UNIVERSIDAD AUTONÓMA DE BAJA CALIFORNIA

FACULTAD DE INGENIERÍA ENSENADA

MAESTRÍA Y DOCTORADO EN CIENCIAS E INGENIERÍA

ENCRIPTAMIENTO DE INFORMACIÓN MEDIANTE CAOS

TESIS

Que con el objeto de cubrir parcialmente los requisitos para obtener el grado de **MAESTRO EN INGENIERÍA** presenta:

JUAN MANUEL MEJÍA CAMACHO

Ensenada Baja California, México

Marzo de 2007

TESIS DEFENDIDA POR

Juan Manuel Mejía Camacho

Y APROBADA POR EL SIGUIENTE COMITÉ.

Dr. César Cruz Hernández
Director del Comité

Dr. Miguel Enrique Martínez Rosas
Miembro del Comité

M. C. Humberto Cervantes Ávila
Miembro del Comité

Ensenada Baja California, México. Marzo de 2007

RESUMEN de la tesis de **JUAN MANUEL MEJÍA CAMACHO**, presentada como requisito parcial para la obtención del grado de **MAESTRO EN INGENIERÍA, CON ORIENTACIÓN EN INSTRUMENTACIÓN Y CONTROL.** Ensenada, Baja California, México, Marzo de 2007.

ENCRIPTAMIENTO DE INFORMACIÓN MEDIANTE CAOS.

Resumen aprobado por:

Dr. César Cruz Hernández
Director de tesis

El presente trabajo de tesis trata sobre la transmisión de información confidencial encriptada, empleando dinámicas caóticas. En el esquema de comunicación propuesto, los procesos de encriptado y desencriptado se realizan mediante la sincronización caótica de los transmisores y receptores. En particular, como generador caótico se utiliza al circuito de Chua. Se sincroniza el circuito de Chua por el método de formas hamiltonianas (para el sistema maestro) y el diseño de un observador (para el sistema esclavo). Con base en lo anterior, se transmite información confidencial empleando diferentes técnicas de encriptado, en una red simétrica (igual número de transmisores que receptores) de usuarios. Los resultados son ilustrados en una red de 2 usuarios, transmitiendo por un solo canal público de comunicación.

Palabras Claves: Encriptado, desencriptado, sincronización caótica, circuito de Chua, formas hamiltonianas, observador, red simétrica y canal público.

ABSTRACT of the thesis of **JUAN MANUEL MEJÍA CAMACHO,** presented as a partial requirement to obtain the **MASTER DEGREE in ENGINEERING, ORIENTED TO INSTRUMENTATION and CONTROL.** Ensenada, Baja California, México, March 2007.

INFORMATION ENCRYPTED USING CHAOS

Abstract approved by:

Dr. César Cruz Hernández
Thesis advisor

The present thesis work treats on the transmission of confidential information encrypted by chaotic dynamics. In the proposed communications diagram, the encrypted and unencrypted processes are made by the chaotic synchronization of the transmitters and receivers. In particular, as chaos generator it is used the circuit of Chua. The circuit of Chua is synchronized by the method of hamiltonian forms (for the master system) and the design of an observer (for the slave system). With base in the previous mentioned, confidential information are transmitted using different encrypted techniques, in a symmetrical network (equal number of receivers and transmitters) of users. The results are illustrated in a network of 2 users, transmitting by a single public channel of communication.

Keywords: Encrypted, unencrypted, chaotic synchronization, circuit of Chua, hamiltonian forms, observer, symmetrical network and public channel.

DEDICATORIA

A mi MADRE, a quien le debo todo lo que he logrado en la vida.
Luz Berthila Camacho Muñoz

A mi HERMANA, por todo su apoyo y comprensión.
Viridiana Alejandra Berenice Mejía Camacho

A mi ABUELITA, por todo el cariño que me brindó.
Alejandra Muñoz

A mi TIA, por su confianza y enseñanzas de la vida.
Alejandra Camacho Muñoz

A mis PRIMOS, por su buena vibra y amistad.
Li Guevara Camacho.
Víctor Guevara Camacho.

A toda mi FAMILIA, por toda la fuerza brindada.
La familia es la mayor fuente de energía y razón de vivir

A DIOS, por todo lo que me ha dado en la vida.

AGRADECIMIENTOS

A mi director de tesis Dr. César Cruz Hernández, por su amistad y todo el apoyo brindado en la elaboración de esta tesis.

A los miembros del comité de tesis: Dr. Miguel Enrique Martínez Rosas y M. C. Humberto Cervantes Ávila, por sus comentarios y correcciones del presente documento.

A todos y a cada uno de mis maestros que formaron parte en el camino para lograr este trabajo.

A Carmina, por su amor, apoyo incondicional y estímulo continuo. Por estar en los momentos más felices, pero sobre todo en los más difíciles. Te quiero.

A mis compañeros y amigos, por su amistad y alegría. Erick, Enrique, Eduardo, Guadalupe, Canek,, Leticia, Juan Manuel, Juan Carlos, Hazael, Marybel y todos los que estuvieron en estos momentos de mi vida, gracias por su apoyo y mistad.

Al Proyecto de Investigación en Ciencia Básica (CONACYT) con referencia P50051-Y.

A todas y cada una de las personas que a lo largo de mi vida y mis estudios me han apoyado, y que por falta de memoria y la gran cantidad de hojas que necesitaría, no incluí individualmente en estos agradecimientos.

Contenido

Lista de Figuras

1 Introducción

1.1 Motivación

Debido a la vertiginosa evolución de los sistemas de comunicaciones actuales, a su acelerada proliferación y uso en todo el mundo, es que surge la impostergable necesidad de *servicios que garanticen seguridad en el almacenamiento y en la transmisión de información*, con el propósito de resguardar o proteger información confidencial. A lo largo de la historia del hombre, se han utilizado diversos algoritmos para el encriptado de información. El *DES* por sus siglas en inglés (*Data Encryption Standard)* Estándar de Encriptamiento de Información, es el algoritmo criptográfico más empleado en la historia reciente.

En el pasado, la criptografía se utilizó principalmente para fines bélicos. Por ejemplo, tuvo inmenso auge durante la Segunda Guerra Mundial, actualmente la criptografía se emplea en instituciones gubernamentales, las cuales manejan información de estado muy valiosa, el lector interesado en más detalles puede consultar (Sing S. 1999), o bien (Kahn D. 1996).

Por otra parte, recientemente, el hombre se percató de "cierto" comportamiento en los sistemas no lineales, la aparición de oscilaciones aperiódicas. Principalmente, en procesos industriales y tecnológicos, la presencia de este comportamiento provocó pánico entre los ingenieros y técnicos, a quienes se obliga a operar a los sistemas en regiones donde no se pudiera presentar dicho comportamiento. Tiempo después, se comprobó que esta práctica, limita el desempeño óptimo de los sistemas o al menos, un mejor rendimiento en beneficio del hombre. En la actualidad, después de muchos estudios teóricos e investigaciones experimentales, se reconoce que el **caos** es útil en muchas aplicaciones y en los últimos tiempos, se ha incrementado el interés por utilizarlo en diversas disciplinas. La razón principal por el interés en el caos, se debe a su "complejidad" y a su comportamiento dinámico muy parecido al ruido. Sin embargo, el caos es generado por un sistema determinístico, regido por ecuaciones diferenciales o en diferencias no lineales y sensible a condiciones iniciales. Cuando el caos se encuentra bajo control, es capaz de proporcionar una variedad de propiedades especiales benéficas para el hombre. Por ejemplo, existen pruebas que el caos se manifiesta en circuitos electrónicos de manera importante y en dispositivos de alto desempeño, en sistemas biológicos, en el procesamiento de información en el cerebro, en el mezclado de líquidos, en el diseño de sistemas de **comunicaciones privadas**, entre otras aplicaciones numerosas.

El **encriptado de información mediante caos** fue sugerido por Pecora y Carroll en 1990 (Pecora y Carroll 1990) como alternativa de cifrado. Este difiere de los métodos convencionales; los cuales, se construyen con base en algoritmos matemáticos sofisticados, como: factorización en números primos, curvas elípticas, entre otros (ver por ejemplo, Menezes *et al.* 2001). A partir del trabajo citado de Pecora y Carroll, se han propuesto y probado a nivel experimental diversas metodologías, para transmitir información encriptada con base en sincronización de sistemas caóticos, como *encriptado caótico aditivo* (Kocarev *et al.* 1992; Cuomo *et al.* 1993), *conmutación entre distintos atractores caóticos* (Parlitz *et al.* 1992; Palaniyandi y Lakshmanan 2001), *modulación paramétrica* (Yang y Chua 1996; Wang y Wang 2003), etc.

Los sistemas de **comunicaciones privadas empleando caos**, son esquemas constituidos usualmente por un transmisor caótico y un receptor idéntico, donde la información confidencial, se mezcla con la señal caótica generada en el transmisor y empleada como portadora, mediante modulación directa, adición o cualquier otra técnica. En el extremo remoto del receptor, si la sincronización caótica entre transmisor y receptor es obtenida, entonces se puede reconstruir la información oculta (cifrada) a partir de la señal de recepción (ver Cruz-Hernández y López-Mancilla 2007).

La literatura especializada en los tópicos de cifrado caótico es extensa, ver por ejemplo (Kocarev *et al.* 1992; Cuomo *et al.* 1993; Parlitz *et al.* 1992; Palaniyandi y Lakshmanan 2001; Yang y Chua 1996; Wang y Wang 2003; Aguilar-Bustos y Cruz-Hernández 2002; Cruz-Hernández 2005; López-Mancilla y Cruz-Hernández 2005; Cruz-Hernández *et al.* 2005; Cruz-Hernández y López-Mancilla 2007; Posadas-Castillo *et al.* 2007) y las referencias incluidas allí. Sin embargo, es hasta los últimos

años, que empiezan a aparecer trabajos donde se reporta la necesidad de aplicar el cifrado caótico a sistemas donde se requiere la comunicación privada entre múltiples usuarios. Por otra parte, es de sobra conocida la importancia y actualidad de las comunicaciones privadas entre mutiusuarios; por ejemplo, en la comunicación por redes de computadoras, en las comunicaciones por correo electrónico, el comercio por internet, las operaciones bancarias, los pagos de servicios por internet y en algunas unidades de teléfonos, etc.

Motivados por los argumentos expuestos, este trabajo de tesis se propuso contribuir a la comunicación privada empleando caos. En particular, mediante la extensión de los resultados reportados en la literatura, en particular en (Sira-Ramírez y Cruz-Hernández 2000; 2001) a una red de comunicación entre múltiples usuarios.

1.2 Algunos antecedentes sobre encriptado empleando caos

Como se mencionó, fueron Pecora y Carroll quienes sugirieron por primera vez, la posibilidad del cifrado mediante caos (Pecora y Carroll 1990). Desde entonces, se han llevado numerosas investigaciones al respecto. A continuación de manera breve, se daran algunos antecedentes sobre este tópico, por supuesto haciendo énfasis en los trabajos de cifrado por caos, relacionados con la metodología adoptada en este trabajo de tesis, para alcanzar sincronización de sistemas caóticos.

En (Posadas-Castillo 2001) se lleva acabo la sincronización entre dos osciladores de Lorenz por formas hamiltonianas y también la comunicación binaria entre ellos. En (Meranza-Castillón 2002) se presenta la sincronización entre dos circuitos hypercaoticos, así como la implementación de un sistema de encriptamiento hipercaótico. En (Gámez-Guzmán 2004) se muestra un encriptador de información con base en la sincronía de atractores con enrrollamientos múltiples. En (López-Mancilla 2005; López-Mancilla y Cruz-Hernández 2005) se reporta la sincronización de sistemas caóticos en configuración maestro y esclavo. Se presentan dos casos de estudio: uno para sistemas idénticos y otro para sistemas no idénticos. La sincronización se logra mediante acoplamiento a modelos, metodología inspirada de la teoría de control no lineal. Haciendo una aplicación al campo de las comunicaciones, encriptando mediante caos información de audio en el sistema maestro y desencriptando después en el sistema esclavo. En (Aguilar-Bustos 2006; Aguilar-Bustos y Cruz-Hernández 2002) presentan la transmisión de información confidencial entre dos sistemas hipercaóticos de tiempo discreto acoplados de forma unidireccional. Otro método se sugiere en (Serrano-Guerrero 2004; Cruz-Hernández y Serrano-Guerrero 2005). En este método en particular, utilizan una combinación de sincronización de caos y una función de encriptado compleja para ocultar la información, con el objetivo de incrementar la complejidad del encriptado. Encriptan información privada tanto analógica como digital. En (Romero Haros 2005; Cruz-Hernández y Romero Haros 2007) utilizan el circuito de Chua con la retroalimentación de un retardo de tiempo para transmitir información privada encriptada. Dicha retroalimentación produce que el circuito de Chua desarrolle un comportamiento caótico más complejo. Se muestran dos esquemas para llevar a cabo la transmisión. En el primero, se lleva acabo la sincronización caótica entre el transmisor y receptor mediante un canal, y por un segundo canal se envía la información encriptada. En el segundo método, tanto la sincronización como la transmisión de información se lleva a cabo por el mismo canal público. En (López-Mancilla 2005; López-Mancilla y Cruz-Hernández 2007) se presenta la sincronización entre dos sistemas caóticos bajo la presencia de perturbaciones no desvanecientes. Para llevar acabo la sincronización se utiliza el acoplamiento a modelos.

Motivados por los antecedentes expuestos sobre el cifrado no convencional de información, este **trabajo de tesis** se propone **contribuir a la transmisión privada de información mediante sincronía de caos**, con la diferencia sustancial de que los sistemas de comunicaciones mencionados, se restringen a una pareja de usuarios, es decir un transmisor y un receptor, en el presente trabajo de tesis se propone el diseño de un esquema de comunicación privada, donde se extenderá la comunicación privada para una red de usuarios, empleando un solo canal de transmisión.

1.3 Planteamiento del problema de estudio

La transmisión de información privada de manera segura entre destinos remotos, o bien, el almacenamiento de información confidencial son problemas a los que se ha enfrentado la humanidad desde tiempos antiguos. Una manera confiable de proteger o resguardar esta información es sin duda mediante el **cifrado**. Podemos decir, que **encriptamiento** es el proceso de "revolver" u "ocultar" el contenido de un mensaje con el propósito de hacer a éste indescifrable a toda persona no autorizada; es decir, que no cuente con la clave (o llave) con la que se llevo acabo este proceso de cifrado (Cruz-Hernández y López-Mancilla 2007).

Por ejemplo, si **Alicia** pretende comunicarse de manera segura con **Juan** y no quiere que otra persona (**Oscar**) se entere qué información está transmitiendo. Entonces, encripta la información empleando una clave secreta, de esta manera, la mantiene segura de Oscar. Por tanto, Alicia encriptará la información utilizando una clave y enviará la información encriptada a través de un canal público a Juan, el cual, es accesible a Oscar o a cualquier persona (de ahí que se diga que el canal empleado es inseguro). De esta manera, solamente la persona que tenga la clave, podrá descifrar la información. Por tanto, si Juan tiene la clave (y acceso a la señal encriptada que transmite Alicia), entonces podrá saber el contenido de la información. Oscar sin la clave no podrá reconstruir dicha información enviada. Esta situación, puede apreciarse gráficamente en la figura 1.

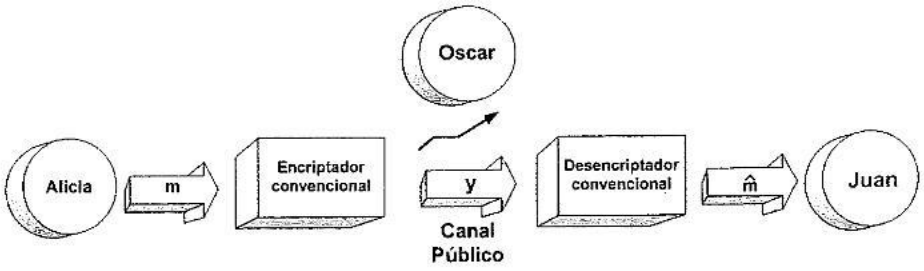

Figura 1: Comunicación remota de información entre Alicia y Juan, a través de un canal público. m: mensaje privado por enviarse encriptado a Juan, y: mensaje encriptado ilegible para el intruso Oscar, $\hat{m}$: mensaje desencriptado entendible para Juan.

El problema particular de estudio en este trabajo de tesis, es sustituir los algoritmos de encriptado convencionales que utilizan Alicia y Juan para su comunicación, por otro medio de encriptado, en nuestro caso, empleando dinámicas caóticas con el propósito de alcanzar el mismo objetivo, es decir la información cofidencial no debe ser comprendida por el intruso Oscar (ver figura 2).

El generador caótico que se propone emplear en este sistema de comunicación confidencial es el circuito de Chua. Ya que para este circuito se ha desmostrado experimental y analíticamente la existencia de caos. Además, se propone ampliar este esquema de comunicación a una red de múltiples usuarios, ver figura 3.

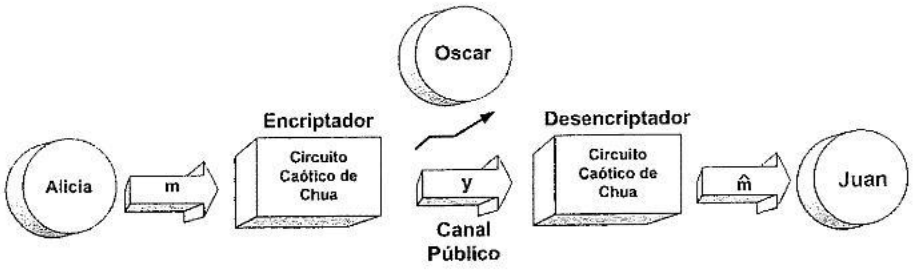

Figura 2: Comunicación remota de información entre Alicia y Juan, a través de un canal público. m: mensaje privado por enviarse a Juan, y: mensaje encriptado ilegible para el intruso Oscar, $\hat{m}$: mensaje desencriptado entendible para Juan.

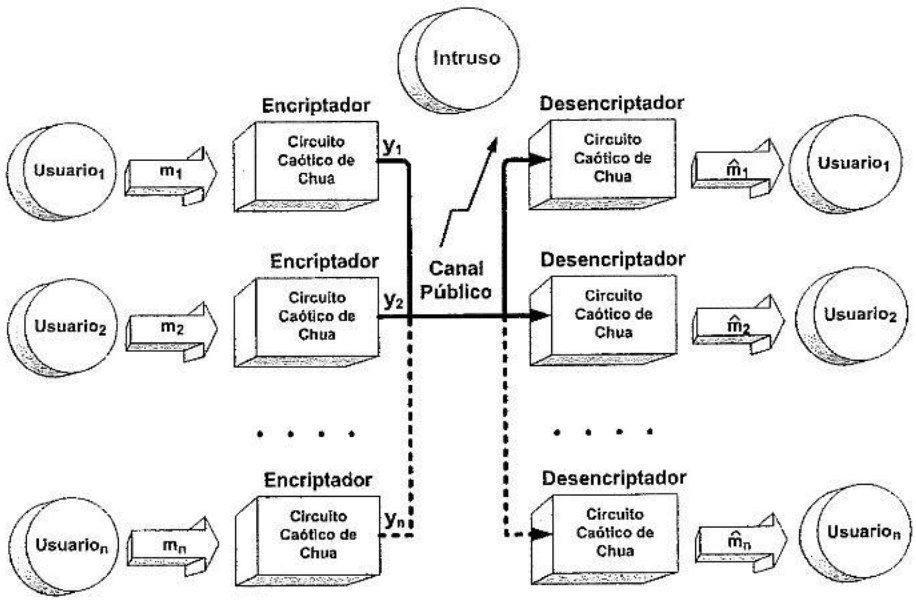

Figura 3: Comunicación remota de información entre múltiples usuarios en el transmisor y receptor, a través de un canal público. m_1, m_2,..., m_n: mensajes confidenciales por enviar simultaneamente a través de un canal público, y_1, y_2, ..., y_n: mensajes encriptados e ilegibles para el intruso Oscar, $\hat{m}_1$, $\hat{m}_2$, ..., $\hat{m}_n$: mensajes desencriptados entendibles para los destinatarios Usuario$_1$, Usuario$_2$, ..., Ususario$_n$, respectivamente.

1.4 Objetivos

Con la realización de este trabajo de tesis, se conseguirá alcanzar el siguiente **objetivo general**, *lograr el encriptado de información confidencial basado en sincronía de caos en una red de múltiples usuarios.*

Donde los **objetivos particulares** son:

- Diseñar y simular numéricamente un sistema de encriptado con base en el circuito caótico de Chua.
- Implementar en circuitería electrónica el sistema de encriptado para una pareja de usuarios; empleando el circuito de Chua como generador de caos.
- Sincronizar múltiples maestros y múltiples esclavos empleando formas hamiltonianas y el diseño de un observador no lineal (Sira-Ramírez y Cruz-Hernández 2000; 2001).
- Extender el esquema de comunicación propuesto a una red de usuarios. Diseñar éste y simular numéricamente la transmisión de información entre el sistema transmisor y receptor, conformados por múltiples usuarios.

1.5 Metodología adoptada

El sistema de comunicación de información confidencial entre una red de usuarios, se basa en la sincronía de múltiples circuitos caóticos de Chua. Por tanto, en este trabajo se adopta el método de sincronización por formas hamiltonianas generalizadas y el diseño de un observador no lineal para sincronizar los múltiples esclavos, metodología propuesta en (Sira-Ramírez y Cruz-Hernandéz 2000; 2001), la cual, presenta las siguientes ventajas por encima de otros métodos de sincronización de sistemas caóticos reportados en la literatura:

- La sincronización se obtiene de manera sistemática.
- Es posible aplicarlo a muchos sistemas caóticos e hipercaóticos.
- No se necesita el cálculo de ningún exponente de Lyapunov.
- No requiere que las condiciones iniciales pertenezcan a la misma cuenca de atracción.
- Permite conocer la señal acoplante adecuada para llevar a cabo la sincronización.

1.6 Organización del manuscrito

El material contenido en este trabajo de tesis, está **organizado** de la siguiente forma: En el **capítulo 2** se presenta el problema fundamental de la criptografía, seguido de conceptos, definiciones y nomenclatura, empleados comunmente en esta disciplina. También, se describe brevemente la historia de la criptografía y de los algoritmos criptográficos de mayor empleo.

En el **capítulo 3** se proporcionan las características de los sistemas dinámicos, como son la representación en variables de estado y sus estados de equilibrio. Se define un sistema caótico, se muestran las propiedades más importantes que manifiesta el caos, se ilustra su reperesentación gráfica y las maneras de medir la cantidad de caos en un sistema. Por último, se presentan algunos ejemplos de sistemas caóticos.

El **capítulo 4** expone lo relativo al circuito de Chua, sus ecuaciones de estado así como las ecuaciones normalizadas de dicho circuito. También se muestran las dinámicas del circuito (punto de equilibrio, cíclico límite y atractor caótico) tanto por simulaciones numéricas como de forma experimental, mediante la implementación física de dicho circuito.

El **capítulo 5** está dedicado a la sincronización del circuito caótico de Chua, la cual, se logra a partir de formas hamiltonianas y el diseño de un observador no lineal. Se muestran gráficas obtenidas mediante simulación de las ecuaciones de estado del circuito de Chua, así como gráficas experimentales mediante la implementación física de dichas ecuaciones de estado utilizando circuitería. Por último, se mencionan algunas conclusiones.

El **capítulo 6** trata la sincronización entre múltiples maestros y esclavos mediante el método de sincronización en base a formas hamiltonianas y el diseño de un observador. Se presentan resultados numéricos de dicha sincronización mediante la simulación de las ecuaciones de estado de los múltiples maestros y esclavos.

El **capítulo 7** trata la comunicación de información confidencial con base en sincronía de caos a través de un canal público inseguro. Esta comunicación se realiza entre dos circuitos de Chua (transmisor y receptor), los cuales fueron previamente sincronizados en el capítulo 5. Se muestra la señal encriptadora, el mensaje a enviar por el transmisor, la señal resultante de la transmisión así como el mensaje recuperado en el sistema receptor. Los resultados se obtuvieron mediante simulaciones numéricas y por la implementación física mediante circuitería. Este capítulo también contiene el material más imporatante de este trabajo de tesis, en éste se reporta la comunicación de información confidencial con base en caos a través de un canal público inseguro, a través de una red de múltiples usuarios. Donde, tanto la sincronización (transmisor y receptor) como la transmisión de la información entre los usuarios se realiza a través de un solo canal y de forma simultánea. Resultados son ilustrados mediante simulación numérica que se lleva acabo. Al final se dan algunas conclusiones respecto a lo planteado en este capítulo.

Finalmente, en el **capítulo 8**, se dan las conclusiones de mayor relevancia, relacionadas a los resultados obtenidos durante la realización de este trabajo de tesis. También se mencionan algunos problemas abiertos, así como recomendaciones para trabajos futuros en esta dirección. Por supuesto, se mencionan las aportaciones que este trabajo de tesis arroja al campo de las comunicaciones de información confidencial empleando caos.

Al final de este manuscrito se incluyen los programas con los que fueron realizadas todas las simulaciones numéricas de este trabajo, reunidas en un apéndice.

2 Criptografía

En este capítulo se da una breve explicación sobre algunos aspectos relacionados a la criptografía. El propósito de éste, es presentar principios básicos, con el objetivo de que el lector se familiarice con ellos y así logre una mejor comprensión de los temas a tratar en los siguientes capítulos. Se remite al lector con interés en profundizar en el material presentado en este capítulo a (Menezes A. *et al*; Zbigniew Kotulski y Janusz Szczepanski 1997) y el sitio www.wikipedia.com.

2.1 Conceptos y definiciones

La criptografía se define como la técnica de transformación de información de manera de hacerla incomprensibles frente a intrusos. En la jerga de la criptografía, la información original que debe protegerse se denomina **texto claro**. El **cifrado** es el proceso de convertir el texto claro legible en uno ilegible, denominado **texto cifrado** o **criptograma**. Por lo general, la aplicación concreta del **algoritmo de cifrado** (también llamado **cifra**) se basa en la existencia de una **clave**: información secreta que adapta el *algoritmo de cifrado* para cada uso distinto. Cifra es una antigua palabra arábiga para el cero, en la antigüedad cuando Europa empezaba a cambiar del sistema de numeración romano al arábigo, se desconocía el cero por lo que éste resultaba misterioso, de ahí probablemente cifrado signifique misterioso. Las dos técnicas básicas de cifrado en la criptografía clásica son la **sustitución** (que se fundamenta en el cambio de significado de los elementos básicos del mensaje, las letras, los dígitos o los símbolos) y la **trasposición** (que se base en una reordenación de las mismas); la gran mayoría de las *cifras* clásicas son combinaciones de estas dos operaciones básicas. El **descifrado** es el proceso inverso que recupera el texto claro a partir del criptograma y la clave. El **protocolo criptográfico** especifica los detalles de cómo se utilizan los *algoritmos* y las *claves* (y otras operaciones primitivas) para conseguir el efecto deseado. El conjunto de protocolos, algoritmos de cifrado, procesos de gestión de claves y actuaciones de los usuarios, en su globalidad es lo que constituyen un **criptosistema**, que es con lo que el usuario final trabaja e interactúa.

Existen dos grandes grupos de cifras: los algoritmos que utilizan una única clave tanto en el proceso de cifrado como en el de descifrado y los que utilizan una clave para cifrar mensajes y una clave distinta para descifrarlos. Los primeros se denominan **cifras simétricas** o de **clave simétrica** y son la base de los algoritmos de cifrado clásico. Los segundos se denominan **cifras asimétricas**, de **clave asimétrica** o de **clave pública** y **clave privada** y forman el núcleo de los algoritmos de cifrado modernos.

En el lenguaje cotidiano, la palabra código se usa de forma indistinta con cifra. En la jerga de la criptografía, sin embargo, el término tiene un uso técnico especializado: los **códigos** son un método de criptografía clásica que consiste en sustituir unidades textuales más o menos largas o complejas, habitualmente palabras o frases, para ocultar el mensaje; por ejemplo, "cielo azul" podría significar "atacar al amanecer". Por el contrario, las cifras clásicas normalmente sustituyen o reordenan los elementos básicos del mensaje, letras, dígitos o símbolos; en el ejemplo anterior, "rcnm arcteeaal aaa" sería un criptograma obtenido por transposición. Cuando se usa una técnica de códigos, la información secreta suele recopilarse en un libro de códigos.

Con frecuencia los procesos de cifrado y descifrado se encuentran en la literatura como **encriptado** y **desencriptado**, aunque ambos todavía sin reconocimiento académico. Hay quien hace distinción entre "cifrado/descifrado" y "encriptado/desencriptado" según esté hablando de criptografía simétrica o asimétrica.

2.2 Problema fundamental de la criptografía

El problema principal de las comunicaciones privadas es precisamente como establecer una comunicación confidencial de una forma segura mediante un determinado canal público. Ya que con el simple hecho de escribir un mensaje o hablarlo, otras personas pueden saber del contenido del mismo leyendo o escuchando (ver figura 4).

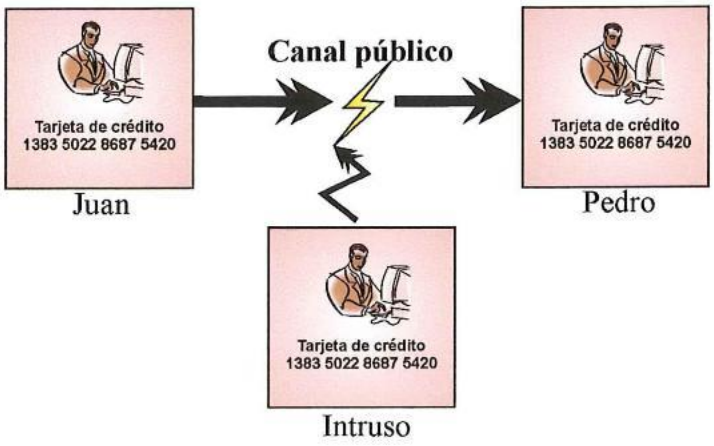

Figura 4: Comunicación confidencial de forma insegura a través de un canal público.

Una de las formas de resolver este problema es ocultar la presencia del mensaje, por ejemplo, utilizando una tinta que a simple vista no pueda ser vista. Otro ejemplo, podría ser durante la Segunda Guerra Mundial, donde agentes de espionaje usaban micro-puntos para mandar información, los puntos eran extremadamente pequeños comparados con los de una letra de una máquina de escribir por lo que en un punto se podía incluir todo un mensaje. A esta técnica se le llama **esteganografía**, la cual se define como la rama de la criptología que trata sobre el ocultamiento de mensajes, para evitar que se perciba la existencia del mismo. Otra forma de resolver este problema, sin ocultar la presencia del mensaje sería hacer ilegible dicho mensaje, es decir, esconder su contenido.

La criptología es el estudio de los criptosistemas: sistemas que ofrecen medios seguros de comunicación en los que el emisor oculta o cifra el mensaje antes de transmitirlo para que sólo un receptor autorizado pueda descifrarlo (ver figura 5). Sus principales áreas de interés son la criptografía y el criptoanálisis. Donde el criptoanálisis es todo lo contrario, es decir, consiste en en desbaratar los mensajes transformados, de tal manera de hacerlos legibles.

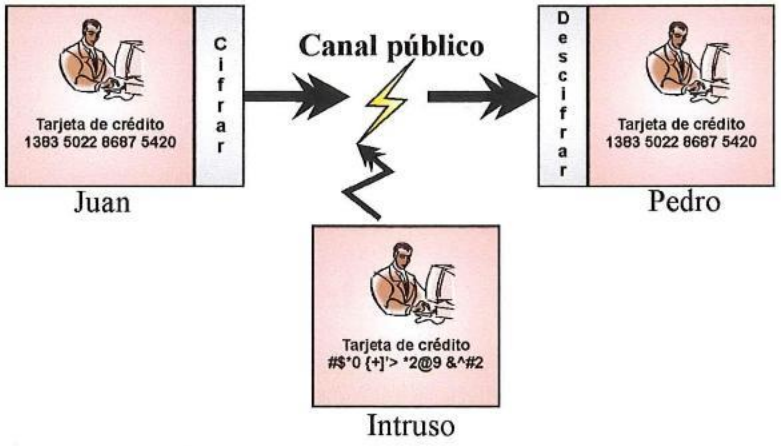

Figura 5: Comunicación confidencial de forma segura a través de un canal público.

Normalmente, se consideran los términos encriptar y cifrar como sinónimos, al igual que sus respectivas contrapartes, desencriptar y descifrar, pero no ocurre lo mismo con el término codificar. Por definición, codificar significa expresar un mensaje utilizando algún código, pero no necesa-

riamente de forma oculta o secreta; escribir en idioma español implica el uso de un código, que será comprensible para los hispanohablantes pero no tanto para quienes no dominan el idioma; la matemática y la lógica tienen sus propios códigos, y en general existen tantos códigos como ideas.

2.3 Historía de la criptografía

La historia de la criptografía se remonta a miles de años. Hasta décadas recientes, ha sido la historia de la criptografía clásica los métodos de cifrado que usan papel y lápiz, o quizás ayuda mecánica sencilla. A principios del siglo XX, la invención de máquinas mecánicas y electromecánicas complejas, como la máquina de rotores Enigma (ver figura 6), proporcionaron métodos de cifrado más sofisticados y eficientes; y la posterior incorporación de la electrónica y la computación han permitido sistemas que siguen teniendo gran complejidad.

Figura 6: Máquina Enigma, utilizada para el cifrado y decifrado de información.

Desde el punto de vista histórico los métodos de cifrado se han dividido en dos categorías: cifradores de sustitución y cifradores de transposición. En un cifrador por sustitución, cada letra o grupo de letras se sustituye por otra letra o grupo de letras para codificarlas. Los cifradores por sustitución preservan el orden de los símbolos del texto en claro, pero los codifican. El cifrador por sustitución más antiguo que se conoce es el cifrador de César, atribuido a Julio César. En este método, la letra A se sustituye por D; B por E; C por F, y así sucesivamente, cada letra se sustituye por la que se encuentra tres lugares delante de ella, considerando que luego de la letra Z vuelve a comenzar por la letra A. Una variante del cifrador de César es permitir que el alfabeto cifrado se pueda desplazar k letras (no sólo 3), convirtiéndose k en la clave.

Una mejora al cifrador de César consisite en relacionar a cada letra del alfabeto con un carácter. En este sistema, llamado sustitución monoalfabética, la clave consistirá en la cadena completa de caracteres del alfabeto. El ataque a los sistemas de encriptado por sustitución consiste en aprovechar las propiedades estadísticas de los lenguajes. Sabiendo el idioma del texto en claro y calculando el porcentaje de ocurrencias de letras y de combinaciones de dos y tres letras se puede adivinar una palabra y así deducir la clave.

Una forma de fortalecer el cifrador de César se logra utilizando múltiples sistemas de César aplicados periódicamente. Este sistema se conoce como cifrado polialfabético, un ejemplo es el sistema criptográfico de Vigenére. Consiste en una matriz cuadrada la cual contiene 26 alfabetos de César. Ahora la clave estaría constituida por una palabra simple mas la matriz de 26 x 26.

Este sistema criptográfico resultó bastante seguro por algún tiempo, debido principalmente a la imposibilidad de determinar el tamaño de la clave. Una vez encontrado el tamaño de la clave, es posible encontrar las sustituciones simples agrupando las letras. En 1863 F. W. Kasiski resolvió el problema de encontrar el tamaño de la clave a través de la técnica llamada: La incidencia de las coincidencias.

El cifrado Vernam es un caso particular del Vigenére con una clave de igual tamaño que el texto a codificar. Eligiendo la clave en forma aleatoria el sistema es incondicionalmente seguro pero tiene el inconveniente que ambos transmisor y receptor deben saber la clave y ésta se debe comunicar por otro canal que sea seguro.

A diferencia de los cifradores de sustitución, los cifradores de transposición, reordenan las letras pero no las disfrazan. Consiste en una tabla con determinado número de columnas, este número de columnas estará dado por la cantidad de caracteres de la clave que a su vez no tendrá ningún caracter repetido. La clave tiene el propósito de numerar las columnas correspondiendo a la primera letra en orden alfabético el número 1. El texto en claro se escribe en las filas de la tabla de arriba hacia abajo, el texto codificado será leído verticalmente comenzando por la columna 1, luego la 2, etc.

Hoy en día, en una computadora el procedimiento de codificación se puede realizar por software o por hardware. La codificación por software puede ser específico de una aplicación. La codificación independiente de la aplicación se puede hacer por hardware o a partir de un programa que funcione casi al mismo nivel que un sistema operativo, por ejemplo, el lenguaje de programación ensamblador.

2.4 Algoritmos criptográficos

El procedimiento utilizado para encriptar información se realiza por medio de un algoritmo, al cual, se le puede considerar como una función matemática. Por lo tanto, un algoritmo de encriptación es una fórmula para desordenar la información de manera que ésta se transforme en incomprensible, usando un código o clave (en ocasiones, mas de una). Los mensajes que se tienen que proteger, denominados texto claro, se transforman mediante esta función, y a la salida del proceso de puesta en clave se obtiene el texto cifrado, o criptograma. En muchos casos, existe un algoritmo de desencriptación encargado de reordenar la información y volverla inteligible, pero no siempre es así. Cuando existen ambas funciones, una para cifrar y otra para descifrar, se dice que el sistema criptográfico es de dos vías o reversible (a partir de un mensaje en claro se puede obtener uno encriptado y a partir de éste se puede obtener el mensaje original), mientras que cuando no existe una función para desencriptar se dice que el sistema es de una sola vía (a partir de un mensaje cifrado no es posible obtener el mensaje en claro que lo generó; la aplicación de esto es, por ejemplo, para el almacenamiento de contraseñas).

La transformación de información provee una posible solución a dos de los problemas de la seguridad en el tratamiento de información. El problema de la privacidad y el de la autenticación, evitando que personas no autorizadas puedan extraer información del canal de comunicación, o modificar esta información.

A continuación se mencionan algunos tipos de algoritmos de cifrado:

- **DES** por sus siglas en inglés (Data Encryption Standard) Encriptado Estándar de Información. 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. Esta basado en la aplicación de todas las teorías criptográficas existentes hasta el momento. Hoy en día, DES se considera inseguro para muchas aplicaciones. Ésto se debe principalmente a que el tamaño de clave de 56 bits es corto; las claves de DES se han roto en menos de 24 horas.
- **TDES** (Triple DES) se llama al algoritmo que hace triple cifrado del DES, éste fue desarrollado por IBM en 1978. El sistema DES se considera en la actualidad poco seguro, debido a la corta longitud de su clave. Para superar este problema y continuar aplicando el DES, se generó 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. El Triple DES está desapareciendo lentamente, siendo reemplazado por el algoritmo AES. Sin embargo, la mayoría de las tarjeta de crédito y otros medios de pago electrónico tienen como estandar el algoritmo Triple DES (anteriormente usaban el DES). El diseño DES y por lo tanto TDES son algoritmos lentos.

- **AES** por sus siglas en inglés (Advance Encryption Standard) Estándar de Encriptamiento Avanzado, también conocido como Rijndael, es un esquema de cifrado por bloque adoptado como un estándar de encriptación por el gobierno de los Estados Unidos, y se espera que sea usado en el mundo entero, como también analizado exhaustivamente, como fue el caso de su predecesor, el Estándar de Encriptación de Datos (DES). AES puede llegar a ser hasta 6 veces más rápido y hasta la fecha no se ha encontrado ninguna vulnerabilidad.

La tecnología del crifrado de información se encuentra evolucionando constantemente. Debido a las vulnerabilidades que se han estado encontrando en los algoritmos de cifrado conforme estos se emplean, existe la necesidad de seguir desarrollando nuevos algoritmos mas robustos y complejos. Esto con el motivo de seguir brindando seguridad en las operaciones que conllevan la transferencia de información privada de un lugar a otro (transferencia de dinero, compras con tarjeta de crédio via internet entre otras).

2.5 Método alternativo de encriptado

El encriptado de información mediante dinámicas caóticas fue sugerido por Pecora y Carroll (1990) como un método alterno para encriptar la información. En la figura se muestra la idea general, la cual consiste encriptar información confidencial por medio de la dinámica compleja de un sistema caótico en el transmisor. Mientras que la información se puede descencriptar mediante el sistema caótico que se encuentra en el receptor, donde este esta sincronizado con el sistema caótico del transmisor.

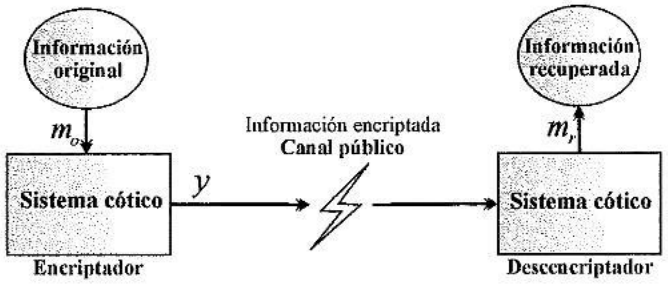

Figura 7: Sistema de encriptado mediante sincronía de sistemas caóticos, donde m_o:información original por encriptar, y: información encriptada y m_r: información recuperadada.

2.5.1 Antecedentes de solución

Gran cantidad de métodos se han presentado para la transmisión segura de información en base a la sincronización caótica:

- Encriptamiento por codificación cótica aditiva, ver por ejemplo (Kocarev *et al* 1992) y (Cuomo *et al* 1993).
- Encriptamiento por conmutación entre diferentes atractores caóticos, ver por ejemplo (Partlitz *et al* 1992) y (Palaniyandi y Lakshmanan 2001).
- Encriptamiento por modulación paramétrica caótica, ver por ejemplo (Yang y Chua 1996) y (Wang y Wang 2003).

Sin embargo, estos métodos solo se han enfocado a la transmisión de información confidencial encriptada, entre un transimisor y un receptor. En la actualidad existe la necesidad de enviar información confidencial encriptada a través de un canal público entre varios transmisores y receptores

a la vez. Esto fue propuesto por (Milanovic y Zaughloul 1996) mediante la teoría de expansión del espectro propuesto en (Pickholtz, Schilling y Milstein 1982).

Una evidencia de la inseguridad que existe en las operaciones electrónicas hoy en día (compras, depositos, etc.) se muestra en el artículo publicado el 3 de diciembre de 2006 en el diario La Jornada. De enero a octubre la Condusef recibió 640 quejas de víctimas de estafa por ese medio. Se dispara en México número de fraudes bancarios por Internet. Plantea directivo de Banorte doble autentificación para usuarios que manejan grandes cantidades, reconocen autoridades que los delincuentes cibernéticos son cada vez más sofisticados (EDUARDO MARTINEZ CANTERO).

2.6 Conclusiones

Los algoritmos matemáticos utilizados hoy en día para el cifrado de información privada son por el momento seguros. Sin embargo, debido a los ataques constantes y cada vez más evolucionados hacia los algoritmos de cifrado, genera la necesidad del desarrollo de nuevos métodos de cifrado más seguros. Es por eso que nos lleva al análisis de sistemas caóticos (circuito de Chua) para aplicar el comportamiento dinámico de estos dentro del cifrado de información. Sin olvidar que por más complejo que sea el algoritmo de cifrado, siempre habra un tiempo que este sea burlado, convirtiendose esto en un problema eterno de encriptado y ruptura.

3 Caos

En este capítulo se presentan algunos conceptos y definiciones básicas para abordar el tema de caos y características fundamentales de los sistemas caóticos. También, se mencionan algunas de las aplicaciones de dichos sistemas caóticos. El lector interesado en profundizar sobre este apasionante tópico de caos, puede consultar la referencia (Chua *et al.* 1993; Ott 2002).

3.1 Preliminares

A continuación se mencionan algunos términos básicos, útiles para la comprensión de la información contenida en los siguientes capítulos.

Sistema. Es un grupo de elementos físicos y lógicos que actuan juntos para realizar un objetivo determinado. Este concepto se aplica a fenómenos dinámicos y abstractos, tales como los que se encuentran en sistemas físicos, biológicos, económicos y parecidos.

Sistema no lineal. Es aquel en el que sus respuestas no son directamente proporcionales a una variable dada tal como una señal de entrada. En este sistema no aplica el principio de superposición. Por tanto, para un sistema no lineal la respuesta a dos entradas no puede calcularse tratando cada una a la vez y sumando resultados.

Sistema dinámico. Es el que experimenta cambios en su estado conforme pasa el tiempo. Los modelos de sistemas dinámicos lineales se han utilizado para describir y modelar dinámicas de varios fenómenos físicos, químicos entre otros. Pero muchos fenómenos pueden presentar dinámicas demasiado complejas, que no pueden representarse como se quisiera mediante modelos lineales.

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

Variables de estado. Son las que forman el conjunto más pequeño de variables que determinan el estado del sistema dinámico. Se necesitan n variables $x_1, x_2, ..., x_n$ para describir por completo el comportamiento de un sistema dinámico de orden n (por lo cual, una vez que se proporciona la entrada para $t \geq t_0$ y se especifica el estado inicial en $t = t_0$, el estado futuro del sistema se determina por completo), n variables son un conjunto de variables de estado.

Vector de estado. Si se necesitan n variables de estado para describir por completo el comportamiento de un sistema determinado, estas n variables de estado se consideran los n componentes de un vector $x \in \mathbb{R}^n$. Tal vector se denomina vector de estado.

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

Ecuaciones en el espacio de estados. En el análisis en el espacio de estados, nos concentramos en tres tipos de variables involucrados en el modelado de sistemas dinámicos: variables de entrada, variables de salida y variables de estado.

El sistema dinámico debe incorporar elementos que memoricen los valores de la entrada para $t \geq t_1$. Dado que los integradores de un sistema de control en tiempo continuo funcionan como dispositivos de memoria, las salidas de tales integradores se consideran las variables que definen el estado interno del sistema dinámico. Por tanto, las salidas de los integradores funcionan como variables de estado. La cantidad de variables de estado necesarias para definir completamente la dinámica del sistema es igual a la cantidad de integradores que contiene el sistema.

3.2 Características del caos

Originalmente, el Caos se refería en la mitología griega a la sustancia primordial de la que nació el universo. En la mitología griega, el Caos o Khaos es el estado primitivo de existencia del que surgieron los primeros dioses. En griego antiguo es $Χάος$ o $Χάεος$, que significa 'vacío que ocupa un hueco', y procede del verbo $Χαίνω$, 'abrirse de par en par', y éste del indoeuropeo *ghen-, *ghn-. También se le llamaba $Aêηρ$ ($Αηρ$, 'aire'). Para mayor detalle visitar www.wikipedia.com.

En la antigua cosmología griega el Caos era la primera cosa que existió y la matriz de la cual surgió todo. Para Hesíodo y los mitos olímpicos el Caos es el «vasto y oscuro» vacío del que surgió la primera deidad (Dios), Gea.(Diosa de la tierra). En el mito pelasgo de la creación, Eurínome (la 'Diosa de todo') surgió de este Caos y creó el Cosmos a partir de él. Para los órficos era llamado el «vientre de la oscuridad», del que surgió el huevo cósmico que contenía el Universo, a veces mezclado con la «negra noche alada». La idea también se encuentra en Mesopotamia y relacionada con Tiamat, el «dragón» del Caos, a partir de cuyo desmembrado cuerpo se formó el mundo. A veces se dice que el Caos primordial es la verdadera fundación de la realidad, particularmente por filósofos como Heráclito y los de la escuela órfica. Era lo opuesto al platonismo. Era también probable que Aristóteles lo tuviese en mente cuando desarrolló el concepto de Prima Materia en su intento por combinar a Platón con los presocráticos y los naturalistas. Fue un concepto heredado por la teoría de la alquimia (www.wikipedia.com). En la figura 8 se muestra lo que en la antiguedad se consideraba caos.

Figura 8: Caos.

El comienzo de la historia del caos según las teorías actuales se puede situar cuando se inventaron los ordenadores de alta velocidad (sobre 1950) y se desarrollaron algunas intuiciones sobre cómo eran los sistemas no lineales. Esto es, cuando se vieron las primeras gráficas sobre el comportamiento de estos sistemas mediante métodos numéricos. En 1963 Edward Lorenz trabajaba en unas ecuaciones, las ecuaciones mundialmente conocidas como ecuaciones de Lorenz, que esperaba predijeran el clima en la atmósfera, y trató mediante los ordenadores ver gráficamente el comportamiento de sus ecuaciones (es decir, su comportamiento dinámico). Aunque se les llamaran ordenadores de alta velocidad, los ordenadores por aquella época eran muy lentos, por lo que Lorenz se fue a tomar un té mientras el ordenador hacía los cálculos, y cuando volvió se encontró con una figura que ahora se conoce como atractor de Lorenz (ver figura 9).

Pensó que había cometido algún error al correr el programa y lo intentó repetidas veces, logrando siempre el mismo resultado, hasta que se dio cuenta de que algo pasaba con su sistema. Después de estudiarlo detenidamente y hacer pruebas con diferentes parámetros, tanto parámetros iniciales

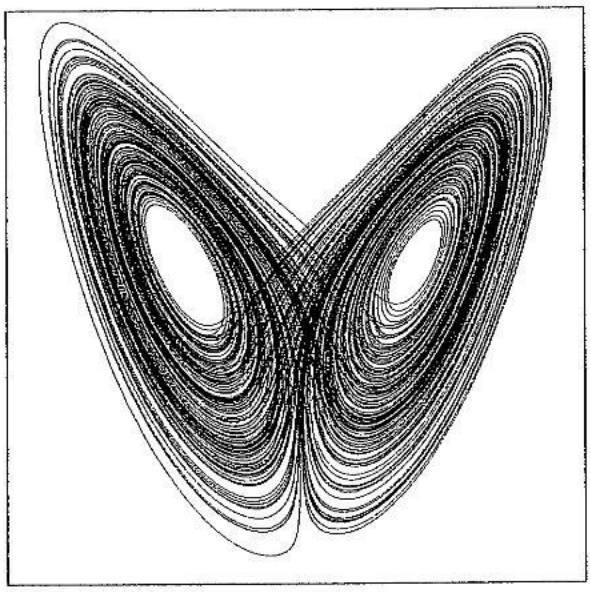

Figura 9: Atractor caótico de Lorenz.

como las constantes del sistema, llegó a la conclusión de que las simulaciones eran muy diferentes para condiciones iniciales muy próximas. Al llegar a esta conclusión, recordó que en el programa, que él había creado para su sistema de meteorología con la computadora Royal McBee, se podían introducir un máximo de 3 decimales para las condiciones iniciales, aunque el programa trabajaba con 6 decimales y los 3 últimos decimales que faltaban se introducían aleatoriamente. Ésta es la razón por la que Lorenz no llegó a encontrar la solución de la meteorología pero encontró el caos, y seguramente se alegró mucho de que su sistema no funcionara (www.wikipedia.com).

En la década de 1970 otros ejemplos de ecuaciones diferenciales caóticas empezaron a ser descubiertas. Una importante contribución fue hecha en 1976 por Otto Rössler, un doctor médico de Alemania. Rössler estuvo interesado en caos en química y biología, y el encontró un sistema de ecuaciones aun más simples que las de Lorenz que exhibían un comportamiento caótico. Lo que el realizó, son las ahora famosas *ecuaciones de Rössler (str*ange attractors by Julian C. Sprott, 2000):

$$\begin{aligned} \dot{x} &= -y - z, \\ \dot{y} &= x + ay, \\ \dot{z} &= b + z(x - c) \end{aligned} \tag{1}$$

donde a, b y c son constantes a las que Rössler asignó los valores $a = 0.2$, $b = 0.2$, y $c = 5.7$. Las ecuaciones de Rössler son a veces descritas como el ejemplo de ecuaciones conocidas más sencillas generadoras de caos de un sistema de ecuaciones diferenciales ordinarias. Estas contienen solo una no linealidad cuadrática (el producto zx en la tercera ecuación). Dichas ecuaciones generan un atractor extraño y dinámicas complejas tal y como se muestra en la figura 10.

Después de numerosos estudios e investigaciones por muchos investigadores en el mundo, ahora se sabe y se ha comprobado que el comportamiento caótico se encuentra presente en un gran número de sistemas en ingeniería y en la naturaleza de esto dan fe el inmenso material reportado en la literatura especializada (ver referencias). Un **sistema caótico** es un sistema determinístico, que a pesar de no tener entradas aleatorias presenta un comportamiento sumamente complejo, aparentemente aleatorio. El hecho de que sea determinístico permite conocer con precisión la secuencia que les

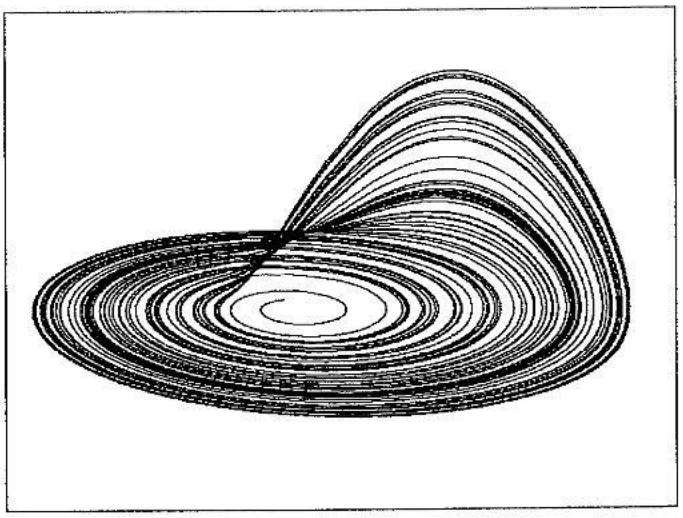

Figura 10: Atractor caótico de Rössler.

da origen, debido a que existe una ecuación determinística que gobierna su conducta basada en el conocimiento de las condiciones iniciales.

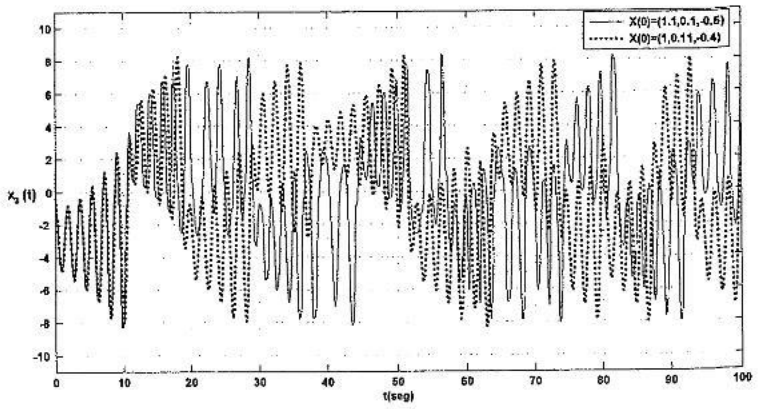

Figura 11: Evolución en el tiempo del estado caótico $x_3(t)$ del circuito de Chua para dos condiciones iniciales diferentes aunque cercanas $x(0) = (1.1, 0.1, -0.5)$ y $x(0) = (1, 0.11, -0.4)$.

La característica principal del caos es que sistemas simples (modelados por estructuras matemáticas sencillas) no lineales determinísticos pueden generar trayectorias que aparentan ser aleatorias. La propiedad esencial de estos sistemas es su **extrema sensibilidad a las condiciones iniciales**. Esto quiere decir, que si un mismo sistema parte de dos conjuntos de condiciones iniciales muy cercanas, después de un breve tiempo las trayectorias de sus estados serán muy distintas. Lo antes dicho se puede observar en la figura 11.

Un **atractor** es una región del espacio de estados hacia la cual convergen todas las trayectorias posibles de un sistema. El atractor de los sistemas estables es un **punto** (ver figura 12a) y el atractor de los sistemas periódicos es un **ciclo límite** (ver figura 12b). Independientemente del sistema que se trate, todas las trayectorias que se generen dentro de la región de atracción de estos sistemas son atraídos a estos atractores. En la figura 12 puede apreciarse por líneas segmentadas las regiones o cuencas de atracción (vecindad del espacio de estados para las condiciones iniciales, donde se generan

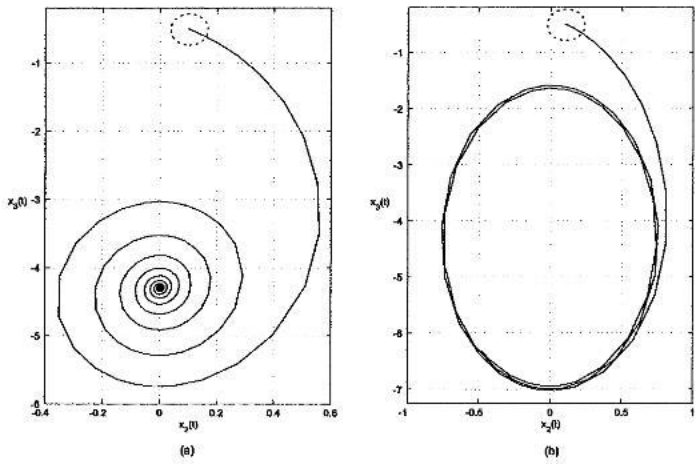

Figura 12: Atractores de un sistema dinámico: a) Punto de equilibrio estable y b) ciclo límite.

trayectorias que van a los atractores de un sistema). En particular, al atractor de un sistema caótico se le llama **atractor extraño**, debido a que sus trayectorias realizan un recorrido un tanto inusual, formando imágenes de una geometría complicada y con **dimensión fractal** como se muestra en la figura 13. Donde se observa el atractor caótico generado por el circuito de Chua, proyectado sobre el plano x_1 versus x_2.

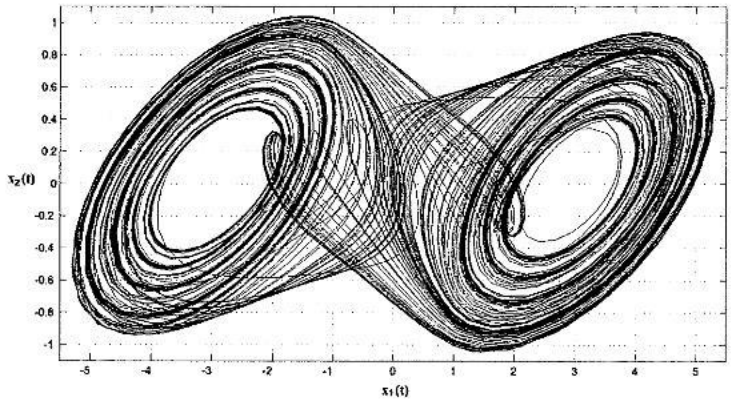

Figura 13: Atractor extraño formado por los estados caóticos $x_1(t)$ y $x_2(t)$ del circuito de Chua.

Uno de los mejores indicadores de la presencia de caos en un sistema, son los **exponentes de Lyapunov**, debido a que contienen información sobre la tasa de cambio promedio de las trayectorias en un atractor generadas por dos condiciones iniciales cercanas. Debido a esto son utilizados para obtener una medida de la dependencia de las condiciones iniciales. La *complejidad* del caos en un sistema se mide por la cantidad de exponentes de Lyapunov positivos, que son proporcionales al orden del sistema; es decir, si un sistema es de orden n, entonces tiene n exponentes de Lyapunov. Un sólo exponente de Lyapunov positivo es suficiente para indicar un comportamiento caótico.

Una característica primordial de estos sistemas, es que entre más caos exista, su función de autocorrelación tiende más rápido a cero (ver figura 14), esto se debe al carácter errático de la historia temporal.

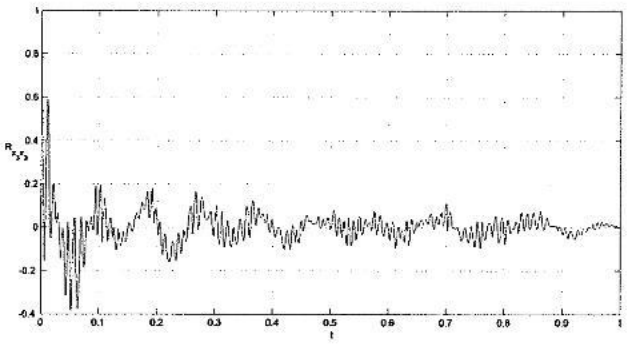

Figura 14: Autocorrelación del estado caótico $x_3(t)$ del circuito de Chua.

Otra característica que presentan los sistemas caóticos, es la apariencia de un espectro de frecuencias continuo, muy parecido al espectro del ruido estocástico, aunque con picos en las frecuencias dominantes (ver figura 15).

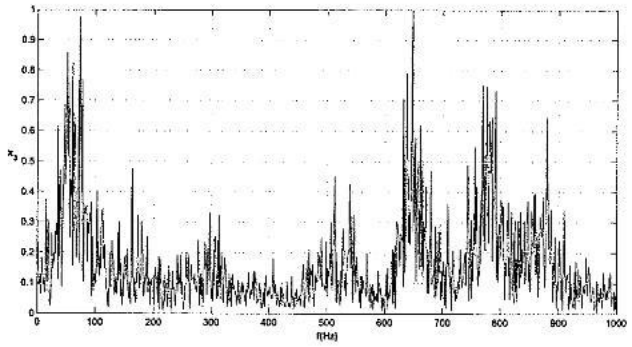

Figura 15: Espectro de frecuencias del estado caótico $x_3(t)$ del circuito de Chua.

3.3 Aplicación del caos

Una de las técnicas empleadas en la actualidad para explicar los cambios aparentemente aleatorios de las variables económicas, es la teoría de caos. Esta teoría plantea que existen evidencias para pensar que los agentes económicos asumen conductas que se reflejan en las variables macroeconómicas de manera parecida a procesos caóticos, los cuales, pueden ser explicados usando modelos no lineales.

La teoría del caos presenta una interesante perspectiva desde el punto de vista económico, principalmente en la explicación de fenómenos que aparentan tener un comportamiento desordenado. Detrás de ese aparente desorden, existe una dinámica que puede ser explicada usando apropiadas técnicas matemáticas y estadísticas, es aquí donde se aplica la teoría del caos. En sistemas dinámicos como los económicos, que cambian constantemente en el tiempo, cambios minúsculos en un momento dado, pueden ser los causantes de grandes consecuencias en un futuro.

Los sistemas caóticos también aparecen en los estudios de fenómenos tan relevantes como los meteorológicos (predicción del clima, interrelación océano y atmósfera por ejemplo) y los movimientos turbulentos de los líquidos y fluidos en general motivan y fecundan la formalización de la dinámica caótica.

En biología moderna, el estudio de la fisiología celular y de la neurobiología es encarado también desde el punto de vista físico y químico como sistemas dinámicos. Se sabe hoy, que el comportamiento de las redes neuronales puede dar lugar a conductas cíclicas estables o a conductas caóticas. Aún no es totalmente conocido el comportamiento global del sistema nervioso de los seres vivos como sistema dinámico, pero las experiencias de laboratorio y las simulaciones computarizadas muestran coincidencias asombrosas y apasionantes con las predicciones que se pueden realizar matemáticamente.

También se pueden predecir conductas caóticas en la dinámica de las células neuronales, así como "marcapasos" con los que se regula el ritmo cardiaco.

La rama biológica ha alcanzado notables avances en la aplicación del caos a tejidos biológicos. En las Facultades de Ciencias y de Medicina se desarrollan trabajos de investigación biológica experimental y teórica en biofísica y biomatemática por ejemplo, tratando modelos caóticos de sistemas vivos.

En la física y la química donde más aparecen los sistemas caóticos. De hecho su descubrimiento fue provocado por los problemas presentados al estudiar sistemas físicos complejos en la dinámica de gases y fluidos por ejemplo. Tienen importantes aplicaciones a la ingeniería moderna, en el diseño de turbomaquinarias, de circuitos de control no lineal, de sistemas de procesamiento de información y de reactores químicos por citar algunos ejemplos.

Otra muy importante aplicación en los sistemas de comunicaciones es el control y sincronización de caos. En donde en lugar de usar una portadora periódica, se utiliza una portadora caótica, cuya amplitud oscila de forma irregular en el tiempo. Utilizando esta portadora, se podría transmitir información de forma privada. El mensaje se extrae en el punto de recepción (sistema esclavo) replicando la portadora caótica mediante un dispositivo prácticamente idéntico al emisor (sistema maestro). El receptor se sincroniza a la portadora caótica del emisor, lo que permite recuperar el mensaje.

En el contexto de las comunicaciones caóticas, otra aplicación y quizas la más interesante y prometedora, es la codificación de información confidencial mediante señales caóticas. Esta propiedad de los sistemas caóticos, es precisamente la que esta tesis pretende explorar, la comunicación de información encriptada y aplicarla a una red de usuarios.

3.4 Conclusiones

Dadas las propiedades naturales del caos, las dinámicas caóticas emergen como excelentes candidatas para ocultar o cifrar información confidencial.

4 Circuito de Chua

En este capítulo se describe el circuito de Chua y su modelo matemático normalizado. Posteriormente se describe la característica no lineal del circuito de Chua, así como el diagrama electrónico, las ecuaciones de estado que modelan su comportamiento dinámico. Después, se muestra un análisis dinámico de este circuito, es decir, se presentan resultados tanto numéricos como experimentales, obtenidos del comportamiento dinámico del circuito y por último, se proporcionan algunas conclusiones respecto al tema.

4.1 Circuito caótico de Chua

Para que pueda existir caos en un circuito eléctrico (sin entradas) construido con resistencias, inductores y capacitores, éste debe contener: *a) al menos un elemento no lineal, b) mínimo un resistor localmente activo y c) al menos tres elementos almacenadores de energía.* El circuito de Chua, mostrado en la figura 16, es el circuito más simple que cumple este criterio (Kennedy 1993). Además, el circuito de Chua presenta una rica variedad de bifurcaciones, diferentes conjuntos límites y finalmente presenta caos. Este circuito es un sistema físico muy sencillo, para el cual, se ha demostrado numéricamente, probado matemáticamente y confirmado experimentalmente la existencia de caos (Madan 1993).

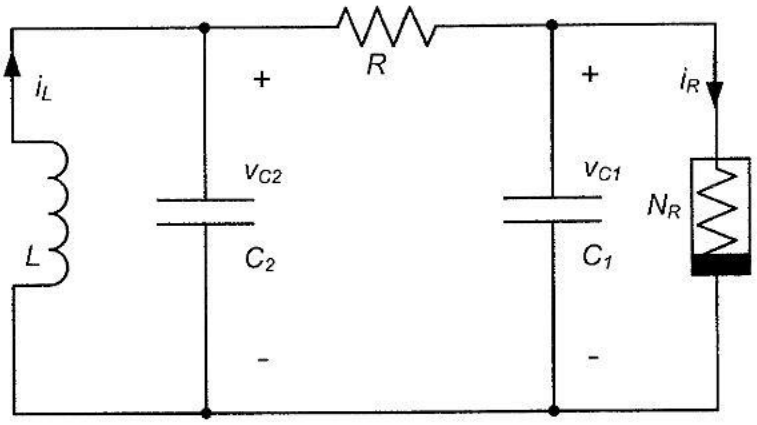

Figura 16: Circuito de Chua, contiene un inductor lineal L, dos capacitores lineales C_1 y C_2, una resistencia lineal R y un resistor no lineal N_R (diodo de Chua).

El circuito de Chua consta de un inductor lineal L, dos capacitores lineales C_1 y C_2, una resistencia lineal y la resistencia no lineal N_R, también conocido como *diodo de Chua.* Éste tiene como característica su linealidad por secciones, como se muestra en la figura 17. Las tres zonas lineales conforman una función no lineal suave.

4.2 Ecuaciones de estado del circiuto de Chua

Empleando las leyes de Kirchhoff, se deducen las siguientes ecuaciones diferenciales que modelan el comportamiento dinámico del circuito de Chua, dichas ecuaciones de estado son (Madan 1993):

$$\begin{aligned}
\frac{dv_{C_1}}{dt} &= \frac{1}{RC_1}(v_{C_2} - v_{C_1}) - \frac{1}{C_1} f(v_{C_1}), \\
\frac{dv_{C_2}}{dt} &= \frac{1}{RC_2}(v_{C_1} - v_{C_2}) - \frac{1}{C_2} i_L, \\
\frac{di_L}{dt} &= -\frac{1}{L} v_{C_2}
\end{aligned} \tag{2}$$

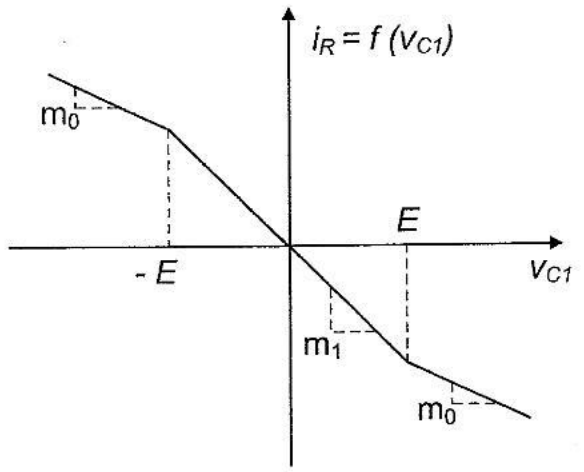

Figura 17: La relación $v - i$ de tres segmentos lineales que modelan el comportamiento de la resistencia no lineal N_R del circuito de Chua.

donde $v_{C1}(t)$ y $v_{C2}(t)$ son los voltajes a través de los capacitores C_1 yC_2, respectivamente. $i(t)$ es la intensidad de corriente a través del inductor L y donde la siguiente función no lineal

$$f(v_{C_1}) = m_1 v_{C_1} + \frac{1}{2}(m_0 - m_1)(|v_{C_1} + E| - |v_{C_1} - E|) \tag{3}$$

es la característica $v - i$ del diodo de Chua, donde m_0 es la pendiente de las regiones externas de la función $f(v_{c_1})$, mientras que la región interna tiene pendiente m_1. Los puntos de quiebre en la función no lineal, se encuentran dados por el voltaje $\pm E$ (ver figura 17).

4.3 Ecuaciones normalizadas del circuito de Chua

Para realizar el análisis dinámico del circuito de Chua, cualquiera que sea su versión, es de gran ayuda trabajar con un modelo matemático que tenga menor cantidad de parámetros y al mismo tiempo, que describa la misma dinámica del circuito de Chua. Para lo cual, es posible transformar el modelo matemático (2) y (3) en un conjunto de ecuaciones adimensionales (normalizadas) mediante el siguiente cambio de variables:

$$\begin{aligned} x_1 &\triangleq \frac{v_{c_1}}{E}, \quad x_2 \triangleq \frac{v_{c_2}}{E}, \quad x_3 \triangleq i_L \left(\frac{R}{E}\right), \\ \alpha &\triangleq \frac{C_2}{C_1}, \quad \beta \triangleq \frac{R^2 C_2}{L}, \\ a &\triangleq Rm_0, \quad b \triangleq Rm_1 \end{aligned} \tag{4}$$

escalando el tiempo

$$\tau \triangleq \frac{t}{RC_2}$$

y definiendo las variables:

$$\dot{x}_1 = \frac{dx_1}{d\tau}, \quad \dot{x}_2 = \frac{dx_2}{d\tau}, \quad \dot{x}_3 = \frac{dx_3}{d\tau} \tag{5}$$

donde E es el voltaje de ruptura de la parte no lineal del diodo de Chua (ver figura 17), el cual, se fijará a un valor de 1. Por lo tanto, las **ecuaciones adimensionales o normalizadas** del circuito de Chua son:

$$\begin{aligned} \dot{x}_1 &= \alpha\{x_2 - x_1 - f(x_1)\}, \\ \dot{x}_2 &= x_1 - x_2 + x_3, \\ \dot{x}_3 &= -\beta x_2 \end{aligned} \tag{6}$$

ahora $f(x_1)$ es la función no lineal y es definida por

$$f(x_1) = bx_1 + \frac{1}{2}(a-b)\{|x_1+1| - |x_1-1|\}. \tag{7}$$

4.4 Dinámicas del circuito de Chua

Con el propósito de observar el comportamiento dinámico del circuito de Chua, se hicieron tanto simulaciones numéricas como mediciones experimentales a partir de la implementación física del circuito de Chua, y utilizando el modelo matemático normalizado (6) y (7). De ésto, se obtuvieron tres tipos de comportamientos dinámicos en la región del espacio de estados, mejor conocida como **atractores**: Un comportamiento estable o punto, otro cíclico o también conocido como ciclo límite y por último un comportamiento caótico. Las simulaciones numéricas presentadas se hicieron mediante *simulink,* para ver estos dirigirse al apéndice incluido en este manuscrito.

4.4.1 Resultados numéricos

En la figura 18 se muestra la evolución en el tiempo de los estados $x_1(t)$, $x_2(t)$ y $x_3(t)$ del circuito de Chua con $\alpha = 4.05, \beta = 6, a = -1.758$ y $b = -0.8248$, donde se puede apreciar un comportamiento estable, es decir, los estados del circuito tienden a un valor constante. La amplitud de las señales con respecto al tiempo se vuelven constantes. En el caso de la variable de estado $x_1(t)$ parte de su valor inicial $x_1(0) = 1.1$ y después tiende al valor constante $x_1(t) = 4.3$, mientras que la variable de estado $x_2(t)$ parte de su valor inicial $x_2(0) = 0.1$ tendiendo después a $x_2(t) = 0$ y la variable de estado $x_3(t)$ parte de su valor inicial $x_3(0) = -0.5$ tendiendo después a $x_2(t) = -4.3$.

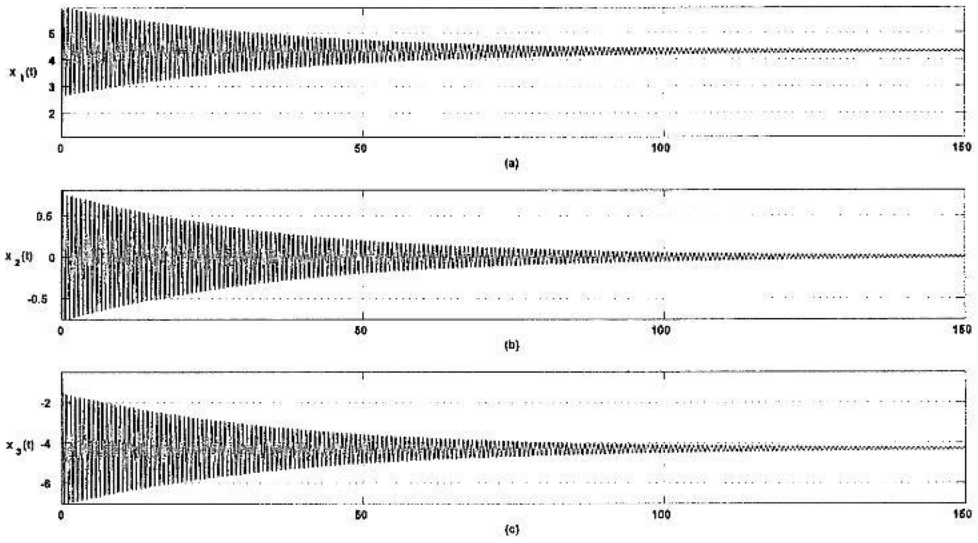

Figura 18: Evolución en el tiempo de los estados del circuito de Chua: a) $x_1(t)$ tiende a 4.3, b) $x_2(t)$ tiende a 0 y c) $x_3(t)$ tiende a -4.3.

El comportamiento dinámico observado anteriormente, también se puede apreciar en el comportamiento de los atractores (proyectados en el espacio de estados), que se muestran en la figura 19, donde estos tienden a un punto fijo.

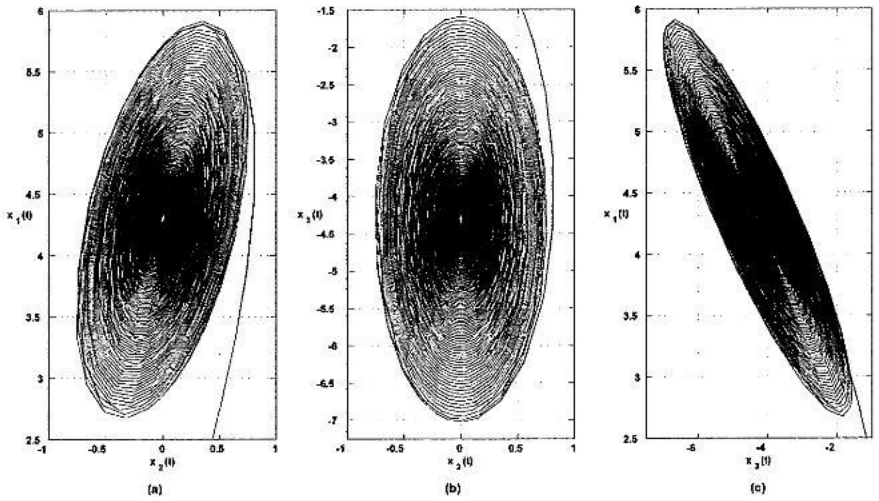

Figura 19: a) Atractor punto $x_1(t)$ vs $x_2(t)$, b) atractor punto $x_3(t)$ vs $x_2(t)$ y c) atractor punto $x_1(t)$ vs $x_3(t)$. Estos resultados se obtuvieron con los siguientes valores para los parámetros: $\alpha = 4.05, \beta = 6, a = -1.758$ y $b = -0.8248$.

En la figura 20 se muestra la evolución en el tiempo de los estados del circuito de Chua con $\alpha = 3.7, \beta = 5.2, a = -1.50309$ y $b = -0.705204$, donde se puede apreciar un comportamiento cíclico en todas las variables de estados $x_1(t)$, $x_2(t)$ y $x_3(t)$.

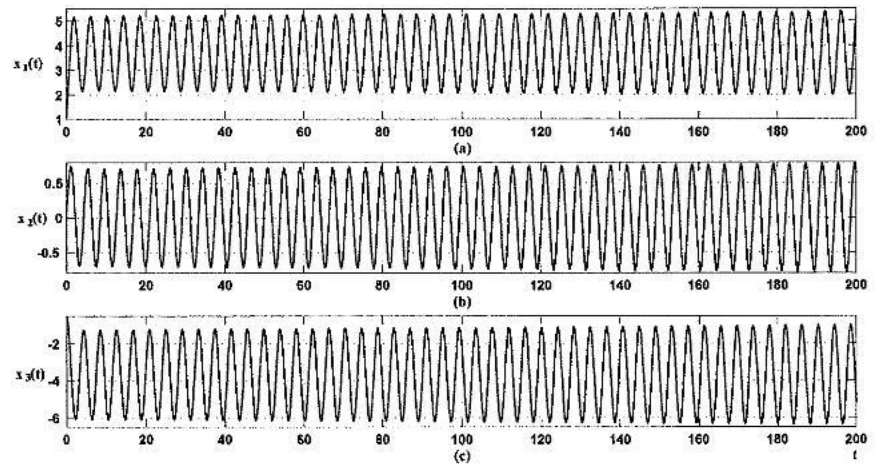

Figura 20: Evolución en el tiempo de los estados: $x_1(t)$, $x_2(t)$ y $x_3(t)$ del circuito de Chua.

Este comportamiento dinámico también se puede apreciar en el comportamiento de los atractores que se muestran en la figura 21, donde estos tienden a un ciclo límite estable.

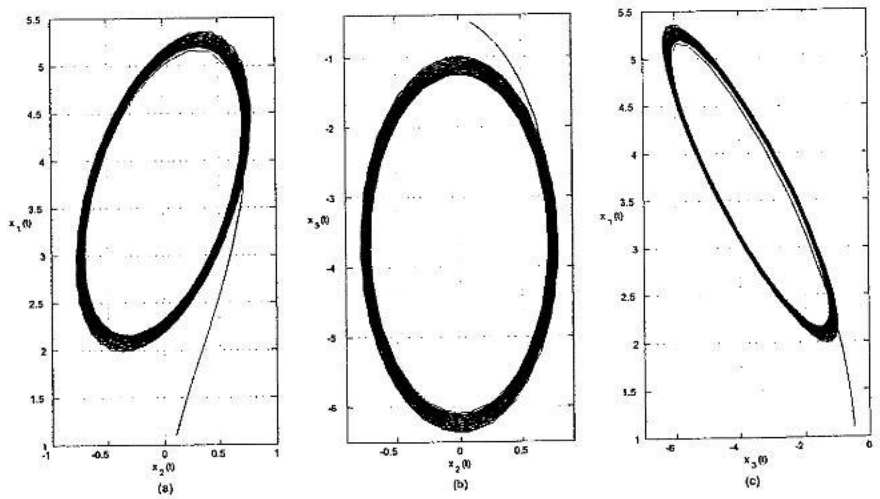

Figura 21: a) Atractor cíclico $x_1(t)$ vs $x_2(t)$, b) atractor cíclico $x_3(t)$ vs $x_2(t)$ y c) atractor cíclico $x_1(t)$ vs $x_3(t)$. Estos resultados se obtuvieron con los siguientes valores para los parámetros: $\alpha = 3.7, \beta = 5.2, a = -1.50309$ y $b = -0.705204$.

En la figura 22 se muestra la evolución en el tiempo de los estados del circuito de Chua con $\alpha = 10, \beta = 19, a = -1.4325$ y $b = -0.7831$, donde se puede apreciar un comportamiento caótico. La amplitud de las señales con respecto al tiempo no exhiben ningún patrón o periodicidad visible. Esto cumple con la primera característica de un sistema caótico.

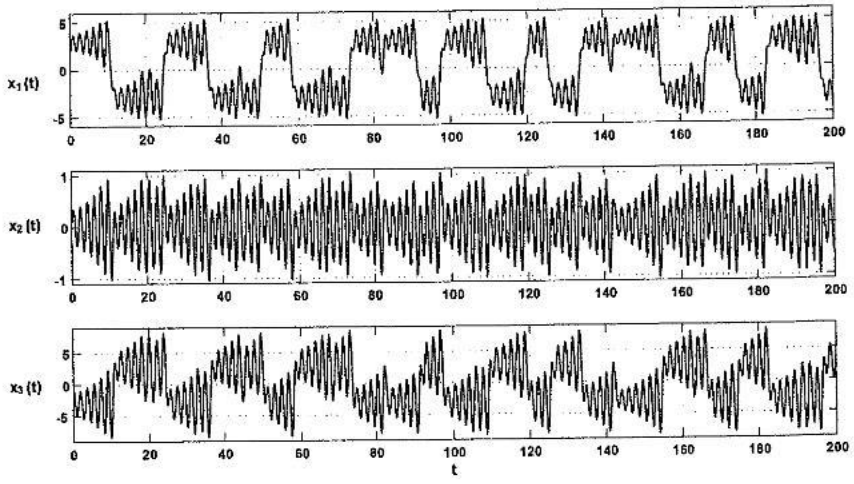

Figura 22: Evolución en el tiempo de los estados $x_1(t), x_2(t)$ y $x_3(t)$ del circuito de Chua.

En la figura 23 se muestran los atractores extraños formados por las trayectorias caóticas de estos estados. Esto cumple con otra característica de un sistema caótico.

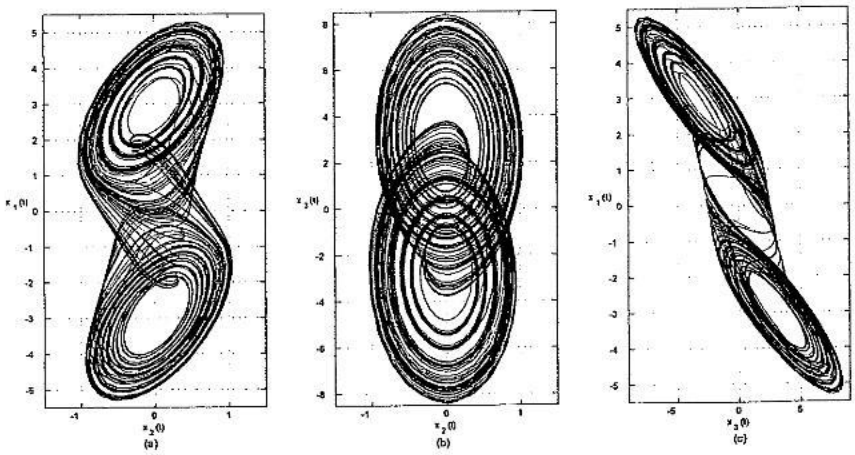

Figura 23: a) Atractor caótico $x_1(t)$ vs $x_2(t)$, b) atractor caótico $x_3(t)$ vs $x_2(t)$ y c) atractor caótico $x_1(t)$ vs $x_3(t)$. Estos resultados se obtuvieron con los siguientes valores para los parámetros: $\alpha = 10, \beta = 19, a = -1.4325$ y $b = -0.7831$.

A continuación se emplearán técnicas de análisis de señales, para determinar el comportamiento dinámico de los estados de un sistema caótico. Una de estas técnicas es la función de **autocorrelación**, la cual arroja como resultado, el parecido de una señal así misma conforme pasa el tiempo, es decir, cuántas componentes periódicas la constituyen. Por lo tanto, la señal que presente la **autocorrelación más pequeña, indicará la que tiene mayor dinámica caótica**.

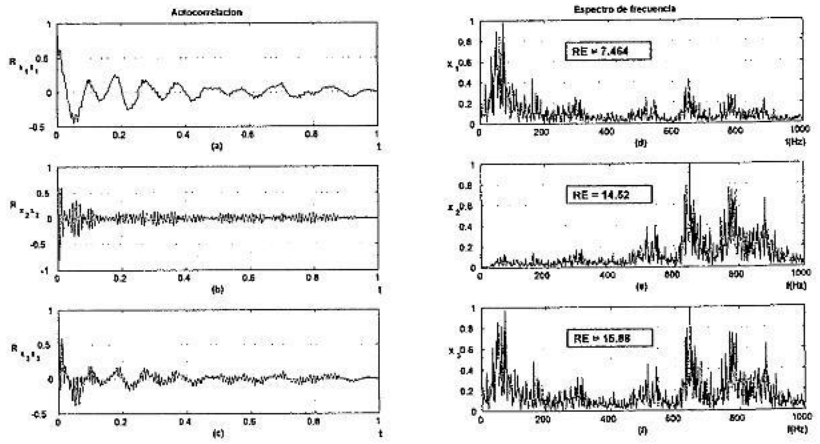

Figura 24: Autocorrelación de las variables de estado del circuito de Chua: a) $x_1(t)$, b) $x_2(t)$ y c) $x_3(t)$. Así como el espectro de frecuencia de: d) $x_1(t)$, e) $x_2(t)$ y f) $x_3(t)$. Para los valores de los parámetros: $\alpha = 10$, $\beta = 19$, $a = -1.4325$ y $b = -0.7831$.

En la figura 24 puede apreciarse que la trayectoria que describe la función de autocorrelación de los estados del circuito de Chua, tiene una envolvente que disminuye rapidamente a cero. Otra manera de analizar la dinámica caótica de las variables de estado del circuito de Chua es en términos de la **frecuencia**, donde una señal caótica presenta espectros con gran cantidad de armónicas excitadas. Los espectros que representan la dinámica caótica del circuito de Chua se muestran en la figura 24, se observa que de los tres estados $x_3(f)$ es el que tiene mayor cantidad de componentes en frecuencia. Una forma de cuantificar la dinámica es mediante el cálculo de la **riqueza espectral**

(Núñez-Pérez 2006), con esto se encuentra que el estado $x_3(t)$ presenta mayor dinámica caótica, con una riqueza espectral de 15.88%. Esto se obtiene mediante la siguiente ecuación:

$$ARE = \frac{\sum fp_{exc}}{\sum fp_{total}} \sum bin_{exc}[bins], \tag{8}$$

donde:

fp_{exc} = picos de frecuencia mayores al umbral,
fp_{total} = número total de picos de frecuencia disponibles según el alcance útil,
bin_{exc} = número de bins excitados por los picos de frecuencia mayores al umbral (i.e.,unidad:bin).

4.4.2 Resultados experimentales

El circuito mostrado en la figura 26, se implementó para obtener resultados experimentales debido a que de este se pueden medir las tres variables de estado $x_1(t)$, $x_2(t)$ y $x_3(t)$ en forma de voltaje, mientras que del circuito de Chua convencional que se mostró en la figura 16 solo se pueden medir las variables estados $x_1(t)$ y $x_2(t)$ en forma de voltaje, ya que la tercer variable de estado $x_3(t)$ es una corriente $i_3(t)$ y no un voltaje.

La figura 25 muestra la pantalla de un osciloscopio, la evolución en el tiempo de los estados del circuito de Chua con los siguientes valores de los parámetros: $\alpha = 4$, $\beta = 6$, $a = -1.75$ y $b = -0.82$, donde se puede apreciar un comportamiento estable. La amplitud de las señales con respecto al tiempo se vuelven constantes. El valor de los parámetros son muy cercanos a los utilizados en las simulaciones numéricas.

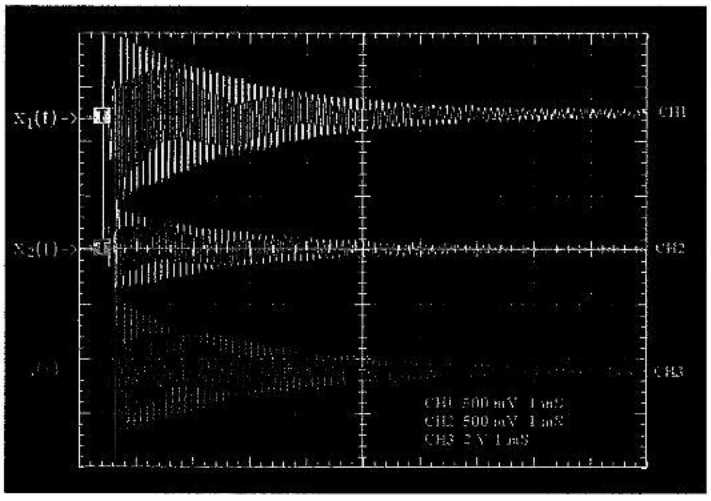

Figura 25: Pantalla de un osciloscopio mostrando la evolución en el tiempo de los estados $x_1(t)$, $x_2(t)$ y $x_3(t)$ del circuito de Chua.

Lo antes dicho también se puede apreciar en el comportamiento de los atractores que se muestran en la figura 27, donde estos tienden a un valor fijo.

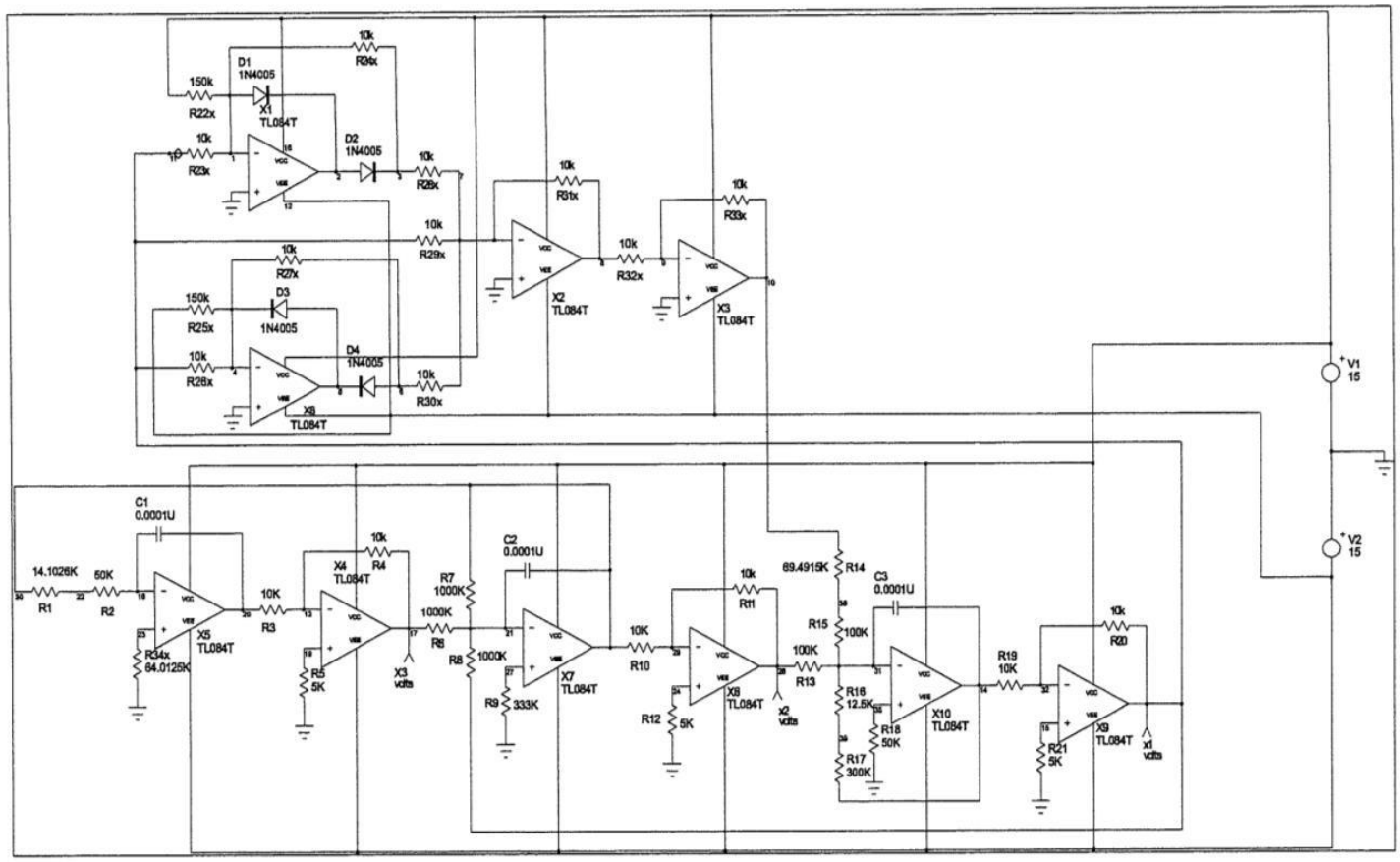

Figura 26: Implementación del circuito de Chua mediante integradores.

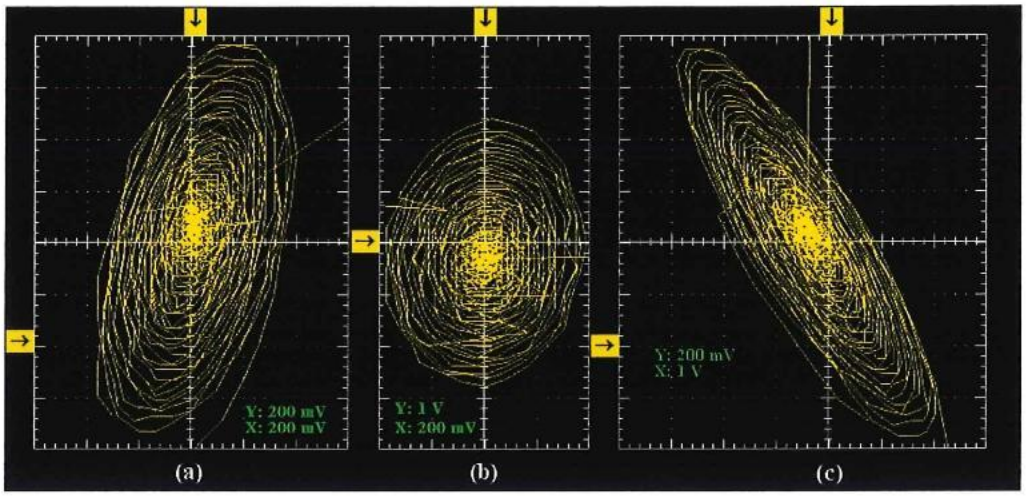

Figura 27: Pantalla de un osciloscopio mostrando: a) Atractor punto $x_1(t)$ vs $x_2(t)$, b) atractor punto $x_3(t)$ vs $x_2(t)$ y c) atractor punto $x_1(t)$ vs $x_3(t)$. Estos resultados se obtuvieron con los siguientes valores de los parametros: $\alpha = 4$, $\beta = 6$, $a = -1.75$ y $b = -0.82$. El valor de los parámetros son muy cercanos a los utilizados en las simulaciones numéricas.

La figura 28 muestra la pantalla de un osciloscopio, la evolución en el tiempo de los estados $x_1(t)$, $x_2(t)$ y $x_3(t)$ del circuito de Chua, con los valores de los parámetros como sigue: $\alpha = 3.7$, $\beta = 5.2$, $a = -1.50$ y $b = -0.70$, donde se puede apreciar un comportamiento cíclico. El valor de los parámetros son muy cercanos a los utilizados en las simulaciones numéricas.

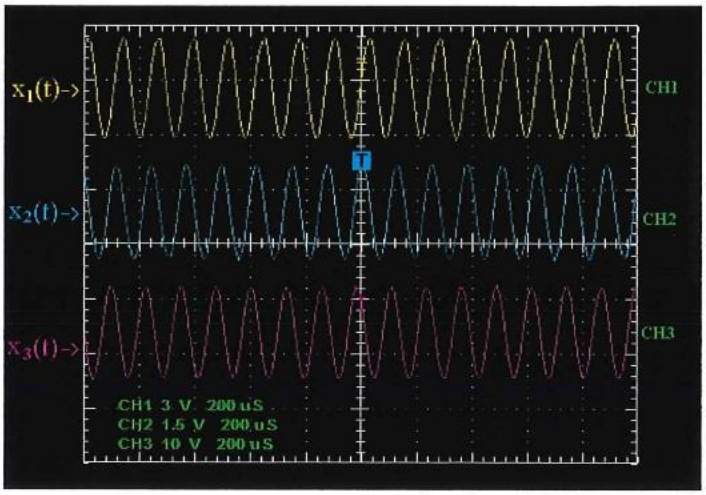

Figura 28: Pantalla de un osciloscopio mostrando la evolución en el tiempo de los estados $x_1(t)$, $x_2(t)$ y $x_3(t)$ del circuito de Chua.

Lo antes dicho también se puede apreciar en el comportamiento de los atractores que se muestran en la figura 29, donde este tiende a un ciclo límite estable.

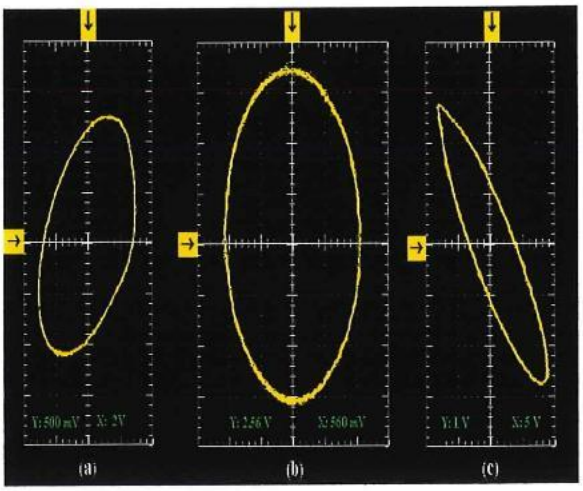

Figura 29: Pantalla de un osciloscopio mostrando: a) Atractor cíclico $x_1(t)$ vs $x_2(t)$, b) atractor cíclico $x_3(t)$ vs $x_2(t)$ y c) atractor cíclico $x_1(t)$ vs $x_3(t)$. Estos resultados se obtuvieron con los valores de los parámetros: $\alpha = 3.7$, $\beta = 5.2$, $a = -1.50$ y $b = -0.70$. El valor de los parámetros son muy cercanos a los utilizados en las simulaciones numéricas.

En la figura 30 se muestra la evolución en el tiempo de los estados $x_1(t)$, $x_2(t)$ y $x_3(t)$ del circuito de Chua, con los siguiente valores de los parámetros: $\alpha = 10, \beta = 19, a = -1.43$ y $b = -0.78$, donde se puede apreciar un comportamiento caótico (estos valores son muy cercanos a los utilizados en las simulaciones numéricas). La amplitud de las señales con respecto al tiempo no exhiben ningún patrón o periodicidad visible. Esto cumple con la primera característica de un sistema caótico.

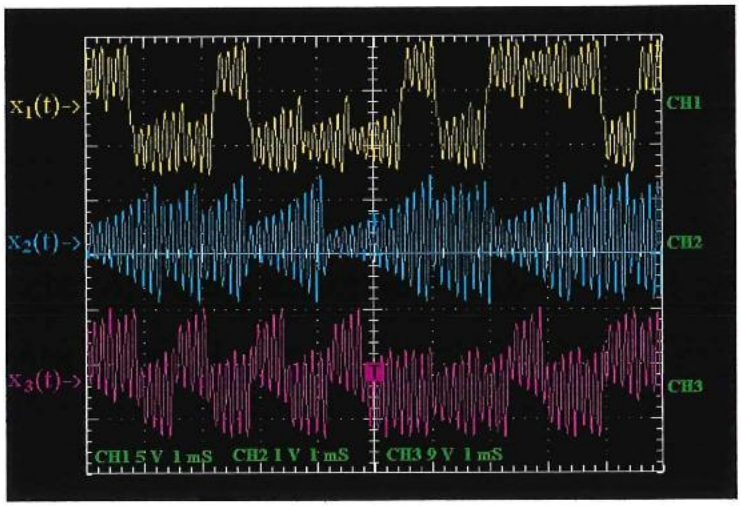

Figura 30: Pantalla de un osciloscopio mostrando la evolución en el tiempo de los estados caóticos $x_1(t)$, $x_2(t)$ y $x_3(t)$ del circuito de Chua.

En la figura 31 se muestran los atractores extraños formados por las trayectorias caóticas de los estos estados. $x_1(t)$, $x_2(t)$ y $x_3(t)$. Esto cumple con la segunda característica de un sistema caótico.

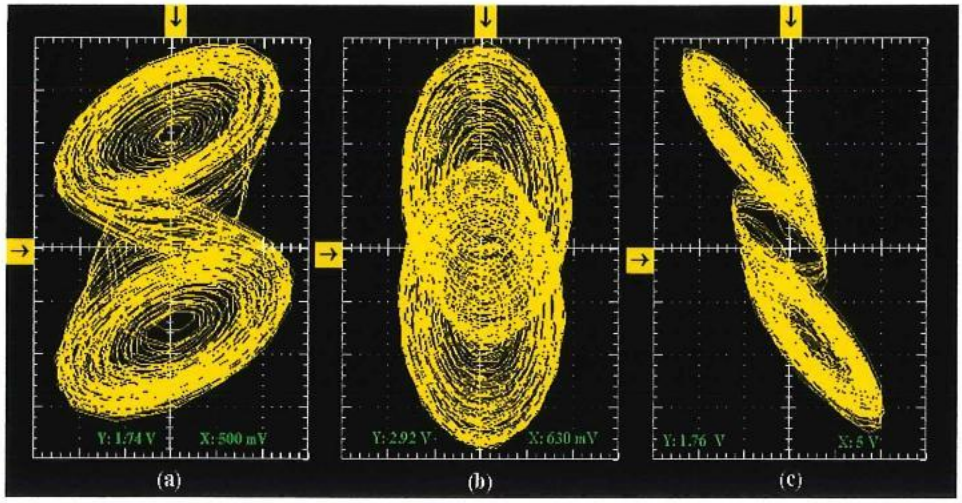

Figura 31: Pantalla de un osciloscopio mostrando: a) Atractor caótico $x_1(t)$ vs $x_2(t)$, b) atractor caótico $x_3(t)$ vs $x_2(t)$ y c) atractor caótico $x_1(t)$ vs $x_3(t)$. Estos resultados se obtuvieron con los valores de los parámetros: $\alpha = 10$, $\beta = -19$, $a = -1.43$ y $b = -0.78$. El valor de los parámetros son muy cercanos a los utilizados en las simulaciones numéricas.

4.5 Conclusiones

Con el propósito de seleccionar el circuito de Chua como el generador de caos, para implementarse en circuitería electrónica y emplearse como encriptador de información, se evaluó su comportamiento dinámico. Calculando así su riqueza espectral y aplicando análisis de autocorrelación a las señales de estado correspondientes. El resultado de esta evaluación, indicó que el circuito de Chua presenta una dinámica compleja en el comportamiento de sus señales caóticas, debido a esto, sencillez del modelo y la similitud obtenida entre los resultados numéricos y experimentales, se eligió para implementarse en simulación numérica y llevar acabo la implementación física mediante circuitería.

5 Sincronización del circuito de Chua

En el presente capítulo se incluye una breve introducción a la sincronía de osciladores. Después, se proporciona la definición de sincronía caótica, también se describen los escenarios de acoplamiento más usuales entre osciladores. Posteriormente, se presentan algunos métodos de sincronización en sistemas caóticos. Luego, se explica el método de sincronización de osciladores caóticos, desde la perspectiva de sistemas hamiltonianos generalizados y el diseño de un observador no lineal sugerido en (Sira-Ramírez y Cruz-Hernández 2000; 2001). A continuación se diseña el sistema esclavo para el circuito de Chua, se reportan los resultados obtenidos tanto de la simulación numérica de la sincronía como de la implementación física mediante circuiteria y finalmente se presentan algunas concluciones.

5.1 Sincronización

5.1.1 Sincronía de osciladores

Se entiende por sicronización como la capacidad de igualar a una misma frencuencia, sistemas osciladores con frecuencias distintas mediante un acoplamiento apropiado. Obtener un comportamiento, tal que, de una conducta de oscilaciones independientes pasa a una conducta común de oscilaciones periódicas, es decir, a oscilaciones de una misma frecuencia. Como resultado de la sincronización, los osciladores modifican sus frecuencias de tal manera, que dichas frecuencias llegan a ser iguales o ralcionadas por un factor racional. De acuerdo a las características de los osciladores considerados, existen diversas explicaciones analíticas de por qué estos osciladores sincronizan.

La sincronización está relacionada de muchas formas con el control. Los dos problemas de sincronizar y controlar movimientos caóticos, tiene raíces comunes en el problema de manejar un sistema no lineal para restringir sus movimientos. En cada caso, se seleccionan los regímenes del parámetro o las fuerzas externas para lograr 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. En la naturaleza se encuentran comportamientos de ritmos biólogicos acoplados, ejemplos de esto son los enjambres de luciérnagas que destellan en sicronía y sincronía de neuronas para procesamiento de información en el cerebro, sincronía de los ritmos cardiacos y respiratorios. Otros ejemplos más 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 manera que la luna siempre muestra la misma cara a la tierra. La sincronía también se puede observar entre sistemas de microondas, la energía de varios dispositivos pueden ser combinados mediante la sincronía, de manera que la energía aumente de forma cuadrática con el número de osciladores.

La capacidad de sincronizar osciladores no lineales, es fundamental para la explicación de muchos procesos en la naturaleza, así pues, la sincronía juega un papel importante en la ciencia. Por ejemplo, en neurociencias, en biología, hasta en el comportamiento colectivos de humanos, numerosas aplicaciones en mecánica, electrónica, comunicaciones privadas/seguras, mediciones y en muchas otras áreas, la sincronía ha demostrado que es extremadamente importante.

5.1.2 Sincronía de sistemas caóticos

El fenómeno caótico se presenta en muchos sistemas tanto naturales como en artificiales. Muchos trabajos de investigación se han enfocado principalmente en el descubrimiento y caracterización del caos. En tiempos recientes, se han propuesto varias ideas y técnicas para usar las propiedades del caos para alcanzar ciertos beneficios. La sincronía de caos se ha utilizado para acoplar circuitos electrónicos, de tal forma de incrementar la potencia en láseres, para controlar oscilaciones en reacciones químicas, para estabilizar el ritmo cardíaco y para seguridad en las comunicaciones mediante la codificación de información. Las aplicaciones del caos en diferentes áreas de la ciencia y tecnología tienen su base en dos problemas, que son el **control del caos** y la **sincronización en sistemas caóticos**.

Se entiende por sincronización caótica cuando dos o más osciladores caóticos están en sincronía, es decir, si finalmente transcurrido el transitorio, las oscilaciones entre los osciladores caóticos coinciden exactamente en todo tiempo, a pesar de iniciar los osciladores bajo condiciones distintas.

La posibilidad de que dos o más sistemas caóticos oscilen de forma coherente y sincronizada no es obvia. Una de las propiedades más importantes asociadas con el caos, es la sensibilidad a las condiciones iniciales. Por tanto, se pudiera concluir que la sincronización de sistemas caóticos no es factible, ya que en sistemas reales no es posible reproducir exactamente condiciones iniciales idénticas. Incluso una desviación infinitesimal en los parámetros o en las condiciones iniciales, eventualmente dará lugar a la divergencia de trayectorias.

Definición 1 (Sincronizació caótica). *Considérese un sistema caótico modelado por la ecuación de estado*

$$\dot{x} = f(x) \tag{9}$$

y otro por

$$\dot{\xi} = f(\xi) \tag{10}$$

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

$$\lim_{t \longrightarrow \infty} \|x(t) - \xi(t)\| \equiv 0. \tag{11}$$

Se define la siguiente diferencia como el **error de sincronía** entre los osciladores (9) y (10)

$$e(t) = x(t) - \xi(t). \tag{12}$$

5.1.3 Escenarios de acoplamiento

El ambiente, comunicación, relación, etc. que se necesita para que dos osciladores (caóticos o no) interactuen y entren en sincronía, se le llama **escenario de acoplamiento**. Los más frecuentes son el escenario de acoplamiento **unidireccional** y el **bidireccional**.

La sincronización con acoplamiento unidireccional, conocida como sincronización maestro y esclavo, se da cuando un sistema A tiene influencia sobre un sistema B, pero no a la inversa, es decir, que el sistema B no tiene influencia sobre el sistema A (ver figura 32). Como su nombre lo indica la información fluye en un solo sentido. En esta forma y como resultado de este acoplamiento, el sistema A (maestro) impone su comportamiento dinámico al sistema B (esclavo).

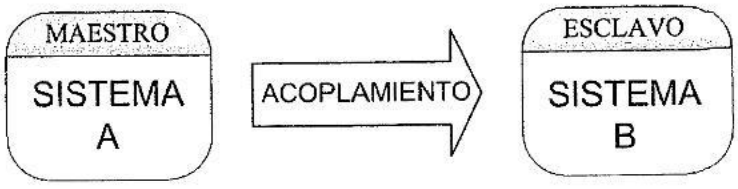

Figura 32: Esquema de acoplamiento unidireccional (maestro y esclavo) para sincronización de osciladores caóticos.

La sincronización con acoplamiento bidireccional, conocida como sincronización mutua, se da cuando un sistema A tiene influencia sobre un sistema B y viceversa, es decir, el sistema B también tiene influencia sobre el sistema A. En este esquema de acomplamiento, la información fluye en ambos sentidos (ver figura 33). Como resultado de este acoplamiento puede dar: a) que las dinámicas de dos osciladores sean iguales a la dinámica del oscilador A o del oscilaor B y b) que las dinámicas de los dos osciladores sean iguales a una tercera dinámica, que no es la del oscilador A ni la del oscilador B.

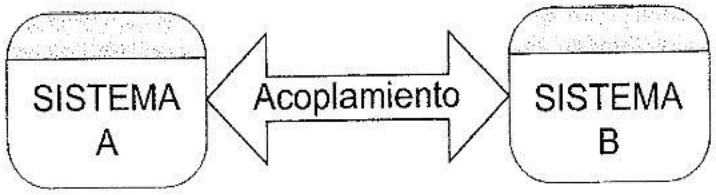

Figura 33: Esquema de acoplamiento bidireccional (mutuo) para sincronización de osciladores caóticos.

5.1.4 Métodos de sincronización de sistemas caóticos

La sicronización unidireccional de sistemas caóticos está compuesta por un sistema caótico (maestro) con un vector de estados compuestos por n elementos y 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 tal forma que, la dinámica del error de sincronía (12) sea cero, por lo menos de manera asintótica. Este error corresponde a la diferencia que existe entre los estados del sistema maestro y los estados del sistema esclavo. De tal manera que no existe una estructura específica para el sistema esclavo.

El diseño de un modelo matemático para el sistema esclavo, fue llevado acabo primeramente por Pecora y Carroll 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 se han desarrollado nuevas propuestas; en algunas de ellas, se han empleado sistemas compensados como Scheweizer y colaboradores en (Scheweizer *et al.* 1995), donde se emplea una especie de observador, mientras que Kapitaniak y colaboladores en (Kapitaniak *et al.* 1994) muestran 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), 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 1998), filtro extendido de Kalman (Cruz y Nijmeijer 2000), últimamente sincronización mediante formas hamiltonianas y observador (Sira-Ramírez y Cruz-Hernández 2000; 2001), por modos deslizantes (López-Mancilla y Cruz-Hernández 2004), por acoplamiento a modelos (Aguilar-Bustos y Cruz-Hernández 2002; 2003; Didier-López y Cruz-Hernández 2005), entre otros.

En este trabajo se ha adoptado la metodología sugerida por (Sira-Ramírez y Cruz-Hernández 2000; 2001) para sincronizar sistemas caóticos. Por tanto, a continuación se explicará con amplitud este método basado en formas hamiltonianas y el diseño de un observador no lineal.

5.2 Formas hamiltonianas y observador

Considere el siguiente sistema autónomo de dimensión n, definido por

$$\dot{x} = f(x), \qquad x \in \mathbb{R}^n \tag{13}$$

el cual representa un sistema que exhibe un comportamiento caótico, donde $x(t) = (x_1(t), ..., x_n(t))^T \in \mathbb{R}^n$ es el vector de estados y f es una función no lineal. A partir de lo establecido en (Sira-Ramírez

y Cruz Hernández 2000; 2001) muchos sistemas físicos descritos por la ecuación de estado (13), pueden ser reescritos en la siguiente *forma canónica hamiltoniana generalizada*,

$$\dot{x} = \Im(x)\frac{\partial H}{\partial x} + S(x)\frac{\partial H}{\partial x} + F(x) \quad x \in \mathbb{R}^n, \tag{14}$$

donde $H(x)$ es una función de energía suave definida positiva globalmente. El vector gradiente de $H(x)$, representado por $\partial H/\partial x$ se considera que existe en cualquier parte. Frecuentemente utilizamos funciones de energía cuadrática de la forma $H(x) = 1/2x^T Mx$, con M siendo una matriz constante, definida positiva y simétrica. Por tal motivo, $\partial H/\partial x = Mx$. Las matrices cuadradas $\Im(x)$ y $S(x)$ mencionadas en la expresión (14), satisfacen para toda $x \in \mathbb{R}^n$, las siguientes propiedades:

$$\Im(x) + \Im^T(x) = 0, \qquad S(x) = S^T(x).$$

El campo vectorial $\Im(x)\partial H/\partial x$ representa la parte **conservativa** del sistema. En lo que respecta al campo vectorial $S(x)\partial H/\partial x$, nos describe la parte **no concervativa** del sistema. En algunos casos, la matriz $S(x)$ es definida negativa o semidefinida negativa. En tales casos, el campo vectorial $S(x)\partial H/\partial x$ representa la parte **disipativa** del sistema. Si por el contario, $S(x)$ es definida positiva, semidefinida positiva o indefinida, este claramente representa la parte desestabilizante del sistema, global, semiglobal o local, respectivamente. En el caso de que $S(x)$ sea definida, ésta se descompone en la suma de una matriz simétrica semidefinida negativa $\Re(x)$ y una matriz simétrica semidefinida positiva $\aleph(x)$. Por último, $F(x)$ representa el campo vectorial **localmente desestabilizante**.

5.2.1 Diseño de un observador no lineal para una clase de osciladores en forma hamiltoniana generalizada

En el contexto de **diseño de observadores**, se considera una clase especial de las formas hamiltonianas con campo vectorial desestabilizante y un mapeo lineal de salida $y(t)$, expresada como sigue

$$\begin{aligned} \dot{x} &= \Im(y)\frac{\partial H}{\partial x} + (I+S)\frac{\partial H}{\partial x} + F(y) \quad x \in \mathbb{R}^n, \\ y &= C\frac{\partial H}{\partial x}, \quad y \in \mathbb{R}^m, \end{aligned} \tag{15}$$

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

Para el diseño de la forma (15), se define el vector estimado de estado $x(t)$ por $\xi(t)$, y se considera la función de energía hamiltoniana $H(\xi)$ como una particularización de H en términos del estado estimado $\xi(t)$. De la misma manera, se indica la salida estimada por $\eta(t)$ calculada en términos de $\xi(t)$. Donde el gradiente $\partial H(\xi)/\partial\xi$ es también de la forma $M\xi$ siendo M una matriz, simétrica constante y definida positiva.

Un observador no lineal para el sistema (15) se obtiene de la siguiente manera

$$\begin{aligned} \dot{\xi} &= \Im(y)\frac{\partial H}{\partial \xi} + (I+S)\frac{\partial H}{\partial \xi} + F(y) + K(y-\eta), \quad \xi \in \mathbb{R}^n, \\ \eta &= C\frac{\partial H}{\partial \xi}, \quad \eta \in \mathbb{R}^m, \end{aligned} \tag{16}$$

donde $K = (k_1, k_2, ..., k_n)^T$ es un vector constante conocido como la **ganancia del observador**. En el contexto de sincronización, el observador (16) **realizará el papel de oscilador esclavo**. Cuya función será estimar (reproducir) las dinámicas completas del sistema maestro (15).

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

$$\begin{aligned} \dot{e} &= \Im(y)\frac{\partial H}{\partial e} + (I + S - KC)\frac{\partial H}{\partial e}, \qquad e \in \mathbb{R}^n, \\ e_y &= C\frac{\partial H}{\partial e}, \qquad e_y \in \mathbb{R}^m \end{aligned} \tag{17}$$

donde $\partial H(e)/\partial e$ con abusos de notación, es el vector gradiente de la función de energía modificada

$$\frac{\partial H(e)}{\partial e} = \frac{\partial H}{\partial x} - \frac{\partial H}{\partial \xi} = M(x - \xi) = Me. \tag{18}$$

Antes de continuar, es conveniente recordar las definiciones básicas de *detectibilidad* y *observabilidad* en sistemas lineales.

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

$$\begin{bmatrix} C \\ sI - A \end{bmatrix} \tag{19}$$

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 (19) es de rango pleno para todos los valores de s en el plano complejo.

Para que el estado $x(t)$ del oscilador no lineal (15) sea global y exponencialmente estimado por el estado $\xi(t)$ del observador no lineal (16), el par de matrices (C, S) debe de ser **observable** o al menos **detectable**, condiciones suficientes reportadas en (Sira-Ramírez y Cruz-Hernández 2000; 2001). En el caso de que resultara que el par de matrices (C, S) es **no observable** o al menos **detectable**, se puede agregar una mariz I a S para de este modo formar una nueva matriz $W = I + S$.

Si el par de matrices (C, W) es *observable* o al menos *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$(W - KC)$ se pueden mover al semiplano izquierdo del plano complejo. La distinción hecha anteriormente, mencionando *valores propios observables*, significa que algunos valores propios de (C, W) pueden ser fijos y no ser influenciados por algún valor de la ganancia del observador. En el caso de un par detectable, aquello *valores propios no observables* tienen una parte real negativa, si el par de matrices (C, W) es *observable*, eso significa que todos los valores propios $W - KC$ pueden ser reubicados en el semiplano izquierdo del plano complejo, con la adecuada selección la matriz K. Por lo tanto, la matriz $(W - KC)^T$ también manifiesta valores propios con parte real negativa.

La matriz $W - KC$ es una matriz cuadrada, con una estructura nada particular. Esta matriz se puede reemplazar por la siguiente suma,

$$W - KC = \left[S - \frac{1}{2}(KC + C^T K^T)\right] + \left[I - \frac{1}{2}(KC - C^T K^T)\right]. \tag{20}$$

Los sumandos de la primer matriz de la ecuación (20), forman una matriz simétrica definida negativa, mientras que los sumandos de la segunda matriz, forman una matriz simétrica.

El sistema dinámico del error puede escribirse como sigue

$$\dot{e} = \left[\Im(y) + I - \frac{1}{2}(KC - C^T K^T)\right]\frac{\partial H}{\partial e} + \left[S - \frac{1}{2}\left(KC + C^T K^T\right)\right]\frac{\partial H}{\partial e}. \tag{21}$$

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

$$H(x) = \frac{1}{2}x^T M x, \tag{22}$$

se encuentra que la derivada en el tiempo de esta función, a lo largo de las trayectorias del sistema dinámico del error (21),

$$\dot{H}(e) = \frac{\partial H(e)}{\partial e^T}\dot{e} = \frac{\partial H(e)}{\partial e^T}\left[S - \frac{1}{2}\left(KC + C^T K^T\right)\right]\frac{\partial H}{\partial e} \leq 0 \tag{23}$$

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

5.2.2 Análisis de estabilidad

Esta parte se dedica al análisis de estabilidad del error de sincronía (18) que existe entre el sistema maestro (15) y el observador no lineal (16), también llamado sistema esclavo.

Teorema 1 [Sira-Ramírez y Cruz Hernández 2001]. *El estado de $x(t)$ del oscilador no lineal (15) puede ser global, asintótica y exponencialemente estimado por el estado $\xi(t)$ de un observador de la forma (16), si y solo si el par de matrices (C, W) ó (C, S) son observables o al menos detectables.*

La observabilidad en cualquiera de los dos pares de matrices (C, W) ó (C, S) es una condición suficiente, mas no necesaria para la reconstrucción asintótica de los estados del sistema maestro (15). Una condición necesaria y suficiente para la 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 sistema (15) puede ser global, exponencial y asintóticamente estimado, por el estado $\xi(t)$ del observafor (16), si y solo si, existe una matriz constante K tal que, la matriz simétrica,*

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

sea definida negativa o semidefinida negativa.

5.3 Sincronización del circuito de Chua mediante formas hamiltonianas y el diseño de un observador

Para realizar las simulaciones numéricas se tomaron en cuenta las ecuaciones normalizadas del circuito de Chua (6) y (7), esto para facilitar dichas simulaciones:

$$\begin{aligned}
\dot{x}_1 &= \alpha\{x_2 - x_1 - f(x_1)\}, \\
\dot{x}_2 &= x_1 - x_2 + x_3, \\
\dot{x}_3 &= -\beta x_2
\end{aligned}$$

ahora $f(x_1)$ es la función no lineal y es definida por

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

Tomando como función de energía Hamiltoniana a

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

De este modo el vector gradiente es

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

El circuito de Chua (6) y (7) se puede reescribir en la forma canónica hamiltoniana, con un vector desestabiliazante como sigue:

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & \beta \\ 0 & -\beta & 0 \end{bmatrix} \frac{\partial H}{\partial x} + \begin{bmatrix} -\alpha^2 & \alpha & 0 \\ \alpha & -1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \frac{\partial H}{\partial x} + \begin{bmatrix} -\alpha f(x_1) \\ 0 \\ 0 \end{bmatrix}. \tag{25}$$

La señal de salida ha ser transmitida por el circiuto de Chua maestro (25) como señal de acoplamiento es el estado $y(t) = x_1(t)$. Mientras que las matrices C, S y I están dadas por

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

Entonces el observador construido para el circuito de Chua maestro (25) queda dado por la expresión

$$\begin{bmatrix} \dot{\xi}_1 \\ \dot{\xi}_2 \\ \dot{\xi}_3 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & \beta \\ 0 & -\beta & 0 \end{bmatrix} \frac{\partial H}{\partial \xi} + \begin{bmatrix} -\alpha^2 & \alpha & 0 \\ \alpha & -1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \frac{\partial H}{\partial \xi} + \begin{bmatrix} -\alpha f(x_1) \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} k_1 \\ k_2 \\ k_3 \end{bmatrix} (x_1 - \xi_1). \tag{26}$$

donde k_1, k_2 y k_3 se eligen de forma apropiada, para garantizar con mayor rapidez la estabilidad exponencial asintótica a cero de la trayectoria del error en la reconstrucción de los estados del circuito de Chua maestro (25).

A partir del teorema 2, condición (24) se encontrarán los valores de k_1, k_2 y k_3, para los cuales se garantiza estabilidad asintótica a cero del error de sincronía

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

Al sustituir S, K y C en (24) nombraremos la matriz simétrica resultante A

$$A = \begin{bmatrix} -2\alpha^2 - 2k_1\alpha & 2\alpha - k_2\alpha & -k_3\alpha \\ 2\alpha - k_2\alpha & -2 & 0 \\ -k_3\alpha & 0 & 0 \end{bmatrix}.$$

Por lo tanto, los valores de k_1, k_2 y k_3 deben estar dentro de los rangos establecidos a continuación (27), para los cuales cumplen que la matriz A es semidefinida negativa, es decir, que satisfagan las desigualdades:

$$\begin{aligned} k_1 &> -\alpha, \\ k_2(1 - \frac{1}{4}k_2) &< -\frac{k_1}{\alpha}, \\ k_3 &= 0. \end{aligned} \tag{27}$$

5.3.1 Resultados numéricos

En esta parte del documento, se muestran los resultados numéricos obtenidos en la sincronización de los circuitos maestro y esclavo, en los cuales, se utilizaron los siguientes valores de los parámetros:

$$\alpha = 10, \ \beta = 19, \ a = -1.4325 \text{ y } b = -0.7831$$

y condiciones iniciales

$$\begin{aligned} x(0) &= (1, 0.1, -0.5), \\ \xi(0) &= (0, 1, -0.1). \end{aligned}$$

Tomando en cuenta tres casos para los valores de ganacia del sistema observador no lineal (esclavo), donde en la primera columna de la figura 34 se muestra la trayectoria del error con respecto al tiempo para las ganancias de $k_1 = 1$, $k_2 = 5$ y $k_3 = 0$, mientras que la segunda columna muestra el error resultante para las ganancias de $k_1 = 3$, $k_2 = 6$ y $k_3 = 0$ y en la tercera y última columna se ve el error obtenido para las ganancias $k_1 = 5$, $k_2 = 8$ y $k_3 = 0$. De la figura 34 puede observarse que la columna 3, $e(t)$ más rapidamente llega a cero (i.e. se obtiene sincronía), esto corresponde para la selección de $k_1 = 5$, $k_2 = 8$, y $k_3 = 0$. Notese que para todos estos casos, las selecciones de k_1, k_2 y k_3 satisfacen las condiciones (27).

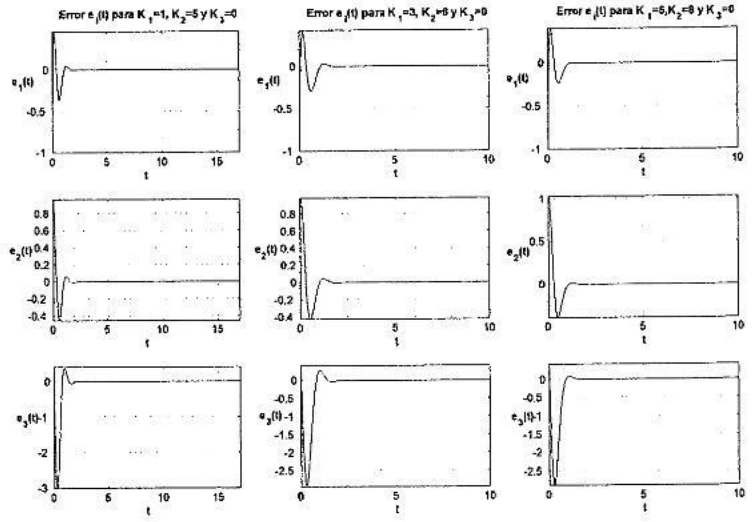

Figura 34: Trayectorias del error de sincronía $e_i(t)$, $i = 1, 2, 3$ para diferentes ganancias del sistema esclavo.

En al figura 35 se muestran las simulaciones de las trayectorias correspondientes tanto de los estados del circuito de Chua maestro como los del circuito de Chua esclavo (observador).

En la figura 36 se muestran los atractores caóticos tanto del circuito de Chua maestro como los del circuito de Chua esclavo.

En la figura 37 se ilustra el comportamiento en el tiempo de las trayectorias del error de sincronía del circuito de Chua maestro y circuito de Chua esclavo.

Por último, en la figura 38 se observa la sincronía en el espacio de estado del circuito de Chua maestro y esclavo.

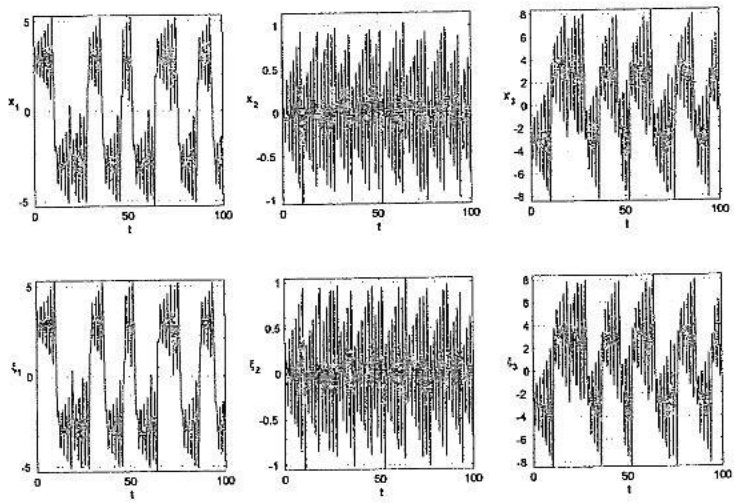

Figura 35: Evolución de las variables de estados en el tiempo tanto del circuito de Chua maestro $\{x_1(t), x_2(t), x_3(t)\}$ como del esclavo $\{\xi_1(t), \xi_2(t), \xi_3(t)\}$.

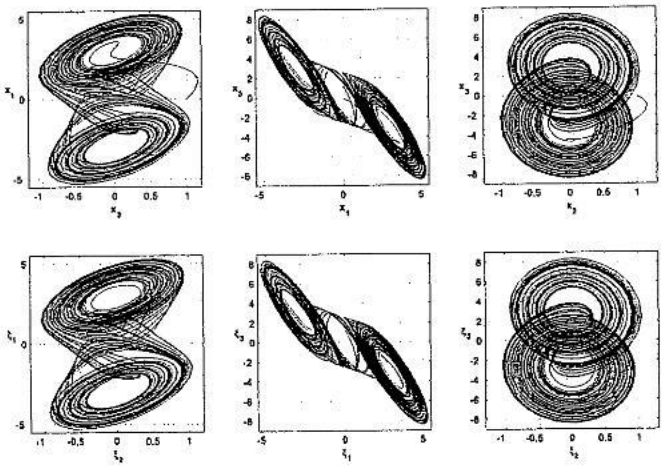

Figura 36: Planos de fase caóticos del circuito de Chua maestro $x_i(t)$ y atractores del esclavo $\xi_i(t)$, para $i = 1, 2, 3$.

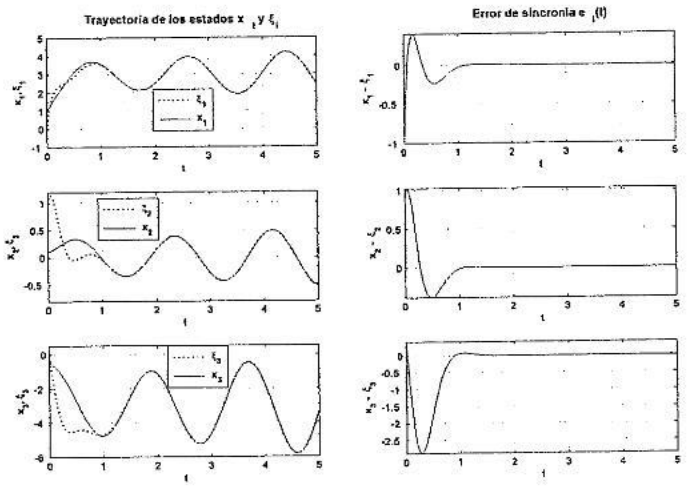

Figura 37: Trayectorias de los estados $x_i(t)$ y $\xi_i(t)$ y el error de sincronía $e_i(t) = x_i(t) - \xi_i(t)$ para $i = 1, 2, 3$.

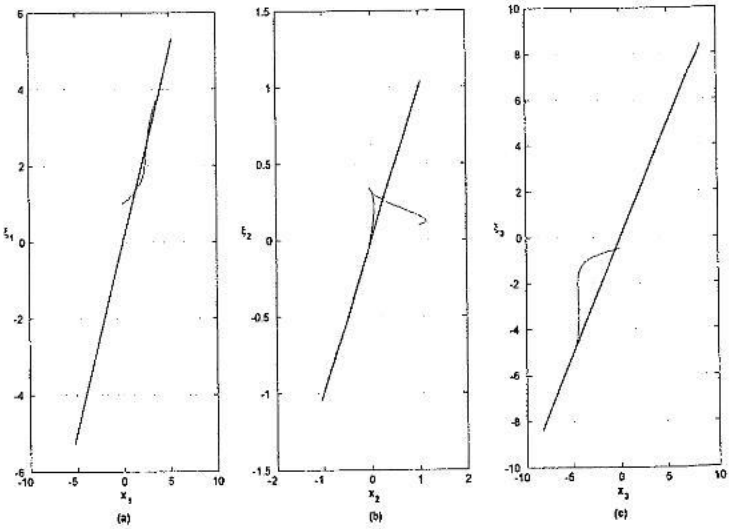

Figura 38: Sincronía entre el circuito maestro y esclavo en el espacio de estado mostrado en plano de fase: (a) x_1 vs ξ_1, (b) x_2 vs ξ_2 y (c) x_3 vs ξ_3.

5.3.2 Resultados experimentales

En esta parte del documento, se muestran resultados experimentales obtenidos en la sincronización de los circuitos maestro (ver figura 42) y esclavo (ver figura 43), en los cuales, se utilizaron valores en los parámetros muy similares a los utilizados en la simulación numérica:

$$\alpha = 10,\ \beta = 19,\ a = -1.43 \text{ y } b = -0.78.$$

Para lograr la sincronía entre el circuito de Chua maestro y esclavo se tomaron los siguientes valores de la ganancia del observador (ver figura 44):

$$k_1 = 5,\ k_2 = 8,\ k_3 = 0.$$

A continuación, se muestran los resultados experimentales de las trayectorias correspondientes tanto del circuito de Chua maestro como las del circuito de Chua esclavo (observador).

La figura 39 muestra la trayectorias del estado $x_1(t)$ del circuito de Chua maestro y la trayectoria del estado $\xi_1(t)$ del circuito de Chua esclavo, mientras que en la figura 40 muestra la trayectoria del estado $x_2(t)$ del maestro y la trayectoria del estado $\xi_2(t)$ del esclavo.

Por último, en la figura 41 se observa la sincronía en el espacio de estado del circuito de Chua maestro y esclavo.

5.4 Conclusiones

Se sincronizó el circuito de Chua en configuración maestro y esclavo, recurriendo a la metodología presentada en (Sira-Ramírez y Cruz Hernández 2000; 2001). Con este método se dividió el circuito de Chua en 3 partes: una concervativa, otra disipativa y por último en un vector desestabilizante. De igual forma, con este método se obtuvo que la señal de salida (acoplante) para lograr la sincronización resultó ser $x_1(t)$. Los resultados tanto numéricos como experimentales obtenidos muestran la efectividad del esclavo diseñado mediante este método, ya que dichos resultados son muy similares entre si. Se observo que este metódo tiene como gran ventaja la aceleración de la sincronización mediante la variación de la ganancia K del observador, es decir, mediante la variación de la ganancia se puede reducir el tiempo de sincronización. Por lo tanto, los resultados obtenidos en la sincronización entre el maestro y el esclavo serán utilizados para la comunicación entre estos.

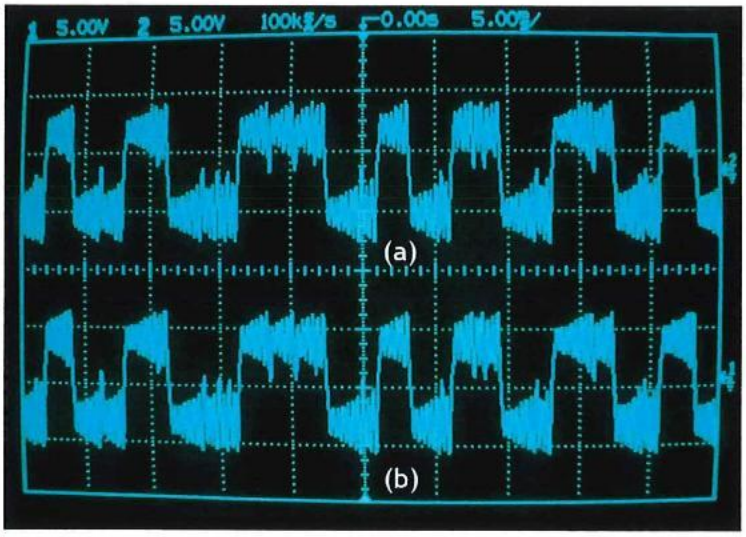

Figura 39: Pantalla de un osciloscopio mostrando la evolución en el tiempo de los estados: (a) $x_1(t)$ del circuito de Chua maestro y (b) $\xi_1(t)$ del circuito de Chua esclavo.

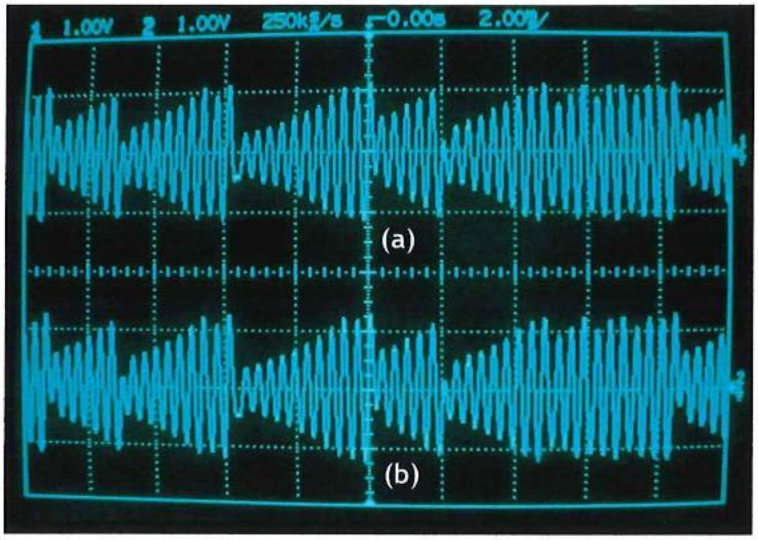

Figura 40: Pantalla de un osciloscopio mostrando la evolución en el tiempo de los estados: (a) $x_2(t)$ del circuito de Chua maestro y (b) $\xi_2(t)$ del circuito de Chua esclavo.

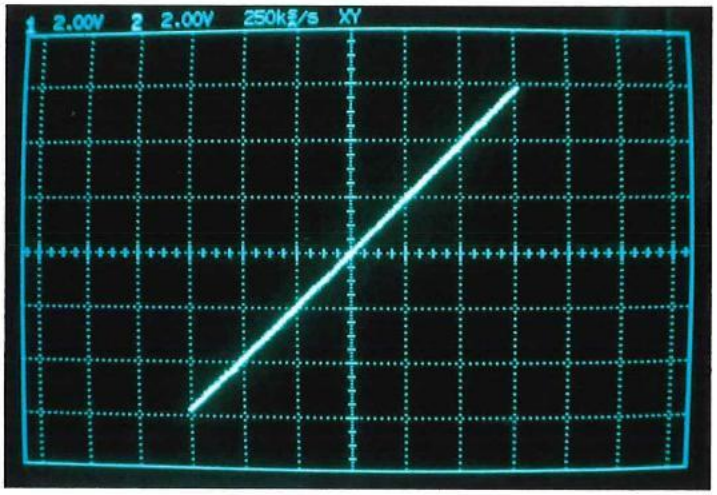

Figura 41: Pantalla de un osciloscopio mostrando la sincronía entre el circuito maestro y esclavo en el espacio de estado $x_1(t)$ vs $\xi_1(t)$, con $x_1(t)$ para el eje horizontal y $\xi_1(t)$ para el eje vertical.

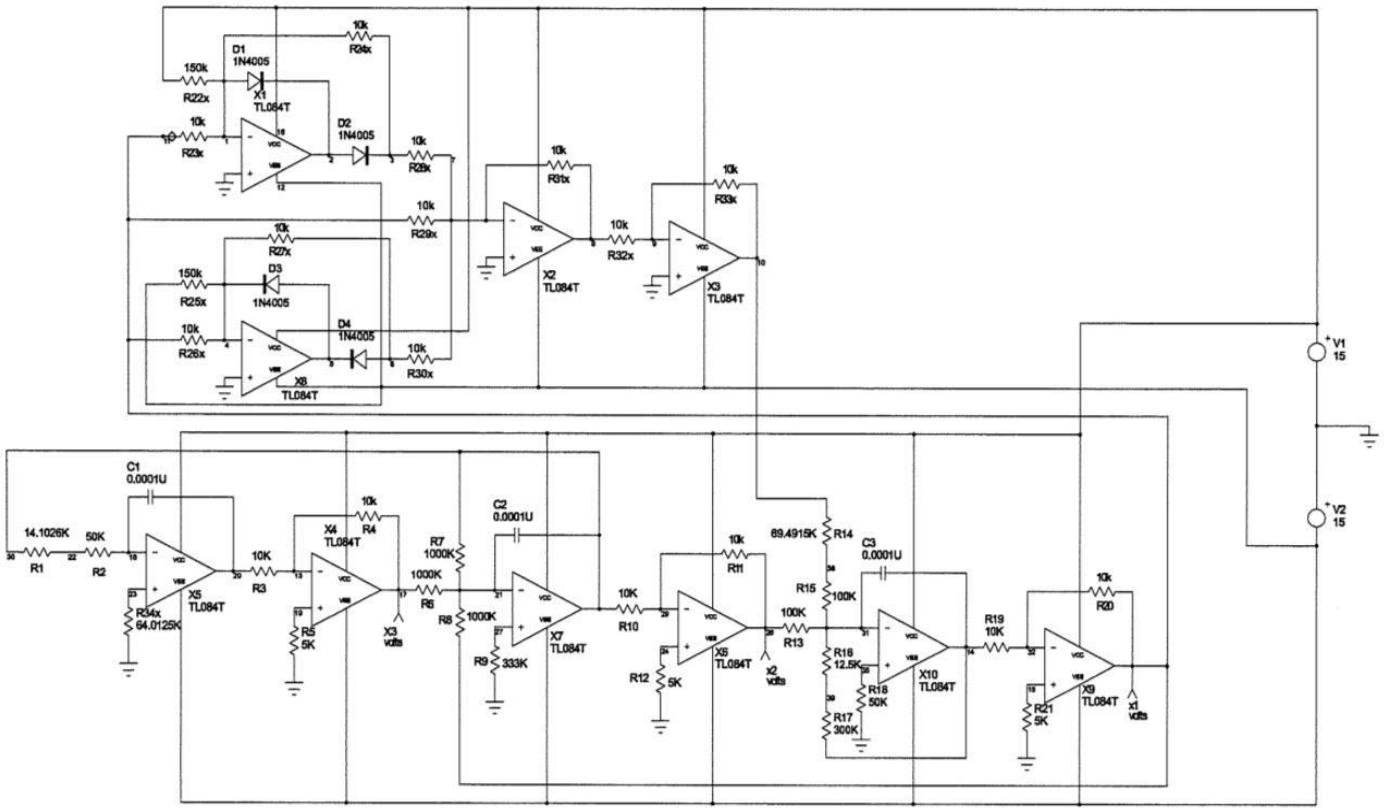

Figura 42: Implementación del circuito de Chua maestro mediante integradores.

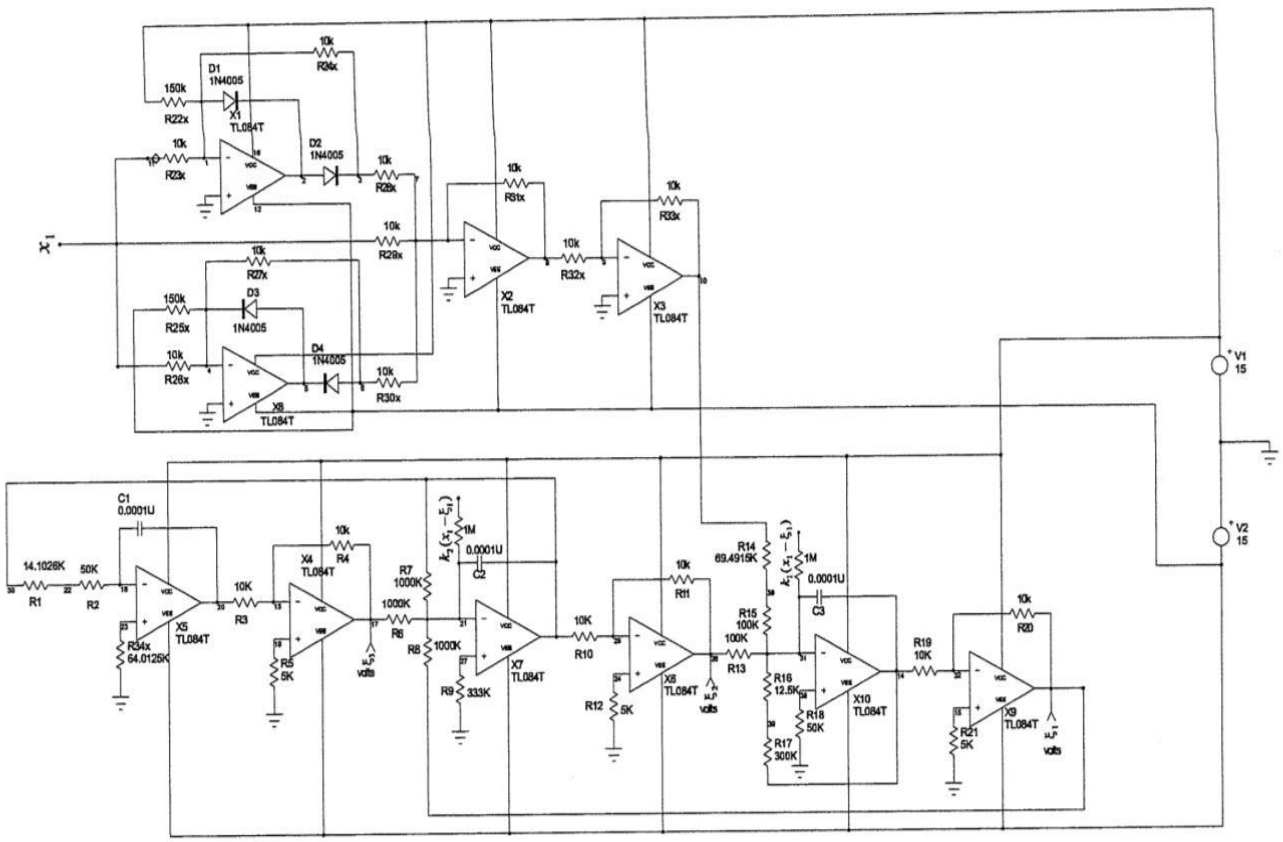

Figura 43: Implementación del circuito de Chua esclavo mediante integradores.

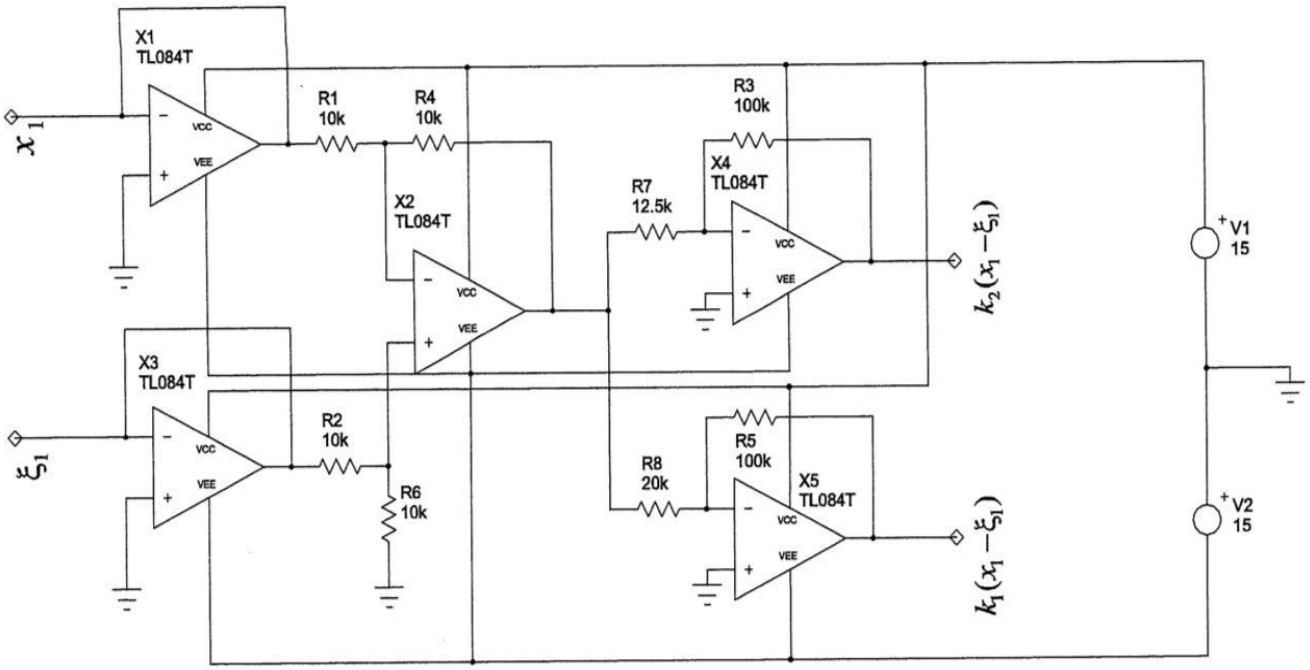

Figura 44: Implementación del vector de ganancia.

6 Sincronización entre múltiples maestros y esclavos

El material contenido en los capítulos previos, se ha limitado a la sincronización numérica y experimental entre dos osciladores caóticos ahora en este capítulo se presentan resultados numéricos de la sincronización de N maestros con N esclavos a través de un canal inseguro, utilizando el esquema de sincronización por retroalimentación propuesta en (Milanović & Zaghloul, 1996) en combinación con el método de sincronización de osciladores caóticos mediante sistemas hamiltonianos generalizados y el diseño de un observador no lineal propuesto en (Sira-Ramírez y Cruz-Hernández, 2000; 2001). Estos resultados constituyen una de las aportaciones de este trabajo de tesis.

6.1 Sincronización

La sincronización de N sistemas maestros con N sistemas esclavos a través de un canal se efectua mediante un acoplamiento unidireccional, también conocido como **acoplamiento maestro y esclavo.** El objetivo anterior se puede lograr mediante el esquema de sincronización por retroalimentación sugerido en (Milanović &Zaghloul, 1996b) en combinación con el método de sincronización de osciladores caóticos mediante sistemas hamiltonianos generalizados y el diseño de un observador no lineal propuesto en (Sira-Ramírez y Cruz-Hernández, 2000; 2001).

En la figura 45 se muestra el diagrama a bloques del conjunto de N de *sistemas maestros,* el cual cuenta con una señal $s(t)$, resultante de la suma de $y_i(t)$ señales de salida de los M_i maestros, donde $i = 1, 2, ..., N$ circuitos de Chua. Esto último se muestra como sigue

$$s(t) = y_1(t) + y_2(t) + ... + y_N(t). \tag{28}$$

Esta señal resultante (28) será la **señal de acoplamiento** que se envía hacia el *conjunto de N esclavos,* ubicado remotamente, mediante un canal público inseguro. Al mismo tiempo, se retroalimenta al conjunto de sistemas maestros, mediante el circuito de Chua_{0T}. Esto es necesario para llevar acabo la sincronización y lograr un acoplamiento unidireccional maestro y esclavo. Al igual que el conjunto de N sistemas maestros, el conjunto de sistemas esclavos (ver figura 46) cuenta con $\eta_i(t)$ señales de salida de los E_i esclavos, donde $i = 1, 2, ..., N$. Las señales de salida $y_i(t)$ del conjunto de maestros se utilizarán para ocultar la información de u_i usuarios en el transmisor de la red, respectivamente, mientras que las señales de salida $\eta_i(t)$ de los esclavos se utilizarán para recuperar la información de u_i usuarios en el receptor de la red de dichos sistemas esclavos. Lo antes dicho se verá en el siguiente capítulo.

6.1.1 Conjunto de N sistemas maestros

Conjunto de ecuaciones de estado para el generador de caos del sistema maestro en forma hamiltoniana generalizada, está dado por:

Circuito de Chua cero del maestro (Chua_{0T})

$$\begin{aligned} \dot{x}_0 &= \Im(\frac{s}{N})\frac{\partial H}{\partial x} + (I+S)\frac{\partial H}{\partial x} + f(\frac{s}{N}) + K(\frac{s}{N} - y_0), \quad x_0 \in \mathbb{R}^n, \\ y_0 &= C\frac{\partial H}{\partial x}, \quad y_0 \in \mathbb{R}^m. \end{aligned}$$

Maestro 1

$$\begin{aligned} \dot{x}_1 &= \Im(y_0)\frac{\partial H}{\partial x} + (I+S)\frac{\partial H}{\partial x} + f(y_0) + K(y_0 - y_1), \quad x_1 \in \mathbb{R}^n, \\ y_1 &= C\frac{\partial H}{\partial x}, \quad y_1 \in \mathbb{R}^m. \end{aligned} \tag{29}$$

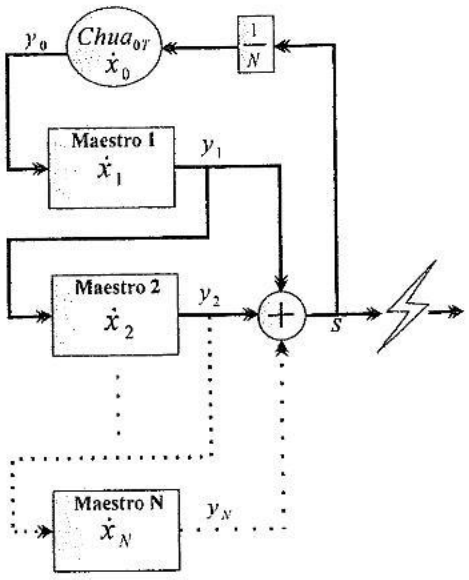

Figura 45: Diagrama a bloques del conjunto de N maestros para sincronización entre múltiples maestros y esclavos, utilizando $N + 1$ circuitos de Chua: Uno para Chua_{0T}, utilizado para la retroalimentación de la señal s y N para los N usuarios en el transmisor de la red.

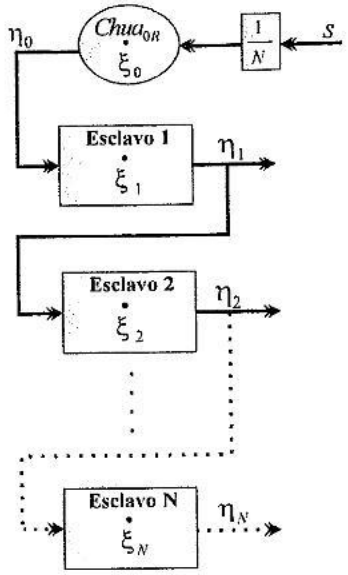

Figura 46: Diagrama a bloques del conjunto de N esclavos para sincronización entre múltiples maestros y esclavos, utilizando $N + 1$ circuitos de Chua: Uno para Chua_{0R}, utilizado para ingresar primero a la señal s y N para los N usuarios en el receptor de la red.

Maestro 2

$$\begin{aligned}\dot{x}_2 &= \Im(y_1)\frac{\partial H}{\partial x} + (I+S)\frac{\partial H}{\partial x} + f(y_1) + K(y_1 - y_2), \quad x_2 \in \mathbb{R}^n, \\ y_2 &= C\frac{\partial H}{\partial x}, \quad y_2 \in \mathbb{R}^m.\end{aligned}$$

Maestro N

$$\begin{aligned}\dot{x}_N &= \Im(y_{N-1})\frac{\partial H}{\partial x} + (I+S)\frac{\partial H}{\partial x} + f(y_{N-1}) + K(y_{N-1} - y_N), \quad x_N \in \mathbb{R}^n, \\ y_N &= C\frac{\partial H}{\partial x}, \quad y_N \in \mathbb{R}^m.\end{aligned}$$

6.1.2 Conjunto de N sistemas esclavos

El conjunto de N sistemas caóticos esclavos tiene la misma forma que la del conjunto de N sistemas maestros, y es dirigido por la señal de entrada $s(t)$ proveniente de dicho conjunto de N sistemas maestros a través del canal público inseguro. Esto se muestra en el siguiente conjuto de ecuaciónes de estado en forma hamiltoniana generalizada:

Circuito de Chua cero del esclavo (Chua_{0R})

$$\begin{aligned}\dot{\xi}_0 &= \Im(\frac{s}{N})\frac{\partial H}{\partial \xi} + (I+S)\frac{\partial H}{\partial \xi} + f(\frac{s}{N}) + K(\frac{s}{N} - \eta_0), \quad \xi_0 \in R^n, \\ \eta_0 &= C\frac{\partial H}{\partial \xi}, \quad \eta_0 \in \mathbb{R}^m.\end{aligned}$$

Esclavo 1

$$\begin{aligned}\dot{\xi}_1 &= \Im(\eta_0)\frac{\partial H}{\partial \xi} + (I+S)\frac{\partial H}{\partial \xi} + f(\eta_0) + K(\eta_0 - \eta_1), \quad \xi_1 \in R^n, \\ \eta_1 &= C\frac{\partial H}{\partial \xi}, \quad \eta_1 \in \mathbb{R}^m.\end{aligned} \tag{30}$$

Esclavo 2

$$\begin{aligned}\dot{\xi}_2 &= \Im(\eta_1)\frac{\partial H}{\partial \xi} + (I+S)\frac{\partial H}{\partial \xi} + f(\eta_1) + K(\eta_1 - \eta_2), \quad \xi_2 \in R^n, \\ \eta_2 &= C\frac{\partial H}{\partial \xi}, \quad \eta_2 \in \mathbb{R}^m.\end{aligned}$$

Esclavo N

$$\begin{aligned}\dot{\xi}_N &= \Im(\eta_{N-1})\frac{\partial H}{\partial \xi} + (I+S)\frac{\partial H}{\partial \xi} + f(\eta_{N-1}) + K(\eta_{N-1} - \eta_N), \quad \xi_N \in R^n, \\ \eta_N &= C\frac{\partial H}{\partial \xi}, \quad \eta_N \in \mathbb{R}^m.\end{aligned}$$

6.2 Resultados numéricos

Por simplicidad y con propósitos ilustrativos, se consideran solo dos ($N = 2$) maestros y dos esclavos formando la red de osciladores caóticos por sincronizar. En los siguientes resultados numéricos, para lo cual se utilizan las ecuaciones normalizadas del circuito de Chua, es decir, se utiliza al circuito de Chua como generador de caos. Mientras que la sincronización se realiza aplicando el método retroalimentación en combinación con el método de sincronización de osciladores caóticos mediante sistemas hamiltonianos generalizados y el diseño de un observador no lineal. De acuerdo al capítulo 5 el valor de la ganancia K del observador es como sigue

$$K = (5, 8, 0)^T.$$

A continuación, se presentan las ecuaciones normalizadas tanto del conjunto de 2 sistemas maestros como las del conjunto de 2 sistemas esclavos que se utilizarán en las simulaciones.

6.2.1 Ecuaciones normalizadas del conjunto de 2 sistemas maestros

Circuito de Chua cero del maestro (Chua_{0T})

$$\begin{aligned} \dot{x}_{1_0} &= -\alpha_0 x_{1_0} + \alpha_0 x_{2_0} - \alpha_0 f(s) + k_1(s - x_{1_0}), \\ \dot{x}_{2_0} &= x_{3_0} + x_{1_0} - x_{2_0} + k_2(s - x_{1_0}), \\ \dot{x}_{3_0} &= -\beta_0 x_{2_0} + k_3(s - x_{1_0}), \\ f(s) &= bs + \frac{1}{2}(a - b)(|s + 1| - |s - 1|), \qquad a, b < 0. \end{aligned} \tag{31}$$

Maestro 1

$$\begin{aligned} \dot{x}_{1_1} &= -\alpha_1 x_{1_1} + \alpha_1 x_{2_1} - \alpha_1 f(x_{1_0}) + k_1(x_{1_0} - x_{1_1}), \\ \dot{x}_{2_1} &= x_{3_1} + x_{1_1} - x_{2_1} + k_2(x_{1_0} - x_{1_1}), \\ \dot{x}_{3_1} &= -\beta_1 x_{2_1} + k_3(x_{1_0} - x_{1_1}), \\ f(x_{1_0}) &= bx_{1_1} + \frac{1}{2}(a - b)(|x_{1_0} + 1| - |x_{1_0} - 1|), \qquad a, b < 0. \end{aligned} \tag{32}$$

Maestro 2

$$\begin{aligned} \dot{x}_{1_2} &= -\alpha_2 x_{1_2} + \alpha_2 x_{2_2} - \alpha_2 f(x_{1_1}) + k_1(x_{1_1} - x_{1_2}), \\ \dot{x}_{2_2} &= x_{3_2} + x_{1_2} - x_{2_2} + k_2(x_{1_1} - x_{1_2}), \\ \dot{x}_{3_2} &= -\beta_2 x_{2_2} + k_3(x_{1_1} - x_{1_2}), \\ f(x_{1_1}) &= bx_{1_2} + \frac{1}{2}(a - b)(|x_{1_1} + 1| - |x_{1_1} - 1|), \qquad a, b < 0. \end{aligned} \tag{33}$$

Donde el valor de $a = -1.4325$ y $b = -0.7831$ se asignan para todos los circuitos de Chua del sistema maestro. Condiciones inciales para los estados de Chua_{0T}: $x_{1_0}(0) = 1$, $x_{2_0}(0) = -0.01$, $x_{3_0}(0) = -1$, donde $\beta_0 = 19$ y $\alpha_0 = 10$. Mientras que los del **maestro 1**: $x_{1_1}(0) = -1$, $x_{2_1}(0) = -1$, $x_{3_1}(0) = 0.1$, $\beta_1 = 17$ y $\alpha_1 = 9$. Y para los del **maestro 2**: $x_{1_2}(0) = -0.01$, $x_{2_2}(0) = 1$, $x_{3_2}(0) = 1$, $\beta_2 = 15$ y $\alpha_2 = 8$.

En la figura 47, se muestra la evolución en el tiempo del comportamiento de los estados tanto del circuito de Chua Chua_{0T} como los circuitos de Chua maestro 1 y maestro 2 del sistema maestro.

Mientras que en la figura 48, se muestra los atractores caóticos tanto del circuito de Chua Chua_{0T} como los circuitos de Chua maestro 1 y maestro 2 del sistema maestro.

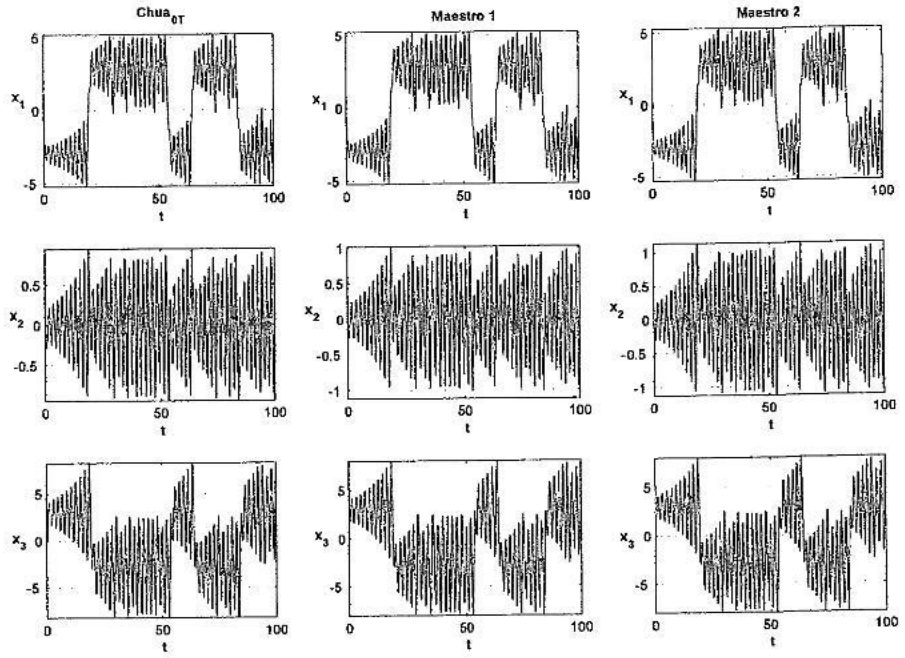

Figura 47: Evolución en el tiempo de los estados caóticos $x_1(t)$, $x_2(t)$, $x_3(t)$ en el tiempo de los circuitos de Chua Chua$_{0T}$, maestro 1 y maestro 2 del conjunto de sistemas maestros.

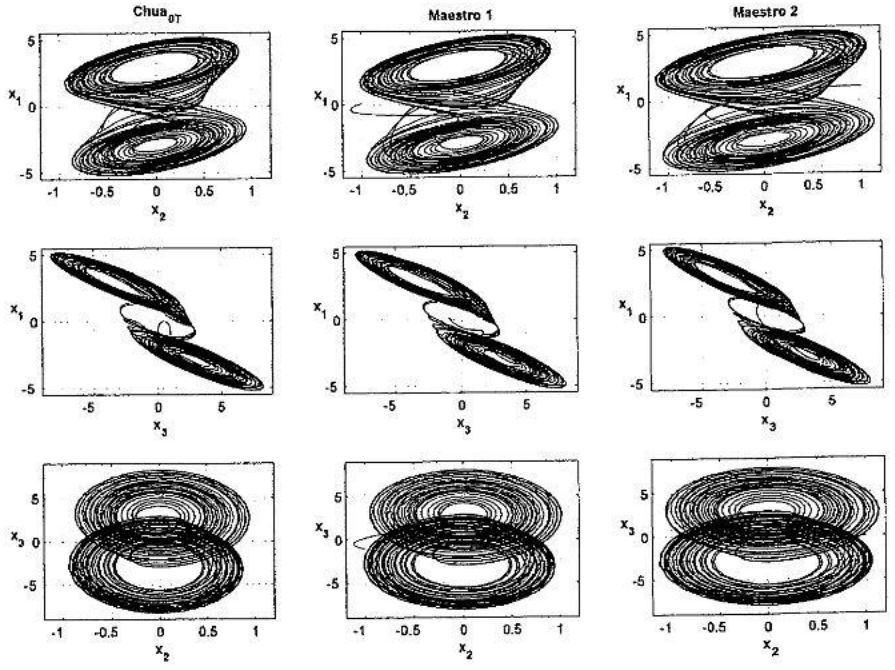

Figura 48: Atractores caóticos del circuito de Chua Chua$_{0T}$, maestro 1 y maestro 2 del conjunto de sistemas maestros.

6.2.2 Ecuaciones normalizadas del conjunto de 2 sistemas esclavos

Circuito de Chua cero del esclavo (Chua_{0R})

$$\begin{aligned}
\dot{\xi}_{1_0} &= -\alpha_0\xi_{1_0} + \alpha_0\xi_{2_0} - \alpha_0 f(s) + k_1(s - \xi_{1_0}),\\
\dot{\xi}_{2_0} &= \xi_{3_0} + \xi_{1_0} - \xi_{2_0} + k_2(s - \xi_{1_0}),\\
\dot{\xi}_{3_0} &= -\beta_0\xi_{2_0} + k_3(s - \xi_{1_0}),\\
f(s) &= bs + \frac{1}{2}(a-b)(|s+1| - |s-1|), \qquad a, b < 0.
\end{aligned} \tag{34}$$

Esclavo 1

$$\begin{aligned}
\dot{\xi}_{1_1} &= -\alpha_1\xi_{1_1} + \alpha_1\xi_{2_1} - \alpha_1 f(\xi_{1_0}) + k_1(\xi_{1_0} - \xi_{1_1}),\\
\dot{\xi}_{2_1} &= \xi_{3_1} + \xi_{1_1} - \xi_{2_1} + k_2(\xi_{1_0} - \xi_{1_1}),\\
\dot{\xi}_{3_1} &= -\beta_1\xi_{2_1} + k_3(\xi_{1_0} - \xi_{1_1}),\\
f(\xi_{1_0}) &= b\xi_{1_0} + \frac{1}{2}(a-b)(|\xi_{1_0} + 1| - |\xi_{1_0} - 1|), \qquad a, b < 0.
\end{aligned} \tag{35}$$

Esclavo 2

$$\begin{aligned}
\dot{\xi}_{1_2} &= -\alpha_2\xi_{1_2} + \alpha_2\xi_{2_2} - \alpha_2 f(\xi_{1_1}) + k_1(\xi_{1_1} - \xi_{1_2}),\\
\dot{\xi}_{2_2} &= \xi_{3_2} + \xi_{1_2} - \xi_{2_2} + k_2(\xi_{1_1} - \xi_{1_2}),\\
\dot{\xi}_{3_2} &= -\beta_2\xi_{2_2} + k_3(\xi_{1_1} - \xi_{1_2}),\\
f(\xi_{1_1}) &= b\xi_{1_1} + \frac{1}{2}(a-b)(|\xi_{1_1} + 1| - |\xi_{1_1} - 1|), \qquad a, b < 0.
\end{aligned} \tag{36}$$

Donde el valor de $a = -1.4325$ y $b = -0.7831$ se asigna para todos los circuitos de Chua del sistema esclavo. Condiciones iniciales para los estados de **Chua_{0R}:** $\xi_{1_0}(0) = 0.01$, $\xi_{2_0}(0) = -1$, $\xi_{3_0}(0) = 0$, donde $\beta_0 = 19$ y $\alpha_0 = 10$. Mientras que para el **esclavo 1:** $\xi_{1_1}(0) = 0$, $\xi_{2_1}(0) = 1$, $\xi_{3_1}(0) = -0.1$, $\beta_1 = 17$ y $\alpha_1 = 9$. Y para el **esclavo 2:** $\xi_{1_2}(0) = 0$, $\xi_{2_2}(0) = 1$, $\xi_{3_2}(0) = -0.1$, $\beta_2 = 15$ y $\alpha_2 = 8$.

En la figura 49, se muestra la evolución en el tiempo del comportamiento de los estados tanto del circuito de Chua Chua_{0R} como los circuitos de Chua esclavo 1 y esclavo 2 del conjunto de sistemas esclavos.

Mientras que en la figura 50, se muestra los atractores caóticos tanto del circuito de Chua Chua_{0R} como los circuitos de Chua esclavo 1 y esclavo 2 del conjunto de sistemas esclavos.

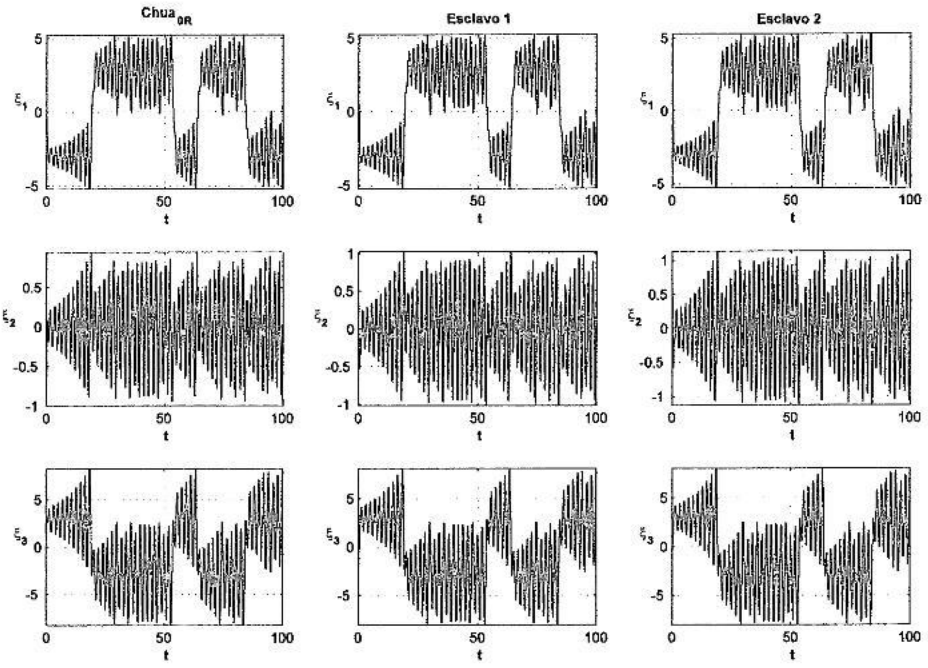

Figura 49: Evolución en el tiempo de los estados caóticos $\xi_1(t)$, $\xi_2(t)$, $\xi_3(t)$ de los circuitos de Chua $\text{Chua}_{0\text{R}}$, esclavo 1 y esclavo 2 del conjunto de sistemas esclavos.

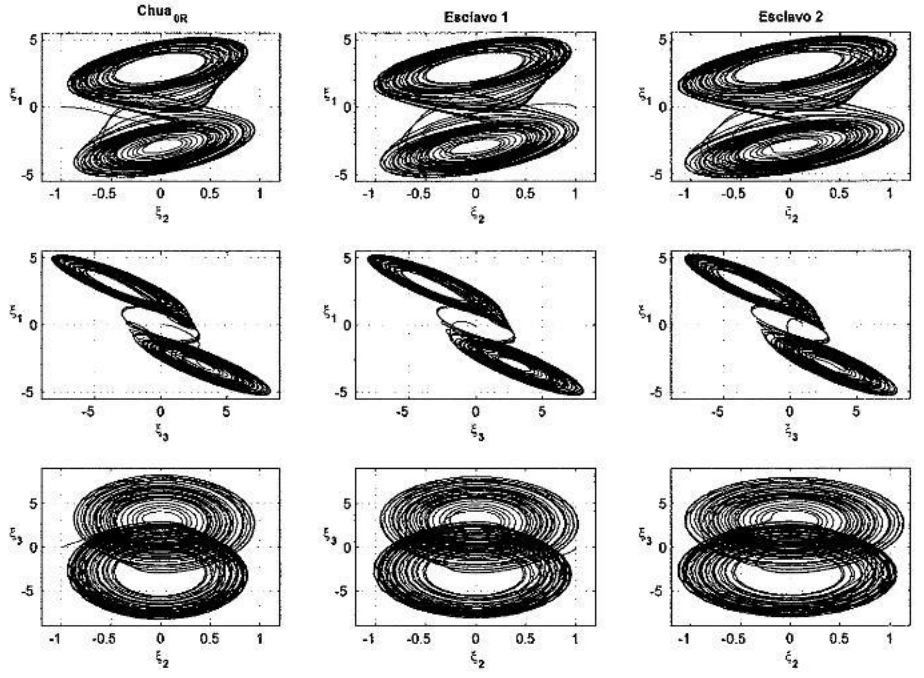

Figura 50: Atractores caóticos del circuito de Chua $\text{Chua}_{0\text{R}}$, esclavo 1 y esclavo 2 del conjunto de sistemas esclavos.

6.2.3 Sincronización

En la figura 51, se muestra el plano de fase de sincronía en el espacio de estado entre el circuito de Chua maestro 1 y el circuito de Chua esclavo 1.

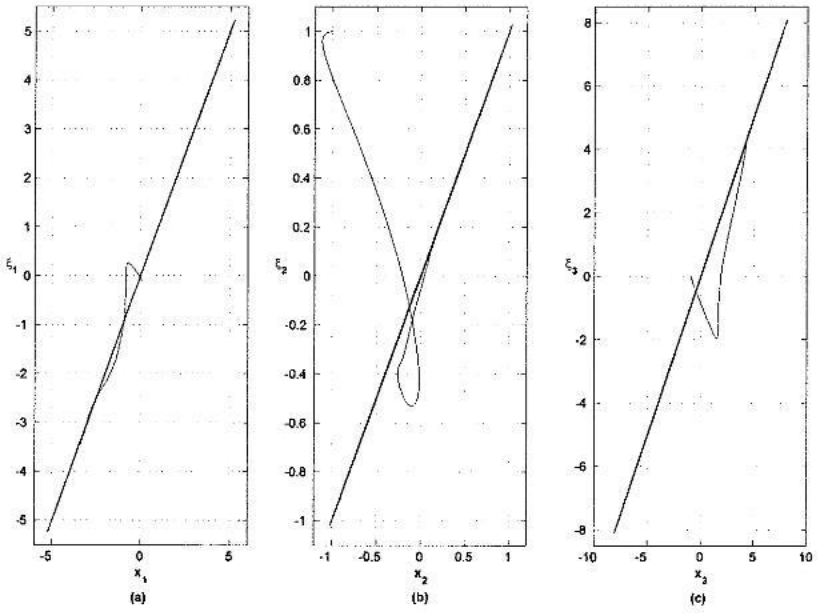

Figura 51: Plano de fase de la sincronía entre el circuito de Chua maestro 1 y el circuito de Chua esclavo 1 en el espacio de estado: (a) x_1 vs ξ_1, (b) x_2 vs ξ_2 y (c) x_3 vs ξ_3.

En la figura 52 se ilustra el comportamiento en el tiempo de las trayectorias del error de sincronía entre el circuito de Chua maestro 1 y el circuito de Chua esclavo 1.

Mientras que en la figura 53, se muestra el plano de fase de sincronía en el espacio de estado entre el cicuito de Chua maestro 2 y el circuito de Chua esclavo 2.

En la figura 54 se ilustra el comportamiento en el tiempo de las trayectorias del error de sincronía entre el circuito de Chua maestro 2 y el circuito de Chua esclavo 2, donde se puede apreciar que el error de sincronía es muy pequeño, pero nunca totalmente cero. Aun así la recuperación del mensaje puede llevarse acabo, tal y como se demostrará a en el siguiente capítulo.

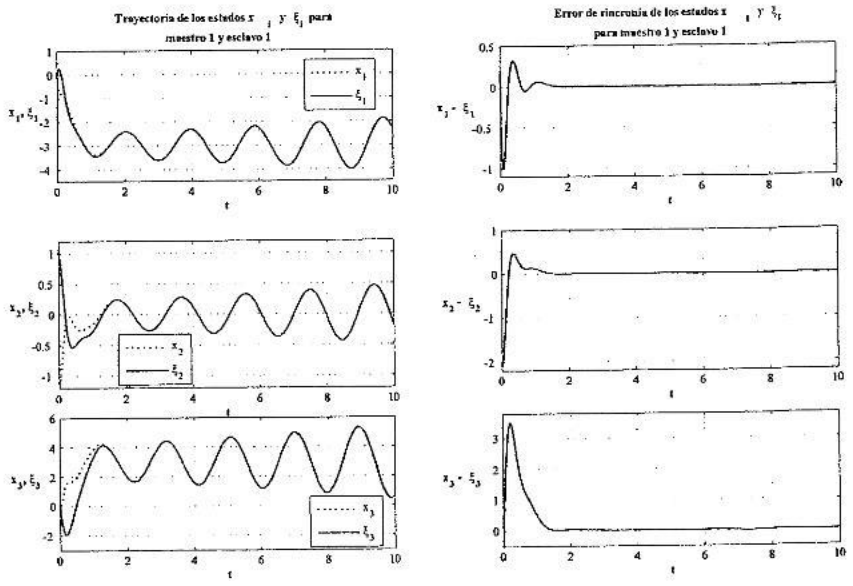

Figura 52: Trayectoria de los estados $x_i(t)$ y $\xi_i(t)$ y el error de sincronía $e_i(t) = x_i(t) - \xi_i(t)$ para el maestro 1 y esclavo 1, donde $i = 1, 2, 3$.

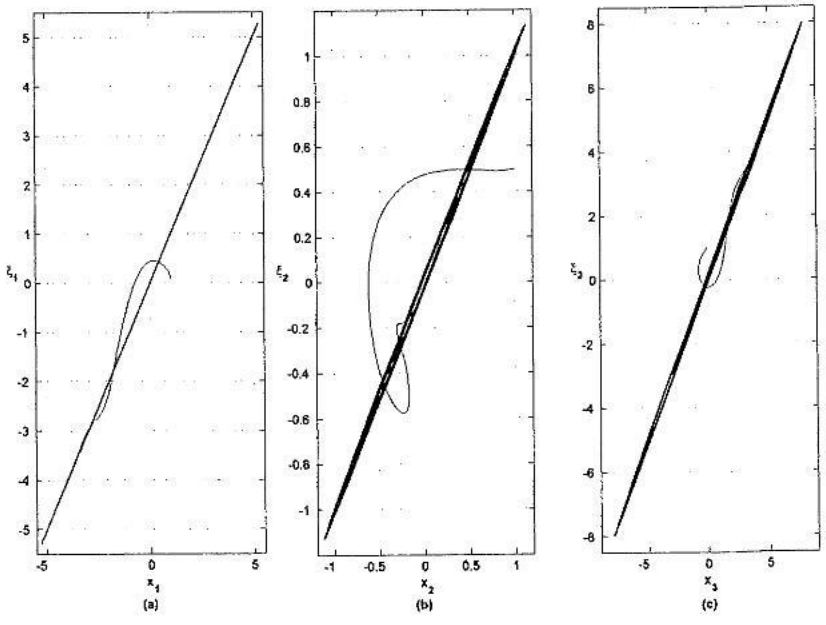

Figura 53: Plano de fase de la sincronía entre el circuito de Chua maestro 2 y el circuito de Chua esclavo 2 en el espacio de estado: (a) x_1 vs ξ_1, (b) x_2 vs ξ_2 y (c) x_3 vs ξ_3.

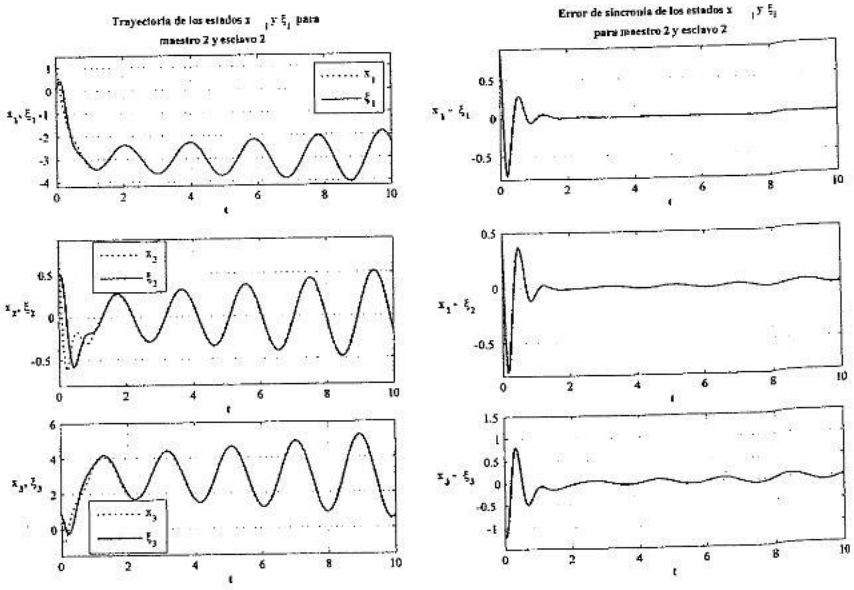

Figura 54: Trayectoria de los estados $x_i(t)$ y $\xi_i(t)$ y el error de sincronía $e_i(t) = x_i(t) - \xi_i(t)$ para el maestro 2 y esclavo 2, donde $i = 1, 2, 3$.

6.3 Conclusiones

Un esquema para la sincronización entre dos conjuntos de N maestros y N esclavos fue propuesto en este capítulo. A manera de ilustración, se presentó una red con dos maestros y dos esclavos. Se mostró que para ambos, utilizando el esquema de sincronización por retroalimentación en combinación con el método de sincronización de osciladores caóticos mediante sistemas hamiltonianos generalizados y el diseño de un observador no lineal, es posible llevar acabo la sincronización de 2 maestros con 2 esclavos con muy buenos resultados.

7 Comunicación caótica

En este capítulo se presentan resultados numéricos y experimentales de la comunicación secreta de información entre un transmisor y un receptor acoplados de forma unidireccional mediante un canal público inseguro con el método de sincronización de osciladores caóticos mediante sistemas hamiltonianos generalizados y el diseño de un observador no lineal propuesto en (Sira-Ramírez y Cruz-Hernández 2000; 2001) reportados en la literatura. Además, la simulación numérica se realiza para una red de N usuarios, en la cual la comunicación secreta de información se lleva acabo a través de un solo canal público inseguro, el acoplamiento unidireccional en dicha red, como ya se mencionó en el capítulo anterior, se realiza mediante el esquema de sincronización por retroalimentación propuesta en (Milanović y Zaghloul, 1996) en combinación con el método de sincronización de osciladores caóticos mediante sistemas hamiltonianos generalizados y el diseño de un observador no lineal propuesto en (Sira-Ramírez y Cruz-Hernández 2000; 2001).

7.1 Comunicación caótica entre un transmisor y receptor

La transmisión de información binaria privada entre un circuito transmisor (25) y un circuito receptor (26) se llevará acabo mediante la técnica de **conmutación entre 2 atractores caóticos** propuesta en (Cruz-Hernández *et al.* 2004). Un esquema general de dicha técnica se muestra en la figura 55. Esta consiste en seleccionar uno o más parámetros del circuito transmisor y alternarlos entre dos valores distintos, por ejemplo p y p', tomando la precaución de que dicho circuito se mantenga oscilando de forma caótica todo el tiempo. Esto conlleva al circuito transmisor a conmutar entre dos atractores caóticos distintos. El circuito del receptor se mantiene fijo, ya que el valor del parámetro para este es siempre p. Esto provoca que en un intervalo de tiempo t el circuito transmisor y receptor estén sincronizados mediante la señal acoplante $x_1(t)$, cuando ambos tengan el mismo valor del parámetro p. Mientras que en otro intervalo de tiempo t, el circuito transmisor y receptor estarán fuera de sincronía, ya que el parámetro del transmisor tendrá como valor p', mientras que el parámetro del circuito receptor mantendra su valor p. Aplicando lo antes dicho de manera partícular al circuito de Chua transmisor, el parametro a variar en este es β, es decir, variará entre un valor β y un valor β', mientras que el circuito de Chua receptor se mantendra en un valor β. La regla que se siguió para llevar acabo dicha conmutación fue la siguiente:

$$\beta(t) = \beta(t) + r \cdot m(t) \tag{37}$$

r es una constante y $m(t)$ es el mensaje binario que se desea transmitir. Por lo tanto, en un tiempo determiado $m(t) = 1$, entonces el parámetro tendrá un valor de β', pero cuando $m(t) = 0$, el parámetro tendrá un valor de β.

Los procesos de sincronización y no sincronización se interpretan por el circuito de Chua receptor, por ejemplo, como un "0" o "1" respectivamente. Esta interpretación se lleva a cabo mediante la evaluación del error de sincronía entre el circuito de Chua transmisor y receptor, definido por

$$e(t) = x_1(t) - \xi_1(t).$$

Cuando $e(t) \neq 0$, el bit recuperado para $\hat{m}(t)$ es un "1", mientras que cuando $e(t) = 0$, el bit recuperado para $\hat{m}(t)$ es un "0".

7.1.1 Resultados numéricos

Se utiliza el circuito de Chua transmisor (25) el cual tiene un comportamiento caótico sincronizado con base en formas hamiltonianas con el circuito de Chua receptor (26), en el escenario de acoplamiento unidireccional maestro y esclavo. Donde la señal de acoplamiento resulta ser $x_1(t)$ de acuerdo con el análisis de estabilidad realizado anteriormente. El esquema para estos circuitos se muestra en la figura 55.

En los siguientes resultados la conmutación de los atractores se obtuvo al variar el parámetro β en el circuito Chua transmisor, con valores de $\beta' = 17.85$ al cual le corresponde la transmisión

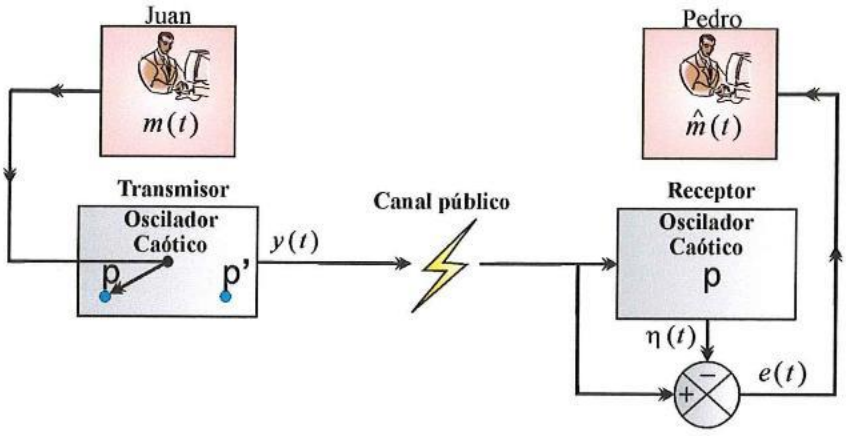

Figura 55: Configuración de comunicación privada entre dos destinos por conmutación entre diferentes atractores caóticos.

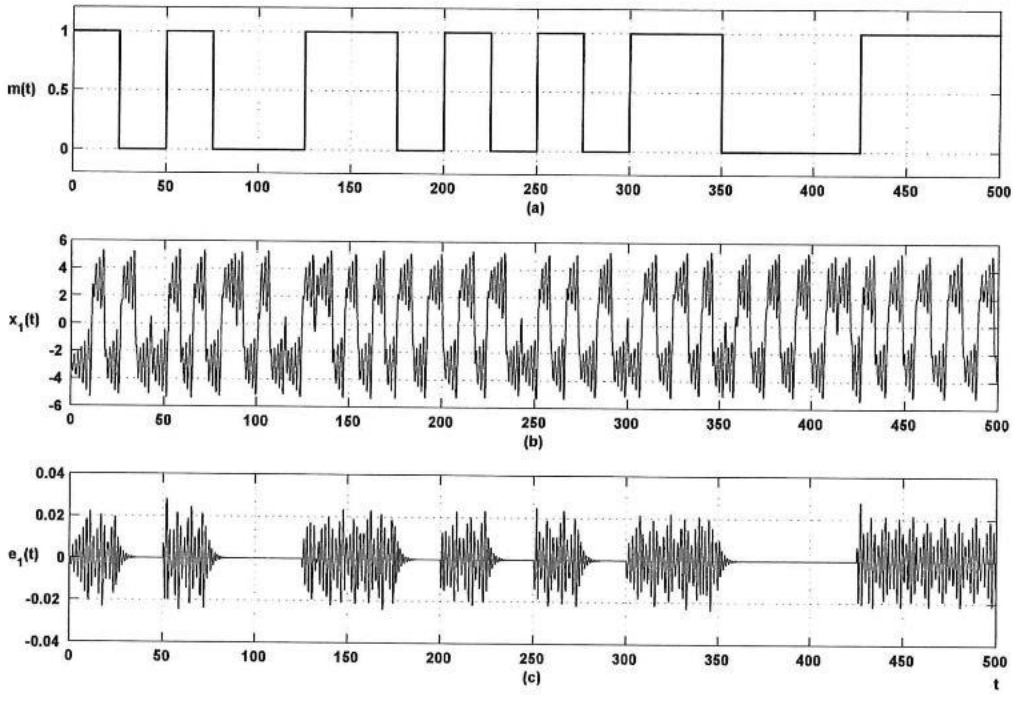

Figura 56: Encriptado, transmisión y recuperación de información confidencial mediante conmutación de atractores: (a) $m(t)$ mensaje binario por ocultar, (b) $x_1(t)$ señal de transmisión por el canal público (conteniendo información encriptada) y (c) información recuperada en forma de error de sincronización $e(t)$.

de el dígito "1" (no sincronización) y $\beta = 19$ al cual le corresponde la transmisión de el dígito "0" (sincronización), donde $\beta = 19$ para el circuito de Chua receptor todo el tiempo. La señal bianaria a transmitir es $m(t) = [10100110101011000111]$. Con la regla de conmutación (37), donde $r = 1.15$. Este proceso de transmisión privada de información binaria se puede apreciar en la figura 56, donde la figura 56a muestra el mensaje binario $m(t)$ a transmitir, la figura 56b la señal caótica de transmisión (siendo muy difícil de apreciar de aquí $m(t)$) y en la figura 56c la señal del error de sincronía entre las salidas del transmisor y del receptor.

7.1.2 Resultados experimentales

En la figura 57 se muestra el diagrama del circuto de Chua que fue implementado en (Cruz-Hernández *et al.* 2004) para generar el circuito transmisor y circuito receptor.

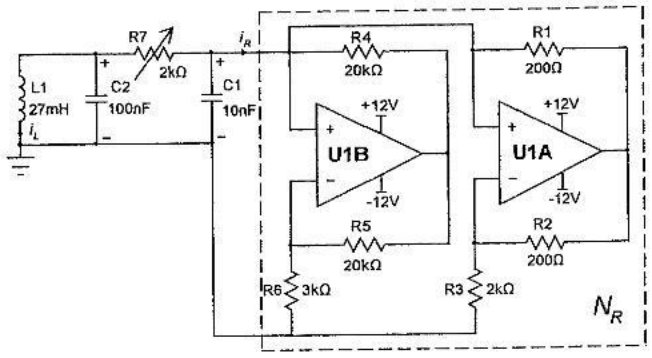

Figura 57: Implementación del circuito de Chua usando dos amplificadores operacionales y seis resistores lineales para crear un resistor no lineal.

La conmutación entre los atractores del circuito transmisor se logró al variar el parámetro β, con valores de $\beta' = 17.85$ al cual le corresponde la transmisión de el dígito "1" (circuito transmisor y recepector no sincronizan) y $\beta = 19$ al cual le corresponde la transmisión de el dígito "0" (circuito transmisor y receptor sincronizan), esto con $\beta = 19$ para el circuito receptor todo el tiempo. Donde el mensaje a transmitir es un tren de pulsos, es decir, este mensaje no es el mismo $m(t)$ que el de arriba ya mencionado en las simulaciones, ahora es: $m(t) = 1\ 0\ 1\ 0\ 1...$ Esto se lleva acabo mediante el circuito mostrado en la figura 58, con el cual se varía el ya antes mencionado parámetro β en las ecuaciones de Chua (2), generando así dos comportamientos caóticos diferentes. El primero es generado con $R'2 = 820\Omega$ para el cual $\beta = 19$ y el segundo es generado con $R'1 = 750\Omega$ para el cual $B = 17.85$.

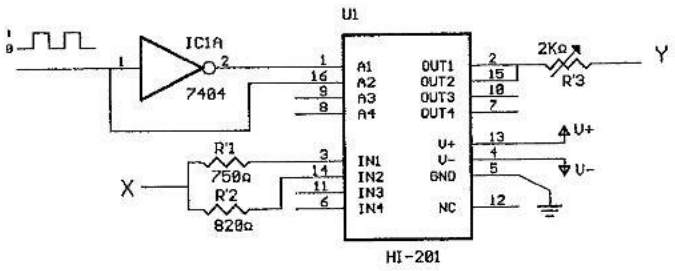

Figura 58: Circuito de conmutación para variar el parámetro β de un valor de 19 a 17.85, esto mediante el cambio de $R'2$ a $R'1$, respectivamente.

En la figura 59 se muestra la señal caótica transmitida $x_1(t)$ y la señal binaria confidencial por encriptar $m(t)$, mientras que en la figura 60 se muestra la señal binaria confidencial por ocultar $m(t)$ y señal recuperada por detección del error de sincronía $e(t) = x_1 - \xi_1(t)$.

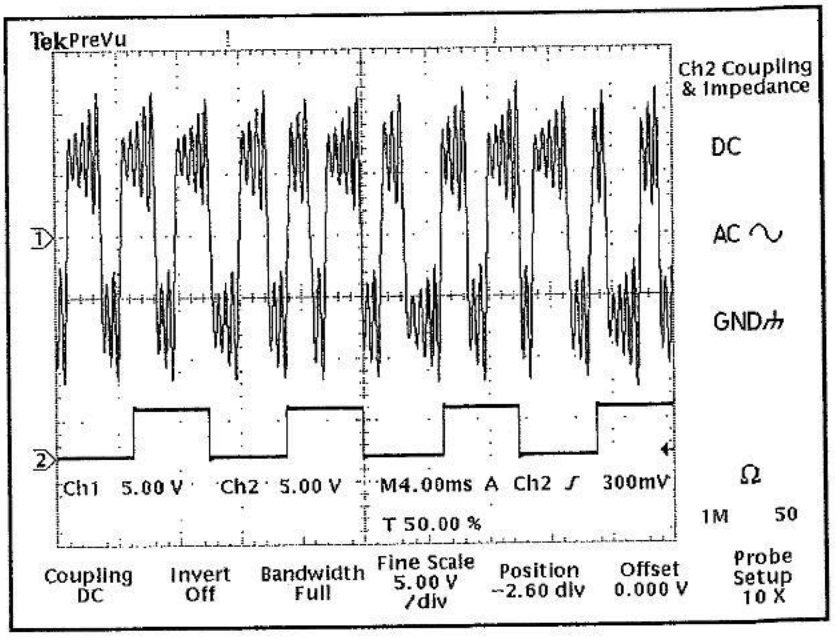

Figura 59: *Ch1*: Señal caótica transmitida $x_1(t)$ hacia el circuito receptor, *Ch2*: Señal binaria confidencial por ocultar $m(t) = 10101...$

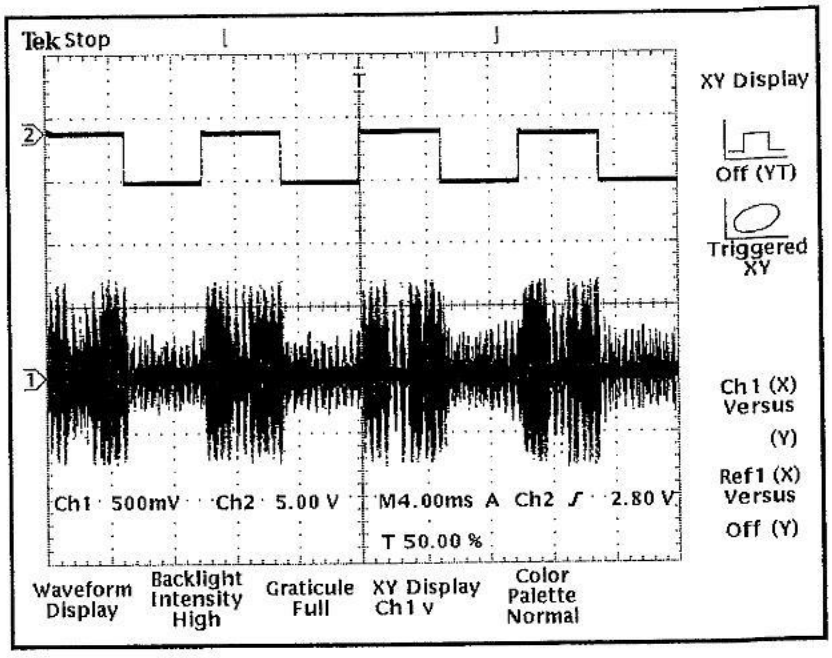

Figura 60: *Ch1*: Señal binaria confidencial por ocultar $m(t) = 10101...$, *Ch2:* Detección del error de sincronía.

7.2 Comunicación caótica entre multiusuarios

Una vez que se logró la sincronización caótica entre dos conjuntos de N sistemas maestros y N sistemas esclavos y expuesto el material de la sección anterior sobre comunicación digital entre un transmisor y un receptor. Ahora en adelante, el material esta dedicado a la comunicación entre multiusuarios, el sistema caótico del transmisor debe producir $y_i(t)$ señales que no tengan correlación entre si, las cuales se usan para codificar (encriptar) información binaria para u_i, usuarios, donde $i = 1, 2, ..., N$. Los receptores deben poseer la misma secuencia que los transmisores, de tal manera que puedan decodificar (desencriptar) la señal y obtener la información. El transmisor y el receptor tienen $N+1$ circuitos de Chua, mientras que las $y_i(t)$ señales de salida de los circuitos de Chua, desde $y_1(t)$ a $y_N(t)$ son utilizadas como codificadores para N usuarios, la señal de salida y_0 del circuito de Chua_{0T} (31) se utiliza para la sincronización con el receptor (30). Para lograr la individualidad de las señales de datos de diferentes usuarios en un solo canal, se utilizará la técnica convencional de espectro esparcido (Pickholtz *et al.* 1982).

El transmisor propuesto se puede apreciar en la figura 61. Los datos provenientes de cada usuario, m_i, $i = 1, 2, ..., N$, trasmiten un bit ± 1 con una duración de T segundos. El dato (bit) de u_i usuario es multiplicado por una secuencia caótica $y_i(t)$. La red caótica del transmisor produce las señales $y_i(t)$ donde el subíndice i indica las señales de salida de los circuitos caóticos de Chua de 1 a N. El dato binario proveniente de los usuarios, se encripta mediante la multiplicación con su respectiva señal caótica de salida $y_i(t)$ y posteriormente combinado en un canal común $s(t)$. Esto se refleja en la siguiente expresión

$$s(t) = y_1(t) \cdot m_1 + y_2(t) \cdot m_2 + ... + y_N(t) \cdot m_N. \tag{38}$$

La señal resultante, $s(t)$ es transmitida a través del canal inseguro hacia el conjunto de receptores remotos que se muestra en la figura 62. Al mismo tiempo, es retroalimentada al circuito de Chua_{0T} del conjunto de transmisores.

Una vez que se reciben los mensajes encriptados en la señal de transmisión $s(t)$ por el canal inseguro en el sistema receptor, este decodifica (desencripta) el mensaje del usuario u_i, obteniendo la función signo del resultado de la sumatoria del producto de la señal que se recibe $s(t)$ con la señal cáotica de salida η_i de dicho usuario u_i del receptor. La sumatoria de los resultados del producto antes mencionada, va desde el tiempo t donde inicio el bit que se esta transmitiendo hasta nT, donde n es el número de bit que se esta transmitiendo y T es la duración del bit. Esto se explica por la siguiente expresión

$$\hat{m}_i = sgn\left[\sum_{t}^{nT} \eta_i \cdot s(t)\right], \tag{39}$$

7.3 Resultados numéricos

En la misma forma que para sincronización, por simplicidad y con propósitos ilustrativos, se consideran solo dos ($N = 2$) usuarios. Para la obtención de resultados numéricos, se utilizan las ecuaciones normalizadas del circuito de Chua. Donde las ecuaciones (31), (32) y (33) vistas en el capítulo anterior le corresponden al sistema transmisor constituido por el circuito de Chua cero (Chua_{0T}), circuito de Chua usuario 1 y circuito de Chua usuario 2 de dicho sistema transmisor, respectivamente. Mientras que las ecuaciones (34), (35) y (36) también vistas en el capítulo anterior le corresponden al sistema receptor formado por el circuito de Chua cero (Chua_{0R}), el circuito de Chua usuario 1 y circuito de Chua usuario 2 de dicho sistema receptor, respectivamente. Donde la sincronización se lleva acabo mediante el esquema de sincronización por retroalimentación en combinación con el método en base en formas hamiltonianas con el sistema caótico receptor, en el escenario de acoplamiento unidireccional maestro y esclavo. De acuerdo al capítulo 5 el valor de la ganancia K del observador es como sigue

$$K = (5, 8, 0)^T.$$

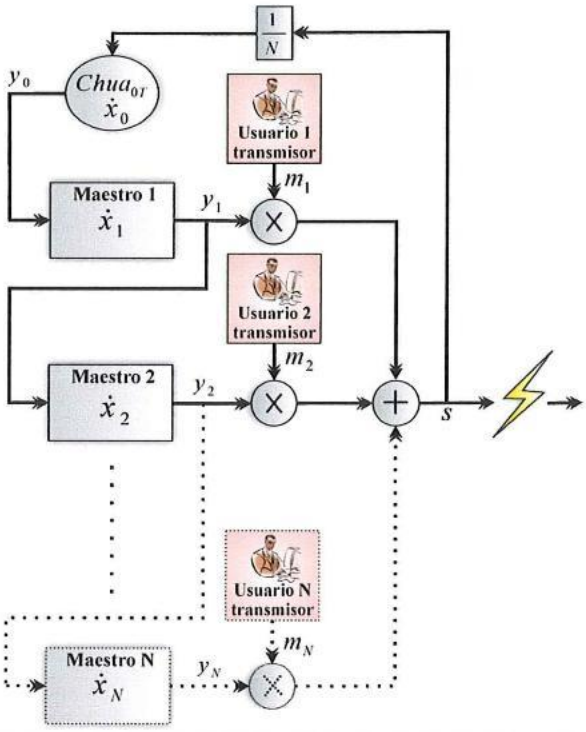

Figura 61: Diagrama a bloques del conjunto de sistemas transmisores en esquema para multiusuarios, utilizando circuitos de Chua y técnica de espectro esparcido.

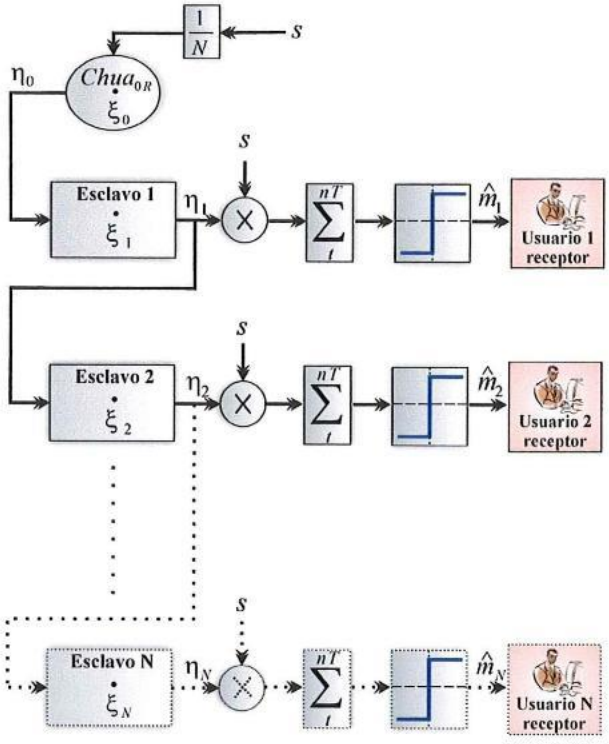

Figura 62: Diagrama a bloques del conjunto de sistemas receptores en esquema para multiusuarios, utilizando circuitos de Chua y técnica de espectro esparcido.

7.3.1 Recuperación de mensajes

Ahora, una vez que se ha generado caos en el sistema transmisor y se logró sincronización entre el sistema transmisor y receptor, se procederá con el envío de los mensajes confidenciales (m_1 y m_2) de manera simultanea, por un solo canal público inseguro y además la recuperación de dichos mensajes ($\hat{m}_1$ y $\hat{m}_2$) por los usuarios 1 y 2 respectivamente. Por ejemplo, una vez que se recibió el mensaje encriptado en la señal de transmisión $s(t)$ por el canal inseguro en el usuario 1 del receptor remoto, éste decodifica (desencripta) el mensaje, obteniendo la función signo del resultado de la sumatoria del producto de la señal que se recibe $s(t)$ con la señal cáotica de salida $\xi_{1_N}(t)$ de dicho usuario. La sumatoria de los resultados del producto antes mencionado, va desde el tiempo t donde inicio el bit que se esta transmitiendo hasta nT, donde n es el número de bit que se esta transmitiendo y T es la duración del bit. Lo antes dicho se refleja en la ecuación (40) para el usuario 1 y en la ecuación (41) para el usuario 2.

$$\hat{m}_1(t) = signo\left[\sum_{t}^{nT} \xi_{1_1}(t)s(t)\right] \tag{40}$$

$$\hat{m}_2(t) = signo\left[\sum_{t}^{nT} \xi_{1_2}(t)s(t)\right] \tag{41}$$

En la figura 63a y 63b se muestran los mensajes binarios $m_1(t)$ y $m_2(t)$ pertenecientes al usuario 1 y usuario 2, respectivamente. La información confidencial $m_1(t)$ corresponde a l tarjetas de crédito en base binario al igual que $m_2(t)$. En el caso de $m_1(t)$ en la figura 63a, se muestra la tarjeta de crédito No. 1 (1383 5022 8687 5420) y parte de la tarjeta de crédito No. 2 (1279.....) en base binario, mientras que $m_2(t)$ en la figura 63b se muestra la tarjeta de crédito No. 1 (1323 1520 5552 2138) y parte de la tarjeta de crédito No. 2 (3871.....) en base binario. En la figura 63c se muestra $m_1(t)$ y $m_2(t)$ ocultas en la señal caótica $s(t)$ que se envía a través de un solo canal público inseguro y de manera simultanea hacia el sistema receptor remoto. En las figuras 63d y 63e se muestran recuperados la información $\hat{m}_1(t)$ y $\hat{m}_2(t)$ pertenecientes al usuario 1 y usuario 2, respectivamente del sistema receptor. Donde $\hat{m}_1(t)$ corresponde a l tarjetas de crédito en base binario al igual que $\hat{m}_2(t)$. En el caso de $\hat{m}_1(t)$, en la figura 63d se muestra la tarjeta de crédito No. 1 desencriptada (1383 5022 8687 5420) y parte de la tarjeta de crédito No. 2 (1279.....) en base binario, mientras que $\hat{m}_2(t)$ en la figura 63e se muestra la tarjeta de crédito No. 1 desencriptada (1323 1520 5552 2138) y parte de la tarjeta de crédito No. 2 (3871.....) en base binario.

7.4 Conclusiones

Los resultados tanto numéricos como experimentales mostrados en la comunicación binaria con la técnica de conmutación de 2 atractores, demuestra su capacidad para proporcionar seguridad y la efectividad para recuperar el mensaje original, mediante la sincronía de los dos circuitos caóticos transmisor y receptor.

Ahora, el esquema de comunicación entre N usuarios fue propuesto también en este capítulo. A manera de ilustración, se presentó una red de dos usuarios. Se mostró que para ambos, utilizando el esquema de sincronización por retroalimentación en conjunto con el método de sincronización de osciladores caóticos mediante sistemas hamiltonianos generalizados y el diseño de un observador, es posible lograr una comunicación entre el sistema transmisor y receptor, es decir, recuperar en el sistema receptor para cada uno de los dos usuarios la información enviada por el sistema transmisor.

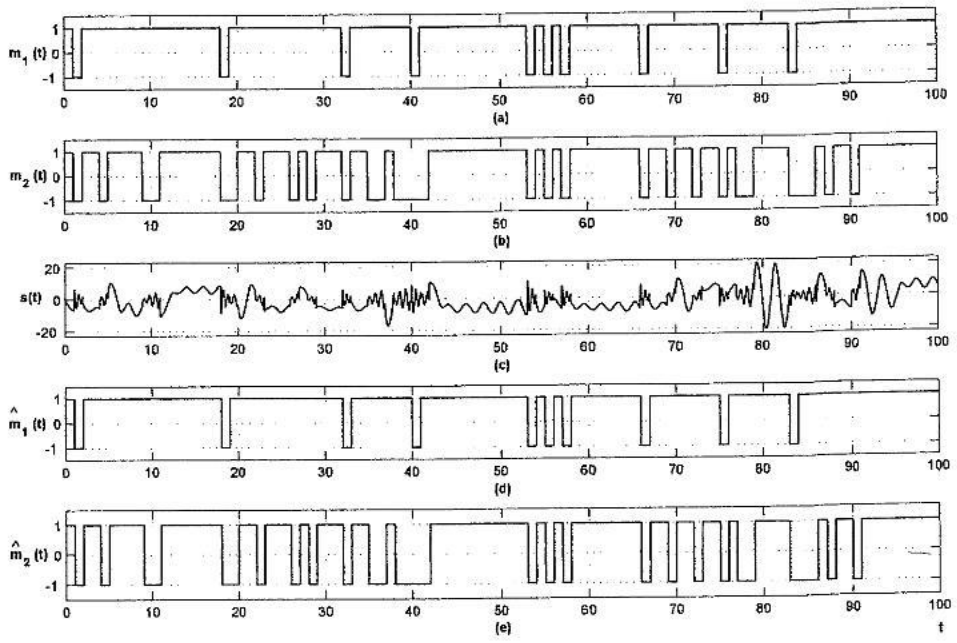

Figura 63: Encriptado, transmisión y recuperación de información confidencial: (a) $m_1(t)$ información enviada por el Usuario 1, (b) $m_2(t)$ información enviada por el usuario 2, (c) $s(t)$ señal de transmisión por el canal inseguro (conteniendo la información encriptada), (d) $\hat{m}_1(t)$ información recuperada por el usuario 1 y (e) $\hat{m}_2$ información recuperada por el usuario 2.

8 Conclusiones

La aportación principal del trabajo presentado en esta tesis es la comunicación caótica en una red de usuarios. Dicha red esta formada de N circuitos de Chua transmisores y N circuitos de Chua receptores, dichos circuitos cuentan con una dinámica caótica. La sincronización entre los circuitos de Chua transmisores y receptores se llevó a cabo mediante el esquema de sincronización por retroalimentación, en combinanción con el método de sincronización de osciladores caóticos mediante sistemas hamiltonianos generalizados y el diseño de un observador. Relacionado a lo antes mencionado se obtuvieron los siguientes resultados:

- Se encontró tanto con el estudio numérico como experimental que el circuito de Chua para valores de los parámetros $\alpha = 10, \beta = -19, a = -1.43$ y $b = -0.78$ es capaz de generar señales de dinámicas complejas.
- En cuanto a la sincronización en configuración maestro y esclavo entre dos circuitos de Chua cóticos, para los valores de ganancia del observador $k_1 = 5$, $k_2 = 8$ y $k_3 = 0$ se obuvo la sincronización óptima. Esto se verificó tanto por el estudio numérico como experimental. De igual manera, en el estudio numérico para estos mismos valores de ganancia del observador se encontró que para una red de 2 transmisores y 2 receptores se obtiene una sincronización óptima.
- Una vez que se logró la sincronización, la comunicación caótica se realizó tanto en un transmisor y receptor como en una red compuesta por 2 transmisores y 2 receptores. En cuanto a la comunicación entre un transmisor y receptor a través de un canal público inseguro, se realizó tanto el estudio numérico y experimental, logrando la transmisión de un mensaje binario y tren de pulsos, respectivamente. Mientras que en la red compuesta por 2 transmisores y 2 receptores, se realizó el estudió numérico, obteniendo muy buenos resultados tanto en la transmisión simultanea de mensajes binarios por ambos transmisores a través de un canal público inseguro, así como en la recuperación de los mismos en sus respectivos receptores.

Trabajo futuro

Las actividades futuras a realizar respecto al tema principal de este trabajo son las siguientes:

1. Investigar la robustez a variaciones paramétricas y a ruido en la señal de acoplamiento utilizada para llevar a cabo la sincronización entre sistema transmisor y receptor.
2. Analizar el comportamiento del encriptado de información digital bajo la presencia de ruido en el canal de transmisión.
3. Llevar a cabo la implementación física de la transmisión de información en una red de usuarios.
4. Realizar investigación más a fondo en cuanto a la aplicación de la comunicación caótica en una red de usuarios dentro del mercado de las telecomunicaciones.

Referencias

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

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

[3] Aguilar Bustos Ana Yaveni (2006), *Sincronización de osciladores caóticos discretos*, Tesis doctoral DET-CICESE.

[4] Barker G. L. y Gollub J. P. (1990), *Chaotic dynamics, an introduction*, Cambridge University Press.

[5] Chen G. y Dong X. (1998), *From chaos to order, Methodologies, Perspectives and Applications*, World Scientific, Singapore.

[6] Chua L. O., Kocarev L. y Eckert K. (1993), "Chaos synchronization in Chua's circuit", *J. Circuits. Syst. Computers*, **3**(1), 93-108 pp.

[7] 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 pp.

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

[9] Cruz-Hernández C., López-Mancilla (2004), García-Gradilla, Serrano-Guerrero y Nuñez-Pérez, "Experimental realization of binary signals transmission using Chaos", *Journal of Circuits*, Systems and Computers, **14**(3), 453 - 468 pp.

[10] Cruz C. y Nijmeijer H. (2000), "Synchronization through filtering", *Int. J. Bifurc. Chaos*, **10**(4), 763-755 pp.

[11] Cruz-Hernández C., Posadas C y Sira-Ramírez H., "Synchronization of two hyperchaotic Chua circuits: A generalized Hamiltonian systems approach". In: *Procs. of the 15th IFAC World Congress*, july 21-26, 2002 Barcelona, España.

[12] Cruz-Hernández C. y Romero-Haros N. (2006), "Communicating via synchronized time-delay Chua's circuits", *Communications in Nonlinear Science and Numerical Simulation* (doi:10.1016/j.cnsns.2006.06010).

[13] Cruz Hernández César y López Mancilla D. (2007), *Synchronization of oscillations: Application to chaotic communications*, Cambridge Scientific Publishers Ltd. Por publicarse.

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

[15] Devaney R. L. (1989), *An introduction to chaotic dynamical systems*, Segunda edición, Addison-Wesley Pub.

[16] Feldman U., Hasler M. y Schwarz W. (1996), "Communication by chaotic signals: the inverse system approach", *Int. J. Circ Theory Appl.*, **24**, 551-579 pp.

[17] Gámez Guzmán Luís (2004), *Encriptador de información con base en la sincronía de atractores con errollamientos múltiples*, Tesis de maestría DET-CICESE, 156 pp.

[18] 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 pp.

[19] Julien C. Sprott (2000), *Strange attractors: Creating Patterns in Chaos*, 576 pp.

[20] Kahn D. (1996), *The code breakers, The comprehensive history of secret communication from anciant times to the internet*, Scribner, New York.

[21] 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 pp.

[22] Kennedy M. P. (1993), "Three steps to chaos part II: A Chua's Circuit", *IEEE Trans. Circuits Syst.* I, **40**(10): 657-674 pp.

[23] Kocarev L., Halle K. S., Eckert K., Chua L. O. y Parlitz U. (1992), "Experimental demostration of secure communications via chotic synchronization", *Int. J. Bifurc. and Chaos*, **2**, 709-713 pp.

[24] Leon O. Chua, Chai Wah Wu, Anshan Huang, and Guo-Qun Zhong, "A Universal Circuit for Studying and Generating Chaos - Part I: Routes to Chaos", *IEEE Transactions on Circuits and Systems -I: Fundamental Theory and Applications*, **40**(10), 732-744 pp.

[25] Leon O. Chua, Chai Wah Wu, Anshan Huang, and Guo-Qun Zhong, "A Universal Circuit for Studying and Generating Chaos - Part II: Strange Attractors", *IEEE Transaction on Circuits and Systems-I: Fundamental Theory and Applications*, **40**, 745 - 761 pp.

[26] 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 pp.

[27] López-Mancilla, D. y Cruz-Hernández, C. (2005), "Output Syncronization of Chaotic Systems: Model-Matching Approach with Application to Secure Communication", *Nonlinear Dynamics and Systems Theory*, **5**(2), 141 - 156 pp.

[28] López D. y Cruz-Hernández C. (2005), "A note on chaos-based communication schemes", *Revista Mexicana de Física*, **51**(3), 265-269 pp.

[29] López Mancilla Didier (2005), *Sincronización de osciladores caóticos perturbados con aplicación a sistemas de comunicaciones*, Tesis doctoral DET-CICESE.

[30] López-Mancilla D y Cruz-Hernández C. (2006), "Output synchronization of chaotic systems under novanishing perturbations", *Chaos, Solitons, and Fractals* (doi:10.1016/j.chaos.2006.10.020).

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

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

[33] Meranza Castillón Manuel Omar (2002), *Implementación de un sistema de encriptamiento hipercaótico*, Tesis de maestría DET-CICESE.

[34] Murillo Camacho Amada Elizabeth (2006), *Transmisión de información codificada por caos*, Tesis de licenciatura ITESCA.

[35] Nijmeijer H. y Mareels I. (1997), "An observer looks at synchronization", *IEEE Trans. Circuit Syst. I*, **44**(10), 882-890 pp.

[36] Nuñez P. Ricardo (2006), "Algoritmo de riqueza espectral que califica la sincronización caótica", SOMI XXI Congreso de instrumentación, Ensenada Baja California, Octubre 2006.

[37] Ott E. (2002), *Chaos in dynamical systems*, segunda edición, Cambridge University Press.

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

[39] Pikovsky A., Rosenblum M. y Kurths J. (2001), *Synchronization: A universal concept in nonlinear sciences*, Cambridge University Press.

[40] Posadas Castillo Cornelio (2001), *Sincronización de osciladores de Lorenz por formas hamiltonianas*, Tesis de maestría DET-CICESE.

[41] Posadas-Castillo C., Cruz-Hernández C., y Núñez R. (2004), "Experimental realization of binary signals transmission based on synchronized Lorenz circuits", *J. Appl. Research Tech.*, **2**(2),127-137 pp.

[42] Raymond L. Pickholtz, Donald L. Schilling y Laurence B. Milstein (1982), "Theory of Spread-Spectrum Communications - A Tutorial", *IEEE Transactions on Communications*, **30**(5), 855 - 884 pp.

[43] Romero Haros Néstor Rubén (2005), *Sincronización del circuito de Chua con retardo: aplicación a la transmisión secreta de información*, Tesis de maestría, DET-CICESE, 122 pp.

[44] 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 pp.

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

[46] Serrano Guerrero Hazael (2002), *Implementación de un sistema encriptador con base en la sincronía de circuitos de Chua*, Tesis de maestría DET-CICESE.

[47] Sing S. (1999), *The code book, The science of secrecy from Ancient Egypt to quantum cryptography*, Anchor Books, New York.

[48] Sira-Ramírez y Cruz Hernández (2000), "Synchronization of chaotic systems: A generalized Hamiltonian systems approach", *Procs. of America Control Conference (ACC'2000)*, Chicago, USA, 769-773 pp.

[49] Sira Ramírez y Cruz Hernández (2001), "Sinchronization of chaotic systmems: A generalized Hamiltonian systems approach", *Int. J. Bifurc. Chaos*, **11**(5), 1381-1395 pp.

[50] Ushio T. (1996), "Synthesis of chotically synchronized systems based on observers", *Proccedings Int. Conference Nonlinearity Bifurc. Chaos*, 251-254 pp.

[51] Veljko Milanovic y Mona E. Zaghloul. (1996), "Synchronization of chaotic neural networks and application to communications", Int. J. Bifurc. and Chaos, **6**(12B), 2571-2585 pp.

[52] www.wikipedia.com.

[53] Zbigniew Kotulski y Janusz Szczepanski, "Discrete chaotic cryptography (DCC)", *Proc. NEEDSt97, 1997.*

A Apéndice: Programas

A continuación se presentan los programas elaborados en *simulink* que se utilizaron para realizar las simulaciones numéricas en este trabajo de tesis.

A.1 Ecuaciones normalizadas del circiuto de chua (6)-(7)

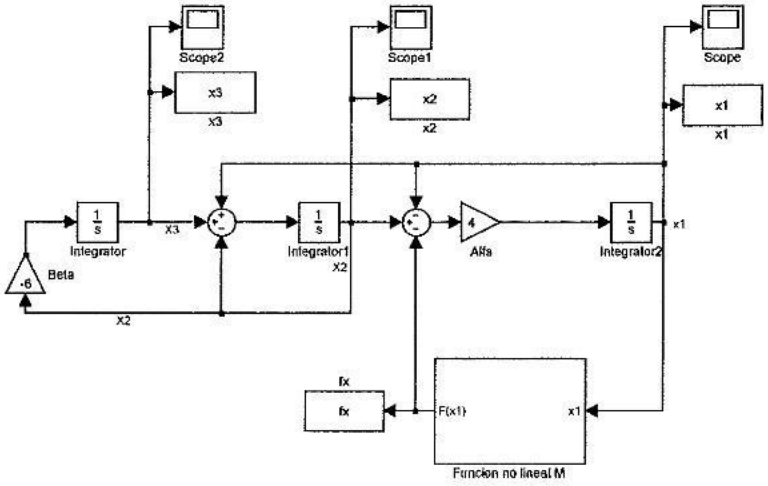

Figura 64: Ecuaciones adimensionales o normalizadas del circuito de Chua.

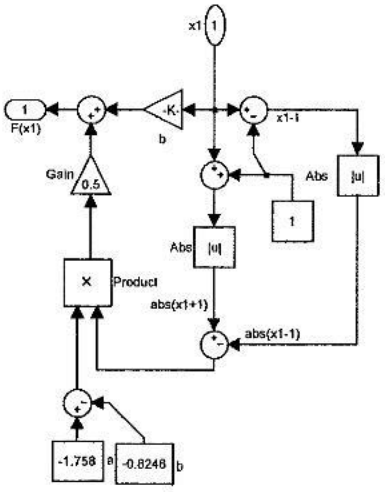

Figura 65: Función no lineal normalizada del circuito de Chua.

A.2 Ecuaciones de forma canónica hamiltoniana del sistema maestro y esclavo de chua (25)-(26)

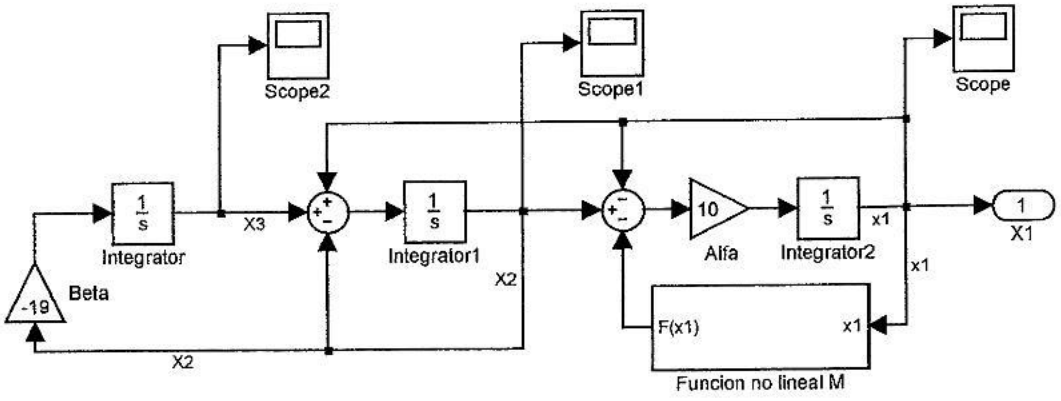

Figura 66: Sistema maestro del circiuto de Chua.

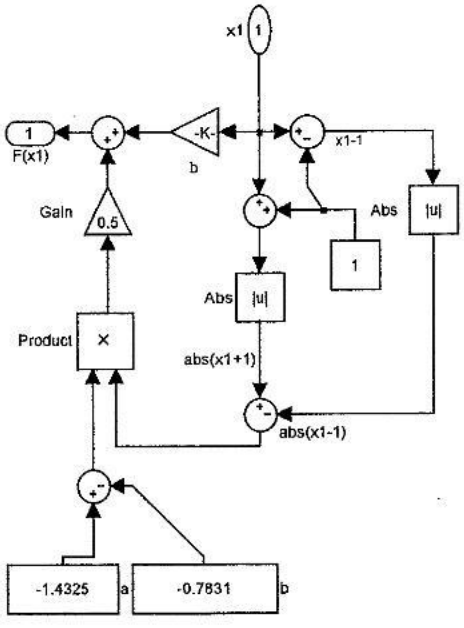

Figura 67: Función no lineal del sistema maestro de Chua.

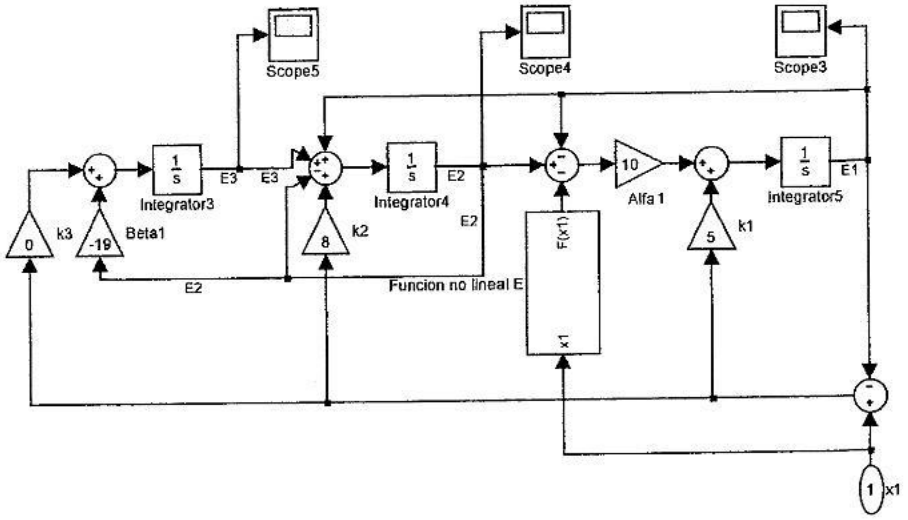

Figura 68: Sistema esclavo del circiuto de Chua.

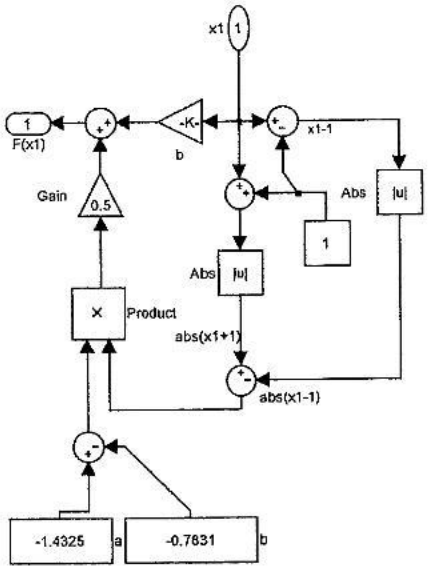

Figura 69: Función no lineal del sistema esclavo de Chua.

A.3 Sincronización entre múltiples maestros y esclavos (31), (32), (33), (34), (35) y (36)

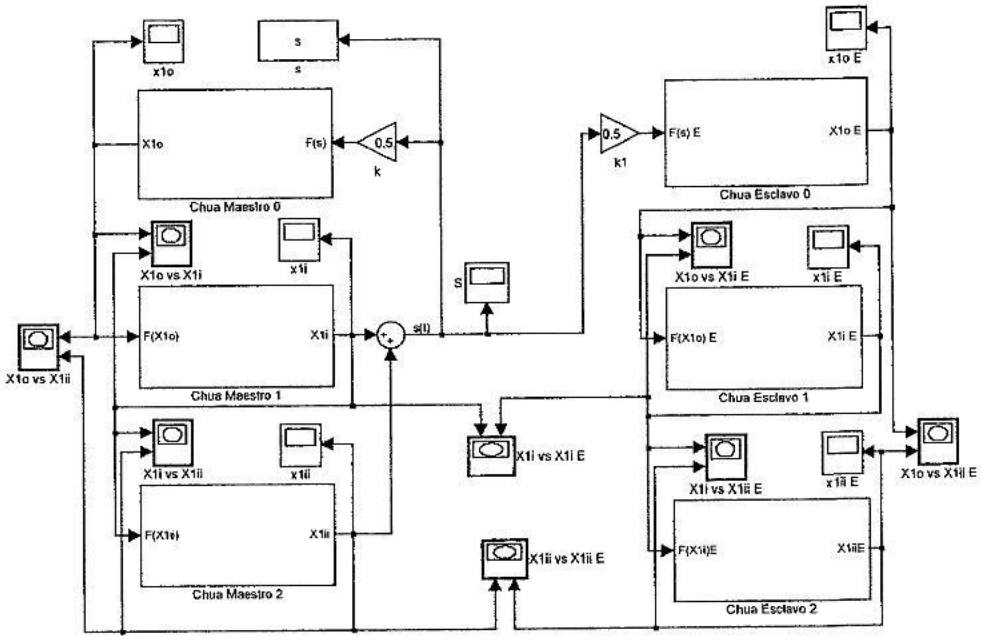

Figura 70: Sincronización entre múltiples maestros y esclavos.

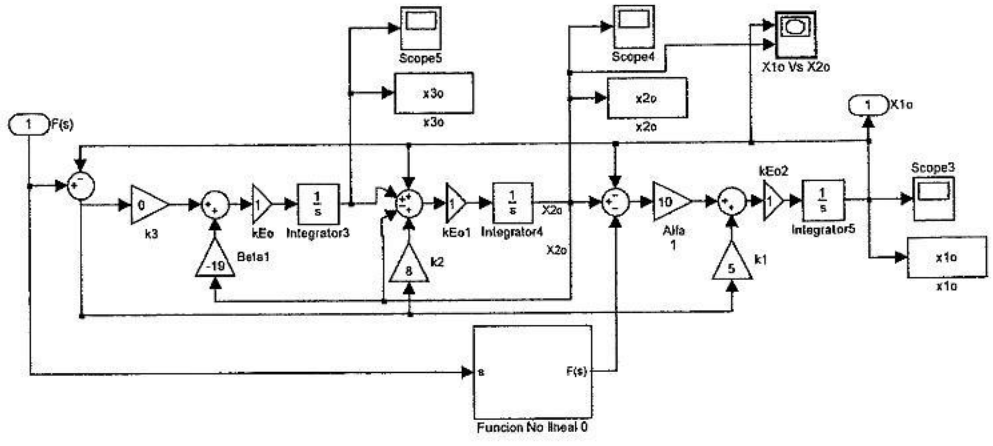

Figura 71: Circuito Chua maestro cero (Chua_{0T}).

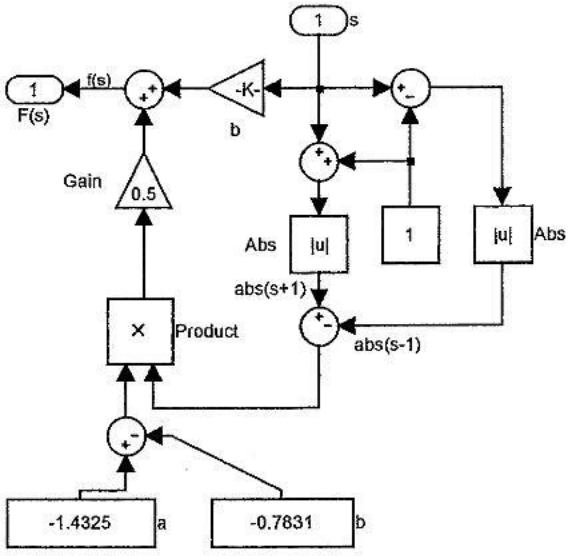

Figura 72: Función no lineal del circuito Chua maestro cero (Chua_{OT}).

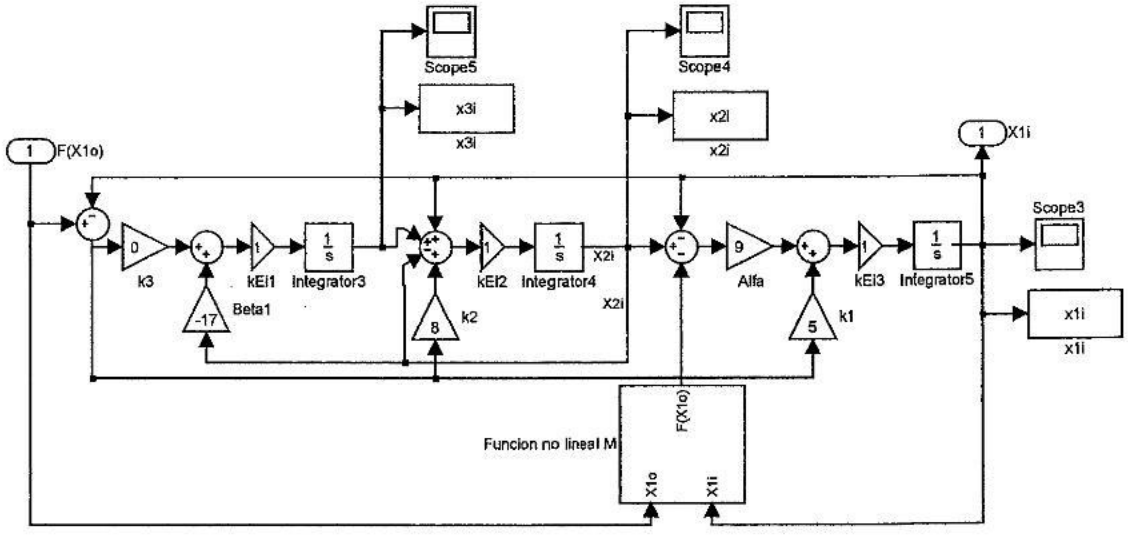

Figura 73: Circuito Chua maestro uno.

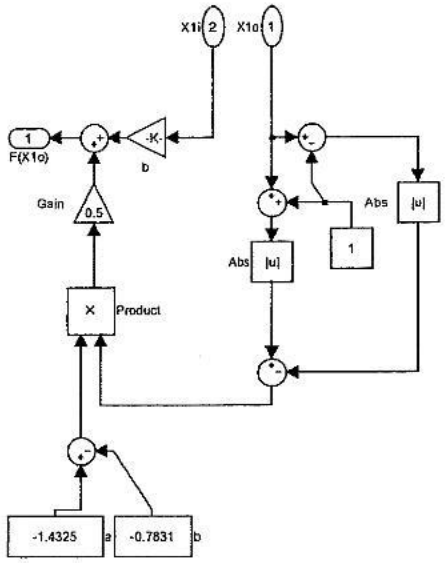

Figura 74: Función no lineal del circuito de Chua maestro uno.

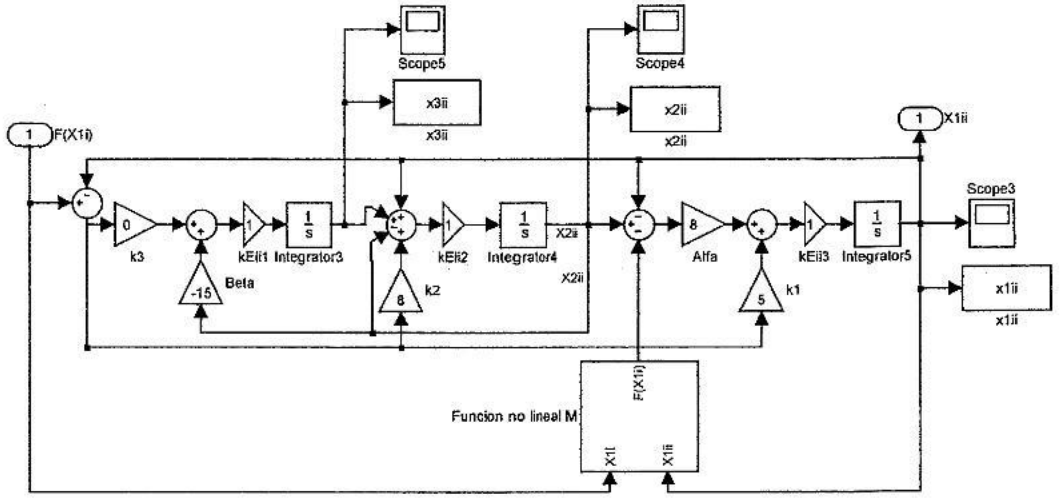

Figura 75: Circuito de Chua maestro dos.

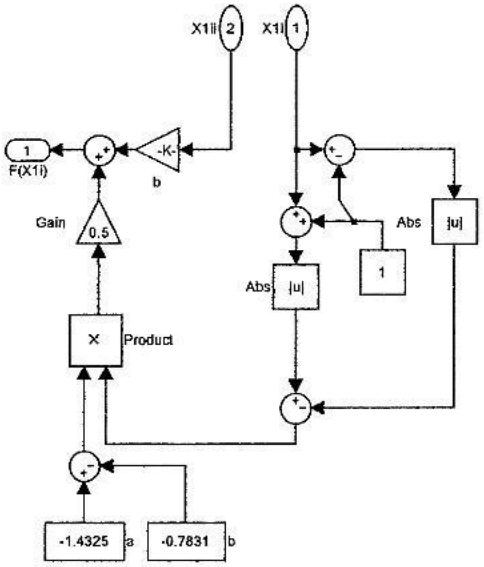

Figura 76: Función no lineal del circuito de Chua maestro dos.

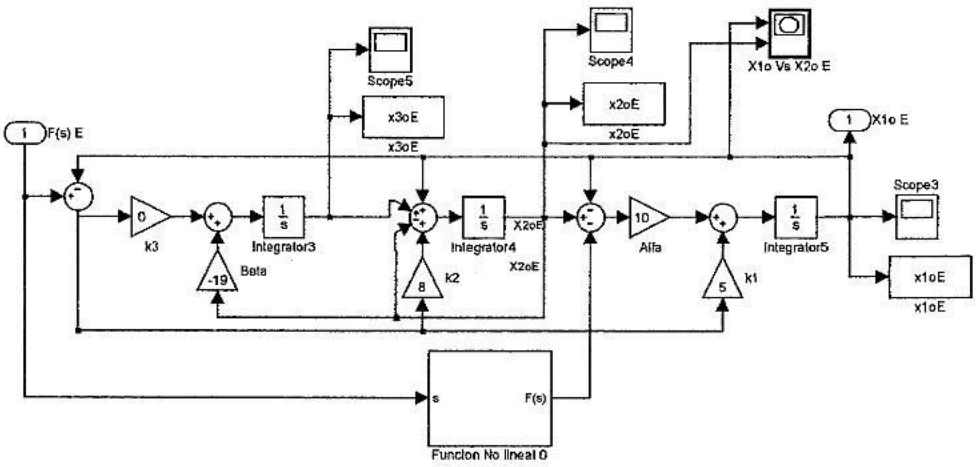

Figura 77: Circuito Chua cero del esclavo (Chua_{0R}).

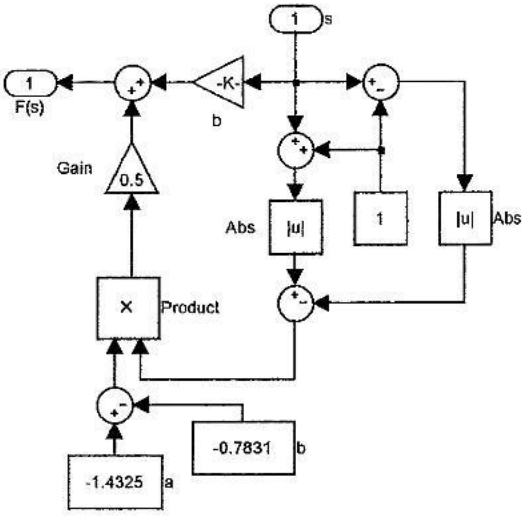

Figura 78: Función no lineal del circuito Chua cero del esclavo (Chua_{0R}).

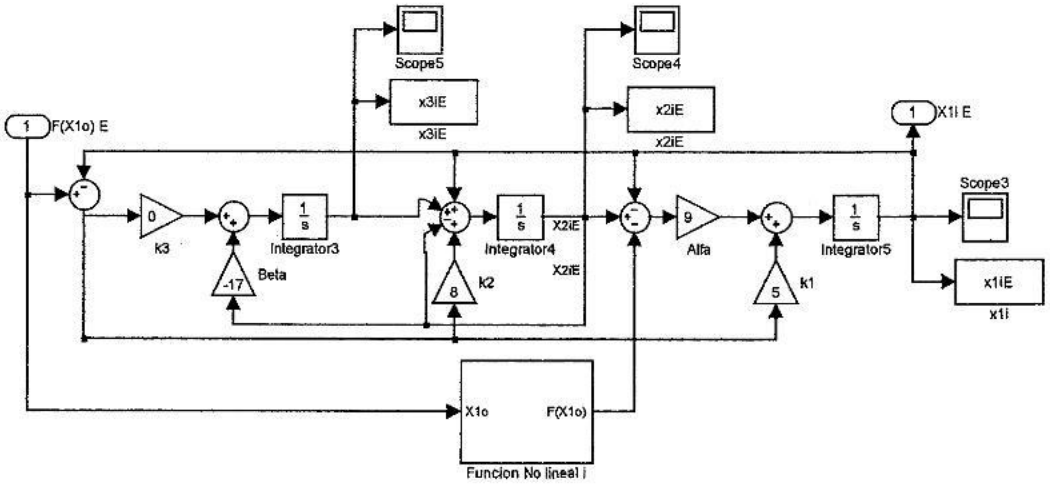

Figura 79: Circuito de Chua esclavo uno.

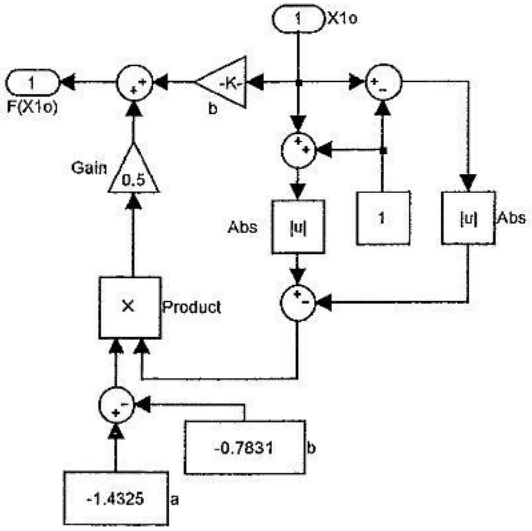

Figura 80: Función no lineal del circuito Chua esclavo uno.

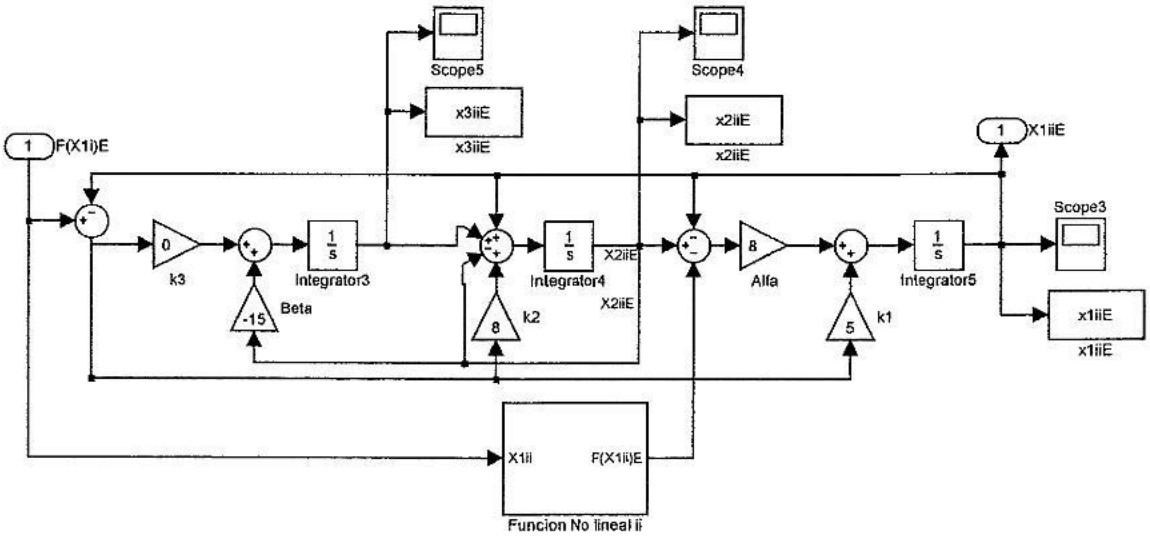

Figura 81: Circuito de Chua esclavo dos.

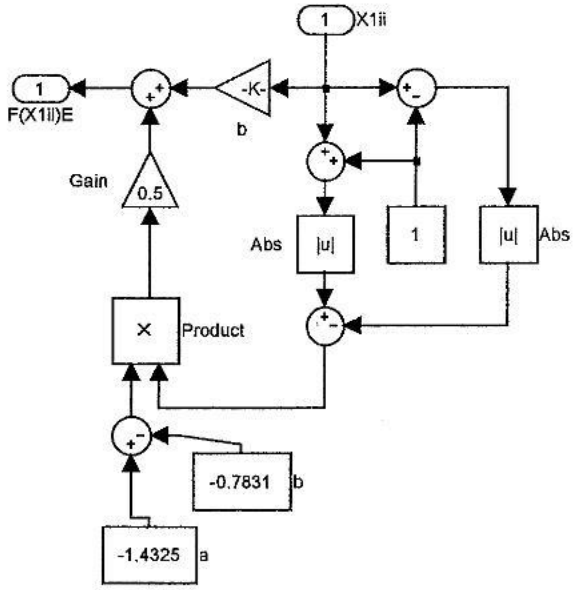

Figura 82: Función no lineal del circuito Chua esclavo dos.

A.4 Comunicación caótica entre multiusuarios (38)

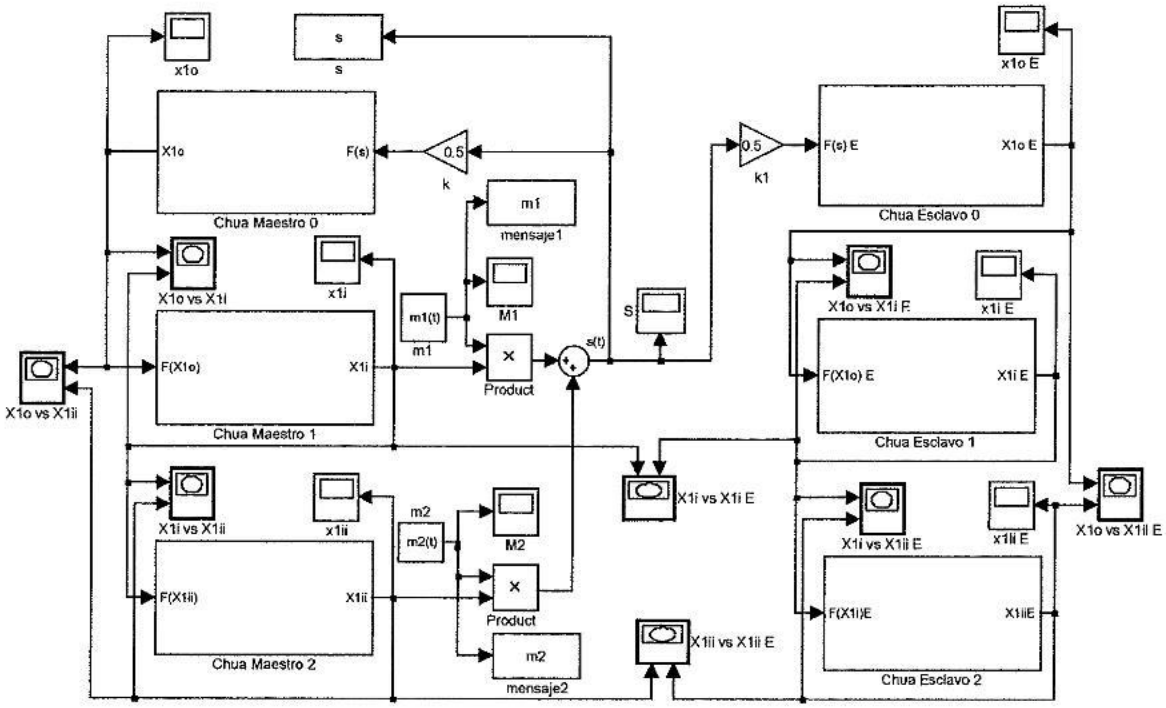

Figura 83: Comunicación caótica entre multiusuarios.

A.5 Recuperación de los mensajes originales (40)-(41)

```
%Matlab 7.0.
% Descripción: Recuperación de mensajes en una red de multiusuarios.
% Revisión: Junio-14-2006.
% Autor: Juan Manuel Mejia Camacho.
N=1;
t=1;
%Inicia sumatoria para recuperación de mensajes.
while (tout(t)<100 )&(t<6108)
u1=0;
u2=0;
while (tout(t) <=N)&(t<6108)
u1=x1iE(t)*s(t)+u1;
u2=x1iiE(t)*s(t)+u2;
Almacen(t)=u1;
Almacen1(t)=u2;
t=t+1;
end;
%Función signo de la sumatoria para recuperar el bit encriptado.
m1r(N)=sign(u1);
m2r(N)=sign(u2);
N=N+1;
end;
N=1;
```

```
t=1;
%Gráficas de los resultados obtenidos.
while (tout(t)<100)&(t<6108)
while (tout(t) <=N)&(t<6108)
mr1(t)=m1r(N);
mr2(t)=m2r(N);
t=t+1;
end;
N=N+1;
end;
Almacen(6108)=u1;
Almacen1(6108)=u2;
mr1(6108)=mr1(6107);
mr2(6108)=mr2(6107);
subplot(7,1,1);plot(tout,m1,'-k');
subplot(7,1,2);plot(tout,Almacen,'-k');
subplot(7,1,3);plot(tout,mr1,'-k');
subplot(7,1,4);plot(tout,s,'-k');
subplot(7,1,5);plot(tout,m2,'-k');
subplot(7,1,6);plot(tout,Almacen1,'-k');
subplot(7,1,7);plot(tout,mr2,'-k');
```