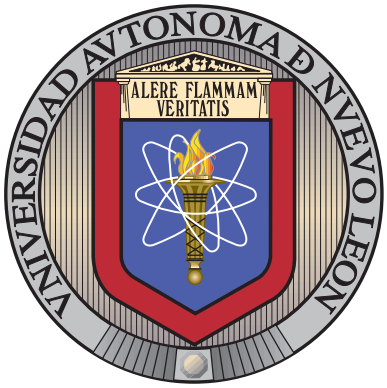
Universidad Autónoma de Nuevo León

Facultad de Ingeniería Mecánica y Eléctrica

Subdirección de Estudios de Posgrado



Sincronización de redes complejas no estructurales vía control pinning y su aplicación al encriptado caótico

por

Otoniel García Sepúlveda

como requisito parcial para obtener el grado de

doctorado en ingeniería eléctrica

Diciembre de 2020

Universidad Autónoma de Nuevo León

Facultad de Ingeniería Mecánica y Eléctrica

Subdirección de Estudios de Posgrado

Sincronización de redes complejas no estructurales vía control pinning y su aplicación al encriptado caótico

por

Otoniel García Sepúlveda

como requisito parcial para obtener el grado de

DOCTORADO EN INGENIERÍA ELÉCTRICA

Diciembre de 2020

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 "Sincronización de redes complejas no estructurales vía control pinning y su aplicación al encriptado caótico", realizada por el alumno Otoniel García Sepúlveda, con número de matrícula 1384113, sea aceptada para su defensa como requisito para obtener el grado de Doctorado en Ingeniería Eléctrica.

El comité de Tesis

Dr. Cornelio Posadas Castillo
Director

Dr. Miguel Ángel Platas Garza
Co-Director

Dr. David A. Díaz Romero
Revisor

Dr. Efraín Alcorta García
Revisor

Dr. Eliezer Garza González
Revisor

Dr. Didier López Mancilla
Revisor

Vo. Bo.

Dr. Simón Martínez Martínez
Subdirector de Estudios de Posgrado

SUBDIRECCIÓN DE ESTUDIOS DE POSGRADO
FACULTAD DE INGENIERÍA MECÁNICA Y ELÉCTRICA
U.A.N.L.

FIME
073

San Nicolás de los Garza, Nuevo León, diciembre de 2020

Ciudad Universitaria Pedro de Alba s/n, C.P. 66455. A.P. 076 Suc. "F"
San Nicolás de los Garza, Nuevo León, México. Tels: (81) 8332 0903 /
Conm.: 8329 4020 / Fax: (81) 8332 0904

Índice general

Índice de figuras

Índice de tablas

Agradecimientos

Le agradezco a mi familia, por su comprensión y apoyo incondicional.

A mi asesor, el Dr. Cornelio Posadas Castillo, por su tiempo, su excelente disposición, y los valiosos comentarios otorgados en beneficio de la presente investigación.

A mi comité de tesis, por las pertinentes observaciones, correciones, y sugerencias otorgadas durante el proceso de revisión.

Al Consejo Nacional de Ciencia y Tecnología (CONACyT), por el apoyo económico otorgado para la realización de este trabajo de investigación.

Resumen

Otoniel García Sepúlveda.

Candidato para obtener el grado de Doctorado en Ingeniería Eléctrica.

Universidad Autónoma de Nuevo León.

Facultad de Ingeniería Mecánica y Eléctrica.

Título del estudio: Sincronización de redes complejas no estructurales vía control pinning y su aplicación al encriptado caótico.

Número de páginas: 87.

Objetivos y método de estudio: El objetivo de la tesis se enfoca en modificar las dinámicas emergentes de una red compleja, compuesta por osciladores caóticos o hipercaóticos de orden fraccionario, mediante control pinning. Esto, con la intención de llevar a la red a un estado final deseado. De esta manera, se busca proponer una aplicación del control pinning al encriptado de datos, y elaborar un algoritmo o método de encriptado confiable, que ofrezca ventajas comparado con los métodos convencionales. Para esto, se realizó una investigación exhaustiva acerca de temas como: redes complejas, sincronía, caos, criptología, osciladores caóticos e hipercaóticos de orden fraccionario y teoría del control pinning. Se realizaron varias simulaciones numéricas para llevar a cabo los experimentos mostrados en la tesis.

CONTRIBUCIONES Y CONLUSIONES: Dentro de las contribuciones más destacables de la tesis, se encuentra la propuesta de una metodología para encriptar imagenes BMP tipo RGB, y un esquema de comunicación segura en modalidad de múltiples usuarios aplicando control pinning. En conclusión, se comprobó la hipótesis formulada y se cumplieron todos los objetivos de la tesis.

Firma del director: _____

Dr. Cornelio Posadas Castillo

Capítulo 1

Introducción

Esta tesis versa principalmente sobre el encriptado caótico. Las dinámicas de osciladores cuyos comportamientos exhiben trayectorias caóticas, son utilizadas para encriptar información.

La palábra *caos*, deriva de la palábra griega $\chi\alpha o\sigma$ (cháos). En el área de las matemáticas y la física, la Real Académia Española define el caos como: *"comportamiento aparentemente errático e impredecible de algunos sistemas dinámicos deterministas con gran sensibilidad a las condiciones iniciales".*

En el año de 1963, Edward Lorenz, un matemático y meteorólogo actualmente reconocido como uno de los pioneros de la teoría del caos, intentaba predecir el comportamiento atmosférico mediante un modelo matemático. Observó que al existir alteraciónes en las condiciones iniciales de las ecuaciones que conformaban el modelo matemático, las trayectorias del sistema divergían [1].

El modelo matemático que constituye al sistema caótico de Lorenz es el siguiente:

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

donde $\alpha = 10$, $\rho = 28$, $\beta = 8/3$ [2].

Al atractor de este sistema se le dió el nombre de atractor caótico de Lorenz en su honor, y es ilustrado en la Figura 1.1. Al efecto que causa alterar las condiciones iniciales de un sistema como éste, y los grandes cambios que puede producir dicha alteración en el comportamiento del sistema, se le conoce como efecto mariposa.

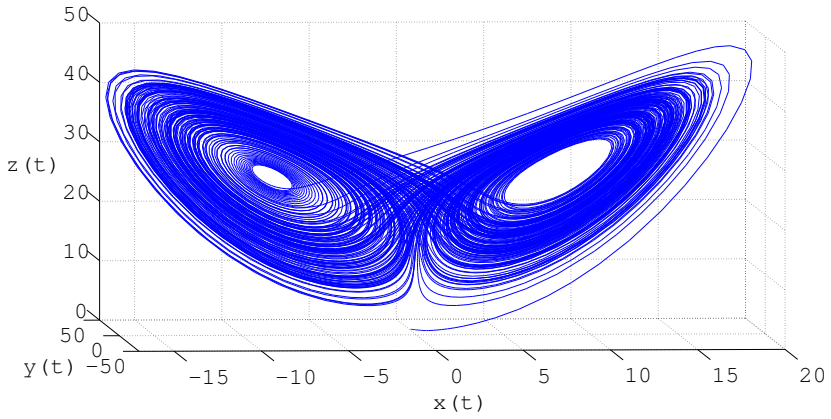


Figura 1.1: Atractor caótico de Lorenz.

En esta tesis, se utilizan osciladores caóticos de orden fraccionario ya que ofrecen un amplio espacio de llave en comparación a los osciladores caóticos de orden entero. En esta modalidad, los osciladores estan conformados por un conjunto de ecuaciones diferenciales cuyas derivadas están denotadas por D^{α} en donde $\alpha \in \mathbb{R}$.

Para llevar a cabo el proceso de encriptado de información, es importante mencionar el concepto de la criptología.

La palabra criptología, deriva de la palabra griega $\kappa\rho\iota\pi\tau\acute{o}\varsigma$ (kryptós), que significa "oculto", y logos que significa "discurso". La criptología puede ser dividida en dos disciplinas. La criptografía y el criptoanálisis.

La criptografía, definida por la Real Académia Española como: *"arte de escribir con clave secreta o de un modo enigmático"*, se encarga del diseño de criptosistemas.

El criptoanálisis, definido por la Real Académia Española como: *"arte de de-*

cifrar criptogramas", estudia la forma de romper los criptosistemas y hacerlos vulnerables para decifrar la información que esconden [4].

En esta tesis, la recuperación de los mensajes encriptados se lleva a cabo mediante la sincronía entre el emisor y el receptor.

El término *sincronía*, definida por la Real Académia Española como *"coincidencia de hechos o fenómenos en el tiempo"*, proviene del griego $\sigma\acute{\upsilon}\nu$ (syn), "con"y de la mitología griega $\chi\rho\acute{o}\nu o\varsigma$ (chronos), "tiempo".

La sincronía se refiere a la coincidencia en el tiempo de dos o más fenómenos. En general se puede decir que la sincronía, ocurre cuando dos o más objetos con comportamientos independientes, actúan de manera idéntica en el tiempo, ante la presencia de una conexión o de un medio físico de acoplamiento.

En el año de 1665, el físico holandés Christiaan Huygens, registró el primer fenómeno de sincronía mediante un experimento, producto de una observación accidental, que incluía dos relojes de péndulo acoplados mediante una viga. Dichos relojes sincronizaban el movimiento de sus péndulos al paso del tiempo aún cuando sus oscilaciones eran alteradas. Con lo anterior, Huygens concluyó que este fenómeno se debía a vibraciones imperceptibles que viajaban a través de la viga [3]. Su experimento es ilustrado en la Figura 1.2.

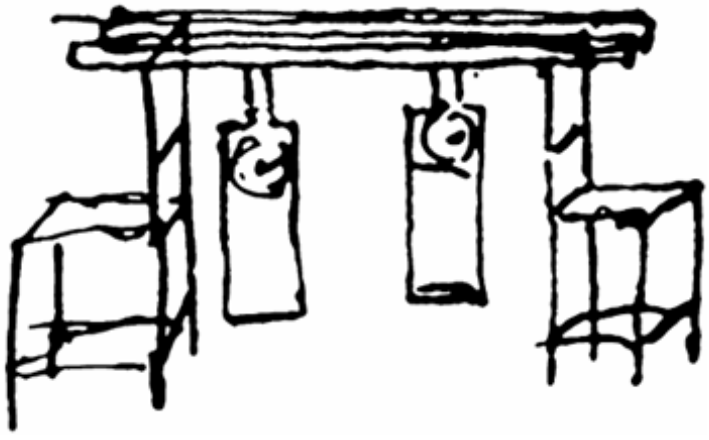


Figura 1.2: Boceto del experimento de Christiaan Huygens

1.1 Motivación

Desde la antigüedad, el hombre ha buscado ocultar y proteger información que considere valiosa. En la actualidad, esto no es la excepción. El continuo incremento del uso de los medios de comunicación por parte del hombre para transmitir información, exige la existencia de métodos que garanticen la privacidad en los canales que se utilizan.

Por esta razón, en este trabajo de investigación se busca proponer un algoritmo para encriptar información utilizando osciladores caóticos de orden fraccionario, e incrementar la seguridad en un esquema de comunicación emisor-receptor.

Se busca utilizar una red compleja en configuración bidireccional tanto en el emisor como en el receptor, idénticas en topología pero con condiciones iniciales diferentes una de la otra. Esto con la intención de simular un ecenario más realista. En una implementación fisica, resulta difícil asegurar que las condiciones iniciales del emisor y el receptor sean iguales en todo momento. Esto se debe a diversos factores, entre ellos el desgaste de los elementos que los constituyen. Por esta razón, se recurre a una sincronización entre ambas partes.

En primer instancia, la red emisora y receptora alcanzan la sincronía por separado. Al no existir un nodo maestro en ellas, se genera una dinámica emergente en cada red. Se utiliza la dinámica emergente de la red emisora, para encriptar el mensaje. Este mensaje es enviado a través de un canal público, hacia el receptor.

Se sugiere la aplicación del control pinning para sincronizar la red receptora a un nodo de referencia. Este nodo de referencia debe ser sincronizado a un nodo de la red emisora previamente sincronizada. La técnica de control pinning permite la manipulación de una red sin la necesidad de conectar todos los nodos que la conforman con el nodo de referencia. Esto provoca que la dinámica emergente producida por la red receptora, sincronice con la red emisora, asegurando la recuperación de

los mensajes en todo momento.

1.2 Hipótesis

La técnica de control pinning nos permitirá modificar la dinámica final a la cuál una red compleja en configuración bidireccional, constituida por osciladores caóticos ó hipercaóticos de orden fraccionario, converge una vez sincronizada (dinámica emergente). Es posible aplicar esta técnica de control al cifrado de información y proponer una metodología de encriptado que ofrezca alguna ventaja en comparación con métodos convencionales.

1.3 Objetivos y alcances de la tesis

Modificar la dinámica final a la que convergen los osciladores presentes en una red compleja sincronizada, en ausencia de un nodo maestro.

Proponer un algoritmo o método de encriptado confiable que ofrezca ventajas comparado con los métodos convencionales.

1.4 Objetivos particulares

Sincronizar redes complejas en configuración bidireccional, conformadas por osciladores caóticos o hipercaóticos de orden fraccionario, y obtener sus dinámicas emergentes.

Aplicar la teoría del control pinning para sincornizar una red compleja en configuración bidireccional a un nodo de referencia. Manipular las dinámicas emergentes obtenidas.

Utilizar las dinámicas emergentes obtenidas, para encriptar y recuperar mensajes en un esquema de comunicación en el que existan múltiples usuarios.

1.5 Organización del trabajo de tesis

En esta sección, se explica brevemente la organización de este trabajo de investigación.

El Capítulo 2, versa sobre el concepto de redes complejas, la topología y la configuración en la que éstas pueden presentarse. Se habla sobre las redes estructurales, que incluyen: las redes regulares e irregulares; y algunas redes no estructurales, tales como: redes libres de escala, redes de mundo pequeño y redes aleatorias.

En el Capítulo 3, se exponen algunos osciladores de orden fraccionario, en régimen caótico. Se muestran los preliminares matemáticos necesarios para la solución numérica de estos osciladores. Se exhiben algunos ejemplos simulados de osciladores caóticos de orden fraccionario y los atractores a los que convergen sus trayectorias.

El Capítulo 4, aborda el tema de la criptografía. En este capítulo se da a conocer la definición de un sistema criptográfico y se explican algunos niveles de seguridad que éste puede tener, tales como: error de descifrado, espacio de llave secreta, sensibilidad a la llave secreta, histograma, análisis de correlación y entropía.

El Capítulo 5, presenta el algoritmo de cifrado caótico propuesto utilizando imágenes en mapa de bits (BMP) tipo RGB. Se muestra el proceso de manipulación de los píxeles de este tipo de imágenes. Se habla sobre el método convencional de encriptado aditivo y el algoritmo propuesto. Se exponen ejemplos de los experimentos llevados a cabo.

En el Capítulo 6, se da a conocer la definición de la técnica de control pinning y la importancia de aplicarla en redes bidireccionales para este trabajo de investigación. Se mencionan algunas estrategias para seleccionar los osciladores que son conectados

al nodo de referencia. Se muestra la metodología de control utilizada. Se exponen ejemplos antes y después de aplicar la técnica de control pinning con la intención de observar sus efectos.

En el Capítulo 7, se aborda el tema de la transmisión de información en modalidad multiusuario. Se muestra el esquema multi-usuario convencional y el esquema multi-usuario propuesto aplicando la técnica de control pinning. Se obtienen resultados mediante un ejemplo completo del proceso de encriptado, transmisión y recuperación del mensaje.

Por último, en el Capítulo 8 se presentan las conclusiones, aportes de la tesis y trabajo a futuro propuesto.

Capítulo 2

Redes complejas

Una red compleja puede definirse como un conjunto de nodos interconectados entre sí, en donde cada nodo es parte fundamental de la red que contiene información detallada de ella [5].

La definición anterior, se debe a que una red compleja posee las siguientes características:

- Está compuesta por muchas partes (nodos) que interactúan entre sí.
- Estos nodos poseen comportamientos independientes y únicos ya que cuentan con estructura interna propia, y son unidades fundamentales de la red.
- Presenta comportamientos emergentes en ausencia de un nodo maestro.

2.1 Topología y configuración de redes complejas

La forma en que los nodos están organizados o acoplados en una red compleja, se le denomina topología.

Matemáticamente, este acoplamiento puede ser representado mediante una matriz de acoplamiento $A = (a_{ij}) \in \mathbb{R}^{N\times N}$. Excluyendo los elementos de la diagonal principal, si existe conexión entre el nodo i y el nodo j, entonces $a_{ij} = 1$, de lo contrario $a_{ij} = 0$. La diagonal principal de la matriz de acoplamiento indica el número de conexiones totales de cada nodo con signo negativo y se calcula de la siguiente manera:

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

Por otro lado, la configuración de una red, hace referencia al sentido o dirección en que fluye la información entre los nodos que conforman la red compleja.

En la configuración unidireccional o maestro-esclavo, la información fluye en una sola dirección. En este escenario el nodo maestro impone su dinámica al/los nodo(s) esclavo(s).

En la configuración bidireccional, la información fluye en ambas direcciones. Esto puede ser representado gráficamente por flechas en ambas direcciones o sin ellas.

En la Figura 2.1, se muestran las configuraciones mencionadas anteriormente.

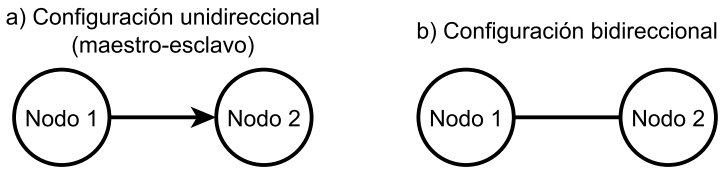


Figura 2.1: Configuraciones convencionales disponibles entre un par de nodos conectados. a) En la configuración unidireccional, la información fluye en un solo sentido, b) en la configuración bidireccional, la información fluye en ambos sentidos.

2.2 Redes estructurales

Las redes estructurales hacen referencia al grupo de redes regulares, que incluye a las redes cuyo acoplamiento exhibe un patrón definido y ordenado, tales como el acoplamiento global, anillo o estrella, y al grupo de redes irregulares las cuales no tienen patrónes definidos. Lo anterior, se explica de forma extendida a continuación.

2.2.1 Redes regulares

La topología de este tipo de redes forma patrones definidos y ordenados. A continuación se describen los tres escenarios de acoplamiento de las redes regulares.

- **Acoplamiento global:** En este tipo de acoplamiento, todos los nodos de la red están interconectados entre sí.
- **Acoplamiento anillo:** En este tipo de acoplamiento, cada nodo i está conectado a sus vecinos más cercanos $i \pm 1, i \pm 2, \ldots, i \pm K/2$, donde K es un número par.
- **Acoplamiento estrella:** En este tipo de acoplamiento, la red dispone de un nodo central conectado al resto de los nodos que conforman la red.

En la Figura 2.2, se muestran los tres tipos de redes regulares descritos anteriormente, en configuración bidireccional.

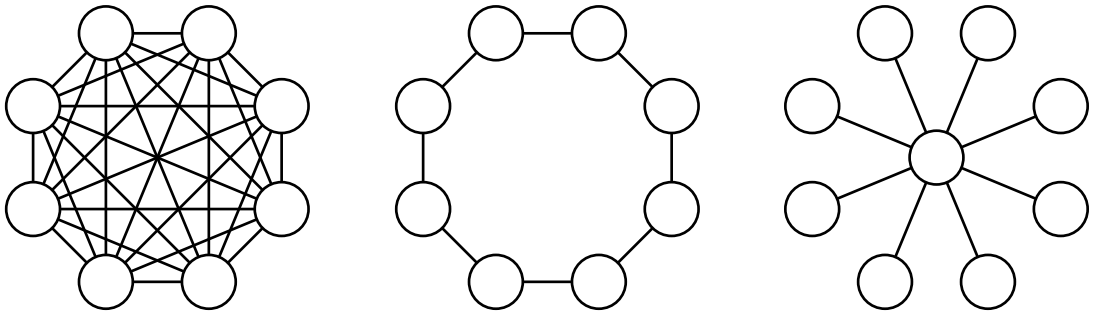


Figura 2.2: Topologías disponibles de las redes regulares. Las redes mostradas disponen de nodos interconectados en configuración bidireccional.

2.2.2 Redes irregulares

En esta topología, los nodos están interconectados entre sí de manera arbitraria y carece de patrones definidos. En la Figura 2.3, se muestra una red con acoplamiento irregular, en configuración bidireccional.

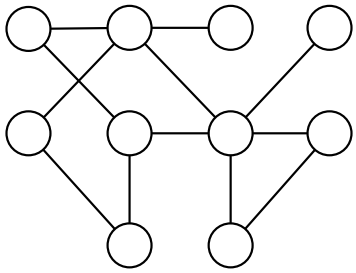


Figura 2.3: Ejemplo de una red con topología irregular y nodos conectados entre sí bidireccionalmente.

2.3 Redes no estructurales

Consideramos como redes no estructurales, a aquellas redes que no están catalogadas como redes regulares o irregulares.

Algunos ejemplos de este tipo de redes son: las redes libres de escala (free-scale networks), redes de mundo pequeño (small-world networks), y redes aleatorias (random networks). A continuación, se proporciona una breve descripción de este tipo de redes.

2.3.1 Redes libres de escala

Este tipo de redes, cumplen la ley-potencia $P(k)^{-\gamma}$, donde la función de distribución $P(k)$, es la probabilidad de conexión entre un nodo y los k nodos de la red, γ es un número real positivo [6]. Su nombre de debe a que las leyes-potencia son libres de una escala característica. En la Figura 2.4 se muestra un ejemplo de red libre de escala.

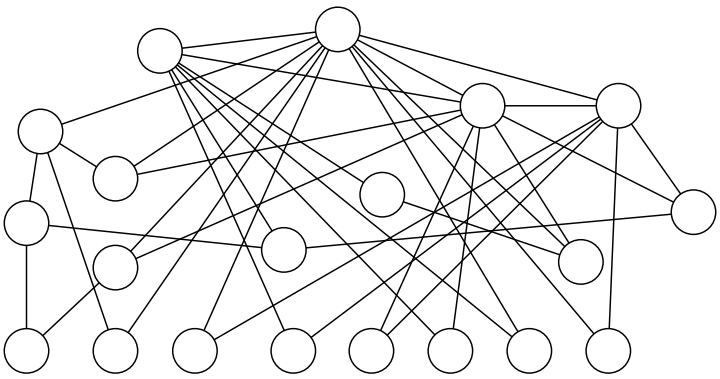


Figura 2.4: Ejemplo de una red libre de escala conformada por 20 nodos en configuración bidireccional.

2.3.2 Redes de mundo pequeño

A continuación, se describen brevemente los modelos de Watts-Strogatz (WS) y Newman-Watts (NW), para generar redes de mundo pequeño. Ambos modelos toman como punto de partida una red regular anillo con conexiones entre sus vecinos más cercanos [7]:

- Modelo Watts-Strogatz (WS): se realizan reconexiones entre los nodos con una probabilidad p. Dichas reconexiones consisten en cambiar un extremo de la conexión existente entre un par de nodos, hacia un nuevo vértice existente en la red.
- Modelo Newman-Watts (NW): no se realizan reconexiones. En este modelo se colocan nuevas conexiones entre par de nodos con probabilidad p. Se tienen las mismas restricciones que en el modelo anterior. Para $p = 0$ se produce la red original, para $p = 1$ se obtiene una red con acoplamiento global.

Se debe cumplir, que ningún vértice puede estar conectado a sí mismo, y dos vértices diferentes no pueden tener más de una conexión entre ellos. Lo anterior, se ilustra en la Figura 2.5.

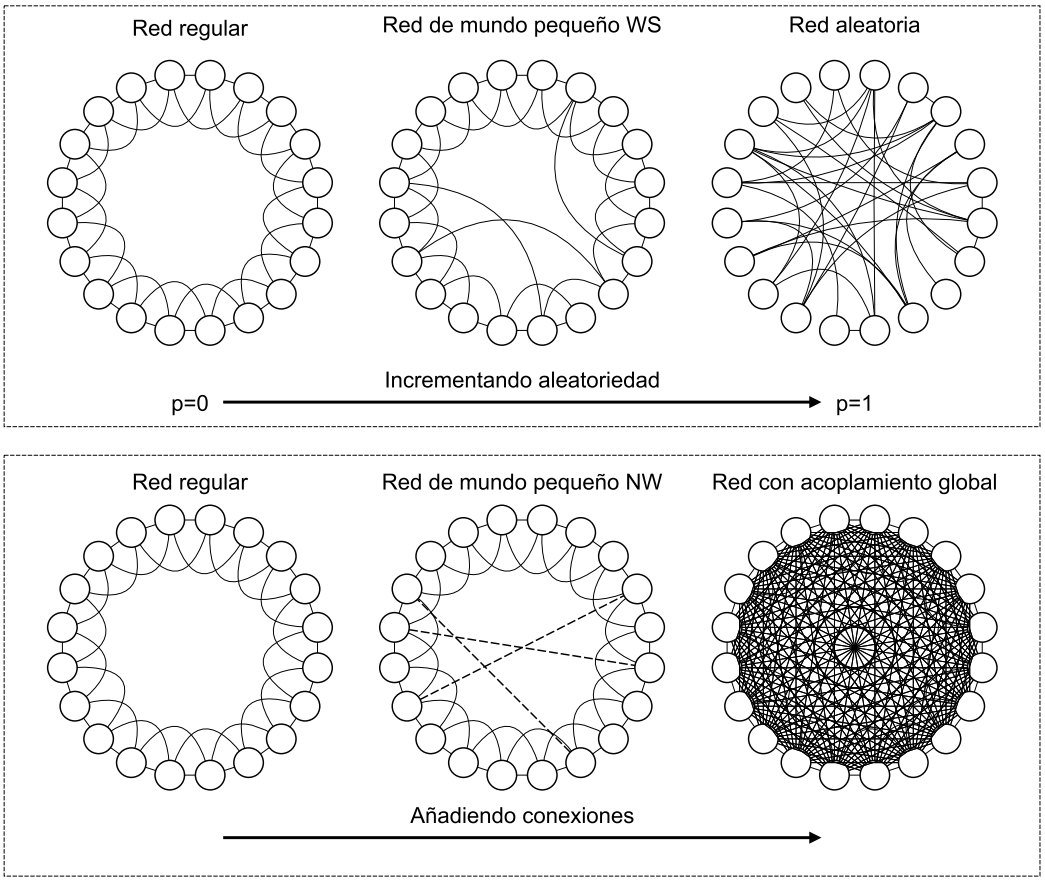


Figura 2.5: Redes de mundo pequeño: modelo Watts-Strogatz (parte superior), modelo Newman-Watts (parte inferior).

Se recomienda al lector interesado en conocer más a cerca de este tipo de redes, y explorar formas alternas de generar redes de mundo pequeño, ver [8]; referencia en la cual los autores combinan las propiedades de los modelos de Watts-Strogatz y Newman-Watts, para generar redes de mundo pequeño mediante patrones inteligentes.

2.3.3 Redes aleatorias

Este tipo de red está compuesta por N nodos, donde cada par de nodos está conectado con una probabilidad p.

Es posible obtener una red aleatoria iniciando con N nodos aislados. Se selecciona un par de nodos y se genera un número aleatorio entre 0 y 1. Si el número es mayor que p, se conecta el par de nodos. De lo contrario, permanecen desconectados. Lo anterior, se repite por cada par de nodos $N(N-1)/2$ [9].

Las redes aleatorias, son también conocidas como redes Erdős-Rényi. Esto, en honor a los dos matemáticos de nacionalidad húngara Paul Erdős y Alfréd Rényi, quienes tomaron un papel importante en el entendimiento de las propiedades de este tipo de redes.

Existen dos definiciones de red aleatoria:

- Modelo $G(N, L)$: N nodos están conectados mediante L enlaces, colocados aleatoriamente. Erdős y Rényi utilizaron esta definición en sus artículos acerca de redes aleatorias [10].
- Modelo $G(N, p)$: Cada par de N nodos está conectado con una probabilidad p, éste, es un modelo introducido por el matemático E. N. Gilbert [11].

El modelo $G(N, L)$, fija el número de conexiones existentes en la red, es decir la topología de estas redes no cambia con el paso del tiempo. Por otro lado, en el modelo $G(N, p)$, la topología sí puede variar debido a que las conexiones no permanecen constantes, ofreciendo un ambiente más cercano a lo que ocurre en el mundo real.

En este trabajo de investigación suponemos que la topología de las redes no varía. Por esta razón, las redes aleatorias mostradas en los ejemplos realizados en capítulos posteriores, son generadas mediante el modelo $G(N, L)$.

Capítulo 3

Osciladores caóticos de orden fraccionario

En el presente capítulo, se habla brevemente sobre la historia del cálculo fraccionario. Se presentan los preliminares matemáticos necesarios para la solución numérica de los osciladores caóticos utilizados en la tesis y algúnas simulaciones.

3.1 Origen del cálculo fraccionario

El cálculo fraccionario, se originó en 1695, cuando Gottfried Leibiniz escribió una carta a Guillaume de l'Hôpital, preguntándole si las derivadas de orden entero podrían ser generalizadas a derivadas de orden no entero. A lo que l'Hôpital respondió con una pregunta: "¿Que pasaría si el orden fuera 1/2?". El 30 de septiembre de 1695, fecha considerada como el nacimiento del cálculo fraccionario, Leibiniz respondió: "Eso conducirá a una paradoja, de la cuál algún día se extraerán consecuencias útiles"[12].

De las definiciones más populares para la solución de la integro-diferencial fraccionaria están: La definición de Caputo, la definición de Riemann-Liouville y la definicion de Gründwald-Letnikov. Esta última definición, ha sido utilizada en

numerosos trabajos de la literatura para la solución numérica de la derivada fraccionaria. En esta tesis, utilizamos la definición de Gründwald-Letnikov debido a su popularidad para desarrollar simulaciónes numéricas entre los expertos en el tema del cálculo fraccionario.

3.2 Preliminares matemáticos del cálculo fraccionario

El cálculo fraccionario, es una generalización de la integración y la diferenciación al operador integro-diferencial de orden no entero ${}_aD_t^\alpha$, con a y t como los límites de la operación, y $\alpha \in \mathbb{R}$ [13]. El operador continuo integro-diferencial, está definido por:

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

Como ya se mencionó anteriormente, la definición de Grünwald-Letnikov fue utilizada para la solución numérica de las ecuaciones diferenciales de orden fraccionario que se presentan en la tesis. Esta definición, está descrita matemáticamente de la siguiente manera:

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

Los coeficientes binomiales son calculados mediante la relación entre la función *Gamma* de Euler denotada por Γ_e y la factorial de la siguiente manera:

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

La siguiente expresion surge de una relación derivada de la definición de Grünwald-Letnikov y puede ser utilizada para la solución numérica de las derivadas fraccionarias:

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

donde L_m es la "longitud de memoria", $t_k = kh$, h es el paso de tiempo y $(-1)^j \begin{pmatrix} q \\ j \end{pmatrix}$ son los coeficientes binomiales $c_j^{(q)} (j = 0, 1, \ldots)$. Los coeficientes binomiales se calculan de la siguiente manera:

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

De lo anterior, la solución general para la ecuación diferencial

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

puede ser expresada de la siguiente forma:

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

donde $v = 1$ para $k < (L_m/h)$ y $v = k - (L_m/h)$ para $k > (L_m/h)$. Si el principio de memoria corta no es utilizado, entonces $v = 1 \; \forall k$.

3.3 Osciladores caóticos de orden fraccionario

Este tipo de osciladores, presentan un comportamiento caótico, para ciertos valores en los parámetros que conforman su modelo matemático. Se consideran de orden fraccionario, pues el orden de las ecuaciones diferenciales que constituyen al oscilador, no es de orden entero. Este tipo de osciladores permite modelar comportamientos de una manera más precisa, ya que cuentan con una mayor resolución. En el encriptado caótico de datos, ofrecen un mayor espacio de llave, gracias a esta característica.

En un sistema n-dimensional constituido por ecuaciones diferenciales de orden fraccionario. El orden de la derivada fraccionaria está definido por $q_1, q_2, \ldots, q_n$. Se le conoce como sistema conmensurado si $q_1 = q_2 = \cdots = q_n$, de lo contrario, se le conoce como sistema no conmensurado.

En este trabajo de tesis, se emplean ambos tipos de sistemas en los ejemplos mostrados posteriormente. Sin embargo, es importante aclarar que durante las simulaciones, q_n no varía una vez fijado su valor numérico; esto provocaría un cambio en las dinámicas del sistema debido a su naturaleza caótica. Una variación en estas dinámicas resultaría en una recuperación erronea de los mensajes encriptados, y no es conveniente para los fines de este trabajo de investigación.

A continuación, se presentan ejemplos de algunos osciladores caóticos de orden fraccionario. Las simulaciones realizadas fueron programadas en lenguaje C++ sin utilizar el principio de memoria corta. Los valores numéricos obtenidos, fueron graficados mediante MATLAB®.

3.3.1 Oscilador Lü caótico de orden fraccionario

El modelo matemático correspondiente al oscilador Lü caótico de orden fraccionario [14], es el siguiente:

$$\begin{cases} {}_0D_t^{q_1}x(t) &= a(y(t)-x(t)), \\ {}_0D_t^{q_2}y(t) &= -x(t)z(t)+cy(t), \\ {}_0D_t^{q_3}z(t) &= x(t)y(t)-bz(t). \end{cases} \tag{3.8}$$

En la Figura 3.1, se muestra el atractor al cuál convergen las trayectorias del oscilador Lü, el cual presenta un comportamiento caótico utilizando los parámetros: $a = 36, b = 3, c = 20$ y un orden en sus derivadas derivadas: $q_1 = q_2 = q_3 = 0.95$ [13]. Las condiciones iniciales utilizadas para generar el atractor mostrado en la Figura 3.1, son: $(x(0), y(0), z(0)) = (0.1, 0.1, 2)$.

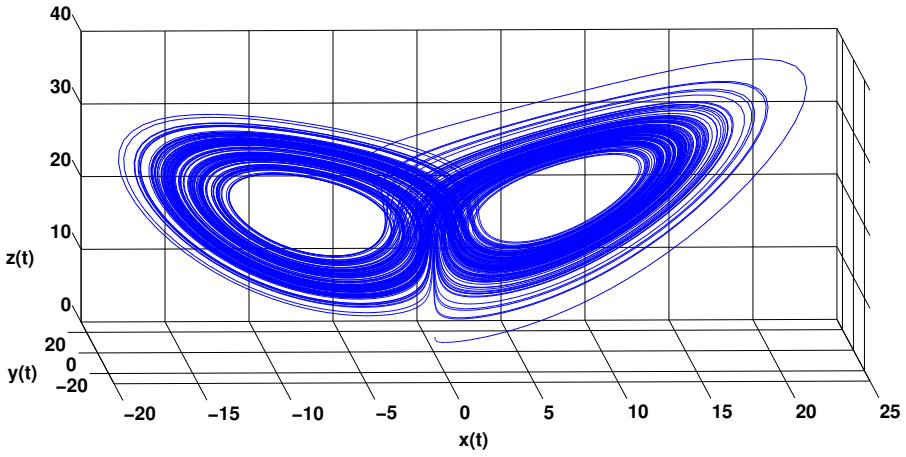


Figura 3.1: Atractor caótico del oscilador Lü de orden fraccionario para parámetros: $a = 36, b = 3, c = 20$, derivadas: $q_1 = q_2 = q_3 = 0.95$, y condiciones iniciales: $(x(0), y(0), z(0)) = (0.1, 0.1, 2)$.

En la Figura 3.2, se muestra la evolución temporal de los estados del oscilador Lü caótico de orden fraccionario.

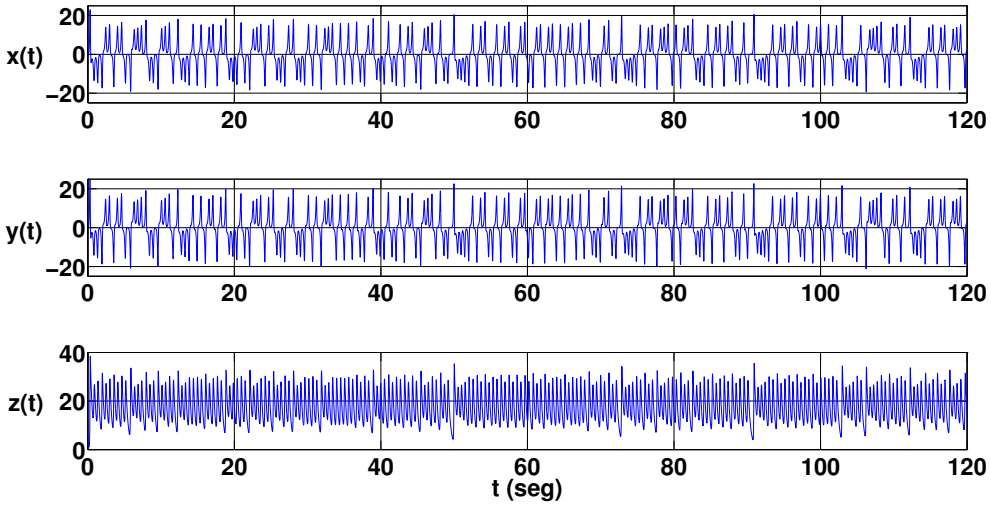


Figura 3.2: Evolución temporal de los estados $x(t), y(t)$ y $z(t)$ del oscilador Lü caótico de orden fraccionario.

3.3.2 Oscilador Rössler caótico de orden fraccionario

El conjunto de ecuaciones que describen el comportamiento del oscilador Rössler caótico de orden fraccionario [15], es el siguiente:

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

En la Figura 3.3, se muestra el atractor caótico del oscilador Rössler en su versión fraccionaria con valores en sus parámetros: $a = 0.5, b = 0.2, c = 10$, derivadas: $q_1 = q_2 = q_3 = 0.9$ [13], y condiciones iniciales: $(x(0), y(0), z(0)) = (0.5, 1.5, 0.1)$.

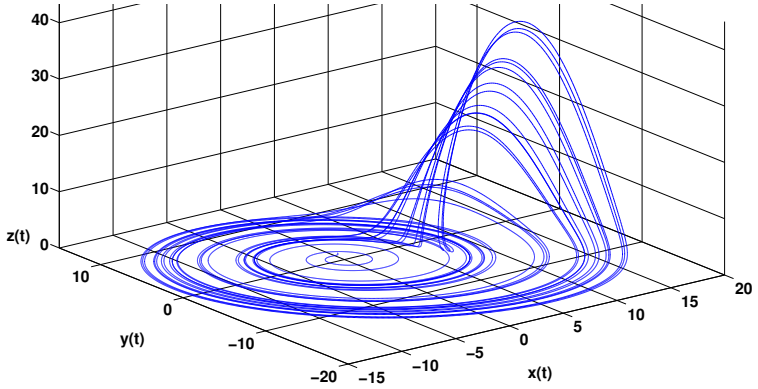


Figura 3.3: Atractor caótico del oscilador Rössler de orden fraccionario para parámetros: $a = 0.5, b = 0.2, c = 10$, derivadas: $q_1 = q_2 = q_3 = 0.9$, y condiciones iniciales: $(x(0), y(0), z(0)) = (0.5, 1.5, 0.1)$.

En la Figura 3.4, se muestra la evolución temporal de los estados del oscilador Rössler caótico de orden fraccionario.

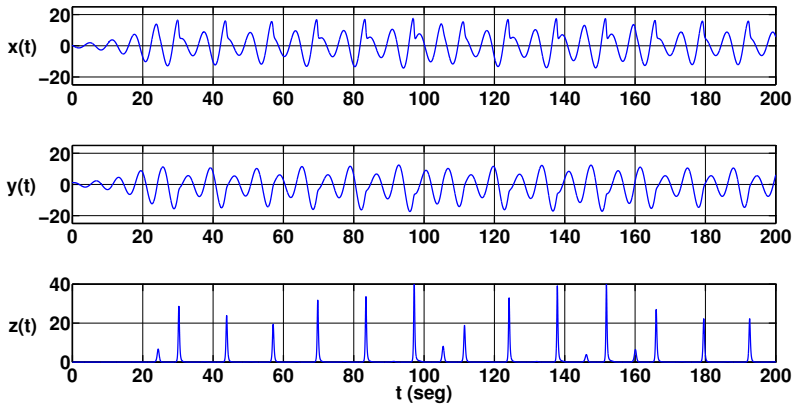


Figura 3.4: Evolución temporal de los estados $x(t), y(t)$ y $z(t)$.

3.3.3 Oscilador Arneodo caótico de orden fraccionario

El conjunto de ecuaciones que describen el comportamiento del oscilador Arneodo de orden fraccionario [16], es el siguiente:

$$\begin{cases} {}_0D_t^{q_1}x(t) &= y(t), \\ {}_0D_t^{q_2}y(t) &= z(t), \\ {}_0D_t^{q_3}z(t) &= -\beta_1 x(t) - \beta_2 y(t) - \beta_3 z(t) + \beta_4 x^3(t). \end{cases} \tag{3.10}$$

El oscilador Arneodo en su versión fraccionaria, presenta un comportamiento caótico para parámetros: $\beta_1 = -5.5, \beta_2 = 3.5, \beta_3 = 0.8, \beta_4 = -1$, y orden de sus derivadas: $q_1 = 0.97$, $q_2 = 0.97$, $q_3 = 0.96$ [13]. Su atractor caótico, se ilustra en la Figura 3.5, utilizando condiciones iniciales en: $(x(0), y(0), z(0)) = (2.1, -1.9, 3.2)$.

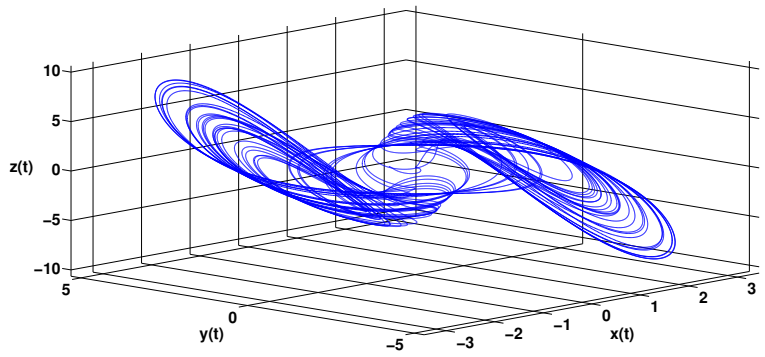


Figura 3.5: Atractor caótico del oscilador Arneodo de orden fraccionario para parámetros: $\beta_1 = -5.5, \beta_2 = 3.5, \beta_3 = 0.8, \beta_4 = -1$, derivadas: $q_1 = 0.97, q_2 = 0.97, q_3 = 0.96$, y condiciones iniciales: $(x(0), y(0), z(0)) = (2.1, -1.9, 3.2)$.

En la Figura 3.6, se muestra la evolución temporal de los estados del oscilador Arneodo caótico de orden fraccionario.

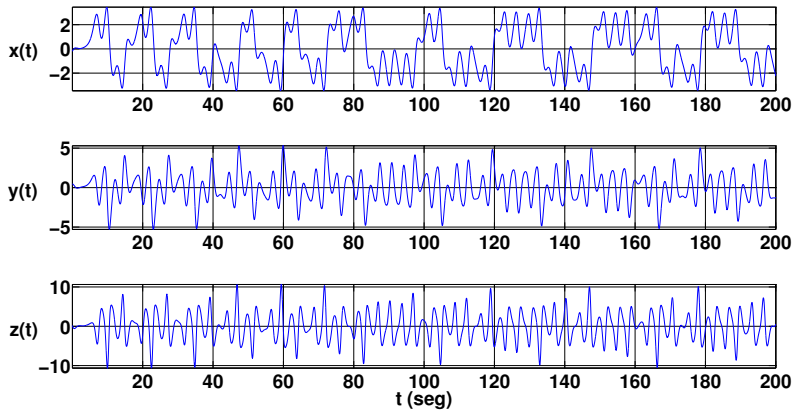


Figura 3.6: Evolución temporal de los estados $x(t), y(t)$ y $z(t)$.

Capítulo 4

Criptografía

En este capítulo, se abordan diversos puntos a considerar durante la utilización de sistemas criptográficos. De igual manera, se dan a conocer conceptos importantes para el presente trabajo de investigación.

4.1 Introducción

Como ya se había mencionado en el Capítulo 1, la criptografía, es la parte de la criptología que se encarga del diseño de sistemas criptográficos; también conocidos como criptosistemas.

A continuación, se expone un concepto concreto de sistema criptográfico, su objetivo principal y puntos a considerar para complir con dicho objetivo.

4.2 Sistemas criptográficos

Se le conoce como sistema criptográfico, al conjunto de elementos que tienen como objetivo procesar datos y hacerlos ilegibles para entidades no autorizadas; pero recuperables y legibles para el receptor autorizado. Comúnmente estos elementos son:

la llave, el algoritmo de cifrado, y el algoritmo de descifrado.

4.3 Seguridad de un sistema criptográfico

Un sistema criptográfico, tiene como objetivo principal dar seguridad a alguna tarea en particular. Este trabajo de investigación esta enfocado a la transmisión de mensajes de un emisor hacia uno o varios receptores. Por lo tanto, es de interés dar seguridad a dichas entidades y proteger su información contra amenazas durante el intercambio de datos.

A continuación se mencionan algunos puntos importantes a considerar, para favorecer la seguridad de un sistema criptográfico.

4.3.1 Espacio de llave secreta

El espacio de la llave, hace referencia a la riqueza o versatilidad que ofrece al ser utilizada por el algoritmo de encriptado. También se puede ver como la amplitud del rango de valores que pudiera presentar la llave.

De lo anterior, se puede deducir que una mayor amplitud de espacio de llave, conlleva un mayor nivel de seguridad en el algoritmo. Esto, debido al incremento de combinaciones posibles que puede tomar la llave.

4.3.2 Sensibilidad a llave secreta

Este concepto esta ligado al efecto que produce la modificación de la llave, sobre el algoritmo de encriptado o sobre el dato recuperado.

Lo anterior, es muy notable en el encriptado caótico, ya que frecuentemente

las condiciones iniciales del sistema son utilizadas como la llave del algoritmo. Debido a la dependencia sensitiva propia de los sistemas caóticos, un ligero cambio en sus condiciones iniciales, conduce a una divergencia entre las dinámicas finales del sistema caótico. Afectando así, los valores numéricos utilizados por el algoritmo de encriptado, y a su vez provocando un error de descifrado.

Se dice que un sistema es sensible a sus condiciones iniciales si cumple con la siguiente definición [17]:

Definicion 1. $f : J \to J$ tiene dependencia sensitiva a condiciones iniciales si existe $\delta > 0$ tal que, para cualquier $x \in J$ y cualquier vecino N de x, existe $y \in N$ y $n \geq 0$ tal que $|f^n(x) - f^n(y)| > \delta$.

En la Figura 4.1 se muestra la divergencia entre las dinámicas del estado $x(t)$ de un oscilador caótico Lü de orden fraccionario al sufrir un cambio en sus condiciones iniciales.

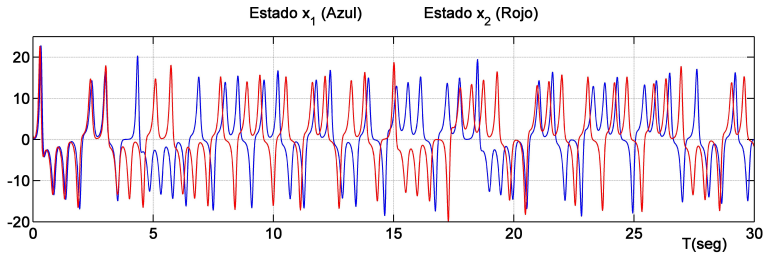


Figura 4.1: Dependencia a condiciones iniciales: Oscilador caótico Lü de orden fraccionario: $x_1(0), y_1(0), z_1(0) = (1, 0.1, 2.5)$ y $x_2(0), y_2(0), z_2(0) = (1, 0.2, 2.5)$.

4.3.3 Error de descifrado

Tal como su nombre lo indica. Si existe una diferencia entre el dato recuperado y el dato original, hablamos de un error de recuperación o error de descifrado.

Dependiendo del tipo de dato, se puede considerar un margen de tolerancia en el error de recuperación. Es decir, que tan grande puede ser el error sin que afecte

realmente el objetivo del sistema criptográfico.

4.3.4 Histograma

En el ámbito del encriptado caótico, el histograma es comúnmente utilizado en el procesamiento de imágenes. En esta área, el histograma de una imagen expone una gráfica de barras, en la cual se agrupan los valores numéricos de los píxeles de la imagen, agrupados ordenadamente dependiendo su valor.

Antes de continuar, es necesario comprender los siguientes conceptos:

- Píxel: En una imagen tipo RGB, un píxel es la unidad básica de color compuesto por tres valores numéricos.
- Intensidad de brillo: En una imagen tipo RGB, es el valor numérico que posee cada canal del píxel.

En la Figura 4.2, se muestra una imagen de un león en formato BMP tipo RGB. También se muestran los histogramas de sus tres canales correspondientes R, G y B.

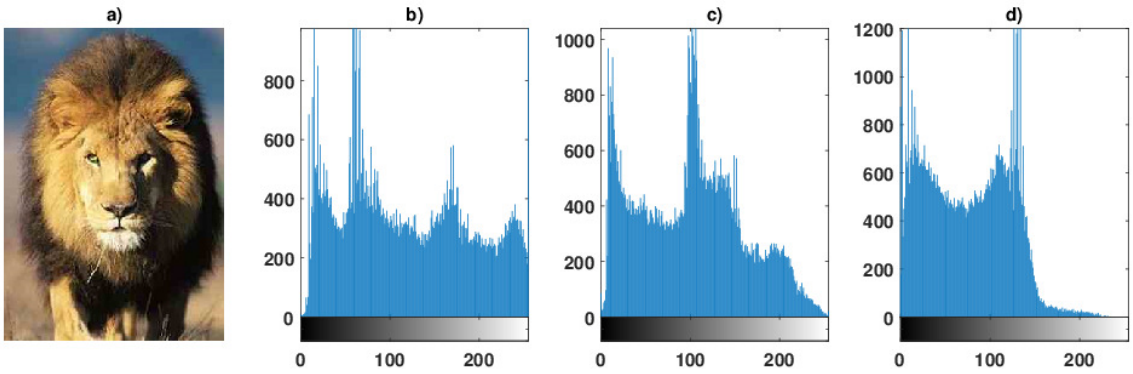


Figura 4.2: a) Imagen de león, b) Histograma del canal R, c) Histograma del canal G, d) Histograma del canal B.

Posteriormente, los píxeles de la imagen son revueltos aleatoriamente como se muestra la Figura 4.3. Los histogramas resultantes son iguales a los de la Figura 4.2 debido a que los píxeles solo fueron cambiados de posición en la imagen integramente.

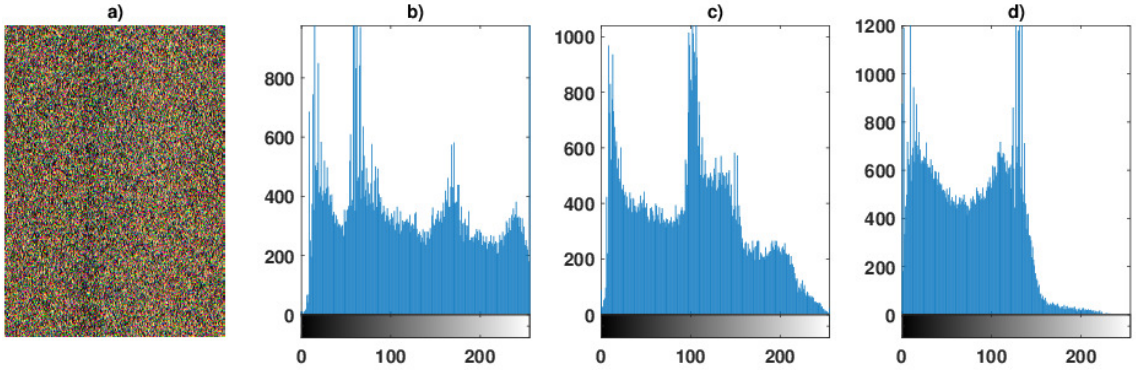


Figura 4.3: a) Imagen de león con sus píxeles revueltos, b) Histograma del canal R, c) Histograma del canal G, d) Histograma del canal B.

De lo anterior, se puede inferir que en el encriptado de imágenes, es importante considerar que el algoritmo de cifrado logre modificar también los histogramas de la imagen. Esto, con la intención de despistar al atacante y mejorar la efectividad del encriptado.

4.3.5 Análisis de correlación

En el encriptado de información, un análisis de correlación de señales proporciona una idea sobre la integridad del algoritmo que se está utilizando para cifrar los mensajes. Otorga un panorama acerca de la similitud entre el mensaje entrante y el mensaje encriptado. De esta forma, se puede modificar el algoritmo de manera pertinente en caso de ser necesario, y así mejorar su seguridad.

Matemáticamente, la correlación realiza una comparación entre dos valores numéricos. Si la alteración del primer valor afecta al segundo, existe una dependen-

cia entre ellos y se dice que dichos valores estan correlacionados. El grado en que estos valores estan correlacionados puede ser medido mediante los coeficientes de correlación.

El coeficiente de correlación C_{AB} para cada par de secuencias $A = [a_1, \ldots, a_N]$ y $B = [b_1, \ldots, b_N]$, donde N es el número de elementos que componen dichas secuencias, se calculan como [18]:

$$C_{AB} = \frac{\sum_{i=1}^{N}(A_i - \bar{A})(B_i - \bar{B})}{[\sum_{i=1}^{N}(A_i - \bar{A})^2]^{1/2}[\sum_{i=1}^{N}(B_i - \bar{B})^2]^{1/2}}, \tag{4.1}$$

donde $\bar{A} = \frac{1}{N}\sum_{i=1}^{N} A_i$ y $\bar{B} = \frac{1}{N}\sum_{i=1}^{N} B_i$ son los valores principales de A y B respectivamente.

En la Figura 4.4, se muestra una imagen antes y después de ser encriptada mediante el método de encriptado aditivo convencional [19]. Posteriormente se calcula la correlación que existe entre ambas imágenes.

Figura 4.4: a) Imagen original, b) Imagen encriptada mediante el método de encriptado aditivo convencional .

En la Tabla 4.1 se muestran los resultados obtenidos del análisis de correlación mediante la ecuación (4.1) entre la imagen original y la imagen encriptada mediante

el método de encriptado aditivo convencional.

Tabla 4.1: Coeficientes de correlación obtenidos

Canal	Coeficiente de correlación entre la imagen original y la imagen encriptada
Rojo	-0.0792
Verde	-0.0736
Azul	-0.0155

4.3.5.1 Interpretación de los coeficientes de correlación

A continuación, se proporciona información importante para interpretar los valores numéricos obtenidos de los coeficientes de correlación.

- **Correlación negativa:** Si el coeficiente de correlación es negativo, existe correlación inversa. A valores altos de una de las variables le suelen corresponden valores bajos de la otra y viceversa. Cuanto más próximo sea el valor del coeficiente de correlación a -1 más correlacionadas están estas variables en sentido opuesto.
- **Correlación negativa perfecta:** Cuando el coeficiente de correlación entre dos variables es -1 supone una relación lineal con pendiente negativa.
- **Correlación positiva:** Si el coeficiente de correlación es positivo, existe correlación directa. A valores altos de una de las variables le corresponden valores altos de la otra y de igual manera si se trata de valores bajos. Cuanto más próximo sea el valor del coeficiente de correlación a 1 más correlacionadas están estas variables en sentido opuesto.
- **Correlación positiva perfecta:** Cuando el coeficiente de correlación entre dos variables es 1 supone una relación lineal con pendiente positiva.

- **Correlación nula:** No existe correlación entre ambas variables si el coeficiente de correlación es igual a cero.

4.3.6 Entropía

En informática, la entropía es una medida de incertidumbre existente en un conjunto de mensajes. También, se puede interpretar como una medida de desorden causado por un algorítmo de encriptado sobre el dato que se desea cifrar. Un buen método de encriptado provoca una alta entropía o un mayor grado de desorden en el dato encriptado.

La entropía $H(m)$ de un mensaje m_i es calculada de la siguiente forma [20]:

$$H(m) = \sum_{i=0}^{2^N} p(m_i)\log_2(1/p(m_i)). \tag{4.2}$$

Donde N representa el número de bits del mensaje; 2^N denota los posibles valores; $p(m_i)$ es la probabilidad de m_i; $\log_2$ representa al logaritmo base 2. En el caso ideal, se desea que el valor numérico de la entropía sea equivalente al número de bits de la imagen, i.e. $H(m) = N$.

4.3.7 Tiempo de cifrado y descifrado

Si bien es importante considerar el esfuerzo computacional al momento de seleccionar un algoritmo para encriptar los mensajes, también es de vital importancia considerar el tiempo de descifrado; principalmente por entidades no autorizadas.

Durante la transmisión de datos, es prioridad asegurar la fortaleza del dato encriptado. El tiempo de procesamiento depende de diversos factores: el tamaño de la llave, el algoritmo utilizado y principalmente la potencia del sistema de cómputo.

En el peor de los casos, se debe considerar que el mensaje puede ser vulnerado. El tiempo que puede tardar una tercer persona en descifrar el mensaje sin autorizacion, debe ser considerado impráctico para suponer un sistema criptográfico seguro.

Como se menciona anteriormente, existen diversas maneras de aumentar la seguridad de un sistema criptográfico; la selección de éstas, dependerá de las necesidades del experto en encriptado de información.

Capítulo 5

Algoritmo de cifrado caótico propuesto

5.1 Encriptado de imágenes tipo RGB

Una imagen tipo RGB (por sus siglas en inglés: red, green, blue) crea los colores a partir de la combinación del rojo, el verde y el azul.

En una imagen BMP tipo RGB, los datos numéricos de cada píxel se guardan en tres bytes. Cada byte almacena información sobre la intensidad de brillo para el rojo, verde y azul. El rango convencional de valores esta entre 0 y 255, dando un total de 256 niveles de intensidad. En total, brindan $256 \times 256 \times 256 = 16.777.216$ opciones de color. A estas imágenes se les conoce como imágenes de color verdadero. Esto se muestra en la Figura 5.1, en donde se puede observar un breve catálogo de colores.

Color	Nombre	Intensidad Rojo, Verde, Azul.
	Blanco	255,255,255
	Negro	0,0,0
	Rojo	255,0,0
	Verde	0,255,0
	Azul	0,0,255
	Amarillo	255,255,0
	Morado	128,0,128

Figura 5.1: Breve catálogo de colores.

En este trabajo de investigación, definimos tres matrices en las que se almacenan los valores numéricos de la intensidad de brillo de cada píxel. Hemos llamado a estas matrices: R, G y $B \in \mathbb{R}^{n\times p}$. Las cuales pueden ser definidas matemáticamente como sigue:

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

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

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

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

5.2 Manipulación de la imagen

Para encriptar las imágenes, las columnas de las matrices R, G y $B \in \mathbb{R}^{n\times p}$ fueron concatenadas formando tres nuevas matrices columna:

$$R' = \begin{pmatrix} R_1 \\ R_2 \\ \vdots \\ R_p \end{pmatrix} = \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_v \end{pmatrix} \; ; \quad G' = \begin{pmatrix} G_1 \\ G_2 \\ \vdots \\ G_p \end{pmatrix} = \begin{pmatrix} g_1 \\ g_2 \\ \vdots \\ g_v \end{pmatrix} \; ; \quad B' = \begin{pmatrix} B_1 \\ B_2 \\ \vdots \\ B_p \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_v \end{pmatrix} ,$$

donde $v = n \times p$.

De esta manera se tienen tres matrices definidas como: $R' = (r_v) \in \mathbb{N}^{v\times 1}$, $G' = (g_v) \in \mathbb{N}^{v\times 1}$, $B' = (b_v) \in \mathbb{N}^{v\times 1}$, las cuales contienen valores entre $[0, 255]$.

5.3 Algoritmo aditivo convencional

El método aditivo convencional consiste en sumar una señal de salida (en este caso se utilizan señales caóticas), a la señal de información. Esta suma es enviada a través de un canal público desde el emisor al receptor. Una segunda señal caótica del emisor es enviada y utilizada por el receptor. Éste, sincroniza un sistema caótico equivalente al del emisor. El mensaje es recuperado mediante la sustracción de la señal reconstruida a la suma transmitida [19]. Lo anterior, se ilustra mediante el diagrama de la Figura 5.2.

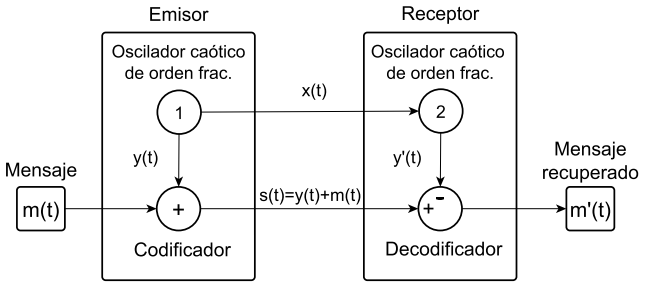


Figura 5.2: Diagrama básico del encriptado caótico convencional de dos canales. El mensaje encriptado $s(t)$ resulta de la suma entre el mensaje original $m(t)$ y una señal caótica $x(t)$. El dato encriptado es enviado a través de un canal público al receptor. En paralelo se envía un estado $y(t)$ al receptor para generar un estado $x'(t)$. El estado generado es sustraido de $s(t)$ recuperando un mensaje $m'(t)$.

5.4 Algoritmo propuesto

El objetivo es proponer un algoritmo más ligero en comparación al método de encriptado aditivo convencional, proteger los datos que se envían a travéz del canal público y mejorar la calidad de encriptado, conservando la característica de ser un algoritmo sencillo.

Para comenzar, se manipula la imagen con la finalidad de esconder sus histogramas. Este proceso consta de dos pasos: cambiar la posición de los píxeles de la imagen conservando los tres valores que los constituyen, es decir sus intensidades de brillo no se desordenan. Posteriormente desordenar los valores numéricos de las intensidades de brillo de los píxeles a través de los canales; cada canal conserva el mismo número de valores pero no necesariamente los mismos que poseían originalmente. Como resultado se obtiene una imagen desordenada con histogramas diferentes a los de la imagen original.

Debido a las amplitudes que presentan las muestras de las señales caóticas con las que se trabajaron en esta tesis, se opta por cambiar el rango de valores de los píxeles de las imágenes de $[0, 255] \rightarrow [0, 1]$. Lo anterior, se debe a que de otra manera, se tendrían que amplificar los valores de la señal caótica por una ganancia equivalente a 255. Para realizar

una implementación fisica, resulta más conveniente manipular los píxeles de la imagen que amplificar las señales caóticas.

Con el objetivo de esconder las condiciones iniciales utilizadas para generar las dinámicas caóticas y evitar enviarlas a travéz de algún canal público, se propone iniciar el proceso de encriptado en $x_{i+l}, y_{i+l}, z_{i+l}, w_{i+l}$ con $l \neq 0$. Lo anterior se ilustra en la Figura 5.3 aplicando el método de encriptado aditivo convencional para simplificar las operaciones.

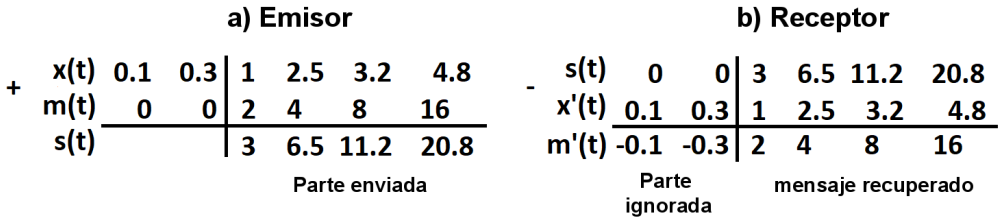


Figura 5.3: Ejemplo ilustrado del envío del archivo encriptado sin exponer las condiciones iniciales del oscilador. a) Un mensaje $m(t)$ es sumado a la señal caótica $x(t)$ en un punto inicial seleccionado. El mensaje encriptado $s(t)$ es enviado a través de un canal público sin incluir la condición inicial $x(t) = 0.1$. b) La señal caótica $x'(t)$ es sustraída del mensaje encriptado, recuperando el mensaje $m(t)$ ignorando los datos anteriores al punto inicial seleccionado para encriptar.

Para compensar el desfase en el encriptado, se generan l muestras adicionales de las señales caóticas. Matemáticamente esto se puede representar mediante $X, Y, Z, W \in \mathbb{R}^{v' \times 1}$, donde $v' = v + l$:

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{v'} \end{pmatrix} \quad ; \quad Y = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_{v'} \end{pmatrix} \quad ; \quad Z = \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_{v'} \end{pmatrix} \quad ; \quad W = \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_{v'} \end{pmatrix} .$$

El algoritmo utilizado por el emisor es el siguiente:

$$\begin{cases} \Psi_{R_i} = (\zeta r_i + x_{i+l})w_{i+l}, \\ \Psi_{G_i} = (\zeta g_i + y_{i+l})w_{i+l}, \quad i = 1, 2, \ldots, v. \\ \Psi_{B_i} = (\zeta b_i + z_{i+l})w_{i+l}. \end{cases} \tag{5.1}$$

Donde $\zeta = 1/255$ se encarga de cambiar la escala de los píxeles a $[0, 1]$; r_i, g_i, b_i contienen los valores numéricos de las intensidades de brillo de la imagen en cada canal; x_{i+l}, y_{i+l}, z_{i+l}, w_{i+l} contienen los valores numéricos de las amplitudes de las muestras de las señales caóticas.

De lo anterior, Ψ_{R_i}, Ψ_{G_i}, $\Psi_{B_i} \in \mathbb{R}$ contienen los valores numéricos encriptados extraídos de las operaciones realizadas por el algoritmo propuesto.

El algoritmo utilizado por el receptor es el siguiente:

$$\begin{cases} r_i = \zeta'((\Psi_{R_i}/w_{i+l}) - x_{i+l}), \\ g_i = \zeta'((\Psi_{G_i}/w_{i+l}) - x_{i+l}), \\ b_i = \zeta'((\Psi_{B_i}/w_{i+l}) - x_{i+l}), \end{cases} \tag{5.2}$$

Donde $\zeta' = 255$ se encarga de cambiar la escala de los píxeles a $[0, 255]$. Debido a que el valor de los píxeles es estríctamente de orden entero, en este paso se realiza un redondeo estandar. Como resultado, r_i, g_i, b_i contienen las intensidades de brillo recuperadas sin decimales.

5.5 Ataques convencionales

La metodología propuesta fue sometida a cuatro ataques convencionales [21]:

- **Ataque al texto encriptado:** El atacante solo tiene acceso al dato encriptado.
- **Ataque con texto llano conocido:** El atacante tiene acceso al dato encriptado y a su versión decodificada.
- **Ataque con texto llano elegido:** El atacante tiene acceso a la máquina de encriptado. Puede elegir arbitrariamente textos llanos y obtener su versión encriptada.

- **Ataque con texto encriptado elegido:** El atacante tiene acceso al decodificador. Puede elegir arbitrariamente textos encriptados y obtener su versión decodificada.

El objetivo de estos ataques es obtener cualquier clase de información que ayude a vulnerar la seguridad del algoritmo de encriptado. En el peor de los casos, el atacante podría obtener la llave con la que el algoritmo encripta el/los mensaje(s).

En la Figura 5.4 se propone un esquema de comunicación. Este esquema está basado en un escenario en el cuál el usuario actúa como emisor y receptor, no es necesaria la sincronía y por lo tanto no existe error de recuperación. En este escenario, se pretende almacenar datos de forma segura en un ambiente poco confiable. Un ejemplo de esto, es el almacenamiento de datos en línea utilizando servidores de terceros.

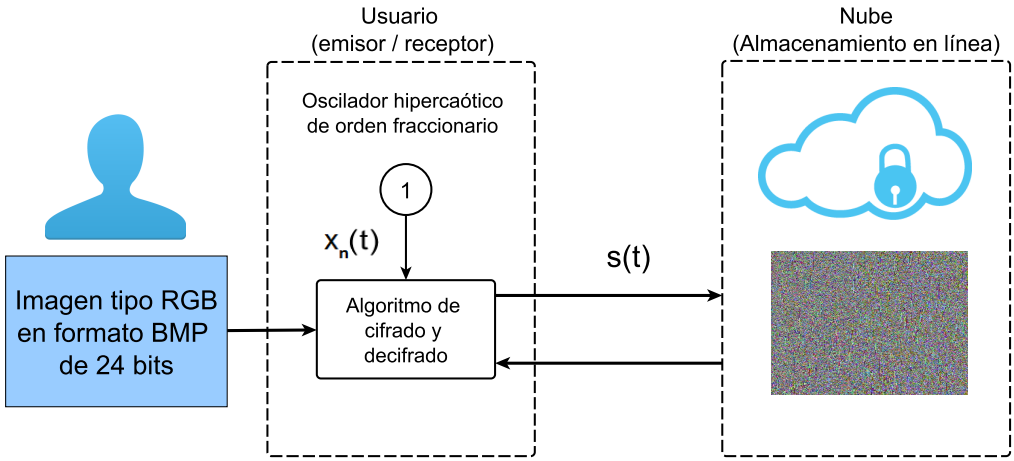


Figura 5.4: Esquema de encriptado Usuario-Nube. El usuario selecciona una llave, encripta el mensaje y lo almacena en un servidor en línea. El usuario descarga el dato encriptado y recupera el mensaje sin error de recuperación.

5.6 Ejemplos

El oscilador hipercaótico de orden fraccionario utilizado en los próximos ejemplos está definido matemáticamente como sigue:

$$\begin{cases} {}_0D_t^{q_1}x(t) &= a(y(t)-x(t))+\mu y(t)z(t), \\ {}_0D_t^{q_2}y(t) &= cx(t)-dx(t)z(t)+y(t)+w(t), \\ {}_0D_t^{q_3}z(t) &= x(t)y(t)-bz(t), \\ {}_0D_t^{q_4}w(t) &= -vy(t). \end{cases} \tag{5.3}$$

Este sistema exhibe un comportamiento hipercaótico cuando sus párametros equivalen a $q_1 = q_2 = q_3 = q_4 = 0.95$, $a = 35, b = 4, c = 25, \mu = 35, v = 100$ [22]. Las condiciones iniciales utilizadas en estos dos ejemplos, actúan como la llave del método de encriptado.

5.6.1 Ejemplo: Efecto producido por la selección de la muestra para iniciar el encriptado

En este ejemplo, se encripta una imagen BMP tipo RGB, utilizando el algoritmo propuesto aplicado al esquema usuario-nube. Debido a que el objetivo de este ejemplo es observar el efecto que causa seleccionar un punto inicial diferente al recuperar la imagen con respecto al seleccionado para encriptarla, la imagen no es desordenada y no se realiza ningún análisis de los histogramas.

En la Figura 5.5 se muestra la imagen a encriptar.

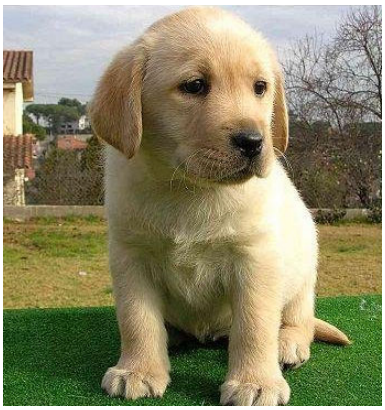


Figura 5.5: Imagen tipo RGB, formato BMP.

Las características de la imagen son las siguientes:

- Tipo de imagen: RGB.
- Dimensiones de la imagen: $n = 364$, $p = 344$.
- $v = n \cdot p = 125,216$.

Información requerida para encriptar y decodificar la imagen:

- Paso de integración: $h = 0.005$ (200 muestras por segundo)
- Muestras de la señal caótica necesarias: $125,216$ muestras.
- Para compensar el desfase del encriptado se agregan 5 segundos a la simulación ($1,000$ muestras).
- Condiciones iniciales (llave correcta): $x(0) = 3.146219, y(0) = 0.102032, z(0) = -1.421112, w(0) = -5.901028$
- Condiciones iniciales (llave errada): $x(0) = 3.146219, y(0) = 0.102032, z(0) = -1.421121$ (error de 9×10^{-6}), $w(0) = -5.901028$

En la Figura 5.6 se muestran los resultados de encriptar la imagen de la Figura 5.5 variando la muestra a partir de la cuál se encripta el mensaje. Se observa la recuperación del mensaje en ambos casos, utilizando la llave correcta y una llave errada.

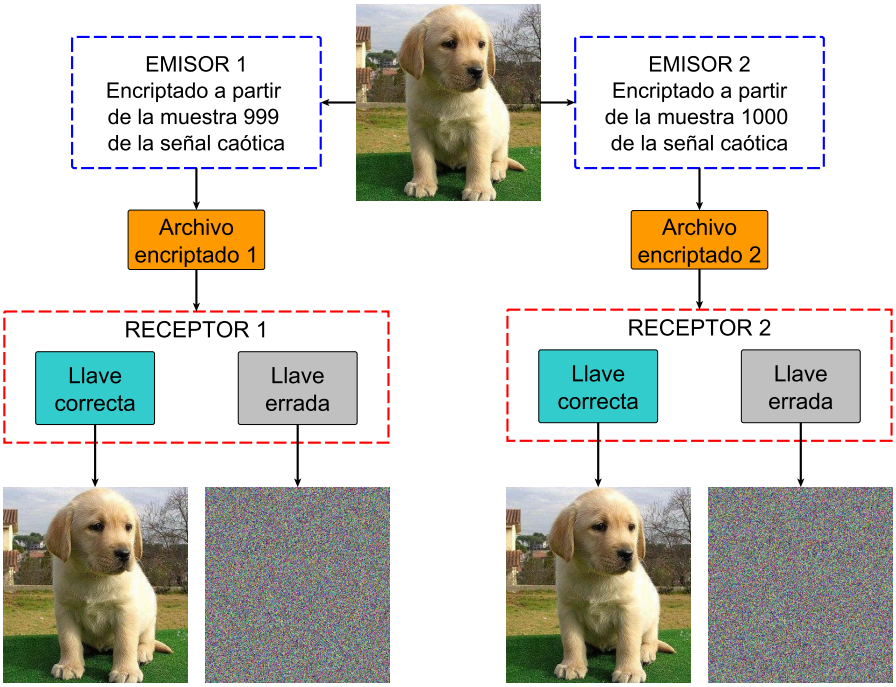


Figura 5.6: Encriptado caótico con desfase de una imagen BMP tipo RGB.

La Figura 5.7 muestra que, el archivo encriptado 1, no puede ser recuperado mediante el receptor 2, aún cuando se utiliza la llave correcta. Esto se debe a que la muestra en la que empieza a decodificar el mensaje no coincide con la muestra inicial utilizada por el emisor para encriptar la imagen.

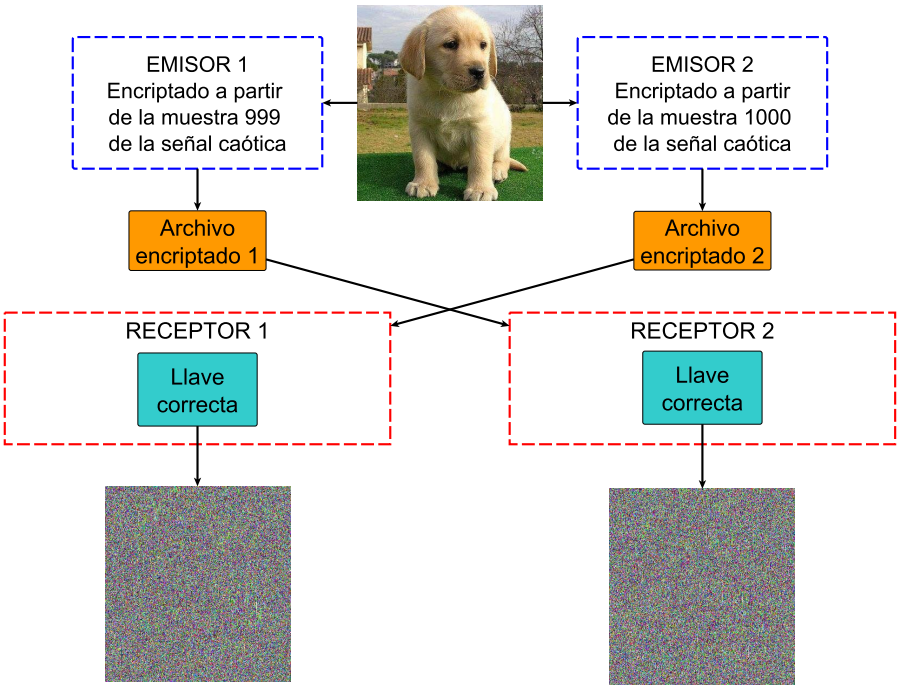


Figura 5.7: Recuperación del archivo encriptado utilizando un receptor con diferente desfase.

5.6.2 Ejemplo: Encriptado de las dimensiones de la imagen y el efecto producido por una recuperación errónea

En este ejemplo, el usuario almacena el archivo encriptado, utilizando algún servicio de almacenamiento en línea (esquema usuario-nube). La Figura 5.8 muestra la imagen a encriptar. Posteriormente se intenta recuperar la imagen utilizando una llave correcta y una llave con error en las condiciones iniciales que enmascaran parte de las dimensiones de la imagen. Se observan los resultados.

La imagen de la Figura 5.8, es encriptada utilizando los siguientes parámetros: condiciones iniciales: $x(0) = 0.572$, $y(0) = 0.931$, $z(0) = 1.245$, $w(0) = 2.923$. Muestra inicial: $k = 12$.

Figura 5.8: Imagen de tres leopardos bebiendo agua. Dimensiones: 1920×1080.

En la Figura 5.9 se muestra la imagen recuperada utilizando la llave correcta.

Figura 5.9: Imagen recuperada utilizando la llave correcta. Dimensiones 1920×1080.

La Figura 5.10 muestra la imagen recuperada con el siguiente error en la llave:

- Condiciones iniciales: $\mathbf{x(0)=1.5}$, $y(0) = 0.931$, z(0)=1.245, w(0)=2.923. Muestra inicial: $k = 12$.

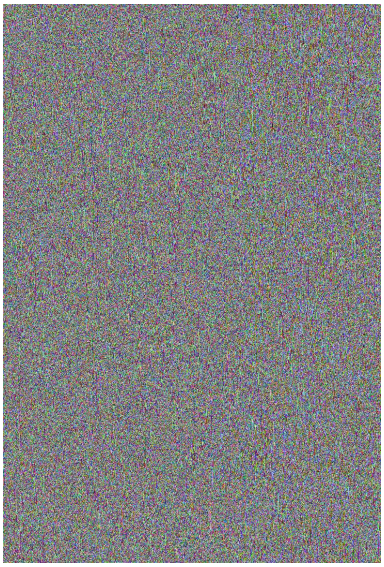


Figura 5.10: Imagen recuperada con error en la llave. Dimensiones: 732×1080.

En la Figura 5.10 se puede observar que la imagen recuperada consta de dimensiones diferentes a la de la imagen original. Esto se debe a que las dimensiones de la imagen son encriptadas utilizando algunos estados del oscilador caótico. Al diferir las condiciones iniciales encargadas de ocultar las dimensiones de la imagen, ésta también sufre cambios al ser recuperada.

Es importante mencionar, que una imagen RGB de dimensiones 1920×1080 posee $2,073,600$ píxeles. Cada píxel esta representado por 3 valores numéricos que representan la intensidad de brillo en R, G y B. A continuación se muestra una breve comparación entre el método aditivo convencional y el propuesto:

- **Método aditivo convencional:**
  - Muestras de la señal necesarias: $6,220,800$
  - Longitud de memoria mínima necesaria: $L_m > 6,220.8$
- **Método propuesto:**
  - Muestras de la señal necesarias: $2,073,600$
  - Longitud de memoria mínima necesaria: $L_m > 2,073.6$

5.7 Análisis de seguridad y comparación con otros algoritmos en la literatura

A continuación se presenta un ejemplo en el cual se encripta una imagen utilizando el algoritmo y la metodología propuesta. En éste apartado se propone desordenar los píxeles de la imagen, y el valor de sus intensidades de brillo. Ésto con la intención de ocultar los histogramas y despistar al atacante agregando incertidumbre al proceso.

5.7.1 Espacio de llave

En el mundo real, no existe llave (contraseña) inmune a ataques exhaustivos (brute-force). Sin embargo, es posible incrementar el tiempo que tarda un ataque exhaustivo en obtenerla. En la Figura 5.11, se muestra una comparación del tiempo que tarda un ataque exhaustivo en vulnerar la llave utilizada por el algoritmo propuesto utilizando hipercáos [1] para encriptar el mensaje, y un algoritmo de encriptado reportado en la literatura.

		Permutaciones por segundo		
Encriptado	Permutaciones totales	1,000 (ataque en línea)	100 billones (ataque rapido fuera de línea	100 trillones (ataque masivo)
Hipercáos[1]	1.11x10^33	3.53x10^17 siglos	3.53x10^12 siglos	3.53x10^9 siglos
Aes-256	1.11x10^77	3.53x10^64 siglos	3.53x10^56 siglos	3.53x10^53 siglos

Figura 5.11: Comparación medida en años que toma un ataque exhaustivo de diferente magnitud en vulnerar la llave al utilizar ciertos algoritmos de encriptado.

[1] Hipercáos suponiendo que se tiene un sistema de cuatro estados, condiciones iniciales entre 20 y -20 con precisión de 6 decimales y una variación en las derivadas fraccionarias de las ecuaciones del sistema entre 0.95 y 0.999

- **Advanced Encryption Standard 256 bits (AES-256)**: 1.1×10^{77} permutaciones.
- **Encriptado con osciladores hipercaóticos de orden fraccionario**: Para condiciones iniciales entre -20 y 20 con precisión de 6 decimales, y un rango de valores en las derivadas fraccionarias entre 0.95 y 0.999 se tienen 1.53×10^{33} permutaciones.

Se observa que el método AES-256 al utilizar una llave de mayor longitud retrasa los ataques exhaustivos por más tiempo. Sin embargo, la longitud de la llave en el encriptado con osciladores hipercaóticos de orden fraccionario no es fija. Es posible incrementar el espacio de llave modificando los parámetros del sistema y aumentando la precisión del algoritmo. De la Figura 5.11, podemos comprobar que el método propuesto es adecuado ya que hace imprácticos los ataques exhaustivos.

5.7.2 Histogramas

A continuación se presentan los resultados de procesar y encriptar una imagen BMP tipo RGB. En la Figura 5.12 se muestra el cambio que sufren los histogramas de la imagen original durante el procedimiento de encriptado.

En el inciso “a”, se exponen los histogramas de la imagen original. En el inciso “b”, se observan los histogramas de la imagen después de desordenar sus píxeles. Se observa que los histogramas no se alteran ya que sus píxeles mantienen sus tres valores en R, G y B intactos.

En el inciso “c”, los valores que conforman a cada píxel, fueron colocados en un solo vector, posteriormente fueron revueltos. Se observa que los histogramas son diferentes. Esto se debe a que todas las intensidades de brillo fueron desordenadas, provocando un cambio de posición y de canal. Es importante mencionar que esto no significa que la amplitud de dichos valores se modifique.

En el inciso “d”, se muestra la imagen mostrada en el inciso “c”, encriptada con el método de encriptado propuesto. Se observa que sus histogramas son diferentes con respecto a los de la imagen original.

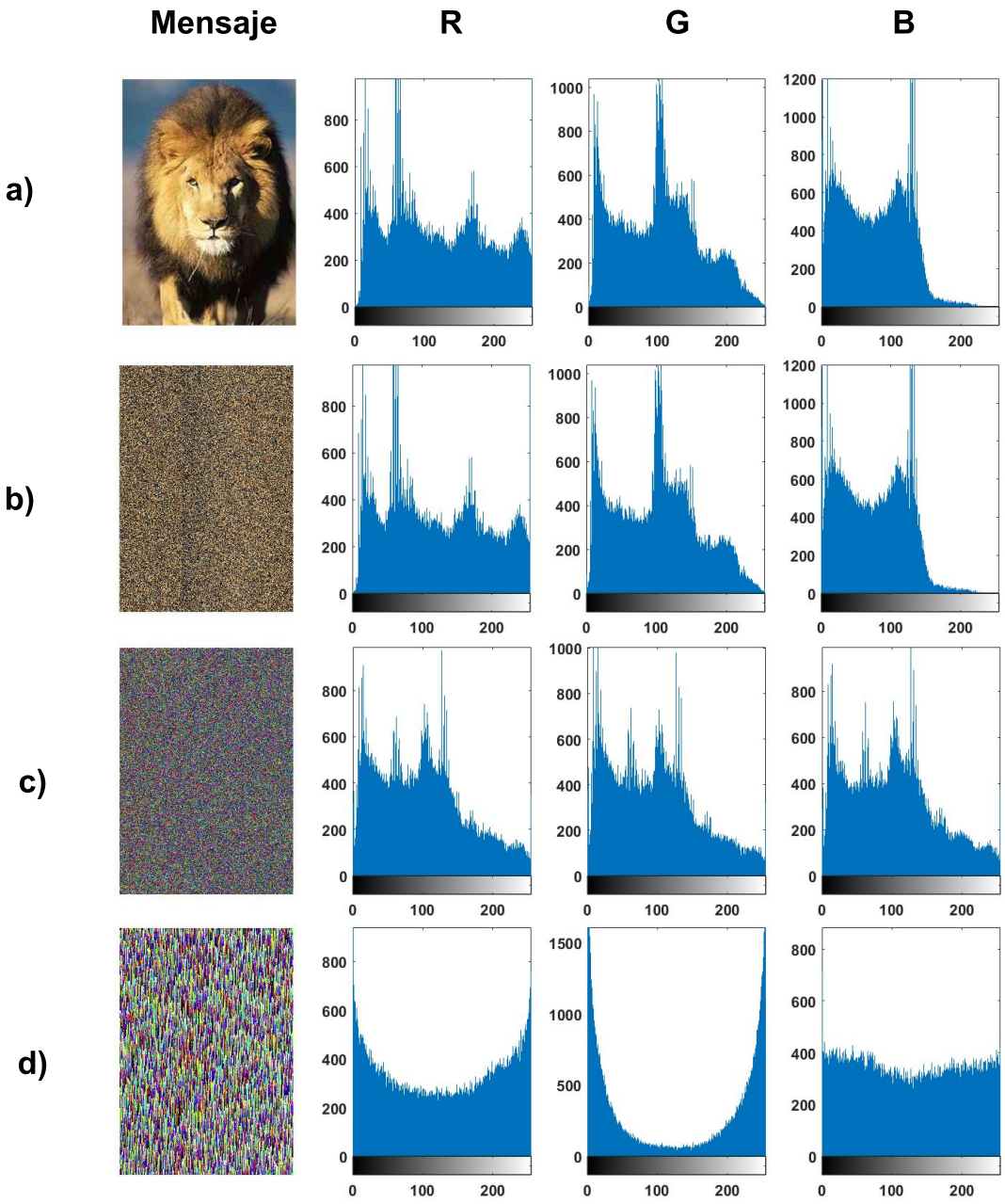


Figura 5.12: a) Histogramas de la imagen original, b) Histogramas de la imagen original con píxeles desordenados, c) Histogramas de la imagen desordenada revolviendo las intensidades de brillo a través de los tres canales, d) Imagen desordenada y encriptada con el método propuesto.

5.7.3 Análisis de correlación y cálculo de la entropía

En la Figura 5.13 se muestra la imagen original antes y despés de ser encriptada. En el inciso "a"se aprecia la imagen original; en el inciso "b"se muestra la imagen encriptada utilizando el método de encriptado aditivo; en el inciso "c"se muestra la imagen encriptada por el método propuesto.

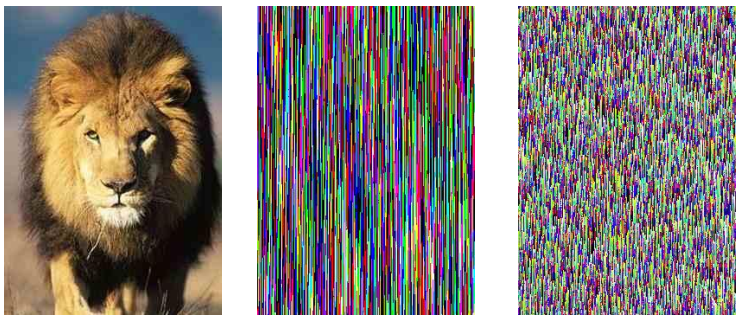


Figura 5.13: a) Imagen original, b) Imagen encriptada con el método de encriptado aditivo convencional, c) Imagen encriptada con el método de encriptado propuesto.

En la Tabla 5.1 se muestran los resultados de calcular los coeficientes de correlación mediante la ecuación (4.1) entre la imagen original y los métodos de encriptado comparados.

Tabla 5.1: Coeficientes de correlación entre la imagen original y los métodos de encriptado comparados.

Canal	Método aditivo	Método propuesto
R	-0.0791	-0.0002
G	-0.0736	-0.0119
B	-0.0155	-0.0248

En la Tabla 5.2 se muestra la entropía que poseen las imágenes mostradas en la Figura 5.13, la cual fue calculada mediante la ecuación (4.2). En imágenes de 8 bits como las que se presentan en esta tesis, lo ideal es obtener un valor de entropía cercano a 8.

Tabla 5.2: Cálculo de entropía

Mensaje	Entropía
Imagen Original	7.7953
Encriptado aditivo	4.5666
Encriptado propuesto	7.7994

5.8 Conclusiones

La metodología propuesta tiene como objetivo proteger la imagen encriptada, evitar incluir cualquier condición inicial del oscilador en el archivo encriptado y reducir el costo computacional en comparación al método de encriptado aditivo. Se comprueba que los ataques de fuerza bruta son imprácticos y se concluye que el método de encriptado es adecuado.

Los píxeles de la imagen son desordenados con la intención de agregar incertidumbre y despistar al atacante, ocultando los histogramas de la imagen original antes de ser encriptada con el algorítmo propuesto. Se observa que con el método propuesto se obtiene una menor correlación entre la imagen original y la encriptada, y posee una mayor entropía en comparación al método de encriptado aditivo convencional.

Capítulo 6

Control Pinning

En este capítulo, se muestran los preliminares matemáticos necesarios para lograr la sincronía entre los nodos que conforman una red compleja. Se muestra una serie de ejemplos sobre sincronización de redes complejas en configuración bidireccional, y la utilización de la técnica de control pinning para manipular las dinámicas emergentes que estas producen.

6.1 Sincronización de redes complejas no estructurales via control pinning

El control pinning, es una estrategia de control que puede ser utilizada para manipular de manera directa, una fracción de los nodos presentes en una red compleja. Estos nodos son seleccionados estratégicamente como se muestra en la Figura 6.1, en la cuál se seleccionaron los tres nodos de mayor grado presentes en la red.

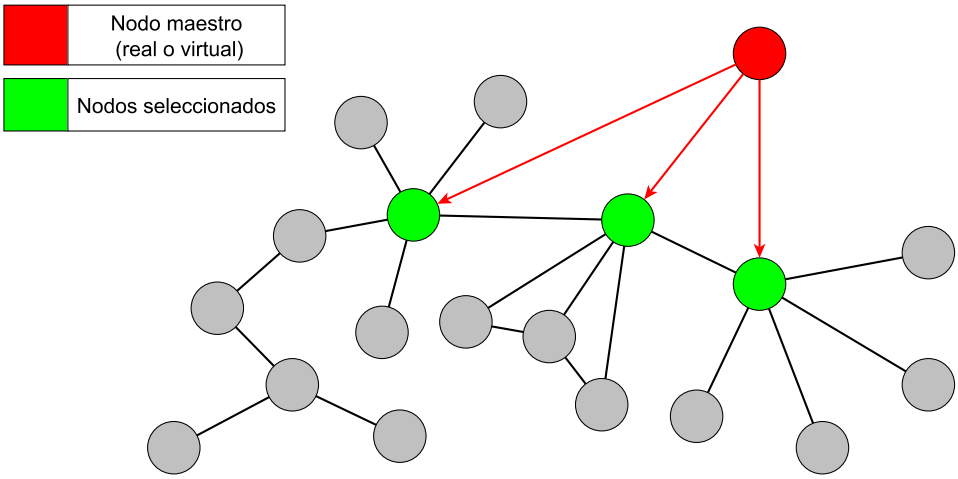


Figura 6.1: Ejemplo de selección de nodos a controlar en una red libre de escala.

6.1.1 Estrategias de selección

En el control pinning, la estrategia para seleccionar los nodos que serán conectados al nodo de referencia, puede ser específica o no específica. Esto se describe brevemente a continuación:

- **Control pinning específico:** Se seleccionan nodos a conciencia. Comúnmente, esta selección se enfoca en los nodos de alto número de conexiones, también conocidos como nodos de alto grado [5], los nodos adyacentes a estos, etc. Esta estrategia resulta especialmente útil cuando se trabaja con redes de naturaleza no homogénea, e.g. redes libres de escala [23].
- **Control pinning no específico:** En este caso, los nodos son seleccionados de manera aleatoria. Debido a la naturaleza homogénea de algunas redes, e.g redes de mundo pequeño, redes aleatorias, la diferencia entre seleccionar nodos de alto grado y otros, no es muy notable [24].

En este trabajo de tesis, la estrategia de selección utilizada, para el caso de redes libres de escala, da prioridad a los nodos de alto grado, posteriormente a los nodos adyacen-

tes a éstos y así sucesivamente. En el caso de redes de mundo pequeño o redes aleatorias, seleccionamos los nodos de manera aleatoria.

El objetivo de aplicar esta técnica de control en este trabajo de investigación, es llevar la dinámica final de una red bidireccional (caso en ausencia de nodo maestro), a un estado final deseado sin la necesidad de controlar todos los nodos de la red (caso maestro-esclavo).

6.1.2 Metodología de control

Considere una red compuesta por N osciladores caóticos idénticos. Cada oscilador es un subsistema dinámico n-dimensional.

La red queda descrita de la forma:

$$\dot{x_i}(t) = f(x_i(t), t) + \sum_{j=1, j\neq 1}^{N} ca_{ij}\Gamma(x_j(t) - x_i(t)), \quad i = 1, ..., N, \tag{6.1}$$

Donde $c > 0$ es la fuerza de acoplamiento. $\Gamma = \text{diag}(r_1, r_2, \ldots, r_n) \in \mathbb{R}^n$ es una matriz diagonal constante, con $r_n = 1$ si se trata del estado por el cual esta acoplada la red, y $r_n = 0$ en caso contrario.

Para el cálculo de la fuerza de acoplamiento, el siguiente lema es utilizado [7]:

Lema 1 *Considere la red 6.1. Sea λ_1 el valor propio mayor no cero de la matriz de acoplamiento A. La sincronización de estados de la red 6.1 definida por $x_1 = x_2 = \cdots = x_n$ es asintóticamente estable, si*

$$\lambda_1 \leq -\frac{T}{c}, \tag{6.2}$$

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

$$\begin{aligned} \dot{x_1} &= f_1(x) - Tx_1, \\ \dot{x_2} &= f_2(x), \\ \dot{x_n} &= f_n(x). \end{aligned} \tag{6.3}$$

Se dice que la red (6.1) alcanza sincronía completa, si

$$\lim_{t\to\infty} \|x_i(t) - x_j(t)\| = 0 \tag{6.4}$$

$\forall i$ y $\forall j$.

El problema de control pinning, para sincronizar la red de la ecuación (6.1), es controlar directamente una fracción δ $(0 < \delta \ll 1)$ de los N nodos disponibles en la red, conectados al nodo de referencia $\bar{x}(t)$, tal que:

$$\lim_{t\to\infty} \|x_i(t) - \bar{x}(t)\| = 0, \qquad i = 1, \ldots, N. \tag{6.5}$$

Donde el estado estacionario homogéneo satisface:

$$f(\bar{x}(t), t) = 0. \tag{6.6}$$

La red controlada, queda descrita con una ley local de control de retroalimentación negativa como sigue:

$$\dot{x_i}(t) = f(x_i(t), t) + \sum_{j=1, j\neq 1}^{N} c a_{ij} \Gamma(x_j(t) - x_i(t)) + h_i c \Gamma(\bar{x}(t) - x_i(t)) \tag{6.7}$$
$$i = 1, ..., N,$$

Donde $h = 1$, si el nodo i está conectado al nodo de referencia, $h = 0$ en caso contrario [24].

Suponga que los nodos $i_1, i_2, ..., i_l$ son seleccionados, $l = \delta N$ con $l \in \mathbb{N}$. Entonces, si se desea seleccionar el 35 % de los nodos de una red de 250 osciladores, se tiene que $l = (0.35)(250) = 87.5$. Se seleccionan 87 nodos (valor truncado ya que no es posible seleccionar una fracción de nodo), con $h = 1$, y $h = 0$ para el resto de los nodos.

6.1.3 Ejemplo 6.1

El ejemplo mostrado a continuación consta de dos partes. Primero, se sincroniza una red compleja en configuración bidireccional, obteniendo una dinámica emergente (caso 1). Posteriormente, utilizando la técnica de control pinning para manipular la dinámica emergente obtenida, es llevada a un estado final deseado variando las condiciones iniciales del nodo de referencia (caso 2a y 2b).

En la Figura 6.2 se muestra una red libre de escala conformada por 10 osciladores Lü caóticos de orden fraccionario. El flujo de información entre los nodos es bidireccional.

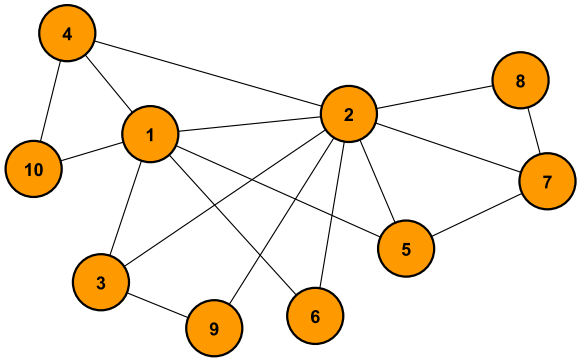


Figura 6.2: Red libre de escala conformada por 10 nodos en configuración bidireccional.

El conjunto de ecuaciones que describe las dinámicas del oscilador Lü en su versión fraccionaria es el siguiente:

$$\begin{cases} {}_0D_t^{q_1}x(t) &= a(y(t)-x(t)), \\ {}_0D_t^{q_2}y(t) &= -x(t)z(t)+cy(t), \\ {}_0D_t^{q_3}z(t) &= x(t)y(t)-bz(t). \end{cases} \tag{6.8}$$

Este oscilador fraccionario presenta caos para los parámetros: $a = 36, b = 3, c = 20$, y derivadas: $q_1 = q_2 = q_3 = 0.95$ [12].

La matriz de acoplamiento correspondiente a la red de la Figura 6.2 es la siguiente:

$$A = \begin{pmatrix} -6 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & -8 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & -3 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & -3 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & -3 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & -3 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & -2 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & -2 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -2 \end{pmatrix} \tag{6.9}$$

Las condiciones iniciales utilizadas por la red mostrada en la Figura 6.2 fueron redactadas arbitrariamente y se muestran en la Tabla 6.1.

Tabla 6.1: Condiciones iniciales de la red con osciladores Lü caóticos de orden fraccionario.

Nodo	$x(t)$	$y(t)$	$z(t)$
1	5.0003	-8.3208	-2.9502
2	-1.3903	2.1136	-8.3510
3	2.3582	-6.0642	0.3310
4	3.2618	1.6353	5.4132
5	5.0304	-3.2545	1.2853
6	-4.7219	-6.6089	4.6241
7	0.0002	-0.2746	4.5556
8	2.9729	1.7510	6.2513
9	4.6489	1.1988	-3.4518
10	-3.2578	5.9605	-8.0592

6.1.3.1 Caso 1 (red bidireccional)

Como primer ejemplo, la red mostrada en la Figura 6.2 es llevada a la sincronía. Esto, con la finalidad de observar numérica y gráficamente el comportamiento de la red en ausencia de un nodo maestro. Es decir, observamos el comportamiento de la dinámica emergente.

La red controlada libre de escala de la Figura 6.2, queda descrita matemáticamente como sigue:

$$\dot{x_i}(t) = f(x_i(t), t) + \sum_{j=1, j\neq 1}^{N} c a_{ij} \Gamma(x_j(t) - x_i(t)), \quad i = 1, ..., N, \tag{6.10}$$

donde la fuerza de acoplamiento utilizada es $c = 19$, a_{ij} son los elementos de la matriz de acoplamiento (6.9), y $\Gamma = diag(0, 1, 0)$.

En la Figura 6.3 se observan algunos atractores de los nodos presentes en la red sincronizada.

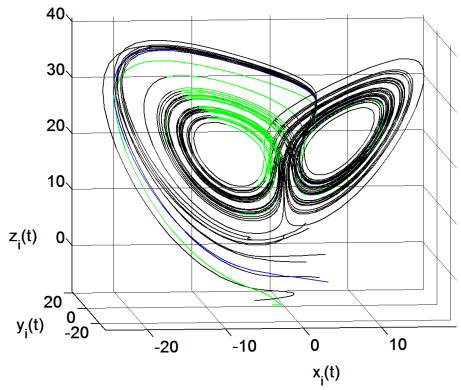


Figura 6.3: Atractores caóticos de los nodos presentes en la red.

En la Figura 6.4 se muestra la evolución temporal de algunos nodos presentes en la red. Ésto, con la finalidad de observar gráficamente que los nodos presentes en la red sincronizan con el paso del tiempo.

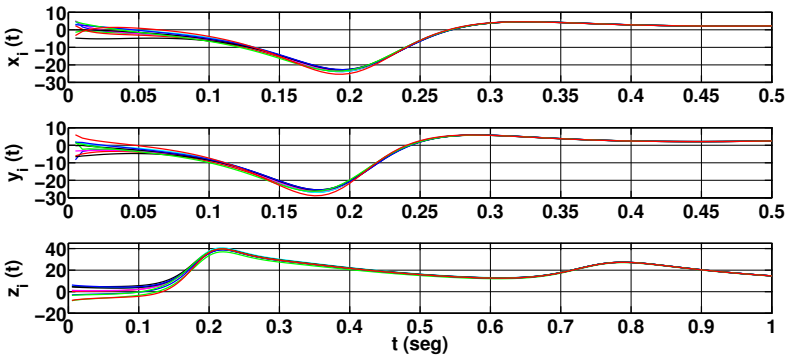


Figura 6.4: Evolución temporal de los estados $x_i(t), y_i(t), z_i(t)$, de la red (donde $i = 1, 2, \ldots, 10$).

La Figura 6.4 muestra el error de sincronía entre las dinámicas de algunos nodos de la red. La Figura 6.6 muestra algunos planos de fase de la red.

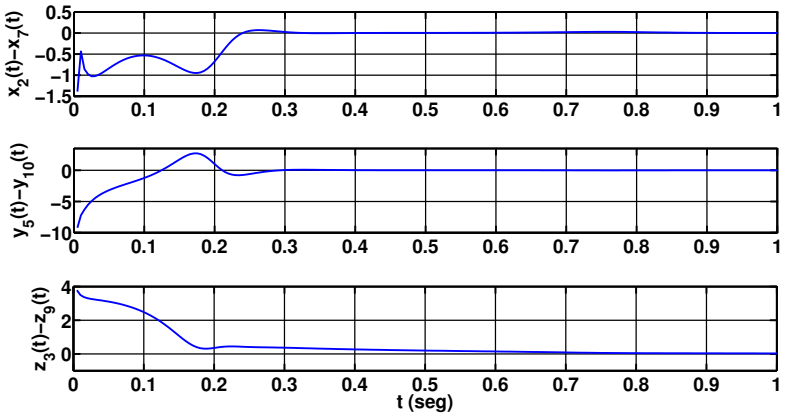


Figura 6.5: Evolución temporal del error de sincronización entre los estados $x_2 - x_7$, $y_5 - y_{10}$, y $z_3 - z_9$ de la red.

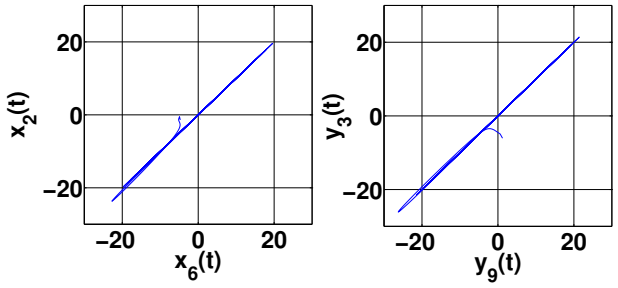


Figura 6.6: Planos de fase de los estados x_2 vs x_6, y_3 vs y_9, de la red.

Con la fuerza de acoplamiento utilizada y con la evidencia gráfica, concluimos que la red bidireccional alcanza la sincronía y su dinámica emergente es observada gráficamente.

6.1.3.2 Caso 2-a (Aplicando nodo de referencia)

Sin alterar el acoplamiento y configuración de la red utilizada en la subsección 6.1.3.1, se colocó un nodo maestro independiente al cual llamaremos nodo de referencia. Los nodos seleccionados para recibir información del nodo de referencia son: nodos de alto grado N1 (grado 6), N2 (grado 8) y 3 nodos adyacentes a ellos N3, N4 y N5 (grado 3). Esto se ilustra en la Figura 6.7.

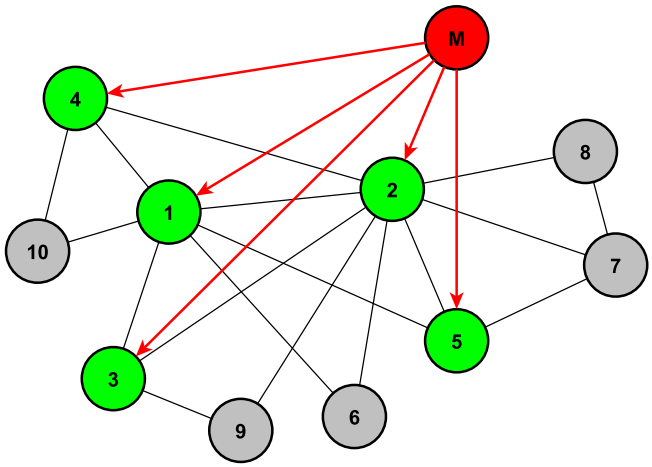


Figura 6.7: Selección de nodos que son acoplados al nodo de referencia.

La red controlada, está descrita matemáticamente como sigue:

$$\dot{x_i}(t) = f(x_i(t), t) + \sum_{j=1, j\neq 1}^{N} ca_{ij}\Gamma(x_j(t) - x_i(t)) + h_i c\Gamma(\bar{x}(t) - x_i(t)) \tag{6.11}$$

$$i = 1, ..., N,$$

donde la fuerza de acoplamiento que garantiza que la ecuación (6.4) se cumple, llevando la red controlada (6.11) a la sincronía, es $c = 19$, a_{ij} son los elementos de la matriz de acoplamiento (6.9), $\Gamma = diag(0, 1, 0)$, $h_i = 1$ para $i = 1, \ldots, 5$ y $h_i = 0$ para $i = 6, \ldots, 10$.

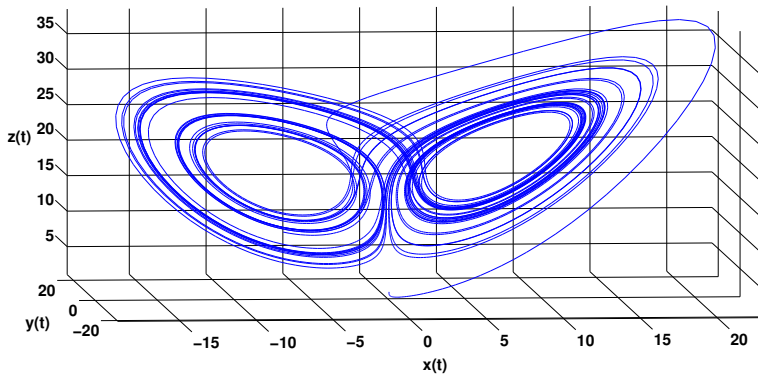


Figura 6.8: Atractor caótico del nodo de referencia con condiciones iniciales ($x(0)$, $y(0)$, $z(0)$) = $(0.1, 0.1, 2)$.

En la Figura 6.8 se muestra el atractor al cual convergen las dinámicas del nodo de referencia. En la Figura 6.9 se muestran algunos atractores al cual convergen las dinámicas de los nodos de la red.

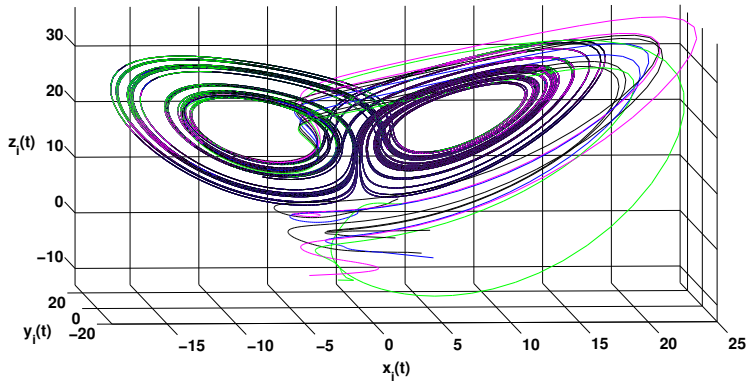


Figura 6.9: Atractores caóticos de los nodos presentes en la red.

En la Figura 6.10 se muestran algunos planos de fase de la red con respecto al nodo de referencia.

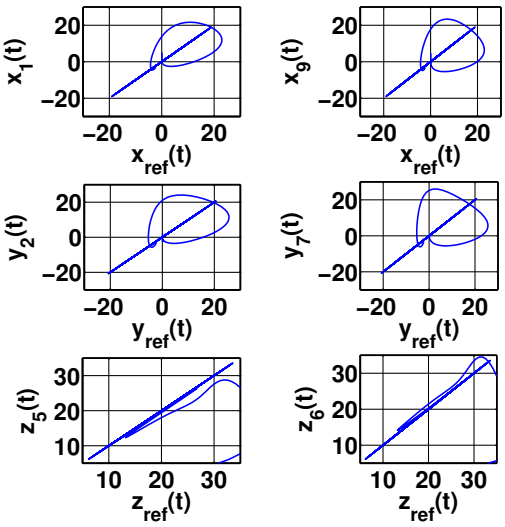


Figura 6.10: Planos de fase de los estados x_1 vs x_{ref}, x_9 vs x_{ref}, y_2 vs y_{ref}, y_7 vs y_{ref}, z_5 vs z_{ref}, z_6 vs z_{ref} de la red.

En la Figura 6.11 se muestra el error de sincronía de algunos nodos de la red con respecto al nodo de referencia.

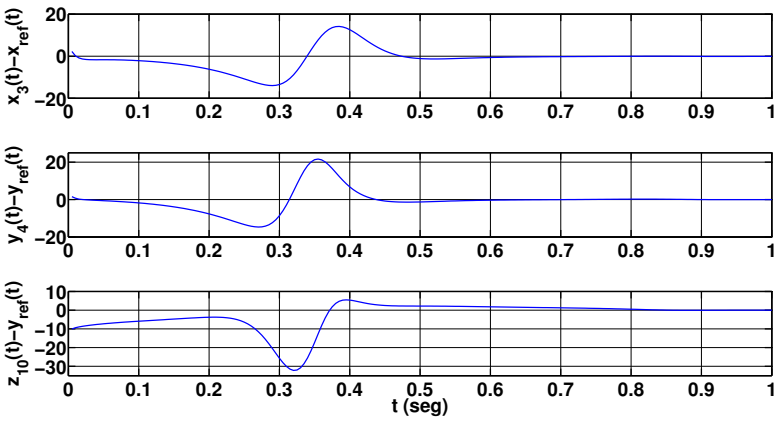


Figura 6.11: Evolución temporal del error de sincronización entre los estados de algunos nodos de la red y el nodo de referencia $x_3 - x_{ref}$, $y_4 - y_{ref}$, y $z_{10} - z_{ref}$.

La evidencia gráfica mostrada en las Figuras 6.10 y 6.11, corrobora que la red descrita por la ecuación 6.11, alcanza la sincronía con respecto al nodo de referencia.

6.1.3.3 Caso 2-b (Modificando condiciones iniciales del nodo de referencia)

El objetivo de este experimento, es comprobar si es posible manipular la dinámica final de la red bidireccional, a un estado final diferente al obtenido anteriormente. Para esto, únicamente las condiciónes iniciales del nodo de referencia fueron modificadas.

Como en el caso anterior, las Figuras 6.12 y 6.13 muestran los atractores a los cuales convergen las dinámicas del nodo de referencia y los nodos de la red respectivamente.

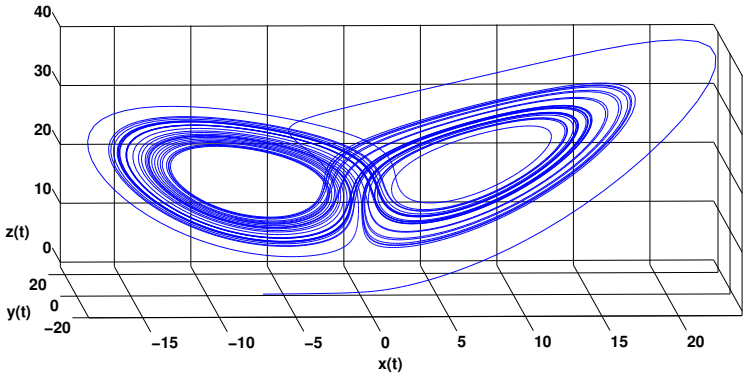


Figura 6.12: Atractor caótico del nodo de referencia con condiciones iniciales ($x(0)$, $y(0)$, $z(0)$) = $(-6.3034, 1.2939, -0.7873)$.

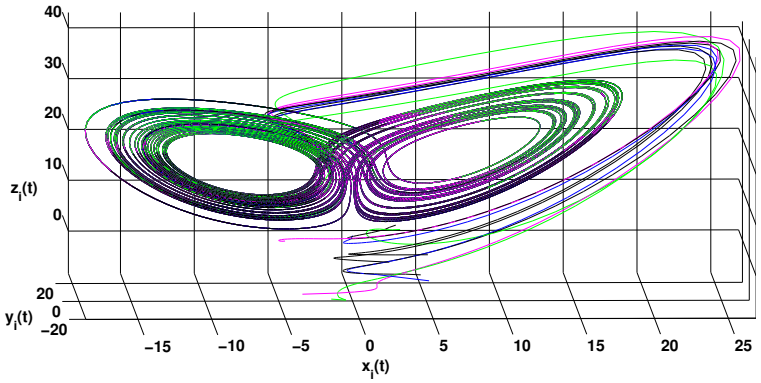


Figura 6.13: Atractores caóticos de los nodos presentes en la red.

En la Figura 6.14 se muestran algunos planos de fase de la red con respecto al nodo de referencia.

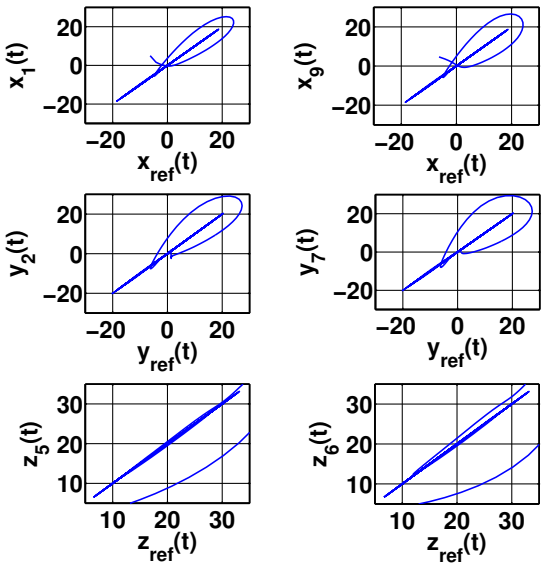


Figura 6.14: Planos de fase de los estados x_1 vs x_{ref}, x_9 vs x_{ref}, y_2 vs y_{ref}, y_7 vs y_{ref}, z_5 vs z_{ref}, z_6 vs z_{ref} de la red.

En la Figura 6.15 se muestra el error de sincronía de algunos nodos de la red con respecto al nodo de referencia.

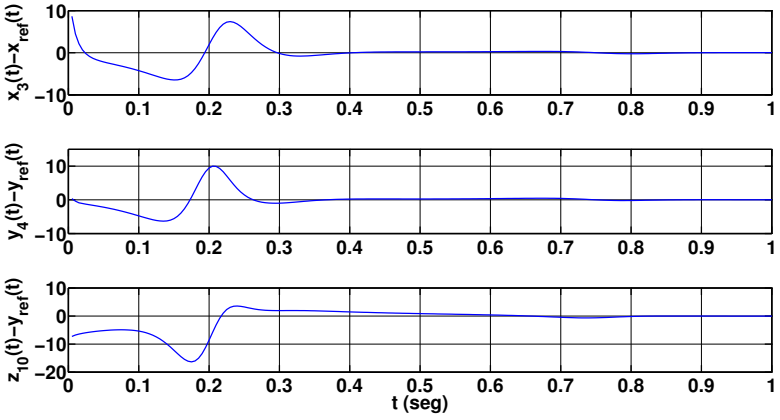


Figura 6.15: Evolución temporal del error de sincronización entre los estados de algunos nodos de la red y el nodo de referencia $x_3 - x_{ref}$, $y_4 - y_{ref}$, y $z_{10} - z_{ref}$.

La dinámica emergente de la red es manipulada variando las condiciones iniciales

del nodo de referencia, es llevada a un estado final diferente al obtenido en el caso 2.1. Cumpliendo así, con el objetivo del experimento.

6.1.4 Ejemplo 6.2

En este ejemplo se utilizó una red de mundo pequeño Newman-Watts en configuración bidireccional constituida por 20 osciladores Arneodo caóticos de orden fraccionario. Las condiciones iniciales de la red fueron obtenidas aleatoriamente en un rango arbitrario entre -4.4 y 10.46

Las condiciones iniciales del nodo de referencia son: $(x(0), y(0), z(0)) = (1.145, -1.225, 0.378)$.

Se aplica control pinning a una fracción δ $(0 < \delta \ll 1)$ de nodos en la red. En este caso, se desea controlar directamente el 30 % de los nodos de la red. Por lo tanto, δ $(0 < 0.3 \ll 1)$; se seleccionan $l = \delta N$ nodos. Ésto da como resultado $l = (0.3)(20) = 6$.

La red controlada esta definida matemáticamente como sigue:

$$\dot{x_i}(t) = f(x_i(t), t) + \sum_{j=1, j\neq 1}^{N} c a_{ij} \Gamma(x_j(t) - x_i(t)) + h_i c \Gamma(\bar{x}(t) - x_i(t)) \qquad (6.12)$$
$$i = 1, ..., N,$$

donde la fuerza de acoplamiento que cumple con la ecuación (6.4) y garantiza la sincronía de la red (6.12), es $c = 10$. Los osciladores son acoplados mediante el primer estado, i.e. $\Gamma = diag(1, 0, 0)$; $h_i = 1$ para $i = 5, 8, 10, 13, 18, 20$, y $h_i = 0$ para el resto de los nodos.

En la Figura 6.16 se muestran algunos planos de fase de la red con respecto al nodo de referencia.

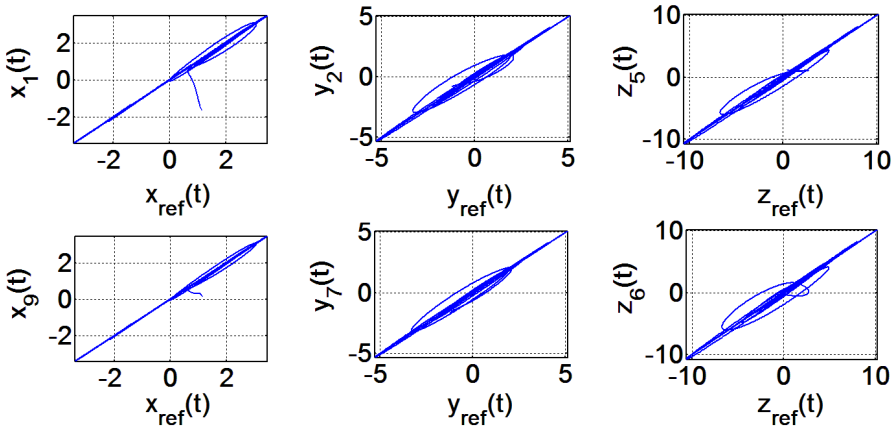


Figura 6.16: Planos de fase de los estados x_1 vs x_{ref}, x_9 vs x_{ref}, y_2 vs y_{ref}, y_7 vs y_{ref}, z_5 vs z_{ref}, z_6 vs z_{ref} de la red.

En la Figura 6.17 se muestra el error de sincronía de algunos nodos de la red con respecto al nodo de referencia.

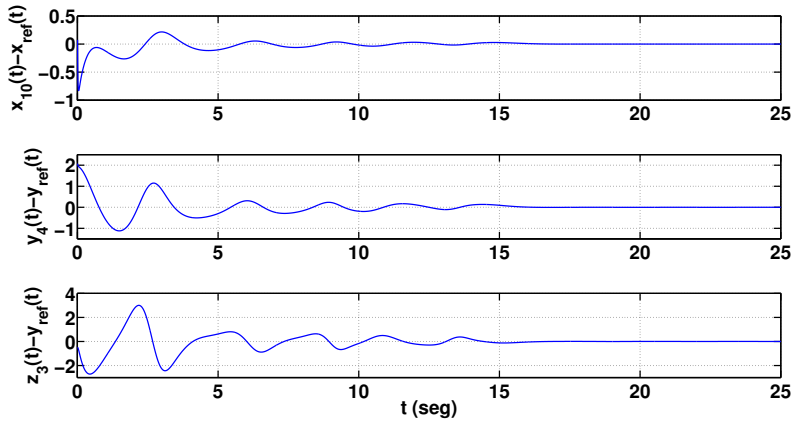


Figura 6.17: Evolución temporal del error de sincronización entre los estados de algunos nodos de la red y el nodo de referencia $x_{10} - x_{ref}$, $y_4 - y_{ref}$, y $z_3 - z_{ref}$.

Capítulo 7

Control pinning: aplicación a comunicaciones seguras

Este capítulo, está enfocado a la transmisión de datos encriptados de un emisor a múltiples usuarios. Se explica el esquema multiusuario convencional y el propuesto en este trabajo de investigación.

7.1 Esquema multiusuario convencional

El esquema convencional multiusuario, se compone de un emisor y múltiples receptores. Estos receptores, pueden estar localizados en el mismo entorno o en uno diferente e independiente. El mensaje es sumado a una señal, en este caso caótica, y es enviado a través de un canal público. Se repite el mensaje para cada receptor. Un segundo canal público es utilizado para enviar un estado del oscilador presente en el emisor a cada receptor. El receptor obtiene la dinámica con la que es encriptado el mensaje debido al efecto de sincronía, y recupera el mensaje.

La Figura 7.1 muestra el diagrama convencional para el encriptado aditivo de datos con múltiples receptores.

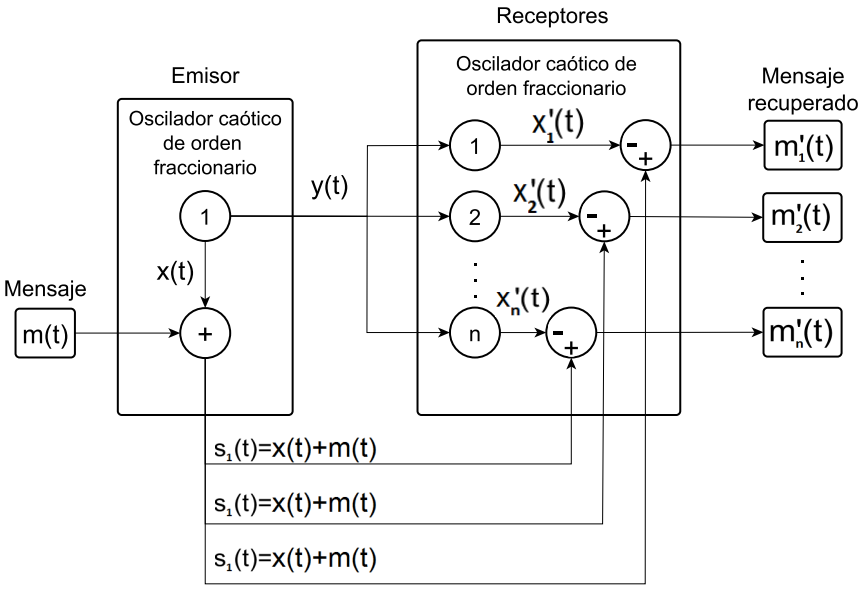


Figura 7.1: Diagrama de encriptado aditivo convencional, con recuperación del mensaje en modalidad multiusuario. El mensaje $m(t)$ es sumado a una señal caótica $x(t)$ dando como resultado un mensaje encriptado $s(t)$. Este es enviado a través de un canal público a multiples usuarios. De manera simultánea se envía un estado $y(t)$ a cada receptor para generar un estado $x'(t)$. El estado generado es sustraido de $s(t)$ recuperando un mensaje $m'(t)$.

7.2 Esquema multiusuario propuesto

Se propone utilizar la técnica de control pinning para evitar manipular todos los nodos presentes en la red del receptor. Esto evita costos adicionales durante la implementación física, debido a que solo se controla directamente una fracción de la red receptora para manipular su dinámica final. Para lograrlo, el nodo de referencia es sincronizado a un nodo cualquiera de la red sincronizada del emisor. Este nodo de referencia es conectado a algunos nodos del receptor, seleccionados estratégicamente. Así, la red del receptor tendrá una dinámica emergente idéntica a la de la red del emisor. Asegurando así, que ambas redes estarán sincronizadas y que la recuperación de los mensajes enviados sera correcta en todo momento.

La Figura 7.2 muestra el diagrama propuesto para encriptar datos, y enviarlos a múltiples usuarios. Se observa que la red del emisor y la del receptor son idénticas en topología y configuración. Es importante mencionar que dichas redes fueron colocadas con fines ilustrativos y no fueron utilizadas en los ejemplos que se muestran en el presente capítulo.

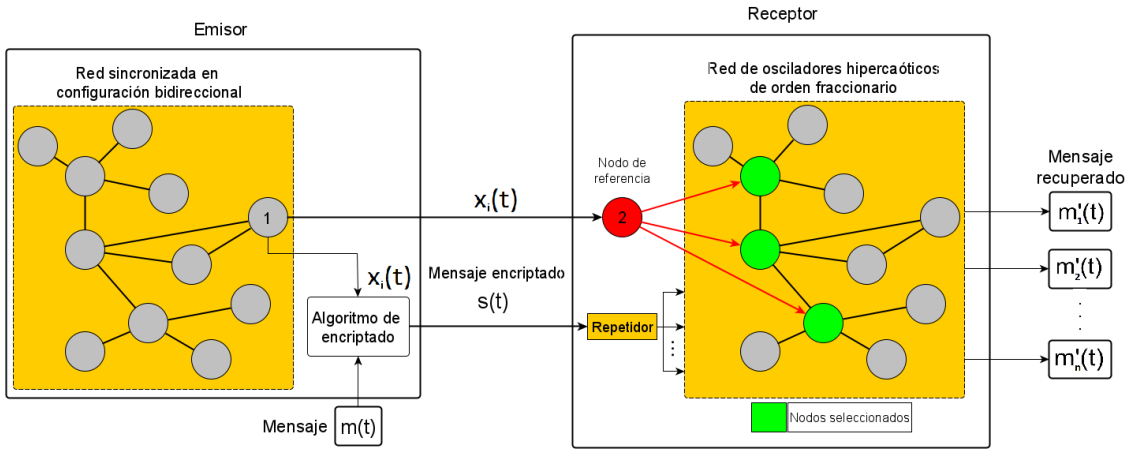


Figura 7.2: Diagrama para encriptado de datos utilizando redes complejas, con recuperación del mensaje en modalidad multiusuario mediante control pinning. Sea n la dimensión del oscilador caótico empleado, el mensaje $m(t)$ y las señales caóticas $x_i(t)$ con $i = 1, ..., n$, son utilizados por el algoritmo propuesto generando un mensaje encriptado $s(t)$. Este es enviado a través de un canal público a un repetidor, evitando el uso de múltiples canales públicos para transmitir el mensaje encriptado. De manera simultánea se envía $x_i(t)$ donde i es el estado por el cual sincroniza la red emisora y es utilizado por el nodo de referencia para generar dinámicas equivalentes al nodo seleccionado en el emisor. La red receptora debe sincronizar al nodo de referencia y recuperar los mensajes $m'_n(t)$.

Al utilizar una red compleja en configuración bidireccional, la dinámica emergente actúa como una llave adicional. Esta dinámica emergente, difiere de cualquier dinámica presente en la red antes de ser sincronizada y solo puede ser reproducida utilizando la misma combinación de los siguientes factores: número de nodos que conforman la red,

condiciones iniciales de los osciladores, y la topología de la red.

De lo anterior, se puede inferir que este tipo de dinámica es impredecible si se modifican los parámetros de la red. Es decir, si modificamos los parámetros de la red, no podemos saber como se va a comportar la red sincronizada. Sin embargo, este comportamiento es determinístico, ya que puede ser reproducido una y otra vez si se utilizan los mismos parámetros con las que ésta se generó principalmente. Esta característica representa una ventaja explotable y es parte fundamental en este trabajo de investigación.

En el caso práctico, cuando se tienen dos redes (emisora y receptora), no se puede asegurar que las condiciónes iniciales de ambas redes siempre sean las mismas. Por esta razón, la equivalencia entre las condiciones iniciales utilizadas en el emisor y las del receptor puede ser total, parcial o nula. En los experimentos, se utilizan condiciones iniciales diferentes para cada red. Ésto, con el fin de observar el efecto de sincronía entre ellas.

Lo anterior se debe a diversos factores, entre ellos el desgaste que sufren los componentes electrónicos utilizados. Es posible conectar todos los nodos presentes en la red receptora, a un nodo de referencia en configuración maestro-esclavo para manipular el estado final de la red receptora. Sin embargo, esto implica que se tiene una ley de control adicional por cada nodo presente en la red y el costo de implementación podría ser poco práctico.

Por esta razón, se propone aplicar el control pinning, en el cuál se utiliza un nodo de referencia conectado a algunos nodos de la red receptora estratégicamente, evadiendo costos de implementación innecesarios. Al sincronizar esta red al nodo de referencia, se garantiza que el receptor tendrá siempre la dinámica deseada. Recuperando así el mensaje correctamente, aún cuando las condiciones iniciales del emisor o del receptor varíen.

A diferencia del esquema convencional multiusuario en el que el mensaje es repetido para cada receptor, debido a que la ubicación de los receptores no necesariamente deba ser la misma, este esquema supone que los receptores están conectados a una misma red, como en el caso de algunas redes privadas. De esta forma, los receptores se encuentran ubicados relativamente cerca unos de otros, y el mensaje encriptado puede ser enviado a un repetidor de señales que se encargue de transmitirlo a los receptores. Si hablámos de

una red privada, el nodo de referencia es el único que tiene contacto con el canal público.

A continuación, se explica la metodología utilizada por el esquema propuesto mediante un ejemplo dividido en dos partes: la red 1 presente en el emisor, y la red 2 presente en el receptor. Ambas redes poseen condiciones iniciales diferentes. Por lo tanto, las dinámicas emergentes obtenidas difieren entre el emisor y el receptor. Es necesario sincronizar las dinámicas emergentes del emisor y del receptor con el objetivo de recuperar los mensajes.

7.2.1 Ejemplo del esquema propuesto parte 1

El emisor y el receptor estan compuestos por una red aleatoria constituida por 20 osciladores hipercaóticos de orden fraccionario.

El oscilador hipercaótico de orden fraccionario utilizado en cada nodo de las redes, está definido matemáticamente como sigue:

$$\begin{cases} {}_0D_t^{q_1}x(t) &= a(y(t)-x(t))+\mu y(t)z(t), \\ {}_0D_t^{q_2}y(t) &= cx(t)-dx(t)z(t)+y(t)+w(t), \\ {}_0D_t^{q_3}z(t) &= x(t)y(t)-bz(t), \\ {}_0D_t^{q_4}w(t) &= -vy(t). \end{cases} \tag{7.1}$$

Este sistema exhibe un comportamiento hipercaótico cuando sus parámetros equivalen a $q_1 = q_2 = q_3 = q_4 = 0.95$, $a = 35, b = 4, c = 25, \mu = 35, v = 100$ [22]. En la Figura 7.3, se muestran algunos planos de fase de este oscilador hipercaótico.

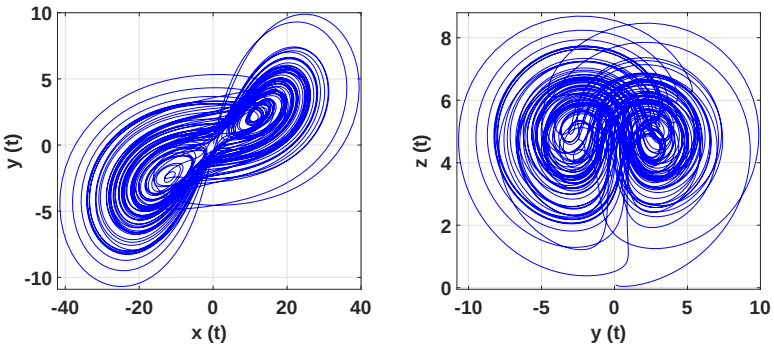


Figura 7.3: Planos de fase $x(t)$ vs $y(t)$ y $y(t)$ vs $w(t)$ del oscilador hipercaótico de orden fraccionario.

7.2.1.1 Red 1 (emisor)

La condiciónes iniciales utilizadas para la red emisora, fueron calculadas en un rango de $[-5, 5]$ aleatoriamente.

Matemáticamente, la red controlada está definida por:

$$\dot{x_i}(t) = f(x_i(t), t) + \sum_{j=1, j\neq 1}^{N} ca_{ij}\Gamma(x_j(t) - x_i(t)), \quad i = 1, ..., N. \tag{7.2}$$

La fuerza de acoplamiento utilizada que cumple con la ecuación (6.4) y garantiza la sincronía de la red (7.2), es $c = 25$; a_{ij} son los elementos de la matriz de acoplamiento, y $\Gamma = diag(0, 1, 0, 0)$ ya que los osciladores estan acoplados mediante el segundo estado del oscilador.

En la Figura 7.4 se muestra la imagen a encriptar por el emisor.

Figura 7.4: Imagen original. Dimensiones: 640×359.

Con la finalidad de visualizar gráficamente la existencia de sincronía en la red (7.2), la Figura 7.5 muestra la evolución temporal de algunos estados de la red. Se observa que sus dinámicas convergen con el paso del tiempo, logrando la sincronía.

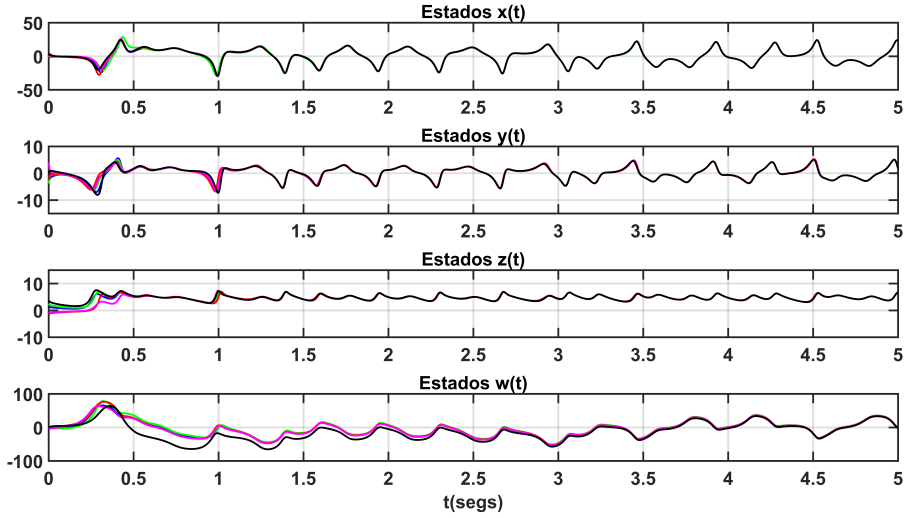


Figura 7.5: Evolución temporal de algunos estados de la red emisora sincronizada.

La Figura 7.6 muestra la evolución temporal del error de sincronía de algunos estados de la red. La Figura 7.7 muestra algunos planos de fase de la red a 45 grados.

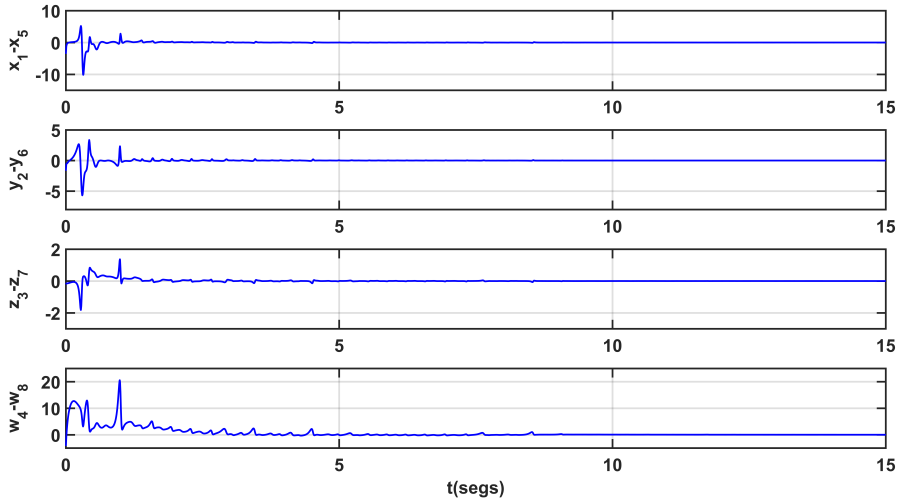


Figura 7.6: Error de sincronización entre algunos estados de la red emisora.

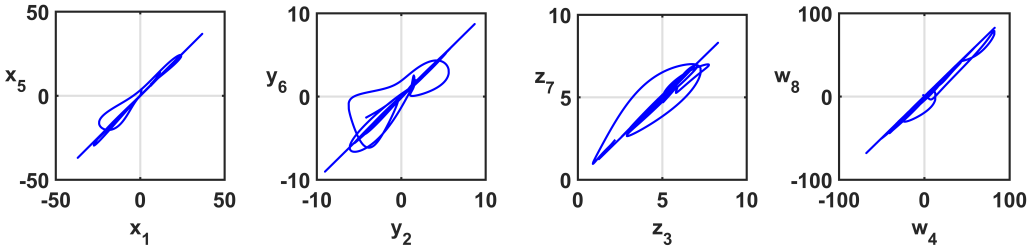


Figura 7.7: Planos de fase de algunos estados de la red emisora sincronizada

Es importante mencionar, que a través del canal público no se envía una imagen, sino una serie de datos que contienen la información encriptada, de los píxeles de la imagen. Suponiendo que esta serie de datos, es reacomodada de manera correcta y con las dimensiones correspondientes a la imagen original: la Figura 7.8 muestra el proceso de manipulación y encriptado, al cuál es sometida la imagen original. Se muestran los histogramas en R, G y B para cada paso del proceso. Se observa que los histogramas de la imagen encriptada no coinciden con los de la imagen original, es decir se ocultan los histogramas iniciales.

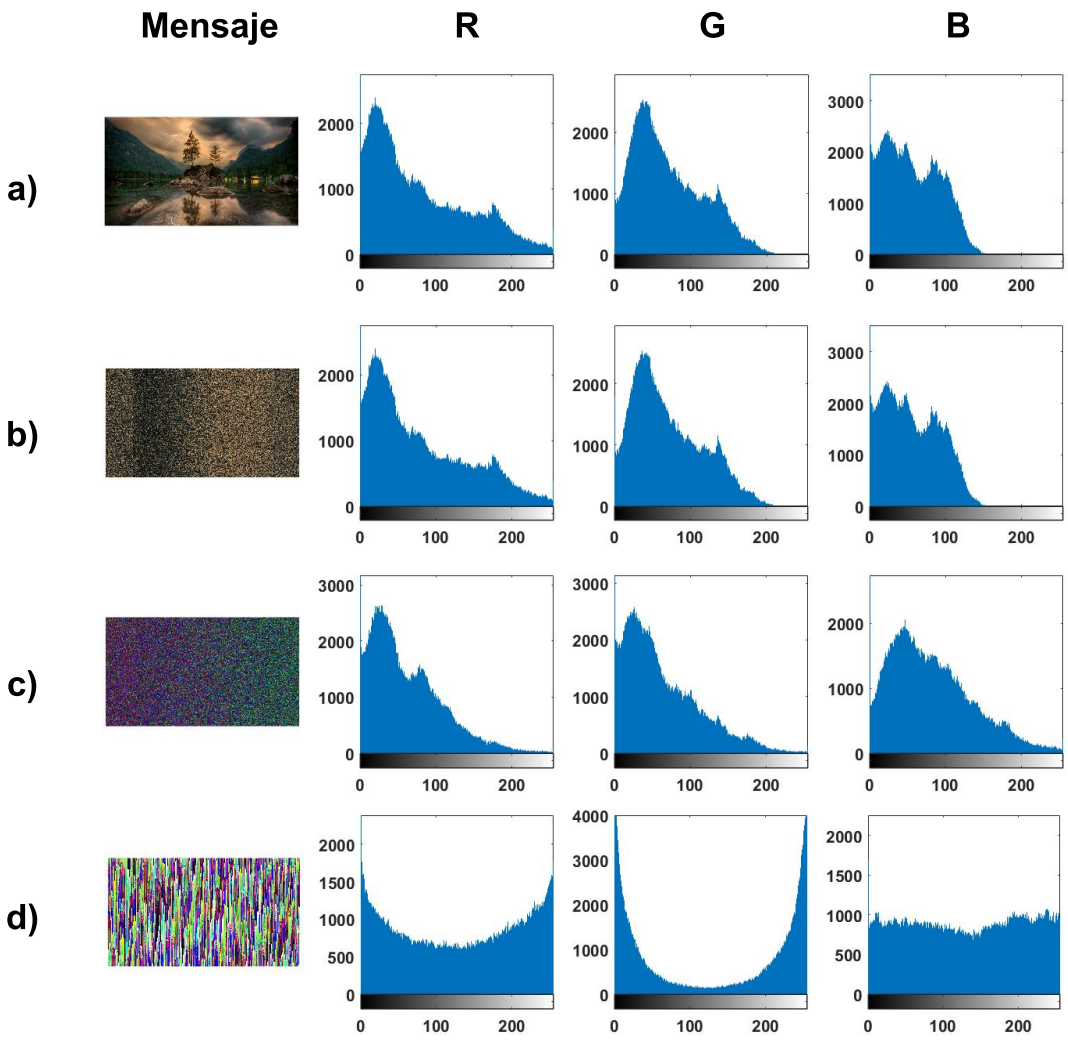


Figura 7.8: a) Histogramas de la imagen original, b) Histogramas de la imagen con píxeles desordenados, c) Histogramas de la imagen desordenada revolviendo las intensidades de brillo, d) Histogramas de la imagen encriptada.

De la ecuación (4.1), en la Tabla 7.1 se muestran los coeficientes de correlación entre la imagen original y la imagen encriptada. Los resultados muestran que las imágenes tienen muy poca correlación i.e. $c \ll 0$.

Tabla 7.1: Coeficientes de correlación entre la imagen original y la imagen encriptada.

Canal	Coeficiente de correlación
R	0.0064
G	-0.0006
B	0.0021

En la Tabla 7.2 se muestra el resultado del cálculo de la entropía de la imagen original y la imagen encriptada mediante la ecuación (4.2). Se obtiene una mayor entropía en la imagen encriptada con respecto a la que posee la imagen original.

Tabla 7.2: Cálculo de entropía

Mensaje	Entropía
Imagen original	7.4445
Imagen encriptada	7.8065

7.2.1.2 Red 2 (receptor)

Las condiciones iniciales de la red receptora fueron calculadas en un rango de $[-5, 5]$ aleatoriamente, y difieren de las utilizadas en la red (7.2). Lo que implica que la dinámica emergente de las redes en el emisor y el receptor, divergen una de otra.

Aplicando control pinning, la red controlada del receptor queda descrita matemáticamente por:

$$\dot{x_i}(t) = f(x_i(t), t) + \sum_{j=1, j\neq 1}^{N} ca_{ij}\Gamma(x_j(t) - x_i(t)) + h_i c\Gamma(\bar{x}(t) - x_i(t)) \qquad (7.3)$$
$$i = 1, ..., N,$$

donde la fuerza de acoplamiento que cumple con la ecuación (6.4), y garantiza la sincronía de la red (7.3), es $c = 25$; a_{ij} son los elementos de la matriz de acoplamiento; $\Gamma = diag(0, 1, 0, 0)$; $h_i = 1$, para $i = 1, 2, 3, 5, 6, 7, 8, 9, 12, 13, 15, 19$, y $h_i = 0$, para el resto de los nodos.

Como evidencia gráfica, la Figura 7.9 muestra la evolución temporal de algunos estados presentes en la red (7.3). Las dinámicas convergen y la red alcanza la sincronía.

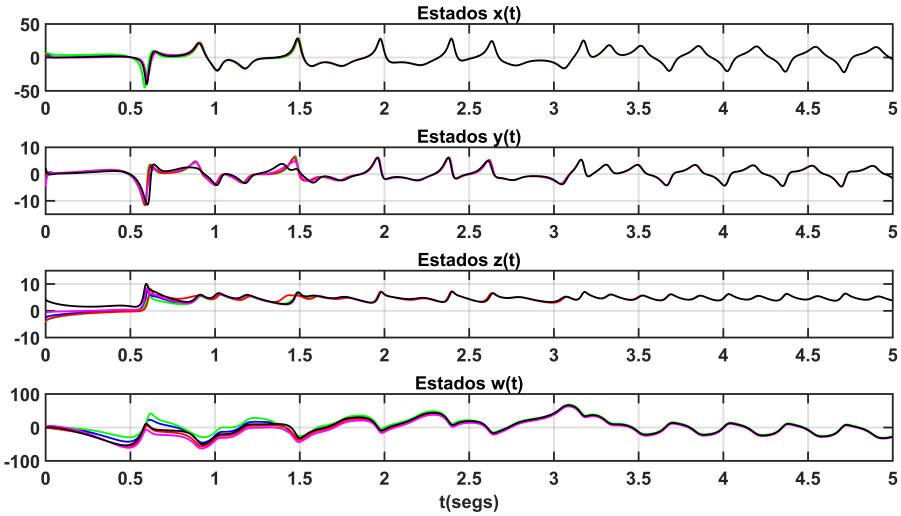


Figura 7.9: Evolución temporal de algunos estados de la red 2 sincronizada.

La Figura 7.10 muestra la evolución temporal del error de sincronía de algunos estados de la red. La Figura 7.11 muestra algunos planos de fase de la red a 45 grados.

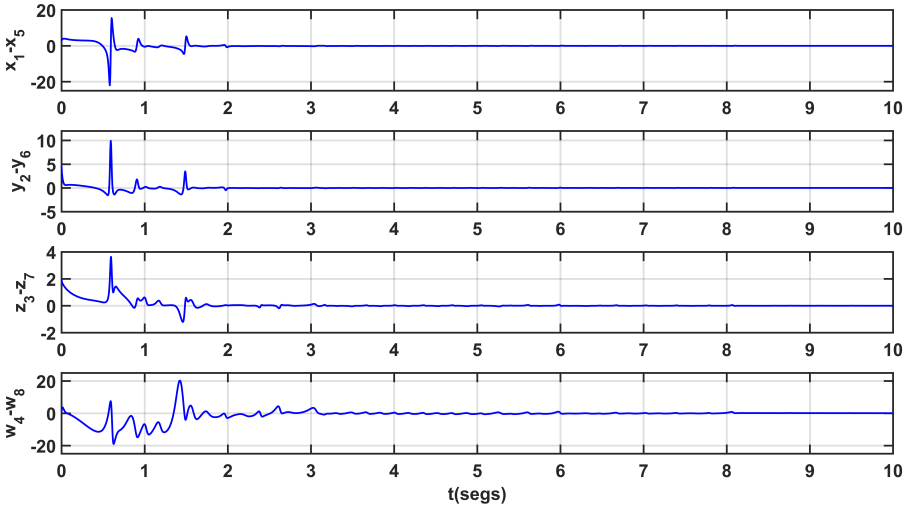


Figura 7.10: Error de sincronización entre algunos estados de la red receptora.

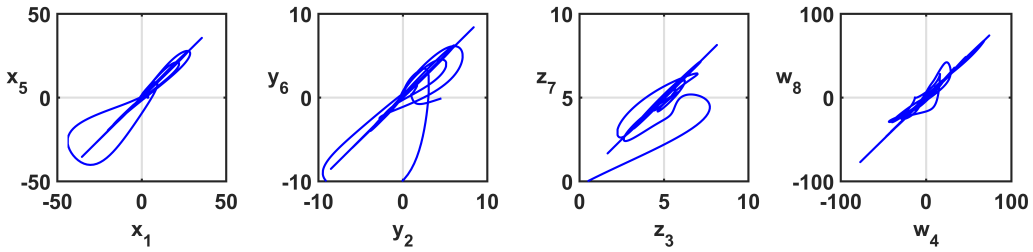


Figura 7.11: Planos de fase de algunos estados de la red receptora sincronizada

En la Figura 7.12 se muestra el error de sincronía de algunos estados de la red con respecto al nodo de referencia. Gráficamente, se puede observar que la red receptora está sincronizada con las dinámicas del nodo de referencia, el cual posee la dinámica deseada y necesaria para recuperar los mensajes correctamente.

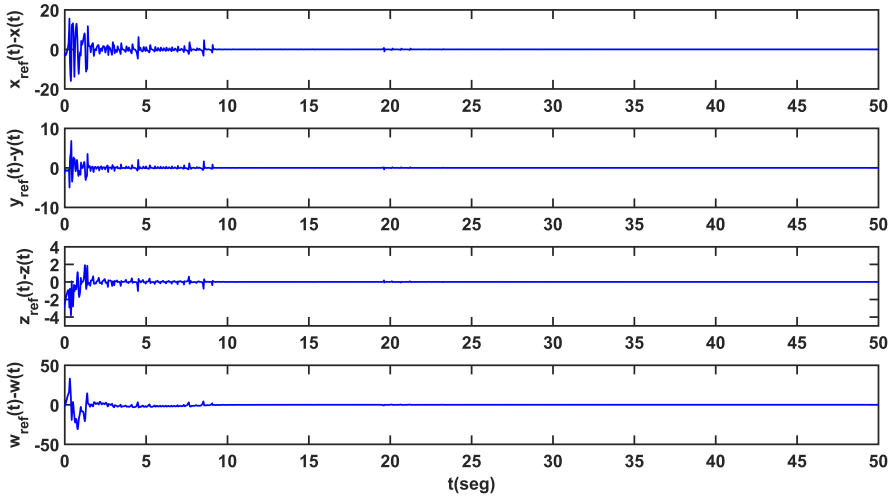


Figura 7.12: Error de sincronía de algunos estados de la red receptora con respecto al nodo de referencia.

La Figura 7.13 muestra la imagen recuperada. A continuación se dan a conocer los resultados de la recuperación.

Figura 7.13: Imagen recuperada. Dimensiones: 640×359.

Los siguientes datos del experimento resultan de calcular la diferencia entre los valóres numéricos de las intensidades de brillo de la imagen original y la imagen recuperada:

- Total de muestras ($v = n \times p$): $689,280$.
- Muestras con error $e = 0$: $357,477$.
- Muestras con error $e \neq 0$: $331,803$. Esto representa un $48.13\,\%$ del total de muestras en la imagen.
- Muestras con error $e \leq 1$: $688,448$.

En la escala del 0 al 255, 255 representa el $100\,\%$ de error posible en la intensidad de brillo que constituye a un píxel, un error $e \leq 1$ constituye un $0.392\,\%$ de error. Se concluye que el $99.88\,\%$ de la imagen es recuperada con un error $0\,\% \leq e \leq 0.392\,\%$.

Capítulo 8

Conclusiones, aportaciones y trabajo a futuro

En este capítulo, se mencionan las conclusiones, las aportaciones más importantes del trabajo de tesis y los posibles caminos que pueden seguir futuras investigaciones.

8.1 Conclusiones

A continuación se mencionan las conclusiones divididas por capítulos, debido a que se llevaron a cabo experimentos en diferentes escenarios.

En el Capítulo 5, se supone un escenario en el que el usuario encripta el mensaje, lo almacena en un sistema de almacenamiento externo y este mismo usuario recupera el mensaje. Se concluye que:

- El método aditivo convencional utiliza un estado del oscilador con una longitud igual a 3 veces el número de pixeles totales presentes en la imagen. En el método propuesto el número de muestras es igual al número de pixeles de la imagen, ya que la carga se divide entre tres estados del oscilador. Disminuyendo también la L_m mínima necesaria un 66 %. Esta modificación reduce el esfuerzo computacional y el tiempo de ejecución.

- No se transmite ningún estado del emisor a ningún canal público, es decir no se envía parte de la llave. El sistema de almacenamiento guarda el archivo encriptado aislado sin ninguna información sobre la llave.
- Se pueden encriptar imágenes de alta densidad con menor esfuerzo computacional que al utilizar el método convencional aditivo.
- No existe error de recuperación al contar con dinámicas idénticas.

En el Capítulo 6, se llevan a cabo diferentes experimentos, aplicando la técnica de control pinning. Se concluye que:

- Al aplicar la técnica de control pinning, se coloca un nodo de referencia. Éste, está conectado a una fracción del número total de nodos presentes en la red seleccionados estratégicamente. Es posible modificar la dinámica final a la cual converge una red bidireccional, modificando las condiciones iniciales del nodo de referencia. De esta manera se lleva la red a un estado final deseado.

En el Capítulo 7, se propone una aplicación al encriptado caótico en un escenario con múltiples receptores. Se concluye que:

- En la práctica, el desgaste de los componentes electrónicos impide garantizar que las condiciones iniciales de ambas redes permanezcas identicas en todo momento. Por esta razón, convencionalmente se utiliza un canal público para enviar el mensaje y otro adicional que transmite una variable de estado con la cual el receptor, por medio de sincronía, reconstruye un nodo idéntico para recuperar el mensaje. Lo anterior se realiza para cada receptor.
- En el esquema propuesto, se utilizan en total dos canales públicos. El emisor está compuesto por una red. Se encripta un mensaje utilizando la dinámica emergente de la red 1 (emisor). Se envía una variable de estado a través del primer canal público a un nodo de referencia del receptor. El mensaje encriptado se envía a través del segundo canal público a un repetidor que entrega el mensaje encriptado a los múltiples receptores. Después mediante control pinning, la red 2 (receptor)

se sincroniza al nodo de referencia obteniendo la dinamica emergente con la que se encripta el mensaje. De esta manera, todos los usuarios recuperan el mensaje correctamente.

8.2 Aportes de la tesis

- Se propone un algoritmo alternativo al encriptado aditivo. Se reduce el esfuerzo computacional al dividir la carga entre los estados del oscilador. Se utiliza una ganancia generada por caos para agregar incertidumbre a los resultados numéricos.
- Se propone un esquema Usuario-Nube, para guardar información mediante un almacenamiento en línea de forma segura, utilizando osciladores caóticos o hipercaóticos de orden fraccionario.
- Se propone una metodología para el procesamiento y encriptado de imágenes BMP tipo RGB.
- Se propone una aplicación de la técnica de control pinning, al esquema de comunicación segura entre un emisor y multiples receptores. Se garantiza la recepción del mensaje, aunque las condiciones iniciales de la red del receptor, difieran con respecto a las del emisor.

8.3 Trabajo a futuro

- Aplicar la metodología de encriptado propuesto en el capítulo 5, a otros formatos de imagen, e.g. jpg, png, gif.
- Aplicar la metodología de encriptado propuesto en el capítulo 5, al encriptado de voz o video.
- Aplicar el esquema propuesto en el capítulo 7, al encriptado de voz o video.

- Implementar físicamente el esquema propuesto en el capítulo 6, para comprobar los resultados obtenidos con respecto a los resultados teóricos mostrados.
- Modificar el orden de las derivadas y los parámetros de las ecuaciones diferenciales, estableciendo un rango que mantenga el comportamiento caótico del sistema. Esto, agrega incertidumbre a beneficio del algoritmo de encriptado.
- Establecer un sistema de comunicación aplicando control pinning, como se muestra en el Capítulo 7:
  - Utilizar una red en el emisor, cuya topología difiera con respecto a la del receptor.
  - Suponer un escenario en el cual la fuerza de acoplamiento de las redes utilizadas cambie con el paso del tiempo.

Bibliografía

[1] Resler, L. M. (2016). Edward N Lorenz's 1963 paper,"Deterministic nonperiodic flow", in Journal of the Atmospheric Sciences, Vol 20, pages 130-141: Its history and relevance to physical geography. Progress in Physical Geography, 40(1), 175-180.

[2] Lorenz, E. N. (1963). Deterministic nonperiodic flow. Journal of the atmospheric sciences, 20(2), 130-141.

[3] Ramirez, J. P., Olvera, L. A., Nijmeijer, H., & Alvarez, J. (2016). The sympathy of two pendulum clocks: beyond Huygens' observations. Scientific reports, 6, 23580.

[4] Van Tilborg, H. C. (2012). An introduction to cryptology (Vol. 52). Springer Science & Business Media.

[5] Wang, X. F. (2002). Complex networks: topology, dynamics and synchronization. International journal of bifurcation and chaos, 12(05), 885-916.

[6] Wang, X. F., & Chen, G. (2002). Synchronization in scale-free dynamical networks: robustness and fragility. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 49(1), 54-62.

[7] Wang, X. F., & Chen, G. (2002). Synchronization in small-world dynamical networks. International Journal of Bifurcation and chaos, 12(01), 187-192.

[8] Soriano-Sánchez, A. G., & Posadas-Castillo, C. (2018). Smart pattern to generate small–world networks. Chaos, Solitons & Fractals, 114, 415-422.

[9] Su, H., & Wang, X. (2013). Pinning control for complete synchronization of complex dynamical networks. In Pinning Control of Complex Networked Systems (pp. 17-44). Springer, Berlin, Heidelberg.

[10] Erdős, P., & Rényi, A. (1959). On random graphs. Publicationes mathematicae, 6(26), 290-297.

[11] Gilbert, E. N. (1959). Random graphs. The Annals of Mathematical Statistics, 30(4), 1141-1144.

[12] Leibnitz, G. W. (1962). Letter from hanover, germany, september 30, 1695 to ga l'hospital. Leibnizen Mathematische Schriften.

[13] Petráš, I. (2011). Fractional-order nonlinear systems: modeling, analysis and simulation. Springer Science & Business Media.

[14] Yadav, V. K., Shukla, V. K., Srivastava, M., & Das, S. (2020). Stability Analysis, Control of Simple Chaotic System and its Hybrid Projective Synchronization with Fractional Lu System. Journal of Applied Nonlinear Dynamics, 9(1), 93-107.

[15] Joshi, R., & Handa, H. (2019, March). Synchronization of Similar and Dissimilar Fractional Order Chaotic System. In 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN) (pp. 845-849). IEEE.

[16] Rabah, K., & Ladaci, S. (2020). A fractional adaptive sliding mode control configuration for synchronizing disturbed fractional-order chaotic systems. Circuits, Systems, and Signal Processing, 39(3), 1244-1264.

[17] Devaney, R.L. (1989). An introduction to chaotic dynamical systems, 2nd edition, p. 49.

[18] García-Martínez, M., & Campos-Cantón, E. (2015). Pseudo-random bit generator based on multi-modal maps. Nonlinear Dynamics, 82(4), 2119-2131.

[19] Dachselt, F., & Schwarz, W. (2001). Chaos and cryptography. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 48(12), 1498-1509.

[20] Murillo-Escobar, M. A., Cruz-Hernández, C., Abundiz-Pérez, F., López-Gutiérrez, R. M., & Del Campo, O. A. (2015). A RGB image encryption algorithm based on total plain image characteristics and chaos. Signal Processing, 109, 119-131.

[21] DeMillo, R. A. (Ed.). (1983). Applied Cryptology, cryptographic protocols, and computer security models (Vol. 29). American Mathematical Soc..

[22] Matouk, A. E. (2009). Stability conditions, hyperchaos and control in a novel fractional order hyperchaotic system. Physics Letters A, 373(25), 2166-2173.

[23] Wang, X. F., & Chen, G. (2002). Pinning control of scale-free dynamical networks. Physica A: Statistical Mechanics and its Applications, 310(3-4), 521-531.

[24] Su, H., & Wang, X. (2013). Pinning control of complex networked systems: Synchronization, consensus and flocking of networked systems via pinning. Springer Science & Business Media.