UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

FACULTAD DE INGENIERÍA, ARQUITECTURA Y DISEÑO

CIFRADO CAÓTICO DE IMÁGENES MÉDICAS PARA E-SALUD

TESIS

que para cubrir parcialmente los requisitos necesarios para obtener el título de

INGENIERO EN ELECTRÓNICA

presenta:

Alonso Ibarra Barrios

Ensenada, Baja California, México, Junio de 2025.

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA
FACULTAD DE INGENIERÍA, ARQUITECTURA Y DISEÑO

"Cifrado caótico de imágenes médicas para e-salud"

TESIS

PARA CUBRIR LOS REQUISITOS NECESARIOS PARA OBTENER EL TÍTULO DE

Ingeniero en Electrónica

PRESENTA

Alonso Ibarra Barrios
338934

A quien el Comité de Tesis autoriza el trabajo terminal, después de haber efectuado una revisión minuciosa del mismo y de acuerdo con el Art. 19 del R.G.E.P.E.P, las y los señores profesores emiten los siguientes votos aprobatorios mediante rúbrica:

Dra. Rosa Martha López Gutiérrez
DIRECTOR

Dr. Miguel Angel Murillo Escobar
CODIRECTOR

Mtra. Eltania Jiménez García
SINODAL

Dr. César Cruz Hernández
SINODAL

Dr. Adrian Arellano Delgado
SINODAL

"Por la Realización Plena del Ser"

C.c.p.- Archivo
C.c.p.- Minutario

RESUMEN de la tesis presentada por Alonso Ibarra Barrios, como requerimiento parcial para obtener el título de **INGENIERO EN ELECTRÓNICA**, del programa de Licenciatura de la **Universidad Autónoma de Baja California**, Ensenada, Baja California, México. Junio de 2025.

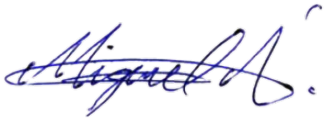
CIFRADO CAÓTICO DE IMÁGENES MÉDICAS PARA E-SALUD

Este trabajo presenta el diseño e implementación de un algoritmo de cifrado caótico para la protección de imágenes médicas en aplicaciones de e-salud. La creciente digitalización y transmisión de información sensible en el ámbito médico demanda soluciones robustas que garanticen la privacidad, integridad y disponibilidad de los datos. El sistema propuesto utiliza el mapa logístico para generar claves caóticas, combinadas con técnicas de permutación de bloques y operaciones XOR, logrando ocultar eficazmente el contenido visual de las imágenes. La implementación se realizó en MATLAB, evaluando la calidad de la encriptación mediante análisis de histogramas, cálculo de entropía y del exponente de Lyapunov. Los resultados muestran un alto nivel de aleatoriedad y sensibilidad a las condiciones iniciales, evidenciando la eficacia del esquema frente a ataques de fuerza bruta y análisis estadísticos. Este enfoque contribuye a mejorar la seguridad de los sistemas de telemedicina y sienta las bases para futuras investigaciones en criptografía caótica aplicada a entornos médicos.

Palabras clave: criptografía caótica, telemedicina, e-salud, imágenes médicas, mapa logístico, entropía, exponente de Lyapunov.

Resumen aprobado por:

Dra. Rosa Martha López Gutiérrez



Dr. Miguel Ángel Murillo Escobar

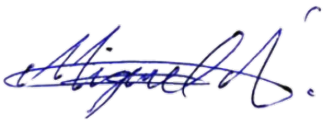
ABSTRACT of the thesis presented by Alonso Ibarra Barrios, as a partial fulfillment of the requirements for the degree of **Bachelor of Science in Electronics Engineering**, from the undergraduate program at the **Universidad Autónoma de Baja California**, Ensenada, Baja California, Mexico. June 2025.

CHAOTIC ENCRYPTION OF MEDICAL IMAGES FOR E-HEALTH

This work presents the design and implementation of a chaotic encryption algorithm for protecting medical images in e-health applications. The increasing digitization and transmission of sensitive medical information demand robust solutions that ensure data privacy, integrity, and availability. The proposed system employs the logistic map to generate chaotic keys, combined with block permutation techniques and XOR operations, effectively concealing the visual content of the images. The implementation was carried out in MATLAB, with the encryption quality evaluated through histogram analysis, entropy calculation, and Lyapunov exponent measurement. The results demonstrate a high level of randomness and sensitivity to initial conditions, highlighting the scheme's effectiveness against brute-force attacks and statistical analyses. This approach enhances the security of telemedicine systems and lays the groundwork for future research in chaotic cryptography applied to medical environments.

Keywords: chaotic cryptography, telemedicine, e-health, medical images, logistic map, entropy, Lyapunov exponent.

Dra. Rosa Martha López Gutiérrez



Dr. Miguel Ángel Murillo Escobar

A mi familia, quienes han formado parte de cada etapa importante en mi vida.

A mi Familia, mis padres Alonso y Bertha, mi abuela Manuela, que con su apoyo y amor incondicional me han impulsado a luchar y materializar mis sueños.

Al Dr. Miguel Ángel Murillo Escobar, por su guía y orientación en la elaboración de este trabajo y durante la carrera, y por su paciencia y confianza puesta en mí a lo largo de este proyecto.

A la Dra. Rosa Martha López Gutiérrez, por su invaluable acompañamiento a lo largo de mi formación profesional. Su ejemplo y apoyo quedarán siempre como una referencia en mi desarrollo académico y personal.

Al Comité de Tesis, por el tiempo y la disposición dedicados al análisis y evaluación de este trabajo. Valoro profundamente el compromiso que implica revisar este trabajo con detenimiento, y agradezco la atención brindada a los resultados y aportaciones presentados.

A la Universidad Autónoma de Baja California (UABC), por brindarme la oportunidad de perseguir un futuro profesional de calidad.

Al Consejo Nacional de Humanidades, Ciencia y Tecnología (CONAHCYT), por el apoyo económico brindado a través del Proyecto de Investigación en Ciencia Básica entre instituciones, "Sincronización de Sistemas Complejos y Algunas Aplicaciones". (A1-S-31628).

Ensenada, B.C., México.
Junio de 2025.

Alonso Ibarra Barrios

Tabla de Contenido

Lista de Figuras

Capítulo 1

Introducción

En la actualidad, las tecnologías de la información y de la comunicación se han establecido como pilares fundamentales para el desarrollo social y económico de nuestras sociedades. Es por ello que se puede observar una creciente transmisión tanto de datos personales como no-personales que requieren en menor o mayor medida ciertos niveles de seguridad para su transmisión, con el fin de asegurar que solo las partes involucradas puedan tener acceso a los datos confidenciales.

Diferentes servicios, tales como seguros, gubernamentales, bancarios, servicios médicos, etc., dependen de la información personal para funcionar eficientemente. Además, hay que tomar en cuenta que la difusión de datos personales no afecta solo al sujeto involucrado sino también a las vidas de sus familiares, amigos y miembros de su círculo social más cercano.

En cuanto a la información personal, hay que tomar en cuenta que su pérdida, reproducción no autorizada, o incluso robo, no resulta en una pérdida económica solamente, sino que también afecta al usuario en cuestión. De hecho, esta manipulación de datos personales no autorizada puede tener repercusiones tan graves como el fraude o el uso indebido de la identidad.

Asimismo, la violación a la privacidad de los datos personales puede llegar a ocurrir sin el conocimiento del dueño, haciendo que la tarea de rastrear y castigar a los responsables sea más difícil.

De ahí el especial interés por encontrar opciones que satisfagan dicha necesidad por la privacidad y la seguridad en la transmisión de datos.

Es en este contexto que se propone a la criptografía como un método fiable para la seguridad de la información transmitida a través del internet. La criptografía, siendo la disciplina que estudia la secrecía en las comunicaciones, asegura que la información enviada sea recibida solamente por el destinatario. Incluso si dicha información fuera interceptada, no podría ser entendida por algún tercero, a menos de que fuera desencriptada y, por lo tanto, el tercero no llegaría tener acceso a la información.

1.1. Motivación

Diversos sectores se han beneficiado de las contribuciones de las tecnologías de la información y las ventajas que éstas ofrecen, tal como el sector de la salud. Los sistemas electrónicos del sector salud almacenan y comparten diferentes tipos de archivos tales como imágenes médicas, historial médico digital del paciente, así como otros datos sensibles relacionados tanto con el paciente como con el hospital que lo atiende.

Estos archivos médicos son un tipo muy delicado de información, razón por la cual se han aplicado diferentes estrategias y técnicas a través de los años con el objetivo de salvaguardar su privacidad. Una de dichas técnicas es la de la criptografía, la cual se encarga de cambiar la información de su forma comprensible y clara a una forma confusa y ambigua.

Incluso, un ciberataque cuyo propósito sea el de robar información médica delicada puede llegar a limitar la capacidad operativa del hospital o centro de salud afectado. No es extraño leer noticias relacionadas con ello en las que se recuenta el nivel de afectación alcanzado, como en el ataque de un hospital en España, durante el cual, toda la operación dentro del mismo se vio limitada a aquellas actividades que no requirieran una computadora, debido a que no podían consultarse historias clínicas, ni llevarse a cabo pruebas. Además, la información médica filtrada fue difundida en la dark web, entre cuyos archivos se encontraban fotografías, identificaciones e informes médicos.

1.2. Objetivo general

Diseñar e implementar un algoritmo de cifrado caótico de imágenes médicas para aplicaciones de e-salud.

1.3. Objetivos particulares

- Implementar un sistema caótico en el software de Matlab.
- Comprobar la dinámica caótica con el exponente de Lyapunov.
- Implementar el algoritmo desarrollado mediante programación en Matlab para la encriptación y desencriptación de imágenes médicas.
- Realizar análisis de seguridad a los criptogramas obtenidos en Matlab.

1.4. Organización del manuscrito

- **Capítulo 1**: se presenta el tópico principal del tema mediante una breve introducción, así como la motivación que respalda la realización del presente trabajo, y, finalmente, los objetivos perseguidos por la tesis.
- **Capítulo 2**: se presenta la telemedicina como una aplicación con rasgos muy particulares de la medicina, una breve reseña histórica de la misma, sus campos de aplicación y algunos aspectos importantes a considerar relacionados con la seguridad de la información tratada por ella.
- **Capítulo 3**: se presenta al caos como disciplina, las principales propiedades de un sistema caótico, así como sus principales clasificaciones y los sistemas caóticos estudiados en el presente trabajo.
- **Capítulo 4**: se desarrolla el algoritmo propuesto cuyo objetivo es el de la encriptación y desencriptación de imágenes médicas.
- **Capítulo 5**: se exponen las conclusiones, se mencionan las contribuciones del presente trabajo de investigación, así como algunos puntos para su consideración dentro de un trabajo a futuro.

Capítulo 2

Fundamentos teóricos

2.1. E-Salud

Haciendo una remembranza de las experiencias recopiladas durante la pandemia de COVID-19 en los años pasados, podemos notar que la dificultad al acceso a los servicios de salud en distintos países se elevó, con lo que se debieron buscar alternativas para satisfacer esta importante demanda. De hecho, la ONU realizó una recomendación a través de la cual declaraba que la enfermedad podía controlarse a través de una serie de confinamientos o cuarentenas con el fin de que el virus no se propagara.

Con la vivencia de la pandemia se aceleraron los procesos para la disminución de las dificultades existentes para el acceso a la salud en las poblaciones cuyas condiciones las ponen en situaciones vulnerables.

Es interesante también constatar que los términos de e-Salud, e-Health y salud en línea se han popularizado, tal como constata el sitio web Google Trends. Eso nos indica un creciente interés por parte de los usuarios del mencionado buscador web en temas novedosos relacionados con la salud, lo cual seguramente no hará sino aumentar tomando en cuenta los hechos ocurridos en los pasados dos años.

2.1.1. Objetivos de la e-salud

De entre los objetivos planteados por la OMS con relación a la e-salud (también llamada cibersalud), podemos destacar el mejorar el acceso a los servicios de salud y su calidad, gracias a la utilización de las tecnologías de la información y la comunicación, la formación en alfabetización digital, el acceso a información basada en pruebas científicas y formación continua y la implementación de diversos métodos con el fin último de apoyar la formación de sociedades democráticas y más informadas.

La estrategia de e-salud de la OMS se basa principalmente en los siguientes ejes:

- Registro médico electrónico (o historia clínica electrónica).
- Telesalud (incluyéndose la telemedicina).
- mSalud (salud por dispositivos móviles).
- eLearning (formación y aprendizaje a distancia).
- Educación continua en tecnologías de la información y la comunicación.
- Estandarización e interoperabilidad.

Con relación a la información de imágenes médicas, hay ciertos criterios básicos que deben cumplirse en sistemas de seguridad de e-salud, los cuales podemos resumir en los siguientes tres:

- **Confidencialidad**: significa que los sistemas de seguridad deben ser capaces de limitar el acceso a la información sólo a ciertas personas.
- **Confiabilidad** (integridad y autenticación): significa que el sistema de seguridad debe ser capaz de garantizar que la información recibida fue generada por una fuente confiable y que no ha sufrido ninguna modificación.
- **Disponibilidad**: significa que debería existir un acceso programado a la información.

2.1.2. Clasificación y uso de la información

Las aplicaciones de las tecnologías de la información y la comunicación en el área de la salud son muy diversas, y podemos encontrar las siguientes tan solo por mencionar algunas:

- Telesalud
- Historia Clínica Electrónica
- Apps para la salud o salud móvil
- Dispositivos vestibles (wearables)
- Internet de las cosas
- Sistemas de información administrativos y clínicos
- Aplicaciones de macrodatos
- Redes sociales
- Realidad aumentada
- Juegos para la salud

Así como una gran variedad de aplicaciones electrónicas motivadas por el mejoramiento de la salud y la prevención y control de enfermedades.

2.2. Caos y criptografía

En este capítulo, se hablará brevemente sobre la teoría del caos, desde su concepción hasta sus aplicaciones más recientes, pasando por las características que debe presentar un sistema para denominarse caótico. Asimismo, se mostrarán algunos de los mapas caóticos más comunes y sus rasgos más notables, además de presentar el mapa caótico seleccionado para el presente trabajo.

2.2.1. Antecedentes del caos

A pesar de que los trabajos de Laplace permitían calcular con precisión el pasado y el futuro del sistema solar, se dependía de la capacidad de conocer las condiciones iniciales del sistema, lo cual resultaba un verdadero reto para los geómetras de aquella época, como lo dijeran d'Holbach y Le Verrier.

El punto de vista de Henri Poincaré fue distinto y se basó en lo siguiente: para estudiar el desarrollo y evolución de un sistema físico a través del tiempo, se debe construir un modelo basado en las leyes de la física e incluir suficientes parámetros que caractericen al sistema. Normalmente se utilizan ecuaciones diferenciales en estos modelos. Así, uno puede describir el estado de un sistema en un momento dado, nombrando al conjunto de estos estados como espacio fásico.

Otro término relevante para entender el nacimiento de la teoría del caos es el de sensibilidad a las condiciones iniciales, el cual fue descubierto por Poincaré en su análisis sobre el problema de los n cuerpos. Se utilizó este concepto para describir el hecho de que no todos los sistemas pueden ser predichos, sino que hay otros cuyas condiciones iniciales pueden presentar pequeñas variaciones y dichas variaciones ocasionar grandes diferencias en el desarrollo posterior del fenómeno. Y, con ello, la predicción resulta imposible, obteniendo así un fenómeno aleatorio. Hasta aquí podemos decir que la teoría del caos habría tenido su comienzo.

No obstante, el verdadero mérito del descubrimiento de la teoría del caos se lo lleva Edward Lorenz, que formaba parte del Massachusetts Institute of Technology (MIT). Sus primeras observaciones del fenómeno caótico se remontan al año 1961 para, finalmente, descubrir la teoría del caos como tal en 1963 mientras realizaba cálculos sobre aproximaciones que intentaban predecir el clima. Lorenz, como muchos otros matemáticos de su época, consideraba que un ligero cambio al inicio del cálculo acarrearía una diferencia en el resultado del mismo orden de magnitud que la variación inicial, lo cual, ahora sabemos, no era correcto. El segundo descubrimiento de Lorenz fue el de las imágenes que aparecían al utilizar su computadora, las cuales eran una descripción gráfica del caos. Dichas imágenes se denominaron atractores.

2.2.2. Propiedades de los sistemas caóticos

- **Sensibilidad a las condiciones iniciales**: cambios muy pequeños en las condiciones iniciales pueden llevar a grandes diferencias en el estado final.
- **Aleatoriedad**: se refiere a la impredecibilidad inherente del sistema caótico que surge debido a la sensibilidad extrema a las condiciones iniciales, la cual produce pequeñas variaciones en el estado inicial las cuales pueden llevar a comportamientos significativamente distintos a lo largo del tiempo.
- **Universalidad**: consiste en que, aun en diferentes sistemas caóticos, se producen comportamientos similares al acercarse a ciertos puntos críticos.
- **Ergodicidad**: dentro de los sistemas caóticos, la ergodicidad ayuda a generar un comportamiento que puede parecer impredecible, pero que está determinado por las leyes dinámicas del sistema, lo cual resulta esencial en aplicaciones como la criptografía por la seguridad que le otorga.
- **Delimitado**: se dice que un sistema caótico está delimitado debido a que sus trayectorias permanecen confinadas dentro de una región limitada del espacio de fases, conocido como atractor extraño.

2.2.3. Sistemas lineales y no lineales

Al momento de su concepción en la segunda mitad del siglo XX, el caos estuvo relacionado con el clima y la meteorología. Se habían realizado diversas definiciones que se pueden resumir como que el estado aleatorio generado en un sistema determinístico es un estado irregular, aunque, en realidad, es el movimiento producido por el movimiento del sistema de acuerdo a un sistema dinámico no lineal.

Se dice que un sistema no lineal produce una salida que no es proporcional a la entrada, y que la frecuencia puede variar. La principal característica de un sistema lineal es que la salida es proporcional a la entrada, además de que la frecuencia permanece constante.

2.2.4. Métodos de identificación de caos

- **Exponente de Lyapunov**: al calcular el exponente de Lyapunov, si el máximo exponente de Lyapunov del sistema es positivo, el sistema se considera como caótico.
- **Dimensión de Hausdorf**: al calcular la dimensión de Hausdorf de un sistema, si se obtienen dimensiones fractales, el sistema es caótico.
- **Método de Melnikov**: al calcular la función de Melnikov se puede determinar si el sistema de trayectoria homoclínica o heteroclínica puede aparecer en caos después de ser perturbado.

- **Método de espectro de potencia**: al trazar una imagen de espectro de potencia, el espectro de potencia solo tiene líneas espectrales discretas en la frecuencia de movimiento y de su división y multiplicación. Si el espectro de potencia que aparece es continuo, el sistema es caótico.

2.2.5. Exponente de Lyapunov

Los exponentes de Lyapunov son la medida de la predictibilidad y de la sensibilidad a los cambios en las condiciones iniciales de un sistema. En un sistema caótico, al menos un exponente de Lyapunov debe ser positivo.

2.3. Criptografía

2.3.1. Definición

La criptografía puede definirse como la ciencia que estudia la "transformación de mensajes o información en un formato incomprensible cuyo propósito es la confidencialidad, integridad, autenticación, y estado de no repudio de su origen".

Los sistemas criptográficos tradicionalmente involucran dos elementos principales: un emisor y un receptor con quien se desea comunicar un mensaje en secreto. Adicionalmente, puede utilizarse la criptografía para el almacenamiento seguro de datos, así como en el empleo de firmas digitales.

Sin importar el uso que se le dé, la criptografía incluye dos procesos principales: la encriptación y la desencriptación. La encriptación consiste en el proceso de codificar la información en un formato incomprensible a través de la utilización de una clave. Mientras que la desencriptación consiste en la decodificación de dicha información hacia un formato comprensible a través del uso de la clave criptográfica y un algoritmo relacionado con el proceso de encriptación.

2.3.2. Sistemas antiguos

Aunque la criptografía esté muy relacionada con los sistemas electrónicos en la actualidad, podemos encontrar ejemplos de su utilización en épocas tan remotas como el año 2000 a.C., cuando, en el antiguo Egipto, se aplicaban jeroglíficos secretos para cifrar mensajes escritos.

También existen casos documentados de escritura cifrada en la antigua Grecia, con la utilización de la escítala, que consistía en una cinta de cuero enrollada en un bastón de mando sobre la cual se escribía de manera longitudinal el mensaje a comunicar, o el famoso cifrado César en la antigua Roma.

2.3.3. Criptosistema y su clasificación

Encontramos dos principales clasificaciones para los criptosistemas, en función de la disponibilidad de la clave de cifrado/descifrado, las cuales son las siguientes:

Criptosistemas de clave secreta Es aquel sistema en que la clave de cifrado puede ser calculada a partir de la de descifrado, y viceversa. A su vez, este tipo de criptosistema puede dividirse en dos grandes grupos: los cifradores de flujo (solo se puede cifrar un bit de texto al mismo tiempo, por lo que su cifrado se produce bit a bit), y los cifradores de bloque (que pueden cifrar un bloque de bits, que normalmente consiste en 64 bits).

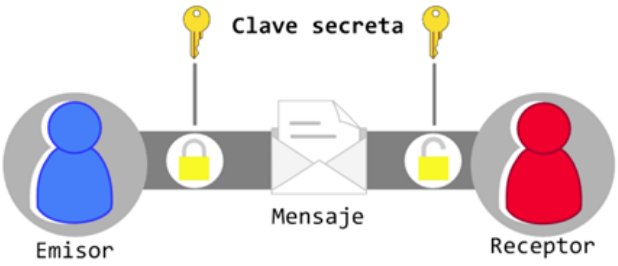


Figura 2.1: Esquema básico de un sistema de cifrado simétrico.

Criptosistemas de clave pública En estos sistemas la clave de cifrado es conocida (por lo que recibe el nombre de clave pública). Sin embargo, la clave de descifrado es desconocida (clave privada); no obstante, las claves no son independientes, por lo que no es posible deducir la clave privada a partir de la pública. Este tipo de criptosistema recibe también el nombre de asimétrico.

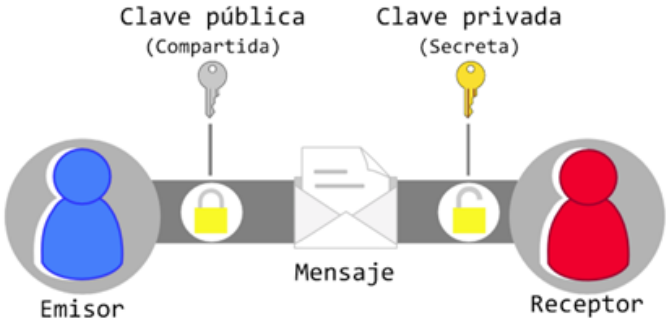


Figura 2.2: Esquema básico de un sistema de cifrado asimétrico.

Capítulo 3

Algoritmo de cifrado propuesto

3.1. Introducción

Para la elaboración del presente trabajo se eligió el mapa caótico logístico, del cual se presenta una breve descripción a continuación:

El mapa logístico consiste en un sistema dinámico ampliamente estudiado y que se define con la siguiente ecuación:

$$x_{n+1} = \mu \cdot x_n(1 - x_n) \tag{3.1}$$

donde μ es el parámetro de bifurcación, n es el número de iteración, y x_n es el enésimo estado. El parámetro μ es de suma importancia, debido a que es el que determina si el sistema es caótico o no.

3.2. Desarrollo

El esquema general del algoritmo que describe el cifrado utilizado consta de los siguientes elementos:

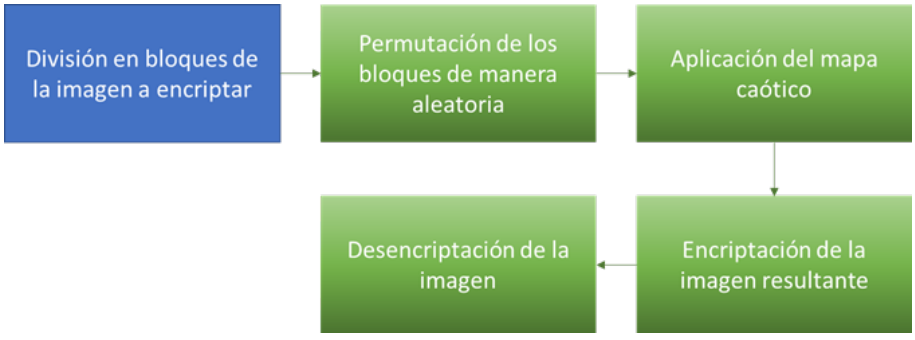


Figura 3.1: Diagrama de flujo del proceso de cifrado y descifrado de imágenes utilizado.

3.3. Implementación del algoritmo de cifrado caótico mediante Matlab

```
close all;
clear;
clc;

% Leer imagen original
original_img = imread('imagen_original');

% Si es a color, guarda los valores RGB originales antes de convertir a escala
    de grises
if size(original_img, 3) == 3
    R_original = original_img(:,:,1);
    G_original = original_img(:,:,2);
    B_original = original_img(:,:,3);
    original_img = rgb2gray(original_img);
    color_flag = true;
else
    color_flag = false;
end

[row, col] = size(original_img);
s = row * col;

% División en bloques y permutación
A = mat2tiles(original_img, [32, 32]);
[m, n] = size(A);
row_perm = randperm(m);
col_perm = randperm(n);
A_perm = A(row_perm, col_perm);
B = cell2mat(A_perm);

% Mostrar y guardar imagen permutada
figure;
imshow(B);
title('Imagen␣con␣bloques␣permutados');
saveas(gcf, 'TOMOGRAFIA_random.png');

% Mapa logístico para generar secuencia caótica
r = 3.99;
x = zeros(1, s);
x(1) = 0.7;
for i = 1:s-1
    x(i+1) = r * x(i) * (1 - x(i));
end
key = uint8(mod(floor(x * 256), 256));

% Cálculo del exponente de Lyapunov
N = 1000;
x0 = 0.234567898765432;
eps = 0.0000000005;
x = x0;
x_eps = x0 - eps;
```

```
sum_lyap = 0;

for n = 1:N
    x1 = x;
    xeps1 = x_eps;

    x = r * x1 * (1 - x1);
    x_eps = r * xeps1 * (1 - xeps1);

    distancia = abs(x - x_eps);
    sum_lyap = sum_lyap + log(distancia / eps);

    x_eps = x - eps;
end

Lambda = sum_lyap / N;
disp(['Exponente de Lyapunov para r = ', num2str(r), ': ', num2str(Lambda)]);

% Encriptación con XOR
timg = reshape(B, 1, s);
encrimg = bitxor(uint8(timg), key);
ImageEncr = reshape(encrimg, row, col);

figure;
imshow(ImageEncr);
title('Imagen Encriptada');
saveas(gcf, 'Imagen_encriptada.png');

% Desencriptación con XOR
decrimg = bitxor(encrimg, key);
ImageDecr = reshape(decrimg, row, col);

figure;
imshow(ImageDecr);
title('Imagen Desencriptada');
saveas(gcf, 'ImageDecr.png');

% Reordenar imagen desencriptada
blocks = mat2tiles(ImageDecr, [32 32]);
[~, row_inv] = sort(row_perm);
[~, col_inv] = sort(col_perm);
blocks_recovered = blocks(row_inv, col_inv);
ImageReordenada = cell2mat(blocks_recovered);

figure;
imshow(ImageReordenada);
title('Imagen Reordenada');
saveas(gcf, 'Imagen_reordenada.png');

% Reconstrucción de la imagen a color
if color_flag
    ImagenColorRecuperada = cat(3, R_original, G_original, B_original);

    figure;
    imshow(ImagenColorRecuperada);
    title('Imagen a Color Recuperada');
```

```
    imwrite(ImagenColorRecuperada, 'Imagen_color_recuperada.png');
end

\begin{lstlisting}[language=Matlab, caption={Análisis de histogramas y cálculo de
    entropía}, label={lst:analisis_histogramas}]

% Análisis de histogramas
img_original = original_img;
img_permutada = B;
img_encriptada = ImageEncr;
img_desencriptada = ImageDecr;
img_reordenada = ImageReordenada;

hist_original = imhist(img_original);
hist_permutada = imhist(img_permutada);
hist_encriptada = imhist(img_encriptada);
hist_desencriptada = imhist(img_desencriptada);
hist_reordenada = imhist(img_reordenada);

figure;
subplot(5,2,1);
imshow(img_original);
title('Imagen␣Original');

subplot(5,2,2);
bar(hist_original);
title('Histograma␣-␣Imagen␣original');
xlim([0 255]);

subplot(5,2,3);
imshow(img_permutada);
title('Imagen␣Permutada');

subplot(5,2,4);
bar(hist_permutada);
title('Histograma␣-␣Imagen␣permutada');
xlim([0 255]);

subplot(5,2,5);
imshow(img_encriptada);
title('Imagen␣Encriptada');

subplot(5,2,6);
bar(hist_encriptada);
title('Histograma␣-␣Imagen␣encriptada');
xlim([0 255]);

subplot(5,2,7);
imshow(img_desencriptada);
title('Imagen␣Desencriptada');

subplot(5,2,8);
bar(hist_desencriptada);
title('Histograma␣-␣Imagen␣desencriptada');
xlim([0 255]);

```

```
subplot(5,2,9);
imshow(img_reordenada);
title('Imagen Reordenada');

subplot(5,2,10);
bar(hist_reordenada);
title('Histograma - Imagen reordenada');
xlim([0 255]);

% Guardar figura completa
saveas(gcf, 'Comparacion_Histogramas_Completa.png');

% Calcular entropía de la imagen original y encriptada
entropy_original = entropy(original_img);
entropy_encrypted = entropy(ImageEncr);

disp(['Entropía de la imagen original: ', num2str(entropy_original)]);
disp(['Entropía de la imagen encriptada: ', num2str(entropy_encrypted)]);
```

Listing 3.1: Código de implementación del algoritmo de cifrado caótico en Matlab

3.4. Definición de la clave secreta

Se puede definir a la clave secreta como el conjunto de parámetros y condiciones iniciales que dominan el comportamiento del sistema caótico. En el caso del código propuesto, se pueden distinguir tres componentes fundamentales de la clave secreta empleada:

- **Condiciones iniciales**: $x_0 = 0{,}7$.
- **Parámetros del sistema caótico utilizado (Mapa logístico)**: $r = 3{,}99$.
- **Secuencia generada (key)**: consiste en la clave caótica utilizada en la operación XOR en el código, y su longitud equivale al número total de píxeles contenidos en la imagen (s).

A partir de los tres elementos anteriores, se puede asegurar que la información transmitida sea resistente a ataques y se mantenga íntegra.

Capítulo 4

Resultados experimentales

En esta sección se presentan los resultados obtenidos a partir de la implementación del algoritmo de encriptado y desencriptado desarrollado en `MATLAB`, basado en un sistema caótico. A través de estos experimentos se buscó evaluar el desempeño del método propuesto en términos de seguridad, calidad de reconstrucción de la imagen y robustez frente a distintos tipos de análisis.

A continuación se mostrarán las imágenes procesadas en cada etapa del algoritmo, así como los histogramas correspondientes, resultado del cálculo del exponente de Lyapunov, al igual que los resultados obtenidos en el cálculo de la entropía para cada caso de estudio, con el fin de valorar la efectividad del sistema implementado.

4.1. Caso de estudio 1: Imagen clara no. 1

La primera imagen que se utilizó en la implementación del código fue una tomografía en blanco y negro, de tamaño 512×512 píxeles.

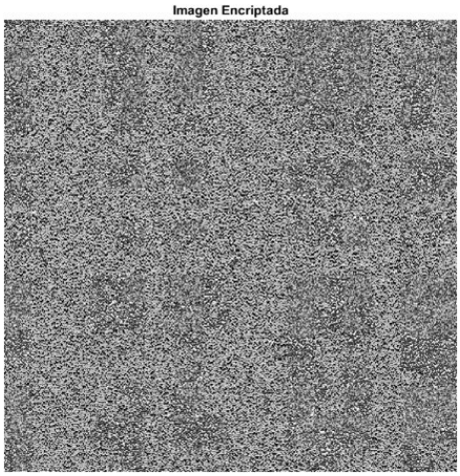
4.2. Caso de estudio 2: Imagen clara no. 2

Para el segundo caso, se utilizó una imagen a color (RGB), de tamaño 512×512 píxeles, correspondiente a una endoscopía.

Figura 4.1: Imagen clara no. 1, correspondiente a una tomografía.

(a) Imagen original

(b) Bloques permutados



(c) Imagen encriptada

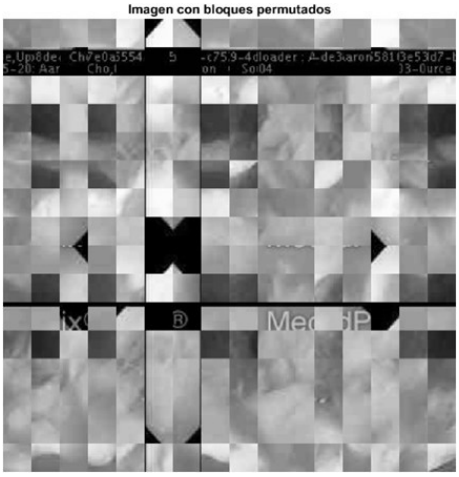
(d) Imagen desencriptada

(e) Imagen reordenada

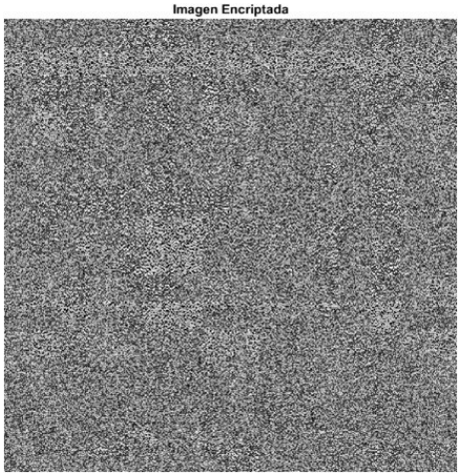
Figura 4.2: Etapas del algoritmo aplicado a la imagen clara no. 1.

Figura 4.3: Imagen clara no. 2.

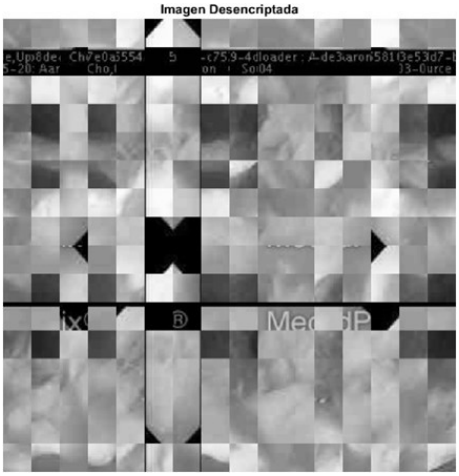
(a) Imagen original



(b) Bloques permutados (escala de grises)



(c) Imagen encriptada



(d) Imagen desencriptada

(e) Imagen reordenada

(f) Imagen con valores RGB restaurados

Figura 4.4: Etapas del algoritmo aplicado a la imagen clara no. 2.

4.3. Resultados de los análisis de seguridad

En esta sección se muestran los resultados obtenidos al analizar la seguridad del sistema de encriptación desarrollado. El objetivo fue comprobar qué tan robusto es el esquema propuesto ante algunos análisis de seguridad. Para ello, se recurrió a una serie de pruebas y métricas comúnmente utilizadas en criptografía, como el cálculo de entropía, el cálculo del exponente de Lyapunov, así como el estudio de los histogramas resultantes.

A continuación, se presentan los resultados de cada análisis junto con una interpretación general de su significado.

4.3.1. Resultados para la imagen clara no. 1

- **Exponente de Lyapunov para** $r = 3{,}99$**:** 0.64568
- **Entropía de la imagen original:** 2.8185
- **Entropía de la imagen encriptada:** 7.9035

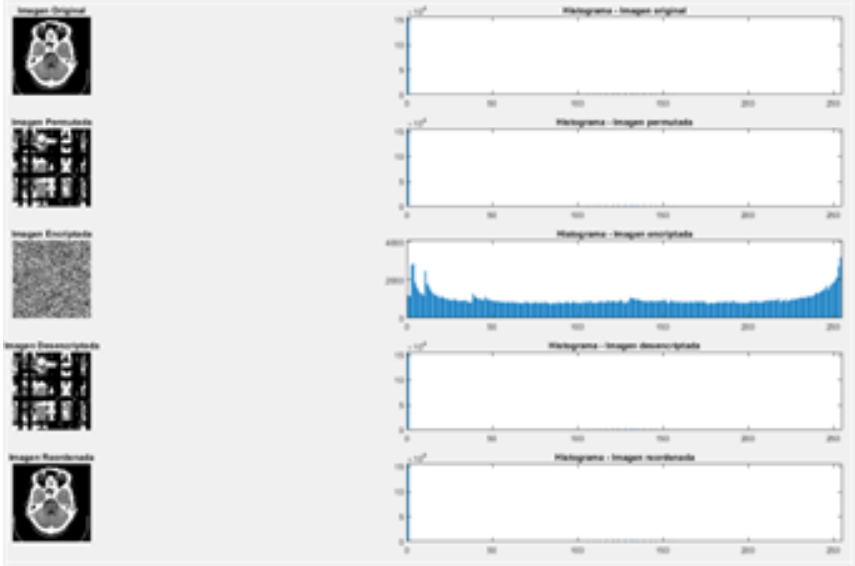


Figura 4.5: Análisis de histogramas para imagen clara no. 1.

4.3.2. Resultados para la imagen clara no. 2

- **Exponente de Lyapunov para** $r = 3{,}99$**:** 0.64568
- **Entropía de la imagen original:** 7.4491
- **Entropía de la imagen encriptada:** 7.988

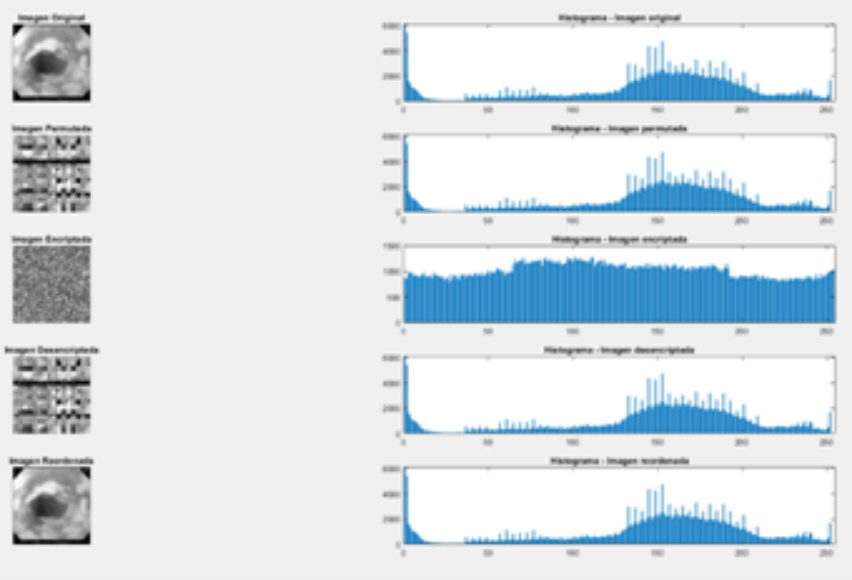


Figura 4.6: Análisis de histogramas para imagen clara no. 2.

4.3.3. Interpretación de los resultados del análisis de seguridad

- **Exponente de Lyapunov:** El exponente de Lyapunov es una medida de la divergencia de trayectorias cercanas en un sistema dinámico, y su positividad es un indicativo claro del comportamiento caótico del sistema. El exponente de Lyapunov positivo en ambos casos confirma que el sistema caótico utilizado (mapa logístico con $r = 3{,}99$) presenta un comportamiento sensible a las condiciones iniciales. Este nivel de caos es deseable en criptografía, ya que garantiza que pequeñas variaciones en la clave inicial producen resultados completamente diferentes, dificultando la predicción o el ataque por fuerza bruta. El hecho de que ambas imágenes compartan este valor indica que el generador caótico es estable y consistente en su comportamiento caótico.
- **Entropía de la imagen original vs. imagen encriptada:**
  - **Para imagen clara no. 1:** La imagen original presenta un nivel de entropía relativamente bajo, lo cual sugiere la presencia de regiones homogéneas o patrones visuales repetitivos, como áreas uniformes u oscuras. Tras aplicar el proceso de encriptación, la entropía se eleva significativamente hasta alcanzar un valor de 7.90, muy cercano al máximo teórico de 8 para imágenes en escala de grises de 8 bits. Este aumento indica que la imagen encriptada adquiere un comportamiento estadístico similar al del ruido aleatorio, lo que evidencia que la información visual original ha sido completamente oculta. Este resultado representa un indicio claro de la eficacia del esquema criptográfico.
  - **Para imagen clara no. 2:** En este segundo caso, la imagen original ya contaba con una entropía elevada, lo cual refleja una mayor compleji-

dad visual y una mayor variabilidad en la distribución de los valores de píxel. A pesar de ello, el proceso de encriptación logró incrementar ligeramente la entropía, alcanzando un valor muy cercano al límite superior. Este resultado demuestra que el sistema no solo es capaz de ocultar eficazmente el contenido original, sino que también mejora la aleatoriedad en la distribución de los valores, fortaleciendo aún más la seguridad del cifrado.

Capítulo 5

Conclusiones y trabajo futuro

5.1. Conclusiones

El presente trabajo de tesis abordó el diseño e implementación de un sistema de cifrado de imágenes médicas basado en técnicas de criptografía caótica. A través de la integración del mapa logístico, la permutación de bloques y la operación XOR, se logró un esquema de encriptación capaz de ocultar eficazmente la información visual contenida en imágenes de uso clínico, contribuyendo así al fortalecimiento de la seguridad en sistemas de telemedicina.

Los resultados experimentales evidenciaron que el algoritmo propuesto genera imágenes cifradas con características estadísticas propias del ruido aleatorio, como lo confirman los análisis de histogramas y los valores elevados de entropía obtenidos. Asimismo, el cálculo del exponente de Lyapunov demostró que el sistema caótico empleado es altamente sensible a las condiciones iniciales, aportando un nivel adicional de robustez frente a ataques por fuerza bruta.

De manera general, se puede concluir que el enfoque desarrollado en esta investigación cumple con los objetivos planteados y constituye una alternativa viable para la protección de imágenes médicas en entornos de e-salud, donde la confidencialidad de los datos es un requisito fundamental.

5.2. Trabajo futuro

Si bien los resultados alcanzados son satisfactorios, existen diversas líneas de trabajo que pueden explorarse en investigaciones futuras para ampliar y perfeccionar el sistema presentado:

- **Extensión a imágenes de mayor resolución:** Analizar el desempeño del algoritmo al procesar imágenes de alta resolución o volúmenes 3D, como estudios tomográficos avanzados.

- **Integración con otros sistemas caóticos:** Explorar la utilización de mapas caóticos de mayor complejidad o de dimensión superior, con el fin de incrementar la entropía y la impredecibilidad del cifrado.
- **Optimización del rendimiento:** Implementar el algoritmo en plataformas de hardware acelerado (GPU, FPGA) para reducir los tiempos de procesamiento y facilitar su integración en sistemas de telemedicina en tiempo real.
- **Análisis frente a ataques avanzados:** Realizar pruebas de seguridad más exhaustivas, incluyendo ataques de texto conocido y ataques de correlación, para validar la resistencia del esquema en escenarios más exigentes.
- **Aplicación en entornos normativos:** Evaluar la conformidad del sistema con estándares internacionales de protección de datos médicos, como HIPAA o GDPR, para facilitar su adopción en sistemas clínicos reales.

Estas posibles líneas de desarrollo permitirán consolidar y extender el impacto de las técnicas de criptografía caótica en el ámbito de la seguridad de la información médica, contribuyendo al avance de soluciones más seguras y confiables en la práctica de la telemedicina.

Referencias

[1] K. T. Alligood, T. D. Sauer, and J. A. Yorke, *Chaos: An Introduction to Dynamical Systems*. Springer, 1996.

[2] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, no. 5560, pp. 459–467, 1976.

[3] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379–423, 623–656, 1948.

[4] L. Kocarev and G. Jakimoski, "Chaos-based cryptography: a brief overview," *IEEE Circuits and Systems Magazine*, vol. 1, no. 3, pp. 6–21, 2001.

[5] World Health Organization, "Global strategy on digital health 2020–2025," 2021.

[6] HIMSS, "Security and privacy in telehealth," 2020. White Paper.

[7] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996.

[8] National Electrical Manufacturers Association, "Digital imaging and communications in medicine (dicom) standard," 2020.

[9] United Nations, "Policy brief: The impact of covid-19 on the world's health systems," 2020.

[10] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3d chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[11] M. U. Morales, "Cifrado caótico para imágenes basado en modulación de fase cuántica," 2022. Tesis de Maestría, CICESE.

[12] N. C. Hernandez and L. M. Flores, "Encriptación de imágenes con algoritmos caóticos," in *Memorias del Congreso Nacional de Control Automático, AMCA 2014*, 2014.