "Experimental demostration of secure communications via chaotic synchronization", *Int. J. Bifurc. Chaos*, **2**: 709-713 p.

Kolumbán, G., Kennedy, M. P. y Chua, L. O., (1997), "The role of synchronization in digital communications", *IEEE Trans. Circuits Syst. I*, **44**(10): 927-935 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): 364-369 p.

López-Mancilla, D. y Cruz-Hernández, C. (en proceso), "Output synchronization of chaotic systems: Model-matching approach with application to secure communication", *Nonlinear Dynamics and Systems Theory*, **5**(1).

López-Mancilla, D. y Cruz-Hernández, C. (en proceso), "A note on chaos-based communications schemes", *Revista Mexicana de Física.*

López-Mancilla, D. y Cruz-Hernández, C. (en proceso), "Output synchronization of chaotic systems: Model-matching approach with application to secure communication", *Nonlinear Dynamics and Systems Theory*, **5**(1).

López-Mancilla, D. y Cruz-Hernández, C. (2005), "Output synchronization of chaotic oscillator and communications", *16th IFAC World Congress*, Praga, República Checa, Julio 2005, 2335-2340 p.

Lu, H. y He, Z. (1996), "Chaotic behaviors in first-order autonomous continuous-time systems with delay", *IEEE Trans. Circuits Syst. I*, **43**: 700-702 p.

Madan, R. N. (1993), *Chua's circuit: a paradigm for chaos*, World Scientific Series on Nonlinear Science. Series B, Vol. I, Singapore. 1088 pp.

Menezes, A. J., Van P. C. y Vanstone, S. A. (2001), "Handbook of applied cryptography", *CRC Press*, Quinta edición, Boca Raton, Florida. 780 pp.

Mensour, B. y Longtin, A. (1998), "Synchronization of delay-differential equations with application to private communication", *Physics Letters*, **A244**: 59-70 p.

Meranza-Castillón, M. (2002), "Implementación de un sistema de encriptamiento hipercaótico", *tesis de maestría, Centro de Investigación Científica y de Educación Superior de Ensenada (DET-CICESE).* 107 pp.

Meranza-Castillón, M. y Cruz-Hernández, C. (2002a), "Estudio experimental de la sincronía de dos circuitos hipercaóticos de Chua", *Proceedings of the* 2^{nd} *International Conference on Automatic Control AUTOMATICA 2002*, Santiago de Cuba, Cuba, julio 2002.

Meranza-Castillón, M. y Cruz-Hernández, C. (2002b), "Estudio experimental sobre comunicación privada usando sincronía de circuitos hipercaóticos de Chua", *Memorias del X Congreso Latinoamericano de control Automático CLCA2002*, Guadalajara, México, diciembre 2002.

Minai, A. A. y Pandian, T. D. (1998), "Communicating with noise: how chaos and noise combine to generate secure encryption keys", *Chaos*, **8**: 621-628 p.

Moon, F.C. (1992), "Chaotic and fractal dynamics: an introduction for applied scientists and engineers", *John Wiley and Sons Inc.*, Primera edición, New York, New York. 528 pp.

Murali, K. y Lakshmanan, M. (1998), "Secure communication using a compound signal from generalized synchronizable chaotic systems", *Physics Letters*, **A241**: 303-310 p.

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

Núñez-Pérez, R. F. [2003], "Aplicación en Instrumentación del Análisis Digital de Señales", *curso* **ET631**, *Centro de Investigación Científica y de Educación Superior de Ensenada.*

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

Palaniyandi, P. y Lakshmanan, M. (2001), "Secure digital transmission by multistep parameter modulation and alternative driving of transmitter variables", *Int. J. Bifurc. Chaos*, **11**(7): 2031-2036 p.

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

Pecora, L. M. y Carroll, T. L. (1990), "Synchronization in chaotic systems", *Phys. Rev. Lett.*, **64**(8): 821-824 p.

Pérez, G. y Cerdeira, H. A. (1995), "Extracting messages masked by chaos", *Phys. Rev. Lett.* **74**: 1970-1973 p.

Posadas-Castillo, C. (2001), "Sincronización de osciladores de Lorenz por formas hamiltonianas", *tesis de maestría, Centro de Investigación Científica y de Educación Superior de Ensenada (DET-CICESE).* 115 pp.

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

Short, K. M. (1994), "Steps toward unmasking secure communications", *Int. J. Bifurc. Chaos*, **4**(4): 959-977 p.

Short, K. M. (1996), "Unmasking a modulated chaotic communications scheme", *Int. J. Bifurc. Chaos*, **6**(2): 367-375 p.

Serrano-Guerrero, H. (2002), "Implementación de un sistema encriptador con base en la sincronía de circuitos de Chua", *tesis de maestría, Centro de Investigación Científica y de Educación Superior de Ensenada (DET-CICESE).* 86 pp.

Serrano-Guerrero, H. y Cruz-Hernández, C. (2002a), "Dos sistemas de encriptamiento con base en la sincronía de circuitos de Chua", *Proceedings of the* 2^{nd} *International Conference on Automatic Control AUTOMATICA 2002*, Santiago de Cuba, Cuba, julio 2002.

Serrano-Guerrero, H. y Cruz-Hernández, C. (2002b), "Sistema encriptador con base en la sincronía de circuitos de Chua", *Memorias del X Congreso Latinoamericano de control Automático CLCA2002*, Guadalajara, México, diciembre 2002.

Sira-Ramírez, H. y Cruz-Hernández, C. (2000), "Synchronization of chaotic systems: a generalized Hamiltonian systems approach", *Procs. of American Control Conference (ACC'2000)*, Chicago, USA: 769-773 p.

Sira-Ramírez, H. y Cruz-Hernández, C. (2001), "Synchronization of chaotic systems: a generalized Hamiltonian systems approach", *Int. J. Bifurc. Chaos*, **11**(5), 1381-1395.

Schweizer, J., Kennedy, M. P., Hasler, M. y Dedieu, H. (1995) "Synchronization theorem for a chaotic system", *Int. J. Bifurc. Chaos*, **5**(1): 297-302 p.

Tao, C. y Du, G. (2003), "A new approach to breaking down chaotic secure communication", *Int. J. Bifurc. Chaos*, **13**(9): 2689-2698 p.

Wang, X. F., Zhong, G. Q., Tang, K. S., Man, K. F. y Liu, Z. F. (2001) "Generating chaos in Chua's circuit via time-delay feedback", *IEEE Trans. Circuits Syst. I*, **48**(9): 1151-1156 p.

Ushio, T. (1996) "Synthesis of chaotically synchronized systems based on observers", *Proceedings Int. Conference Nonlinearity Bifur. Chaos*: 251-254 p.

Yang, T., Yang, L. B., y Yang, C. M. (1998), "Breaking chaotic switching using generalized synchronization: Examples", *IEEE Trans. Circuits Syst. I*, **45**(10): 1062-1067 p.

Yang, T., Wu, C. W. y Chua, L.O. (1997), "Cryptography based on chaotic systems", *IEEE Trans. Circuits Syst. I*, **44**(5): 469-472 p.

Yang, T. y Chua, L. O. (1996), "Secure communication via chaotic parameter modulation", *IEEE Trans. Circuits Syst. I*, **43**(9): 817-819 p.