UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

REDES NEURONALES PARA LA DESENCRIPTACIÓN DE MENSAJES CODIFICADOS CON ATRACTORES CAÓTICOS.

Sergio Duvan Nuñez Sanchez

Universidad Distrital Francisco José de Caldas

Facultad de Ingeniería

Ingeniería de Sistemas

Bogotá D.C.

2022

REDES NEURONALES PARA LA DESENCRIPTACIÓN DE MENSAJES CODIFICADOS CON ATRACTORES CAÓTICOS.

Sergio Duvan Nuñez Sanchez

Anteproyecto de grado presentado como requisito parcial para optar al título de Ingeniero de Sistemas

Trabajo que se enmarca en el proyecto de investigación: *Modelos de seguridad informática basados en herramientas matemáticas e inteligencia Artificial*. Institucionalizado por el grupo de investigación ComplexUD ante el centro de investigaciones y desarrollo científico CIDC.

Directora:

Dr. Luz Deicy Alvarado Nieto

Universidad Distrital Francisco José de Caldas

Facultad de Ingeniería

Ingeniería de Sistemas

Bogotá D.C.

2022

Contenido

1. Introducción

La intención de este proyecto es plantear un modelo de encriptación que utilice redes neuronales en conjunto con atractores caóticos con fin de realizar encriptación de texto, para ello se utilizará un texto en ASCII obteniendo 256 representaciones de distintos caracteres con el fin de construir bloques y encriptarlos a través del entrenamiento de redes neuronales, mediante la simulación de una función que asocie la generación pseudoaleatoria de caracteres y envíe los bloques bajo una compresión basada en frecuencia utilizando códigos de Huffman, obteniendo un único mensaje, el cual será enviado al receptor junto a la semilla de un atractor caótico utilizada como parte de la llave de este mensaje encriptado.

La importancia de este trabajo radica en consolidar una propuesta actual y original, enfocada a la seguridad de la información, la cual cumpla con estándares de seguridad acordes a los reportados en trabajos recientes que utilicen principios matemáticos y de inteligencia artificial similares a los que se planea utilizar en esta propuesta.

2. Planteamiento del problema

La necesidad de nuevos modelos de encriptación ha sido un desafío constante a lo largo de la historia y sus avances han evolucionado simultáneamente con la tecnología, por otro lado, el resurgimiento de las redes neuronales las hace eje de nuevos modelos que permiten encontrar soluciones a problemáticas actuales. Así mismo, los atractores caóticos por sus propiedades, tales como determinismo (no son probabilísticos), alta sensibilidad a las condiciones iniciales, transitividad topológica y densidad de puntos periódicos son potencialmente útiles para la generación de secuencias cifrantes, en tal dirección, el propósito de este proyecto es fusionar elementos de redes neuronales y teoría del caos para consolidar un algoritmo criptográfico enfocado a la encriptación de cadenas de texto.

El paradigma planteado por el surgimiento de la computación cuántica ha generado preocupación sobre los métodos actuales de encriptación, pues la capacidad de procesamiento paralelo de esta tecnología es tan alta que pueden hacer ver a las estructuras actuales de encriptación vulnerables ante posibles ataques (Bernstein, Introduction to post-quantum cryptography, 2009). Los atractores caóticos junto con las redes neuronales son una alternativa viable para disminuir tales

riesgos, el presente trabajo busca dar respuesta a la siguiente incógnita: ¿cómo aprovechar las redes neuronales y los atractores caóticos para proponer un modelo criptográfico enfocado a la seguridad de textos?

3. Justificación

La criptografía se ha convertido en una de las mayores prioridades tras el surgimiento de los computadores cuánticos, debido a la capacidad de superar en tiempos aceptables las encriptaciones convencionales bajo algoritmos de naturaleza cuántica ya que los modelos de criptografía post cuántica e híbridos de tipo simétrico que utilizan funciones hash criptográficas presentan una baja vulnerabilidad, excluyendo el algoritmo de Grover (Bernstein, Grover vs. McEliece, 2010).

La inteligencia artificial, gracias al boom en la última década con las redes neuronales, se ha convertido en herramienta viable para generar nuevos modelos criptográficos, la cual se puede combinar con atractores caóticos. Este enfoque ha sido abordado en varios trabajos (Bevi, 2021) (Bigdeli, 2012) (F. Yang, 2020) (Ilya Sutskever, 2011) (Z. Man, 2011), sin embargo, los autores consultados no implementaron un proceso de aprendizaje en la red, solamente se apoyaron en la naturaleza caótica implícita de las redes neuronales, hecho que ignora la verdadera utilidad de las mismas, en este sentido, el propósito de este trabajo es diseñar un modelo de encriptación basado en el aprendizaje de redes neuronales caóticas aplicado a la seguridad de textos, tomando como base trabajos encontrados en la literatura reciente pero implementando aprendizaje en la red.

4. Objetivos

4.1. Objetivo general

Diseñar un modelo criptográfico enfocado a textos, que combine el uso de atractores caóticos y redes neuronales.

4.2. Objetivos específicos

- Emplear atractores caóticos para generar secuencias pseudoaleatorias utilizadas en el proceso criptográfico.
- Asociar secuencias pseudoaleatorias con caracteres determinados por su representación

binaria, a fin de utilizarlos como entradas de la red neuronal.

- Entrenar redes neuronales para lograr un modelo de asociación de grupos de caracteres con la representación de secuencias obtenidas con los atractores caóticos seleccionados.
- Representar las redes neuronales matricialmente y reducir su tamaño para realizar el envío.
- Aplicar indicadores de seguridad y desempeño para validar el modelo propuesto.

5. Estado del arte

En la literatura científica se pueden encontrar diversos artículos que mezclan los atractores caóticos con redes neuronales con el fin de desarrollar nuevos modelos de encriptación, entre ellos se encuentra *Cryptography based on delayed chaotic neural networks*, donde utilizan redes neuronales caóticas de Hopfield para generar secuencias binarias que encripta el texto sin formato, sin embargo, estas redes no utilizan aprendizaje más allá del comportamiento caótico que se puede inducir del entrenamiento de redes neuronales (Cao, 2006).

Por otra parte, como se evidencia en *Double image encryption algorithm based on neural network and chaos*, se propone un algoritmo de cifrado para imágenes basado en una red neuronal convolucional junto a difusión adaptativa dinámica, la propuesta es enfocada a doble canal (digital/ óptico), garantizando la seguridad de la imagen alusiva a cada canal, partiendo de un atractor caótico como un núcleo de convolución para controlar la operación de codificación de dos imágenes las cuales fusionan en partes diferentes según la cantidad de información contenida. Los autores reportan que la encriptación del canal digital tiene mejor paralelismo y mayor eficiencia de cifrado, mientras que el óptico tiene mayor complejidad computacional y mejor confiabilidad de cifrado (Z. Man, 2011).

En el trabajo de (Bigdeli, 2012), el cual se basa en redes neuronales caóticas, los autores utilizan dos capas compuestas por tres neuronas, de las cuales, una de ellas aplica uno de los atractores caóticos Chua, Lorenz o Lu, además de un atractor basado en permutaciones, cuyos

tres valores son las componentes RGB de una imagen, repitiendo el proceso hasta que la información sea difuminada y exista una permutación tridimensional de esta misma, lo cual les garantiza un algoritmo robusto siendo un modelo que aprovecha al máximo el uso de atractores caóticos.

De otra parte, en la propuesta de (Adel A. El-Zoghab, 2013), utilizaron Tree Parity Machines (TPM) para generar una clave secreta sobre el canal público en la salida de cada partner. En este modelo la red es empleada con varios propósitos, de un lado, la red neuronal con mapa logístico caótico es utilizada para un proceso criptografico, esto genera los bits de salida que se aprenderán, mientras que una red neuronal de regresión general (GRNN) es empleada para el proceso de cifrado y descifrado a lo largo de tres capas, donde dividieron los datos de entrada en 3 bits y 8 bits como salida. Así mismo, una red neuronal de retropropagación de entrenamiento actuó como clave pública, mientras que el álgebra booleana como clave privada. Finalmente, usaron la red neuronal caótica de Hopfield, con retardo variable en el tiempo, para generar una secuencia binaria de texto sin formato, considerada como una función de cambio aleatorio para el mapa caótico.

En la misma dirección, partiendo de la red neuronal caótica para el cifrado de señales de Yen y Guo, en *Cryptanalysis of a Chaotic Neural Network Based Multimedia Encryption Scheme,* los autores evalúan la seguridad de un esquema de cifrado basado en redes neuronales caóticas, donde señalan que no es seguro desde el punto de vista criptográfico, pues puede romperse fácilmente mediante ataques de texto sin formato conocido, además de sobreestimarse mucho su seguridad contra el ataque de fuerza bruta. Muestran algunos experimentos para respaldar los resultados dados en este documento y formulan una propuesta de mejora al esquema de encriptación evaluado (L. Chengquing, 2004).

Así mismo, en el trabajo de (F. Yang, 2020) titulado: *An Image Encryption Algorithm Based on BP Neural Network and Hyperchaotic System,* proponen un algoritmo de compresión y encriptación de imágenes basado en un sistema hipercaótico memristivo de orden fraccional y una red neuronal Back Propagation (BP), con la cual comprimen los valores de los píxeles de la imagen y utilizan las secuencias caóticas del sistema hipercaótico memristivo de orden fraccional para difundir los valores de los píxeles.

También *en Artificial neural network based chaotic general network based chaotic generator for cryptology* los autores aprovechan las propiedades de los sistemas caóticos y la dinámica del circuito de Chua, proponiendo una red neuronal artificial (ANN) entrenada con varias estructuras usando diferentes algoritmos de aprendizaje. Para entrenar la ANN, utilizaron 24 conjuntos diferentes, incluidas las condiciones iniciales del circuito de Chua, y cada uno de ellos constaba de aproximadamente 1800 datos de entrada y salida. Los autores afirman, de acuerdo a los resultados experimentales, que un perceptrón multicapa (MLP) feed-forward, entrenado con el algoritmo de retropropagación de regulación Bayesiana, constituye una buena estrategia de encriptación (Kenan, 2010).

Con el mismo enfoque se destacan los trabajos de (Burak, 2015) y (T. Graham, 2019) titulados *Parallelization of an Encryption Algorithm Based on a Spatiotemporal Chaotic System and a Chaotic Neural Network* y *Chaotic Encryption Algorithm With Key Controlled Neural Networks for Intelligent Transportation Systems, Graham R. W. Thoms* respectivamente, en el primero presentan los resultados de paralelizar un cifrado de bloques basado en un sistema caótico espaciotemporal y una red neuronal caótica, mientras que en el segundo presentan una aplicación directa de un algoritmo de encriptación de imágenes basado en el atractor caótico de Lorenz y en la novedosa red neuronal de campo finito controlada por clave, denominado ChaosNet, que utiliza redes neuronales controladas por claves caóticas para la integración con las unidades de carretera de sistemas de transporte inteligente (ITS).

Finalmente, en el trabajo de (Bevi, 2021) denominado *Design of a novel chaotic neural network based encryption system for security applications,* diseñan una red neuronal caótica para proponer un algoritmo de cifrado y descifrado fundamentado en un mecanismo de encadenamiento de bloques de cifrado apta para una amplia gama de entradas, la red funciona con caracteres basados en UTF-8. Este trabajo es base para la elaboración de la presente propuesta.

6. Marco teórico

6.1 Criptografía

La Criptografía es el conjunto de disciplinas que abarcan la teoría de la información, la teoría de códigos, la comprensión de la información, el envío de datos, la teoría de números, la

probabilidad y hasta el diseño de hardware y algoritmia. Esta facilita actualmente las compras en línea, las firmas digitales, elecciones y otro gran número de aplicaciones. (Plaza, 2021)

La criptografía es una disciplina con fundamento matemático apoyada en ciencias de la computación, cuyo propósito es hacer ininteligible la información mediante la aplicación de algoritmos, usando una o más claves (Maiorano, 2009)

Los algoritmos criptográficos se clasifican así:

- Criptografía simétrica: Se tiene en este modelo que tanto emisor como receptor comparten una misma clave que sirve tanto para cirfrar como decifrar. Como cada emisor y receptor requieren una clave para comunicarse, para n usuarios, se necesitan C(n,2) claves en total. Además, requiere un canal seguro para establecer la clave por primera vez. Estos algoritmos radican su fuerza en múltiples iteraciones o tamaños de clave muy grandes. (Plaza, 2021) Algunos de estos algoritmos son: Twofish, Serpent, AES (Rijndael), Camellia, Salsa20, ChaCha20, Blowfish, CAST5, Kuznyechik, RC4, DES, 3DES, Skipjack, Safer, and IDEA. (Wikipedia, Symmetric-key algorithm, 2022)

- Criptografía asimétrica: En este modelo no se asume la existencia de un canal seguro entre emisor y receptor, y su estructura consiste en dos componentes: una clave pública y una clave privada. (Plaza, 2021) algunos ejemplos de estos algoritmos son: El protocolo de llave de Diffie–Hellman, DSS (Digital Signature Standard), que incorpora el algoritmo de firma digital, ElGamal, criptografía de curvas elípticas y de curvas elípticas con firma digital (ECDSA), también se tiene las curvas elípticas de Diffie–Hellman (ECDH), Ed25519 y Ed448 (EdDSA), X25519 y X448 (ECDH/EdDH), Criptosistemas de Paillier y algoritmos de encriptación RSA. (Wikipedia, Public-key cryptography, 2022)

- Sin uso de claves: en este campo se evidencia la aplicación de hashing, el cual por medio de estrategias matemáticas transforma la información de entrada en otra estructura de datos fija (Donohue, 2014)

6.2 Compresión de datos por Huffmann

Este algoritmo es un algoritmo de creación de un árbol binario que almacena los datos aprovechando la entropía de un mensaje para poder determinar la cadena más apropiada a utilizar para representar cada dato presente en el mensaje. Esto reduce el espacio utilizado por el mensaje, el algoritmo consiste en los siguientes pasos:

1. Se crean varios árboles, uno por cada símbolo del alfabeto, consistiendo cada árbol en un nodo sin hijos, etiquetado cada uno con su símbolo asociado y su frecuencia de aparición.

2. Se toman los dos árboles de menor frecuencia, y se unen creando un nuevo árbol. La etiqueta de la raíz será la suma de las frecuencias de las raíces de los dos árboles que se unen, cada uno de estos árboles será un hijo del nuevo árbol. También se etiquetan las dos ramas del nuevo árbol: con un 0 la de la izquierda, y con un 1 la de la derecha.

3. Se repite el paso 2 hasta que sólo quede un árbol con el cual se puede conocer el código asociado a un símbolo, así como obtener el símbolo asociado a un determinado código.

Para obtener el código asociado a un símbolo se debe proceder del siguiente modo:

a. Comenzar con un código vacío.

b. Iniciar el recorrido del árbol en la hoja asociada al símbolo.

c. Comenzar un recorrido del árbol hacia arriba.

d. Cada vez que se suba un nivel, añadir al código la etiqueta de la rama que se ha recorrido.

e. Tras llegar a la raíz, invertir el código.

f. El resultado es el código Huffman deseado.

Para obtener un símbolo a partir de un código se debe hacer lo siguiente:

i. Comenzar el recorrido del árbol en la raíz de éste.

ii. Extraer el primer símbolo del código a descodificar.

iii. Descender por la rama etiquetada con ese símbolo.

iv. Volver al paso ii hasta que se llegue a una hoja, que será el símbolo asociado al código.

En la práctica, casi siempre se utiliza el árbol para obtener todos los códigos de una sola vez; luego se guardan en tablas y se descarta el árbol. (Wikipedia, Algoritmo de Huffman, 2022)

6.3 Redes neuronales

Las Redes Neuronales están inspiradas en el funcionamiento del cerebro el cual está compuesto por billones de neuronas interconectadas. Constan de unidades de procesamiento que intercambian datos o información con el fin de reconocer patrones, incluyendo imágenes, manuscritos y secuencias de tiempo, teniendo capacidad de aprender y mejorar su funcionamiento. Una clasificación de los modelos de redes neuronales, de acuerdo a su similitud con la realidad biológica, es (Jones, 2019):

- El modelo de tipo biológico. Este comprende las redes que tratan de simular los sistemas neuronales biológicos, así como las funciones auditivas o básicas de la visión.
- El modelo dirigido a aplicación. Este modelo no tiene por qué guardar similitud con los sistemas biológicos. Su arquitectura está fuertemente ligada a las necesidades de las aplicaciones para la que es diseñada.

Algunas definiciones para redes neuronales, encontradas en la literatura, son:

- Un sistema de computación compuesto por un gran número de elementos simples, elementos de procesos muy interconectados, los cuales procesan información por medio de su estado dinámico como respuesta a entradas externas (Isasi Viñuela & Galván León, 2004).
- Redes neuronales artificiales son redes interconectadas masivamente en paralelo de elementos simples (usualmente adaptativos) y con organización jerárquica, las cuales intentan interactuar con los objetos del mundo real del mismo modo que lo hace el

sistema nervioso biológico (Basualdo, 2001).

Las Redes Neuronales Artificiales, se inspiran en la bilogía misma del cerebro humano, tratando de modelar la neurona y demás funciones cognitivas, teniendo propiedades propias como el aprender de la experiencia cambiando su comportamiento en función del entorno para, a partir de un conjunto de entradas, obtener un conjunto de salidas consistentes; generalizar ejemplos previos y abstraer características de la esencia de un conjunto de entradas que aparentemente no presentan aspectos comunes o relativos (Basogain, 2008), razón por la cual son consideradas una herramienta útil para aplicaciones en diversas áreas del conocimiento, para este caso se utilizarán en el área de la seguridad informática.

6.4 Atractores Caóticos

El caos tiende a despertar el pensamiento colectivo de ser sinónimo de "desorden" o "complicado", pero si se revisa su significado etimológico indica 'abertura' (por su raíz griega). Para que un sistema pueda ser considerado matemáticamente como caótico, este debe poseer dinámica no lineal, sensibilidad a condiciones iniciales, exponentes de Lyapunov positivos, estar vinculado a un atractor extraño y una dimensión fractal en los atractores (García Sepulveda, 2015).

Un atractor es la condición que poseen algunos sistemas complejos que presentan en algún momento patrones de coincidencia, teniendo presente su inicio caótico, los cuales son anomalías que surgen de eventos impredecibles y éstos configurarán una modificación potencialmente organizada de los sistemas mismos (Baptiste, 2018)

Existen diferentes tipos de atractores caóticos o extraños cómo los bautizó Edward Lorenz, matemático pionero de la teoría del caos, uno de los cuales lleva su nombre y es descrito por el sistema de ecuaciones (1):

$\dot{x} = \sigma(x - y)$	(1)
$\dot{y} = rx - y - xz$	
$\dot{z} = xy - bz$	

Donde $x(t)$, $y(t)$ y $z(t)$ son las variables del sistema y σ, b y r son parámetros positivos. En la figura 1 se ilustra este atractor para los valores

$\sigma = 10$, $b = \frac{8}{3}$ y $r = 28$.

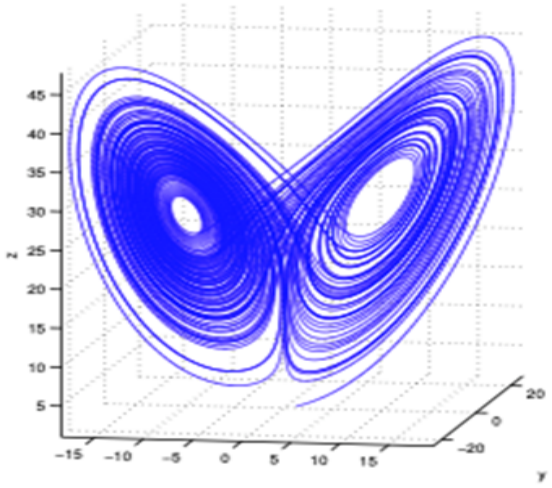

Figura 1. Atractor de Lorenz. Elaboración propia usando Matlab.

Otro tipo de atractor es el propuesto por Chen en 1999, el cual es una modificación y generalización del sistema de Lorenz y es descrito por el sistema de ecuaciones dado en (2).

$\dot{x} = \sigma(y - x)$	(2)
$\dot{y} = rx + sy - xz$	
$\dot{z} = xy - bz$	

Donde $x(t)$, $y(t)$ y $z(t)$ son las variables del sistema y σ, b, r y s son parámetros reales, la figura 2 se obtiene de los valores $\sigma = 36$, $r = 0$, $s = 20$ y $b = 3$

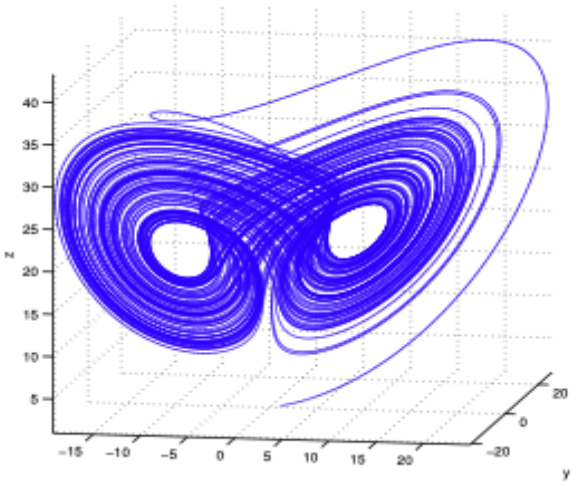

Figura 2. Atractor de Chen. Elaboración propia usando Matlab.

Los sistemas dinámicos antes mostrados son de tipo continuo (Piña, 2019), existen discretos, los cuales son modelados por medio de ecuaciones en diferencias, relaciones de recursión y mapas iterados, para los cuales las condiciones necesarias del caos se ven presentes constantemente y requieren un extenso análisis, alguno de ellos como el atractor caótico (Guyeux, 2013). El estudio de los sistemas dinámicos está en constante evolución, influenciado por los avances tecnológicos que han permitido que su simulación sea más sencilla y rápida.

7. Alcances y Limitaciones

Este proyecto pretende ser aplicado sobre cualquier tipo de simbolización de 256 elementos potencialmente representativos, idealmente en código ASCII, buscando la encriptación de textos, para lo cual se requerirá usar un computador convencional para la generación de los bloques, consiguiendo con ello independencia de cualquier intermediario para la encriptación.

Una limitante hace referencia a que se requiere siempre un almacenamiento 27 veces el tamaño del texto en su formato de 256-bits, junto a un procesador o GPU de al menos 1.8 Ghz para realizar la simulación de cada red neuronal sin sufrir colapsos.

8. Metodología de la Investigación

A continuación, se presenta el marco metodológico de tipo cuantitativo, que será aplicado en el desarrollo de este trabajo de investigación, donde, inicialmente se realizará una revisión para la elección del modelo de aprendizaje, del atractor caótico y de los criterios de encriptación, para posteriormente tomar en cuenta el establecimiento de un tipo de red neuronal y delimitar las características del modelo. Con lo cual se tomarán los datos y se desarrollará un prototipo para iniciar las pruebas de validación, según el resultado de éstas, se ajustará el modelo y se realizará la evaluación, además de las pruebas para cumplir con los objetivos de la propuesta. En la figura 3 se sintetiza el esquema metodológico.

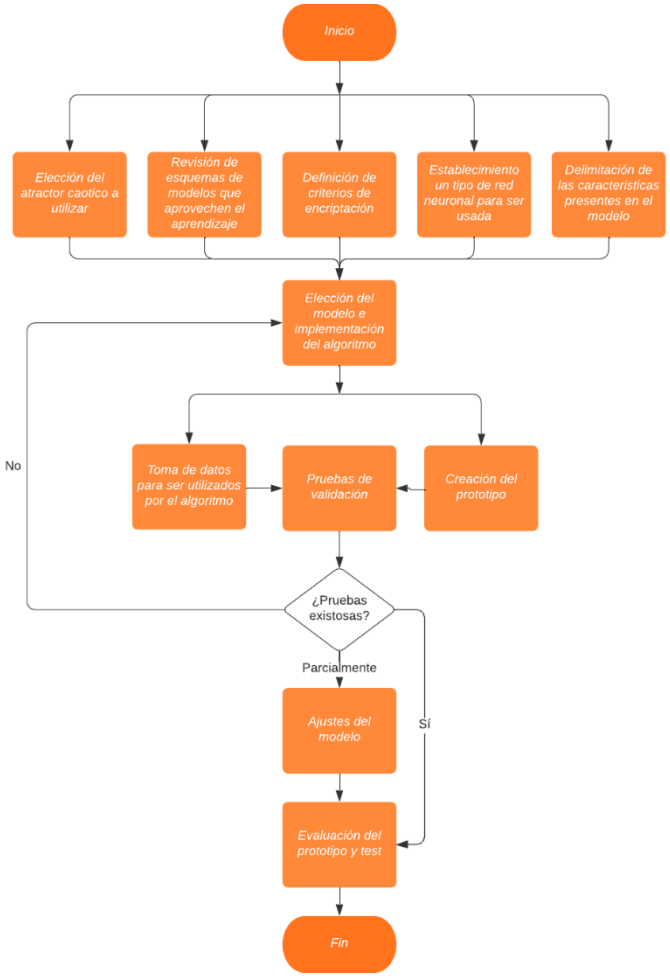

Figura 3. Diagrama de la metodología de la investigación.

9.Cronograma de Actividades

Actividades	Meses					
	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6
Elección del atractor caotico a utilizar						
Revisión de esquemas de modelos que aprovechen el aprendizaje						
Definición de criterios de encriptación						
Establecimiento de un tipo de red neuronal para ser usada						
Delimitación de las caracteristicas presentes en el modelo						
Elección del modelo e implementación						
Toma de datos para ser utilizados por el algoritmo						
Pruebas de validación						
Creación del prototipo						
Ajustes del modelo						
Evaluación del prototipo y test						
Elaboración del documento final						

Tabla 1. Cronograma de actividades.

10. Recursos y presupuesto

Para la ejecución de la presente propuesta se tienen en cuenta de una parte, los recursos físicos y de otra los humanos:

Recursos humanos:

Rol	N° de personas	Salario	Tiempo (semanas)	Costo Total
Director	2	$8’000.000	16	$32.000.000
Estudiante	1	$1.000.000	16	$4.000.000

Tabla 2. Tabla de recursos humanos.

Gastos generales:

Concepto	Descripción	Costo Total
Computador de mesa o portátil.	Equipo con las condiciones necesarias para el desarrollo de la propuesta	$3.200.000
Servicios públicos y de Internet	Requeridos para el funcionamiento del equipo de cómputo y acceso a información	$720.000
Papelería e impresiones	Cuadernos, lápices y marcadores	$200.000
Transportes	Pasajes y parqueaderos	$300.000

Tabla 3. Tabla de gastos generales.

Presupuesto total:

Concepto	Costo
Recursos Humanos	$36.000.000
Gastos generales	$4.420.000
Total	**$40.420.000**

Tabla 4. Tabla de presupuesto total.

Bibliografía

Adel A. El-Zoghab, A. H. (2013). Survey Report on Cryptography Based on Neural Network. *International Journal of Emerging Technology and Advanced Engineering*, 456-462.

Baptiste, B. (17 de Agosto de 2018). *Atractores*. Recuperado el 28 de Noviembre de 2022, de https://divulgacion.minciencias.gov.co/atractores

Basogain, O. (Diciembre de 2008). *Curso: Redes Neuronales Artificiales y sus Aplicaciones*. Obtenido de https://ocw.ehu.eus/pluginfile.php/40137/mod_resource/content/1/redes_neuro/contenidos/pdf/libro-del-curso.pdf

Basualdo, C. R. (2001). *Redes Neuronales: Conceptos Básicos y.* Universidad Tecnológica Nacional, Facultad Regional Rosario. Grupo de Investigación Aplicada a la Ingeniería Química (GIAIQ). Recuperado el 28 de Noviembre de 2022, de https://www.frro.utn.edu.ar/repositorio/catedras/quimica/5_anio/orientadora1/monografias/matich-redesneuronales.pdf

Bernstein, D. (2009). Introduction to post-quantum cryptography. En D. J. Bernstein, *Post-Quantum Cryptography* (págs. 1-14). Berlin, Heidelberg: Springer Berlin Heidelberg. doi:https://doi.org/10.1007/978-3-540-88702-7_1

Bernstein, D. (2010). Grover vs. McEliece. En D. J. Bernstein, *Post-Quantum Cryptography* (págs. 73-80). Berlin, Heidelberg: Springer Berlin Heidelberg.

Bevi, A. B. (2021). Design of a novel chaotic neural network based encryption system for security applications. *Journal of the Chinese Institute of Engineers, 44*, 424-439. doi:https://doi.org/10.1080/02533839.2021.1919558

Bigdeli, N. F. (2012). A novel image encryption/decryption scheme based on chaotic neural networks. *Engineering Applications of Artificial Intelligence*, 753-765. doi:https://doi.org/10.1016/j.engappai.2012.01.007

Burak, D. (2015). {Parallelization of an Encryption Algorithm Based on a Spatiotemporal Chaotic System and a Chaotic Neural Network. *Procedia Computer Science, 51*, 2888-2892. doi:https://doi.org/10.1016/j.procs.2015.05.453

Cao, W. Y. (Agosto de 2006). Cryptography based on delayed chaotic neural networks. *Physics Letters A*, 333-338. doi:https://doi.org/10.1016/j.physleta.2006.03.069

Donohue, B. (10 de Abril de 2014). *¿Qué Es Un Hash Y Cómo Funciona?* Recuperado el 28 de Noviembre de 2022, de https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/

F. Yang, J. M. (2020). An image encryption algorithm based on BP neural network and hyperchaotic system. *China Communications, 17*(5), 21-28. doi:10.23919/JCC.2020.05.003

Guyeux, J. B. (2013). *Discrete dynamical systems and chaotic machines.* Londres: Chapman.

Ilya Sutskever, J. M. (2 de Julio de 2011). Generating Text with Recurrent Neural Networks. *Proceedings of the 28th International Conference on Machine Learning (ICML-11)*, (págs. 1017-1024). Recuperado el 4 de octubre de 2022, de Fortieth International Conference on Machine Learning : https://icml.cc/2011/papers/524_icmlpaper.pdf

Isasi Viñuela, P., & Galván León, I. M. (2004). *Redes de neuronas artificiales. Un enfoque Práctico.* Madrid, España: Pearson Prentice-Hall.

Jones, H. (2019). *Las redes neuronales: Una guía esencial para principiantes de las redes neuronales artificiales y su papel en el aprendizaje automático y la inteligencia artificial.* España: Bravex Publications.

Kenan, D. I. (2010). Artificial neural network based chaotic general network based chaotic generator for cryptology. *Turk J Elec Eng & Comp Sci*. doi:10.3906/elk-0907-140

L. Chengquing, L. S. (Noviembre de 2004). Cryptanalysis of a Chaotic Neural Network Based Multimedia Encryption Scheme. *Lecture Notes in Computer Science, 3333*, 418-425.

Maiorano, A. (2009). *Criptografía - Técnicas de desarrollo para profesionales.* Alfaomega.

Piña, I. (2019). *Puente entre los sistemas de Lorenz y Chen.* Instituto politecnico nacional, Unidad profesional interdiciplinaria en ingeniería y tecnologías avanzadas. Instituto politecnico nacional. Obtenido de https://www.academia.edu/40257039/Puente_entre_los_sistemas_de_Lorenz_y_Chen

Plaza, F. (2021). *Manual de Criptografía - Fundamentos matemáticos de la criptografía para un estudiante de Grado.* Salamanca, España: ONIX. doi:https://doi.org/10.14201/0DD0169

T. Graham, R. M. (Octubre de 2019). Chaotic Encryption Algorithm With Key Controlled Neural Networks for Intelligent Transportation Systems. *IEEE Acces, 7*. doi:10.1109/ACCESS.2019.2950007

Wikipedia, G. (2022). *Algoritmo de Huffman*. Obtenido de https://es.wikipedia.org/wiki/Algoritmo_de_Huffman

Wikipedia, G. (2022). *Public-key cryptography*. Recuperado el 28 de Noviembre de 2022, de https://en.wikipedia.org/wiki/Public-key_cryptography

Wikipedia, G. (2022). *Symmetric-key algorithm*. Recuperado el 28 de Noviembre de 2022, de https://en.wikipedia.org/wiki/Symmetric-key_algorithm

Z. Man, J. L. (Noviembre de 2011). Double image encryption algorithm based on neural network and chaos. *Chaos, Solitons & Fractals, 152*. doi:https://doi.org/10.1016/j.chaos.2021.111318