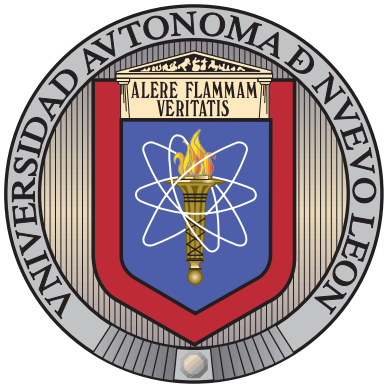
Universidad Autónoma de Nuevo León

Facultad de Ingeniería Mecánica y Eléctrica

Subdirección de Estudios de Posgrado



Encriptado de datos con osciladores caóticos de orden fraccionario

por

Otoniel García Sepúlveda

como requisito parcial para obtener el grado de

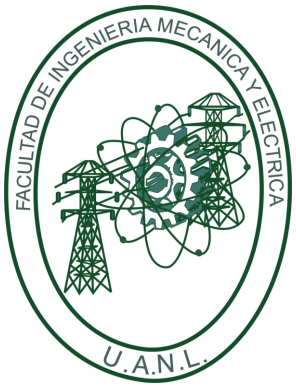
maestría en ciencias de la ingeniería eléctrica

Julio 2015

Universidad Autónoma de Nuevo León

Facultad de Ingeniería Mecánica y Eléctrica

Subdirección de Estudios de Posgrado



Encriptado de datos con osciladores caóticos de orden fraccionario

por

Otoniel García Sepúlveda

como requisito parcial para obtener el grado de

maestría en ciencias de la ingeniería eléctrica

Julio 2015

Universidad Autónoma de Nuevo León

Facultad de Ingeniería Mecánica y Eléctrica

Subdirección de Estudios de Posgrado

Los miembros del Comité de Tesis recomendamos que la Tesis «**ENCRIPTADO DE DATOS CON OSCILADORES CAÓTICOS DE ORDEN FRACCIONARIO**», realizada por el alumno **Otoniel García Sepúlveda**, con número de matrícula **1384113**, sea aceptada para su defensa como requisito parcial para obtener el grado de **Maestría en Ciencias de la Ingeniería Eléctrica**.

El Comité de Tesis

Dr. Cornelio Posadas Castillo
Asesor

Dr. Miguel Ángel Platas Garza
Revisor

M. C. Guadalupe Evaristo Cedillo Garza
Revisor

Vo. Bo.

Dr. Simón Martínez Martínez
Subdirección de Estudios de Posgrado

San Nicolás de los Garza, Nuevo León, julio 2015

Dedicada a mi padre y a mi madre.

Por todo su apoyo y confianza en mí...

Índice general

Agradecimientos xiv

Resumen xv

1. Introducción 1

1.1. Motivación 1

1.2. Objetivo general 2

1.3. Objetivos particulares 2

1.4. Antecedentes 2

1.4.1. Sincronía 2

1.4.2. Caos 4

1.4.3. Criptología 7

1.4.4. Encriptado caótico 9

1.5. Organización del trabajo de tesis 10

2. Redes complejas 13

2.1. Antecedentes históricos 13

2.1.1. Los siete puentes de Königsberg 13

2.2. Redes en el mundo real 15

2.3. Definiciones 16

2.4. Topologías de las redes complejas 17

2.4.1. Topología regular 18

2.4.2. Topología irregular 21

3. Osciladores caóticos de orden fraccionario 23

3.1. Preliminares matemáticos del cálculo fraccionario 24

3.2. Oscilador caótico Lorenz de orden fraccionario 25

3.3. Oscilador caótico Rössler de orden fraccionario 27

3.4. Oscilador caótico Genesio-Tesi de orden fraccionario 29

3.5. Oscilador caótico Chen de orden fraccionario 30

3.6. Oscilador caótico Lü de orden fraccionario 32

3.7. Oscilador caótico Arneodo de orden fraccionario 33

4. Sincronización de redes complejas 36

4.1. Definiciónes de sincronización 37

4.2. Sincronización de una red compleja de N osciladores caóticos Lü de orden fraccionario 39

4.3. Sincronización de una red compleja de N osciladores caóticos Arneodo de orden fraccionario 43

4.4. Sincronización de una red compleja de N osciladores caóticos Genesio-Tesi de orden fraccionario 49

5. Encriptado caótico de datos 54

5.1. Encriptado caótico con osciladores fraccionarios 55

5.1.1. Encriptado caótico de voz 56

5.1.2. Encriptado caótico de imagen 65

6. Conclusiones, aportaciones y trabajos a futuro. 71

6.1. Aportaciones de este trabajo de tesis 72

6.2. Trabajos a futuro 73

Índice de figuras

1.1. Dibujo hecho por Christiaan Hyugens ilustrando su experimento. . . . 3

1.2. Ejemplos de sincronía en el mundo real. 4

1.3. Atractor caótico de Lorenz de orden entero. 5

1.4. Atractores caóticos de los dos osciladores Lorenz de orden entero con diferentes condiciones iniciales. $(x_1(0), y_1(0), z_1(0)) = (-0.1, 0.5, 0.2)$, $(x_2(0), y_2(0), z_2(0)) = (-0.11, 0.5, 0.2)$. 6

1.5. Evolución temporal de los estados de dos osciladores caóticos Lorenz de orden entero con condiciones iniciales diferentes. $(x_1(0), y_1(0), z_1(0)) = (-0.1, 0.5, 0.2)$, $(x_2(0), y_2(0), z_2(0)) = (-0.11, 0.5, 0.2)$. 7

1.6. Tabla de Vigenère utilizada para cifrar mensajes. 9

1.7. Proceso de encriptado, transmisión y recuperación del mensaje. . . . 10

2.1. Esquema de los siete puendes de Königsberg en donde se pueden apreciar las zonas A, B, C y D. 14

2.2. Ejemplos de redes en la naturaleza: a) redes neuronales, b) redes sociales, c) redes comerciales, d) redes de vias aéreas. 15

2.3. a) Configuración maestro-esclavo: la información fluye unidireccionalmente del nodo maestro al nodo esclavo b) configuración bidireccional: la información fluye del nodo A al nodo B y viceversa. 17

2.4. Red compleja en acoplamiento global y configuración bidireccional. . 19

2.5. Red compleja en acoplamiento anillo y configuración bidireccional. . . 20

2.6. Red compleja en acoplamiento estrella y configuración bidireccional. . 21

2.7. Red compleja en topología irregular y configuración bidireccional. . . 22

3.1. Atractor caótico del oscilador Lorenz de orden fraccionario para parámetros: $\sigma = 10, \rho = 28, \beta = 8/3$, derivadas: $q_1 = q_2 = q_3 = 0.995$, y condiciones iniciales: $(x(0), y(0), z(0)) = (0.1, 0.1, 0.1)$. 26

3.2. Evolución temporal de los estados del oscilador caótico Lorenz de orden fraccionario. 27

3.3. Atractor caótico del oscilador Rössler de orden fraccionario para parámetros: $a = 0.5, b = 0.2, c = 10$, derivadas: $q_1 = q_2 = q_3 = 0.9$, y condiciones iniciales: $(x(0), y(0), z(0)) = (0.5, 1.5, 0.1)$. 28

3.4. Evolución temporal de los estados del oscilador caótico Rössler de orden fraccionario. 28

3.5. Atractor caótico del oscilador Genesio-Tesi de orden fraccionario para parámetros: $b_1 = 1.1, b_2 = 1.1, b_3 = 0.45, b_4 = 1$, derivadas: $q_1 = 1, q_2 = 1, q_3 = 0.95$, y condiciones iniciales: $(x(0), y(0), z(0)) = (0.1, -0.5, 0.2)$. 29

3.6. Evolución temporal de los estados del oscilador caótico Genesio-Tesi de orden fraccionario. 30

3.7. Atractor caótico del oscilador Chen de orden fraccionario para parámetros: $a = 35, b = 3, c = 28, d = -7$, derivadas: $q_1 = q_2 = q_3 = 0.9$, y condiciones iniciales: $(x(0), y(0), z(0)) = (1, 0.1, 2.5)$. 31

3.8. Evolución temporal de los estados del oscilador caótico Chen de orden fraccionario. 31

3.9. Atractor caótico del oscilador Lü de orden fraccionario para parámetros: $a = 36, b = 3, c = 20$, derivadas: $q_1 = q_2 = q_3 = 0.95$, y condiciones iniciales: $(x(0), y(0), z(0)) = (1, 0.1, 2.5)$. 32

3.10. Evolución temporal de los estados del oscilador caótico Lü de orden fraccionario. 33

3.11. Atractor caótico del oscilador Arneodo de orden fraccionario para parámetros: $\beta_1 = -5.5, \beta_2 = 3.5, \beta_3 = 0.8, \beta_4 = -1$, derivadas: $q_1 = 0.97, q_2 = 0.97, q_3 = 0.96$, y condiciones iniciales: $(x(0), y(0), z(0)) = (2.1, -1.9, 3.2)$. 34

3.12. Evolución temporal de los estados del oscilador caótico Arneodo de orden fraccionario. 34

4.1. Topología de la red compleja regular con acoplamiento estrella y configuración bidireccional. 39

4.2. Evolución temporal de los estados $x_i(t), y_i(t), z_i(t)$, de la red mostrada en la Figura 4.1 (donde $i = 1, 2, \ldots, 6$). 42

4.3. Planos de fase de los estados y_1 vs y_2, y_6 vs y_7, y_8 vs y_{12} de la red mostrada en la Figura 4.1. 42

4.4. Evolución temporal del error de sincronización entre los estados $y_4 - y_{11}$, $y_5 - y_{10}$, y $y_3 - y_9$ de la red mostrada en la Figura 4.1. 43

4.5. Topología de la red compleja irregular y configuración bidireccional. . 44

4.6. Evolución temporal de los estados $x_i(t), y_i(t), z_i(t)$ de la red mostrada en la Figura 4.5 (donde $i = 14, 15, \ldots, 20$). 48

4.7. Planos de fase de los estados x_1 vs x_2, x_1 vs x_3, ..., x_1 vs x_{13} de la red mostrada en la Figura 4.5. 48

4.8. Evolución temporal del error de sincronización entre los estados $x_1 - x_2$, $x_1 - x_3$, y $x_2 - x_3$ de la red mostrada en la Figura 4.5. 49

4.9. Topología de la red compleja regular y configuración maestro-esclavo. 50

4.10. Evolución temporal de los estados $x_i(t), y_i(t), z_i(t)$, de la red mostrada en la Figura 4.9 (donde $i = 1, 2, \ldots, 20$). 52

4.11. Planos de fase de los estados x_1 vs x_2, x_1 vs x_3, ..., x_1 vs x_{13} de la red mostrada en la Figura 4.9. 52

4.12. Evolución temporal del error de sincronización entre los estados $x_1 - x_2$, $x_1 - x_6$, y $x_1 - x_7$ de la red mostrada en la Figura 4.9. 53

5.1. Niveles de energía de las variables de estado del primer oscilador (Lü de orden fraccionario) de la red. 57

5.2. Filtro pasa banda de Butterworth, utilizado para filtrar las señales de este capítulo. 57

5.3. Niveles de energía de las variables de estado del primer oscilador (Lü de orden fraccionario) de la red, en la banda de frecuencias del mensaje $m(t)$. 58

5.4. Diagrama básico de encriptamiento caótico de dos canales. 59

5.5. (a) Mensaje a encriptar $m(t)$, (b) Mensaje encriptado $s_1(t)$ y (c) Mensaje recuperado $m'(t)$. 60

5.6. Diagrama de encriptado aditivo y modulación del estado $y(t)$. 62

5.7. Niveles de energía anteriores (azul) y posteriores (verde) a la modulación de las variables de estado del primer oscilador (Lü de orden fraccionario) de la red, en la banda de frecuencias del mensaje $m(t)$. . 62

5.8. (a) Mensaje a encriptar $m(t)$, (b) Mensaje encriptado $s_2(t)$ y (c) Mensaje recuperado $m'(t)$. 64

5.9. Imagen a encriptar: Tierra.jpeg, dimensiones: 120×120 pixeles. . . . 68

5.10. Niveles de energía de las variables de estado del oscilador caótico Lü de orden fraccionario. 68

5.11. Encriptado de imagen con el oscilador caótico Lü de orden fraccionario: (a) Imagen a encriptar, (b) Imagen encriptada y (c) Imagen recuperada. 69

5.12. Imagen a encriptar: Leopardo.jpeg, dimensiones: 107×160 pixeles. . 69

5.13. Niveles de energía de las variables de estado del oscilador caótico Chen de orden fraccionario. 70

5.14. Encriptado de imagen con el oscilador caótico Chen de orden fraccionario: (a) Imagen a encriptar, (b) Imagen encriptada y (c) Imagen recuperada. 70

Índice de tablas

4.1. Condiciones iniciales de la red compleja con osciladores Lü de orden fraccionario. 41

4.2. Valores propios $\lambda(A)$ de la red. 46

4.3. Condiciones iniciales de la red compleja irregular con osciladores Arneodo de orden fraccionario. 47

4.4. Condiciones iniciales de la red compleja con osciladores Genesio-Tesi de orden fraccionario. 51

5.1. Valores obtenidos de los criterios de selección de las señales caóticas de la red compleja sincronizada. E_c Energía de la señal caótica, E. P. energía ponderada, J_1 y J_2 criterios de selección, A. B. ancho de banda. 58

5.2. Valores obtenidos de la red compleja con el criterio J_2. E. P. M. Energía ponderada resultante de modular las variables de estado, J_2 criterio de selección basado en el dominio de la frecuencia, $J_{2,m}$ criterio de selección basado en el dominio de la frecuencia posterior a la modulación de las variables de estado, B relación entre $J_{2,m}$ y J_2, A. B. ancho de banda. 63

Agradecimientos

A mi padre y a mi madre, por apoyarme en todo momento.

A mi asesor, el Dr. Cornelio Posadas Castillo, por guiarme adecuadamente para la elaboración de esta tesis. Por su buena disposición, comentarios y correcciones.

A mis revisores, el Dr. Miguel A. Platas Garza y el M. C. Guadalupe Evaristo Cedillo Garza, por su colaboración, por las ideas sugeridas para el beneficio de esta tesis, y por sus oportunas correcciones.

A mis profesores del DIE, por el conocimiento brindado durante mis estudios, el cual fue imprescindible para la comprensión de los temas tratados en esta tesis.

A las personas que me brindaron su ayuda sincera e incondicional, Sara Angulo Guzmán, Allan G. Soriano Sánchez y Eliezer Garza González.

Al Consejo Nacional de Ciencia y Tecnología (CONACyT), por el apoyo económico otorgado para mis estudios durante estos años de investigación.

Resumen

Otoniel García Sepúlveda.

Candidato para obtener el grado de Maestría en Ciencias de la Ingeniería Eléctrica.

Universidad Autónoma de Nuevo León.

Facultad de Ingeniería Mecánica y Eléctrica.

Título del estudio: Encriptado de datos con osciladores caóticos de orden fraccionario.

Número de páginas: 76.

Objetivos y método de estudio: El objetivo es contribuir al encriptado de datos utilizando osciladores caóticos de orden fraccionario obteniendo un encriptado más eficaz con respecto al obtenido con osciladores caóticos de orden entero.

Este trabajo de investigación trata sobre encriptado caótico utilizando osciladores de orden fraccionario. Para la realización de esta tesis fue necesaria la comprensión de los temas sobre caos, sincronía, ecuaciones diferenciales de orden fraccionario y encriptado caótico.

Firma del asesor: _____

Dr. Cornelio Posadas Castillo

Capítulo 1

Introducción

En este capítulo se mencionan tanto el objetivo general de la tesis como también los objetivos particulares. Se presenta también la motivación que nos exhortó para la realización de esta investigación.

1.1 Motivación

El encriptado caótico mediante el uso de sistemas enteros previene que una persona no deseada descifre el mensaje encriptado si es que ésta desconoce los parámetros del oscilador usado y las condiciones iniciales del mismo. En el caso de haber utilizado estos osciladores dentro de una red, esta tercer persona desconoce la topología de la red y su configuración.

En este trabajo de tesis, se propone utilizar los osciladores caóticos de orden fraccionario (orden no entero), porque, añadido a todas las interrogantes antes mencionadas, esta persona indeseada, desconoce también el orden de las derivadas del sistema en cada una de las ecuaciónes que describen su comportamiento, el cual, es totalmente diferente para un valor distinto en el orden de sus derivadas.

1.2 Objetivo general

Contribuir al encriptado de datos utilizando osciladores caóticos de orden fraccionario obteniendo un encriptamiento más eficaz con respecto al obtenido con osciladores caóticos de orden entero.

1.3 Objetivos particulares

- Explorar las diferentes técnicas y aplicaciones para sincronizar osciladores caóticos de orden fraccionario.
- Aplicar la sincronización de este tipo de redes al cifrado de información. Cifrado caótico aditivo, por conmutación entre atractores caóticos o por técnicas de modulación paramétrica.

1.4 Antecedentes

En esta sección se mencionan algunos conceptos importantes como sincronía, caos y criptología, así como también algunos de sus antecedentes históricos. También se explica a que se refiere el encriptamiento caótico y se muestran visualmente los diagramas del metodo de encriptado utilizado en esta investigación.

1.4.1 Sincronía

La palabra sincronía proviene de la etimología griega *syn* que significa "con, a la vez"y de la mitología griega Chronos ($X\rho\hat{o}\nu o\varsigma$) que significa "tiempo". En conjunto, el término se refiere a la coincidencia en el tiempo de ciertos sucesos o fenómenos.

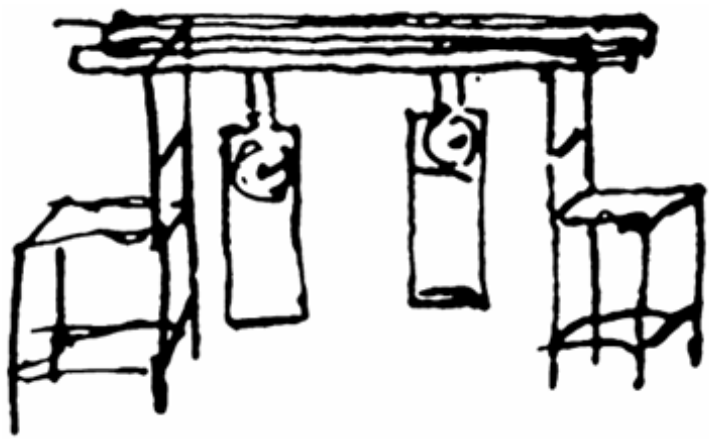


Figura 1.1: Dibujo hecho por Christiaan Hyugens ilustrando su experimento.

El fenómeno de la sincronía fue registrado en el año de 1665 por el físico holandés Christian Huygens, quien pudo observar accidentalmente que los péndulos de dos relojes de sala colocados uno al lado del otro oscilaban simultáneamente sin variación. Por más que intentaba evitar la sincronía alterándolas oscilaciones de los péndulos, Huygens comprobó que, al cabo de sólo media hora, estos volvían a sincronizar sus movimientos. Con este experimento pudo concluir que ambos relojes sincronizaban sus movimientos por medio de vibraciones imperceptibles a través de la viga. Su experimento es ilustrado en la Figura 1.1.

La sincronía se puede observar en el mundo real de muchas maneras. La Figura 1.2 muestra algunos ejemplos de sincronía tales como en el vuelo de las aves Figura 1.2a, en la industria Figura 1.2b, en actividades deportivas como las artes marciales Figura 1.2c, en las artes escénicas como en la danza Figura 1.2d, entre otros.

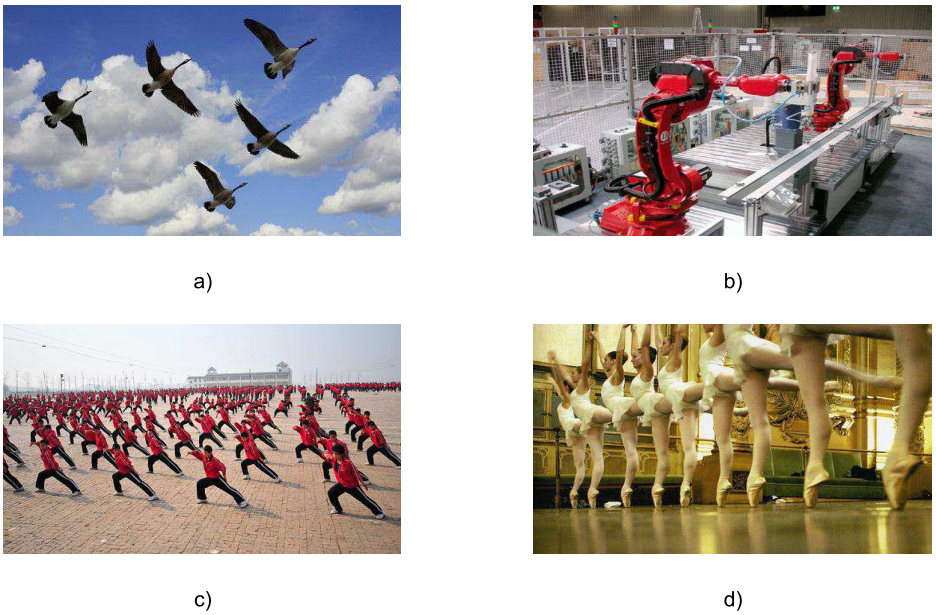


Figura 1.2: Ejemplos de sincronía en el mundo real.

1.4.2 Caos

La palabra caos deriva del griego $X\acute{a}o\varsigma$, que significa "abertura"y generalmente la asociamos a un comportamiento desordenado. Sin embargo, este comportamiento está bien definido por ecuaciones que lo hacen de naturaleza determinística, es aperiódico y es extremadamente sensible a las condiciones iniciales.

En 1963, el matemático y meteorólogo Edward Lorenz introdujo el termino de atractores extraños y el de efecto mariposa, siendo uno de los pioneros de la teoría del caos. Lorenz intentaba predecir el comportamiento de la atmosfera por medio de un modelo matemático y al observar las soluciones de éste, se dio cuenta de que si había cambios muy pequeños en sus condiciones iniciales, las soluciones que obtenía eran completamente divergentes.

El conjunto de ecuaciónes diferenciales del oscilador de Lorenz de orden entero está dado por [1]:

$$\begin{cases} \dot{x} &= \alpha(y-x), \\ \dot{y} &= x(\rho-z)-y, \\ \dot{z} &= xy-\beta z. \end{cases} \tag{1.1}$$

con valores de parámetros $\alpha = 10$, $\rho = 28$, $\beta = 8/3$.

La Figura 1.3 muestra el atractor de este sistema conocido como el atractor de Lorenz.

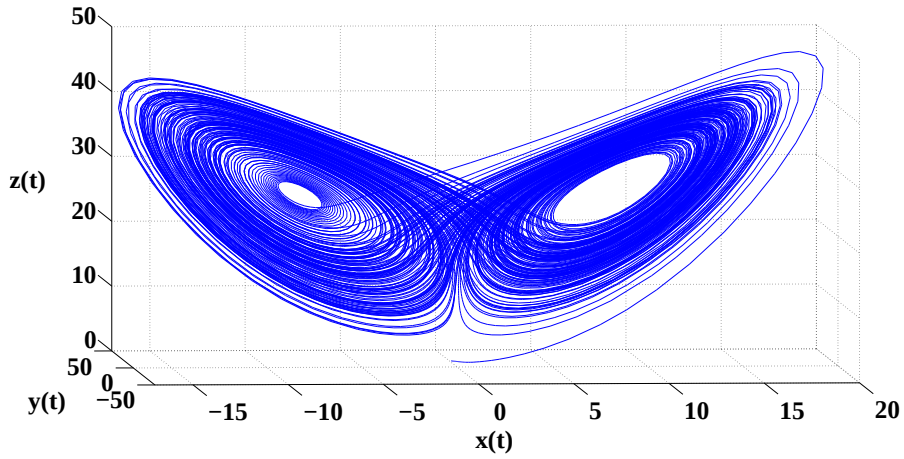


Figura 1.3: Atractor caótico de Lorenz de orden entero.

Para que un sistema sea considerado como caótico, debe cumplir con ciertas características presentadas a continuación:

- **Dinámica no lineal:** El cáos solo se presenta en sistemas no lineales de orden tres como mínimo.
- **Sensibilidad a condiciones iniciales:** El sistema se comporta de una manera totalmente diferente para condiciones iniciales distintas.

- **Exponentes de Lyapunov positivos:** Los exponentes de Lyapunov describen el grado de divergencia de dos trayectorias con vectores de estado inicial muy cercanos uno del otro. La presencia de exponentes de Lyapunov positivos en sistemas de ecuaciones diferenciales no lineales indican un comportamiento caótico. El sistema debe tener al menos un exponente de Lyapunov positivo para ser considerado caótico.

- **Atractor extraño:** Está vinculado al comportamiento caótico. Describe la forma en la que evolucionan las trayectorias del sistema.

- **Dimensión fractal en los atractores:** Es la medida de su grado de irregularidad. Una dimensión fractal mayor significa que el fractal es más irregular.

El efecto resultante de variar las condiciones iniciales del sistema caótico de Lorenz de orden entero es mostrado en la Figura 1.4 y 1.5. En la Figura 1.4 se observan los diferentes atractores a los que converge el sistema para diferentes condiciones iniciales. La Figura 1.5 muestra la evolución temporal de los estados de ambos osciladores, en la que se puede observar, como los estados del oscilador son diferentes uno del otro para una variación relativamente pequeña en sus condiciones iniciales.

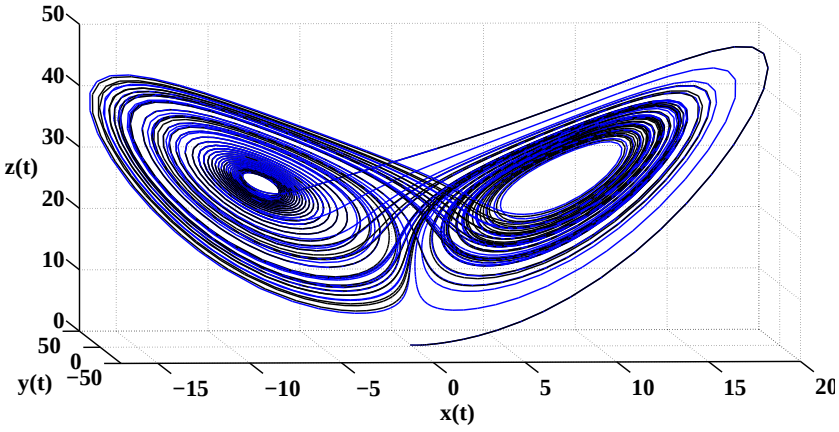


Figura 1.4: Atractores caóticos de los dos osciladores Lorenz de orden entero con diferentes condiciones iniciales. $(x_1(0), y_1(0), z_1(0)) = (-0.1, 0.5, 0.2)$, $(x_2(0), y_2(0), z_2(0)) = (-0.11, 0.5, 0.2)$.

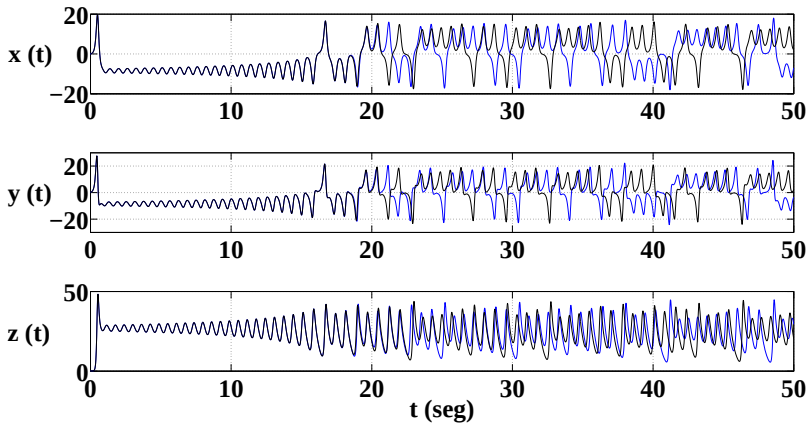


Figura 1.5: Evolución temporal de los estados de dos osciladores caóticos Lorenz de orden entero con condiciones iniciales diferentes. $(x_1(0), y_1(0), z_1(0)) = (-0.1, 0.5, 0.2)$, $(x_2(0), y_2(0), z_2(0)) = (-0.11, 0.5, 0.2)$.

1.4.3 Criptología

La palabra criptología proviene de la raíz griega *krypto* que significa "oculto"y logos que significa "discurso"y es la disciplina que se encarga de estudiar la escritura secreta o mensajes que han sido procesados de alguna manera y convertirlos en difíciles o casi imposibles de leer por personas que no han sido autorizadas.

Las áreas que estudia la criptología son la criptografía y el criptoanálisis:

- Criptografía: es la ciencia de cifrar y descifrar mensajes mediante el uso de técnicas que hacen posible el intercambio de información de manera que sólo puede ser vista por el emisor y el receptor.
- Criptoanálisis: es el estudio de los métodos que hacen posible el cifrado y descifrado de la información.

Algunos ejemplos de métodos de cifrado antigüo son el cifrado de la escitala Espartana, el cifrado de Julio César, el cifrado de Polybios, el cifrado de Vinegère,

entre otros. A continuación se describe uno de los cifrados antigüos más conocidos y se expone un ejemplo.

1.4.3.1 Cifrado de Vigenère

Este cifrado esta basado en el cifrado de César el cual remplaza la letra original del texto por otra letra que se encuentra más adelante dependiendo de un número que sería fijo para todas las letras. En el cifrado de Vigenère, es necesaria una palabra clave además del mensaje que se desea cifrar. Las letras del alfabeto forman una tabla, conocida como tabla de Vigenère mostrada en la Figura 1.6. La primera fila le corresponde al mensaje a cifrar y la primera columna le corresponde a la palabra clave. El mensaje cifrado será la intersección entre cada una de las letras de la palabra clave y el mensaje.

Por ejemplo, para cifrar la palabra "Investigación", utilizando la palabra "ciencia"como clave, se debe repetir la palabra clave, tal que tenga el mismo número de letras que el mensaje: INVESTIGACION, CIENCIACIENCI. El primer punto de intersección es $(C, I) = K$, el segundo punto de intersección es $(I, N) = U$, asi sucesivamente. El mensaje cifrado es: KUZQUBIIIGUQU, de acuerdo con la tabla de Vigenère.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y

Figura 1.6: Tabla de Vigenère utilizada para cifrar mensajes.

1.4.4 Encriptado caótico

El encriptado caótico se refiere al cifrado de un mensaje utilizando las dinámicas proporcionadas por un oscilador caótico. En este trabajo de tesis los osciladores caóticos utilizado son de orden fraccionario.

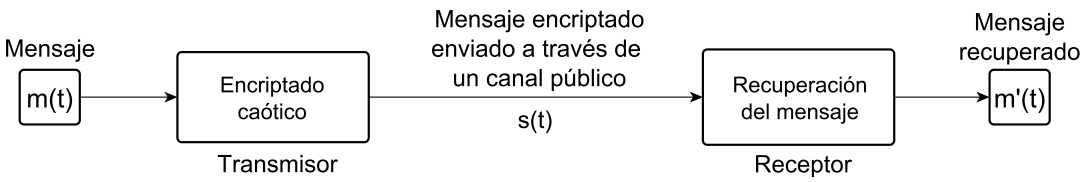


Figura 1.7: Proceso de encriptado, transmisión y recuperación del mensaje.

La Figura 1.7 muestra el procedimiento básico del encriptado caótico. El mensaje $m(t)$ es encriptado utilizando las dinámicas del oscilador caótico presente en el transmisor. El mensaje encriptado $s(t)$ es enviado a travéz de un canal público al receptor. El receptor se encarga de recuperar el mensaje $m'(t)$.

1.5 Organización del trabajo de tesis

A continuación se da a conocer un panorama general de este trabajo de tesis.

En el Capítulo 2 se aborda el tema de las redes complejas, se presenta un antecedente histórico sobre el nacimiento de la teoría de grafos y su relación con las redes complejas, asi como también, se mencionan las características más importantes de las redes complejas, las topologias y configuraciones en las que pueden presentarse, y la metodología para calcular la matriz de acoplamiento en cada una de ellas.

En el Capítulo 3 se dan preliminares matemáticos del cálculo fraccionario, y se exhiben algunos de los osciladores caóticos más famosos en su modalidad fraccionaria, mostrando los prarámetros para los cuáles presentan un comportamiento caótico, asi como también sus atractores caóticos y la evolución en el tiempo de sus varibables de estado.

En el Capítulo 4 se habla sobre la metodología que se utilizó en este trabajo de tesis para lograr sincronizar redes complejas utilizando algunos de los oscilado-

res caóticos de orden fraccionario presentados en el Capítulo 3. Se llevó a cabo la sincronización de una red compleja regular en configuración bidireccional, la sincronización de una red irregular en configuración bidireccional, y la sincronización de una red regular en configuración maestro-esclavo. Se dan a conocer las condiciónes iniciales utilizadas para cada red compleja, las leyes de control utilizadas, los valores propios de la matriz de acoplamiento y la fuerza de acoplamiento necesaria para alcanzar la sincronía de acuerdo con la teoría de Wang y Chen. También se muestra la evolución temporal de algunos estados de la red, permitiendo al lector observar como las dinámicas de la red convergen a un mismo valor en un tiempo finito. Se muestran también algunos planos de fase de la red, y gráficas que muestran el error convergiendo a cero entre dos estados seleccionados arbitrariamente de la red , probando así, que dichas variables de estado tienden a tener dinámicas idénticas en un tiempo finito. Con todo esto, y cumpliendo con la teoría de Wang y Chen, se prueba que las redes con las que se trabajó en esta tesis alcanzan la sincronía.

En el Capítulo 5 se proporcióna la información más importante de este trabajo de investigación. Se aborda el tema del encriptado caótico de datos utilizando las variables de estado proporcionadas por osciladores caóticos de orden fraccionario. Se mencionan los criterios utilizados para la selección de la variable de estado, con la cual se llevó a cabo el encriptado del mensaje. Se presentan dos diferentes casos de estudio: encriptado de voz y encriptado de imagen. En ambos casos se presenta una tabla con los valores de la energía proporcionada por los estados de un oscilador presente en la red sincronizada, se muestran los valores de los criterios de selección y el ancho de banda de las señales caóticas, asi como también los resultados obtenidos del encriptamiento del mensaje con la señal caótica seleccionada. En el caso de encriptamiento caótico de voz, se llevó a cabo el proceso de modulación de las variables de estado del oscilador caótico fraccionario, con la finalidad de mejorar la calidad de encriptamiento, obteniendo una nueva tabla con valores más favorables para el encriptado del mensaje. La correlación cruzada y los coeficientes de correlación de Pearson fueron utilizados para visualizar la diferencia en la calidad del encriptado.

Así mismo, se aborda el tema de encriptado de imágenes. La metodología que se puso en práctica para ocultar el mensaje es presentada. Se exhiben los resultados visualmente de la imagen a encriptar, la señal encriptada, y la imagen recuperada.

En el Capítulo 6 se mencionan las conclusiones y aportaciones más destacadas de este trabajo de tesis. Se proponen también, opciónes y caminos a seguir para trabajos a futuro.

Capítulo 2

Redes complejas

En este capítulo se aborda el tema de las redes complejas, se presentan sus características, topologías y configuraciónes más importantes. También se exponen algunos antecedentes históricos y definiciónes que fueron importantes para este trabajo de tesis.

2.1 Antecedentes históricos

2.1.1 Los siete puentes de Königsberg

El río Pregel que rodea a la isla Kneiphof en Königsberg, se divide en dos brazos. Sobre los brazos estaban construidos siete puentes y para los habitantes era motivo de distracción descubrir un itinerario de manera tal, que pudieran regresar al punto de partida, después de haber cruzado por los siete puentes pero pasando sólo una vez por cada uno de ellos. Leonhard Euler un matemático y físico suizo, estudió el asunto, representando las distintas zonas A, B, C y D por medio de puntos, mientras que los puentes estaban representados por líneas. A la figura la llamó grafo, a los puntos los llamó vértices y a las líneas las denominó aristas. Estudió si una figura se podía dibujar con un solo trazo, sin levantar el lápiz del papel y sin pasar

dos veces por el mismo sitio.

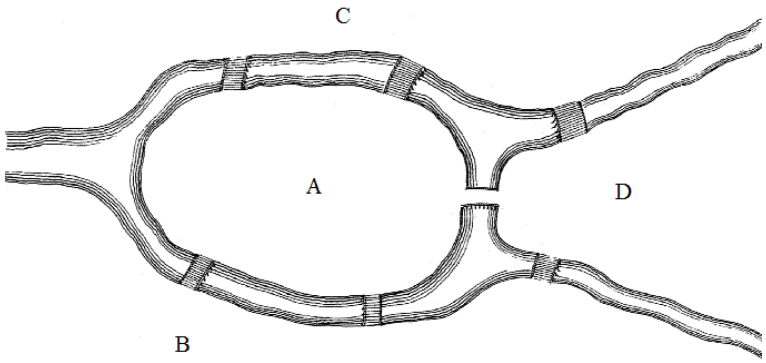


Figura 2.1: Esquema de los siete puendes de Königsberg en donde se pueden apreciar las zonas A, B, C y D.

Llegó a la siguiente conclusión:

1. Es imposible si hay más de dos vértices impares.
2. Es posible cuando:
   a) Todos los vértices son pares y el punto de partida puede ser cualquiera.
   b) Cuando no hay más de dos vértices impares y en este caso el comienzo del recorrido comienza en uno de ellos y termina en el otro. (Se dice que un vértice es impar si de él parten un número impar de caminos).

A la isla A llegan 5 puentes; a la orilla B llegan 3 puentes; a la orilla C llegan 3 puentes y a la isla D llegan 3 puentes, por tanto, según las conclusiones anteriores, el problema no tiene solución.

Este estudio de Euler dio origen a la teoría de grafos que se emplean en el estudio de las redes complejas, circuitos eléctricos, en problemas de transporte, etc [2].

2.2 Redes en el mundo real

Las redes están presentes en el mundo real de diversas maneras ya sea en la naturaleza como en la vida cotidiana. Algunos ejemplos de redes presentes en el mundo real se mencionan a continuación. Las redes de información como las citas en los artículos académicos y/o la WWW (World Wide Web). Redes tecnológicas como la red de energía eléctrica, redes telefónicas, redes utilizadas por oficinas postales o compañias de paquetería. Redes biológicas como las redes de regulación genética, redes de proteínas, redes metabólicas, redes neuronales, y redes tróficas. Redes de comunicaión como las redes sociales, redes de vías aéreas, redes de carreteras, redes comerciales entre otras [3].

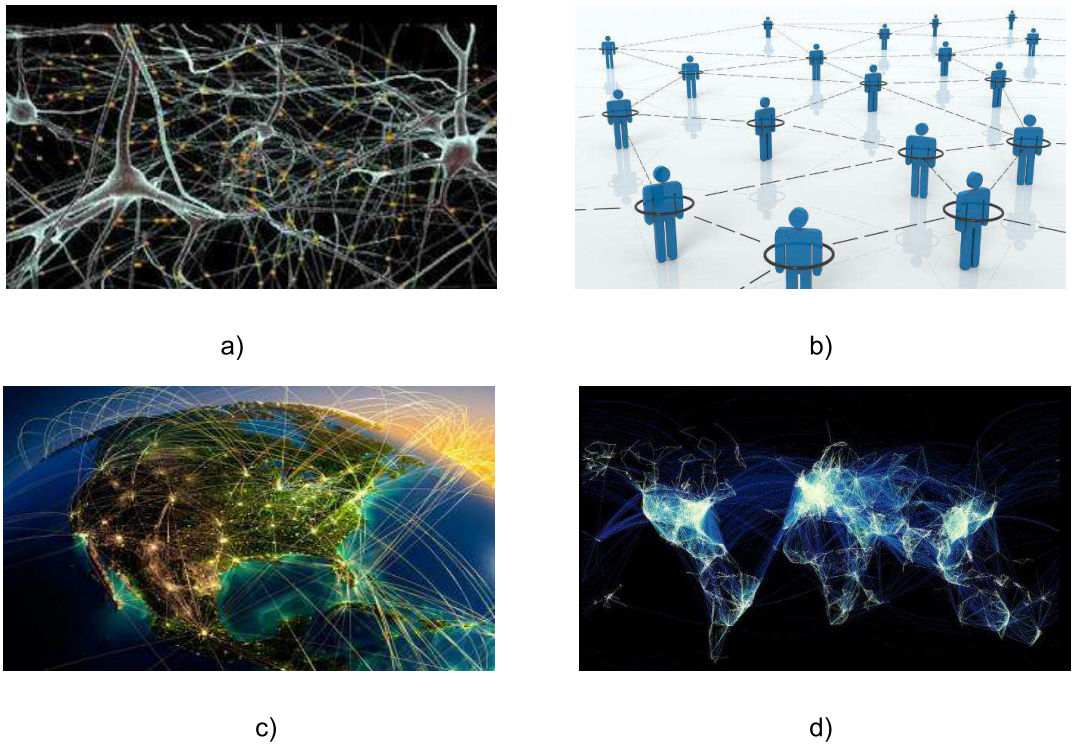


Figura 2.2: Ejemplos de redes en la naturaleza: a) redes neuronales, b) redes sociales, c) redes comerciales, d) redes de vias aéreas.

La Figura 2.2 muestra algunos ejemplos: redes neuronales, Figura 2.2a; redes sociales, Figura 2.2b; redes comerciales a nivel mundial, Figura 2.2c; y redes de vias aéreas en el mundo, Figura 2.2d.

2.3 Definiciones

Desde el punto de vista matemático, una red puede ser modelada formalmente por medio de un grafo, de la siguiente forma [4]:

Definición 2.1 *Una red R consiste de un conjunto de nodos $V = v_1, v_2, \ldots, v_N$, y un conjunto de parejas ordenadas $V = (v_i, v_j) \subset V \times V$. Cada pareja ordenada (v_i, v_j) se llama conexión dirigida del nodo v_j. La red R se llama no dirigida si para cada pareja $(v_i, v_j) \in V$ también existe una pareja $(v_j, v_i) \in V$. De lo contrario se le llama dirigida. A los nodos que están directamente conectados a un nodo v_i se les llama vecinos. Finalmente, el número k_i de vecinos del nodo v_i, es decir el número de conexiones de v_i se le llama conectividad de v_i y el promedio de estas conectividades, $\langle k \rangle = N^{-1} \sum_{i=1}^{N} k_i$ es la conectividad de la red, donde N denota al número de nodos que existen en la red.*

Antes de definir las redes complejas, se enuncian las características más destacables que presentan los sistemas complejos:

- Están compuestos de muchas partes que interactúan entre sí (nodos).
- Cada parte tiene estructura interna propia y está encargada de una tarea especifica.
- Presentan comportamientos emergentes al no existir un nodo maestro.

Una vez dicho esto, definimos a una red compleja vista como un sistema complejo, como un conjunto de nodos interconectados que interactúan entre sí, donde

cada nodo es la unidad fundamental de la red que contiene información detallada de la red [5], [6].

2.4 Topologías de las redes complejas

La topología es la disposición o la forma en la que están acoplados o conectados los nodos de una red, mientras que la configuración es el tipo de conexión que determina el flujo de información entre los nodos.

Las redes complejas se clasifican en dos grupos: estructurales y no estructurales. En esta investigación se consideraron unicamente las redes estructurales, las cuales se dividen en dos grupos de acuerdo con la topología que presentan: regular o irregular, y cada una de ellas en dos grupos más, de acuerdo con su configuración: bidireccional o maestro-esclavo. A continuación se describen las configuraciónes maestro-esclavo y bidireccional, así como las topologías regular e irregular.

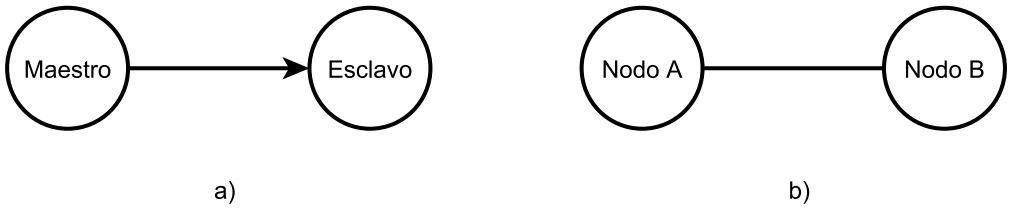


Figura 2.3: a) Configuración maestro-esclavo: la información fluye unidireccionalmente del nodo maestro al nodo esclavo b) configuración bidireccional: la información fluye del nodo A al nodo B y viceversa.

La Figura 2.3 muestra los dos tipos de configuración que puede presentar una red estructural. En la configuración maestro-esclavo (con nodo aislado), o también llamada unidireccional, el nodo maestro impone su dinámica a los demás nodos de la red, es decir, el nodo maestro se encarga de enviar información a los nodos esclavos, los cuales solo reciben información adoptando el comportamiento del nodo maestro.

En la configuracón bidireccional (sin nodo aislado), los nodos interconectados en la red envían y reciben información. Al no existir un nodo maestro del cual adoptar un comportamiento específico, surge un comportamiento o dinámica emergente, la cual, es totalmente diferente a cualquiera de las dinámicas de los nodos presentes en la red.

2.4.1 Topología regular

Dentro de la topología regular existen tres ecenarios de acoplamiento: acoplamiento global, acoplamiento anillo y acoplamiento estrella. El acoplamiento de la red esta representado por una matriz de acoplamiento $A = (a_{ij}) \in \Re^{N\times N}$. Si existe una conexión entre el nodo i y el nodo j el elemento $a_{ij} = 1$ en caso contrario entonces $a_{ij} = 0$ $(i \neq j)$ [5]. Los elementos de la diagonal principal de la matriz de acoplamiento A están definidos de la siguiente forma:

$$a_{ii} = -\sum_{j=1, j\neq i}^{N} a_{ij} = -\sum_{j=1, j\neq i}^{N} a_{ji}, \quad \text{para} \;\; i = 1, 2, \ldots, N. \tag{2.1}$$

A continuación, se describen los tres tipos de conexión o acoplamiento que pueden presentarse entre los nodos de una red con topología regular.

2.4.1.1 Acoplamiento global

En este tipo de redes, dos nodos cualquiera están conectados directamente, es decir, cada uno de sus nodos tiene una conexión con el resto de los nodos. La Figura 2.4 muestra una red compleja en acoplamiento global y configuración bidireccional.

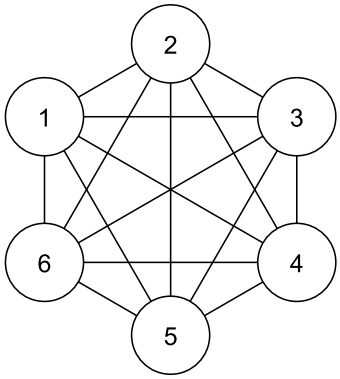


Figura 2.4: Red compleja en acoplamiento global y configuración bidireccional.

La matriz de acoplamiento correspondiente a este tipo de red esta dada por:

$$A = \begin{pmatrix} -N+1 & 1 & 1 & \cdots & 1 \\ 1 & -N+1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & 1 & \ddots & 1 \\ 1 & 1 & 1 & \cdots & -N+1 \end{pmatrix}. \tag{2.2}$$

Uno de los valores propios de esta matriz de acoplamiento está ubicado en 0 y los demás en $-N$. El segundo valor propio mayor de esta matriz (2.2) es $\lambda_2 = -N$ el cual decrece a medida que $N \to \infty$, esto es:

$$\lim_{N\to\infty} \lambda_2 = -\infty. \tag{2.3}$$

2.4.1.2 Acoplamiento anillo

En este tipo de acoplamiento los nodos están ubicados uno después de otro formando un anillo y están acoplados, cada uno, a sus nodos más cercanos. Cada nodo i está conectado a sus nodos vecinos $i \pm 1, i \pm 2, \ldots, i \pm K/2$, donde K es

un número par. La Figura 2.5 muestra una red compleja en acoplamiento anillo y configuración bidireccional.

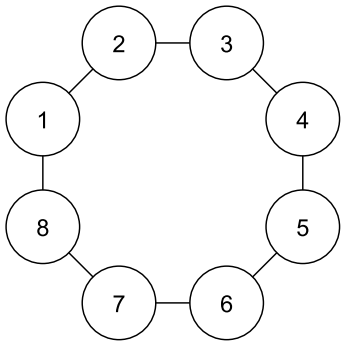


Figura 2.5: Red compleja en acoplamiento anillo y configuración bidireccional.

La matriz de acoplamiento correspondiente a este tipo de red esta dada por:

$$A = \begin{pmatrix} -K & 1 & 0 & \cdots & 1 \\ 1 & -K & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 1 & \ddots & 1 \\ 1 & 0 & 1 & \cdots & -K \end{pmatrix}. \tag{2.4}$$

El segundo valor propio de esta matriz de acoplamiento esta dado por:

$$\lambda_2 = -4 \sum_{j=1}^{K/2} \text{sen}^2(\frac{j\pi}{N}), \tag{2.5}$$

para un valor fijo de K, de la ecuación (2.5) se tiene que:

$$\lim_{N \to \infty} \lambda_2 = 0. \tag{2.6}$$

2.4.1.3 Acoplamiento estrella

En este tipo de acoplamiento, un nodo esta colocado al centro de la red, al cual todos los nodos restantes estan conectados. La Figura 2.6 muestra una red compleja en acoplamiento estrella y configuración bidireccional.

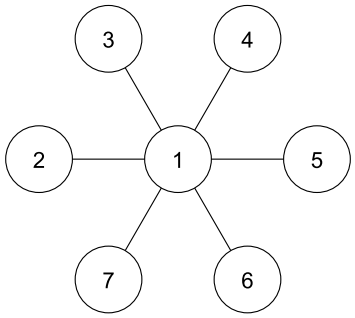


Figura 2.6: Red compleja en acoplamiento estrella y configuración bidireccional.

La matriz de acoplamiento correspondiente a este tipo de red esta dada por:

$$A = \begin{pmatrix} -N+1 & 1 & \cdots & 1 & 1 \\ 1 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 0 & \cdots & -1 & 0 \\ 1 & 0 & \cdots & 0 & -1 \end{pmatrix}. \tag{2.7}$$

Los valores propios de la matriz de acoplamiento son $\lambda(A) = \{0, -N, -1, \ldots, -1\}$, por lo tanto el segundo valor propio mayor de A es $\lambda_2 = -1$.

2.4.2 Topología irregular

Las redes irregulares no presentan un patrón definido en sus conexiónes pudiendo generarse diferentes redes con un mismo número de nodos. Debido a esto no

existe una matriz de acoplamiento general para este tipo de topología, por lo que es necesario generarla y/o ajustarla a la red.

Un ejemplo de una red irregular se propone a continuación con finalidad demostrativa.

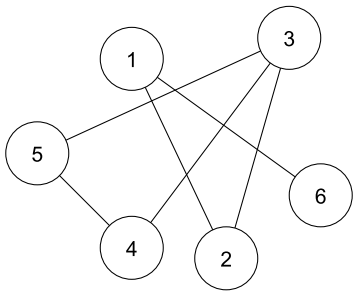


Figura 2.7: Red compleja en topología irregular y configuración bidireccional.

La matriz de acoplamiento para este caso en particular es la siguiente:

$$A = \begin{pmatrix} -2 & 1 & 0 & 0 & 0 & 1 \\ 1 & -2 & 1 & 0 & 0 & 0 \\ 0 & 1 & -3 & 1 & 1 & 0 \\ 0 & 0 & 1 & -2 & 1 & 0 \\ 0 & 0 & 1 & 1 & -2 & 0 \\ 1 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}. \tag{2.8}$$

Los valores propios de la matriz de la matriz de acoplamiento son $\lambda(A) = \{0, -0.3249, -1.4608, -3, -3, -4.2143\}$.

Capítulo 3

Osciladores caóticos de orden fraccionario

En este capítulo se exponen algunos osciladores caóticos de orden fraccionario, así como lo parámetros para los cuales presentan un comportamiento caótico. Se presentan también, preliminares matemáticos relacionados al cálculo fraccionario, utilizados para las simulaciónes que se llevaron a cabo en este trabajo de investigación.

El cálculo fraccionario, permite describir y modelar un objeto real de forma más precisa que los métodos "enteros"clásicos [7]. La razón principal de utilizar estos modelos de orden entero, era la ausencia de métodos para la solución de ecuaciones diferenciales de orden fraccionario [8]. En la actualidad existen muchos métodos para la aproximación de la derivada e integral fraccionaria [7].

Las contribuciónes más importantes fueron aportadas por Leibiniz, L'Hospital, S. F. Lacroix, L. Euler, J. B. J. Fourier, N. H. Abel, J. Liouville entre $1965 - 1974$. Otros investigadores que también abordaron el tema del cálculo fraccionario son mencionados tales como J. L. Lagrange, P. S. Laplace, O. Heaveside, M. Riesz, H. Weyl, K. B. Oldham, J. Spanier, A. K. Grünwald, M. Caputo, G. F. B. Riemann, I. Podlubny and many others [7]

3.1 Preliminares matemáticos del cálculo fraccionario

El cálculo fraccionario es una generalización de integración y diferenciación a un operador fundamental de orden no entero ${}_aD_t^\alpha$, donde a y t son los límites de la operación y $\alpha \in \Re$. El operador integro-diferencial continuo de [7] y [9] está definido como:

$${}_aD_t^\alpha = \begin{cases} \frac{d^\alpha}{dt^\alpha}, \alpha > 0, \\ 1, \alpha = 0, \\ \int_a^t (d\tau)^{-\alpha}, \alpha < 0. \end{cases} \tag{3.1}$$

Existen tres definiciones comunes de la derivada fraccionaria: definición de Caputo [7], definición de Grüwald-Letnikov [9], y la definición de Riemann-Liouville [10]. Estas definiciónes son equivalentes bajo ciertas condiciónes [9]. La definición de Grünwald-Letnikov para derivadas no enteras está dada por la siguiente ecuación:

$${}_aD_t^\alpha f(t) = \lim_{h \to 0} h^{-\alpha} \sum_{j=0}^{\frac{t-a}{h}} (-1)^j \begin{pmatrix} \alpha \\ j \end{pmatrix} f(t - jh). \tag{3.2}$$

Para el calculo de los coeficientes binomiales, la relación entre la función *Gamma* de Euler y el factorial es usada y está definida como:

$$\begin{pmatrix} \alpha \\ j \end{pmatrix} = \frac{\alpha!}{j!(\alpha - j)!} = \frac{\Gamma(\alpha + 1)}{\Gamma(j + 1)\Gamma(\alpha - j + 1)}, \tag{3.3}$$

Para la solución numérica de las derivadas de orden fraccionario, la relación derivada de la definición de Grünwald-Letnikov [7], [9] dada por la siguiente expresion es utilizada:

$$_{k-L_m/h}D^q_{t_k} f(t) \approx h^{-q} \sum_{j=0}^{k} (-1)^j \begin{pmatrix} \alpha \\ j \end{pmatrix} f(t_k - j), \tag{3.4}$$

donde L_m es la "longitud de memoria", $t_k = kh$, h es el paso de tiempo del calculo y $(-1)^j \begin{pmatrix} q \\ j \end{pmatrix}$ son los coeficientes binomiales $c_j^{(q)} (j = 0, 1, \ldots)$. El cálculo de los coeficientes binomiales está dado por:

$$\begin{aligned} c_0^{(q)} &= 1, \\ c_j^{(q)} &= \left(1 - \frac{1+q}{j}\right) c_{j-1}^{(q)}. \end{aligned} \tag{3.5}$$

La solución general de la ecuación diferencial fraccionaria

$$_aD^q_t y(t) = f(y(t), t), \tag{3.6}$$

puede ser expresada como sigue:

$$y(t_k) = f(y(t_k), t_k) h^q - \sum_{j=v}^{k} c_j^{(q)} y(t_k - j). \tag{3.7}$$

En las secciónes $3.1 - 3.6$ se presentan algunos ejemplos de osciladores de orden fraccionario en régimen caótico, así como sus atractores caóticos y la evolución temporal de sus estados.

3.2 Oscilador caótico Lorenz de orden fraccionario

Llamado así en honor a Edward Lorenz, quien, en el año de 1963, tratando de predecir el clima mediante un modelo matemático, descubrió que bajo diferentes

condiciones iniciales, este sistema se comportaba de una manera totalmente diferente. El modelo matemático de este oscilador fraccionario es el siguiente [7]:

$$\begin{cases} {}_0D_t^{q_1}x(t) &= \sigma(y(t)-x(t)), \\ {}_0D_t^{q_2}y(t) &= x(t)(\rho - z(t)) - y(t), \\ {}_0D_t^{q_3}z(t) &= x(t)y(t) - \beta z(t). \end{cases} \tag{3.8}$$

Los parámetros bajo los cuales este sistema presenta un comportamiento caótico son: $\sigma = 10, \rho = 28, \beta = 8/3$, con valores de $q_1 = q_2 = q_3 = 0.995$ en sus derivadas.

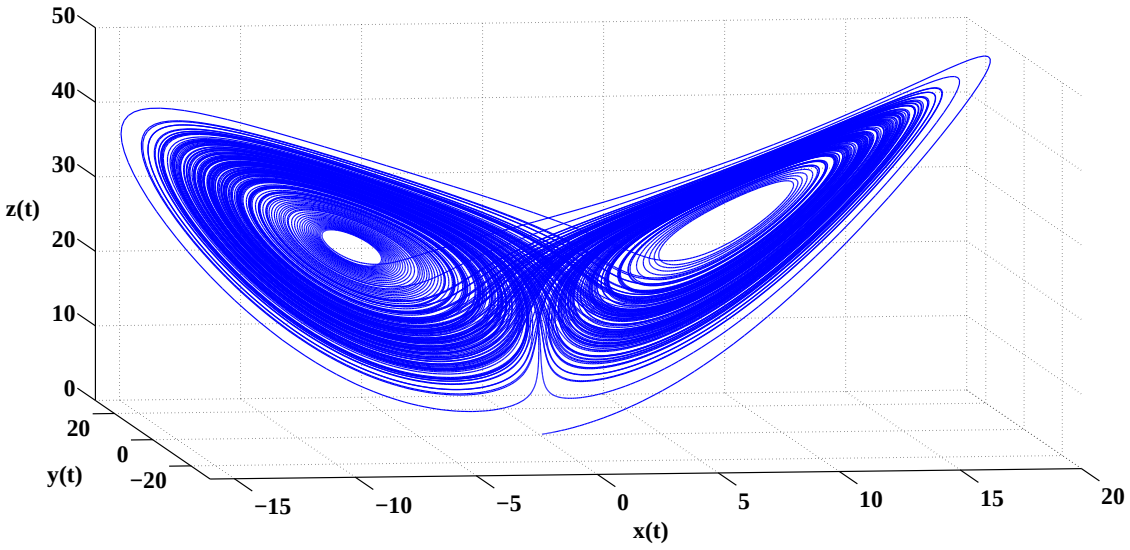


Figura 3.1: Atractor caótico del oscilador Lorenz de orden fraccionario para parámetros: $\sigma = 10, \rho = 28, \beta = 8/3$, derivadas: $q_1 = q_2 = q_3 = 0.995$, y condiciones iniciales: $(x(0), y(0), z(0)) = (0.1, 0.1, 0.1)$.

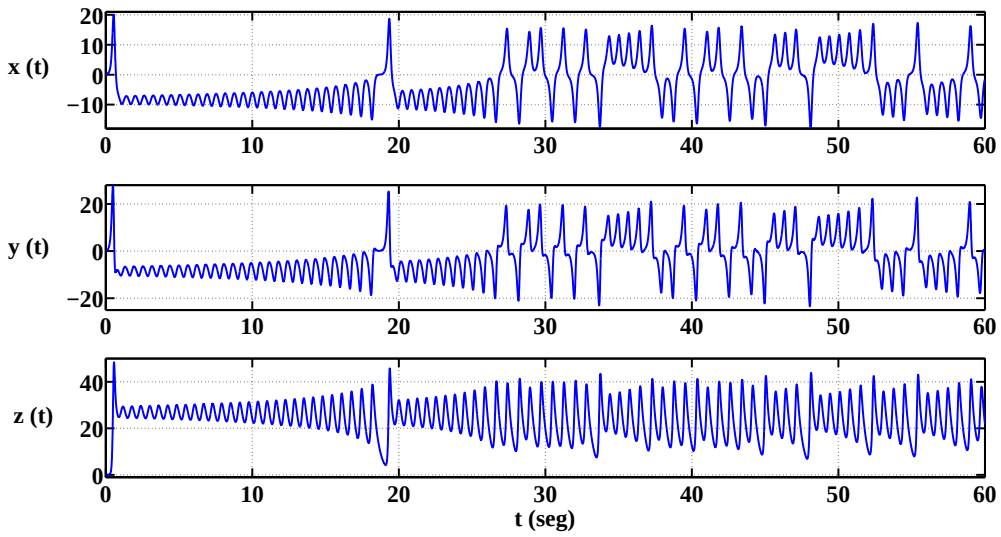


Figura 3.2: Evolución temporal de los estados del oscilador caótico Lorenz de orden fraccionario.

La Figura 3.1 muestra el atractor caótico de este oscilador. La evolución temporal de sus estados es mostrada en la Figura 3.2.

3.3 Oscilador caótico Rössler de orden fraccionario

En 1976, Otto Rössler propuso que este oscilador presentaba un atractor extraño. El conjunto de ecuaciones que describen el comportamiento de este oscilador fraccionario es el siguiente [7]:

$$\begin{cases} {}_0D_t^{q_1}x(t) &= -y(t) - z(t), \\ {}_0D_t^{q_2}y(t) &= x(t) + ay(t), \\ {}_0D_t^{q_3}z(t) &= b + z(t)(x(t) - c). \end{cases} \tag{3.9}$$

Para los parámetros: $a = 0.5, b = 0.2, c = 10$, y valores en sus derivadas:

$q_1 = q_2 = q_3 = 0.9$, este oscilador presenta un comportamiento caótico.

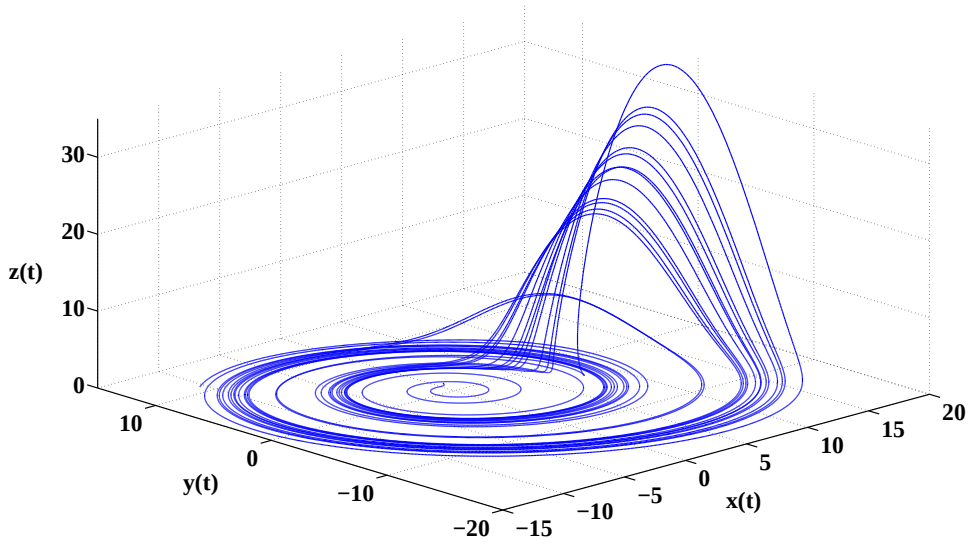


Figura 3.3: Atractor caótico del oscilador Rössler de orden fraccionario para parámetros: $a = 0.5, b = 0.2, c = 10$, derivadas: $q_1 = q_2 = q_3 = 0.9$, y condiciones iniciales: $(x(0), y(0), z(0)) = (0.5, 1.5, 0.1)$.

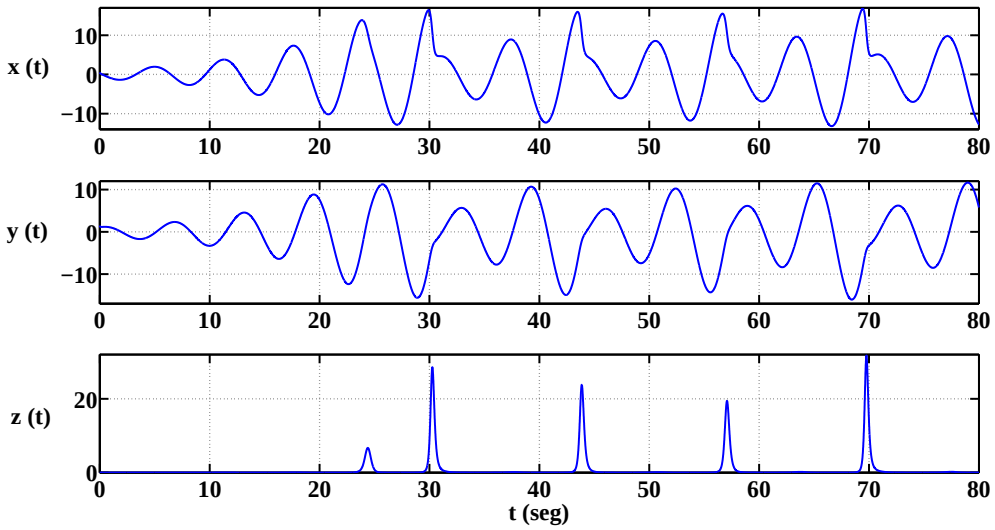


Figura 3.4: Evolución temporal de los estados del oscilador caótico Rössler de orden fraccionario.

La Figura 3.3 muestra el atractor caótico de este oscilador. La Figura 3.4 muestra la evolución temporal de sus estados.

3.4 Oscilador caótico Genesio-Tesi de orden fraccionario

El conjunto de ecuaciones que describen el comportamiento de este sistema fraccionario es el siguiente [7]:

$$\begin{cases} {}_0D_t^{q_1}x(t) &= y(t), \\ {}_0D_t^{q_2}y(t) &= z(t), \\ {}_0D_t^{q_3}z(t) &= -b_1x(t) - b_2y(t) - b_3z(t) + b_4x^2(t). \end{cases} \tag{3.10}$$

Este oscilador es caótico para los parámetros: $b_1 = 1.1, b_2 = 1.1, b_3 = 0.45, b_4 = 1$, y valores en sus derivadas: $q_1 = 1, q_2 = 1, q_3 = 0.95$.

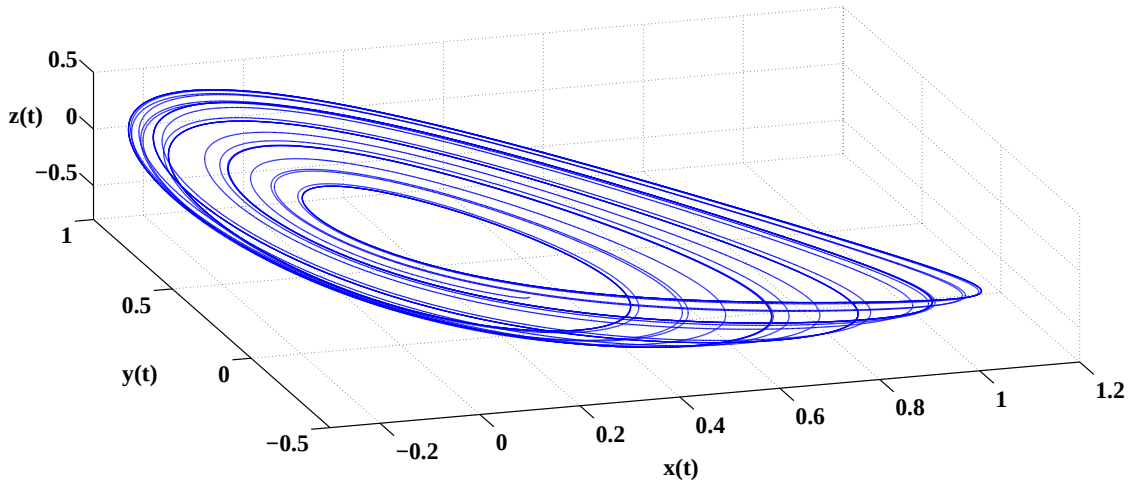


Figura 3.5: Atractor caótico del oscilador Genesio-Tesi de orden fraccionario para parámetros: $b_1 = 1.1, b_2 = 1.1, b_3 = 0.45, b_4 = 1$, derivadas: $q_1 = 1, q_2 = 1, q_3 = 0.95$, y condiciones iniciales: $(x(0), y(0), z(0)) = (0.1, -0.5, 0.2)$.

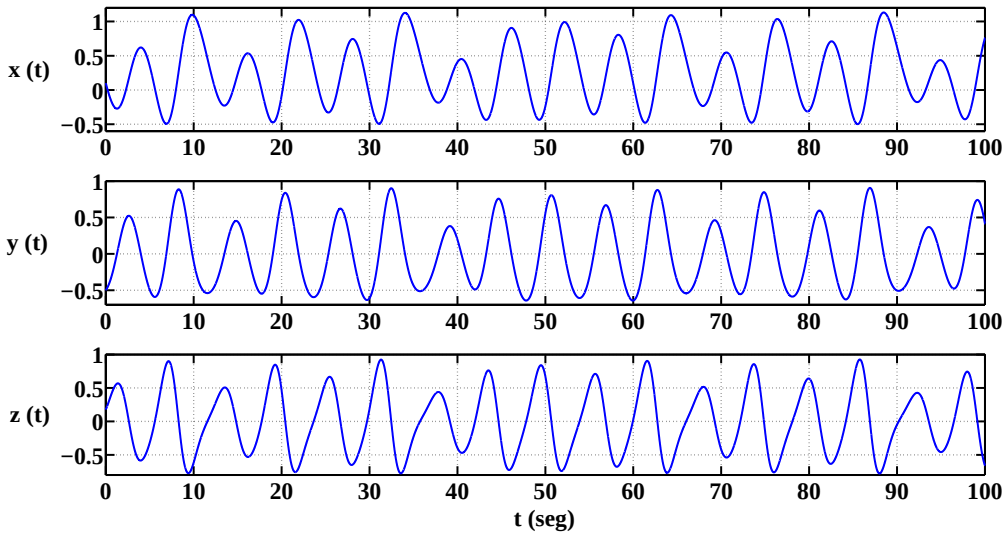


Figura 3.6: Evolución temporal de los estados del oscilador caótico Genesio-Tesi de orden fraccionario.

El atractor caótico de este oscilador se muestra en la Figura 3.5. La evolución temporal de sus estados es mostrada en la Figura 3.6.

3.5 Oscilador caótico Chen de orden fraccionario

Chen encontró un sistema autónomo tri-dimensional que no es topológicamente equivalente al sistema de Lorenz, y que también presenta un atractor caótico. El oscilador caótico Chen de orden fraccionario está descrito por el siguiente conjunto de ecuaciones [7]:

$$\begin{cases} {}_0D_t^{q_1}x(t) &= a(y(t)-x(t)), \\ {}_0D_t^{q_2}y(t) &= dx(t)-x(t)z(t)+cy(t), \\ {}_0D_t^{q_3}z(t) &= x(t)y(t)-bz(t), \end{cases} \tag{3.11}$$

y es caótico bajo los parámetros: $a = 35, b = 3, c = 28, d = -7$, y valores en sus derivadas de: $q_1 = q_2 = q_3 = 0.9$.

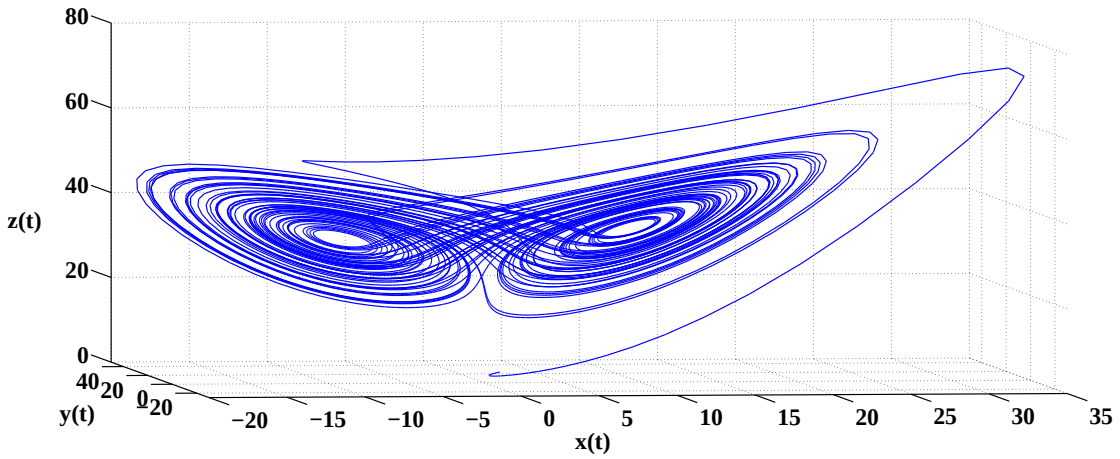


Figura 3.7: Atractor caótico del oscilador Chen de orden fraccionario para parámetros: $a = 35, b = 3, c = 28, d = -7$, derivadas: $q_1 = q_2 = q_3 = 0.9$, y condiciones iniciales: $(x(0), y(0), z(0)) = (1, 0.1, 2.5)$.

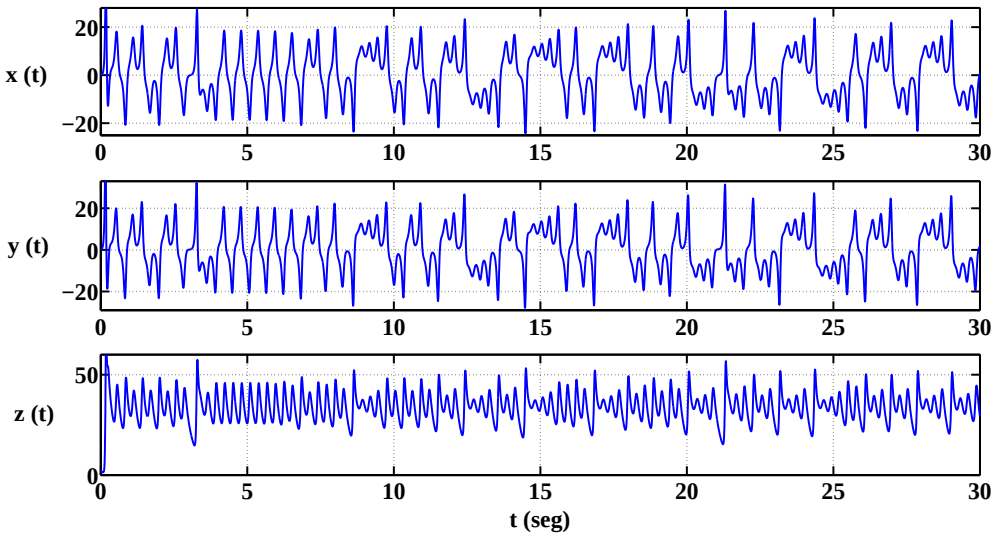


Figura 3.8: Evolución temporal de los estados del oscilador caótico Chen de orden fraccionario.

La Figura 3.7 muestra el atractor caótico de este oscilador. La Figura 3.8 muestra la evolución temporal de sus estados.

3.6 Oscilador caótico Lü de orden fraccionario

El oscilador conocido como sistema de Lü es un puente entre los sistemas de Chen y Lorenz [7]. El conjunto de ecuaciones que describe las dinámicas de este oscilador para su versión fraccionaria es el siguiente [11]:

$$\begin{cases} {}_0D_t^{q_1}x(t) &= a(y(t)-x(t)), \\ {}_0D_t^{q_2}y(t) &= -x(t)z(t)+cy(t), \\ {}_0D_t^{q_3}z(t) &= x(t)y(t)-bz(t). \end{cases} \tag{3.12}$$

Este oscilador fraccionario presenta cáos para los parámetros: $a = 36, b = 3, c = 20$, y derivadas: $q_1 = q_2 = q_3 = 0.95$ [7].

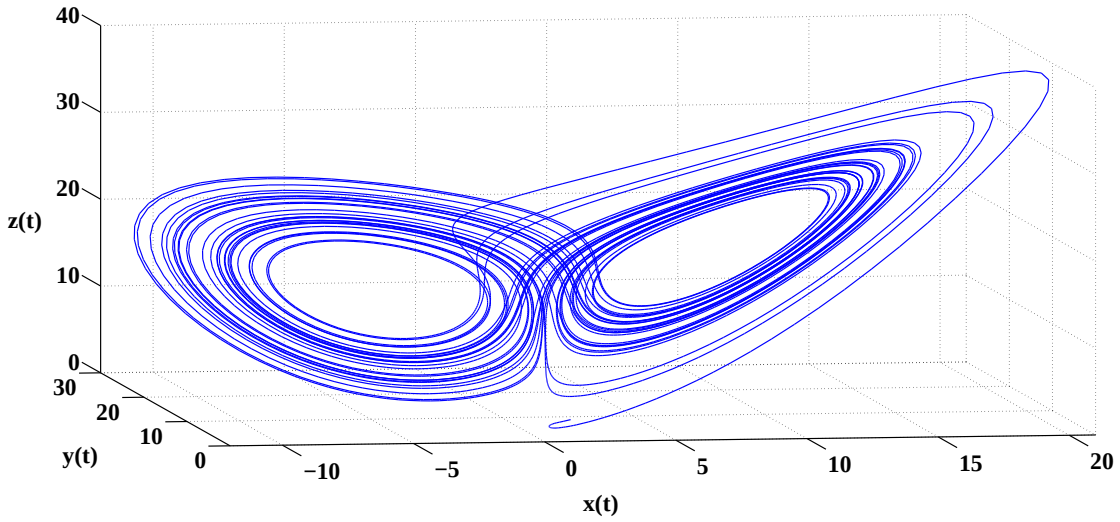


Figura 3.9: Atractor caótico del oscilador Lü de orden fraccionario para parámetros: $a = 36, b = 3, c = 20$, derivadas: $q_1 = q_2 = q_3 = 0.95$, y condiciones iniciales: $(x(0), y(0), z(0)) = (1, 0.1, 2.5)$.

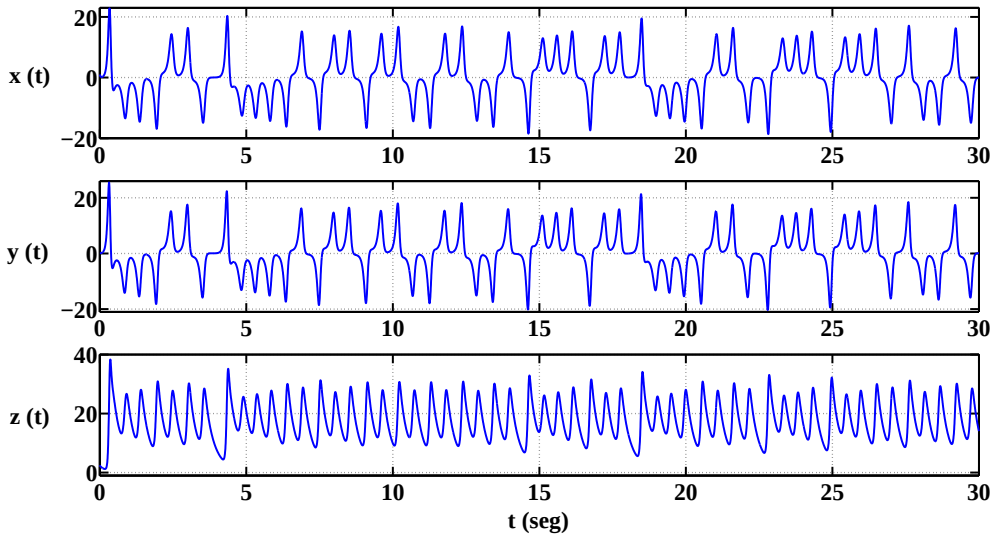


Figura 3.10: Evolución temporal de los estados del oscilador caótico Lü de orden fraccionario.

La Figura 3.9 muestra el atractor caótico de este oscilador caótico de orden fraccionario. La Figura 3.10 muestra la evolución temporal de sus estados.

3.7 Oscilador caótico Arneodo de orden fraccionario

El conjunto de ecuaciones que describen el comportamiento de este sistema fraccionario es el siguiente [7]:

$$\begin{cases} {}_0D_t^{q_1}x(t) &= y(t), \\ {}_0D_t^{q_2}y(t) &= z(t), \\ {}_0D_t^{q_3}z(t) &= -\beta_1 x(t) - \beta_2 y(t) - \beta_3 z(t) + \beta_4 x^3(t). \end{cases} \tag{3.13}$$

Este oscilador es caótico para los parámetros: $\beta_1 = -5.5, \beta_2 = 3.5, \beta_3 = 0.8, \beta_4 = -1$, y valores en sus derivadas: $q_1 = 0.97, q_2 = 0.97, q_3 = 0.96$.

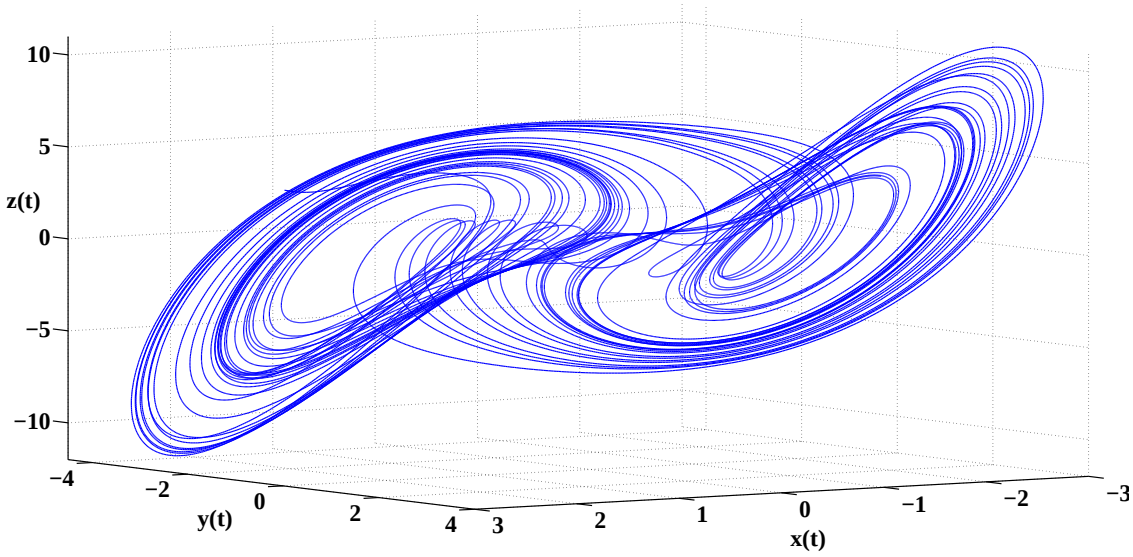


Figura 3.11: Atractor caótico del oscilador Arneodo de orden fraccionario para parámetros: $\beta_1 = -5.5, \beta_2 = 3.5, \beta_3 = 0.8, \beta_4 = -1$, derivadas: $q_1 = 0.97, q_2 = 0.97, q_3 = 0.96$, y condiciones iniciales: $(x(0), y(0), z(0)) = (2.1, -1.9, 3.2)$.

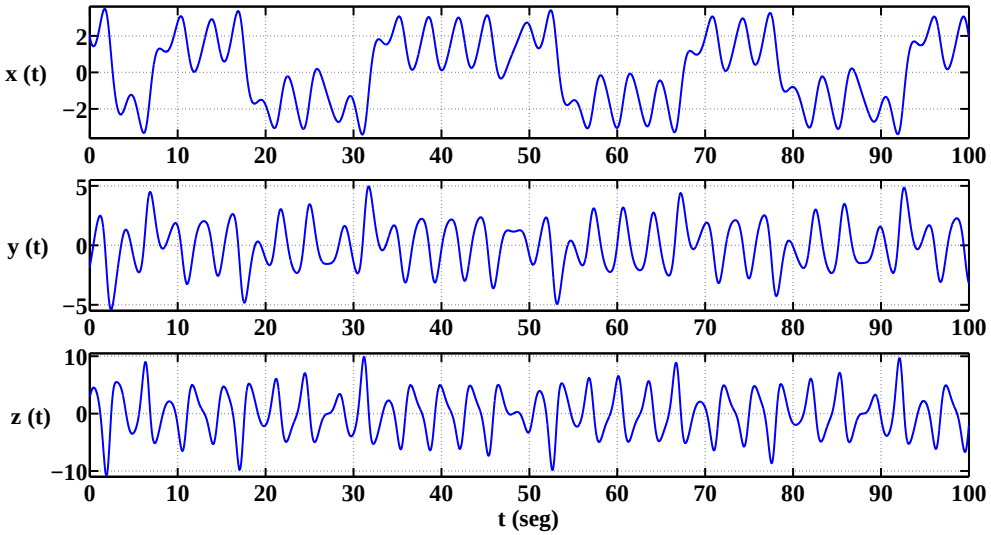


Figura 3.12: Evolución temporal de los estados del oscilador caótico Arneodo de orden fraccionario.

El atractor caótico de este oscilador se muestra en la Figura 3.11. La evolución temporal de los estados de este oscilador es mostrada en la Figura 3.12.

Capítulo 4

Sincronización de redes complejas

En este capítulo, se presentan definiciónes importantes sobre redes complejas, así como el método utilizado en este trabajo de tesis para sincronizar dichas redes. Se exponen también los resultados obtenidos de la sincronización de diferentes redes complejas, con topología regular y configuración maestro-esclavo y bidireccional, e irregular en configuración bidireccional.

Una red compleja es definida como un conjunto de nodos interconectados (dos o más). Donde cada nodo es una unidad fundamental con dinámica dependiente de la naturaleza de la red compleja. En este trabajo de investigación, los nodos que conforman las redes complejas, son osciladores caóticos de orden fraccionario.

Existen muchos métodos para alcanzar la sincronía entre dos o más osciladores, tales como el método Pecora-Carroll [12], via control de modo deslizante [13], control activo [14], control lineal [15], etc. Desde que Pecora y Carrol provaron la sincronía de sistemas caóticos, numerosos resultados fueron reportados en la literatura [16 – 18].

4.1 Definiciónes de sincronización

Considere una red de N osciladores idénticos, siendo cada oscilador un subsistema dinámico n-dimensional.

Las ecuaciones de estado en la red están definidas como sigue:

$$ {}_aD_t^{\alpha} x_{ni}(t) = f_n(x_i, t) + u_i, \qquad i = 1, 2, \ldots, N, \tag{4.1} $$

donde $x_i = (x_{1i}, x_{2i}, \ldots, x_{ni})^T \in \Re^n$ son las variables de estado del oscilador i y u_i es la ley de control definida para cada oscilador de la red como sigue [19 − 21]:

$$ u_i = c \sum_{j=1}^{N} a_{ij} \Gamma x_j, \qquad i = 1, 2, \ldots, N. \tag{4.2} $$

La constante $c > 0$ representa la fuerza de acoplamiento, y Γ es una matriz constante que define el estado por el cual los osciladores de la red están acoplados. Asuma que $\Gamma = \text{diag}(r_1, r_2, \ldots, r_n) \in \Re^n$ es una matriz diagonal con $r_n = 1$ si es el estado de acoplamiento de la red, y $r_n = 0$ en caso contrario.

La matriz $A = (a_{ij}) \in \Re^{N \times N}$ es la matriz de acoplamiento que muestra una conexión entre el oscilador i y j, si existe dicha conexión $a_{ij} = 1$, de otro modo $a_{ij} = 0$ para $i \neq j$. Los elementos de la diagonal principal de A están definidos como:

$$ a_{ii} = -\sum_{j=1, j \neq i}^{N} a_{ij} = -\sum_{j=1, j \neq i}^{N} a_{ji}, \ i = 1, 2, \ldots, N. \tag{4.3} $$

La red dinámica alcanza sincronía idéntica [22] si

$$ \lim_{t \to \infty} \| \, x(t) - \hat{x}(t) \, \| = 0. \tag{4.4} $$

A continuación se presenta el Teorema 4.1 y el Lema 1, resultado de una modifiración basada en la teoría propuesta por Wang & Chen, donde $\alpha = 1$ para el caso de ecuaciónes diferenciales de orden entero.

Teorema 4.1 *Considere la red dinámica (4.1).*
Sean:

$$0 = \lambda_1 > \lambda_2 \geq \lambda_3 \geq \ldots \geq \lambda_N. \tag{4.5}$$

Los valores propios de su matriz de acoplamiento A. Suponga que existe una matriz diagonal $\boldsymbol{D} > 0$ *de* $n \times n$ *y dos constantes* $\overline{d} < 0$ *y* $\tau > 0$*, tal que:*

$$[{}_aD_t^\alpha f(s(t)) + d\Gamma]^T \boldsymbol{D} + \boldsymbol{D}[{}_aD_t^\alpha f(s(t)) + d\Gamma] \leq -\tau \boldsymbol{I}_n, \tag{4.6}$$

para toda $d \leq \overline{d}$ *donde* $\boldsymbol{I}_n \in \Re^{n\times n}$ *es la matriz unitaria. Si, además,*

$$c\lambda_2 \leq \overline{d}. \tag{4.7}$$

Entonces, la sincronización del estado es exponencialmente estable.

Lemma 1 *Considere la red (4.1). Sea* λ_1 *el valor propio mayor no cero de la matriz de acoplamiento A. La sincronización de estados de la red (4.1) definida por* $x_1 = x_2 = \cdots = x_n$ *es asintóticamente estable, si*

$$\lambda_1 \leq -\frac{T}{c}, \tag{4.8}$$

donde $c > 0$ *es la fuerza de acoplamiento de la red y* $T > 0$ *es una constante positiva tal que cero es un punto exponencialmente estable del sistema n-dimensional*

$$\begin{aligned} {}_aD_t^\alpha z_1 &= f_1(z) - Tz_1, \\ {}_aD_t^\alpha z_2 &= f_2(z), \\ {}_aD_t^\alpha z_n &= f_n(z). \end{aligned} \tag{4.9}$$

A continuación se presentan tres ejemplos de sincronización. Se utilizaron los osciladores Lü, Arneodo y Genesio-Tesi en régimen caótico de orden fraccionario para la realización de dichos ejemplos. Los parámetros mostrados en el Capítulo 3 para cada oscilador fueron utilizados.

4.2 Sincronización de una red compleja de N osciladores caóticos Lü de orden fraccionario

Considere una red caótica de 12 osciladores Lü en régimen caóticos de orden fraccionario idénticos. La Figura 4.1 muestra esta red de topología regular con acoplamiento estrella y configuración bidireccional.

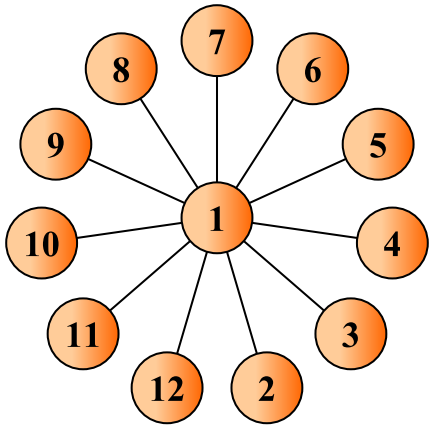


Figura 4.1: Topología de la red compleja regular con acoplamiento estrella y configuración bidireccional.

La matriz de acoplamiento A para esta red está dada por

$$A = \begin{pmatrix} -N+1 & 1 & \cdots & 1 & 1 \\ 1 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 0 & \cdots & -1 & 0 \\ 1 & 0 & \cdots & 0 & -1 \end{pmatrix}. \tag{4.10}$$

Para este caso, la matriz Γ está definida como $\Gamma = \text{diag}(0, 1, 0)$ porque los osciladores presentes en la red están acoplados mediante su segundo estado. Por lo tanto las leyes de control son aplicadas a los estados $y_i(t)$ de la red compleja. Por

medio de las ecuaciones (4.1), (4.2) y (4.3), el modelo matemático queda descrito como sigue:

$$\begin{cases} {}_0D_t^{q_1} x_i(t) &= \sigma(y_i(t) - x_i(t)), \\ {}_0D_t^{q_2} y_i(t) &= -x_i(t)z_i(t) + \gamma y_i(t) + u_{i2}, \\ {}_0D_t^{q_3} z_i(t) &= x_i(t)y_i(t) - \beta z_i(t), \end{cases} \tag{4.11}$$

donde $i = 1, 2, 3, \ldots, 12$, y representa cada oscilador de la red compleja.

Las leyes de control están dadas por

$$\begin{aligned} u_{1,2} &= c(-11y_1 + y_2 + y_3 + y_4 + y_5 + y_6 + y_7 + y_8 + y_9 + y_{10} + y_{11} + y_{12}), \\ u_{2,2} &= c(y_1 - y_2), \\ \vdots &\quad \vdots \\ u_{12,2} &= c(y_1 - y_{12}). \end{aligned} \tag{4.12}$$

Las condiciónes iniciales utilizadas para este ejemplo se muestran en la Tabla 4.1.

Tabla 4.1: Condiciones iniciales de la red compleja con osciladores Lü de orden fraccionario.

Osc. / Var.	1	2	3	4	5	6
$x(0)$	5.0003	-1.3903	2.3582	3.2618	5.0304	-4.7219
$y(0)$	-8.3208	2.1136	-6.0642	1.6353	-3.2545	-6.6089
$z(0)$	-2.9502	-8.3510	0.3310	5.4132	1.2853	4.6241
Osc. / Var.	7	8	9	10	11	12
$x(0)$	0.0002	2.9729	4.6489	-3.2578	-0.1223	4.3086
$y(0)$	-0.2746	1.7510	1.1988	5.9605	-9.7442	0.0058
$z(0)$	4.5556	6.2513	-3.4518	-8.0592	5.1025	-0.3542

De acuerdo con el Lemma 1, una fuerza de acoplamiento $c = 19$ garantiza que el Teorema 4.1 se cumple. La ecuación (4.4) se cumple, por lo tanto la sincronización de la red de la Figura 4.1 es alcanzada. La Figura 4.2 muestra la evolución temporal de algunas de las variables de estado $x_i(t), y_i(t), z_i(t)$ de la red. La Figura 4.3 muestra los planos de fase de algunos estados $y_i(t)$ de la red. La Figura 4.4 muestra algunos errores de sincronización entre los estados $y_i(t)$ de la red compleja.

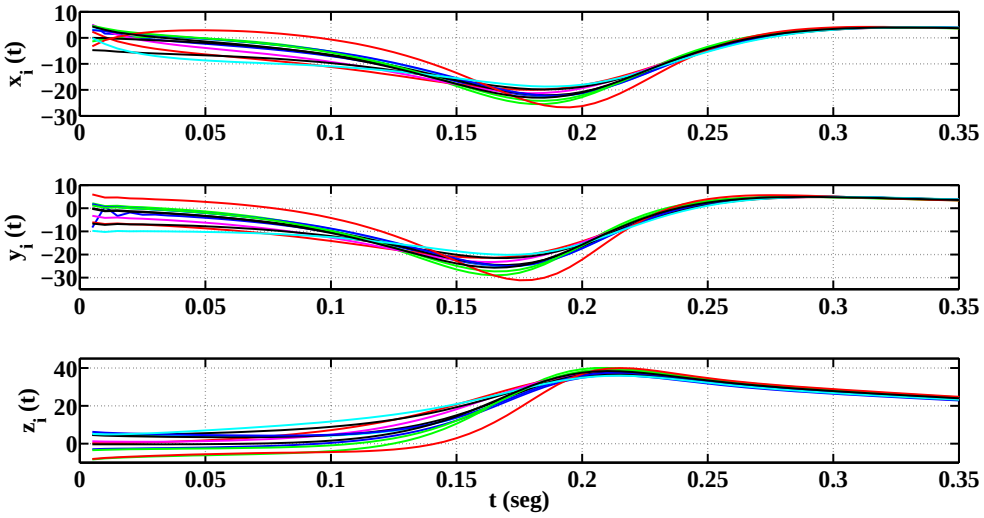


Figura 4.2: Evolución temporal de los estados $x_i(t), y_i(t), z_i(t)$, de la red mostrada en la Figura 4.1 (donde $i = 1, 2, \ldots, 6$).

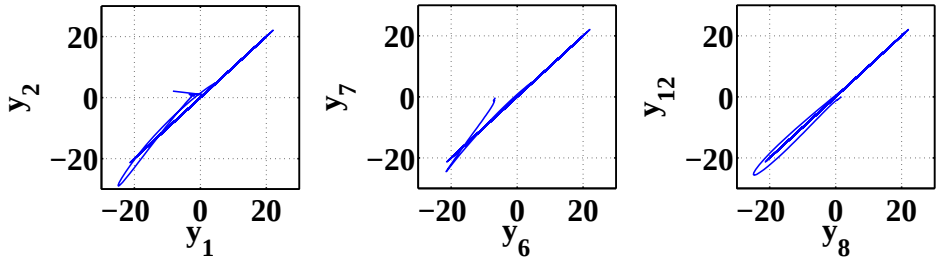


Figura 4.3: Planos de fase de los estados y_1 vs y_2, y_6 vs y_7, y_8 vs y_{12} de la red mostrada en la Figura 4.1.

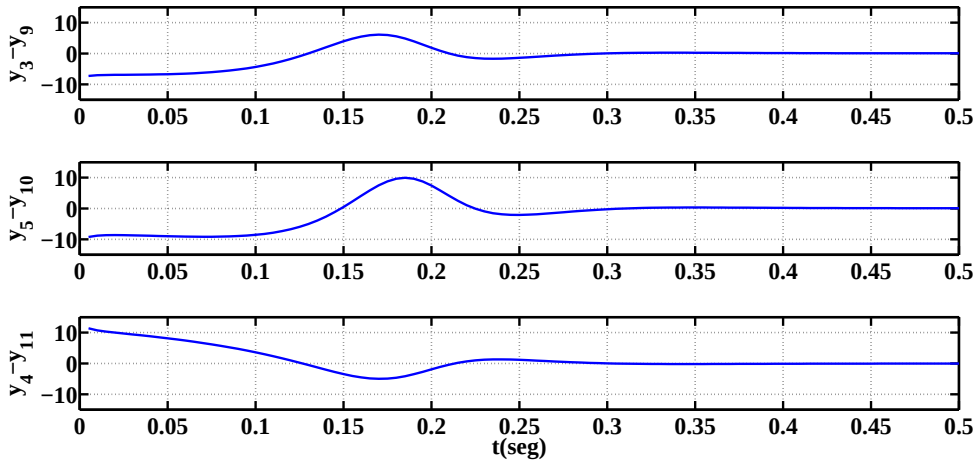


Figura 4.4: Evolución temporal del error de sincronización entre los estados $y_4 - y_{11}$, $y_5 - y_{10}$, y $y_3 - y_9$ de la red mostrada en la Figura 4.1.

4.3 Sincronización de una red compleja de N osciladores caóticos Arneodo de orden fraccionario

Considere una red irregular de 20 osciladores Arneodo en régimen caótico, idénticos, de orden fraccionario como la que se muestra en la Figura 4.5.

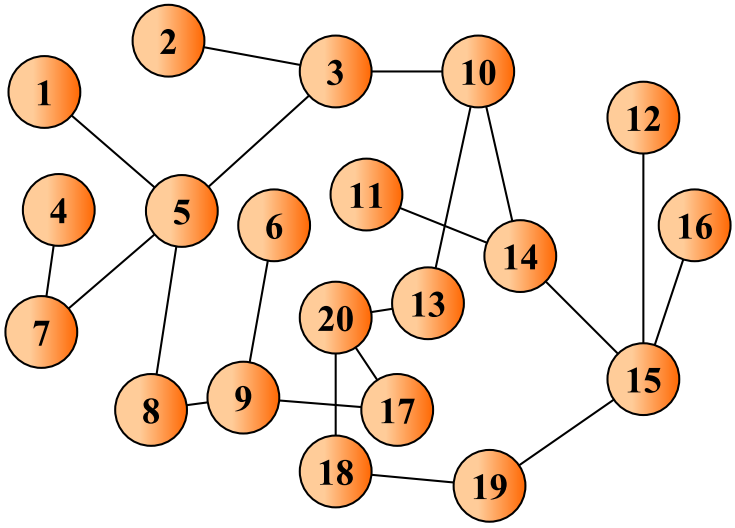


Figura 4.5: Topología de la red compleja irregular y configuración bidireccional.

Para este caso, la matriz Γ está definida como $\Gamma = \text{diag}(1, 0, 0)$ porque los osciladores de la red están acoplados mediante su primer estado. Por lo tanto las leyes de control son aplicadas a los estados $x_i(t)$ de la red compleja.

Utilizando las ecuaciones (4.1), (4.2) y (4.3), el modelo matemático queda descrito como sigue:

$$\begin{cases} {}_0D_t^{q_1} x_i(t) &= y_i(t) + u_{i1}, \\ {}_0D_t^{q_2} y_i(t) &= z_i(t), \\ {}_0D_t^{q_3} z_i(t) &= -\beta_1 x_i(t) - \beta_2 y_i(t) - \beta_3 z_i(t) + \beta_4 x_i^3(t). \end{cases} \tag{4.13}$$

donde $i = 1, 2, 3, \ldots, 20$, y representa cada oscilador de la red compleja.

Las leyes de control están dadas por

$$
\begin{aligned}
u_{1,1} &= c(-x_1 + x_5),\\
u_{2,1} &= c(-x_2 + x_3),\\
u_{3,1} &= c(x_2 - 3x_3 + x_5 + x_{10}),\\
u_{4,1} &= c(-x_4 + x_7),\\
u_{5,1} &= c(x_1 + x_3 - 4x_5 + x_7 + x_8),\\
u_{6,1} &= c(-x_6 + x_9),\\
u_{7,1} &= c(x_4 + x_5 - 2x_7),\\
u_{8,1} &= c(x_5 - 2x_8 + x_9),\\
u_{9,1} &= c(x_6 + x_8 - 3x_9 + x_{17}),\\
u_{10,1} &= c(x_3 - 3x_{10} + x_{13} + x_{14}),\\
u_{11,1} &= c(-x_{11} + x_{14}),\\
u_{12,1} &= c(-x_{12} + x_{15}),\\
u_{13,1} &= c(x_{10} - 2x_{13} + x_{20}),\\
u_{14,1} &= c(x_{10} + x_{11} - 3x_{14} + x_{15}),\\
u_{15,1} &= c(x_{12} + x_{14} - 4x_{15} + x_{16} + x_{19}),\\
u_{16,1} &= c(x_{15} - x_{16}),\\
u_{17,1} &= c(x_9 - 2x_{17} + x_{20}),\\
u_{18,1} &= c(-2x_{18} + x_{19} + x_{20}),\\
u_{19,1} &= c(x_{15} + x_{18} - 2x_{19}),\\
u_{20,1} &= c(x_{13} + x_{17} + x_{18} - 3x_{20}).
\end{aligned}
\tag{4.14}
$$

Debido al tamaño de la matriz de acoplamiento A, solo se muestran los valores propios $\lambda(A)$ de la misma en la Tabla 4.2.

Tabla 4.2: Valores propios $\lambda(A)$ de la red.

λ_1	λ_2	λ_3	λ_4	λ_5	λ_6	λ_7	λ_8	λ_9	λ_{10}
0	-0.135	-0.278	-0.424	-0.577	-0.591	-0.734	-1	-1.123	-1.374
λ_{11}	λ_{12}	λ_{13}	λ_{14}	λ_{15}	λ_{16}	λ_{17}	λ_{18}	λ_{19}	λ_{20}
-1.594	-2.277	-2.380	-2.761	-3.169	-3.752	-4.355	-4.615	-5.327	-5.526

Para este ejemplo se utilizaron las condiciones iniciales mostradas en la Tabla 4.3.

Tabla 4.3: Condiciones iniciales de la red compleja irregular con osciladores Arneodo de orden fraccionario.

Osc. / Var.	1	2	3	4	5	6	7	8	9	10
$x(0)$	2.1	4.2	3.3	1.4	-2.5	-3.6	-4.7	0.8	0.9	-0.1
$y(0)$	-1.9	3.8	2.7	1.6	4.5	-4.4	-3.3	0.2	0.1	0.9
$z(0)$	3.2	-2.8	4.0	1.7	-1.4	4.9	-4.2	-0.2	0.2	-0.6
Osc. / Var.	11	12	13	14	15	16	17	18	19	20
$x(0)$	-0.2	-0.3	-0.4	-0.5	-0.6	-0.7	-0.8	-0.9	1.0	-1.0
$y(0)$	1.0	-0.5	1.2	-0.4	-0.3	-0.4	-0.6	-0.7	-0.8	-1.3
$z(0)$	-1.3	-0.3	1.1	-0.7	0.5	0.7	-0.5	0.2	0.3	0.6

De acuerdo con el Lemma 1, una fuerza de acoplamiento $c = 15$ garantiza que el Teorema 4.1 se cumple. La ecuación (4.4) se cumple, por lo tanto la sincronización de la red de la Figura 4.5 es alcanzada. La Figura 4.6 muestra la evolución temporal de algunas de las variables de estado $x_i(t), y_i(t), z_i(t)$ de la red. La Figura 4.7 muestra los planos de fase de algunos estados $y_i(t)$ de la red. La Figura 4.8 muestra algunos errores de sincronización entre los estados $y_i(t)$ de la red compleja.

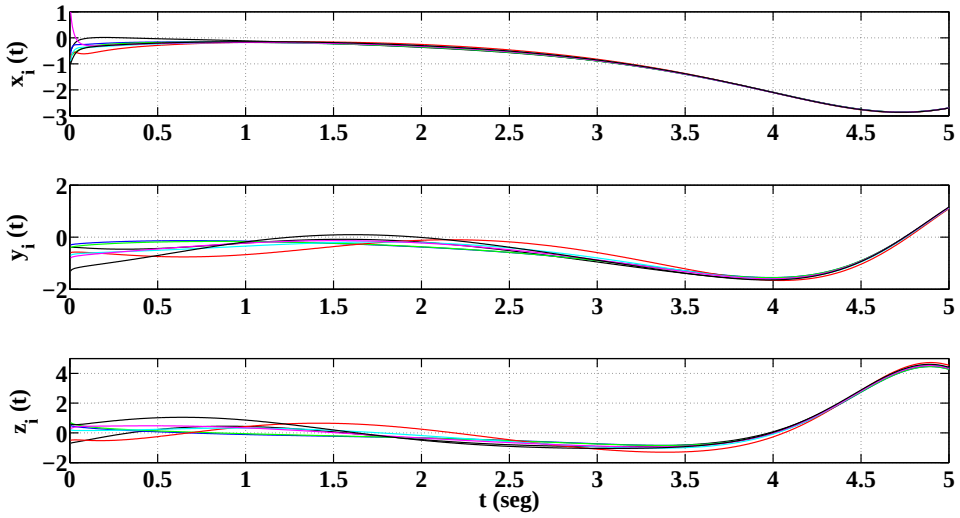


Figura 4.6: Evolución temporal de los estados $x_i(t), y_i(t), z_i(t)$ de la red mostrada en la Figura 4.5 (donde $i = 14, 15, \ldots, 20$).

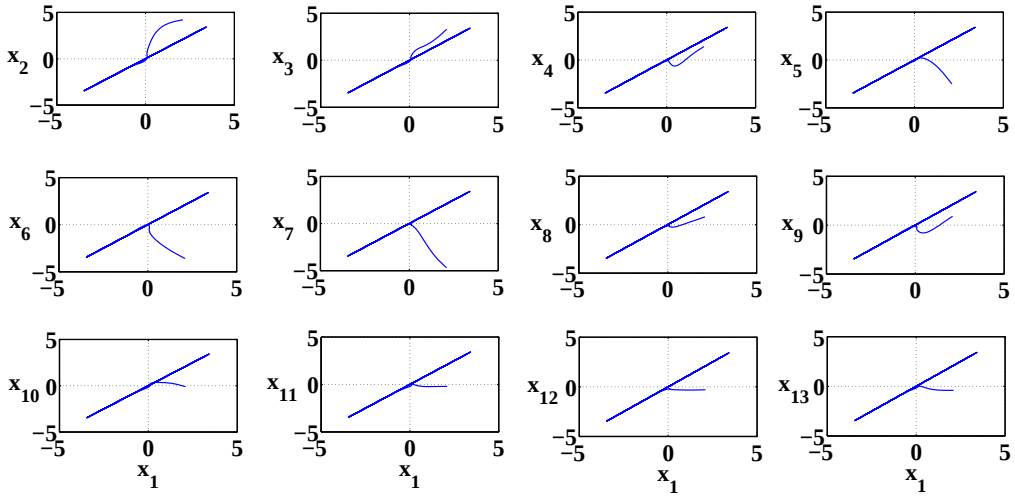


Figura 4.7: Planos de fase de los estados x_1 vs x_2, x_1 vs x_3, ..., x_1 vs x_{13} de la red mostrada en la Figura 4.5.

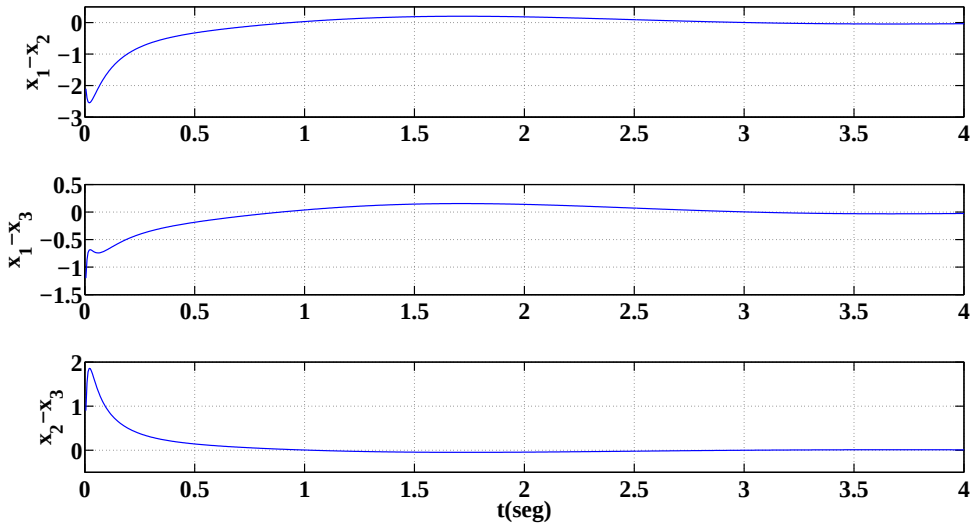


Figura 4.8: Evolución temporal del error de sincronización entre los estados $x_1 - x_2$, $x_1 - x_3$, y $x_2 - x_3$ de la red mostrada en la Figura 4.5.

4.4 Sincronización de una red compleja de N osciladores caóticos Genesio-Tesi de orden fraccionario

Considere una red de 20 osciladores Genesio-Tesi en régimen caótico, idénticos, de orden fraccionario como la que se muestra en la Figura 4.9.

Para este caso, la matriz Γ está definida como $\Gamma = \text{diag}(1, 0, 0)$ indicando que los osciladores de la red están acoplados mediante su primer estado. Por lo tanto las leyes de control son aplicadas a los estados $x_i(t)$ de la red compleja.

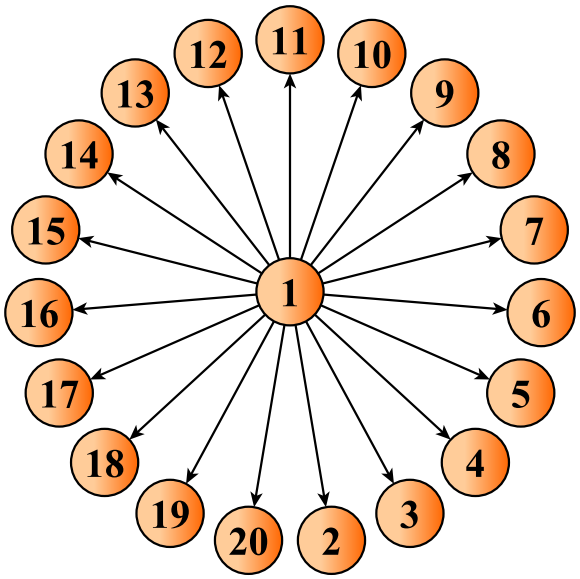


Figura 4.9: Topología de la red compleja regular y configuración maestro-esclavo.

Basado en (4.1), (4.2) y (4.3), el modelo matemático queda descrito como sigue:

$$\begin{cases} {}_0D_t^{q_1} x_i(t) &= y_i(t) + u_{i1}, \\ {}_0D_t^{q_2} y_i(t) &= z_i(t), \\ {}_0D_t^{q_3} z_i(t) &= -b_1 x_i(t) - b_2 y_i(t) - b_3 z_i(t) + b_4 x_i^2(t), \end{cases} \tag{4.15}$$

donde $i = 1, 2, 3, \ldots, 20$, y representa cada oscilador de la red compleja.

Las leyes de control están dadas por

$$\begin{aligned} u_{1,1} &= 0, \\ u_{2,1} &= c(y_1 - y_2), \\ &\vdots \quad\quad \vdots \\ u_{20,1} &= c(y_1 - y_{12}). \end{aligned} \tag{4.16}$$

Debido al tamaño de la matriz de acoplamiento, solo se muestran los valores propios de la misma, los cuales están ubicados en $\lambda(A) = \{0, -1, \ldots, -1\}$.

Para este ejemplo se utilizaron las condiciones iniciales mostradas en la Tabla 4.4.

Tabla 4.4: Condiciones iniciales de la red compleja con osciladores Genesio-Tesi de orden fraccionario.

Osc. / Var.	1	2	3	4	5	6	7	8	9	10
$x(0)$	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
$y(0)$	-0.5	-0.6	-0.7	-0.8	-0.9	-1.0	-1.1	-1.2	-1.3	-1.4
$z(0)$	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0	1.1
Osc. / Var.	11	12	13	14	15	16	17	18	19	20
$x(0)$	1.1	1.2	-0.1	-0.2	-0.3	-0.4	-0.5	-0.6	-1.0	-0.9
$y(0)$	-1.5	-1.6	0.5	0.6	0.7	0.8	0.9	1.0	0.4	0.3
$z(0)$	1.2	1.3	-0.2	-0.3	-0.4	-0.5	-0.6	-0.7	0.1	-1.4

De acuerdo con el Lemma 1, una fuerza de acoplamiento $c = 1$ garantiza que el Teorema 4.1 se cumple. La ecuación (4.4) se cumple, por lo tanto la sincronización de la red de la Figura 4.9 es alcanzada. La Figura 4.10 muestra la evolución temporal de algunas de las variables de estado $x_i(t), y_i(t), z_i(t)$ de la red. La Figura 4.11 muestra los planos de fase de algunos estados $y_i(t)$ de la red. La Figura 4.12 muestra algunos errores de sincronización entre los estados $y_i(t)$ de la red compleja.

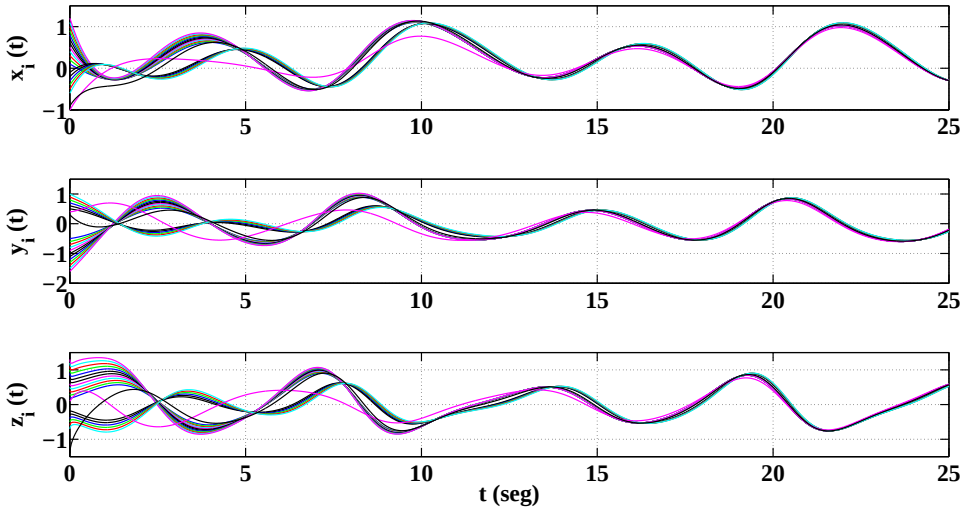


Figura 4.10: Evolución temporal de los estados $x_i(t), y_i(t), z_i(t)$, de la red mostrada en la Figura 4.9 (donde $i = 1, 2, \ldots, 20$).

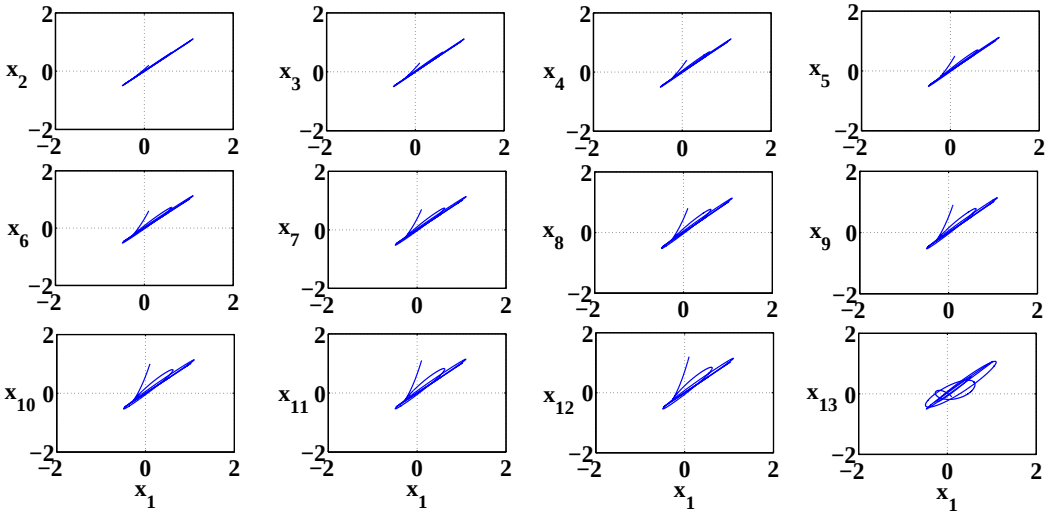


Figura 4.11: Planos de fase de los estados x_1 vs x_2, x_1 vs x_3, $\ldots$, x_1 vs x_{13} de la red mostrada en la Figura 4.9.

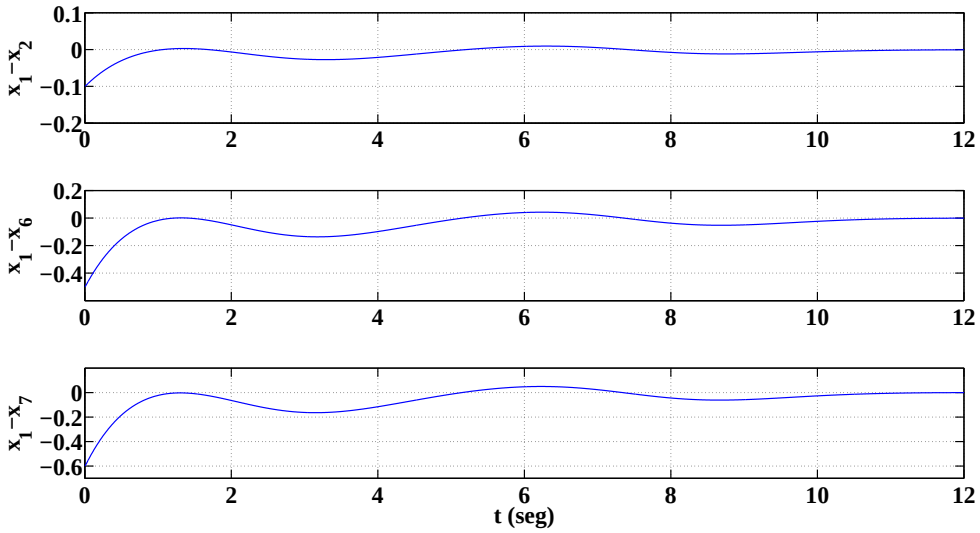


Figura 4.12: Evolución temporal del error de sincronización entre los estados $x_1 - x_2$, $x_1 - x_6$, y $x_1 - x_7$ de la red mostrada en la Figura 4.9.

Capítulo 5

Encriptado caótico de datos

En este capítulo se lleva a cabo el encriptado caótico de voz y de imagen, mediante el encriptado aditivo, también conocído como enmascaramiento. Para realizar esto, el mensaje es sumado a una de las variables de estado proporcionadas por el oscilador caótico de orden fraccionario.

Para asegurar un encriptado de máxima calidad posible con el oscilador seleccionado, se emplean dos criterios de selección basados en los níveles de energía de las señales caóticas. Desafortunadamente, ésto no siempre es suficiente para asegurar un encriptado de calidad. Se puede tener un encriptado pobre al no aprovechar la máxima cantidad de energía proporcionada por las señales caóticas del oscilador. El problema está en el hecho de que, posiblemente, la banda de frecuencias en el que está ubicada la mayor cantidad de energía de las variables de estado del oscilador caótico, en este caso de orden fraccionario, no coincide en frecuencia con la del mensaje a encriptar.

Se propone la modulación de las variables de estado del oscilador caótico utilizado, para dar solución al caso en el cual, el mensaje y las señales caóticas no coinciden en frecuencia. Con esto, se asegura que el mensaje y la señal caótica seleccionada para encriptar, coincidan en frecuencia, mejorando el resultado obtenido por los criterios de selección que serán mencionados más adelante.

La señal del mensaje original es comparada mediante la correlación cruzada y los coeficientes de Pearson, contra la señal resultante del encriptamiento caótico, antes y después de modular las variables de estado, mostrando así la diferencia en la calidad del encriptado.

5.1 Encriptado caótico con osciladores fraccionarios

Una vez que la red compleja es sincronizada, todos los osciladores tienen las mismas dinámicas. En este caso, se seleccionó el primer oscilador de la red, el cual es idéntico a los demás. La variable de estado que es utilizada para encriptar el mensaje es seleccionada de acuerdo a los siguientes criterios propuestos en [23]:

Criterio 1: selección basada en la energía de la señal caótica

$$\sum_{n=0}^{N-1} |x_c|^2 \gg \sum_{n=0}^{N-1} |x_m|^2. \tag{5.1}$$

donde $x_c(n)$ es la señal caótica muestreada, y $x_m(n)$ es la señal muestreada del mensaje. El criterio J_1 muestra cuantas veces la energía de $x_c(n)$ excede la energía de $x_m(n)$. Por lo tanto, $J_1 \gg 1$ conduce a un buen encriptado.

Criterion 2: selección basada en la energía de la señal caótica en el dominio de la frecuencia

$$\sum_{k=0}^{N-1} \eta(k)|X_c(k)|^2 \gg \sum_{k=0}^{N-1} \eta(k)|X_m|^2, \tag{5.2}$$

donde $X_c(k)$ son las muestras del espectro de la señal caótica, $X_m(k)$ son las muestras del espectro del mensaje, y $\eta(k)$ es la función de ponderación de frecuencia que selecciona la banda de frecuencias en la que se encuentra el mensaje. El criterio J_2 muestra cuantas veces la energía ponderada de $X_c(k)$ excede la energía ponderada

de $X_m(k)$ en una banda seleccionada de frecuencias si $\alpha(k) = 1$ en $K \in [k_1, k_2]$. De este modo, $J_2 \gg 1$ resulta en un buen encriptado en la banda de frecuencias en donde está localizado el mensaje.

5.1.1 Encriptado caótico de voz

En esta sección, se presentan los resultados obtenidos de encriptar el mensaje utilizando una variable de estado del oscilador antes y despúes de ser modulada. La variable de estado con la cual se encripta el mensaje es seleccionada en base a los criterios J_1 y J_2. En este caso, nuestro mensaje es una grabación de voz: "encriptado de datos con osciladores caóticos de orden fraccionario", localizado en una banda de frecuencias entre 0.3 kHz - 3 kHz [24] con una frecuencia de muestreo $F_s = 11.025$ kHz.

Es importante señalar que J_2 indica que para un valor mucho mayor a 1 tendremos un mejor encriptado, sin embargo, no indica un valor mínimo necesario de J_2 para el cual el mensaje sea inaudible. Se obtuvieron resultados en los cuáles el mensaje era audible antes y después de modular las variables de estado, dichos resultados no son mostrados en la tesis ya que se dió solución a este problema atenuando el mensaje para incrementar más el valor de J_2. Los resultados mostrados a continuación fueron obtenidos después de atenuar el mensaje por un factor de 0.1.

La Figura 5.1 muestra los niveles de energía proporcionados por las variables de estado del oscilador fraccionario.

Por medio de un filtro pasa banda se obtuvieron los niveles de energía de las variables de estado, en la banda de frecuencias del mensaje. Uno de los filtros más básicos es el conocido como filtro de Butterworth, el cual ofrece una respuesta en frecuencia lo más cercana posible a la de un filtro ideal. Este filtro en modo pasabanda es mostrado en la Figura 5.2. Los niveles de energía ponderada se muestran en la Figura 5.3.

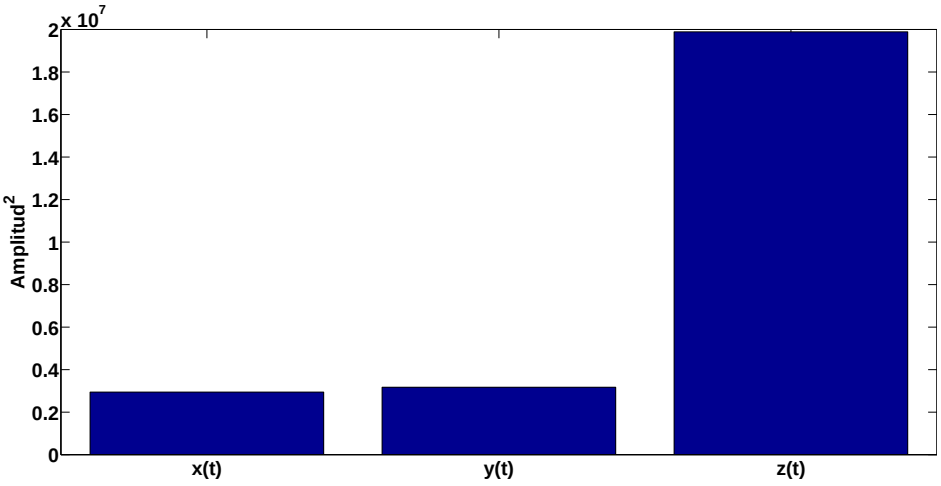


Figura 5.1: Niveles de energía de las variables de estado del primer oscilador (Lü de orden fraccionario) de la red.

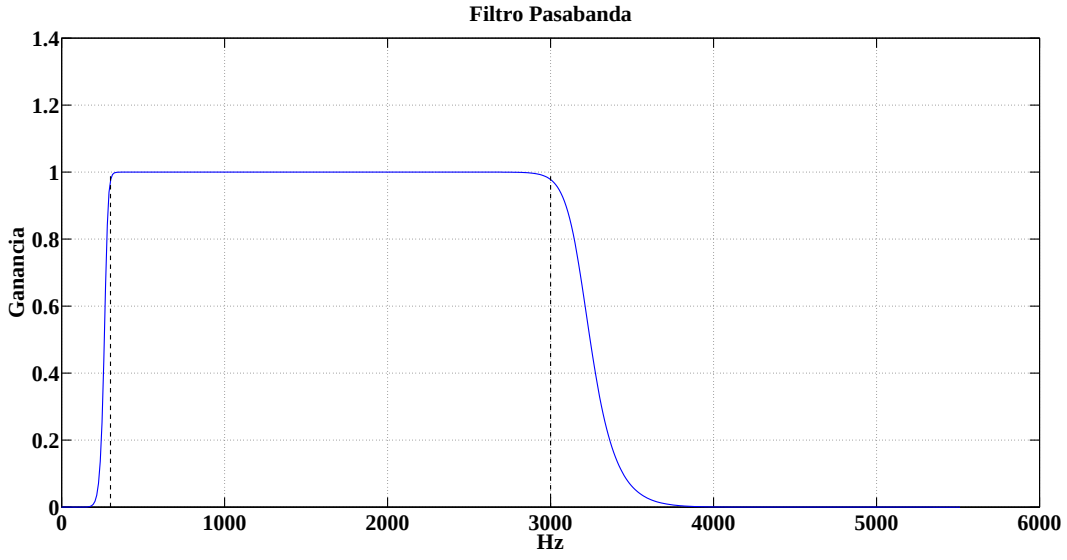


Figura 5.2: Filtro pasa banda de Butterworth, utilizado para filtrar las señales de este capítulo.

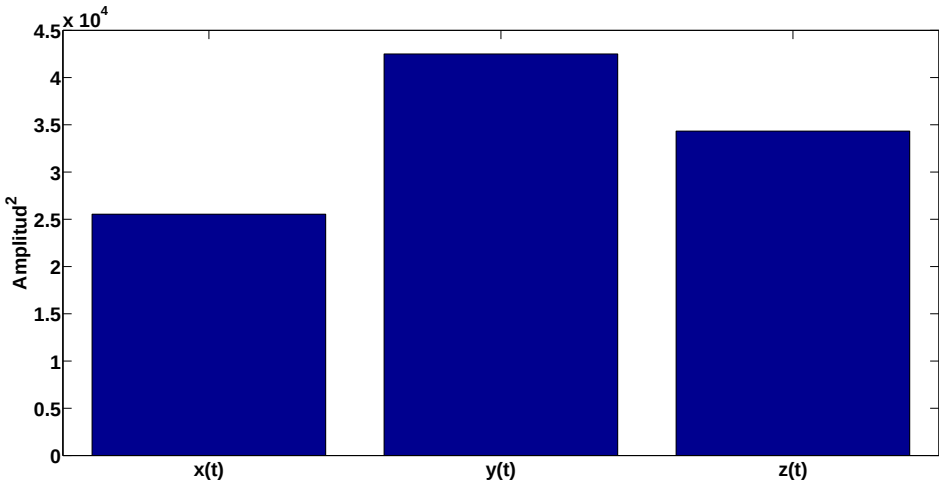


Figura 5.3: Niveles de energía de las variables de estado del primer oscilador (Lü de orden fraccionario) de la red, en la banda de frecuencias del mensaje $m(t)$.

La Tabla 5.1 muestra J_1 obtenido de (5.1) el cual representa cuántas veces la energía de la señal caótica es mayor que la energía del mensaje. J_2 obtenido de (5.2) muestra cuántas veces la energía de la señal caótica es mayor que la energía del mensaje en la banda de frecuencias en el cual está localizado el mensaje.

Tabla 5.1: Valores obtenidos de los criterios de selección de las señales caóticas de la red compleja sincronizada. E_c Energía de la señal caótica, E. P. energía ponderada, J_1 y J_2 criterios de selección, A. B. ancho de banda.

Estado	$E_c(10^7)$	E. P.(10^4)	$J_1(10^4)$	$J_2(10^2)$	A. B.
$x(t)$	0.2943	2.5542	12.959	18.353	0.1971 kHz
$y(t)$	0.3172	4.2501	13.968	30.538	0.274 kHz
$z(t)$	1.9887	3.4334	87.561	24.67	0.6087 kHz

De acuerdo con J_1 de la Tabla 5.1, $z(t)$ provee el mayor valor. Sin embargo, el mejor candidato para encriptar el mensaje, de acuerdo con J_2, es el estado $y(t)$, ya

que proporciona un nivel más alto de energía en la banda de frecuencias en el que está localizado el mensaje. Entonces, $y(t)$ es seleccionado como la variable de estado para encriptar el mensaje. Para este caso, se utilizó el encriptado caótico aditivo. Este método consiste en la aplicación de osciladores caóticos autónomos cuya señal de salida es sumada a la señal de información. Esta suma es enviada a través de un canal de comunicación. Una segunda señal caótica del transmisor es transmitida y utilizada por el receptor para sincronizar un sistema caótico equivalente con el sistema del transmisor. La señal reconstruida es sustraída de la suma transmitida recuperando el mensaje original [25], ésto, está ilustrado en la Figura 5.4.

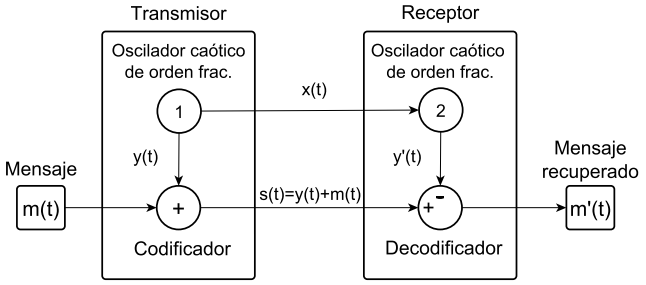


Figura 5.4: Diagrama básico de encriptamiento caótico de dos canales.

La Figura 5.5 muestra los resultados del encriptado, siendo (a) $m(t)$ el mensaje a encriptar previamente mencionado, (b) $s_1(t) = y(t) + m(t)$ representa el mensaje encriptado, y, (c) $m'(t) = s_1(t) - y'(t)$ es el mensaje recuperado.

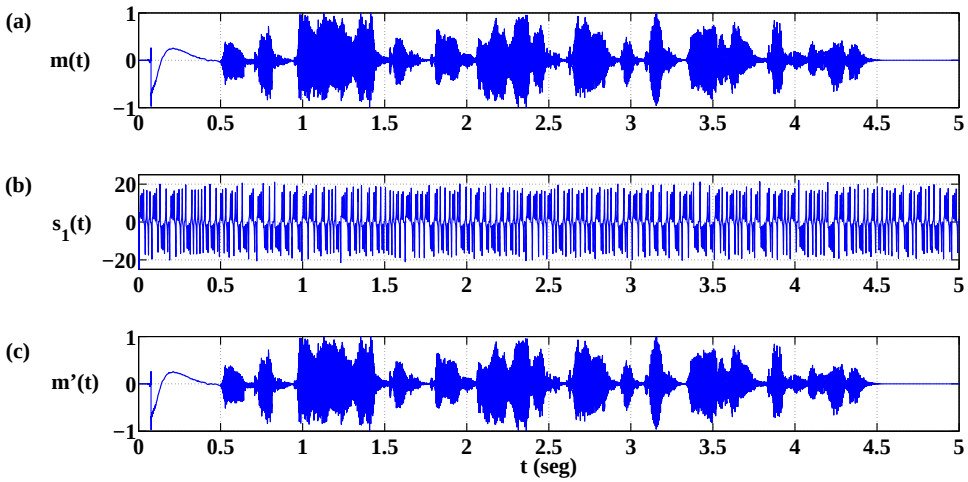


Figura 5.5: (a) Mensaje a encriptar $m(t)$, (b) Mensaje encriptado $s_1(t)$ y (c) Mensaje recuperado $m'(t)$.

Para garantizar que la energía proporcionada por el oscilador caótico de orden fraccionario sea aprovechada al máximo, es necesario que las señales caóticas y la señal del mensaje coincidan en frecuencia, para lograr ésto, se propone la modulación de las variables de estado del oscilador. Esto moverá la energía del oscilador a la banda de frecuencias en el que está localizado el mensaje. La mejoría del encriptado es reflejado en los valores de J_2, ya que un valor mayor de J_2, significa un incremento de energía de la señal caótica en la banda de frecuencias del mensaje.

5.1.1.1 Modulación de las variables de estado del oscilador caótico de orden fraccionario

En esta sección, las variables de estado del primer oscilador de la red compleja previamente sincronizada, son moduladas para aprovechar mejor la energía proporcionada por el oscilador caótico. Los criterios de selección de la señal caótica para encriptar el mensaje es utilizado una vez más.

El mensaje a encriptar es la misma grabación de voz, con la misma atenuación,

con la finalidad de observar la diferencia en la calidad del encriptado.

Por el teorema de modulación [26], si

$$x(n) \overset{F}{\longleftrightarrow} X(\omega), \tag{5.3}$$

entonces

$$e^{j\omega_0 n}x(n) \overset{F}{\longleftrightarrow} X(\omega - \omega_0). \tag{5.4}$$

De acuerdo a esta propiedad, la multiplicación de una secuencia $x(n)$ por $e^{j\omega_0 n}$ es equivalente a una translación en frecuencia del espectro $X(\omega)$ por ω_0. Puesto a que el espectro $X(\omega)$ es periódico, el cambio ω_0 aplica a la señal del espectro en cada período.

Entonces

$$x(n)\cos(\omega_0 n) \overset{F}{\longleftrightarrow} \frac{1}{2}[X(\omega + \omega_0) + X(\omega - \omega_0)]. \tag{5.5}$$

Una vez mencionado todo lo anterior, se llevó a cabo la modulación de las variables de estado del oscilador fraccionario de la siguiente manera:

$$\begin{aligned} x_{f_0}(n) &= x_1(n)\cos(\omega_0 n), \\ y_{f_0}(n) &= y_1(n)\cos(\omega_0 n), \\ z_{f_0}(n) &= z_1(n)\cos(\omega_0 n), \end{aligned} \tag{5.6}$$

con $\omega_0 = \frac{2\pi f_0}{F_s}$, donde f_0 es la frecuencia de la banda del mensaje a la cual se quiere mover la señal caótica.

Como el mensaje $m(t)$ está localizado en una banda de frecuencias de 0.3 kHz - 3 kHz, consideramos $\omega_0 = \pi\frac{300}{5512.5} rad/seg$. Esto para mover la energía de las

variables de estado del primer oscilador de la red compleja, a la banda de frecuencias del mensaje. La Figura 5.6 muestra un diagrama de como el estado $y(t)$ es modulado y utilizado para encriprar el mensaje.

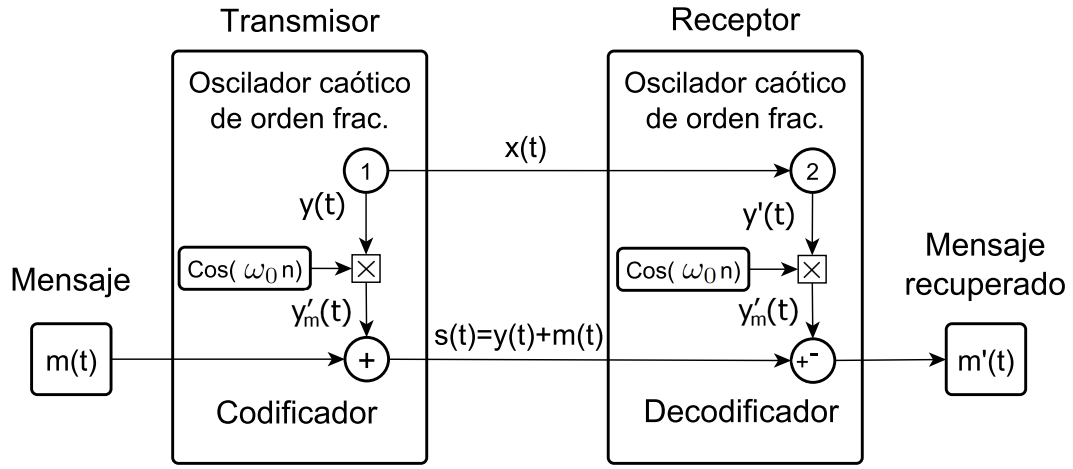


Figura 5.6: Diagrama de encriptado aditivo y modulación del estado $y(t)$.

De acuerdo con (5.2), se obtuvieron valores diferentes que en el caso sin modulación. Estos nuevos niveles de energía son mostrados en la Figura 5.7.

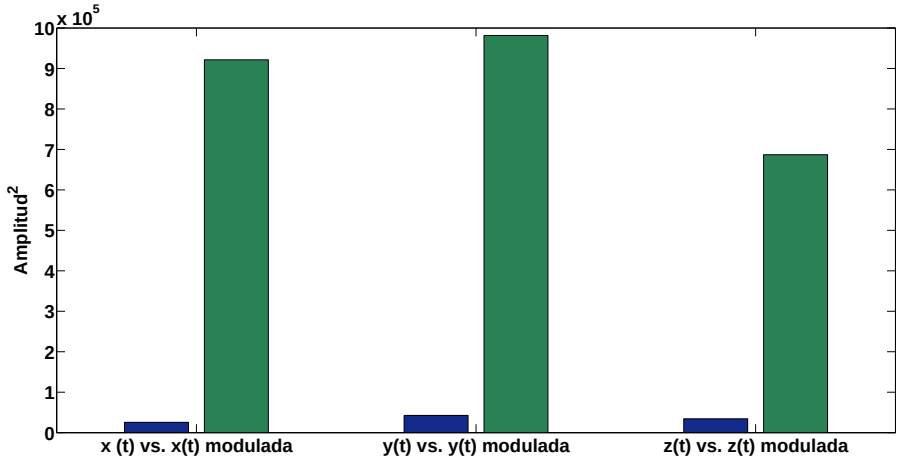


Figura 5.7: Niveles de energía anteriores (azul) y posteriores (verde) a la modulación de las variables de estado del primer oscilador (Lü de orden fraccionario) de la red, en la banda de frecuencias del mensaje $m(t)$.

La Tabla 5.2 muestra los valores resultantes de J_2 posteriores al proceso de modulación de las variables de estado del primer oscilador de la red. E. P. M., representa la energía ponderada después de modular las variables de estado. J_2 muestra los valores del criterio basado en frecuencia previos a la modulación de las variables de estado. $J_{2,m}$ resulta del criterio de selección basado en el dominio de la frecuencia posterior a la modulación de las variables de estado. B es la proporción entre los criterios $J_{2,m}$ y J_2. A. B. es el ancho de banda de las señales caóticas.

Tabla 5.2: Valores obtenidos de la red compleja con el criterio J_2. E. P. M. Energía ponderada resultante de modular las variables de estado, J_2 criterio de selección basado en el dominio de la frecuencia, $J_{2,m}$ criterio de selección basado en el dominio de la frecuencia posterior a la modulación de las variables de estado, B relación entre $J_{2,m}$ y J_2, A. B. ancho de banda.

Estado	E. P. M.(10^4)	$J_2(10^2)$	$J_{2,m}(10^2)$	B	A. B.
$x(t)$	92.133	18.353	661.99	36.1	0.6993 kHz
$y(t)$	98.148	30.539	705.22	23.1	0.7483 kHz
$z(t)$	68.693	24.67	493.58	20	0.8077 kHz

Se observa que los valores de J_2 son mayores que los obtenidos en la Tabla 5.1. Esto significa que la energía de las señales caóticas del oscilador está ubicada en la banda de frecuencias del mensaje, mejorando la calidad de encriptado. Hemos seleccionado el estado $y(t)$ para encriptar el mensaje porque presenta el valor de J_2 más alto.

La Figura 5.8 muestra los resultados del encriptado obtenido con las variables de estado moduladas del primer oscilador de la red compleja, siendo (a) $m(t)$ el mensaje, (b) $s_2(t) = y_{f_0}(t) + m(t)$ el mensaje encriptado, y (c) $m'(t) = s_2(t) - y'_{f_0}(t)$

el mensaje recuperado.

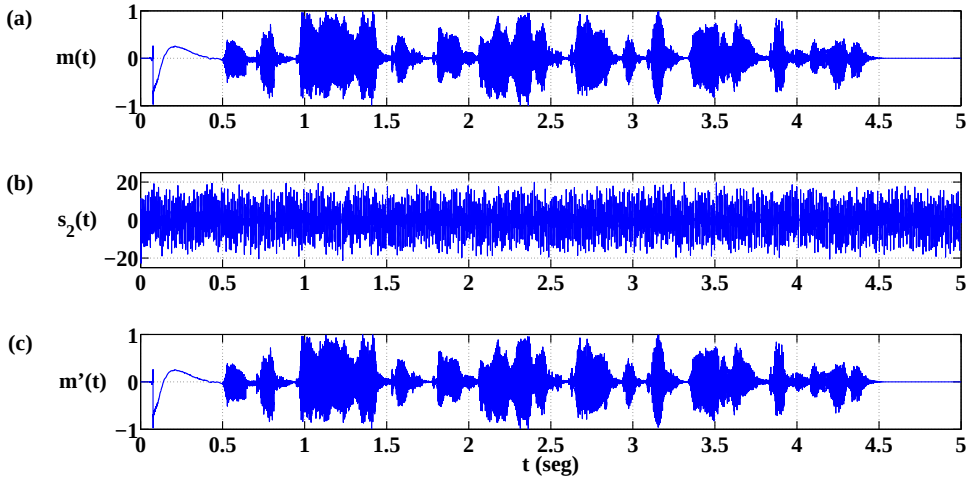


Figura 5.8: (a) Mensaje a encriptar $m(t)$, (b) Mensaje encriptado $s_2(t)$ y (c) Mensaje recuperado $m'(t)$.

Utilizando la correlación cruzada, se observa que tan diferente es el mensaje original $m(t)$ y la señal resultante del encriptamiento $s_1(t)$, así como también la diferencia entre $m(t)$ y la señal resultante del encriptamiento $s_2(t)$ aplicando la modulación de las variables de estado. La matriz de correlación es utilizada para esta finalidad.

La matriz de correlación D es una matriz cuadrada $n \times n$ constituida por los coeficientes de correlación de Pearson de cada pareja de variables. Su diagonal principal es unitaria, y los elementos no diagonales (i, j) son los correspondientes coeficientes de correlación de Pearson d_{ij} . La matriz de correlación es simétrica, y conserva las propiedades de ser definida positiva y tener un determinante no negativo.

La matriz resultante de comparar la señal $m(t)$ con la señal $s_1(t)$ es la siguiente:

$$D = \begin{pmatrix} 1 & 0.0064 \\ 0.0064 & 1 \end{pmatrix}. \tag{5.7}$$

En la matriz mostrada a continuación se aprecian los coeficientes de correlación de Pearson resultante de comparar la señal $m(t)$ con la señal $s_2(t)$ (modulación de las variables de estado aplicada):

$$D_m = \begin{pmatrix} 1 & 0.0008 \\ 0.0008 & 1 \end{pmatrix}. \tag{5.8}$$

Los elementos de la diagonal secundaria de (5.7) y (5.8) muestran que la señal $m(t)$ está débilmente correlacionada, i.e. está oculta de una mejor manera, utilizando la modulación de las variables de estado.

5.1.2 Encriptado caótico de imagen

En este trabajo de tesis, se utilizaron imagenes en formato JPG, de tipo RGB de 8 bits. Dichas imagenes fueron manipuladas mediante MATLAB el cual genera un número determinado de matrices dependiendo del tipo de imagen utilizada. Estas matrices contienen los valores de cada pixel de la imagen.

Es importante mencionar que duplicamos el número de bits a 16, debido al rango de valores que puede tomar cada pixel. Esto hace posible utilizar los valores obtenidos de las señales caóticas, en el encriptado de la imagen.

Para poder encriptar las imagenes mostradas en la Figura 5.8 y Figura 5.10 utilizando el método aditivo, es necesario transformar las matrices generadas por MATLAB, a un vector fila. Una vez hecho esto, es necesario generar una señal caótica de la misma longitud que el vector fila. Al igual que en el caso de voz, la imagen es enmascarada mediante el método aditivo y es enviada simultaneamente con un estado de la red a travéz de un canal público. El receptor se encarga de generar un oscilador equivalente utilizando el estado recibido. La imagen es recuperada de la suma transmitida mediante la sustracción del estado utilizado para encriptar la imagen.

5.1.2.1 Manipulación de la imagen previa a encriptar

En esta investigación se utilizaron imagenes en modo RGB. Las matrices correspondientes para este tipo de imagenes las hemos llamado R, G y B, las cuales contienen los valores de cada pixel de la imagen. Dichas matrices pueden ser representadas de la siguiente manera:

$$R = \begin{pmatrix} R_1 \\ R_2 \\ \vdots \\ R_n \end{pmatrix} = \begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1p} \\ r_{21} & r_{22} & \cdots & r_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{np} \end{pmatrix}, \tag{5.9}$$

$$G = \begin{pmatrix} G_1 \\ G_2 \\ \vdots \\ G_n \end{pmatrix} = \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1p} \\ g_{21} & g_{22} & \cdots & g_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ g_{n1} & g_{n2} & \cdots & g_{np} \end{pmatrix}, \tag{5.10}$$

$$B = \begin{pmatrix} B_1 \\ B_2 \\ \vdots \\ B_n \end{pmatrix} = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1p} \\ b_{21} & b_{22} & \cdots & b_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{np} \end{pmatrix}, \tag{5.11}$$

donde n es el número de filas de la matriz y p el número de columnas.

Para encriptar la imagen, utilizando el método aditivo, es necesario formar un vector fila $V = (r, g, b) \in \Re^p$, para poder sumarlo a una de las variables de estado del oscilador caótico. Para esto primero es necesario concatenar las filas de cada matriz de la siguiente forma:

$$r = \begin{pmatrix} R_1 & \vdots & R_2 & \vdots & \cdots & \vdots & R_n \end{pmatrix}, \tag{5.12}$$

$$g = \begin{pmatrix} G_1 & \vdots & G_2 & \vdots & \cdots & \vdots & G_n \end{pmatrix}, \tag{5.13}$$

$$b = \begin{pmatrix} B_1 & \vdots & B_2 & \vdots & \cdots & \vdots & B_n \end{pmatrix}. \tag{5.14}$$

Una vez hecho esto, los vectores fila (5.12), (5.13) y (5.14) deben ser contatenados de la siguiente forma:

$$V = \begin{pmatrix} r & \vdots & g & \vdots & b \end{pmatrix}. \tag{5.15}$$

De este modo, nuestro vector está listo para ser utilizado en el encriptado, utilizando una de las variables de estado del oscilador caótico. Esta variable de estado utilizada para encriptar nuestra imagen, es seleccionada en base al criterio J_1 unicamente. Es importante mencionar, que este procedimento debe hacerse cuidadosamente, ya que para desencriptar, es decir, recuperar la imagen original, es necesario llevar a cabo este procedimento de manera inversa, tal que, recuperemos las matrices R, G y B originales.

A continuación, se presentan los resultados obtenidos del encriptado de imagenes, mediante el uso del método de encriptado aditivo. Se utiliza el vector de estado proporcionado por osciladores caóticos de orden fraccionario, seleccionado según el criterio J_1. El procedimiento de manipulación de cada una de las imagenes descrito en esta sección es utilizado.

5.1.2.2 Resultados obtenidos del encriptamiento caótico de imagenes

La imagen que se desea encriptar en este primer ejemplo, es mostrada en la Figura 5.9. MATLAB genera tres matrices de 120×120, nuestro vector fila generado consta de $43,200$ elementos. Para la simulación es necesario generar $43,200$ puntos de la señal caótica con la que se desea encriptar la imagen.

Figura 5.9: Imagen a encriptar: Tierra.jpg, dimensiones: 120×120 pixeles.

La Figura 5.10 muestra los niveles de energía de las variables de estado del oscilador caótico Lü de orden fraccionario con parámetros: $a = 36, b = 3, c = 20$, derivadas: $q_1 = q_2 = q_3 = 0.95$, y condiciones iniciales: $(x(0), y(0), z(0)) = (1, 0.1, 2.5)$.

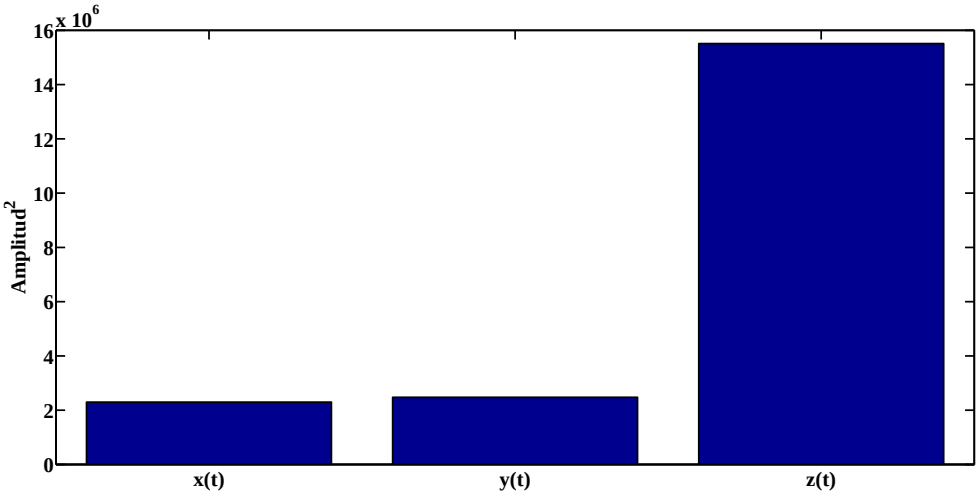


Figura 5.10: Niveles de energía de las variables de estado del oscilador caótico Lü de orden fraccionario.

La Figura 5.11, muestra los resultados del encriptamiento caótico utilizando el estado $z(t)$ del oscilador Lü.

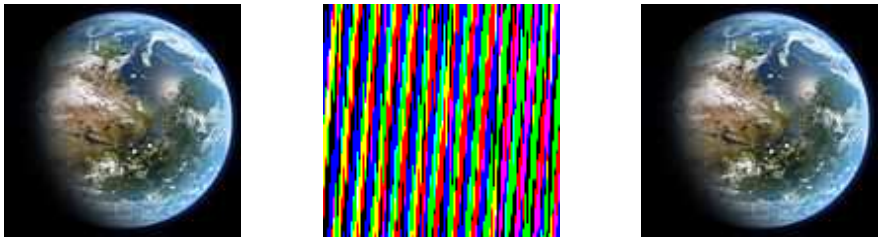


Figura 5.11: Encriptado de imagen con el oscilador caótico Lü de orden fraccionario: (a) Imagen a encriptar, (b) Imagen encriptada y (c) Imagen recuperada.

La Figura 5.12, muestra la imagen "Leopardo.jpg", la cual se desea encriptar. MATLAB genera tres matrices de 160×107, por lo tanto, nuestro vector fila generado consta de $51,360$ elementos. Para la simulación es necesario generar $51,360$ puntos de la señal caótica con la que se desea encriptar la imagen.

Figura 5.12: Imagen a encriptar: Leopardo.jpg, dimensiones: 107×160 pixeles.

La Figura 5.13 muestra los niveles de energía de las variables de estado del oscilador caótico Chen de orden fraccionario con parámetros: $a = 35, b = 3, c = 28, d = -7$, derivadas: $q_1 = 0.985, q_2 = 0.99, q_3 = 0.98$, y condiciones iniciales: $(x(0), y(0), z(0)) = (1, 0.1, 2.5)$.

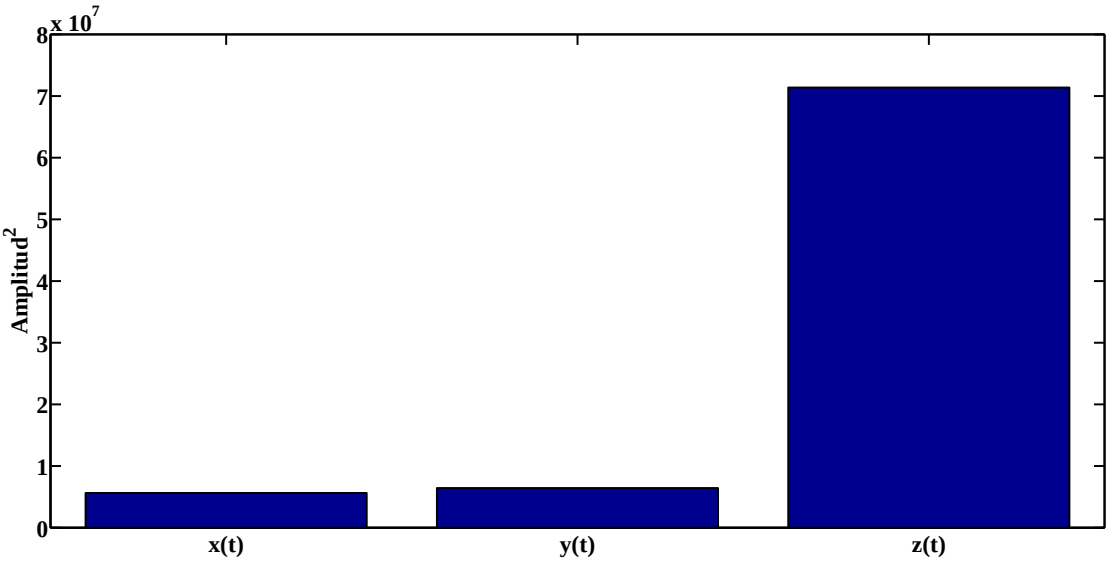


Figura 5.13: Niveles de energía de las variables de estado del oscilador caótico Chen de orden fraccionario.

La Figura 5.14, muestra los resultados del encriptamiento caótico utilizando el estado $z(t)$ del oscilador Chen.

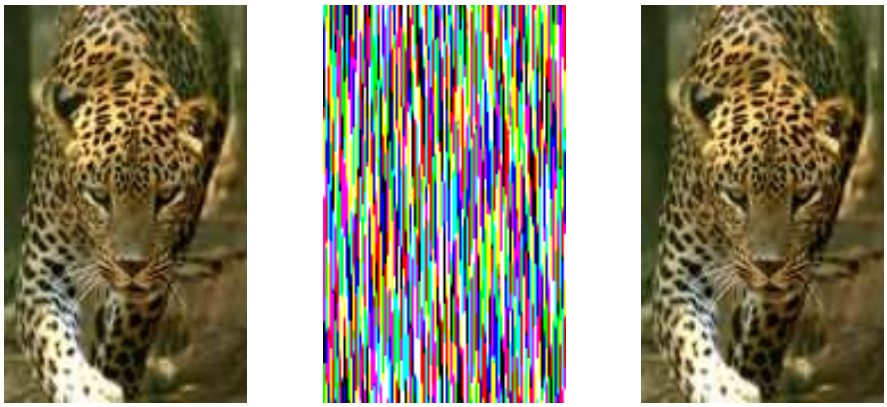


Figura 5.14: Encriptado de imagen con el oscilador caótico Chen de orden fraccionario: (a) Imagen a encriptar, (b) Imagen encriptada y (c) Imagen recuperada.

Capítulo 6

Conclusiones, aportaciones y trabajos a futuro.

En este trabajo de investigación se llevó a cabo el encriptamiento caótico de voz e imagen, utilizando las variables de estado de osciladores caóticos de orden fraccionario. Para esto, fue necesaria la comprensión y realización de redes complejas, así como lograr sincronizar dichas redes para utilizar las variables de estado en el encriptado del mensaje.

En el encriptado caótico utilizando osciladores de orden fraccionario, existen parámetros desconocidos en contra de personas no deseadas. Dichos parámetros son aquellos valores específicos para los cuales el sistema exhibe un comportamiento caótico, las condiciones iniciales, y el orden de las ecuaciones diferenciales fraccionarias. Adicionalmente, la banda de frecuencias a la cual la energía de las señales caóticas son transladadas, representa otro parámetro desconocido para una tercera persona no deseada que quisiera recuperar el mensaje.

El oscilador caótico de orden fraccionario mostrado en el ejemplo de encriptado de audio del Capítulo 5, presenta su energía a menores frecuencias que el mensaje. La energía de las señales caóticas del oscilador no estaba localizada en la banda de frecuencias del mensaje, obteniendo un encriptado pobre. Modulando las variables de

estado del oscilador, transladamos su energía a la banda de frecuencias del mensaje, ayudándonos a mejorar el encriptado obtenido en un factor de 23.

6.1 Aportaciones de este trabajo de tesis

Las aportaciones más destacables que proporciona este trabajo de tesis son las siguientes:

- Sicronización completa de redes complejas formadas por osciladores caóticos de orden fraccionario idénticos, con topología regular e irregular en configuración maestro-esclavo y bidireccional.
- Encriptado caótico de voz e imagen utilizando las dinámicas generadas por osciladores caóticos de orden fraccionario.
- Propuesta y aplicación de la modulación de las variables de estado de osciladores caóticos fraccionarios, como solución alternativa al problema en el cual, la señal del mensaje y la señal caótica no coinciden en el dominio de la frecuencia.
- Aplicación de la correlación cruzada y coeficientes de Pearson como un método de comparación, entre la señal del mensaje original y la señal del mensaje encriptado, mostrando la mejoría en la calidad del encriptado, utilizando la modulación de las variables de estado.
- Representación matemática del proceso de manipulación de la imagen a encriptar, para generar un vector fila, necesario para poder hacer uso del encriptado aditivo.

6.2 Trabajos a futuro

Como caminos a seguir en trabajos futuros, se proponen los siguientes:

- Encriptado de datos utilizando redes complejas con osciladores caóticos fraccionarios no idénticos.
- Encriptado múltiple (encriptar más de un mensaje en una sola sseñal caótica) utilizando osciladores caóticos de orden fraccionario.
- Encriptado caótico de video con osciladores caóticos de orden fraccionario

Bibliografía

[1] AlSharawi, Z., Cushing, J.M., and Elaydi S. (2013). Theory and Applications of Difference Equations and Discrete Dynamical Systems. New York: Springer.

[2] Kasner, E. and Newman, J. (2007). Matemáticas e imaginación. México: QED.

[3] Newman, M.E.J. (2003). The structure and function of complex networks. DOI:10.1137/S003614450342480

[4] Bocaletti, S., Latora, V., Moreno, Y., Chavez, M., and Hwang, D.U. (2006). Complex networks: Structure and dynamics. Physics Reports, 175-308.

[5] Wang, X.F. (2008). Complex networks: topology, dynamics and synchronization. International Journal of Bifurcation and Chaos, 885-916.

[6] Angulo-Guzmán, S.Y., Posadas-Castillo, C., Díaz-Romero, D.A., López-Gutiérrez, R.M., and Cruz-Hernández, C. (2012). Chaotic synchronization of regular complex networks with fractional-order oscillators. IEEE, 921-927.

[7] Petráš, I. (2011), Fractional-Order Nonlinear Systems Modeling, Analysis and Simulation. Springer.

[8] Petráš, I., Podlubny, I., O'Learly, P., Dorčák, Ľ., and Vinagre, M. (2002). Analogue realization of fractional order controllers. Nonlinear Dynamics, 281-296.

[9] Podlubny, I. (1999). Fractional Differential Equations. San Diego: Academic Press.

[10] Oldham, K.B., and Spanier, J. (2006). The Fractional Calculus: Theory and Applications of Differentiation and Integration to Arbitrary Order. Mineola, New York: Dover Books on Mathematics.

[11] Deng, W.H., and Li, C.P. (2005). Chaos synchronization of the fractional Lü system. Physica A: Statistical Mechanicsand its Applications, 62-72.

[12] Pecora, L.M., and Carroll, T.L. (1990). Synchronization in chaotic systems. Physical Review Letters, 821-824.

[13] Xu, Y., and Wang, H. (2013). Synchronization of Fractional-Order Chaotic Systems with Gaussian Fluctuation by Sliding Mode Control. Abstract and Applied Analysis. DOI:10.1155/2013/948782.

[14] Wu, X., and Yang, Y. (2010). Chaos in the fractional-order Qi system and its synchronization using active control. IEEE, 109-112.

[15] Odibat, Z.M., Corson, N., Aziz-Alaoui, M., and Bertelle, C. (2010). Synchronization of chaotic fractional-order systems via linear control. International Journal of Bifurcation and Chaos, 1-15.

[16] López-Gutiérrez, R.M., Posadas-Castillo, C., López-Mancilla, D., Cruz-Hernández, C. (2009). Communicating via robust synchronization of chaotic lasers. Chaos, Solitons and Fractals, 277-285.

[17] Serrano-Guerrero, H., Cruz-Hernández, C., López-Gutiérrez, R.M., Posadas-Castillo, C., Inzunza-González, E. (2011). Chaotic Synchronization in Star Coupled Networks of 3D CNNs and Its Application in Communications. International Journal of Nonlinear Sciences and Numerical Simulation, 571-580.

[18] Cruz-Hernández, C., López-Gutiérrez, R.M., Aguilar-Bustos, A.Y., Posadas-Castillo, C. (2010). Comunicating Encrypted Information Based on Synchronized Hyperchaotic Maps. International Journal of Nonlinear Sciences and Numerical Simulation, 337-349.

[19] Wang, X.F., and Chen, G. (2002). Synchronization in Small-World Dynamical Networks. International Journal of Bifurcation and Chaos, 187-192.

[20] Wang, J., Xiong, X., and Zhang Y. (2006). Extending synchronization scheme to chaotic fractional-order Chen systems. Physica A: Statistical Mechanicsand its Applications, 279-285.

[21] Posadas-Castillo, C., Garza-González, E., Cruz-Hernández, C., Alcorta-García, E., and Díaz-Romero, D.A. (2011). Chaotic synchronizationof complex networks with Rössler oscillators in Hamiltonian form like nodes. The 4th Chaotic modeling and simulation international conference.

[22] Bocaletti, S., Kurths, J., Osipov, G., Valladares, D.L., and Zhou, C.S. (2002). The synchronization of chaotic systems. Physics Reports, 1-101.

[23] Soriano-Sánchez, A.G., Posadas-Castillo, C., Platas-Garza, M.A., Diaz-Romero, D.A. (2015). Performance improvement of chaotic encryption via energy and frequency location criteria. Mathematics and Computers in Simulation. DOI:10.1016/j.matcom.2015.01.007.

[24] Tomasi, W. (2001). Electronic Communication Systems: Fundamentals through Advanced. Upper Saddle River, New Jersey: Prentice Hall.

[25] Dachzelt, F., and Schwarz, W. (2001). Chaos and Cryptography. IEEE Transactions on Circuits and Systems I, 1498-1509.

[26] Proakis, J.G., and Manolakis, D.G. (1996). Digital Signal Processing. New Jersey: Prentice Hall.