Universidad Autónoma de Baja California

Facultad de Ingeniería Ensenada

Maestría y Doctorado en Ciencias e Ingeniería (MyDCI)

Comunicaciones seguras en una red de usuarios utilizando sistemas hipercaóticos

TESIS

Con el objetivo de cubrir parcialmente los requisitos para obtener el grado de MAESTRO EN INGENIERÍA presenta:

Oscar Ricardo Acosta Del Campo

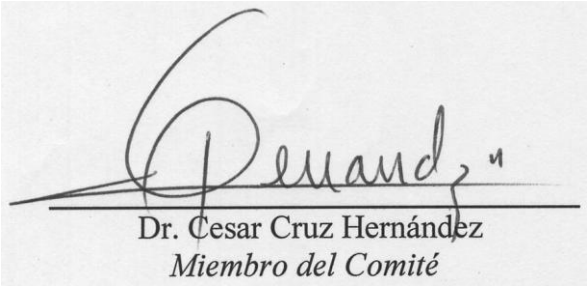
Ensenada Baja California, México Julio de 2009

TESIS DEFENDIDA POR

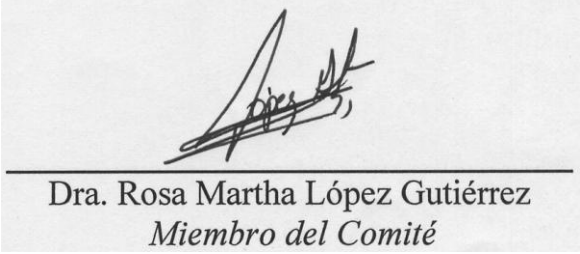
Oscar Ricardo Acosta Del Campo

Y APROBADA POR EL SIGUIENTE COMITÉ

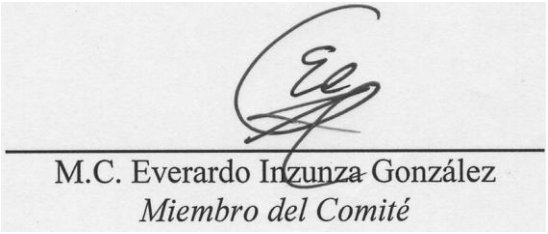
Dr. Enrique Efrén García Guerrero
Director del comité



Dr. Cesar Cruz Hernández
Miembro del Comité



Dra. Rosa Martha López Gutiérrez
Miembro del Comité



M.C. Everardo Inzunza González
Miembro del Comité

Ensenada Baja California, México, Julio 2009

RESUMEN de la tesis de OSCAR RICARDO ACOSTA DEL CAMPO, presentada como requisito parcial para la obtención del grado de MAESTRO EN INGENIERÍA. Ensenada, Baja California, México, Julio de 2009.

Comunicaciones seguras en una red de usuarios utilizando sistemas hipercaóticos

Resumen aprobado por:

Dr. Enrique Efrén García Guerrero
Director del comité

Este trabajo versa sobre la transmisión segura de información confidencial. El encriptado se produce por sincronía de sistemas hipercaóticos, la cual, se obtiene del diseño de un observador no lineal. En particular, se emplea como generador de hipercaos al circuito de Chua de cuarto orden, caracterizado por una no linealidad cubica suave, cuya implementación física no requiere gran cantidad de circuitería electrónica comparada con la de la función no lineal por segmentos en que se basa el circuito original de Chua. Comportamiento hipercaótico significa que el sistema tiene más de un exponente de Lyapunov positivo, es decir, sus dinámicas se expanden no solo en una dirección sino en dos o más direcciones, obteniéndose con esto, un incremento en la complejidad del sistema. Esta propiedad hace que el sistema hipercaótico sea grandemente atractivo para su empleo en comunicaciones seguras.

En este trabajo de tesis, se proporcionara un estudio analítico sobre condiciones que garantizan la convergencia del error de sincronía. Finalmente, se da una aplicación al encriptado, transmisión y desencriptado de información.

Palabras clave: Circuito de Chua de cuarto orden, hipercaos, sincronización de hipercaos, observador, formas hamiltonianas, comunicación secreta.

Dedicatoria

A mis padres, Pablo Acosta y Rosa M. Del Campo por darme la vida ya que gracias a ellos soy quien soy hoy en día, fueron los que me dieron el cariño y amor necesario, son los que han velado por mi salud, mis estudios, mi educación alimentación y muchas cosas más, son ellos a quien les debo todo, horas de consejos , de regaños, de tristezas y de alegrías lo cual estoy seguro que lo han hecho con todo el amor del mundo para formarme como un ser de bien y de los cuales me siento muy orgulloso.

A mis hermanos, Pablo, Jennifer, Breeanna y Marissa por el cariño y apoyo que me dan, por todo lo que hemos compartido y todos los momentos significativos que hemos vivido.

Agradecimientos

A todos los miembros de mi comité de tesis al Dr. Enrique Efrén García, al Dr. Cesar Cruz, a la Dra. Rosa Martha López y al M.C. Everardo Inzunza por sus valiosas sugerencias, consejos y acertados aportes durante el desarrollo de este trabajo, pero sobre todo por su amistad.

A todos mis amigos por su amistad, apoyo y por todos los momentos que han hecho que la vida sea más sencilla y alegre.

A Roxana por su amor, comprensión y su constante apoyo, gracias por estar siempre que te necesito.

A todos mis maestros porque son ellos los que a lo largo de mi vida me han ido forjando con todos sus conocimientos y enseñanzas.

A CONACYT por el apoyo económico brindado a este trabajo de tesis.

Lista de figuras

Índice general

Capítulo 1

Capítulo 2

Capítulo 3

Capítulo 4

Capítulo 5

Capítulo 6

Capítulo 7

Capítulo 8

Capítulo 9

Capítulo 1

Introducción

1.1 – Motivación

En la actualidad ha aumentado la demanda de servicios de comunicación, que es soportada por un rápido incremento en la transmisión y capacidad en las redes de comunicación. El *software* adecuado es usual para el cifrado de datos, pero el continuo incremento en avances científicos, tecnológicos y el aumento en la velocidad de cálculo de las computadoras amenaza la seguridad de estos procesos, es por ello que se han buscado alternativas de solución para este problema, muchas de estas opciones involucran sistemas muy complejos para su implementación y los cuales la mayoría de las veces son demasiado caros, lo que provoca que no sean tan accesibles para la mayoría de las aplicaciones.

Por este motivo se requiere de sistemas menos complejos y más accesibles sin disminuir su capacidad de protección de información. A partir que se logró la sincronización de sistemas caóticos [Pecorra y Carroll 1990] se presentó la posibilidad de utilizarlos para la encriptación de información y de esta manera, tener un sistema eficiente para ocultar información de una manera muy segura, y al mismo tiempo, disminuyendo su complejidad con respecto de otros sistemas de encriptado.

Con las técnicas de modulación y demodulación apropiadas, la naturaleza aparentemente aleatoria y las propiedades espectrales similares al ruido de las señales caóticas e hipercaóticas hacen que pueden ser usadas para proporcionar simultáneamente la expansión y modulación de una transmisión de información.

1.2 - Planteamiento del problema de estudio

Es difícil imaginar cómo sería la vida moderna sin el acceso fácil a medios de comunicación fiables, económicos y eficientes. Ciertamente, la *comunicación* es la transmisión o conducción de información de un punto a otro ubicado remotamente, donde muchas de las veces, este enlace se tiene que hacer de manera segura o restringida, por medio de un canal público, donde sólo usuarios autorizados puedan conocer esa información.

Almacenar, transmitir y procesar información privada (sea voz, audio, datos o imágenes) de manera segura, es un problema al que se ha enfrentado la humanidad desde tiempos remotos. Una manera confiable de resguardar esta información es recurriendo al encriptado. Podemos decir, que *encriptamiento* es el proceso de *revolver* u *ocultar* el contenido de un mensaje con el propósito de hacer a éste incomprensible a toda persona no autorizada, es decir, que no cuente con la "clave" (o "llave") con la que se llevó a cabo este proceso.

Por ejemplo, consideremos el siguiente escenario: si **Alicia** (transmisor) desea comunicarse de manera segura con **Bob** (receptor remoto) y no quiere que ninguna otra persona se entere de qué información está transmitiendo, entonces encripta la información empleando una clave secreta, de esta manera la mantiene segura de **Oscar** (intruso o receptor no autorizado). Por tanto, **Alicia** encriptará la información utilizando la clave y enviará la información encriptada a través de un canal público de transmisión a **Bob**, de esta manera, solamente la persona que tenga la clave, podrá descifrar la información. Por tanto, si **Bob** tiene la clave (con acceso a la señal que transmite **Alicia** a **Bob**), entonces podrá saber el contenido de la información, en cambio, **Oscar** sin la clave no tendrá acceso a dicha información, este proceso de comunicación segura se muestra en la figura 1.

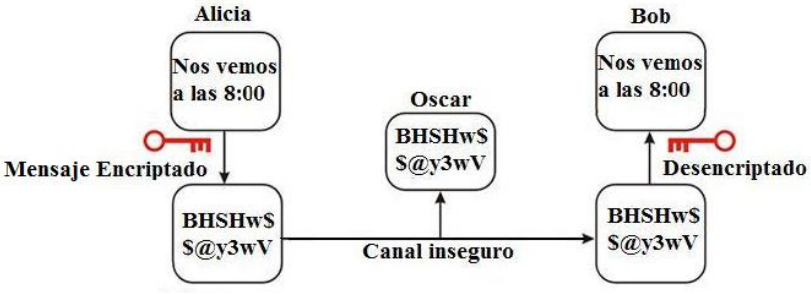


Figura 1. Proceso de encriptado en la transmisión de información.

La comunicación empleando sistemas hipercaóticos es una manera de transmitir información segura, ya que un sistema hipercaótico se puede tratar como un caso especial de un generador de secuencias pseudoaleatorias con la principal diferencia de que un sistema hipercaótico posee un número infinito de estados analógicos, mientras que un generador pseudoaleatorio presenta un número finito de estados analógicos. Una secuencia aleatoria es producida visitando cada estado del sistema una vez, de una manera determinista. Si tenemos un número finito de estados para visitar, la secuencia de salida será irremediablemente periódica. En contraparte, si disponemos de un generador hipercaótico se podrá visitar un número infinito de estados de una manera determinista y por lo tanto, producir una secuencia de salida que nunca se repita, de esta forma podríamos transmitir información de manera segura.

Los primeros intentos para usar señales aleatorias en comunicaciones seguras fueron probablemente debidos a **Vernam**, los cuales datan de 1926. Desde entonces, tal uso ha puesto una considerable relevancia en la criptografía. La importancia del concepto de sincronización caótica en comunicaciones seguras ha sido muy destacada por el procesamiento de señales, circuitos y comunicaciones seguras. Por ejemplo, en particular la sincronización de hipercaos puede usarse para codificar información añadiendo una señal hipercaótica a una señal que se desee transmitir como mensaje o información, la señal hipercaótica usada es reproducida por el receptor gracias a la sincronización.

Dadas la características de las señales caóticas existe un enorme interés en la explotación de las propiedades del caos en comunicaciones seguras, además, que poseen un espectro de banda ancha y pueden ser generadas con una circuitería relativamente sencilla, es por ello que se consideran como la solución idónea para la transmisión segura de información. Aprovechando estas propiedades naturales de los sistemas hipercaóticos (generadores de dinámicas más complejas que las generadas por los sistemas caóticos) en este trabajo de tesis se plantea realizar el encriptado de información a partir de la sincronía de osciladores hipercaóticos, en particular, sincronizar los sistemas utilizando la metodología hamiltoniana y diseño de observador metodología propuesta en [Sira-Ramírez y Cruz-Hernández 2000; 2001].

1.3 – Antecedentes

En los trabajos de Fujisaka y Yamada [1983] y de Pecora y Carroll [1990] se demostró tanto téorica como experimentalmente la sincronía de sistemas caóticos. En la literatura se reportan diferentes métodos (ver por ejemplo [Aguilar y Cruz 2002; Chen y Dong 1998; Chen y Ueta 2002; Cruz y Nijmeijer 2000; Cruz y Martynyuk 2009; Feldmann 1996; Fradkov y Pogromsk 1998; González 2004; Kapitaniak 2000; Lakshmanan y Murali 1996; López y Cruz 2005; Nijmeijer y Mareels 1997; Número especial 1997; Número Especial 2000; Ogorzalek 1997; Sira y Cruz 2000; 2001; Wu 2002] y sus referencias). 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 han propuesto para este fin, por ejemplo, encriptado aditivo [Cuomo, *et al.* 1993], conmutación entre dos atractores caóticos [Parlitz, *et al*. 1992] y modulación paramétrica [Yang y Chua 1996] y otras técnicas vistas por ejemplo en [Cuomo y Oppenheim 1993; Cruz y Serrano 2005; Cruz, López, García, Serrano y Núñez 2005; Dedieu y Kennedy 1993; Kennedy, Chua, Kocarev, Halle y Shang 1992; López y Cruz 2001;Palaniyandi P, Lakshmanan 2001; Yang y Chua 1996; Yang, Wu y Chua 1997; Wu y Chua 1993;]. Sin embargo, algunos trabajos posteriores mostraron que estas técnicas tienen un grado de seguridad poco confiable (ver por ejemplo [Alvarez, Montoya, Romera y Pastor 2004; Short 1994; Pérez y Cerdeira 1995; Short 1996; Short 1998;Yang 1995]). Para enfrentar 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 2002] se propone el uso de formas hamiltonianas y diseño de un observador para sincronizar dos circuitos hipercaóticos de Chua acoplados unidireccionalmente. Algunos ejemplos de sincronización hipercaótica son [Aguilar y Cruz 2002; Cruz 2004; Cruz, Posadas y Sira 2002; Mensour y Longtin 1998; Peng, Ding y Yang 1996; Pyragas 1998]. Algunos ejemplos de la aplicación de sincronización de hipercaos a las comunicaciones los podemos encontrar en [Aguilar y Cruz 2008; Aguilar, Cruz, López y Posadas 2008 ; Brucoli, Cafagna y Carnimeo 1999; Cruz 2004; Cruz y Romero 2008; Gámez, Cruz, López y García 2008; Gámez, Cruz, López y García 2009; Mensour, Longtin 1998; Tamaševicius ,Cenys, Namaj, Mykolaitis 1998;]

El objetivo de este trabajo de tesis es la construcción física, utilizando circuitería electrónica de un sistema de encriptado hipercaótico con base en la sincronía de dos circuitos hipercaóticos de Chua modificados. El circuito hipercaótico de Chua modificado se expresa en forma hamiltoniana generalizada y de ahí se construye un observador de estado no lineal. Una vez sincronizados el maestro y el esclavo, se construye el sistema encriptador, con el fin de transmitir información altamente segura.

Es conveniente por el interés, mencionar algunos trabajos relacionados con el presente, derivados de tesis como [Gámez-Guzmán 2004; Mejía-Camacho 2007; Meranza-Castillón 2002; Romero-Haros 2005]

1.4 – Objetivos

Con la realización de la presente tesis de maestría, se pretende alcanzar el objetivo general:

Construir una red de comunicaciones con información encriptada a través de un sistema hipercaótico para la transmisión segura de información entre usuarios.

Y alcanzar los objetivos particulares:

Emplear un sistema hipercaótico con lo que se aumente la complejidad del encriptado: Simulación y experimental.

Sincronizar sistemas hipercaóticos empleando formas hamiltonianas y diseño de un observador no lineal de estado: Simulación y experimental

Transmitir información privada de manera segura, mediante la sincronización de los sistemas hipercaóticos.

Realizar la transmisión de información en una red de usuarios, empleando hipercaos: Simulación y experimental.

1.5 - Metodología adoptada

Para alcanzar los objetivos planteados se utilizará el circuito modificado de Chua de cuatro estados, generador de hipercaos y la metodología de sincronización por formas hamiltonianas y diseño de un observador no lineal de estado reportada en [Sira-Ramírez y Cruz-Hernández 2000; 2001].

Las señales hipercaóticas presentan dinámicas mucho más complejas que las caóticas [Kapitaniak y Chua 1994], la consecuencia de utilizar señales hipercaóticas como portadoras de información en un sistema de encriptamiento, es que el mensaje oculto en la señal transmitida sería más difícil de descifrar por personas ajenas al sistema de comunicación.

El circuito hipercaótico de Chua se expresa en forma hamiltoniana generalizada y se construye un observador no lineal. Estos osciladores se acoplan en una configuración de maestro y esclavo. Una vez sincronizados el maestro y el esclavo, se construye el sistema encriptador, con el fin de transmitir información altamente segura.

La justificación de por qué se adopta la sincronía de osciladores caóticos o hipercaóticos por formas hamiltonianas y el diseño de un observador, se mencionan a continuación algunas ventajas sobre otros métodos:

i) La sincronización se obtiene en forma sistemática.

ii) Muchos osciladores caóticos (incluso hipercaóticos) se pueden expresar en forma hamiltoniana.

iii) Este método no requiere el cálculo de ningún exponente de Lyapunov.

iv) Este método no requiere que las condiciones iniciales pertenezcan a la misma cuenca de atracción.

En concreto, se pretende implementar un sistema de encriptado hipercaótico, mediante circuitería electrónica, y de esta manera hacer la transmisión de información segura, utilizando como circuito encriptador al circuito modificado de Chua de cuarto orden reportado en [Thamilmaran y Lakshmanan 2004], el cual, presenta las dinámicas hipercaóticas necesarias.

1.6 – Organización de esta tesis

Este trabajo de tesis de maestría está organizado como sigue:

En el capítulo 1 se da una breve reseña acerca de la motivación para la realización de este trabajo de tesis, así como el planteamiento del problema de estudio y algunos antecedentes acerca de la comunicación hipercaótica, también se muestran los objetivos planteados para la realización de la tesis y la metodología adoptada para llevarla a cabo.

En el capítulo 2 se hace una descripción de los sistemas de encriptado primeramente con una pequeña introducción y enseguida con algunos conceptos básicos que serán mencionados a lo largo de este trabajo de tesis, después se habla del problema fundamental de la criptografía y enseguida algunos apuntes históricos acerca de la misma, también se mencionan las técnicas de encriptado utilizadas desde la antigüedad hasta la fecha, se menciona el objetivo del encriptado así como también algunas alternativas de solución al problema de encriptado y una propuesta de solución para esta tesis.

En el capítulo 3 se habla del caos, iniciando con una definición y breve historia, así como también las características que presentan estos sistemas. Además, se mencionan las aplicaciones donde está involucrado y se da un ejemplo de un sistema caótico, el conocido circuito de Chua, donde se muestran sus ecuaciones de estado y se ilustran algunas simulaciones numéricas, mostrando sus dinámicas tanto estables, periódicas y caóticas.

En el capítulo 4 se hace mención al circuito modificado de Chua utilizado en este trabajo de tesis, que es el circuito hipercaótico de Chua, donde se muestra también su circuito y las ecuaciones de estado que lo rigen, enseguida se hacen las simulaciones numéricas de las dinámicas que genera y también se presentan sus dinámicas en forma experimental.

En el capítulo 5 se presenta la sincronización por formas hamiltonianas y diseño de un observador, iniciando con una introducción donde se hace mención al fenómeno de sincronización así como con algunos antecedentes y definiciones, también se habla de los escenarios de acoplamiento para sistemas caóticos e hipercaóticos, y enseguida se habla de la sincronización que se utilizó en este trabajo de tesis que es la sincronización por formas hamiltonianas y diseño de un observador, donde se muestra el circuito utilizado expresado en forma hamiltoniana y se diseña un observador para este circuito y se realiza la sincronización entre ellos, por último se dan los resultados numéricos y experimentales de su sincronización.

En el capítulo 6 se da la sincronización por retroalimentación en combinación con la metodología hamiltoniana pero entre múltiples maestros y esclavos, aquí se muestran las ecuaciones de estado de los maestros y de los esclavos y enseguida se hace la sincronización y se muestran los resultados numéricos donde se muestran los estados con respecto al tiempo y los estados del maestro con respecto a los del esclavo donde se muestra la sincronía entre ellos gracias al plano de fase y por último se dan las graficas del error de sincronía donde se observa el tiempo de sincronía entre maestros y esclavos.

En el capítulo 7 se hace la sincronización en una red con otra configuración, es este caso la sincronización en configuración estrella, donde se muestran las ecuaciones del maestro y los esclavos los cuales imitaran las dinámicas del maestro, de igual manera se utiliza la metodología hamiltoniana para lograr la sincronía en esta configuración por último se dan los resultados numéricos pertenecientes a la sincronización, como los son las graficas en el tiempo de los estados del maestro y los esclavos y las graficas en el plano de fase donde se aprecia la sincronía y también las graficas de error de sincronía.

En el capítulo 8 se realizó la aplicación a las comunicaciones seguras, es decir, se realizó la comunicación para las diferentes configuraciones usadas en este trabajo de tesis, primero la comunicación entre un maestro y un esclavo donde la información es transmitida al esclavo y ahí es nuevamente recuperada, en la segunda configuración se hace la transmisión en una red de usuarios con N maestros y N esclavos y por último se realiza la transmisión de información en configuración estrella todo esto en forma numérica.

En el capítulo 9 por último, se dan las conclusiones generales acerca del trabajo de tesis, se mencionan las aportaciones que arrojo y también se dejan algunos problemas abiertos y trabajo a futuro que queda para una posterior realización.

Capítulo 2
Sistemas de encriptado

2.1 – Introducción

El ser humano siempre ha tenido secretos de muy diversa índole, y ha buscado mecanismos para mantenerlos fuera del alcance de miradas indiscretas. **Julio César** empleaba una sencilla técnica para evitar que sus comunicaciones militares fueran interceptadas. **Leonardo Da Vinci** escribía las anotaciones sobre sus trabajos de derecha a izquierda y con la mano zurda. Otros personajes, como Sir **Francis Bacon** y **Edgar Allan Poe** eran conocidos por su afición a los códigos criptográficos, que en muchas ocasiones constituían un apasionante pasatiempo y un reto para su ingenio.

En este capítulo del trabajo de tesis se proporciona un breve repaso de los mecanismos criptográficos considerados clásicos y modernos. Podemos llamar **criptografía clásica** a todos los sistemas de cifrado anteriores a la II Guerra Mundial o al nacimiento de las computadoras. Estas técnicas tienen en común que pueden ser empleadas usando simplemente lápiz y papel, y que pueden ser criptoanalizadas casi de la misma forma. De hecho, con la ayuda de las computadoras, los mensajes cifrados mediante el uso de estos códigos son fácilmente descifrables, por lo que cayeron rápidamente en desuso.

La transición desde la criptografía clásica a la moderna se da precisamente durante la II Guerra Mundial, cuando el Servicio de Inteligencia aliado rompe dos sistemas criptográficos empleados por el ejército alemán, la máquina ENIGMA y el cifrado de adjunto, considerados hasta ese momento absolutamente invencibles. Pero lo más importante de esa victoria es que se consigue a través de revolucionarios desarrollos matemáticos, combinados con el nacimiento de las computadoras modernas.

Todos los algoritmos criptográficos clásicos son de carácter simétrico, ya que hasta mediados de los años setenta del siglo pasado nació la criptografía asimétrica.

2.2 – Conceptos y definiciones

En este apartado se da una explicación breve del significado etimológico de criptografía, así como la utilidad práctica de ésta para la transmisión segura de información.

La palabra *criptografía* procede de los términos griegos: *kryptos* (oculto) y *graphos* (escritura). Es decir, *escritura oculta***.**

Del significado etimológico de la palabra, puede decirse que la criptografía es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos (conocedores de las claves). Con más precisión, cuando se habla de esta área

del conocimiento como ciencia se debería hablar de *criptología*, que engloba tanto las técnicas de cifrado, la criptografía propiamente dicha, como sus técnicas complementarias: el *criptoanálisis*, que estudia los métodos que se utilizan para romper información cifrada con objeto de recuperar la información original en ausencia de la clave.

A continuación se da una breve definición de los términos usados con frecuencia en el ámbito de la criptografía.

Texto en claro: Se trata de la información original a la cual queremos proteger (ver figura 2).

Cifrado: Proceso de conversión del texto en claro en un texto deformado de tal forma que solo sea legible por aquéllos a los que vaya dirigida la información. Las dos técnicas más comunes de cifrado dentro de la criptografía clásica son: *la sustitución*, que supone el cambio de significado de los elementos básicos del mensaje. Por ejemplo, una sustitución de las grafías del mensaje por sus correspondientes posiciones en el abecedario. A➔0. B➔1. C➔2…Y *la trasposición*, basada en cambiar el orden de los distintos elementos que componen el cifrado. Por ejemplo, puede ordenar las grafías de tal forma que sean leídas de forma inversa, eliminar los espacios en blanco, agrupar la información en bloques de longitud N, etc. Normalmente, se utilizan ambas técnicas para el cifrado clásico de un mensaje (ver figura 2).

Texto cifrado o criptograma: El texto resultante después de aplicar un determinado cifrado (ver figura 2).

Algoritmo de cifrado o cifra: Hace referencia a la metodología usada para el cifrado de los datos. Todo algoritmo de cifrado está basado en una clave. Existen dos grandes grupos de cifras: las *cifras simétricas*, aquellas que utilizan una única clave (denominada clave simétrica o privada) tanto para el proceso de cifrado como de descifrado, éstas constituyen la base de los algoritmos de cifrado clásico. Y por otro lado, las cifras asimétricas, las cuales usan una clave (denominada clave asimétrica o pública) para el cifrado del mensaje y otra distinta para el proceso de descifrado. Éstas últimas son el núcleo de la criptografía moderna (ver figura 2).

Clave: Información secreta que adapta el algoritmo de cifrado para cada uso distinto (ver figura 2).

Descifrado: es el proceso inverso que recupera el texto en claro a partir del criptograma y la clave (ver figura 2).

Protocolo criptográfico: Especifica los detalles de cómo deben utilizarse los algoritmos y las claves para conseguir el cifrado o descifrado de la información.

Sistema criptográfico: Se llama sistema criptográfico al conjunto de protocolos, algoritmos, claves e intervenciones requeridas por el usuario. Es el sistema criptográfico, con lo que el usuario final trabaja (ver figura 2).

Código: Es un tipo de algoritmo de cifrado clásico que consiste en sustituir un determinado fragmento textual por otro que guarda cierta similitud (ver figura 2).

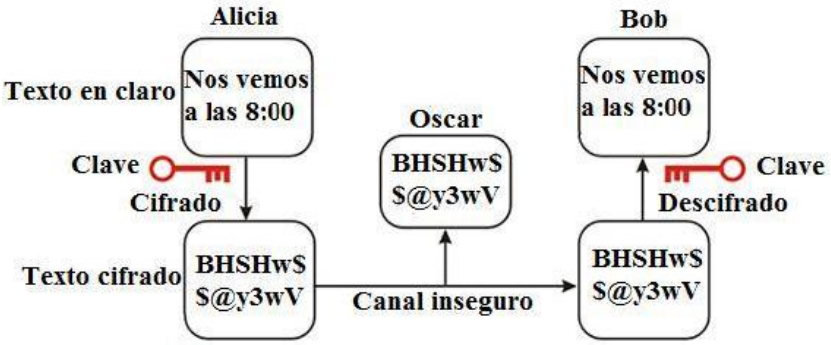


Figura 2. Diagrama de un sistema criptográfico.

2.3 – Problema de la criptografía

El problema al que se enfrenta, enfrentó y enfrentará la criptografía es que la seguridad en la transmisión de información es muy vulnerable, es por ello que se han desarrollado sistemas para evitarlo, sin embargo su eficiencia disminuye conforme pasa el tiempo, ya sea por los avances científicos, tecnológicos o por simple fuerza bruta, estos sistemas siempre serán vulnerables.

Es por eso que se requiere un constante avance en sistemas de encriptado y la investigación científica en cuanto a sistemas caóticos y su aplicación a la criptografía ha ido elevando su potencial para que en un futuro se conviertan en una solución alterna para el encriptado de información.

2.4 – Algunos apuntes históricos de la criptografía

La criptografía es tan antigua como la escritura. Desde que el *homo sapiens* inició su recorrido sobre este planeta, ha necesitado comunicarse con sus semejantes, pero en ocasiones no quiere que otros se enteren. Las razones son evidentes, ya que a ninguno le gustaría que el enemigo conociera su estrategia si lograse interceptar un mensaje.

Se dice que las primeras civilizaciones que usaron la criptografía fueron la egipcia, la mesopotámica, la india y la china. Los espartanos, 400 años antes de Cristo, utilizaban un sistema secreto de escritura, el cual consistía en un cilindro al cual se colocaba un papiro en forma de espiral. Se escribía entonces el texto en cada una de las vueltas del papiro, pero de arriba hacia abajo. Una vez desenrollado, sólo se podía leer una serie de letras aparentemente inconexas. Para descifrar el mensaje era necesario colocar el papiro exactamente en la misma posición en la que había sido escrito. Antiguos textos judíos fueron encriptados siguiendo el método de sustituir la primera letra del alfabeto por la última y así sucesivamente. En la Biblia (Jeremías 25:26) el nombre de *Babilonia* aparece encriptado como "Sheshech".

Pero a quien se atribuye el primer método de encriptado con su debida documentación es al general romano **Julio César**, quien creó un sistema simple de sustitución de letras, que consistía en escribir el documento codificado con la tercera letra que siguiera a la que realmente correspondía. La A era sustituida por la D, la B por la E y así sucesivamente. En la Edad Media el uso de la escritura codificada se incrementó. Un libro de astronomía escrito en 1390 y atribuido a **Geoffrey Chaucer** contiene trozos cifrados.

En 1470, **León Battista Alberti** publica el *Tratado de cifras* donde describe una cifra capaz de encriptar un pequeño código. No obstante se considera al abate **Johannes Trithemius** el padre de la criptografía moderna. Este religioso escribió en 1530 *Poligrafía*, el primer libro impreso sobre el tema. **Trithemius** introdujo el concepto de tabla ajustada, en el cual el alfabeto normal es permutado para codificar los mensajes. Son legendarios los mapas de tesoro escondidos durante los siglos XVII y XVIII. En ellos los piratas supuestamente encriptaban la localización de enormes tesoros, basándose principalmente en métodos de sustitución de alfabeto.

El principal uso de la criptografía en la era moderna ha sido militar. En 1917, por ejemplo, el servicio de Inteligencia Naval de Inglaterra entregó a los Estados Unidos un mensaje que había sido enviado al embajador alemán en Ciudad de México por el gobierno germano. En el mismo se autorizaba al diplomático a negociar un acuerdo con México para entrar a favor de Alemania en la Primera Guerra Mundial. A cambio, los mexicanos recibirían los territorios de Nuevo México, Arizona y Texas, en el caso de que resultasen vencedores. El texto conocido como el telegrama *Zimmermann* impulsó a los norteamericanos a participar en esa guerra contra Alemania.

Los códigos de la máquina Enigma, usada por los mismos alemanes durante la Segunda Guerra Mundial, fueron rotos por los analistas norteamericanos, al igual que los códigos usados por los japoneses.

La innovación vendría de la mano de las máquinas de cálculo para el cifrado de la información. La más conocida de las máquinas de cifrado, posiblemente sea la máquina alemana Enigma, una máquina de rotores que automatizaba considerablemente los cálculos que era necesario realizar para las operaciones de cifrado y descifrado de mensajes.

En la figura 3 se muestra la máquina de cifrado adjunto y en la figura 4 se muestra la maquina Enigma las cuales fueron usadas durante la Segunda Guerra Mundial.

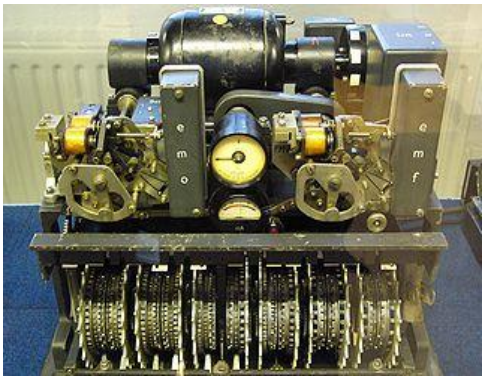


Figura 3. Máquina alemana de cifrado adjunto, usada en la Segunda Guerra Mundial para el cifrado de los mensajes por los generales de alto rango. (Imagen tomada de http://es.wikipedia.org/wiki/Criptografia)

Figura 4. Máquina Enigma utilizada por los alemanes durante la II Guerra Mundial. (Imagen tomada de http://es.wikipedia.org/wiki/Criptografia)

Tras la conclusión de la Segunda Guerra Mundial, la criptografía experimentó un gran desarrollo teórico gracias a la contribución de matemáticos como **Claude Shannon** y no fue hasta los años 70, cuando apareció el primer estándar criptográfico el **DES** (Data Encryption Standard, por sus siglas en ingles).

Desde los orígenes de la criptografía hasta bien entrado el siglo XIX, todos los sistemas criptográficos aparecidos eran simétricos (es decir, empleaba la misma clave para el cifrado y descifrado). Las claves asimétricas empezaron a utilizarse hasta finales del siglo XIX. La utilización de este tipo de claves ha sido la última gran revolución que ha sufrido la criptografía desde la automatización de los cálculos criptográficos.

2.4.1 - Criptografía clásica

El uso más antiguo conocido de la criptografía se halla en jeroglíficos tallados en monumentos del antiguo Egipto (hace más de 4500 años). Sin embargo, no se piensa que sean intentos serios de comunicación secreta, sino intentos de conseguir misterio, intriga o incluso diversión para el espectador letrado. Son ejemplos de otros usos de la criptografía, o de algo que se le parece. Más tarde, eruditos hebreos hicieron uso de sencillos cifrados por sustitución monoalfabéticos (como el cifrado Atbash), quizás desde el 500 al 600 a.C. La criptografía tiene una larga tradición en las escrituras religiosas que podrían ofender a la cultura dominante o a las autoridades políticas. Quizás el caso más famoso es el número de la bestia, del libro del Apocalipsis en el Nuevo Testamento cristiano. El 666 puede ser una forma criptográfica (es decir, cifrada) de ocultar una referencia peligrosa; muchos expertos creen que es una referencia oculta al Imperio Romano, o más probablemente al propio emperador Nerón (y así a las políticas persecutorias romanas), que sería entendida por los iniciados (los que tenían la clave del entendimiento), y sin embargo sería segura o al menos negable (y por tanto menos peligrosa) si atraía la atención de las autoridades. Al menos para las escrituras ortodoxas cristianas, casi toda esta necesidad de ocultación desapareció con la conversión y adopción del cristianismo como religión oficial del imperio por parte del emperador Constantino.

Figura 5. La escitala, uno de los primeros dispositivos de cifrado.

Los griegos de la época clásica conocían el cifrado (por ejemplo, los militares espartanos utilizaban el cifrado por transposición de la escítala). **Heródoto** nos habla de mensajes secretos ocultos físicamente detrás de la cera en tablas de madera, o como tatuajes en la cabeza de un esclavo, bajo el cabello, aunque esto no son ejemplos verdaderos de criptografía, ya que el mensaje, una vez conocido, es legible directamente; esto se conoce como *esteganografía*. Los romanos sí sabían algo de criptografía con toda seguridad (por ejemplo, el cifrado **Julio César** y sus variantes). Hay una mención antigua a un libro sobre criptografía militar romana, especialmente la de **Julio César**, desafortunadamente, se ha perdido.

En la India también se conocía la criptografía. El *Kama Sutra* la recomienda como técnica para que los amantes se comuniquen sin ser descubiertos.

Fue probablemente el análisis textual del *Corán*, de motivación religiosa, lo que llevó a la invención de la técnica del análisis de frecuencias para romper los cifrados por *sustitución monoalfabéticos*, en algún momento alrededor del año 1000. Fue el avance criptoanalítico más importante hasta la Segunda Guerra Mundial. Esencialmente, todos los cifrados fueron vulnerados a esta técnica criptoanalítica hasta la invención del *cifrado polialfabético* por **Leon Battista Alberti** (1465), y muchos lo siguieron siendo desde entonces.

La criptografía se hizo todavía más importante como consecuencia de la competencia política y la revolución religiosa. Por ejemplo, en Europa durante el Renacimiento, ciudadanos de varios estados italianos, incluidos los Estados Pontificios y la Iglesia Católica, fueron responsables de una rápida proliferación de técnicas criptoanalíticas, de las cuales, muy pocas reflejaban un entendimiento (o siquiera el conocimiento) del avance de **Alberti**. Los cifrados avanzados, incluso después de **Alberti**, no eran tan avanzados como afirmaban sus creadores, puede que este sobrado optimismo sea algo inherente a la criptografía, ya que entonces y hoy en día es fundamentalmente difícil saber realmente que tan vulnerable es un sistema.

La criptografía, el criptoanálisis y la traición cometida por agentes y mensajeros en la conspiración de Babington, durante el reinado de la reina Isabel I de Inglaterra, provocaron la ejecución de **María**, reina de los escoceses. Un mensaje cifrado de la época del hombre de la máscara de hierro (descifrado poco antes del año 1900 por **Étienne Bazeries**) ha arrojado algo de luz (no definitiva, lamentablemente) sobre la identidad real de ese desafortunado prisionero legendario. La criptografía estuvo implicada en la conspiración que condujo a la ejecución de **Mata Hari** y en la confabulación que provocó la ridícula condena y encarcelamiento de **Dreyfus**, ambos hechos acaecidos a principios del siglo XX. Afortunadamente, los criptógrafos también jugaron su papel para exponer las maquinaciones que provocaron los problemas de **Dreyfus**; **Mata Hari**, en cambio, fue fusilada.

Fuera del Medio Oriente y Europa, la criptografía permaneció comparativamente subdesarrollada. En Japón no se utilizó la criptografía hasta 1510 y las técnicas avanzadas no se conocieron hasta la apertura del país a occidente en los años 1860.

Aunque la criptografía tiene una historia larga y compleja, hasta el siglo XIX no desarrolló nada más que soluciones *"ad hoc"* para el cifrado y el criptoanálisis. Ejemplos de lo último son el trabajo de **Charles Babbage**, en la época de la Guerra de Crimea, sobre el criptoanálisis matemático de los cifrados *polialfabéticos*, redescubierto y publicado algo después por el prusiano **Fiedrich Kasiski**. En esa época, el conocimiento de la criptografía consistía normalmente en reglas generales averiguadas con dificultad. **Edgar Allan Poe** desarrolló métodos sistemáticos para resolver cifrados en los años 1840. Concretamente, colocó un anuncio de sus capacidades en el periódico de Filadelfia *Alexander's Weekly (Express) Messenger*, invitando al envío de cifrados, que él procedía a resolver. Su éxito creó excitación entre el público durante unos meses. Más tarde escribió un ensayo sobre los métodos criptográficos que resultaron útiles para descifrar los códigos alemanes empleados durante la Primera Guerra Mundial.

Proliferaron métodos matemáticos en la época justo anterior a la Segunda Guerra Mundial, principalmente con la aplicación, por parte de **William F. Friedman**, de las técnicas estadísticas al desarrollo del criptoanálisis y del cifrado, y la rotura inicial de **Marian Rejewski** de la versión del Ejército Alemán del sistema Enigma.

La máquina Enigma (figura 4) fue utilizada extensamente por la Alemania nazi, el criptoanálisis aplicado por los aliados proporcionó una vital inteligencia.

En la Segunda Guerra Mundial, las máquinas de cifrado mecánicas y electromecánicas se utilizaban extensamente, aunque allá donde estas máquinas eran poco prácticas, los sistemas manuales continuaron en uso. Se hicieron grandes avances en la rotura de cifrados, todos en secreto. La información acerca de esta época ha empezado a desclasificarse al llegar a su fin el periodo de secreto británico de 50 años, al abrirse lentamente los archivos estadounidenses y al irse publicando diversas memorias y artículos.

Los alemanes hicieron gran uso de diversas variantes de una máquina de rotores electromecánica llamada Enigma. El matemático **Marian Rejewski**, de la Oficina de Cifrado polaca, reconstruyó en diciembre de 1932 la máquina Enigma del ejército alemán, utilizando la matemática y la limitada documentación proporcionada por el capitán **Gustave Bertrand,** de la inteligencia militar francesa. Este fue el mayor avance del criptoanálisis en más de mil años. **Rejewsky** y sus colegas de la Oficina de Cifrado, **Jerzy Różycki** y **Henryk Zygalski**, continuaron desentrañando la Enigma y siguiendo el ritmo de la evolución de los componentes de la máquina y los procedimientos de cifrado. Al irse deteriorando los recursos financieros de Polonia por los cambios introducidos por los alemanes, y al irse avecinando la guerra, la oficina de cifrado, bajo órdenes del estado mayor polaco, presentaron a representantes de la inteligencia francesa y británica los secretos del descifrado de la máquina Enigma, el 25 de julio de 1939 en Varsovia.

Poco después de que estallara la Segunda Guerra Mundial el 1 de septiembre de 1939, el personal clave de la oficina de cifrado fue evacuado hacia el sureste, el 17 de septiembre, tras la entrada de la Unión Soviética en el este de Polonia, cruzaron Rumanía. Desde allí alcanzaron París en Francia; en la estación de inteligencia polaco-francesa PC Bruno, cerca de París, continuaron rompiendo la Enigma, colaborando con los criptólogos británicos de **Bletchley Park**, que se habían puesto al día con el tema. Con el tiempo, los criptólogos británicos en los que se incluían lumbreras como **Gordon Welchman** y **Alan Turing**, el fundador conceptual de la computación moderna hicieron progresar sustancialmente la escala y tecnología del descifrado Enigma.

El 19 de abril de 1945 se ordenó a los oficiales superiores británicos que nunca debían revelar que se había roto el código de la máquina Enigma alemana, porque esto le daría la oportunidad al enemigo de decir que "no fueron vencidos justa y satisfactoriamente".

Los criptógrafos de la armada estadounidense, en cooperación con criptógrafos británicos y holandeses a partir de 1940, rompieron varios sistemas criptográficos de la armada japonesa. La rotura de uno de ellos, el JN-25, condujo a la célebre victoria

estadounidense de la Batalla de Midway. Un grupo del ejército estadounidense, el SIS, consiguió romper el sistema criptográfico diplomático japonés de alta seguridad (una máquina electromecánica llamada Púrpura por los estadounidenses) antes incluso del comienzo de la Segunda Guerra Mundial. Los estadounidenses llamaron a la inteligencia derivada del criptoanálisis, quizás en especial la derivada de la máquina Púrpura, como "Magic" (Magia). Finalmente los británicos se decidieron por "Ultra" para la inteligencia derivada del criptoanálisis, en especial la derivada del tráfico de mensajes cifrados con las diversas Enigmas. Un término británico anterior para Ultra fue "Boniface".

Los militares alemanes también desarrollaron varios intentos de implementar mecánicamente la libreta de un solo uso. **Bletchley Park** los llamó cifrados Fish, y **Max Newman** y sus colegas diseñaron e implementaron el primer ordenador electrónico digital programable del mundo, *Colossus*, para ayudarles con el criptoanálisis. La oficina de asuntos exteriores alemana empezó a usar la libreta de un solo uso en 1919, parte de este tráfico fue leído en la Segunda Guerra Mundial como resultado de la recuperación de material importante en Sudamérica que fue desechado con poco cuidado por un mensajero alemán.

La oficina de asuntos exteriores japonesa utilizó un sistema eléctrico lógico basado en uniselectores (llamado Púrpura por EU), también utilizó varias máquinas similares para los agregados de algunas embajadas japonesas. Una de estas recibió el nombre de "Máquina M" por EU y otra fue apodada "Red". Todas fueron rotas (vulneradas) en mayor o menor grado por los aliados.

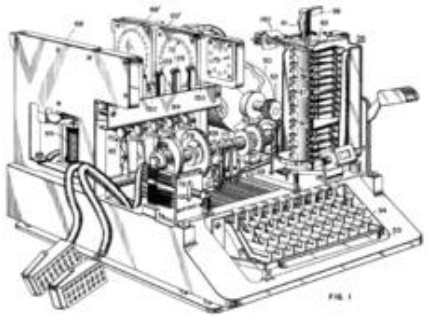


Figura 6. La máquina SIGABA se describe en la Patente USPTO nº 6175625, registrada en 1944 pero no publicada hasta 2001 (Imagen tomada de http://es.wikipedia.org/wiki/Historia_de_la_criptografía).

Las máquinas de cifrado aliadas utilizadas en la Segunda Guerra Mundial incluían la *Typex* británica y la *SIGABA* (Figura 6) estadounidense, ambos eran diseños de rotores electromecánicos similares en espíritu a la Enigma, aunque con mejoras importantes. No se tiene constancia de que ninguna de ellas fuera rota durante la guerra. Los polacos utilizaron la máquina *Lacida*, pero se demostró que era poco segura y se canceló su uso. Las tropas de campo utilizaron las familias M-209 y M-94. Los agentes SOE utilizaron inicialmente cifrados de poema (las claves eran poemas memorizados), pero más avanzada la guerra empezaron a utilizar libretas de un solo uso.

2.4.2 - Criptografía moderna

En la era moderna las deficiencias de los sistemas clásicos se rompieron, debido principalmente a los siguientes factores:

- *Velocidad de cálculo*: con la aparición de las computadoras digitales se dispuso de una potencia de cálculo muy superior a la de los métodos clásicos.

- *Avance de las matemáticas*: que permitieron encontrar y definir con claridad sistemas criptográficos estables y seguros.

- *Necesidades de seguridad*: surgieron muchas actividades nuevas que precisaban el ocultamiento de datos, con lo que la criptología experimentó un gran avance.

A partir de estas bases surgieron nuevos y complejos sistemas criptográficos, que se clasificaron en dos tipos o familias principales, los de clave simétrica y los de clave pública. Los modernos algoritmos de encriptado simétricos mezclan la trasposición y la permutación, mientras que los de clave pública se basan más en complejas operaciones matemáticas.

La era de la criptografía moderna comienza realmente con **Claude Shannon**, que podría decirse que es el padre de la criptografía matemática. En 1949 publicó el artículo *Communication Theory of Secrecy Systems* en la Bell System Technical Journal, y poco después el libro *Mathematical Theory of Communication*, con **Warren Weaver**. Estos trabajos, junto con los otros que publicó sobre la teoría de la información y la comunicación, establecieron una sólida base teórica para la criptografía y el criptoanálisis. Y a la vez, la criptografía desapareció de la escena para quedarse dentro de las organizaciones gubernamentales secretas como la NSA. Muy pocos trabajos se hicieron públicos hasta mediados de los años 70 cuando todo cambió.

A mediados de los 70 se vivieron dos importantes avances públicos (es decir, no secretos). El primero fue la publicación del borrador del *Data Encryption Standard* en el *Registro Federal* estadounidense el 17 de marzo de 1975. La propuesta fue enviada por IBM, por invitación de la Oficina Nacional de Estándares (ahora NIST), en un esfuerzo por desarrollar sistemas de comunicación electrónica segura para las empresas como los bancos y otras organizaciones financieras grandes. Tras asesoramiento y ciertas modificaciones por parte de la NSA, fue adoptado y publicado como un Federal Information Processing Standard en 1977 (actualmente el FIPS 46-3). El DES fue el primer cifrado accesible públicamente que fue bendecido por una agencia nacional como la NSA. La publicación de sus especificaciones por la NBS estimuló una explosión del interés público y académico por la criptografía.

DES fue suplantado oficialmente por el Advanced Encryption Standard (AES, por sus siglas en ingles) en 2001, cuando el NIST anunció el FIPS 197. Tras una competición abierta, el NIST seleccionó el Rijndael, enviado por dos criptógrafos belgas, para convertirse en el AES. El DES y otras variantes más seguras (como el Triple DES; ver FIPS 46-3), todavía se utilizan hoy en día, y se han incorporado en muchos estándares

nacionales y de organizaciones. Sin embargo, se ha demostrado que el tamaño de su clave, 56 bits, es insuficiente ante ataques de fuerza bruta (un ataque así, llevado a cabo por el grupo pro libertades civiles digitales Electronic Frontier Foundation en 1997, tuvo éxito en 56 horas la historia se cuenta en *Cracking DES*, publicado por O'Reilly Associates). Como resultado, hoy en día el uso sin más del cifrado DES es sin duda inseguro para los nuevos diseños de criptosistemas, y los mensajes protegidos por viejos criptosistemas que utilizan el DES, y de hecho todos los mensajes enviados desde 1976 que usan el DES, también están en riesgo. A pesar de su calidad inherente, el tamaño de la clave DES (56 bits) fue considerado por algunos como demasiado pequeño incluso en 1976; quizás la voz más sonora fue la de **Whitfield Diffie**. Había sospechas de que las organizaciones gubernamentales tenían suficiente potencia de cálculo para romper los mensajes DES; ahora es evidente que otros han logrado esa capacidad.

El segundo desarrollo en 1976, fue quizás más importante todavía, ya que cambió de manera fundamental la forma en la que los sistemas criptográficos pueden funcionar. Fue la publicación del artículo *New Directions in Cryptography* de **Whitfield Diffie** y **Martin Hellman**. Introdujo un método radicalmente nuevo para distribuir las claves criptográficas, dando un gran paso para resolver uno de los problemas fundamentales de la criptografía, la distribución de claves y ha terminado llamándose intercambio de claves **Diffie-Hellman**. El artículo también estimuló el desarrollo público casi inmediato de un nuevo tipo de algoritmo de cifrado, los algoritmos de *cifrado asimétrico*.

Antes de eso, todos los algoritmos de cifrado útiles eran algoritmos de cifrado simétrico, en los que tanto el remitente como el destinatario utilizan la misma clave criptográfica, que ambos deben mantener en secreto. Todas las máquinas electromecánicas utilizadas en la Segunda Guerra Mundial eran de esta clase lógica, al igual que los cifrados César, Atbash y en esencia todos los cifrados y sistemas de códigos de la historia. La clave de un código es, por supuesto, el libro de códigos, que debe asimismo distribuirse y mantenerse en secreto.

En estos sistemas era necesario que la partes que se iban a comunicar intercambiaran las claves de alguna forma segura antes del uso del sistema (el término que se solía utilizar era “mediante un canal seguro”), como un mensajero de confianza con un maletín esposado a su muñeca o un contacto cara a cara o una paloma mensajera fiel. Este requisito nunca es trivial y se hace inmantenible rápidamente al crecer el número de participantes, o cuando no hay canales seguros disponibles para el intercambio de claves, o cuando las claves cambian con frecuencia (una práctica criptográfica sensata). En particular, si se pretende que los mensajes sean seguros frente a otros usuarios, hace falta una clave distinta para cada par de usuarios. Un sistema de este tipo se conoce como sistema criptográfico de clave secreta o de clave simétrica. El intercambio de claves D-H (y las posteriores mejoras y variantes) hizo que el manejo de estos sistemas fuera mucho más sencillo y seguro que nunca.

En contraste, el cifrado de clave asimétrica utiliza un par de claves relacionadas matemáticamente, en el que una de ellas descifra el cifrado que se realiza con la otra. Algunos (pero no todos) de estos algoritmos poseen la propiedad adicional de que una de las claves del par no se puede deducir de la otra por ningún método conocido que no sea el

ensayo y error. Con un algoritmo de este tipo, cada usuario sólo necesita un par de claves. Designando una de las claves del par como privada (siempre secreta) y la otra como pública (a menudo visible), no se necesita ningún canal seguro para el intercambio de claves. Mientras la clave privada permanezca en secreto, la clave pública puede ser conocida públicamente durante mucho tiempo sin comprometer la seguridad, haciendo que sea seguro reutilizar el mismo par de claves de forma indefinida.

Para que dos usuarios de un algoritmo de clave asimétrica puedan comunicarse de forma segura a través de un canal inseguro, cada usuario necesita conocer su clave pública y privada y la clave pública del otro usuario. Véase este escenario básico: **Alicia** y **Bob** tienen cada uno un par de claves que han utilizado durante años con muchos otros usuarios. Al comienzo de su mensaje, intercambian las claves públicas sin cifrar por una línea insegura. Luego **Alicia** cifra un mensaje utilizando su clave privada, y luego re-cifra el resultado utilizando la clave pública de **Bob**. Luego el mensaje cifrado doblemente se envía en forma de datos digitales mediante un cable desde **Alicia** hasta **Bob**. **Bob** recibe el flujo de bits y lo descifra usando su clave privada, y luego descifra el resultado utilizando la clave pública de **Alicia**. Si el resultado final es un mensaje reconocible, **Bob** puede estar seguro de que el mensaje procede realmente de alguien que conoce la clave privada de **Alicia**, y que cualquiera que haya pinchado el canal necesitará las claves privadas de **Alicia** y **Bob** para entender el mensaje.

La efectividad de los algoritmos asimétricos depende de una clase de problemas matemáticos conocidos como funciones de un solo sentido, que requieren relativamente poca potencia de cálculo para ejecutarse, pero muchísima potencia para calcular la inversa. Un ejemplo clásico de función de un sentido es la multiplicación de números primos grandes. Es bastante rápido multiplicar dos primos grandes, pero muy difícil factorizar el producto de dos primos grandes. Debido a las propiedades matemáticas de las funciones de un sentido, la mayor parte de las claves posibles tienen poca calidad para su uso criptográfico, solo una pequeña parte de las claves posibles de una cierta longitud son candidatas ideales, y por tanto los algoritmos asimétricos requieren claves muy largas para alcanzar el mismo nivel de seguridad proporcionado por las claves simétricas, relativamente más cortas. Las exigencias de generar el par de claves y realizar el cifrado/descifrado hacen que los algoritmos asimétricos sean costosos computacionalmente. Como, a menudo, los algoritmos simétricos pueden usar como clave cualquier serie pseudoaleatoria de bits, se puede generar rápidamente una clave de sesión desechable para uso a corto plazo. Por consiguiente, es una práctica común utilizar una clave asimétrica larga para intercambiar una clave simétrica desechable mucho más corta (pero igual de fuerte). El algoritmo asimétrico, más lento, envía de forma segura una clave simétrica de sesión, y entonces el algoritmo simétrico, más rápido, toma el control para el resto del mensaje.

La criptografía de clave asimétrica, el intercambio de claves Diffie-Hellman y los famosos algoritmos de clave pública/privada (es decir, lo que se suele llamara algoritmo RSA), parecen haber sido desarrollados de manera independiente en una agencia de inteligencia británica antes del anuncio público de **Diffie** y **Hellman** en el año 76. El GCHQ ha publicado documentos que afirman que ellos habían desarrollado la criptografía de clave pública antes de la publicación del artículo de **Diffie** y **Hellman**. Varios artículos

clasificados fueron escritos en el GCHQ durante los años 60 y 70, que finalmente llevaron a unos sistemas esencialmente idénticos al cifrado RSA y al intercambio de claves Diffie-Hellman en 1973 y 1974. Algunos de ellos se publicaron hasta hace poco, y los inventores (**James H. Ellis, Clifford Cocks** y **Malcolm Williamson** han hecho público parte de su trabajo.

2.5 – Técnicas de encriptado

En esta sección se mostrarán algunos sistemas criptográficos que en la actualidad han perdido su eficacia, debido a que son fácilmente criptoanalizables empleando las computadoras digitales, mediante análisis estadísticos o directamente por fuerza bruta, pero que fueron empleados con éxito en la antigüedad. Algunos se remontan incluso, como el algoritmo de César, a la Roma Imperial. Sin embargo, aún conservan el interés teórico, ya que algunas de sus propiedades resultan muy útiles para entender mejor los algoritmos modernos, así como también sistemas criptográficos que funcionan en la actualidad y que en los cuales, se basan muchos sistemas de comunicación cotidianos.

Comenzaremos mencionando los dos tipos de criptografía que existen, la criptografía *simétrica* y la *asimétrica* y algunos algoritmos que se basan en ellas.

2.5.1 - Criptografía simétrica

Incluye los sistemas clásicos y se caracteriza porque en ellos se usa la misma clave para encriptar y para desencriptar, motivo por el que se denomina simétrica. En la figura 7 se muestra un diagrama donde se aprecia su funcionamiento.

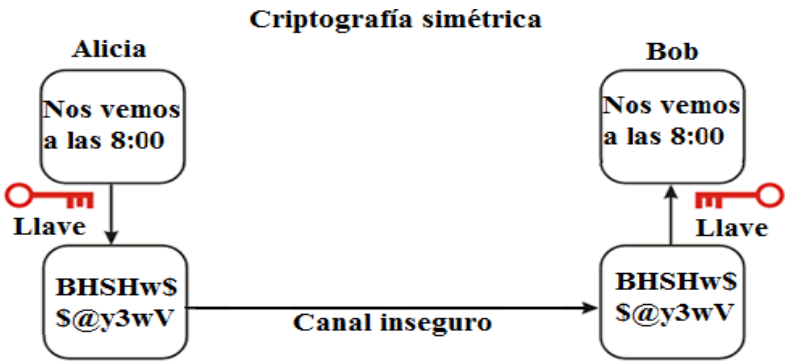


Figura 7. Criptografía Simétrica.

Toda la seguridad de este sistema está basada en la llave simétrica, por lo que es misión fundamental tanto del emisor como del receptor conocer esta clave y mantenerla en secreto. Si la llave cae en manos de terceros, el sistema deja de ser seguro, por lo que habría que desechar dicha llave y generar una nueva.

Para que un algoritmo de este tipo sea considerado fiable debe cumplir varios requisitos básicos:

1. Conocido el criptograma (texto cifrado) no se pueden obtener de él ni el texto en claro ni la clave.

2. Conocidos el texto en claro y el texto cifrado debe resultar más caro en tiempo o dinero descifrar la clave que el valor posible de la información obtenida por terceros.

Generalmente el algoritmo de encriptado es conocido, se divulga públicamente, por lo que la fortaleza del mismo dependerá de su complejidad interna y sobre todo de la longitud de la clave empleada, ya que una de las formas de criptoanálisis primario de cualquier tipo de sistema es de prueba-ensayo, mediante la que se van probando diferentes claves hasta encontrar la correcta.

Los algoritmos simétricos encriptan bloques de texto del documento original, y son más sencillos que los sistemas de clave pública, por lo que sus procesos de encriptado y desencriptado son más rápidos.

Todos los sistemas criptográficos clásicos se pueden considerar simétricos, y los principales algoritmos simétricos actuales son **DES**, **IDEA** y **RC5**. Se llevo a cabo un proceso de selección para establecer un sistema simétrico estándar, que se llama **AES** (Advanced Encryption Standard), que se quiere que sea el nuevo sistema que se adopte a nivel mundial.

Las principales desventajas de los métodos simétricos son la distribución de las claves, el peligro que muchas personas deban conocer una misma clave y la dificultad de almacenar y proteger muchas claves diferentes.

2.5.2 - Criptografía asimétrica

También llamada de **clave pública**, se basa en el uso de dos claves diferentes, claves que poseen una propiedad fundamental: una clave puede desencriptar lo que la otra ha encriptado, este sistema es mostrado en la figura 8.

Generalmente una de las claves de la pareja, denominada *clave privada*, se usa por el propietario para encriptar los mensajes, mientras que la otra, llamada *clave pública*, se usa para desencriptar el mensaje cifrado.

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

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

Mientras que la clave privada debe mantenerla en secreto su propietario, ya que es la base de la seguridad del sistema, la clave pública es difundida ampliamente, para que esté al alcance del mayor número posible de personas.

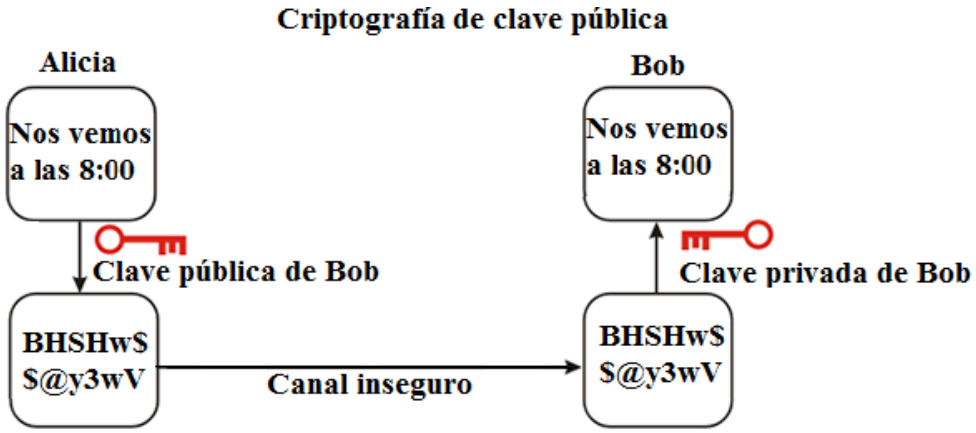


Figura 8. Criptografía asimétrica (clave pública).

En éste sistema, para enviar un documento con seguridad, **Alicia** encripta el mensaje con la clave pública de **Bob** y lo envía por el medio inseguro. Este documento está totalmente protegido en su viaje por el canal público, ya que sólo se puede desencriptar con la clave privada correspondiente, conocida solamente por **Bob**. Al llegar el mensaje cifrado a su destino, **Bob** usa su clave privada para obtener el mensaje en claro.

Una variante de este sistema criptográfico se produce cuando **Alicia** encripta un mensaje con su clave privada, enviando por el medio inseguro tanto el mensaje en claro como el cifrado. Así, **Bob** puede comprobar que el emisor ha sido **Alicia** y no otro que lo suplante, con tan sólo desencriptar el texto cifrado con la clave pública de **Alicia** y comprobar que coincide con el texto sin cifrar. Como sólo **Alicia** conoce su clave privada, **Bob** puede estar seguro de la autenticidad del emisor del mensaje. Este sistema de autentificación se denomina *firma digital* y es mostrado en la figura 9.

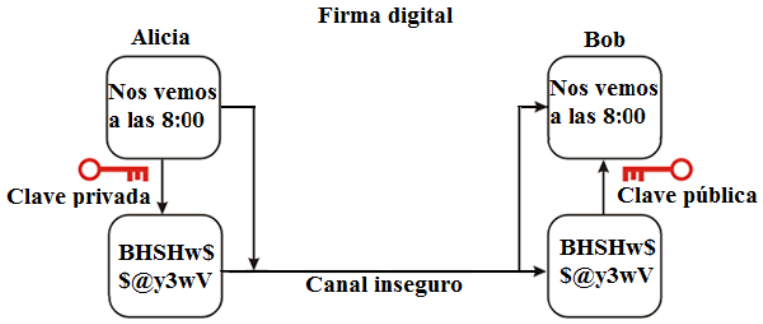


Figura 9. Esquema de funcionamiento de la firma digital.

Para que un algoritmo de clave pública sea considerado seguro debe cumplir con los siguientes requerimientos:

1. Conocido el texto cifrado no debe ser posible encontrar el texto en claro ni la clave privada.

2. Conocido el texto cifrado y el texto en claro debe resultar más caro en tiempo o en dinero descifrar la clave que el valor posible de la información obtenida por terceros.

3. Conocida la clave pública y el texto en claro no se puede generar un criptograma correcto encriptado con la clave privada.

4. Dado un texto cifrado con una clave privada sólo existe una clave pública capaz de desencriptarlo y viceversa.

La principal ventaja de los sistemas de clave pública frente a los simétricos es que la clave pública y el algoritmo de cifrado son o pueden ser de dominio público y que no es necesario poner en peligro la clave privada en tránsito por los medios inseguros, ya que ésta está siempre oculta y en poder únicamente de su propietario. Como desventaja, los sistemas de clave pública dificultan la implementación del sistema y son mucho más lentos que los simétricos.

Generalmente y debido a la lentitud para el cálculo del algoritmo de los sistemas de llave pública, estos se utilizan para el envío seguro de claves simétricas, mientras que éstas últimas se usan para el envío general de los datos encriptados.

El primer sistema de clave pública que apareció fue el Diffie-Hellman en 1976, y fue la base para el desarrollo de los que después aparecieron, entre los que cabe destacar el **RSA,** el más utilizado en la actualidad.

2.5.3 - Criptografía mixta

En muchas ocasiones se implementan sistemas criptográficos mixtos, en los que se usa la llave pública del receptor para encriptar una clave simétrica que se usará en el proceso de comunicación encriptada. De esta forma se aprovechan las ventajas de ambos sistemas, usando el sistema asimétrico para el envío de la clave sensible y el simétrico, con mayor velocidad de proceso, para el envío masivo de datos.

2.6 – Objetivo del cifrado

El objetivo principal del encriptado es brindar comunicaciones seguras, la cual se hace principalmente por canales inseguros lo que facilitaría la extracción de información, si bien sabemos al hablar de criptografía no hablamos de seguridad, hablamos de la herramienta utilizada para formar un sistema con una complejidad variable, lo cual proporciona el servicio de seguridad y de confidencialidad.

Los principales sistemas de cifrado utilizaban técnicas no muy complejas, por ejemplo, la técnica de rotación de caracteres en un mensaje. La seguridad en estos sistemas era basada en mantener en secreto el algoritmo usado para la rotación, los cuales eran fácilmente descifrables utilizando métodos estadísticos, en la actualidad estos métodos son utilizados como parte de otro sistema o solo por aficionados.

Al utilizar sistemas profesionales se usan microsistemas, que tratan de funciones matemáticas parametrizadas en la que los datos de entrada no se pueden obtener a partir de la salida. En la actualidad la seguridad no es basada en mantener en secreto el algoritmo utilizado sino que es público y lo que se mantiene en secreto son las claves o parámetros del mismo.

2.7 – Alternativa de solución no convencional

Al obtener la sincronización de sistemas caóticos [Pecorra y Carroll 1990] se abre la alternativa de utilizarlos para el encriptado de información y así dar solución al problema planteado de encriptado de información confidencial. La idea principal es la construcción de un sistema hipercaótico y su sincronía con otro para enviar información confidencial de manera altamente segura. En la figura 10 se puede apreciar el sistema utilizado como alternativa de solución

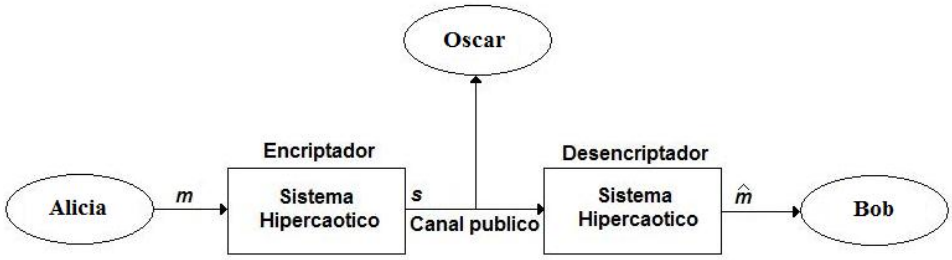


Figura 10. Esquema general de comunicaciones privada basada en sincronía de sistemas hipercaóticos.

En la figura 10 se observa que **Alicia** manda el mensaje (*m*) al sistema encriptador, de ahí sale por un canal público (*s*) que es el mensaje adherido al hipercaos y donde Oscar no podría conocer el mensaje, *s* llega al desencriptador donde se obtiene $\hat{m}$ que es el mensaje recuperado.

2.7.1- Propuesta de solución de esta tesis

En este trabajo de tesis se pretende realizar la sincronización de sistemas hipercaóticos por medio de formas hamiltonianas y el diseño de un observador [Sira-Ramírez y Cruz-Hernández 2000; 2001] donde ésta sincronización se hará de manera numérica y experimental utilizando el circuito hipercaótico de Chua de cuarto orden. Para finalmente construir una red de usuarios para comunicaciones seguras.

2.8 – Conclusiones

A lo largo de la historia los sistemas de encriptado han cumplido su objetivo, que es proteger la información (relevante o al menos confidencial) de intrusos a los cuales no va dirigida. Sin embargo, el avance en las matemáticas (antes de la segunda guerra mundial) o los avances científicos (en la actualidad las computadoras) han logrado que estos sistemas sean vulnerables a ataques que ponen en riesgo la confidencialidad del mensaje donde muchas, por no decir la mayoría de las veces, estos mensajes son extraídos del sistema, haciendo que el sistema sea ineficiente y se requiera de otro con más eficiencia para proteger la información.

La información contenida en este capítulo fue tomada de las siguientes fuentes [Galende 1995], [Lucena López 1999], [Simon Singh 2000] y [www.wikipedia.com].

Capítulo 3

Caos

3.1 – Introducción

El **caos** (palabra que deriva del griego, Χάος) habitualmente se refiere a lo impredecible y es uno de los principales conceptos del Cosmos. *Caos* deriva de la raíz *ghn* o *ghen* del lenguaje protoindoeuropeo ("hueco", "muy abierto"). Debido a variaciones lingüísticas, el significado de la palabra se desplazó a *desorden* [www.wikipedia.com].

El caos es la complejidad de la supuesta causalidad en la relación entre eventos sin que se observe un comportamiento que relacione la causa con el efecto. Esto significa que cualquier evento insignificante del universo tiene el poder potencial de desencadenar una ola de eventos que alteren el sistema completo.

Los sistemas dinámicos y teoría del caos son ramas de las matemáticas, desarrolladas en la segunda mitad del siglo XX, que estudian lo complicado, lo impredecible, lo que no es lineal. A veces se la llama matemática de lo no lineal.

La idea de la que parte la *teoría del caos* es simple: en determinados sistemas naturales, pequeños cambios en las condiciones iniciales conducen a enormes discrepancias en los resultados. Este principio suele llamarse *efecto mariposa* debido a que, en meteorología, la naturaleza no lineal de la atmósfera ha hecho afirmar que es posible que el aleteo de una mariposa en determinado lugar y momento, pueda ser la causa de un terrible huracán varios meses más tarde en la otra punta del globo.

Un ejemplo ilustrativo del efecto mariposa es soltar una pelota justo sobre la arista del tejado de una casa varias veces; pequeñas desviaciones en la posición inicial pueden hacer que la pelota caiga por uno de los lados del tejado o por el otro, conduciendo a trayectorias de caída y posiciones de reposo final completamente diferentes. Cambios minúsculos que conducen a resultados totalmente divergentes.

La teoría del caos no tiene un padre fundador, sino muchos. Entre ellos destacan **Edward Lorenz** (meteorólogo), **Benoit Mandelbrot** (ingeniero de comunicaciones), **Mitchell Feigenbaum** (matemático), **Libchaber** (físico), **Arthur Winfree** (biólogo), **Mandell** (psiquiatra) y otros muchos, la mayoría de ellos vivos actualmente.

Esta teoría surgió cuando **Edward Lorenz** dio a conocer en 1963 un modelo climático que, por su comportamiento, atrajo la atención de muchos físicos, aunque se basa en trabajos anteriores, como los de **Julia, Poincaré** y **Lyapunov**. Junto a la mecánica cuántica y a la teoría de la relatividad, se considera la tercera gran teoría del siglo XX. Algunos la consideran como la ciencia de la totalidad, ya que consideran determinismo e indeterminismo como uno solo.

En teoría del caos los sistemas dinámicos son estudiados a partir de su espacio de estados, es decir, la representación de coordenadas de sus variables independientes.

El atractor es uno de los conceptos fundamentales del caos, que se utiliza para representar la evolución en un sistema dinámico. Este tipo de representación ya había sido usado por **Henri Poincaré**.

En este escenario se suele hablar del concepto de *atractores extraños* (no puntos de equilibrio, ni ciclos límite) trayectorias en el espacio de fases hacia las que tienden todas las trayectorias normales. En el caso de un péndulo oscilante, el atractor sería el punto de equilibrio central.

Un atractor extraño es una imagen en el espacio de fases de algún sistema caótico concreto, los cuales suelen tener formas geométricas caprichosas y en muchos casos, parecidos o similitudes a diferentes escalas.

El atractor de Lorenz fue el primer atractor extraño que el hombre generó (mostrado en la figura 11).

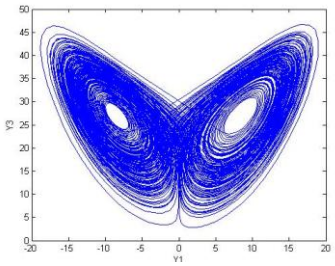


Figura 11. Atractor de Lorenz.

Edward Lorenz por el año 1963 investigaba el hecho de que fuese imposible predecir los fenómenos meteorológicos a largo plazo. Creó un modelo matemático para poder simularlo por ordenador. Este modelo se basaba inicialmente en la convección de fluidos y la no linealidad.

Así descubrió una de las propiedades más importantes de los sistemas caóticos, la dependencia a las condiciones iniciales. Si partimos de dos puntos del espacio de estados, las trayectorias correspondientes a estos dos puntos son diferentes aunque los puntos estén muy próximos. Los puntos serían los conjuntos de condiciones iniciales y las trayectorias la diferente evolución del sistema dependiendo del punto de partida.

Como no se pueden medir de forma precisa las condiciones iniciales de un sistema, es imposible predecir a largo plazo el comportamiento del sistema, si éste depende de las condiciones iniciales.

3.2 - Características del caos

La teoría del caos trata ciertos tipos de comportamientos impredecibles de los sistemas dinámicos, donde los sistemas dinámicos se pueden clasificar básicamente en:

- Estables
- Inestables
- Caóticos

Un sistema estable por ejemplo, tiende a lo largo del tiempo a un punto fijo o una órbita (como atractores), según su dimensión. Un sistema inestable por ejemplo, se escapa de los atractores. Y un sistema caótico por ejemplo, manifiesta los dos comportamientos. Por un lado, existe un atractor por el que el sistema se ve atraído, pero a la vez, hay fuerzas que lo alejan de éste. De esa manera, el sistema permanece confinado en una zona de su espacio de estados, pero sin tender a un atractor fijo.

Una de las mayores características de un sistema inestable es que tiene una gran dependencia de las condiciones iniciales. De un sistema del que se conocen sus ecuaciones características, y con unas condiciones iniciales fijas, se puede conocer exactamente su evolución en el tiempo. Pero en el caso de los sistemas caóticos, una mínima diferencia en esas condiciones hace que el sistema evolucione de manera totalmente distinta. Ejemplos de tales sistemas incluyen la atmósfera terrestre, el sistema solar, las placas tectónicas, los fluidos en régimen turbulento y los crecimientos de población.

Por ejemplo, el clima atmosférico, según describió **Edward Lorenz**, se describe por 3 ecuaciones diferenciales ordinarias no lineales bien definidas. Siendo así, conociendo las condiciones iniciales se podría conocer la predicción del clima en el futuro. Sin embargo, al ser éste un sistema caótico, y no poder conocer nunca con exactitud los parámetros que fijan las condiciones iniciales (en cualquier sistema de medición, por definición, siempre se comete un error, por pequeño que éste sea) hace que aunque se conozca el modelo, éste diverja de la realidad pasado un cierto tiempo. Por otra parte, el modelo atmosférico es teórico y puede no ser perfecto, y el determinismo, en el que se basa, es también teórico.

Un sistema caótico tiene las siguientes características:

- Debe ser sensible a condiciones iniciales.
- Debe ser transitivo.
- Sus órbitas periódicas deben formar un conjunto denso en una región compacta del espacio de estados.
- Un exponente de Lyapunov positivo.

3.3 – Algunas aplicaciones del caos

La teoría del caos ha tenido gran relevancia en muchos campos científicos actuales como la medicina, la biología, la ingeniería, la economía, la meteorología, la arquitectura, la física cuántica y otras. En el campo de la medicina se pueden encontrar varias estructuras

fractales: redes neuronales, disposición espacial de las glándulas, etcétera. Dentro de la ingeniería la teoría del caos se entiende como una herramienta de análisis, que ha permitido afrontar problemas que hasta hace poco era imposible abordar como, por ejemplo, responder a las siguientes cuestiones:

- Las leyes de propagación de una fractura
- Las averías de máquinas
- Por qué las nubes de humo de dos cigarrillos, de la misma marca, encendidos a la vez, no se parecen en nada tras un breve periodo de tiempo

Actualmente hay varios ejemplos de aplicación en la arquitectura a través de los fractales, por ejemplo el Jardín Botánico en Barcelona de **Carlos Ferrater**.

En la teoría del caos, un sistema dinámico puede referirse a la bolsa de valores para un economista o al corazón humano para un médico y algunos científicos consideran la teoría fractal como una herramienta necesaria para estudiar sistemas dinámicos como los mencionados anteriormente u otros que suceden en la naturaleza.

Otra aplicación del caos es en la comunicación, donde se utiliza para el cifrado de información confidencial con muy buenos resultados donde esta aplicación será la utilizada en este trabajo de tesis.

3.4 - Circuito caótico de Chua

En los últimos años se ha intensificado el estudio de los sistemas dinámicos debido a su interés intrínseco y a sus potenciales aplicaciones en la ciencia y tecnología [Lakshmanam y Murali 1995]. Algunas características de los sistemas dinámicos pueden ser analizadas con circuitos eléctricos y uno de los circuitos autónomos y el más simple que presenta un comportamiento caótico fue concebido y diseñado por **León O. Chua** en 1963. El circuito de Chua es una red electrónica muy simple, el cual, exhibe una variedad de fenómenos de bifurcación y caos con sus correspondientes atractores extraños. Este circuito consta de cuatro elementos lineales, un inductor L, una resistencia R, dos capacitares C_1 y C_2 y un elemento no lineal N_R (conocida como diodo de Chua) El circuito de Chua (Chua *et al* 1992) se muestra en la figura 12.

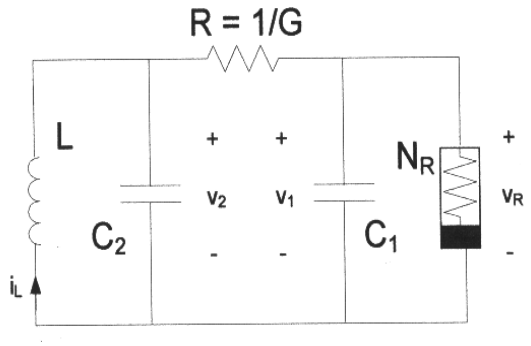


Figura 12. Circuito de Chua.

La relación V_R - I_R de la resistencia no lineal N_R, se muestra en la figura 13

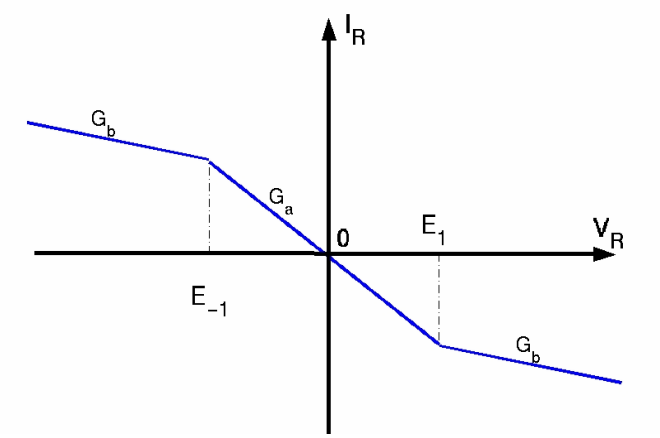


Figura 13. Función de respuesta del elemento no lineal N_R.

3.5 - Ecuaciones de estado del circuito de Chua

Las ecuaciones diferenciales no lineales que modelan el comportamiento del circuito de Chua mostrado en la figura 12 y que se obtienen al aplicar la teoría de circuitos se presentan a continuación:

$$C_1 \frac{dv_{c_1}}{dt} = G(v_{c_2} - v_{c_1}) - g(v_{c_1}) \ , \qquad (1)$$

$$C_2 \frac{dv_{c_2}}{dt} = G(v_{c_1} - v_{c_2}) + i_l \ ,$$

$$L \frac{di_L}{dt} = -v_{c_2}$$

donde la función no lineal se expresa como

$$g(v_{c_1}) = m_0 v_{c_1} + \frac{1}{2}(m_1 - m_0)[\left|v_{c_1} + B_p\right| - \left|v_{c_1} - B_p\right|] \ . \qquad (2)$$

3.6 - Ecuaciones normalizadas del circuito de Chua

Mediante un cambio de variable apropiado es posible transformar (1) y (2) en un conjunto de ecuaciones adimensionales. Los voltajes v_1 y v_2 y la corriente i_l en el circuito de Chua son transformados a las variables normalizadas x_1, x_2 y x_3 respectivamente, definidas por

$$x_1 \triangleq \frac{Vc_1}{E}, \qquad x_2 \triangleq \frac{Vc_2}{E}, \qquad x_3 \triangleq i_l \left(\frac{R}{E}\right),$$

donde E representa el voltaje de ruptura de la parte lineal del diodo de Chua, de la misma forma, los parámetros del circuito de Chua son transformados en parámetros normalizados definidos por

$$\propto \triangleq \frac{c_2}{c_1}, \qquad \beta \triangleq \frac{R^2 c_2}{L}, \qquad a \triangleq RG_1, \qquad b \triangleq RG_2.$$

De este modo obtenemos finalmente, las ecuaciones normalizadas del circuito de Chua [Chua *et al.* 1992]

$$\begin{aligned} \dot{x}_1 &= \alpha(x_2 - x_1 - f(x_1)), \\ \dot{x}_2 &= x_1 - x_2 + x_3, \\ \dot{x}_3 &= -\beta x_2 \end{aligned} \tag{3}$$

donde la función no lineal es

$$f(x_1) = bx_1 + \frac{1}{2}(a - b)(|x_1 + 1| - |x_1 - 1|). \tag{4}$$

3.7 – Dinámicas del circuito de Chua

Con el objetivo de mostrar el comportamiento dinámico del circuito de Chua, se realizaron un conjunto de simulaciones numéricas utilizando el modelo normalizado (3) y (4). En estas simulaciones, se obtuvieron tres tipos de comportamientos en el espacio de estados (atractor). Los comportamientos que presenta el circuito de Chua fueron, un comportamiento estable o punto fijo, otro fue un ciclo limite y por último, un comportamiento caótico.

3.7.1 – Resultados numéricos

En la figura 14 se muestra la evolución en el tiempo de los estados de circuito de Chua donde se puede apreciar que su comportamiento es estable con los valores de $\alpha = 4.05$, $\beta = 6$, $a = -1.758$ y $b = -0.8248$ y condiciones iniciales $x_1(0) = 1.1$, $x_2(0) = 0.1$ y $x_3(0) = -0.5$ con estos valores se observa que los estados del circuito tienden a un valor constante donde $x_1 \to -5.5$, $x_2 \to 0$ y $x_3 \to 5.5$

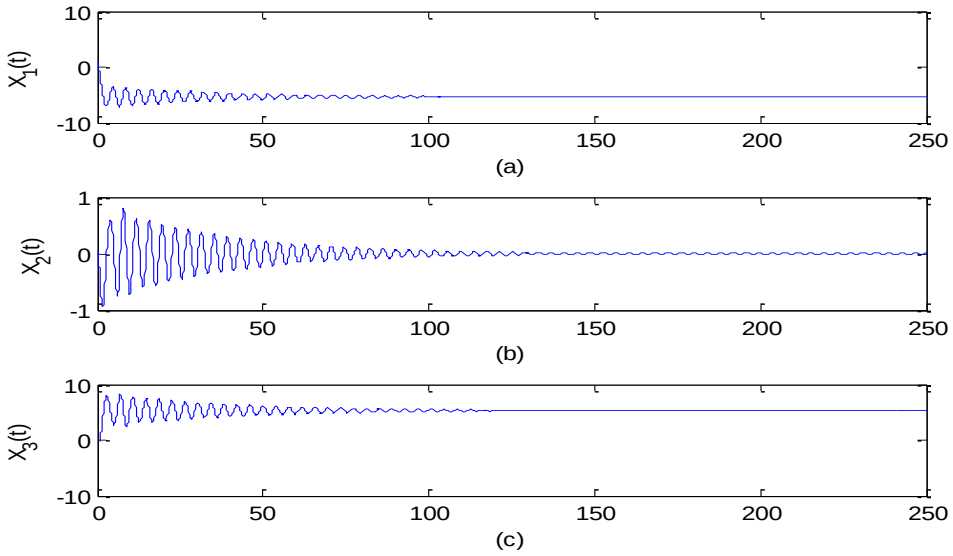


Figura 14. Evolución en el tiempo de los estados del circuito de Chua: a) $x_1(t)$, b) $x_2(t)$, c) $x_3(t)$.

El comportamiento dinámico a través del tiempo de los estados del circuito de Chua también se puede observar en el espacio de estados, es decir, mostrando sus atractores, como lo ilustra la figura 15, donde se observa que estos comportamientos tienden a un punto fijo.

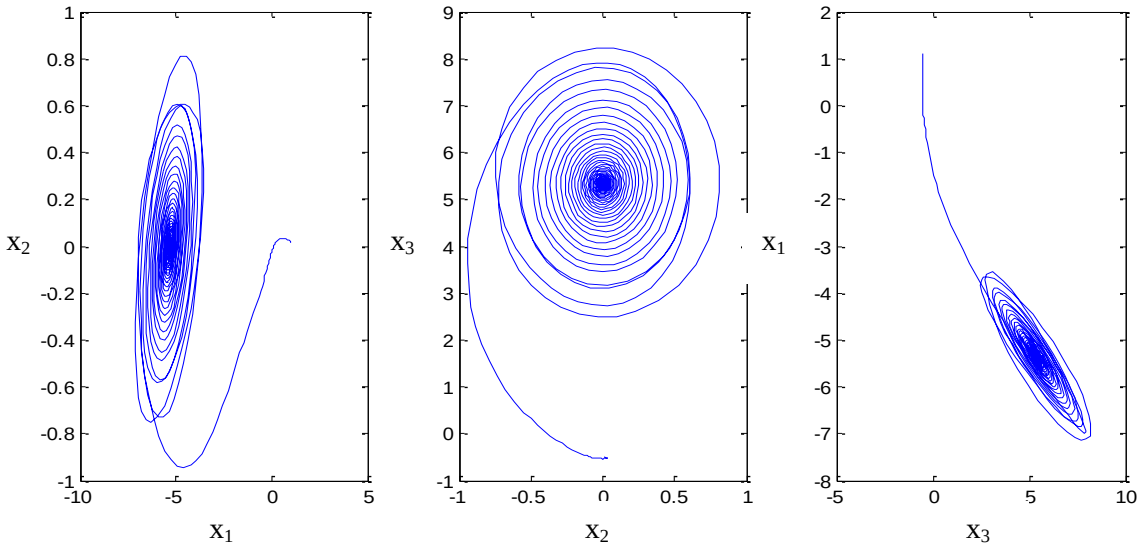


Figura 15. a) Punto atractor proyectado en el plano x_1 *vs* x_2, b) Punto atractor proyectado en el plano x_2 *vs* x_3, c) Punto atractor proyectado en el plano x_3 *vs* x_1.

En la figura 16 se muestra la evolución en el tiempo de los estados de circuito de Chua donde se puede apreciar que su comportamiento es periódico con los valores de $\alpha = 3.7$, $\beta = 5.2$, a = -1.50309 y b = -0.705204 y condiciones iniciales $x_1(0) = 1.1$, $x_2(0) = 0.1$ y $x_3(0) = -0.5$ se observa que todos los estados exhiben comportamiento cíclico.

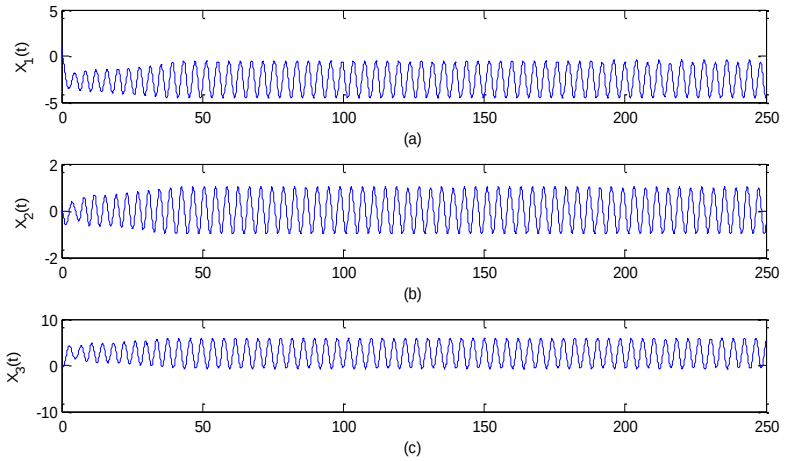
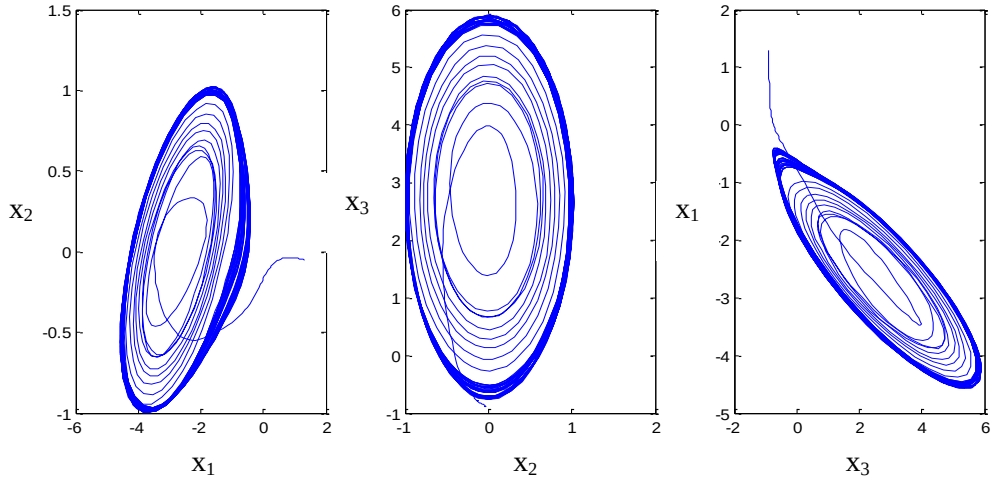


Figura 16. Evolución periódica en el tiempo de los estados $x_1(t)$, $x_2(t)$ y $x_3(t)$ del circuito de Chua.

El comportamiento dinámico a través del tiempo de los estados del circuito de Chua también se puede observar en el espacio de estados, mostrando los atractores, que se muestra en la figura 17, donde se observa que estos comportamientos tienden a un *ciclo límite estable*.



(a) (b) (c)

Figura 17. a) Ciclo atractor proyectado en el plano x_1 *vs* x_2, b) ciclo atractor proyectado en el plano x_2 *vs* x_3, c) ciclo atractor proyectado en el plano x_3 *vs* x_1.

En la figura 18 se muestra la evolución en el tiempo de los estados de circuito de Chua donde se puede apreciar que su comportamiento es caótico con los valores de $\alpha = 10$, $\beta = 19$, $a = -1.4325$ y $b = -0.7831$ y condiciones iniciales $x_1(0) = 1.1$, $x_2(0) = 0.1$ y $x_3(0) = -0.5$ se puede observar que la amplitud de las señales con respecto al tiempo no exhiben patrón o periodicidad visible, esto cumple con una de las características de los sistemas caóticos.

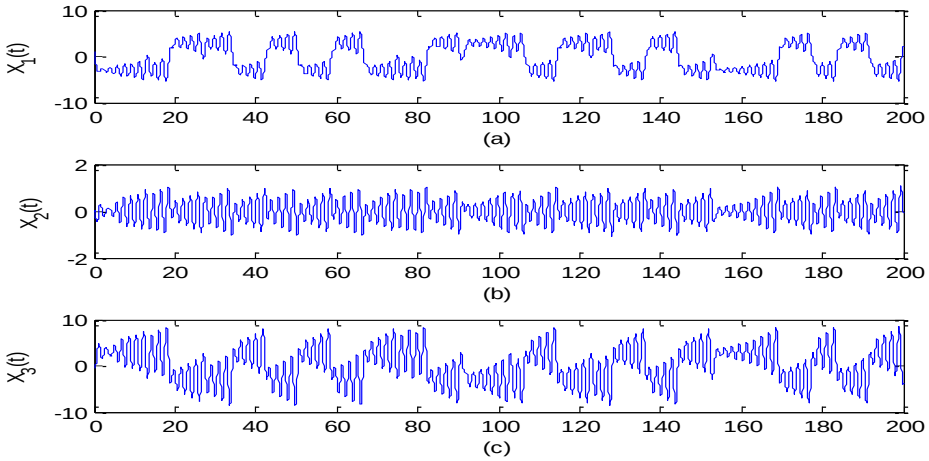


Figura 18. Evolución caótica en el tiempo de los estados $x_1(t)$, $x_2(t)$ y $x_3(t)$ del circuito de Chua.

En la figura 19 se muestran los atractores caóticos o extraños formados por las trayectorias caóticas de los estados.

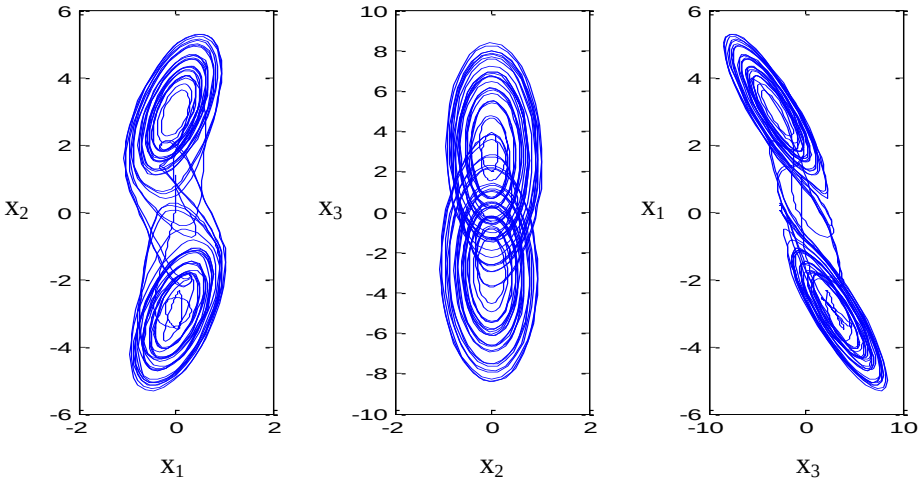


Figura 19. a) Atractor caótico proyectado en el plano x_1 *vs* x_2, b) atractor caótico proyectado en el plano x_2 *vs* x_3, c) atractor caótico proyectado en el plano x_3 *vs* x_1.

3.8 - Conclusiones

El circuito de Chua representa una herramienta versátil para analizar muchas de las características asociadas a sistemas no lineales: orbitas estables, periódicas y caóticas. Como herramienta didáctica y de investigación, el circuito de Chua resulta muy adecuado para estos propósitos ya que a pesar de ser muy sencillo puede ser utilizado como un sistema de encriptamiento capaz proteger la información que se desee transmitir.

Capítulo 4

Circuito hipercaótico de Chua

4.1 – Introducción

En este capítulo se mostrará el circuito de Chua de cuarto orden el cual exhibe un comportamiento hipercaótico. Este circuito es el utilizado en este trabajo de tesis, aquí se mostrarán sus características principales y de igual manera sus dinámicas. Además, se describe su implementación física y algunas pruebas experimentales.

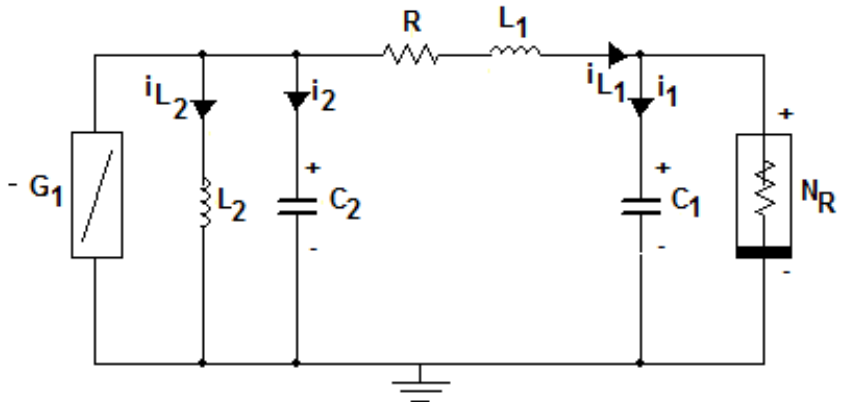
4.1.1 - Circuito hipercaótico de Chua

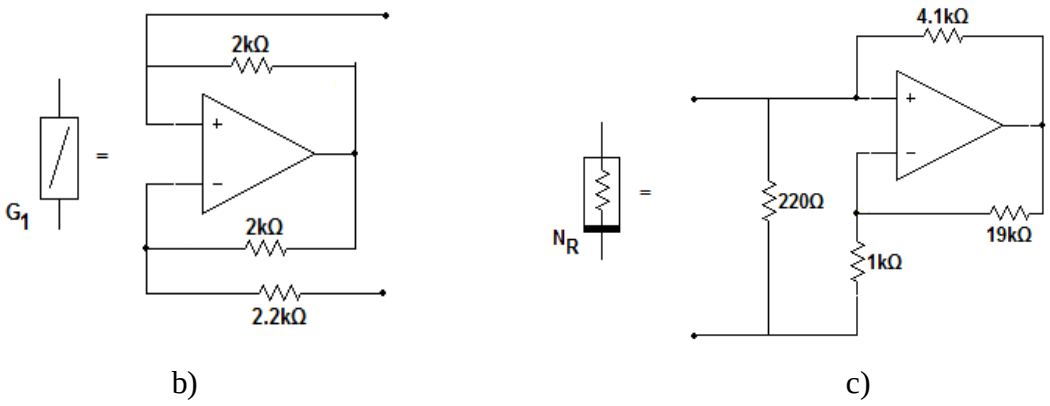
Un sistema hipercaótico se define como un sistema dinámico, el cual, exhibe más de un exponente de Lyapunov positivo, es decir, sus dinámicas se expanden no solo en una dirección sino en dos o más direcciones, obteniéndose con esto, un incremento en la complejidad de las dinámicas del sistema. Esta propiedad hace que el sistema hipercaótico sea grandemente atractivo para su empleo en comunicaciones seguras.

El sistema hipercaótico utilizado en esta tesis fue propuesto en [Thamilmaran y Lakshmanan 2004] es un circuito de Chua de cuarto orden caracterizado por una no linealidad cubica suave, cuya implementación física no requiere gran cantidad de circuitería electrónica comparada con la de la función no lineal por segmentos en que se basa el circuito original de Chua (descrito por las ecuaciones (1) y (2)).

En la figura 20 se muestra el circuito de Chua de cuarto orden utilizado en este trabajo, donde se puede observar que su implementación no requiere de gran problema, pues es un circuito relativamente sencillo pero con gran potencial.

a)





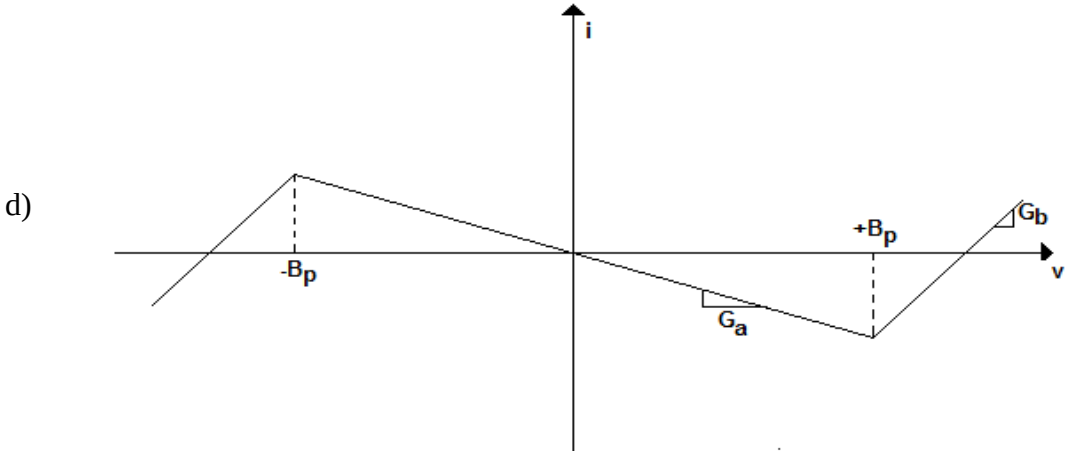


Figura 20. a) Circuito hipercaótico de Chua de cuarto orden, b) Conductancia negativa, c) Resistencia negativa, d) Función de respuesta de la resistencia no lineal.

4.2 - Ecuaciones de estado del circuito hipercaótico de Chua

Las ecuaciones diferenciales que modelan el comportamiento del circuito de Chua de cuarto orden y que se obtienen al aplicar las leyes de Kirchhoff, se presentan a continuación:

$$C_1 \frac{dv_1}{dt} = i_{L_1} - g(v_1) \,,$$

$$C_2 \frac{dv_2}{dt} = -G_1 v_2 - \; i_{L_1} - \; i_{L_2} \,, \qquad (5)$$

$$L_1 \frac{di_1}{dt} = v_2 - \; v_1 - \; R\, i_{L_1} \,,$$

$$L_2 \frac{di_2}{dt} = v_2$$

donde la función no lineal se expresa como

$$g(v_1) = G_b v_1 + \frac{1}{2}(G_a - G_b)\left[\left|v_1 + B_p\right| - \left|v_1 - B_p\right|\right]. \quad (6)$$

4.3 - Ecuaciones normalizadas del circuito hipercaótico de Chua

Mediante un cambio de variable apropiado es posible transformar las ecuaciones (5) y (6) en un conjunto de ecuaciones adimensionales. Los voltajes v_1 y v_2 y las corrientes i_1 y i_2 en el circuito de Chua de cuarto orden son transformados a las variables normalizadas x_1, x_2, x_3 y x_4 respectivamente, definidas por

$$x_1 \triangleq \frac{v_1}{B_p}, \qquad x_2 \triangleq \frac{v_2}{B_p}, \qquad x_3 \triangleq \frac{i_1}{GB_p}, \qquad x_4 \triangleq \frac{i_2}{GB_p}.$$

De la misma forma, los parámetros del circuito de Chua de cuarto orden son transformados en parámetros normalizados definidos por

$$\propto_1 \triangleq \frac{c_2}{c_1}, \qquad \propto_2 \triangleq \frac{G_1}{G}, \qquad \beta_1 \triangleq \frac{c_2}{L_1 G^2}, \qquad \beta_2 \triangleq \frac{c_2}{L_2 G^2}, \qquad a \triangleq \frac{G_a}{G}, \qquad b \triangleq \frac{G_b}{G},$$

$$G = \frac{1}{R}, \quad f(x_1) = \left(\frac{1}{GB_P}\right) g(B_P x_1).$$

De este modo, obtenemos finalmente las ecuaciones normalizadas del circuito de Chua de cuarto orden propuesto en [Thamilmaran y Lakshmanan 2004] como sigue:

$$\begin{aligned} \dot{x}_1 &= \alpha_1(x_3 - f(x_1)), \\ \dot{x}_2 &= -\alpha_2 x_2 - x_3 - x_4, \\ \dot{x}_3 &= \beta_1(x_2 - x_1 - x_3), \\ \dot{x}_4 &= \beta_2 x_2 \end{aligned} \quad (7)$$

donde la función no lineal está definida como

$$f(x_1) = bx_1 + \frac{1}{2}(a - b)(|x_1 + 1| - |x_1 - 1|). \quad (8)$$

4.4 - Dinámicas del circuito hipercaótico de Chua

4.4.1 - Resultados numéricos

Con el objetivo de mostrar el comportamiento dinámico del circuito de Chua de cuarto orden, se hicieron las simulaciones numéricas utilizando el modelo normalizado (7) y (8). En estas simulaciones se obtuvieron los comportamientos hipercaóticos que exhibe el sistema, mostrados en los siguientes resultados numéricos.

En la figura 21 se muestra la evolución en el tiempo de los cuatro estados de circuito de Chua de cuarto orden, se puede apreciar que su comportamiento es hipercaótico con los valores de $\alpha_1 = 2.1429$, $\alpha_2 = -0.1283$, $\beta_1 = 0.0393$, $\beta_2 = 0.0015$, a = -0.0299 y b = 1.995, se puede observar como la amplitud de las señales con respecto al tiempo no exhiben un patrón o una periodicidad visible.

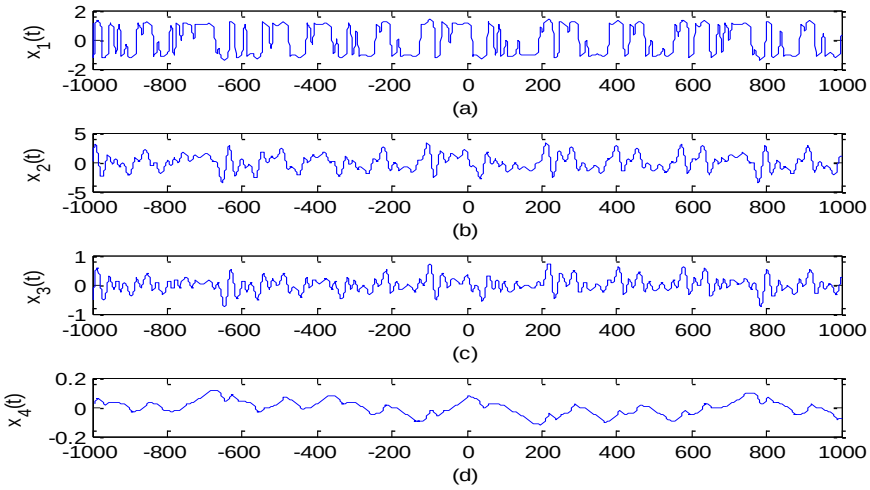


Figura 21. Evolución en el tiempo de los estados hipercaóticos $x_1(t)$, $x_2(t)$, $x_3(t)$ y $x_4(t)$ del circuito de Chua de cuarto orden.

En la figura 22 se muestran los atractores hipercaóticos formados por las trayectorias de los estados del circuito de Chua de cuarto orden.

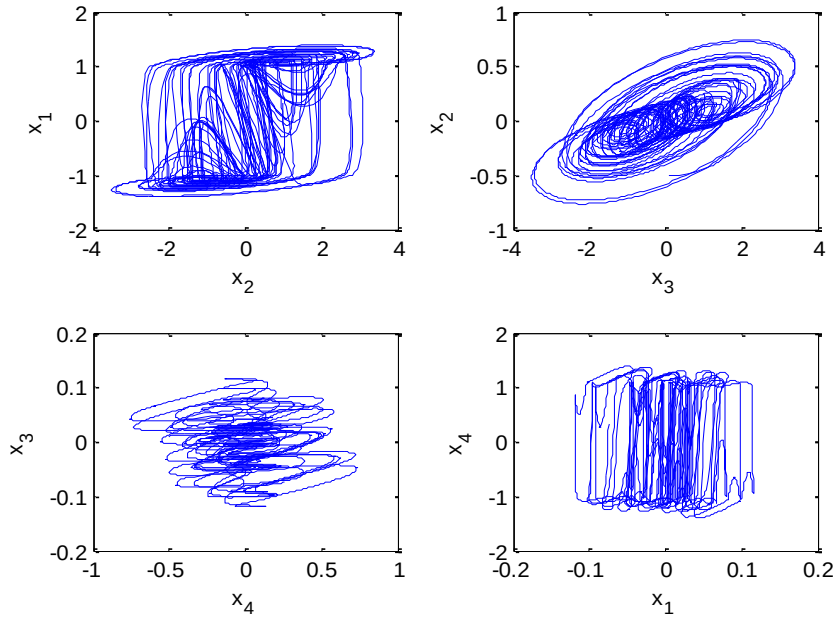


Figura 22. a) Atractor caótico proyectado en el plano x_1 vs x_2, b) atractor caótico proyectado en el plano x_2 vs x_3, c) atractor caótico proyectado en el plano x_3 vs x_4, d) atractor caótico proyectado en el plano x_4 vs x_1.

4.4.2 – Resultados experimentales

En la figura 23 se aprecia el diagrama esquemático del circuito de Chua de cuarto orden que se implementó físicamente en este trabajo de tesis

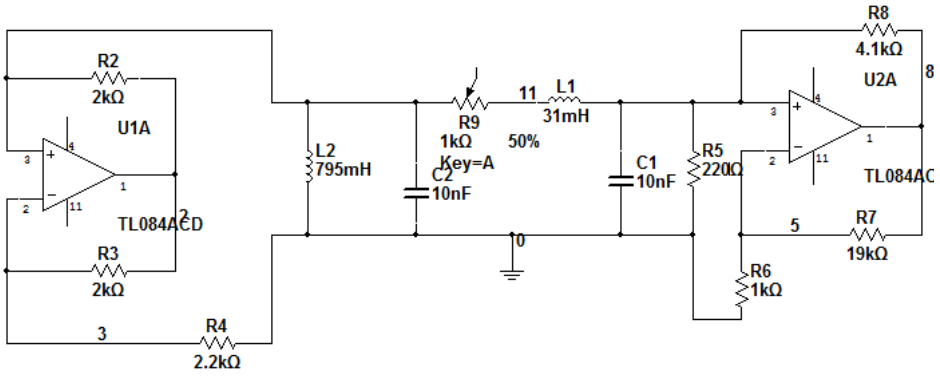


Figura 23. Diagrama esquemático del circuito de Chua de cuarto orden.

En la figura 24 se muestra el circuito de Chua de cuarto orden de forma experimental.

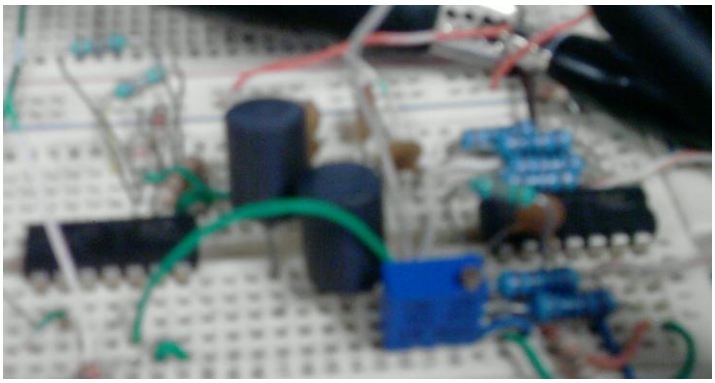


Figura 24. Implementación física del circuito de Chua de cuarto orden

La figura 25 muestra la evolución en el tiempo de los estados del circuito de Chua de cuarto orden, donde la señal amarilla representa el estado $x_1(t)$ (arriba), la señal azul el estado $x_2(t)$ (en medio) y la señal violeta $x_3(t)$ (abajo), todas mostradas en la pantalla de un osciloscopio.

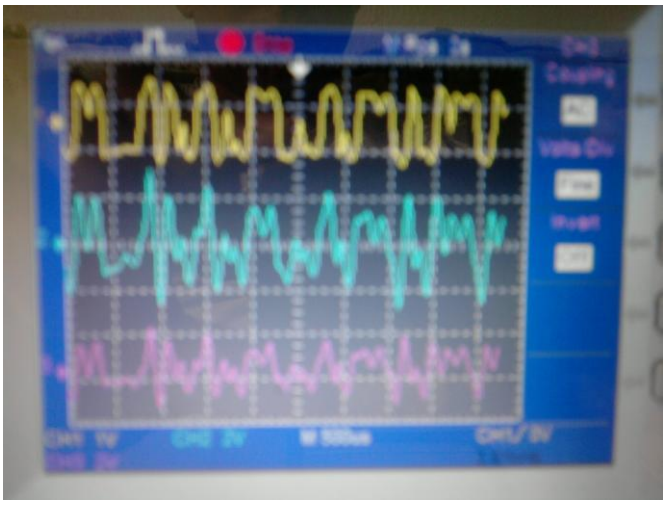
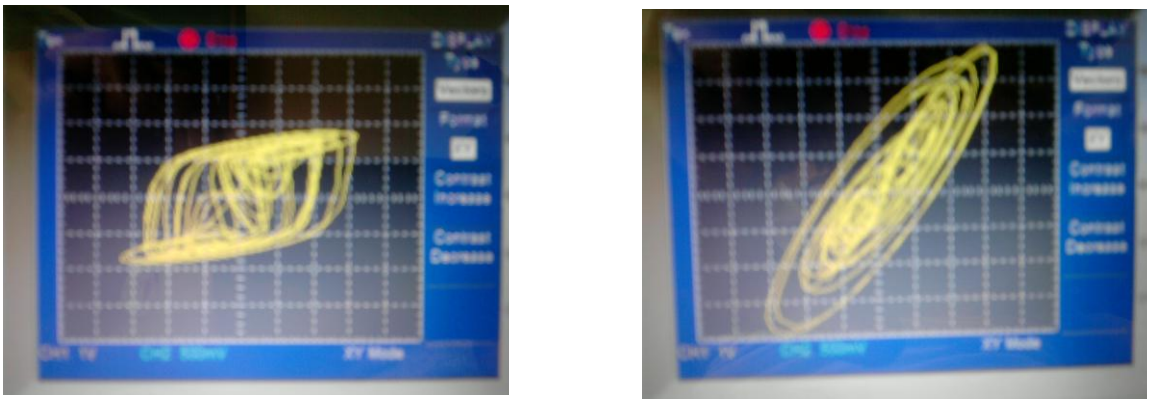


Figura 25. Evolución en el tiempo de los estados del circuito de Chua de cuarto orden

En la figura 26 se muestran los atractores hipercaóticos que genera el circuito de Chua de cuarto orden, donde la figura 26 (a) representa al estado $x_1 \, vs \, x_2$ y la figura 26 (b) representa $x_2 \, vs \, x_3$.



a) b)

Figura 26. Atractores hipercaóticos del circuito de Chua de cuarto orden. (a) $x_1 \, vs \, x_2$, (b) $x_2 \, vs \, x_3$

4.5 - Conclusiones

En este capítulo se mostró el circuito modificado de Chua de cuarto orden utilizado en este trabajo de tesis, se mencionaron las características que definen a un sistema hipercaótico y se mostraron los resultados numéricos y experimentales obtenidos, como son las dinámicas hipercaóticas de los cuatro estados a través del tiempo y los atractores hipercaóticos que forman estos estados. Fue mostrado la coincidencia entre los resultados numéricos y los resultados experimentales.

Capítulo 5

Sincronización por formas hamiltonianas y diseño de un observador

5.1 – Introducción

En este capítulo se proporciona una reseña de lo que es la sincronía de osciladores caóticos así como también algunos escenarios de acoplamiento de estos sistemas. Posteriormente se presenta el método de sincronía utilizado en este trabajo de tesis que es el de sincronización por forma hamiltonianas y diseño de observador sugerido en [Sira-Ramírez y Cruz-Hernández 2000; 2001]. Enseguida se muestra su aplicación para el circuito de Chua de cuarto orden presentado en el capítulo anterior, también se hace un análisis de estabilidad y se reportan los resultados obtenidos.

5.2 - Sincronización de sistemas caóticos e hipercaóticos

El concepto de sincronización está usualmente ligado al movimiento periódico. Dos señales periódicas están sincronizadas si sus periodos son idénticos. Esta definición resulta ser inadecuada en el contexto de las señales caóticas, en este caso se requiere que las señales sean idénticas, al menos asintóticamente cuando $t \rightarrow \infty$.

Como ya se ha mencionado, el fenómeno del caos se encuentra en la mayoría de los sistemas, tanto naturales como artificiales y como es bien sabido en tiempos recientes se han propuesto muchas ideas y técnicas para aprovechar estos sistemas y utilizarlos en forma benéfica. Desde que se logró la sincronía caótica se ha venido utilizando en diferentes áreas, para acoplar circuitos electrónicos, para aumentar la potencia en láseres, para controlar oscilaciones en reacciones químicas, para estabilizar el ritmo cardíaco y para el encriptado de información, estas aplicaciones tienen su base en dos problemas, que son el control del caos y la sincronización de sistemas caóticos.

Se creyó en un tiempo, que la sincronía en osciladores caóticos no se puede llevar a cabo, ya que una de las características de estos sistemas es su sensibilidad a condiciones iniciales, así que, un pequeño cambio en ellas altera completamente el comportamiento.

Se dice que dos sistemas caóticos están es sincronía cuando finalmente transcurrido el transitorio, sus oscilaciones coinciden en todo tiempo, a pesar de iniciar bajo condiciones distintas.

En general, la investigación de la sincronización se ha enfocado en dos áreas. La primera tiene que ver con el empleo de observadores de estado, donde las principales aplicaciones recaen en la sincronización de osciladores caóticos. La segunda es el uso de leyes de control, las cuales permiten alcanzar la sincronización entre osciladores no lineales

con diferente estructura y orden [Wu y Chua 1994]. Un interés particular es la conexión entre los observadores para sistemas no lineales y la sincronización caótica, que se conoce también como configuración maestro y esclavo. Por lo que el problema de sincronización caótica se puede ver como un procedimiento de diseño de observadores [Nijmeijer y Mareels 1997].

Definición (Sincronización caótica) [Cruz-Hernández y Mortynyuk 2009]: *Considere un sistema caótico modelado por la ecuación de estado*

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

y otro por

$$\dot{\hat{x}} = f(x) \tag{10}$$

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

$$\lim_{t\to 0}\|x(t) - \hat{x}(t)\| \equiv 0. \tag{11}$$

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

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

5.3 - Escenarios de Acoplamiento

Desde la observación de **Pecora** y **Carroll** acerca de la posibilidad de sincronizar dos sistemas caóticos, se han desarrollado bastantes esquemas de sincronización. La sincronización se puede clasificar en sincronización maestro y esclavo (o acoplamiento unidireccional) [Pecora y Carroll 1990] y sincronización mutua (o acoplamiento bidireccional) [Ushio 1999].

5.3.1 - Acoplamiento unidireccional

La sincronización con acoplamiento unidireccional, conocida como sincronización maestro y esclavo, se da cuando un sistema *A* tiene influencia sobre un sistema *B*, pero no a la inversa, es decir, que el sistema *B* no tiene influencia sobre el sistema *A* (ver figura 27). Como su nombre lo indica la información solo fluye en un sentido. En esta forma y como resultado de este acoplamiento, el sistema *A* (maestro) impone su comportamiento dinámico al sistema *B* (esclavo) [Mejía – Camacho 2007].

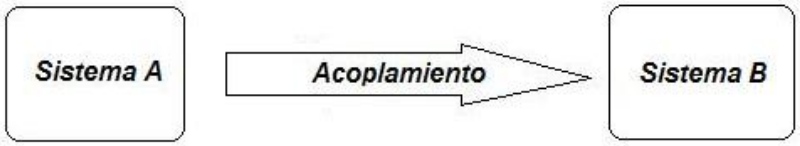


Figura 27. Esquema de acoplamiento unidireccional entre los sistemas A y B

5.3.2 - Acoplamiento bidireccional

La sincronización con acoplamiento bidireccional, conocida como sincronización mutua, se da cuando un sistema *A* tiene influencia sobre un sistema *B* y viceversa, es decir, el sistema *B* también tiene influencia sobre el sistema *A* [Mejía – Camacho 2007]. En este esquema de acoplamiento, la información fluye en ambos sentidos (ver figura 28). Como resultado de este acoplamiento se puede dar:

a) Que las dinámicas de los dos osciladores sean iguales a la dinámica del oscilador *A* o del oscilador *B.*
b) Que las dinámicas de los dos osciladores sean iguales a una tercera dinámica, diferente a la del oscilador *A* y oscilador *B.*

Figura 28. Esquema de acoplamiento bidireccional entre los sistemas A y B.

5.4 - Sincronización por formas hamiltonianas

Considérese un sistema autónomo de la forma

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

el cual, representa un sistema que exhibe un comportamiento *hipercaótico*. Donde $x(t) = \left(x_1(t), \ldots, x_n(t)\right)^T \in \Re^n$ 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 descritos por (13) pueden escribirse en la siguiente forma canónica de un hamiltoniano generalizado

$$\dot{x} = \mathcal{J}(x)\frac{\partial H}{\partial x} + S(x)\frac{\partial H}{\partial x} + \mathcal{F}(x), \quad x \in \Re^{n} \tag{14}$$

donde *H(x)* nos indica una función de energía suave, la cual, es definida positiva globalmente en $\Re^{n}$. El vector gradiente de *H*, representado por $\partial H/\partial x$ es considerado que existe en cualquier parte. Frecuentemente utilizamos funciones de energía cuadráticas de la forma $H(x)=(1/2)x^{T}Mx$ con M una matriz constante, definida positiva y simétrica. En tales casos, $\partial H/\partial x = Mx$.

Las matrices cuadradas, $\mathcal{J}(x)$ y $S(x)$ mencionadas en la expresión (14) deben satisfacer para toda $x \in \Re^{n}$ las propiedades:

$$\mathcal{J}(x) + \mathcal{J}^{T}(x) = 0 \quad \text{y} \quad S(x) = S^{T}(x).$$

El vector de campo $\mathcal{J}(x)\partial H/\partial x$ representa la parte *conservativa* del sistema y el vector de campo $S(x)\partial H/\partial x$, nos describe la parte *no conservativa* del sistema. Para ciertos casos, la matriz simétrica $S(x)$ es definida negativa o semi-definida negativa. En tales casos, el campo vectorial $S(x)\partial H/\partial x$ representa la parte *disipativa* del sistema. Si por el contrario, $S(x)$ es definida positiva, semi-definida positiva o indefinida, éste claramente representa, la parte *desestabilizante* del sistema, global, semi-global o local, respectivamente. En el caso de ser $S(x)$ indefinida, ésta se descompone en la suma de una matriz simétrica semi-definida negativa $\mathcal{R}(x)$ y una matriz simétrica semi-definida positiva $\aleph(x)$. Y donde $\mathcal{F}(x)$ representa el vector de campo localmente desestabilizante.

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

En el contexto de diseño de observadores, en nuestro caso, consideramos una clase especial de las formas hamiltonianas con vector de campo desestabilizante y un mapeo lineal de salida $y(t)$, expresada como sigue

$$\begin{aligned} \dot{x} &= \mathcal{J}(x)\frac{\partial H}{\partial x} + (\beth + S)\frac{\partial H}{\partial x} + \mathcal{F}(y), \quad x \in \Re^{n} \\ y &= C\frac{\partial H}{\partial x}, \quad y \in \Re^{m} \end{aligned} \tag{15}$$

donde S es una matriz constante simétrica, no necesariamente de signo definido, la matriz $\beth$ es una matriz constante antisimétrica, y es la salida del sistema y C es una matriz constante.

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

Por tanto, podemos obtener un observador de estado no lineal para (15) de la siguiente forma

$$\dot{\hat{x}} = \mathcal{J}(y)\frac{\partial H}{\partial \hat{x}} + (\mathcal{R} + S)\frac{\partial H}{\partial \hat{x}} + \mathcal{F}(y) + K(y - \hat{y})\,,$$

$$y = C\frac{\partial H}{\partial \hat{x}} \tag{16}$$

donde $K = (k_1,\, k_2, \ldots, k_n)^T$ es una matriz constante, conocida como *ganancia del observador*. En el contexto de la sincronización, el observador (16) realizará el papel de oscilador esclavo, cuya función será estimar las dinámicas completas del sistema (15).

El error estimado del estado, definido como $e = x - \hat{x}$. Y el error estimado de la salida, definido como $e_y = y - \hat{y}$, son gobernados por

$$\dot{e} = \mathcal{J}(y)\frac{\partial H}{\partial e} + (\mathcal{R} + S - KC)\frac{\partial H}{\partial e}\,, \qquad e \in \Re^{n}\,,$$

$$e_y = C\frac{\partial H}{\partial e}, \qquad e_y \in \Re^{m} \tag{17}$$

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

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

5.4.2 - Análisis de estabilidad de sincronía

En esta sección, se dan condiciones de estabilidad para el error de sincronía (17) entre los circuitos maestro (15) y esclavo (16)

Teorema 1 [Sira-Ramírez y Cruz-Hernández 2000; 2001]: *El estado $x(t)$ del oscilador no lineal (15) puede ser global, asintótica y exponencialmente estimado por el estado $\hat{x}(t)$ de un observador de la forma (16), 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, más no necesaria para la reconstrucción asintótica de los estados del sistema maestro (15). Una condición necesaria y suficiente para estabilidad asintótica global del error de estimación (13), está dada por el siguiente teorema.

Teorema 2 [Sira-Ramírez y Cruz-Hernández 2000; 2001]: *El estado $x(t)$ del sistema (15) puede ser global, asintótica y exponencialmente estimado por el estado $\hat{x}(t)$ del observador (16), si y sólo si, existe una matriz constante K, tal que la matriz simétrica*

$$[W - KC] + [W - KC]^T = [S - KC] + [S - KC]^T = 2\left[S - \frac{1}{2}(KC + C^T K^T)\right] \qquad (19)$$

sea definida negativa.

5.5 - Sincronización de dos circuitos hipercaóticos de Chua

Se dice que el sistema receptor (16) sincroniza con el sistema transmisor (15), si $e(t) \rightarrow 0$ a medida que $t \rightarrow \infty$, donde $e(t)$ representa el error de sincronía.

5.5.1 - Sincronización de dos circuitos hipercaóticos de Chua

Para realizar las simulaciones numéricas se tomaron en cuenta las ecuaciones normalizadas del circuito de Chua de cuarto orden (7) y (8) las cuales facilitan dichas simulaciones:

Considere el siguiente circuito de Chua de cuarto orden (7) propuesto en [Thamilmaran y Lakshmanan, 2004]

$$\begin{aligned}
\dot{x}_1 &= \alpha_1(x_3 - f(x_1)), \\
\dot{x}_2 &= -\alpha_2 x_2 - x_3 - x_4, \\
\dot{x}_3 &= \beta_1(x_2 - x_1 - x_3), \\
\dot{x}_4 &= \beta_2 x_2
\end{aligned}$$

donde la función no lineal es definida como

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

Considerando como función de energía hamiltoniana a

$$H(x) = \frac{1}{2}\left[\frac{x_1^2}{\alpha_1} + x_2^2 + \frac{x_3^2}{\beta_1} + \frac{x_4^2}{\beta_2}\right] \tag{20}$$

el sistema (7) se puede reescribir en forma canónica hamiltoniana generalizada de acuerdo a la ecuación (15) como

$$\begin{bmatrix} \dot{x_1} \\ \dot{x_2} \\ \dot{x_3} \\ \dot{x_4} \end{bmatrix} = \begin{bmatrix} 0 & 0 & \alpha_1\beta_1 & 0 \\ 0 & 0 & -\beta_1 & -\beta_2 \\ -\alpha_1\beta_1 & \beta_1 & 0 & 0 \\ 0 & \beta_2 & 0 & 0 \end{bmatrix} \frac{\partial H}{\partial x} + \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & -\alpha_2 & 0 & 0 \\ 0 & 0 & -\beta_1^2 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \frac{\partial H}{\partial x} + \begin{bmatrix} -\alpha_1 f(x_1) \\ 0 \\ 0 \\ 0 \end{bmatrix}. \tag{21}$$

Siendo el vector gradiente

$$\frac{\partial H}{\partial x} = \begin{bmatrix} \frac{1}{\alpha_1} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\beta_1} & 0 \\ 0 & 0 & 0 & \frac{1}{\beta_2} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} \frac{x_1}{\alpha_1} \\ x_2 \\ \frac{x_3}{\beta_1} \\ \frac{x_4}{\beta_2} \end{bmatrix}. \tag{22}$$

En (21) se identifica que el vector desestabilizante se encuentra gobernado por $x_1(t)$, lo que indica que este estado será transmitido hacia el circuito esclavo. La salida de (15) que será transmitida a (16) es *y(t)* = $x_1(t)$. C, S y ך están dadas por

$$C^T = \begin{bmatrix} \alpha_1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \qquad S = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & -\alpha_2 & 0 & 0 \\ 0 & 0 & -\beta_1^2 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

$$ך = \begin{bmatrix} 0 & 0 & \alpha_1\beta_1 & 0 \\ 0 & 0 & -\beta_1 & -\beta_2 \\ -\alpha_1\beta_1 & \beta_1 & 0 & 0 \\ 0 & \beta_2 & 0 & 0 \end{bmatrix}. \tag{23}$$

La salida queda de la siguiente forma

$$y = [\alpha_1 \quad o \quad o \quad o]^T \frac{\partial H}{\partial x}. \tag{24}$$

Entonces el observador construido queda dado por la expresión

$$\begin{bmatrix} \dot{\widehat{x_1}} \\ \dot{\widehat{x_2}} \\ \dot{\widehat{x_3}} \\ \dot{\widehat{x_4}} \end{bmatrix} = \begin{bmatrix} 0 & 0 & \alpha_1\beta_1 & 0 \\ 0 & 0 & -\beta_1 & -\beta_2 \\ -\alpha_1\beta_1 & \beta_1 & 0 & 0 \\ 0 & \beta_2 & 0 & 0 \end{bmatrix} \frac{\partial H}{\partial \hat{x}} + \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & -\alpha_2 & 0 & 0 \\ 0 & 0 & -\beta_1^2 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \frac{\partial H}{\partial \hat{x}} + \begin{bmatrix} -\alpha_1 f(y) \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} k_1 \\ k_2 \\ k_3 \\ k_4 \end{bmatrix} e_y, \tag{25}$$

donde el error esta dado por

$$e_y = [x_1 - \hat{x}_1]. \tag{26}$$

El sistema dinámico del error es

$$\begin{bmatrix} \dot{e_1} \\ \dot{e_2} \\ \dot{e_3} \\ \dot{e_4} \end{bmatrix} = \begin{bmatrix} 0 & \frac{k_2\alpha_1}{2} & \alpha_1\beta_1 + \frac{k_3\alpha_1}{2} & \frac{k_4\alpha_1}{2} \\ -\frac{k_2\alpha_1}{2} & 0 & -\beta_1 & -\beta_2 \\ -\alpha_1\beta_1 - \frac{k_3\alpha_1}{2} & \beta_1 & 0 & 0 \\ -\frac{k_4\alpha_1}{2} & \beta_2 & 0 & 0 \end{bmatrix} \frac{\partial H}{\partial x}$$

$$+ \begin{bmatrix} -k_1\alpha_1 & -\frac{k_2\alpha_1}{2} & -\frac{k_3\alpha_1}{2} & -\frac{k_4\alpha_1}{2} \\ -\frac{k_2\alpha_1}{2} & -\alpha_2 & 0 & 0 \\ -\frac{k_3\alpha_1}{2} & 0 & -\beta_1^2 & 0 \\ -\frac{k_4\alpha_1}{2} & 0 & 0 & 0 \end{bmatrix} \frac{\partial H}{\partial x}. \tag{27}$$

Con base en el Teorema 2, tenemos que para encontrar los valores $k_1, k_2, k_3\ y\ k_4$ para los cuales se garantiza estabilidad asintótica a cero de la trayectoria del error de sincronía, se tiene que cumplir con

$$2\left[S - \frac{1}{2}(KC + C^T K^T)\right] < 0 \tag{28}$$

es decir, al sustituir S, K y C en (19) la matriz simétrica resultante será:

$$\begin{bmatrix} -2k_1\alpha_1 & -k_2\alpha_1 & -k_3\alpha_1 & -k_4\alpha_1 \\ -k_2\alpha_1 & -2\alpha_2 & 0 & 0 \\ -k_3\alpha_1 & 0 & -2\beta_1^2 & 0 \\ -k_4\alpha_1 & 0 & 0 & 0 \end{bmatrix} < 0 \tag{29}$$

K debe tomar valores tal que la condición (19) se satisfaga, para esto, el valor elegido para la ganancia K está limitado por las siguientes condiciones:

$$\begin{gathered} k_1 \geq 0\,, \\ 4k_1\alpha_1\alpha_2 - k_2^2\alpha_1^2 \geq 0\,, \\ 2\left[\alpha_1\beta_1^2(\alpha_1 k_2^2 - 4k_1\alpha_2) + k_3^2\alpha_1^2\alpha_2\right] \geq 0\,, \\ k_4 = 0. \end{gathered} \tag{30}$$

Los valores elegidos para las ganancias del circuito esclavo (25) son K = $[k_1\ k_2\ k_3\ k_4]^T$ con $k_1 = 2.3$, $k_2 = 1$, $k_3 = 0.3$ y $k_4 = 0$ con lo cual cumple lo establecido en el Teorema 2, condición (19), garantizando la estabilidad asintótica y exponencial del error de sincronía *e(t)*.

5.6 - Resultados numéricos

En las siguientes figuras se muestra la sincronización obtenida da manera numérica entre el sistema maestro (7) y el sistema observador esclavo (25).

Con los siguientes valores se llevaron a cabo las simulaciones mostradas a continuación.

Parámetros del sistema y esclavo

$\alpha_1 = 2.1429$, $\alpha_2 = -12.83$, $\beta_1 = 0.0393$, $\beta_2 = 0.0015$, a=-0.0299 y b=1.995

Condiciones iniciales del maestro

$$x(0) = (1.1, 0.1, -0.5, 0.01)$$

Condiciones iniciales del esclavo

$$\hat{x}(0) = (0,0,0,0)$$

Ganancias del esclavo para garantizar la sincronización

$$k_1 = 2.3, \quad k_2 = 1, \quad k_3 = 0.3 \quad y \quad k_4 = 0\,.$$

En la figura 29 se muestra el comportamiento a través del tiempo de los estados del maestro y del esclavo

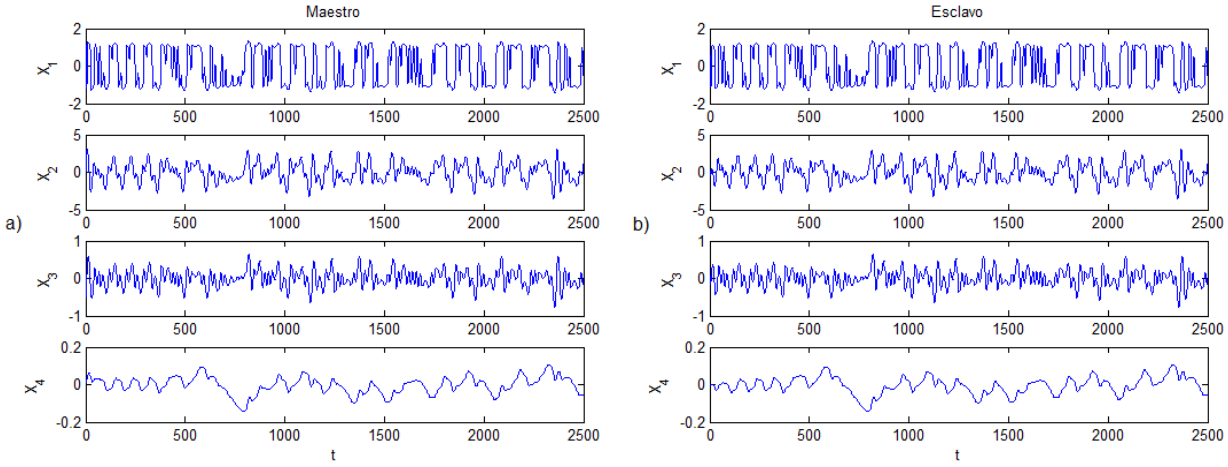


Figura 29. a) Comportamiento en el tiempo del maestro. b) Comportamiento en el tiempo del esclavo.

En la figura 30 se muestra la sincronía entre el maestro y el esclavo a través del tiempo, donde se puede apreciar que en el instante de inicio los comportamientos son totalmente diferentes y con el transcurso del tiempo los comportamientos se asemejan hasta lograr la sincronía, es decir, comportamientos iguales.

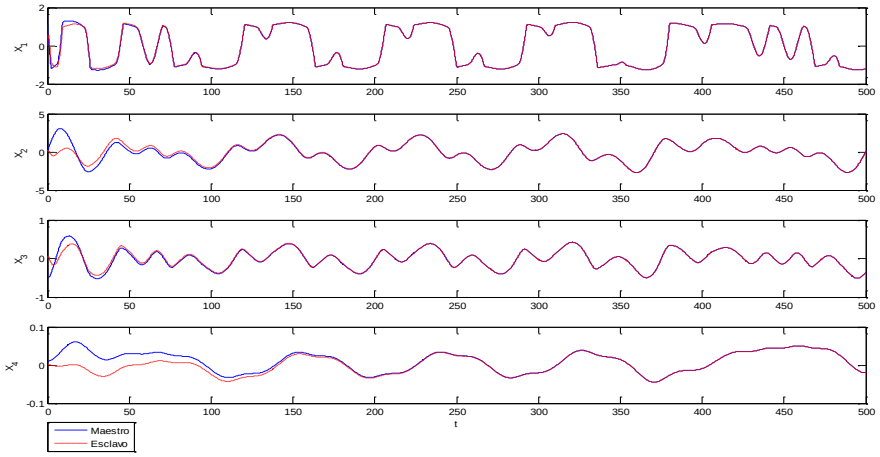


Figura 30. Sincronía entre maestro y esclavo a través del tiempo

La figura 31 muestra el error de sincronía a través del tiempo existente entre el maestro y el esclavo $e_i(t) = x_i(t) - \hat{x}_i(t), i = 1,2,3,4$

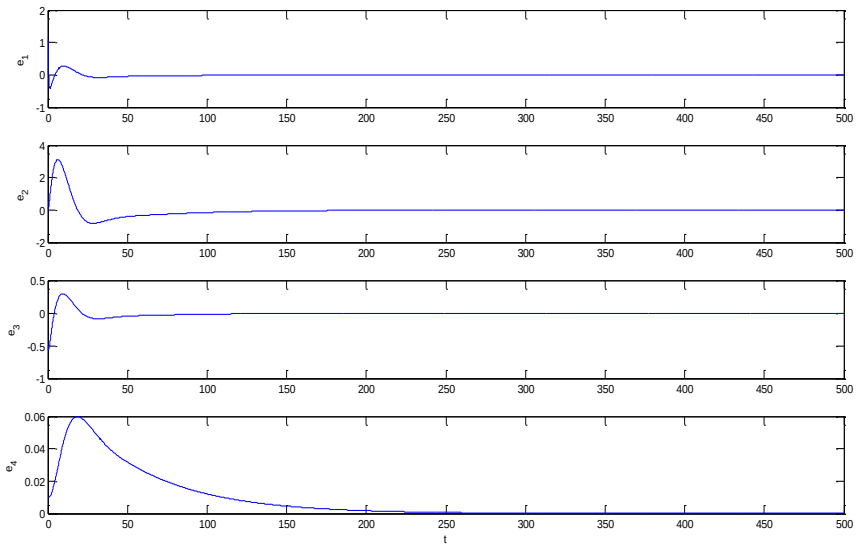


Figura 31. Error de sincronía entre el maestro y el esclavo.

En la figura 32 se muestra el plano de fase existente entre los estados del maestro y el esclavo.

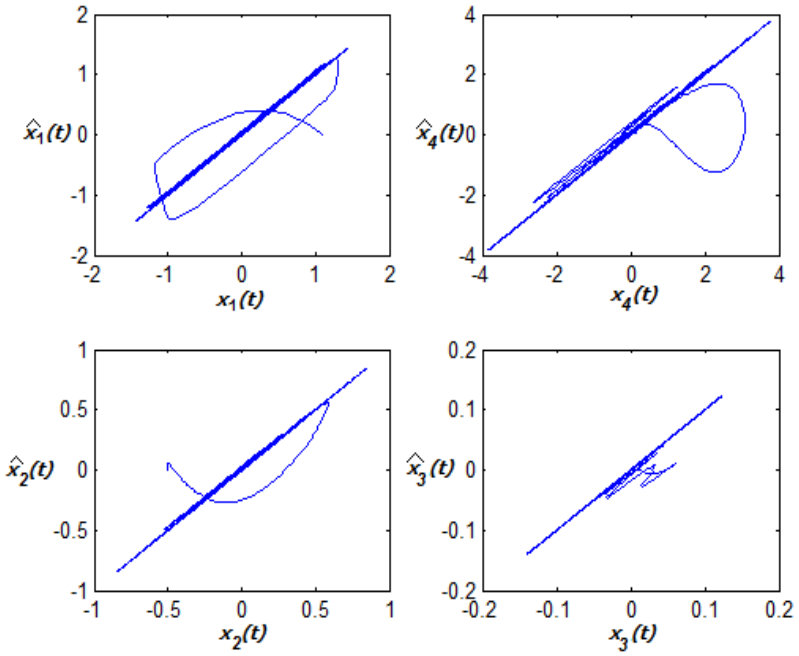


Figura 32. Plano de fase entre el circuito maestro y esclavo.

5.7 - Resultados experimentales

En la figura 33 se muestra el diagrama esquemático implementado para la sincronización entre el maestro y el esclavo por formas hamiltonianas y un observador.

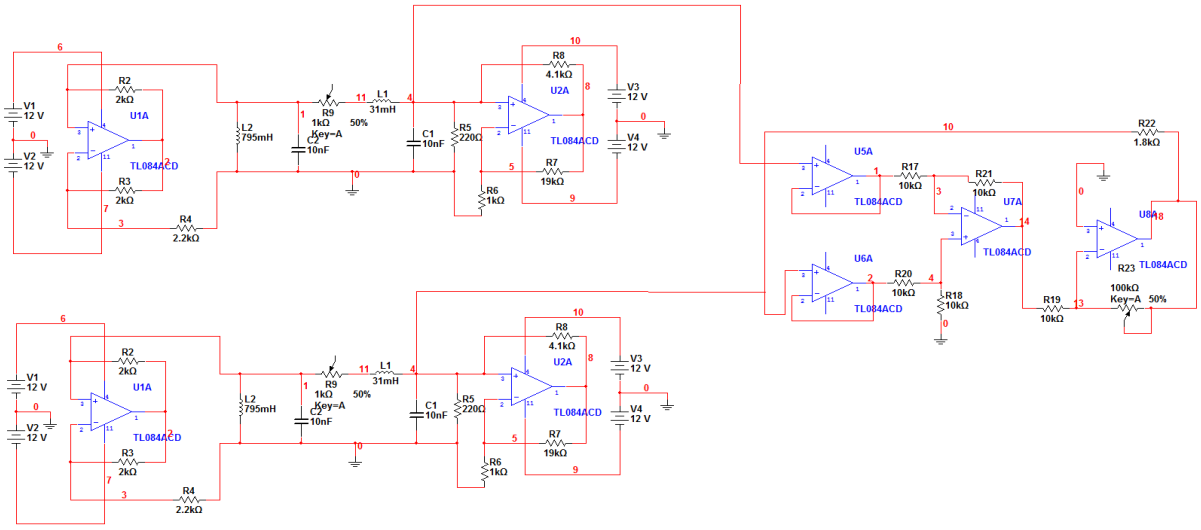


Figura 33. Diagrama esquemático de la sincronización entre maestro y esclavo.

En la figura 34 se muestra el comportamiento a través del tiempo de los estados del maestro y del esclavo en forma experimental.

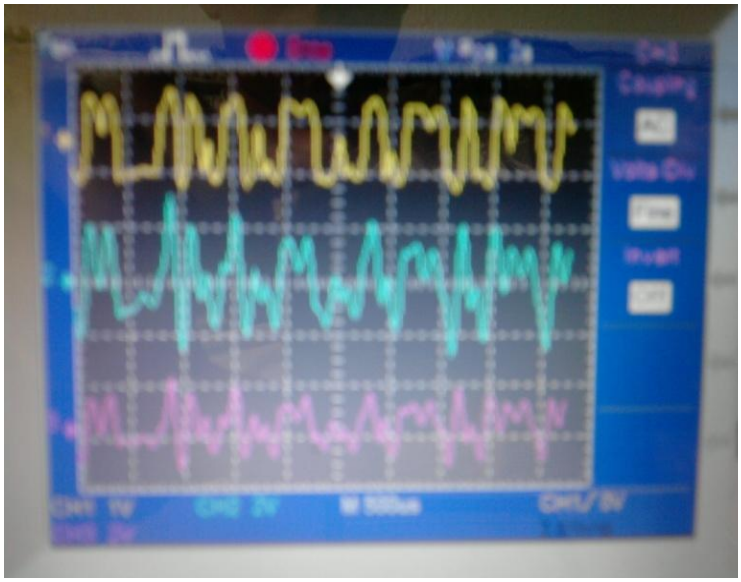


Figura 34. Estados del circuito de Chua de cuarto orden a través del tiempo.

En la figura 35 se muestra el plano de fase entre los estados del maestro y del esclavo.

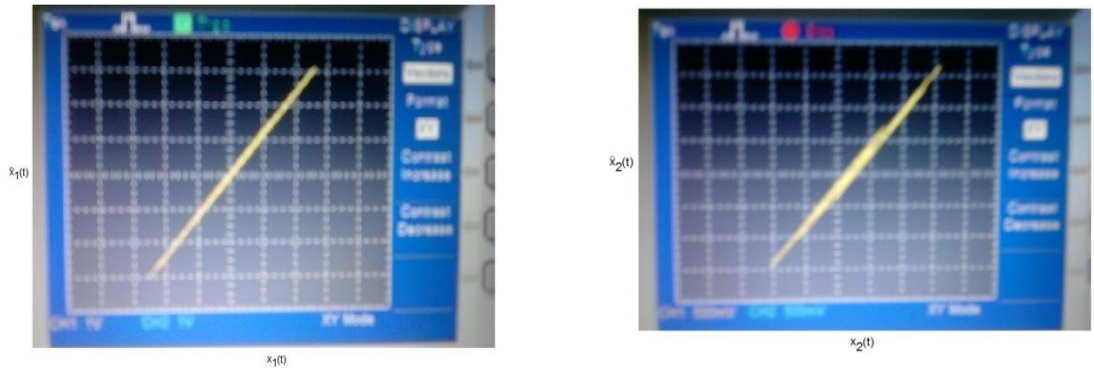


Figura 35. Plano de fase de los estados, mostrando la sincronía en la pantalla de un osciloscopio.

5.8 – Conclusiones

En este capítulo se llevó a cabo la sincronización de dos circuitos de Chua de cuarto orden los cuales exhiben comportamiento hipercaótico. La sincronización se llevo a cabo por la metodología hamiltoniana y diseño de un observador, de esta manera se obtuvieron las ganancias del observador las cuales garantizan la sincronización y por último se mostraron los resultados obtenidos tanto numéricos como experimentales.

Capítulo 6

Sincronización entre múltiples maestros y esclavos

6.1 – Introducción

En los capítulos anteriores la sincronización tanto numérica como experimental sólo se ha realizado entre dos sistemas hipercaóticos. En cambio, este capítulo se presentan resultados numéricos de la sincronización de *N* maestros con *N* esclavos a través de un canal, utilizando el esquema de sincronización por retroalimentación propuesta en [Milanovic y Zaghloul, 1996] combinado con de sincronización de osciladores caóticos por formas hamiltonianas generalizado y el diseño de un observador propuesto en [Sira-Ramírez y Cruz-Hernández, 2000; 2001]. Esta metodología se aplicó exitosamente en [Mejía-Camacho 2007] donde fueron sincronizados *N* circuitos de Chua.

6.2 – Sincronización de múltiples maestros y esclavos

La sincronización de *N* maestros con *N* esclavos a través de un canal se efectúa mediante un acoplamiento unidireccional, también conocido como acoplamiento maestro y esclavo.

En la figura 36 se muestra el diagrama a bloques del conjunto de N sistemas maestros, el cual cuenta con una señal $s(t)$, resultante de la suma de $y_i(t)$, señales de salida de los M_i maestros, donde $i = 1,2,\dots,N$ circuitos de Chua de cuarto orden. Esto se indica como sigue

$$s(t) = y_1(t) + y_2(t) + \cdots + y_N(t). \tag{31}$$

Esta señal resultante (31) será la señal de acoplamiento que se envía hacia el conjunto de ***N*** esclavos ubicado remotamente, conectados mediante un canal público. Al mismo tiempo, se retroalimenta al conjunto de sistemas maestros, mediante el circuito de $\text{Chua}_{0\text{T}}$. 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 37) cuenta con $n_i(t)$ señales de salida E_i esclavos, donde $i = 1,2,\dots,N$. las señales de salida $y_i(t)$ del conjunto de maestros se utilizarán para ocultar 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 utilizarán para recuperar la información de u_i usuarios en el receptor de la red de dichos sistemas esclavos.

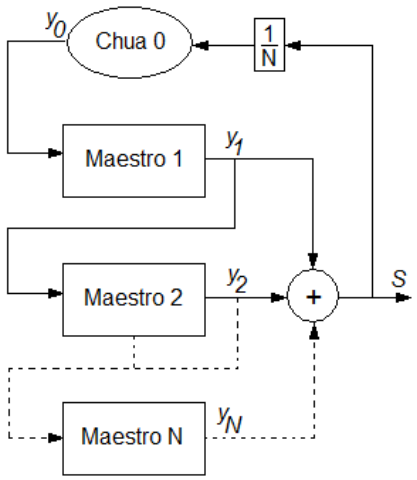


Figura 36. Diagrama a bloques del conjunto de *N* maestros para la sincronización entre múltiples maestros y esclavos, utilizando *N + 1* circuitos de Chua de cuarto orden, uno para $Chua_{0T}$, utilizado para la retroalimentación de la señal *s* y *N* para los *N* usuarios en el transmisor de la red.

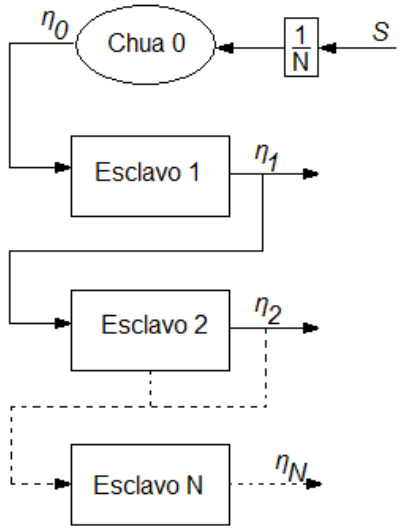


Figura 37. Diagrama a bloques del conjunto de *N* esclavos para la sincronización entre múltiples maestros y esclavos, utilizando *N + 1* circuitos de Chua de cuarto orden, uno para $Chua_{0R}$, utilizado para primero ingresar a la señal *s* y *N* para los *N* usuarios en el receptor de la red.

6.2.1 - Conjunto de N sistemas maestros

El conjunto de ecuaciones de estado para el generador de hipercaos del sistema maestro en forma hamiltoniana generalizada, está dada por:

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

$$\dot{x_0} = \mathcal{J}\left(\frac{s}{N}\right)\frac{\partial H}{\partial x} + (I+S)\frac{\partial H}{\partial x} + f\left(\frac{s}{N}\right) + K_0\left(\frac{s}{N} - y_0\right), \qquad x_0 \in \Re^n,$$

$$y_0 = C\frac{\partial H}{\partial x}, \qquad y_0 \in \Re^m.$$

Maestro 1

$$\dot{x_1} = \mathcal{J}(y_0)\frac{\partial H}{\partial x} + (I+S)\frac{\partial H}{\partial x} + f(y_0) + K_1(y_0 - y_1), \qquad x_1 \in \Re^n,$$

$$y_1 = C\frac{\partial H}{\partial x}, \qquad y_1 \in \Re^m.$$

Maestro 2

$$\dot{x_2} = \mathcal{J}(y_1)\frac{\partial H}{\partial x} + (I+S)\frac{\partial H}{\partial x} + f(y_1) + K_2(y_1 - y_2), \qquad x_2 \in \Re^n,$$

$$y_2 = C\frac{\partial H}{\partial x}, \qquad y_2 \in \Re^m.$$

Maestro N

$$\dot{x_N} = \mathcal{J}(y_{N-1})\frac{\partial H}{\partial x} + (I+S)\frac{\partial H}{\partial x} + f(y_{N-1}) + K_N(y_{N-1} - y_N), \qquad x_N \in \Re^n,$$

$$y_N = C\frac{\partial H}{\partial x}, \qquad y_N \in \Re^m.$$

6.2.2 - Conjunto de N sistemas esclavos

El conjunto de N sistemas hipercaóticos 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 de acoplamiento. Esto se muestra en el siguiente conjunto de ecuaciones de estado en forma hamiltoniana generalizada:

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

$$\dot{\widehat{x_0}} = \mathcal{J}\left(\frac{s}{N}\right)\frac{\partial H}{\partial \hat{x}} + (I+S)\frac{\partial H}{\partial \hat{x}} + f\left(\frac{s}{N}\right) + K_0\left(\frac{s}{N} - \eta_0\right), \qquad \widehat{x_0} \in \Re^n,$$

$$\eta_0 = C\frac{\partial H}{\partial \hat{x}}, \qquad \eta_0 \in \Re^m.$$

Esclavo 1

$$\dot{\widehat{x_1}} = \mathcal{J}(\eta_0)\frac{\partial H}{\partial \hat{x}} + (I+S)\frac{\partial H}{\partial \hat{x}} + f(\eta_0) + K_1(\eta_0 - \eta_1), \qquad \widehat{x_1} \in \Re^n,$$

$$\eta_1 = C\frac{\partial H}{\partial \hat{x}}, \qquad \eta_1 \in \Re^m.$$

Esclavo 2

$$\dot{\widehat{x_2}} = \mathcal{J}(\eta_1)\frac{\partial H}{\partial \hat{x}} + (I+S)\frac{\partial H}{\partial \hat{x}} + f(\eta_1) + K_2(\eta_1 - \eta_2), \qquad \widehat{x_2} \in \Re^n,$$

$$\eta_2 = C\frac{\partial H}{\partial \hat{x}}, \qquad \eta_2 \in \Re^m.$$

Esclavo N

$$\dot{\widehat{x_N}} = \mathcal{J}(\eta_{N-1})\frac{\partial H}{\partial \hat{x}} + (I+S)\frac{\partial H}{\partial \hat{x}} + f(\eta_{N-1}) + K_N(\eta_{N-1} - \eta_N), \qquad \widehat{x_N} \in \Re^n,$$

$$\eta_N = C\frac{\partial H}{\partial \hat{x}}, \qquad \eta_N \in \Re^m.$$

6.3 - Resultados numéricos

Por simplicidad y con propósitos ilustrativos, se consideraron sólo dos maestros ($N = 2$) y dos esclavos formando la red de osciladores hipercaóticos por sincronizar. En los siguientes resultados numéricos, se utilizaron las ecuaciones normalizadas del circuito de Chua de cuarto orden, es decir, se utiliza al circuito de Chua de cuarto orden como generador de hipercaos, mientras que la sincronización de osciladores hipercaóticos mediante sistemas

hamiltonianos generalizados y el diseño de un observador no lineal. De acuerdo al capítulo 5 el valor de la ganancia K es como sigue:

$$K = (2.3, 1, 0.3, 0)^T$$

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

6.3.1 – Ecuaciones normalizadas del conjunto de 2 sistemas maestros

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

$$\begin{aligned}
\dot{x}_{1_0} &= \alpha_{1_0}(x_{3_0} - f(x_{1_0})) + k_1(s - x_{1_0}),\\
\dot{x}_{2_0} &= -\alpha_{2_0}x_{2_0} - x_{3_0} - x_{4_0} + k_2(s - x_{1_0}),\\
\dot{x}_{3_0} &= \beta_{1_0}(x_{2_0} - x_{1_0} - x_{3_0}) + k_3(s - x_{1_0}),\\
\dot{x}_{4_0} &= \beta_{2_0}x_{2_0} + k_4(s - x_{1_0}),\\
f(s) &= bs + \tfrac{1}{2}(a - b)(|s + 1| - |s - 1|).
\end{aligned} \tag{37}$$

Maestro 1

$$\begin{aligned}
\dot{x}_{1_1} &= \alpha_{1_1}(x_{3_1} - f(x_{1_1})) + k_1(x_{1_0} - x_{1_1}),\\
\dot{x}_{2_1} &= -\alpha_{2_1}x_{2_1} - x_{3_1} - x_{4_1} + k_2(x_{1_0} - x_{1_1}),\\
\dot{x}_{3_1} &= \beta_{1_1}(x_{2_1} - x_{1_1} - x_{3_1}) + k_3(x_{1_0} - x_{1_1}),\\
\dot{x}_{4_1} &= \beta_{2_1}x_{2_1} + k_4(x_{1_0} - x_{1_1}),\\
f(x_{1_0}) &= bx_{1_0} + \tfrac{1}{2}(a - b)(|x_{1_0} + 1| - |x_{1_0} - 1|).
\end{aligned} \tag{38}$$

Maestro 2

$$\begin{aligned}
\dot{x}_{1_2} &= \alpha_{1_2}(x_{3_2} - f(x_{1_2})) + k_1(x_{1_1} - x_{1_2}),\\
\dot{x}_{2_2} &= -\alpha_{2_2}x_{2_2} - x_{3_2} - x_{4_2} + k_2(x_{1_1} - x_{1_2}),\\
\dot{x}_{3_2} &= \beta_{1_2}(x_{2_2} - x_{1_2} - x_{3_2}) + k_3(x_{1_1} - x_{1_2}),\\
\dot{x}_{4_2} &= \beta_{2_2}x_{2_2} + k_4(x_{1_1} - x_{1_2}),\\
f(x_{1_1}) &= bx_{1_1} + \tfrac{1}{2}(a - b)(|x_{1_1} + 1| - |x_{1_1} - 1|).
\end{aligned} \tag{39}$$

Donde el valor de $a = -0.0299$ y $b = 1.995$ se asignan para todos los circuitos de Chua de cuarto orden del sistema maestro.

Las condiciones iniciales para los estados de **$\mathbf{Chua_{0T}}$**:

$$x_{1_0}(0) = 1.1,\ x_{2_0}(0) = 0.1,\ x_{3_0}(0) = -0.5\ \ y\ \ x_{4_0}(0) = 0.01.$$

y donde:

$$\propto_1 = 2.1429, \qquad \propto_2 = -0.1283, \qquad \beta_1 = 0.0393\ \ y\ \ \beta_2 = 0.0015.$$

Mientras que las condiciones iniciales del maestro 1 son:

$$x_{1_1}(0) = 1.0,\ x_{2_1}(0) = 0.15,\ x_{3_1}(0) = -0.3\quad y\quad x_{4_1}(0) = 0.009.$$

y donde:

$$\propto_1 = 3.1428;\ \propto_2 = -0.1282;\quad \beta_1 = 0.0395\quad y\quad \beta_2 = 0.0014.$$

Mientras que las condiciones iniciales del maestro 2 son:

$$x_{1_1}(0) = 0.9,\ x_{2_1}(0) = 0.09,\ x_{3_1}(0) = 0.0\ \ y\ \ x_{4_1}(0) = 0.05.$$

y donde:

$$\propto_1 = 1.1430;\ \propto_2 = -0.1284;\quad \beta_1 = 0.0391\quad y\quad \beta_2 = 0.0016.$$

En la figura 38, se muestra la evolución en el tiempo del comportamiento de los estados tanto del circuito Chua de cuarto orden $Chua_{0T}$ como los circuitos de Chua de cuarto orden maestro 1 y maestro 2 del sistema maestro.

Mientras que en la figura 39, se muestra los atractores hipercaóticos tanto del circuito de Chua de cuarto orden $Chua_{0T}$ como los circuitos de Chua de cuarto orden maestro 1 y maestro 2 del sistema maestro.

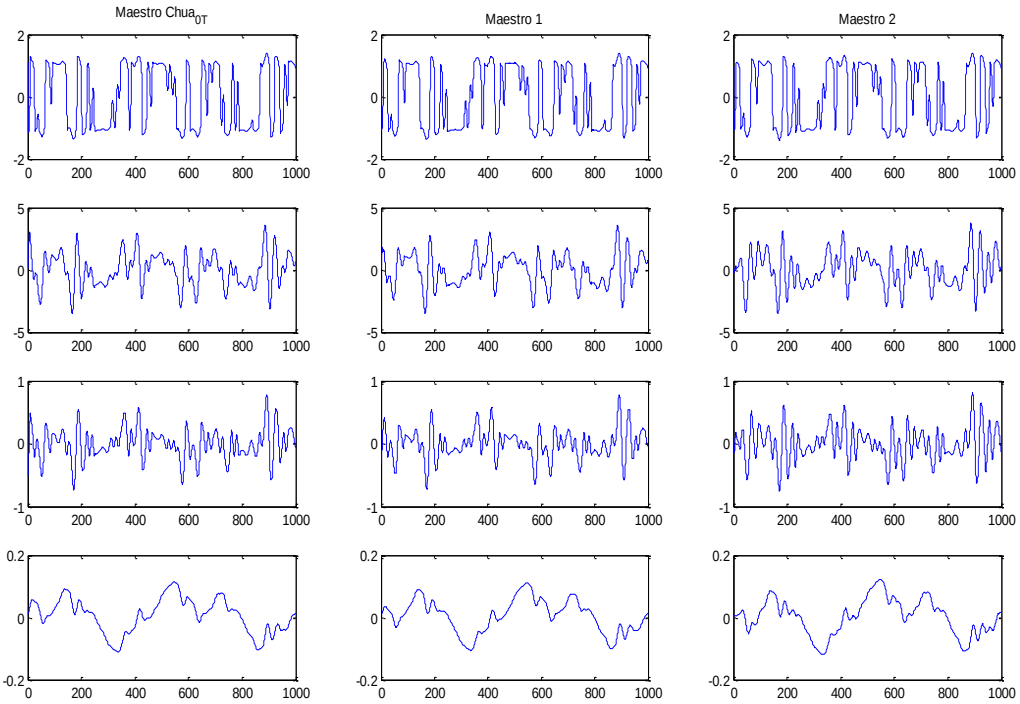


Figura 38. Evolución en el tiempo de los estados hipercaóticos $x_1(t),\ x_2(t),\ x_3(t)\ y\ x_4(t)$ en el tiempo, de los circuitos $Chua_{0T}$, maestro 1 y maestro 2.

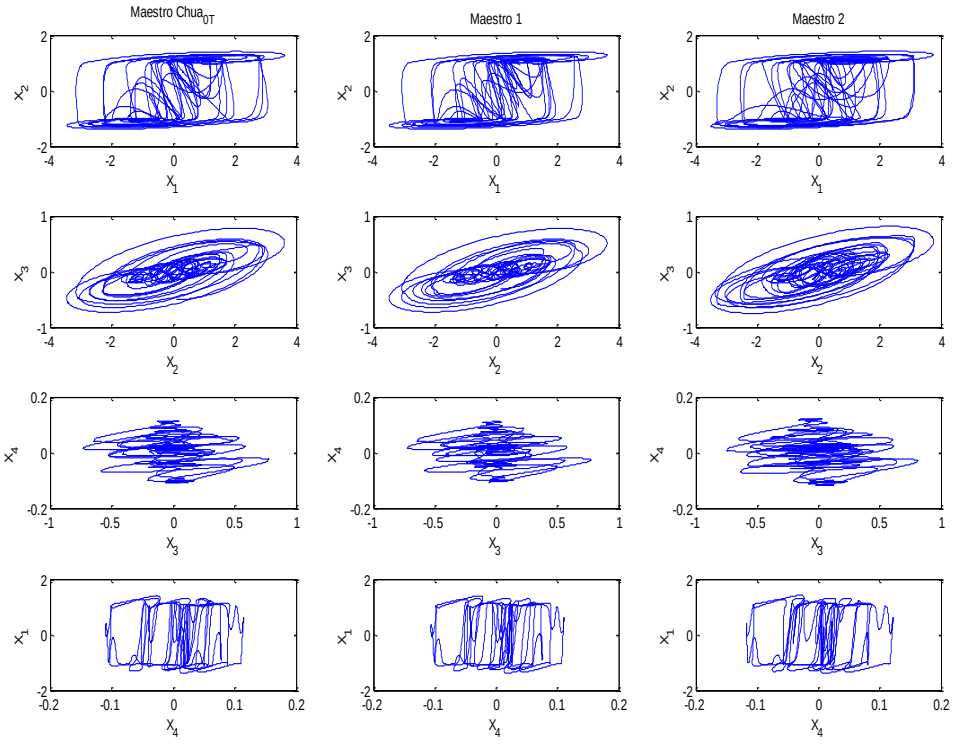


Figura 39. Atractores hipercaóticos de los circuitos $Chua_{0T}$, maestro 1 y maestro 2

6.3.2 – Ecuaciones normalizadas del conjunto de 2 sistemas esclavos

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

$$\begin{aligned}
\dot{\hat{x}}_{1_0} &= \alpha_{1_0}(x_{3_0} - f(x_{1_0})) + k_1(s - x_{1_0}),\\
\dot{\hat{x}}_{2_0} &= -\alpha_{2_0}x_{2_0} - x_{3_0} - x_{4_0} + k_2(s - x_{1_0}),\\
\dot{\hat{x}}_{3_0} &= \beta_{1_0}(x_{2_0} - x_{1_0} - x_{3_0}) + k_3(s - x_{1_0}),\\
\dot{\hat{x}}_{4_0} &= \beta_{2_0}x_{2_0} + k_4(s - x_{1_0}),\\
f(s) &= bs + \tfrac{1}{2}(a - b)(|s + 1| - |s - 1|).
\end{aligned} \tag{35}$$

Esclavo 1

$$\begin{aligned}
\dot{\hat{x}}_{1_1} &= \alpha_{1_1}(x_{3_1} - f(x_{1_1})) + k_1(x_{1_0} - x_{1_1}),\\
\dot{\hat{x}}_{2_1} &= -\alpha_{2_1}x_{2_1} - x_{3_1} - x_{4_1} + k_2(x_{1_0} - x_{1_1}),\\
\dot{\hat{x}}_{3_1} &= \beta_{1_1}(x_{2_1} - x_{1_1} - x_{3_1}) + k_3(x_{1_0} - x_{1_1}),\\
\dot{\hat{x}}_{4_1} &= \beta_{2_1}x_{2_1} + k_4(x_{1_0} - x_{1_1}),\\
f(x_{1_0}) &= bx_{1_0} + \tfrac{1}{2}(a - b)(|x_{1_0} + 1| - |x_{1_0} - 1|).
\end{aligned} \tag{36}$$

Esclavo 2

$$\begin{aligned}
\dot{\hat{x}}_{1_2} &= \alpha_{1_2}(x_{3_2} - f(x_{1_2})) + k_1(x_{1_1} - x_{1_2}),\\
\dot{\hat{x}}_{2_2} &= -\alpha_{2_2}x_{2_2} - x_{3_2} - x_{4_2} + k_2(x_{1_1} - x_{1_2}),\\
\dot{\hat{x}}_{3_2} &= \beta_{1_2}(x_{2_2} - x_{1_2} - x_{3_2}) + k_3(x_{1_1} - x_{1_2}),\\
\dot{\hat{x}}_{4_2} &= \beta_{2_2}x_{2_2} + k_4(x_{1_1} - x_{1_2}),\\
f(x_{1_1}) &= bx_{1_1} + \tfrac{1}{2}(a - b)(|x_{1_1} + 1| - |x_{1_1} - 1|).
\end{aligned} \tag{37}$$

Donde el valor de $a = -0.0299$ y $b = 1.995$ se asignan para tos los circuitos de Chua de cuarto orden del sistema esclavo.

Las condiciones iniciales para los estados de **Chua$_{0R}$** :

$$x_{1_0}(0) = 0.5,\ x_{2_0}(0) = 0.03,\ x_{3_0}(0) = -0.2\ \ y\ \ x_{4_0}(0) = 0.05.$$

y donde:

$$\propto_1 = 2.1429;\ \propto_2 = -0.1283;\ \ \beta_1 = 0.0393\ \ y\ \ \beta_2 = 0.0015.$$

Mientras que las condiciones iniciales del esclavo 1 son:

$$x_{1_1}(0) = 0.8,\ x_{2_1}(0) = 0.0,\ x_{3_1}(0) = -1.0\ \ y\ \ x_{4_1}(0) = 0.1.$$

y donde:

$$\propto_1 = 3.1428;\ \propto_2 = -0.1282;\ \beta_1 = 0.0395\ \ y\ \ \beta_2 = 0.0014.$$

Mientras que las condiciones iniciales del maestro 2 son:

$$x_{1_1}(0) = 0.0,\ x_{2_1}(0) = 0.0,\ x_{3_1}(0) = 0.0\ \ \ y\ \ x_{4_1}(0) = 0.0.$$

y donde:

$$\propto_1 = 1.1430;\ \propto_2 = -0.1284;\ \ \beta_1 = 0.0391\ \ \ y\ \ \beta_2 = 0.0016.$$

En la figura 40, se muestra la evolución en el tiempo del comportamiento de los estados tanto del circuito Chua de cuarto orden Chua_{0T} como los circuitos de Chua de cuarto orden esclavo 1 y esclavo 2 del sistema esclavo.

Mientras que en la figura 41, se muestra los atractores hipercaóticos tanto del circuito de Chua de cuarto orden Chua_{0T} como los circuitos de Chua de cuarto orden maestro 1 y maestro 2 del sistema maestro

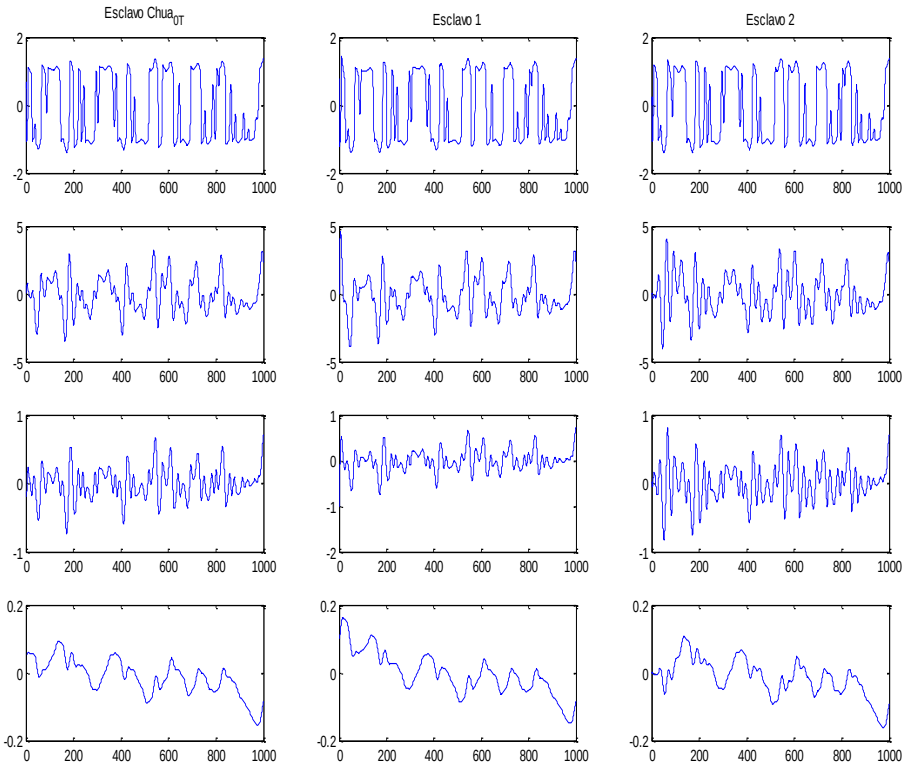


Figura 40. Evolución en el tiempo de los estados hipercaóticos $x_1(t),\ x_2(t),\ \ x_3(t)\ y\ x_4(t)$ en el tiempo de los circuitos Chua_{0R}, esclavo 1 y esclavo 2.

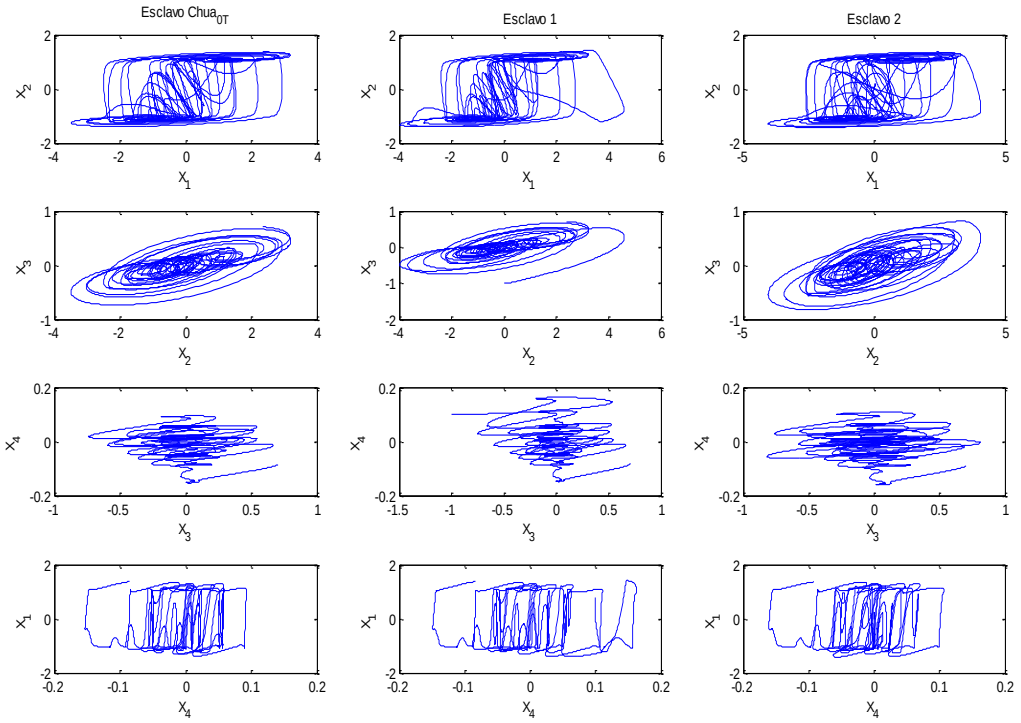


Figura 41. Atractores hipercaóticos de los circuitos $Chua_{0R}$, esclavo 1 y esclavo 2.

6.3.3 – Sincronización

En la figura 42, se muestra el plano de fase de sincronía en el espacio de estado entre los estados del circuito de Chua de cuarto orden maestro 1 y los estados del circuito de Chua de cuarto orden esclavo 1.

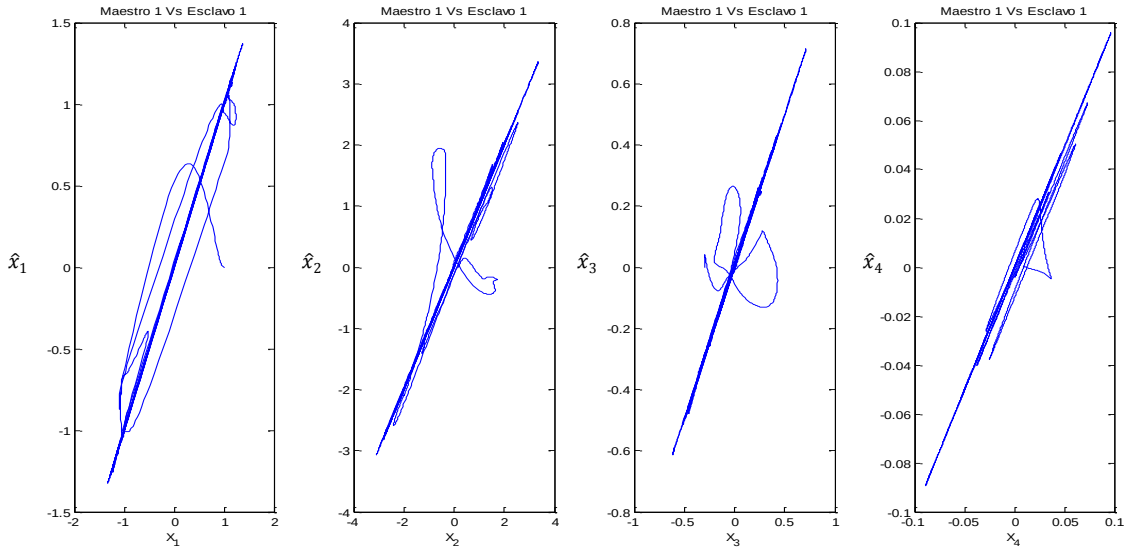


Figura 42. Plano de fase de la sincronía entre el circuito maestro 1 y el circuito esclavo 1.

En la figura 43 se ilustra el comportamiento en el tiempo de las trayectorias del error de sincronía entre el circuito de Chua de cuarto orden maestro 1 y el circuito de Chua de cuarto orden esclavo 1.

Mientras que en la figura 44, se muestra el plano de fase de sincronía en el espacio de estado entre los estados del circuito de Chua de cuarto orden maestro 2 y los estados del circuito de Chua de cuarto orden esclavo 1.

En la figura 45 se ilustra el comportamiento en el tiempo de las trayectorias del error de sincronía entre el circuito de Chua de cuarto orden maestro 2 y el circuito de Chua de cuarto orden esclavo 2, donde se puede apreciar que el error de sincronía es muy pequeño hasta que llega a cero.

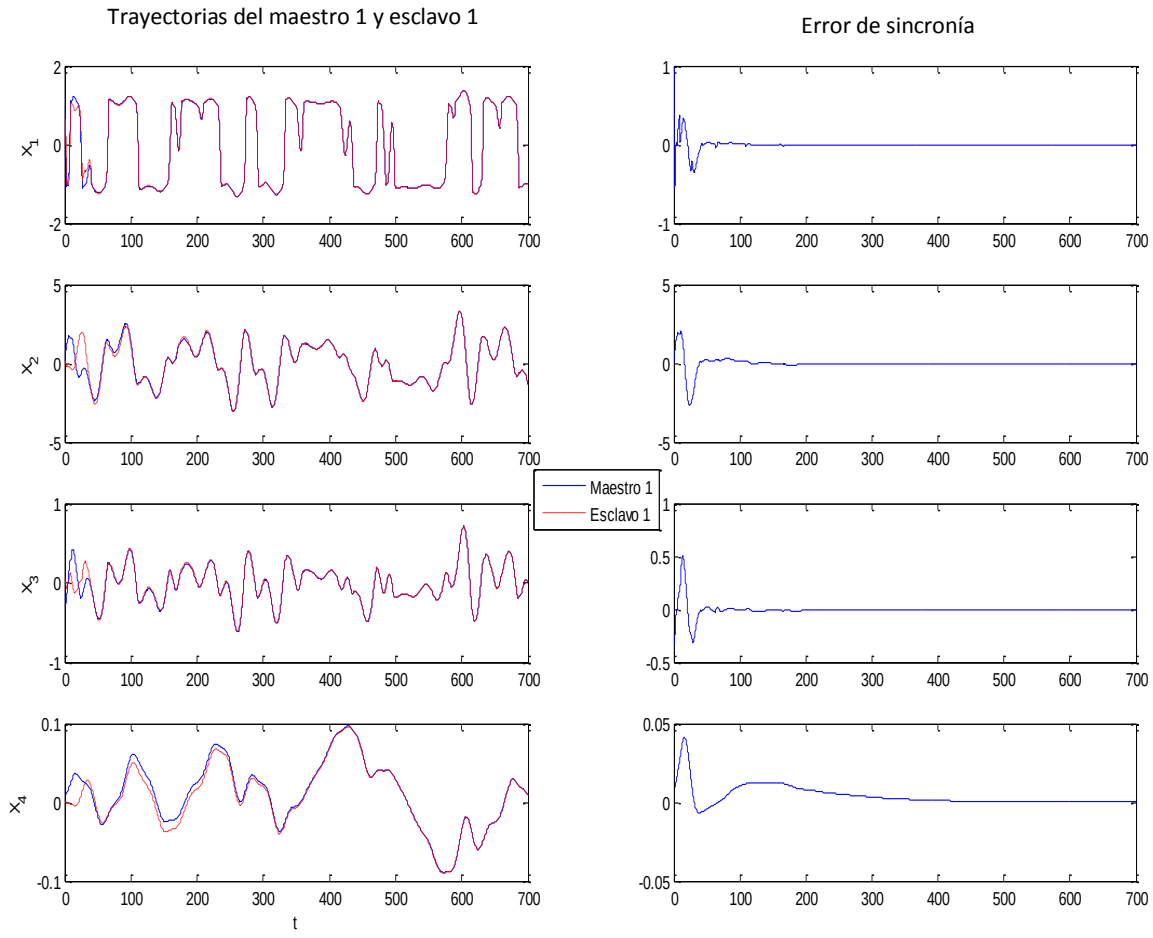


Figura 43. Trayectoria de los estados $x_i(t)$ y $\hat{x}_i(t)$ y el error de sincronía $e_i(t) = x_i(t) - \hat{x}_i(t)$ para el maestro 1 y esclavo 1, donde $i = 1,2,3,4$.

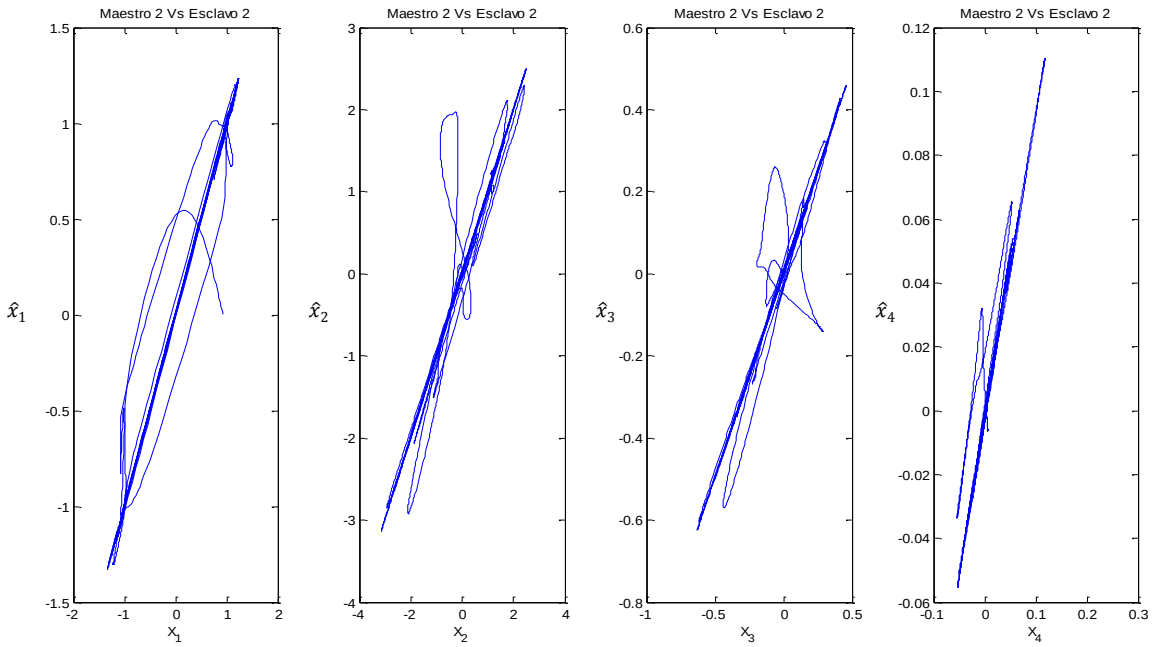


Figura 44. Plano de fase de la sincronía entre el circuito maestro 2 y el circuito esclavo 2.

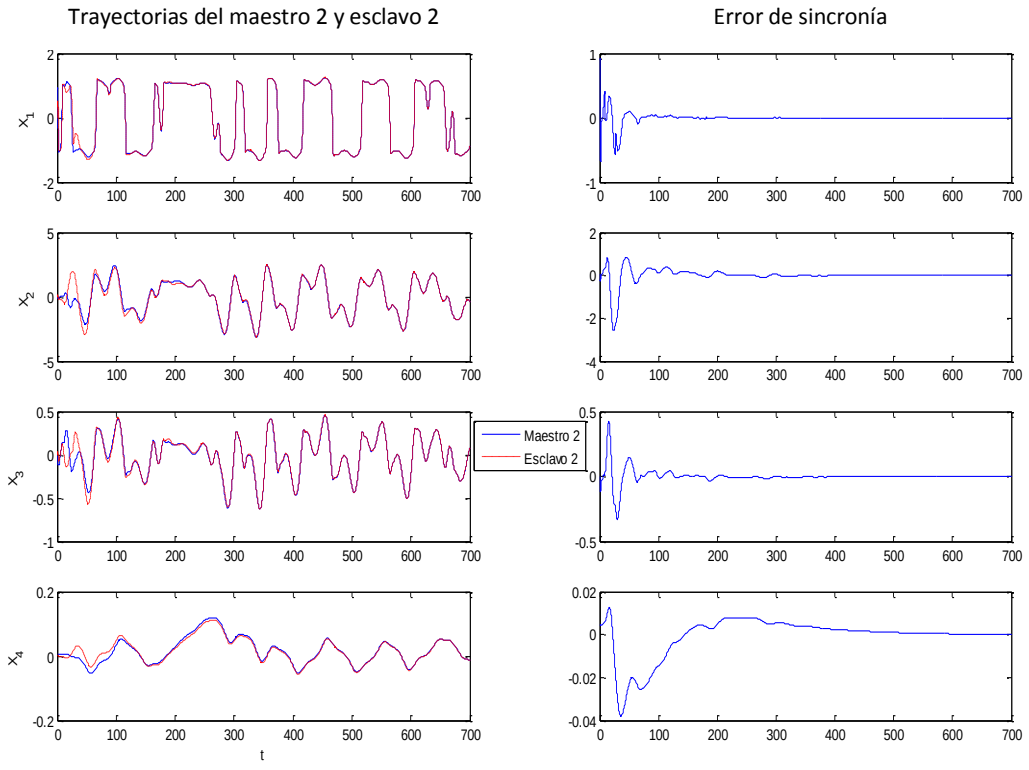


Figura 45. Trayectoria de los estados $x_i(t)$ y $\hat{x}_i(t)$ y el error de sincronía $e_i(t) = x_i(t) - \hat{x}_i(t)$ para el maestro 2 y esclavo 2, donde $i = 1,2,3,4$.

6.4- Conclusiones

En este capítulo se utilizó un esquema para la sincronización entre dos conjuntos de N maestros y N esclavos, a manera de ilustración se presentó una red con dos maestros y dos esclavos utilizando circuitos hipercaóticos de Chua de cuarto orden, previamente empleado para el circuito de Chua en trabajos anteriores. La sincronización se realizó por medio de retroalimentación combinándola con el método de sincronización de osciladores caóticos mediante sistemas hamiltonianos generalizados y el diseño de un observador no lineal, como se demostró, la sincronización entre dos maestros y dos esclavos se llevo a cabo con éxito por lo que se deduce que se podrían utilizar N maestros y N esclavos. Para poder emplearse para comunicaciones seguras en una red de multiusuarios.

Capítulo 7

Sincronización en configuración estrella

7.1 – Introducción

En este capítulo se muestra otro tipo de configuración para lograr la sincronización en una red, esta es la configuración estrella, donde a continuación se mostrarán sus características principales y la sincronización entre un maestro y cuatro nodos.

7.2 - Configuración estrella

La sincronización de los nodos de una red en configuración estrella puede ser aplicada para transmitir mensajes encriptados, desde un simple transmisor a múltiples receptores en una red de sistemas de comunicación. El objetivo de este capítulo es sincronizar cuatro circuitos de Chua modificados de cuarto orden (los cuales exhiben comportamientos hipercaóticos) en configuración estrella por medio de formas hamiltonianas y diseño de un observador

7.3 - Sincronización en configuración estrella

Considere el siguiente conjunto de N sistemas dinámicos idénticos interconectados

$$x_i = f(x_i) + u_i, \qquad i = 1, 2, \ldots, N, \tag{38}$$

donde $x_i = (x_{i1}, x_{i2}, \ldots, x_{in})^T \in \Re^n$ es el vector de estado $u_i = u_{i1} \in R$ es la señal de entrada del sistema i. Teniendo en cuenta que, si $u_{i1} = 0, i = 1, 2, \ldots, N$, se tiene un conjunto de N sistemas aislados, que operan con su propia dinámica. Mientras si $u_{i1} \neq 0$ el conjunto constituye una red dinámica y cada sistema dinámico i es llamado nodo i. Y con una apropiada u_{i1} la red dinámica puede lograr comportamientos colectivos. Es evidente que, la señal de entrada u_{i1} determina el tipo de acoplamiento entre los nodos de la red. Las configuraciones de acoplamiento más comúnmente estudiadas de sincronización de redes de dinámicas complejas son llamadas, redes globalmente acopladas, redes con acoplamiento estrella. La matriz de acoplamiento en configuración estrella está dada por

$$A = \begin{pmatrix} N-1 & -1 & -1 & \cdots & -1 \\ -1 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ -1 & 0 & 0 & \cdots & 0 \\ -1 & 0 & 0 & \cdots & 0 \end{pmatrix} \tag{39}$$

La configuración en acoplamiento estrella para N nodos es mostrado en la figura 46, con un nodo común o central.

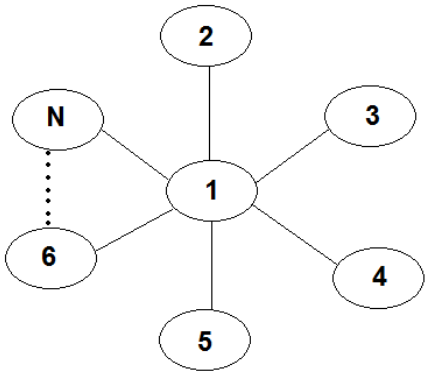


Figura 46. Acoplamiento en configuración estrella con *N* nodos.

La dinámica de la red compleja (38) se dice que logra la sincronización (asintótica) [Wang 2002] si:

$$x_1(t) = x_2(t) = \cdots = x_N(t) \quad cuando\ t \to \infty. \tag{40}$$

El estado de sincronización en (38) puede ser un punto de equilibrio, una órbita periódica o un atractor caótico. En este caso se utilizó un nodo maestro con el objetivo de imponer sus dinámicas de manera colectiva. El objetivo de este capítulo es la sincronización de una red con un maestro y N nodos, los cuales están dados por el circuito modificado de Chua de cuarto orden. Esta topología de acoplamiento particularmente es importante para la aplicación a sistemas de comunicaciones en red, para transmitir información de un solo transmisor a múltiples receptores [Chow *et al.* 2001].

A continuación se presentan las ecuaciones de estado expresadas en forma hamiltoniana pertenecientes al maestro y los N esclavos.

7.3.1 - Circuito de Chua de cuarto orden maestro

El sistema de ecuaciones de estado para el generador de hipercaos del sistema maestro en forma hamiltoniana generalizada, está dada por:

Circuito de Chua de cuarto orden maestro

$$\dot{x_0} = \mathcal{J}\left(\frac{S}{N}\right)\frac{\partial H}{\partial x} + (I+S)\frac{\partial H}{\partial x} + f\left(\frac{S}{N}\right) + k\left(\frac{S}{N} - y_0\right), \qquad x_0 \in \Re^n,$$

$$y_0 = C\frac{\partial H}{\partial x}, \qquad y_0 \in \Re^m.$$

7.3.2 - Conjunto de N sistemas esclavos

El conjunto de N sistemas hipercaóticos esclavos tiene la misma forma que el sistema maestro y es dirigido por la señal de entrada $x_{1_0}(t)$ proveniente de dicho sistema maestro a través del canal público inseguro. Esto se muestra en el siguiente conjunto de ecuaciones de estado en forma hamiltoniana generalizada:

Esclavo 1

$$\dot{\widehat{x_1}} = \mathcal{J}(\eta_1)\frac{\partial H}{\partial \hat{x}} + (I+S)\frac{\partial H}{\partial \hat{x}} + f(\eta_1) + k_1\left(\eta_1 - x_{1_0}\right), \qquad \widehat{x_1} \in \Re^n,$$

$$\eta_1 = C\,\frac{\partial H}{\partial \hat{x}}, \qquad \eta_1 \in \Re^m.$$

Esclavo 2

$$\dot{\widehat{x_2}} = \mathcal{J}(\eta_1)\frac{\partial H}{\partial \hat{x}} + (I+S)\frac{\partial H}{\partial \hat{x}} + f(\eta_1) + k_2(\eta_1 - \eta_2), \qquad \widehat{x_2} \in \Re^n,$$

$$\eta_2 = C\,\frac{\partial H}{\partial \hat{x}}, \qquad \eta_2 \in \Re^m.$$

Esclavo N

$$\dot{\widehat{x_N}} = \mathcal{J}(\eta_{N-1})\frac{\partial H}{\partial \hat{x}} + (I+S)\frac{\partial H}{\partial \hat{x}} + f(\eta_{N-1}) + k_N(\eta_{N-1} - \eta_N), \qquad \widehat{x_N} \in \Re^n,$$

$$\eta_N = C\,\frac{\partial H}{\partial \hat{x}}, \qquad \eta_N \in \Re^m.$$

7.4 - Resultados numéricos

Por simplicidad y con propósitos ilustrativos, se consideraron solo un maestro y cuatro esclavos formando la red de osciladores hipercaóticos por sincronizar. En los siguientes resultados numéricos se utilizaron las ecuaciones normalizadas del circuito de Chua de cuarto orden, es decir se utiliza al circuito de Chua de cuarto orden como generador de hipercaos, mientras que la sincronización de osciladores hipercaóticos mediante sistemas hamiltonianos generalizados y el diseño de un observador no lineal. De acuerdo al capítulo 5 el valor de la ganancia K es como sigue:

$$K = (2.3, 1, 0.3, 0)^T.$$

A continuación, se presentan las ecuaciones normalizadas tanto del maestro como de 4 sistemas esclavos que se utilizarán en las simulaciones.

7.4.1 – Ecuaciones normalizadas del maestro y esclavos

Circuito de Chua de cuarto orden maestro

$$\begin{aligned} \dot{x}_{1_0} &= \alpha_{1_0}(x_{3_0} - f(x_{1_0})), \\ \dot{x}_{2_0} &= -\alpha_{2_0} x_{2_0} - x_{3_0} - x_{4_0}, \\ \dot{x}_{3_0} &= \beta_{1_0}(x_{2_0} - x_{1_0} - x_{3_0}), \\ \dot{x}_{4_0} &= \beta_{2_0} x_{2_0}, \\ f(x_{1_0}) &= bs + \tfrac{1}{2}(a - b)(|x_{1_0} + 1| - |x_{1_0} - 1|), \end{aligned} \tag{41}$$

donde el valor de $a = -0.0299$ y $b = 1.995$ es asignado para tos los circuitos de Chua de cuarto orden del sistema maestro.

Las condiciones iniciales para los estados de **Chua$_{0T}$**:

$$x_{1_0}(0) = 1.1,\ x_{2_0}(0) = 0.1,\ x_{3_0}(0) = -0.5 \ \ y \ x_{4_0}(0) = 0.01,$$

y donde:

$$\propto_1 = 2.1429;\ \propto_2 = -0.1283;\ \ \beta_1 = 0.0393 \ \ y \ \ \beta_2 = 0.0015.$$

Circuitos esclavos de Chua de cuarto orden

Esclavo 1

$$\begin{aligned}
\dot{\hat{x}}_{1_1} &= \alpha_{1_1}(x_{3_1} - f(x_{1_1})) + k_1\left(x_{1_1} - x_{1_0}\right),\\
\dot{\hat{x}}_{2_1} &= -\alpha_{2_1}x_{2_1} - x_{3_1} - x_{4_1} + k_2\left(x_{1_1} - x_{1_0}\right),\\
\dot{\hat{x}}_{3_1} &= \beta_{1_1}(x_{2_1} - x_{1_1} - x_{3_1}) + k_3\left(x_{1_1} - x_{1_0}\right),\\
\dot{\hat{x}}_{4_1} &= \beta_{2_1}x_{2_1} + k_4\left(x_{1_1} - x_{1_0}\right),\\
f(x_{1_1}) &= bx_{1_1} + \tfrac{1}{2}(a - b)(\left|x_{1_1} + 1\right| - \left|x_{1_1} - 1\right|).
\end{aligned} \tag{42}$$

Mientras que las condiciones iniciales del esclavo 1 son:

$$x_{1_1}(0) = 0.5,\ x_{2_1}(0) = 0.3,\ x_{3_1}(0) = -0.4\ \ y\ \ x_{4_1}(0) = 0.0,$$

y donde:

$$\propto_1 = 3.1428;\ \propto_2 = -0.1282;\ \ \beta_1 = 0.0395\ \ y\ \ \beta_2 = 0.0014.$$

Esclavo 2

$$\begin{aligned}
\dot{\hat{x}}_{1_2} &= \alpha_{1_2}(x_{3_2} - f(x_{1_2})) + k_1\left(x_{1_2} - x_{1_0}\right),\\
\dot{\hat{x}}_{2_2} &= -\alpha_{2_2}x_{2_2} - x_{3_2} - x_{4_2} + k_2\left(x_{1_2} - x_{1_0}\right),\\
\dot{\hat{x}}_{3_2} &= \beta_{1_2}(x_{2_2} - x_{1_2} - x_{3_2}) + k_3\left(x_{1_2} - x_{1_0}\right),\\
\dot{\hat{x}}_{4_2} &= \beta_{2_2}x_{2_2} + k_4\left(x_{1_2} - x_{1_0}\right),\\
f(x_{1_2}) &= bx_{1_2} + \tfrac{1}{2}(a - b)(\left|x_{1_2} + 1\right| - \left|x_{1_2} - 1\right|).
\end{aligned} \tag{43}$$

Mientras que las condiciones iniciales del esclavo 2 son:

$$x_{1_1}(0) = 1.0,\ x_{2_1}(0) = 0.0,\ x_{3_1}(0) = -0.2\ \ \ y\ x_{4_1}(0) = 0.04,$$

y donde:

$$\propto_1 = 1.1430;\ \propto_2 = -0.1284;\ \ \beta_1 = 0.0391\ \ y\ \ \beta_2 = 0.0016.$$

Esclavo 3

$$\begin{aligned}
\dot{\hat{x}}_{1_2} &= \alpha_{1_2}(x_{3_2} - f(x_{1_2})) + k_1(x_{1_3} - x_{1_0}),\\
\dot{\hat{x}}_{2_2} &= -\alpha_{2_2}x_{2_2} - x_{3_2} - x_{4_2} + k_2(x_{1_3} - x_{1_0}),\\
\dot{\hat{x}}_{3_2} &= \beta_{1_2}(x_{2_2} - x_{1_2} - x_{3_2}) + k_3(x_{1_3} - x_{1_0}),\\
\dot{\hat{x}}_{4_2} &= \beta_{2_2}x_{2_2} + k_4(x_{1_3} - x_{1_0}),\\
f(x_{1_3}) &= bx_{1_3} + \tfrac{1}{2}(a - b)(|x_{1_3} + 1| - |x_{1_3} - 1|).
\end{aligned} \tag{44}$$

Mientras que las condiciones iniciales del esclavo 3 son:

$$x_{1_1}(0) = 0.9,\ x_{2_1}(0) = 0.4,\ x_{3_1}(0) = -1.0 \quad y \quad x_{4_1}(0) = 0.02,$$

y donde:

$$\propto_1 = 1.1430;\ \propto_2 = -0.1284;\ \beta_1 = 0.0391 \quad y \quad \beta_2 = 0.0016.$$

Esclavo 4

$$\begin{aligned}
\dot{\hat{x}}_{1_2} &= \alpha_{1_2}(x_{3_2} - f(x_{1_2})) + k_1(x_{1_4} - x_{1_0}),\\
\dot{\hat{x}}_{2_2} &= -\alpha_{2_2}x_{2_2} - x_{3_2} - x_{4_2} + k_2(x_{1_4} - x_{1_0}),\\
\dot{\hat{x}}_{3_2} &= \beta_{1_2}(x_{2_2} - x_{1_2} - x_{3_2}) + k_3(x_{1_4} - x_{1_0}),\\
\dot{\hat{x}}_{4_2} &= \beta_{2_2}x_{2_2} + k_4(x_{1_4} - x_{1_0}),\\
f(x_{1_4}) &= bx_{1_4} + \tfrac{1}{2}(a - b)(|x_{1_4} + 1| - |x_{1_4} - 1|).
\end{aligned} \tag{45}$$

Mientras que las condiciones iniciales del esclavo 4 son:

$$x_{1_1}(0) = 0.3,\ x_{2_1}(0) = 0.2, \qquad x_{3_1}(0) = 0.0 \quad y \quad x_{4_1}(0) = 0.06,$$

y donde:

$$\propto_1 = 1.1430;\ \propto_2 = -0.1284;\ \beta_1 = 0.0391 \quad y \quad \beta_2 = 0.0016.$$

En la figura 47, se muestra la evolución en el tiempo del comportamiento de los estados tanto del circuito Chua de cuarto orden Chua_{0T} maestro como de los circuitos de Chua de cuarto orden esclavo 1, esclavo 2, esclavo 3 y esclavo 4.

Mientras que en la figura 48, se muestra los atractores hipercaóticos tanto del circuito de Chua de cuarto orden $Chua_{0T}$ maestro como los circuitos de Chua de cuarto orden esclavo 1, esclavo 2, esclavo 3 y esclavo 4.

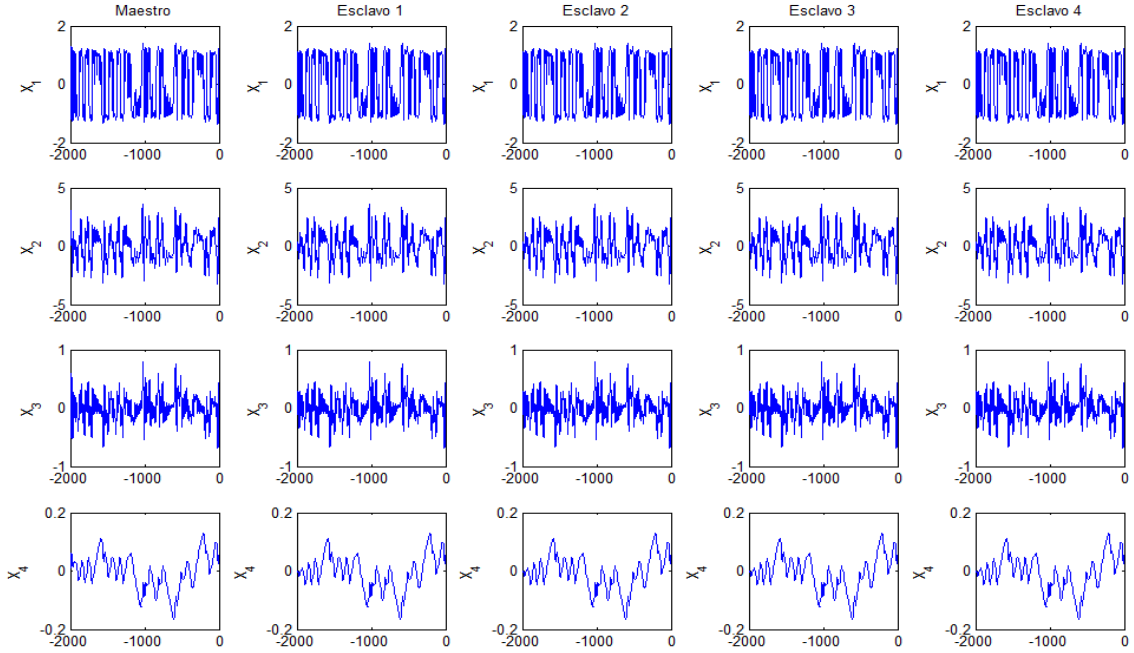


Figura 47. Evolución en el tiempo de los estados hipercaóticos $x_1(t)$, $x_2(t)$, $x_3(t)$, $x_4(t)$ de los circuitos $Chua_{0T}$, esclavo 1, esclavo 2, esclavo 3 y esclavo 4.

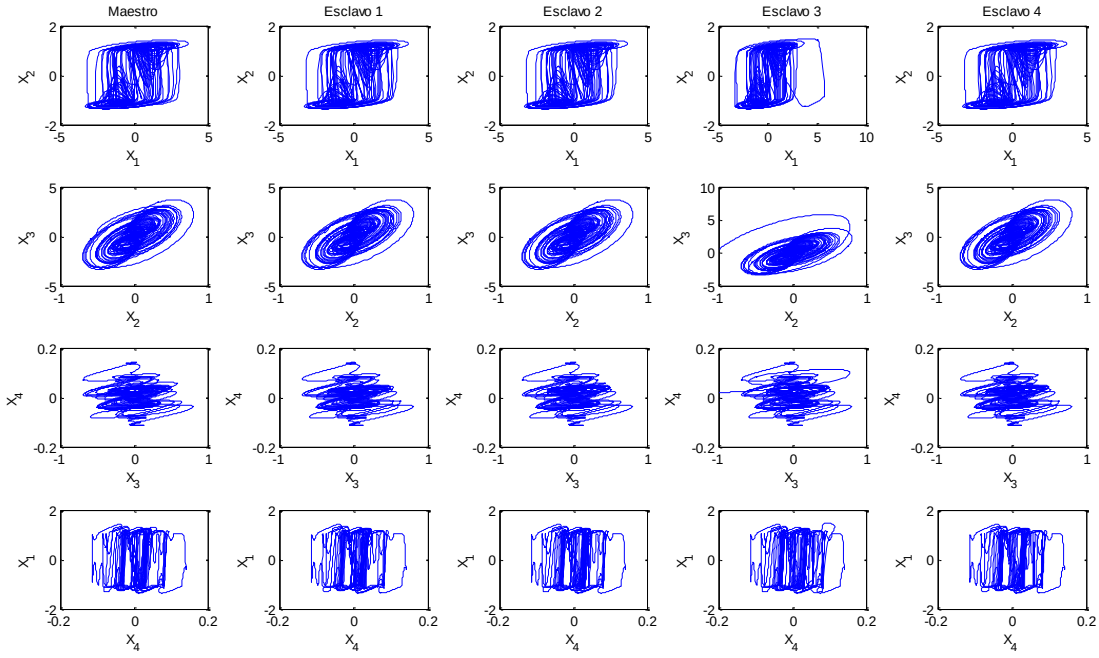


Figura 48. Atractores hipercaóticos de los circuitos $Chua_{0T}$, esclavo 1, esclavo 2, esclavo 3 y esclavo 4.

7.4.2 – Sincronización en la red

En la figura 49, se muestra el plano de fase de sincronía en el espacio de estado entre los estados del circuito maestro de Chua de cuarto orden y los estados de los circuitos esclavos de Chua de cuarto orden.

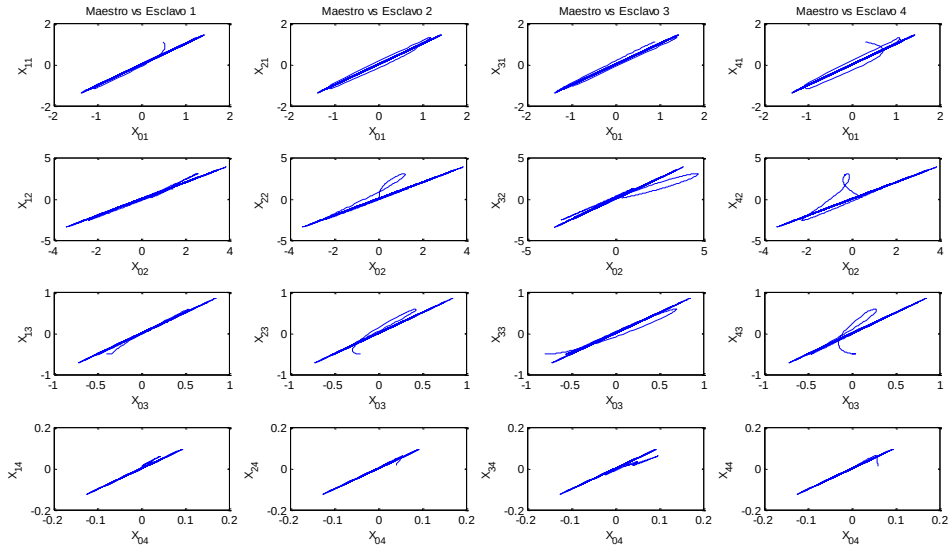


Figura 49. Plano de fase de la sincronía entre el circuito maestro y los circuitos esclavos.

En la figura 50 se ilustra el comportamiento en el tiempo de las trayectorias del error de sincronía entre el circuito maestro de Chua de cuarto orden y el circuito de Chua de cuarto orden (esclavo 1).

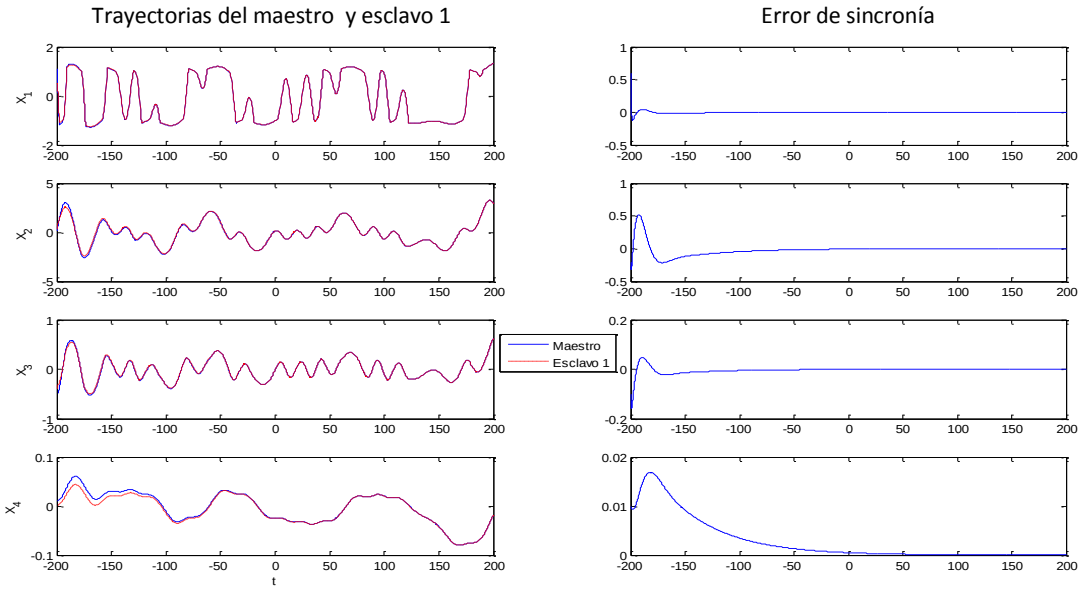


Figura 50. Trayectoria de los estados $x_i(t)$ y $\hat{x}_i(t)$ y el error de sincronía $e_i(t) = x_i(t) - \hat{x}_i(t)$ para el maestro y esclavo 1, donde $i = 1,2,3,4$.

En la figura 51 se ilustra el comportamiento en el tiempo de las trayectorias del error de sincronía entre el circuito maestro de Chua de cuarto orden y el circuito de Chua de cuarto orden (esclavo 2).

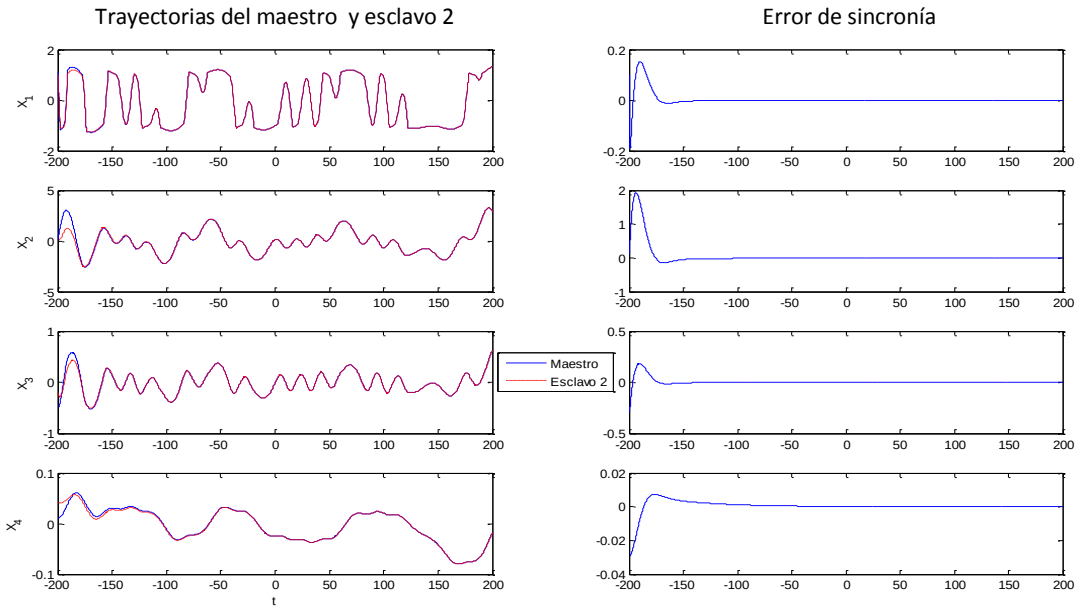


Figura 51. Trayectoria de los estados $x_i(t)$ y $\hat{x}_i(t)$ y el error de sincronía $e_i(t) = x_i(t) - \hat{x}_i(t)$ para el maestro y esclavo 2, donde $i = 1,2,3,4$.

En la figura 52 se ilustra el comportamiento en el tiempo de las trayectorias del error de sincronía entre el circuito maestro de Chua de cuarto orden y el circuito de Chua de cuarto orden (esclavo 3).

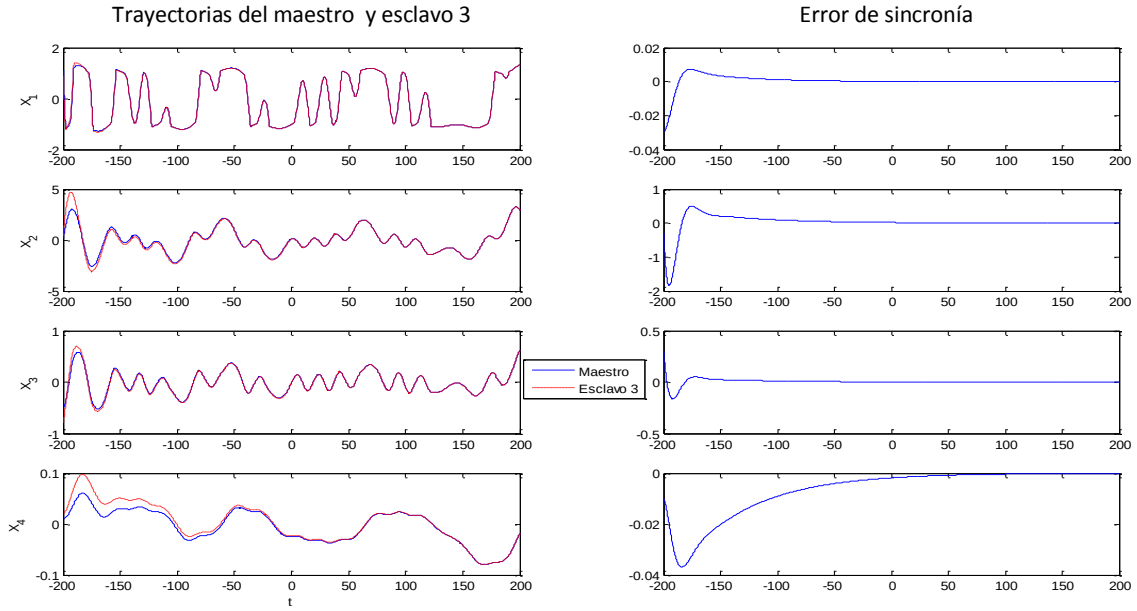


Figura 52. Trayectoria de los estados $x_i(t)$ y $\hat{x}_i(t)$ y el error de sincronía $e_i(t) = x_i(t) - \hat{x}_i(t)$ para el maestro y esclavo 3, donde $i = 1,2,3,4$.

En la figura 53 se ilustra el comportamiento en el tiempo de las trayectorias del error de sincronía entre el circuito maestro de Chua de cuarto orden y el circuito de Chua de cuarto orden (esclavo 4).

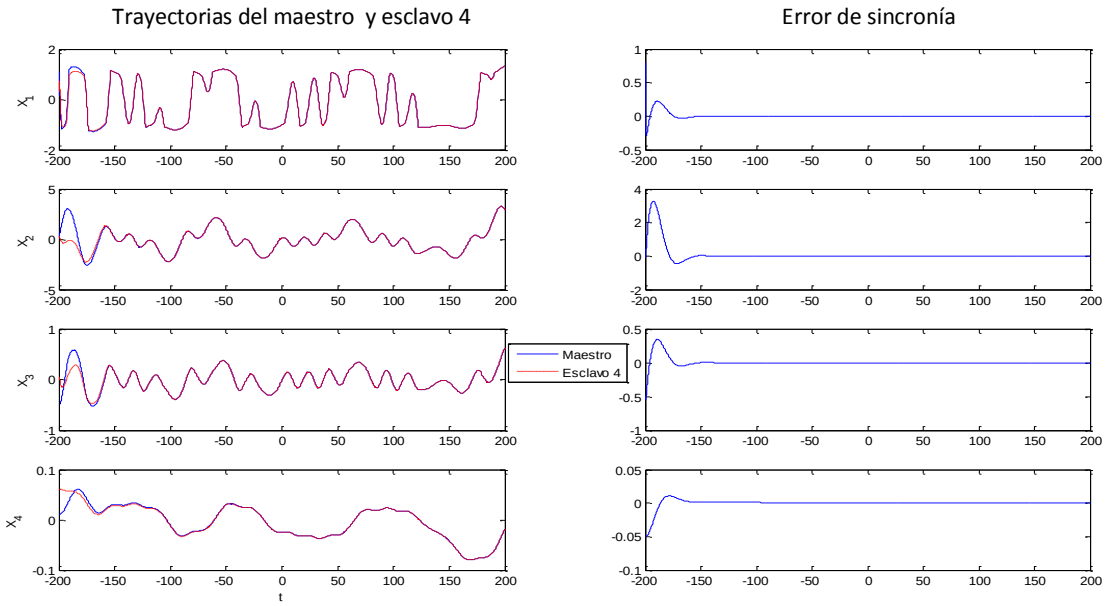


Figura 53. Trayectoria de los estados $x_i(t)$ y $\hat{x}_i(t)$ y el error de sincronía $e_i(t) = x_i(t) - \hat{x}_i(t)$ para el maestro y esclavo 4, donde $i = 1,2,3,4$.

7.5 - Conclusiones

En este capítulo se utilizó un esquema para la sincronización entre un maestro y N esclavos, a manera de ilustración se presento una red con un maestro y cuatro esclavos. La sincronización se realizo por medio de la configuración estrella combinándola con el método de sincronización de osciladores caóticos mediante sistemas hamiltonianos generalizados y el diseño de un observador no lineal, como se demostró, la sincronización entre un maestro y cuatro esclavos se llevo a cabo con éxito por lo que se deduce que se podrían utilizar un maestro y N esclavos, garantizando la sincronía.

Capítulo 8

Aplicación a las comunicaciones seguras

8.1 – Introducción

En este capítulo se presentan resultados numéricos y experimentales de la comunicación secreta entre un transmisor y un receptor acoplados de forma unidireccional por un canal público inseguro con el método de sincronización de osciladores caóticos mediante sistemas hamiltonianos generalizados y el diseño de un observador no lineal propuesto en [Sira-Ramírez y Cruz-Hernández 2000; 2001]. Además se realizó la simulación numérica de una red de usuarios por medio de configuración estrella, en la cual la comunicación secreta de información se lleva a cabo a partir de un sólo canal público inseguro, el acoplamiento unidireccional en dicha red, se realiza mediante el esquema de sincronización en configuración estrella propuesto en [Chow *et al.* 2001] en combinación con el método de sincronización de osciladores caóticos mediante sistemas hamiltonianos generalizados y el diseño de un observador no lineal propuesto en [Sira-Ramírez y Cruz-Hernández 2000; 2001].

8.2 - Comunicación hipercaótica entre un transmisor y un receptor

La transmisión de información analógica privada entre un circuito transmisor y un circuito receptor se llevo a cabo mediante la técnica de codificación caótica aditiva por un canal de transmisión, un esquema general se muestra en la figura 54, donde se puede observar que el mensaje a transmitir es sumado al estado $x_1(t)$ que también es usado para la sincronización de los dos sistemas, una vez sumado el mensaje y sincronizados los sistemas transmisor y receptor se hace la resta del estado $x_1(t)$ del transmisor menos el estado $\widehat{x_1}(t)$ del receptor obteniendo de esta forma el mensaje enviado en el maestro.

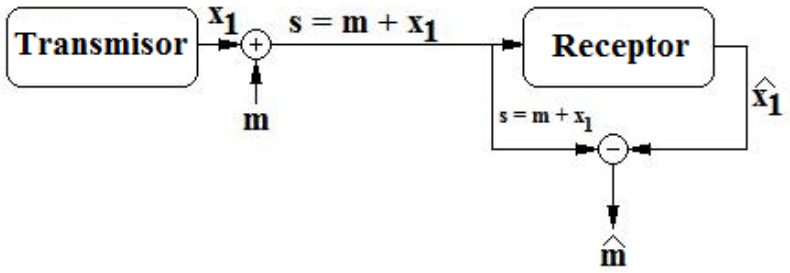


Figura 54. Esquema de la comunicación entre un transmisor y un receptor.

8.2.1 - Resultados numéricos

Se utiliza el circuito de Chua de cuarto orden transmisor (7) el cual exhibe un comportamiento hipercaótico con el cual el circuito de Chua de cuarto orden receptor (25)

sincroniza, con un escenario de acoplamiento unidireccional maestro-esclavo. Donde la señal de acoplamiento resulta ser $x_1(t)$ de acuerdo con los análisis hechos en capítulos anteriores.

Parámetros del sistema transmisor y receptor

$\alpha_1 = 2.1429$, $\alpha_2 = -0.1283$, $\beta_1 = 0.0393$, $\beta_2 = 0.0015$, $a = -0.0299$ y $b = 1.995$.

Condiciones iniciales del transmisor

$$x(0) = (1.1, 0.1, -0.5, 0.01).$$

Condiciones iniciales del receptor

$$x'(0) = (0,0,0,0).$$

Ganancias del esclavo para garantizar la sincronización

$$k_1 = 2.3, \quad k_2 = 1, \quad k_3 = 0.3 \quad y \quad k_4 = 0\,.$$

Mensaje a transmitir

En la figura 55 se observa el mensaje utilizado en la transmisión de información encriptada, este mensaje fue grabado por medio del micrófono de la computadora.

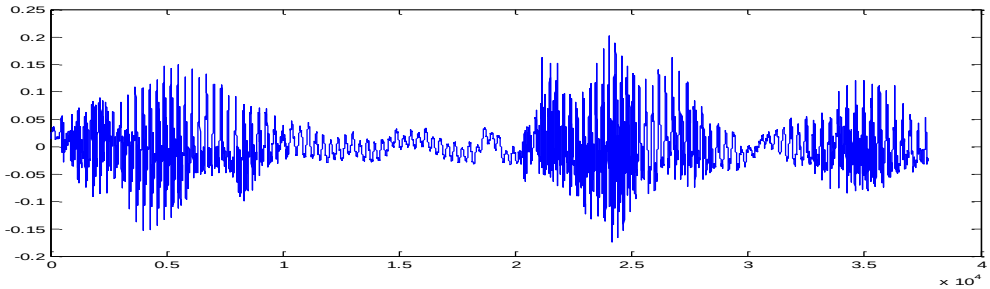


Figura 55. Mensaje a ser encriptado y transmitido por el maestro hacia el esclavo.

En la figura 56 (a) se muestra la evolución en el tiempo del estado $x_1(t)$ cuando aun no se adherido el mensaje a transmitir y la figura 56 (b) cuando ya se sumó la información al estado $x_1(t)$, donde se observa que las dos figuras (a) y (b) son prácticamente iguales, lo que provoca que se siga dando la sincronía entre el transmisor y receptor lográndose la transmisión de información de manera segura y efectiva.

En la figura 57 (a) se muestra el mensaje que se transmitió a través del estado $x_1(t)$ y la figura 57 (b) muestra el mensaje recuperado en el circuito esclavo, donde se observa que se recupera en su totalidad y al ser reproducido por medio de la computadora se aprecia que la calidad del mensaje recuperado es muy similar a la del mensaje transmitido.

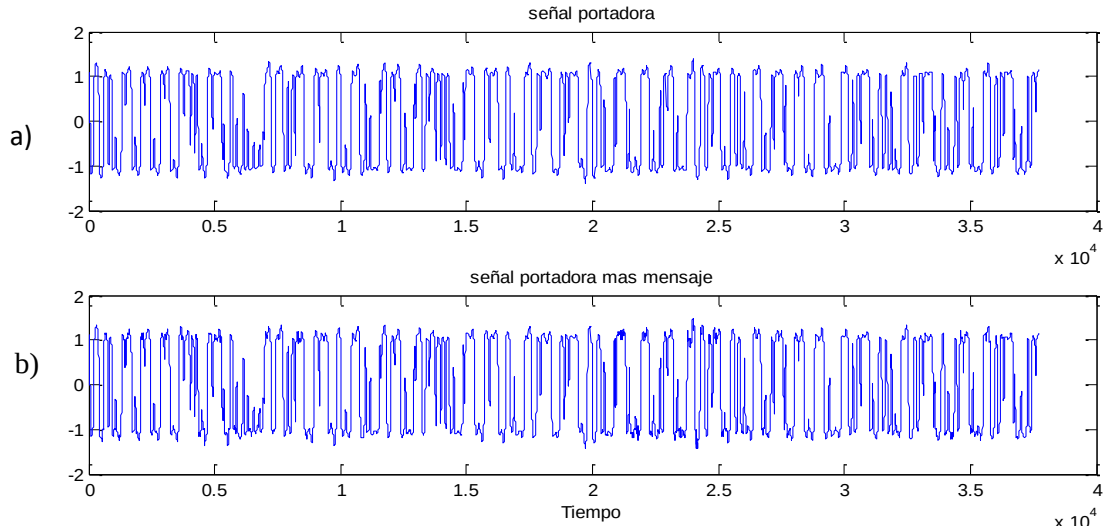


Figura 56. (a) Estado $x_1(t)$ y (b) estado $x_1(t)$ mas mensaje adherido a través del tiempo.

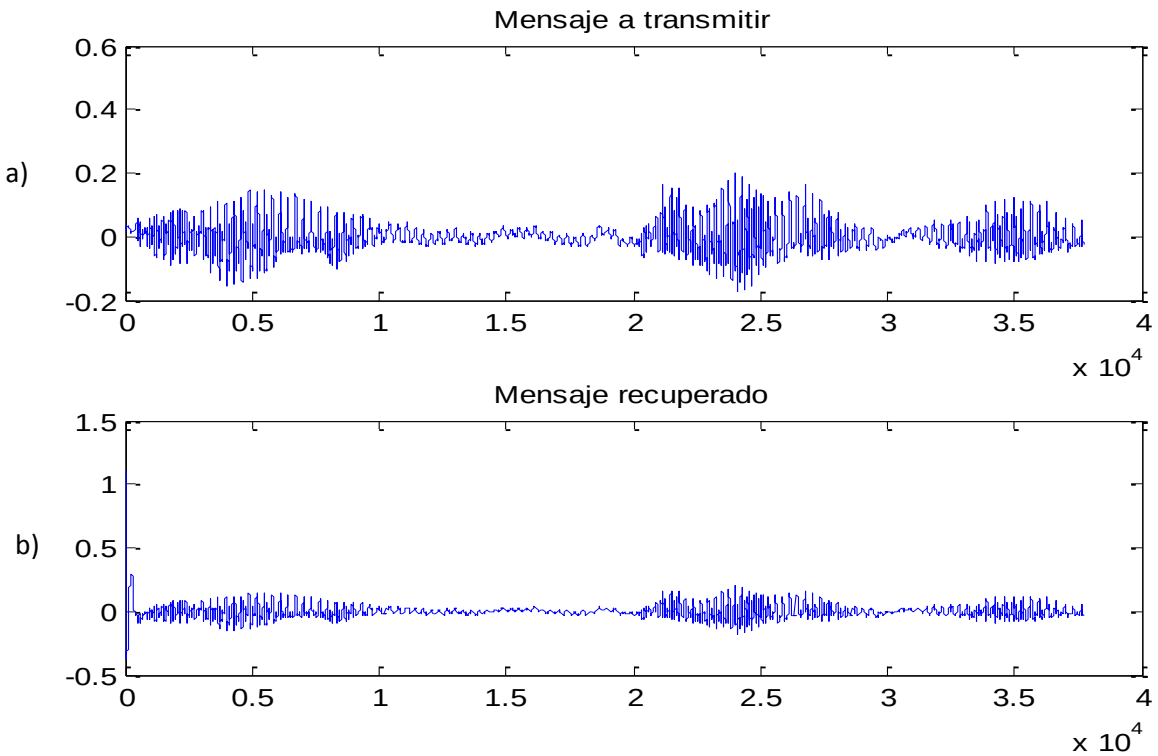


Figura 57. (a) Mensaje transmitido, (b) mensaje recuperado en el esclavo.

En la figura 58 se muestra la sincronía entre el estado $x_1(t)$ del transmisor contra el estado $x_1(t)$ del receptor y se observa que no se pierde la sincronía al hacer la transmisión de información entre ellos.

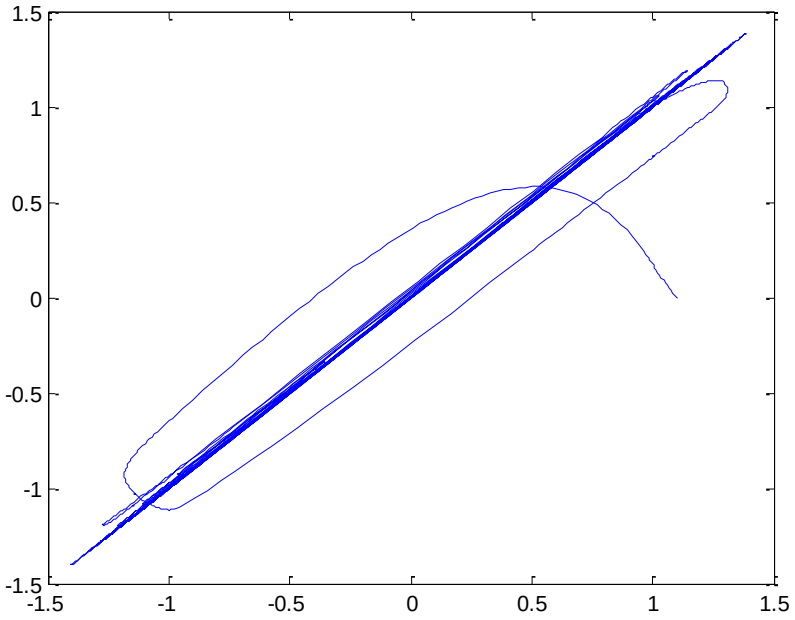


Figura 58. Sincronía entre maestro y esclavo.

8.2.2 – Resultados experimentales

Para obtener los resultados experimentales se utilizó el diagrama de la figura 23 y a su vez el circuito experimental de la figura 24 tanto como transmisor y otro para receptor, el mensaje que se utilizó para la transmisión fue una onda sinusoidal obtenida de un generador de funciones con una amplitud de 1 Volt y frecuencia al azar solo para propósitos ilustrativos (ver figura 59), este mensaje fue sumado a la señal $V_1(t)$ que a su vez es la señal de acoplamiento con la cual se realizó la sincronía entre el transmisor y el receptor, una vez realizada la sincronización se obtiene el error entre el voltaje $V_1(t)$ del transmisor y el voltaje $V_1(t)$ del receptor, este error obtenido corresponde al mensaje recuperado.

El diagrama de este proceso se muestra en la figura 60 y los resultados obtenidos son mostrados a continuación.

En la figura 61 (a) se muestra la evolución en el tiempo de la señal $V_1(t)$ cuando aun no se adherido el mensaje a transmitir y la figura 61 (b) cuando ya se sumo la información a la señal $V_1(t)$, donde se observa que las dos figuras (a) y (b) son prácticamente iguales, lo que provoca que se siga dando la sincronía entre el transmisor y receptor logrando la transmisión de información de manera segura y efectiva.

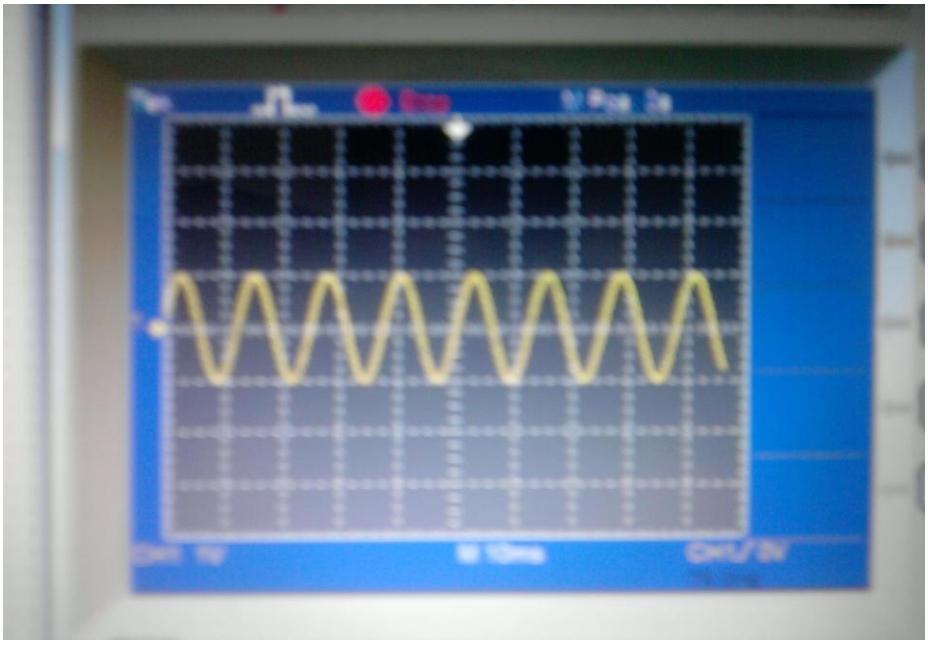


Figura 59. Mensaje utilizado para la transmisión de información

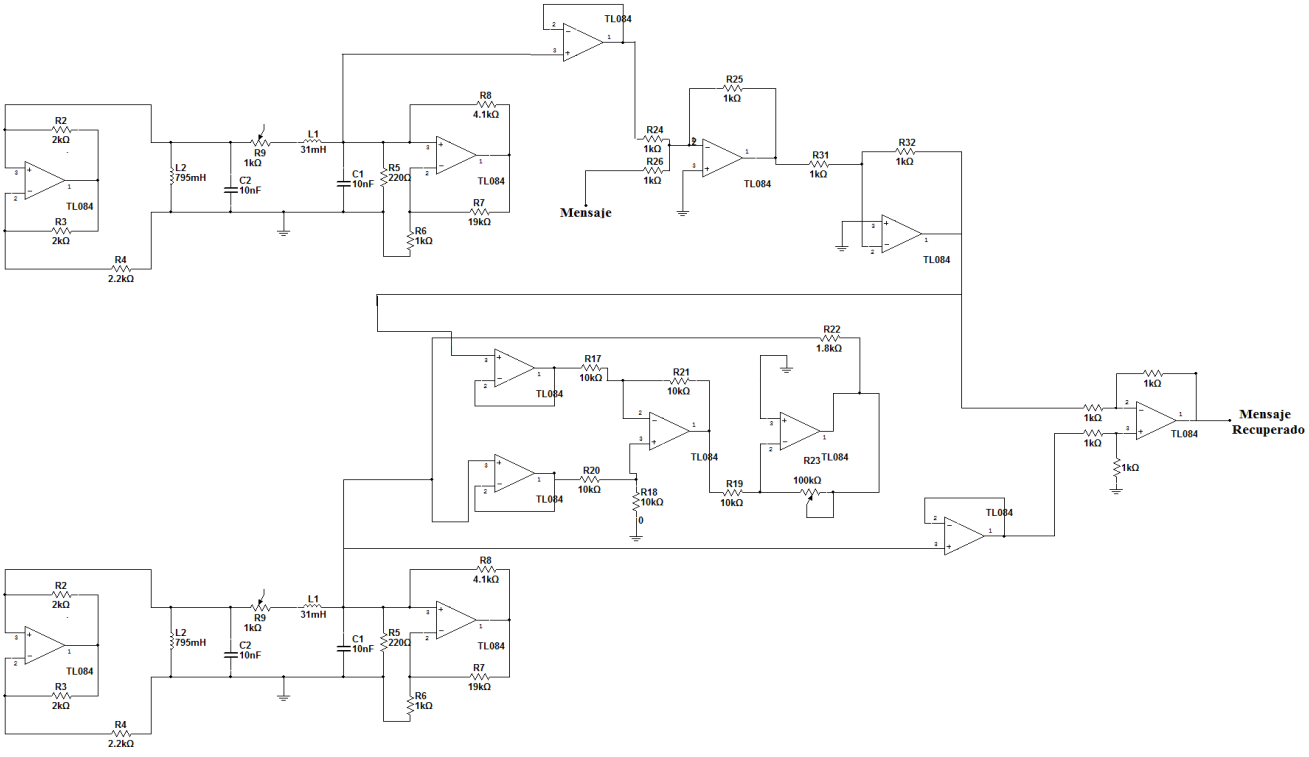


Figura 60. Diagrama del proceso de comunicación entre un transmisor y un receptor.

Figura 61. (a) Señal de voltaje $V_1(t)$ y (b) Señal de voltaje $V_1(t)$ mas mensaje adherido a través del tiempo.

En la figura 62 (a) se muestra el mensaje que se transmitió a través del maestro y la figura 62 (b) muestra el mensaje recuperado en el circuito receptor, donde se observa que se logró recuperar la onda señal sinusoidal transmitida.

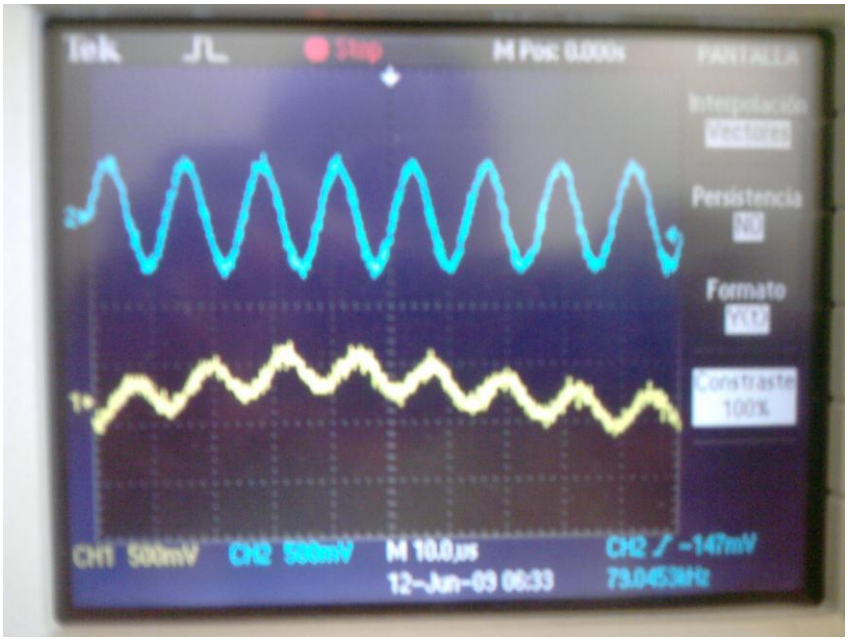


Figura 62 (a) Mensaje transmitido, (b) mensaje recuperado en el receptor.

En la figura 63 se muestra la sincronía entre el transmisor contra el receptor y se observa que no se pierde la sincronía al hacer la transmisión de información entre ellos.

Figura 63. Sincronía entre transmisor y receptor.

8.3 – Comunicación en configuración estrella

La transmisión de información analógica privada entre un circuito transmisor y cuatro circuitos receptores se llevo a cabo mediante la técnica de codificación caótica aditiva por un canal de transmisión, un esquema general se muestra en la figura 64, donde se puede observar que el mensaje a transmitir es sumado al estado $x_1(t)$ que también es usado para la sincronización del sistema transmisor con los sistemas receptores, una vez sumado el mensaje y sincronizados los sistemas transmisor y receptor se hace la resta del estado $x_1(t)$ del transmisor menos el estado $\widehat{x_1}(t)$ de cada sistema receptor obteniendo de esta forma el mensaje enviado en el transmisor.

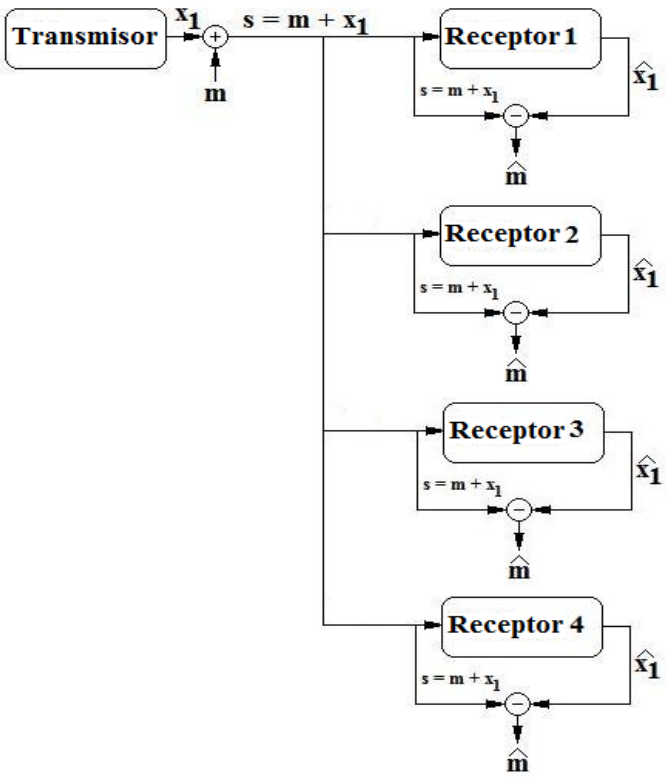


Figura 64. Esquema de la comunicación entre un transmisor y cuatro receptores.

8.3.1 - Resultados numéricos

Se utiliza el circuito de Chua de cuarto orden transmisor (7) el cual exhibe un comportamiento hipercaótico con el cual se sincronizan los circuitos de Chua de cuarto orden receptores descritos por (25), con un escenario de acoplamiento unidireccional maestro y esclavos. Donde la señal de acoplamiento resulta ser $x_1(t)$ de acuerdo con los análisis hechos en capítulos anteriores.

Parámetros del sistema transmisor

$\alpha_1 = 2.1429$, $\alpha_2 = -0.1283$, $\beta_1 = 0.0393$, $\beta_2 = 0.0015$, $a = -0.0299$ y $b = 1.995$.

Condiciones iniciales del transmisor

$$x(0) = (1.1, 0.1, -0.5, 0.01).$$

Circuitos receptores de Chua de cuarto orden

Receptor 1

Las condiciones iniciales del receptor 1 son:

$$x_{1_1}(0) = 0.5,\ x_{2_1}(0) = 0.3,\ x_{3_1}(0) = -0.4 \ \ y \ \ x_{4_1}(0) = 0.0.$$

y donde:

$$\propto_1 = 3.1428;\ \propto_2 = -0.1282;\ \ \beta_1 = 0.0395 \ \ y \ \ \beta_2 = 0.0014.$$

Receptor 2

Las condiciones iniciales del receptor 2 son:

$$x_{1_1}(0) = 1.0,\ x_{2_1}(0) = 0.0,\ x_{3_1}(0) = -0.2 \ \ y \ x_{4_1}(0) = 0.04.$$

y donde:

$$\propto_1 = 1.1430;\ \propto_2 = -0.1284;\ \ \beta_1 = 0.0391 \ \ y \ \ \beta_2 = 0.0016.$$

Receptor 3

Las condiciones iniciales del receptor 3 son:

$$x_{1_1}(0) = 0.9,\ x_{2_1}(0) = 0.4,\ x_{3_1}(0) = -1.0 \ \ y \ \ x_{4_1}(0) = 0.02.$$

y donde:

$$\propto_1 = 1.1430;\ \propto_2 = -0.1284;\ \ \beta_1 = 0.0391 \ \ y \ \ \beta_2 = 0.0016.$$

Receptor 4

Las condiciones iniciales del receptor 4 son:

$$x_{1_1}(0) = 0.3,\ x_{2_1}(0) = 0.2,\ \ \ \ x_{3_1}(0) = 0.0 \ \ y \ x_{4_1}(0) = 0.06.$$

y donde:

$$\propto_1 = 1.1430;\ \propto_2 = -0.1284;\ \beta_1 = 0.0391 \ \ y \ \ \beta_2 = 0.0016.$$

Mensaje a transmitir

En la figura 65 se observa el mensaje utilizado en la transmisión de información encriptada, este mensaje fue grabado por medio del micrófono de la computadora.

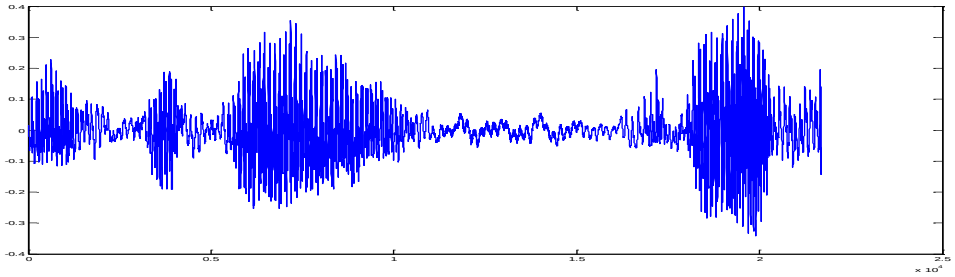
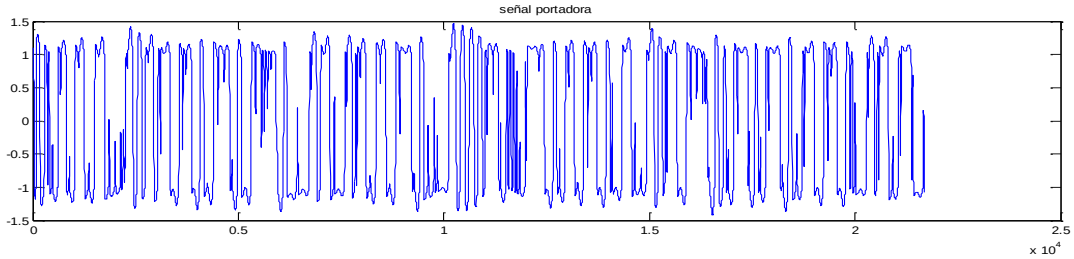


Figura 65. Mensaje a ser encriptado y transmitido por el transmisor a los cuatro receptores.

En la figura 66 (a) se muestra la evolución en el tiempo del estado $x_1(t)$ cuando aun no se adherido el mensaje a transmitir y la figura 66 (b) cuando ya se sumo la información al estado $x_1(t)$, donde se observa que las dos figuras (a) y (b) son prácticamente iguales, lo que provoca que se siga dando la sincronía entre el transmisor y los receptores y se pueda hacer la transmisión de información de manera segura y efectiva.

En la figura 67 se muestra el mensaje que se transmitió a través del estado $x_1(t)$ y el mensaje recuperado en cada uno de los circuitos receptores, donde se observa que se recupera en su totalidad y al ser reproducido por medio de la computadora se aprecia que la calidad del mensaje recuperado es muy similar a la del mensaje transmitido.

a)



b)

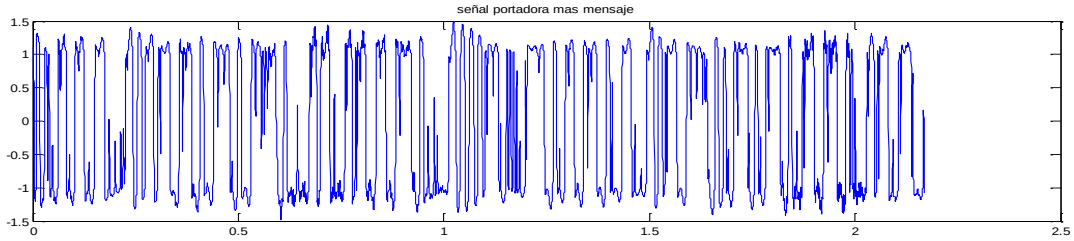


Figura 66 (a) Estado $x_1(t)$ y (b) estado $x_1(t)$ mas mensaje adherido a través del tiempo.

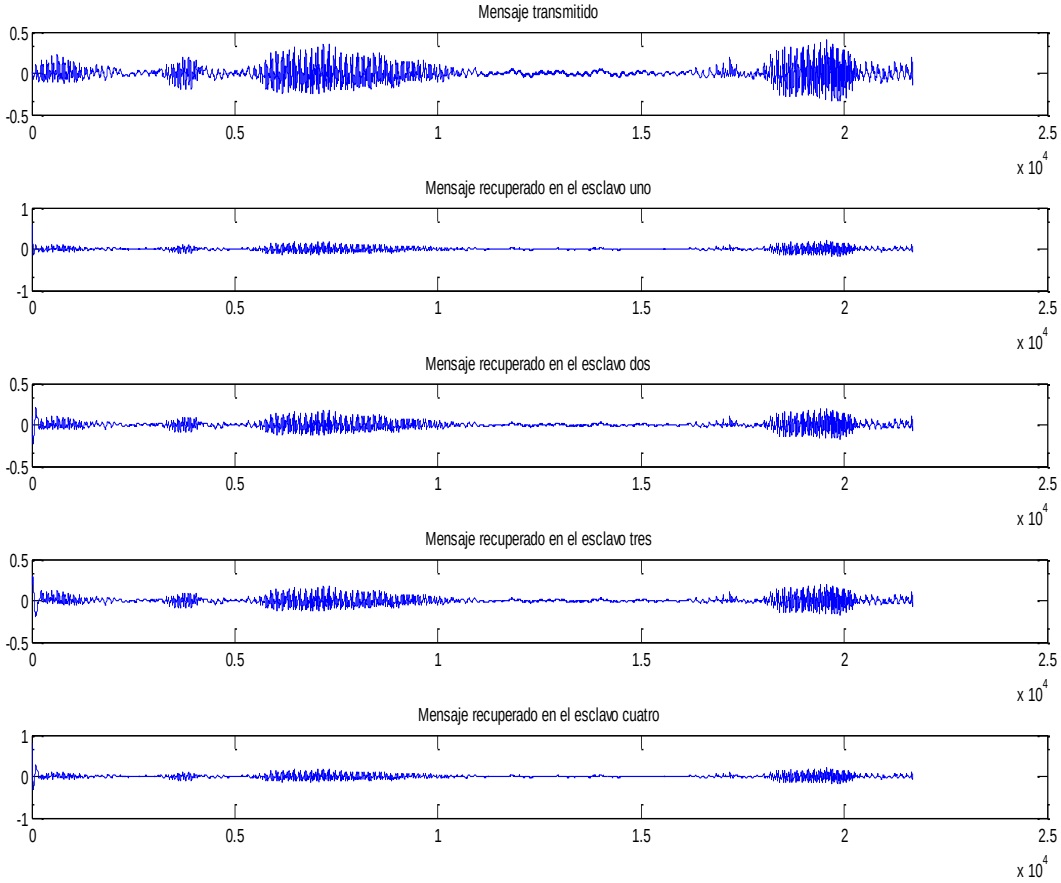


Figura 67. (a) Mensaje transmitido, (b) mensaje recuperado en el receptor.

En la figura 68 se muestra la sincronía entre el estado $x_1(t)$ del transmisor contra el estado $x_1(t)$ de cada uno de los receptores y se observa que no se pierde la sincronía al hacer la transmisión de información en este tipo de configuración.

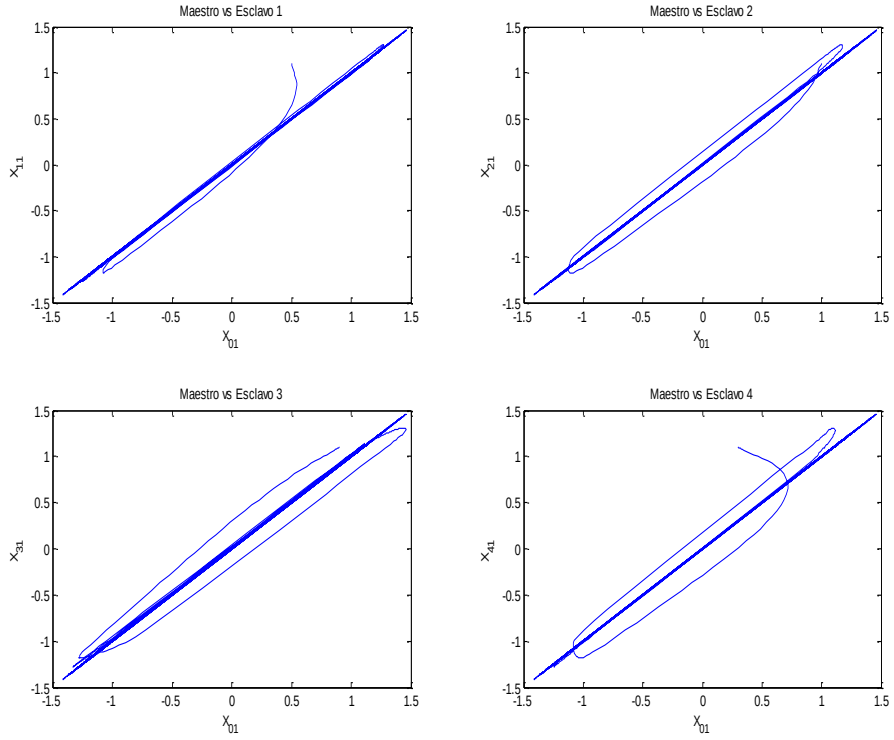


Figura 68. Sincronía entre transmisor y receptores.

8.4- Conclusiones

En este capítulo se dio la aplicación a las comunicaciones seguras donde se hizo la transmisión de información en dos tipos de configuraciones. La primera configuración fue la de maestro y esclavo en la cual se hizo la comunicación en forma numérica y experimental con muy buenos resultados, la forma numérica fue por medio de la grabación de un mensaje de voz y en forma experimental el mensaje fue una onda sinusoidal proveniente de un generador de funciones. La otra configuración utilizada para la transmisión de información fue la configuración estrella, en esta configuración se obtuvieron solo resultados numéricos, donde el mensaje transmitido fue una grabación de voz hacia cuatro receptores en los cuales se recupero el mensaje de forma satisfactoria en cada uno de ellos.

Capítulo 9

Conclusiones generales, aportaciones y trabajo a futuro

A continuación se mencionan algunas **conclusiones generales** sobre esta investigación.

En este trabajo de tesis se realizó la aplicación de sistemas hipercaóticos al encriptado y transmisión de información utilizando el circuito de Chua de cuarto orden propuesto en [Thamilmaran y Lakshmanan 2004], el cual exhibe el comportamiento hipercaótico requerido para este trabajo de tesis.

Primeramente se obtuvieron resultados numéricos de las dinámicas hipercaóticas que genera el circuito de Chua de cuarto orden.

Posteriormente se implementó físicamente el circuito reproduciendo sus dinámicas en el osciloscopio, después se obtuvo la sincronización con un observador diseñado a partir de la forma hamiltoniana de las ecuaciones de estado de este circuito, metodología propuesta en [Sira-Ramírez y Cruz-Hernández 2000; 2001], obteniendo resultados numéricos y experimentales.

También se obtuvo la sincronía en una red de usuarios por medio de la configuración estrella, la cual, no estaba contemplada en los objetivos iniciales, donde se sincronizó un maestro con N esclavos. La otra configuración utilizada fue la de sincronización entre N maestros con N esclavos, en estas dos configuraciones de red se obtuvieron solo 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 cuarto orden, y el mensaje se recuperó en el receptor de manera satisfactoria, en esta transmisión de información se tuvieron resultados numéricos y experimentales.

También se realizó la comunicación en configuración estrella, donde el mensaje fue sumado al estado del receptor y transmitido hacia 4 receptores, y el mensaje se recuperó satisfactoriamente en el receptor, estos resultados obtenidos fueron resultados numéricos.

Con estos resultados obtenidos en este trabajo de tesis se cumplieron en su totalidad y a plena satisfacción con los objetivos propuestos originalmente y más aun, se superaron.

El circuito hipercaótico de Chua utilizado cumplió satisfactoriamente con los objetivos, funcionando perfectamente con la técnica de sincronización propuesta en [Sira-Ramírez y Cruz-Hernández 2000; 2001]. Además, pudiendo ser utilizado en otras aplicaciones donde se requiera la sincronización de múltiples sistemas, redes en diferentes topologías, etc.

En cuanto su aplicación a la comunicación, se logró realizar la transmisión de manera segura en tres configuraciones diferentes recuperando la información transmitida en cada uno de los receptores utilizados.

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

1. **Encriptado de información utilizando hipercaos**, presentado en el *Congreso Anual de la Sociedad Mexicana de Instrumentación (SOMI)*, celebrado en Xalapa, Veracruz realizado del 1 al 3 octubre de 2008.

2. **Synchronization of Modified Chua's Circuits in Star Coupled Networks**, presentado en la *6th International Conference on Informatics in Control, Automatization and Robotics (ICINCO 2009)* realizado en Milán, Italia del 2 al 5 julio de 2009.

3. **Synchronization of a modified Chua's Circuit and its application to communication,** presentado en el *Second IFAC Meeting Related to Analysis and Control of Chaotic Systems (CHAOS09)*, celebrado en Londres, Inglaterra del 22 al 24 de junio de 2009.

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

- Realizar la comunicación digital entre un maestro y un esclavo de forma numérica y experimental.

- Realizar la comunicación en configuración estrella de forma experimental (comunicación analógica y digital).

- Realizar la comunicación en red entre *N* maestros y *N* esclavos de forma numérica y experimental (comunicación analógica y experimental).

- Análisis de comportamiento de la información bajo la presencia de ruido en el canal de transmisión para cada una de las configuraciones mencionadas anteriormente.

- Utilizar la sincronización hipercaótica en otras aplicaciones o configuraciones.

- Extender este trabajo de tesis a la sincronización de redes complejas y sus aplicaciones en comunicaciones.

Referencias

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

Aguilar–Bustos A.Y. y Cruz–Hernández C., R.M. López–Gutiiérrez y C. Posadas–Castillo, [2008]. Synchronization of Different Hyperchaotic Maps for Encryption, Nonlinear Dynamics and Systems Theory, 8(3) 221–236.

Aguilar-Bustos A.Y. y Cruz-Hernández C [2009]. Synchronization of discrete-time hyperchaotic systems: An application in communications, Chaos, Solitons & Fractals, 41(3), 1301-1310.

Alvarez G, Montoya F, Romera M y Pastor G. [2004]. Breaking parameter modulated chaotic secure communication system. Chaos Solitons & Fractals; 21(4):783–7.

Brucoli, M., Cafagna, D. y Carnimeo, L. [1999].Design of a hyperchaotic cryptosystem based on identical and generalized synchronization. Int. J. Bifurc. Chaos 9(10) 2027–2037.

Chen G. y Ueta T. [2002], Chaos in circuits and systems, World Scientific, Singapore.

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

Chow T.W.S., Jiu-Chao F., y Ng K.T. [2001], Chaotic network synchronization with applications to communications, International Journal of Communication systems, 14, 217-30.

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

Cruz-Hernandez C., Posadas C. y Sira-Ramírez H. [2002]. Synchronization of two hyperchaotic Chua Circuits: a generalized Hamiltonian systems approach, IFAC'2002, Barcelona, España.

Cruz-Hernández C, Martynyuk AA. [2009]. Advances in chaotic dynamics with applications, vol. 4. London: Cambridge Scientific Publishers.

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

Cruz-Hernández C, Serrano-Guerrero H. [2005]. Cryptosystems based on synchronized Chua's circuits. In: Proceedings of the 16th IFAC world congress, Prague, Czech Republic.

Cruz-Hernández C. [2004]. Synchronization of Time-Delay Chua's Oscillator with Application to Secure Communication, Nonlinear Dynamics and Systems Theory, 4(1) 1-13.

Cruz-Hernández C y Romero-Haros N. [2008]. Communicating via synchronized time-delay Chua's circuits. Communications in Nonlinear Science and Numerical Simulation; 13(3):645–59.

Cruz-Hernández C, López-Mancilla D, García V, Serrano H, Núñez R. [2005]. Experimental realization of binary signal transmission using chaos. J. Circ. Syst. Comput. 14(3):453–68.

Dedieu, H., Kennedy, M.P. y Hasler, M. [1993]. Chaotic shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits. IEEE Trans. Circuits Syst. II 40(10) 634–642.

Fradkov A.L. y Yu A. [1998]. Pogromsk, Introduction to Control of Oscillations and Chaos, World Scientific, Singapore.

Feldmann U. [1996]. Communication by chaotic signal: the inverse system approach, Int. J. Circuits Theory Applications, 24, 551-579.

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

Galende, J.C. (1995): Criptografía: Historia de la escritura cifrada. Ed. Complutense,. Madrid.

Gámez-Guzmán L, Cruz-Hernández C, López-Gutiérrez RM y García-Guerrero EE.[2008]. Synchronization of multi-scroll chaos generators: application to private communication. Revista Mexicana de Física;54(4):299–305.

Gámez-Guzmán L., Cruz-Hernández C., López-Gutiérrez R.M. y García-Guerrero E.E. [2009]Synchronization of Chua's circuits with multi-scroll attractors: Application to communication. Communications in Nonlinear Science and Numerical Simulation, 14 2765–2775.

Gámez-Guzmán L. [2004] Encriptador de información con base en la sincronía de atractores con enrollamientos múltiples. Tesis de maestría, DET-CICESE.

González-Miranda J. M. [2004], Synchronization and control of chaos, Imperial College Press, Singapore.

http://es.wikipedia.org/wiki/Cifrado_Vernam.

Kapitaniak T. y Chua L.O. [1994]. Hyperchaotic attractors of unidirectionally coupled Chua's circuits. Int. J. Bifurcation and Chaos 4, 477–482.

Kapitaniak T. [2000]. Chaos for Engineers: Theory, Applications and Control. Springer, Second Ed.

Kennedy M.P. [1992]. Robust op amp realization of Chua´s circuit, Frequenz, Vol. 46, 3-4, 1992, pp. 66-80.

Lakshmanam M. y Murali K. [1995]. Trans. Roy. Soc. London, Trans A353.

Lakshmanan M. y Murali K. [1996], Chaos in nonlinear oscillatiors, Controlling and synchronization, World Scientific, Singapore.

López-Mancilla D. y Cruz-Hernández C. [2005]. Output synchronization of chaotic systems: model-matching approach with application to secure communication. Nonlinear Dyn Syst Theory 5(2):141–56.

López-Mancilla D, Cruz-Hernández C.[2005]. A note on chaos-based communication schemes. Revista Mexicana de Física;51(3):265–9.

López-Mancilla D. y Cruz-Hernández C. [2008] Output synchronization of chaotic systems under non-vanishing perturbations. Chaos Solitons & Fractals 37(4):1172–86.

Manuel José Lucena López [1999]: Criptografía y Seguridad en Computadores Segunda Edición.

Matsumoto T. [1984] A chaotic attractor from Chua´s circuit. IEEE Trans. Circuits Syst.,I-31(12): 1055-1058.

Mejía-Camacho J.M. [2007] Encriptamiento de información mediante caos. Tesis de maestría, Facultad de Ingeniería Ensenada, UABC.

Mensour, B. and Longtin, A. [1998] Synchronization of delay-differential equations with application to private communication. Phys. Lett. A 244(1) 59–70.

Meranza-Castillón M.O. [2002] Implementación de un sistema de encriptamiento hipercaótico. Tesis de maestría, DET-CICESE.

Milanovic V. Zaghloul M.E. [1996]. Synchronization of chaotic neural networks for secure communications. Circuits and Systems, 1996. ISCAS '96., Connecting the World., 1996 IEEE International Symposium on. 12/06/199606/1996; 3:28-31 vol.3.

Moon Francis [1990]. Chaotic and Fractal Dynamics. Springer-Verlag New York, LLC.

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

Número especial [1997a] Control of chaos and synchronization, Systems and Control Letters 3(5).

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

Número especial [2000] on Control and synchronization of chaos. Int. J. Bifurc. Chaos 10(3–4).

Ogorzalek M. J. [1997], Chaos and complexity in nonlinear electronic circuits, World Scientific, Singapore.

Ott Edward [2002]. Chaos in Dynamical Systems. Cambridge University Press New, York.

Palaniyandi P, Lakshmanan M.[2001]. Secure digital transmission by multistep parameter modulation and alternative driving of transmitter variables. Int. J. Bifurct. Chaos 11(7):2031–6.

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

Pecora L. y Carroll T.L. [1991]. Synchronizing chaotic circuits, IEEE Trans. Circuits Syst. 38(4), 453-456.

Peng, J.H., Ding, E.J., Ding, M. and Yang, W. [1996].Synchronizing hyperchaos with a scalar transmitted signal. Phys. Rev. Lett. 76(6) 904–907.

Perez G. y Cerdeira H. A. [1995]. Extracting messages masked by chaos, Phys. Rev. Lett. 74, 1970-1973

Pyragas, K. [1998].Transmission of signals via synchronization of chaotic time-delay systems. Int. J. Bifurc. Chaos 8(9) 1839–1842

Romero-Haros N.R. [2005] Sincronización del circuito de Chua con retardo: aplicación a la transmisión secreta de información. Tesis de maestría, DET-CICESE.

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

Short K.M. y Parker A.T [1998]. Unmasking a hyperchaotic communication scheme. Phys Rev;E58(1):1159–62.

Simon Singh [2000], Los códigos secretos : el arte y la ciencia de la criptografía, desde el antiguo Egipto a la era Internet, Barcelona, Debate.

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

Tamaševicius A,Cenys A, Namaj_unas A, Mykolaitis G. [1998]. Synchronising hyperchaos in infinite-dimensional dynamical systems. Chaos Solitons & Fractals;9(8):1403–8.

Thalmiran K. y Lakshamanan M. [2004] Hyperchaos in a modified canonical Chua's circuit, Int J. Bifurcation and Chaos 14, 221-243

Ushio, T. [1999]. Synthesis of synchronized chaotic systems based on observers. Int. J. Bifurcation and Chaos, 9(3):541—546.

Wu, W. y Chua, L. [1994]. A unified framework for synchronization and control of dynamical systems. Int. J. Bifurcation and Chaos, 4:979-998.

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

Wu W. [2002], Synchronization in coupled chaotic circuits and systems, World Scientific, Singapore.

Yang, T., Wu, C.W. y Chua, L.O. [1997]. Cryptography based on chaotic systems. IEEE Trans. Circuits Syst. I 44(5) 469–472.

Yang T. y Chua L., [1996]. Secure communication via chaotic parameter modulation, IEEE Trans. Circuits Syst. I 44(5), 817-819.

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

Zhong G.Q. y Ayrom F. [1985] Experimental confirmation of Chua´s circuit. Int. J. Circuit theory Appl-13 (11): 93-98.