ALGORITMO DE CIFRADO DE AUDIO DIGITAL MEDIANTE ATRACTORES CAÓTICOS

SANTIAGO JIMÉNEZ BONILLA

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

FACULTAD DE INGENIERÍA

INGENIERÍA DE SISTEMAS

BOGOTÁ

2020

ALGORITMO DE CIFRADO DE AUDIO DIGITAL MEDIANTE ATRACTORES CAÓTICOS

SANTIAGO JIMÉNEZ BONILLA

TRABAJO DE GRADO PARA OPTAR AL TÍTULO DE:

INGENIERO DE SISTEMAS

CODIRECTORA

Dr. Sc. DEICY ALVARADO

CODIRECTORA

M. Sc. ISABEL AMAYA

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

FACULTAD DE INGENIERÍA

INGENIERÍA DE SISTEMAS

BOGOTÁ

2020

Tabla de contenido

1. Introducción

El mensaje, como objeto fundamental de comunicación entre sociedades se ha puesto a prueba desde sus inicios, la integridad de este objeto es de vital importancia para que el ejercicio de la comunicación sea efectivo, es por esto, que en ciertos casos es necesario proteger este mensaje mediante algún mecanismo que evite que este pueda ser interceptado, manipulado o suplantado de alguna forma por sujetos no autorizados, es aquí donde la criptografía se hace presente. El objetivo fundamental de la criptografía es ocultar la información sensible que existe en el mensaje a través de operaciones que hacen ilegible el mensaje para todos excepto para el remitente y el receptor.

La criptografía ha sido usada desde casi los inicios mismos de la escritura tomando mayor importancia a principios del siglo XX, siendo un pilar de la seguridad interna de las naciones y una herramienta de espionaje en época de conflictos, y que, con el auge de las tecnologías de la información se ha venido entremezclando con las actividades cotidianas del mundo donde presupone ser la base de la seguridad de la información en la revolución informática que estamos viviendo en este nuevo milenio, es por esto que se dedica un gran esfuerzo en el desarrollo de nuevos mecanismos y sistemas criptográficos que suplan las necesidades constantemente cambiantes del mundo moderno y las actividades humanas basadas en información digital.

Por otra parte, dentro del vasto mundo de los sistemas físicos, o mejor, sistemas que describen el mundo, se pueden encontrar algunos que no es posible modelarlos de forma tradicional y que llegan a presentar peculiares e inesperados comportamientos, estos son sistemas

dinámicos no lineales y que han sido estudiados y dieron origen a lo que hoy se conoce como teoría del caos (Strogatz, 2015).

Este proyecto se enmarca dentro de la línea de investigación sobre caos propuesta por el grupo de complejidad de la Universidad Distrital (ComplexUD), y tendrá como objetivo la generación de un algoritmo para cifrar archivos de audio digital aplicando sistemas matemáticos estudiados por la teoría del caos que presentan características que pueden proveer a los sistemas de cifrado grandes fortalezas.

2. Planteamiento del problema de investigación

El desarrollo de nuevos sistemas criptográficos y herramientas que permitan proteger la información sensible que se maneja día a día a través de sistemas informáticos como computadores o teléfonos inteligentes ha ganado gran importancia y esfuerzo científicos durante los últimos años. La gran mayoría de la información existe ahora en medios digitales, ya sea en aplicaciones de mensajería, o en proveedores de servicios de almacenamiento en la nube. Toda esta información es tratada y mantenida por tecnologías de cifrado propias de los proveedores de estos servicios quienes son blanco de ataque constante. Pese a esto, los algoritmos de cifrado utilizados por la comunidad en general y teniendo como principal referencia el AES y el RSA (Paar & Pelzl, 2010) deben ser mejorados y actualizados de manera constante para evitar ser vulnerados y así exponer la información de quienes usan estos sistemas criptográficos. Así pues, es de vital importancia que existan alternativas que diversifiquen el uso de sistemas criptográficos como los mencionados anteriormente, que potencien el campo de la seguridad informática y provean herramientas suficientes para solventar el mejoramiento de los sistemas computacionales utilizados para romper los algoritmos de cifrado. Por lo tanto, y para propósitos investigativos se da lugar al siguiente interrogante ¿Cómo aplicar las propiedades caóticas de los sistemas no lineales en el diseño de un algoritmo de cifrado simétrico para archivos en formato digital?

3. Objetivos

3.1. Objetivo general

- Proponer un algoritmo de encriptación de audio digital a través del uso de atractores caóticos que cumpla con los estándares de seguridad, eficiencia y eficacia acordes con los reportados en la literatura científica actual.

3.2. Objetivos específicos

- Seleccionar el modelo caótico que permita establecer las operaciones de confusión y difusión propias del sistema criptográfico.
- Evaluar experimentalmente el modelo criptográfico propuesto para verificar que cumpla con los estándares de seguridad, eficiencia y eficacia acordes con los reportados en la literatura científica actual

4. Justificación

La situación que se vive actualmente en el mundo debido a la pandemia producida por el virus SARS-CoV-2 (COVID-19) (Andersen, Rambaut, Lipkin, Holmes, & Garry, 2020) ha hecho que los gobiernos mundiales tomen medidas de distanciamiento social y cuarentenas estrictas provocando que la interacción social se vuelque en su mayoría a medios digitales, esto trajo consigo un aumento de los casos de ciberataques como lo evidencia el Centro Nacional de Ciber Seguridad del Reino Unido (NCSC) en compañía del Departamento de Seguridad de los Estados Unidos y la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) (National Cyber Security Centre, Homeland Security, & Cybersecurity and Infrastruture Security, 2020), así como el reporte elaborado por el gobierno australiano y organizaciones nacionales (*ACSC Annual Cyber Threat Report*, 2019).

Las nuevas necesidades de sistemas de protección de datos van acompañadas del aumento de la información digital manejada alrededor del mundo y que muestra un incremento exponencial (Ben Ayed, Ben Halima, & Alimi, 2015), lo cual requiere de un mayor esfuerzo y actualización constante de sistemas de seguridad que sean más rápidos y eficaces y que logren suplir las necesidades generadas diariamente. Una de las posibles alternativas es la utilización de sistemas complejos, sistemas dinámicos no lineales que por sus propiedades de irregularidad y aleatoriedad proveen sin mucho esfuerzo computacional, comportamientos difíciles de rastrear y descifrar que permiten generar sistemas de cifrado más robustos y seguros (Ganesh Sekar & Arun, 2020) logrando resultados superiores a algunos métodos de encriptación convencionales (Babu & Singh, 2013; Thein, Nugroho, Adji, & Mustika, 2018).

5. Antecedentes de investigación

En las últimas décadas la comunidad científica ha efectuado grandes esfuerzos en el desarrollo de nuevos sistemas criptográficos de acuerdo a las necesidades de la sociedad, es por eso que han incursionado en la implementación y generación de sistemas de criptografía alternativos a los ya comúnmente utilizados y difundidos por el sector tecnológico.

En 1991 los autores proponen un algoritmo de cifrado para texto plano utilizando la función Tienda por su simplicidad y robustez debido a las características intrínsecas del sistema caótico (Habutsu, Nishio, Sasase, & Mori, 1991). Posteriormente se diseñaron algoritmos para cifrado de texto aplicando otros sistemas caóticos, como la función del Panadero, que a pesar de no otorgar resultados prometedores por el comportamiento cíclico y rápida convergencia del sistema, brindaron un valioso análisis acerca de la caracterización de esta función para la criptografía (Masuda, 1999).

Para el año 2005, se desarrolló un algoritmo de cifrado asimétrico para audio haciendo uso de la sincronización caótica de sistemas y la función de Sinai alcanzando buenos índices de seguridad por su amplio espacio de clave (Zhang & Min, 2005). Investigaciones como las propuestas en (Gnanajeyaraman & Prasadh, 2009; Jia, 2010; Wong, Kwok, & Yuen, 2009) permiten observar una mejora considerable en la aplicación de caos en la criptografía de audio e imágenes, identificando características y sistemas útiles para cada etapa o proceso de cifrado (difusión y confusión) otorgando resultados efectivos y robustos para su implementación.

En el año 2011 se plantea un algoritmo de cifrado asimétrico que genera, a partir la función Logística, una secuencia de valores usados por una red neuronal para el cifrado y descifrado de contenido multimedia (Lian & Chen, 2011).

Por otra parte, Radha y Venkatesulu desarrollaron un sistema de cifrado de bloques de 512 bits para la protección de señales multimedia en tiempo real, aplicando operadores XOR y técnicas de shuffling con un espacio de clave de 2^{512}, además, se utilizaron técnicas de análisis de distribución y correlación de los resultados obtenidos (Radha & Venkatesulu, 2012).

De igual forma, en el año 2013, Ganesh y Ilango propusieron un sistema criptográfico para señales de audio que son cuantificadas en frecuencias con una precisión de 16 bits y transformándolas mediante el uso de una función caótica de dimensión 8 definido a partir de la función Cat de Arnold, usándolo como generador de valores pseudoaleatorios para el proceso de confusión mediante tablas Look-Up (Ganesh Babu & Ilango, 2013).

Así mismo, en el año 2014 se reportó un algoritmo de cifrado de audio que usó los sistemas caóticos, generados por las funciones Logística y del panadero, aplicándolos en ambas etapas del proceso de cifrado, otorgando seguridad en varias capas con un espacio de clave de 2^{242} suficientemente robusto para evitar ataques de fuerza bruta (Alsaad & Hato, 2014).

Sin embargo, paulatinamente se propusieron algoritmos de doble canal para el cifrado de archivos de audio, como lo muestra (Liu, Kadir, & Li, 2016) donde hace uso de un sistema caótico multi-scroll con cuatro parámetros de control para generar un arreglo de claves utilizado en la difusión y confusión del audio, adicionalmente se integraron valores hash para calcular las condiciones iniciales del sistema usando un algoritmo SHA-256. Mediante

análisis de correlación, PSNR (Peak signal-to-noise ratio) e histogramas de frecuencias, comprobaron la eficiencia y eficacia del algoritmo propuesto.

Un año después se desarrolló un algoritmo basado en cifrado de bloques para archivos de audio con formato WAV (Waveform Audio Format) utilizando la función Tienda para la etapa de difusión, un generador de claves a partir de polinomios de Chebyshev y un método de sustitución basado en el algoritmo de Euclides con un espacio de clave final de 2^{319} haciéndolo impenetrable a los ataques de fuerza buta. Mediante análisis de correlación, PSNR, análisis de histogramas al igual que en las investigaciones ya mencionadas, se demuestra la robustez y fiabilidad del algoritmo añadiendo al abanico de pruebas un análisis de MSE (Mean Squared Error) (Albahrani, 2017).

Finalmente, en el año 2019, se propuso un sistema de cifrado de audio integrando la función circular y las ecuaciones de rotación modificadas, en el que se justificó el uso de más de un atractor caótico para fortalecer la seguridad de los algoritmos de cifrado basados en teoría del caos, debido a investigaciones recientes que han detectado vulnerabilidades en algoritmos basados en un único atractor caótico. Las pruebas que realizaron les permitieron asegurar que el algoritmo es lo suficientemente seguro para el cifrado de audio (Kordov, 2019).

6. Marco teórico conceptual

6.1. Criptografía simétrica

Una de las ramas de la criptografía o mejor, uno de los tipos de sistemas criptográficos son los llamados sistemas de criptografía de clave simétrica. Estos sistemas hacen uso de una única clave para cifrar y descifrar un texto plano, por lo que es necesario que esta clave debe ser privada (Garewal, 2020). Esto puede ser representado como (1)

$$E(P, K) = C \tag{1}$$

donde E es el algoritmo de cifrado, P es el texto plano a proteger, K es la clave privada que será utilizada para transformar la información y C es el nuevo texto plano cifrado. A su vez, este texto plano cifrado es utilizado en (2)

$$D(C, K) = P \tag{2}$$

donde D es el algoritmo de descifrado que utilizará la misma clave privada para obtener el texto plano original P.

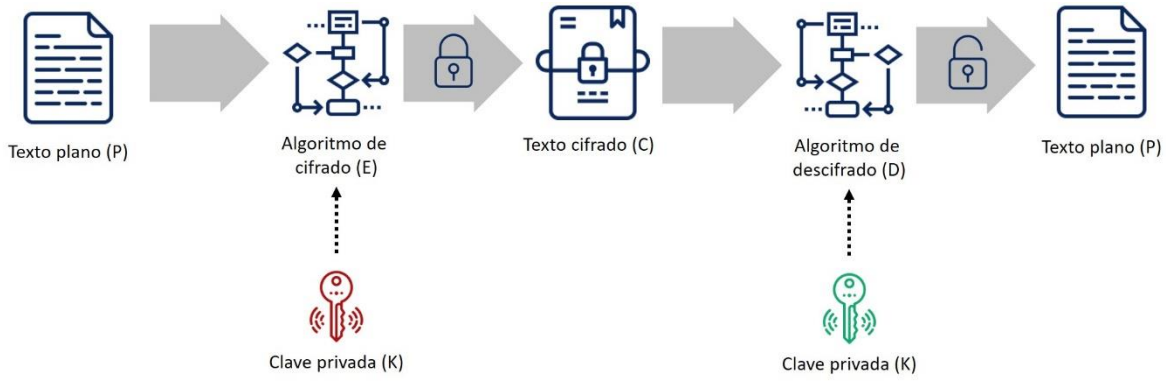

Figura 1. Proceso de cifrado y descifrado. Elaboración propia

Dentro de los algoritmos de cifrado simétrico se encuentran los de cifrado de bloque y los de cifrado de flujo. El cifrado de bloque hace uso de conjuntos de bits que serán operados en su totalidad, es decir, las operaciones se efectuarán sobre todo el bloque y no sobre los bits en particular, en cambio, el cifrado de flujo toma cada bit de forma independiente para ser operado y transformado en uno nuevo con el fin de obtener un nuevo flujo de bits cifrado (Alenezi, Alabdulrazzaq, & Mohammad, 2020).

6.2. Sistemas de cifrado de bloques

La mayoría de los sistemas de cifrado poseen dos operaciones fundamentales que estructuran el flujo y transformación de la información que se pretende cifrar, estas dos operaciones son la *confusión* y la *difusión* y determinan el nivel de seguridad que posee un algoritmo, las cuales fueron definidas por primera vez por el precursor de la criptografía (Shannon, 1949).

Confusión: está relacionada con la sustitución de la información dentro del texto plano que se cifrará y que pretende entregar

Difusión: está relacionada con la permutación o trasposición de los símbolos que componen el texto plano.

Un sistema de cifrado de bloques hace uso de texto plano expresado en bits, los cuales van a ser organizados en bloques P y serán operados para generar un nuevo bloque cifrado Q de texto plano expresado en bits. La clave K juega un papel fundamental en el proceso de cifrado ya que todas las transformaciones que se ejecutarán sobre el bloque inicial P serán dictaminadas por esta clave, por lo cual, este cifrado podría ser expresado como (3)

$$E(P, K) = C \tag{3}$$

donde E es el algoritmo de transformación de bloques aplicado.

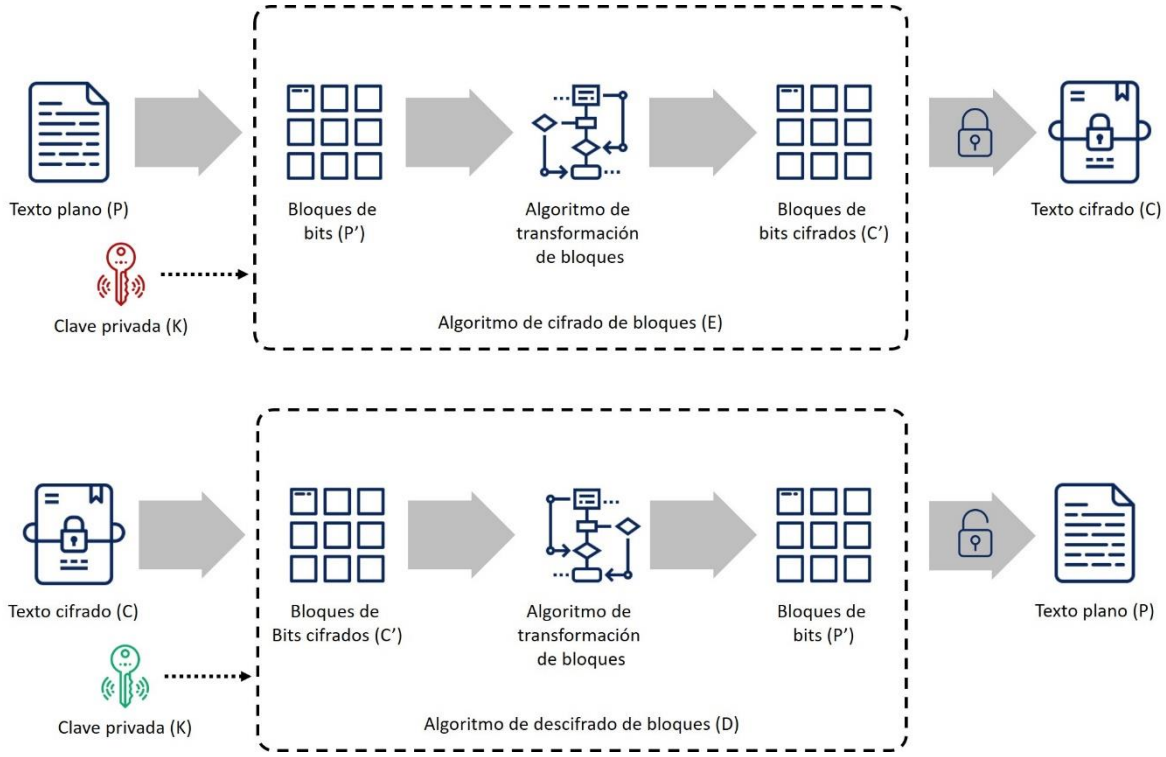

Figura 2. Proceso de cifrado y descifrado por bloques. Elaboración propia

Algunos de los sistemas de cifrado de bloques más utilizados y comúnmente conocidos son el AES (Advanced Encryption Standard) y el DES (Data Encryption Standard) (Kapoor & Pandya, 2013) donde el primer algoritmo mencionado aún es considerado seguro y virtualmente imposible de romper por ataques de fuerza bruta a diferencia del DES, el cual ya ha sido vulnerado en repetidas ocasiones por lo que ya no es recomendado su uso (Nelson, 1999).

6.3. Sistemas dinámicos no lineales

La dinámica como foco de estudio dentro de las ciencias físicas, busca comprender el movimiento o cambio de diferentes magnitudes a través del tiempo. Dentro de la dinámica pueden describirse sistemas de la mecánica clásica, cinética química, comportamientos de crecimiento biológico, etc. Sin embargo, existen sistemas que presentan dentro de su definición relaciones no lineales, estos fueron "descubiertos" durante la definición matemática del movimiento de tres cuerpos celestes, el sol, la tierra y la luna orbitando alrededor de esta, aplicando la misma teoría y métodos propuestos por Newton a través de ecuaciones diferenciales (Hadjidemetriou, 1963). Este problema no pudo ser resuelto hasta que se incluyó un análisis cualitativo al sistema, donde se responden a preguntas de estabilidad del sistema y comportamiento en términos geométricos. Fue Poincaré quién se aproximó a la solución del problema de los tres cuerpos e introdujo la posibilidad de caos en los sistemas (Chenciner, 2015), en los cuales, un sistema determinístico describe un comportamiento aperiódico que está supeditado a las condiciones iniciales y que una pequeña variación de estas provoca comportamientos diferentes del sistema sin ninguna tendencia en particular haciendo imposible su predicción a largo plazo. Estos cambios de comportamiento en la dinámica del sistema son llamados bifurcaciones y los valores de los parámetros en los que ocurren son los puntos de bifurcación. Existen tres tipos de puntos de bifurcación:

- Bifurcación de silla-nodo: se presenta cuando dos puntos fijos inversos, es decir, un punto fijo repulsor y otro atractor, colisionan y desaparecen del sistema. Se puede observar este comportamiento en la ecuación (4)

$$\dot{x} = r + x^2 \tag{4}$$

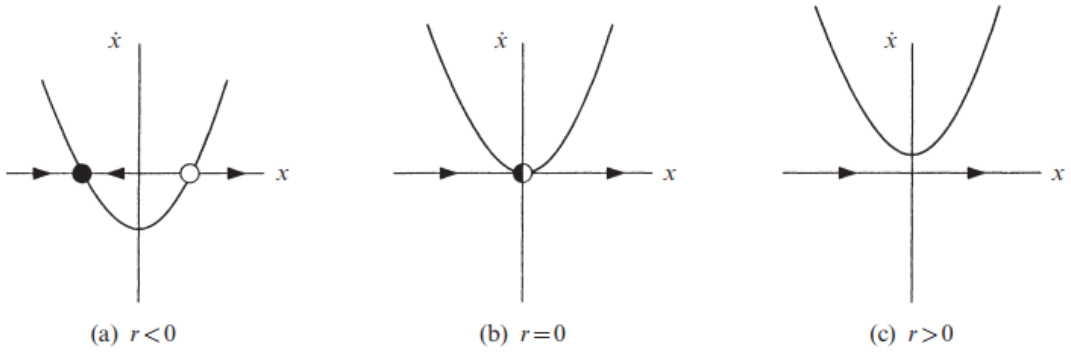

Figura 3. Bifurcación de silla-nodo. Tomado de (Strogatz, 2015)

- Bifurcación transcrítica: son puntos fijos que se perpetuán en el sistema sin importar los valores de los parámetros de control. Su comportamiento se muestra en la ecuación (5)

$$\dot{x} = rx - x^2 \tag{5}$$

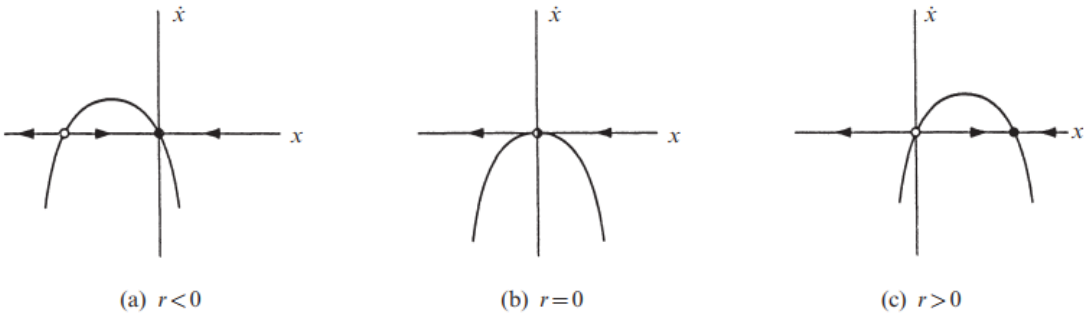

Figura 4. Bifurcación transcrítica. Tomado de (Strogatz, 2015)

- Bifurcación tridente: se presentan comúnmente en funciones simétricas, donde los puntos fijos aparecen o desaparecen de forma equivalente. En la ecuación (6) se puede apreciar este tipo de bifurcación:

$$\dot{x} = rx - x^3 \tag{6}$$

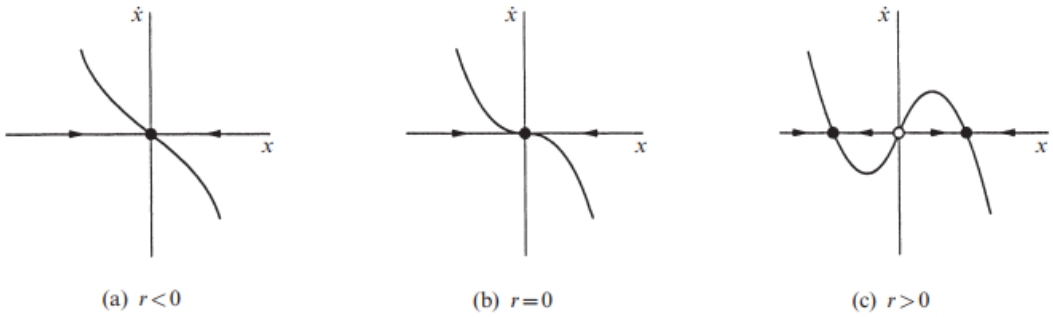

Figura 5. Bifurcación de tridente. Tomado de (Strogatz, 2015)

Estos puntos son importantes en el estudio de la no linealidad ya que son usados para manipular la estabilidad de los sistemas. Por último, la diferencia crucial del porqué los sistemas no lineales no pueden ser resueltos como los sistemas lineales (de forma analítica) es que no es posible fraccionar los sistemas no lineales en sus partes, estos deben ser tratados como un todo, por eso se han desarrollado técnicas cualitativas para comprenderlos (Strogatz, 2015).

6.4. Atractores caóticos

En 1963 Edward Lorenz mediante una simulación computarizada identificó un sistema dinámico que a simple vista no parecía tener ningún comportamiento extraño, sin embargo, sobre un amplio rango de valores de los parámetros, el comportamiento de este era extremadamente impredecible. El sistema nunca repetía exactamente un valor anterior pero siempre oscilaba dentro de una misma región, un espacio limite que contenía al sistema denominando a este un atractor caótico (Strogatz, 2015).

Las ecuaciones de Lorenz que describen el sistema son dadas por (7)

$$\dot{x} = \sigma(y - x)\dot{y} = rx - y - xz\dot{z} = xy - bz \qquad (7)$$

Donde $\sigma, r, b > 0$ son parámetros de control.

Lorenz descubrió que para los valores $\sigma = 10,\ r = 28,\ b = \frac{8}{3}$ el sistema presenta un comportamiento caótico (Guckenheimer & Williams, 1979). La figura (6) muestra la dinámica del sistema para estos valores:

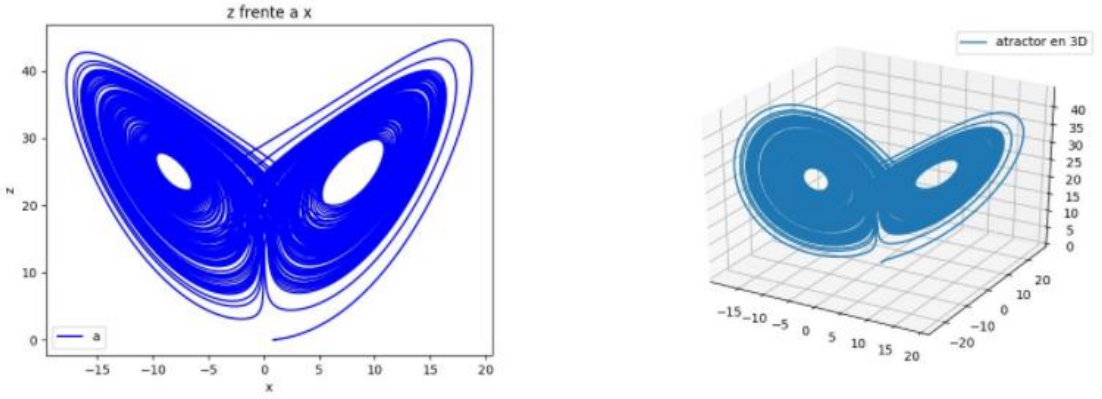

Figura 6. Diagrama de simulación del atractor de Lorenz. Tomado de ("Sistemas caóticos y teoría del caos, una breve introducción - NUSGREM," n.d.)

Los parámetros son los que determinan el comportamiento que tendrá el sistema y su grado de pseudoaleatoriedad.

Posteriormente, Michel Hénon propuso investigar al sistema de ecuaciones de Lorenz mediante el uso de un modelo discreto, debido a que estos son más sencillos, y se pueden simular con resultados dentro de un rango mucho más extenso por su naturaleza iterativa.

El atractor de Hénon está definido por medio de las ecuaciones dadas en (8)

$$x_{n+1} = y_n + 1 - ax_n^2 y_{n+1} = bx_n \tag{8}$$

Donde a, b son parámetros de control. Este atractor surgió de un proceso de transformación creativo del sistema de Lorenz, tomando una región del espacio y "doblándola" mediante los parámetros de control (Strogatz, 2015).

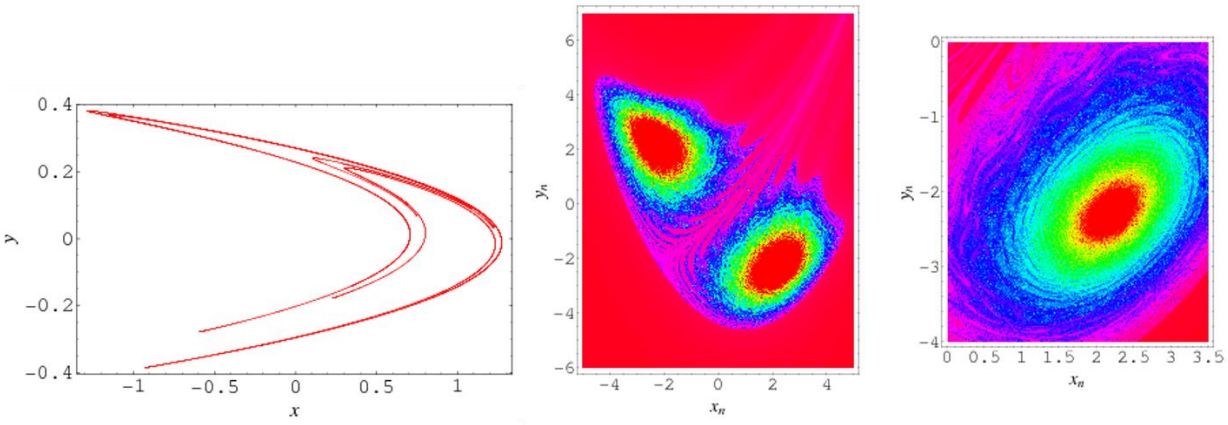

Figura 7. Diagramas de simulación del atractor de Hénon ("Hénon Map -- from Wolfram MathWorld," n.d.)

Los atractores de Hénon y Lorenz, presentan grandes similitudes, como los dos puntos fijos mostrados en las figuras (6) y (7), sin embargo, tienen una diferencia crucial en cuanto a la estabilidad del sistema ya que el sistema de Hénon describe valores que tienden al infinito en algunas de sus trayectorias.

Con base en los descubrimientos hechos por Lorenz y Michel Hénon, se llevaron a cabo más estudios que finalmente dieron origen a lo que se conoce como un atractor caótico. Más adelante se encontraron nuevos sistemas caóticos, incluso sistemas unimodales como la función Tienda descrita por (9)

$$x_{i+1} = \{\frac{x_i}{\alpha} \qquad si\ x\ \in [0,\alpha]\ \frac{1-x_i}{1-\alpha} \qquad si\ x\ \in (\alpha,1] \tag{9}$$

Este es un sistema iterativo discreto con un único parámetro de control α y una condición inicial x_i. La función tienda es un sistema extremadamente sencillo matemáticamente hablando, pero presenta comportamientos caóticos cuando $\alpha = 0.5$.

La figura (8) muestra la dinámica de la función Tienda con x_{i+1} en el eje de las ordenadas y x en el de las abscisas, donde se puede apreciar que forma un triángulo asemejando una tienda de campaña, razón por la que lleva este nombre (Li, 2004).

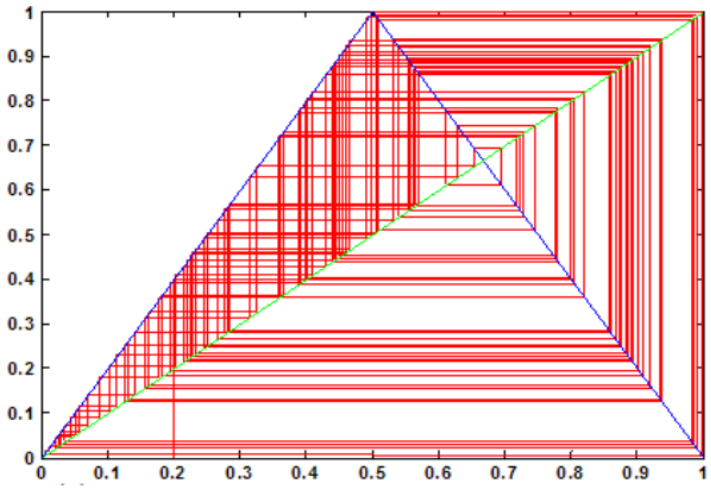

Figura 8. Diagrama de Cobweb de la función Tienda. Tomado de (Tian, 2015)

6.5. Caos en el contexto de la criptografía

Los sistemas caóticos presentar tres características fundamentales (Strogatz, 2015):

- Dependencia sensible a condiciones iniciales: pequeños cambios en los valores iniciales generan grandes diferencias en el comportamiento del sistema a través del tiempo.
- Determinista: a pesar de contener comportamientos irregulares dentro de un espacio definido, estos pueden ser reproducidos perfectamente si las condiciones iniciales y

parámetros de control son los mismos, esto quiere decir que el comportamiento irregular del sistema viene de la no linealidad del sistema y no de fuerzas externas no definidas.

- Cambios cualitativos en las características de las soluciones: indican que el sistema puede presentar variaciones en el comportamiento de las bifurcaciones, presentando atractores, repulsores, puntos fijos u orbitas que no se existen para otras condiciones.

Teniendo en cuenta estas características, es posible realizar una comparación de las propiedades caóticas y las propiedades criptográficas.

Tabla 1. Comparación entre propiedades caóticas y criptográficas. Tomado de (Kocarev & Lian, 2011)

Propiedad caótica	Propiedad criptográfica	Descripción
Ergodicidad	Confusión	La salida posee la misma distribución para cualquier entrada
Sensibilidad a condiciones iniciales y parámetros de control	Difusión del texto plano o bloques de datos a causa de la clave secreta	Pequeños cambios en las entradas causan grandes cambios en las salidas
Comportamiento determinista	Pseudoaleatoriedad determinista	Un proceso determinístico puede generar valores pseudoaleatorios.
Complejidad estructural	Complejidad algorítmica	Un proceso simple con gran complejidad

Entonces, es posible apreciar varias ventajas de la implementación de sistemas caóticos dentro de sistemas criptográficos, por ejemplo, el uso de números reales como parámetros de control y condiciones iniciales, así mismo, espacios de fase dentro de un subconjunto de los

números reales, a esto se le suma el hecho de tener sistemas altamente sensibles a las condiciones iniciales, conservando todas las propiedades determinísticas necesarias en la criptografía. Así pues, la criptografía clásica utiliza la aritmética como principal herramienta para la transformación de la información, en contraste con la criptografía basada en caos, la cual hace uso de sistemas complejos pero computacionalmente sencillos de iterar que expresan características muy robustas en las ciencias criptográficas. Adicionalmente, la tendencia de aumento de la información y el tamaño de la información a procesar hace del caos una herramienta ideal para el tratamiento de grandes conjuntos de datos o mejor, archivos de gran tamaño (Kocarev & Lian, 2011).

6. Alcances y limitaciones

Este proyecto pretende diseñar y desarrollar un algoritmo de cifrado de audio haciendo uso de sistemas caóticos como principal herramienta debido a sus propiedades de pseudoaleatoriedad, sensibilidad a condiciones iniciales, determinismo y simpleza algorítmica, para ello, se requiere utilizar un formato de audio especifico, por lo que no podrán ser tratados los múltiples formatos existentes hasta el momento.

Adicionalmente, se llevarán a cabo pruebas de rendimiento y seguridad utilizadas en la literatura científica para comprobar la eficiencia y efectividad del algoritmo frente a sistemas de cifrado de bloques tradicionales. El algoritmo será ejecutado en tres equipos con distintas características computacionales para llevar a cabo pruebas de cifrado y descifrado de archivos de audio de múltiples tamaños, abarcando audios de corta y larga duración, sin embargo, esto será determinado por las características de los equipos que se dispongan para realizar estas pruebas.

7. Metodología

En la figura (9), se muestra el marco metodológico que se aplicará en el desarrollo de este trabajo de investigación, donde, inicialmente se realizará una revisión de investigaciones y trabajos científicos recientes con enfoques y objetivos similares al propuesto en este proyecto, con enfoques similares al propuesto en este proyecto, con el fin de definir los elementos propios a utilizar tales como: atractores caóticos y sus parámetros de control, técnicas criptográficas, mecanismos de validación y verificación de resultados, formato de los archivos de audio. A continuación, se ajustará la metodología de trabajo a un desarrollo cíclico en donde se establecerán las herramientas de desarrollo a utilizar para posteriormente plantear e implementar el sistema de cifrado, realizando los ajustes pertinentes en cada iteración hasta cumplir con las pruebas de seguridad y desempeño para validar la propuesta.

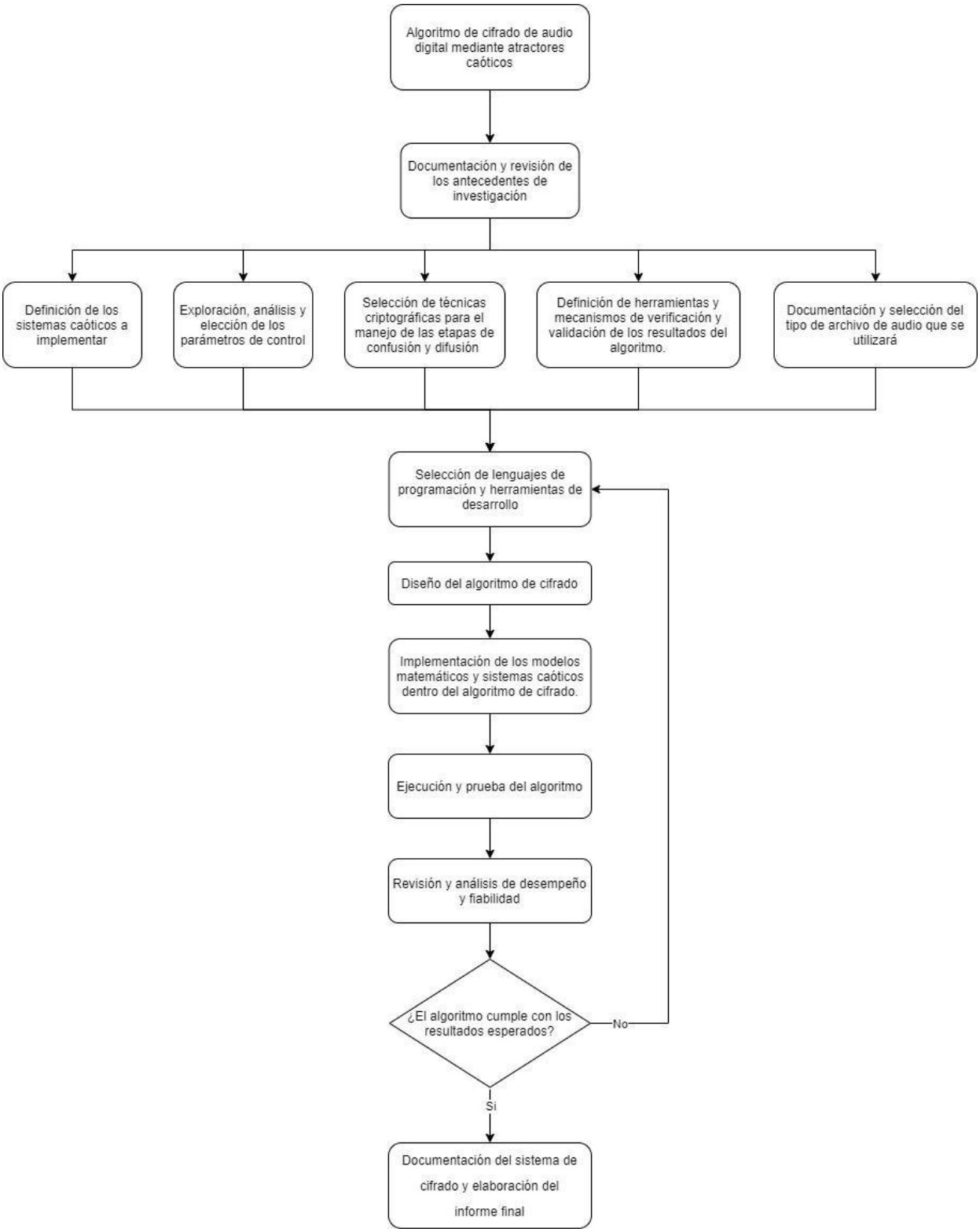

Figura 9. Diagrama de metodología de investigación. Elaboración propia

8. Cronograma

La figura (10) presenta el cronograma de actividades que regirá el desarrollo de este proyecto de investigación.

Figura 10. Diagrama de Gantt – Cronograma de investigación. Elaboración propia usando ("Chaos Cryptographic Algorithm | TeamGantt," n.d.)

9. Presupuesto

En las tablas 2, 3 y 4, se describen los recursos y costos requeridos para el desarrollo del proyecto.

- Director de proyecto: tendrá como responsabilidad gestionar y liderar el proyecto para su consecución, facilitando los medios técnicos y teóricos necesarios para cumplir con las tareas definidas en el tiempo establecido dentro del cronograma.
- Ingeniero de sistemas: encargado del diseño e implementación del proyecto de investigación, así como de los recursos documentales que se presentarán una vez se haya llegado a los resultados esperados.

Tabla 2. Costos referentes a recursos humanos. Elaboración propia

Recurso	Cantidad	Costo	Tiempo (días)	Total
Director de proyecto	2	$7.500.000	120	$60.000.000
Ingeniero de sistemas	1	$5.000.000	120	$20.000.000
			Total	$80.000.000

Tabla 3. Costos referentes a recursos físicos. Elaboración propia

Recurso	Cantidad	Costo	Total
Computadores	3	$2.500.000	$7.500.000
Recursos de papelería, servicios y otros gastos		$1.500.000	$1.500.000
		Total	$9.000.000

Tabla 4. Costos totales del proyecto. Elaboración propia

Recurso	Costo
Recursos humanos	$80.000.000
Recursos físicos	$9.000.000
Total	$89.000.000

10. Bibliografía

ACSC Annual Cyber Threat Report. (2019).

Albahrani, E. A. (2017). A new audio encryption algorithm based on chaotic block cipher. *2017 Annual Conference on New Trends in Information and Communications Technology Applications, NTICT 2017*, 22–27. https://doi.org/10.1109/NTICT.2017.7976129

Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q. (2020). Symmetric Encryption Algorithms: Review and Evaluation study. In *International Journal of Communication Networks and Information Security (IJCNIS* (Vol. 12).

Alsaad, S., & Hato, E. (2014). A Speech Encryption based on Chaotic Maps. *International Journal of Computer Applications*, *93*, 19–28. https://doi.org/10.5120/16203-5488

Andersen, K. G., Rambaut, A., Lipkin, W. I., Holmes, E. C., & Garry, R. F. (2020). The proximal origin of SARS-CoV-2. *Nature Medicine*, *26*(4), 450–452. https://doi.org/10.1038/s41591-020-0820-9

Babu, A. M., & Singh, K. J. (2013). Performance evaluation of chaotic encryption technique. *American Journal of Applied Sciences*, *10*(1), 35–41. https://doi.org/10.3844/ajassp.2013.35.41

Ben Ayed, A., Ben Halima, M., & Alimi, A. M. (2015). Big data analytics for logistics and transportation. *2015 4th IEEE International Conference on Advanced Logistics and Transport, IEEE ICALT 2015*, 311–316. https://doi.org/10.1109/ICAdLT.2015.7136630

Chaos Cryptographic Algorithm | TeamGantt. (n.d.). Retrieved November 14, 2020, from https://prod.teamgantt.com/gantt/schedule/?ids=2408125#ids=2408125&user=12498315&custom=&company=&hide_completed=false&date_filter=&color_filter=

Chenciner, A. (2015). Poincaré and the three-body problem. *Progress in Mathematical Physics*, *67*, 51–149. https://doi.org/10.1007/978-3-0348-0834-7_2

Ganesh Babu, S., & Ilango, P. (2013). Higher dimensional chaos for Audio encryption. *Proceedings of the 2013 IEEE Symposium on Computational Intelligence in Cyber Security, CICS 2013 - 2013 IEEE Symposium Series on Computational Intelligence, SSCI 2013*, 52–58. https://doi.org/10.1109/CICYBS.2013.6597206

Ganesh Sekar, J., & Arun, C. (2020). Journal of Critical Reviews COMPARATIVE PERFORMANCE ANALYSIS OF CHAOS BASED IMAGE ENCRYPTION TECHNIQUES. *Journal of Critical Reviews*, 1138. https://doi.org/10.31838/jcr.07.09.209

Garewal, K. S. (2020). Symmetric Encryption. In *Practical Blockchains and Cryptocurrencies* (pp. 29–36). https://doi.org/10.1007/978-1-4842-5893-4_3

Gnanajeyaraman, R., & Prasadh, K. (2009). Audio encryption using higher dimensional chaotic map. In *International Journal of Recent Trends in Engineering* (Vol. 1).

Guckenheimer, J., & Williams, R. F. (1979). Structural stability of Lorenz attractors. *Publications Mathématiques de L'Institut Des Hautes Scientifiques*, *50*(1), 59–72. https://doi.org/10.1007/BF02684769

Habutsu, T., Nishio, Y., Sasase, I., & Mori, S. (1991). A secret key cryptosystem by iterating a chaotic map. *Lecture Notes in Computer Science (Including Subseries Lecture Notes*

in Artificial Intelligence and Lecture Notes in Bioinformatics), 547 LNCS, 127–140. https://doi.org/10.1007/3-540-46416-6_11

Hadjidemetriou, J. D. (1963). Two-body problem with variable mass: A new approach. *Icarus*, *2*, 440–451. https://doi.org/https://doi.org/10.1016/0019-1035(63)90072-1

Hénon Map -- from Wolfram MathWorld. (n.d.). Retrieved November 6, 2020, from https://mathworld.wolfram.com/HenonMap.html

Jia, X. (2010). Image encryption using the Ikeda map. *Proceedings - 2010 International Conference on Intelligent Computing and Cognitive Informatics, ICICCI 2010*, 455–458. https://doi.org/10.1109/ICICCI.2010.124

Kapoor, B., & Pandya, P. (2013). Data Encryption. In *Cyber Security and IT Infrastructure Protection* (pp. 29–73). https://doi.org/10.1016/B978-0-12-416681-3.00002-1

Kocarev, L., & Lian, S. (Eds.). (2011). *Chaos-Based Cryptography*. https://doi.org/10.1007/978-3-642-20542-2

Kordov, K. (2019). A Novel Audio Encryption Algorithm with Permutation-Substitution Architecture. *Electronics*, *8*, 530. https://doi.org/10.3390/electronics8050530

Li, C. (2004). A new method of determining chaos-parameter-region for the tent map. *Chaos, Solitons & Fractals*, *21*(4), 863–867. https://doi.org/https://doi.org/10.1016/j.chaos.2003.12.025

Lian, S., & Chen, X. (2011). Traceable content protection based on chaos and neural networks. *Applied Soft Computing Journal*, *11*(7), 4293–4301. https://doi.org/10.1016/j.asoc.2010.05.033

Liu, H., Kadir, A., & Li, Y. (2016). Audio encryption scheme by confusion and diffusion based on multi-scroll chaotic system and one-time keys. *Optik*, *127*(19), 7431–7438. https://doi.org/10.1016/j.ijleo.2016.05.073

Masuda, N. (1999). A chaotic cryptosystem based on a finite-state baker's map and its security analysis. *Proc. NOLTA'99*. Retrieved from http://ci.nii.ac.jp/naid/10022336370/en/

National Cyber Security Centre, U. K., Homeland Security, U. S. D., & Cybersecurity and Infrastruture Security, A. (2020). *Advisory: COVID-19 exploited by malicious cyber actors*. Retrieved from https://www.ncsc.gov.uk/files/Final Joint Advisory COVID-19 exploited by malicious cyber actors v3.pdf

Nelson, M. (1999). 56-bit DES algorithm broken in record time. *Computers & Security*, *18*(2), 149–150.

Paar, C., & Pelzl, J. (2010). Understanding Cryptography. In *Understanding Cryptography*. https://doi.org/10.1007/978-3-642-04101-3

Radha, N., & Venkatesulu, M. (2012). A Chaotic Block Cipher for Real-Time Multimedia. *Journal of Computer Science*, *8*, 994–1000. https://doi.org/10.3844/jcssp.2012.994.1000

Shannon, C. E. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal*, *28*(4), 656–715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

Sistemas caóticos y teoría del caos, una breve introducción - NUSGREM. (n.d.). Retrieved November 5, 2020, from https://nusgrem.es/sistemas-caoticos-y-teoria-del-caos/

Strogatz, S. (2015). *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering — Steven Strogatz* (Second edi). Retrieved from http://www.stevenstrogatz.com/books/nonlinear-dynamics-and-chaos-with-applications-to-physics-biology-chemistry-and-engineering

Thein, N., Nugroho, H. A., Adji, T. B., & Mustika, I. W. (2018). Comparative Performance Study on Ordinary and Chaos Image Encryption Schemes. *Proceedings - 2017 International Conference on Advanced Computing and Applications, ACOMP 2017*, 122–126. https://doi.org/10.1109/ACOMP.2017.25

Tian, D. (2015). Particle swarm optimization with chaotic maps and Gaussian mutation for function optimization. *International Journal of Grid and Distributed Computing*, *8*, 123–134. https://doi.org/10.14257/ijgdc.2015.8.4.12

Wong, K. W., Kwok, B. S. H., & Yuen, C. H. (2009). An efficient diffusion approach for chaos-based image encryption. *Chaos, Solitons and Fractals*, *41*(5), 2652–2663. https://doi.org/10.1016/j.chaos.2008.09.047

Zhang, X., & Min, L. (2005). A generalized chaos synchronization based encryption algorithm for sound signal communication. *Circuits, Systems, and Signal Processing*, *24*(5 SPEC. ISS.), 535–548. https://doi.org/10.1007/s00034-005-2405-8