UNIVERSIDAD AUTONOMA DE BAJA CALIFORNIA

FACULTAD DE INGENIERIA ENSENADA

MAESTRIA Y DOCTORADO EN CIENCIAS E INGENIERIA

CIFRADO DE INFORMACIÓN CON BASE EN SINCRONIA DE ATRACTORES CAÓTICOS CON MULTIPLES ENROLLAMIENTOS

TESIS

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

EDUARDO RODRIGUEZ OROZCO

Ensenada Baja California, México Agosto de 2009

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

FACULTAD DE INGENIERÍA
UNIDAD ENSENADA

CIFRADO DE INFROMACIÓN CON BASE EN SINCRONIA DE ATRACTORES CAÓTICOS CON MULTIPLES ENROLLAMIENTOS

TESIS

Que para obtener el grado de maestría en ingeniería presenta:

Eduardo Rodríguez Orozco

Aprobada por:

Dra. Rosa Martha López Gutiérrez
Director de tesis

Dr. Cesar Cruz Hernández
Miembro del comité

Dr. Enrique Efrén García Guerrero
Miembro del comité

Ensenada Baja California, México. Octubre 2009

DEDICATORIA

A mi madre Edelmira por traerme al mundo y educarme, a mi esposa Lolita por su complicidad, a mi hija Iliana Sofía por abrirme los ojos a un amor que me era desconocido, a mis hermanos Rafael, Marcial, Trinidad, Martin, Lolis, Leticia, Gabriel, Ángeles y Raymundo por su apoyo y su tiempo, a mis amigos Rodolfo, Jesús, Octaviano, Daniel, Eduardo, Rogelio por sus motivación.

AGRADECIMIENTOS

A mis sinodales la Dra. Rosa Martha López, al Dr. Cesar Cruz, al Dr. Efrén García y al M. C. Everardo Inzunza que me han apoyado y enseñado muchas cosas a lo largo de 2 años de convivencia.

A mis profesores que han estado a lo largo de mi vida ya que ellos son un ejemplo a seguir profesional y académicamente.

A la Universidad Autónoma de Baja California, por abrir sus puertas y permitir que estudie en sus instalaciones.

Al CONACYT por el apoyo económico recibido.

Lista de figuras

1. Introducción

1.1. Antecedentes

En la década pasada, el estudio de sincronización de osciladores caóticos de dimensión menor inspiró algunas posibles aplicaciones, incluyendo las *comunicaciones seguras*.

A partir de la sincronía de sistemas caóticos, se abre la potencial aplicación de este principio para construir sistemas de encriptado que sustituyan a los complicados algoritmos convencionales, con el fin de transmitir información privada de manera segura. Varias técnicas de comunicación caótica se reportan en la literatura, por ejemplo, encriptado aditivo [Cuomo, *et al*., 1993], conmutación entre dos atractores caóticos [Parlitz, *et al*., 1992] y modulación paramétrica [Yang y Chua, 1996]. Sin embargo, algunos trabajos posteriores han mostrado que estas técnicas tienen un grado de seguridad poco confiable (ver por ejemplo [Short, 1994; Pérez y Cerdeira, 1995; Yang, 1995; Short, 1996]).

Para enfrentar a esto, recientemente se han propuesto algunos métodos para aumentar la complejidad de la dinámica de los sistemas caóticos y de este modo, hacer que la identificación de la información sea más difícil. Por ejemplo, en Cruz- Hernández, *et al*. [2002] se propone el uso de formas hamiltonianas y el diseño de un observador para sincronizar dos circuitos hipercaóticos de Chua acoplados unidireccionalmente. Los autores aplican este método para transmitir información digital y obtienen que la calidad de la información recobrada sea mayor que en las técnicas de los observadores tradicionales, mientras la codificación permanece potencialmente segura.

En la actualidad, resulta claro que tales aplicaciones requieren un mejor entendimiento de las dinámicas de sistemas acoplados de dimensión mayor, exhibiendo **hipercaos** (dinámicas caracterizadas por múltiples exponentes de Lyapunov positivos). Por ejemplo, los esquemas para comunicaciones seguras deberían ser basados en la sincronización de osciladores hipercaóticos, ya que el caos de dimensión menor no es suficientemente complejo para enmascarar u ocultar de manera segura la información.

Un asunto fundamental en la sincronización de osciladores hipercaóticos, es el número de señales de acoplamientos (distintos), necesarias para lograr la sincronía. Rápidamente, se conjeturó que el número de señales de acoplamiento debería ser mayor o igual que el número de exponentes de Lyapunov positivos. Esta conjetura se ha probada que es incorrecta. Estudios teóricos sobre varios osciladores hipercaóticos muestran que es posible obtener estabilidad asintótica de los estados sincronizados, empleando sólo una señal acoplante [Sira y Cruz, 2001].

Encriptado es el proceso de revolver u ocultar el contenido de un mensaje con el propósito de hacer a éste indescifrable a toda persona que no posea la ‘‘clave’’ con la que se llevo a cabo este proceso. El encriptado de información es un problema muy antiguo para el hombre y en la actualidad es un asunto de gran relevancia. Muy recientemente, a partir del logro de la sincronización de sistemas caóticos [Pecora y Carroll 1990], se abre la potencial aplicación de este hecho para construir sistemas de encriptado que sustituyan a los complicados algoritmos convencionales.

Aprovechando las propiedades naturales de los sistemas hipercaóticos (dinámicas más complejas que las caóticas), se plantea primeramente estudiar el problema de encriptado de información a partir de la sincronización de osciladores hipercaóticos hipercaóticos. En particular, se sincronizarán los osciladores por el método de sistemas hamiltonianos [Sira y Cruz, 2001] y, finalmente, se realizará una aplicación a las comunicaciones seguras.

1.2. Planteamiento del problema

La transmisión de imágenes, audio, documentos es simple y cotidiana, sin embargo, los usuarios de los medios de comunicación no se dan cuenta del trabajo que hay antes de que ellos hagan una llamada o que transmitan los datos de su tarjeta de crédito por medio de una página de Internet. La utilización del medio de transmisión, la tecnología que se usa en el enlace y la seguridad del mensaje son esenciales en la actualidad, sin embargo tener la confianza en la tecnología que se usa para mandar cualquier tipo de información se basa en mantenerla segura cuando se transmite remotamente de un lugar a otro, empleando un canal público, es decir, con acceso a cualquier persona. En la figura 1 se muestra un ejemplo de comunicación insegura entre dos terminales remotas.

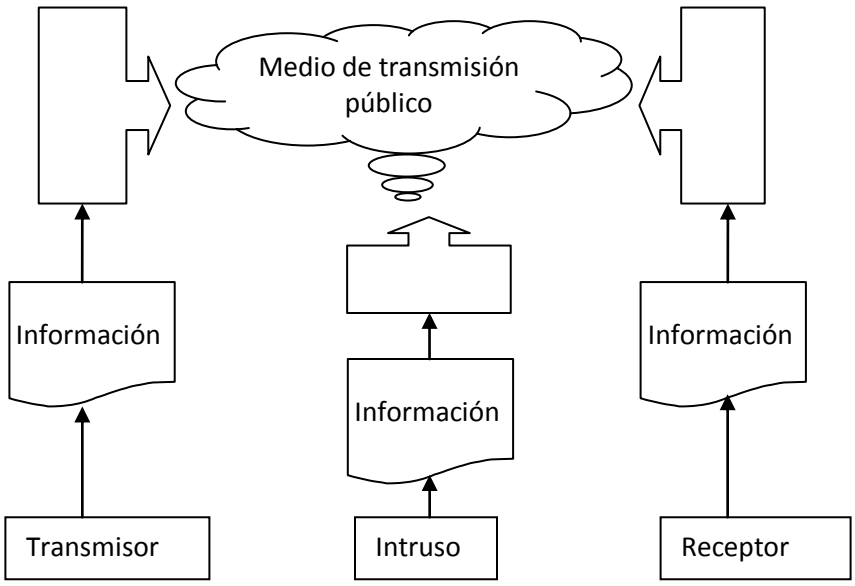

Figura 1. Transmisor y receptor tienen una conversación pero el intruso quiere la información y trata de encontrar la manera de lograr su cometido.

En cambio, si el transmisor desea comunicarse de manera segura con el receptor, es decir, no quiere que otra persona se entere de que información está transmitiendo, entonces encripta la información empleando una clave secreta, de esta manera, la mantiene segura del intruso. Por tanto, el transmisor encriptará la información utilizando la clave y enviará la información encriptada a través del canal público de transmisión al receptor, de esta manera, solamente el receptor que tenga la clave, podrá descifrar la información. Por tanto, si el transmisor tiene la clave (con acceso a la señal que transmite el transmisor al receptor), entonces podrá saber el contenido de la información, con lo cual, el intruso sin la clave no tendrá acceso a dicha información enviada. Este proceso de comunicación segura puede apreciarse en la figura 2.

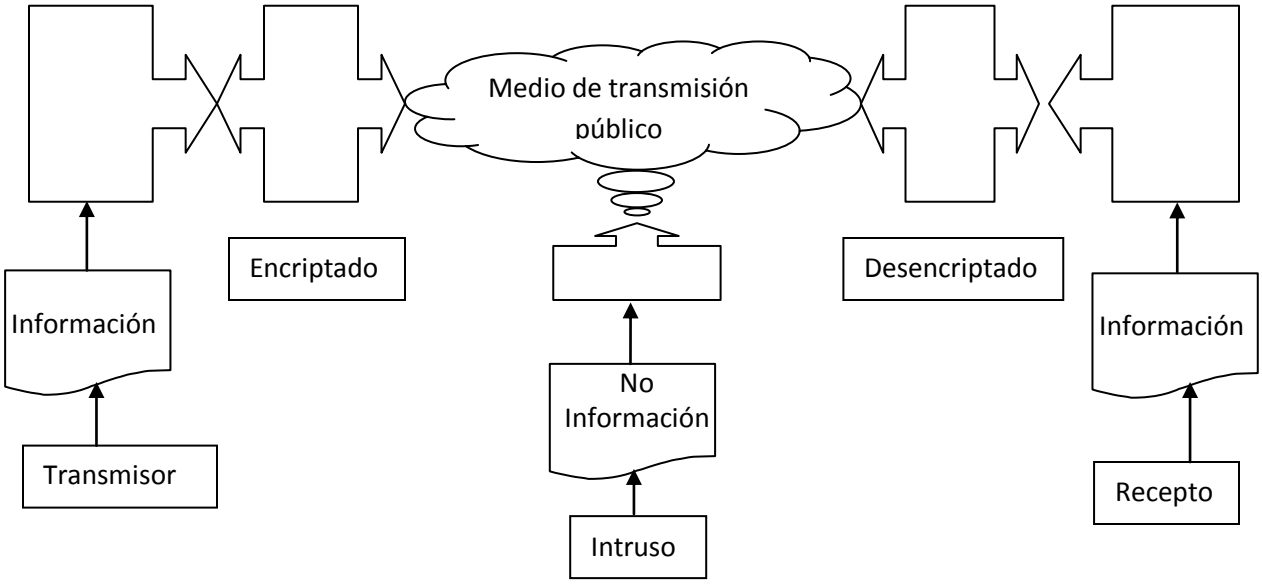

Figura 2. El transmisor y el receptor tienen una conversación pero el intruso quiere la información y trata de encontrar la manera de lograr su cometido pero esta vez no puede ya que no cuenta con el desencriptador.

La propuesta en este trabajo de tesis, es sustituir los algoritmos de encriptado convencionales que utilizan el transmisor y el receptor, por otro medio de encriptado, empleando dinámicas caóticas con el propósito de alcanzar el mismo objetivo, la información no debe ser comprendida por el intruso. El generador hipercaótico (para que sirva de encriptador) que se propone emplear en este sistema de comunicación confidencial es un circuito Chua modificado, el cual, produce atractores caóticos con múltiples enrollamientos.

La técnica de encriptado empleando hipercaos propuesta en este trabajo de tesis, proporcionará como resultado una mayor seguridad en el cifrado de la información confidencial a transmitir, ya sea voz, datos o audio por medio de un canal público. De tal forma, que dicha información únicamente pueda ser comprendida por receptores autorizados, es decir, personas que tengan conocimiento de la clave empleada en el encriptado.

1.3. Objetivos del trabajo de tesis

- Objetivo general

  Simular ecuaciones dinámicas que generan sistema de encriptamiento hipercaótico con el propósito de transmitir información confidencial (analógica y digital) altamente segura.

- Objetivos específicos

  Sincronizar atractores con enrollamientos múltiples: resultados numéricos.
  Transmitir información privada analógica y digital de manera segura: resultados numéricos y experimentales.
  Determinar el ancho en frecuencias de cada estado de la ecuación.
  Caracterizar los estados de la ecuación.

1.4. Metodología adoptada

La comunicación secreta con base en sincronía de atractores caóticos con múltiples enrollamientos se basa en la sincronía de múltiples circuitos de Chua generalizados. De esta manera, esta tesis se adopta el método de sincronización por la forma hamiltoniana generalizada, un diseño de un observador lineal [Díaz E. *et Al.* 2003] y la técnica de Red para Multiusuario que se implementara es el esquema de sincronización por retroalimentación sugerido por [Milanovic y Zaghloul, 1996].

El método de sincronización empleado en este trabajo tiene las siguientes ventajas sobre otros métodos 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 obtener la sincronización.

Para la transmisión de información confidencial, se emplearán distintos métodos de comunicación caótica, por ejemplo [Sira-Ramírez H. y Cruz-Hernández C., 2001], [Arena P. *et al*., 1995], [Mejía C., 2007] y de modulación paramétrica.

La figura 3 muestra un diagrama de bloques de la comunicación que se tendrá entre un transmisor y un receptor aplicando circuitos hipercaóticos para el encriptado y lograr la comunicación segura.

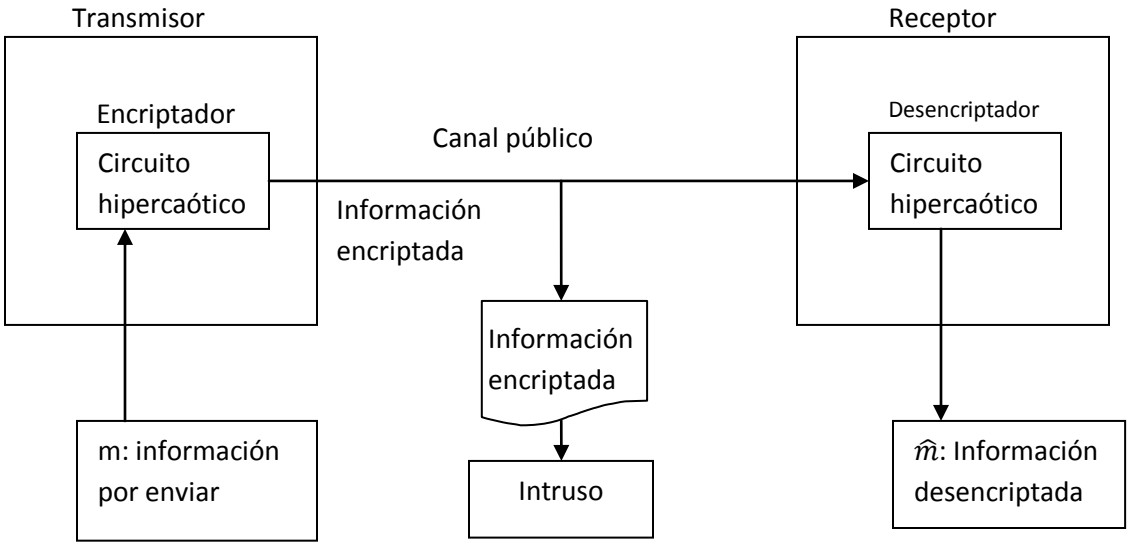

Figura 3. Diagrama de bloques de un sistema de comunicación seguro con encriptado hipercaótico.

1.5. Organización de la memoria

El resto de este documento está organizado de la siguiente manera.

En el capítulo 2, se menciona de manera breve un poco de la historia de la criptografía, objetivos y conceptos básicos de la misma.

El capítulo 3 de esta tesis se desarrollaran los conceptos de sistema caótico, la sincronización, su implementación en la encriptación por caos y la forma hamiltoniana generalizada, la cual, es el método por el cual se logra la sincronización de los sistemas caóticos.

El capitulo 4 trata de la sincronización de las ecuaciones de Chua con atractores caóticos con múltiples enrollamientos. Se implementara la forma hamiltoniana generalizada para el sistema de ecuaciones Chua [Suykens *et al*, 1997] y los resultados de la simulación de la sincronización.

En el apartado 5 mostrara como es el método de sincronización multiusuario, la técnica de Red para Multiusuario que se implementara es el esquema de sincronización por

retroalimentación sugerido por [Milanovic y Zaghloul, 1996] en combinación con el método de sincronización de osciladores caóticos mediante la forma hamiltoniana generalizada y el diseño de un observador no lineal propuesto en [Sira-Ramírez y Cruz-Hernández, 2001]. También se ilustrara con imágenes los resultados de la sincronía.

La sección donde se observaran los resultados de la comunicación con encriptación caótico será la 6, en la cual estarán las imágenes del los tipos de comunicación y el diagrama de bloques de cada esquema.

En la última parte se hablará de las conclusiones generales y el trabajo a futuro, producto de la presente investigación.

Capitulo 2

Cifrado de información

En el capítulo 2 de este trabajo de tesis, se establecerán los conceptos básicos del cifrado de información, así como algunos apuntes históricos y el estado que guarda en la actualidad, y consultar las referencias [Belmonte, *et al*.2006].

2.1. Historia de la criptografía

La humanidad siempre ha tenido la necesidad de ocultar conocimientos, datos, nombres, fechas, acontecimientos, dinero y por supuesto información o comandos bélicos usados en la guerra.

Pero que es la criptografía viene de *krypto*, que significa oculto y *graphos*, escribir, se entiende entonces por **escritura oculta**. En el sentido científico, la criptografía es la ciencia de cifrar y descifrar información mediante técnicas especiales y se emplea frecuentemente

para permitir un intercambio de mensajes que sólo puedan ser entendidos por personas a las que van dirigidos, es decir, que poseen los medios para descifrarlos.

La *criptología* es el estudio de los sistemas criptográficos, que ofrecen medios seguros de comunicación en los que un emisor oculta o cifra un mensaje antes de transmitirlo para que sólo un receptor autorizado pueda descifrarlo. Sus áreas principales de estudio son la criptografía y el criptoanálisis, pero también se incluye la esteganografía como parte de esta ciencia aplicada.

Los primeros hechos históricos de la criptografía datan del tiempo de Julio César el emperador romano. El primer sistema criptografico que se conoce es documentado por el historiador griego Polibio: un sistema de sustitución basado en la posición de las letras en una tabla. Esta técnica y las que le prosiguieron fueron obsoletas con el transcurso del tiempo, pero todas ellas fueron importantes y lograron su objetivo, ocultar la información.

En 1466 Leon Alberti inventó el disco cifrado y la clave criptográfica. El disco de cifrado de Alberti era polialfabético, significando que un nuevo alfabeto podía ser creado cada vez que girara el disco. Este tipo de disco fue el único método de uso de este tipo de cifrado hasta el siglo XVI. Alberti pensó que este cifrado era irrompible. Esta afirmación se baso en sus investigaciones en análisis de frecuencia, el cual es el método más efectivo de descifrado de criptogramas monoalfabéticos. Proporcionando suficiente texto cifrado, se puede usar la frecuencia de las letras en referencia de una distribución normal para encontrar el desplazamiento y resolver el criptograma. Este sistema falló al resolver los criptogramas polialfabéticos. El siguiente ejemplo muestra el funcionamiento del disco para diferentes claves dadas:

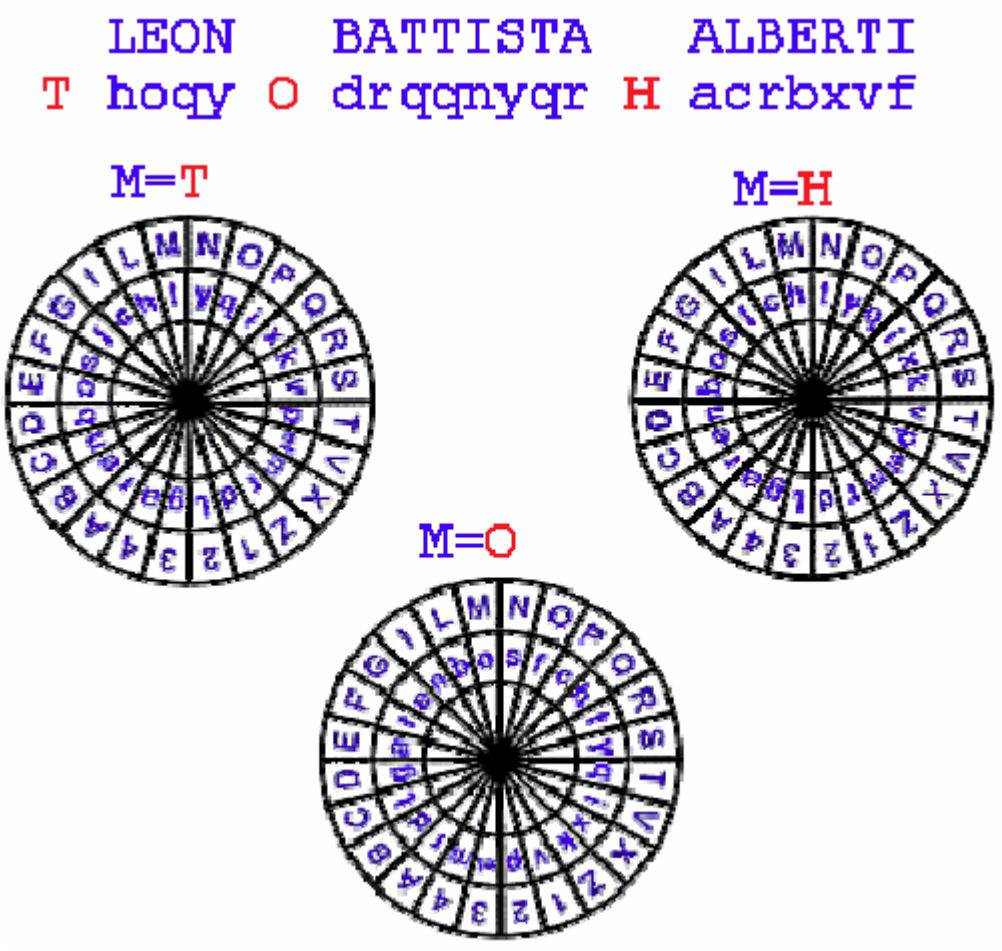

Figura 4. Ejemplo de encriptado mediante el disco inventado por león Alberti.

Una cifrado de nomenclatura desarrollada por Bonaventure Rossignols, nombrado el gran cifrado. Cada número se colocaba por una silaba francesa en vez de las letras simples. El gran cifrado se empleó para encriptar los mensajes más secretos del Rey Luis XIV. De hecho la identidad del Hombre de la Máscara de Hierro se protegió por el gran cifrado. El gran cifrado no se rompió hasta que el comandante Etienne Bazeries fue capaz de tomar los números que se tenían frecuentemente para descifrar una palabra común.

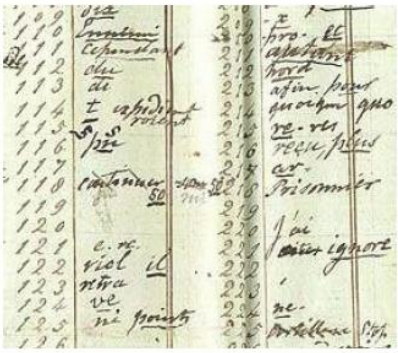

Figura 5. El gran cifrado.

El telegrama Zimmerman daba instrucciones al embajador alemán en México para proponer a este país una alianza en caso de que estallara la guerra entre los Estados Unidos y Alemania, con la promesa de que México recuperaría Texas, Nuevo México y California. Más aun, sugería al presidente Carranza la posibilidad de una alianza con Japón para atacar a los Estados Unidos. Zimmerman tuvo que cifrar su telegrama porque era consciente de que los aliados interceptaban todas sus comunicaciones trasatlánticas. En efecto, el telegrama fue interceptado por los británicos quienes consiguieron descifrarlo completamente, prueba de la supremacía de los criptoanalistas aliados durante la Primera Guerra Mundial.

La máquina enigma, la solución al fracaso en la seguridad de las comunicaciones alemanas durante la Primera Guerra Mundial fue el Enigma, la máquina de cifrado de mensajes más avanzada hasta la llegada de la computadora y la cual supuso un punto de inflexión en la historia de la criptografía.

La máquina Enigma fue inventada por Arthur Scherbius, ingeniero alemán. Básicamente, Enigma era una máquina electromecánica que constaba de los siguientes elementos:

- Un teclado de 26 letras, similar al de una máquina de escribir.
- Un tablero luminoso, formado por 26 bombillas, una para cada letra.
- Una unidad de modificadores o rotores, discos circulares con 26 contactos. Cada uno de estos discos estaba conectado al siguiente mediante un complejo cableado.
- Un clavijero, situado en la parte frontal, de 26 clavijas, cada una de las cuales correspondía a una letra.
- Un reflector.

La rotación del modificador es la característica esencial de la maquina Enigma. Cada vez que se pulsa una letra en el teclado, el primer modificador gira un espacio. El segundo disco modificador permanece inmóvil hasta que el primero realiza una revolución completa, y así sucesivamente con el resto de los modificadores que haya. La corriente eléctrica que transmite el cableado hace que encienda en el tablero luminoso la bombilla correspondiente a la letra ya cifrada.

Figura 6. Máquina enigma.

A pesar de la complejidad interna de la máquina, su manejo era muy sencillo: una vez que el operador dispone la configuración inicial, tecleaba el texto a cifrar y cada vez que una tecla era pulsada se iluminaba su letra equivalente en el texto cifrado. Entonces se apuntan las letras que se iban iluminando y se transmitía el mensaje. La inclusión del reflector permitió que el cifrado y descifrado fuera simétrico, es decir, que la misma clave que se utilizaba para cifrar sirviese para descifrar.

El desciframiento de la Enigma por parte de los aliados supuso un esfuerzo colectivo sin precedentes en la historia. Los criptoanalistas luchaban a diario desde la media noche en que los operadores alemanes cambiaban a la nueva clave del día, los descifradores empezaban de cero.

En la actualidad se usan muchos tipos de encriptación. Ya que hay organizaciones que usan sus propios sistemas de encriptado de información, generalmente estas empresas tienen su fuente principal de trabajo en la seguridad de las páginas web.

2.2. Objetivo de la criptografía

El objetivo de la criptografía es, en primer lugar, garantizar el secreto en la comunicación entre dos entidades (personas, organizaciones, etc.) y, en segundo lugar, asegurar que la información que se envía es auténtica en un doble sentido: que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado, habitualmente denominado criptograma, no haya sido modificado en su tránsito (ver figura 7).

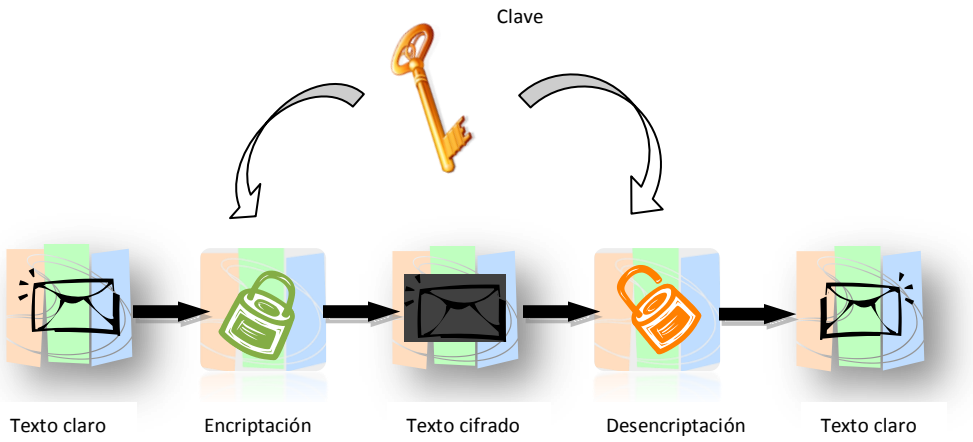

Figura 7. Un documento, pasa por un medio de encriptación, el resultado será un documento encriptado enviado por un medio de transmisión público, después pasa por un proceso de desencriptación y al final tenemos el documento original.

2.3. Conceptos básicos de la criptografía

La información original que debe protegerse se denomina *texto en claro*. El *cifrado* es el proceso de convertir el *texto plano* en un galimatías 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.

Las dos técnicas más sencillas de *cifrado*, en la criptografía clásica, son la *sustitución* (que supone el cambio de significado de los elementos básicos del mensaje -las letras, l0os dígitos o los símbolos-) y la *trasposición* (que supone una reordenación de los mismos); la gran mayoría de las *cifras* clásicas son combinaciones de estas dos operaciones básicas.

El *descifrado* es el proceso inverso que recupera el *texto plano* 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 conjunto 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*, de *clave simétrica* o de *clave privada* y son la base de los algoritmos de cifrado clásico. Los segundos se denominan *cifras asimétricas*, de *clave asimétrica* o de *clave pública* y forman el núcleo de las técnicas de cifrado modernas.

2.3.1. Criptografía asimétrica

La criptografía asimétrica es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es *pública* y se puede entregar a cualquier persona, la otra clave es *privada* y el propietario debe guardarla de modo que nadie tenga acceso a ella (ver figura 8). Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de clave

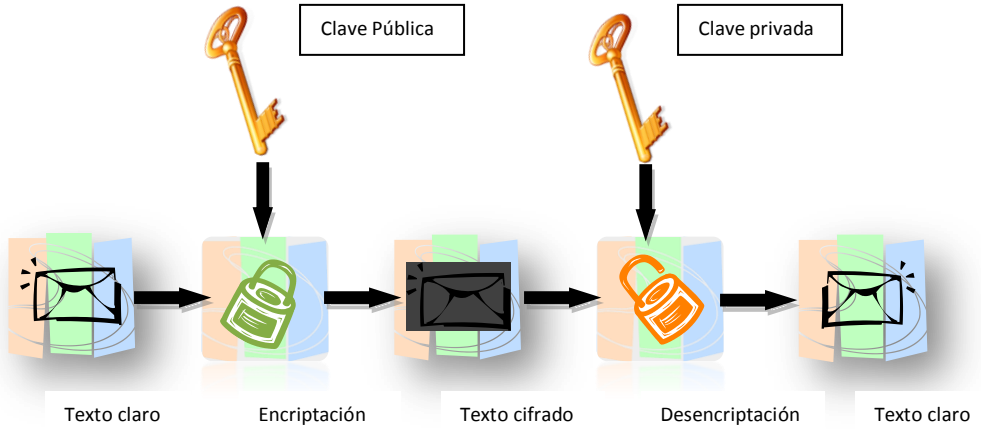

Figura 8. Se observa cómo es la función de la encriptación asimétrica, todos conocen la clave pública, pero solo algunos conocen la clave privada.

Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la *confidencialidad* del envío del mensaje, nadie salvo el destinatario puede descifrarlo.

Si el propietario del par de claves usa su clave privada para cifrar el mensaje, cualquiera puede descifrarlo utilizando su clave pública. En este caso se consigue por tanto la *identificación* y *autenticación* del remitente, ya que se sabe que sólo pudo haber sido él quien utilizó su clave privada (salvo que alguien se la hubiese podido robar). Esta idea es el fundamento de la firma electrónica.

Los sistemas de cifrado de clave pública o sistemas de cifrado asimétricos se inventaron con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos. Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear. Todo lo que se requiere es que, antes de iniciar la comunicación secreta, el remitente consiga una copia de la clave pública del destinatario. Es más, esa misma clave pública puede ser usada por cualquiera que desee

comunicarse con su propietario. Por tanto, se necesitarán sólo **n** pares de claves por cada **n** personas que deseen comunicarse entre sí.

Como con los sistemas de cifrado simétricos buenos, con un buen sistema de cifrado de clave pública toda la seguridad descansa en la clave y no en el algoritmo. Por lo tanto el tamaño de la clave es una medida de la seguridad del sistema, pero no se puede comparar el tamaño del cifrado simétrico con el del cifrado de clave pública para medir la seguridad. En un ataque de fuerza bruta sobre un cifrado simétrico con una clave de un tamaño de 80 bits, el atacante debe probar hasta 2^{80}-1 claves para encontrar la clave correcta. En un ataque de fuerza bruta sobre un cifrado de clave pública con una clave de un tamaño de 512 bits, el atacante debe factorizar un número compuesto codificado en 512 bits (hasta 155 dígitos decimales).

La cantidad de trabajo para el atacante será diferente dependiendo del cifrado que esté atacando. Mientras 128 bits son suficientes para cifrados simétricos, dada la tecnología de factorización de hoy en día, se recomienda el uso de claves públicas de 1024 bits para la mayoría de los casos.

La mayor ventaja de la criptografía asimétrica es que se puede cifrar con una clave y descifrar con la otra, pero este sistema tiene bastantes desventajas:

- Para una misma longitud de clave y mensaje se necesita mayor tiempo de proceso.
- Las claves deben ser de mayor tamaño que las simétricas.
- El mensaje cifrado ocupa más espacio que el original.

Herramientas como PGP (Pretty Good Privacy), SSH (Secure SHell) o la capa de seguridad SSL (Secure Sockets Layer) para la jerarquía de protocolos TCP/IP (Protocolo de Control de Transmisión/Protocolo de Internet) utilizan un híbrido formado por la criptografía asimétrica para intercambiar claves de criptografía simétrica, y la criptografía simétrica para la transmisión de la información.

2.3.2. Criptografía simétrica

La criptografía simétrica es el método criptográfico que usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma (ver figura 7).

Un buen sistema de cifrado pone toda la seguridad en la clave y ninguna en el algoritmo. En otras palabras, *no debería ser de ninguna ayuda para un atacante conocer el algoritmo que se está usando*.

Dado que toda la seguridad está en la clave, es importante que sea muy difícil adivinar el tipo de clave. Esto quiere decir que el abanico de claves posibles, o sea, el espacio de posibilidades de claves, debe ser amplio.

Actualmente, los ordenadores pueden descifrar claves con extrema rapidez, y ésta es la razón por la cual el tamaño de la clave es importante en los criptosistemas modernos. El algoritmo de cifrado DES (Data Encryption Standard) usa una clave de 56 bits, lo que significa que hay 2 elevado a 56 claves posibles (72.057.594.037.927.936 claves). Esto representa un número muy alto de claves, pero una máquina computadora de uso general puede comprobar el conjunto posible de claves en cuestión de días. Una máquina especializada puede hacerlo en horas. Algoritmos de cifrado de diseño más reciente como TDES (Triple Data Encryption Standard), ASD (Advanced Encryption Standard), Blowfish e IDEA (International Data Encryption Algorithm) usan claves de 128 bits, lo que significa que existen 2 elevado a 128 claves posibles, con excepción de ASD que usa claves de mínimo 128, 192 y 256.

El principal problema con los sistemas de cifrado simétrico no está ligado a su seguridad, sino al intercambio de claves. Una vez que el remitente y el destinatario hayan intercambiado las claves pueden usarlas para comunicarse con seguridad, pero ¿qué canal de comunicación que sea seguro han usado para transmitirse las claves? Sería mucho más fácil para un atacante intentar interceptar una clave que probar las posibles combinaciones del espacio de claves.

Otro problema es el número de claves que se necesitan. Si tenemos un número **n** de personas que necesitan comunicarse entre sí, se necesitan **n/2** claves para cada pareja de personas que tengan que comunicarse de modo privado. Esto puede funcionar con un grupo reducido de personas, pero sería imposible llevarlo a cabo con grupos más grandes.

Un algoritmo de encriptación simétrica no convencional fue propuesto por [Pecora y Carroll, 1990] este trataba con la sincronización de sistemas caóticos, utilizando sistemas de ecuaciones diferenciales que reproduzcan un comportamiento caótico. La cual consiste en encriptar información confidencial por medio de una dinámica compleja de un sistema caótico en el transmisor. Mientras que la información se puede desencriptar mediante el sistema caótico que se encuentra en el receptor, donde este está sincronizado con el sistema caótico del transmisor. Este procedimiento de cifrado se hace en caos, se explicara en el siguiente capítulo.

Capitulo 3

Sistema caótico, Chua normal (3 estados) y teoría Chua 6

En este capítulo se presentan conceptos, definiciones, historia y aplicaciones de los sistemas caóticos.

3.1. Historia del caos

El concepto de **caos** es ambiguo, ha tenido muchas definiciones que se mostraran a continuación. Una de las primeras civilizaciones la griega definía al Caos o Khaos como 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'. También, para los antiguos astrólogos era la primara cosa que existió y la matriz de la cual surgió todo. Se puede observar a los filósofos como Heraclido y Aristóteles, que el caos es la primera fundación de la realidad y que debía haber pensado en el caos cuando desarrollo el concepto de Prima Materia en su intento por combinar a platón con los presocráticos y los naturalistas.

Hasta tiempos recientes se asumía que era posible hacer una predicción precisa de cualquier sistema físico si se conocían bien las condiciones iniciales y el modelo matemático. El descubrimiento de los sistemas caóticos en la naturaleza, algunas décadas atrás, ha modificado completamente esa idea.

Hay que conocer un concepto muy importante, el **determinismo**. El cuál es la creencia filosófica que cada evento o acción es el resultado inevitable de eventos o acciones precedentes.

Un ejemplo son las leyes de Newton, las cuales son completamente determinísticas. Claro está, estas leyes se expresan en términos numéricos no solo en palabras, es decir por ecuaciones matemáticas. Para saber el comportamiento de un objeto gobernado por dichas leyes se requiere tomar una referencia, es decir medidas tomadas en un tiempo inicial, a las cuales se les llama **condiciones iniciales**.

En el año de 1900, Henri Poincaré quien se interesaba en las ecuaciones que describían el movimiento de los planetas alrededor del sol (que son una aplicación de las leyes de Newton), se percató que no todos los sistemas físicos obedecían la idea que si se aumentaba la precisión en las condiciones iniciales, se disminuiría la incertidumbre en las predicciones. Poincaré mostró que una mínima imprecisión en las condiciones iniciales cambiaría enormemente el resultado al transcurrir el tiempo. El análisis matemático de Poincaré fue una prueba de que para esos sistemas complejos, la única manera de obtener predicciones con un grado de precisión, supondría especificar las condiciones iniciales con precisión absoluta. La extrema sensibilidad a las condiciones iniciales presente en los sistemas estudiados por Poincaré se ha venido llamando inestabilidad dinámica o simplemente caos.

No fue sino hasta principios de la década de los sesenta cuando se produjo un descubrimiento muy importante. En 1963 un investigador llamado Edward Lorenz desarrollaba un programa de software matemático para estudiar un modelo simplificado para pronosticar el clima. El código del programa contenía las ecuaciones diferenciales que modelaban el flujo de las corrientes de aire. Como el código del programa es completamente determinístico, Lorenz pensaba que al poner las mismas condiciones iniciales el resultado sería idéntico. Sin embargo, Lorenz se sorprendió al encontrar que, cuando él creía poner las mismas condiciones iniciales, el resultado cambiaba drásticamente cada vez que corría el programa. Entonces al examinar más de cerca lo que había hecho, se dio cuenta que las condiciones iniciales que ponía en el código del programa variaban ligeramente unas de otras, de hecho se consideraban microscópicas e insignificantes por los estándares comunes. La figura 9 muestra la evolución del modelo

al transcurrir el tiempo para dos condiciones iniciales distintas para una simplificación de este programa.

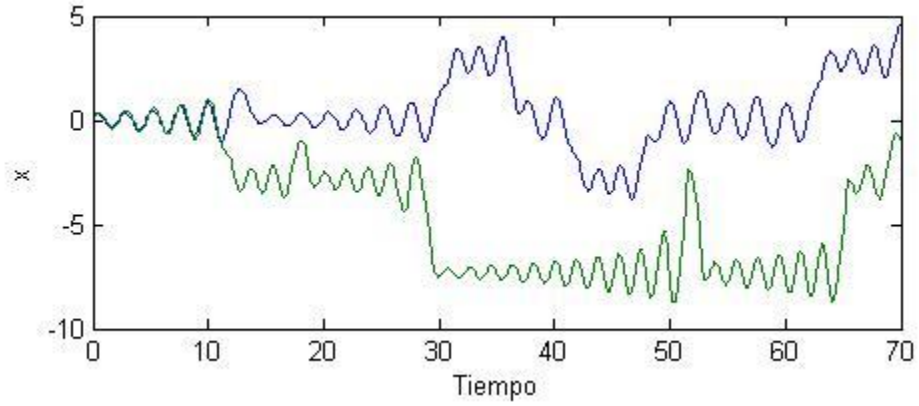

Figura 9. Gráfica del modelo de Chua, con dos conjuntos de condiciones iniciales muy próximas, dando dinámicas completamente distintas.

Con el tiempo y estudio de este sistema y otros "semejantes", se llegó a la conclusión de que hay sistemas no lineales determinísticos que tienen un comportamiento aparentemente estocástico. En este caso, el modelo de Lorenz indicaba una característica notable de un sistema caótico [Trump Matthew A, 2009].

3.2. Conceptos, definición y propiedades del caos

Aunque es difícil dar una definición formal y exacta de caos, hay algunas características aceptadas que describen el comportamiento de los sistemas dinámicos caóticos. En este documento, más que proporcionar una definición formal de tales características, se considera preferible entender lo que su presencia implica en el comportamiento de un sistema dinámico. Por lo anterior, de manera general se puede definir a un sistema caótico como un sistema determinístico, regido por ecuaciones diferenciales ordinarias o en diferencias no lineales, que presenta un comportamiento dinámico aparentemente aleatorio y sensible a condiciones iniciales [Aguilar-Bustos Ana, 2005].

Sus características principales son:

- **Dinámica no lineal.** El caos es un fenómeno exclusivo de los sistemas dinámicos no lineales. Un sistema lineal, sin importar el orden que tenga, no puede presentar este comportamiento.

- **Espectro amplio de frecuencia**. En el dominio de la frecuencia, una señal caótica presenta un espectro continuo, muy parecido al ruido estocástico, pero con pico en las frecuencias dominantes.

- **Sensibilidad extrema a condiciones iniciales.** A partir de condiciones iniciales diferentes, aunque muy cercanas unas de otras, las trayectorias correspondientes que se producen tienden a ser distintas o divergen exponencialmente conforme el tiempo transcurre, sin existir correlación alguna entre dichas trayectorias. Esto se puede observar de una mejor manera en la figura 9 en donde las condiciones iniciales son muy cercanas pero las trayectorias varían exponencialmente al pasar el tiempo.

- **Presencia de atractores extraños.** Teniendo dos trayectorias que parten muy próximas en el espacio de fases, divergen rápidamente alejándose cada vez mas. Con esto, se forman atractores extraños los cuales tienen una estructura muy complicada, que reflejan dos tendencias opuestas: al tratarse de un atractor, las trayectorias deben converger hacia él, pero por tratarse de un caso de sensibilidad a las condiciones iniciales, las trayectorias deben, al mismo tiempo, divergen distanciándose cada vez mas. Para concebir estas figuras es necesario salir de la geometría de Euclides, donde las dimensiones son números enteros, para dar cabida a formas irregulares y fragmentadas. A estas dimensiones el matemático Benoit Mandelbrot las llamo fractales.

- **Exponentes de Lyapunov positivos.** Los exponentes de Lyapunov podría decirse que dan una medida de la expansión exponencial, en la cual, órbitas cercanas se van apartando o acercando. En algún sentido, determinan la complejidad de un sistema no lineal. Se dice que el sistema es caótico, si el sistema tiene al menos un exponente de Lyapunov positivo.

3.3. Ejemplos de caos

Se pueden comentar muchos ejemplos de sistemas caóticos, en este caso se mostraran solo un par de ellos.

- Biología moderna

La biología ha alcanzado notables avances en la aplicación del caos a tejidos biológicos. Estos trabajos los desarrollan a partir de investigaciones de biología experimental y teórica basada en biofísica y biomatemática, tratando modelos caóticos de sistemas vivos.

El estudio de la filosofía celular y de la neurología es encarado también desde el punto de vista físico y químico como sistemas dinámicos. Se sabe hoy, que le

comportamiento de las redes neuronales puede dar lugar a conductas cíclicas estables o a conductas caóticas.

- Astronomía

Los astrónomos han observado ciertos tipos de inestabilidades que ocurren por todo el sistema solar, en los movimientos del Hiperión lunar de saturno, en huecos en el cinturón de asteroides entre Marte y Júpiter y en las órbitas de los planetas del sistema. Un objeto que se comporta de manera caótica puede tener, por ejemplo, una excentricidad orbital que varia cíclicamente dentro de ciertos límites para miles o hasta millones de años, y luego repentinamente su patrón de variación cambia. El resultado es una ruptura aguda en la historia del objeto, así su comportamiento del pasado, ya no dice nada sobre su comportamiento futuro.

Pero que se pueden lograr con los sistemas caóticos, si se conoce el comportamiento de estos procesos generaran una concepción del los problemas desde un ángulo totalmente distinto. En el caso particular de esta tesis es la encriptación de información por canales de comunicación. En el capítulo 6 se hablaran de cómo es posible dicha encriptación.

3.4. Circuito Chua normal (3 estados)

Actualmente hay muchos sistemas no lineales que generan caos [Sira-Ramírez H. y Cruz-Hernández C., 2001] los cuales pueden ser utilizados para el encriptado de información de manera segura.

Hablando estrictamente de un circuito eléctrico (sin entradas), que pueda tener un comportamiento caótico, debe ser construido con resistencias, inductores y capacitores, este debe contener: *a) al menos un elemento no lineal, b) mínimo un resistor locamente activo y c) al menos 3 elementos almacenadores de energía*. Ver figura 10.

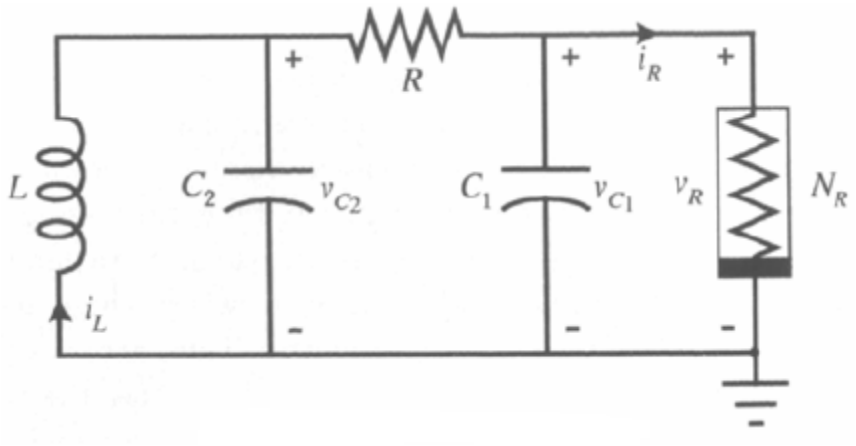

Figura 10. Circuito de Chua.

Uno de los más estudiados es el circuito Chua ya que es uno de los sistemas físicos para el cual la presencia de caos ha sido establecida experimentalmente, confirmada numéricamente y probada matemáticamente [Madan N. R., 1993].

El circuito de Chua consta de solo cuatro elementos lineales (un resistor R, un inductor L, dos capacitares C1 y C2) y un elemento no lineal (el llamado diodo de Chua NR).

La resistencia no lineal NR, también llamada diodo Chua, tiene una característica v-i que es lineal por secciones, como se observa en la figura 11

. Las tres zonas lineales confirman una función no lineal suave.

3.4.1. Ecuaciones de estado del circuito Chua

Se dedujeron las siguientes ecuaciones diferencias, por medio de las leyes de Kirchhoff, que modelan el comportamiento dinámico del circuito de Chua [Madan N. R., 1993]:

$$\begin{aligned}\frac{dv_{C_1}}{dt} &= \frac{1}{RC_1}\left(v_{C_2} - v_{C_1}\right) - \frac{1}{C_1} f\left(v_{c_1}\right), \\ \frac{dv_{C_2}}{dt} &= \frac{1}{RC_2}\left(v_{C_1} - v_{C_2}\right) - \frac{1}{C_2} i_L, \\ \frac{di_L}{dt} &= -\frac{1}{L} v_{C_2}\end{aligned} \tag{1}$$

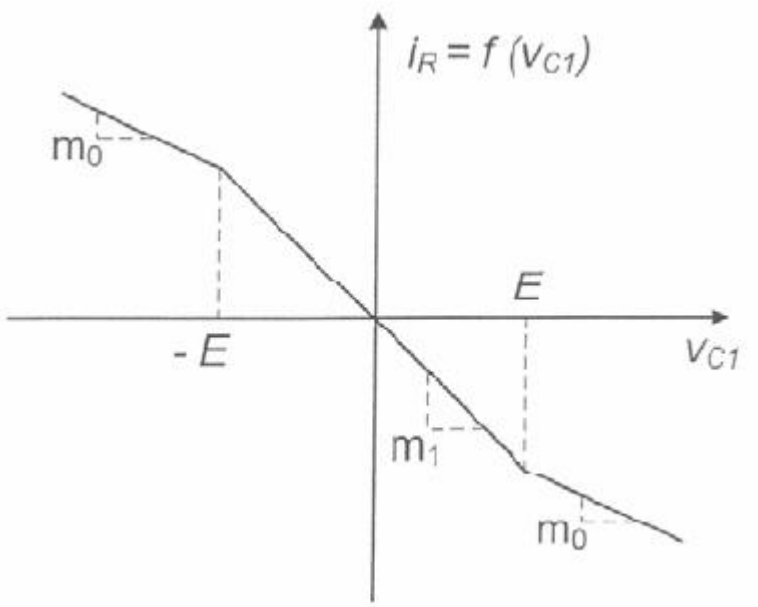

Figura 11. Característica v-i de tres segmentos lineales de la resistencia no lineal NR del circuito de Chua. Las regiones externas tienen pendiente m0; la región interna tiene pendiente m1. Los puntos de quiebre se encuentran dados por ±E.

donde $v_{C_1}(t)\ y\ v_{C_2}(t)$ son los voltajes a través de los capacitores $C_1\ y\ C_2$, respectivamente. $i(t)$ es la intensidad de corriente a través del inductor L y donde la siguiente función no lineal

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

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 12).

3.4.2. Ecuaciones normalizadas del circuito de Chua

Se transformara el modelo matemático del circuito Chua (1) y (2) en un conjunto de ecuaciones adimensionales (normalizadas) mediante el siguiente cambio de variables:

$$\begin{aligned} &x_1 \triangleq \frac{v_{C_1}}{E}, x_2 \triangleq \frac{v_{C_2}}{E}, x_3 \triangleq i_L\left(\frac{R}{E}\right), \\ &\alpha \triangleq \frac{C_2}{C_1}, \beta \triangleq \frac{R^2 C_2}{L}, \\ &a \triangleq Rm_0, b \triangleq Rm_1 \end{aligned} \tag{3}$$

escalando el tiempo

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

y definiendo las variables:

$$\dot{x}_1 = \frac{dx_1}{d\tau}, \dot{x}_2 = \frac{dx_2}{d\tau}, \dot{x}_3 = \frac{dx_3}{d\tau} \tag{4}$$

donde *E* es el voltaje de ruptura de la parte no lineal del diodo de Chua (ver figura 12), el cual, se fijara a un valor de 1. Por lo tanto, las **ecuaciones adimencionales** o **normalizadas** del circuito de Chua son:

$$\begin{aligned} \dot{x}_1 &= \alpha\{x_2 - x_1 - f(x_1)\}, \\ \dot{x}_2 &= x_1 - x_2 + x_3, \\ \dot{x}_3 &= -\beta x_2, \end{aligned} \tag{5}$$

$f(x_1)$ es una función no lineal y está definida por:

$$f(x_1) = bx_1 + \frac{1}{2}(a-b)(|x_1+1| - |x_1-1|). \tag{6}$$

3.5. Circuito de Chua de 6 estados

Para este trabajo de tesis se utilizo unas ecuaciones de un circuito de Chua modificado tomado de [Suykens *et al*, 1997], el cual es de un sistema hipercaótico con doble atractor, esto quiere decir que es un sistema donde los atractores se pueden aumentar o disminuir dependiendo de la ecuación $f(x_1)$.

El sistema de ecuaciones del circuito Chua modificado tiene una diferencia respecto al mostrado en (5), la cual se encuentra en la primera ecuación y es la eliminación de x_1, en las otras dos ecuaciones son idénticos.

$$\begin{aligned} \dot{x}_1 &= \alpha\{x_2 - f(x_1)\}, \\ \dot{x}_2 &= x_1 - x_2 + x_3, \\ \dot{x}_3 &= -\beta x_2. \end{aligned} \tag{7}$$

Las ecuaciones que se encuentran en un estado caótico son susceptibles al mínimo cambio de uno de sus parámetros, por eso estos dos sistemas de ecuaciones (5) y (7) son muy diferentes entre sí, para demostrar esto se simularan los dos sistemas caóticos. El sistema de 6 estados que se utiliza en esta tesis es un arreglo especial de dos circuitos Chua modificados:

$$\begin{aligned} \dot{x}_1 &= \alpha\{x_2 - f(x_1)\}, \\ \dot{x}_2 &= x_1 - x_2 + x_3, \\ \dot{x}_3 &= -\beta x_2, \\ \dot{x}_4 &= \alpha\{x_5 - f(x_4)\} + K(x_4 - x_1), \\ \dot{x}_5 &= x_4 - x_5 + x_6, \\ \dot{x}_6 &= -\beta x_5. \end{aligned} \tag{8}$$

la unión de estos dos sistemas de ecuaciones se logra mediante un acoplamiento unidireccional $K(x_4 - x_1)$ con K=0.01.

En la simulación numérica se observa la diferencia entre cada uno de los 3 circuitos de Chua.

3.5.1. Simulación numérica de las ecuaciones de Chua normal, modificado y de 6 estados

Para observar el comportamiento dinámico del circuito de Chua (5), se realizaron simulaciones numéricas, utilizando el modelo normalizado con valores de los parámetros:

$$\alpha = 10, \beta = 19, a = -1.758 \; y \; b = -0.8248 \; .$$

Las condiciones iniciales son $x_1 = 1.1, x_2 = 0.1 \; y \; x_3 = -0.5$. La figura 12 ilustra como es el comportamiento de los estados caóticos del circuito Chua (5).

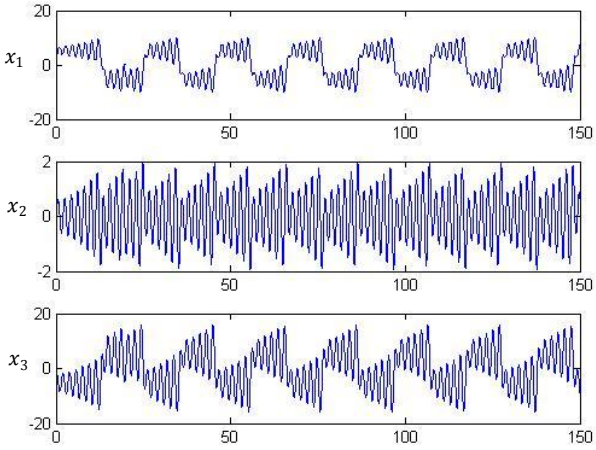

Figura 12. Estados caóticos respecto el tiempo del circuito Chua (5) x_1, x_2 y x_3.

La imagen 13 muestra como son los atractores caóticos formados por la ecuación (5). La cual es la típica imagen de los atractores Chua.

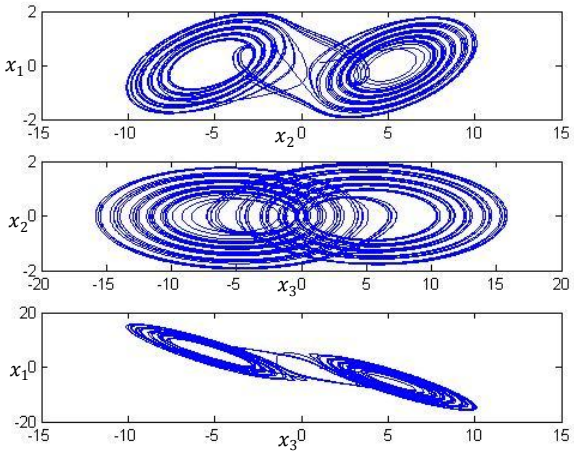

Figura 13. Estado de fase de los estados caóticos (x_1, x_2), (x_2, x_3) y (x_1, x_3)

El circuito de Chua modificado (7) tiene el siguiente comportamiento, el cual es totalmente diferente al resultado mostrado en las figuras 12 y 13, con valores de los parámetros:

$$\alpha = 9, \beta = 14.286, a = -1/7 \; y \; b = 2/7 \, .$$

Las condiciones iniciales son $x_1 = 1.1, x_2 = 0.1 \; y \; x_3 = -0.5$. La figura 14 ilustra como es el comportamiento de los estados caóticos del circuito Chua modificado.

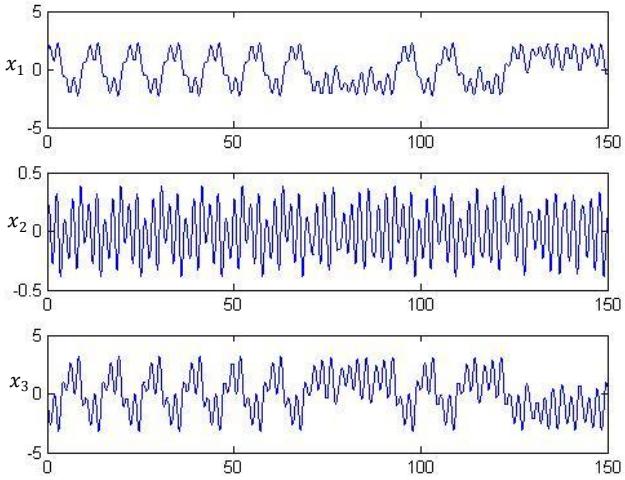

Figura 14. Estados caóticos respecto el tiempo del circuito Chua modificado (7) x_1, x_2 y x_3.

La figura 15 define el estado de fase de los estados caóticos de circuito Chua modificado (7).

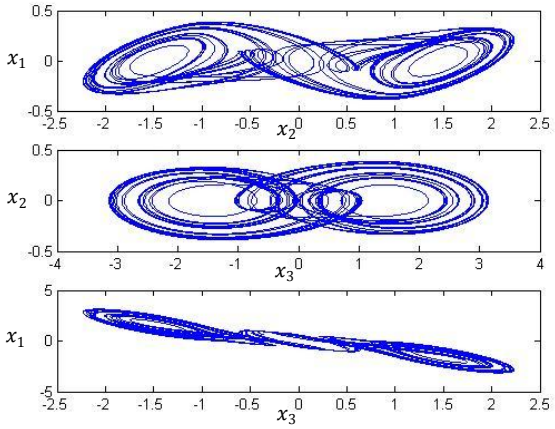

Figura 15. Estado de fase de los estados caóticos (x_1, x_2), (x_2, x_3) y (x_1, x_3).

El circuito de Chua modificado de 6 estados (8) tiene el siguiente comportamiento, el cual es totalmente igual al resultado mostrado en las figuras 14 y 15, con valores de los parámetros:

$$\alpha = 9, \beta = 14.286, a = -1/7 \; y \; b = 2/7 \, .$$

Las condiciones iniciales son $x_1 = 1.1, x_2 = 0.1, x_3 = -0.5, x_4 = 1.1, x_5 = 0.1 \; y \; x_6 = -0.5$. La figura 16 ilustra como es el comportamiento de los estados caóticos del circuito Chua modificado. Aunque son iguales este circuito puede ser modificado para poder hacer más atractores por medio de (6) esta modificación se mostrara en el capítulo 5.

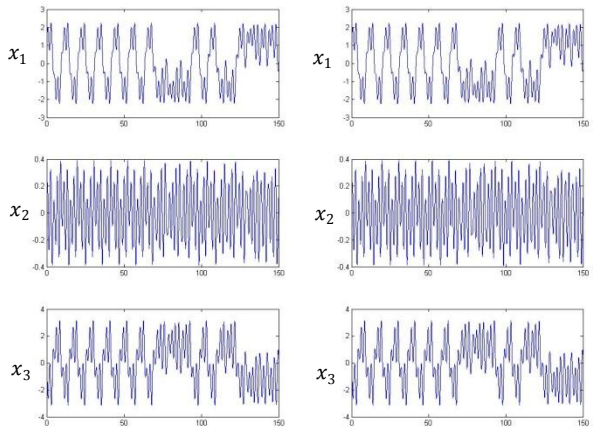

Figura 16. Estados caóticos respecto el tiempo del circuito Chua modificado de 6 estados (8) $x_1, x_2, x_{3,} x_{4,} x_5$, y x_6.

La figura 17 define el estado de fase de los estados caóticos de circuito Chua modificado de 6 estados (8).

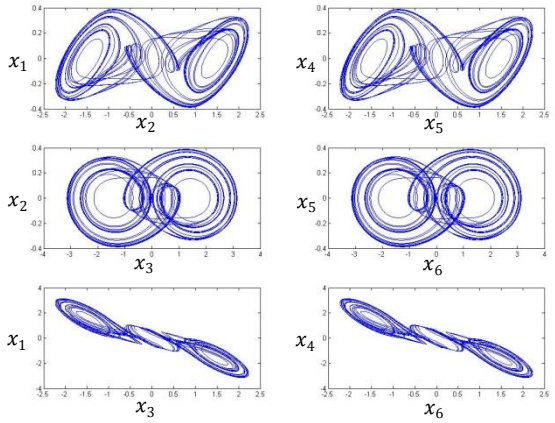

Figura 17. Estado de fase de los estados caóticos (x_1, x_2), (x_2, x_3), (x_1, x_3),(x_4, x_5), (x_5, x_6) y (x_4, x_6).

Capitulo 4

Sincronización

Se proporcionara el concepto de sincronía y se mostrará el método de sincronización, de sistemas caóticos por la forma hamiltoniana generalizada y el diseño de un observador reportado en [Sira-Ramírez y Cruz-Hernández, 2001].

4.1.1. Sincronía de sistemas

El término **sincronía** proviene de la etimología griega *syn*, "con, juntamente, a la vez" y de la mitología griega, *Chronos* o *Khronos* (en griego *Χρόνος*), "tiempo". En latín *Chronus*. Se entiende como un término que se refiere a coincidencia en el tiempo o simultaneidad de hechos o fenómenos.

Aunque en esta tesis se hablara mucho acerca de la sincronía entre dos o más ecuaciones caóticas Chua con atractores caóticos con múltiples enrollamientos, debemos entender que la sincronía no es única en estas teorías si no que en cualquier campo es inevitable hablar de la relación de sincronía como en psicología, comportamiento de masas, en economía como son los comportamientos de la bolsa de valores de un país y otro, así en

física se encuentra también en la mecánica y las máquinas como sincronismo, disposición especial por medio de la cual todos los movimientos de una máquina cualquiera se transmiten con completa exactitud y se verifican en el mismo momento en otras máquinas semejantes a la primera; el sincronismo puede establecerse por medios mecánicos. El ejemplo de uso y explicación más evidente es el mecanismo de los relojes (mecánicos sobre todo).

4.1.2. Sincronía de ecuaciones caótico

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

La teoría del caos resulto ser una herramienta con aplicaciones a muchos campos de la ciencia y la tecnología. Gracias a estas aplicaciones el nombre se torna paradójico, dado que muchas de las prácticas que se realizan con la matemática caótica tienen resultados concretos porque los sistemas que se estudian están basados estrictamente con leyes deterministas aplicadas a sistemas dinámicos.

La teoría del caos ya no es en sí una teoría: tiene postulados, fórmulas y parámetros recientemente establecidos con aplicaciones, por ejemplo, en las áreas de la meteorología o la física cuántica, y actualmente hay varios ejemplos de aplicación en la arquitectura a través de los fractales. En el caso de esta tesis el enfoque es estrictamente la simulación de la encriptación de información atreves de un canal inseguro utilizando un encriptado caótico con Atractores de múltiples enrollamientos.

Una manera de visualizar el movimiento caótico, o cualquier tipo de movimiento, es hacer un diagrama de fases del movimiento. En tal diagrama el tiempo es implícito y cada eje representa una dimensión del estado.

Algunas veces el movimiento representado con estos diagramas de fases no muestra una trayectoria bien definida, sino que ésta se encuentra errada alrededor de algún movimiento bien definido. Cuando esto sucede se dice que el sistema es atraído hacia un tipo de movimiento, es decir, que hay un atractor.

De acuerdo a la forma en que sus trayectorias evolucionen, los atractores pueden ser clasificados como periódicos, cuasi-periódicos y extraños. Estos nombres se relacionan exactamente con el tipo de movimiento que provocan en los sistemas. Para los sistemas caóticos sus atractores se identifican como extraños.

Una de las propiedades más importantes asociadas con el caos, es la sensibilidad a las condiciones iníciales. 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 iníciales idénticas. Incluso una desviación infinitesimal en los parámetros o en las condiciones iníciales, eventualmente dará lugar a la divergencia de trayectorias.

4.1.3. Métodos de sincronización de sistemas caóticos

En los trabajos Fujisaka y Yamada [1983] y en Pecora y Carroll [1990] se demostró tanto téorica como experimentalmente la sincronía de sistemas caóticos. En la literatura se reportan diferentes métodos sistemas compensados como scheweizer y colaboradores en [Scheweizer *et al.* 1995], donde se emplea una especie de observador, mientras que Kapitaniak y colaboradores 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 la forma hamiltoniana generalizadas 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 López-Mancilla 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 explicara con amplitud este método basado en la forma hamiltoniana generalizada y el diseño de un observador no lineal.

4.2. Sincronización de sistemas caóticos

Considere el siguiente sistema dinámico, definido por

$$\dot{x} = f(x), \qquad x \in \mathbb{R}^n. \tag{9}$$

El cual representa un sistema que exhibe un comportamiento caótico, donde $x(t) = \big(x_1(t), \dots, x_n(t)\big)^T \in \mathbb{R}^n$ 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 (9), pueden ser reescritos en la siguiente *forma canoníca hamiltoniana generalizada*,

$$\dot{x} = \Im(x)\frac{\partial H}{\partial x} + S(x)\frac{\partial H}{\partial x} + F(x), \qquad x \in \mathbb{R}^n, \tag{10}$$

donde H es una función de energía suave definida positiva globalmente. El vector gradiente de H, representado por $\partial H/\partial x$ se considera que existe en cualquier parte. Frecuentemente utilizamos funciones de energía cuadrática de la forma $H(x) = 1/2(x^T M x)$, con M siendo una matriz constante, definida positiva y simétrica, donde $\frac{\partial H}{\partial x} = Mx$. Las matrices cuadradas $\Im(x)\ y\ S(x)$ mencionadas en la expresión (10), satisfacen para toda $x \in \mathbb{R}^n$, las siguientes propiedades:

$$\mathfrak{J}(x) + \mathfrak{J}^T(x) = 0,$$

$$S(x) = S^T(x).$$

El campo vectorial $\mathfrak{J}(x)\partial H/\partial x$ representa la parte **conservativa** del sistema. En lo que respecta al campo vectorial $S(x)\partial H/\partial x$, nos describe la parte **no conservativa** del sistema. En algunos casos, la matriz $S(x)$ es definida negativa o semidefinida negativa. En tales casos, el campo vectorial $\mathfrak{J}(x)\partial H/\partial x$ representa la parte **disipativa** del sistema. Si por el contrario, $S(x)$ es definida positiva, semidefinida positiva o indefinida, éste 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 $\mathfrak{R}(x)$ y una matriz simétrica semidefinida positiva $\aleph(x)$. Por último, $F(x)$ representa el campo vectorial **localmente desestabilizante**.

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

En el contexto de diseño de observador, es considerada una clase especial de la forma hamiltoniana generalizada con campo vectorial desestabilizante y un mapeo lineal de salida $y(t)$, expresada como sigue

$$\dot{x} = \mathfrak{J}(y)\frac{\partial H}{\partial x} + (I + S)\frac{\partial H}{\partial x} + F(y), \qquad x \in \mathbb{R}^n, \tag{11}$$

$$y = C\frac{\partial H}{\partial x}, \quad y \in \mathbb{R}^m$$

donde S es una matriz simétrica constante, no necesariamente de signo definido, I es una matriz constante antisimétrica. C es una matriz constante.

Para el diseño de un observador para la forma (11), se define el vector de estado estimado $x(t)$ 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 (3) se obtiene de la siguiente manera

$$\dot{\xi} = \Im(y)\frac{\partial H}{\partial \xi} + (I+S)\frac{\partial H}{\partial \xi} + F(y) + K(y-\eta), \qquad \xi \in \mathbb{R}^n, \tag{12}$$

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

donde $K = (k_1, k_2, \dots, k_n)^T$ es un vector constante conocido como la **ganancia del observador**. En el contexto de sincronización, el observador (12) **realizará el papel de oscilador esclavo**. Cuya función será estimar (reproducir) las dinámicas completas del sistema maestro (11).

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

$$\dot{e} = \Im(y)\frac{\partial H}{\partial e} + (I+S-KC)\frac{\partial H}{\partial e}, \qquad e \in \mathbb{R}^n,$$
$$e_y = C\frac{\partial H}{\partial e}, \quad e_y \in \mathbb{R}^m, \tag{13}$$

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

$$\frac{\partial H(e)}{\partial e} = \frac{\partial H}{\partial x} - \frac{\partial H}{\partial \xi} = M(x-\xi) = Me. \tag{14}$$

Antes de continuar, es conveniente recordar las definiciones básicas de *detectivilidad y observavilidad*.

Definición 1 (Detectabilidad y observalibilidad) [Mejía C. Juan M., 2007]. *Dado un par de matrices constantes* (C,A) *de dimensión m x n y n x m respectivamente, se dice que el par es detectable si la matriz*

$$\begin{bmatrix} C \\ sI - A \end{bmatrix} \tag{15}$$

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

Para que el estado $x(t)$ del oscilador no lineal (11) sea global y exponencialmente estimado por el estado $\xi(t)$ del observador no lineal (12), 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 matriz I a S para de este modo formar una nueva matriz $W=I+S$ y repetir la prueba.

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 de los valores de *(C,W)* pueden ser propios 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 complejo, con la adecuada selección la matriz *K*. Por lo tanto, la matriz $(W-KC)^T$ también manifesta valores propios con parte real negativa.

La matriz $W-KC$ es una matriz cuadrada y se puede remplazar por la siguiente suma,

$$W-KC=\left[S-\frac{1}{2}(KC+C^TK^T)\right]+\left[I-\frac{1}{2}(KC-C^TK^T)\right]. \tag{16}$$

En la parte derecha de la igualdad (16). La matriz de la izquierda de la ecuación, forman una matriz simétrica definida negativa, mientras que la parte de la derecha de la segunda matriz, forman una matriz simétrica.

Entonces, el sistema dinámico del error de estimación puede escribirse como sigue

$$\dot{e}=\left[\Im(y)+I-\tfrac{1}{2}(KC-C^TK^T)\right]\tfrac{\partial H}{\partial e}+\left[S-\tfrac{1}{2}(KC+C^TK^T)\right]\tfrac{\partial H}{\partial e}. \tag{17}$$

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

$$H(x)=\tfrac{1}{2}(x^TMx), \tag{18}$$

se encuentra que la derivada en el tiempo de esta función, a lo largo de las trayectorias del sistema dinámico del error (17), es como sigue

$$\dot{H(e)} = \frac{\partial H(e)}{\partial e^T}\dot{e} = \frac{\partial H(e)}{\partial e^T}\left[S - \frac{1}{2}(KC + C^T K^T)\right]\frac{\partial H}{\partial e} \leq 0 \tag{19}$$

con $H(e) = 0$ si y solo si $e(t) = 0$.

4.2.2. Análisis de estabilidad

A continuación se recogen los resultados presentados en dos teoremas.

Teorema 1 [Sira-Ramírez y Cruz-Hernández]. *El estado $x(t)$ del oscilador no lineal (11) puede ser global, asintóticamente y exponencialmente estimado por el estado $\xi(t)$ de un observador de la forma (12), si y solo si el par de matrices (C,W) o (C,S) son observables o al menos detectables.*

La observabilidad en cualquiera de los dos pares de matrices (C,W) o (C,S) es una condición suficiente, mas no necesaria para la reconstrucción asintótica de los estados del sistema maestro (11). 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 (11) puede ser global, exponencial y asintóticamente estimado, por el estado $\xi(t)$ de un observador de la forma (12), si y solo si, existe una matriz constante K tal que, la matriz simétrica,*

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

sea definida negativa.

Capitulo 5

5. Sincronización de dos circuitos de Chua de sexto orden con múltiples enrollamientos

En este capítulo se mostrará la sincronización de dos circuitos hipercaóticos de Chua que generan atractores caóticos con múltiples enrollamientos. Para lograr la sincronía entre los osciladores hipercaóticos se utilizará la metodología propuesta en [Sira-Ramírez y Cruz-Hernández, 2000; 2001] para obtener la forma hamiltoniana generalizada.

5.1. Sincronización del circuito de Chua con atractores hipercaóticos con múltiples enrollamientos mediante la forma hamiltoniana generalizada y el diseño de un observador

Considere el circuito modificado de Chua propuesto en [Suykens y Chua 1997], descrito por las siguientes ecuaciones

$$\begin{aligned}
\dot{x}_1 &= \alpha[x_2 - h(x_1)],\\
\dot{x}_2 &= x_1 - x_2 + x_3,\\
\dot{x}_3 &= -\beta x_2,\\
\dot{x}_4 &= \alpha[x_5 - h(x_4)] + K_p(x_4 - x_1),\\
\dot{x}_5 &= x_4 - x_5 + x_6,\\
\dot{x}_6 &= -\beta x_5
\end{aligned} \tag{21}$$

donde h(x_1) es una función no linear como se muestra a continuación,

$$h(x_1) = m_{2n-1}x_1 + \frac{1}{2}\sum_{i=1}^{2n-1}(m_{i-1} - m_i)(|x_1 + c_i| - |x_1 - c_i|) \tag{22}$$

A continuación se mostrará la representación del circuito modificado de Chua (21) en forma hamiltoniana (11). Para este fin, utilizamos la ecuación de energía hamiltoniana siguiente,

$$H(x) = \frac{1}{2}\left(\frac{1}{\alpha}x_1 + x_2 + \frac{1}{\beta}x_3 + \frac{1}{\alpha}x_4 + x_5 + \frac{1}{\beta}x_6\right) \tag{23}$$

de este modo el vector gradiente es

$$\frac{\partial H}{\partial x} = \begin{bmatrix} \frac{1}{\alpha} & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{\beta} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{\alpha} & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{\beta} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{bmatrix} = \begin{bmatrix} \frac{1}{\alpha}x_1 \\ x_2 \\ \frac{1}{\beta}x_3 \\ \frac{1}{\alpha}x_4 \\ x_5 \\ \frac{1}{\beta}x_6 \end{bmatrix}.$$

El sistema (21) se expresa en la forma hamiltoniana generalizada siguiente

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \\ \dot{x}_5 \\ \dot{x}_6 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & \frac{K_p}{2} & 0 & 0 \\ 0 & 0 & \beta & 0 & 0 & 0 \\ 0 & -\beta & 0 & 0 & 0 & 0 \\ -\frac{K_p}{2} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \beta \\ 0 & 0 & 0 & 0 & -\beta & 0 \end{bmatrix} \frac{\partial H}{\partial x} + \begin{bmatrix} 0 & \alpha & 0 & -\frac{K_p}{2} & 0 & 0 \\ \alpha & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ -\frac{K_p}{2} & 0 & 0 & K_p & \alpha & 0 \\ 0 & 0 & 0 & \alpha & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \frac{\partial H}{\partial x} + \begin{bmatrix} \alpha H(x_1) \\ 0 \\ 0 \\ \alpha H(x_4) \\ 0 \\ 0 \end{bmatrix}. \tag{24}$$

La salida de (24) que será transmitida m es y = x_1 sistema esclavo.

Las matrices S; I y C están dadas por:

$$C = \begin{bmatrix} \alpha & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha & 0 & 0 \end{bmatrix}, S = \begin{bmatrix} 0 & \alpha & 0 & -\frac{K_p}{2} & 0 & 0 \\ \alpha & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ -\frac{K_p}{2} & 0 & 0 & K_p & \alpha & 0 \\ 0 & 0 & 0 & \alpha & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} y \; I = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \beta \\ 0 & 0 & 0 & 0 & -\beta & 0 \end{bmatrix}.$$

Entonces el observador construido queda dado por la expresión

$$\begin{bmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \\ \xi_4 \\ \xi_5 \\ \xi_6 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & \frac{K_p}{2} & 0 & 0 \\ 0 & 0 & \beta & 0 & 0 & 0 \\ 0 & -\beta & 0 & 0 & 0 & 0 \\ -\frac{K_p}{2} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \beta \\ 0 & 0 & 0 & 0 & -\beta & 0 \end{bmatrix} \frac{\partial H}{\partial \xi} + \begin{bmatrix} 0 & \alpha & 0 & -\frac{K_p}{2} & 0 & 0 \\ \alpha & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ -\frac{K_p}{2} & 0 & 0 & K_p & \alpha & 0 \\ 0 & 0 & 0 & \alpha & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \frac{\partial H}{\partial \xi} + \begin{bmatrix} \alpha H(x_1) \\ 0 \\ 0 \\ \alpha H(x_4) \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} k_1 & 0 \\ k_2 & 0 \\ k_3 & 0 \\ 0 & k_4 \\ 0 & k_5 \\ 0 & k_6 \end{bmatrix} e_y \;, \quad (25)$$

donde el error es $e_y = \begin{bmatrix} x_1 - \xi_1 \\ x_4 - \xi_4 \end{bmatrix}$ y se eligen de forma adecuada los valores de $k_1, k_2, k_3, k_4, k_5 \; y \; k_6$, para garantizar la estabilidad exponencial asintótica a cero de las trayectorias de los errores de reconstrucción de los estados del circuito de Chua modificado, descritos por las ecuaciones:

A partir del teorema A, condición (20) donde se encuentran los valores de $k_1, k_2, k_3, k_4, k_5 \; y \; k_6$ para los cuales se garantiza estabilidad asintótica a cero del error de sincronía, es decir la siguiente condición debe cumplirse

$$2\left[S - \frac{1}{2}(kC + C^T k^T)\right] < 0. \quad (26)$$

Al sustituir *S*, *k*, y *C* en (26) obtenemos la siguiente condición.

$$\begin{bmatrix} -2k_1\alpha & 2\alpha - k_2\alpha & -k_3\alpha & -Kp & 0 & 0 \\ 2\alpha - k_2\alpha & -2 & 0 & 0 & 0 & 0 \\ -k_3\alpha & 0 & 0 & 0 & 0 & 0 \\ -Kp & 0 & 0 & 2Kp - 2k_4\alpha & 2\alpha - k_5\alpha & -k_6\alpha \\ 0 & 0 & 0 & 2\alpha - k_5\alpha & -2 & 0 \\ 0 & 0 & 0 & -k_6\alpha & 0 & 0 \end{bmatrix} < 0 \,. \quad (27)$$

Por lo tanto, los valores de $k_1, k_2, k_3, k_4, k_5 \; y \; k_6$ deben estar dentro de los rangos establecidos a continuación, para los cuales, satisfagan las desigualdades:

$$
\begin{aligned}
&-2k_1 \propto \leq 0\\
&4k_2 - k_2^2 \leq 3.7194\\
&2k_3^2 \propto^2 = 0\\
&-4k_3^2 K_p \propto -4k_3^2 k_4 \propto^2 \leq 0\\
&4k_5 - k_5^2 \leq 4.00049\\
&k_6 = 0
\end{aligned}
\tag{28}
$$

Las condiciones anteriores para las ganancias k se obtuvieron a partir del teorema de Silverter [Ogata, 19xx]. Las ganancias k_3 y k_6 son igual a cero y k_1=k_4=1, k_2=2 y k_5=1.82. Estos valores, cumplen con las condiciones (28).

A partir de (24) y (25) el sistema dinámico del error es

$$
\begin{bmatrix} \dot{e}_1 \\ \dot{e}_2 \\ \dot{e}_3 \\ \dot{e}_4 \\ \dot{e}_5 \\ \dot{e}_6 \end{bmatrix} = \begin{bmatrix} 0 & \frac{k_2\alpha}{2} & \frac{k_3\alpha\beta}{2} & \frac{K_P\alpha}{2} & 0 & 0 \\ \frac{-k_2\alpha}{2} & 0 & \beta & 0 & 0 & 0 \\ \frac{-k_3\alpha}{2} & -\beta & 0 & 0 & 0 & 0 \\ -\frac{K_P\alpha}{2} & 0 & 0 & 0 & \frac{k_5\alpha}{2} & \frac{k_6\alpha\beta}{2} \\ 0 & 0 & 0 & \frac{-k_5\alpha}{2} & 0 & \beta \\ 0 & 0 & 0 & \frac{-k_6\alpha}{2} & -\beta & 0 \end{bmatrix} \frac{\partial H}{\partial e} + \begin{bmatrix} -k_1\alpha & \alpha\left(1-\frac{k_2}{2}\right) & \frac{k_3\alpha\beta}{2} & -\frac{K_P\alpha}{2} & 0 & 0 \\ \alpha\left(1-\frac{k_2}{2}\right) & -1 & 0 & 0 & 0 & 0 \\ \frac{-k_3\alpha}{2} & 0 & 0 & 0 & 0 & 0 \\ -\frac{K_P\alpha}{2} & 0 & 0 & K_P\alpha - k_4\alpha & \alpha\left(1-\frac{k_5}{2}\right) & -\frac{k_6\alpha\beta}{2} \\ 0 & 0 & 0 & \alpha\left(1-\frac{k_5}{2}\right) & -1 & 0 \\ 0 & 0 & 0 & \frac{-k_6\alpha}{2} & 0 & 0 \end{bmatrix} \frac{\partial H}{\partial e}. \tag{29}
$$

5.2. Simulación numérica

Las simulaciones siguientes fueron obtenidas con el programa MatLab. Estas imágenes muestran la sincronización de los sistemas maestros (24) y esclavo (25).

Para lograr esta emulación se utilizaron los siguientes valores de los parámetros:

n=3, K_p=0.01, $\alpha = 9\ \ \beta = 14.28$,
m=[0.9/7,-3/7,3.5/7,2.7/7,4/7,-2.4/7] y
c=[1,2.15,3.6,6.2,9]

y las condiciones iniciales:

$$x(0) = (0.1,0.1,0,0.1,0.1,0),$$

$$\xi(0) = (0.1,0.1,8,0.1,0.1,8)\,.$$

Las figuras 18 y 19 ilustran el resultado en el espacio de estados de la sincronía entre los estados del maestro (24) y el esclavo (25).

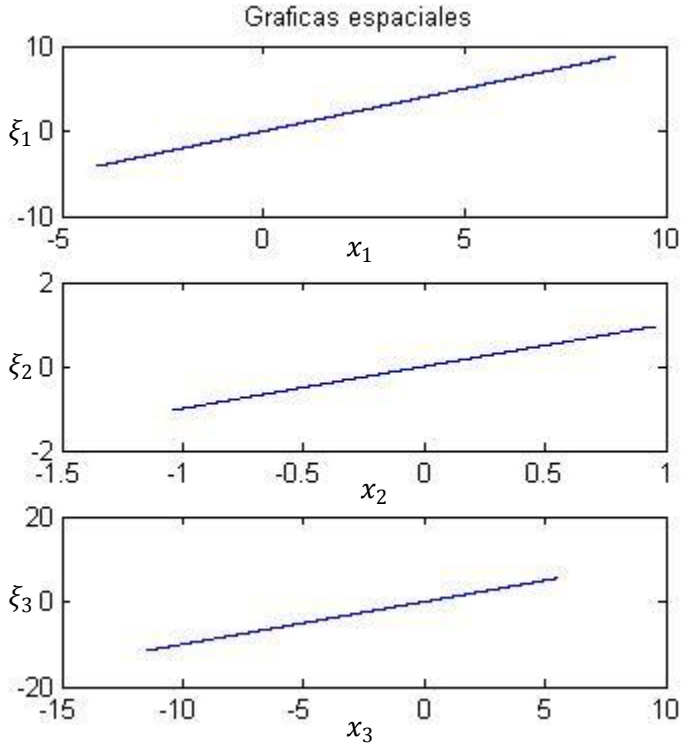

Figura 18. Sincronía entre maestro (24) y esclavo (25) para los estados $(x_1, \xi_1), (x_2, \xi_2)\ y\ (x_3, \xi_3)$.

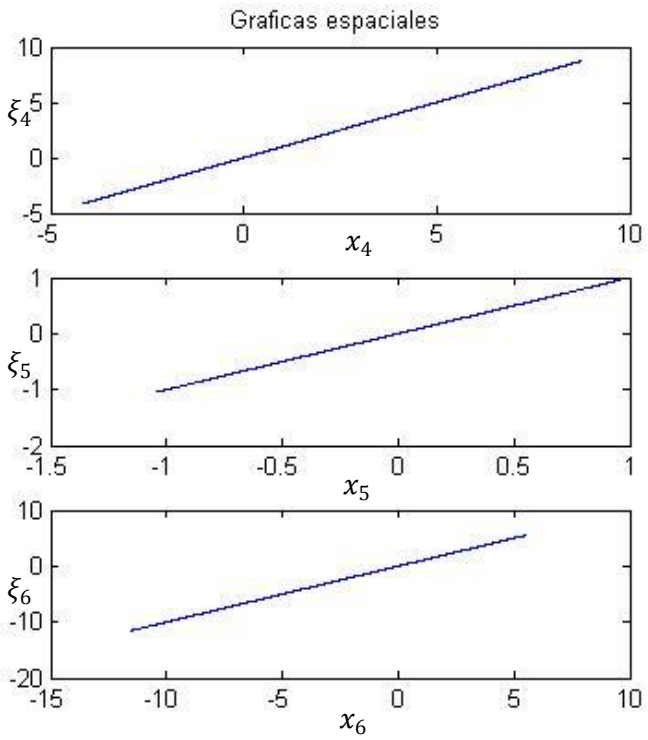

Figura 19. Sincronía entre maestro (24) y esclavo (25) para los estados $(x_4, \xi_4), (x_5, \xi_5)\ y\ (x_6, \xi_6)$.

Las figuras 20 y 21 ilustran el error de sincronía entre cada uno de los estados hipercaóticos del maestro y el esclavo, estas figuras ilustran un error igual a cero pero con un transitorio, este se presenta cuando las condiciones de los estados caóticos entre el maestro y el esclavo no son iguales.

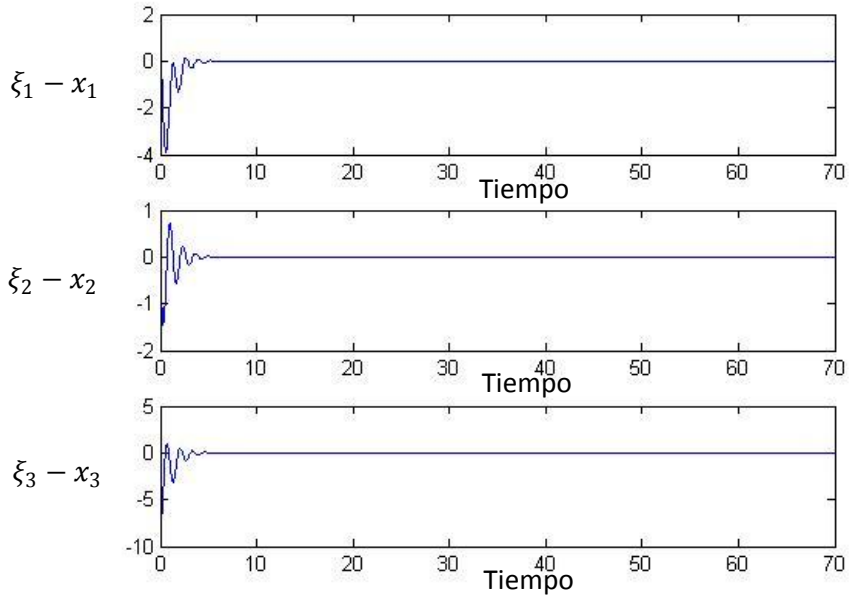

Figura 20. Error de sincronía entre maestro y esclavo.

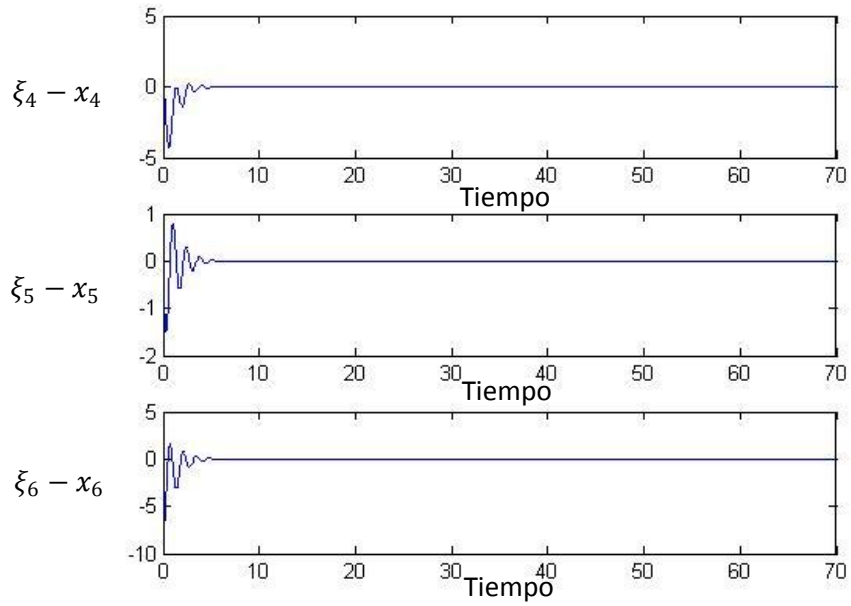

Figura 21. Error de sincronía entre el esclavo y maestro.

Por último, las figuras 22 y 23 muestran los atractores generados por el maestro y el esclavo respectivamente. En la figura 22, se ilustran dos conjuntos de atractores debido a que son 6 estados hipercaóticos, el a) pertenece a la parte formada por los estados x_1, x_2, y

x_3, el b) se forma a partir de x_4, x_5 y x_6, uno superior y uno inferior. Así mismo se forma un conjunto de atractores hipercaóticos para el esclavo, uno superior y otro inferior. Hay una diferencia entre los atractores del maestro y esclavo, es debido a las condiciones iniciales, las cuales provocan el transitorio.

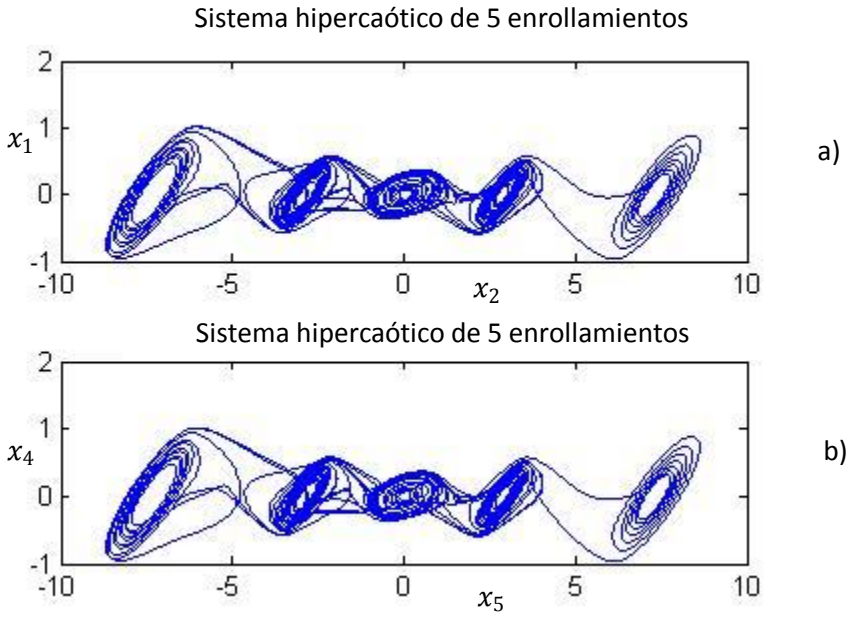

Figura 22. Atractores del sistema hipercaótico del maestro los cuales son casi iguales.

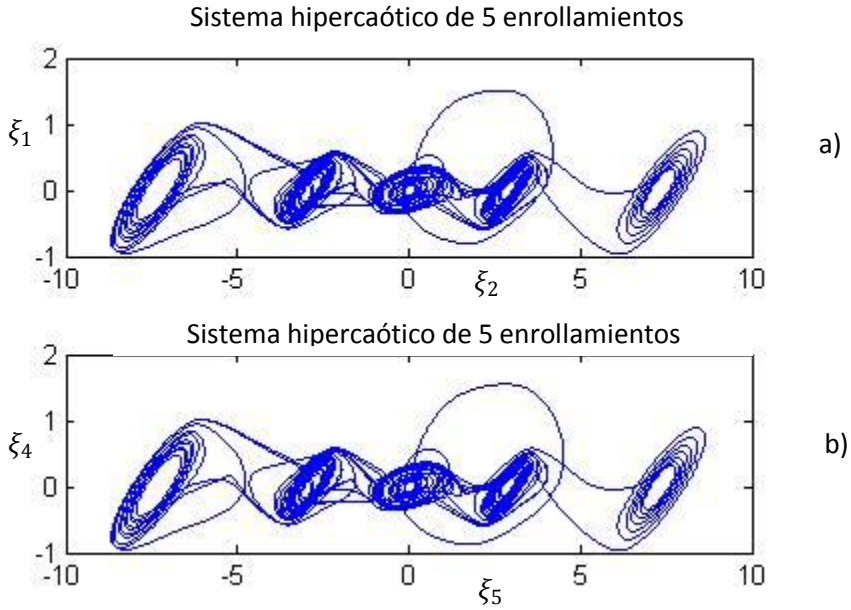

Figura 23. Atractores del esclavo.

Aunque se puede observar de manera sencilla la diferencia entre los atractores del maestro y del esclavo, aun cuando las condiciones iniciales no sean iguales en el maestro y el esclavo la sincronización se logra.

Capitulo 6

6. Sincronización de múltiples circuitos de con Chua de sexto orden

El principal interés de este trabajo es demostrar que un sistema de ecuaciones caóticas, en este caso el circuito modificado de Chua sistema n-doble enrollamientos [Suykens y Chua, 1997], tiene la capacidad de hacer el encriptado de información y estar en un una red de usuarios.

Por lo cual se ha investigado que la sincronía de atractores caóticos con múltiples enrollamientos es factible por el método de la generalización hamiltoniana [Sira-Ramírez H. y Cruz-Hernández C., 2000; 2001]. La técnica de red para multiusuario que se implementará es el esquema de sincronización por retroalimentación sugerido por [Milanovic y Zaghloul, 1996] en combinación con el método de sincronización de osciladores caóticos mediante un sistema hamiltoniano generalizado y el diseño de un observador no lineal propuesto en [Sira-Ramírez H. y Cruz-Hernández C., 2000; 2001].

6.1. Método de retroalimentación en combinación del sistema hamiltoniano Generalizado

Para poder tener una red de usuarios, se utilizaran *N* maestros y *N* esclavos, la sincronización se logra mediante un acoplamiento unidireccional, conocido como acoplamiento maestro y esclavo.

La utilización de retroalimentación sugerido por [Milanovic 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 H. y Cruz-Hernández C., 2000; 2001], hace que la red de usuarios sea posible.

En la figura 24 se muestra el diagrama a bloques del conjunto de *N* de sistemas maestros, el cual cuanta 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* sistemas de ecuaciones de Chua. Esto último se muestra como sigue

$$s(t) = y_1(t) + y_2(t) + \cdots + y_N(t) \qquad (30)$$

Esta señal resultante (30) será la señal de acoplamiento que se envía hacia el conjunto de *N* esclavos, ubicados remotamente, mediante un canal público inseguro. Al mismo tiempo, se retroalimenta al conjunto de sistemas maestros, mediante las ecuaciones de Chua. Esto es necesario para llevar a cabo la sincronización y lograr un acoplamiento unidireccional maestro y esclavo. Al igual que el conjunto de *N* sistemas maestros, el conjunto de *N* sistemas esclavos (ver figura 25) cuanta con $n_i(t)$ 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 utiliza para ocultar la información de u_i usuarios en el transmisor de la red, respectivamente, mientras que las señales de salida $n_i(t)$ de los esclavos se utilizaran para recuperar la información de u_i usuarios en el receptor de la red de dichos sistemas esclavos.

En el siguiente punto se mostrará matemáticamente el resultado de la técnica anteriormente mencionada

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, esta dado por:

Maestro Cero

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

Maestro 1

$$\dot{x_1} = \Im(y_0)\frac{\partial H}{\partial x} + (I+S)\frac{\partial H}{\partial x} + f(y_0) + K(y_0 - y_1), \quad x_1 \in \mathbb{R}^n,$$
$$y_1 = C\frac{\partial H}{\partial x}, \; y_1 \in \mathbb{R}^m. \tag{31}$$

Maestro 2

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

Maestro N

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

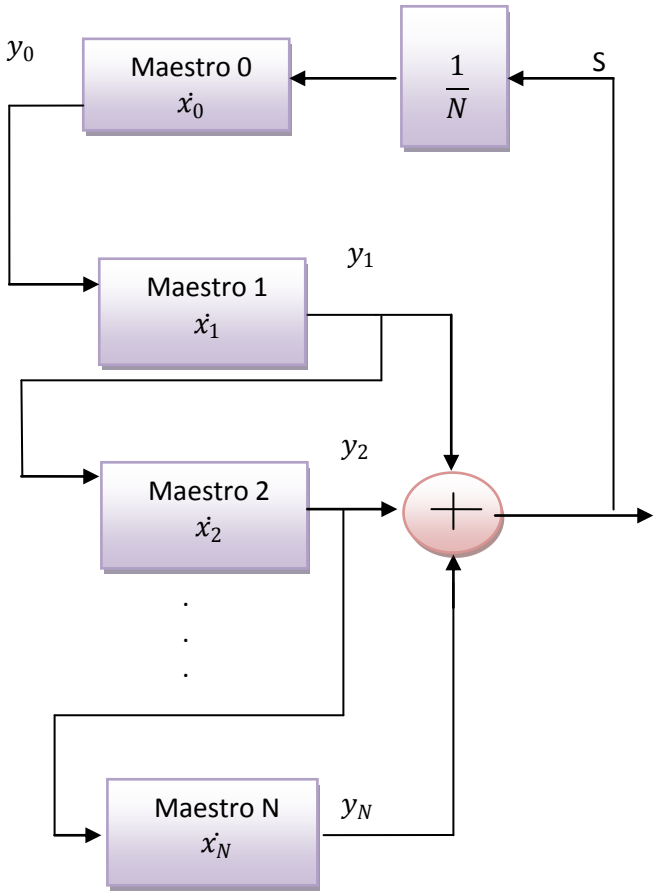

Figura 24. Diagrama a bloques del conjunto de *N* maestros para sincronización entre múltiples maestros y esclavos.

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 conjunto de ecuaciones de estado en forma hamiltoniana generalizada:

Esclavo Cero

$$\dot{\xi}_0 = \Im\left(\frac{s}{N}\right)\frac{\partial H}{\partial x} + (I+S)\frac{\partial H}{\partial x} + f\left(\frac{s}{N}\right) + K\left(\frac{S}{N} - n_0\right), \quad \xi_0 \in \mathbb{R}^n,$$
$$n_0 = C\frac{\partial H}{\partial x}, \qquad n_0 \in \mathbb{R}^m.$$

Esclavo 1

$$\dot{\xi}_1 = \Im(n)\frac{\partial H}{\partial x} + (I+S)\frac{\partial H}{\partial x} + f(n_0) + K(n_0 - n_1), \quad \xi_1 \in \mathbb{R}^n, \tag{32}$$
$$n_1 = C\frac{\partial H}{\partial x}, \qquad n_1 \in \mathbb{R}^m.$$

Esclavo 2

$$\dot{\xi}_2 = \Im(n_1)\frac{\partial H}{\partial x} + (I+S)\frac{\partial H}{\partial x} + f(n_1) + K(n_1 - n_2), \quad \xi_2 \in \mathbb{R}^n,$$
$$n_2 = C\frac{\partial H}{\partial x}, \qquad n_2 \in \mathbb{R}^m.$$

Esclavo N

$$\dot{\xi}_N = \Im(n_{n-1})\frac{\partial H}{\partial x} + (I+S)\frac{\partial H}{\partial x} + f(n_{N-1}) + K(n_{N-1} - n_N), \quad \xi_N \in \mathbb{R}^n,$$
$$n_N = C\frac{\partial H}{\partial x}, \qquad n_N \in \mathbb{R}^n.$$

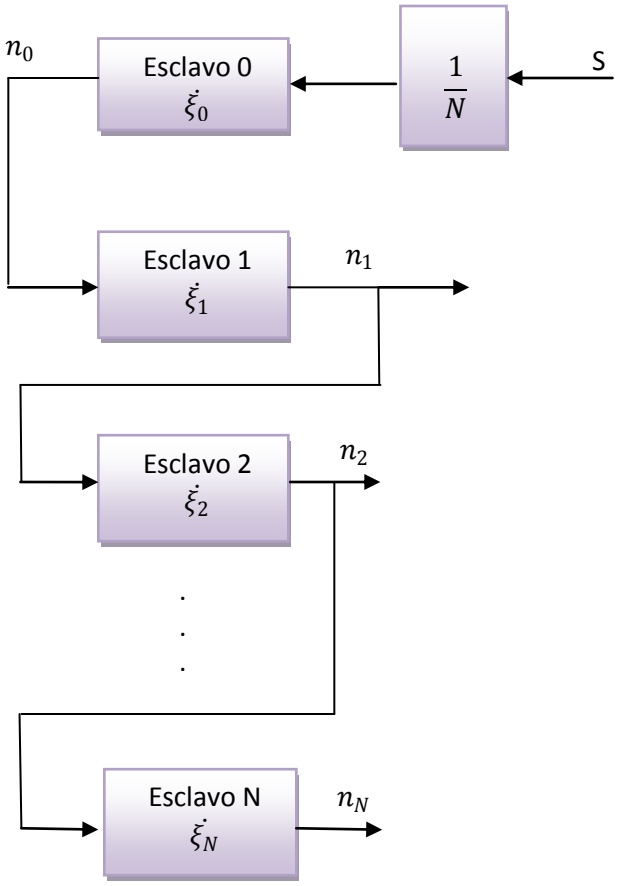

Figura 25. Diagrama a bloques del conjunto de *N* maestros para sincronización entre múltiples maestros y esclavos. Utilizando para ingresar primero la señal *S* y *N* para los usuarios en el receptor de la red.

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 la cual se utilizan las ecuaciones normalizadas de sistema Chua. 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 in observador no línea.

Basándonos en los resultados presentados en el capítulo 4 de sincronía de sexto orden [Suykens y Chua, 1997].

Las ganancias de sistema hamiltoniano generalizado para las ecuaciones de Chua son:

$$K_1 = (1, 2, 0, 0, 0, 0)^T$$
$$K_2 = (0, 0, 0, 1, 1.85, 0)^T$$

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

Los parámetros de estas ecuaciones de Chua de sexto orden son los siguientes

$$\alpha_1 = 10, \qquad \beta_1 = 16.28,$$
$$\alpha_2 = 9, \qquad \beta_2 = 14.28,$$
$$\alpha_3 = 8, \qquad \beta_3 = 12.28,$$

Estas constantes son para hacer una diferencia entre los maestros y esclavos, esto tiene el fin de tener una comunicación entre la red de usuarios única para cada uno de los usuarios.

6.2.1. Ecuaciones normalizadas del conjunto de 2 sistemas maestros

Maestro Cero

$$\begin{aligned}
\dot{x}_{0_1} &= \alpha_1 \left(x_{0_2} - h(s_1)\right) - k_1(s_1 - x_{0_1}), \\
\dot{x}_{0_2} &= x_{0_1} - x_{0_2} + x_{0_3} - k_2(s_1 - x_{0_1}), \\
\dot{x}_{0_3} &= -\beta_1 x_{0_2} - k_3(s_1 - x_{0_1}), \\
\dot{x}_{0_4} &= \alpha_1 \left(x_{0_5} - h(s_2)\right) + K_p(x_{0_4} - x_{0_1}) - k_4(s_2 - x_{0_5}), \\
\dot{x}_{0_5} &= x_{0_4} - x_{0_5} + x_{0_6} - k_5(s_2 - x_{0_5}), \\
\dot{x}_{0_6} &= -\beta_1 x_{0_5} - k_6(s_2 - x_{0_5}).
\end{aligned} \tag{32}$$

Maestro uno

$$
\begin{aligned}
\dot{x}_{1_1} &= \alpha_2\left(x_{1_2} - h\left(x_{0_1}\right)\right) - k_1\left(x_{0_1} - x_{1_1}\right), \\
\dot{x}_{1_2} &= x_{1_1} - x_{1_2} + x_{1_3} - k_2\left(x_{0_1} - x_{1_1}\right), \\
\dot{x}_{1_3} &= -\beta_2 x_{1_2} - k_3\left(x_{0_1} - x_{1_1}\right), \\
\dot{x}_{1_4} &= \alpha_2\left(x_{1_5} - h\left(x_{0_4}\right)\right) + K_p\left(x_{1_4} - x_{1_1}\right) - k_4\left(x_{0_4} - x_{1_4}\right), \quad (33) \\
\dot{x}_{1_5} &= x_{1_4} - x_{1_5} + x_{1_6} - k_5\left(x_{0_4} - x_{1_4}\right), \\
\dot{x}_{1_6} &= -\beta_2 x_{1_5} - k_6\left(x_{0_4} - x_{1_4}\right).
\end{aligned}
$$

Maestro dos

$$
\begin{aligned}
\dot{x}_{2_1} &= \alpha_3\left(x_{2_2} - h\left(x_{1_1}\right)\right) - k_1\left(x_{1_1} - x_{2_1}\right), \\
\dot{x}_{2_2} &= x_{2_1} - x_{2_2} + x_{2_3} - k_2\left(x_{1_1} - x_{2_1}\right), \\
\dot{x}_{2_3} &= -\beta_3 x_{2_2} - k_3\left(x_{1_1} - x_{2_1}\right), \\
\dot{x}_{2_4} &= \alpha_3\left(x_{2_5} - h\left(x_{1_4}\right)\right) + K_p\left(x_{2_4} - x_{2_1}\right) - k_4\left(x_{1_4} - x_{2_4}\right), \quad (34) \\
\dot{x}_{2_5} &= x_{2_4} - x_{2_5} + x_{2_6} - k_5\left(x_{1_4} - x_{2_4}\right), \\
\dot{x}_{2_6} &= -\beta_3 x_{2_5} - k_6\left(x_{1_4} - x_{2_4}\right).
\end{aligned}
$$

Donde las condiciones iníciales para los estados de las ecuaciones de Chua son las siguientes:

$$
\begin{array}{lll}
\dot{x}_{0_1} = 0.1 & \dot{x}_{1_1} = 0.1 & \dot{x}_{2_1} = 0.1 \\
\dot{x}_{0_2} = 0.1 & \dot{x}_{1_2} = 0.1 & \dot{x}_{2_2} = 0.1 \\
\dot{x}_{0_3} = 0 & \dot{x}_{1_3} = 0 & \dot{x}_{2_3} = 0 \\
\dot{x}_{0_4} = 0.1 & \dot{x}_{1_4} = 0.1 & \dot{x}_{2_4} = 0.1 \\
\dot{x}_{0_5} = 0.1 & \dot{x}_{1_5} = 0.1 & \dot{x}_{2_5} = 0.1 \\
\dot{x}_{0_6} = 0 & \dot{x}_{1_6} = 0 & \dot{x}_{2_6} = 0
\end{array}
$$

La figura 26 muestra el comportamiento de cada estado respecto al tiempo, en la primera columna se observa los estados del maestro cero, la segunda columna ilustra el movimiento de los estados del maestro uno y por último se tiene al maestro dos. Las graficas son muy semejantes pero existe una diferencia que se observa en intervalos de tiempo. Con esa diferencia se comprueba que los sistemas caóticos cero, uno y dos son totalmente diferentes, por lo cual se utilizara para sincronizar, aunque más adelante se comprobara con graficas de error de sincronía.

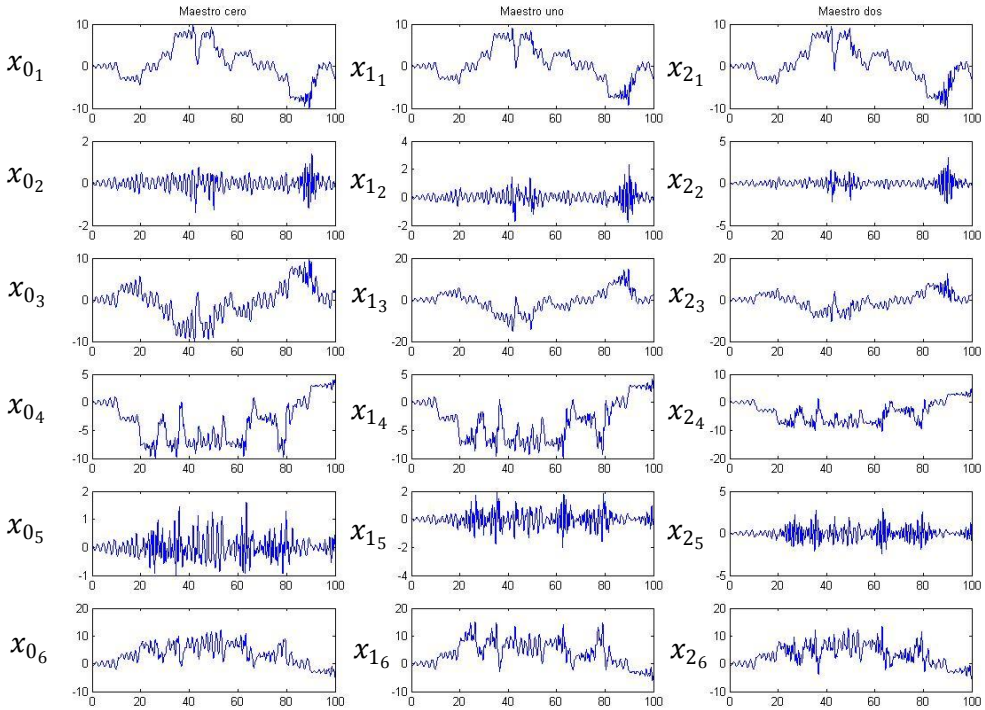

Figura 26. Muestra la evolución en el tiempo de los estados de cada maestro.

La imagen 27 muestra los atractores caóticos formados por el maestro cero, uno y dos, en esta imagen se puede observar que los atractores de cada maestro es diferente entre si este es un ejemplo más de la diferencia entre estos sistemas caóticos.

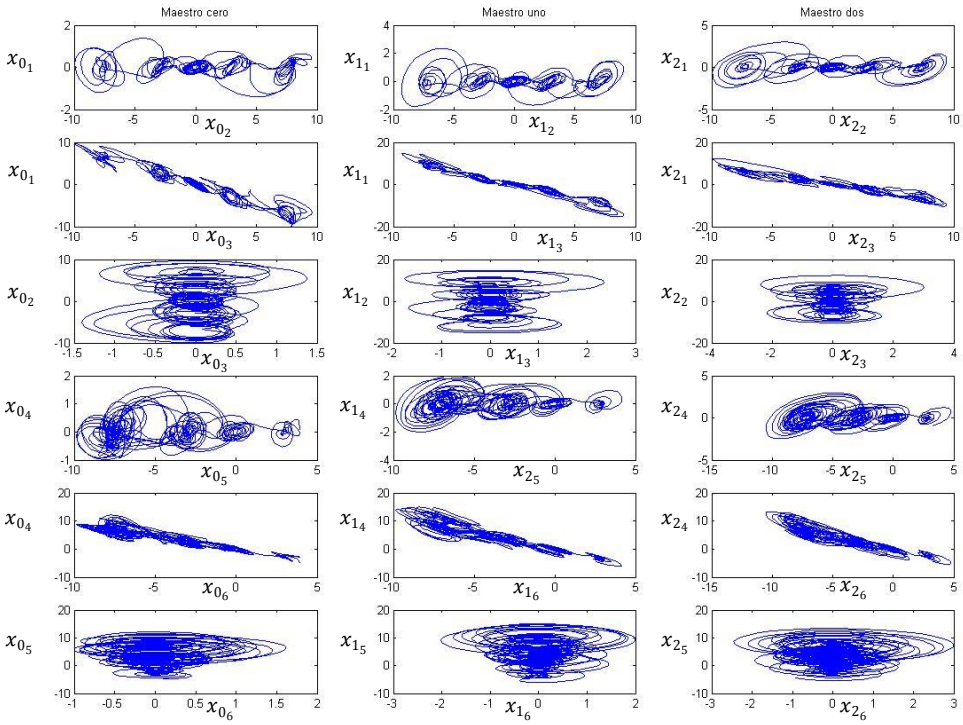

Figura 27. Muestra los atractores caóticos de cada ecuación este sistema tiene dos tipos de atractores uno alto y otro bajo, formados por $(x_{0_1}, x_{0_2}), (x_{0_1}, x_{0_3})\ y\ (x_{0_2}, x_{0_3})$ parte alta del maestro cero y$(x_{0_4}, x_{0_5}), (x_{0_4}, x_{0_6})\ y\ (x_{0_5}, x_{0_6})$, las graficas del maestro uno son las siguientes $(x_{1_1}, x_{1_2}), (x_{1_1}, x_{1_3})\ y\ (x_{1_2}, x_{1_3})$ parte alta y la parte baja por $(x_{1_4}, x_{1_5}), (x_{1_4}, x_{1_6})\ y\ (x_{1_5}, x_{1_6})$ y por ultimo el maestro dos está compuesto por $(x_{2_1}, x_{2_2}), (x_{2_1}, x_{2_3})\ y\ (x_{2_2}, x_{2_3})$ y por $(x_{2_4}, x_{2_5}), (x_{2_4}, x_{2_6})\ y\ (x_{2_5}, x_{2_6})$.

6.2.2. Ecuaciones normalizadas del conjunto de 2 sistemas esclavos

Ecuaciones de Chua de sexto orden del esclavo cero

$$\begin{aligned}
\dot{\xi}_{0_1} &= \alpha_1\left(\xi_{0_2} - h(s_1)\right) - k_1(s_1 - \xi_{0_1}),\\
\dot{\xi}_{0_2} &= \xi_{0_1} - \xi_{0_2} + \xi_{0_3} - k_2(s_1 - \xi_{0_1}),\\
\dot{\xi}_{0_3} &= -\beta_1\xi_{0_2} - k_3(s_1 - \xi_{0_1}),\\
\dot{\xi}_{0_4} &= \alpha_1\left(\xi_{0_5} - h(\xi_2)\right) + K_p(\xi_{0_4} - \xi_{0_1}) - k_4(s_2 - \xi_{0_5}),\\
\dot{\xi}_{0_5} &= \xi_{0_4} - \xi_{0_5} + \xi_{0_6} - k_5(s_2 - \xi_{0_5}),\\
\dot{\xi}_{0_6} &= -\beta_{1_1}\xi_{0_5} - k_6(s_2 - \xi_{0_5}).
\end{aligned} \tag{35}$$

Ecuación de Chua de sexto orden del esclavo uno

$$\begin{aligned}
\dot{\xi}_{1_1} &= \alpha_2\left(\xi_{1_2} - h(\xi_{0_1})\right) - k_1(\xi_{0_1} - \xi_{1_1}),\\
\dot{\xi}_{1_2} &= \xi_{1_1} - \xi_{1_2} + \xi_{1_3} - k_2(\xi_{0_1} - \xi_{1_1}),\\
\dot{\xi}_{1_3} &= -\beta_2\xi_{1_2} - k_3(\xi_{0_1} - \xi_{1_1}),\\
\dot{\xi}_{1_4} &= \alpha_2\left(\xi_{1_5} - h(\xi_{0_4})\right) + K_p(\xi_{1_4} - \xi_{1_1}) - k_4(\xi_{0_4} - \xi_{1_4}),\\
\dot{\xi}_{1_5} &= \xi_{1_4} - \xi_{1_5} + \xi_{1_6} - k_5(\xi_{0_4} - \xi_{1_4}),\\
\dot{\xi}_{1_6} &= -\beta_2\xi_{1_5} - k_6(\xi_{0_4} - \xi_{1_4}).
\end{aligned} \tag{36}$$

Ecuación de Chua de seto orden del esclavo dos

$$\begin{aligned}
\dot{\xi}_{2_1} &= \alpha_3\left(\xi_{2_2} - h(\xi_{1_1})\right) - k_1(\xi_{1_1} - \xi_{2_1}),\\
\dot{\xi}_{2_2} &= \xi_{2_1} - \xi_{2_2} + \xi_{2_3} - k_2(\xi_{1_1} - \xi_{2_1}),\\
\dot{\xi}_{2_3} &= -\beta_3\xi_{2_2} - k_3(\xi_{1_1} - \xi_{2_1}),\\
\dot{\xi}_{2_4} &= \alpha_3\left(\xi_{2_5} - h(\xi_{1_4})\right) + K_p(\xi_{2_4} - \xi_{2_1}) - k_4(\xi_{1_4} - \xi_{2_4}),\\
\dot{\xi}_{2_5} &= \xi_{2_4} - \xi_{2_5} + \xi_{2_6} - k_5(\xi_{1_4} - \xi_{2_4}),\\
\dot{\xi}_{2_6} &= -\beta_3\xi_{2_5} - k_6(\xi_{1_4} - \xi_{2_4}).
\end{aligned} \tag{37}$$

Donde las condiciones iníciales para los estados de las ecuaciones de Chua de sexto orden, son las siguientes:

$$\xi_{0_1} = 1.1 \qquad \xi_{1_1} = 1.1 \qquad \xi_{2_1} = 1.1$$
$$\xi_{0_2} = 1.1 \qquad \xi_{1_2} = 1.1 \qquad \xi_{2_2} = 1.1$$
$$\xi_{0_3} = 1 \qquad \xi_{1_3} = 1 \qquad \xi_{2_3} = 1$$
$$\xi_{0_4} = 1.1 \qquad \xi_{1_4} = 1.1 \qquad \xi_{2_4} = 1.1$$
$$\xi_{0_5} = 1.1 \qquad \xi_{1_5} = 1.1 \qquad \xi_{2_5} = 1.1$$
$$\xi_{0_6} = 1 \qquad \xi_{1_6} = 1 \qquad \xi_{2_6} = 1$$

La figura 28 muestra el comportamiento de cada una de estados en función del tiempo, este resultado se obtuvo al sincronizar los maestros con los esclavos, ya que con las condiciones iniciales distintas el comportamiento de los estados sería totalmente distinto al de los maestros.

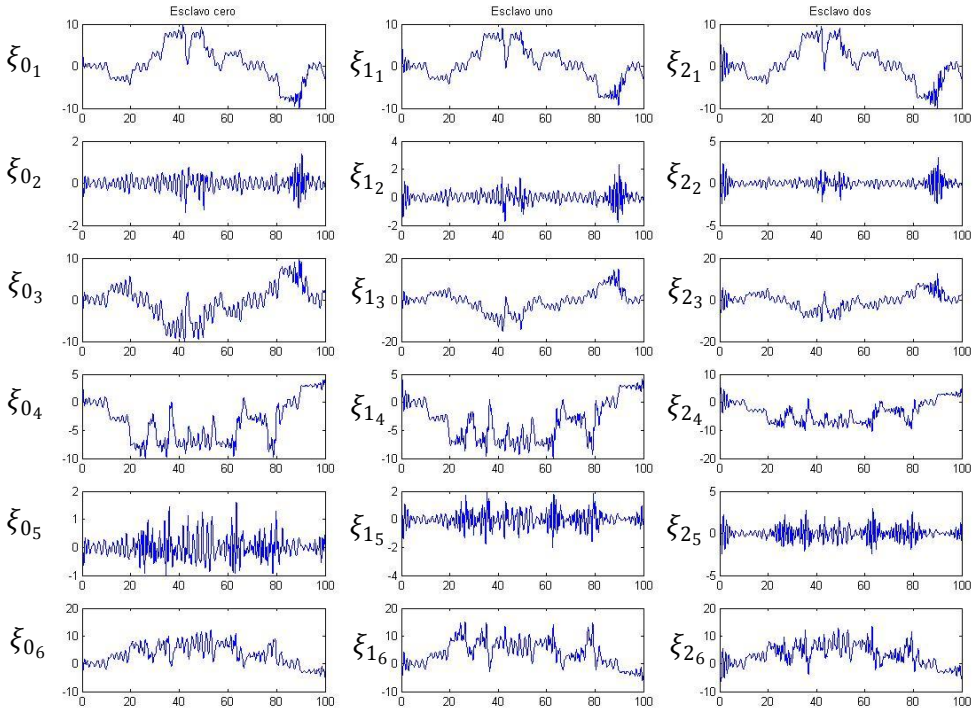

Figura 28. Muestra la evolución en el tiempo de los estados del esclavo cero, uno y dos.

La imagen 29 ilustra los atractores caóticos formados por los esclavos cero, uno y dos, se puede observar que los atractores son diferente entre si, como la sincronía tiene su efecto observable en cada grafica que muestra la figura 27 y es casi idéntica a las graficas mostradas en la imagen 29 pero con su respectivo retraso por el transitorio y esto es debido a que tienen diferentes condiciones iniciales.

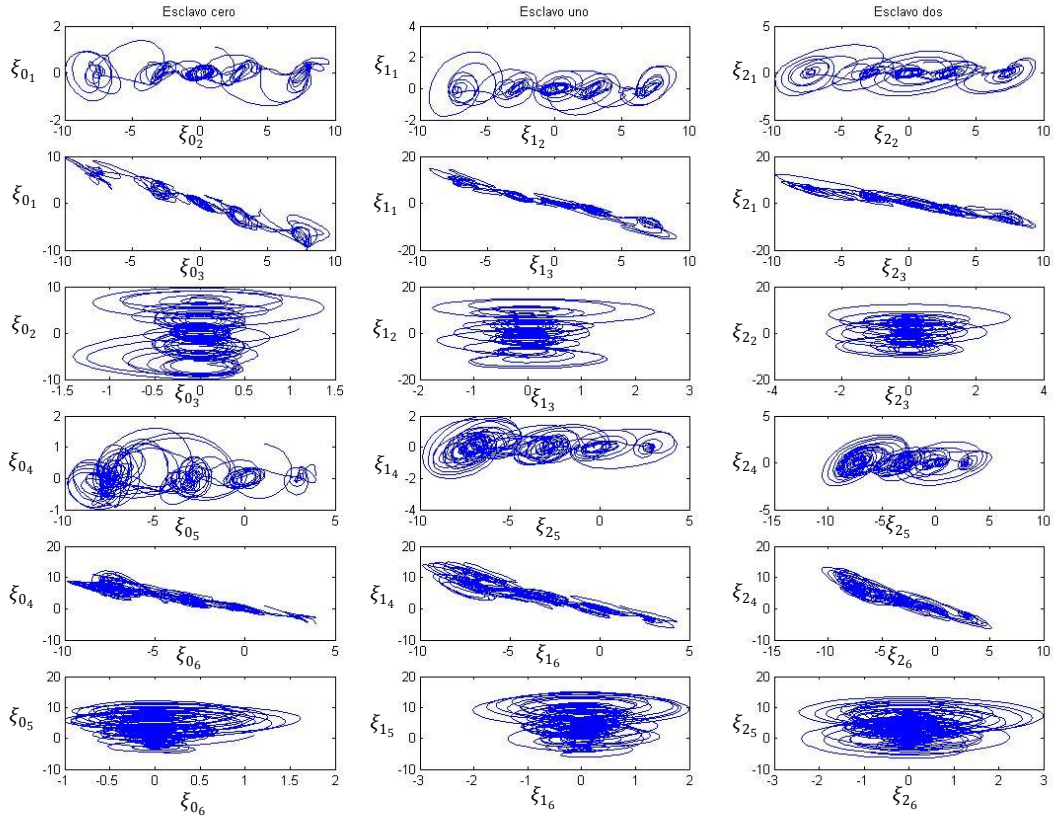

Figure 29. Muestra los atractores caóticos de cada ecuación este sistema tiene dos tipos de atractores uno alto y otro bajo, formados por $(\xi_{0_1}, \xi_{0_2}), (\xi_{0_1}, \xi_{0_3})\ y\ (\xi_{0_2}, \xi_{0_3})$ parte alta del esclavo cero y $(\xi_{0_4}, \xi_{0_5}), (\xi_{0_4}, \xi_{0_6})\ y\ (\xi_{0_5}, \xi_{0_6})$, las graficas del esclavo uno son las siguientes $(\xi_{1_1}, \xi_{1_2}), (\xi_{1_1}, \xi_{1_3})\ y\ (\xi_{1_2}, \xi_{1_3})$ parte alta y la parte baja por $(\xi_{1_4}, \xi_{1_5}), (\xi_{1_4}, \xi_{1_6})\ y\ (\xi_{1_5}, \xi_{1_6})$ y por ultimo el esclavo dos está compuesto por $(\xi_{2_1}, \xi_{2_2}), (\xi_{2_1}, \xi_{2_3})\ y\ (\xi_{2_2}, \xi_{2_3})$ y por $(\xi_{2_4}, \xi_{2_5}), (\xi_{2_4}, \xi_{2_6})\ y\ (\xi_{2_5}, \xi_{2_6})$.

La función $h(x_1)$ es una función no lineal como se muestra a continuación. Por medio de esta ecuación se forma los atractores, para este caso se utilizaron 5 enrollamientos.

$$h(x_1) = m_{2n-1}x_1 \ + \frac{1}{2}\sum_{i=1}^{2n-1}(m_{i-1} - m_i)(|x_1 + c_i| - |x_1 - c_i|) \quad (38)$$

Donde:

n=3
K_p=0.01
$\alpha = 9 \ \beta = 14.28$
m=[0.9/7,-3/7,3.5/7,2.7/7,4/7,-2.4/7]
c=[1,2.15,3.6,6.2,9]

6.3. Sincronización

La sincronización entre el maestro y esclavo se muestra con el plano de fase (figura 30). La figura 32 ilustra el plano de fase de sincronía en el espacio de estados entre las ecuaciones del maestro 2 y el esclavo 2.

Para que un sistema entre en sincronía su gráfica de plano de fase debe ilustrar una pendiente de 45 grados, lo cual se observa en estas gráficas pero con un transitorio lo cual existe debido a las diferencias entre las condiciones iniciales entre el maestro y el esclavo

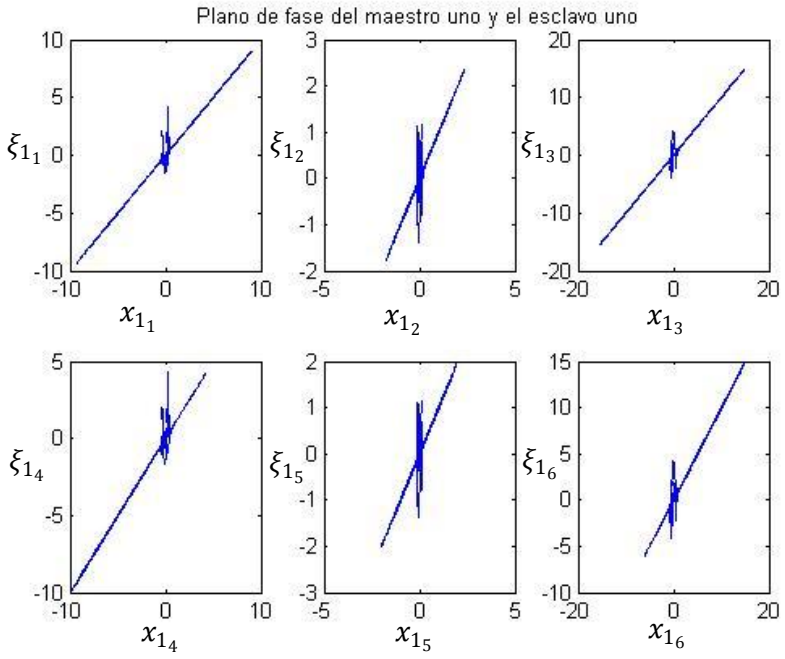

Figura 30. Plano de fase de la sincronía entre el maestro 1 y el esclavo 1 en el espacio de estados.

La figura 31 y 33 muestran el error de sincronía entre el maestro uno y el esclavo uno y el maestro dos y el esclavo dos respectivamente.

El resultado del error de sincronía debe de ser cero para tener una sincronía entre el maestro y el esclavo, si el error es diferente de cero no se podrá recuperar la información en el esclavo.

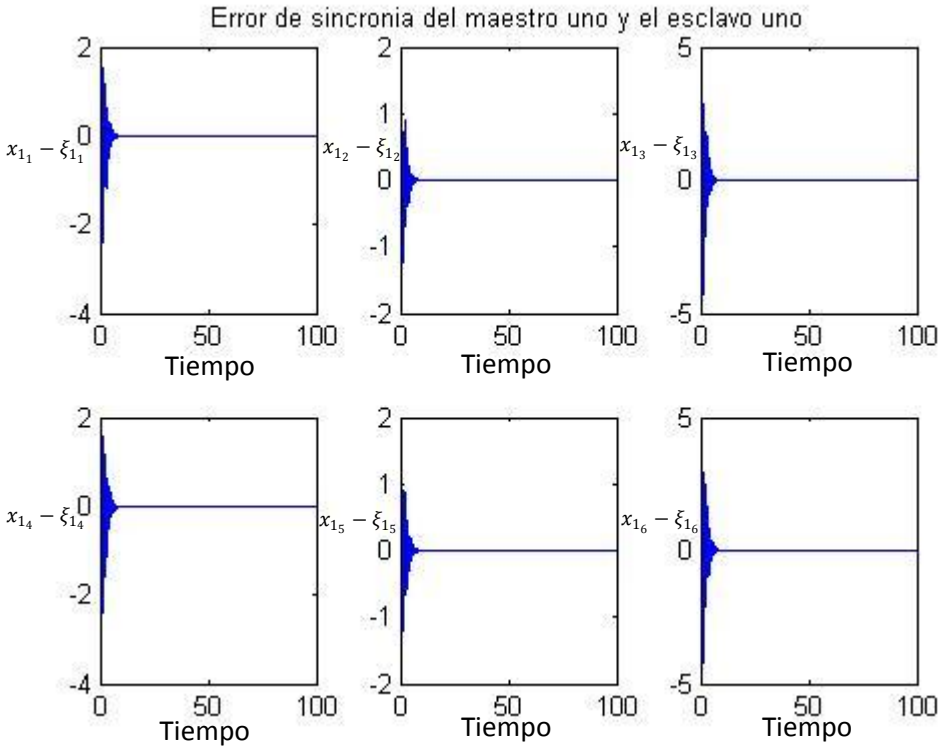

Figura 31. Se muestra el error de sincronía $e_{ij} = x_{ij}(t) - \xi_{ij}(t)$ para el maestro 1 y el esclavo 1, donde *i*=1 y *j*=1, 2, 3, 4, 5, 6.

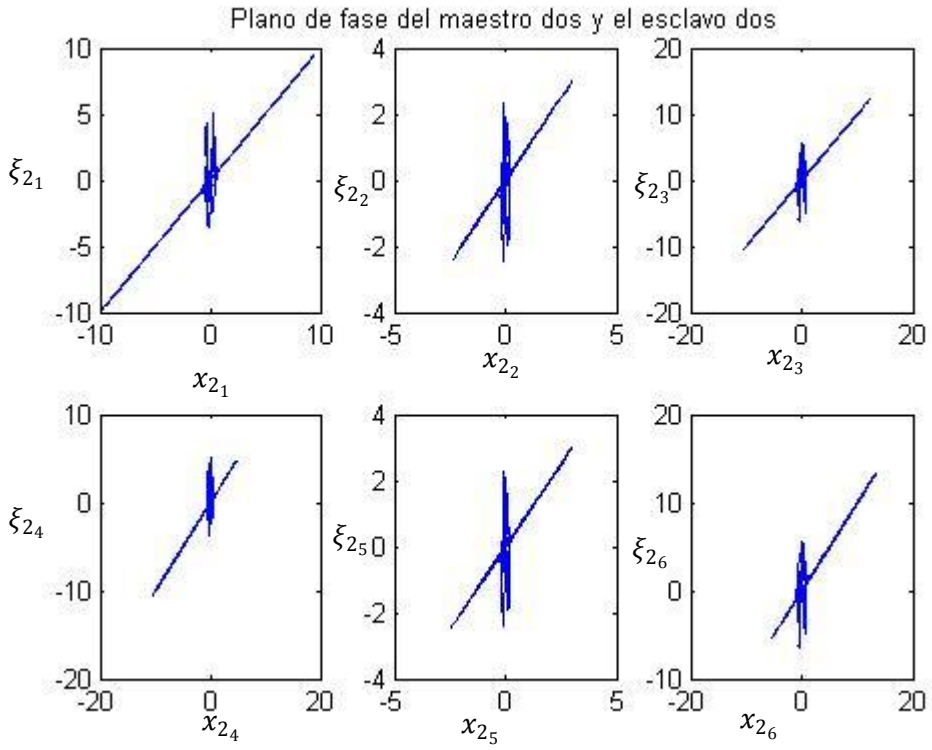

Figura 32. Plano de fase de la sincronía entre el maestro 2 y el esclavo 2 en el espacio de estados.

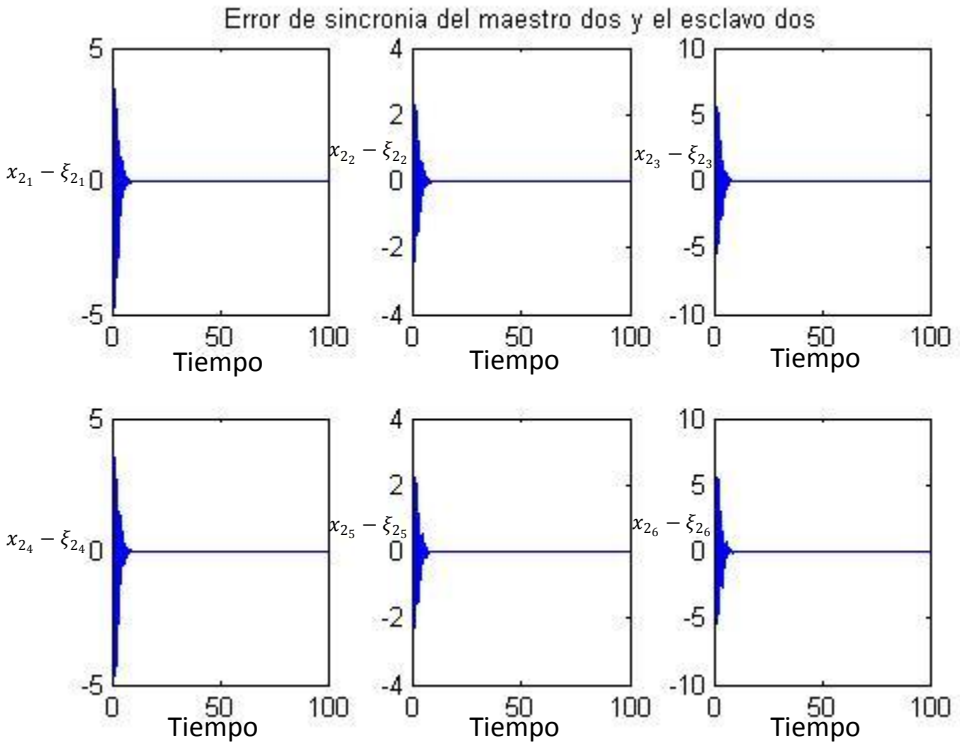

Figura 33. El error de sincronía $e_{ij} = x_{ij}(t) - \xi_{ij}(t)$ para el maestro 2 y el esclavo 2, donde *i*=2 y *j*=1, 2, 3, 4, 5, 6.

En la figura 34 se muestra que no existe sincronía entre el maestro dos y el esclavo uno. Así que es obvia la diferencia entre ellos con eso es suficiente para que un esclavo no pueda conocer la información del otro esclavo y viceversa.

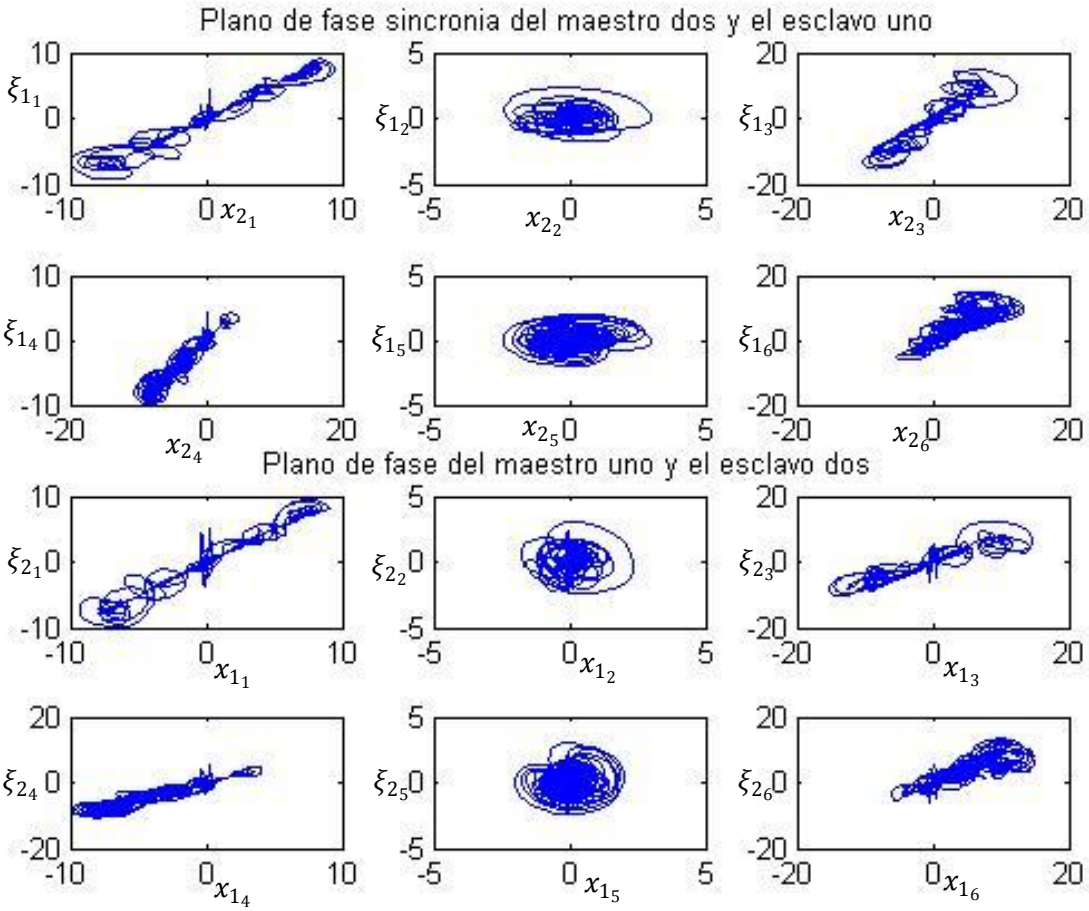

Figura 34. Muestra el plano de fase entre los estados caóticos del maestro uno y el esclavo dos, también del maestro dos y el esclavo uno. Se observa que existe no existe una pendiente de 45 grados, las dinámicas son diferentes en todo el tiempo por ende no hay sincronía entre ellos.

Capitulo 7

7. Comunicación por los sistemas caóticos

Las señales caóticas con su característico ancho de banda, son candidatas naturales para codificar información, las señales resultantes tienen espectros expandidos, grandes anchos de banda y baja densidad de potencia espectral, lo cual hace más difícil la detección de la información oculta. Con los sistemas caóticos, es fácil producir señales con estas características debido a la sensibilidad a las condiciones iníciales y variación de los parámetros. Así que, generar caos representa en bajo costo y su empleo proporciona una gran variedad de medios para las comunicaciones de espectro expandido [Cruz, C. y Nijmeijer, H., 2000].

Obtenida la sincronización unidireccional de dos sistemas caóticos, puede emplearse de distintas maneras para codificar información confidencial. En el contexto de las comunicaciones, de manera general, el oscilador maestro es el sistema transmisor y el oscilador esclavo es el sistema receptor. Existen varias formas de encriptado, aquí solo se verán tres de ellas.

7.1. Comunicación caótica aditiva empleando dos canales de transmisión

Con el propósito de recuperar o reconstruir exactamente la información cifrada en el receptor, en esta parte de la tesis, se usa el encriptado caótico aditivo, empleando dos canales de transmisión [Cruz, C. y Nijmeijer, H., 1999]. Como se ilustra en la figura 35, este esquema de comunicación consiste en sincronizar los sistemas en configuración maestro y esclavo, por un canal $y(y) = x_1(t)$, mientras que la información confidencial m(t) es sumada en otra señal caótica $x_2(t)$, esta señal se envía utilizando un segundo canal de transmisión [Ulysses Ronquillo, 2009].

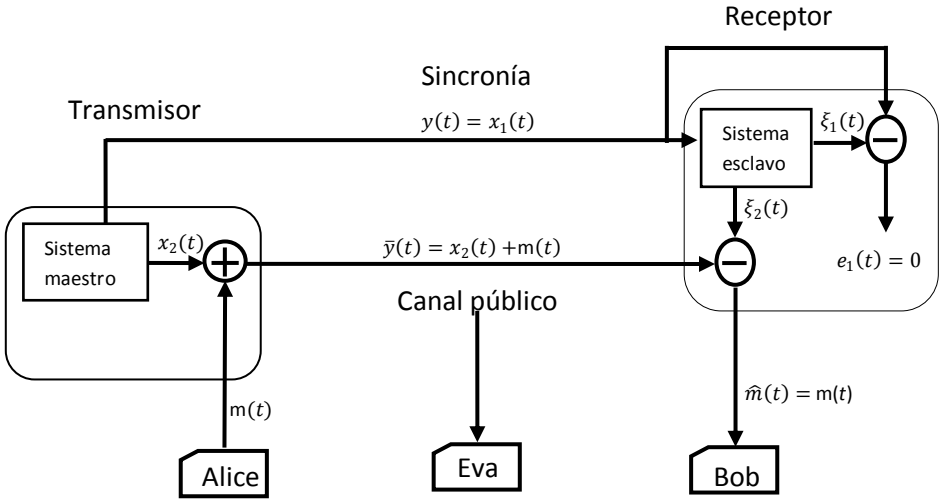

Figura 35. Esquema de encriptado caótico aditivo empleando dos líneas de transmisión.

La reconstrucción de la información confidencial, se lleva a cabo realizando la substracción a la señal recibida $y(t) = x_2(t)$ + m(t) y a $x_1(t)$ para la recuperación fiel de la información original. Es importante observar que el error de sincronía $e_1(t) = x_1(t) - \varepsilon_1(t) = 0$, por lo cual, $\hat{m}(t)$= m(t).

7.2. Encriptado por conmutación entre atractores caóticos

En esta última parte, se presenta un esquema de comunicación caótica, dedicado a la transmisión de información digital. La transmisión de información privada por conmutación entre dos atractores caóticos, consiste en seleccionar uno o más parámetros del sistema maestro (transmisor) y alternarlos entre dos valores distintos p y p′, cuidando que el transmisor se mantenga funcionando en régimen caótico todo el tiempo. Esto hará que el sistema transmisor se encuentre conmutando entre dos atractores caóticos distintos, un atractor caótico (Ap) generado con el valor p y otro (Ap′), generado por el valor p′. En el sistema receptor se mantiene fijo el conjunto de valores de parámetros p, es decir aquí se genera todo el tiempo el atractor caótico (Ap). Esto provoca que en un intervalo de tiempo, maestro y esclavo estén sincronizados (Ap = Ap) y en otro no (Ap′ 6= Ap). Este esquema

de comunicación caótica se emplea para transmitir solo información binaria [Nijmeijer, H. y Mareels, 1997]. En la figura siguiente, se muestra un diagrama de este esquema.

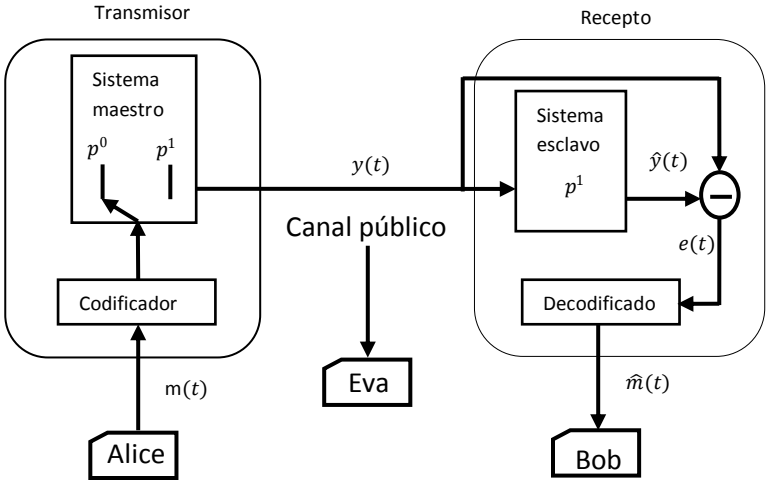

Figura 36. Configuración de comunicación por conmutación entre diferentes atractores caóticos.

7.3. Resultados de la simulación

Utilizando la comunicación caótica aditiva empleando dos canales de transmisión se asegura la sincronía y la encriptación, usando el segundo estado del maestro para sumar el mensaje, aun qué se puede utilizar x_3, x_5 y x_6. Así en la figura 37, 38 y 39 se observa este resultado con tres tipos de señales distintas, utilizando un mensaje diferente en cada imagen 0.2*seno(60*t), 0.2*seno((1+seno(0.2*t))) y un audio "hay peor miedo que el miedo mismo, ni mayor derrota que él no intentarlo" respectivamente,

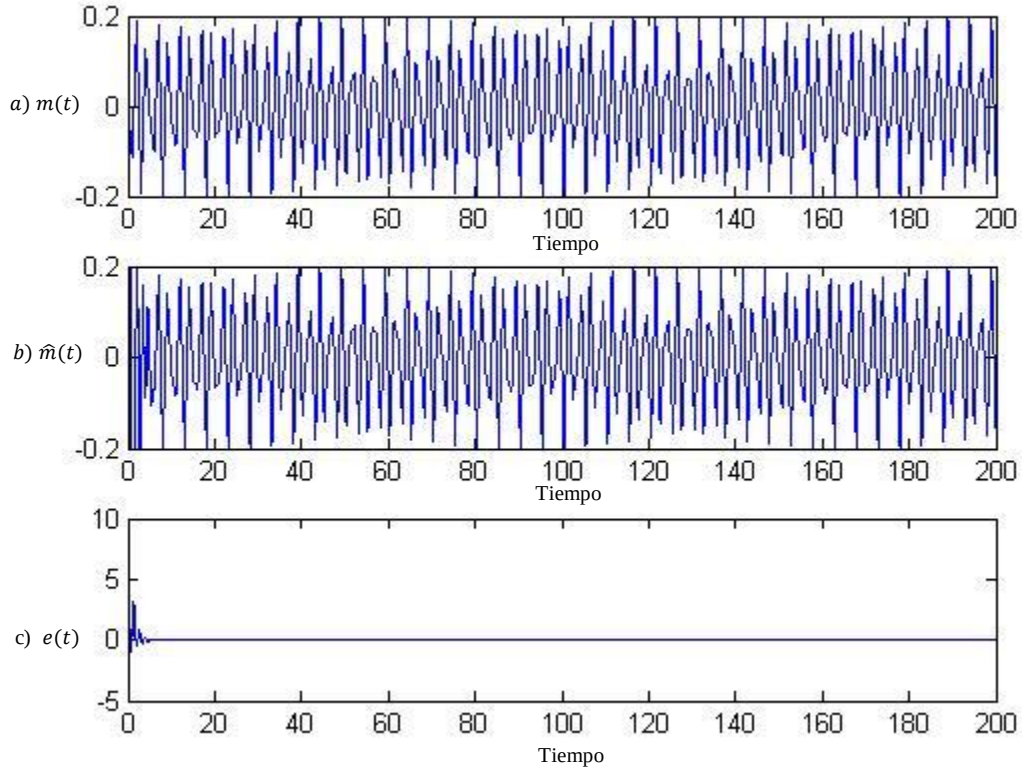

Figura 37. En la grafica se observa el mensaje a transmitir a), después en la b) se tiene el mensaje en el receptor el cual es idéntico al mensaje original pero con la parte del inicio diferente ya que esta no se puede identificar debido al transitorio. En la parte c) se comprueba que los mensajes son idénticos.

En la figura 37 se demuestra como es la recuperación del mensaje respecto al mensaje original, la parte a) es el mensaje original, es el mismo utilizado anteriormente en la configuración de encriptado caótico aditivo utilizando un canal, b) es el mensaje recuperado, como se ilustra en la grafica una pequeña parte de la información no es recuperada y por último es el error de sincronía donde se demuestra que si hay sincronía porque es igual a cero.

La grafica 38 utiliza este mensaje 0.2*seno((1+seno(0.2*t))) y se comprobó que la encriptación, sincronía y recuperación del mensaje es el esperado.

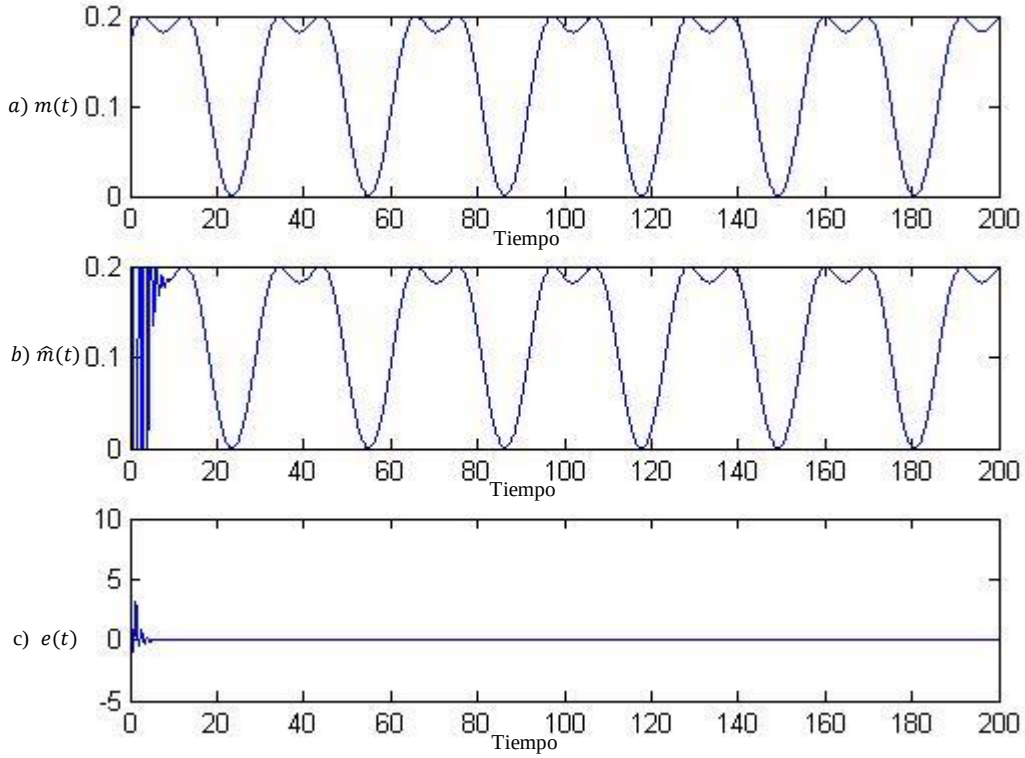

Figura 38. Ilustra en a) el mensaje a transmitir, en b) es el mensaje en el receptor el cual es idéntico al mensaje original pero con la parte del inicio diferente y la c) se comprueba que los mensajes son idénticos.

El sonido es encriptado en la figura 39, el cual tiene el mismo resultado que las graficas 37 y 38, hay que recalcar que una señal muy grande en amplitud se debe adecuar para poder hacer un encriptado y transmitirla.

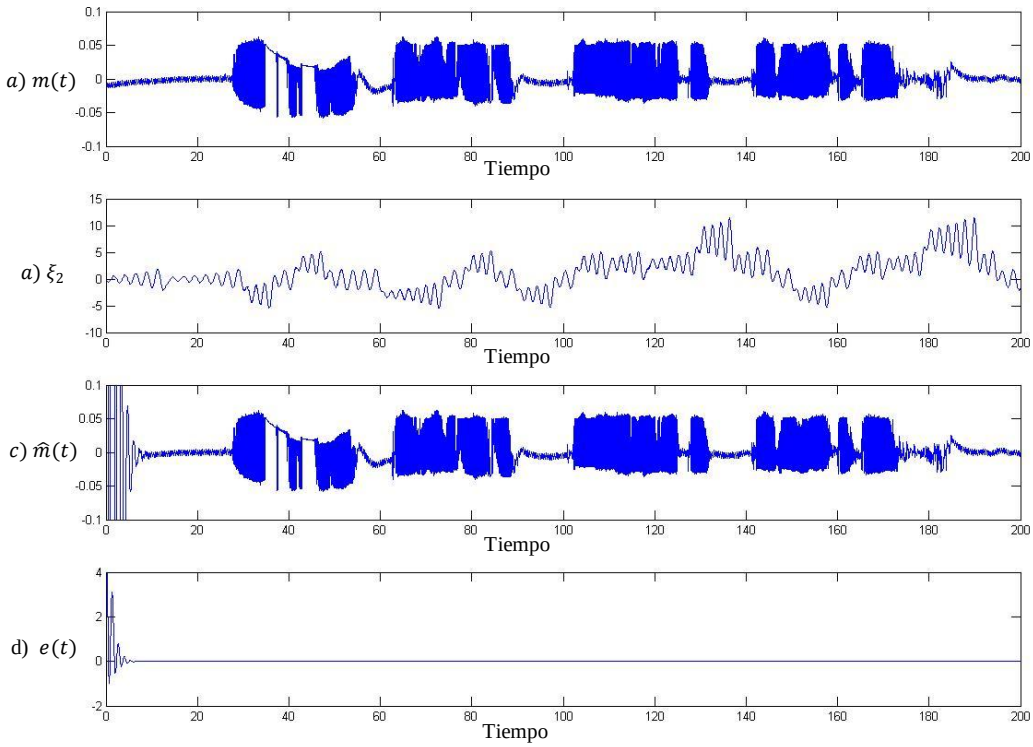

Figura 39. Esta imagen tiene un mensaje de audio, "no hay peor miedo que el miedo mismo, ni mayor derrota que él no intentarlo", la cual es encriptado y el resultado es muy bueno en calidad de audio, solo que el archivo de audio a transmitir tiene que ser modificado en amplitud en una décima parte.

En figura 37 se observa como es el comportamiento de una de los estados de esclavo para este caso es ξ_1, en el se comprueba que en diferentes periodos de la señal no hay sincronía debido a que la comunicación paramétrica trabaja en este sentido. Al mandar un bit encriptado en un sistema caótico paramétrico, se cambia uno o algunos de los parámetros, para este ejemplo el bit "1" significa que no hay sincronía y un bit "0" es que la hay.

El mensaje de bits a encriptar fue el siguiente [1 0 1 0 1 0 1 0 1], donde se observa que los dos primeros bits son "1" y por ende no hay sincronía, cabe resaltar que después de cambiar los parámetros al sistema caótico paramétrico se tiene un tiempo transitorio para que estén en sincronía. Este transitorio es de suma importancia en el tiempo de muestreo.

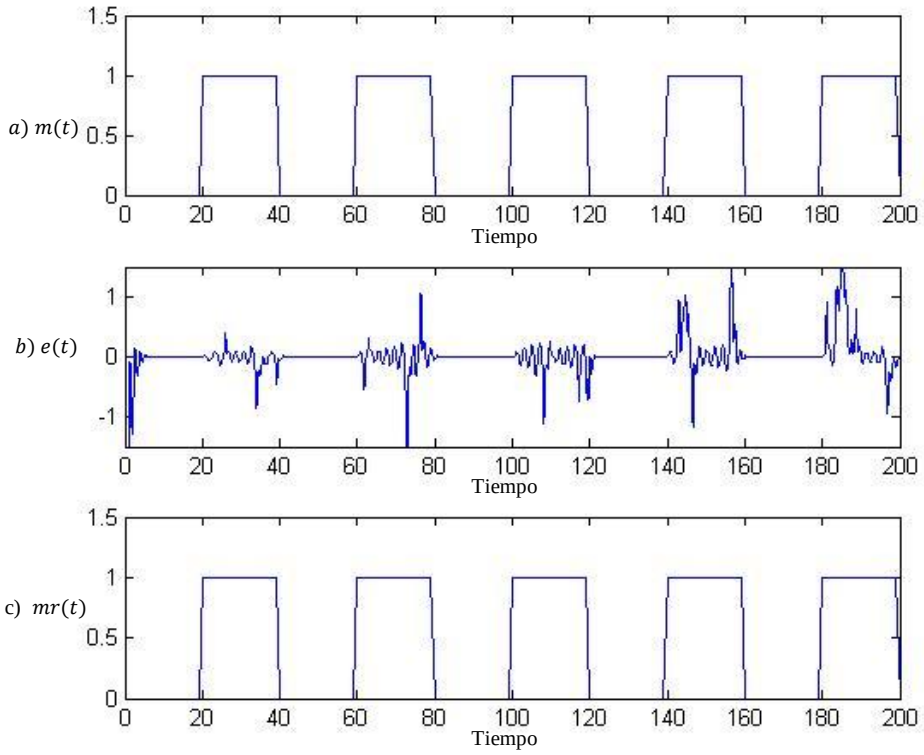

Figura 40. Se ilustra en a) como es el mensaje de bits, en b) se observa como es el comportamiento del estado de error ξ_1 y c) la recuperación de la cadena de bits que se encripto. El transitorio se puede observar cuando pasamos de un bit "1" a un "0".

Capitulo 8

Conclusiones generales, aportaciones y trabajo a futuro

A continuación se mencionan algunas **conclusiones generales** sobre este trabajo de investigación.

En este trabajo de tesis se realizó la aplicación de sistemas hipercaótios al encriptado y transmisión de información utilizando el circuito de Chua de sexto orden, el cual exhibe el comportamiento hipercaótico requerido para este trabajo.

Se obtuvieron resultados numéricos de las dinámicas hipercaóticas que genera el circuito de Chua de sexto orden.

La sincronización con un observador diseñado a partir de la forma hamiltoniana de las ecuaciones de estado de ese circuito, metodología propuesta en [Sira-Ramírez y Cruz-Hernández 2000; 2001] se obtuvo numéricamente.

Se logró la sincronización en una red de usuarios por medio de la configuración N maestros con N esclavos, se obtuvieron los resultados numéricos.

Con base en esta sincronía se realizó la comunicación entre un transmisor y un receptor, donde el mensaje fue sumado al estado del transmisor con el cual se sincronizaron los circuitos de Chua de sexto orden, y el mensaje se recuperó en el receptor de manera satisfactoria, en esta transmisión de información se tuvieron resultados numéricos.

En cuanto su aplicación a la comunicación punto a punto, se logró realizar la transmisión de manera segura para información analógica y digital, recuperando la información transmitida.

Con estos resultados obtenidos se cubre el objetivo de la tesis.

Las **aportaciones** que generó este trabajo de tesis fueron las siguientes:

1. **Comunicación Secreta con Base en Sincronía de Atractores Caóticos con Múltiples Enrollamientos**, presentado en el Congreso Anual de la Sociedad Mexicana de Instrumentación (SOMI), celebrado en Xalapa, Veracruz realizado del 1 al 3 de octubre de 2008.

2. **Secret communications using synchronized sixth-order Chua's circuits**, CESSE 2009, París realizado del 24 al 26 de Junio de 2009.

El **trabajo futuro** con el cual se puede continuar este trabajo de tesis se presenta a continuación:

- Realizar experimentalmente el Chua de seis estados.
- Realizar comunicación (digital y analógica) entre maestro y esclavo experimentalmente.
- Realizar la comunicación en red entre N maestros y N esclavos en forma numérica y experimental.
- Análisis de la información recuperada en presencia de ruido en el canal de trasmisión.
- Extender este trabajo a sincronización de redes.

Bibliografía

[Aguilar A. y Cruz C, 2002] Aguilar, A. y Cruz, C. [2002]. “Synchronization of two hyperchaotc Rossler systems: Modelmatching approach", WSEAS Transaction on systemss, 1(2), 198-203.

[Aguilar-Bustos Ana, 2005] Aguilar-Bustos Ana [2005]. Sincronización de osciladores caóticos discretos. Tesis de doctorado, Centro de Investigación Científica y de Educación Superior de Ensenada (DET-CICESE).

[Arena *et al.*, 1995] Arena P., Baglio S., Fortuna L., y Manganaro G. [1995] “Chua’s Circuit Can Be Generated by CNN Cells”, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS-I: 42, NO. 2, pp. 123-125.

[Belmonte I. *ed al.*, 2006] Belmonte I. Rubén, Noriega U. David ed. All.,”Sincronización de sistemas complejos”, CICESE, Ensenada, B.C., a 18 de agosto de 2006.

[Chua *ed al.* 1992] Chua, L. O., Kokarev, Lj., Eckert, K., Itoh, M., [1992]. “Experimental chaos synchronization in Chuat,s circuit", Int. J. Bifurc. Chaos 2(3), 705-708.

[Cruz, C. y Nijmeijer, H, 1999] Cruz, C. y Nijmeijer, H. [1999] “Synchronization through extended Kalman …ltering,” New Trends in Nonlinear Observer Design, eds.

[Cruz, C. y Nijmeijer, H, 2000] Cruz, C. y Nijmeijer, H. [2000]. “Synchronization through …ltering,” Int. J. Bifurc. Chaos 10(4), 763-775.

[Cuomo *ed al.*, 1993] Cuomo, K. M., Oppenheim, A. V. y Strogratz, S. H. [1993]. “Synchronization of Lorenz based circuits with applications to communications,” IEEE Trans. Circuits Syst. II 40(10), 634-642.

[Diaz E. *ed al.*, 2003] Díaz E., Gámez L., Ayala P., C. Cruz-Hernández y Núñez R. [2003] "Sincronización de atractores con múltiples enrollamientos y una aplicación a la comunicación secreta", *Memorias del Congreso Nacional de Control Automático de la AMCA2003,* 15-17 de octubre, Ensenada B.C., México. 6p.

[Feldman, U., 1996] Feldmann, U., [1996]. “Comunication by chaotic signals: The inverse system aproach", Int. J. Circuit Theory and Applications 24, 551-579.

[Fradkon. A. L. y Pogromsky, A. Yu., 1998] Fradkov, A.L. y Pogromsky, A. Yu., [1998]. “Introduction to control of oscilations and chaos", World Scienti…cvol. 24, Singapure.

[Fujisaka, H y Yamada, T., 1983] Fujisaka, H. y Yamada, T. [1983]. Stability theory of synchronized motion in coupled-oscillator systems, Prog. Theor. Phys. 69(1), 32-47.

[Gámez G. Luis M., 2004] Gámez Guzmán Luis Manuel, *Encriptador de información con base en la sincronía de atractores con enrollamientos múltiples,* DET-CICESE. 20 de agosto de 2004.

[Gámez L. *ed al.*, 2004] Gámez L., C. Cruz-Hernández y Núñez R. [2004] "Sincronización de atractores con enrollamientos de 3x3 en cuadrícula 2D: aplicación a la comunicación secreta", *Memorias del Congreso Latinoamericano de Control Automático,* 10 al 15 de mayo de 2004, La Habana, Cuba. 6p.

[Inixia, 2009] INIXI seguridad de la información-seguridad informática-soluciones en criptografía y cifrado de información. **INIXA · ©2003** www.inixa.com/seguridad_criptografia.php (02/06/2009)

[Madan N. R., 1993] Madan N. R. [1993], *Chua´s circuit: a paradigm for chaos*, World Scientific Series on Non-linear Science. Series B, Vol. I, Singapore, 1088 pp.

[Mejia A., 2007]Mejia Camacho, "*Encriptamiento de información mediante caos"*, Universidad Autónoma de Baja California, marzo de 2007.

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

[Número especial, 1997] Número especial [1997] sobre "Chaos synchronization an control: Theori and applications," IEEE Trans. Circuits syst. I,44(10).

[Número especial, 2000] Número especial [2000] sobre "Control and synchronization of chaos," IEEE Trans. Circuits syst. I, 10(34).

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

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

[Romero-Haros, 2005] Romero-Haros Néstor [2005]. Sincronización del circuito de chua con retardo: aplicación a la transmisión secreta de información', tesis de maestría, Centro de Investigación Científica y de Educación Superior de Ensenada (DET-CICESE).

[Schweiser J., *et al.*, 1995] Schweiser J., Et Al.(1995),"Synchronization theorem for a chaotic system", *Int. J. Bifur. Chaos,* **5**(1), 297-302 pp.

[Serrano G. H., 2002] Serrano Guerrero Hazael [2002]. Implementación de un sistema encriptador con base en la sincronía de circuitos de Chua. Tesis de maestría, Centro de Investigación Científica y de Educación Superior de Ensenada (DET-CICESE).

[Serrano-Guerrero y Cruz-Hernández, 2002]Serrano-Guerrero y Cruz-Hernández, [2002]. "Sistema encriptador con base en la sincronía de circuitos de Chua," 2da Conferencia Internacional Automática 2002, 17 al 19 de Julio de 2002, Santiago de Cuba, Cuba.

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

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

[Sira-Ramírez y Cruz-Hernández, 2001] Sira-Ramírez H. y Cruz-Hernández C. [2001], "Synchronization of Chaotic Systems: A Generalized Hamiltonian Systems Approach", *International Journal of Bifurcation and Chaos,* Vol. 11, No. 5, pp. 1381-1395, mayo, 2001.

[Suykens *ed al.* 1997] Suykens, Curran, Chua. [1997]. 'Master-slave synchronization using dynamic output feeback'. Internacional journal of bifurcation and chaos, vol. 7, No. 3, 671-679,

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

www.wikipedia.com.

[Yang, T., 1995] Yang, T. [1995]. "Recovery of digital signals from chaotic switching," Int. J. Circuits Theory and Applications 23, 611-615.

[Yang y Chua, 1996] Yang, T. y Chua, L. O. [1996]. "Secure communication via chaotic parameter modulation," Int. J. of Bifurc. Chaos 3(6), 1619-1627.

[Yang *ed al.*, 1997] Yang, T.,Wu, C.W. and Chua, L.O. [1997]. "Cryptography based on chaotic systems," IEEE Trans. Circuits Syst. I 44(5), 469-472.