SEP
SECRETARÍA DE EDUCACIÓN PÚBLICA

TECNOLÓGICO NACIONAL DE MÉXICO

Tecnológico Nacional de México

Centro Nacional de Investigación y Desarrollo Tecnológico

Tesis de Maestría

Control y Sincronización de Sistemas Caóticos de Orden Fraccionario Aplicados a la Encriptación de Imágenes

presentada por

Ing. Luis Felipe Avalos Ruiz

como requisito para la obtención del grado de

Maestro en Ciencias en Ingeniería Electrónica

Director de tesis

Dr. José Francisco Gómez Aguilar

Cuernavaca, Morelos, México. Enero de 2020.

cenidet
Centro Nacional de Investigación y Desarrollo Tecnológico

"2019, Año del Caudillo del Sur, Emiliano Zapata"

Cuernavaca, Mor., 16/diciembre/2019
No. de Oficio: DIE/267/2019
Asunto: Aceptación de documentos de tesis

DR. GERARDO VICENTE GUERRERO RAMÍREZ
SUBDIRECTOR ACADÉMICO
PRESENTE

Por este conducto, los integrantes de Comité Tutorial del **C. Ing. Luis Felipe Avalos Ruiz**, con número de control **M18CE049** de la Maestría en Ciencias en Ingeniería Electrónica, le informamos que hemos revisado el trabajo de tesis profesional titulado **"Control y sincronización de sistemas caóticos de orden fraccionario aplicado a la encriptación de imágenes"** y hemos encontrado que se han realizado todas las correcciones y observaciones que se le indicaron, por lo que hemos acordado aceptar el documento de tesis y le solicitamos la autorización de impresión definitiva.

DIRECTOR DE TESIS

Dr. José Francisco Gómez Aguilar
Doctor en Física
Cédula profesional 9124781

CODIRECTOR DE TESIS

REVISOR 1.

Dr. Juan Reyes Reyes
Doctor en Ciencias en la Especialidad de Control Automático
Cédula profesional 4214833

REVISOR 2.

Dr. Ricardo Fabricio Escobar Jiménez
Doctor en Ciencias en Ingeniería Electrónica
Cédula profesional 7534115

C.p. M.E. Guadalupe Garrido Rivera- Jefa del Departamento de Servicios Escolares
Estudiante
Expediente

MPS/lrr.

"2020, Año de Leona Vicario, Benemérita Madre de la Patria"

Cuernavaca, Morelos, 13/enero/2020

OFICIO No. SAC/006/2020
Asunto: Autorización de impresión de tesis

ING. LUIS FELIPE AVALOS RUIZ
CANDIDATO AL GRADO DE MAESTRO EN CIENCIAS
EN INGENIERÍA ELECTRÓNICA
P R E S E N T E

Por este conducto, tengo el agrado de comunicarle que el Comité Tutorial asignado a su trabajo de tesis titulado "***Control y sincronización de sistemas caóticos de orden fraccionario aplicado a la encriptación de imágenes***", ha informado a esta Subdirección Académica, que están de acuerdo con el trabajo presentado. Por lo anterior, se le autoriza a que proceda con la impresión definitiva de su trabajo de tesis.

Esperando que el logro del mismo sea acorde con sus aspiraciones profesionales, reciba un cordial saludo.

A T E N T A M E N T E
Excelencia en Educación Tecnológica®
"Conocimiento y tecnología al servicio de México"

DR. GERARDO VICENTE GUERRERO RAMÍREZ
SUBDIRECTOR ACADÉMICO

SEP TecNM
CENTRO NACIONAL
DE INVESTIGACIÓN
Y DESARROLLO
TECNOLÓGICO
SUBDIRECCIÓN
ACADÉMICA

C.p. M.E. Guadalupe Garrido Rivera. Jefa del Departamento de Servicios Escolares.
Expediente.

GVGR/chg

Agradecimientos

El presente trabajo fue realizado bajo la supervisión del Dr. José Francisco Gómez Aguilar a quien agradezco su paciencia, dedicación y apoyo para elaboración de este trabajo. Agradezco también a los integrantes del comité revisor; el Dr. Juan Reyes Reyes y al Dr. Ricardo Fabricio Escobar Jimenez, ya que sus comentarios y observaciones fueron valiosos a lo largo de este proceso.

Así mismo deseo expresar mi gratitud a Carlos Zuñiga por su amistad y apoyo académico, así como a todos mis profesores de maestría quienes dedicaron su tiempo para compartir sus conocimientos.

A la Lic. Lorena por su apoyo en todos los tramites necesarios a lo largo de este trabajo.

A mi familia; mis padres y mi hermano, por su incondicional apoyo y cariño. Por educarme y ser ejemplos a seguir.

Al Consejo Nacional de Ciencias y Tecnología (CONACYT) y al Tecnológico Nacional de México (TecNM) por los apoyos otorgados durante el periodo en el que se desarrollo este trabajo.

Por ultimo, al Centro Nacional de Investigación y Desarrollo Tecnológico (CENIDET) por la oportunidad de estudiar la maestría en esta excelente institución.

Resumen

En este trabajo de tesis se analizaron tres algoritmos de encriptación de imágenes en escala de grises los cuales utilizan sistemas caóticos para la generación de secuencias pseudoaleatorias.

El primer algoritmo estudiado emplea el esquema de sincronización de Pecora-Carroll para la sincronización de dos sistemas de Lorenz. El sistema maestro es utilizado para la encriptación de información, mientras que el sistema esclavo sincronizado por medio de el estado y es utilizado para desencriptar los datos.

El segundo caso de estudio aprovecha las propiedades caóticas del mapa de Mandelbrot-Julia para la generación de secuencias pseudoaleatorias utilizadas para convertir la información original.

El tercer caso utiliza un controlador de modos deslizantes robusto para la sincronización de dos sistemas de la familia de Genesio-Tesi, con lo cual es posible sincronizar los sistemas compartiendo un solo estado del sistema.

En todos los casos se generalizó el operador de derivada utilizando definiciones de cálculo generalizado, particularmente la definición de derivada fraccionaria en el sentido de Caputo y la definición de derivada conformable fraccionaria de Khalil.

Los resultados obtenidos muestran índices de desempeño similares a los obtenidos en la literatura, sin embargo la aparición de un nuevo grado de libertad presentada por el orden de derivación incrementa el tamaño de la llave necesaria para recuperar la información de interés.

Abstract

In this thesis, three grayscale image encryption algorithms, which use chaotic systems for the generation of pseudorandom sequences were analyzed.

The first studied algorithm uses the Pecora-Carroll synchronization scheme for the synchronization of two Lorenz systems. The master system is used for the information encryption, while the slave system, synchronized using the system variable y, is used to decrypt the data.

The second case takes advantage of the chaotic properties of the Mandelbrot-Julia map for the generation of pseudo-random sequences used to convert the original information.

The third case uses a robust sliding mode controller for the synchronization of two systems of the Genesio-Tesi family. The scheme makes it possible to synchronize the systems by sharing a single state variable.

In all studied cases the derivative operator was generalized using generalized calculus definitions, particularly the definition of fractional derivative in the Caputo sense and the definition of Khalil for the fractional conformable derivative.

The results obtained show a comparable performance between the proposed methods and those obtained in the literature, however the appearance of a new degree of freedom presented by the order of derivation increases the key size needed to retrieve the information of interest.

Índice

Índice de figuras

Índice de tablas

Capítulo 1

Introducción

En la actualidad se estima que el número de contraseñas existentes ascenderá a 300 billones [1]. El crecimiento de la disponibilidad de información personal en internet trae consigo el problema de proteger estos datos de tal manera que solo los usuarios permitidos tengan acceso a ellos. Debido a esto, el diseño de sistemas de encriptación para el resguardo de información es un tema relevante en la actualidad.

Los sistemas de encriptación engloban al conjunto de algoritmos o protocolos utilizados para convertir información de interés de tal manera que impida a personas no autorizadas acceder a los datos originales [2]. Para el proceso de la recuperación, o bien de desencriptación, es necesario el uso de una tira de datos conocida como llave de encriptación. Es posible dividir los sistemas de encriptación de información en dos partes: la primera genera secuencias de números pseudoaleatorios que posteriormente son aprovechados por la segunda parte, la cual transforma los datos.

Una manera de generar secuencias pseudoaleatorias es mediante el uso de sistemas caóticos. Los sistemas caóticos son conjuntos de ecuaciones dinámicas que presentan ciertas características como no linealidad y sensibilidad a sus parámetros y condiciones iniciales. Debido a que los sistemas caóticos son descritos como sistemas de ecuaciones diferenciales es posible generalizar el operador de derivada utilizando cálculo fraccionario, lo cual permite obtener dinámicas completamente nuevas e imposibles de conseguir con cálculo ordinario. Estas peculiaridades los vuelven candidatos para su uso en sistemas de encriptación.

Una técnica utilizada para inserción de sistemas caóticos en sistemas de encriptación es la sincronización de caos, la cual puede ser lograda por diversos métodos, como el esquema Pecora-Carroll o bien, con el uso de controladores.

En este trabajo de tesis se analizaron tres esquemas de encriptación que utilizan sistemas caóticos para la generación de secuencias pseudoaleatorias, estos algoritmos fueron posteriormente modificados generalizando los operadores diferenciales utilizando cálculo fraccionario para la obtención de métodos de encriptación mas robustos.

1.1. Estudio del estado del arte

Hao en [3], diseñó una metodología mediante la cual es posible realizar un esquema maestro-esclavo utilizando un controlador backstepping activo para dos sistemas de tipo Rössler hipercaóticos.

El trabajo realizado por Alvarez [4], explica que cualidades de un sistema caótico afectan a un método de encriptación y el reflejo que estos tienen en la seguridad de la información. Además propone guias para resolver los tres principales problemas presentados en la criptografía:

- Implementación.
- Manejo de contraseñas.
- Análisis de seguridad.

También presenta equivalencias entre propiedades de sistemas caóticos y propiedades de sistemas criptográficos.

En el trabajo de Saleh [5], se estudia la sincronización por medio de un controlador de modos deslizantes basado en un esquema unidireccional considerando dos casos de estudio, el primero con dos sistemas de tipo Chen y el segundo con dos sistemas de tipo Lü. Ambos sistemas son de orden fraccionario y utiliza para su simulación el método del dominio en la frecuencia y un esquema predictor-corrector. Se demuestra que el controlador por modos deslizantes es robusto y que el comportamiento de dicho controlador puede ser ajustado por medio de sus parámetros.

En el artículo presentado por Rhouma [6], se proponen dos ataques diferentes para romper la encriptación de un algoritmo basado en híper-caos, en este se demuestra que usar la clave de seguridad mas de una vez durante la encriptación debilita la seguridad del sistema de encriptación.

El trabajo presentado por Mazloom y Eftekhari-Moghadam [7] propone un algoritmo de imágenes basado en caos, utilizando un acoplamiento no lineal basado en un mapa caótico para cifrar imágenes de color. La técnica que se utiliza en este artículo pertenece a la criptograía de clave simétrica con dos enfoques principales de la dinámica caótica: sistemas caóticos para generar secuencias pseudoaleatorias, el texto sin formato se utiliza como estado inicial y el texto cifrado se desprende de la órbita que se genera. En los resultados obtenidos se demuestra que el algoritmo con las tranformaciones realizadas así como la estructura de acoplamiento del CNCM han mejorado la seguridad del sistema criptográfico.

En el trabajo presentado por Liñán [8], se presenta una metodología y esquemas basados en técnicas de modos deslizantes de alto orden para lograr la sincronización unidireccional generalizada en orden reducido, además presenta un esquema para supresión de oscilaciones caóticas basado en un controlador retroalimentado y un observador adaptable.

En el trabajo de Lin [9], se utiliza un esquema de sincronización de dos sistemas caóticos de tipo Sprott para la implementación de un sistema de comunicación digital seguro. Para la implementación de este esquema se utilizan componentes electrónicos básicos.

El artículo presentado por Lang [10] propone un nuevo enfoque para el cifrado de imágenes basado en la combinación de la transformada de Fourier fraccionaria discreta de parámetros múltiples y el uso de mapas caóticos logísticos. Los resultados muestran que la metodología de cifrado de imagen propuesto proporciona una forma eficiente y segura de cifrado de imagen.

En el trabajo presentado por Yoon [11], se propone un nuevo algoritmo de encriptación basado en una permutación pseudoaleatoria que se genera a partir de pequeñas matrices de permutación basadas en mapas caóticos. El autor muestra que la metodología de encriptación propuesta proporciona una seguridad comparable con los sistemas de encriptación convencionales basados en el mapa de Baker.

En el trabajo presentado por Kumar Kowar [12] se presenta una discusión acerca de los esfuerzos de investigaciones actuales en técnicas de cifrado de imágenes basadas en esquemas caóticos. El resultado de la discusión ha sido que entre los diversos esquemas ya existentes y actuales se podrá obtener una seguridad de imágenes y multimedia de moderado a bajo en ciertos casos pero haciendo hincapié en aquellas técnicas que se basan en sistemas caóticos, el autor encuentra una mejora de nivel de seguridad del mismo algoritmo mediante el uso de propiedades del caos.

En el trabajo de Indrakanti [13], se presenta la permutación de imágenes y el autor propone una clasificación en tres categorías: permutación de posición, transformación de valor y transformación visual. Como resultado principal el procesamiento con la permutación que genera es único y ese método puede extenderse al tratar de manejar múltiples imágenes en lugar de una sola imagen.

Kuo en [14], utiliza un controlador de modos deslizantes difuso para la sincronización idéntica de dos sistemas caóticos de orden entero. Se utiliza la teoría de estabilidad de Lyapunov para garantizar la efectividad del controlador.

En el trabajo de Chen [15], se utiliza un controlador de modos deslizantes para estabilizar cuatro sistemas caóticos distintos. La técnica propuesta también fue probada con perturbaciones externas, ante las cuales el controlador cumplió su objetivo de estabilización.

En el trabajo de Wang [16], se utiliza un sistema caótico para encriptar los componentes RGB de una imagen en color al mismo tiempo y hacer que estos tres componentes se afecten entre sí, esto lleva a que las correlaciones entre los componentes R, G, B se pueda reducir y se aumente la seguridad del algoritmo. Las simulaciones muestran que el algoritmo propuesto puede cifrar la imagen en color de manera efectiva y resistir varios ataques típicos.

Angulo Guzmán en [17], exploró el tema de sincronización de redes complejas utilizando sistemas de orden fraccionario como nodos. En este trabajo se logró sincronizar tanto redes regulares con distintos acoplamientos, así como redes irregulares, además se presentan simulaciones con sistemas de orden fraccionario pero utilizando circuitos electrónicos y su implementación en redes regulares e irregulares en las cuales se obtuvo sincronización completa.

En el trabajo presentado por Wei [18], se propone un nuevo algoritmo para encriptación de imágenes

a color basado en la operación de secuencias de ADN y sistemas híper-caóticos. El autor propone un método para mejorar la capacidad de resistir un ataque diferencial usando la distancia de Hamming para generar las llaves, además concluye que su algoritmo tiene un buen efecto de cifrado y es capaz de resistir ataques exhaustivos, ataques estadísticos y ataques diferenciales.

En el trabajo de Volos [19], se presenta el esquema original encriptado basado en verdaderos bits aleatorios. El autor toma como elemento principal de su esquema la sincronización caótica completa y como elemento secundario la sincronización inversa p-lag. La finalidad de este esquema es su posible implemntación en sistemas de comunicación confiables, rápidos y seguros para la transmisión de imágenes o fotograías en muchas aplicaciones.

En el articulo de Pai [20], se presenta un controlador de modos deslizantes discreto para la sincronización de sistemas caóticos, además se analiza el problema del chatering así como su reducción. El diseño del controlador es relativamente sencillo y se aplica a un sistema de tipo Lorenz de orden entero.

El trabajo de Yong Xu [21], presenta una investigación sobre el cifrado de imágenes para aumentar la seguridad. Se enfoca en la sincronización del orden caótico de Lorenz de orden fraccionario, los resultados obtenidos de la simulación demuestran que la imagen original y textos cifrados se recuperan con éxito a tráves de señales de sincronización. La validación del esquema se obtuvo mediante las técnicas de histograma, de entropía de información, y una análisis del tamaño de la clave.

En el trabajo de Onma [22], se presenta la sincronización de dos sistemas de tipo Lorenz tanto en su modalidad usual como en su versión hipercaótica utilizando un control de tipo backstepping extendido. La principal característica del controlador empleado es que reduce el esfuerzo de control respecto a otros controladores, lo cual permite su posible implementación física y una reducción en el consumo de energía.

En el articulo presentado por Muthukumar [23], se aplicó la sincronización de dos sistemas de tipo Rey Cobra de orden fraccionario y la sincronización fue aplicada al problema de la encriptación de imágenes. Posteriormente se analizó el nivel de seguridad de esta encriptación con 3 pruebas distintas de las cuales ninguna pudo recuperar la imagen original.

En el trabajo de Chaparro Guevara [24], se utiliza una metodología propuesta procedente de la teoría del control de sistemas dinámicos caóticos para sustentar teóricamente el uso de reglas de política monetaria como un estudio de técnicas del control de sistemas caóticos en la dinámica económica.

En el trabajo presentado por Jafari [25], se tiene la sincronización y estabilización de sistemas no lineales de orden fraccionario por medio de un controlador difuso adaptable. El autor concluye que debido a la falta de conocimiento sobre el comportamiento de la planta de orden de integración fraccionario, el diseño de funciones de membresía apropiadas es complicado, comentando que un controlador difuso tradicional no podría controlar la planta de manera efectiva.

Taher en [26], presenta una compilación de métodos estudiados para el control y sincronización de sis-

temas caóticos de orden fraccionario. El enfoque principal se centra en las aplicaciones de controladores de orden fraccionario así como su uso en la teoría del caos y la sincronización.

En el trabajo de Rajagopal [27], se proponen tres metodologías para suprimir el caos en el modelo de orden fraccionario de un motor brushless de corriente directa. Los tres controladores utilizados para este propósito fueron: un controlador por modos deslizantes, un controlador robusto y un controlador de back-stepping extendido.

En el trabajo de Jinde Cao [28], se estudia la sincronización en un tiempo previamente definido de sistemas memristivos con retraso. En particular se utilizan los conceptos de funciones de Lyapunov y un controlador discontinuo para garantizar la sincronización de los sistemas. Esta metodología se compara además con la sincronización en tiempo finito obteniendo buenos resultados.

En el trabajo de Ouannas [29], se presenta la sincronización híbrida basada en los conceptos de sincronización generalizada y sincronización generalizada inversa en distintos sistemas caóticos de orden fraccionario. En este caso, el autor considera que los sistemas pueden poseer distintas estructuras, además no necesariamente deben ser del mismo orden. La complejidad del algoritmo propuesto incremento la seguridad para su posible uso en sistemas de encriptación caóticos.

En el trabajo presentado por Coronel Escamilla [30], se utiliza una metodología basada en un observador de estados para la sincronización de sistemas caóticos de orden fraccionario variable en el tiempo. En este trabajo se utilizan las definiciones de derivada de Liouville-Caputo y Atangana-Baleanu-Caputo. Para los ordenes variables de las derivadas se utilizan funciones suaves acotadas entre cero y uno.

En el trabajo de Zambrano-Serrano [31], se estudia el comportamiento de la sincronización entre dos sistemas caóticos de orden fraccionario que describen el comportamiento de células β en el páncreas. El uso de un modelo fraccionario provee distintos comportamientos en los sistemas, imposibles de obtener con el modelo de orden entero. Se utiliza también un esquema de sincronización unidireccional que garantiza la sincronización idéntica de ambos sistemas.

En el trabajo realizado por Wang [32], se analiza un sistema caótico de orden fraccionario que para ciertas condiciones iniciales y parámetros presenta dos puntos de equilibrio. Además estudia dos esquemas para la sincronización basados en la sincronización proyectiva híbrida, estos esquemas permiten sincronizar el sistema con un sistema fraccionario de orden mayor.

En el trabajo realizado por Aguilar [33], se utiliza la estructura de un observador robusto para la sincronización de ciertos sistemas caóticos en una configuración maestro-esclavo utilizando el método de inmersión e invarianza. Al aplicar la metodología propuesta se remarca que el sistema esclavo puede, bajo ciertas consideraciones, comportarse como un observador de alta ganancia de orden reducido. El desempeño del observador propuesto se compara con el de un observador de Luenberger clásico.

En el trabajo presentado por Delfin-Prieto [34], se propone una metodología para generar un observador de estados para sistemas caóticos de orden fraccionario. La metodología propuesta presenta robustez

ante la incertidumbre, por lo tanto el observador obtenido presenta convergencia asintótica a pesar de la aparición de perturbaciones.

1.2. Planteamiento del problema

La protección de información privada es un problema que continúa evolucionando con el avance de la tecnología, por lo tanto la generación de métodos que permitan ocultar datos es un tema de estudio de interés en la actualidad.

La base de la criptografía consiste en utilizar un algoritmo para transformar información utilizando una clave la cual permite recuperar el mensaje original. Este algoritmo consiste en general de dos partes fundamentales: la generación de números aleatorios y un proceso de confusión. Debido a que sus propiedades incluyen alta sensibilidad a parámetros y condiciones iniciales, los sistemas caóticos e hipercaóticos han sido utilizados para la generación de números aleatorios. Debido a que los sistemas caóticos son descritos por ecuaciones diferenciales es posible generalizarlos y describirlos utilizando el cálculo fraccionario, la generalización permite añadir un parámetro adicional (orden de la derivada), el cual modifica la dinámica del sistema incrementando el número de trayectorias fractales obtenibles.

1.3. Objetivo

1.3.1. General

Obtener nuevas dinámicas en sistemas caóticos aplicando definiciones de cálculo generalizado para su aplicación en sistemas criptográficos.

Utilizar técnicas de control activo, robusto y modos deslizantes para sincronizar diferentes sistemas dinámicos caóticos e hipercaóticos de orden fraccionario.

1.3.2. Específicos

- Sincronizar sistemas dinámicos caóticos de orden fraccionario y aplicarlos en comunicaciones seguras de señales analógicas digitales y sistemas criptográficos.
- Investigar la interrelación entre el orden fraccionario y la sincronización en diferentes sistemas caóticos.
- Desarrollar controladores para sincronizar sistemas caóticos de orden fraccionario en la estructura maestro-esclavo.
- Analizar las ventajas y/o desventajas de implementar derivadas fraccionarias de orden variable y constante.
- Aplicar estos esquemas en sistemas caóticos que generan familias de atractores (multi-scrolls).

1.3.3. Metas

- Utilizar distintos métodos de sincronización de sistemas caóticos y aplicarlos a sistemas de orden de integración no entero.
- Desarrollar una metodología que permita el uso de sistemas caóticos de orden no entero para la encriptación de información.

1.3.4. Justificación

El incremento de la disponibilidad de información personal y su protección aumentan la necesidad del uso de algoritmos de encriptación. El uso de sistemas caóticos, enriqueciendo su dinámica generalizando su orden de derivación, provee una alternativa novedosa para la protección de datos. Algunas estadísticas sobre la protección de información se muestran a continuación:

- Se estima que para el 2020 el número de contraseñas ascenderá a 300 billones.
- 7 de cada 10 empresas mexicanas han experimentado un incidente relacionado con seguridad informática.
- México es el país de América latina con mayor número de ciberataques por año.

1.4. Hipótesis

El enriquecimiento de las dinámicas obtenibles al generalizar el orden de las derivadas que describen sistemas caóticos permitirá el diseño de esquemas de encriptación mas robustos y seguros.

1.5. Alcance

Para este trabajo de investigación se analizaran tres esquemas de encriptación distintos los cuales utilizan el caos para la generación de secuencias pseudoaleatorias del algoritmo. Se modificaran dichos sistemas introduciendo definiciones de cálculo fraccionario para la obtención de nuevos comportamientos caóticos que permitan encriptar la información con mayor robustez.

1.6. Organización del documento

El presente documento está organizado de la siguiente manera:

En el capítulo 2 se presentan conceptos de sistemas caóticos y su sincronización.

En el capítulo 3 se introducen las definiciones de cálculo fraccionario que se utilizaron a lo largo de este trabajo así como sus características.

En el capítulo 4 se mencionan conceptos básicos de encriptación de sistemas.

En el capitulo 5 se discuten los resultados obtenidos al generalizar los operador diferenciales a diversos sistemas caóticos aplicados en estructuras de encriptación.

Finalmente en el capitulo 6 se comentan las conclusiones y posibles trabajos futuros.

Capítulo 2

Sincronización de Sistemas Caóticos

2.1. Sistemas Caóticos

La teoría del caos es la rama de las matemáticas que lidia con el estudio de la aparición de desorden e irregularidades en sistemas dinámicos, los cuales son comúnmente gobernados por leyes deterministas que son altamente sensibles a condiciones iniciales [35]. La teoría del caos ha sido utilizada para el estudio de diversos sistemas dinámicos deterministas que a simple vista parecen tener comportamientos impredecibles, a pesar de su aparente sencillez. Los sistemas estudiados se pueden encontrar en una multitud de disciplinas como por ejemplo: economía, ingeniería, biología, física, meteorología, sociología entre otras.

Los sistemas caóticos presentan, para valores iniciales arbitrariamente cercanos, trayectorias futuras diferentes. Esto se traduce a que un pequeño cambio en las condiciones iniciales o parámetros del sistema genera valores cada vez mas distintos conforme avanza el tiempo. Debido a esto, si no se tiene exactamente los valores de condiciones iniciales y parámetros de un sistema caótico es prácticamente imposible predecir su comportamiento a largo plazo. Por ejemplo, es posible predecir la temperatura de una región generalmente con una semana de anticipación, sin embargo la predicción de eventos mas lejana es basada en ciertas restricciones observables del sistema. En la Figura 2.1 se muestran tres trayectorias obtenidas del sistema de Lorenz al hacer cambios arbitrariamente pequeños en las condiciones iniciales, como se puede ver incluso cambios relativamente pequeños en los parámetros o condiciones iniciales del sistema provocan trayectorias distintas acotadas alrededor de los mismos valores de amplitud.

Una manera de describir la divergencia causada por el cambio de condiciones iniciales es a través de el exponente de Lyapunov, mostrado en la ecuación (2.1)

$$|\delta Z(t)| \approx e^{\lambda t}|\delta Z_0|, \tag{2.1}$$

donde t es el tiempo, λ es el exponente de Lyapunov y δZ_0 se refiere a una separación inicial. El exponente de Lyapunov se refiere a la relación exponencial de separación de dos trayectorias de un sistema debido a una separación infinitesimal entre sus condiciones iniciales. El número de exponentes de Lyapunov obtenibles para un sistema es igual a su número de estados, por lo tanto se refiere normalmente al exponente máximo de Lyapunov debido a que determina la predictibilidad del sistema. Si el sistema

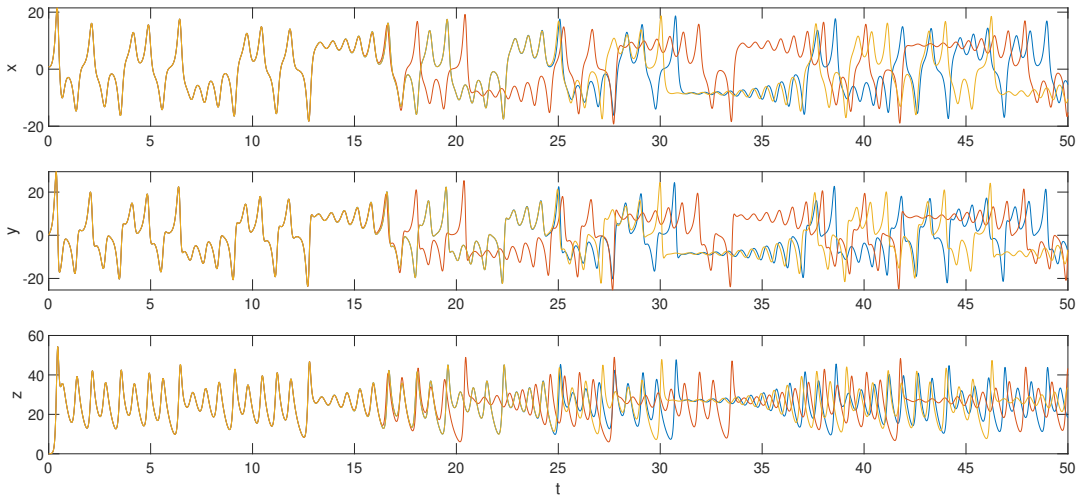


Fig. 2.1. Tres simulaciones de sistemas de Lorenz con parámetros idénticos solamente cambiando el valor inicial de el primer estado. En azul 1, en rojo 1.00001 y en amarillo 1.000000001.

es conservativo la suma de sus exponentes de Lyapunov será 0. Por otro lado si el sistema es disipativo, la suma de sus exponentes de Lyapunov será negativa.

Otra propiedad compartida entre los sistemas caóticos es la existencia de atractores. Los atractores de un sistema caótico son conjuntos de valores numéricos hacia los cuales un sistema tiende a evolucionar para una gran variedad de combinaciones entre condiciones iniciales y parámetros. Valores del sistema que se acercan lo suficiente a un atractor se mantienen cerca incluso ante perturbaciones pequeñas. Cualquier trayectoria que se encuentre en un atractor estará en el para $t \to \infty$ Esto provoca que los sistemas presenten comportamientos pseudoperiodicos, donde los valores usualmente obtenidos cerca del atractor se mantienen acotados en un rango cercano a este, sin embargo las orbitas obtenidas no se repiten entre ellas.

El primer sistema caótico propuesto fue postulado por Edward Lorenz en 1963, quien intentaba obtener un modelo simplificado del fenómeno de convección en la atmósfera. Las ecuaciones que definen el modelo de Lorenz se presentan en la ecuación (2.2)

$$\begin{aligned} \dot{x} &= A\,(x - y)\,, \\ \dot{y} &= Bx - y - xz, \\ \dot{z} &= xy - Cz, \end{aligned} \tag{2.2}$$

donde x es proporcional a la velocidad de convección, y se refiere a la variación de temperatura horizontal y z es la variación de temperatura vertical. Las constantes A, B y C son parámetros del sistema. El uso de retratos fase es común para el análisis de estos sistemas. El retrato fase es la relación de dos estados entre si, al obtenerlo para un sistema es posible ver los puntos a los que tiende a evolucionar después de un tiempo. En la Figura 2.2 se muestra el retrato fase del sistema de Lorenz.

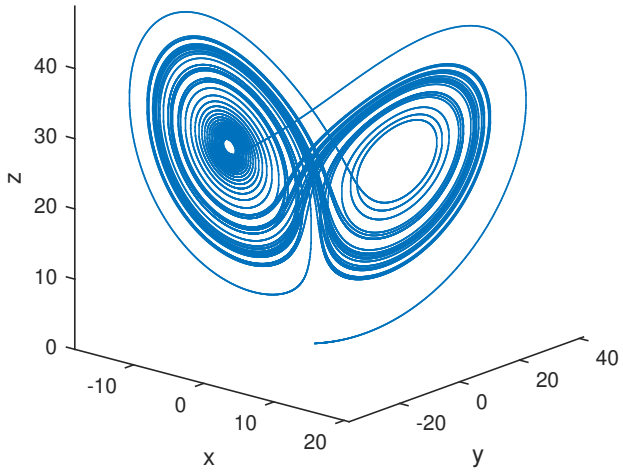


Fig. 2.2. Sistema de Lorenz con $a = 10$, $b = \frac{8}{3}$, $c = 28$ y condiciones iniciales [0.1 0 0].

Existen también sistemas caóticos discretos conocidos como mapas caóticos, el ejemplo mas simple es el mapa logistico. Estudiado por Robert May en 1976, el mapa logístico es un ejemplo de la aparición de comportamiento caótico en un sistema no lineal simple. El modelo pretende describir de manera simplificada el cambio de una población respecto al tiempo considerando el crecimiento por reproducción y un decremento ocasionado por hambruna. En la ecuación (2.3) se presenta la ecuación del mapa logístico

$$x_{n+1} = r x_n (1 - x_n), \tag{2.3}$$

donde x_n es un número entre cero y uno que representa la relación entre la población actual y la población máxima posible, mientras que $r \in [0, 4]$ describe los efectos de mortandad y natalidad. Para visualizar de una manera sencilla los valores de r para los cuales el sistema presenta caos es útil el uso de diagramas de bifurcación.

Un diagrama de bifurcación muestra los valores a los cuales se acerca un sistema de manera asintótica un sistema en función del cambio de un parámetro de bifurcación. Esto es útil debido a que permite apreciar los valores de un parámetro para los cuales un sistema presenta comportamientos caóticos. Numéricamente la obtención de un diagrama de bifurcación sigue los pasos mostrados a continuación:

- Se define el parámetro de bifurcación y se ajustan los demás parámetros en valores fijos.
- Se define un rango para el parámetro de bifurcación, así como un paso en el que aumentará en cada iteración.

- Se simulan las ecuaciones del sistema variando el parámetro de bifurcación en el rango previamente establecido y se guardan los últimos valores de cada simulación.
- Posteriormente se grafican los datos obtenidos de cada simulación.

En la Figura 2.3 se muestra el diagrama de bifurcación respecto al parámetro r para la ecuación del mapa logístico. En el eje horizontal se tiene el parámetro de bifurcación, mientras que en el eje vertical se tienen los últimos valores de simulación para cada valor de r. Como se puede ver en la figura, para valores de r entre 3.57 y 4 presenta comportamiento caótico, sin embargo es posible apreciar ciertas regiones de estabilidad, representadas como franjas aparentemente vacias.

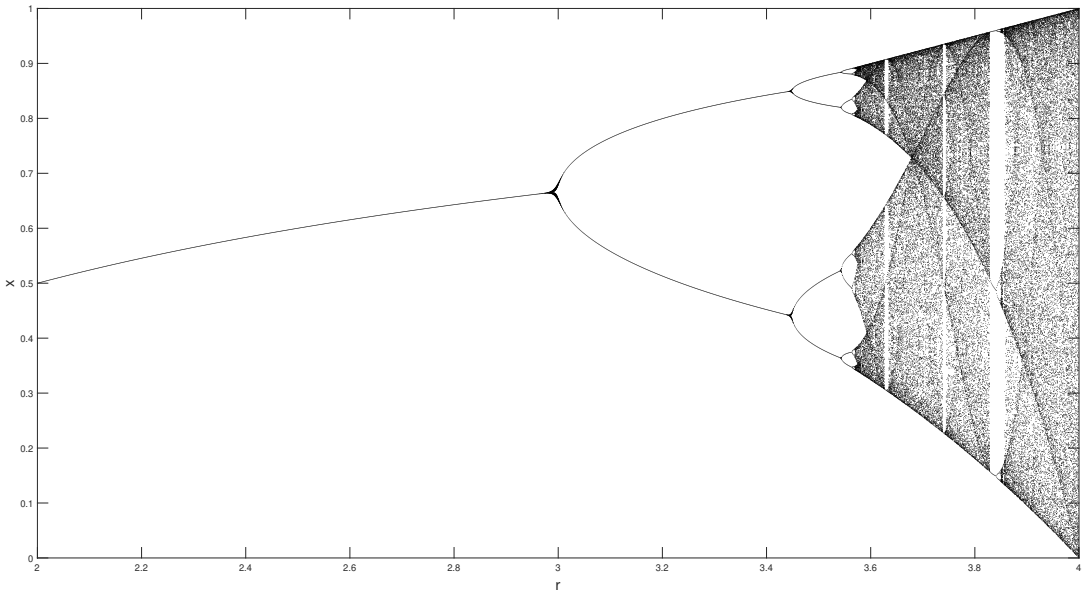


Fig. 2.3. Diagrama de bifurcación de mapa logístico respecto a r.

2.2. Sincronización

La sincronización se refiere al ajuste temporal de eventos para que estos ocurran en un orden predefinido o en su defecto al mismo tiempo [36]. El primer caso reportado de su estudio en un fenómeno físico fue comunicado por Huygens en 1673, quien estudió el fenómeno de sincronización en péndulos interconectados. Encontró que dos relojes que colgaban de la misma viga oscilaban a exactamente la misma frecuencia y fase opuesta, esto ocurre debido al acoplamiento físico existente entre los dos relojes. En este caso, los relojes solo se sincronizaban cuando sus frecuencias individuales eran similares. En el caso particular de sistemas caóticos existen distintos tipos de sincronización, a continuación se listan algunos de ellos:

- Sincronización generalizada:
  Dos sistemas Σ_1 y Σ_2 presentan el caso de sincronización generalizada si en el límite $t \to \infty$

sus estados se encuentran relacionados por una función H tal que $||H(\Sigma_1) - \Sigma_2|| \to 0$. Si el acoplamiento entre los sistemas es bidireccional entonces la función H debe tener inversa.

- Sincronización de fase:
  La sincronización de fase se presenta cuando la diferencia entre la fase de los sistemas se vuelve constante. Si ϕ_1 y ϕ_2 denotan la fase de dos sistemas acoplados, entonces la sincronización de fase ocurre cuando $n\phi = m\phi$, $n, m \in \mathbb{N}$. Esta condición es independiente de la amplitud de los sistemas, la cual puede ser completamente distinta.

- Sincronización idéntica:
  En este caso se cumple, para dos sistemas acoplados Σ_1 y Σ_2, la condición $\Sigma_1 - \Sigma_2 \to 0$ cuando $t \to \infty$. Esto quiere decir que incluso para condiciones iniciales diferentes ambos sistemas convergerán a la misma trayectoria.

Basado en el tipo de acoplamiento, los esquemas de sincronización pueden dividirse en dos tipos:

- Acoplamiento bidireccional:
  Ambos sistemas son conectados de tal manera que sus trayectorias están mutuamente influenciadas por el comportamiento del otro. En la ecuación (2.4) se muestran dos sistemas de Lorenz acoplados de manera bidireccional, donde el acoplamiento se puede ver en el primer estado de ambos sistemas.

$$\begin{array}{cc} \dot{x} = A(x-y) - D(y-\hat{y}), & \dot{\hat{x}} = A(\hat{x}-\hat{y}) - D(y-\hat{y}), \\ \dot{y} = Bx - y - xz, & \dot{\hat{y}} = B\hat{x} - \hat{y} - \hat{x}\hat{z}, \\ \dot{z} = xy - Cz, & \dot{\hat{z}} = \hat{x}\hat{y} - C\hat{z}. \end{array} \tag{2.4}$$

  En este caso particular los sistemas son iguales entre ellos, siendo la diferencia su valor inicial. En la Figura 2.4 se muestra el comportamiento de ambos sistemas con condiciones iniciales [10 5 0] y [3 0 4], respectivamente.

- Acoplamiento unidireccional:
  También conocido como acoplamiento maestro-esclavo. En este caso se tiene un sistema llamado esclavo cuya dinámica depende de un segundo sistema llamado maestro. En la literatura es común encontrar el uso de controladores para definir el acoplamiento del sistema esclavo y asegurar así la sincronización idéntica de los sistemas. La Figura 2.5 muestra la sincronización de dos sistemas caóticos con parámetros distintos por medio de un acoplamiento unidireccional. El método de sincronización utilizado emplea un controlador adaptable, el cual varia los parámetros del sistema esclavo con el objetivo de que siga la trayectoria del sistema maestro.

Particularmente, para el desarrollo de esta tesis se han explorado dos métodos de sincronización unidireccional idéntica.

Primer Caso. Involucra el uso de un controlador para la sincronización de dos sistemas caóticos en un esquema maestro-esclavo, aplicando esta técnica a un sistema de Lorenz se obtiene

$$\begin{array}{cc} \dot{x} = A(x-y), & \dot{\hat{x}} = A(\hat{x}-\hat{y}) + u_1, \\ \dot{y} = Bx - y - xz, & \dot{\hat{y}} = B\hat{x} - \hat{y} - \hat{x}\hat{z} + u_2, \\ \dot{z} = xy - Cz, & \dot{\hat{z}} = \hat{x}\hat{y} - C\hat{z} + u_3, \end{array} \tag{2.5}$$

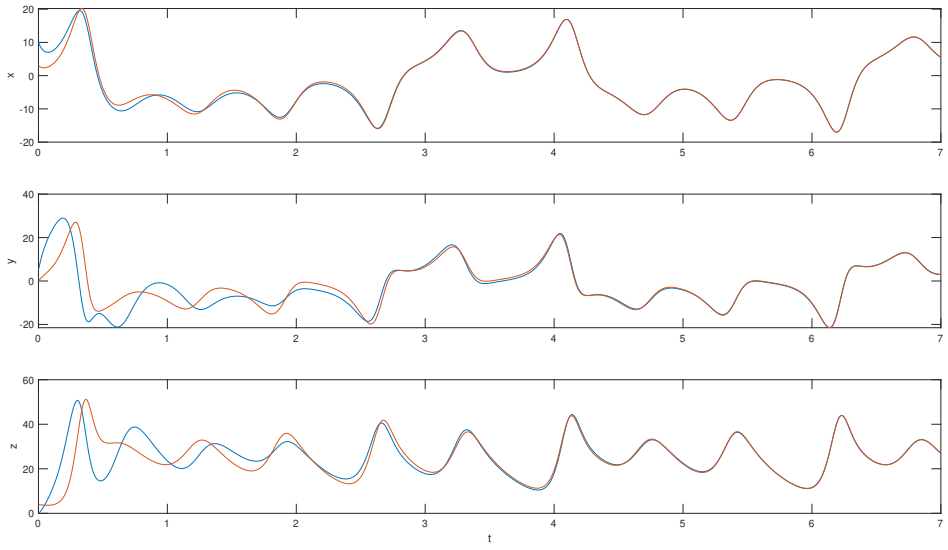


Fig. 2.4. Sincronización idéntica de los sistemas propuestos en la ecuación (2.4).

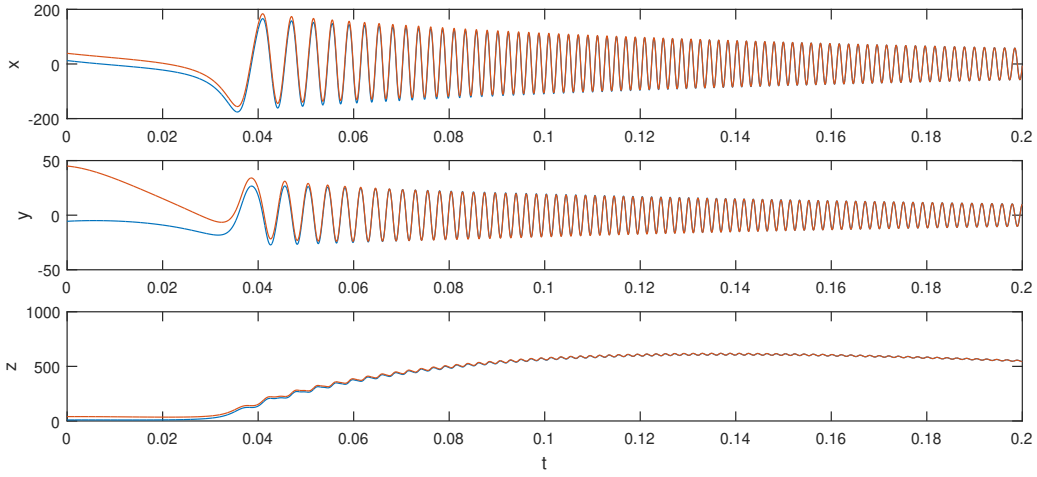


Fig. 2.5. Sincronización unidireccional de dos sistemas caóticos. En azul se muestra el sistema maestro y en rojo el sistema esclavo.

donde u_i representa la ley de control, que puede ser obtenida aplicando distintos controladores, como por ejemplo: modos deslizantes, control activo o control robusto (particularmente en este trabajo de tesís adoptamos el esquema basado en modos deslizantes).

Segundo Caso. En este caso consideraremos el propuesto por Pecora-Carroll [37] en el cual el sistema

maestro comparte uno de sus estados con el sistema esclavo como se muestra en la ecuación (2.6)

$$\begin{array}{ll} \dot{x} = A\left(x - y\right), & \dot{\hat{x}} = A\left(\hat{x} - y\right), \\ \dot{y} = Bx - y - xz, & \dot{y} = Bx - y - xz, \\ \dot{z} = xy - Cz, & \dot{\hat{z}} = \hat{x}y - C\hat{z}. \end{array} \tag{2.6}$$

El estado que debe ser compartido entre ambos sistemas es elegido de acuerdo a los exponentes de Lyapunov del sistema, en el caso de el sistema de Lorenz con los parámetros $A = 10$, $B = \frac{8}{3}$ y $C = 60$ se representan en la Tabla 2.1, si la suma de ambos exponentes de Lyapunov obtenidos es negativa, entonces se cumplira la condición de sincronización idéntica, entre mas negativos sean los exponentes, la condición se cumplirá en un menor tiempo.

Estado Conductor	Estados del sistema esclavo	Exponentes de Lyapunov
x	(y,z)	(-1.81,-1.86)
y	(x,z)	(-2.67, -9.99)
z	(x,y)	(0.0108,-11.01)

Tabla 2.1. Exponentes de Lyapunov para el sistema de Lorenz.

Capítulo 3

Cálculo Fraccionario

El cálculo fraccionario es la extensión del cálculo que considera ordenes de integración y derivación no enteros [38]. Estos ordenes pueden ser fracciones, números imaginarios o funciones variantes en el tiempo. Para este trabajo se considerará la notación presentada en la ecuación (3.1), en donde el operador de derivada se representa con la letra $\mathcal{D}$, t_0 y t corresponden a los límites inferior y superior respectivamente de la integral asociada. El orden de la derivada se representa con $\alpha(t)$, es importante recalcar que en sistemas de ecuaciones diferenciales los ordenes de derivación no necesariamente deben ser iguales entre ellos. A pesar de que $\alpha(t)$ es variante en el tiempo, para la notación de este trabajo se considerará constante a menos que se indique lo contrario.

$$\left({}_{t_0}^{Q}\mathcal{D}_t^{\alpha(t)}\right) x(t). \tag{3.1}$$

Cuando el orden de la derivada es negativo se refiere entonces a la integral asociada a la definición como se muestra en la ecuación (3.2)

$$\left({}_{t_0}^{Q}\mathcal{D}_t^{\alpha(t)}\right) x(t) = \begin{cases} \frac{d}{dt}x(t) & \alpha = 1, \\ x(t) & \alpha = 0, \\ \int_{t_0}^{t} x(t)dt & \alpha = -1. \end{cases} \tag{3.2}$$

El cálculo fraccionario parte de la necesidad de encontrar la solución a ecuaciones diferenciales cuyos órdenes son distintos de uno, si bien esta idea es casi tan antigua como la del cálculo tradicional las primeras bases en el tema fueron sentadas por Liouville en 1832. Diversas ramas han sido creadas con la intención de resolver este problema. Las aplicaciones del cálculo fraccionario fueron limitadas en su origen debido a la falta de una interpretación física y su complejidad de procesamiento. En años recientes, el creciente interés en el tema y la inclusión de nueva tecnología han llevado a su uso en el modelado de sistemas. El cálculo fraccionario recurre usualmente al uso de funciones superiores como la función Gamma o la función de Mittag-Leffler.

La función Gamma permite extender la definición del factorial a los números imaginarios y negativos no enteros. Al ser una función que generaliza una operación necesaria para las definiciones de derivadas, es una función sumamente importante dentro del cálculo fraccionario. La definición matemática de esta función se muestra en la ecuación (3.3)

$$\Gamma(z) = \int_0^\infty e^{-t}t^{z-1}dt. \tag{3.3}$$

Es posible recuperar la operación factorial para números naturales por medio de la siguiente propiedad

$$\Gamma(z+1) = z\Gamma(z), \tag{3.4}$$

se tiene entonces que

$$\Gamma(z+1) = z!. \tag{3.5}$$

La función de Mittag-Leffler permite la generalización de la función exponencial, lo cual le proporciona una gran relevancia dentro del ámbito del cálculo fraccionario debido a que al momento de resolver ecuaciones diferenciales de primer orden se obtienen comportamientos exponenciales, por lo tanto, resolver ecuaciones diferenciales de orden fraccionario cercano a 1 genera comportamientos pseudoexponenciales que son posibles de describir con esta función [39]. La función uniparamétrica de Mittag-Leffler esta dada por la siguiente expresión (3.6)

$$E_\alpha(z) = \sum_{k=0}^{\infty} \frac{z^k}{\Gamma(\alpha k + 1)}, \tag{3.6}$$

en donde α es el parámetro de la función y debe ser positivo.

Para distintos ordenes de α es posible recuperar distintos comportamientos, algunos de ellos se muestran a continuación:

- Para $\alpha = 0$ se recupera la forma de una progresión geométrica

$$E_0(z) = \frac{1}{1-z}. \tag{3.7}$$

- Para $\alpha = 1$ se tiene una función exponencial

$$E_1(z) = \sum_{k=0}^{\infty} \frac{z^k}{k!} = e^z. \tag{3.8}$$

- Para $\alpha = 2$ se encuentran cosenos como se muestra en la ecuación (3.9)

$$\begin{aligned} E_2(z) &= cosh\left(\sqrt{z}\right), \\ E_2(-z^2) &= cos\left(z\right). \end{aligned} \tag{3.9}$$

En la Figura 3.1 se presenta un esquema en el cual es posible observar distintas ramificaciones del cálculo que han sido desarrolladas para lidiar con el problema de ordenes de integración no enteros. El cálculo fraccionario, el cálculo conformable y el cálculo conformable fraccionario son herramientas que han sido creadas con la finalidad de obtener dinámicas con distintos ordenes de integración. En el caso del cálculo fraccionario se tiene un orden de integración denotado en la imagen como $\alpha(t)$ el cual al ser igual a 1 se recupera el caso del cálculo ordinario, de igual manera en el cálculo conformable se recupera el caso clásico cuando el orden de derivación β es igual a 1. El cálculo conformable fraccionario es una generalización de la definición de Liouville-Caputo la cual comparte características con ciertos operadores conformables. En el caso del calculo conformable fraccionario se tienen dos ordenes, $\alpha(t)$ que corresponde al orden de la parte fraccionaria y $\beta(t)$ que corresponde al orden de la parte conformable. En la siguiente parte de este capitulo se procederá a mencionarlos a mayor detalle.

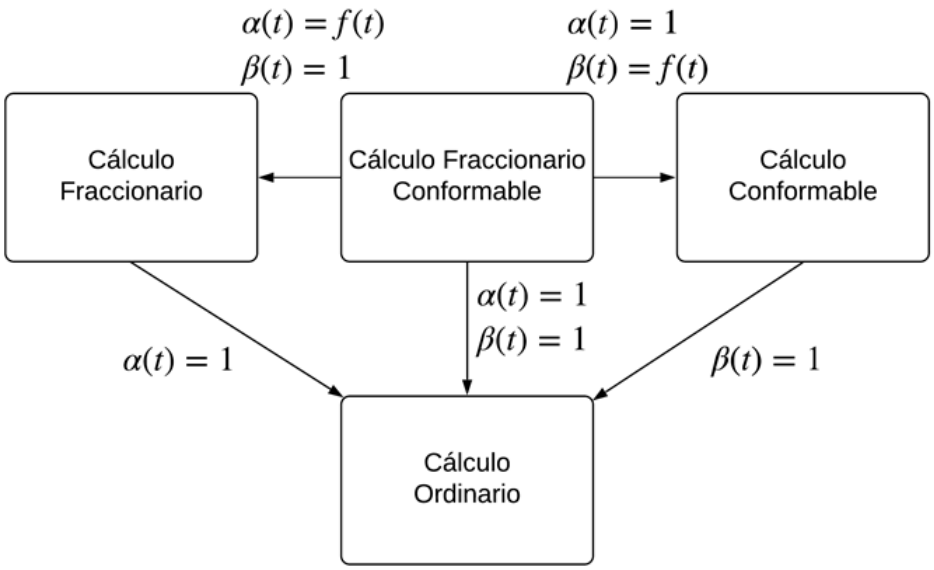


Fig. 3.1. Diversas generalizaciones del cálculo tradicional.

3.1. Cálculo Fraccionario

El cálculo fraccionario fue desarrollado inicialmente por Liouville en 1832. Desde entonces múltiples definiciones de derivadas fraccionarias han sido propuestas, por ejemplo las definiciones de Riemann-Liouville (RL), Liouville-Caputo (C), Caputo-Fabrizio (CF) o Atangana-Baleanu (AB), por mencionar algunas [40]. Cada una de estas definiciones puede ser separada en una parte con un operador diferencial y una parte de convolución. En la ecuación (3.10) se muestra la definición de una convolución en el dominio del tiempo.

$$(f * g)(t) = \int_{-\infty}^{\infty} f(\eta) g(t-\eta) d\eta. \tag{3.10}$$

Las definiciones presentadas a continuación pueden ser interpretadas como la convolución de la derivada de la función con un kernel de memoria; el cual puede ser exponencial, de potencia o una función Mittag-Leffler [41]. Una interpretación estadística de la interpolación es el promedio móvil ponderado, por lo tanto, estas definiciones podrían representarse como la función ponderada por el kernel de la definición, lo cual provoca el efecto de memoria.

Definición 1. Sea x: $\mathbb{R} \to \mathbb{R} \times [a, b]$, $\alpha \in [n-1, n]$ entonces, la definición de Riemann-Liouville (RL) de orden variable se define como

$$\left({}_a^{RL}\mathcal{D}_b^{\alpha(t)} x\right)(t) = \frac{1}{\Gamma(n-\alpha(t))} \frac{d^n}{dt^n} \int_a^b \frac{x(\tau)}{(t-\tau)^{\alpha(\tau)-n+1}} d\tau. \tag{3.11}$$

Es posible separar la derivada fraccionaria de Riemman-Liouville en dos partes, la primera constituye un proceso de convolución entre la función a derivar y un kernel de potencia y la segunda, un proceso de diferenciación de la función obtenida. En este caso, la convolución con el kernel describe un efecto

interpretado como memoria si la derivada es respecto al tiempo, o bien fractalidad si se deriva respecto al espacio. El efecto de memoria recuperado por la definición de Riemman-Liouville es útil para la descripción de fenómenos de difusión anómalos encontrados en física, química y biología. Además se ha demostrado que el uso de esta definición utilizando órdenes variables ha sido una herramienta útil para modelar fenómenos viscoelásticos. Sin embargo, la definición de derivada de Riemman-Liouville presenta ciertas desventajas desde un punto de vista físico. Primeramente, la derivada de una constante no es cero. Además, al momento de encontrar la solución para ecuaciones diferenciales de orden fraccionario, se requieren condiciones iniciales fraccionarias, las cuales no tienen una interpretación física evidente. Para encontrar la solución numérica de la definición de Riemman-Liouville se suele recurrir a la definición de Grunwald-Letnikov.

Definición 2. Sea $x : \mathbb{R} \to \mathbb{R}$, $\alpha \in (n-1, n]$, entonces, la definición de Grünwald-Letnikov (GL) de orden variable está dada como

$$\left({}_a^{GL}\mathcal{D}_b^{\alpha(t)}x\right)(t) = \lim_{h\to 0} h^{-\alpha(t)} \sum_{j=0}^{\frac{b-a}{h}} (-1)^j \binom{\alpha(j)}{j} x(t-jh). \tag{3.12}$$

La principal característica de la derivada de Grunwald-Letnikov radica en que es discreta. Esta definición puede ser considerada como una extensión del método de Euler para ecuaciones diferenciales de orden no entero. Para esta definición cuando $\alpha = 1$ se recupera el método de Euler.

Definición 3. Sea x: $\mathbb{R} \to \mathbb{R} \times [a, b]$,$\alpha \in [n-1, n]$, entonces la definición de Liouville-Caputo (C) de orden variable se define como

$$\left({}_a^{C}\mathcal{D}_b^{\alpha(t)}x\right)(t) = \frac{1}{\Gamma(n-\alpha(t))} \int_a^b \frac{d^n}{dt^n} \frac{x(\tau)}{(t-\tau)^{\alpha(t)-n+1}} d\tau. \tag{3.13}$$

La definición de derivada de Liouville-Caputo es muy similar a la definición de Riemman-Liouville presentada en la ecuación (3.11), siendo la diferencia la ubicación del operador diferencial. En el caso de la definición de Riemman-Liouville el operador se encuentra fuera de la integral, mientras que en el caso de la definición de Liouville-Caputo el operador se encuentra dentro de la integral. Debido a esto, al momento de encontrar la solución a ecuaciones diferenciales fraccionarias utilizando esta definición, se utilizan condiciones iniciales y condiciones de frontera tradicionales. La derivada fraccionaria de Liouville-Caputo para una constante es 0. Debido a estas características, la derivada fraccionaria de Liouville-Caputo es preferida para problemas encontrados en el mundo real y permite describir aplicaciones en campos como física e ingeniería. Sin embargo, al calcular esta definición se requiere la derivada entera de la función, por lo tanto, solo esta definida para funciones diferenciales, en cambio funciones que no tienen derivada de primer orden pueden tener derivadas fraccionarias para ordenes menores a 1 con la definición de Riemman-Liouville.

Definición 4. Sea x: $\mathbb{R} \to \mathbb{R} \times [a, b]$,$a \in [-\infty, b]$, $f \in C^1$ entonces, la definición de la derivada fraccionaria en el sentido de Caputo-Fabrizio-Caputo de orden variable esta dada por

$$\left({}_a^{CFC}\mathcal{D}_b^{\alpha(t)}x\right)(t) = \frac{M(\alpha(t))}{1-\alpha(t)} \int_a^b \frac{d^n}{dt^n}(x(\tau)) \exp\left[-\frac{\alpha(t)}{1-\alpha(t)}(t-\tau)\right] d\tau, \tag{3.14}$$

donde,

$$M(\alpha(t)) = 1 - \alpha(t) + \frac{\alpha(t)}{\Gamma(\alpha(t))}. \tag{3.15}$$

La derivada de Caputo-Fabrizio posee un kernel exponencial a diferencia de las definiciones de Riemman-Liouville y de Liouville-Caputo, las cuales presentan un kernel de potencia. Al tener la memoria ponderada por una función exponencial, el efecto de memoria presentado por el operador es mas débil al compararlo con otras definiciones. Debido a que la función exponencial aparece comúnmente en fenómenos encontrados en la naturaleza, esta definición permite describir mejor esos comportamientos. En la ecuación (3.14) se presenta la definición de derivada fraccionaria de Caputo-Fabrizio en el sentido de Liouville-Caputo, donde con sentido se refiere a la ubicación de el operador diferencial en la ecuación (el operador se encuentra dentro de la integral), existe también el sentido de Riemman, donde la única diferencia es la ubicación del operador diferencial (fuera de la integral).

Definición 5. Sea x: $\mathbb{R} \to \mathbb{R}$, la definición de derivada fraccionaria en el sentido de Atangana-Baleanu-Caputo de orden variable esta dada por

$$\left({}_a^{ABC}\mathcal{D}_b^{\alpha(t)}x\right)(t) = \frac{B(\alpha(t))}{1-\alpha(t)}\int_a^b \frac{d}{dt}(x(\tau))E_{\alpha(t)}\left[-\frac{\alpha(t)}{1-\alpha(t)}(t-\tau)^{\alpha(t)}\right]d\tau, \tag{3.16}$$

donde,

$$B(\alpha(t)) = 1 - \alpha(t) + \frac{\alpha(t)}{\Gamma(\alpha(t))}. \tag{3.17}$$

La definición de derivada fraccionaria de Atangana-Baleanu en el sentido de Liouville-Caputo se caracteriza por tener por kernel una función de Mittag-Leffler, esta función permite para ciertos valores de α recuperar comportamientos presentados tanto por el kernel de potencia de la definición de Liouville-Caputo como del kernel exponencial de la definición de Caputo-Fabrizio, volviéndose entonces estas definiciones casos particulares de la definición de Atangana-Baleanu.

Algunas características importantes que comparten todas estas definiciones se listan a continuación:

- No satisfacen la fórmula conocida para la derivación del producto de dos funciones.

$${}_a\mathcal{D}_b^{\alpha(t)}(fg) \neq f\,{}_a\mathcal{D}_b^{\alpha(t)}(g) + g\,{}_a\mathcal{D}_b^{\alpha(t)}(f).$$

- No satisfacen la fórmula conocida para la derivación del cociente de dos funciones.

$${}_a\mathcal{D}_b^{\alpha(t)}\left(\frac{f}{g}\right) \neq \frac{g\,{}_a\mathcal{D}_b^{\alpha(t)}(f) - f\,{}_a\mathcal{D}_b^{\alpha(t)}(g)}{g^2}.$$

- No se cumple la regla de la cadena.

$${}_a\mathcal{D}_b^{\alpha(t)}(f\circ g) \neq \frac{g\,{}_a\mathcal{D}_b^{\alpha(t)}(f) - f\,{}_a\mathcal{D}_b^{\alpha(t)}(g)}{g^2}.$$

3.2. Cálculo Conformable

Motivado por crear una definición de cálculo fraccionario mas sencilla de resolver tanto de manera analítica como numérica, en 2013 Khalil [42] propuso su propia definición de derivada.

Definición 6. Dada una función $x : [0, \infty) \to \mathbb{R}$. Entonces la derivada conformable de Khalil de orden $\beta(t)$ se define con la ecuación (3.18)

$$\left({}^{K}\mathcal{D}^{\beta(t)}x\right)(t) = \lim_{\epsilon \to 0} \frac{x\left(t + \epsilon t^{1-\beta(t)}\right) - x(t)}{\epsilon}. \tag{3.18}$$

Es de notar que a diferencia de las definiciones fraccionarias, el operador no posee subíndices debido a la ausencia de una integral en la definición. Como se observa en la definición, la derivada conformable de Khalil no posee un kernel asociado, por lo tanto no puede describir comportamientos con memoria, sin embargo puede ser utilizada para representar procesos fractales. La derivada conformable de Khalil satisface además las siguientes propiedades:

- ${}^{K}\mathcal{D}^{\beta(t)}(af + bg) = a\,{}^{K}\mathcal{D}^{\beta(t)}(f) + b\,{}^{K}\mathcal{D}^{\beta(t)}(g)$. $a, b \in \mathbb{R}$.
- ${}^{K}\mathcal{D}^{\beta(t)}(t^p) = pt^{p-\beta(t)}$ para toda $p \in \mathbb{R}$.
- ${}^{K}\mathcal{D}^{\beta(t)}(fg) = f\,{}^{K}\mathcal{D}^{\beta(t)}(g) + g\,{}^{K}\mathcal{D}^{\beta(t)}(f)$.
- ${}^{K}\mathcal{D}^{\beta(t)}\left(\frac{f}{g}\right) = \frac{g\,{}^{K}\mathcal{D}^{\beta(t)}(f) - f\,{}^{K}\mathcal{D}^{\beta(t)}(g)}{g^2}$.

Ademas de esto, si la función x es diferenciable, entonces es posible utilizar la definición de cálculo conformable como un operador que depende del tiempo. Partiendo de la definición de derivada conformable mostrada en (3.18) se define que $h = \epsilon t^{1-\beta(t)}$ como se muestra en la ecuación (3.19)

$${}^{K}\mathcal{D}^{\beta(t)}(x) = \lim_{\epsilon \to 0} \frac{x(t+h) - x(t)}{ht^{\beta(t)-1}}, \tag{3.19}$$

se separa entonces el término de tiempo que se encuentra en el limite como se muestra en la ecuación (3.20)

$${}^{K}\mathcal{D}^{\beta(t)}(x) = t^{\beta(t)-1} \lim_{\epsilon \to 0} \frac{x(t+h) - x(t)}{h}, \tag{3.20}$$

obteniendose entonces la definición de derivada de orden entero, sustituyendola entonces se consigue la ecuación (3.21)

$${}^{K}\mathcal{D}^{\beta(t)}(x) = t^{\beta(t)-1} \frac{dx}{dt}. \tag{3.21}$$

Como se muestra, la derivada conformable de Khalil es una buena alternativa para representar comportamientos fractales, debido a su facilidad de cálculo y de manejo analítico, sin embargo no permite describir comportamientos de memoria como las definiciones fraccionarias.

3.3. Cálculo Fraccionario Conformable

En 2017, Fahd Jarad [43] propuso nuevas definiciones de derivadas de orden no entero, aplicando un proceso similar al cual se obtuvieron las definiciones de cálculo fraccionario mediante la iteración de la derivada ordinaria; siendo la principal diferencia que aplico este proceso a la definición de integral conformable de Khalil, obteniendo así una nueva expresión de cálculo.

Partiendo de la definición de integral conformable mostrada en la ecuación (3.22)

$$ {}^{K}_{a}\mathcal{I}^{\beta(t)}x(t) = \int_a^t \frac{x(\tau)}{(\tau-a)^{1-\beta(t)}}d\tau, \tag{3.22} $$

iterando la integral n veces y cambiando el orden de las integrales se obtiene la ecuación (3.23)

$$ {}^{K}_{a}\mathcal{I}^{n,\beta(t)}x(t) = \int_a^t \frac{d\tau_1}{(\tau_1-a)^{1-\beta(t)}}\int_a^{\tau_1}\frac{d\tau_2}{(\tau_2-a)^{1-\beta(t)}}\cdots\int_a^{\tau_{n-1}}\frac{x(\tau_n)d\tau_n}{(\tau_n-a)^{1-\beta(t)}}, \tag{3.23} $$

remplazando n por $\alpha \in \mathbb{C}, Re(\alpha) > 0$ se obtiene la definición de integral fraccionaria conformable mostrada en la ecuación (3.24)

$$ {}^{CFK}_{a}\mathcal{I}^{\alpha(t),\beta(t)}x(t) = \frac{1}{\Gamma(\alpha)}\int_a^t \left(\frac{(t-a)^{\beta}-(\tau-a)^{\beta}}{\beta}\right)^{\alpha-1}\frac{x(\tau)}{(\tau-a)^{1-\beta}}d\tau. \tag{3.24} $$

en donde $\alpha(t)$ se refiere al orden de laparte fraccionaria y $\beta(t)$ al orden de la parte conformable. Apartir de esta definición de integral es posible proponer distintas definiciones de derivadas fraccionarias conformables, para este trabajo se consideró la definición de derivada conformable fraccionaria en el sentido de Louville-Caputo.

Definición 7. $Re(\alpha) \geq 0, n = [Re(\alpha)] + 1, x \in C^n_{\alpha,a}([a,b]), \left(x \in C^n_{\beta(t),b}([a,b])\right)$. La derivada conformable fraccionaria en el sentido de Liouville-Caputo está dada por

$$ {}^{CFK}_{a}\mathcal{D}^{\alpha(t),\beta(t)}_{b}x(t) = \frac{1}{\Gamma(n-\alpha(t))}\int_a^b \left(\frac{(b-a)^{\beta(t)}-(\tau-a)^{\beta(t)}}{\beta(t)}\right)^{n-\alpha(t)-1}\frac{{}^{\alpha}_{a}\mathcal{D}^{\beta(t)}_{\tau}x(\tau)}{(\tau-a)^{1-\beta(t)}}d\tau. \tag{3.25} $$

Es de notar que, para para diferentes valores tanto como de $\alpha(t)$ como de $\beta(t)$ existen cuatro casos posibles:

- Si $\alpha(t) = 1$ y $\beta(t) = 1$ se recupera la definición de derivada clásica.
- Si $\alpha(t) \neq 1$ y $\beta(t) = 1$ se obtiene entonces la definición de derivada fraccionaria de Caputo presentada en la ecuación (3.13).
- Si $\alpha(t) = 1$ y $\beta(t) \neq 1$ se presenta la derivada conformable en el sentido de Khalil presentada en la ecuación (3.18).
- Si $\alpha(t) \neq 1$ y $\beta(t) \neq 1$ se obtiene la definición de cálculo fraccionario conformable.

Al ser una definición que presenta naturalmente dos ordenes de derivación, uno para la parte fraccionaria ($\alpha(t)$) y otro para la parte conformable ($\beta(t)$) permite representar dinámicas de sistemas mas complejos, por ejemplo en problemas de control óptimo.

Capítulo 4

Criptología

Con la aparición de la informática y el uso masivo de las telecomunicaciones, la facilidad de acceso a información tanto personal como de uso general trae consigo diversas problemáticas; entre ellas la protección de datos y las comunicaciones seguras. La criptología es la disciplina dedicada al estudio de técnicas utilizadas para mantener segura la información, se encuentra dividida en cuatro partes:

- La criptografía se encarga del estudio de técnicas, procesos o algoritmos utilizados para la protección de datos.
- El criptoanálisis tiene un objetivo opuesto al de la criptografía, estudia los sistemas criptográficos con la finalidad de encontrar debilidades y romper su seguridad.
- La Esteganografía consiste en ocultar mensajes de tal manera que puedan ser comunicados por un canal inseguro sin siquiera ser percibidos.
- El Estegoanálisis se ocupa de encontrar información oculta mediante esteganografía.

Los algoritmos de protección de información comúnmente utilizan tanto una parte criptográfica como una parte esteganográfica, sin embargo en este trabajo se realizó un enfoque a la parte criptográfica. El cifrado en criptografía se refiere al proceso mediante el cual cierta información de interés, como imágenes o texto, es transformada utilizando un algoritmo de codificación de tal manera que impide a personas no autorizadas acceder a la información original. Para la recuperación o desencriptación de la información es necesario el uso de un conjunto de datos conocidos como llave o clave. Es importante aclarar que si bien la Real Academia Española no define la palabra encriptación o desencriptación son términos adoptados para referirse al cifrado de información. Los esquemas de encriptación se dividen en dos tipos de acuerdo al manejo de la clave [44].

- Clave simétrica o privada.
  Las claves utilizadas tanto para transformar la información como para su recuperación son las mismas. Ambas partes deben tener acceso a la misma llave para lograr la comunicación correcta de los datos originales. Se requiere ademas el uso de un canal de comunicación seguro para el intercambio de la llave secreta.
- Clave asimétrica o pública.
  El esquema utiliza dos llaves. La clave de encriptación es compartida o publicada de tal manera

que cualquier persona puede encriptar mensajes, sin embargo solo quien recibe los datos tiene acceso a la clave que le permite recuperar los datos originales.

El tamaño de la llave es tambien una característica importante de un sistema criptográfico que desempeña un papel fundamental en la seguridad del mismo. Entre mayor sea el tamaño de la llave de cifrado, mas robustez tendra el sistema contra ataques de fuerza bruta, por lo tanto un espacio de clave grande es una condición necesaria, sin embargo no suficiente, para garantizar la seguridad del sistema.

Tamaño de la llave	Tiempo de computo
56 - 64 bits	Horas o dias
112 - 128 bits	Décadas en ausencia de computadoras cuánticas
256 bits	Décadas aun con computadoras cuánticas

La codificación generalmente utiliza una llave pseudo aleatoria generada por un algoritmo. El esquema básico de comunicación utilizando la encriptación de datos se presenta en la Figura 4.1.

Una opción para la generación de números pseudoaleatorios es el uso de sistemas caóticos, los cuales debido tanto a su alta sensibilidad a condiciones iniciales y parámetros así como el hecho de que para ciertos conjuntos de datos la salida de estos sistemas tiene la misma distribución, permiten generar claves seguras. Se han desarrollado también algoritmos de codificación y decodificación que utilizan la sincronización de sistemas caóticos para la transformación de la información original.

4.1. Índices de desempeño

Existen diversos índices de desempeño para evaluar la eficiencia de distintos sistemas criptográficos. Debido a que en esta tesis se hace enfoque en métodos de encriptación de imágenes en escala de grises se muestran a continuación diversos índices aplicables. El promedio unificado de intensidad de cambio UACI por sus siglas en inglés, el cual esta dado por la ecuación (4.1)

$$UACI = \frac{100}{M \times N}\left(\sum_{i,j}\frac{|C_1(i,j) - C_2(i,j)|}{2^n - 1}\right), \tag{4.1}$$

donde M y N corresponden a las dimensiones de la imagen, $2^n - 1$ es el valor numérico mas alto que puede tomar un píxel y tanto C_1 como C_2 son imágenes cifradas utilizando el algoritmo. C_1 corresponde al cifrado de una imagen mientras que C_2 corresponde al cifrado de la misma imagen cambiando únicamente un pixel o un valor en las condiciónes iniciales o parámetros del sistema.
La razón de cambio de píxeles o NPCR por sus siglas en inglés se describe con la ecuación (4.2)

$$NPCR = \frac{100}{M \times N}\left(\sum_{i,j} G(i,j)\right), \tag{4.2}$$

donde,

$$G(i,j) = \begin{cases} 1, & C_1(i,j) = C_2(i,j) \\ 0, & C_1(i,j) \neq C_2(i,j) \end{cases}, \tag{4.3}$$

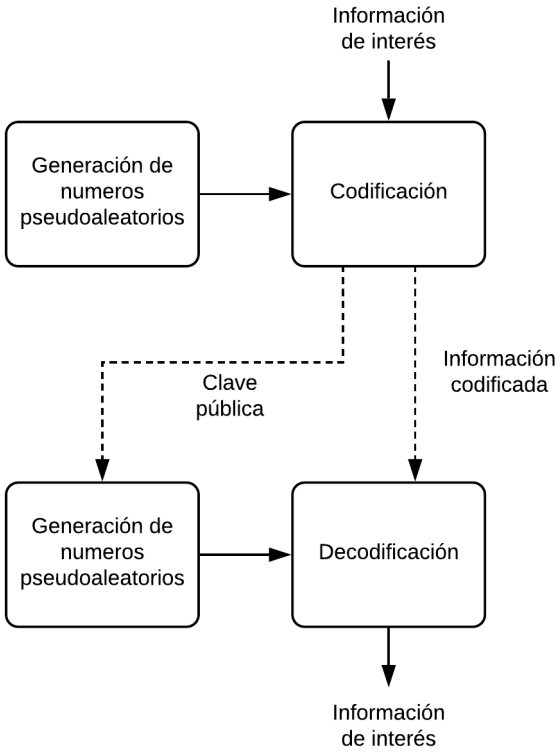


Fig. 4.1. Diagrama general de un sistema de encriptación. El uso de sistemas caóticos se involucra en el algoritmo de generación de números pseudoaleatorios, sin embargo también puede aparecer en la codificación.

entre mas alto sea este porcentaje, menos probable es que al cambiar un parámetro o un píxel de la imagen de interés el algoritmo de como resultado el mismo valor numérico en el mismo píxel de la imágen.
Otro indicador elegido es la entropía de la imagen mostrada en la ecuación (4.4), este indicador es usado debido a que indica el nivel de aleatoriedad en los píxeles de las imágenes cifradas, la siguiente ecuación representa la manera de obtener este indicador

$$H(s) = \sum_{i=1}^{N} P(s_i) log_2 \frac{1}{P(s_i)}, \tag{4.4}$$

donde N es la cantidad de valores posibles, en el caso de imágenes en escala de grises cada píxel puede tomar 256 valores posibles y $P(s_i)$ se refiere a la probabilidad de que el valor s_i aparezca en la imagen. En el caso particular de imágenes en escala de grises, si la distribución de valores fuera ideal, la probabilidad de ocurrencia de cada sombra de gris sería $\frac{1}{255}$ a lo cual corresponde un valor de entropía de 8.
El índice de correlación, descrito por la ecuación (4.5), es calculado entre la imagen original y la imagen

después de ser encriptada para determinar que ambas imágenes no guardan relación entre ellas.

$$r = \frac{\sum_m \sum_n \left(P_{mn} - \bar{P}\right)\left(C_{mn} - \bar{C}\right)}{\sqrt{\sum_m \sum_n \left(P_{mn} - \bar{P}\right)^2 \sum_m \sum_n \left(C_{mn} - \bar{C}\right)^2}}, \tag{4.5}$$

donde P corresponde a la imagen original, $\bar{P}$ es el valor promedio de la imagen original. C es la imagen cifrada y $\bar{C}$ es el valor de intensidad medio de la imagen cifrada.

Capítulo 5

Resultados

En este capítulo se presentan los resultados obtenidos al tomar tres algoritmos de encriptación encontrados en la literatura que involucran el uso de sistemas caóticos y generalizarlos utilizando definciones de derivadas fraccionarias de tal manera que aumente su seguridad.

5.1. Caso 1

Se replicó el algoritmo de encriptación propuesto en el trabajo de Rodríguez [45], el cual fue utilizado para la encriptación de imágenes en escala de grises de tamaño $M \times N$ píxeles. Este algoritmo utiliza un sistema de Lorenz para la generación de la llave de encriptación y considera la sincronización de Pecora-Carroll para recuperar la información original, en este trabajo se añadió el uso del cálculo fraccionario en la simulación del sistema de Lorenz para así obtener dinámicas diferentes. Los pasos del algoritmo se muestran a continuación:

1. Se utiliza un atractor de Lorenz dividido en subsistemas maestro y esclavo, utilizando y como variable sincronizante.

2. Ambos sistemas se inicializan con condiciones iniciales distintas.

3. Se generan los primeros 700 valores del atractor maestro y se envían como llave al atractor esclavo.

4. Se generan dos secesiones $x_j, j = 1, \ldots, M$ y $z_i, i = 1 \ldots N$ tomando únicamente los últimos tres dígitos de cada valor.

5. Se relaciona cada valor de x_j con cada columna j de la matriz, el cual indicará el número de posiciones que se desplaza cada píxel verticalmente. Si $x_j < N/2$ el desplazamiento se hará hacia abajo. Cada valor de z_i indica las posiciones que los píxeles se desplazarán de manera horizontal. Si $z_i < M/2$ el desplazamiento se hará hacia la derecha. Este paso es repetido 4 veces obteniendo la matriz P.

6. Se genera una matriz A de dimensiones $M \times N$ utilizando las secesiones del paso 4, la cual es sumada a la matriz a la matriz obtenida en el paso 5.

7. Se aplican las siguientes ecuaciones

$$D_1(k,i) = \left(P(k,i) + A\left(ceil\left(\frac{M}{2}\right) + 1 - k, (N+1) - i\right)\right) mod 256, \tag{5.1}$$

$$D_2(k,i) = \left(D_1(k,i) + A\left((M+1) - k\right), i\right)) mod 256, \tag{5.2}$$

$$D_3(l,i) = D_2(l,i) + P\left((M+1) - l, (N+1) - i\right) mod 256, \tag{5.3}$$

donde $i = 1, 2, \ldots, N$, $l = 1, 2, \ldots, floor\left(\frac{M}{2}\right)$ y $k = 1, 2, \ldots, ceil\left(\frac{M}{2}\right)$.

8. Por ultimo se concatenan las matrices D_2 y D_3 obteniendo

$$C(j,i) = \left[D_2(k,i), D_3(l,i)\right]. \tag{5.4}$$

La imagen encriptada está representada por la matriz C mientras que la llave utilizada son los primeros 700 datos del estado y del sistema maestro. Para recuperar la imagen original se utiliza el estado y para sincronizar el sistema esclavo, después simplemente se repiten los pasos 5, 6 y 7 en orden inverso. El esquema resumido del procedimiento se presenta en la Figura 5.1.

Para el proceso de desencriptación se recibe la imagen cifrada C y los primeros 700 datos del estado y, los parámetros utilizados para el atractor de Lorenz se encuentran previamente acordados por el emisor y el receptor. Con esta información se realiza un proceso inverso para recuperar la imagen original usando los siguientes pasos:

1. Se toma el estado y enviado y se utiliza para simular un sistema esclavo utilizando el esquema de Peccora-Carroll, posteriormente se continua la simulación durante un numero de muestras igual a la dimensión mas grande de la imagen cifrada.

2. Se obtiene la matriz A a partir de los estados x y z del sistema esclavo de manera análoga a su obtención al proceso de encriptación en el paso 6. La matriz obtenida es separada en dos submatrices de la siguiente manera:

$$A_1(k,i) = A\left(ceil\left(\frac{M}{2}\right) + 1 - k, N + 1 - i\right), \tag{5.5}$$

$$A_2(k,i) = A\left(M + 1 - k, i\right), \tag{5.6}$$

donde $i = 1, 2, \cdots, N$ y $k = 1, 2, \cdots, ceil\left(\frac{M}{2}\right)$.

3. Se aplican las siguientes ecuaciones

$$D_2(k,i) = C(k,i), \tag{5.7}$$

$$D_3(k,i) = C(m,i), \tag{5.8}$$

$$D_1(k,i) = \left(D_2(k,i) - mod(A_2(k,i))\right) mod 256, \tag{5.9}$$

donde $i = 1, 2, \cdots, N$, $m = ceil\left(\frac{M}{2}\right) + 1, ceil\left(\frac{M}{2}\right) + 2, \cdots, M$ y $k = 1, 2, \cdots, N$.

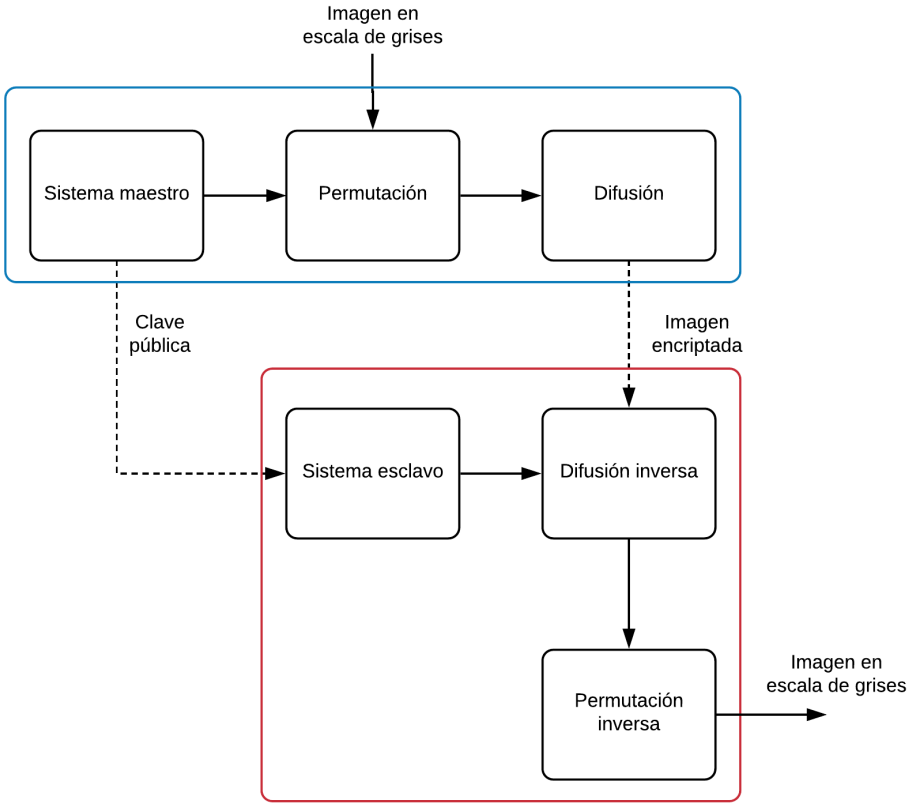


Fig. 5.1. Resumen esquemático del proceso de encriptación utilizado, el recuadro azul representa las partes que utiliza el remitente y el recuadro rojo las del receptor.

4. Para obtener entonces la imagen permutada se tiene que

$$P_1 = \left(D_1\left(k,i\right) - \left(A_1\left(k,i\right)\right) mod256\right) mod256, \tag{5.10}$$

$$P_2 = \left(D_3\left(k,i\right) - \left(D_2\left(k,i\right)\right) mod256\right) mod256, \tag{5.11}$$

$$P_e\left(j,i\right) = \left[P_1\left(k,i\right), P_2\left(k,i\right)\right]. \tag{5.12}$$

5. Por ultimo se repiten los pasos 4 y 5 del proceso de encriptación, invirtiendo las direcciones de desplazamiento de los píxeles.

Los ordenes de integración para el sistema se definen previamente analizando el diagrama de bifurcación correspondiente mostrado en la Figura 5.2, este diagrama presenta el comportamiento de el estado x de un sistema de Lorenz dado por la ecuación (2.2) con parámetros $A = 10, B = 38$ y $C = \frac{8}{3}$ utilizando la definición de derivada de Liouville-Caputo. Como se observa en la figura, para ordenes $\alpha < 0.937$ el sistema no presenta comportamiento caótico, por lo tanto se debe escoger un orden mayor para el

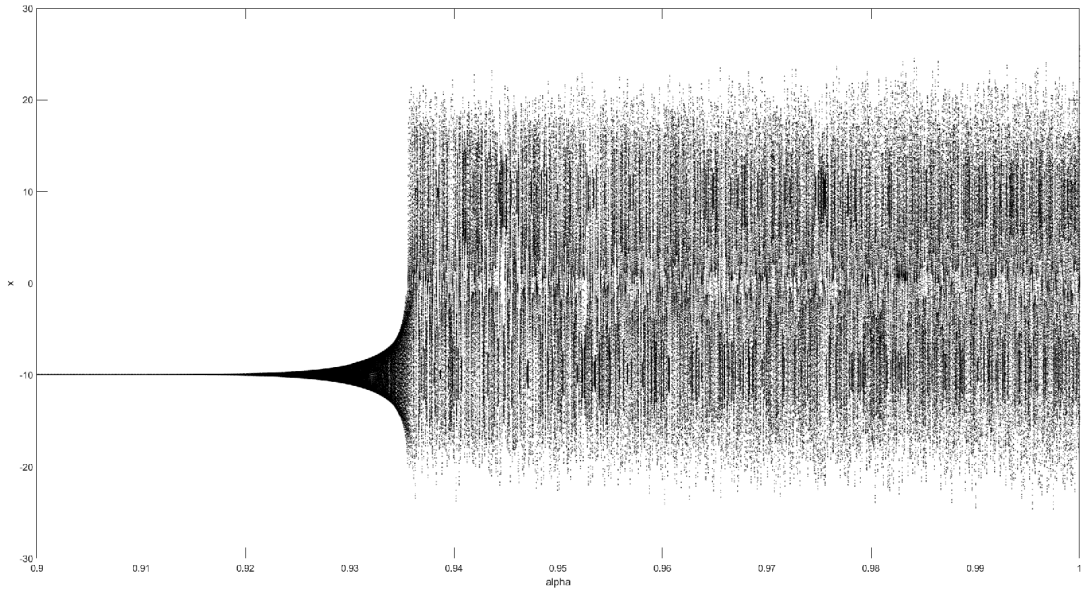
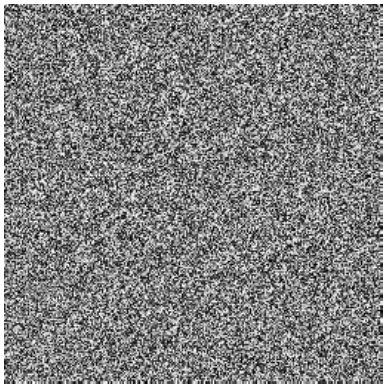


Fig. 5.2. Diagrama de bifurcación del estado x del sistema de Lorenz respecto a un orden de integración α.

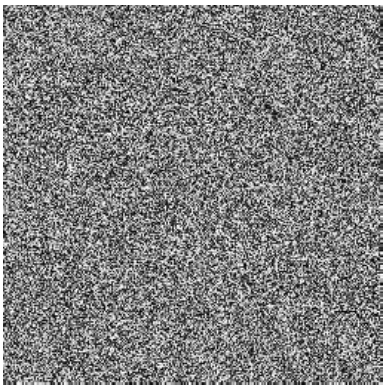
algoritmo de encriptación.

A continuación se muestran los resultados obtenidos al encriptar cuatro imágenes previamente escogidas con el método de encriptación propuesto. Para cada caso se muestra la imagen original, la imagen encriptada utilizando el método con un orden de integración $\alpha = 1$, posteriormente se muestra cada imagen encriptada utilizando la metodología propuesta con un orden de integración constante arbitrario. Por ultimo se muestra la imagen recuperada para ambos casos, cabe destacar que en todos los casos se comprobó que se recuperara exactamente la imagen original calculando el error entre ella y la imagen recuperada.

(a) Imagen original.



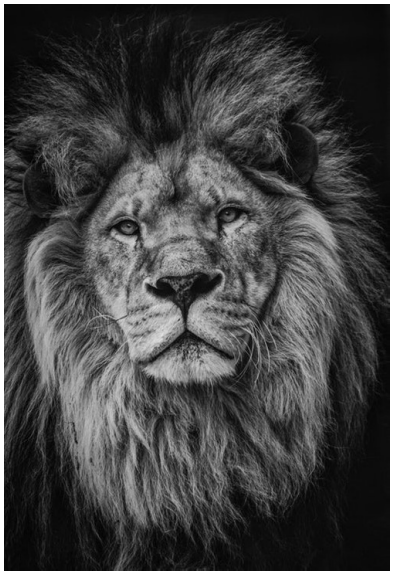
(b) Imagen encriptada utilizando la metodología de orden entero.



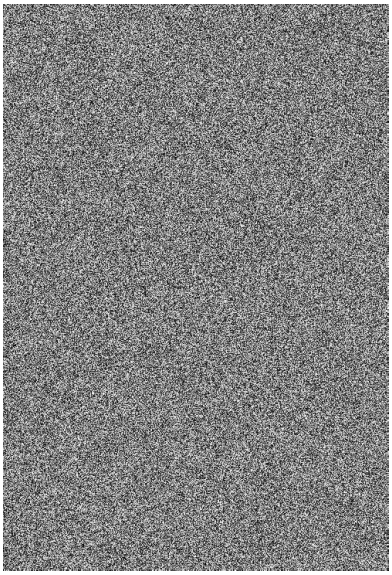
(c) Imagen encriptada utilizando la metodología de orden fraccionario $\alpha = 0.99999999$.

(d) Imagen recuperada.

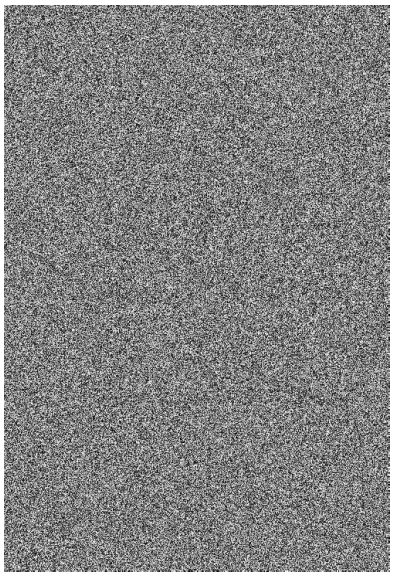
Fig. 5.3. Imagen de árboles encriptada utilizando la metodología descrita en el caso 1.



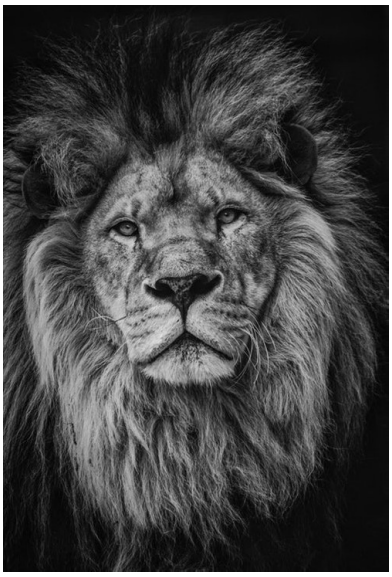
(a) Imagen original.



(b) Imagen encriptada utilizando la metodología de orden entero.



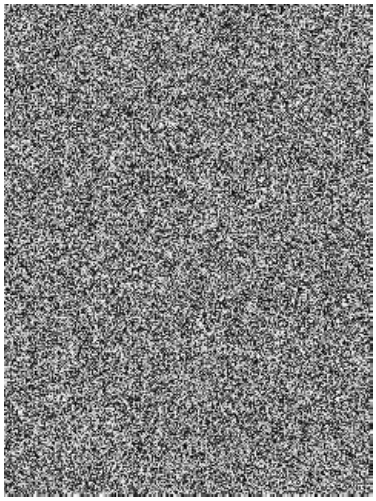
(c) Imagen encriptada utilizando la metodología propuesta con orden $\alpha = 0.9999$



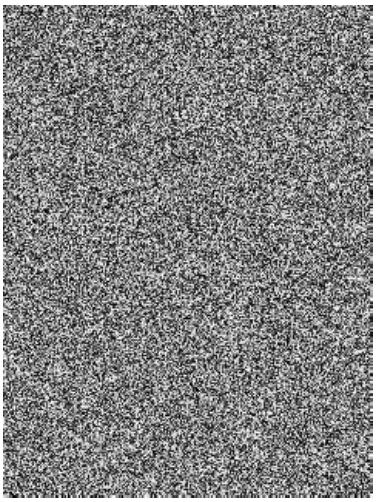
(d) Imagen recuperada.

Fig. 5.4. Imagen de león encriptada utilizando la metodología descrita en el caso 1.

(a) Imagen original.



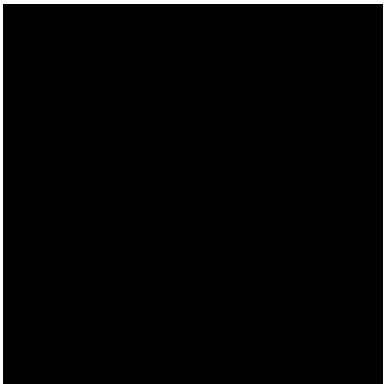
(b) Imagen encriptada utilizando la metodología de orden entero.



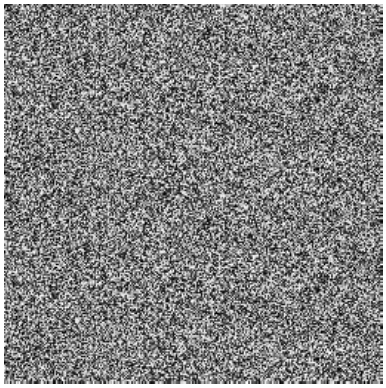
(c) Imagen encriptada utilizando un orden $\alpha = 0.999$.

(d) Imagen recuperada.

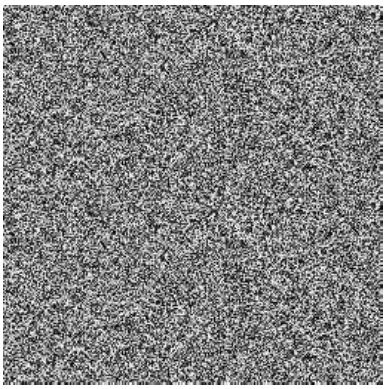
Fig. 5.5. Imagen de la torre Eiffel encriptada utilizando la metodología descrita en el caso 1.



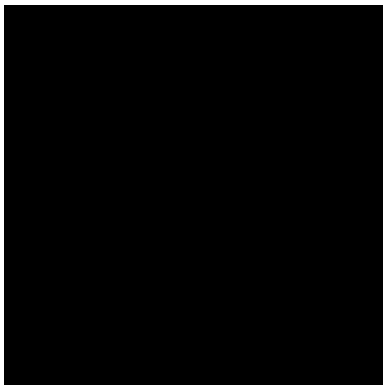
(a) Imagen original.



(b) Imagen encriptada utilizando la metodología de orden entero.



(c) Imagen encriptada utilizando la metodología propuesta y un $\alpha = 0.99999999$.



(d) Imagen recuperada.

Fig. 5.6. Imagen completamente negra encriptada utilizando la metodología descrita en el caso 1.

Se calcularon los índices de desempeño con los ordenes mostrados, los resultados se muestran en la Tabla 5.1. Los índices obtenidos son comparables con los presentados en la referencia original y se mantienen incluso para valores de $\alpha = 0.99999999$, lo que quiere decir que el sistema de Lorenz es también relativamente sensible al orden de derivación α. Por tanto, se tiene entonces que si se toman valores $0.937 < \alpha < 1$ en pasos de 1×10^{-8}, existen 6.3×10^{6} valores posibles para α lo cual incrementa el espacio original de la llave en 2^{23}.

Se realizó también una prueba con la finalidad de observar el desempeño del algoritmo al ruido tanto en la imagen cifrada como en la llave de encriptación. Primero se realizó una prueba aplicando distintos tipos de ruido a la imagen cifrada. Para este ejercicio se tomo la imagen de la torre Eiffel y se aplicaron

Índices de evaluación.				
Imagen	**UACI**	**NPCR**	**Entropía**	**Coeficiente de Correlación**
Árboles	33.4589 %	99.6215 %	7.9894	-0.0056581
Torre Eiffel	33.4356 %	99.6471 %	7.9899	-0.0042048
León	33.4393 %	99.5980 %	7.9917	-0.0001778
Negro	33.5209 %	99.5574 %	7.9090	-

Tabla 5.1. Índices de evaluación del algoritmo de encriptación con sincronización de Peccora-Carroll.

dos pruebas distintas, una con ruido gaussiano y otra con ruido de tipo sal y pimienta. Los resultados de estas pruebas se muestran a continuación. En la imagen 5.7 se muestra la imagen recuperada al contaminar la imagen cifrada con ruido Gaussiano de varianza 0.01, la imagen recuperada guarda un índice de correlación $r = 0.6496127$. En la imagen 5.8 se muestra la imagen recuperada al contaminar la imagen cifrada con ruido sal y pimienta de densidad 0.05. En la segunda prueba se obtuvo un índice de correlación de $r = 0.9162055$. En ambos casos se utilizó un orden de integración de $\alpha = 0.99999999$. En ambos casos es posible reconocer la imagen recuperada al menos a grandes rasgos.

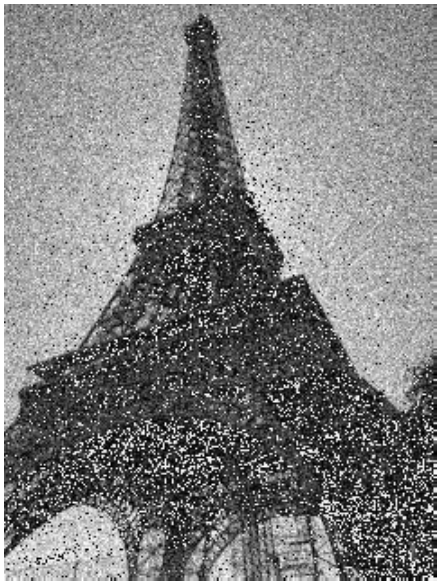


Fig. 5.7. Imagen recuperada al contaminar la imagen cifrada con ruido Gaussiano.

Se realizó también una prueba de ruido en la variable de estado y, compartida entre ambos sistemas de Lorenz para su sincronización. Se aplico a la señal ruido blanco Gaussiano aditivo de distintas intensidades. El orden de integración se mantuvo constante entre las pruebas ($\alpha = 0.99999$). En la Figura 5.9 se muestra una sección de las llaves utilizadas para la prueba.

Fig. 5.8. Imagen recuperada al contaminar la imagen cifrada con ruido sal y pimienta.

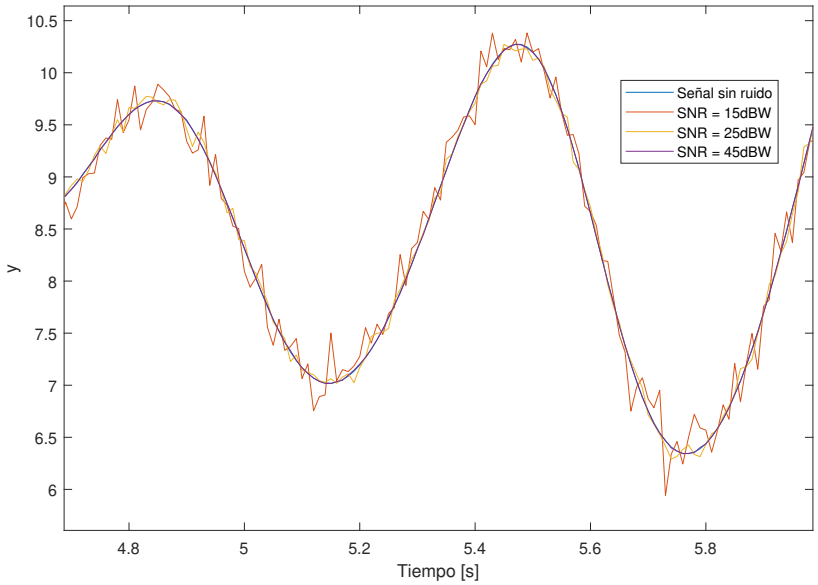
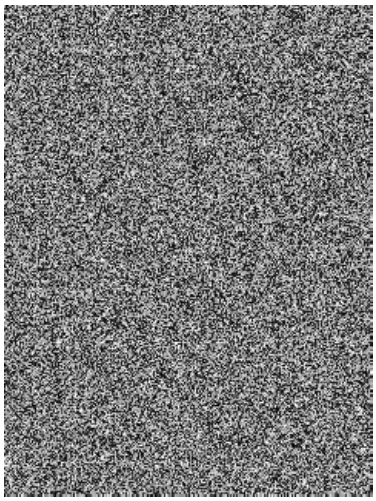
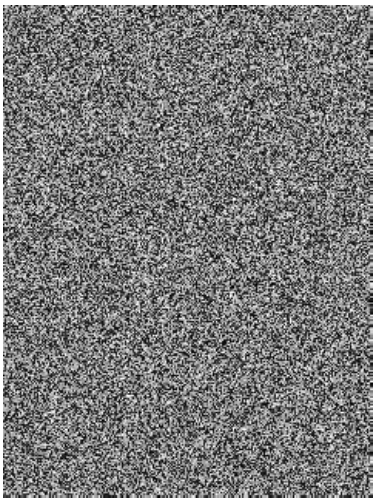


Fig. 5.9. Sección de las llaves utilizadas para la prueba.

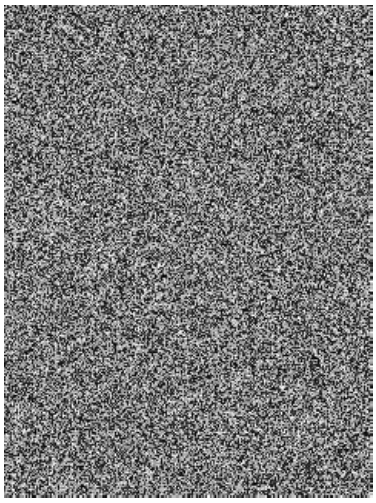
(a) Imagen recuperada sin ruido en la llave.



(b) Imagen recuperada con ruido $SNR = 15dBW$.



(c) Imagen recuperada con ruido $SNR = 25dBW$.



(d) Imagen recuperada con ruido $SNR = 45dBW$.

Fig. 5.10. Intentos de recuperación de imagen original con ruido aditivo Gaussiano en la llave de encriptación

5.2. Caso 2

En el trabajo presentado por Gao [46], se utiliza un algoritmo de encriptación basado en el mapa de Mandelbrot-Julia descrito en la ecuación (5.13)

$$f(Z) = a_n Z^{n+b_n} + a_{n-1} Z^{n-1+b_n} + \cdots + a_1 Z^{1+b_1} a_1 Z^{1+b_1} + C, \tag{5.13}$$

donde $n = 1, 2, \cdots, 20$, $a_n = x_n + iy_n$ y Z es una variable compleja. Esta forma fue escogida debido a la cantidad de parámetros libres que es posible utilizar. En este trabajo se propone utilizar derivadas fraccionarias variantes en el tiempo en lugar de una representación que aumente el número de parámetros.

Además, se decidió sustituir arbitrariamente el mapa de Mandelbrot-Julia por el mapa del ave mítica [47] descrito por la ecuación (5.14)

$$\begin{aligned} x_{n+1} &= y_n + a(1 - 0.05y_n^2)y_n + \mu x_n + \frac{2(1-\mu)x_n^2}{1+x_n^2}, \\ y_{n+1} &= -x_n + \mu x_{n+1} + \frac{2(1-\mu)x_{n+1}^2}{1+x_{n+1}^2}, \end{aligned} \tag{5.14}$$

donde μ y a son constantes.
Aplicando el método de Euler se tiene el siguiente sistema de ecacuiones

$$\begin{aligned} \frac{x_{n+1} - x_n}{h} &= \frac{1}{h}\left(y_n + a(1 - 0.05y_n^2)y_n + \mu x_n + \frac{2(1-\mu)x_n^2}{1+x_n^2} - x_n \right), \\ \frac{y_{n+1} - y_n}{h} &= \frac{1}{h}\left(-x_n + \mu x_{n+1} + \frac{2(1-\mu)x_{n+1}^2}{1+x_{n+1}^2} - y_n \right), \end{aligned} \tag{5.15}$$

si $h \to 0$ entonces el sistema puede ser escrito como se muestra en la ecuación (5.16)

$$\begin{aligned} \dot{x}(t) &= \frac{1}{h}\left(y(t) + a(1 - 0.05y^2(t))y(t) + \mu x(t) + \frac{2(1-\mu)x^2(t)}{1+x^2(t)} - x(t) \right), \\ \dot{y}(t) &= \frac{1}{h}\left(-x(t) + \mu x(t+h) + \frac{2(1-\mu)x(t+h)^2}{1+x(t+h)^2} - y(t) \right). \end{aligned} \tag{5.16}$$

Por ultimo se generalizó el operador de derivada por el operador conformable fraccionario.

$$\begin{aligned} {}_{t_0}^{CFK}\mathcal{D}_t^{\alpha_1(t),\beta_1(t)} x(t) &= \frac{1}{h}\left(y(t) + a(1 - 0.05y^2(t))y(t) + \mu x(t) + \frac{2(1-\mu)x^2(t)}{1+x^2(t)} - x(t) \right), \\ {}_{t_0}^{CFK}\mathcal{D}_t^{\alpha_2(t),\beta_2(t)} y(t) &= \frac{1}{h}\left(-x(t) + \mu x(t+h) + \frac{2(1-\mu)x^2(t+h)}{1+x^2(t+h)} - y(t) \right). \end{aligned} \tag{5.17}$$

Como se muestra en la ecuación (5.17) los ordenes de derivación de los estados son inconmensurados, es decir, pueden tomar distintos valores entre ellos, además de que son variantes en el tiempo. En la

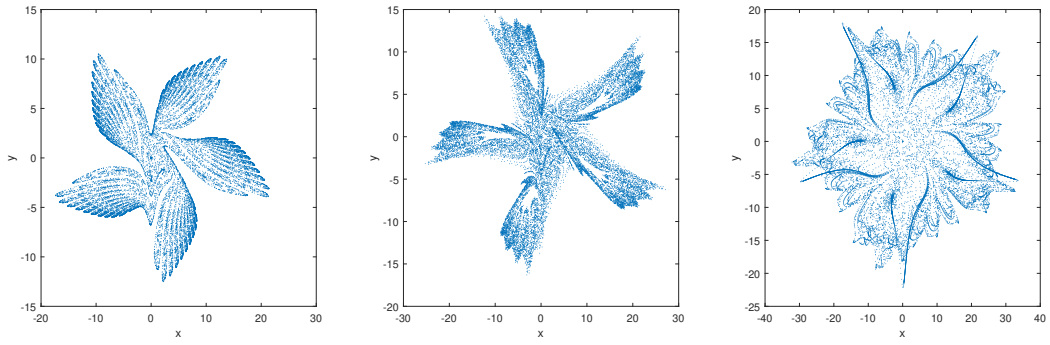


Fig. 5.11. Comportamiento del mapa del ave mítica ante distintos ordenes. $\alpha = 1$ (izquierda), $\alpha = 0.995$ (centro), y $\alpha = 0.005tanh(0.001(t - 500)) + 0.9$ (derecha).

Figura 5.11, se muestra la respuesta del sistema ante diversos órdenes, nótese que aún ante cambios relativamente pequeños de α el mapa presenta dinámicas completamente distintas lo cual es batante favorable para poder ser implementado en nuestro esquema de encriptación.

La Figura 5.12, presenta el diagrama de bifurcación del estado x respecto al orden α. Para este caso en particular existe una región de ordenes entre $0.9935 < \alpha < 0.995$, en la cual el sistema no presenta comportamiento caótico, por lo tanto ese conjunto de órdenes debe ser omitido por el algoritmo.
Los pasos utilizados para la encriptación de este algoritmo se muestran a continuación:

- Se tiene como entrada una imagen en escala de grises I de dimensiones $m \times n$ y señales de ruido ambiental N.
- Se utiliza el algoritmo SHA512 (algoritmo que transforma un conjunto de datos en un único valor de longitud fija) en la señal de audio para obtener una tira de 64 datos de 8 bits, estos datos son normalizados para obtener valores entre 0.9 y 1.
- Los valores obtenidos son utilizados como órdenes de integración para el sistema descrito en la ecuación (5.17), el estado x es utilizado de la siguiente manera:

$$S = floor\left(x \times 10^{14}\right) mod 256. \tag{5.18}$$

- Por último, la encriptación se realiza como se muestra en la ecuación (5.19), iterando esta ecuación tres veces

$$C_i = (C_{i-1} + I)\, mod 256 \oplus S. \tag{5.19}$$

Para el proceso de desencriptación se utilizan los mismos pasos, simplemente cambiando la ecuación (5.19) por la ecuación (5.20)

$$I = (C_i \oplus S - C_{i-1})\, mod 256. \tag{5.20}$$

Ejemplos de imágenes cifradas con este método se muestran a continuación. Los índices de desempeño obtenidos se muestran en la Tabla 5.2. Estos índices fueron obtenidos con dos imágenes cifradas variando el orden de integración de 1 a 0.999. Al igual que en el algoritmo anterior los índices de desempeño

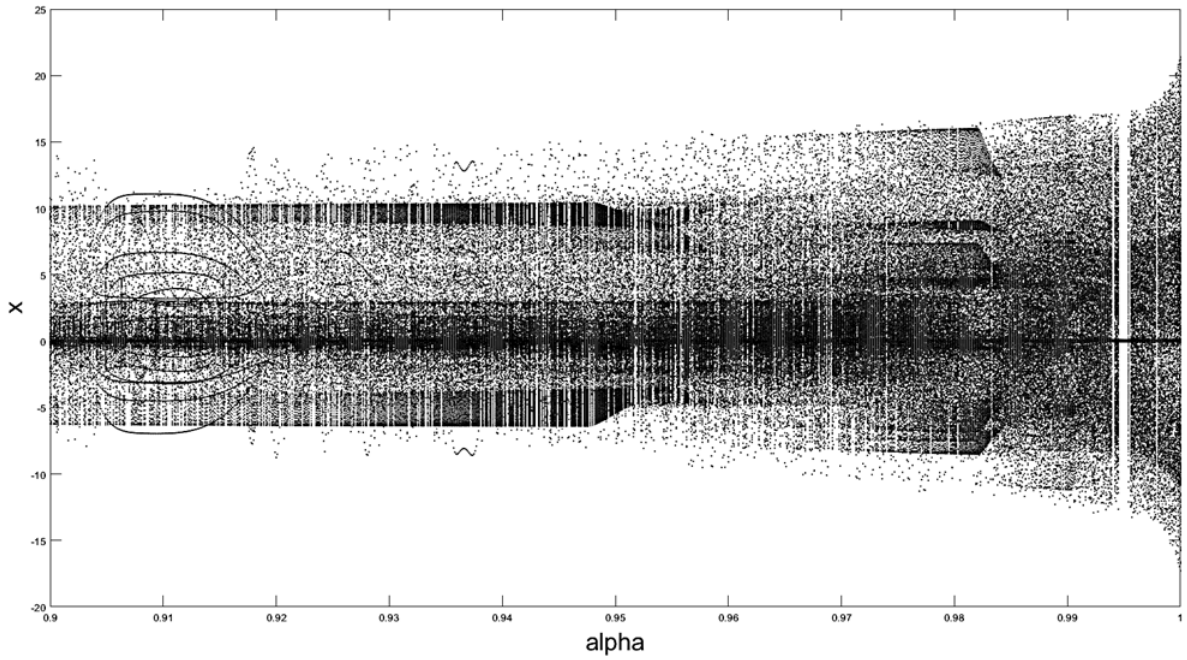


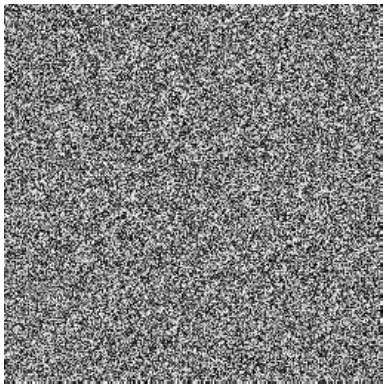
Fig. 5.12. Diagrama de bifurcación del estado x del mapa ave mítica respecto al orden de derivación α.

Índices de evaluación				
Imagen	**UACI**	**NPCR**	**Entropía**	**Coeficiente de Correlación**
Árboles	33.2556 %	99.6276 %	7.9895	0.0038121
Torre Eiffel	33.4591 %	99.6184 %	7.9893	0.0085041
León	33.4685 %	99.6106 %	7.9914	0.0023723
Negro	33.5526 %	99.6139 %	7.9892	-

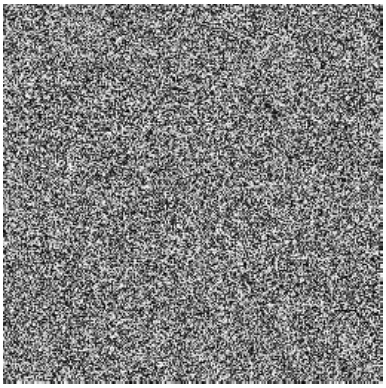
Tabla 5.2. Índices de evaluación del algoritmo de encriptación utilizando mapas caóticos de orden variable en el tiempo.

se mantienen, en este caso, utilizando el orden de integración α como llave de encriptación en vez de los parámetros del sistema como se propone originalmente en la literatura. Al ser comparables con los índices originales la variación de orden α puede ser usada como llave de encriptación para el sistema. En este caso el número posible de llaves aumenta no solo debido a la sensibilidad a la precisión del orden si no también debido a que éste es variable en el tiempo.

(a) Imagen original.



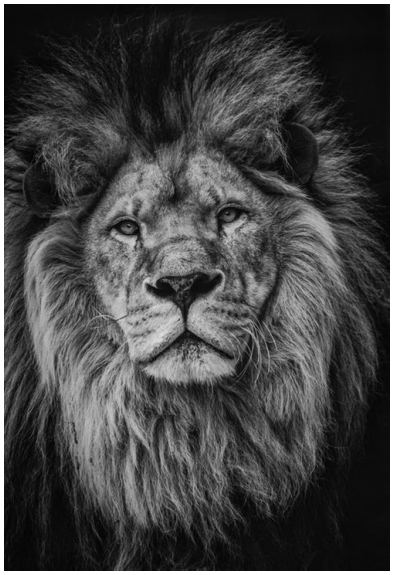
(b) Imagen encriptada con ordenes $\alpha = \beta = 1$



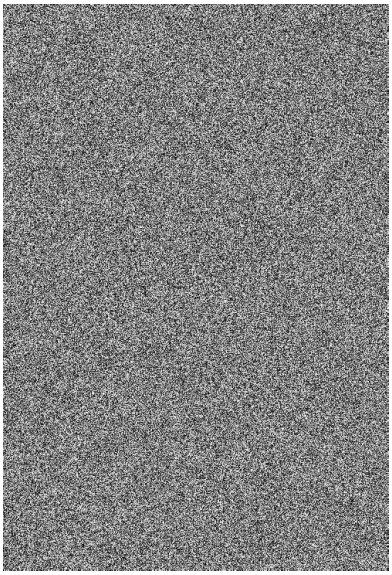
(c) Imagen encriptada con ordenes $\alpha = \beta = 0.99999999999999$.

(d) Imagen recuperada.

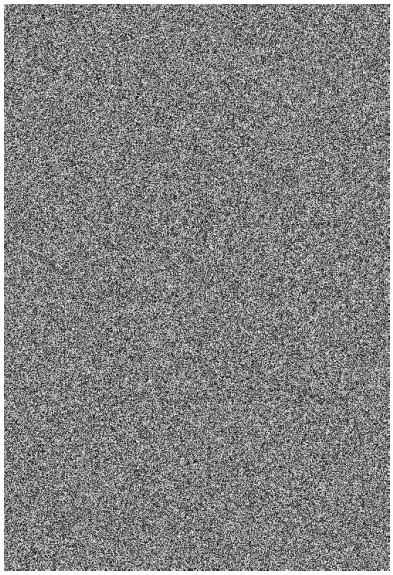
Fig. 5.13. Imagen de árboles encriptada utilizando la metodología descrita en el caso 2.



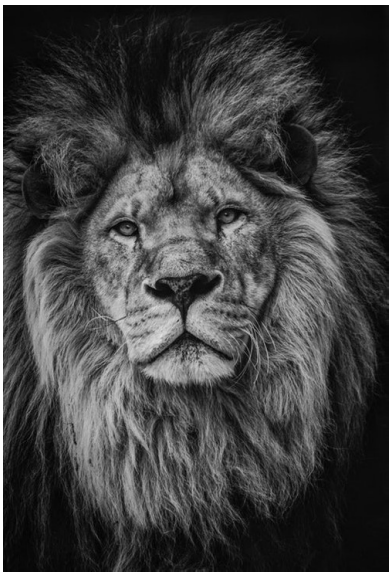
(a) Imagen original.



(b) Imagen encriptada con ordenes $\alpha = \beta = 1$



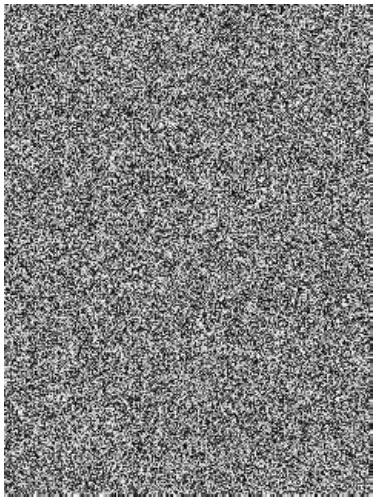
(c) Imagen encriptada con ordenes $\alpha = 1$,$\beta = 0.005sen(t) + 0.995$



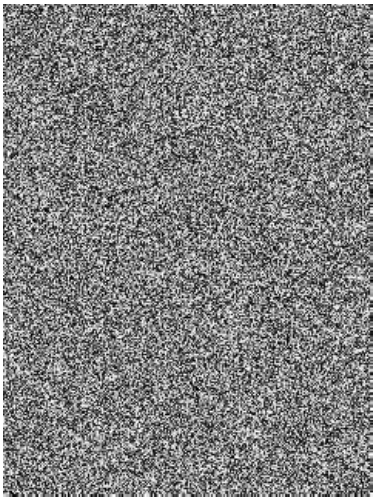
(d) Imagen recuperada.

Fig. 5.14. Imagen de león encriptada utilizando la metodología descrita en el caso 2.

(a) Imagen original.



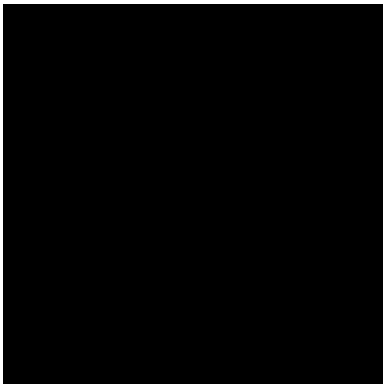
(b) Imagen encriptada con ordenes $\alpha = \beta = 1$



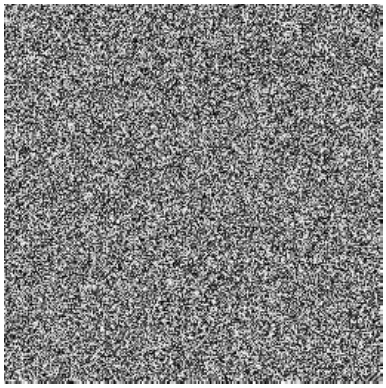
(c) Imagen encriptada con ordenes $\alpha = 0.005cos(t) + 0.995$, $\beta = 1$.

(d) Imagen recuperada.

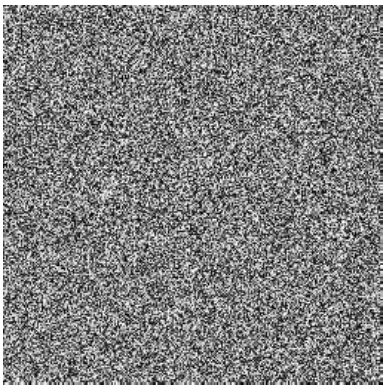
Fig. 5.15. Imagen de la torre Eiffel encriptada utilizando la metodología descrita en el caso 2.



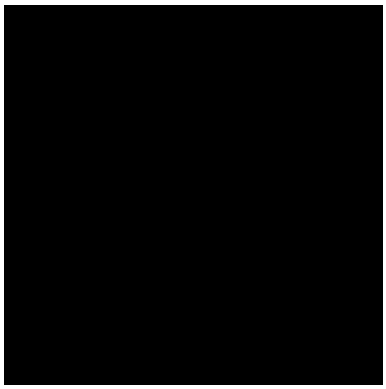
(a) Imagen original.



(b) Imagen encriptada con ordenes $\alpha = \beta = 1$



(c) Imagen encriptada con ordenes $\alpha = \beta = 0.99999999999999$.



(d) Imagen recuperada.

Fig. 5.16. Imagen completamente negra utilizando la metodología descrita en el caso 2.

Se realizó tambien una prueba de ruido para este caso, en esta prueba se contamino la imagen cifrada con ruido de tipo Gaussiano (ver Figura 5.17) y con ruido sal y pimienta (ver Figura 5.18). Como se ve en las imágenes, en ambas ocasiones se recupera una imagen reconocible con respecto a la original. Posteriormente se realizó una prueba aplicando ruido Gaussiano de distintas intensidades sobre la llave de encriptación tal y como se muestra en la Figura 5.19.

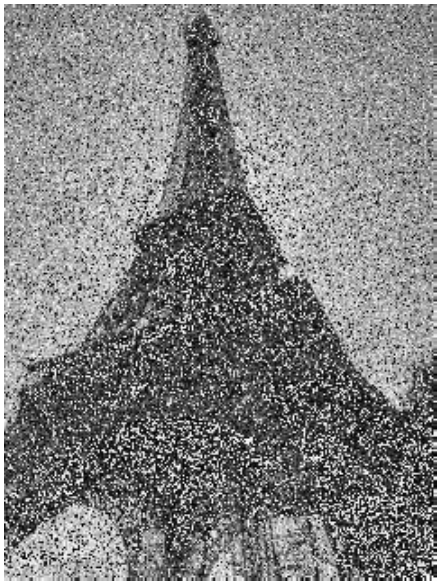
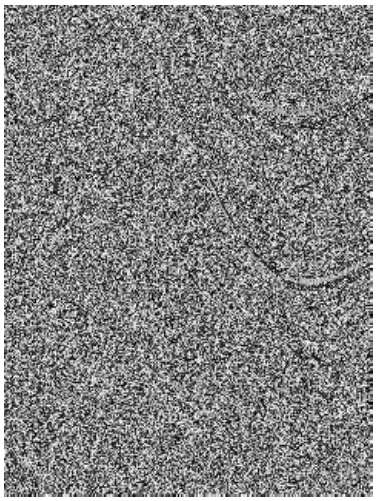


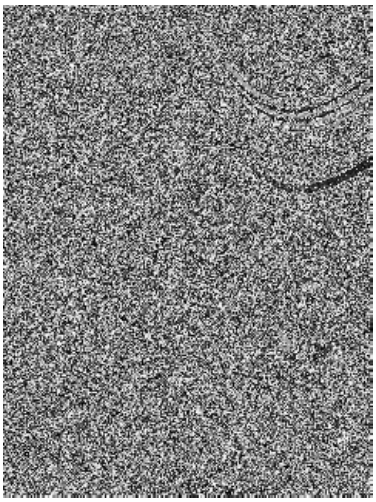
Fig. 5.17. Imagen recuperada al contaminar la imagen cifrada con ruido Gaussiano $r = 0.4517592$.

Fig. 5.18. Imagen recuperada al contaminar la imagen cifrada con ruido sal y pimienta $r = 0.8910745$.

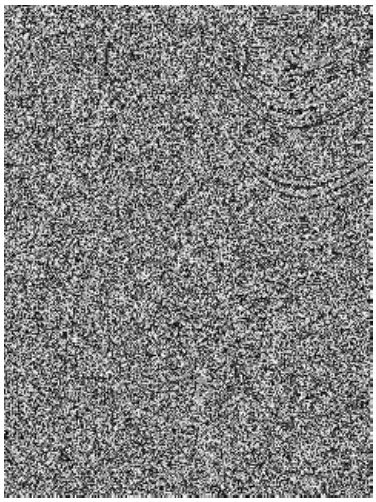
(a) Imagen recuperada sin ruido en la llave.



(b) Imagen recuperada con ruido $SNR = 70dBW$.



(c) Imagen recuperada con ruido $SNR = 75dBW$.



(d) Imagen recuperada con ruido $SNR = 80dBW$.

Fig. 5.19. Intentos de recuperación de imagen original con ruido aditivo Gaussiano en la llave de encriptación utilizando la segunda metodología propuesta.

5.3. Caso 3

En el trabajo de Li [48], se propone un sistema de encriptación basado en una topología específica de sistemas caóticos la cual es mostrada en la ecuación (5.21)

$$\begin{aligned} \mathcal{D}^{\alpha} x_i &= x_{i+1}, \\ \mathcal{D}^{\alpha} x_n &= f\left(X,t\right), \end{aligned} \tag{5.21}$$

donde $1 \leq i \leq n-1$, α es el orden de integración y $X(t) = [x_1, x_2, \cdots, x_n]^T \in \mathcal{R}^n$ es un vector con los estados del sistema maestro. De manera similar se define un sistema esclavo tal como se muestra en la ecuación (5.22)

$$\begin{aligned} \mathcal{D}^{\alpha} y_i &= y_{i+1}, \\ \mathcal{D}^{\alpha} x_n &= g\left(Y,t\right) + d(t) + u(t), \end{aligned} \tag{5.22}$$

donde Y es un vector que contiene los estados del sistema esclavo. Considerando las ecuaciones (5.21) y (5.22), el error se define como (5.23)

$$e(t) = Y(t) - X(t), \tag{5.23}$$

por lo tanto la dinámica del error puede ser definida como se muestra a continuación

$$\mathcal{D}^{\alpha} e_i = e_{i+1}, \mathcal{D}^{\alpha} e_n = g\left(Y,t\right) + d(t) - f(X,t) + u(t). \tag{5.24}$$

La superficie deslizante propuesta se muestra en la ecuación (5.25)

$$s(t) = m\mathcal{D}^{\alpha-1} e_n + k_1 \mathcal{D}^{\alpha-1} + k_2 \int_0^t \sum_{i=1}^{n} c_i e_i(t) dt, \tag{5.25}$$

donde m,k_1,k_2,q y p son parámetros positivos utilizados para sintonizar el controlador. Considerando la derivada ordinaria en la ecuación , se tiene que

$$\dot{s}(t) = m\mathcal{D}^{\alpha} e_n + k_1 \mathcal{D}^{\alpha} e_n^{\frac{q}{p}} + k_2 \sum_{i=1}^{n} c_i e_i(t) = 0. \tag{5.26}$$

Recordando la dinámica del error expuesta en la ecuación (5.24) se tiene que la ley de control se puede describir por la siguiente ecuación

$$u_{eq}(t) = f\left(X,t\right) - g(Y,t) - K\left(\sum_{i=1}^{n} c_i e_i + \mathcal{D}^{\alpha} e_n^{\frac{q}{p}}\right) + u_r, \tag{5.27}$$

donde se agrega u_r para mejorar la robustez del controlador ante incertidumbres y esta se define con la ecuación (5.28)

$$u_r(t) = -K * sign(s(t)), \tag{5.28}$$

donde K es una ganancia adaptable descrita por las ecuaciones (5.29) y (5.30)

$$K = \mu\hat{\lambda}, \qquad \lambda > 0, \tag{5.29}$$

$$\dot{\hat{\lambda}} = \mu|s|. \tag{5.30}$$

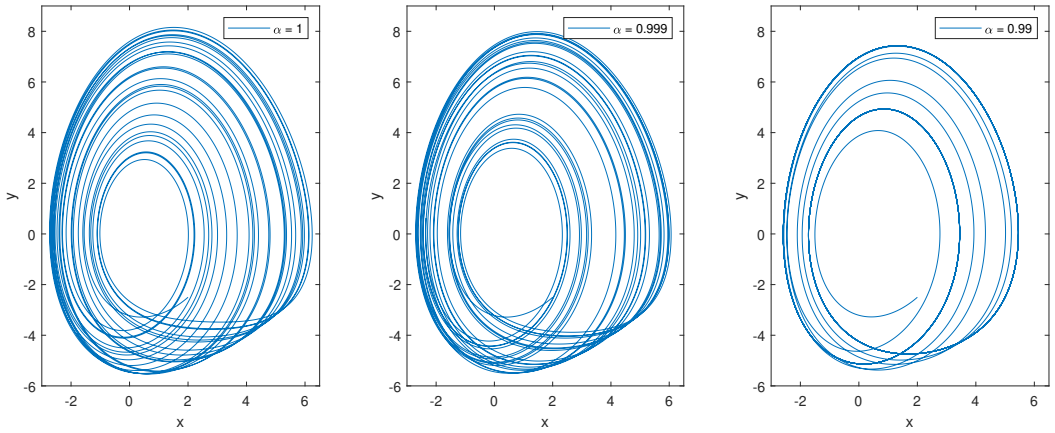


Fig. 5.20. Respuesta del sistema Genesio-Tesi con parámetros $a = 1.2$, $b = -2.92$ y $c = -6$ ante cambios en el orden de integración α, dados por $\alpha = 1$, $\alpha = 0.999$ y $\alpha = 0.99$.

Para reducir el efecto de chattering en el estado estable se decidió utilizar una función tangente hiperbólica en lugar de la función signo, teniendo finalmente como resultado la ley de control mostrada en la ecuación (5.31)

$$u_{eq}(t) = f\left(X,t\right) - g(Y,t) - K\left(\sum_{i=1}^{n} c_i e_i + \mathcal{D}^{\alpha} e_n^{\frac{q}{p}} + tanh\left(100 * s(t)\right)\right). \tag{5.31}$$

Para este trabajo de teiss se decidio utilizar el sistema de Genesio-Tesi presentado en la ecuación (5.32) debido a que cumple con la topología deseada. En la Figura 5.20 se puede ver el comportamiento de este sistema ante cambios en el orden de integración α.

$$\begin{aligned} \mathcal{D}^{\alpha} x_1 &= x_2, \\ \mathcal{D}^{\alpha} x_2 &= x_3, \\ \mathcal{D}^{\alpha} x_3 &= -c x_1 - b x_2 - a x_3 + x_1^2. \end{aligned} \tag{5.32}$$

Los ordenes de integración fueron determinados utilizando el diagrama de bifurcación mostrado en la Figura 5.21. Para este caso particular, el diagrama de bifurcación obtenido no brinda suficiente información para seleccionar los ordenes de integración, por lo tanto se determinó empíricamente el intervalo de $0.99 \leq \alpha \leq 1$.

Para la etapa de codificación se utilizó el mismo algoritmo que el empleado en el caso 1. Los índices de evaluación se presentan en la Tabla 5.3, como se observa, los índices se mantienen comparables a aquellos obtenidos utilizando la metodología original, sin embargo una vez mas, el orden de integración como parámetro adicional suma al tamaño de la llave requerida para la encriptación y recuperación de la información mientras que mantiene sensibilidad a cambios relativamente pequeños. A continuación se muestran los resultados obtenidos para este método.

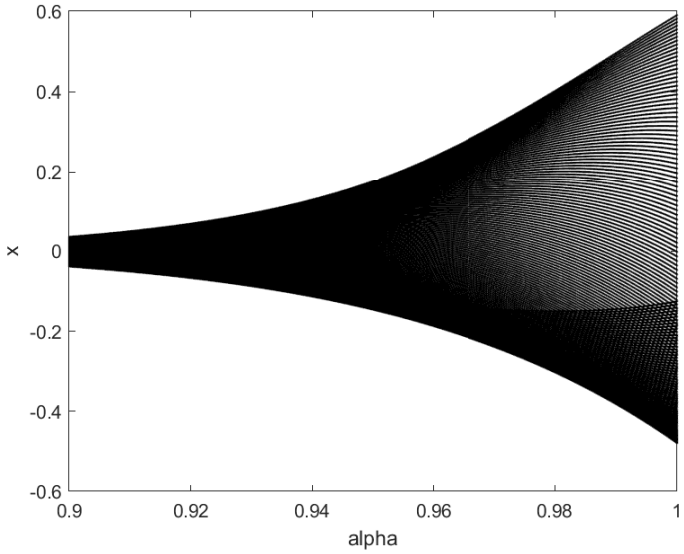
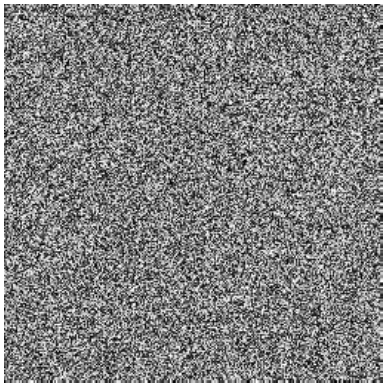


Fig. 5.21. Diagrama de bifurcación del estado x del sistema de Genesio-Tesi respecto al orden α.

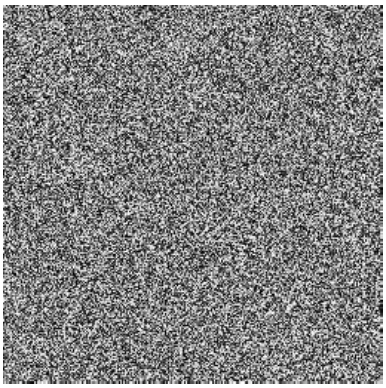
Índices de evaluación				
Imagen	**UACI**	**NPCR**	**Entropía**	**Coeficiente de Correlación**
Árboles	33.4593 %	99.6063 %	7.9893	-0.0025551
Eiffel	33.4265 %	99.6159 %	7.9897	-0.0032580
León	33.4625 %	99.6163 %	7.9917	0.0016845
Negro	33.3138 %	99.5728 %	7.9872	-

Tabla 5.3. Índices de evaluación de algoritmo de encriptación utilizando controlador de modos deslizantes.

(a) Imagen original.



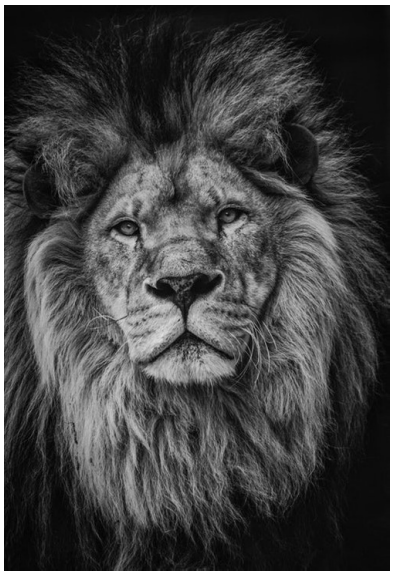
(b) Imagen encriptada utilizando metodología de orden entero.



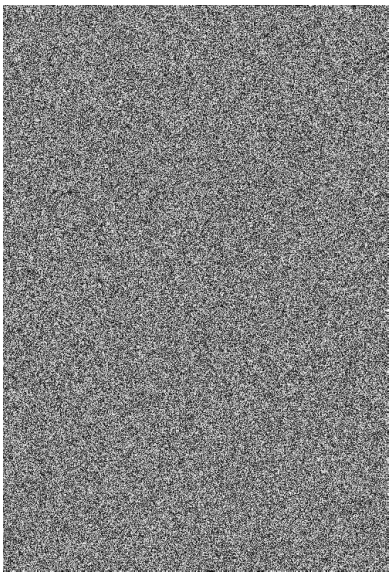
(c) Imagen encriptada con orden $\alpha = 0.99999$

(d) Imagen recuperada.

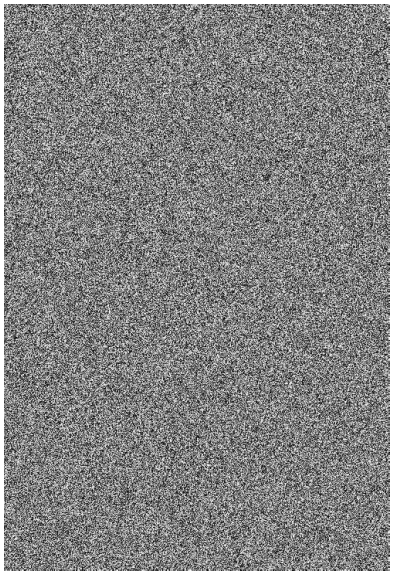
Fig. 5.22. Imagen de árboles encriptada utilizando la metodología descrita en el caso 3.



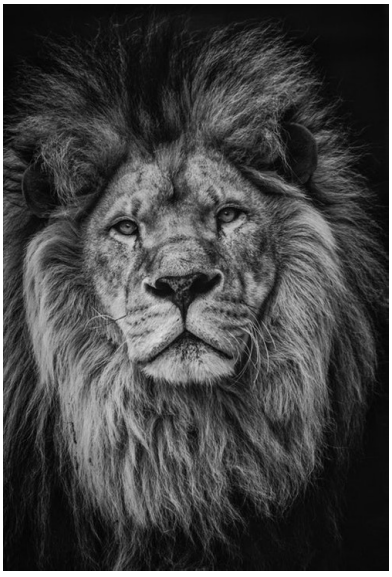
(a) Imagen original.



(b) Imagen encriptada utilizando la metodología de orden entero.



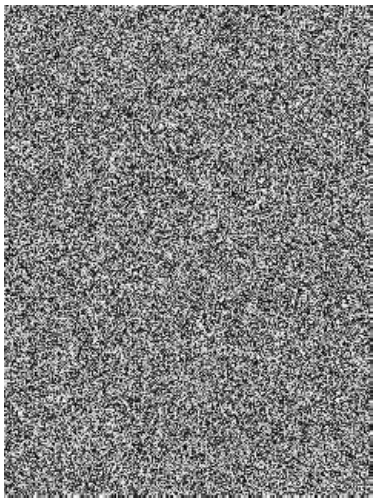
(c) Imagen encriptada con orden $\alpha = 0.99$



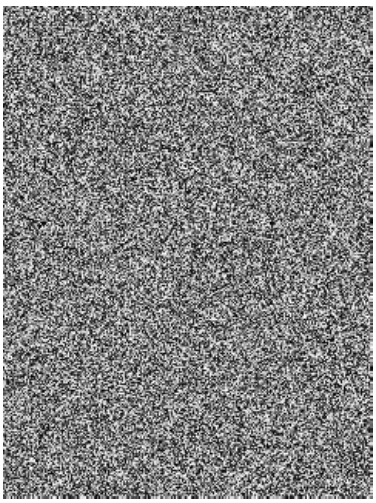
(d) Imagen recuperada.

Fig. 5.23. Imagen de león encriptada utilizando la metodología descrita en el caso 3.

(a) Imagen original.



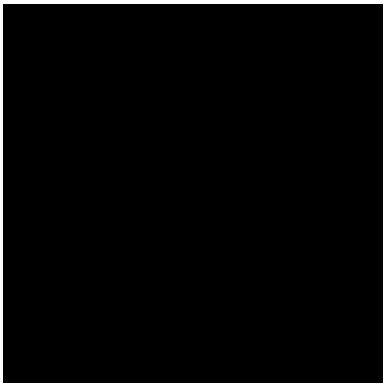
(b) Imagen encriptada utilizando la metodología de orden entero.



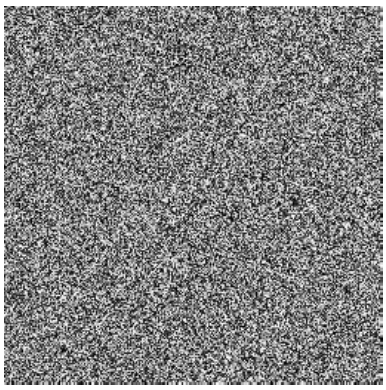
(c) Imagen encriptada con orden $\alpha = 0.9999$.

(d) Imagen recuperada.

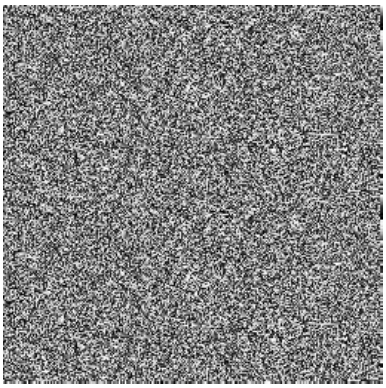
Fig. 5.24. Imagen de torre Eiffel encriptada utilizando la metodología descrita en el caso 3.



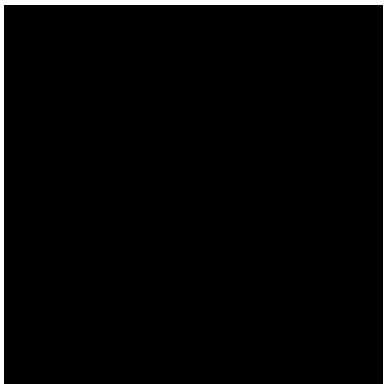
(a) Imagen original.



(b) Imagen encriptada utilizando la metodología de orden entero.



(c) Imagen encriptada con orden $\alpha = 0.99999$



(d) Imagen recuperada.

Fig. 5.25. Imagen completamente negra encriptada utilizando la metodología descrita en el caso 3.

De manera similar a los casos anteriores se realizaron pruebas para comprobar el desempeño de la metodología al efecto del ruido tanto en la imagen cifrada como en la llave de encriptación. En la Figura 5.26 se aplicó un ruido Gaussiano a la imagen encriptada, mientras que en la Figura 5.27 se aplicó ruido tipo sal y pimienta.

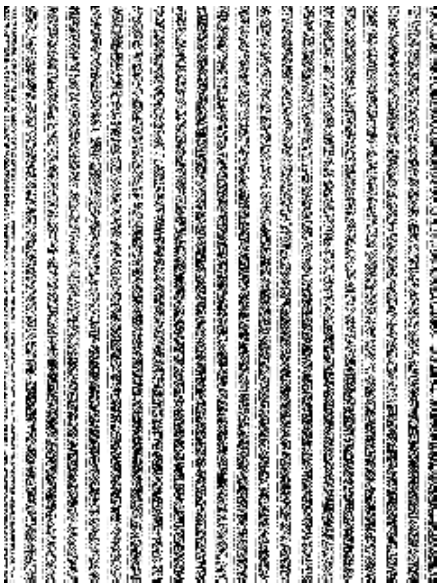


Fig. 5.26. Imagen recuperada al contaminar la imagen cifrada con ruido Gaussiano.

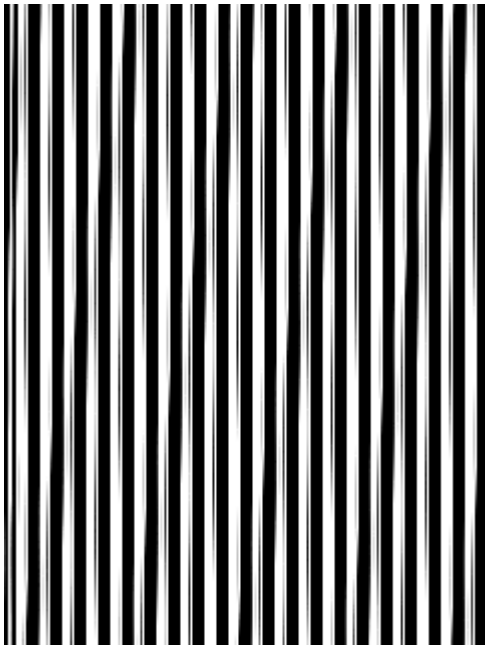


Fig. 5.27. Imagen recuperada al contaminar la imagen cifrada con ruido sal y pimienta.

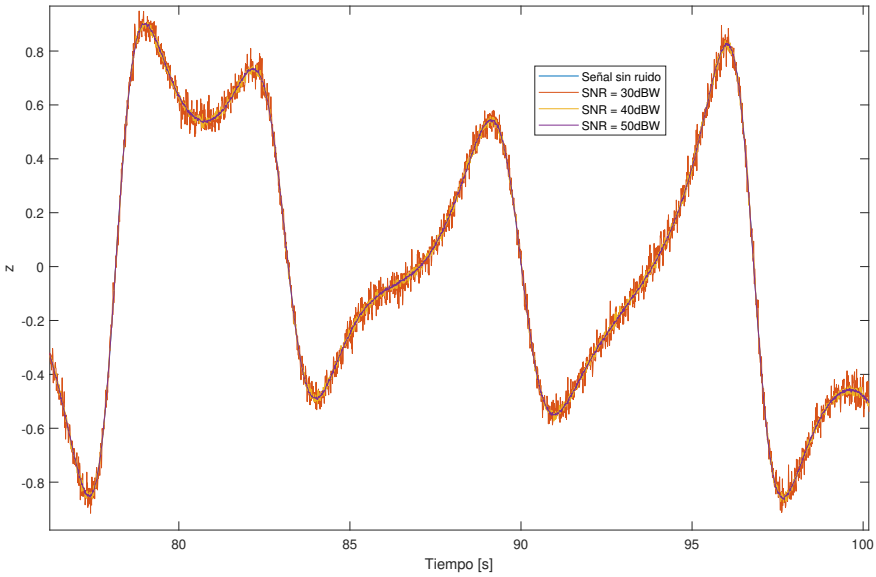
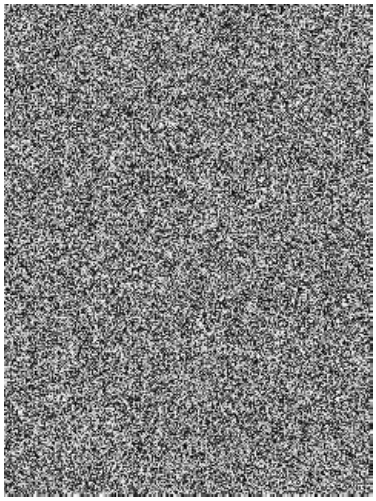
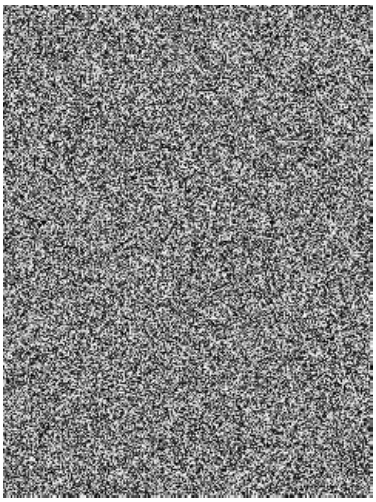


Fig. 5.28. Imagen recuperada al contaminar la imagen cifrada con ruido sal y pimienta.

(a) Imagen recuperada sin ruido.



(b) Imagen recuperada con ruido Gaussiano $SNR = 30dBW$.



(c) Imagen recuperada con ruido Gaussiano $SNR = 40dBW$.

(d) Imagen recuperada con ruido Gaussiano $SNR = 50dBW$.

Fig. 5.29. Imagen de torre Eiffel encriptada utilizando la metodología descrita en el caso 3 con ruido en la llave de encriptación.

Capítulo 6

Conclusiones

Los sistemas caóticos poseen diversas características que los convierte en un campo de estudio interesante; la existencia de atractores, la posibilidad de ser sincronizados y su relativamente alta sensibilidad a parámetros y condiciones iniciales entre otras. El estudio de estas particularidades ha llevado al diseño de algoritmos de encriptación que emplean caos como medio para obtener secuencias pseudoaleatorias. Para este trabajo, tres algoritmos de encriptación que involucran sistemas caóticos fueron modificados de tal manera que sus ecuaciones dinámicas se generalizaran.

En el primer caso, un esquema de Pecora-Carrol fue utilizado para la sincronización de dos sistemas de Lorenz utilizando la variable de estado y como variable sincronizante y como llave de encriptación. Ambos sistemas de Lorenz fueron generalizados utilizando la definición de derivada fraccionaria de Caputo. En el segundo caso, se proponía originalmente el uso de una representación del mapa caótico de Julia-Mandelbrot para la encriptación de información, sin embargo el tamaño de la llave se veía muy limitado. El mapa del ave mítica fue propuesto como sustituto y el orden de integración fue utilizado como llave de encriptación. Para este caso se utilizo la definición de derivada conformable fraccionaria en el sentido de Khalil. Finalmente en el caso 3 se empleo un controlador de modos deslizantes para la sincronización de dos atractores caóticos pertenecientes a la familia de Genesio-Tesi, utilizando únicamente la variable de estado z.

Todos los algoritmos fueron aplicados a las mismas cuatro imágenes. Los tres métodos presentaron índices de desempeño similares entre ellos y a los métodos originales; Sin embargo los métodos propuestos en este trabajo incrementan el tamaño de la llave de los algoritmos, lo cual se traduce en mas seguridad de la información encriptada.

Como producto de este trabajo se hicieron dos publicaciones. La primera de ellas presenta la supresión de caos en diversos sistemas utilizando un controlador de modos deslizantes y su implementación en una tarjeta FPGA. En la segunda publicación se presentan diversos comportamientos de mapas caóticos utilizando derivadas fraccionarias, conformables y conformables fraccionarias de orden variable e inconmensurado. Ambos trabajos fueron publicados en la revista Çhaos, Solitons & Fractals Journal". ISSN: 0960-0779. Con un factor de impacto de 3.064 (cuartil Q1).

6.1. Trabajos Futuros

En base a los resultados obtenidos y el trabajo obtenido se proponen las siguientes ideas:

- Analizar a fondo mediante diagramas de bifurcación lo que sucede con la dinámica de los sistemas caóticos al variar el orden de integración α.
- Experimentar con mas combinaciones de ordenes variables en sistemas mixtos con diversos sistemas caóticos.
- Desarrollar métodos de criptoanálisis que permitan atacar de manera eficiente los sistemas de encriptación que involucran caos y operadores fraccionarios con la finalidad de verificar su seguridad.
- La implementación de las metodologías propuestas en sistemas de comunicación.

Bibliografía

[1] Morgan, S., & Carson, J. (2017). The World Will Need to Protect 300 Billion Passwords By 2020. Cybersecurity Ventures.

[2] Loshin, P. (2013). Simple steps to data encryption: a practical guide to secure computing. Newnes.

[3] Hao, Z., Xi-Kui, M., Yu, Y., & Cui-Dong, X. (2005). Generalized synchronization of hyperchaos and chaos using active backstepping design. Chinese Physics, 14(1), 86.

[4] Alvarez, G., & Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. International Journal of Bifurcation and Chaos, 16(08), 2129-2151.

[5] Tavazoei, M. S., & Haeri, M. (2008). Synchronization of chaotic fractional-order systems via active sliding mode controller. Physica A: Statistical Mechanics and its Applications, 387(1), 57-70.

[6] Rhouma, R., & Belghith, S. (2008). Cryptanalysis of a new image encryption algorithm based on hyper-chaos. Physics Letters A, 372(38), 5973-5978.

[7] Mazloom, S., & Eftekhari-Moghadam, A. M. (2009). Color image encryption based on coupled nonlinear chaotic map. Chaos, Solitons & Fractals, 42(3), 1745-1754.

[8] Liñán, J. Á. R., Morales, J. D. L., Ibarra, J. R. M., Carmona, R., Bonilla, H. R., Hernández, V. G., ... & González, M. A. P. (2009). Sincronización generalizada en orden reducido para sistemas caóticos. Ingenierías, 12(45), 2.

[9] Lin, J. S., Huang, C. F., Liao, T. L., & Yan, J. J. (2010). Design and implementation of digital secure communication based on synchronized chaotic systems. Digital Signal Processing, 20(1), 229-237.

[10] Lang, J., Tao, R., & Wang, Y. (2010). Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function. Optics Communications, 283(10), 2092-2096.

[11] Yoon, J. W., &Kim, H. (2010). An image encryption scheme with a pseudorandom permutation based on chaotic maps. Communications in Nonlinear Science and Numerical Simulation, 15(12), 3998-4006.

[12] Sharma, M., & Kowar, M. K. (2010). Image encryption techniques using chaotic schemes: a review.

[13] Indrakanti, S. P., & Avadhani, P. S. (2011). Permutation based image encryption technique. International Journal of Computer Applications, 28(8), 45-47.

[14] Kuo, C. L. (2011). Design of a fuzzy sliding-mode synchronization controller for two different chaos systems. Computers & Mathematics with Applications, 61(8), 2090-2095.

[15] Chen, D. Y., Liu, Y. X., Ma, X. Y., & Zhang, R. F. (2012). Control of a class of fractional-order chaotic systems via sliding mode. Nonlinear Dynamics, 67(1), 893-901.

[16] Wang, X., Teng, L., & Qin, X. (2012). A novel colour image encryption algorithm based on chaos. Signal Processing, 92(4), 1101-1108.

[17] Angulo Guzmán, S. Y. (2012). Sincronización de redes complejas con osciladores caóticos de orden fraccionario (Doctoral dissertation, Universidad Autónoma de Nuevo León).

[18] Wei, X., Guo, L., Zhang, Q., Zhang, J., & Lian, S. (2012). A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. Journal of Systems and Software, 85(2), 290-299.

[19] Volos, C. K., Kyprianidis, I. M., & Stouboulos, I. N. (2013). Image encryption process based on chaotic synchronization phenomena. Signal Processing, 93(5), 1328-1340.

[20] Pai, M. C. (2014). Global synchronization of uncertain chaotic systems via discrete-time sliding mode control. Applied Mathematics and Computation, 227, 663-671.

[21] Xu, Y., Wang, H., Li, Y., & Pei, B. (2014). Image encryption based on synchronization of fractional chaotic systems. Communications in Nonlinear Science and Numerical Simulation, 19(10), 3735-3744.

[22] Onma, O. S., Olusola, O. I., & Njah, A. N. (2014). Control and synchronization of chaotic and hyperchaotic Lorenz systems via extended backstepping techniques. Journal of Nonlinear Dynamics, 2014.

[23] Muthukumar, P., Balasubramaniam, P., & Ratnavelu, K. (2014). Synchronization and an application of a novel fractional order King Cobra chaotic system. Chaos: An Interdisciplinary Journal of Nonlinear Science, 24(3), 033105.

[24] Chaparro Guevara, G., & Escot Mangas, L. (2015). El control de sistemas dinámicos caóticos en economía aplicación a un modelo de hiperinflación. Revista Finanzas y Política Económica, Vol. 7, no. 1 (ene.–jul. 2015); p. 131-145. http://dx. doi. org/10.14718/revfinanzpolitecon. 2018.10. 1.7.

[25] Jafari, P., Teshnehlab, M., & Tavakoli-Kakhki, M. (2017). Synchronization and stabilization of fractional order nonlinear systems with adaptive fuzzy controller and compensation signal. Nonlinear Dynamics, 90(2), 1037-1052.

[26] Azar, A. T., Vaidyanathan, S., & Ouannas, A. (Eds.). (2017). Fractional order control and synchronization of chaotic systems (Vol. 688). Springer.

[27] Rajagopal, K., Vaidyanathan, S., Karthikeyan, A., & Duraisamy, P. (2017). Dynamic analysis and chaos suppression in a fractional order brushless DC motor. Electrical Engineering, 99(2), 721-733.

[28] Cao, J., & Li, R. (2017). Fixed-time synchronization of delayed memristor-based recurrent neural networks. Science China Information Sciences, 60(3), 032201.

[29] Ouannas, A., Azar, A. T., & Vaidyanathan, S. (2017). A robust method for new fractional hybrid chaos synchronization. Mathematical Methods in the Applied Sciences, 40(5), 1804-1812.

[30] Coronel-Escamilla, A., Gómez-Aguilar, J. F., Torres, L., Escobar-Jiménez, R. F., & Valtierra-Rodríguez, M. (2017). Synchronization of chaotic systems involving fractional operators of Liouville–Caputo type with variable-order. Physica A: Statistical Mechanics and its Applications, 487, 1-21.

[31] Zambrano-Serrano, E., Munoz-Pacheco, J. M., Gómez-Pavón, L. C., Luis-Ramos, A., & Chen, G. (2018). Synchronization in a fractional-order model of pancreatic β-cells. The European Physical Journal Special Topics, 227(7-9), 907-919

[32] Wang, X., Ouannas, A., Pham, V. T., & Abdolmohammadi, H. R. (2018). A fractional-order form of a system with stable equilibria and its synchronization. Advances in Difference Equations, 2018(1), 20.

[33] Aguilar-Ibañez, C., García-Canseco, E., Martínez-García, R., Martínez-García, J. C., & Suarez-Castañon, M. S. (2018). An I&I-based observer to solve the output-feedback synchronization problem for a class of chaotic systems. Asian Journal of Control, 20(4), 1491-1503.

[34] Delfín-Prieto, S. M., Martínez-Guerra, R., & Trejo-Zúñiga, I. (2018, September). Robust State-Estimation for Fractional-Order Liouvillian Systems. In 2018 15th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE) (pp. 1-6). IEEE.

[35] González-Miranda, J. M. (2004). Synchronization and control of chaos: an introduction for scientists and engineers. Synchronization and Control of Chaos: An Introduction for Scientists and Engineers. Edited by GONZALEZ-MIRANDA J M. Published by World Scientific Publishing Co. Pte. Ltd. ISBN# 9781860945229.

[36] Pikovsky, A., Kurths, J., Rosenblum, M., & Kurths, J. (2003). Synchronization: a universal concept in nonlinear sciences (Vol. 12). Cambridge university press.

[37] Pecora, L. M., & Carroll, T. L. (2015). Synchronization of chaotic systems. Chaos: An Interdisciplinary Journal of Nonlinear Science, 25(9), 097611.

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

[39] Agarwal, R. P. (1953). A propos d'une note de M. Pierre Humbert. CR Acad. Sci. Paris, 236(21), 2031-2032.

[40] Podlubny, I. (1998). Fractional differential equations: an introduction to fractional derivatives, fractional differential equations, to methods of their solution and some of their applications (Vol. 198). Elsevier.

[41] Solís-Pérez, J. E., Gómez-Aguilar, J. F., & Atangana, A. (2018). Novel numerical method for solving variable-order fractional differential equations with power, exponential and Mittag-Leffler laws. Chaos, Solitons & Fractals, 114, 175-185.

[42] Khalil, R., Al Horani, M., Yousef, A., & Sababheh, M. (2014). A new definition of fractional derivative. Journal of Computational and Applied Mathematics, 264, 65-70.

[43] Jarad, F., Uğurlu, E., Abdeljawad, T., & Baleanu, D. (2017). On a new class of fractional operators. Advances in Difference Equations, 2017(1), 247.

[44] García Sepúlveda, O. (2015). Encriptado de datos con osciladores caóticos de orden fraccionario (Doctoral dissertation, Universidad Autónoma de Nuevo León).

[45] Rodriguez, I. F., Amaya, E. I., Suarez, C. A., & Moreno, J. D. (2017). Images Encryption Algorithm Using the Lorenz's Chaotic Attractor. Ingeniería, 22(3), 396-412.

[46] Gao, W., Sun, J., Qiao, W., & Zhang, X. (2019). Digital image encryption scheme based on generalized Mandelbrot-Julia set. Optik, 185, 917-929.

[47] Ávalos-Ruiz, L. F., Gómez-Aguilar, J. F., Atangana, A., & Owolabi, K. M. (2019). On the dynamics of fractional maps with power-law, exponential decay and Mittag–Leffler memory. Chaos, Solitons & Fractals, 127, 364-388.

[48] Li, Y., Wang, H., & Tian, Y. (2019). Fractional-order adaptive controller for chaotic synchronization and application to a dual-channel secure communication system. Modern Physics Letters B, 33(24), 1950290.

Anexos

Anexo A

Productos

Chaos, Solitons and Fractals 115 (2018) 177–189

Contents lists available at ScienceDirect

Chaos, Solitons and Fractals

Nonlinear Science, and Nonequilibrium and Complex Phenomena

journal homepage: www.elsevier.com/locate/chaos

FPGA implementation and control of chaotic systems involving the variable-order fractional operator with Mittag–Leffler law

L.F. Ávalos-Ruiz[a], C.J. Zúñiga-Aguilar[a], J.F. Gómez-Aguilar[b,*], R.F. Escobar-Jiménez[a], H.M. Romero-Ugalde[c]

[a] Tecnológico Nacional de México/CENIDET, Interior Internado Palmira S/N, Col. Palmira, C.P. 62490, Cuernavaca Morelos, México
[b] CONACyT-Tecnológico Nacional de México/CENIDET, Interior Internado Palmira S/N, Col. Palmira, C.P. 62490, Cuernavaca Morelos, México
[c] Diabeloop SA, 155 Cours Berriat, F-38000 Grenoble, France

ARTICLE INFO

Article history:
Received 13 June 2018
Revised 17 August 2018
Accepted 21 August 2018

Keywords:
Fractional calculus
Variable-order fractional operators
Nonlinear systems
Chaos
LabVIEW software
FPGA implementation

ABSTRACT

This paper presents the simulation and control implementation on a Field Programmable Gate Array (FPGA) for a class of variable-order fractional chaotic systems by using sliding mode control strategy. Four different fractional variable-order chaotic systems via Atangana–Baleanu–Caputo fractional-order derivative were considered; Dadras, Aizawa, Thomas and 4 Wings attractors. A methodology has been developed to construct variable-order fractional chaotic systems using LabVIEW® software for its implementation in the National Instruments myRio-1900 (Xilinx FPGA Z-7010)® device. The variable-order fractional differential equations and the control law were solved using the variable-order Adams algorithm. Finally, simulation results show that FPGA provides high-speed realizations with the desired accuracy and demonstrate the effectiveness of the proposed sliding mode control.

1. Introduction

Fractional calculus is the mathematical generalisation of classical calculus, this mathematical tool has been used in the recent decades for modeling real world problems in many field's science, technology and engineering [1–8]. Fractional-Order Differential Equations (FODE's) have increasingly attracted attention for the evaluation of dynamical systems. The fractional derivative operator is non-local, which expresses that the system's response will be affected at any time by all previous responses. FODE's give an exact description of different physical phenomena, also, FODE's give a description of the inherent relation of different processes with memory and hereditary properties [9]. In the literature there are several definitions of fractional-order derivatives, for instance, Riemann–Liouville, Grünwald–Letnikov, Liouville–Caputo, Caputo–Fabrizio and Atangana–Baleanu [10–25]. The order of the fractional derivative can be interpreted as the index of memory of the system. This fractional-order can be real, rational or irrational, or even complex. Samko, in [26], stated that the fractional integrals and derivative can be generalized introducing in the fractional order a function of time or space or space-time variables $q(x, t)$. Several studies have been reported in the literature employing this proposal with excellent results [27–32].

Chaos, as a very interesting nonlinear phenomenon, has been intensively studied in the last decades. In the literature, there are several works on different control techniques applied to a variety of chaotic systems [33–36]. The chaos control problem in a fractional order brushless DC motor was studied by the authors in [37], in this work, the sliding mode control, robust control, and extended back-stepping techniques were represented in the Liouville–Caputo sense. The chaos control for a general class of chaotic systems based on the sliding mode control theory was studied by Wang et al. [38]. The authors used feedback controllers to guarantee asymptotic stability of the chaotic systems. Yin et al. [39] presented a sliding mode control law for controlling a class of fractional-order chaotic systems. Authors in [40] developed a modified sliding mode approach for synchronizing fractional-order chaotic systems using neural networks. In recent years, the hardware implementation of fractional chaotic systems has increasingly attracted attention. Nevertheless, the implementation of the algorithms is complicated due to their memory dependence and the hardware requires the use of high-order integer order systems. Several digital implementations of chaotic systems have been implemented on FPGAs.

FPGAs are well-known for their processing speed and hardware flexibility. The maind advantage of this technology is its low con-

* Corresponding author.
E-mail address: jgomez@cenidet.edu.mx (J.F. Gómez-Aguilar).

https://doi.org/10.1016/j.chaos.2018.08.021
0960-0779/

Chaos, Solitons and Fractals 127 (2019) 364–388

Contents lists available at ScienceDirect

Chaos, Solitons and Fractals

Nonlinear Science, and Nonequilibrium and Complex Phenomena

journal homepage: www.elsevier.com/locate/chaos

Frontiers

On the dynamics of fractional maps with power-law, exponential decay and Mittag–Leffler memory

L.F. Ávalos-Ruiz [a], J.F. Gómez-Aguilar [b,*], A. Atangana [c], Kolade M. Owolabi [d]

[a] Tecnológico Nacional de México/CENIDET. Interior Internado Palmira S/N, Col. Palmira, C.P. 62490, Cuernavaca Morelos, México
[b] CONACyT-Tecnológico Nacional de México/CENIDET. Interior Internado Palmira S/N, Col. Palmira C.P. 62490, Cuernavaca Morelos, México
[c] Institute for Groundwater Studies, University of the Free State, Bloemfontein 9301, South Africa
[d] Department of Mathematical Sciences, Federal University of Technology, PMB 704, Akure Ondo State, Nigeria

ARTICLE INFO

Article history:
Received 17 June 2019
Accepted 10 July 2019

Keywords:
Fractional calculus
Variable-order fractional operators
Chaotical maps
Mixed schemes

ABSTRACT

In this paper, we propose a fractional form of two-dimensional generalized mythical bird, butterfly wings and paradise bird maps involving the fractional conformable derivative of Khalil's and Atangana's type, the Liouville–Caputo and Atangana–Baleanu derivatives with constant and variable-order. We obtain new chaotical behaviors considering numerical schemes based on the fundamental theorem of fractional calculus and the Lagrange polynomial interpolation. Also, the dynamics of the proposed maps are investigated numerically through phase plots considering combinations of these derivatives and mixed integration methods for each map. The numerical simulations show very strange and new behaviors for the first time in this manuscript.

1. Introduction

Modeling chaotic processes have been of great important within field of dynamical system in the last pass years. We can recall for readers sake that dynamical systems are commonly depicted by one or more differential or difference equations. In particular differential equations using the concept of derivative, which varies from classical which are rate of change to fractional which are convolutions [1–8]. The equation used to model these dynamical system specify its behavior over any given short period of time. However, in order to capture the system behavior for a longer period, it is sometime necessary to integrate the equations, sometimes via analytical means or via iterations, this can well be achieved using computational power. Additionally, we can stress on the fact that, attractors are portions or subsets of the phase space of a dynamical system, often depicting real world observed facts. Before 1960 attractors were considered to representing simple geometric subsets of the phase space for instance, surfaces, points, line and simple regions of three dimensional space. Nevertheless it was recognized that, more complex attractor that cannot be classified as simple geometric subsets, such topologically sets, were recognized as at that period, but this trends of ideas were fragile anomalies. However, Stephen Smale revealed that his horseshoe map was robust and that it attractor had the structure of a Cantor set [9]. A proof that these physical problems cannot be captured using simple mathematical operators like classical differential operator [10–18]. Very strange attractors have been suggested including mythical bird, butterfly wings and paradise bird maps [19], however have never being investigated under the framework of the new trends of fractional differential and integral operators including the fractional conformable derivative of Khalil's and Atangana's type and the Atangana–Baleanu type with constant and variable-order. Also no one have studied the behavior of such model when using the well-known conformable derivative that, is same like fractal derivative [20–27].

The main of the present paper is studying the chaotic dynamics of the two-dimensional generalized mythical bird, butterfly wings and paradise bird maps involving the fractional conformable derivative of Khalil's and Atangana's type, the Liouville–Caputo and Atangana–Baleanu derivatives with constant and variable-order. Numerical simulations including phase plots considering combinations of these derivatives and mixed integration methods for each map are presented.

2. Preliminaries on fractional calculus

Now, we present some definitions which will be used in our study.

* Corresponding author.
E-mail address: jgomez@cenidet.edu.mx (J.F. Gómez-Aguilar).

https://doi.org/10.1016/j.chaos.2019.07.010
0960-0779/