



UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

CIFRADO DE VÍDEOS TRANSMITIDOS EN TIEMPO REAL UTILIZANDO EL ATRACTOR DE LORENZ

Paula Andrea Barragán Guzmán
Camilo Andrés Arias Sarria

Universidad Distrital Francisco José de Caldas
Facultad de Ingeniería, Ingeniería de Sistemas
Bogotá, Colombia
2019

CIFRADO DE VÍDEOS TRANSMITIDOS EN TIEMPO REAL UTILIZANDO EL ATRACTOR DE LORENZ

**Paula Andrea Barragán Guzmán
Camilo Andres Arias Sarria**

Proyecto de grado presentado como requisito parcial para optar al título de:
Ingeniero de sistemas

Director:
EDILMA ISABEL AMAYA BARRERA

Línea de Investigación:
Teoría del caos, seguridad informática, matemática aplicada

Universidad Distrital Francisco José de Caldas
Facultad de Ingeniería, Ingeniería de Sistemas
Bogotá, Colombia
2019

Índice general

Índice de figuras	6
Índice de cuadros	7
INTRODUCCIÓN	1
1. TITULO Y DEFINICIÓN DEL TEMA DE INVESTIGACIÓN	5
2. ESTUDIO DEL PROBLEMA DE INVESTIGACIÓN	6
2.1. Planteamiento del Problema	6
2.2. Formulación del Problema	7
2.3. Sistematización del Problema	7
3. OBJETIVOS DE LA INVESTIGACIÓN	8
3.1. Objetivo General	8
3.2. Objetivos Específicos	8
4. JUSTIFICACIÓN DE LA INVESTIGACIÓN	9
5. HIPÓTESIS DE TRABAJO	11
6. ESTADO DEL ARTE	12
7. MARCO DE REFERENCIA	17
7.1. Atractor de Lorenz	17
7.1.1. Propiedades más importantes del atractor de Lorenz . .	18
7.2. Cifrado de vídeos	20

7.3. Técnicas de hacking	20
8. ASPECTOS METODOLÓGICOS	22
8.1. Tipo de Estudio	22
8.2. Método de Investigación	22
8.2.1. Exploratoria	22
8.2.2. Diseño	23
8.2.3. Implementación	23
8.2.4. Resultados	24
8.2.5. Documentación	24
8.3. Fuentes y Técnicas para la Recolección de la Información . . .	24
8.4. Tratamiento de la Información	24
9. ALCANCES, LIMITACIONES Y RESULTADOS ESPERADOS	25
9.1. Alcances	25
9.2. Limitaciones	25
9.3. Resultados Esperados	26
10. ALGORITMO PROPUESTO	27
11. METODOLOGÍA	31
12. RESULTADOS	34
12.1. RENDIMIENTO DEL ALGORITMO	34
12.2. ESPACIO DE CLAVE	34
12.3. ATAQUES INFERENCIALES	35
12.4. ENTROPÍA	35
12.5. SENSIBILIDAD DE LA CLAVE	36
12.6. GRÁFICAS DE CORRELACIÓN Y DENSIDAD DE PÍXELES	38
12.7. ANÁLISIS COMPARATIVO	38
13. CONCLUSIONES	40
13.1. Verificación, contraste y evaluación de objetivos	40
13.2. Aportes Originales	41

<i>ÍNDICE GENERAL</i>	5
Bibliografía	42

Índice de figuras

7.1. Sincronización de atractores. Fuente [1]	18
10.1. Descripción del algoritmo utilizado para realizar el proceso de encriptación.	30
11.1. Pruebas de Cifrado	33
12.1. Sensibilidad de Clave	37
12.2. Gráficas de Correlación	39

Índice de cuadros

12.1. Comparación de resultados obtenidos.	38
----------------------------------------------------	----

INTRODUCCIÓN

Desde tiempos ancestrales ha sido una preocupación del ser humano salvaguardar la información confidencial, en principio con técnicas mecánicas que se aplicaron en los ámbitos religioso, social y político, posteriormente de la mano del desarrollo de la tecnología se han consolidado métodos de criptografía vivientes, con fundamentos que reposan sobre la matemática y constituyen el avance tecnológico más importante de los últimos 1000 años, según Lawrence Lessig [2].

La palabra criptografía proviene de las raíces griegas *kriptos* y *graphein* que traducen escondido y escritura respectivamente, y según el diccionario de la real academia de la lengua española la definición adoptada para ésta es: “Arte de escribir con clave secreta o de un modo enigmático”. Históricamente una de las aplicaciones de la criptografía ha estado relacionada con el ambiente militar y con los secretos de estado, de hecho durante la segunda guerra mundial tuvo gran incidencia debido a que un objetivo en ella era el cifrado y descifrado de información secreta. El ingeniero Alemán Arthur Scherbius experto en electromecánica tenía como propósito aplicar la tecnología del momento en pro de mejorar los esquemas de criptografía de los ejércitos y logró diseñar un dispositivo electromecánico de cifrado conocido como “ENIGMA”, el cual permitió a los alemanes enviar sus mensajes en forma secreta, evitando que sus planes y estrategias de ataque se filtraran a los aliados [3].

La máquina ENIGMA tuvo tanta acogida que Alemania en el año 1933 nacionalizó la compañía Enigma y empezó a equipar al ejército alemán con éstas máquinas como mecanismo oficial de encriptación, ellos se sentían avenajados ya que hasta ese momento el código de ENIGMA era indescifrable. Sin embargo un grupo polaco, dentro del cual se destacó el matemático Marian Rejewski, en el año 1929 comenzó su trabajo orientado hacia descifrar el código ENIGMA, logrando diseñar una réplica que les sirvió de base para

este fin y proponiendo un modelo conocido como “máquina bomba” que servía para explorar muchas posibilidades de descifrar los mensajes, usado posteriormente para el trabajo del grupo británico Bletchley Parken, encabezado por el matemático británico experto en seguridad Alan Mathison Turing quienes con otro esquema de trabajo continuaron descifrando el código de ENIGMA mediante el diseño de una máquina electromecánica conocida como “La bomba de Turing”, con una mejora añadida que sugirió el matemático Gordon Welchman, era la herramienta principal que usaban los criptógrafos aliados para leer los códigos de ENIGMA, sin embargo todo esto era un proyecto secreto y de máxima seguridad, hay quienes han estimado que gracias a todos los resultados de estos trabajos, la segunda guerra se acortó entre dos y cuatro años.[2]

Se puede afirmar que gracias a la criptografía durante la segunda guerra mundial nacieron los primeros computadores, cuyas bases fueron dadas por Shannon, Turing y el matemático John Von Neumann.

Al terminar la segunda guerra las oficinas de seguridad de las potencias mundiales invirtieron mucho presupuesto para investigar en técnicas de cifrado y desde este momento los avances tanto de la tecnología como de la criptografía han estado ligados y han surgido desarrollos teóricos muy importantes [2]. Uno de los investigadores en este tema fué el ingeniero electricista y matemático Claude Elwood Shannon quien contribuyó durante la segunda guerra mundial con trabajos sobre la seguridad y el descifrado de códigos para proteger la seguridad Estadounidense, sus trabajos más conocidos son: “A mathematical theory of communication”[4] y “Communication theory of secrecy systems”[5] publicados en el año 1948 y 1949 respectivamente, es considerado el padre de la teoría de la información.

En la actualidad la criptografía se encarga de fusionar la tecnología y la matemática para transformar la información de tal forma que resulte incomprendible para todas las personas que no tengan permiso de acceder a ésta. Los métodos convencionales actuales se basan en la teoría de números, curvas elípticas, código ADN, autómatas celulares, y han habido desarrollos teóricos muy prominentes en el campo de la computación cuántica. En las últimas décadas ha surgido una corriente enfocada hacia la seguridad por medio del uso de atractores caóticos, este trabajo se enfoca en esta dirección.

La teoría del caos se enmarca dentro del estudio de los sistemas dinámicos no lineales, el precursor de éste fué el matemático y físico Francés Jules Henri Poincaré, quien a finales del siglo XIX se interesó por el estudio de las ecua-

ciones diferenciales no lineales desde un punto de vista no analítico llamado análisis cualitativo, el cual se enfoca en analizar el comportamiento de los sistemas dinámicos no lineales con respecto a determinar la estabilidad o no del sistema a largo plazo, y si para algunas condiciones iniciales y valores de los parámetros el sistema presenta periodicidad.

Aunque las contribuciones de Poincaré sentaron las bases de la teoría del caos [6], vale la pena resaltar que tardó mucho tiempo en que otros matemáticos y físicos se interesaran por este tema, quizás porque no existían las herramientas apropiadas para su análisis, situación que se superó con el avance significativo de los computadores. Algunos de ellos son el matemático estadounidense George David Birkhoff y más tarde los matemáticos estadounidenses Stephen Smale y Edward Lorenz, así como los matemáticos Soviéticos Andréi Nikoláievich Kolmogorov, Vladimir Arnold y Aleksandr Mijáilovich Liapunov, quienes contribuyeron a consolidar la fundamentación teórica de la teoría del caos, la cual ha permeado diversas áreas del conocimiento como biología, química, física, sociales, ingeniería entre otras [6].

En este trabajo se pretende aprovechar las propiedades inherentes de los atractores caóticos para fortalecer la seguridad de los sistemas de criptografía que involucran videos, ya que los métodos convencionales para la encriptación de textos como RSA, DES, IDEA, y AES, no son apropiados para aplicarlos al cifrado de imágenes o videos, dado el volumen de datos que se manejan y la poca variación en los píxeles adyacentes, lo que implica mucha redundancia y dificulta ocultar la información. [7]

La encriptación de videos debe ser eficiente en los siguientes aspectos: seguridad, baja complejidad computacional, tiempo de ejecución, estabilidad durante el proceso de compresión y conformidad con el formato de video [8]. Los esquemas de encriptación de videos utilizando atractores caóticos se pueden clasificar en tres tipos según la forma de encriptación que se maneje, pudiendo ser: completa, selectiva o una combinación compresión con encriptación.[1]

Basados en los artículos referenciados en [9] y en [1], donde se plantea el uso de las propiedades de los atractores caóticos para la encriptación de imágenes y texto, además, bajo el marco del proyecto de investigación 'Modelos de Encriptación basados en Atractores Caóticos' institucionalizado por el grupo de complejidad UD ante el Centro de Investigaciones de la Universidad Distrital, en este trabajo de tesis, se propone un algoritmo para el cifrado de videos en tiempo real o llamado comúnmente streaming. Combinando técnicas de permutación y difusión mejoradas y componentes de software dispuestos es-

pecialmente para el manejo de vídeos, logrando consolidar un algoritmo capaz de cifrar un vídeo en un tiempo mínimo y con un retardo imperceptible.

Capítulo 1

TITULO Y DEFINICIÓN DEL TEMA DE INVESTIGACIÓN

CIFRADO DE VÍDEOS TRANSMITIDOS EN TIEMPO REAL UTILIZANDO EL ATRACTOR DE LORENZ

Tema de Investigación

Teoría del caos, Matemática aplicada, Seguridad informática, Transmisión de vídeos.

Holotipo de Investigación

Esta investigación permitirá diseñar, implementar y evaluar en un ambiente local, una solución comparable con los esquemas desarrollados en campos similares a los tratados aquí, para mejorar la seguridad del conocido *streaming* utilizando para ello los temas de investigación previamente definidos, por lo tanto el holotipo de la investigación es *proyectiva*.

Capítulo 2

ESTUDIO DEL PROBLEMA DE INVESTIGACIÓN

2.1. Planteamiento del Problema

El creciente auge en el ámbito tecnológico ha permitido que las distancias no sean tan relevantes a la hora de contactarse con otras personas, teniendo la posibilidad que éstas se comuniquen por medio de llamadas de audio y vídeo, en ámbitos personales, comerciales, de investigación e incluso gubernamentales, utilizando como canal el internet.

Al encontrarse esta información en un entorno virtual puede ser vulnerada, de manera que personas diferentes a las involucradas en la conversación puedan obtener este mensaje y lucrarse ilegalmente de la misma.

En consecuencia, se quiere diseñar un algoritmo capaz de enfrentar los retos que pueda llevar el avance tecnológico, acotándolo al cifrado de vídeos en tiempo real y aprovechando las características del atractor de Lorenz. Este algoritmo debe garantizar un bajo costo computacional a la hora de realizar la encriptación de la información, y a su vez debe evidenciar un alto nivel de seguridad para que sea inviable para un atacante poder tener acceso a la información.

2.2. Formulación del Problema

¿Es posible realizar un algoritmo para cifrar vídeos en tiempo real utilizando el atractor de Lorenz?

2.3. Sistematización del Problema

- ¿Qué parámetros debe tener el atractor de Lorenz para ofrecer las mejores condiciones de cifrado?
- ¿Qué condiciones debe cumplir el vídeo para poder realizar el cifrado correctamente?
- ¿Cuáles son los requisitos mínimos computacionales para que el método de cifrado sea óptimo para un usuario final?

Capítulo 3

OBJETIVOS DE LA INVESTIGACIÓN

3.1. Objetivo General

Desarrollar un algoritmo basado en el atractor caótico de Lorenz y sus propiedades para cifrar un vídeo transmitido en tiempo real

3.2. Objetivos Específicos

- Construir un modelo de cifrado para videos transmitidos en tiempo real basado en fuentes relacionadas con el atractor de Lorenz y cifrado de contenido multimedia.
- Implementar un algoritmo usando una colección de librerías especializadas en el manejo de fotogramas para cifrar un vídeo transmitido en tiempo real.
- Evaluar el algoritmo comparando con las fuentes recopiladas para analizar los niveles de seguridad y la confiabilidad en el mismo.

Capítulo 4

JUSTIFICACIÓN DE LA INVESTIGACIÓN

La criptografía es la rama encargada de fusionar la tecnología y la matemática para transformar la información de tal forma que resulte incomprendible para todas las personas que no tengan permiso de acceder a ésta.

Actualmente, los métodos de encriptación se basan en lo propuesto por el Sistema RSA. Este sistema consiste en la selección de dos números enteros p y q , de aproximadamente 100 dígitos cada uno, para calcular el número $n = pq$. Posteriormente, se selecciona un entero e tal que $(e, \varphi(n)) = 1$ (siendo $\varphi(n)$ la función indicatriz de Euler), y se calcula el inverso d de e módulo $\varphi(n)$. La clave pública consiste en la pareja formada por los números (n, e) y la clave privada es el número d [10].

Este sistema funciona basado en la suposición de que no hay un procedimiento computacionalmente eficiente para factorizar el numero e . Se sabe que usando el algoritmo de factorización más rápido conocido, cuando p y q tienen 100 dígitos, se requieren $3,8 \times 10^9$ años de computador para factorizar el entero $n = pq$ [10].

Sin embargo, el desarrollo de tecnologías, como la computación cuántica, promete potencializar la capacidad de procesamiento de las máquinas actuales. Por lo anterior, es posible que algún día existan procedimientos capaces de factorizar los números y que RSA sea vulnerable al criptoanálisis.

Es por esta razón que se necesitan desarrollar algoritmos de encriptación capaces de evitar esta eventual vulnerabilidad, en los cuales no se haga uso de una clave pública en función de números primos, sino se utilice un sistema más

complejo. El algoritmo propuesto en este trabajo utiliza el atractor de Lorenz, ya que cuenta con propiedades ideales para solucionar este tipo de problemas como la sincronización y la alta sensibilidad a las condiciones iniciales.

Capítulo 5

HIPÓTESIS DE TRABAJO

¿Es viable utilizar un método no convencional como el atractor de Lorenz para encriptar un vídeo transmitido en tiempo real, y que sea equiparable a algoritmos planteados en trabajos recientes?

Capítulo 6

ESTADO DEL ARTE

En la literatura existen esquemas propuestos usando atractores caóticos para implementar procesos de encriptación de imágenes y vídeos, algunos de los trabajos que se destacan en esta temática son:

El desarrollado en [8], donde los autores proponen un algoritmo para encriptación de vídeos a partir de dos atractores caóticos unidimensionales, diseñando un generador eficiente de números pseudoaleatorios que convierten en un binario no negativo de 32 bits, para generar flujo de claves y cifrar elementos de sintaxis de vídeo en formato H.264 / AVC. Los autores combinan el proceso de encriptación con el de compresión de la imagen para ahorrar recursos informáticos; muestran que el esquema es robusto con respecto a seguridad y tiempo de ejecución, la complejidad es de orden lineal, tiene dependencia sensitiva a pequeños cambios en la clave, y por tanto concluyen que el algoritmo de encriptación de vídeo propuesto cumple con todos los requisitos ideales de un sistema que involucre compresión y encriptación conjuntamente.

En [11] proponen un algoritmo para comprimir y encriptar vídeos utilizando la transformada discreta de cosenos para la compresión, y las sucesiones caóticas generadas por un atractor hipercaótico de Chen para encriptar los coeficientes provistos por la transformada discreta de cosenos. Los resultados muestran una alta sensibilidad a las condiciones iniciales y buena aleatoriedad, así como un amplio espacio de clave, velocidad de encriptación alta y buen rendimiento temporal, los autores indican que puede ser utilizado para la transmisión de vídeos en tiempo real.

En [12] se propone un algoritmo de encriptación de vídeos en formato MPEG, a través de un atractor caótico definido a partir de la función logística,

que combina la encriptación y la compresión, generando un amplio espacio de clave utilizando sucesiones caóticas. Los autores encriptan solo los signos de los vectores de movimiento, lo que hace que sea un algoritmo de bajo costo computacional; los resultados experimentales muestran que tiene una alta seguridad, el formato original no se modifica y la tasa de afectación por el proceso de compresión es baja, razones por las que el esquema propuesto se ajusta para el manejo de videos en tiempo real.

En [13] presentan un algoritmo de tipo simétrico para cifrar imágenes utilizando el sistema dinámico caótico generado por la función logística, obteniendo tres sucesiones una de las cuales es utilizada para el proceso de difusión, la segunda sucesión la combinan con la información difundida con el fin de incrementar la longitud de la información y la tercera es utilizada para el proceso de confusión. Los autores muestran que el algoritmo es válido para codificar cualquier información dividiéndola en bloques de 8 bits, además de poseer un buen nivel de seguridad y una buena velocidad de cifrado.

En [14], los autores desarrollan un algoritmo caótico para encriptación de videos a partir de la articulación de tres sistemas dinámicos unidimensionales generados por la función tienda, función diente de sierra y la función logística con una pequeña modificación, para lograr que ésta tome valores entre 0 y 255. Estas funciones son utilizadas para generar las sucesiones caóticas y enmascarar la información del video una vez es aplicado el proceso de compresión y seleccionados los bit más significativos en los coeficientes de la transformada discreta de cosenos, mediante un esquema que es combinado con la operación XOR. Las pruebas experimentales les permiten garantizar que el receptor con el conocimiento de la clave es capaz de reproducir las mismas secuencias caóticas del emisor y por consiguiente reconstruir de manera fidedigna la información del video; además la pruebas validan que el sistema propuesto es altamente sensible a las condiciones iniciales y a los parámetros de control de los sistemas caóticos empleados, que el uso de los tres sistemas caóticos aumenta la seguridad sin incrementar significativamente el tiempo de procesamiento, comparándolo con otras referencias encaminadas al uso de atractores caóticos para el mismo fin.

En [15] se muestra un esquema metodológico que opera bajo una plataforma de hardware ARM (Advanced RISC Machine) para encriptación de video en tiempo real, basado en el diseño de un sistema hipercaótico discreto n-dimensional, utilizando para el caso de estudio 8 dimensiones, con el cual se generan sucesiones para el cifrado de las capas de colores de los píxeles que

hay en cada fotograma del vídeo. El manejo de la clave lo hacen a través de la sincronización de dos sistemas caóticos obtenidos a partir del atractor en consideración. Los autores indican que la medida del espacio de clave del algoritmo propuesto puede ser de tipo exponencial, sin embargo, este hecho desencadena un tiempo de ejecución grande en las etapas de encriptación y desencriptación, lo que es una desventaja para el manejo de aplicaciones en tiempo real; por lo que sugieren un espacio de clave no exponencial pero bastante amplio. Además, las pruebas que presentan muestran una alta sensibilidad a las condiciones iniciales, razón por lo que su propuesta la consideran como una buena alternativa para el cifrado de vídeos.

En [16] proponen un algoritmo de encriptación de imágenes o vídeo basado en el uso de un sistema caótico espacio temporal definido a partir de la función logística, con el fin de hallar sucesiones caóticas que son utilizadas para la codificación de los coeficientes de la transformada discreta de cosenos de cada bloque de vídeo, el cual tiene un buen desempeño con respecto a propiedades generadas por el caos, que lo hacen apropiado para el diseño de esquemas de seguridad en comunicaciones y multimedia. El algoritmo propuesto considera tres aspectos: un método de inicialización de malla basado en las iteradas de la función logística para obtener una alta sensibilidad de la clave, las iteraciones del sistema caótico y la cuantificación de éstas que se usan para generar secuencias aleatorias, que finalmente se combinan mediante la operación XOR para cifrar el bloque de imagen original.

En [17] proponen un esquema para encriptar vídeos provenientes de cámaras de vigilancia, cuya base es la separación en cada cuadro del primer plano y del fondo, el algoritmo solo cifra la información correspondiente al primer plano. Para evitar que se destruyan los valores de los píxeles en el proceso de almacenamiento y transmisión, encriptan solo un pixel a la vez, lo que indica que el proceso de tratamiento entre un píxel y otro no se ve afectado, aunque esto reduce el espacio de clave. En el esquema que proponen, el primer plano de cada cuadro tiene su propia clave, así, que a medida que hayan más cuadros en el vídeo, mayor será el espacio de clave, la clave de la imagen se genera con base a una imagen que se elige al azar para aumentar la imprevisibilidad; se aplica operación XOR entre cada dos cadenas convertidas correspondientes a los valores de dos píxeles, uno de la región de primer plano y otro en la misma posición pero en la imagen, y cada nueva cadena binaria se baraja por medio de la utilización de una función caótica definida a partir de una congruencia lineal, es decir, que el atractor se utiliza para encriptar el valor de cada uno

de los pixeles de cada cuadro. Evalúan aspectos concernientes a nivel de seguridad, radio de encriptación, degradación visual y velocidad de encriptación logrando obtener buenos indicadores.

En [18], los autores hacen una implementación de hardware de un algoritmo de encriptación de videos basado en un sistema hipercaótico de tipo continuo y de 8 dimensiones propuesto por ellos. A través del sistema hipercaótico generan las llaves secretas para los procesos de permutación y de difusión implementados en cada fotograma del video. El flujo de datos de video es capturado por una cámara digital en el lado del transmisor, estos datos son mezclados, encriptados y enviados hacia el receptor a través de Wifi. En el lado del receptor, el mismo atractor hipercaótico es usado para recuperar el flujo de datos original del video. El algoritmo propuesto es probado para la transmisión de videos en tiempo real, logran obtener un espacio de clave de casi , los resultados experimentales y el análisis teórico confirman la viabilidad del sistema de encriptación para la transmisión de videos seguros basados en un sistema hipercaótico a través de una red inalámbrica.

En [19], se presenta un algoritmo eficiente para encriptación de videos que incluye inicialmente la etapa de compresión estándar en formato MPEG2, y el proceso de encriptación se basa en un sistema hipercaótico a partir del cual generan sucesiones pseudoaleatorias que utilizan para encriptar los pixeles de cada fotograma del video de tamaño 8X8, la característica principal de este esquema es que la clave es una imagen, lo cual contribuye al aumento de espacio de clave y a la disminución de la complejidad, garantizando mayor seguridad.

En [20], proponen un algoritmo para encriptación de imágenes basado en el atractor caótico generado por la función logística, usan tres parámetros diferentes para conseguir tres sucesiones aleatorias que son usadas para construir tres tablas de modificación del valor de los pixeles las cuales combinan con la tabla de los valores de los píxeles de la imagen original, mediante un proceso que involucra las operaciones módulo y xor, y que garantiza que dos valores de píxeles iguales en posiciones diferentes sean enmascarados de manera diferente. Los análisis de las pruebas que hacen muestran que el espacio de clave es bastante amplio e igual a , el valor de entropía es 7.9997 y el sistema es bastante sensible a pequeñas perturbaciones, además los índices de correlación en la imagen cifrada son casi nulos.

En [21] los autores desarrollan un algoritmo para encriptación de imágenes en escala de grises a partir del uso de un sistema caótico de malla acoplado de

dos dimensiones definido involucrando dos sistemas caóticos unidimensionales de tipo trigonométrico, combinados con las iteradas de la función logística para el parámetro . Por medio de las componentes , obtenidas a partir de las iteradas del sistema caótico acoplado combinadas con la operación módulo y xor define un mecanismo de cifrado. El esquema es probado para algunas imágenes evidenciando buen desempeño con respecto a seguridad, ya que el espacio de clave es mayor que y los coeficientes de correlación de píxeles adyacentes son inferiores a 0.0036.

En [22] proponen un algoritmo para encriptación de imágenes a color implementando la etapa de difusión y permutación en cada capa RGB a través del uso conjunto de los sistemas caóticos tridimensionales generados por una función estándar y la función cat. Las pruebas teóricas y experimentales muestran buena velocidad en el proceso de encriptación, un espacio de clave de , alta sensibilidad a las condiciones iniciales, coeficientes de correlación de píxeles en la imagen encriptada bastante pequeños, y un valor de entropía muy próximo a 8, indicadores que hacen que el algoritmo propuesto sea una buena alternativa para aplicaciones prácticas alusivas a la encriptación de imágenes.

En consonancia con los trabajos descritos anteriormente, y partiendo de la premisa de que el avance de la tecnología ha conllevado a que la tasa de delitos informáticos vaya en constante aumento, es necesario buscar nuevas formas de seguridad en la transferencia de información por redes públicas, ya sea texto, imágenes, videos o audios, y así evitar los problemas de orden personal, económico y judicial que resultan desgastantes y onerosos para los involucrados y las instituciones del estado. Este trabajo de tesis se ajusta dentro de este reto impuesto por la era de la información.

Capítulo 7

MARCO DE REFERENCIA

7.1. Atractor de Lorenz

Cuando se menciona el atractor de Lorenz, se refiere a un sistema dinámico basado en tres ecuaciones:

$$\begin{aligned}\dot{x} &= \sigma(y - x) \\ \dot{y} &= rx - y - xz \\ \dot{z} &= xy - bz\end{aligned}\tag{7.1}$$

Donde $\sigma, r, b > 0$ son parámetros. Edward Lorenz en 1963 derivó esas tres ecuaciones desde un modelo drásticamente simplificado que había diseñado para explicar rollos de convección en la atmósfera de 12 ecuaciones [23]. Estas mismas ecuaciones han sido usadas en distintos experimentos, como el que describe exactamente el movimiento de una rueda de agua fabricado por investigadores del MIT en el año 1970 que constaba de una rueda vertical que tenía varios vasos de papel con fugas en sus bordes. Lorenz descubrió que este sistema podía tener una comportamiento errado extremo: amplio rango de parámetros, las soluciones oscilaban irregularmente, nunca se repetían pero siempre se mantenían en una región limitada del espacio. Cuando él graficó estas trayectorias en tres dimensiones se dio cuenta que el problema al que daban solución encajaba en un conjunto complejo. A diferencia de los puntos fijos estables y los ciclos límite, este atractor caótico no es un punto o una curva o una superficie uniforme, es un fractal, con una dimensión entre dos y tres [23].

7.1.1. Propiedades más importantes del atractor de Lorenz

Para el área de la criptografía, los sistemas no lineales caóticos ofrecen un conjunto de características que son de gran valor para la construcción de modelos de cifrado acordes a las necesidades actuales y futuras, a continuación se exponen las que se consideran fundamentales para el desarrollo de este trabajo de una manera sencilla, y sin ahondar en detalles matemáticos. [23]

■ Sincronización

Una propiedad de los sistemas caóticos aprovechable para el manejo de sistemas de seguridad es la de sincronización, la cual se utiliza en el algoritmo que se presenta en este trabajo.

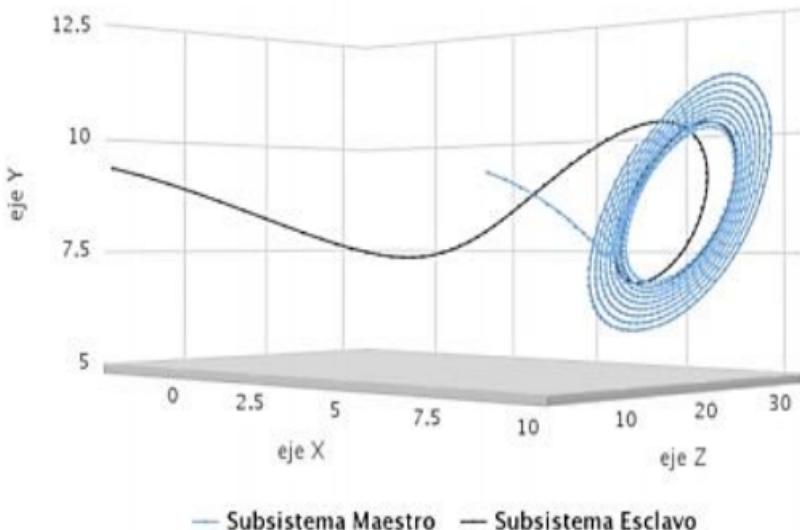


Figura 7.1: Sincronización de atractores. Fuente [1]

A partir del estudio de la presencia de oscilaciones caóticas, surgió la teoría de sincronización, originada a partir de los estudios de Louis M. Pecora y Thomas L. Carroll [24], quienes demostraron experimentalmente que pueden existir comportamientos caóticos aparentemente imprevisibles que a pesar de condiciones iniciales diferentes y cercanas, se

pueden confundir en una sola trayectoria, lo cual se consigue cuando un sistema sigue la trayectoria descrita por otro sistema o ambos siguen una nueva trayectoria. En el año 1989, Pecora y Carroll, descubrieron el sincronismo que se puede tener en atractores caóticos, descomponiendo el sistema en al menos dos subsistemas y encadenando con señales comunes, mostrando que si al menos un exponente de Liapunov es negativo, entonces los sistemas se sincronizan, lo que indica que a medida que transcurre el tiempo la trayectoria de un subsistema tenderá hacia la del otro subsistema.

Para realizar la sincronización se necesitan dos sistemas, uno es llamado sistema maestro, que es el sistema caótico original, y el otro es llamado sistema esclavo el cual se construye a partir de los subsistemas del sistema maestro, se selecciona la variable sincronizante o conductora dependiendo de la naturaleza de los exponentes de Liapunov.

Para el caso concreto del atractor de Lorenz, Pecora demostró que si se selecciona la variable y como maestra, los subsistemas se sincronizan rápidamente, como se muestra en la figura 7.1.

■ No linealidad

Siguiendo las ecuaciones planteadas por Lorenz los términos que garantizan que el sistema no sea lineal son xy y yz , esta propiedad es la que genera la naturaleza fractal

■ Simetría

Si se reemplaza $(x, y) \rightarrow (-x, -y)$ las ecuaciones seguirían siendo las mismas. Por lo tanto si $(x(t), y(t), z(t))$ entonces $(-x(t), -y(t), z(t))$ también lo es. En otras palabras todas las soluciones son simétricas o tienen un par simétrico.

■ Sensibilidad a las condiciones iniciales

Por ser un sistema dinámico caótico una de sus propiedades garantiza que cuando se hacen pequeños cambios en los valores iniciales de las variables, estos cambios pueden ocasionar diferencias impredecibles en los resultados. [7]

7.2. Cifrado de videos

El cifrado de datos es una técnica que se ha venido usando desde hace mucho tiempo con el fin de limitar tanto como sea posible el conocimiento de la información enviada. Las técnicas de cifrado han tenido cambios en la medida en que los datos a encriptar se vuelven más complejos.

Actualmente se cuenta con algoritmos de cifrado como el estándar de encriptación de datos (DES) o el Algoritmo de Encriptación de Datos Internacional (IDEA), con los que se busca realizar un manejo de información en su estado binario. Esto debido a la forma en que hoy en día se manejan los datos y las redes por donde se trasmiten.

Entre las modalidades más comunes de encriptación de datos se encuentra la de bloques y la de secuencia. La primera, es un método en el cual el mensaje se divide en bloques y el cifrado se realiza individualmente en cada bloque. La segunda, es un método en el que se cifra cada byte individualmente. [25].

7.3. Técnicas de hacking

La atención sobre cibercrímenes ha ganado popularidad en los últimos años, sin embargo mucha de esta atención se ha enfocado en prevenir que estos actos ocurran en sistemas tecnológicos con información sensible. El tema ha tenido tanta relevancia que ha llegado a que los criminólogos estudien la etiología de estos delitos cibernéticos. La realidad es algo sorprendente considerando las pérdidas económicas evaluadas en cientos de millones de dólares, lo que ha llamado la atención de los medios de comunicación [26].

Pero ¿qué es un cibercrimen?, según [27] *describiría conductas como acceder ilícitamente a un sistema informático ajeno, o la del adulto que propone a través de Internet un contacto con un menor con la intención de consumar posteriormente un abuso sexual.* para esta investigación se tienen en cuenta las conductas consistentes en acceder ilícitamente a un sistema informático ajeno.

Entre las técnicas más comunes para secuestrar, alterar o robar información se encuentran: predicción de token, ataque MITM (Man In The Middle) y ataque MITM en navegador web [28].

La predicción de token consiste en suponer la variable ID de la sesión a partir de los patrones que se obtienen del análisis del tráfico de red. Estos análisis se llevan a cabo con herramientas de criptoanálisis, cuyos métodos

consisten en capturar gran cantidad de tokens por los cuales se pueda deducir y prever las siguientes variables ID [28].

En el ataque MITM también conocido como man in the middle, el atacante se interpone entre dos dispositivos conectados (ya sea por redes físicas o inalámbricas) en modo promiscuo sin que ninguno de los interlocutores sepa que está ahí, capturando todo el tráfico. El objetivo suele ser manipular los paquetes TCP de las conexiones, infectar la máquina con malware y extraer información mediante el secuestro de las sesiones [28].

En el ataque de MITM en navegador, el atacante debe previamente infectar la máquina de la víctima con algún tipo de malware tipo troyano o RAT especial. El objetivo de este malware es realizar un MITM entre el navegador y el resto de internet directamente, almacenando todo el tráfico de red que le interese para su posterior extracción de información. Cuentas corrientes, visitas webs, emails o chats se verán comprometidos en estos secuestros de navegador. Ataques conocidos como el SSLstrip utilizan estos principios para evadir conexiones seguras HTTPS [28].

Capítulo 8

ASPECTOS METODOLÓGICOS

En este capítulo se describen los aspectos metodológicos de este trabajo de tesis a través de la definición del tipo de estudio, la explicación del método de investigación, la exposición fuentes y técnicas para la recolección de la información y los métodos para el tratamiento de la información.

8.1. Tipo de Estudio

La investigación busca formular un algoritmo que realice el cifrado de fotogramas aprovechando las características del atractor de Lorenz y pueda ser utilizado en la transmisión segura de videos en tiempo real. Por lo tanto, el tipo de estudio es formulativo.

8.2. Método de Investigación

La ejecución de este trabajo de investigación consta de cinco fases con sus correspondientes actividades principales descritas a continuación:

8.2.1. Exploratoria

En esta fase se define el campo de acción en el que se desenvuelve la investigación.

- Investigación de las fuentes relacionadas tanto con el atractor de Lorenz como con los algoritmos semejantes al que se plantea con esta investigación.

8.2.2. Diseño

En esta fase se realiza el diseño del algoritmo de cifrado de fotogramas en tiempo real.

- Análisis de herramientas de tratamiento de fotogramas.
- Selección de lenguaje de programación a utilizar para implementar la solución.
- Diseño de pasos en el proceso de cifrado.
- Selección de métricas para realizar la comparativa entre los diferentes algoritmos seleccionados de la etapa exploratoria y el desarrollado en esta investigación.
- Diseño de pruebas de streaming.
- Diseño de pruebas de rendimiento.

8.2.3. Implementación

En esta parte se realiza la implementación de todo lo definido en la fase de diseño.

- Implementación del algoritmo de cifrado de fotogramas.
- Implementación de funciones que visualicen el resultado de las métricas de rendimiento.
- Implementación de funciones que visualicen el resultado de las métricas de seguridad.

8.2.4. Resultados

En esta fase se realiza el análisis de las pruebas ejecutadas, en caso de no obtener el comportamiento deseado se evalúa la causa y en caso de ser alguna falla en el diseño se vuelve a esta etapa hasta lograr las métricas coherentes que representen el comportamiento del algoritmo.

- Evaluación del algoritmo por medio de las métricas implementadas.
- Análisis de los resultados obtenidos.

8.2.5. Documentación

En esta fase se recolecta y ajusta la documentación obtenida en los puntos anteriores para redactar el documento de tesis.

- Elaboración del documento final de tesis.

8.3. Fuentes y Técnicas para la Recolección de la Información

La recolección de datos se realiza con cámaras incorporadas a los dispositivos dispuestos para realizar la implementación y las pruebas, en este caso máquinas definidas en las limitaciones de la investigación.

8.4. Tratamiento de la Información

Luego de la extracción de los fotogramas por medio de las herramientas que se definan, se debe realizar el tratamiento de las imágenes en un formato comprensible para una máquina como matrices de tres dimensiones, a estas mismas se le realizan diferentes operaciones que están definidas en la etapa de diseño.

Capítulo 9

ALCANCES, LIMITACIONES Y RESULTADOS ESPERADOS

9.1. Alcances

Considerando la complejidad de la implementación de la propuesta, se define como alcance los siguientes aspectos:

- Usando un solo computador se deben cifrar videos obtenidos directamente desde la cámara web y se simulará el envío.
- Se contrastará el algoritmo desarrollado con propuestas que utilicen técnicas similares a las presentadas en esta investigación.
- El algoritmo va a especificar los pasos para realizar el cifrado, no garantiza que dada su ejecución haya seguridad a nivel del canal o de hardware.

9.2. Limitaciones

Dado que para resolver este problema es necesario contar con una serie de recursos humanos, de hardware y de software, se presentan ciertas limitaciones

que se deben tener en cuenta a lo largo del proyecto. Dentro de las principales limitaciones se contemplan las siguientes:

- Se requieren herramientas que provean a la investigación de mecanismos para la recolección y tratamiento de fotogramas sin perder información.
- Los vídeos que serán encriptados no tendrán audio, ya que el objetivo es lograr encriptar los fotogramas de un vídeo únicamente.
- Para la implementación del algoritmo se planea utilizar alguna herramienta de construcción de software lo suficientemente capaz de manejar fotogramas, por lo que se requerirán recursos de procesamiento medios, es decir, máquinas con al menos 8GB, un procesador al menos de cuarta generación, entre otras que permiten la ejecución y pruebas del algoritmo.

9.3. Resultados Esperados

El algoritmo desarrollado será capaz de cifrar los fotogramas de un vídeo transmitido en tiempo real, cumpliendo con los umbrales en las métricas propuestas para evaluarlo.

Capítulo 10

ALGORITMO PROPUESTO

Los pasos que se siguen en el algoritmo desarrollado se esquematizan en la figura 10.1 y se detallan a continuación:

1. El atractor de Lorenz se divide en dos subsistemas maestro y esclavo, utilizamos como variable sincronizante a y , debido a que sus exponentes de Lyapunov son los más negativos (entre más negativos sean éstos, más rápida será la convergencia).
2. Se inicializan los subsistemas con condiciones iniciales aleatorias que estén cercanas a la región del atractor.
3. Se sincronizan los atractores enviando la componente maestra hacia el esclavo. Se generan los 2500 primeros valores del atractor maestro utilizando Runge Kutta 4, con un salto $h = 0,01$ (centésimas de segundo) y se envían los resultados como clave pública k hacia el atractor esclavo.
4. Se toman fotogramas del video cada 0.03 segundos.
5. Se considera un fotograma I de longitud mXn . A partir de Runge Kutta 4 aplicado al atractor de Lorenz, se construye una sucesión S_c de longitud mXn , comenzando en la iteración 2501. Los primeros $m+n$ valores de la sucesión S_c serán usados para el proceso de permutación, mientras que los n valores siguientes serán usados para el proceso de difusión.

Para permutar las filas se aprovechan los primeros m valores obtenidos en la componente x de la sucesión S_c , donde cada valor indica el número

de posiciones que se debe desplazar cada uno de los píxeles de la fila de forma circular hacia la derecha si el valor x es positivo, y hacia la izquierda si es negativo. Posteriormente se usan los siguientes n valores de la componente x de la sucesión S_c para indicar el número de posiciones que se debe desplazar de forma circular cada uno de los píxeles de las columnas del fotograma hacia abajo si el valor de la sucesión es positivo o hacia arriba en caso de ser negativo, obteniendo la matriz de permutación P .

Matemáticamente el desplazamiento de cada uno de los píxeles está dado por la ecuación 10.1.

$$\begin{aligned} I_{ij} &= I_{i((j+S_{C_i}^x) \bmod (n+1))} \\ I_{ij} &= I_{((i+S_{C_{m+j}}^x) \bmod (m+1))j} \end{aligned} \quad (10.1)$$

Donde $S_{C_i}^x$ corresponde a la componente x de la posición i de la sucesión S_c , este tipo de desplazamiento, se le denomina circular, ya que los píxeles de toda una fila o columna son desplazados una cierta cantidad de posiciones y si se pasa de la última posición, se sigue el conteo a partir de la primera posición de la fila o columna. Por simplicidad el resultado de éste proceso se denota por $perm$, dado en la ecuación 10.2.

$$P = perm(I) = perm \left(\begin{vmatrix} I_{11} & \dots & I_{1n} \\ \dots & \dots & \dots \\ I_{m1} & \dots & I_{mn} \end{vmatrix} \right) \quad (10.2)$$

6. Para el proceso de difusión se utilizan los primeros valores obtenidos por la sucesión S_c desde el 2501 al $2501+m$ para generar un vector columna y repetirlo n veces hasta construir una matriz de difusión D .
7. Se suman vectorialmente los valores del fotograma permutado P con la matriz de difusión D . El fotograma cifrado C , corresponde a la ecuación 10.3.

$$C = (P + D) \bmod 256 \quad (10.3)$$

Los pasos anteriores se repiten para cada fotograma generando la encriptación del vídeo.

Cabe mencionar que para recuperar la información se debe realizar el proceso anteriormente descrito pero de manera inversa, es decir se iniciaría con el proceso de difusión ya que fue el último en realizarse. Si para realizar la difusión se efectuaron sumas, para recuperar la información se deben realizar restas, al terminar la ejecución de lo anterior se obtendrá el contenido multimedia de nuevo tal cual como se envío.

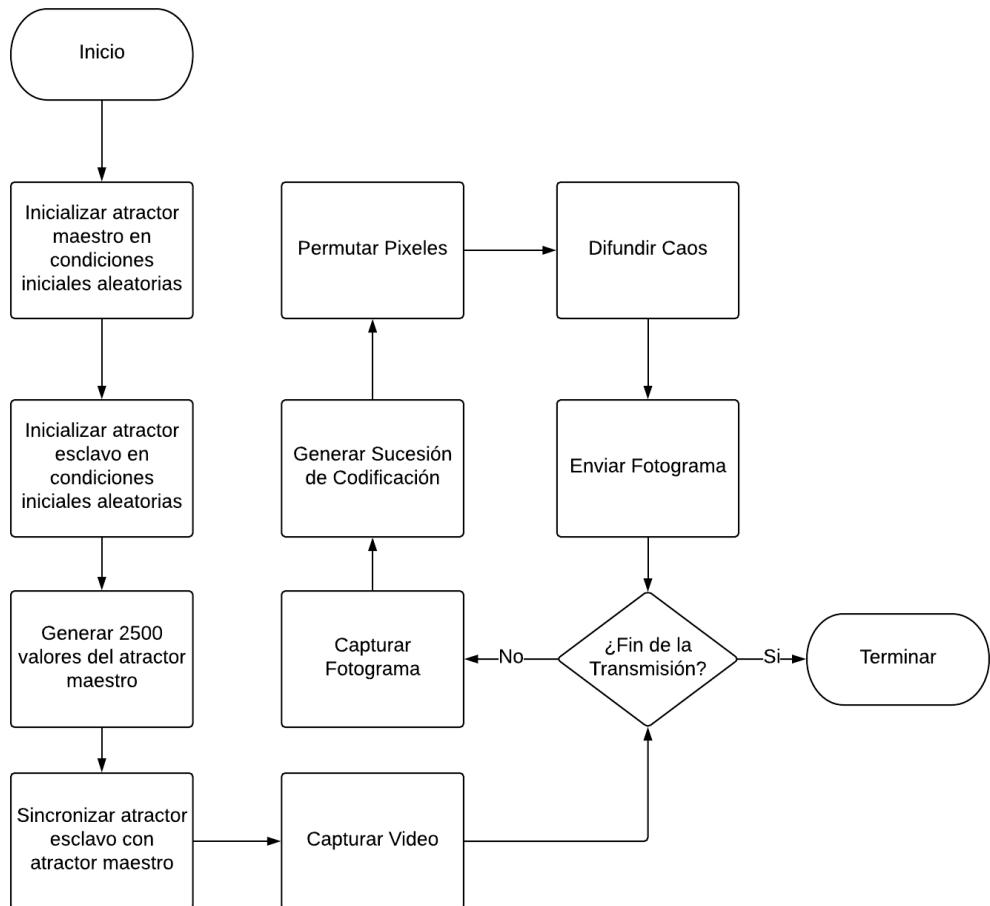


Figura 10.1: Descripción del algoritmo utilizado para realizar el proceso de encriptación.

Capítulo 11

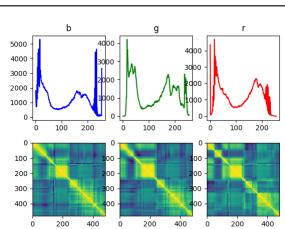
METODOLOGÍA

La primera fase de trabajo consistió en la apropiación de la fundamentación conceptual de la teoría de sistemas dinámicos caóticos y la forma de involucrar los atractores caóticos en la criptografía, utilizando además la propiedad de sincronización.

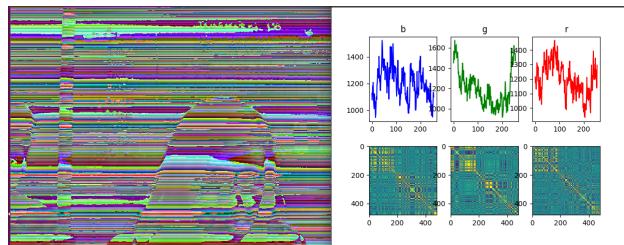
Aprovechando las fortalezas de las técnicas mostradas en las referencias [7, 8, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24] y considerando los requerimientos para transmisión de videos en tiempo real, se propone una técnica basada en el atractor de Lorenz y el principio de sincronización para encriptar ágilmente los fotogramas sin perder tiempo en el envío de claves, para lograr esto se utiliza una única clave, llamada clave de sincronización, que se comparte entre el emisor y receptor y cuya seguridad depende del canal de envío, que es usada para sincronizar el atractor receptor con el atractor emisor. Para la implementación del algoritmo propuesto se seleccionó la librería CV2 del lenguaje Python, que permite manipular fácilmente los fotogramas capturados por la cámara de video.

Se realizaron diferentes pruebas de rendimiento y seguridad enfocadas al orden que deberían llevar los procesos de permutación y difusión. Se ejecutaron tres pruebas de seguridad, en la primera solo se difunde, notando que algunos contornos del fotograma original de la Figura 11.1a, eran visibles, como se observa en la Figura 11.1b. En la segunda prueba solo se utilizó permutación, el fotograma pierde totalmente su apariencia original, como se evidencia en la Figura 11.1c. En la tercera prueba se utilizan los dos procesos de difusión y permutación, observando que si se aplica primero permutación y luego difusión, la correlación aunque mínima sigue presente (Figura 11.1d),

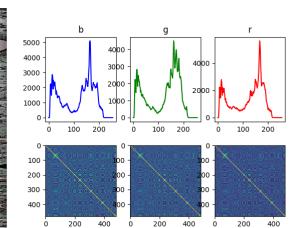
pero implementando primero la difusión y luego permutación (Figura 11.1e), se lograron mejores indicadores y un impacto imperceptible en el rendimiento del algoritmo.



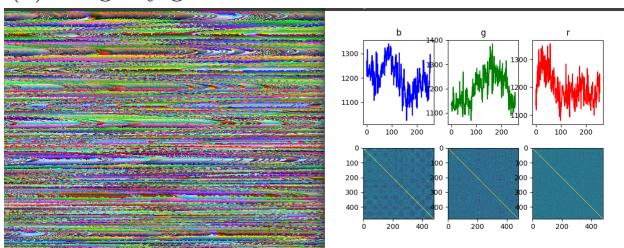
(a) Imagen y gráficos de correlación originales



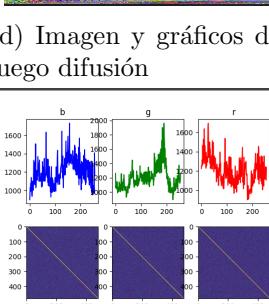
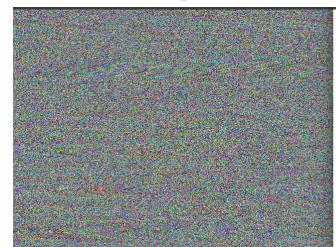
(b) Imagen y gráficos de correlación solo con difusión



(c) Imagen y gráficos de correlación solo con permutación luego difusión



(d) Imagen y gráficos de correlación con permutación y



(e) Imagen y gráficos de correlación con difusión y luego
permutación

Figura 11.1: Pruebas de Cifrado

Capítulo 12

RESULTADOS

12.1. RENDIMIENTO DEL ALGORITMO

Los tiempos de cifrado y descifrado por fotograma en promedio son 0.148201 y 0.143025 segundos respectivamente, estos resultados se obtuvieron utilizando una máquina con un procesador intel core i5 2,4 GHz de 4 núcleos, y una memoria RAM de 8 Gb.

12.2. ESPACIO DE CLAVE

El análisis del espacio de clave es importante para evaluar la seguridad del algoritmo en el caso de que un intruso intente realizar un ataque por fuerza bruta, tratando de acertar a la clave de sincronización por iteración. Calcular el espacio de clave inicial (2500 valores) implica considerar los límites para el atractor caótico de Lorenz (de -10 a 10 para la coordenada en x, de -15 a 15 en la coordenada , y de 0 a 40 en la coordenada), y la unidad de tiempo considerada para el atractor de 0.01, por lo que para cada intervalo de solo una unidad, por ejemplo de -10.00 a -9.00 se encuentran 100 valores, solamente con la componente en x se generarían 2000 números, lo que resulta en 2×10^{10} posibles combinaciones para obtener un punto de coordenadas (x, y, z) , si se tiene en cuenta también que la longitud de la clave es de 2500, el espacio de clave resulta ser 6×10^{13} . Es válido destacar que este espacio de clave es exponencial en la medida en que la unidad de tiempo se reduzca.

12.3. ATAQUES INFERENCIALES

Las métricas UACI (Unified Average Changing Intensity) y NPCR (Number of Pixels Change Rate) se basan en el impacto que puede causar el cambio de un sólo píxel de un fotograma cifrado, usado comúnmente por los atacantes para reconocer un patrón sobre los fotogramas arrojados por los algoritmos de encriptación. El NPCR es la tasa de cambio de píxeles y mide el porcentaje de píxeles diferentes entre dos fotogramas, mientras el UACI es el promedio unificado de intensidad de cambio y mide en porcentaje la diferencia entre dos fotogramas. Las expresiones para el NPCR y el UACI, son dadas por las ecuaciones 12.1 y 12.2.

$$NPCR = \frac{1}{M * N} \sum D(i, j) * 100 \% \quad (12.1)$$

$$UACI = \frac{1}{M * N} \sum \frac{|E_1(i, j) - E_2(i, j)|}{2^n - 1} * 100 \% \quad (12.2)$$

donde M y N representan respectivamente el ancho y alto del fotograma. C_1 , C_2 , denotan dos fotogramas con un sólo píxel de diferencia $D(i, j) = 0$, si $C_1(i, j) = C_2(i, j)$ y 1 en caso contrario. Se considera que entre más cercano esté el $UACI$ a 33,4635 % y el $NPCR$ a 99,6094 % mayor es la seguridad que ofrece el algoritmo. Los resultados para el algoritmo desarrollado en este trabajo fueron en promedio 37.2395833333 % y 99.6327 % para el $UACI$ y el $NPCR$ respectivamente.

12.4. ENTROPIA

La entropía mide esencialmente aleatoriedad o imprevisibilidad, en el caso de la criptografía, la entropía aumenta cada vez que el elemento a cifrar se hace más irreconocible, lo que actúa a favor en el caso de un ataque. La expresión para el cálculo de la entropía está dada por la ecuación 12.3.

$$H(s) = \sum_{i=1}^N P(S_i) \log_2 \frac{1}{P(S_i)} \quad (12.3)$$

donde, $P(S_i)$ es la probabilidad de ocurrencia de una intensidad de color. Para el caso de estudio tratado en este trabajo la entropía tuvo un valor de

7.9812 en promedio, lo cual indica un buen comportamiento de aleatoriedad, ya que el valor ideal es 8.

12.5. SENSIBILIDAD DE LA CLAVE

Dada la naturaleza de los atractores caóticos, cualquier cambio en las condiciones iniciales genera un resultado completamente distinto y aleatorio, esto mismo se aplica para el algoritmo desarrollado en este trabajo, todo cambio en las condiciones iniciales del atractor genera claves completamente distintas. El ejemplo más claro de esto se evidenció al desplazar una unidad de tiempo (0.01) uno de los atractores (maestro o esclavo), y tratar de recuperar de forma fallida un fotograma encriptado previamente como se muestra en la figura 12.1d, el resultado puede ser descrito como un fotograma con una doble encriptación y sin ninguna similitud con el fotograma anterior. En la figura 12.1a se observa un fotograma original, con su respectivo cifrado y descifrado, evidenciando la recuperación fidedigna del fotograma original 12.1c.

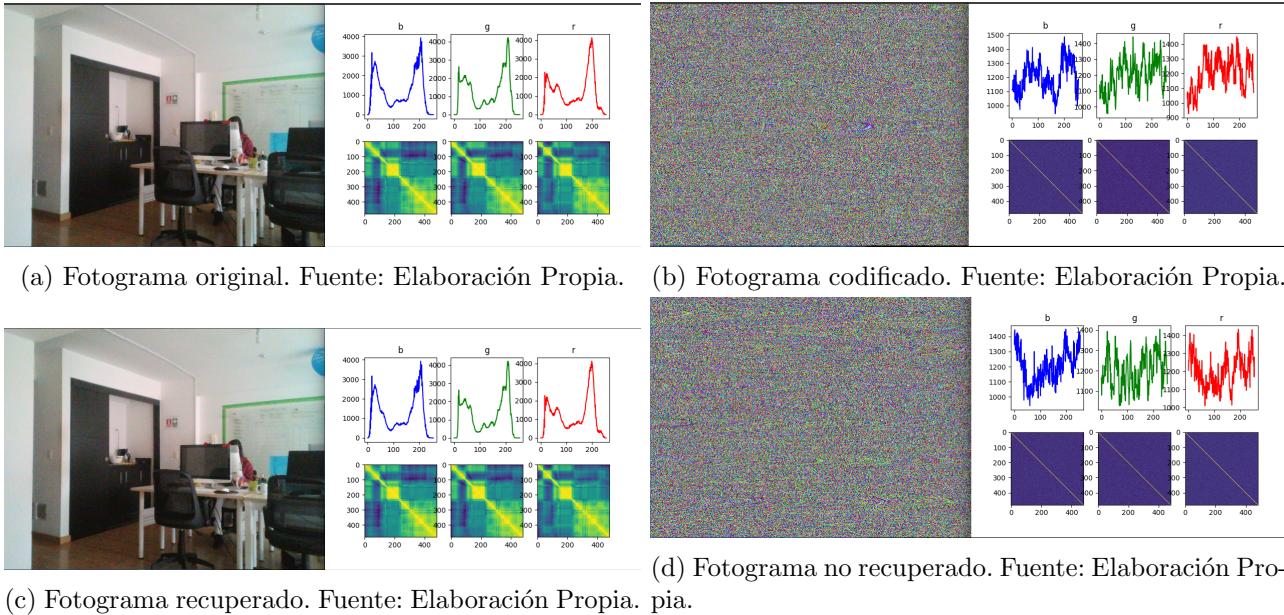


Figura 12.1: Sensibilidad de Clave

12.6. GRÁFICAS DE CORRELACIÓN Y DENSIDAD DE PÍXELES

En la Figura 12.2a, se muestran las gráficas correspondientes a la densidad de píxeles, y la correlación entre píxeles adyacentes en cada capa de color de un fotograma original. En la Figura 12.2b se presentan los mismos esquemas anteriores pero ahora sobre el fotograma cifrado. Como se puede ver en la Figura 12.2a hay una agrupación de píxeles en la línea de correlación, lo que indica que los píxeles adyacentes mantienen una fuerte correlación, mientras que en la Figura 12.2b se observa todo lo contrario.

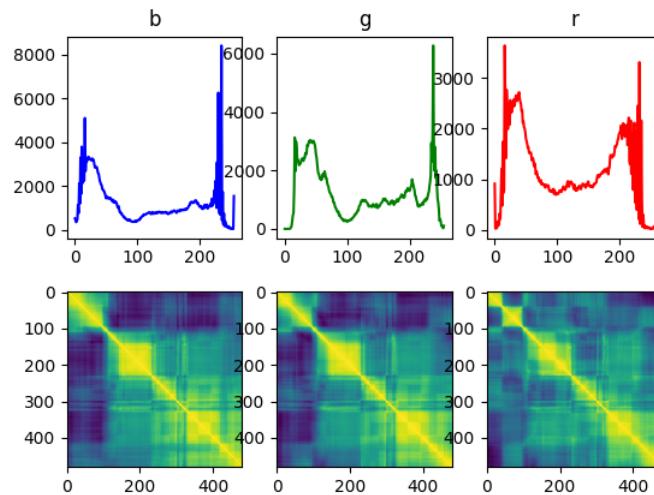
12.7. ANÁLISIS COMPARATIVO

Para validar la propuesta presentada en este trabajo se compararon los coeficientes de correlación y las medidas $NPCR$ y $UACI$ obtenidas, con los resultados presentados en las referencias [18] y [29], obteniendo valores muy cercanos a los reportados en otras referencias en estudio, como se sintetiza en la tabla 12.1.

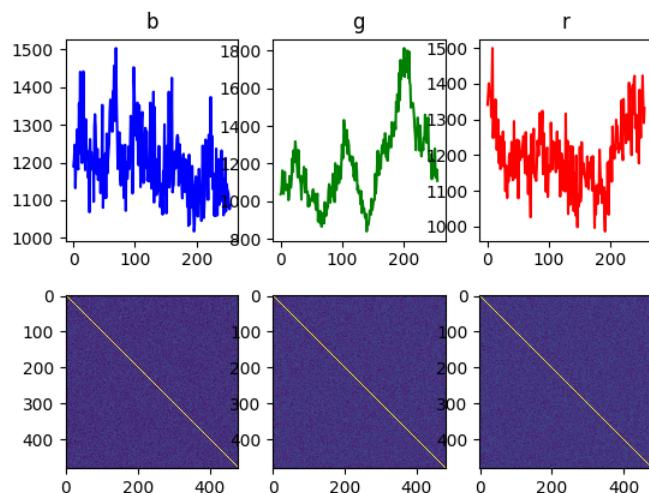
Ref	Corr. Ho- rizontal	Corr. Ver- tical	Corr. Dia- gonal	NCPR (%)	UACI(%)
[10]	0.004080	0.017499	-0.082758	99.6196	50.13
[20]	0.000136	0.000691	0.0025	99.6090	33.4663
Prop.	0.003861	0.002680	0.000502	99.6327	37.2395

Cuadro 12.1: Comparación de resultados obtenidos.

Evidenciando que los índices de correlación se encuentran muy cercanos a 0, esto indica que la relación entre los píxeles adyacentes es débil [24].



(a) Gráficas de densidad de píxeles y correlación entre píxeles adyacentes por capa de color de un fotograma original. Fuente: Elaboración Propia.



(b) Gráficas de densidad de píxeles y correlación entre píxeles adyacentes por capa de color de un fotograma cifrado. Fuente: Elaboración Propia.

Figura 12.2: Gráficas de Correlación

Capítulo 13

CONCLUSIONES

13.1. Verificación, contraste y evaluación de objetivos

Es posible por medio de la teoría del caos lograr un nivel alto de seguridad en la transmisión de videos por redes públicas en tiempo real, contribuyendo de esta forma mediante un ejercicio académico a motivar a otros investigadores interesados en el área de seguridad informática a seguir profundizando en ésta temática.

El producto de este trabajo es un algoritmo desarrollado con el lenguaje de programación Python 3, que cuenta con varias librerías que fueron usadas para el manejo de fotogramas, por lo que para la implementación del algoritmo, solo hubo que concentrarse en la estrategia para permutar y difundir caos en cada iteración, el modelo base para el mismo surgió de la recolección de datos realizado fácilmente gracias a las membresías con las que cuenta la universidad para el acceso a bibliotecas digitales como la IEEE, Spring, entre otras.

Como se evidenció en la sección de resultados, el comportamiento del algoritmo es el esperado, y puede ser usado en casos reales, Se debe resaltar que entre los algoritmos estudiados en otros artículos este sería uno que combina encriptación con técnicas que aplican teoría del caos y videos transmitidos en tiempo real.

13.2. Aportes Originales

- En el sistema de encriptación propuesto se implementaron las técnicas de difusión y permutación para generar un esquema de seguridad robusto en la transmisión de videos en tiempo real. Gracias a la propiedad de sincronización se logró disminuir el tiempo necesario para el cifrado y descifrado de los fotogramas, generando un retardo de 0.15 segundos apróximadamente imperceptible para el ojo humano, lo que lo hace apropiado para utilizarse en transmisión en tiempo real.
- Con relación al análisis de espacio de clave conviene resaltar que aunque sólo se tomó en cuenta la clave de sincronización, es decir, la primera secuencia generada para la sincronización del atractor maestro con el atractor esclavo, si se tomaran en cuenta el resto de las llaves generadas para la encriptación del video en tiempo real, el espacio de clave crecería exponencialmente. Si se requiere de un espacio de clave más grande, se puede aumentar la precisión del algoritmo (número de decimales utilizados), con lo que el tiempo de sincronización sería menor.
- Los tiempos requeridos cifrando y descifrando son mínimos, logrando que a la hora de recuperar la información del video éste no contenga retrasos en la renderización, lo que lo hace apropiado para utilizarse en tiempo real.
- Como trabajo futuro, se plantea experimentar con otro tipo de atractores caóticos y mezclar a este proceso el cifrado, envío y descifrado de audio

Bibliografía

- [1] Iván Rodríguez Rodríguez, Edilma Amaya Barrera, Cesar Suarez Parra, and José Moreno Posada. Images encryption algorithm using the lorenz's chaotic attractor. *Ingeniería*, 22(3):396–412, Sep. 2017.
- [2] Jhonny Pabón Cadavid. La criptografía y la protección a la información digital. *Revista La Propiedad Inmaterial*, (14):59–90, nov. 2010.
- [3] Andrew Hodges. *Alan Turing: The Enigma*. Walker & Company, 2000.
- [4] C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27(3):379–423, July 1948.
- [5] C. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, Vol 28, pp. 656–715, Oktober 1949.
- [6] Eduardo. Silva Ortigoza Ramón Molina Vilchis, María Aurora. Vega Alvarado. Teoría del caos en la protección de información. *Polibits [en linea]*, 2007.
- [7] Zhaopin Su, Shiguo Lian, Guofu Zhang, and Jianguo Jiang. *Chaos-Based Video Encryption Algorithms*, pages 205–226. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.
- [8] Hui Xu, Xiaojun Tong, and Xianwen Meng. An efficient chaos pseudo-random number generator applied to video encryption. *Optik*, 127(20):9305 – 9319, 2016.
- [9] José Moreno, Fabio Parra, Rafael Huérano, Cesár Suarez, and Isabel Amaya. Symmetric encryption model based on chaotic attractors. 21:378–390, 12 2016.

- [10] Rafael Jiménez, Enrique Gordillo, and Gustavo Rubiano. *Teoría de números para principiantes*. Xpress Estudio Gráfico y Digital S.A., Bogotá, D.C., 2012.
- [11] F. Peng, X. Zhu, and M. Long. An roi privacy protection scheme for h.264 video based on fmo and chaos. *IEEE Transactions on Information Forensics and Security*, 8(10):1688–1699, Oct 2013.
- [12] Shiguo Lian, Jinsheng Sun, Zhiqian Wang, and Yuwei Dai. A fast video encryption scheme based-on chaos. In *ICARCV 2004 8th Control, Automation, Robotics and Vision Conference, 2004.*, volume 1, pages 126–131 Vol. 1, Dec 2004.
- [13] Jiménez-Rodríguez Maricela, Flores-Siordia Octavio, and González-Novoa María Guadalupe. Sistema para codificar información implementando varias órbitas caóticas. *Ingeniería, Investigación y Tecnología*, 16(3):335 – 343, 2015.
- [14] F. Chiaraluce, L. Ciccarelli, E. Gambi, P. Pierleoni, and M. Reginelli. A new chaotic algorithm for video encryption. *IEEE Transactions on Consumer Electronics*, 48(4):838–844, Nov 2002.
- [15] Z. Lin, S. Yu, J. Lu, S. Cai, and G. Chen. Design and arm-embedded implementation of a chaotic map-based real-time secure video communication system. *IEEE Transactions on Circuits and Systems for Video Technology*, 25(7):1203–1216, July 2015.
- [16] Shiguo Lian. Efficient image or video encryption based on spatiotemporal chaos system. *Chaos, Solitons and Fractals*, 40(5):2509 – 2519, 2009.
- [17] Xiaochun Cao, Meili Ma, Xiaojie Guo, Ling Du, and Dongdai Lin. A new encryption scheme for surveillance videos. *Frontiers of Computer Science*, 9(5):765–777, Oct 2015.
- [18] M. M. Elkholly, H. M. El Hennawy, A. Elkouny, and S. Zahran. Using hyper chaos in secure video transmission. In *2016 28th International Conference on Microelectronics (ICM)*, pages 65–68, Dec 2016.
- [19] V. Alirezaei and M. Yaghbi. Efficient video encryption by image key based on hyper-chaos system. In *2010 International Conference on Multimedia Communications*, pages 141–144, Aug 2010.

- [20] Hazem M. Al-Najjar and Asem Mohammad Al-Najjar. Image encryption algorithm based on logistic map and pixel mapping table. 2011.
- [21] Sodeif Ahadpour and Yaser Sadra. A chaos-based image encryption scheme using chaotic coupled map lattices. *International Journal of Computer Applications*, 49(2):15–18, Jul 2012.
- [22] Kamlesh Gupta and Sanjay Silakari. New approach for fast color image encryption using chaotic map. *J. Information Security*, 2:139–150, 01 2011.
- [23] Steven Strogatz, Mark Friedman, A. John Mallinckrodt, and Susan McKay. Nonlinear dynamics and chaos: With applications to physics, biology, chemistry, and engineering. *Computers in Physics*, 8(5):532–532, 1994.
- [24] Louis Pecora and T Carroll. Synchronization in chaotic system. *Physical Review Letters*, 64:821, 03 1990.
- [25] IBM. Tipos de cifrado y modalidades de cifrado., 2013.
- [26] R. G. Morris. *Computer Hacking and the Techniques of Neutralization: An Empirical Assessment*. Hershey, PA: IGI Global, Bogotá, D.C., 2011.
- [27] Fernando Miró Llinares. El cibercrimen. fenomenología y criminología de la delincuencia en el ciberespacio. *Marcial Pons, Madrid*, 2012.
- [28] Cristian Jiménez Jiménez. Seguridad en redes y sistemas: Técnicas y conceptos sobre hacking y pentesting., 2016.
- [29] S. Kotel, F. Sbiaa, M. Zeghid, M. Machhout, A. Baganne, and R. Tourki. Efficient hybrid encryption system based on block cipher and chaos generator. In *2016 IEEE International Conference on Computer and Information Technology (CIT)*, pages 375–382, Dec 2016.