



# INSTITUTO POLITÉCNICO NACIONAL

---

---

UNIDAD PROFESIONAL INTERDISCIPLINARIA EN INGENIERÍA Y  
TECNOLOGÍAS AVANZADAS

## INSERCIÓN DE MARCAS DE AGUA OCULTAS Y CIFRÁDAS EN IMÁGENES DE RESONANCIA MAGNÉTICA APLICADAS EN DISPOSITIVOS IOT

PROYECTO TERMINAL II

PRESENTAN

REYES GARCÍA LUIS DANIEL  
VALENZUELA MORALES MISAEL

ASESORES

DRA. IZLIAN YOLANDA OREA FLORES  
DRA. GINA GALLEGOS GARCÍA  
DRA. ICLIA VILLORDO JIMÉNEZ

Junio 2024



# INSTITUTO POLITÉCNICO NACIONAL

UNIDAD PROFESIONAL INTERDISCIPLINARIA EN  
INGENIERÍA Y TECNOLOGÍAS AVANZADAS



## Proyecto Terminal II

**"INSERCIÓN DE MARCAS DE AGUA  
OCULTAS Y CIFRADAS EN  
IMÁGENES DE RESONANCIA  
MAGNÉTICA APLICADAS EN  
DISPOSITIVOS IoT"**

Presentan:

Reyes García Luis Daniel  
Valenzuela Morales Misael

Que para obtener el título de:

**"Ingeniero en Telemática"**

### ASESORES

Dra. Izlian Yolanda Orea  
Flores

Dra. Gina Gallegos García

Dra. Icia Villordo Jiménez

### PRESIDENTE

Dr. Noé Torres  
Cruz

### SECRETARIO

Dra. Blanca Tovar  
Corona



### Autorización de uso de obra

**Instituto Politécnico Nacional**

**P r e s e n t e**

Bajo protesta de decir verdad el que suscribe Reyes García Luis Daniel (se anexa copia simple de identificación oficial), manifiesto ser autor (a) y titular de los derechos morales y patrimoniales de la obra titulada Insertión de Marcas de agua ocultas y cifradas en Imágenes de Resonancia Magnética aplicadas en dispositivos IoT

, en adelante “La Tesis” y de la cual se adjunta copia, por lo que por medio del presente y con fundamento en el artículo 27 fracción II, inciso b) de la Ley Federal del Derecho de Autor, otorgo a el Instituto Politécnico Nacional, en adelante El IPN, autorización no exclusiva para comunicar y exhibir públicamente total o parcialmente en medios digitales, Plataforma de la Dirección de Bibliotecas del IPN y/o consulta directa en la Coordinación de Biblioteca de la UPIITA “La Tesis” por un periodo de 5 años contado a partir de la fecha de la presente autorización, dicho periodo se renovará automáticamente en caso de no dar aviso expreso a “El IPN” de su terminación.

En virtud de lo anterior, “El IPN” deberá reconocer en todo momento mi calidad de autor de “La Tesis”. Adicionalmente, y en mi calidad de autor y titular de los derechos morales y patrimoniales de “La Tesis”, manifiesto que la misma es original y que la presente autorización no contraviene ninguna otorgada por el suscripto respecto de “La Tesis”, por lo que deslindo de toda responsabilidad a El IPN en caso de que el contenido de “La Tesis” o la autorización concedida afecte o viole derechos autorales, industriales, secretos industriales, convenios o contratos de confidencialidad o en general cualquier derecho de propiedad intelectual de terceros y asumo las consecuencias legales y económicas de cualquier demanda o reclamación que puedan derivarse del caso.

Ciudad de México, a 02 de Julio de 2024

**Atentamente**

A handwritten signature in blue ink, appearing to read "Reyes García Luis Daniel".



### Autorización de uso de obra

Instituto Politécnico Nacional

Presente

Bajo protesta de decir verdad el que suscribe Valenzuela Morales Misael (se anexa copia simple de identificación oficial), manifiesto ser autor (a) y titular de los derechos morales y patrimoniales de la obra titulada Insertión de marcas de agua ocultas y cifradas en imágenes de resonancia magnética aplicadas en dispositivos IoT

, en adelante "La Tesis" y de la cual se adjunta copia, por lo que por medio del presente y con fundamento en el artículo 27 fracción II, inciso b) de la Ley Federal del Derecho de Autor, otorgo a el Instituto Politécnico Nacional, en adelante El IPN, autorización no exclusiva para comunicar y exhibir públicamente total o parcialmente en medios digitales, Plataforma de la Dirección de Bibliotecas del IPN y/o consulta directa en la Coordinación de Biblioteca de la UPIITA "La Tesis" por un periodo de 5 años contado a partir de la fecha de la presente autorización, dicho periodo se renovará automáticamente en caso de no dar aviso expreso a "El IPN" de su terminación.

En virtud de lo anterior, "El IPN" deberá reconocer en todo momento mi calidad de autor de "La Tesis". Adicionalmente, y en mi calidad de autor y titular de los derechos morales y patrimoniales de "La Tesis", manifiesto que la misma es original y que la presente autorización no contraviene ninguna otorgada por el suscrito respecto de "La Tesis", por lo que deslindo de toda responsabilidad a El IPN en caso de que el contenido de "La Tesis" o la autorización concedida afecte o viole derechos autorales, industriales, secretos industriales, convenios o contratos de confidencialidad o en general cualquier derecho de propiedad intelectual de terceros y asumo las consecuencias legales y económicas de cualquier demanda o reclamación que puedan derivarse del caso.

Ciudad de México, a 2 de julio de 2024

Atentamente

## **Resumen**

En este Proyecto Terminal se desarrolló un sistema de seguridad, el cuál es capaz de cifrar la información de los pacientes que se realicen estudios médicos que generen Imágenes de Resonancia Magnética. Los datos del paciente son insertados por medio de marcas de agua ocultas utilizando una técnica de esteganografía para ocultar dicha información, además de añadir otro filtro de seguridad con ayuda del cifrado haciendo que estos datos sensibles queden completamente ilegibles si se llegará a extraer la marca de agua, con ello se logra implementar otro nivel de seguridad y confidencialidad, de forma que sólo los doctores autorizados pueden insertar y extraer la información.

El proyecto propone el uso de marcas de agua digitales como una solución eficiente para la protección de los derechos de copia y propiedad de archivos de datos multimedia, posibilitando la identificación del autor o propietario, de las imágenes digitales. La principal ventaja de estos sistemas consiste en que la marca es inseparable del contenido del archivo. El sistema que se desarrolló es capaz de insertar la marca de agua en Imágenes de Resonancia Magnética con formato PNG (con compresión sin pérdida) con los datos de los pacientes (cifrados y ocultos), buscando mitigar la falsificación y mal uso en estudios médicos digitales.

A lo largo del documento se abordarán temas relacionados directamente a la seguridad de la información, así como las propiedades y clasificación de las marcas de agua, se presenta de igual manera el estado del arte relacionado a las técnicas estenográficas, además de clasificar las técnicas criptográficas existentes. De esta forma de presenta el análisis, diseño, desarrollo e implementación, así como las pruebas y resultados del sistema se seguridad que permiten mantener cierto control a los médicos que realicen este tipo de estudios médicos.

## **Palabras clave**

Seguridad, cifrar, Imágenes de Resonancia Magnética, marcas de agua, esteganografía, ilegible, confidencialidad, criptografía.

## Abstract

In this Terminal Project a security system was developed, which is capable of encrypting the information of patients undergoing medical studies that generate Magnetic Resonance Images. The patient data are inserted by means of hidden watermarks using a steganography technique to hide such information, in addition to adding another security filter with the help of encryption making this sensitive data completely unreadable if the watermark is extracted, thus implementing another level of security and confidentiality, so that only authorized doctors can insert and extract the information.

The project proposes the use of digital watermarking as an efficient solution for the protection of copy and property rights of multimedia data files, making it possible to identify the author or owner of the digital images. The main advantage of these systems is that the mark is inseparable from the content of the file. The system that was developed is capable of inserting the watermark in Magnetic Resonance Images with PNG format (with lossless compression) with patient data (encrypted and hidden), seeking to mitigate forgery and misuse in digital medical studies.

Throughout the document, topics directly related to information security will be addressed, as well as the properties and classification of watermarks, the state of the art related to stenographic techniques will also be presented, in addition to classifying the existing cryptographic techniques. In this way, the analysis, design, development and implementation are presented, as well as the tests and results of the security system that allow to maintain certain control to the doctors who perform this type of medical studies.

## KeyWords

Security, encryption, Magnetic Resonance Images, watermarking, steganography, unreadable, confidentiality, cryptography.

## Agradecimientos

En primer lugar agradecemos al Instituto Politécnico Nacional (IPN) y a la Unidad Profesional Interdisciplinaria en Ingeniería y Tecnologías Avanzadas (UPIITA) por la formación académica que nos han brindado a lo largo de nuestro camino educativo. De igual manera agradecemos a las Dra's. Izlian Yolanda Orea Flores, Gina Gallegos García e Iclia Villordo Jiménez, por su inestimable apoyo, guía y paciencia a lo largo de este proyecto. Su vasto conocimiento y dedicación han sido fundamentales para la culminación de este proyecto.

Agradecemos también a los miembros del comité evaluador, el Dr. Noé Torres Cruz y la Dra. Blanca Tovar Corona , por sus valiosas sugerencias, críticas constructivas y tiempo dedicado a revisar el proyecto.

Sus aportes han enriquecido significativamente esta investigación.

Un especial agradecimiento a nuestro profesor y mentor Filio que nos reprobó en 1er semestre en la Unidad de Aprendizaje de Cálculo Diferencial e Integral y nos dio la motivación suficiente para seguir adelante y demostrar si se necesitan las matemáticas para ser ingeniero.

### ■ Reyes García Luis Daniel

Agradezco a Dios por permitirme llegar hasta este día y que me ha dado la oportunidad de poder terminar mis estudios, por darme siempre la fortaleza y la capacidad de llevar a cabo todo lo que aconteció en esta Institución.

A mis padres, Daniel Reyes Plascencia y Reyna García Barrera que me apoyaron durante todo mi recorrido, quienes siempre creyeron en mí y me brindaron su amor y apoyo incondicional. Sin su sacrificio, ánimo y confianza, este logro no habría sido posible. Además de mis hermanos Giovanni y Alejandro que me ayudaron a desestresarme en los momentos difíciles. A la familia de Dana que me ayudó en los últimos meses a darme su apoyo a través de sus oraciones y a ella porque sus palabras me llenan de fuerzas para seguir adelante todos los días.

A mis amigos y compadres Sauer, Andrea, Poncho y Noelia, gracias por sus palabras y constante apoyo, por las largas horas de estudio compartidas, y por los momentos de distracción y compañía que hicieron este viaje más llevadero y agradable.

A mi compañero de proyecto y amigo Misael por brindarme su amistad, apoyo, confianza y la oportunidad de colaborar con él, tanto desde 1er semestre como hasta este último, para llevar a cabo la realización de este proyecto.

Agradezco a mis profesores quienes a través de sus experiencias me ayudaron a mejorar tanto profesionalmente como de manera personal, siempre dándome consejos que atesoraré por siempre.

■ **Valenzuela Morales Misael**

A mis padres Maribel Morales Suárez y Jose Angel Valenzuela Hipolito por darme todo su apoyo y compañía para poder llegar hasta donde estoy ahora, a mis hermanos Karen y Jaret por ser una motivación para seguir adelante con lo que me propongo y que sin ellos todo hubiera sido muy aburrido.

A mis profesores y compañeros de la carrera porque de cada uno con el que coincidí me llevo algo que estoy seguro me va a servir en algún momento de mi vida, los voy a recordar con cariño sin importar el tiempo que hayamos compartido.

A mis amigos que aún conservo desde la vocacional: Josue, Pancho, Chilpa, Ulises, Victor, Cristian, Rosas y Paco que han estado conmigo en los momentos felices y también en los complicados.

A mis amigos que hice a lo largo de la carrera: Sauer, Noelia, Andrea, Poncho y obviamente a Daniel que gracias a ellos todo se sintió mucho mas sencillo todo. Lo vivido a lo largo de este tiempo lo guardare para siempre.

A mi compañero de proyecto Daniel que con sus conocimientos, confianza y apoyo logramos complementarnos para poder desarrollar nuestro proyecto de titulación.

A todos ustedes, agradecemos por ser parte de este viaje y por contribuir de manera significativa a la realización de este proyecto.

# Índice

<b>1 INTRODUCCIÓN</b>	<b>10</b>
1.1 Planteamiento del problema . . . . .	11
1.2 Propuesta solución . . . . .	13
1.3 Alcances . . . . .	16
1.4 Objetivo general . . . . .	17
1.5 Objetivos específicos . . . . .	17
<b>2 MARCO TEÓRICO</b>	<b>19</b>
2.1 Marcas de agua digitales . . . . .	19
2.1.1 Propiedades de las marcas de agua . . . . .	20
2.1.2 Clasificación de las marcas de agua . . . . .	22
2.1.3 Percepción . . . . .	22
2.1.4 Robustez . . . . .	23
2.1.5 Esquema de inserción . . . . .	24
2.1.6 Aplicaciones de las marcas de agua . . . . .	24
2.2 Esteganografía . . . . .	25
2.2.1 Esteganografía en imágenes . . . . .	25
2.2.2 Características de la esteganografía . . . . .	26
2.2.3 Clasificación de la esteganografía . . . . .	26
2.2.4 Clasificación de las técnicas esteganográficas . . . . .	28
2.3 Seguridad de la información . . . . .	29
2.4 Criptografía . . . . .	31
2.4.1 Objetivos criptográficos . . . . .	32
2.4.2 Primitivas criptográficas . . . . .	33
2.4.3 Técnicas de criptografía . . . . .	34
2.4.4 Técnicas de cifrado de información . . . . .	36
2.4.5 Algoritmos de cifrado de llave simétrica . . . . .	37
2.5 RMI (Imagen de Resonancia Magnética) . . . . .	41
2.6 Ventajas y Desventajas de las RMI . . . . .	41
2.7 Archivos de imágenes . . . . .	43
2.7.1 Archivos vectoriales . . . . .	43
2.7.2 Archivos rasterizados . . . . .	43
2.8 Procesamiento digital de imágenes . . . . .	45
2.8.1 Pasos fundamentales en el Procesamiento Digital de Imágenes . . . . .	46
2.9 Técnicas de similitud en imágenes médicas . . . . .	47
2.10 Técnicas de segmentación . . . . .	47
<b>3 ESTADO DEL ARTE</b>	<b>52</b>
3.1 UPIITA . . . . .	52
3.2 Marcas de agua comerciales . . . . .	52
3.3 Confidencialidad de la información . . . . .	53
3.4 Diferencias con proyectos realizados en UPIITA . . . . .	54

<b>4 ANÁLISIS</b>	<b>56</b>
4.1 Propiedades de las marcas de agua . . . . .	56
4.2 Clasificación de las marcas de agua . . . . .	56
4.3 Elección de marca de agua . . . . .	58
4.4 Técnica criptográfica . . . . .	59
4.5 Algoritmo de cifrado . . . . .	60
4.6 Técnica esteganográfica . . . . .	62
4.7 Características fundamentales de la RMI . . . . .	64
4.8 Metodologías del diseño de software . . . . .	65
4.9 Lenguaje de programación para el procesamiento de imágenes . . . . .	67
<b>5 DISEÑO</b>	<b>69</b>
5.1 Requerimientos mínimos necesarios para la instalación . . . . .	69
5.2 Diagrama General del Funcionamiento del sistema . . . . .	70
5.3 Proceso de Autenticación . . . . .	70
5.4 Proceso de Almacenamiento . . . . .	71
5.5 Proceso de Inserción . . . . .	71
5.6 Proceso de Extracción . . . . .	72
5.7 Cifrado de la información . . . . .	73
5.8 Ocultamiento de la información . . . . .	76
<b>6 DESARROLLO E IMPLEMENTACIÓN</b>	<b>80</b>
6.1 Inicio de Sesión . . . . .	80
6.2 Registro de Usuario . . . . .	83
6.2.1 Almacenamiento de Registros de Usuario . . . . .	86
6.3 Selección de Perfil Médico . . . . .	87
6.4 Inserción de Marca de Agua . . . . .	89
6.5 Extracción de Marca de Agua . . . . .	91
<b>7 PRUEBAS Y RESULTADOS</b>	<b>96</b>
7.1 Pruebas de similitud entre RMI's originales y marcadas . . . . .	96
7.2 Evaluación de resultados . . . . .	99
<b>8 CONCLUSIONES</b>	<b>104</b>
<b>9 TRABAJOS A FUTURO</b>	<b>107</b>
<b>REFERENCIAS</b>	<b>110</b>

# Índice de figuras

1	Diagrama de Casos de Usos del sistema . . . . .	14
2	Esquema de la clasificación general de las marcas de agua . . . . .	22
3	Marca de agua visible vs Marca de agua invisible . . . . .	23
4	Imagen ilustrativa de la esteganografía . . . . .	25
5	Esquema general de la Criptografía . . . . .	31
6	Taxonomía de las primitivas criptográficas . . . . .	33
7	Esquema general del Cifrado Simétrico . . . . .	36
8	Esquema general del Cifrado Asimétrico . . . . .	37
9	Imagen de Resonancia Magnética de Rodilla Izquierda . . . . .	42
10	Distribución de secciones de una Imagen de Resonancia Magnética . . . . .	42
11	Diagrama de bloques del método de Umbralización . . . . .	48
12	Crecimiento de región . . . . .	49
13	Esquema del Algoritmo AES . . . . .	61
14	Diagrama de bloques del sistema de seguridad . . . . .	70
15	Diagrama del Proceso de Inserción de una Marca de Agua . . . . .	71
16	Diagrama del Proceso de Extracción de una Marca de Agua . . . . .	72
17	Cifrado de la información . . . . .	73
18	Descifrado de la información . . . . .	73
19	Diagrama de Flujo AES-128 . . . . .	75
20	Diagrama de Flujo algoritmo Bit Menos Significativo . . . . .	77
21	Menú de Inicio de Sesión . . . . .	80
22	Diagrama de Flujo de Inicio de Sesión (Front-end) . . . . .	81
23	Diagrama de Flujo de Inicio de Sesión (Back-end) . . . . .	82
24	Menú de Registro de usuario . . . . .	83
25	Diagrama de Flujo del Registro de Usuario (Front-end) . . . . .	84
26	Diagrama de Flujo del Registro de Usuario (Back-end) . . . . .	85
27	Vista general de la Base de Datos . . . . .	86
28	Visualización de los registros . . . . .	87
29	Menú para Seleccionar Perfil médico . . . . .	87
30	Diagrama de Flujo del Menú para Seleccionar Perfil médico . . . . .	88
31	Diagrama de Flujo del algoritmo Criptográfico y Esteganográfico . . . . .	89
32	Formulario para Insertar la marca de agua . . . . .	90
33	Mensaje de Marcación Exitosa . . . . .	91
34	Menú para Extraer la marca de agua . . . . .	91
35	Diagrama de Flujo del proceso de Extracción . . . . .	92
36	Información del paciente recuperada de la Marca de Agua . . . . .	94
37	Imágenes de Resonancia Magnéticas de diferentes partes del cuerpo . . . . .	96
38	Prueba de similitud en RMI Enfermedad Alzheimer . . . . .	98
39	Prueba de similitud en RMI Demencia Moderada . . . . .	98
40	Prueba de similitud en RMI Tumor cerebral . . . . .	98
41	MSE (Mean Square Error) . . . . .	99
42	PSNR (Peak Signal-to-Noise-Ratio) . . . . .	99

43	NCC (Normalized Cross-Correlation) . . . . .	99
44	RMI Original vs RMI Marcada del cerebro . . . . .	100
45	RMI Original vs RMI Marcada del pecho . . . . .	101
46	RMI Original vs RMI Marcada de rodilla . . . . .	101

## Índice de tablas

1	Herramientas principales a utilizar . . . . .	16
2	Objetivos de la seguridad de la información . . . . .	30
3	Fortalezas vs Vulnerabilidades de algoritmo de cifrado . . . . .	40
4	Comparación de transformadas . . . . .	45
5	Comparación entre Proyectos de Investigación . . . . .	54
6	Clasificación de las marcas de agua de acuerdo a la percepción visual . . . . .	56
7	Clasificación de las marcas de agua de acuerdo a la reacción a modificaciones	57
8	Clasificación de las marcas de agua de acuerdo al dominio . . . . .	58
9	Ventajas y desventajas de algoritmos enfocados a confidencialidad . . . . .	60
10	Tabla comparativa de las técnicas esteganográficas existentes . . . . .	63
11	Resultados de imágenes marcadas. Parte del cuerpo: Cerebro . . . . .	100
12	Resultados de imágenes marcadas. Parte del cuerpo: Pecho . . . . .	100
13	Resultados de imágenes marcadas. Parte del cuerpo: Rodilla . . . . .	101



## INSERCIÓN DE MARCAS DE AGUA OCULTAS Y CIFRADAS EN IMÁGENES DE RESONANCIA MAGNÉTICA APLICADAS EN DISPOSITIVOS IoT

### INTRODUCCIÓN

## 1. INTRODUCCIÓN

Las facilidades que ofrece Internet hoy en día para el acceso y la transmisión de forma sencilla e inmediata de información conlleva asumir nuevos escenarios enfocados al riesgo y vulnerabilidad que se crea al momento de manejar documentos digitales. Esta facilidad para la difusión y el acceso de información conlleva además una debilidad en lo que respecta al control de los datos, en la medida que se facilita la obtención y copia de información, en muchos casos sin una adecuada gestión de los derechos de autor de la misma.

A una persona que crea un documento digital fácilmente es susceptible a caer en problemas de manejo de la información, siendo uno de los más comunes la falsificación de documentos o la apropiación por una tercera persona del documento para utilizarla de manera ilegal.

Para mitigar el mal uso de los documentos digitales médicos se necesita alguna forma de marcar el trabajo para acreditar su autoría y sus derechos ante terceros, de forma que se pueda identificar el creador del material, sin embargo para garantizar la confidencialidad y autenticidad de los médicos es importante ocultar estos datos en la imagen digital, de esta forma la marca de agua será una herramienta útil para ello.

La razón principal por las que se necesitan las marcas de agua es que ayudan a proteger los derechos de autor de un trabajo específico, información confidencial o indicar la validez en un documento digital, de modo que garantiza que no se pueda reutilizar o alterar sin permiso.

En este proyecto se analizan las marcas de agua que se generan a partir de técnicas de esteganografía que permitan insertar información en una portadora para ocultarla, además de utilizar la criptografía como un filtro más de seguridad para poder cifrar la información del paciente. Asimismo se analiza la importancia de las marcas de agua en la actualidad, teniendo en cuenta la creciente amenaza de la falsificación y la necesidad de desarrollar nuevas tecnologías para mantener la seguridad de los documentos digitales como lo son las Imágenes de Resonancia Magnéticas.

Este trabajo de investigación tiene como objetivo proporcionar una visión completa y detallada de este importante elemento de seguridad, así como mostrar el impacto que pueden tener las marcas de agua en documentos digitales tan delicados como son las RMI.

## 1.1. Planteamiento del problema

Hoy en día con el avance de la ciencia y la tecnología existe la manera de obtener y visualizar estudios médicos de forma digital, tal es el caso de las Imágenes de Resonancia Magnética, las cuales actualmente con el equipo tecnológico se pueden obtener con un formato especial que facilita a los especialistas poder analizar y comprender mejor cada uno de los casos médicos.

Para que sea posible la visualización de este tipo de imágenes (RMI) en algún dispositivo diferente al del hospital donde se realizó el estudio o para que el paciente pueda verlas, es necesario hacer una conversión del estándar original, que generalmente en el campo de la medicina se utiliza DICOM (Digital Imaging and Communications in Medicine) o en español Imágenes Médicas y Comunicaciones en la Medicina, que es un estándar hospitalario médico reconocido mundialmente, aplicado a cualquier disciplina que utilice imágenes para el cuidado de la salud [1].

La transformación de la imagen se hace a un formato más comercial, de modo que se pueda visualizar con programas no especializados, este formato puede ser JPEG (Joint Photographic Experts Group) o PNG (Portable Network Graphics) que son los más universales y por lo tanto más utilizados, ya que al ser compatibles con los diferentes dispositivos, son muy eficientes a la hora de realizar el guardado de las imágenes brindando además una buena resolución.

Gracias a esa facilidad que se tiene para manipular las imágenes en formato JPEG o PNG surge a su vez una desventaja significativa, la cual es que cualquier persona que domine un programa de edición pueda corromper la imagen, haciendo que la calidad se pierda o en el peor de los casos que se busque modificar la datos contenidos, esto en el área de la salud puede afectar directamente aspectos como la autenticación, integridad o confidencialidad de la información de cada paciente.

En 2022 el Instituto Nacional de Estadística y Geografía (INEGI) reportó 37,169 muertes por enfermedades cerebro vasculares en México de las cuales 9,534 (25.6 %) se realizaron Imágenes de Resonancia Magnética.

Además en el periodo Enero-Junio de 2022, las defunciones por enfermedades por tumores malignos fueron 90,124 casos, siendo esta la cuarta causa de muerte a nivel nacional de defunciones registradas. De los cuales en el 58 % se realizaron Imágenes de Resonancia Magnética, lo cual nos habla del importante uso que tienen este tipo de estudios médicos digitales, y esto a su vez implica tener mecanismos que permitan salvaguardar la información confidencial de los pacientes.

Rango	Total
1	COVID-19 238 772 En 2020 fueron 200 270
2	Enfermedades del corazón 225 449 En 2020 fueron 218 704
3	Diabetes mellitus 140 729 En 2020 fueron 151 019
4	Tumores malignos 90 124 En 2020 fueron 90 603
5	Influenza y neumonía 54 601 En 2020 fueron 58 037
6	Enfermedades del hígado 41 890 En 2020 fueron 41 492
7	Enfermedades cerebrovasculares 37 169 En 2020 fueron 37 020
8	Agresiones (homicidios) 35 700 En 2020 fueron 36 773

*Principales causas de muerte, INEGI. 2022*

La necesidad de tener un sistema capaz de ayudar al personal médico que se encarga de manipular las Imágenes de Resonancia Magnética es evidente, es por ello que se necesita una forma de validar la autenticación de los estudios realizados, puesto al ser entregadas por medio de memorias portables o por correo electrónico al paciente, estas imágenes podrían ser corrompidas por algún tercero, esto desencadenaría la posibilidad de que éste las utilice ya sea consigo mismo, o que altere su contenido a fin de afectar directamente el tratamiento que se le dará al paciente original, o incluso podría usarse por el mismo propietario para alterar sus mismos estudios y generar así algún tipo de beneficio.

Es fundamental salvaguardar la información de cada paciente, ya que al tratarse de un tema relacionado a su salud conlleva manejar un nivel alto de confidencialidad ya que este tipo de información en su momento podría ser manejada por instituciones financieras especializadas en ofrecer seguros para proteger a las personas, de esta manera con ayuda de este sistema se podrá generar una mayor confianza al estar manejando esta información.

## 1.2. Propuesta solución

Se desarrolla un sistema capaz de insertar la información médica necesaria para poder identificar cada imagen digital a través de marcas de agua, los atributos suficientes que se necesitan para poder identificar el estudio médico son:

- Nombre del paciente
- Nombre del estudio médico
- Nombre del médico radiólogo
- Nombre del médico que solicito el estudio
- Fecha en que se realizó el estudio

Al insertar información del paciente no se busca abarcar la mayor cantidad de información así como puede ser el diagnóstico o el tratamiento, sino solo lo mínimo necesario para poder identificar los estudios y poder asegurar la integridad de la imagen médica de la mejor manera, esto con el fin de no alterar la imagen y así evitar que se generen problemas de interpretación al momento de leer el diagnóstico.

En cuanto a las marca de agua, estas pueden ser un logotipo, una imagen o un texto, y puede ser tan sutil o prominente como se requiera, sin embargo si la marca cubre demasiado espacio, puede comprometer la calidad del trabajo.

La marca de agua digital es un código de identificación que se inserta directamente en el contenido de un archivo multimedia (imagen) y fácilmente se pueden dividir en dos, las marcas visibles y las marcas ocultas, estas últimas se caracterizan por ser difícil de apreciar por el sistema perceptual humano, pero fácil de detectar usando un algoritmo dado y una clave, en un ordenador. Es preciso aclarar que aunque existen sistemas de marcas de agua visibles, estos no serán analizados en este trabajo.

El sistema de seguridad propuesto en este proyecto hará uso de marcas de agua ocultas por medio de esteganografía, añadiendo además el uso de cifrado, teniendo de esta manera un mecanismo de seguridad más completo que ayude a mantener la autenticidad y confiabilidad de las Imágenes de Resonancia Magnética del paciente intactas, haciendo posible que solo la persona autorizada pueda visualizar la información.

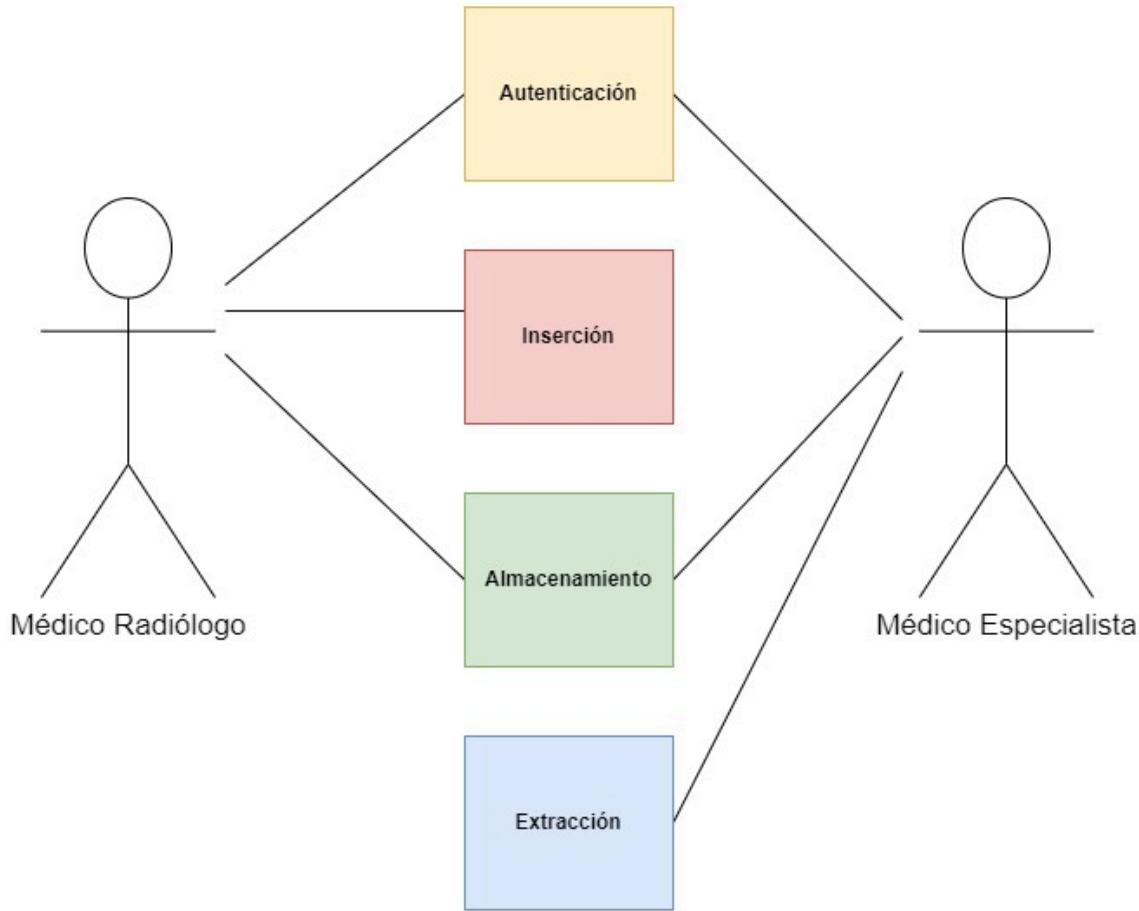


Figura 1: Diagrama de Casos de Usos del sistema

Tener un sistema de marcas de agua involucra un proceso de marcado (Inserción) y otro de detección (Extracción) que, generalmente, requieren una clave de propósito similar a la clave utilizada en los sistemas criptográficos. El nivel de disponibilidad de la clave, determinará quién o quiénes podrán leer o detectar la marca de agua. En la práctica, la mayoría de las técnicas de marcas de agua pueden considerarse como sistemas criptográficos simétricos, en los que se emplea una sola clave, variando en ellos el nivel de acceso a esa clave.

El sistema se desarrolló para abarcar estudios digitales que hayan sido obtenidos por medio de una Imagen de Resonancia Magnética y el formato digital de dichos estudios deberá respetar ser el mismo para el que se desarrolló dicho sistema, siendo este el formato digital PNG (con comprensión sin pérdida), ya que es un formato que puede ser manejado con las librerías de Python a diferencia de DICOM que al ser un formato sofisticado, no es compatible con este lenguaje de programación.

Las RMI se obtuvieron desde la plataforma digital Kaggle, la cual es un repositorio de información masiva. Se tomó como referencia el proyecto: "Preprocessed Alzheimer Disease RMI (Magnetic Resonance Imaging)"[2] donde se tiene alrededor de 6000 RMI's relacionadas con la enfermedad de Alzheimer que fueron utilizadas para realizar las pruebas durante el desarrollo del proyecto.

Las imágenes fueron recopiladas con el fin de realizar una clasificación óptima, con la ayuda de Médicos especialistas, de la enfermedad de Alzheimer. Estas imágenes se dividen en 4 principales categorías:

- Demencia muy leve
- Demencia leve
- Demencia moderada
- No hay demencia

Además otro proyecto con el cual se tomó como referencia es el de "Brain Tumor Classification (RMI)"[3] donde se desarrolla la clasificación de tumores cerebrales, ya que la mejor técnica para detectar esta enfermedad es a través de Imágenes de Resonancia Magnética.

De esta forma, el sistema de seguridad planteado para ser usado únicamente por los médicos radiólogos autorizados, podrá insertar la información mínima necesaria para poder identificar el estudio, cifrarla y posteriormente ocultarla en cualquier Imagen de Resonancia Magnética sin importar el área del cuerpo donde fue tomada.

Para la etapa de pruebas del funcionamiento del sistema, se tuvo un dispositivo con la capacidad de conectarse a internet, ya que con esto le fue posible acceder a la base de datos que se encuentra en la nube, permitiéndole obtener de esta forma la cadena cifrada, además de tener instalado el sistema de seguridad en el dispositivo.

El sistema final estará dirigido únicamente al personal médico que está encargado de manejar este tipo de estudios médicos, es decir, los médicos radiólogos y los médicos especialistas. En dicho sistema se encontrarán un menú con dos opciones: la primera para poder elegir la RMI a la que se le desea insertar la marca de agua con la información que será cifrada y de esta forma, mantenerla oculta.

Y la segunda que únicamente permitirá visualizar las imágenes que ya han sido marcadas. El menú desarrollado puede ser manejado de forma fácil, rápida y de manera accesible, diseñado para que el personal médico encargado, pueda usarlo y probarlo, de manera que ellos podrán evaluar su aplicabilidad y accesibilidad.

	<b>Esteganografía</b>	<b>Criptografía</b>
Ventajas	Ayuda a verificar la confidencialidad de los datos, ya que permite ocultar información que sólo es conocida por el remitente y el destinatario.	Permite mantener la privacidad de la información, ya que sólo puede ser leída por las personas que tienen la clave de descifrado.
Desventajas	La capacidad de ocultar información puede ser limitada por el tamaño, lo que puede hacer que no sea una opción viable en algunas situaciones.	Si se pierde la clave de cifrado, puede ser imposible acceder a los datos cifrados, lo que puede resultar en la pérdida de información importante.
Seguridad	La información oculta es difícil de detectar y puede ayudar a proteger la información.	Permite proteger la información contra posibles ataques intrusos.

Tabla 1: Herramientas principales a utilizar

### 1.3. Alcances

Al final del desarrollo del proyecto se obtuvo un sistema funcional, que tiene un uso útil y práctico en el ámbito médico y se espera que sea utilizado por el personal especializado, ayudando al equipo profesional a mantener una mejor transmisión y comunicación de los resultados de estudios médicos, aplicando capas de seguridad que ayuden a mantener las imágenes médicas digitales confiables.

El sistema de seguridad se le proporcionó al personal médico profesional para aprobar su aplicabilidad, funcionalidad y accesibilidad. Se contó con la Médico Internista Leticia Flores Ponce del Instituto Mexicano del Seguro Social - Unidad Pachuca con cédula profesional 11888567, que se encargó de validar el sistema, de esta forma dictaminó que no se encuentran modificaciones visibles en la Imagen de Resonancia Magnética, esto se realizó comparando una RMI original, con una RMI que contenía la marca de agua con los datos cifrados y ocultos del paciente.

## 1.4. Objetivo general

Desarrollar un sistema que sea capaz de generar mediante una técnica esteganográfica marcas de agua ocultas, las cuales contendrán los datos cifrados del paciente que se realice estudios que generen Imágenes de Resonancia Magnética, con el propósito de generar otro nivel de autenticidad y confidencialidad en los estudios médicos digitales.

## 1.5. Objetivos específicos

- Identificar información precisa acerca de los tipos de marcas de agua existentes.
- Seleccionar el tipo de marca de agua más viable para ser implementada en el proyecto.
- Analizar el estado del arte relacionado con las técnicas de esteganografía, para comprender de mejor manera los temas enfocados en ocultar información.
- Seleccionar la técnica esteganográfica que sea más conveniente para la inserción de la marca de agua en la Imagen de Resonancia Magnética.
- Seleccionar la técnica de criptografía adecuada para el cifrado de la información del paciente.
- Analizar las características fundamentales de una RMI para evaluar la preservación de la información que nos brinda el estudio.
- Diseñar una interfaz para uso exclusivo del personal médico autorizado, en donde sea posible abrir un archivo con extensión PNG.
- Implementar la opción de añadir la marca de agua con los datos que se desean cifrar.



## INSERCIÓN DE MARCAS DE AGUA OCULTAS Y CIFRADAS EN IMÁGENES DE RESONANCIA MAGNÉTICA APLICADAS EN DISPOSITIVOS IoT

### MARCO TEÓRICO

## 2. MARCO TEÓRICO

### 2.1. Marcas de agua digitales

Una marca de agua digital es información que se inserta en un contenido digital que puede ser utilizada para determinar la propiedad del mismo, saber quién lo ha creado o para asegurar su integridad. El término marca de agua procede de una analogía con las imágenes que se graban en los billetes para garantizar su autenticidad, muy difíciles y costosas de reproducir y que generalmente no son perceptibles a simple vista. En inglés se utiliza la palabra watermark, cuya equivalencia en español es filigrana, sin embargo, lo habitual es usar la traducción literal: water (agua), mark (marca).

La utilización de marcas en distintos soportes, generalmente en papel o similares, es una técnica empleada desde la antigüedad. Los griegos ya la utilizaron, pero fue con la aparición de la imprenta cuando su uso se hizo más habitual. Su principal objetivo era la acreditación de la calidad del material así como la originalidad y autenticidad del mismo. [4].

Al ser una marca de agua digital un conjunto de datos que se insertan directamente sobre el material multimedia, esto significa que la marca implica una modificación del propio contenido. La señal digital es modificada y algunos de los bits que representan el contenido son parcial o totalmente cambiados. En ningún caso estas modificaciones deben suponer una degradación de la calidad del material ni alterar las condiciones en las que éste va a ser visto.

Los sentidos del ser humano tienen un rango limitado, dentro del cual, son capaces de percibir las señales que le llegan. El espectro visible se encuentra entre 400 y 700 nm (nanómetros) de longitud de onda, que es lo que una persona puede ver. Longitudes de onda inferiores a 400 nm (ultravioleta) o superiores a 700 nm, (infrarrojo) resultan invisibles para el ojo humano. [4].

El hecho de que no se pueda ver una señal no quiere decir que no pueda formar parte de la información que se envía o se almacena, es precisamente en estos límites donde se puede introducir información en forma de marca de agua.

La aplicación de marcas de agua en imágenes enfocadas a la confidencialidad generalmente cumplen con los siguientes requerimientos que deben satisfacer los métodos de marcado:

- Debe ser invisible a la percepción humana y no debe afectar a la calidad del material digital.
- Debe ser difícil de eliminar mediante algoritmos de procesado de señal.
- Debe ser difícil de falsificar. [5].

Por lo tanto una marca de agua es un logotipo, un texto o una firma que se superpone en una imagen y suele ser transparente para que quienes vean la imagen puedan apreciarla con normalidad. Las imágenes con marca de agua sirven para brindar autenticidad al contenido, garantizan que no se pueda usar sin consentimiento del propietario y que tampoco pueda ser modificada [6].

### **2.1.1. Propiedades de las marcas de agua**

Existe un gran número de publicaciones en las que se discuten los requisitos que deben cumplir las marcas de agua. Es bueno destacar que la seguridad de estos sistemas no debe estar basada en la ocultación de los algoritmos utilizados, sino en la fortaleza de los mismos y en la seguridad de la clave.[5].

A continuación se describirán las propiedades referentes al proceso de inserción: efectividad, imperceptibilidad, indetectabilidad y capacidad; y al proceso de extracción: detección ciega o informada, probabilidad de error y robustez de los esquemas de marcas de agua invisibles. Aunque existen marcas de agua visibles, las propiedades que se discutirán serán únicamente para las marcas de agua invisibles.

#### **a) Efectividad**

La efectividad de un esquema de marcas de agua, se refiere a la eficacia del proceso de inserción de la marca de agua de manera correcta. Un archivo se dice que está marcado si el esquema de extracción encuentra una marca en él. La efectividad del esquema de marca de agua se puede medir insertando a un conjunto grande de imágenes la marca de agua, de ahí calcular el porcentaje de imágenes a las que se les ha detectado positivamente. Este porcentaje es la aproximación de la efectividad del esquema, el cual será más preciso si el conjunto de imágenes es lo suficientemente grande y si la clase de imágenes de prueba tienen las mismas características que se espera en la aplicación.

#### **b) Imperceptibilidad**

La imperceptibilidad o transparencia de la marca tiene como base el comportamiento del sistema perceptual humano. Una marca de agua es imperceptible (transparente), si la degradación que causa en los archivos donde se ha insertado es muy difícil de apreciar. La imperceptibilidad de una marca de agua es la similitud perceptual entre la imagen original y la marcada, es decir, las modificaciones causadas en el proceso de inserción de la marca de agua en la imagen original no deben degradar la calidad de la misma a tal punto que sea perceptible visualmente por el usuario. Las diferencias solo pueden llegar a medirse comparando directamente la imagen original con la marcada.

**c) Indetectabilidad**

La indetectabilidad está relacionada con el modelo estadístico del archivo antes y después de ser marcado. Se dice que la marca es indetectable, si después de haberla insertado, el archivo marcado conserva las mismas propiedades estadísticas que su original, esto quiere decir que, una persona no autorizada, no podrá detectar la presencia de la marca utilizando métodos estadísticos.[8]

**d) Capacidad**

La capacidad se refiere a la cantidad de bits de información que un esquema de marca de agua puede insertar dentro un medio sin comprometer su estructura. Cuando se utiliza la marca de agua para proteger la propiedad de un medio que es transferido a otro propietario en ocasiones es deseable que el sistema sea capaz de insertar distintas marcas de agua en un solo archivo (imagen) y que cada una de las marcas insertadas puedan ser detectadas usando su correspondiente llave.

**e) Detección ciega o informada**

Los esquemas de marcas de agua de detección ciega, son aquellos en los que no se tiene acceso al archivo original al momento de detectar el mensaje oculto, estos esquemas suelen ser muy complicados de elaborar. Los esquemas de detección informada, son aquellos en los que es necesario tener acceso al medio original para poder extraer el mensaje oculto, también existen aquellos esquemas de detección informada en los que, si bien no se tiene el medio original, si se tiene información referente al medio original o una llave de acceso.[7]

**f) Probabilidad de error**

La probabilidad de error se refiere a la posibilidad de detectar una marca de agua en un medio que no lo tiene o de no encontrar la marca de agua en un medio que si este marcado, estos tipos de errores se les llama falso positivo y falso negativo respectivamente. En cualquier esquema de marca de agua es importante tener una probabilidad de error abajo del 15 %, para tener la certeza de un resultado confiable.

**g) Robustez**

La robustez se refiere a la preservación de la marca de agua después de que el medio marcado sufra modificaciones, ya sea de manera deliberada o usando ataques o por manipulaciones comunes tales como compresión, filtrados para la extracción de ruido, cambio de tamaño, cambios en el contraste o brillo, etc. Una marca de agua se considera robusta si perdura después de esas operaciones. Esto es posible siempre y cuando la calidad de la imagen marcada permanezca dentro de límites aceptables.

La valoración de esta propiedad de los sistemas de marcas de agua, no incluye los ataques basados en el conocimiento de los algoritmos de incrustado y detección de la marca, la robustez significa resistencia a ciegas frente a aquellas modificaciones producidas por las operaciones comunes a las que estarán expuestos los archivos multimedia.[7]

### 2.1.2. Clasificación de las marcas de agua

Los esquemas de marca de agua cuentan con ciertas clasificaciones cuya importancia depende de los requerimientos y aplicabilidad que se le esté dando al esquema de la marca como lo son, el tipo de resistencia, la perceptibilidad y el dominio en donde se trabaja, además de las necesidades y objetivos del autor.

A continuación se describirán las diferentes formas de clasificar las marcas siguiendo diferentes criterios, de acuerdo al siguiente diagrama.

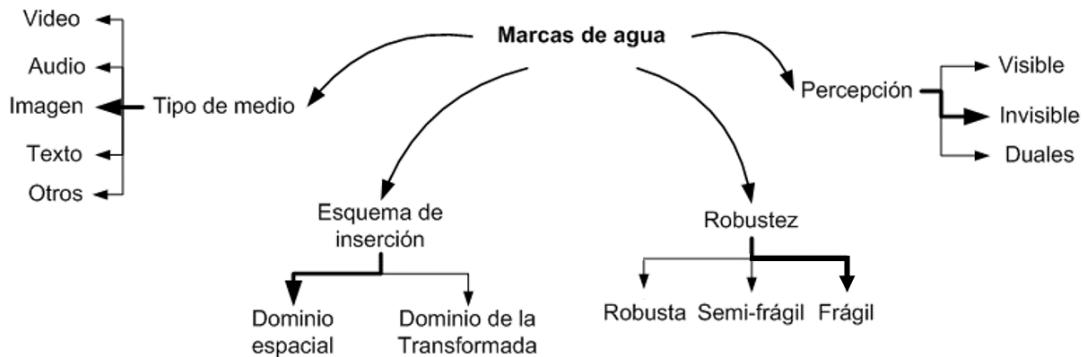


Figura 2: Esquema de la clasificación general de las marcas de agua  
[7]

### 2.1.3. Percepción

Según la percepción visual humana a la marca, estas se clasifican en:

- Visible.** Es una imagen secundaria traslúcida sobrepuerta en una imagen primaria (imagen original), la marca de agua aparece visible para el observador sin necesidad de una inspección cuidadosa.
- Invisible.** Es completamente imperceptible para el sistema visual humano, este tipo de marcas de agua se utiliza cuando se desea mantener la fidelidad o calidad de la imagen original.
- Dual.** Es la combinación entre la marca visible y una marca invisible en una misma imagen. [7]

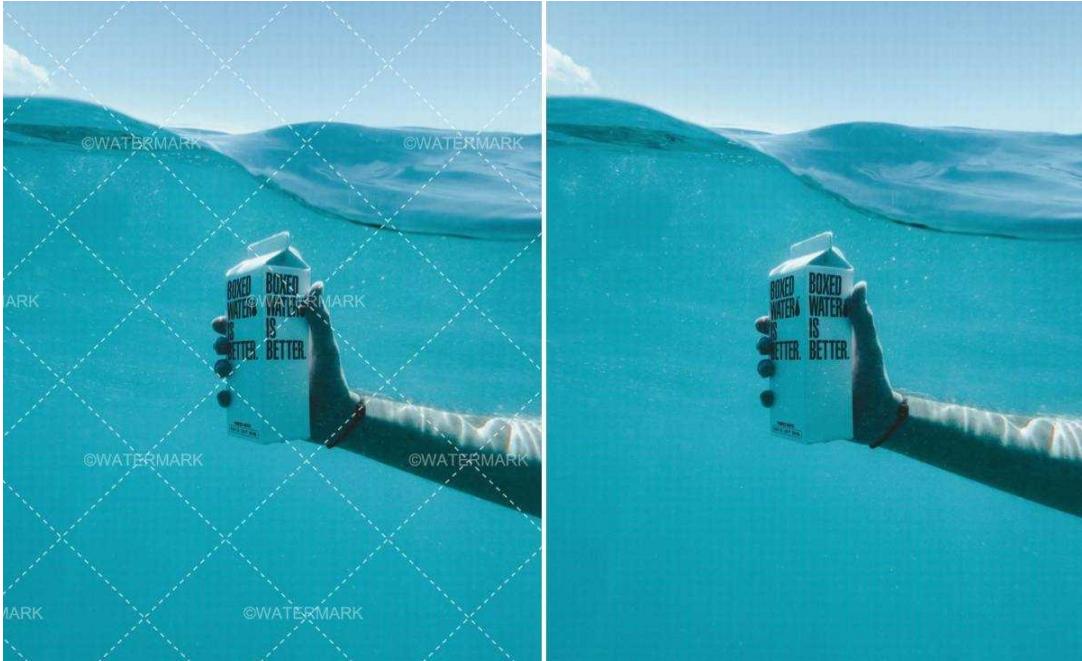


Figura 3: Marca de agua visible vs Marca de agua invisible  
[9]

#### 2.1.4. Robustez

Según su reacción ante los ataques (robustez), sin importar si los ataques son intencionales o no, las marcas se clasifican en:

a) **Robustas**

Las marcas de agua robustas deben resistir todo tipo de ataques, detectándoselas incluso después de producidos los mismos. Sirven para proteger los derechos de autor. En el caso de imágenes, no se puede tolerar la eliminación de la marca por deformaciones geométricas, rotación, escalado o compresión.

b) **Frágiles**

Las marcas de agua frágiles son aquellas que quedan eliminadas o modificadas y dejan de cumplir su función en caso de ataque. La incapacidad de recuperarlas, revela que se produjo algún cambio y ese es el objetivo buscado.

No toleran ninguna transformación, ni siquiera las más comunes en procesamiento de datos. Se utilizan fundamentalmente para asegurar integridad ya que a través de ellas se conoce si el objeto fue alterado.

c) **Semifrágiles**

Las marcas de agua semifrágiles sobreviven a cierto tipo de alteraciones, como compresión sin pérdidas, pero deben destruirse ante cambios importantes, no reversibles. [7]

### 2.1.5. Esquema de inserción

Según el dominio en el que es insertada una marca, las técnicas para imágenes pueden dividirse de la siguiente manera:

#### a) En el dominio espacial

En el dominio espacial se utiliza cambiando el LSB (Least Significant Bit / Bit Menos Significativo) por un bit de la marca según una clave. Esta técnica es de baja capacidad y tiene poca resistencia ante ataques.

#### b) En el dominio de la frecuencia

Ya sea modificando los coeficientes de la Transformada de Fourier, la DCT (Transformada Discreta de Coseno), o bien de alguna de las Transformadas Wavelet.

En el dominio de la frecuencia se comenzó a emplear el embebido en los coeficientes de transformadas sin embargo esto colleva una mayor complejidad computacional. Las técnicas más populares se desarrollaron en el dominio DCT y DWT (Discrete Wavelet Transform). [7]

### 2.1.6. Aplicaciones de las marcas de agua

Los requisitos que deben cumplir en la práctica los algoritmos de marcas de agua deben analizarse dentro del entorno de trabajo del sistema y de acuerdo con la aplicación donde será utilizado, dicho esto algunas de las posibles aplicaciones de las marcas de agua son:

- Marcas de agua como Firmas.

Las marcas pueden utilizarse para firmar archivos multimedia.

- Marcas de agua transaccionales (fingerprinting).

Las marcas de agua también pueden utilizarse para identificar a los compradores de los archivos multimedia, lo que puede servir para la búsqueda del infractor en el caso de distribución de copias ilegales de un archivo dado.

- Control de copias

Las marcas de agua diseñadas para el control de copias, contendrán la información determinada por su propietario, acerca de las reglas de uso y copiado de los archivos en los que se insertan. A diferencia de las marcas de agua transaccionales, que sólo sirven como herramienta para investigar a los transgresores del sistema, las marcas de agua usadas en el control de copias restringen la utilización de los archivos de acuerdo a las regla de uso y copiado que porten.

- Comunicaciones secretas

En esta aplicación, la marca incrustada en los archivos multimedia se utiliza por dos o más personas para comunicarse secretamente sin levantar la sospecha de terceros.

- Marcas de agua para Autenticación

Existen muchas aplicaciones donde la veracidad de una imagen es crucial, tal es el caso de imágenes médicas como las Imágenes de Resonancia Magnética (RMI).

Las marcas utilizadas para la autenticación contendrán la información requerida que determinará la integridad de un archivo multimedia. La marca debe ser invisible y frágil (cualquier modificación de la imagen debe alterar la marca). El uso de la marca posibilitará la detección de las manipulaciones en las imágenes médicas digitales ya que cualquier alteración se verá reflejado en la marca. [5]

## 2.2. Esteganografía

La esteganografía es la técnica de ocultar información dentro de otros datos, como imágenes, textos o archivos, de manera que sea difícil detectar su presencia para aquellos que no conocen el método de ocultamiento.

Las técnicas de esteganografía incluyen ocultar información en bloques de lo que parece ser texto inofensivo; esconder información dentro de las imágenes, ya sea mediante el uso de pistas sutiles o alterando de manera invisible la estructura de una imagen digital, mediante la aplicación de un algoritmo para cambiar el color de los píxeles individuales dentro de la imagen [10].

### 2.2.1. Esteganografía en imágenes

Generalmente, una esteganografía en imágenes utiliza algunos algoritmos o llaves secretas para transformar o cifrar información o imágenes, en archivos multimedia. Solo los usuarios autorizados pueden descifrar imágenes secretas, o en su caso, la información oculta.

Los datos ocultos no pueden ser reconocidos por usuarios no autorizados sin conocer los algoritmos de descifrado [11]. En la mayoría de los casos, la información se oculta en los píxeles y se extrae mediante herramientas especiales.

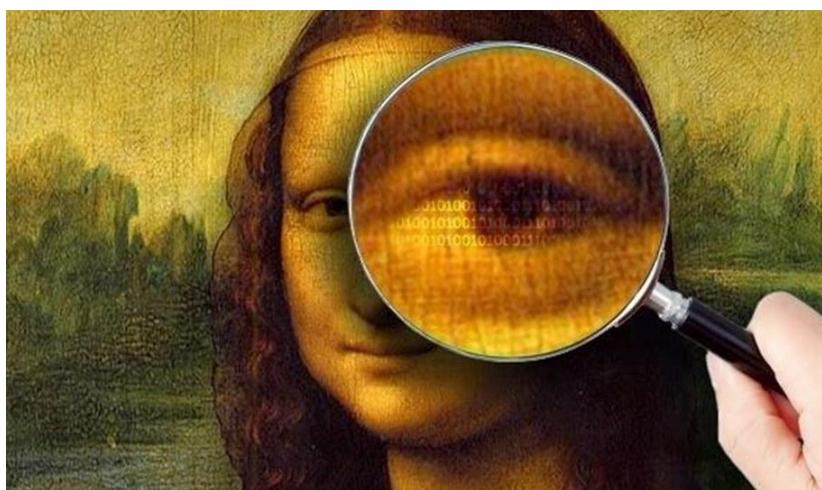


Figura 4: Imagen ilustrativa de la esteganografía  
[12]

### 2.2.2. Características de la esteganografía

Las siguientes características son atributos que permiten determinar la fortaleza o debilidad de su utilidad [13]:

- **Capacidad de incorporación**

Cantidad de datos que pueden ocultarse, en relación con el tamaño. Este atributo se mide con la unidad bit-por-bit (bpb). Un algoritmo con esta característica es ideal para ocultar una cantidad pequeña de datos.

- **Invisibilidad**

Antes de definir esta característica se debe aclarar que cualquier dato oculto en el portador causa que sea modificado. La invisibilidad mide la cantidad de distorsión del portador, siendo una medida cuantitativa. La forma de medirla es comparando el antes y después de la incorporación. Si no se pueden indicar diferencias se le llama altamente invisible. (este atributo se vincula a la percepción visual del ser humano).

- **Indetectabilidad**

Se refiere a las propiedades estadísticas de los datos del portador. Si al examinarlo se encuentran diferencias importantes en comparación a lo esperado generará sospechas de la presencia de información oculta. Un buen algoritmo no debe modificar las propiedades estadísticas del portador.

- **Robustez**

Capacidad para mantener sin cambios los datos embebidos en el portador, incluso después de que el portador se haya sometido a varias modificaciones tales como filtros, rotación, ampliación, entre otros. Este atributo es importante cuando los datos a ocultar consisten en marcas de agua.

Las técnicas que permiten ocultar mayor información (capacidad) son menos robustas y pasan desapercibidas (invisibilidad). Por el contrario, a mayor robustez normalmente se obtiene menor cantidad de información oculta.[14]

### 2.2.3. Clasificación de la esteganografía

Estas son algunas de las formas en las que se pueden dividir a la esteganografía, de manera que se realizó una clasificación general basada en diferentes criterios.

1. Según el tipo de medio en el que se oculta la información:

- a) **Esteganografía en imágenes**

Se oculta información en imágenes digitales. Esto es común en la esteganografía de imágenes en color y en escala de grises.

**b) Esteganografía en audio**

La información se oculta en archivos de audio, como música o grabaciones.

**c) Esteganografía en vídeo**

Similar a la esteganografía en imágenes, pero se oculta información en archivos de vídeo.

2. Según el nivel de ocultación:

**a) Esteganografía de alta capacidad**

Se centra en ocultar una gran cantidad de información en el medio de manera efectiva.

**b) Esteganografía de baja capacidad**

Se utiliza para ocultar una cantidad limitada de información de manera que sea menos perceptible.

3. Segundo la detección y extracción de datos ocultos:

**a) Esteganografía reversible**

Permite recuperar la información oculta sin pérdida de datos.

**b) Esteganografía irreversible**

Implica cierta pérdida de datos durante el proceso de ocultación y recuperación de la información.

4. Segundo la técnica utilizada para ocultar información:

**a) Bit menos significativo (LSB)**

Esta técnica implica ocultar datos en los bits menos significativos de los píxeles de una imagen.

**b) Transformación de dominio**

Se basa en aplicar transformaciones matemáticas o algoritmos específicos para ocultar datos en el dominio de frecuencia o en otros dominios de una señal.

**c) Modulación de frecuencia**

Esta técnica se utiliza en esteganografía de audio y se basa en la modulación de la frecuencia de una señal para ocultar información.

**d) Sustitución de caracteres**

En el caso de texto, se oculta información reemplazando caracteres con otros caracteres o utilizando técnicas como la alteración de espacios en blanco y la modificación de la estructura del texto.

Cada una tiene sus propias aplicaciones y desafíos, y la elección de cada criterio depende de los requisitos y objetivos específicos de ocultación de información. De acuerdo a este proyecto se profundizarán las técnicas utilizadas para ocultar información.

#### **2.2.4. Clasificación de las técnicas esteganográficas**

Las técnicas esteganográficas son métodos utilizados para ocultar información dentro de otros datos (como imágenes, audio o texto) de manera que sea difícil de detectar.

Estas técnicas se utilizan comúnmente para la protección de la privacidad y la seguridad de la información y se clasifican de siguiente manera:

##### **1. Técnicas de dominio espacial**

La información que se va a ocultar se inserta directamente de acuerdo a la intensidad de los píxeles. Lo que significa que algunos valores de los píxeles de la imagen cambiarán durante la ocultación de los datos.

Existen dos técnicas muy utilizadas en esta clasificación:

###### **a) Bit menos significativo (LSB)**

Reemplaza los bits menos significativos sirviendo como encubridor conjuntamente con el mensaje oculto. Tiene baja complejidad computacional. Para el ojo humano, la imagen se verá idéntica a la imagen portadora. Aunque es un método sencillo, puede ser susceptible a baja compresión y a la manipulación como escalamiento, rotación, recorte, entre otras. Debido a la notación posicional, el bit más significativo es el que está más alejado a la izquierda. Como es binario, el bit más significativo puede ser 1 o 0.

###### **b) Diferenciación del valor del píxel (PVD)**

Selecciona dos píxeles consecutivos para esconder los datos. La información se determina al comprobar la diferencia entre esos píxeles, se sustituye por otros similares en los que se incluyen bits de datos a ocultar. [15]

##### **2. Ensanchamiento de espectro**

La información que se quiere ocultar se distribuye en un ancho de banda con frecuencia amplia. La relación señal a ruido en cada banda debe ser tan pequeña con el fin de que sea difícil detectar la presencia de datos. Una ventaja es que si se elimina parte de los datos en algunas bandas, todavía existirá suficiente información en otras bandas para recuperar la información oculta, lo que hace difícil eliminar los datos por completo sin destruir totalmente la imagen. La técnica es muy robusta y se utiliza principalmente en comunicaciones militares. [16]

##### **3. Técnica estadística**

Utiliza propiedades estadísticas propias de la imagen. Cuando las propiedades estadísticas cambian da como resultado 1, de caso contrario el objeto no se modifica.

##### **4. Enmascarado y filtrado**

Se basa en el marcado de una imagen. Solo oculta información cuando las marcas de agua son parte de la imagen. Esta técnica incorpora la información en las áreas más significativas en lugar de esconderla a modo de ruido. Las marcas de agua se pueden aplicar sin temor a destruir la imagen. Es un método usado en imágenes de 24 bits y en escala de grises. [15]

## 5. Técnicas de dominio frecuencial

El mensaje a ocultar se incorpora en el dominio de la frecuencia. Es una forma más compleja de ocultar mensajes en una imagen debido a que usa diferentes algoritmos y transformaciones sobre la imagen. [16]

Los diferentes métodos relacionados al dominio frecuencial son:

### a) Transformada Discreta de Fourier (DFT)

Es el proceso que transforma una señal digital definida en el dominio espacial a la misma señal en el dominio de la frecuencia. En lugar de utilizar descomposición de senos y cosenos se utiliza la descomposición equivalente en exponenciales de números imaginarios. [17]

### b) Transformada Discreta de Coseno (DCT)

Es semejante a la DFT, toma un conjunto de puntos del dominio espacial y los transforma en una representación equivalente en el dominio de la frecuencia. Es la más usada en compresión de imágenes. No guarda relación lineal entre los valores. Los vectores van a depender únicamente del orden de selección de la transformada y no de las propiedades estadísticas de los datos de entrada.[18] La imagen se separa en sub-bandas con respecto a sus componentes de frecuencia y así se obtienen los coeficientes DCT. Los coeficientes cuyo valor no superen un umbral estipulado, determinan las ubicaciones susceptibles para la incorporación de la información a ocultar. [19]

### c) Transformada Discreta Wavelet (DWT)

Se diferencia de las dos anteriores ya que puede proporcionar una representación para ambas representaciones simultáneamente. Es utilizada como funciones base para representar señales e imágenes. Al aplicarla a una imagen digital, se aplica un banco de filtrado proporcionando una matriz de coeficientes llamados coeficientes wavelets. Se obtienen tres matrices de aproximación llamadas sub-bandas de detalle horizontal, vertical y diagonal. [20] La información a ocultar se incorpora en los coeficientes de detalle de la imagen para generar la menor distorsión posible. [19]

## 2.3. Seguridad de la información

La seguridad de la información se manifiesta de muchas maneras según la situación y las necesidades. La información solía almacenarse y transmitirse en papel, gran parte de ella reside ahora en soportes digitales y se transmite a través de sistemas de telecomunicaciones, algunos inalámbricos, esto genera a su vez la oportunidad de copiar y alterar la información.

Independientemente de quién esté implicado, en un grado u otro, todas las partes de una transacción deben tener la confianza de que se han cumplido ciertos objetivos asociados a la seguridad de la información. [21]

Los objetivos más importantes se presentan en la siguiente tabla [22]:

<b>Privacidad o confidencialidad</b>	Mantener la información en secreto, salvo para las personas autorizadas a verla.
<b>Integridad de los datos</b>	Garantizar que la información no ha sido alterada por medios no autorizados o desconocidos.
<b>Autenticación o identificación de entidades</b>	Corroboration de la identidad de una entidad (por ejemplo, una persona, un terminal informático, una tarjeta de crédito, etc.).
<b>Autorización</b>	Transmisión, a otra entidad, de una sanción oficial para hacer o ser algo.
<b>Validación</b>	Medio para garantizar la validez de la autorización para utilizar o manipular información o recursos.
<b>Control de acceso</b>	Restricción del acceso a los recursos a las entidades privilegiadas.
<b>Certificación</b>	Refrendo de la información por una entidad de confianza.
<b>Recepción</b>	Acuse de recibo de una información.
<b>Propiedad</b>	Un medio para otorgar a una entidad el derecho legal a utilizar o transferir un recurso a otros.
<b>Anonimato</b>	Ocultar la identidad de una entidad implicada en algún proceso.
<b>No repudio</b>	Impedir la negación de compromisos o acciones anteriores.

Tabla 2: Objetivos de la seguridad de la información

Hoy en día se pueden hacer miles de copias idénticas de una información almacenada electrónicamente y cada una de ellas es indistinguible del original. En una sociedad en la que la mayor parte de la información se almacena y transmite mayoritariamente en formato electrónico, los objetivos de seguridad de la información se basan únicamente en la propia información digital.

## 2.4. Criptografía

Criptografía viene del griego cripto (oculto) y graphos (escribir), se traduce como escribir mensajes ocultos. Consiste en aplicarle un algoritmo a la información original dando como resultado un nuevo documento que estará cifrado. La privacidad se consigue gracias a la clave del algoritmo que son un conjunto de valores que se combinan con la información original, es necesario conocer ambos para poder descifrar la información.

Es la práctica de asegurar la comunicación de los adversarios. [21]

Dicho de otra manera, la criptografía es el estudio de las técnicas matemáticas relacionadas con aspectos de la seguridad de la información como la confidencialidad, la integridad de los datos, la autenticación de entidades y la autenticación del origen de los datos. La criptografía no es el único medio de proporcionar seguridad a la información, sino más bien un conjunto de técnicas.

La criptografía hace posible que cualquier transacción o proceso en el cual se intercambie información o datos de importancia, sea del tipo comercial, financiera o militar, se efectúe con un alto grado de seguridad y confiabilidad.

La criptografía es la encargada del estudio de la codificación o encriptamiento de la información con el fin de que ningún usuario más que el propietario o una persona autorizada puedan decodificarla o desencriptarla mediante el uso de una clave que solo es conocida por el propietario.

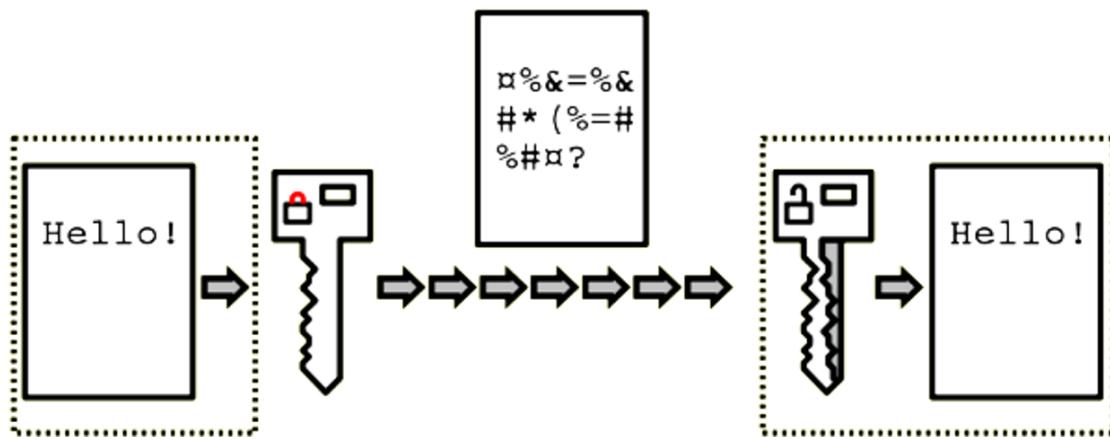


Figura 5: Esquema general de la Criptografía  
[22]

La necesidad de codificar información no es algo reciente, existen indicios de técnicas de codificación en el pasado, por ejemplo, los hebreos empleaban una técnica de codificación llamada Atbash la cual era sencilla pero muy efectiva. Consistía en sustituir la primera letra del alfabeto hebreo por la última, la segunda por la penúltima y así sucesivamente. Al pasar los años las técnicas fueron mejorando hasta llegar a ser lo que hoy conocemos como criptografía clásica. [21]

#### **2.4.1. Objetivos criptográficos**

De todos los objetivos de seguridad de la información enumerados en la Tabla 2, los cuatro siguientes constituyen un marco sobre el que se derivarán los demás [23]:

##### **1. Privacidad o confidencialidad**

Es un servicio utilizado para mantener el contenido de la información alejado de todos, excepto de aquellos autorizados a tenerla.

Existen numerosos enfoques para proporcionar confidencialidad, que van desde la protección física hasta los algoritmos matemáticos que hacen que los datos sean ilegibles. Secrecy (Secreto) es un término sinónimo de confidencialidad y privacidad.

##### **2. Integridad de los datos**

Es un servicio que se ocupa de la alteración no autorizada de los datos. Para garantizar la integridad de los datos, se debe tener la capacidad de detectar la manipulación de los datos por partes no autorizadas. La manipulación de datos incluye la inserción, la supresión y la sustitución.

##### **3. Autenticación**

Es un servicio relacionado con la identificación. Esta función se aplica tanto a las entidades como a la propia información. Dos partes que inician una comunicación deben identificarse entre sí.

La información entregada a través de un canal debe ser autenticada en cuanto a su origen, fecha de origen, contenido de los datos, hora de envío, etc.

Por estas razones, este aspecto de la criptografía suele subdividirse en dos grandes clases: la autenticación de entidades y la autenticación del origen de los datos. La autenticación del origen de los datos garantiza implícitamente la integridad de los datos (ya que si un mensaje se modifica, el origen ha cambiado).

##### **4. No repudio**

Es un servicio que impide a una entidad negar compromisos o acciones anteriores. Cuando surgen controversias debido a que una entidad niega que se hayan realizado determinadas acciones, es necesario un medio para resolver la situación.

Por ejemplo, una entidad puede autorizar la compra de una propiedad por parte de otra entidad y negar posteriormente que se concediera dicha autorización.

Se necesita un procedimiento en el que intervenga un tercero de confianza para resolver la disputa.

Un objetivo fundamental de la criptografía es abordar adecuadamente estas cuatro áreas, tanto en la teoría como en la práctica. La criptografía trata de la prevención y detección de trampas y otras actividades maliciosas.

### 2.4.2. Primitivas criptográficas

Existen una serie de herramientas criptográficas básicas (primitivas) utilizadas para garantizar la seguridad de la información. Algunos ejemplos de primitivas son los esquemas de cifrado, las funciones hash y los esquemas de firma digital.

A continuación se presenta un esquema de las primitivas mencionadas y cómo se relacionan.

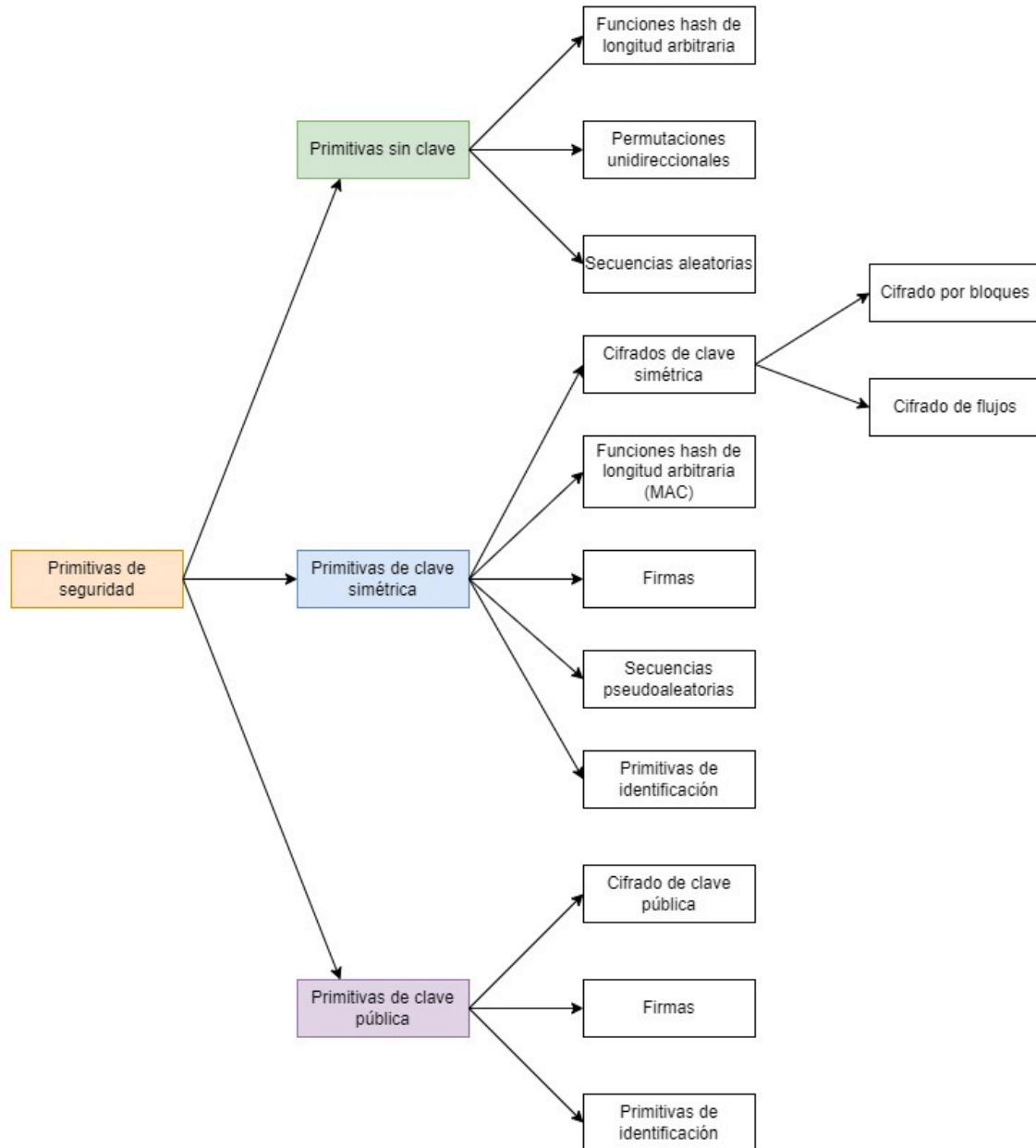


Figura 6: Taxonomía de las primitivas criptográficas  
[23]

Estas primitivas deben evaluarse con respecto a varios criterios como [21]:

a) **Nivel de seguridad**

Suele ser difícil de cuantificar. A menudo se expresa en términos de número de operaciones necesarias (utilizando los mejores métodos conocidos actualmente) para derrotar el objetivo perseguido. Normalmente, el nivel de seguridad se define mediante un límite superior en la cantidad de trabajo necesaria para superar el objetivo.

A veces se denomina factor trabajo.

b) **Funcionalidad**

Las primitivas deberán combinarse para cumplir diversos objetivos de seguridad de la información. Las propiedades básicas de las primitivas determinarán qué primitivas son las más eficaces para un objetivo determinado.

c) **Métodos de funcionamiento**

Las primitivas, cuando se aplican de varias maneras y con varias entradas, mostrarán típicamente características diferentes; por lo tanto, una primitiva podría proporcionar una funcionalidad muy diferente dependiendo de su modo de operación o uso.

d) **Rendimiento**

Se refiere a la eficacia de una primitiva en un modo de funcionamiento concreto. (Por ejemplo, un algoritmo de cifrado puede calificarse por el número de bits por segundo que puede cifrar).

e) **Funcionalidad**

Facilidad de implementación. Se refiere a la dificultad de realizar la primitiva en una instancia práctica. Puede incluir la complejidad de implementar la primitiva en un entorno de software o hardware.

La importancia relativa de los distintos criterios depende en gran medida de la aplicación y de los recursos disponibles. Por ejemplo, en un entorno en el que la potencia de cálculo es limitada es posible que haya que sacrificar un alto nivel de seguridad por un mejor rendimiento del sistema en su conjunto.

#### 2.4.3. Técnicas de criptografía

La criptografía ayudará a que, aunque otras personas ajenas a la información que se está tratando y con intenciones de dañar o alterar el contenido lleguen a tener acceso a ella, no puedan entenderla ni interpretarla, ya que se encontrara cifrada, es ahí donde la criptografía tiene un papel muy importante en el manejo de información.

El cifrado utiliza un algoritmo relacionado con otra variable, lo que conocemos como la clave o llave, hace el texto o la información incomprensible para los que no puedan tener dicha clave o variable. Por todo ello, las técnicas criptográficas son las que se encargan del cifrado del contenido. [24]

Las tres principales técnicas de criptografía son [25]:

- **Simétrica**

Conocida también como criptografía de clave secreta, utiliza una sola clave secreta para cifrar y descifrar la información. Esta clave debe mantenerse secreta entre el emisor y el receptor para garantizar la seguridad de la información. La clave se comparte de forma segura antes de iniciar cualquier tipo de comunicación.

Ejemplos de algoritmos de cifrado simétricos incluyen AES (Advanced Encryption Standard) y DES (Data Encryption Standard).

- **Asimétrica**

También conocida como criptografía de clave pública, utiliza dos claves diferentes para cifrar y descifrar la información: una clave pública y una clave privada. La clave pública se puede compartir ampliamente para cifrar la información, mientras que la clave privada se mantiene en secreto para descifrar la información. Usualmente la clave privada se usa para programar el mensaje y la clave pública es para descifrarlo. Ejemplos de algoritmos de cifrado asimétricos incluyen RSA (Rivest-Shamir-Adleman) y ECC (Elliptic Curve Cryptography).

- **Hashing**

Es una técnica de criptografía que convierte un conjunto de datos de cualquier longitud en un valor de tamaño fijo llamado hash. El objetivo principal de esta técnica es la integridad de los datos, ya que cualquier modificación en los datos originales cambiará el valor del hash.

Ejemplos de algoritmos de hashing incluyen MD5 (Message Digest 5) y SHA (Secure Hash Algorithm).

La criptografía simétrica es más rápida para descifrar los mensajes, esto la hace adecuada para aplicaciones que tienen un tráfico de datos alto y necesitan alta seguridad.

La desventaja, sin embargo, es que necesita disponer de una clave secreta compartida entre los usuarios.

La criptografía asimétrica, ofrece mayor seguridad, ya que necesita dos claves distintas para cifrar y descifrar el mensaje.

La desventaja es su velocidad, ya que toma mucho tiempo cifrar los datos.

Hoy en día existe otra técnica llamada, criptografía de clave compartida, que es una técnica que, como su nombre lo menciona, utiliza una clave compartida entre el emisor y el receptor para cifrar y descifrar la información. Este tipo de criptografía se utiliza principalmente en redes de área local (LAN) y en sistemas de comunicación por radio.

Ejemplos de algoritmos de cifrado de clave compartida incluyen RC4 (Rivest Cipher 4) y RC5 (Rivest Cipher 5). [26]

#### 2.4.4. Técnicas de cifrado de información

El cifrado es el proceso de convertir texto sin formato en texto cifrado. El cifrado es solo una parte de la criptografía y solo trata de transformar los datos en un código secreto. Existen dos técnicas usadas en el cifrado de la información, la simétrica y la asimétrica.

##### a) Cifrado simétrico

Los algoritmos de cifrado simétrico usan la misma clave tanto para cifrar como para descifrar. Son sencillos de usar y bastante eficientes hablando del tiempo en que tardan en cifrar o descifrar. Los más utilizados actualmente son: DES, 3DES, AES, Blowfish e IDEA.

El proceso es simple, se tiene la información que se quiere enviar entonces se le aplica el algoritmo simétrico usando la clave única, que de igual forma es conocida por el receptor, dando como resultado información cifrada. Cuando el receptor recibe la información le aplica el mismo algoritmo con la clave única pero ahora hace la función de descifrar. Si el documento no fue alterado en el camino y la clave coincide con la que se cifró entonces se obtendrá la información original.

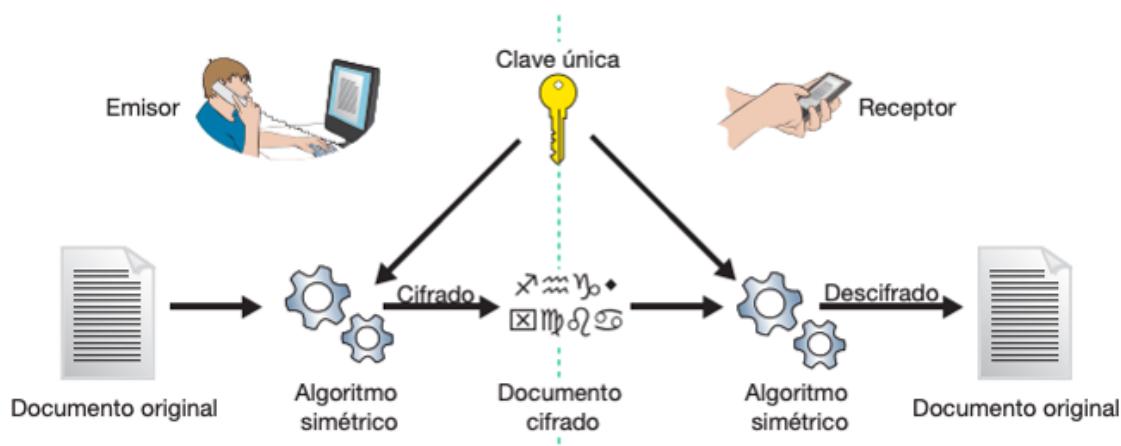


Figura 7: Esquema general del Cifrado Simétrico

[24]

El principal problema que se tiene con el cifrado simétrico es la circulación de las llaves al intentar conseguir que tanto el emisor y el receptor tengan la clave correcta. Se debe usar un segundo canal de comunicación que debe protegerse para que sea seguro.

Otro posible problema es la gestión de las claves almacenadas, puesto si se necesita compartir la misma información con más de una persona, se necesitará la misma cantidad de claves como de personas a las que se compartirá la información. [25]

### b) Cifrado asimétrico

Los criptógrafos Diffie y Hellman publicaron sus investigaciones sobre criptografía en los años setenta. Este algoritmo usaría dos claves matemáticamente relacionadas de forma que al cifrar con una clave solo se puede descifrar con la otra.

Ahora el emisor no necesita conocer y proteger una clave propia, es el receptor que tiene el par de claves.

Se llama clave pública a la que es usada para comunicar si se envía algo cifrado, pero ya no se necesitan los canales protegidos porque aunque un tercero pueda capturar la clave pública y la información cifrada, no podrá descifrar, ya que no conoce la clave de pareja que se le conoce como clave privada, la cual nunca es comunicada y es imposible deducir matemáticamente la clave privada solo conociendo la clave pública.



Figura 8: Esquema general del Cifrado Asimétrico  
[24]

El cifrado asimétrico logra resolver los problemas que se tienen al usar el cifrado simétrico pero tiene sus propios problemas. Empezando porque son poco eficientes, debido a la longitud de las claves suelen tardar bastante tiempo en cifrar o descifrar, además se debe proteger la clave privada guardándola en un llavero que contiene todas las llaves privadas y ese fichero se protegerá con cifrado simétrico, también es recomendable hacer uso de una copia de seguridad del llavero. [21]

#### 2.4.5. Algoritmos de cifrado de llave simétrica

La mayoría de los algoritmos simétricos actuales se apoyan en los conceptos de Confusión y Difusión desarrollados por Claude Shannon sobre la Teoría de la Información a finales de los años cuarenta. Estos métodos consisten en ocultar la relación entre el texto plano, el texto cifrado y la clave (Confusión); y repartir la influencia de cada bit del mensaje original lo más posible entre el mensaje cifrado (Difusión). [27]

La criptografía simétrica o criptografía de una clave, es un método en el cual se usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez que ambas partes tienen acceso a esta clave, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra con la misma clave. [25] A continuación se describe cada uno de los seis principales algoritmos de cifrado de llave simétrica.

## 1. DES (Data Encryption Standard)

Es el algoritmo simétrico más extendido mundialmente. A mediados de los setenta fue adoptado como estándar para las comunicaciones seguras (Estándar AES) del gobierno de EE.UU. En su principio fue diseñado por la NSA (National Security Agency) para ser implementado en hardware, pero al extenderse su algoritmo se comenzó a implementar en software.

DES utiliza bloques de 64 bits, los cuales codifica empleando claves de 56 bits y aplicando permutaciones a nivel de bit en diferentes momentos (mediante tablas de permutaciones y operaciones XOR).

El algoritmo AES es un algoritmo de cifrado de bloques (opera con bloques de un tamaño fijo) que toma texto sin formato en bloques de 128 bits y los convierte en texto cifrado. En la actualidad no se ha podido romper el sistema DES criptanalíticamente (deducir la clave simétrica a partir de la información interceptada). Sin embargo una empresa española sin fines de lucro llamado Electronic Frontier Foundation (EFF) construyó en Enero de 1999 una máquina capaz de probar las 256 claves posibles en DES y romperlo sólo en tres días con fuerza bruta.

A pesar de su caída DES sigue siendo utilizado por su amplia extensión de las implementaciones vía hardware existentes (en cajeros automáticos y señales de video por ejemplo) y se evita tener que confiar en nuevas tecnologías no probadas. En vez de abandonar su utilización se prefiere suplantar a DES con lo que se conoce como cifrado múltiple, es decir aplicar varias veces el mismo algoritmo para fortalecer la longitud de la clave. [27]

## 2. IDEA (International Data Encryption Algorithm)

Fue desarrollado en Alemania a principios de los noventa por James L. Massey y Xuejia Lai. Trabaja con bloques de 64 bits de longitud empleando una clave de 128 bits y, como en el caso de DES, se utiliza el mismo algoritmo tanto para cifrar como para descifrar.

El proceso de encriptación consiste ocho rondas de cifrado idéntico, excepto por las subclaves utilizadas (segmentos de 16 bits de los 128 de la clave), en donde se combinan diferentes operaciones matemáticas (XOR's y Sumas Módulo 16) y una transformación final. [25]

### **3. AES (Advanced Encryption Standard)**

Es uno de los algoritmos más ampliamente utilizados. Este método se conceptualizó por primera vez en 1997, cuando el Instituto Nacional de Estándares y Tecnología en EEUU (NIST por sus siglas en inglés, National Institute of Standards and Technology) pasó a ser vulnerable a los ataques de fuerza bruta y necesitó un método de cifrado más potente. El NIST recurrió a dos desarrolladores, Vincent Rijmen y Joan Daemen, para que solucionaran el problema y desarrollaran la tecnología finalmente elegida, AES, en 1998. AES ha sido la norma de cifrado del NIST desde su adopción a gran escala en 2002.

AES viene en diferentes longitudes de clave (128, 192 o 256 bits) y es altamente seguro y eficiente en términos de velocidad y uso de recursos. El algoritmo AES es un algoritmo de cifrado de bloques (opera con bloques de un tamaño fijo) que toma texto sin formato en bloques y los convierte en texto cifrado. [28]

### **4. BlowFish**

Este algoritmo fue desarrollado por Bruce Schneier en 1993. Para la encriptación emplea bloques de 64 bits y permite claves de encriptación de diversas longitudes (hasta 448 bits).

Generalmente, utiliza valores decimales (aunque puede cambiarse a voluntad) para obtener las funciones de encriptación y desencriptación. Estas funciones emplean operaciones lógicas simples y presentes en cualquier procesador. Esto se traduce en un algoritmo "liviano", que permite su implementación, vía hardware, en cualquier controlador (como teléfonos celulares por ejemplo).

### **5. Twofish**

Es un algoritmo de cifrado de bloque de clave simétrica con un tamaño de bloque de 128 bits y longitudes de clave de hasta 256 bits.

Twofish está relacionado con el anterior cifrado por bloques Blowfish. Las principales características de Twofish son el uso de cajas dependientes de la clave precalculada y un programa de claves relativamente complejo. Una mitad de una clave de n bits se utiliza como clave de cifrado real y la otra mitad de la clave de n bits se utiliza para modificar el algoritmo de cifrado (cajas dependientes de la clave).

### **6. CAST**

Es un buen sistema de cifrado en bloques con una clave CAST-128 bits. Su nombre deriva de las iniciales de sus autores, Carlisle, Adams, Stafford Tavares, de la empresa Northern Telecom (NorTel). CAST no tiene claves débiles o semidébiles y hay fuertes argumentos acerca que este algoritmo de cifrado es completamente inmune a los métodos de criptoanálisis más potentes conocidos.

A continuación en la siguiente tabla se presentan las fortalezas y vulnerabilidades que cada algoritmo de cifrado de llave simétrica posee.

Algoritmo	Fortalezas	Vulnerabilidades
DES	<ul style="list-style-type: none"> <li>-Codifica bloques de 64 bits.</li> <li>-Consta de 16 rondas para descifrar</li> <li>-Es muy rápido y fácil de implementar.</li> </ul>	<ul style="list-style-type: none"> <li>-Emplea una clave demasiado corta.</li> <li>-Tamaño de bloque pequeño.</li> </ul>
IDEA	<ul style="list-style-type: none"> <li>-El espacio de claves es más grande.</li> <li>-Todas las operaciones son algebraicas.</li> <li>-No hay operaciones a nivel bit.</li> </ul>	<ul style="list-style-type: none"> <li>-Velocidad de procesamiento.</li> <li>-Algoritmo de cifrado antiguo.</li> </ul>
AES	<ul style="list-style-type: none"> <li>-Gran velocidad de cifrado y descifrado</li> <li>-Combina la seguridad-eficiencia-velocidad, sencillez y flexibilidad.</li> </ul>	<ul style="list-style-type: none"> <li>-La seguridad depende de un secreto compartido entre emisor y receptor.</li> <li>-La administración de las claves no es escalable</li> </ul>
Blowfish	<ul style="list-style-type: none"> <li>-Tiene una estructura sencilla lo que lo hace fácil de utilizar.</li> <li>-Variables seguras, la longitud de la clave es variable y puede ser hasta de 448 bits.</li> </ul>	<ul style="list-style-type: none"> <li>-Existe una clase de llaves que pueden ser detectadas en 14 rondas o menos pero no rotas por el algoritmo Blowfish.</li> </ul>
Twofish	<ul style="list-style-type: none"> <li>-No hay claves débiles.</li> <li>-Diseño flexible, acepta llaves de longitud variable.</li> </ul>	<ul style="list-style-type: none"> <li>-Puede ser más complejo de implementar y entender debido a su estructura y diseño.</li> </ul>
CAST	<ul style="list-style-type: none"> <li>-Codifica bloques de 64 bits con claves de igual longotud.</li> <li>-Consta de ocho rondas y deposita toda su fuerza en las s-cajas.</li> </ul>	<ul style="list-style-type: none"> <li>-Falta de flexibilidad en tamaños de clave y bloque.</li> <li>-Longitudes de clave más cortas.</li> <li>-Adopción limitada.</li> </ul>

Tabla 3: Fortalezas vs Vulnerabilidades de algoritmo de cifrado

## 2.5. RMI (Imagen de Resonancia Magnética)

La RMI es un procedimiento que utiliza ondas de radio, un imán potente y una computadora a fin de crear una serie de imágenes detalladas del área interior del cuerpo.

Se puede inyectar material de contraste como gadolinio para ayudar a que los tejidos y los órganos se resalten con más claridad en la imagen. La Imagen por Resonancia Magnética se utiliza para diagnosticar enfermedades, planificar el tratamiento o averiguar si existe un buen funcionamiento en el área de estudio. Es útil para examinar el encéfalo, médula espinal, corazón, vasos sanguíneos, huesos, articulaciones, tejidos blandos, órganos de la pelvis y abdomen. Es conocida también como RMN (Imagen por Resonancia Magnética Nuclear) y tomografía por resonancia magnética [30].

Apareció a principios de la década de los 80's y desde entonces se convirtió en el método más utilizado para ciertas aplicaciones médicas y ahora gracias a las nuevas tecnologías que han surgido relacionadas al procesamiento se obtienen imágenes con información anatómica y también información funcional de los órganos.

## 2.6. Ventajas y Desventajas de las RMI

Las Imágenes de Resonancia Magnética cuentan con gran cantidad de ventajas desde un punto de vista tecnológico de las cuales destacan las siguientes:

- En comparación con la radiología o la tomografía computarizada, provee mayor contraste en la visualización de tejidos suaves.
- Gran resolución de contraste lo que permite diferenciar estructuras de densidad similar.
- No usa radiación ionizante.
- Obtiene imágenes multiplanares, es decir, múltiples planos.

Aunque tiene ciertas desventajas estas no han frenado su implementación. Algunas son las siguientes:

- Costo elevado.
- Larga duración de exploración, entre 30 y 60 minutos.
- Poco recomendable para pacientes claustrofóbicos.
- Sufre de falta de homogeneidad.

A pesar de que la resolución y la relación señal a ruido son bastante altas, hay fuentes de ruido que afectan la imagen. Entre esas fuentes están el ruido térmico, movimiento del paciente, actividad fisiológica, variaciones de frecuencia bajas y fluctuaciones vasculares. [1]



Figura 9: Imagen de Resonancia Magnética de Rodilla Izquierda  
[31]

Dentro de la Imagen de Resonancia Magnética se pude observar que principalmente se distribuye la información en 4 secciones, cada sección en cada esquina.

Se logra apreciar que la ubicación de cada sección nos brinda diferente información como se muestra a continuación:



Identifica el tamaño de la imagen.



Delimita características como el zoom, ángulo ocupado y tipo de imagen.



Identifica la ubicación exacta de la parte del cuerpo del paciente.



Define la fecha, la hora y el lugar en donde se tomo la imagen.

Figura 10: Distribución de secciones de una Imagen de Resonancia Magnética

## 2.7. Archivos de imágenes

Existe una gran cantidad de archivos de imágenes disponibles y no hay dos iguales. Conocer las características de cada tipo de archivo de imagen es importante para elegir el formato adecuado para nuestro sistema de seguridad, ya que se tendrán que cumplir con los siguientes criterios [32]:

- Calidad de imagen
- Compatibilidad con el software
- Capacidad de redimensionamiento
- Facilidad para compartir

A continuación se presentarán los archivos de imágenes más conocidos actualmente.

### 2.7.1. Archivos vectoriales

Haciendo uso de fórmulas matemáticas se establecen puntos en una cuadrícula para conseguir imágenes vectoriales. La clave en este tipo de archivos es su versatilidad ya que puede ajustarse su tamaño en innumerables veces sin que se pierda la resolución. Es ideal para imágenes que necesitan cambiar de tamaño con regularidad. [32]

#### 2.7.1.1 Archivos SVG (Scalable Vector Graphics)

Los Gráficos Vectoriales Ampliables son una herramienta que se usa habitualmente para mostrar gráficos, diagramas e ilustraciones bidimensionales en sitios web. Al ser un archivo vectorial se puede ampliar y reducir sin perder resolución. [33]

#### 2.7.1.2 Archivos STL (Stereolithography)

Es un formato de archivo usado con frecuencia para la impresión 3D y el diseño asistido por computadora (CAD). La estereolitografía es una tecnología conocida en la impresión 3D.[34]

#### 2.7.1.3 Archivos EPS (Encapsulated PostScript)

Gestiona los gráficos vectoriales y prepara las imágenes para obtener impresiones de alta resolución, es el estándar para el sector de impresión profesional. Se emplea a menudo en las impresoras y filmadoras PostScript para producir imágenes amplias y detalladas para anuncios publicitarios o material de marketing para captar la atención del público. [35]

### 2.7.2. Archivos rasterizados

Un archivo de imagen rasterizado está compuesto por un número fijo de píxeles de color. Lo que significa que si se cambia el tamaño su resolución podría afectarse. Este tipo de imágenes se encuentran en Internet y en la prensa, una considerable ventaja es que se pueden abrir con una gran variedad de programas. [32]

### **2.7.2.1 Archivos GIF (Graphics Interchange Format)**

El Formato de Intercambio de Gráficos se emplea para mostrar gráficos y logotipos en sitios web. Admite una animación básica por lo que es un formato muy popular para crear imágenes en redes sociales. [36]

### **2.7.2.2 Archivos PNG (Portable Network Graphic)**

El Gráfico de Red Portátil es un tipo de archivo con mucha popularidad debido a su capacidad de procesar los gráficos con fondos transparentes o semitransparentes. No se trata de un archivo patentado por lo que se puede abrir con cualquier software de edición. Se emplea de forma generalizada para mostrar imágenes digitales de alta calidad. Se creó para mejorar el rendimiento del tipo de archivo GIF, ofrece una compresión sin pérdidas de datos y también una paleta de colores más variada y brillante. [37]

### **2.7.2.3 Archivos JPEG (Joint Photographic Experts Group)**

Joint Photographic Experts Group es la organización internacional que estandarizó este formato entre finales de los ochenta y principios de los noventa. Se trata del formato de archivo estándar para las imágenes digitales en la actualidad y está presente en todo el mundo. [38]

### **2.7.2.4 Archivos DNG (Digital Negative)**

Se trata de un tipo de formato de archivo sin procesar empleado en la fotografía digital. Almacena datos sin comprimir lo que permite al usuario almacenar, compartir y editar sin tener problemas con la incompatibilidad. [39]

## 2.8. Procesamiento digital de imágenes

El análisis y procesamiento de imágenes se realiza a través de computadoras, debido a la complejidad y el número de cálculos necesarios para realizarlo. El procesamiento de imágenes tiene como objetivo mejorar el aspecto de las imágenes y hacer más evidentes en ellas ciertos detalles que se desean hacer notar. La imagen puede haber sido generada de muchas maneras, por ejemplo, fotográficamente, o electrónicamente, por medio de monitores de televisión. [40] Para realizar el procesamiento digital de imágenes se requiere hacer uso de transformadas, a continuación se presenta una tabla comparativa con las más usadas actualmente.

	Fourier	Hilbert	Wavelet	Z
Ventajas	Permite un análisis en la frecuencia muy acertado, es sencilla de implementar en señales de transmisión y difusión.	Análisis rápido para poder obtener datos de la propiedad de una señal sin cambiar el plano de análisis.	Un análisis profundo de la señal así como también la eliminación de ruido debido a su gran cantidad de filtros utilizados.	Permite una transmisión de datos más rápida, es más complicada de decodificar por lo que representa seguridad en la transmisión de datos.
Desventajas	No puede filtrar bien el ruido por lo que la señal que deseamos obtener puede causar problemas en la modulación.	Es muy simple y no puede ser considerada de peso en el análisis de frecuencia ya que sólo desplaza el plano a analizar más no cambia de plano.	No permite un análisis de tiempo continuo por lo que no es aplicable a señales analógicas.	
Aplicaciones	Mecánica cuántica, termodinámica, Señales y sistemas, Electricidad, Automatización, Radiodifusión.	Geometría, Señales y sistemas, DCPS.	Radiodifusión, Geología, Fotografía, Animación, Medicina.	Termodinámica, Electrónica, Automatización, Radiodifusión, Señales y sistemas.

Tabla 4: Comparación de transformadas

### 2.8.1. Pasos fundamentales en el Procesamiento Digital de Imágenes

Existen pasos fundamentales para realizar el procesamiento de una imagen como lo son:

- **Adquisición de la imagen.** Puede incluir cierto pre-procesamiento como el escalamiento.
- **Mejora de la imagen.** Consiste en resaltar detalles que son oscuros o no tan claros, o resaltar ciertas características de interés de la imagen. (Restauración subjetiva)
- **Restauración de la Imagen.** Busca mejorar la apariencia de una imagen. Sin embargo, esta restauración es objetiva en comparación con el paso anterior, en el sentido en que las técnicas que se utilizan tienden a basarse en modelos matemáticos y probabilísticos.
- **Procesamiento del color de la imagen.** Sirve para extraer características de interés en una imagen, en comparación con una imagen en tonos de grises.
- **Wavelets.** Son la base para representar imágenes en varios niveles de resolución (por ejemplo, la compresión).
- **Compresión.** Trata con las técnicas para reducir la cantidad de memoria que se requiere para guardar una imagen o el ancho de banda requerido para transmitirla.
- **Procesamiento morfológico.** Consta de herramientas para extraer componentes de la imagen que son útiles en la representación y descripción de la forma.
- **Segmentación.** Consiste en partir una imagen en partes u objetos para las áreas de reconocimiento.
- **Representación y descripción.** Siempre va después de la segmentación y sirve para extraer las características de la imagen (el límite de una región o los puntos de la misma región).
- **Reconocimiento.** Es el proceso que asigna un nivel a un objeto basado en su descripción.

## 2.9. Técnicas de similitud en imágenes médicas

Para poder analizar la similitud entre imágenes médicas es necesario utilizar una herramienta fundamental en el procesamiento de imágenes que es la segmentación. Existen diferentes enfoques y técnicas para la segmentación de imágenes, que van desde métodos simples basados en umbrales hasta algoritmos más avanzados basados en aprendizaje automático y técnicas de procesamiento de señales. La elección del método depende del tipo de imágenes y del contexto de la aplicación específica.

### Segmentación de imágenes

La segmentación de imágenes es una técnica de procesamiento que se refiere a la extracción de información útil de una escena para facilitar su observación y análisis, ya que el resto del contenido de una imagen puede estar contaminado o no ser útil para el propósito buscado. La segmentación de imágenes médicas enfrenta tres problemas principales vinculados a las imágenes [41]:

- Las imágenes contienen gran cantidad de ruido, lo cual dificulta la clasificación de píxeles por intensidad.
- La intensidad en los tejidos y órganos, no es uniforme.
- Un píxel puede tener diferentes intensidades, producto de la mezcla de clases de tejidos.

La segmentación se logra con diferentes métodos y combinación de los mismos.

La clasificación de dichos métodos varía de una bibliografía a otra.

## 2.10. Técnicas de segmentación

Hoy en día existe una gran variedad de métodos de segmentación, por esa razón la selección del método depende en gran medida de la aplicación, del tipo de imagen y de las características de la misma, entre otros factores.

En esta sección se hará una descripción breve de los métodos de segmentación que gozan de popularidad en el campo de la medicina. CITE

### 1. Umbralización (Thresholding)

Consiste básicamente en una comparación de nivel de intensidad píxel a píxel con un determinado umbral, definido previamente por el usuario. Para establecer dicho umbral, es necesario analizar la región de interés que se desea aislar con el propósito de encontrar un nivel de gris característico y exclusivo que la defina. Para cumplir con esta tarea, se suele recurrir al histograma de la imagen. [40]

Para completar el análisis, se debe tomar una decisión significativa: ¿qué hacer con los píxeles que corresponden a la región de interés, y qué con el resto de los píxeles de la imagen? La respuesta no es única, ya que estará en función de lo que se requiera para la aplicación.

Por ejemplo si se desea conservar la información de interés tal cual, el algoritmo implementado debe dejar intactos los valores de los píxeles que corresponden a la región, sin embargo, todos aquellos que no cumplan con la condición del umbral, se les debe asignar un nuevo y único nivel de gris para evitar que la primera información nuevamente se mezcle. La salida de la umbralización se puede ver como la formación de dos planos, el primero que contiene la información aislada y el segundo, la información sobrante, para sintetizar el funcionamiento del método de umbralización, se muestra un diagrama de bloques en la siguiente figura.

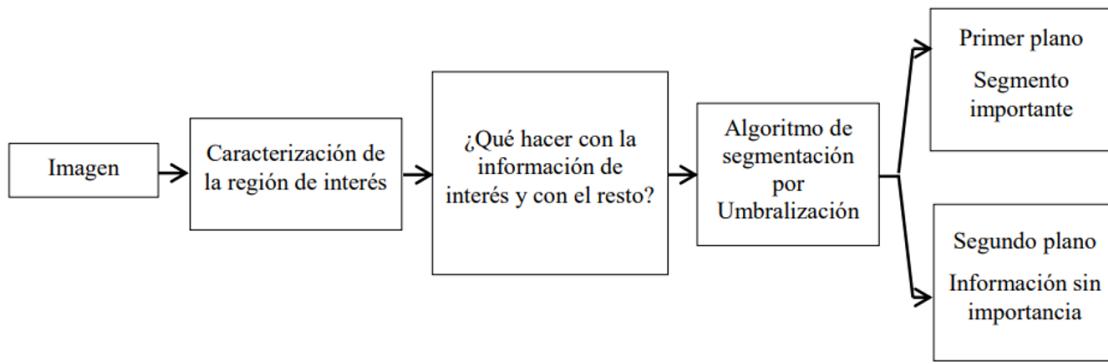


Figura 11: Diagrama de bloques del método de Umbralización  
[41]

## 2. Crecimiento de región (Region Growing)

Es un método basado en similitud, tiene como objetivo determinar los píxeles que cumplen con cierto criterio de semejanza y permite agruparlos en regiones.

El crecimiento de región es un proceso iterativo, que inicia con puntos semilla, los cuales representan las características que definen a la región y que deben tener los píxeles candidatos para poder ser agregados a la misma, este procedimiento se lleva a cabo mediante la comparación de los píxeles vecinos con los puntos semilla, o los puntos pertenecientes a la región. Por lo tanto la selección de los puntos semilla es un paso significativo en este método, ya que los resultados dependerán directamente del criterio de semejanza que se establezca.[39]

El criterio de semejanza es establecido por el usuario y debe contener las características de la información que se desea separar de la imagen original (intensidad, textura, entre otras) para poder fijar el umbral, por lo tanto los píxeles que cumplen con el criterio de dicho umbral, se adicionan a las semillas formando una región, que a su vez será la nueva semilla en la siguiente iteración.

Una vez seleccionados los puntos semilla la región crecerá únicamente hacia los píxeles vecinos que cumplan con el criterio establecido con anterioridad, con lo cual se garantiza conectividad entre los píxeles que constituyen una región.

Para el crecimiento de la región, básicamente se necesitan dos condiciones:

- Los píxeles candidatos deben cumplir con un criterio de semejanza.
- Los píxeles candidatos pueden adherirse a la región, si y sólo si, son vecinos de los puntos semilla, o de algún píxel de la región.

Este proceso se repite, y el crecimiento de la región se detendrá cuando los píxeles vecinos a las semillas, ya no cumplan con el criterio de semejanza que define a la región.

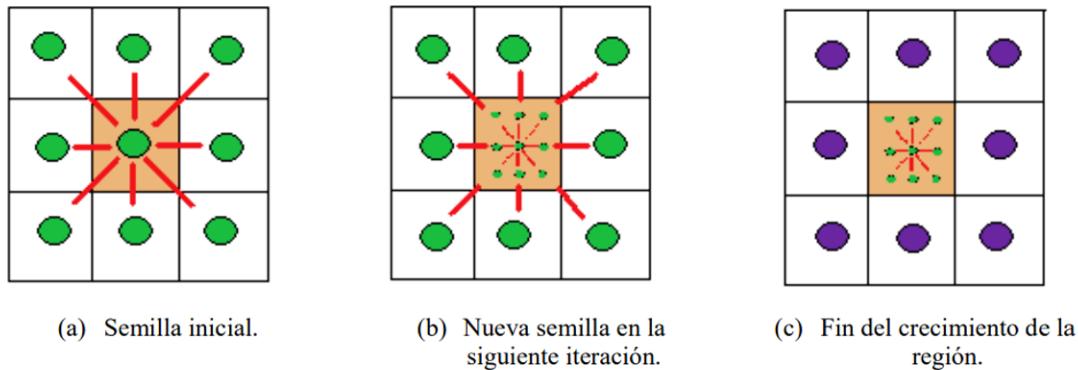


Figura 12: Crecimiento de región

[41]

En la figura anterior sección a) se observa el punto semilla y los píxeles adyacentes (con conectividad 8) que cumplen con el criterio de semejanza, los cuales se adicionan a la región formando una nueva región que se muestra en la imagen sección b) con sus nuevos píxeles vecinos, que al cumplir nuevamente con el criterio de semejanza forman una nueva región, y en la sección c) se muestra esta región con sus píxeles vecinos que ya no cumplen con el criterio de semejanza. Es así que se detiene el crecimiento de la región.

El crecimiento de región es un método utilizado en imágenes médicas bajo la hipótesis de que los píxeles pertenecientes a un mismo tejido u órgano presentan características similares con un significado semántico.

Además de que presenta ciertas ventajas sobre los métodos basados en frontera, sobre todo en imágenes ruidosas donde los bordes son difíciles de detectar, pero a costa de un mayor esfuerzo computacional. [39]

Sin embargo, este método tiene los siguientes inconvenientes: es dependiente de los puntos semilla, aunque, trabajos sobre el mismo buscan disminuir esta dependencia, o cuando la región se propaga hacia zonas fuera del área de interés.

### 3. Detección de bordes

Los bordes son aquellas zonas de la imagen donde el nivel de intensidad varía bruscamente, precisamente estas partes son las que los algoritmos de “Detección de Bordes” tratan de rescatar y sobresaltar. En cuanto más rápido se produzca el cambio de intensidad, el borde será más pronunciado y fácil de detectar por dichos algoritmos. Para detectar los bordes que delimitan a los objetos, es necesario identificar aquellos puntos (píxeles) que los conforman. Esta detección es el paso más delicado del método y la razón por la que existe una gran variedad de algoritmos que tratan de satisfacer esta necesidad.

Para determinar qué píxeles pertenecen al borde, las técnicas buscan una conectividad entre ellos, bajo las siguientes dos condiciones [41]:

- Ser vecinos.
- Cumplir con un criterio de similitud.

La forma común de implementar la “Detección de Bordes”, es mediante filtros u operadores que se basan en herramientas matemáticas para su funcionamiento: gradiente y Laplaciano, por mencionar algunos. Ejemplos de filtros que pertenecen a este tipo de técnicas son el operador Sobel y Prewitt, considerados como detectores de discontinuidades.

La detección de bordes resulta apropiada para imágenes con características bien definidas, con amplio contraste. En cuanto a sus limitaciones se puede mencionar el hecho de que detecta todos los bordes, por lo que el usuario no puede obtener un borde en específico; es impactado fácilmente por el ruido y los resultados entregados sólo son útiles para la visualización del ser humano, pero no para procesamiento de alto nivel. [39]



## INSERCIÓN DE MARCAS DE AGUA OCULTAS Y CIFRADAS EN IMÁGENES DE RESONANCIA MAGNÉTICA APLICADAS EN DISPOSITIVOS IoT

ESTADO DEL ARTE

### **3. ESTADO DEL ARTE**

Este apartado busca dar a conocer precedentes de investigación que se consideran para el desarrollo de este proyecto de investigación acerca de temas relacionados con Marcas de Agua que se han realizado tanto en la Unidad Académica, como de manera comercial, para proyectar un mejor panorama de lo que se ha desarrollado hasta el día de hoy.

#### **3.1. UPIITA**

Dentro de la Unidad Profesional Interdisciplinaria en Ingeniería y Tecnologías Avanzadas se tiene registrados trabajos de investigación tales como “Software para cifrado y descifrado de archivos de texto”, así como “Marcas de agua para archivos de videos” [42]. Asimismo se encuentra una “Galería de arte con marcas de agua” [43] en donde en cada trabajo se utilizan diferentes técnicas de esteganografía, en un caso usando marcas de agua frágiles, mientras que en el otro las marcas de agua son robustas.

En todos los trabajos se utiliza la transformada Wavelet para añadir la marca de agua, y en un principio se pensó que esta transformada sería candidata a ser utilizada en la realización de este proyecto, sin embargo por la cantidad de procesamiento que se requiere para poder utilizarla impide que se tome como solución, ya que lo que se busca en este caso es un cifrado ligero, haciendo el uso del LSB (Least Significant Bit/Bit menos significativo) el mejor candidato a ser utilizado en este proyecto.

#### **3.2. Marcas de agua comerciales**

Las marcas de agua se utilizan comúnmente para garantizar la originalidad y autenticidad de las imágenes y gráficos utilizados en artículos o publicaciones, o en este caso, para estudios médicos. Estas marcas de agua comúnmente son visibles para el público y generalmente contienen información como el nombre del autor y la fecha de creación.

Actualmente gracias al desarrollo tecnológico se pueden encontrar programas comerciales para agregar marcas de agua a las imágenes, tanto gratuitos como de pago, sin embargo se caracterizan todos ellos por brindar el servicio de Marcas de agua visibles.

A continuación se presentan algunos de los programas de marcas de agua más usados comercialmente hoy en día:

- Adobe Photoshop. Uno de los programas de edición de imágenes más populares, que permite agregar marcas de agua visibles para brindar protección y derechos de autor a la imagen, además de ofrecer diferentes marcas de agua robustas [44].
- Watermark Pro. Software de escritorio fácil de usar que permite agregar marcas de agua de texto a las imágenes de forma rápida y sencilla. Brinda información adicional como añadir nombre o el aviso de derechos de autor o, incluso un logotipo como marca de agua en las fotos, así como un sello de autoridad sobre cada imagen [45].

- Add Watermark Free. Es un software de marcas de agua para terminales Android que te permite configurar ángulos de inclinación, distintas tipografías, nivel de detalle y etiquetas GPS como texto de la marca de agua.[46] Sin embargo la mayor desventaja del sistema es que no se encuentra optimizada lo suficientemente para trabajar con imágenes de alta resolución.

### 3.3. Confidencialidad de la información

Ahora bien, la proliferación de ordenadores y sistemas de comunicación en los años 60 trajo consigo una demanda por parte del sector privado de medios para proteger la información en formato digital y proporcionar servicios de seguridad.

Comenzando con el trabajo de Feistel en IBM a principios de los años 70 y culminando en 1977 con la adopción como Norma Federal de Procesamiento de la Información de Estados Unidos para cifrar información no clasificada, el DES (Data Encryption Standard) es el mecanismo criptográfico más conocido de la historia.

El avance más sorprendente en la historia de la criptografía se produjo en 1976, cuando Diffie y Hellman publicaron “New Directions in Cryptography”. Este documento introdujo el revolucionario concepto de criptografía de clave pública y también proporcionó un nuevo e ingenioso método para el intercambio de claves, cuya seguridad se basa en la intratabilidad del problema del logaritmo discreto.

Además, los laboratorios de investigación de IBM en Tokyo, asociados con Yasuda Fire & Marine Inc., han desarrollado el prototipo DataHiding que es un sistema seguro de transmisión e indexado de fotografías digitales desde la cámara digital al ordenador, cuyo propósito es verificar el origen y la integridad de las fotografías digitales.

Los últimos veinte años han sido un periodo de transición en el que la disciplina ha pasado de ser un arte a convertirse en una ciencia. Hoy en día existen conferencias científicas internacionales dedicadas exclusivamente a la criptografía y también una organización científica internacional, la Asociación Internacional para la Investigación Criptológica (IACR), destinada a fomentar la investigación en este campo. [47]

### 3.4. Diferencias con proyectos realizados en UPIITA

Proyecto de investigación		Software para cifrado y descifrado de archivos de texto.	Marcas de agua para archivos de vídeo.	Autenticación de estudios médicos digitales a través de marcas de agua frágiles.	Galería de arte con marcas de agua.	Inserción de marcas de agua ocultas y cifradas en Imágenes de Resonancia Magnética.
Esteganografía	Transformada Wavelet	✓	✓	✓	✓	
	Bit menos significativo					✓
Criptografía	Utiliza	✓				✓
	No utiliza		✓	✓	✓	
Aplicado a		Archivos de texto	Archivos de vídeo	Radiografías	Obras de arte	Imágenes de Resonancia Magnética

Tabla 5: Comparación entre Proyectos de Investigación

En la Tabla 5 se muestra la comparación de los Proyectos de Investigación que han sido realizados en la UPIITA, esto fue de ayuda para poder determinar las diferencias que tendría el proyecto en relación a ellos.

La primera distinción del proyecto con los otros es que será aplicado a las Imágenes de Resonancia Magnética. La segunda diferencia que es importante mencionar es que los demás proyectos de investigación usaron una técnica esteganográfica en el dominio de la frecuencia mientras que en este proyecto se usará una técnica en el dominio del tiempo, precisamente usando el bit menos significativo, lo cual hará que sea un procedimiento más rápido y sin necesitar demasiados requerimientos computacionales.

Por último, en este proyecto se utilizará una técnica criptográfica para darle mayor seguridad al sistema, algo que se realizó en el proyecto "Software para cifrado y descifrado de archivos de texto", sin embargo como lo menciona su nombre, se realizó el cifrado para archivos de texto.



## INSERCIÓN DE MARCAS DE AGUA OCULTAS Y CIFRADAS EN IMÁGENES DE RESONANCIA MAGNÉTICA APLICADAS EN DISPOSITIVOS IoT

ANÁLISIS

## 4. ANÁLISIS

### 4.1. Propiedades de las marcas de agua

Después de analizar cada una de las propiedades de las marcas de agua (respecto al proceso de inserción: efectividad, imperceptibilidad, indetectabilidad, capacidad y al proceso de extracción: detección ciega o informada, probabilidad de error, robustez) que influyen directamente al comportamiento del sistema de seguridad podemos determinar que de acuerdo al proyecto en desarrollo, tratándose de una aplicación especialmente para uso médico, las propiedades qué tiene el sistema son:

- **Para el proceso de inserción:** Imperceptibilidad e indetectabilidad.
- **Para el proceso de extracción:** Detección informada y robustez.

Para el proceso de extracción referente específicamente a la efectividad en el sistema (el esquema de extracción encuentra la marca, si es que se tiene) se tiene un mayor análisis en la sección Pruebas y Resultados.

### 4.2. Clasificación de las marcas de agua

- a) Podemos argumentar que dependiendo la aplicabilidad, las marcas de agua se pueden clasificar de distintas formas, por ejemplo, de acuerdo a como percibe la marca de agua un usuario, las marcas de agua se clasifican de la siguiente manera.

Marca	Descripción
Visible	En este tipo de esquemas, la información del propietario legítimo es percibida a simple vista por el usuario, sin necesidad de aplicar algún filtro o hacer un análisis a la imagen. Este tipo de esquemas se utilizan principalmente en las fotografías de la revistas, billetes y en las transmisiones de programas de televisión.
Invisible	Este tipo de esquemas aprovechan las limitaciones del Sistema Visual Humano (SVH) para insertar la marca de agua de manera que esta solo pueda ser detectada mediante un análisis de la imagen y no por los usuarios.
Dual	Este esquema es la combinación de una marca visible e invisible en la misma imagen con la finalidad de tener un respaldo invisible de la marca visible. [48]

Tabla 6: Clasificación de las marcas de agua de acuerdo a la percepción visual

En cuanto a clasificación de las marcas de agua de acuerdo a la percepción visual lo ideal es trabajar con una marca invisible, ya que se espera que solo pueda ser detectada mediante un análisis técnico de la imagen y no por los usuarios.

- b) Otra forma de clasificación es dependiendo a su reacción frente a las modificaciones que se le hagan a la imagen, es decir, el grado de resistencia, de esta forma se determinó que en cuanto a la clasificación de acuerdo a la reacción a modificaciones se utilizará una marca de agua frágil.

Marca	Descripción
<b>Robusta</b>	<p>Un esquema se dice robusto, si es capaz de recuperar/detectar la marca de agua insertada en una imagen después de que esta haya sido modificada, ya sea intencionalmente o no.</p> <p>Se utilizan principalmente en la protección de derechos de autor.</p> <p><b>Las propiedades que posee son:</b></p> <ul style="list-style-type: none"> <li>-Proceso de inserción: Efectividad, indetectabilidad, capacidad.</li> <li>-Proceso de extracción: Detección ciega, probabilidad de error, robustez.</li> </ul>
<b>Frágil</b>	<p>Se dice frágil si se destruye o altera la marca que fue insertada en la imagen, esto con la finalidad de poner en evidencia las alteraciones realizadas.</p> <p>Este tipo de esquemas se utilizan para autenticación de imágenes.</p> <p><b>Las propiedades que posee son:</b></p> <ul style="list-style-type: none"> <li>-Proceso de inserción: Efectividad, imperceptibilidad, indetectabilidad, capacidad.</li> <li>-Proceso de extracción: Detección informada, probabilidad de error, robustez.</li> </ul>
<b>Semi-frágil</b>	<p>Este tipo de marcas de agua se destruyen solo cuando el ataque es intencionado y se preserva cuando se trata de una manipulación común de la imagen.</p> <p>El mayor reto de este esquema es determinar cuándo una modificación en la imagen se considera maliciosa y cuándo no.</p> <p><b>Las propiedades que posee son:</b></p> <ul style="list-style-type: none"> <li>-Proceso de inserción: Efectividad, imperceptibilidad, indetectabilidad, capacidad.</li> <li>-Proceso de extracción: Detección ciega e informada, probabilidad de error, robustez.</li> </ul>

Tabla 7: Clasificación de las marcas de agua de acuerdo a la reacción a modificaciones

- c) Muchos autores consideran que la clasificación principal de los esquemas de marca de agua es de acuerdo al tipo de dominio en el que se inserta la marca.

Las técnicas que trabajan en el dominio espacial generan menos degradación en las imágenes originales. Sin embargo, estas técnicas son frágiles ante ataques geométricos o ante el filtrado de la imagen marcada.

Por otro lado, los esquemas que trabajan en el dominio de la frecuencia presentan mayor robustez y seguridad ante ataques, pero al contrario de las técnicas del dominio espacial, introducen más degradación en la imagen y la complejidad computacional aumenta con el uso de transformaciones directas e inversas.[49]

De este forma, de acuerdo a este criterio, las marcas de agua se pueden clasificar de la siguiente manera:

Marca	Descripción
Espacial	En los esquemas que usan el dominio espacial, la marca de agua se incrusta en la imagen portadora modificando directamente los valores de los píxeles.[50] Estos métodos tienen un bajo costo computacional y son fáciles de implementar; sin embargo, dado que el proceso de inserción de la marca de agua se realiza en el dominio espacial, la marca de agua es menos segura.
En frecuencia	En los esquemas que usan el dominio en frecuencia, la marca de agua se incrusta modulando los coeficientes de transformación de la imagen portadora. Las transformaciones más comúnmente utilizadas incluyen la Transformada de Coseno Discreta (DCT, por sus siglas en inglés), la Transformada de Wavelet Discreta (DWT, por sus siglas en inglés), y la Descomposición de Valores Singulares (SVD, por sus siglas en inglés) .[51]

Tabla 8: Clasificación de las marcas de agua de acuerdo al dominio

De acuerdo al dominio, después de juzgar las opciones se determinó trabajar con el dominio espacial ya que genera menos degradación en las imágenes originales, a comparación con el dominio en frecuencia, además de que tienen un bajo costo computacional en cuanto procesamiento.

#### 4.3. Elección de marca de agua

La elección de la marca de agua más adecuada para la confidencialidad e integridad de los datos depende de varios factores, como el tipo de datos que se están protegiendo, el propósito de la marca de agua y las amenazas a la seguridad de los datos.

En cuanto a este proyecto, de acuerdo al objetivo que se tiene es importante considerar que lo que se busca es que la marca no sea perceptible al ojo humano, por lo que lo factible es hacerla invisible; además se determinó trabajar con una marca frágil, ya que este tipo de marca de agua se destruyen solo cuando el ataque es intencionado.

En cuanto al dominio en el que es insertada la marca es el espacial, utilizando el bit menos significativo, ya que esto genera menos degradación en las imágenes originales.

Todas estas elecciones ayudan a garantizar la confidencialidad de los datos de los pacientes.

#### 4.4. Técnica criptográfica

Enfocándonos al proceso del proyecto que está relacionado con la modificación de los datos de los pacientes, se utilizó una técnica simétrica, ya que esto permite al sistema ser más sencillo y eficiente de acuerdo a un aspecto criptográfico. La elección de la técnica criptográfica se basó en las siguientes consideraciones técnicas y prácticas. [25]

a) **Rendimiento**

Los algoritmos simétricos tienden a ser más rápidos que los asimétricos. En aplicaciones donde se necesite un procesamiento rápido de datos, como en la visualización de imágenes médicas, la velocidad puede ser crucial. El cifrado simétrico puede ofrecer un rendimiento superior.

b) **Recursos**

Los algoritmos simétricos a menudo requieren menos recursos computacionales (CPU, memoria) en comparación con los algoritmos asimétricos, lo que podría ser ventajoso en entornos con limitaciones de recursos, como dispositivos médicos o sistemas embebidos utilizados en RMI, que se podrán desarrollar en un futuro.

c) **Complejidad**

Los sistemas de cifrado asimétrico suelen ser más complejos de implementar y administrar debido a la necesidad de generar y administrar pares de claves públicas y privadas. En un entorno médico, donde la simplicidad y la fiabilidad son fundamentales, el cifrado simétrico podría ser más práctico y menos propenso a errores.

d) **Seguridad**

Aunque los algoritmos asimétricos son fundamentales en el intercambio seguro de claves y la autenticación, los algoritmos simétricos también pueden proporcionar un alto nivel de seguridad si se implementan adecuadamente.

En resumen, la elección del cifrado simétrico sobre el asimétrico para el proyecto de inserción de marcas de agua en RMI podría justificarse por su mejor rendimiento, eficiencia de recursos, menor complejidad y aún proporcionar un nivel suficiente de seguridad para el entorno médico.

## 4.5. Algoritmo de cifrado

La elección del algoritmo de cifrado apropiado se tomó teniendo en cuenta el uso de la técnica criptográfica de llave simétrica, además de comparar solo los algoritmos enfocados a confidencialidad, recordando que lo que se desea principalmente en el proyecto es fortalecer este servicio de seguridad de datos, para mantener la información privada y protegida, asegurando que solo las personas autorizadas puedan acceder o conocer esa información. El programa LWC (Lightweight Cryptography - Criptografía ligera) del NIST se enfoca en identificar algoritmos criptográficos ligeros y eficientes para aplicaciones específicas como son sistemas integrados con recursos limitados.

A continuación se muestran las ventajas y desventajas de los principales algoritmos.

Algoritmo	Ventajas	Desventajas
AES	<ul style="list-style-type: none"> <li>-Gran velocidad de cifrado y descifrado</li> <li>-Combina la seguridad-eficiencia-velocidad, sencillez y flexibilidad.</li> </ul>	<ul style="list-style-type: none"> <li>-La seguridad depende de un secreto compartido entre emisor y receptor.</li> <li>-La administración de las claves no es escalable.</li> </ul>
SPECK	<ul style="list-style-type: none"> <li>-Codifica bloques de 64 bits.</li> <li>-Consta de 16 rondas para descifrar</li> <li>-Es muy rápido y fácil de implementar.</li> </ul>	<ul style="list-style-type: none"> <li>-Emplea una clave demasiado corta.</li> <li>-Tamaño de bloque pequeño.</li> </ul>
PRESENT	<ul style="list-style-type: none"> <li>-El espacio de claves es más grande.</li> <li>-Todas las operaciones son algebraicas.</li> <li>-No hay operaciones a nivel bit.</li> </ul>	<ul style="list-style-type: none"> <li>-Velocidad de procesamiento.</li> <li>-Algoritmo de cifrado antiguo.</li> </ul>
SKINNY	<ul style="list-style-type: none"> <li>-No hay claves débiles.</li> <li>-Diseño flexible, acepta llaves de longitud variable.</li> </ul>	<ul style="list-style-type: none"> <li>-Puede ser más complejo de implementar y entender debido a su estructura y diseño.</li> </ul>

Tabla 9: Ventajas y desventajas de algoritmos enfocados a confidencialidad

Se puede decir que un buen sistema de cifrado pone toda la seguridad en la clave y ninguna en el algoritmo. En otras palabras, no debería ser de ninguna ayuda para un atacante conocer el algoritmo que se está usando. Sólo si el atacante obtuviera la clave, le serviría conocer el algoritmo. Dado que toda la seguridad está en la clave, es importante que sea muy difícil adivinar el tipo de clave. Esto quiere decir que el abanico de claves posibles, es decir, el espacio de posibilidades de claves, debe ser amplio.

De este modo se determinó que en base al objetivo del proyecto es necesario un algoritmo sencillo y flexible, por lo tanto después de comparar las ventajas y las desventajas de cada algoritmo, el AES fué el utilizado en el proyecto, puesto que combina además eficiencia y velocidad. Es el ideal ya que, al tratar solo de añadir otro nivel de seguridad, no es necesario implementar un algoritmo con claves grandes o de longitud variable.

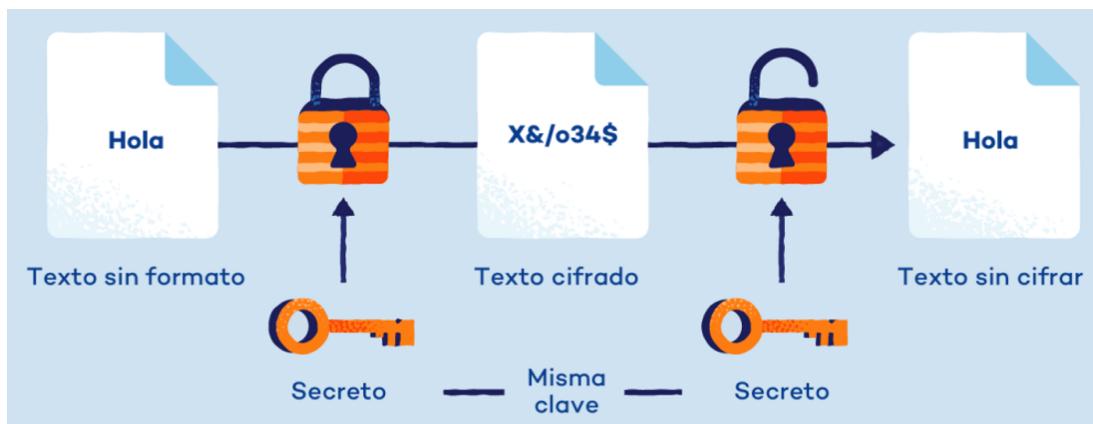


Figura 13: Esquema del Algoritmo AES  
[29]

### Ventajas de AES

AES es el método de cifrado preferido por muchos porque destaca en muchas métricas clave de rendimiento. Algunas de las ventajas de AES son [27]:

- Seguridad. Incluso con el nivel más bajo de cifrado AES, se estima que se tardaría mil millones de millones de años en descifrarlo si se utiliza un método de fuerza bruta.
- Coste. El cifrado AES es gratuito, ya que se desarrolló originalmente para ser distribuido sin derechos de autor.
- Facilidad de uso. El algoritmo AES es fácil de implementar en múltiples aplicaciones y es conocido por su simplicidad y capacidad para adaptarse a distintas plataformas de hardware y software.
- Rapidez. En comparación con otros métodos de cifrado, AES es famoso por su velocidad, ya que ofrece tiempos de cifrado y descifrado más rápidos que otros métodos.

La principal diferencia entre AES y otros métodos de cifrado es que AES utiliza varias rondas de transposición, sustitución y mezcla en lugar de una única fase de cifrado.

Este algoritmo posee distintos tipos de AES [29]:

- **AES-128**

Este método utiliza una longitud de clave de 128 bits para el cifrado y el descifrado, lo que da lugar a 10 series de cifrado con  $3,4 \times 1038$  combinaciones potenciales diferentes.

- **AES-192**

Este método utiliza una longitud de clave de 192 bits para cifrar y descifrar, lo que da lugar a 12 series de cifrado con  $6,2 \times 1057$  combinaciones potenciales diferentes.

- **AES-256**

Este método utiliza una longitud de clave de 256 bits para cifrar y descifrar, lo que da como resultado 14 series de cifrado con  $1,1 \times 1077$  combinaciones potenciales diferentes.

Escoger uno depende del uso específico. AES-256 es la clave de cifrado más fuerte, pero requiere mucha más potencia de procesamiento. De este modo al no ser necesario un algoritmo tan robusto, se determinó utilizar el AES-128, ya que brinda gran velocidad de cifrado/descifrado y no requiere tanta potencia de procesamiento, tiempo y recursos para ejecutarse.

## 4.6. Técnica esteganográfica

Al analizar y comparar distintos trabajos encontrados relacionados a la esteganografía, de todas las técnicas encontradas se clasificaron las cinco principales, que son las más utilizadas para ocultar mensajes en imágenes. De manera que se realizó una tabla comparativa con las técnicas esteganográficas estudiadas considerando las ventajas y desventajas que tendría emplear dicha técnica en un sistema enfocado al uso médico.

Técnica	Ventajas	Desventajas
Dominio espacial	<ul style="list-style-type: none"> <li>■ Baja complejidad computacional.</li> <li>■ Cambios no perceptibles al ojo humano.</li> <li>■ Método sencillo</li> </ul>	<ul style="list-style-type: none"> <li>- Susceptible a baja compresión y a la manipulación</li> </ul>
Ensanchamiento de espectro	<ul style="list-style-type: none"> <li>■ Gran capacidad para recuperar la información en caso de perdidas.</li> <li>■ Se necesita dañar por completo la imagen para perder la información.</li> </ul>	<ul style="list-style-type: none"> <li>- Es una técnica muy robusta y requiere mayor cantidad de recursos computacionales.</li> </ul>
Estadística	<ul style="list-style-type: none"> <li>■ Se enfoca en características estadísticas y no en características físicas de la imagen.</li> </ul>	<ul style="list-style-type: none"> <li>- Los algoritmos se vuelven más complejos por hacer uso de estadística y cálculos matemáticos.</li> </ul>
Enmascarado y filtrado	<ul style="list-style-type: none"> <li>■ Técnica enfocada a imágenes y marcas de agua</li> <li>■ Inserta marcas de agua sin destruir la imagen.</li> </ul>	<ul style="list-style-type: none"> <li>- Solo es usada en imágenes de 24 bits y en escala de grises.</li> </ul>
Dominio frecuencial	<ul style="list-style-type: none"> <li>■ La incrustación de los datos es mucho más fuerte en comparación a las otras técnicas.</li> <li>■ Tiene menor exposición a la compresión.</li> </ul>	<ul style="list-style-type: none"> <li>- Mayor nivel en el procesamiento, es decir gran complejidad computacional.</li> <li>- Son técnicas más complejas.</li> </ul>

Tabla 10: Tabla comparativa de las técnicas esteganográficas existentes

Podemos decir que dependiendo el uso que se le dará, las técnicas esteganográficas poseen ciertas ventajas y desventajas. De acuerdo a este proyecto, al finalizar la tabla comparativa, se determinó utilizar la técnica de dominio espacial, puesto que los cambios que ocurren en las imágenes no son perceptibles al ojo humano, en comparación con las demás técnicas, además de ser más sencillo y tener una baja complejidad computacional, de forma que esta técnica es la que mejor se adapta a nuestras necesidades.

#### 4.7. Características fundamentales de la RMI

Las características específicas de Imágenes de Resonancia Magnética (RMI) pueden variar según varios factores, como el tipo de exploración, la configuración de la máquina y el software utilizado. Sin embargo, en términos generales, las características fundamentales se muestran a continuación.

- **Formato de imagen.** Los formatos de archivo comunes para las RMI's incluyen DICOM (Digital Imaging and Communications in Medicine), que es el estándar ampliamente utilizado en la industria médica para imágenes médicas, y también pueden convertirse a otros formatos más comunes como JPEG, PNG o TIFF para visualización o almacenamiento.
- **Resolución.** Suele tener una alta resolución espacial para una mejor visualización de los tejidos y órganos, permitiendo una visualización detallada de las estructuras internas del cuerpo. Se mide en términos de píxeles por unidad de longitud (píxeles/mm o píxeles/pulgada). La resolución puede variar según la configuración del equipo y la técnica de exploración utilizada.
- **Tamaño del archivo** Los archivos de RMI's pueden variar considerablemente en tamaño dependiendo de varios factores, como la parte del cuerpo escaneada, la resolución, el tipo de secuencia de imágenes utilizada y si se ha aplicado algún tipo de compresión. Los archivos pueden variar desde varios megabytes hasta gigabytes para exploraciones de alta resolución o cuando se capturan múltiples secuencias.

En cuanto al proyecto, se trabajó con imágenes que tienen las siguientes características:

- **Formato de imagen:** PNG
- **Resolución:** 128x128 px
- **Tamaño del archivo:** 3.5 kB - 8 kB

Es importante mencionar que estos aspectos pueden variar según el equipo utilizado, el protocolo de exploración específico y la configuración del sistema de adquisición de imágenes. Además, la tecnología médica avanza constantemente, por lo que pueden surgir cambios en los estándares y las características pueden variar con el tiempo.

## 4.8. Metodologías del diseño de software

Una metodología de desarrollo de software comprende un conjunto de prácticas, técnicas y herramientas usadas por equipos de desarrollo para planificar, diseñar, construir, probar y entregar software de alta calidad de manera eficiente y efectiva.

En estas metodologías se establece una estructura para el ciclo de vida del software, definiendo requisitos, diseño, codificación, prueba, implementación y el mantenimiento. Además establece roles y responsabilidades para los miembros del equipo, procesos para la gestión del proyecto, comunicación y seguimiento del progreso. [52]

### 1. Metodologías tradicionales.

Establecen de forma muy rígida los requerimientos y procesos al inicio del proyecto, esto genera que los ciclos se hagan pocos flexibles impidiendo realizar ajustes a lo largo del proyecto. Al realizarse de manera lineal cada etapa se muestra detrás de otra, impidiendo avanzar. Las más usadas son:

- Método cascada: facilita organizar las actividades de manera vertical (arriba hacia abajo) para ejecutar de forma secuencial, evita pasar a la siguiente si la actual no se ha concluido satisfactoriamente. Su ventaja es que el paso de un nivel a otro se hace de forma segura al saber que la etapa previa ha sido finalizada.
- Método de prototipos: con este método se crea un borrador del software sin importar detalles para que los usuarios puedan dar retroalimentación al interactuar con la aplicación permitiendo verificar fallos técnicos, esto implica un costo adicional en el presupuesto que debe ser considerado.
- Método incremental: se trabaja en fase, en cada etapa se le va agregando una función o aplicabilidad, se puede notar la mejora y adicionalmente verificar el funcionamiento antes de finalizar. Es uno de los más implementados, pero también es uno de los más lentos en la ejecución.
- Método de Diseño Rápido de Aplicaciones: es una técnica que permite desarrollar en corto plazo, basándose en elaborar un prototipo para que sea probado e identificar necesidades y requerimientos.
- COBIT: es mundialmente reconocida y aceptada para proyectos tecnológicos por su gestión y flujo de procesos. Facilita el desarrollo y buenas prácticas en el control, ayuda a comprender, administrar riesgos y beneficios asociados a procesos.

## 2. Metodologías ágiles

En la actualidad son ampliamente utilizadas por la alta flexibilidad y capacidad para adaptarse a cambios. Permiten a los equipos de trabajo ser más productivos y eficientes, además proporciona flexibilidad necesaria para ajustar a medida que surjan necesidades. Este tipo de metodologías se fundamentan en el enfoque incremental, el cual añade nuevas funcionalidades a la aplicación final en cada etapa del desarrollo. Los ciclos son más cortos y rápidos, implicando que se realicen cambios y mejoras de forma gradual incorporando pequeñas funcionalidades en lugar de cambios masivos. Los equipos se reúnen periódicamente para compartir novedades y avances. Las metodologías ágiles más utilizadas son:

- DEVOPS: permite la integración de todas las áreas para garantizar la efectividad y obtener un mejor resultado. La ventaja es su facilidad de fusión e integración con otras metodologías ágiles que se apliquen incrementando beneficios.
- AGILE: permite mejorar la planificación con la finalidad de evitar perder tiempo y recursos. Ayuda a mantener la orientación pero sin ser demasiado rígido. Algunas ventajas son: mejorar la calidad al minimizar errores en los procesos, permite acortar ciclos de producción y una mejor asignación de recursos.
- SCRUM: integra un conjunto de prácticas y roles a un marco de trabajo o conocido como Framework. Permite que los proyectos desarrollados con esta metodología sean más adaptables, interactivos, rápidos, flexibles y eficaces. Su principal característica es la división de tareas y roles bien estructurada y optimizada.
- Kanban: proviene de técnicas gerenciales empleadas por Toyota para agilizar la producción. Se representa en un tablero donde se refleja el flujo de los procesos en un trabajo designado, permitiendo a cada responsable mover sus tareas libremente según los avances, con ello se genera mayor confianza y control a nivel visual.

Tener en cuenta las características de nuestro proyecto, así como también la manera en que se llevará a cabo son dos pasos importantes para saber que metodología encaja de mejor manera. Siendo nuestra elección una metodología ágil ya que además de ser más actuales, brindan mejores ventajas y se consiguen mejores resultados trabajando de la manera correcta como lo indica la metodología. La elección fue SCRUM ya que es la que ha tenido mayor desarrollo por ser la mas utilizada actualmente y se adaptará de mejor manera a la forma de trabajo para el equipo.

#### 4.9. Lenguaje de programación para el procesamiento de imágenes

Para el procesamiento de imágenes se busca el mejor lenguaje de programación que cuente con bibliotecas que puedan ser usadas para cumplir las funcionalidades del sistema.

El primer lenguaje de programación es Python, uno de los más populares y que tiene un aprendizaje auto didáctico. Algunas de sus ventajas son su simplicidad, facilidad de lectura y amplio apoyo que tiene en la comunidad de programadores, lo que lo convierte en la opción ideal para el procesamiento. Ofrece numerosas bibliotecas diseñadas específicamente para el procesamiento de imágenes, tales como: [53]

- Pillow: Es la biblioteca más utilizada para abrir, manipular y guardar diferentes formatos de archivo de imagen. Proporciona extensas capacidades de manipulación de imágenes, pero no soporta operaciones de álgebra lineal o transformaciones de Fourier.
- OpenCV: Ofrece una interfaz integral para el procesamiento de imágenes y la visión por computadora. Incluye características para realizar operaciones complejas en imágenes, aunque puede ser menos intuitiva para los principiantes.
- Scikit-Image: Proporciona una gran cantidad de algoritmos para el procesamiento de imágenes, incluyendo la segmentación de imágenes, morfología y transformaciones. Es una extensión de SciPy, por lo que es compatible con muchos otros paquetes científicos de Python.
- Matplotlib: Es ampliamente utilizada para la visualización de datos en Python, incluyendo imágenes. Proporciona una gran cantidad de opciones para personalizar gráficos y diagramas, pero no es una biblioteca de procesamiento de imágenes.
- ImageIO: Utilizada para leer y escribir una amplia gama de formatos de imagen. También puede leer imágenes directamente desde URL y ofrece soporte para metadatos de imagen y manejo de datos volumétricos 3D.

Además de Python, también c++ y Java ofrecen bibliotecas para el procesamiento de imágenes, por ejemplo Caffe es un marco de aprendizaje desarrollado en c++, es popular por su velocidad y eficiencia, siendo usado ampliamente en tareas de procesamiento de imágenes.

Java ofrece bibliotecas como JavaCV que es un contenedor para OpenCV que proporciona una interfaz para el procesamiento de imágenes.

Dada a la investigación podemos seleccionar el lenguaje de programación Python, ya que este tiene mayor soporte para el procesamiento de imágenes, contando con bibliotecas que pueden ir desde lo más básico hasta lo más complejo, siendo muy útil para los requerimientos del proyecto.



## INSERCIÓN DE MARCAS DE AGUA OCULTAS Y CIFRADAS EN IMÁGENES DE RESONANCIA MAGNÉTICA APLICADAS EN DISPOSITIVOS IoT



### DISEÑO

## 5. DISEÑO

### 5.1. Requerimientos mínimos necesarios para la instalación

#### Memoria y equipo

- Memoria RAM: Es necesario mínimo 8 GB.
- Procesador: Intel, mínimo core i3
- Almacenamiento del disco: 64 GB
- Sistema operativo: Windows/iOS

Una vez cumpliendo con los requerimientos mínimos necesarios para la instalación del sistema de seguridad mencionados anteriormente, los médicos solamente deberán instalar el sistema y contar con conexión a internet para tener un funcionamiento óptimo.

De acuerdo con las anteriores especificaciones el tiempo en que la marca de agua se tarda en añadirse es aproximadamente menor a 8 segundos.

#### Características de las RMI

- Formato de imagen: PNG
- Resolución: 128x128 px
- Tamaño del archivo: 3.5 kB - 8 kB.

En cuanto al proyecto, se trabajó con imágenes que tienen las especificaciones mencionadas anteriormente, de manera que para que el sistema funcione correctamente se deberán tomar en cuenta.

El sistema no se limita en cuanto a alguna parte del cuerpo específica, es decir, siempre y cuando se cumplan con los requerimientos mínimos de memoria y equipo, el formato de la imagen y el tamaño del archivo.

## 5.2. Diagrama General del Funcionamiento del sistema

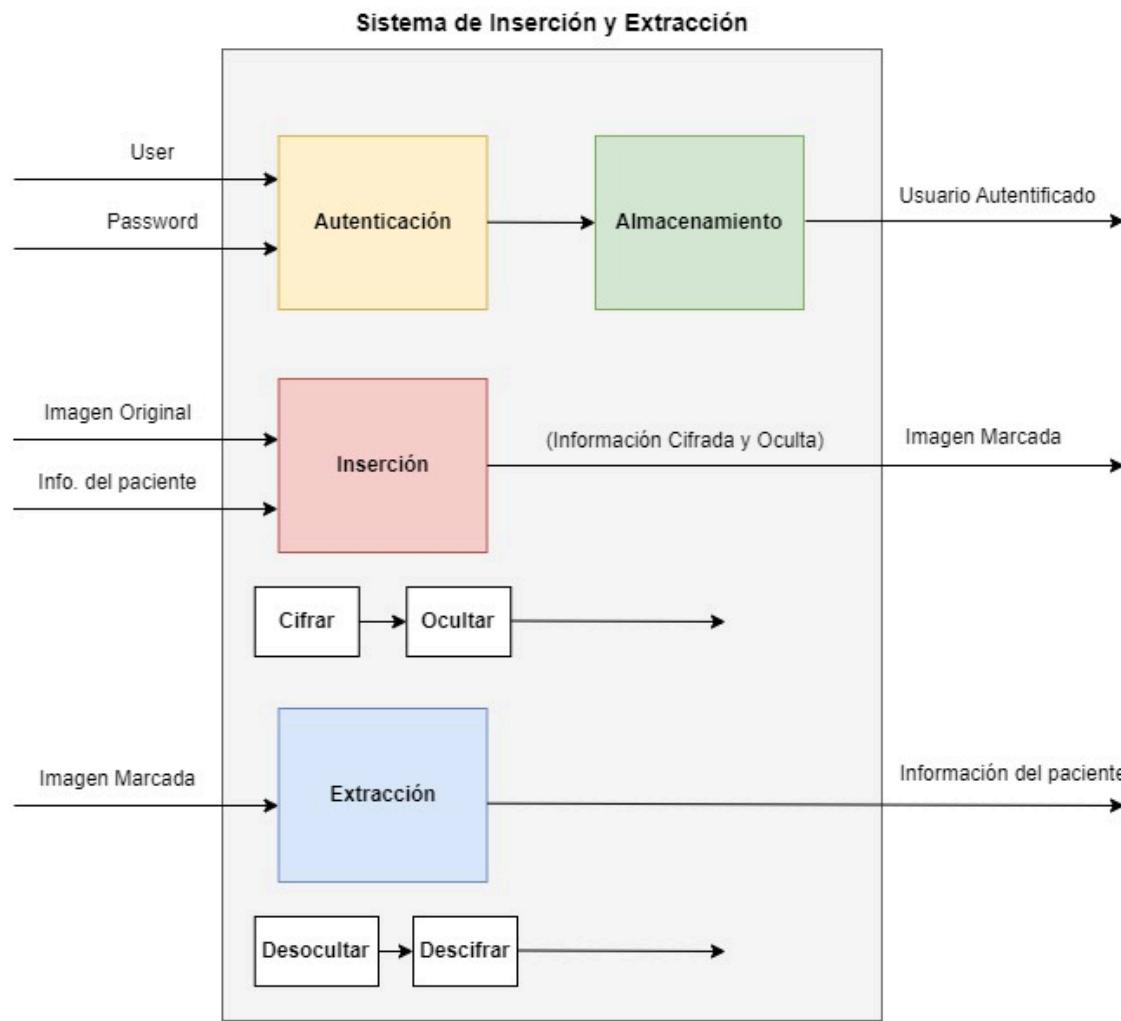


Figura 14: Diagrama de bloques del sistema de seguridad

## 5.3. Proceso de Autenticación

En primer lugar se tiene un registro para los Médicos que la utilizarán el sistema de seguridad. En la caso del Médico Radiólogo, este será el que se encargará de Insertar la Marca de Agua, por otra parte, en el caso del Médico Especialista, este se encargará de Extraer dicha Marca de la imagen.

Posteriormente una vez creado el perfil, el Médico podrá ingresar al sistema de seguridad.

## 5.4. Proceso de Almacenamiento

En este etapa lo que se hace es, subir tanto el usuario, así como la contraseña a una base de datos, esto lo realizará el sistema en el momento en que los médicos se registren por primera vez. La elección de una base de datos siempre depende de las necesidades específicas del proyecto. En este caso, el gestor de Base de datos será Firebase, ya que posee robustez y confiabilidad. Además cuanta con herramientas de administración que permiten facilitar tareas de configuración, monitoreo y respaldo.

## 5.5. Proceso de Inserción

Para insertar la marca de agua se deberán seguir los siguientes pasos que se muestran en el diagrama, esto para evitar errores al la hora del marcado. Es necesario que el Médico Radiólogo posea el sistema de seguridad en su dispositivo.

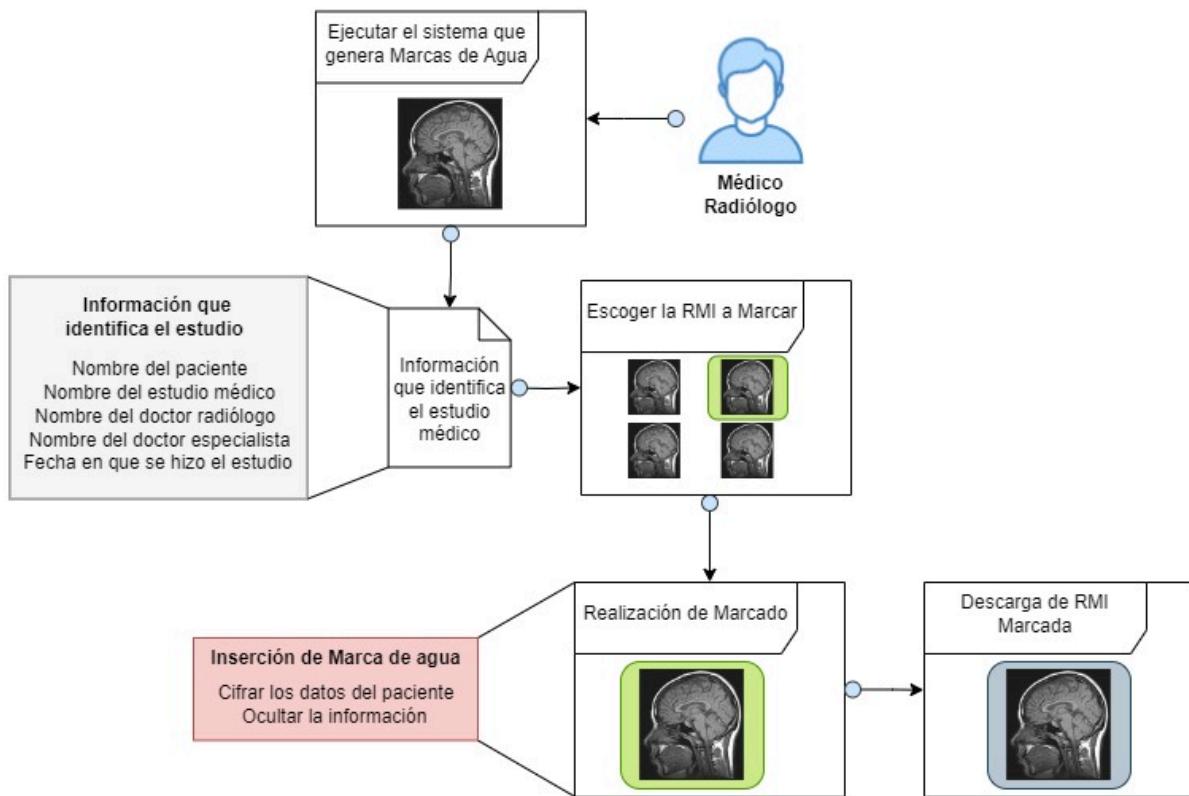


Figura 15: Diagrama del Proceso de Inserción de una Marca de Agua

Una vez que el Médico Radiólogo ejecute el sistema de seguridad en su dispositivo, deberá llenar el formulario que identifica el Estudio Médico, esta información será la que se encontrará oculta en la Imagen de Resonancia Magnética.

Posteriormente deberá escoger la Imagen que desea marcar. En este paso será en donde con ayuda de la técnica criptográfica de cifrado simétrico con el algoritmo AES, la

información confidencial del paciente quedará completamente ilegible.

Una vez realizado este proceso, haciendo uso de bit menos significativo se podrá ocultar esta información en la RMI.

A continuación el sistema procederá a descargar la Imagen de Resonancia Magnética Marcada automáticamente en el dispositivo.

## 5.6. Proceso de Extracción

Para realizar la extracción de la marca de agua se deberán seguir los siguientes pasos que se muestran en el diagrama, esto para evitar errores al la hora de la extracción. Es necesario que el Médico Especialista posea el sistema de seguridad en su dispositivo.

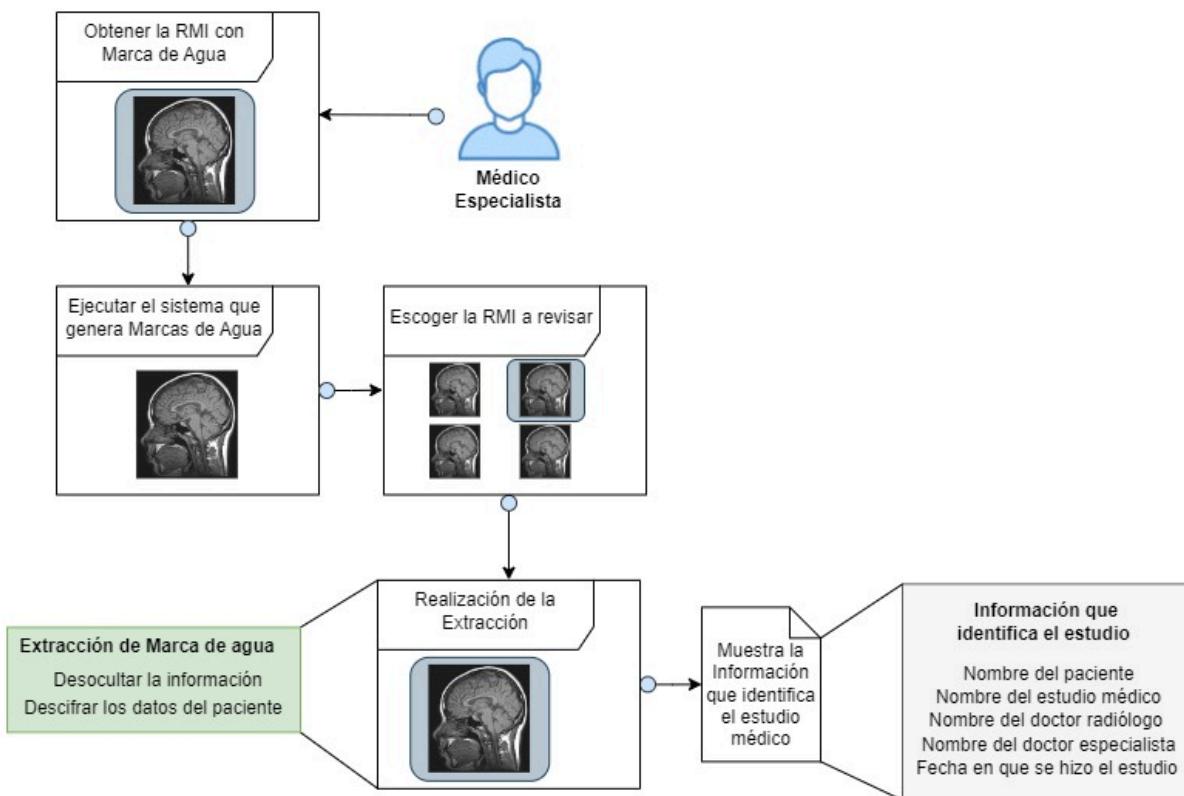


Figura 16: Diagrama del Proceso de Extracción de una Marca de Agua

Una vez que el Médico Especialista tenga una Imagen de Resonancia Magnética marcada y desee visualizar la información confidencial oculta deberá ejecutar el sistema de seguridad en su dispositivo. Hecho esto, seleccionará la RMI a descifrar.

A continuación lo que sucederá es que el sistema realizará la extracción, esto será utilizando la llave que se generó al momento de realizar la Inserción de la Marca de Agua. Una vez hecho esto, entonces finalmente se descifrarán los datos confidenciales del paciente y se mostrarán en el sistema.

### 5.7. Cifrado de la información

Esta etapa toma lugar como primer paso cuando el Médico Radiólogo va a insertar la marca de agua en la Imagen de Resonancia Magnética, como se menciona en la sección 4.4 Técnica criptográfica, la que se utilizará en el proyecto será una técnica simétrica que se explica en los siguientes diagramas, tanto el cifrado como el descifrado de la información del paciente.



Figura 17: Cifrado de la información

Quien estará a cargo del cifrado es el Médico Radiólogo al momento de que se este insertando la marca de agua. La información debe estar cifrada ya que esto ayudará a prevenir que alguna persona pueda leer la información en caso de que se logre extraer la marca, puesto si esto llegará a pasar, no podría descifrar la información sin la clave.



Figura 18: Descifrado de la información

En el descifrado se obtendrá primero la RMI con la marca de agua, después haciendo uso de la cadena cifrada el médico Especialista logrará obtener la información ya descifrada y de este modo, podrá ser visualizada la información del estudio médico por él.

En la sección 4.5 Algoritmo de cifrado, se menciona el algoritmo AES como la herramienta a utilizar en la etapa de criptografía, específicamente se usará AES-128, de forma que los procesos de cifrado del algoritmo pueden resumirse en los siguientes pasos [29]:

#### **1. División y expansión**

El método de cifrado comienza dividiendo el texto sin formato del mensaje que se desea enviar en bloques de bits, o filas, que luego se expanden mediante el programa de claves de AES. El proceso también añade una clave de cifrado -llamada ‘round key’- durante este paso.

#### **2. Sustitución**

Durante la sustitución, el método reemplaza el texto sin formato por el texto cifrado, que se basa en una tabla preestablecida llamada Rijndael S-box.

#### **3. Desplazamiento**

A continuación, todas las filas del texto recién encriptado se desplazan una posición, excepto la primera fila.

#### **4. Mezcla**

Las filas cifradas y desplazadas se vuelven a mezclar. Esto impide que un usuario no autorizado o un pirata informático pueda simplemente desplazar las filas a su posición original para recuperar el contenido.

#### **5. Round Key**

Utilizando la Round Key generada en el primer paso, se vuelve a cifrar la información.

#### **6. Repetir**

Este proceso se repite un número determinado de veces en función del tipo de AES, en el caso de AES-128 son 9 veces.

A continuación se muestra un diagrama de flujo para explicar de mejor manera el funcionamiento de AES-128 y los procesos que lleva a cabo.

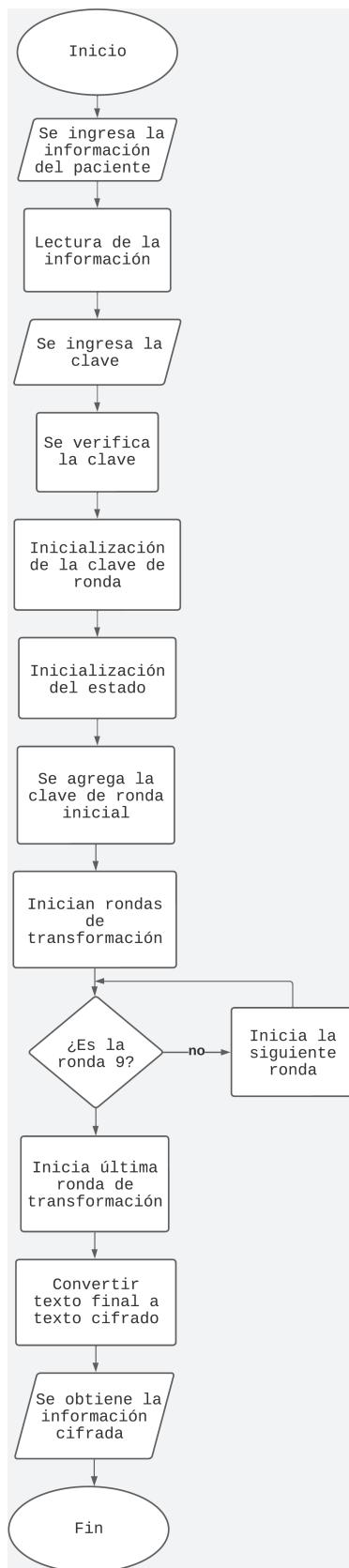


Figura 19: Diagrama de Flujo AES-128

Para explicar de manera más clara el diagrama de flujo, se en listan las características principales de cada acción que se realiza:

- Las entradas con las que funciona el algoritmo son la información y la clave.
- En la inicialización de la clave de ronda se utiliza una función que toma como parámetro la clave y crea un conjunto de claves de ronda, en este caso 9, cada clave de ronda se deriva de la anterior mediante operaciones de rotación y sustitución de bytes.
- Cuando se inicializa el estado, se convierte el texto plano de la información a una matriz de estado de 4x4, donde cada byte representa un elemento de la matriz.
- Al agregar la clave de ronda inicial, cada byte del estado se combina mediante una operación XOR con la clave de ronda inicial.
- Se inician las rondas de transformación y se repite el proceso durante 8 rondas, donde se utilizan 4 funciones principales. La primera para realizar la sustitución de los bytes usando una tabla. La segunda desplaza los bytes de cada fila de la matriz hacia la izquierda, la primera fila no se desplaza, la segunda se desplaza una posición, la tercera dos posiciones y la cuarta tres posiciones. La tercer función se encarga de hacer una operación de mezcla en cada columna de la matriz. Y por último, la cuarta función se encarga de combinar la clave de ronda con el estado de la matriz.
- Cuando se realiza la novena ronda, se sigue el mismo proceso de las demás rondas pero sin tomar en cuenta la tercer función para la operación de mezcla para las columnas.
- Como resultado se obtiene un texto en formato legible pero que no es entendible.

## 5.8. Ocultamiento de la información

En la sección 4.6 Técnica esteganográfica, se realizó la selección de la técnica a utilizar después del análisis y comparación de los distintos tipos que existen. Esta elección fue una técnica que se pudiera emplear en el dominio espacial, ya que por los requerimientos del sistema sería la que se podría utilizar de mejor forma.

El nombre de la técnica es el algoritmo del Bit Menos Significativo (BMS), uno de los algoritmos más utilizados en la esteganografía. Este algoritmo tiene como objetivo ocultar un mensaje dentro de los componentes de color de una imagen.

Los pasos que sigue este algoritmo se muestran en el siguiente diagrama de flujo.

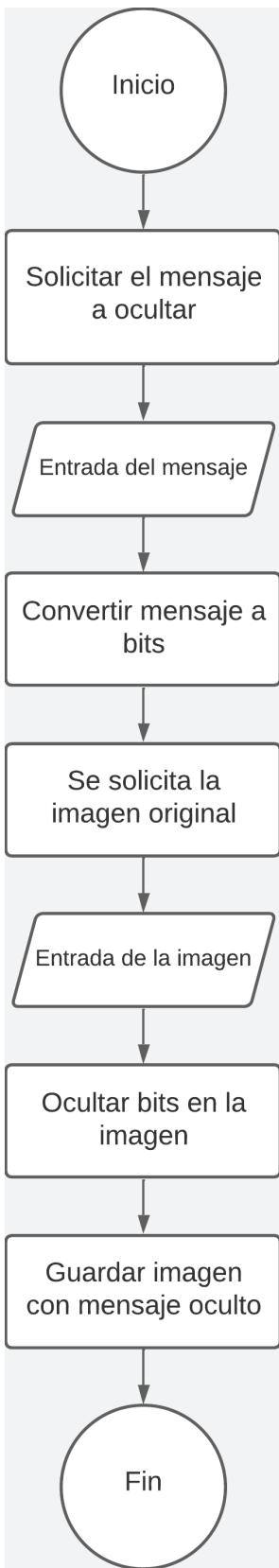


Figura 20: Diagrama de Flujo algoritmo Bit Menos Significativo

Explicando el diagrama, primero se debe tener el mensaje que se quiere ocultar, para este punto, el sistema tendrá como mensaje el texto cifrado con la información del paciente, además se requiere la Imagen de Resonancia Magnética.

El mensaje a ocultar pasa por un proceso para convertirlo a bits, convirtiendo cada carácter del mensaje a su representación en binario, obteniendo una secuencia de bits.

Teniendo cargada la imagen y la secuencia de bits del mensaje, se utilizará una función para ocultar el mensaje en la imagen, la cual tendrá como parámetros esos dos elementos. Esa función recorre cada píxel de la imagen y en cada componente de color, recordando que se tienen 3 componentes: rojo, verde y azul, se reemplazará el bit menos significativo con el siguiente bit del mensaje. El proceso se repite en cada componente y en cada píxel, ocultando gradualmente los bits del mensaje en la imagen.

El resultado es una imagen que visualmente es similar a la original, pero que contiene información adicional oculta en sus píxeles.



## INSERCIÓN DE MARCAS DE AGUA OCULTAS Y CIFRADAS EN IMÁGENES DE RESONANCIA MAGNÉTICA APLICADAS EN DISPOSITIVOS IoT

DESARROLLO E  
IMPLEMENTACIÓN

## 6. DESARROLLO E IMPLEMENTACIÓN

### 6.1. Inicio de Sesión

Para comenzar con el desarrollo del sistema, lo primero que hizo fue diseñar todo el ambiente gráfico para de esta forma posteriormente implementar todos los algoritmos necesarios para cifrar, ocultar e insertar la marca de agua.

Para el sistema de marcado es importante tener un control de quienes pueden acceder y hacer uso de él, es por ello que fue necesario implementar un inicio de sesión, donde el médico se deberá registrar para poder tener acceso al sistema. Una vez registrado ya podrá ingresar a la interfaz. En la siguiente imagen se muestra el primer menú para Iniciar Sesión que fue desarrollado.



Figura 21: Menú de Inicio de Sesión

Para el Front-end del Inicio de Sesión se desarrolló el siguiente diagrama que define la ventana y todos los elementos funcionales para el formulario y los botones.

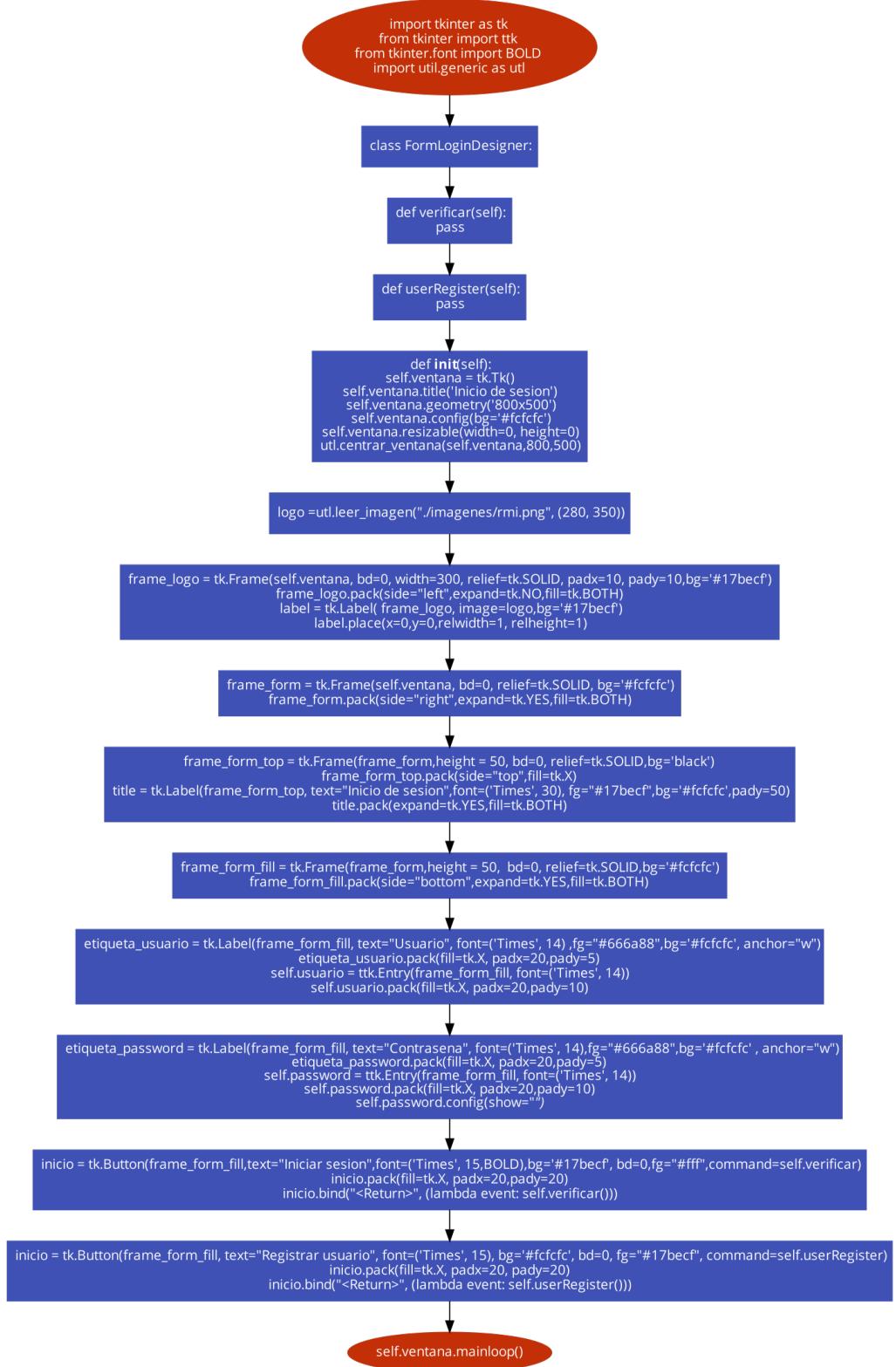


Figura 22: Diagrama de Flujo de Inicio de Sesión (Front-end)

Para el Back-end del Inicio de Sesión se implementaron 3 funciones principales. La primera se encarga de verificar el nombre del usuario en la base datos que se utiliza, la segunda función se usa para determinar si el médico está registrado o no, en caso de que no, solicitará que se registre. La última función determina si la contraseña ingresada coincide con la contraseña registrada en la base de datos.

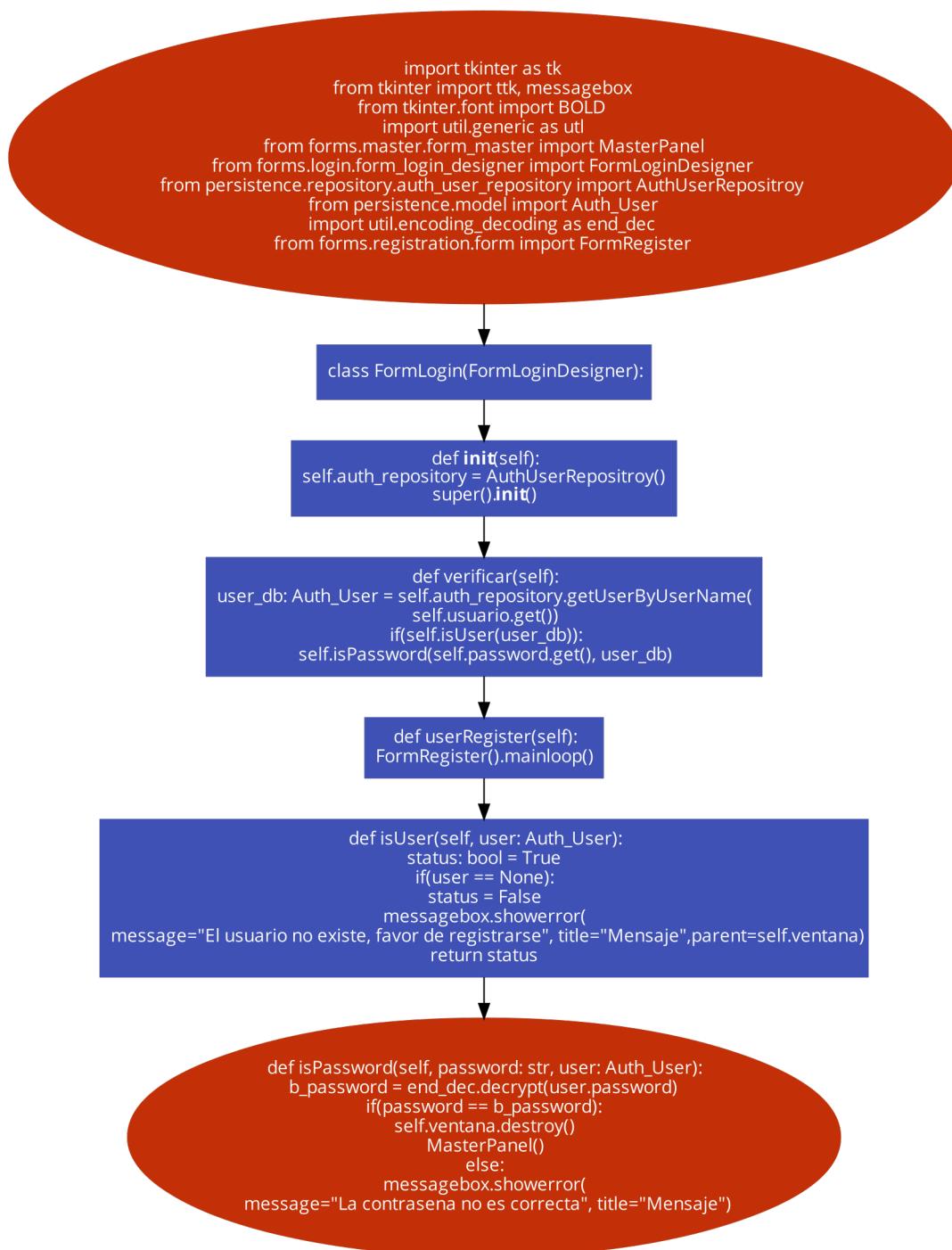


Figura 23: Diagrama de Flujo de Inicio de Sesión (Back-end)

## 6.2. Registro de Usuario

El botón de Registrar Usuario tiene la función de abrir un nuevo menú en el cual el médico dará de alta su nombre de usuario y su contraseña para poder ingresar al sistema, dicho menú se muestra en la siguiente imagen.

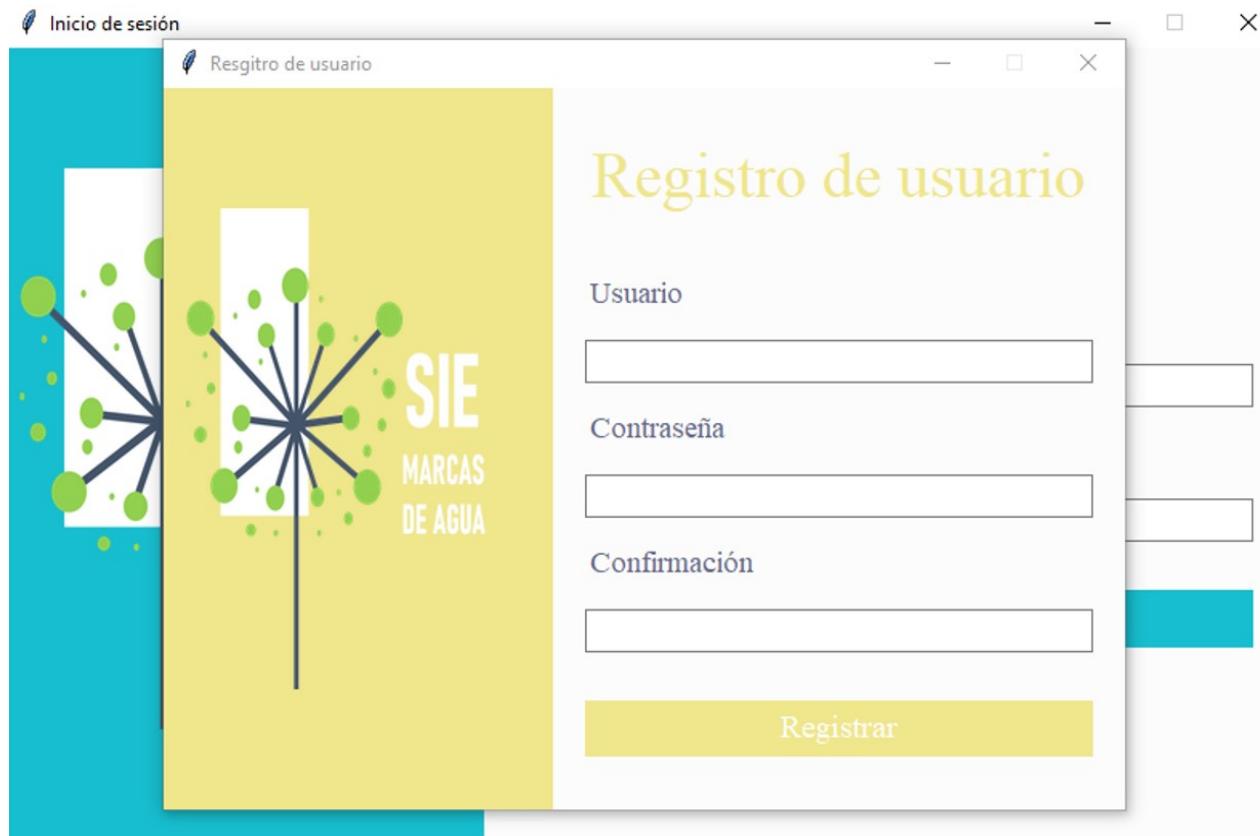


Figura 24: Menú de Registro de usuario

Para esta ventana de igual forma se desarrollaron 2 códigos, el primero para el Front-end y el segundo para el Back-end. El código del Front despliega la ventana con todos los elementos necesarios para realizar el registro. A continuación se presenta el diagrama de flujo de dichos códigos.

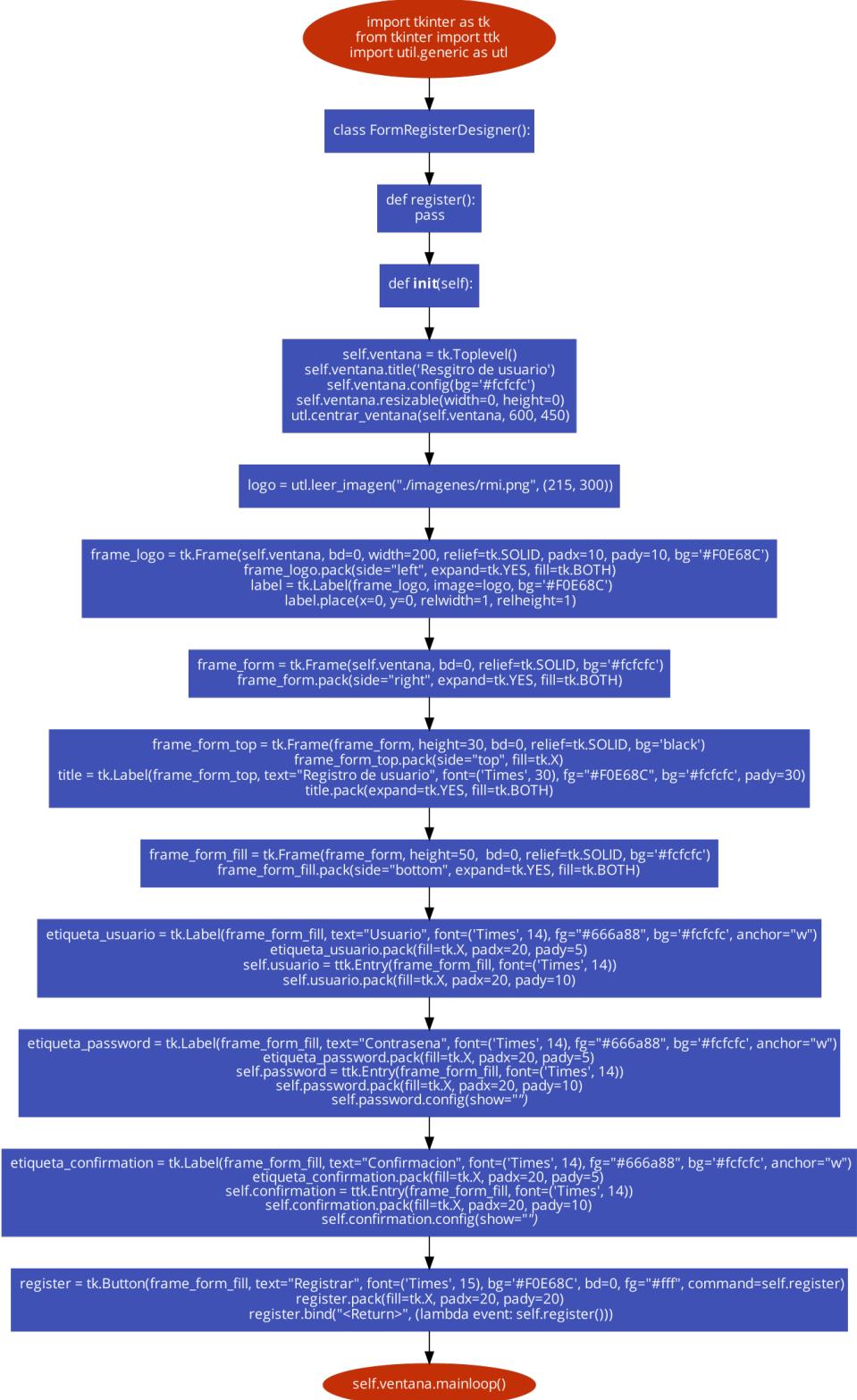


Figura 25: Diagrama de Flujo del Registro de Usuario (Front-end)

Respecto al Back-end se tienen 3 funciones, una para verificar si el usuario ya existe o no en el sistema, la segunda para confirmar que la contraseña y la confirmación coinciden y la última hace uso de las dos anteriores para poder registrar al usuario de manera satisfactoria.

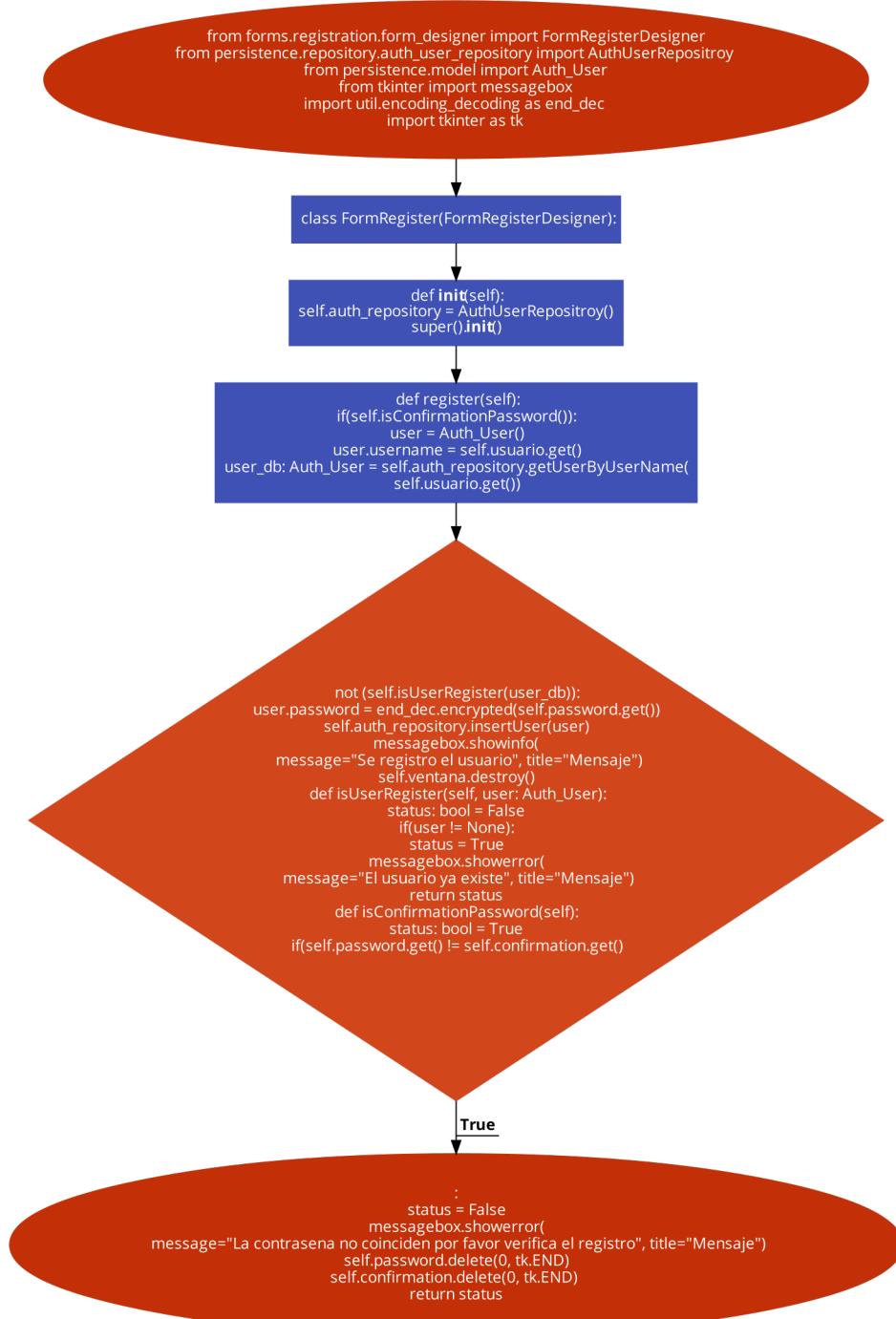


Figura 26: Diagrama de Flujo del Registro de Usuario (Back-end)

### 6.2.1. Almacenamiento de Registros de Usuario

Se implementó el uso de una plataforma llamada Firebase de Google, la cuál brinda distintos servicios, el que fue seleccionado para el proyecto se conoce como Realtime Database que nos permite vincular la base de datos al sistema. De esta manera el médico puede ingresar desde cualquier equipo de cómputo que esté ejecutando el sistema de marcación. Cabe mencionar que la base de datos es del tipo no relacional, lo que permite trabajar con estructuras del tipo json. Para la conexión es importante instalar una librería llamada firebase admin y generar una llave privada en el proyecto en la plataforma de Firebase que da como resultado un archivo .json que debe estar incluido en el proyecto para poder acceder a la base de datos. Se utilizan dos comandos para enlazarse a la base de datos y uno más para inicializarla. El código usado para la conexión es el siguiente:

```

1 import firebase_admin
2 from firebase_admin import credentials
3 from firebase_admin import db
4
5 cred = credentials.Certificate("/sie/db.json")
6 firebase_admin.initialize_app(cred, {
7     'databaseURL' : 'https://credenciales-3ceef-default.firebaseio.
com/' })
8 def initializationBD():
9     ref = db.reference('/Credenciales')
10    return ref

```

Al registrarse un nuevo usuario se realiza la inserción tanto del usuario como la contraseña que está cifrada para contar con mayor seguridad en la BD. Cuando el usuario ingrese sesión se hace una consulta por su nombre y se descifra la contraseña almacenada para comprobar que coincida con la ingresada. La BD se visualiza de la siguiente manera:

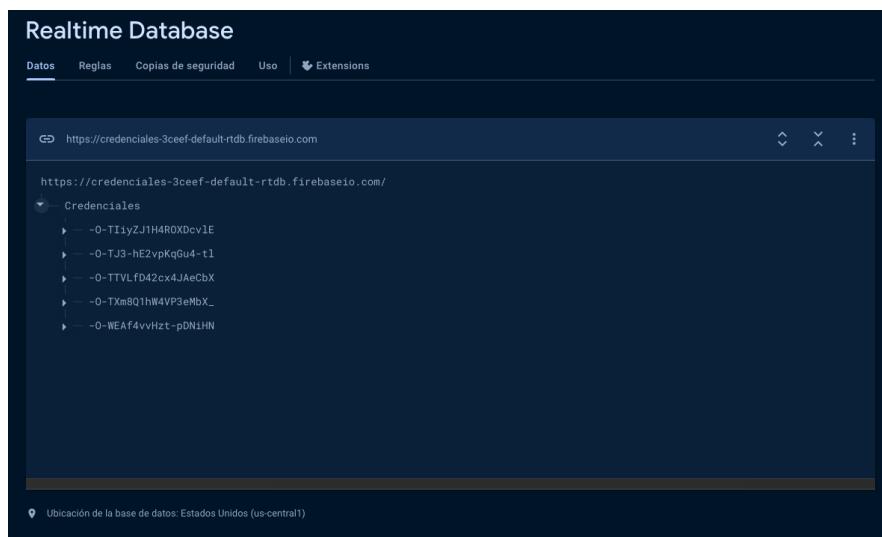


Figura 27: Vista general de la Base de Datos

Cada registro se guarda con un ID automático que al seleccionarlo muestra los datos del médico que son su usuario y la contraseña cifrada.

The screenshot shows the Firebase Realtime Database interface. The database URL is https://credenciales-3ceef-default-rtdb.firebaseio.com/. The main structure is 'Credenciales', which contains three child nodes: '-0-TIiyZJ1H4ROXcv1E', '-0-TJ3-hE2vpKqGu4-t1', and '-0-TIVLfd42c4JaEcBX'. Each node has a 'Clave' field containing an encrypted string and a 'Usuario' field containing the user's name. The names listed are 'Miguel Valenzuela', 'Daniel Reyes', and 'Ana Juarez' respectively. At the bottom left, it says 'Ubicación de la base de datos: Estados Unidos (us-central1)'.

Figura 28: Visualización de los registros

### 6.3. Selección de Perfil Médico

Una vez que el médico accede al sistema, se le presentará un menú en el que seleccionará si es radiólogo o especialista. El desarrollo de este menú únicamente utiliza un código para el Front-end que despliega el menú.



Figura 29: Menú para Seleccionar Perfil médico

El siguiente diagrama se realizo en base al código en donde se muestran dos botones para los perfiles de los médicos que al presionarlos se desplegará una nueva ventana: la de Insertar la marca en caso de que sea Médico Radiólogo y la de Extraer la marca si es un Médico Especialista.

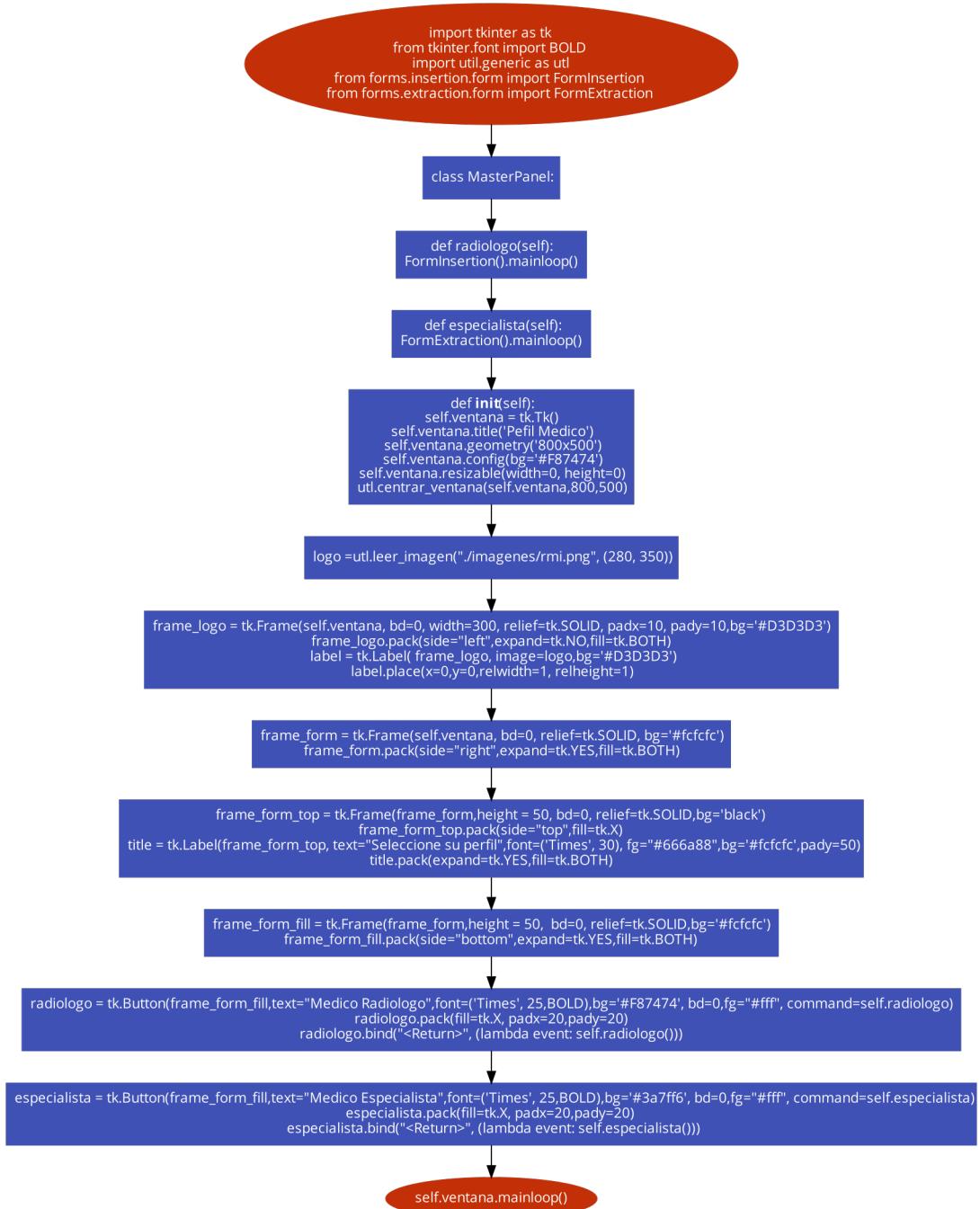


Figura 30: Diagrama de Flujo del Menú para Seleccionar Perfil médico

## 6.4. Inserción de Marca de Agua

El formulario para la Inserción de la marca se desarrolló con dos códigos en dónde ya se implementan los algoritmos tanto para el cifrado como el esteganográfico.

En el primer código se define la ventana y todos los elementos del formulario y botones, además se implementa la función para abrir la imagen a marcar así como la función que implementa el algoritmo esteganográfico. Esta última se utiliza una vez que la función del cifrado tenga la cadena encriptada del formulario llenado por el médico radiólogo. Por último se utiliza una función para subir los datos necesarios para el descifrado a la BD.

La función mencionada donde se implementa la técnica esteganográfica funciona de la siguiente manera: primero abre la imagen y verifica que tenga un modo RGB, en caso de que no, la convierte a RGB esto porque se tiene que poder insertar los bits en los 3 canales de color. Lo siguiente es realizar operaciones binarias para poder transformar el texto cifrado a una cadena binaria. Por último se realiza una iteración en la imagen insertando bit por bit para ocultar los datos, una vez terminado se guarda la imagen marcada.

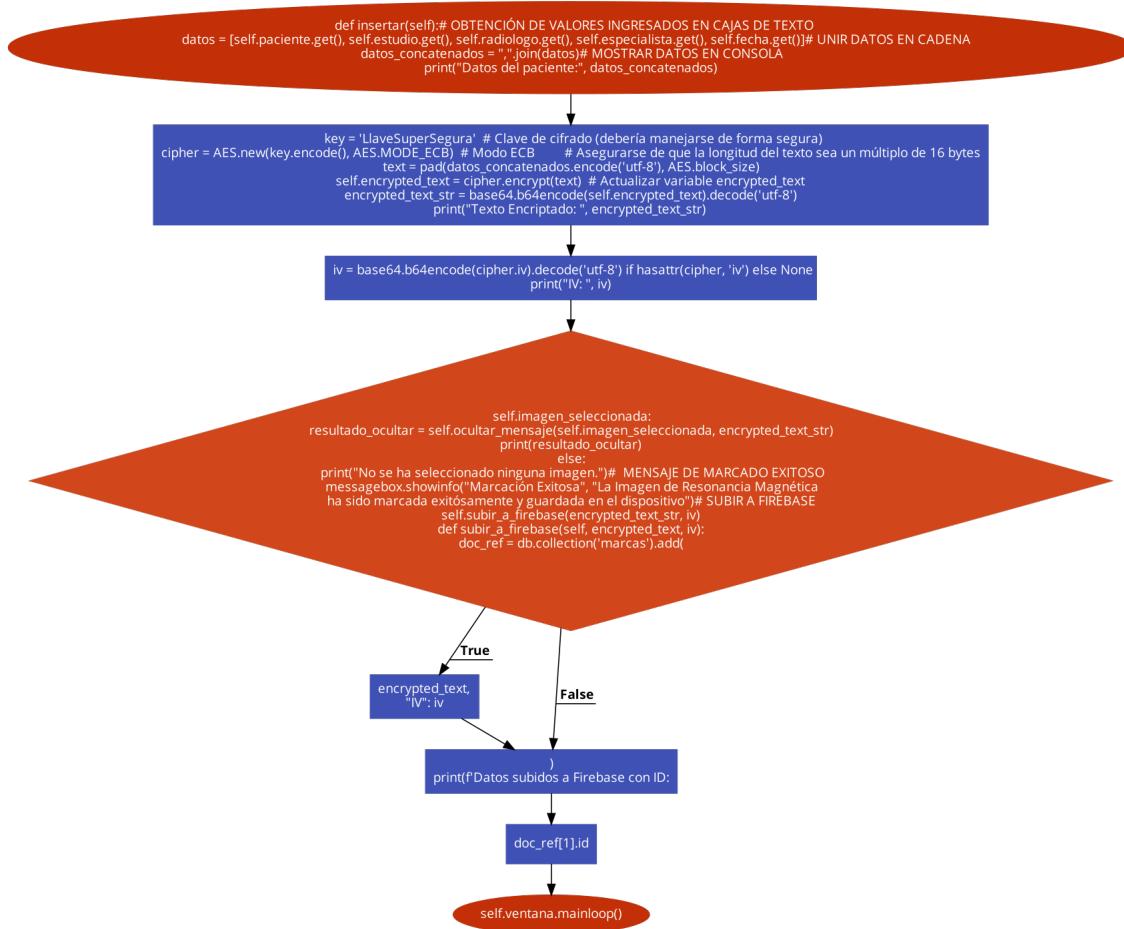


Figura 31: Diagrama de Flujo del algoritmo Criptográfico y Esteganográfico

Para la implementación del algoritmo de cifrado se desarrolló una función que primero obtiene los datos ingresados en los campos del formulario para concatenarlos, después haciendo uso de la librería crypto de Python y las funciones que tiene para trabajar con AES se implementa el cifrado y por último se utiliza la función anterior esteganográfica para insertar la marca.



Figura 32: Formulario para Insertar la marca de agua

El segundo código usado únicamente inicializa todo para poder mostrarse e implementa la función para poder abrir la imagen que se va a marcar.

```

1 class FormInsertion(FormInsertionDesigner):
2
3     def __init__(self):
4         super().__init__()
5
6     def abrirImagen(self):
7         ruta_imagen = filedialog.askopenfilename(filetypes=[("Imagen PNG",
8             ".*.png")])
9         if ruta_imagen:
10             self.imagen_seleccionada = ruta_imagen
11             self.etiqueta_archivo_png.delete(0, tk.END)
12             self.etiqueta_archivo_png.insert(0, ruta_imagen.split('/')[-1])
13             self.ventana.mainloop()

```

Finalmente para la etapa de Inserción se muestra una ventana emergente que nos dice que la RMI se guardó de manera automática en el dispositivo.



Figura 33: Mensaje de Marcación Exitosa

## 6.5. Extracción de Marca de Agua

El último formulario es para extraer la marca, este menú se muestra cuando el Médico Especialista presiona ese botón. El formulario se muestra de la siguiente manera:



Figura 34: Menú para Extraer la marca de agua

El siguiente código desarrollado es el que permite Extraer la marca de agua y por lo tanto los datos registrados en la imagen, consta de una función para inicializar el ambiente gráfico así como las declaraciones de los elementos que son los botones y cajas de texto. Además se desarrollaron cinco funciones para realizar la extracción y descifrado de la marca.

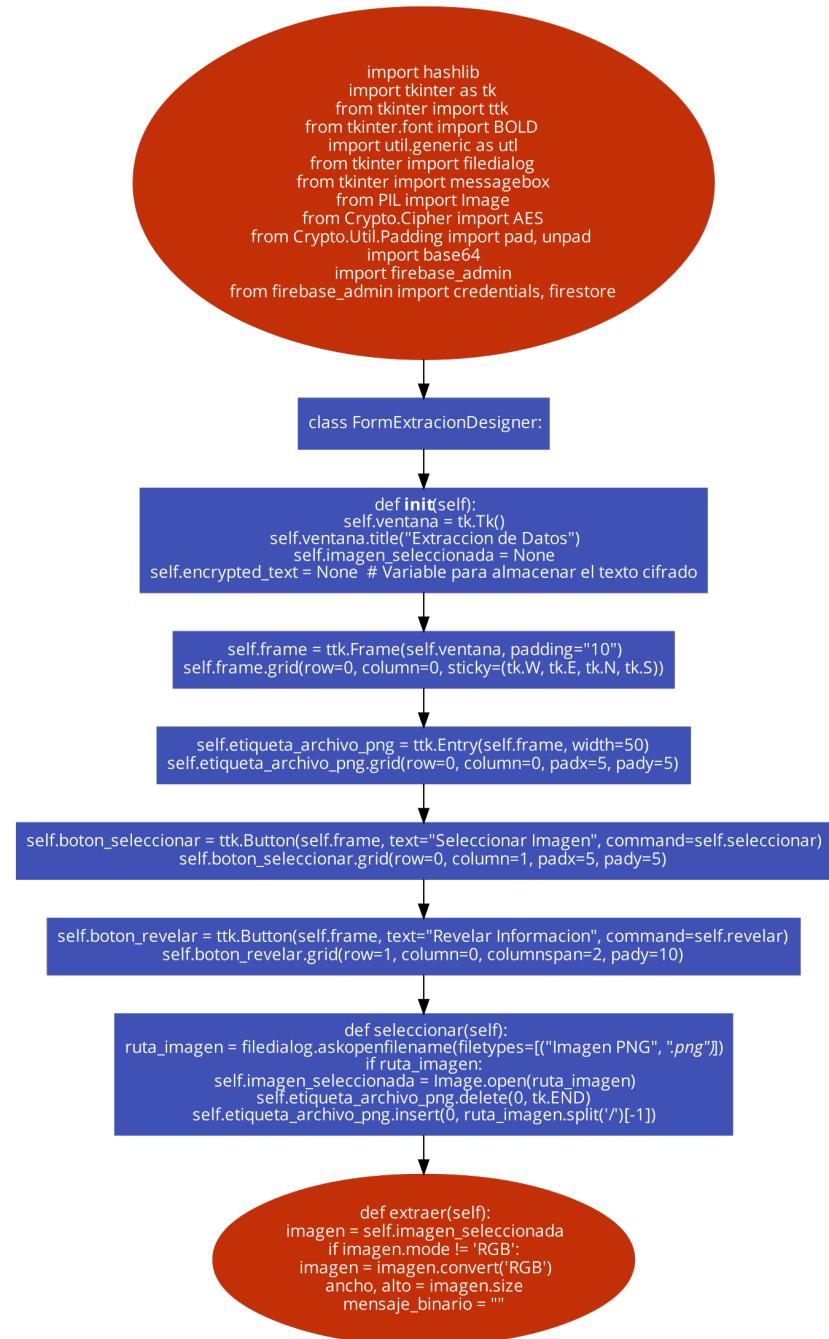


Figura 35: Diagrama de Flujo del proceso de Extracción

La primera función permite al médico seleccionar la imagen ya marcada almacenada en su equipo de computo y mostrar el nombre en el menú.

```

1     def seleccionar(self):
2         ruta_imagen = filedialog.askopenfilename(filetypes=[("Imagen PNG",
3             ".*.png")])
4         if ruta_imagen:
5             self.imagen_seleccionada = Image.open(ruta_imagen)
6             self.etiqueta_archivo_png.delete(0, tk.END)
7             self.etiqueta_archivo_png.insert(0, ruta_imagen.split('/')[-1])

```

Una vez seleccionada la imagen es posible extraer la marca de agua insertada realizando el proceso inverso de cuando se insertó, iterando en los tres canales de color para obtener los bits y después concatenarlos en grupos de 8 para poder pasarlo a una cadena de caracteres. La siguiente función revela la marca y la muestra en el menú.

```

1     def extraer(self):
2         imagen = self.imagen_seleccionada
3         if imagen.mode != 'RGB':
4             imagen = imagen.convert('RGB')
5         ancho, alto = imagen.size
6         mensaje_binario = ""
7
8         for y in range(alto):
9             for x in range(ancho):
10                pixel = imagen.getpixel((x, y))
11                for i in range(3): # Iterar sobre los tres
12                    canales de color RGB
13                    mensaje_binario += str(pixel[i] & 1)
14
15        # Buscar el marcador de fin de mensaje
16        fin_mensaje = mensaje_binario.find('1111111111111110')
17        if fin_mensaje != -1:
18            mensaje_binario = mensaje_binario[:fin_mensaje]
19
20        caracteres = []
21        for i in range(0, len(mensaje_binario), 8):
22            byte = mensaje_binario[i:i+8]
23            if len(byte) == 8:
24                caracteres.append(chr(int(byte, 2)))
25        self.encrypted_text = ''.join(caracteres)
26        self.encrypted_text_entry.insert(0, self.encrypted_text)

```

Antes de poder descifrar la marca fue necesaria una función para definir la forma en que se van a mostrar los datos.

Por último en cuestión de seguridad, la siguiente función implementa el algoritmo de descifrado AES usando la marca que ya fue extraída previamente.

```

1     def decrypt(self, encrypted_text):
2         print("Encrypted text for decryption: ", encrypted_text)
3         key = 'LlaveSuperSegura'
4         # Decodificar el texto cifrado de base64
5         encrypted_text = base64.b64decode(encrypted_text)
6         cipher = AES.new(key.encode(), AES.MODE_ECB)
7         try:
8             # Descifrar el texto y deshacer el relleno
9             decrypted_text = unpad(cipher.decrypt(encrypted_text), AES.
10             block_size).decode('utf-8')
11            return decrypted_text
12        except Exception as e:
13            print("Error durante el descifrado:", e)
14            return None

```

Finalmente para la etapa de Extracción se muestra una ventana emergente que nos dice la información que identifica al paciente que se realizó la Imagen de Resonancia Magnética.

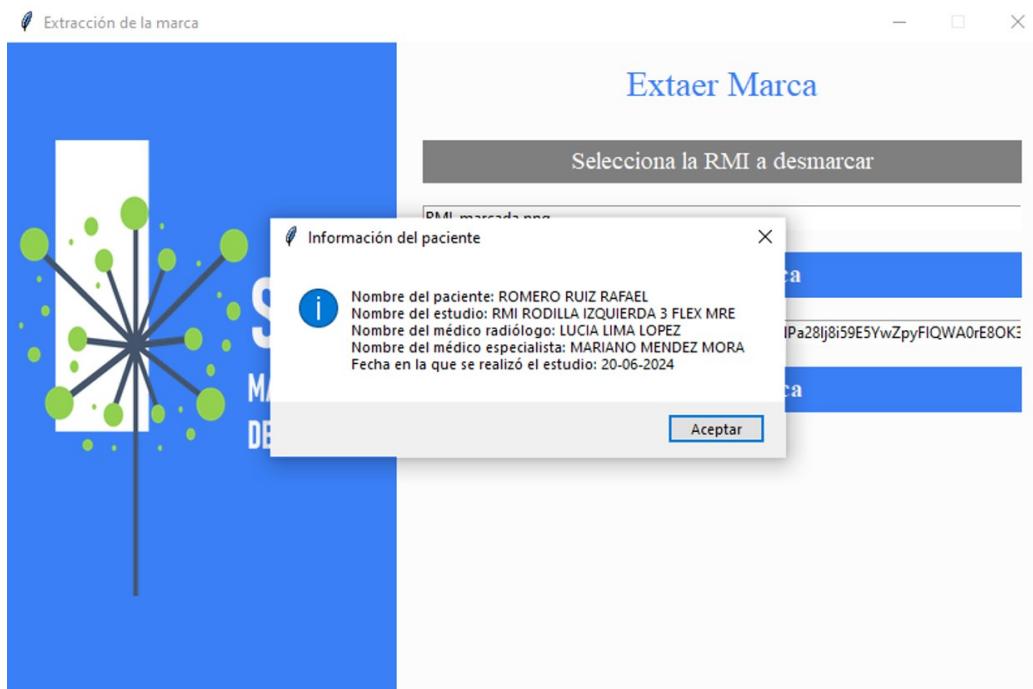


Figura 36: Información del paciente recuperada de la Marca de Agua

El resultado final del desarrollo del sistema e implementación de los algoritmos nos da como resultado una interfaz gráfica que puede ser utilizada en cualquier sistema operativo que tenga instalado Python, capaz de poner Insertar y Extraer marcas de agua invisibles que contengan información médica de un paciente que se realizó un estudio médico con Imágenes de Resonancia Magnética.



## INSERCIÓN DE MARCAS DE AGUA OCULTAS Y CIFRADAS EN IMÁGENES DE RESONANCIA MAGNÉTICA APLICADAS EN DISPOSITIVOS IoT

### PRUEBAS Y RESULTADOS

## 7. PRUEBAS Y RESULTADOS

### 7.1. Pruebas de similitud entre RMI's originales y marcadas

En este capítulo, se presentan las pruebas y resultados realizados utilizando el sistema de marcado que se desarrolló para este proyecto.

Se tomaron como prueba Imágenes de Resonancia Magnética de diferentes partes del cuerpo, como los son el cerebro, el pecho, el hombro, la rodilla, a continuación se muestran algunas imágenes utilizadas.

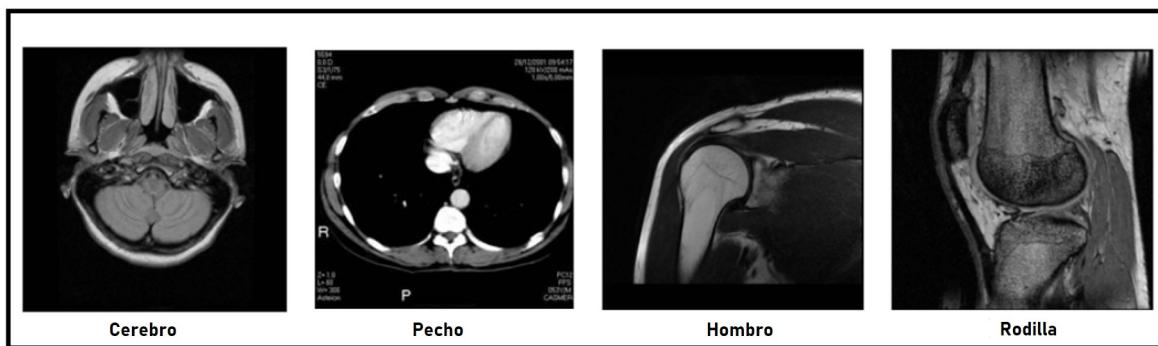


Figura 37: Imágenes de Resonancia Magnéticas de diferentes partes del cuerpo

Las marcas de agua, como se mencionó en el capítulo de Análisis, se trabajaron en el dominio espacial, específicamente con la técnica LSB (acrónimo en inglés de Least Significant Bit) en la cual la marca de agua es insertada en el bit menos significativo de algunos píxeles seleccionados.

Las imágenes utilizadas tienen las siguientes características:

- Formato de imagen: PNG
- Resolución: 128x128 px
- Tamaño del archivo: 3.5 kB - 8 kB.

Para realizar las pruebas de similitud entre la RMI original y la RMI marcada se utilizó el mapa de Similitud Estructural (SSIM) que proporciona una representación visual de las diferencias locales en la similitud estructural entre las imágenes que se están comparando.

Se desarollo un código en python para obtener dicho mapa y su valor promedio en las imágenes.

```
1 import matplotlib.pyplot as plt
2 from skimage import io, color
3 from skimage.metrics import structural_similarity as ssim
4
5 # Cargar las imágenes
6 imagen1 = io.imread('RMI3_o.jpeg')
7 imagen2 = io.imread('RMI_marcada_1.png')
8
9 # Convertir las imágenes a escala de grises si son de color
10 if imagen1.ndim == 3:
11     imagen1 = color.rgb2gray(imagen1)
12
13 if imagen2.ndim == 3:
14     imagen2 = color.rgb2gray(imagen2)
15
16 # Asegurarse de que las imágenes tengan el mismo tamaño
17 if imagen1.shape != imagen2.shape:
18     raise ValueError('Las imágenes deben tener el mismo tamaño.')
19
20 # Determinar el rango de datos
21 data_range = imagen1.max() - imagen1.min()
22
23 # Calcular el índice de similitud estructural (SSIM)
24 ssimval, ssimmap = ssim(imagen1, imagen2, data_range=data_range, full=True)
25
26 # Mostrar el valor de SSIM
27 print(f'El valor de SSIM es: {ssimval:.4f}')
28
29 # Mostrar las imágenes y el mapa de similitud
30 fig, axes = plt.subplots(1, 3, figsize=(10, 4))
31 ax = axes.ravel()
32
33 ax[0].imshow(imagen1, cmap='gray')
34 ax[0].set_title('Imagen original')
35
36 ax[1].imshow(imagen2, cmap='gray')
37 ax[1].set_title('Imagen marcada')
38
39 ax[2].imshow(ssimmap, cmap='jet')
40 ax[2].set_title(f'Mapa SSIM\n SSIM = {ssimval:.4f}')
41 plt.colorbar(ax[2].imshow(ssimmap, cmap='jet'), ax=ax[2])
42
43 for a in ax:
44     a.axis('off')
45
46 plt.tight_layout()
47 plt.show()
```

---

Se puede observar en las siguientes figuras que el mapa tiene un valor de 1 que es el más alto indicando que tienen un alta grado de similitud, aunque se aprecian distintas tonalidades un poco más bajas al color máximo eso no afecta la similitud de las imágenes y mucho menos la percepción que tiene el médico al observar el resultado de la RMI marcada.

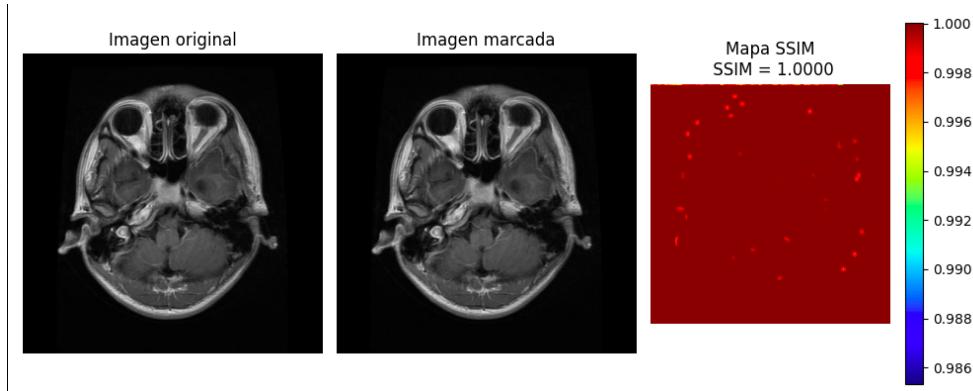


Figura 38: Prueba de similitud en RMI Enfermedad Alzheimer

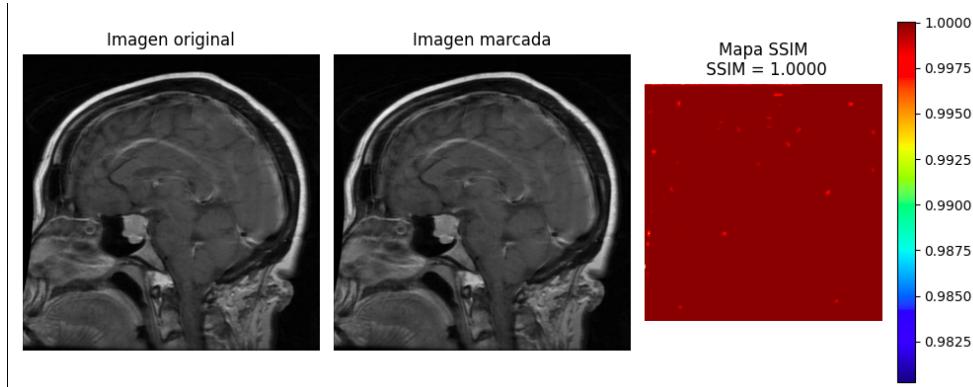


Figura 39: Prueba de similitud en RMI Demencia Moderada

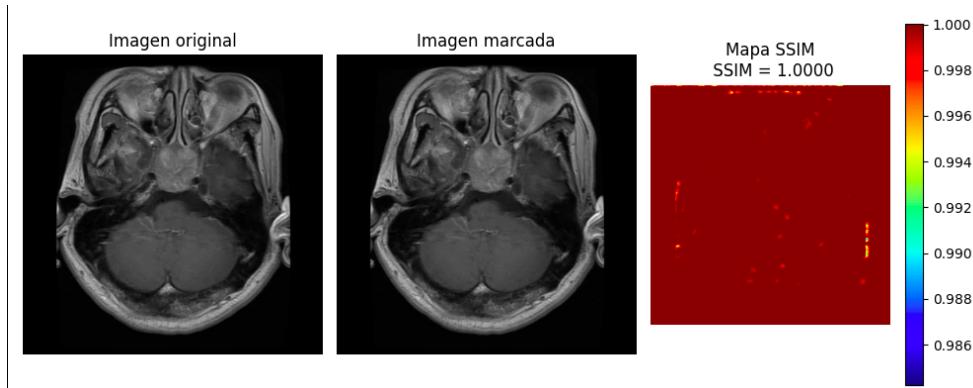


Figura 40: Prueba de similitud en RMI Tumor cerebral

## 7.2. Evaluación de resultados

Para la evaluación de los resultados se aplicaron métricas que permiten evaluar la calidad de una imagen que ha sido modificada con respecto a su estado original, PSNR (Peak Signal-to-Noise-Ratio) y MSE (Normalized Cross-Correlation), de esta manera es posible cuantificar la distorsión generada después de aplicar los algoritmos del sistema de marcado a la imagen.

$$MSE = \frac{1}{M N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (f(x, y) - f'(x, y))^2$$

Figura 41: MSE (Mean Square Error)

Donde M y N son las dimensiones de la imagen,  $f(x, y)$  y  $f'(x, y)$  representan la imagen original y la imagen marcada respectivamente. Esta métrica nos permite conocer la cantidad de degradación que fue introducida en la imagen marcada, valores cercanos a cero indican menor degradación.

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} dB$$

Figura 42: PSNR (Peak Signal-to-Noise-Ratio)

Para obtener la similitud entre la imagen original y la imagen marcada se utilizo la métrica NCC (Normalized Cross-Correlation).

$$NCC = \frac{\sum_{x=0}^{R-1} \sum_{y=0}^{C-1} W(x, y) \cdot W'(x, y)}{\sum_{x=0}^{R-1} \sum_{y=0}^{C-1} |W(x, y)|^2}$$

Figura 43: NCC (Normalized Cross-Correlation)

Donde R y C son las dimensiones de la marca insertada,  $W(x, y)$  y  $W'(x, y)$  representan la marca original y la marca extraída respectivamente. Los valores obtenidos al aplicar esta métrica se encuentran en el rango de 0 a 1, siendo el 0 las imágenes completamente diferentes y 1 las completamente similares.

Se realizaron múltiples pruebas variando el valor de los parámetros de la resolución y tamaño de los archivos. A continuación se presentan algunos ejemplos de imágenes marcadas, mostrando los valores obtenidos en términos de degradación y extracción de la marca insertada.

RMI	PSNR	MSE	NCC
Imagen Marcada 1	33.82	26.93	1.0000
Imagen Marcada 2	45.20	19.60	0.9918

Tabla 11: Resultados de imágenes marcadas. Parte del cuerpo: Cerebro

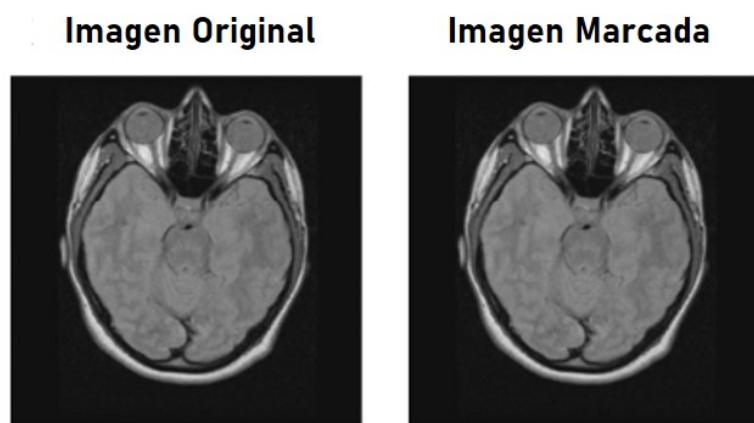


Figura 44: RMI Original vs RMI Marcada del cerebro

RMI	PSNR	MSE	NCC
Imagen Marcada 1	23.64	281.09	1.0000
Imagen Marcada 2	46.67	1.39	0.9554

Tabla 12: Resultados de imágenes marcadas. Parte del cuerpo: Pecho

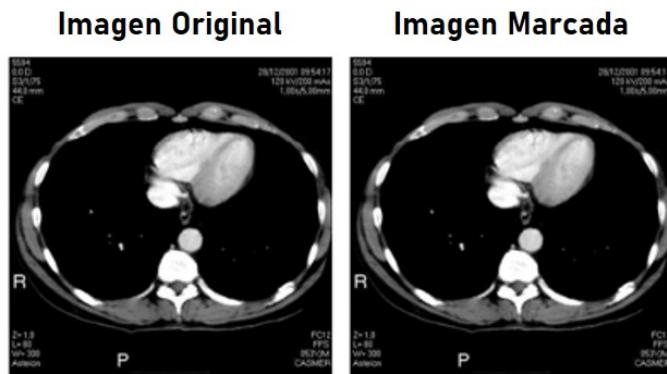


Figura 45: RMI Original vs RMI Marcada del pecho

RMI	PSNR	MSE	NCC
Imagen Marcada 1	21.94	415.50	1.0000
Imagen Marcada 2	36.00	16.32	0.9627

Tabla 13: Resultados de imágenes marcadas. Parte del cuerpo: Rodilla



Figura 46: RMI Original vs RMI Marcada de rodilla

Después de realizar las pruebas de similitud, se puede concluir que se obtuvieron resultados favorables con respecto a la cantidad de información recuperada en el proceso de extracción de la marca, obteniendo de un espacio muestral de 75 RMI's porcentajes de recuperación por arriba del 90%. Un punto a destacar es que si queremos recuperar completamente la información insertada, el sistema podrá recuperar la información siempre y cuando la imagen no sufra problemas de calidad robustos y siempre y cuando el tamaño de la imagen se mantenga.

Recordemos que el NCC (Normalized Cross-Correlation) es una métrica utilizada para evaluar la similitud entre dos imágenes, en este caso, la imagen original y la imagen marcada. El NCC mide cuán parecidas son dos imágenes al calcular la correlación entre ellas, normalizada para compensar por las diferencias en brillo y contraste.

### Interpretación de los Resultados de NCC:

**Valores cercanos a 1:** Indican una alta similitud entre la imagen original y la imagen marcada. Un valor de 1 significa que las imágenes son idénticas en términos de la correlación normalizada.

**Valores cercanos a 0:** Indican baja o ninguna similitud entre las imágenes, sugiriendo que las imágenes son muy diferentes.

**Valores negativos:** Son raros en el contexto de marcas de agua en imágenes, pero en general, indicarían una relación inversa, donde las áreas de alta intensidad en una imagen corresponden a áreas de baja intensidad en la otra.

En el documento proporcionado, los valores de NCC para las diferentes imágenes son los siguientes:

Cerebro:

Imagen Marcada 1: NCC = 1.0000

Imagen Marcada 2: NCC = 0.9918

Pecho:

Imagen Marcada 1: NCC = 1.0000

Imagen Marcada 2: NCC = 0.9554

Rodilla:

Imagen Marcada 1: NCC = 1.0000

Imagen Marcada 2: NCC = 0.9627

Estos valores indican que la mayoría de las imágenes marcadas tienen una alta similitud con sus respectivas imágenes originales. En particular, los valores de NCC igual a 1.0000 sugieren que las imágenes marcadas son casi idénticas a las originales, mientras que valores ligeramente menores, como 0.9918 o 0.9554, todavía indican una alta similitud pero con pequeñas diferencias perceptibles.

En resumen, el NCC es una herramienta útil para cuantificar la similitud entre imágenes, y los resultados obtenidos en el documento sugieren que las técnicas de marcado utilizadas introducen poca distorsión perceptible en las imágenes originales.



## INSERCIÓN DE MARCAS DE AGUA OCULTAS Y CIFRADAS EN IMÁGENES DE RESONANCIA MAGNÉTICA APLICADAS EN DISPOSITIVOS IoT

### CONCLUSIONES

## 8. CONCLUSIONES

La necesidad de utilizar marcas de agua en estudios digitales se debe a la creciente preocupación del aumento de falsificación o manipulación de información médica delicada.

En este trabajo de investigación se implementó un software para realizar marcas de agua aplicado en Imágenes de Resonancia Magnética, este sistema combina técnicas tanto ocultamiento de datos, así como técnicas de cifrado, esto para incrementar la seguridad en la información referente a pacientes y sus estudios médicos digitales.

Es importante mencionar que el sistema de seguridad propuesto tiene la finalidad de utilizarse como una herramienta que pueda ayudar a combatir y en su caso entorpecer, la proliferación de los delitos informáticos.

De acuerdo al desarrollo del proyecto, el sistema desarrollado logró integrar satisfactoriamente la técnica de esteganografía y criptografía para insertar marcas de agua ocultas en imágenes RMI, cumpliendo así con el objetivo general del proyecto, además cada uno de los objetivos específicos se alcanzó de manera exitosa, puesto se identificaron y seleccionaron las técnicas más adecuadas para la inserción de marcas de agua y el cifrado de información y se diseñó una interfaz accesible para el personal médico autorizado.

### **Impacto y Relevancia:**

La interfaz desarrollada facilitó el uso del sistema por parte del personal médico, permitiendo una inserción y extracción de marcas de agua de manera sencilla y segura.

La implementación de marcas de agua ocultas no afectó significativamente la calidad visual de las imágenes ni su interpretabilidad médica.

La implementación de este sistema ofrece una solución innovadora para mitigar los riesgos asociados a la manipulación y falsificación de imágenes médicas digitales, abordando una necesidad crítica en el ámbito de la salud. El uso de técnicas de esteganografía y criptografía en la protección de datos médicos representa un avance significativo en la seguridad de la información, proporcionando una herramienta valiosa para los profesionales de la salud.

### **Limitaciones:**

Aunque el sistema fue diseñado para imágenes en formato PNG, futuras investigaciones podrían expandir su aplicabilidad a otros formatos médicos como DICOM, ampliando su utilidad.

La incorporación de algoritmos más avanzados de detección de manipulación y autenticidad podría mejorar aún más la robustez del sistema.

En resumen, el proyecto logró cumplir con sus objetivos establecidos, demostrando la viabilidad y efectividad de la solución propuesta para proteger la autenticidad y confidencialidad de las imágenes RMI mediante el uso de marcas de agua ocultas y la técnica de cifrado. Este avance contribuye a la seguridad de los documentos digitales en el campo médico, ofreciendo un método confiable y accesible para el personal médico encargado de manejar información sensible.

Las marcas de agua en el contexto médico y conforme al planteamiento del problema, requieren de dos objetivos principales que se cumplieron en este proyecto: El primero es el ocultamiento de información, con el propósito de insertar la información que identifica un estudio médico digital. Y el segundo es tener el control de los médicos que se registran para saber quien entró al sistema.

Hasta el momento, no existe algún esquema o algoritmo que sea robusto ante todos los ataques posibles que pueden ser aplicados a una imagen, ya que cada uno de los algoritmos es diseñado dependiendo la aplicación en la cual será utilizado. Es por esto que este campo de investigación está en constante desarrollo, ideando e implementando métodos que ayuden a mantener la autenticación de los estudios médicos digitales ante ataques.

Este trabajo se considera un buen punto de partida para una mejora continua en cuanto al marcado de estudios digitales, con el fin de que en un futuro cercano se desarrolle e implementen diversas técnicas que ayuden a mantener la confidencialidad de la información de cada uno de los pacientes que se realizan Imágenes de Resonancia Magnética.



## INSERCIÓN DE MARCAS DE AGUA OCULTAS Y CIFRADAS EN IMÁGENES DE RESONANCIA MAGNÉTICA APLICADAS EN DISPOSITIVOS IoT

TRABAJOS A FUTURO

## 9. TRABAJOS A FUTURO

Basándonos en la experiencia obtenida durante el desarrollo de este proyecto de investigación, se propone lo siguiente:

### Seguridad y Cifrado

Algoritmos de Cifrado Avanzados:

Implementación de algoritmos de cifrado más robustos como AES-256 para mejorar la seguridad de la información del paciente.

Investigación y desarrollo de técnicas de cifrado homomórficos que permitan realizar operaciones sobre datos cifrados sin necesidad de desencriptarlos.

Autenticación:

Desarrollo de un sistema de control de acceso basado en roles (RBAC) para gestionar los permisos de los usuarios de manera más efectiva.

Monitoreo y Detección de Intrusiones:

Implementación de sistemas de detección y prevención de intrusiones (IDS/IPS) para monitorear el acceso y uso del sistema en tiempo real.

### Esteganografía

Mejora de Técnicas Esteganográficas:

Evaluación del uso de redes neuronales profundas para mejorar la robustez y capacidad de ocultamiento de las marcas de agua.

Automatización de Procesos:

Desarrollo de herramientas que permitan la evaluación automática de la calidad de las marcas de agua ocultas.

### Interfaz Gráfica Visual

Usabilidad y Experiencia del Usuario:

Realización de estudios de usabilidad para identificar áreas de mejora en la interfaz gráfica y optimizar la experiencia del usuario.

Desarrollo de tutoriales interactivos y documentación accesible para facilitar el uso del sistema por parte del personal médico.

Interactividad y Personalización:

Implementación de funcionalidades interactivas que permitan a los usuarios personalizar la apariencia y disposición de la interfaz.

## Base de Datos

Optimización y Rendimiento:

Implementación de bases de datos distribuidas para manejar grandes volúmenes de datos y mejorar la escalabilidad.

Seguridad de Datos:

Encriptación de datos en reposo y en tránsito para proteger la información almacenada en la base de datos.

## Nube

Integración y Escalabilidad:

Migración a servicios en la nube que ofrezcan escalabilidad automática para manejar aumentos en la carga de trabajo.

Utilización de servicios de contenedores y orquestación (como Kubernetes) para mejorar la flexibilidad y portabilidad del sistema.

Respaldo y Recuperación:

Implementación de estrategias de respaldo y recuperación de los datos.

Configuración de políticas de retención y eliminación segura de datos para cumplir con las regulaciones y normativas de protección de datos.

Estas mejoras y trabajos a futuro no solo fortalecerán la seguridad y funcionalidad del sistema, sino que también optimizarán la experiencia del usuario y la gestión de datos, proporcionando un entorno más seguro y eficiente para la manipulación de Imágenes de Resonancia Magnética y otros documentos médicos digitales.



## INSERCIÓN DE MARCAS DE AGUA OCULTAS Y CIFRADAS EN IMÁGENES DE RESONANCIA MAGNÉTICA APLICADAS EN DISPOSITIVOS IoT

### REFERENCIAS

## Referencias

- [1] L. C. Hernandez Olvera y J. C. Nazario Alvarez. “Eliminación de ruido y segmentación de formas en imágenes médicas”. DSpaceRepository. <http://www.ptolomeo.unam.mx:8080/xmlui/handle/132.248.52.100/171> (accedido el 31 de marzo de 2023).
- [2] S. Kumar y S. Shastri. “Alzheimer RMI Preprocessed Dataset”. Kaggle: Your Machine Learning and Data Science Community. <https://www.kaggle.com/datasets/sachinkumar413/alzheimer-mri-dataset> (accedido el 20 de mayo de 2023).
- [3] J. Sarta. “Brain Tumor Classification (RMI)”. Kaggle: Your Machine Learning and Data Science Community. <https://www.kaggle.com/datasets/sartajbhuvaji/brain-tumor-classification-mri> (accedido el 25 de mayo de 2023).
- [4] J. Unzilla, “Marcas de agua digitales, qué son y para qué sirven”. Blog de la Cátedra de Cultura Científica de la UPV/EHU. <https://culturacientifica.com/2018/05/14/watermarking-marcas-de-agua-digitales-que-son-y-para-que-sirven/>. (accedido el 12 de septiembre de 2023).
- [5] A. Orúe, “Marcas de agua en el mundo real”. Facultad de Ingeniería Eléctrica en la Universidad de Oriente de Santiago de Cuba. <https://digital.csic.es/bitstream/10261/8864/1>. (accedido el 13 de septiembre de 2023).
- [6] Adobe. “Fotografía con marca de agua: Protección de las fotos”. Adobe Creative Cloud. <https://www.adobe.com/es/creativecloud/photography/discover/watermarking-photography.html> (accedido el 12 de abril de 2023).
- [7] J. Toral, “Esquema de marca de agua robusto ante ataques geométricos para la identificación de imágenes con derechos de autor”. Centro de Investigación en Matemáticas, A.C. pags. 29-30. (accedido el 14 de septiembre de 2023).
- [8] P. Alvarado. “Clasificaciones de las marcas de agua, propiedades y aplicaciones”. Watermarkero. <https://watermarkero.blogspot.com/2009/02/clasificaciones-de-las-marcas-de-agua.html> (accedido el 25 de septiembre de 2023).
- [9] Fotor, “Quitar marca de agua online en segundos”. Fotor Everimaging Limited. <https://www.fotor.com/es/features/quitar-marca-de-agua/>. (accedido el 26 de septiembre de 2023).
- [10] Integrating the Healthcare Enterprise. "Making healthcare interoperable". IHE International. <https://www.ihe.net/> (accedido el 8 de abril de 2023).
- [11] InLerning. “¿Qué es la esteganografía?”. LinkedIn. <https://es.linkedin.com/learning/recursos-de-arquitectura-y-diseno-seguros-comptia-security-plus-sy0-601/que-es-la-esteganografia> (accedido el 9 de abril de 2023).

- [12] J. Blitz, “¿Cómo ocultar un archivo dentro de otro? – Esteganografía”. Hack by Security. <https://www.hackbysecurity.com/blog/como-ocultar-un-archivo-dentro-de-otro-esteganografia-1>. (accedido el 30 de octubre de 2023).
- [13] D. Salomon, “Coding for Data and Computer Communications”, Springer”. (accedido el 28 de septiembre de 2023).
- [14] P. Iglesias, “Esteganografía, el arte de ocultar información sensible”. Mundo Hacker. <https://www.pabloyglesias.com/mundohacker-esteganografia/>. (accedido el 28 de septiembre de 2023).
- [15] P. K. Priyanka Sharma, “Review of Various Image Steganography and Steganalysis Techniques”. International Journal of Advanced Research in Computer Science and Software Engineering.(accedido el 28 de septiembre de 2023).
- [16] D. V. Jasleen Kour, “Steganography Techniques - A Review Paper”. International Journal of Emerging Research in Management & Technology. (accedido el 06 de octubre de 2023).
- [17] J. D. Vico, “Esteganografía y Estegoanálisis: Ocultación de datos en streams de audio vorbis”. Universidad Politécnica de Madrid. (accedido el 29 de septiembre de 2023).
- [18] J. L. Velasco, “Esteganografia en una imagen digital en el dominio DCT”. (accedido el 03 de octubre de 2023).
- [19] D. B. Renza, “Método de ocultamiento de píxeles para esteganografía de imágenes en escala de grises sobre imágenes a color”. ISSN:1794-9165 | ISSN-e: 2256-4314, (accedido el 05 de octubre de 2023).
- [20] M. Padrón, “Ocultamiento de datos en imágenes digitales mediante BPCS”. Xalapa. (accedido el 05 de octubre de 2023).
- [21] A. Menezes, P.C. van Oorschot, S. Vanstone, “Handbook of Applied Cryptography”. pág 2 <https://cacr.uwaterloo.ca/hac/about/chap1.pdf> (accedido el 09 de octubre de 2023).
- [22] A. Menezes, P.C. van Oorschot, S. Vanstone, “Handbook of Applied Cryptography”. pág 3 <https://cacr.uwaterloo.ca/hac/about/chap1.pdf> (accedido el 10 de octubre de 2023).
- [23] A. Menezes, P.C. van Oorschot, S. Vanstone, “Handbook of Applied Cryptography”. pág 4-6 <https://cacr.uwaterloo.ca/hac/about/chap1.pdf> (accedido el 10 de octubre de 2023).
- [24] J. Roa Buendía, “Seguridad informática”. McGraw Hill. (accedido el 11 de octubre de 2023).
- [25] Immune Technology Institute, “Tipos de criptografía ¿Cuáles son los más comunes para la privacidad de las comunicaciones?”).ITI. <https://immune.institute/blog/tipos-de-criptografia-seguridad-online/> (accedido el 20 de octubre de 2023).

- [26] Stallings, W. (2014). Cryptography and network security: principles and practice. Pearson Education. (accedido el 24 de octubre de 2023).
- [27] B, Schneier.“Applied Cryptography.” Segunda Edición. EE.UU. 1996. (accedido el 26 de octubre de 2023).
- [28] M. López. “Criptografía y Seguridad en Computadores”. Cuarta edición. Págs. 163-164. (accedido el 28 de octubre de 2023).
- [29] WatchGuard Brand. “¿Qué es el cifrado AES? Una guía sobre el Advanced Encryption Standard”. Panda MediaCenter. <https://www.pandasecurity.com/es/mediacenter/cifrado-aes-guia/> (accedido el 03 de noviembre de 2023).
- [30] Instituto Nacional del Cáncer. "Diccionario de cáncer del NCI". Instituto Nacional del Cáncer. <https://www.cancer.gov/espanol/publicaciones/diccionarios/diccionario-cancer/def/imagen-por-resonancia-magnetica> (accedido el 31 de marzo de 2023).
- [31] Actualpacs. "¿Cuál es el diagnóstico de esta RM de rodilla?". Actualpacs improve your diagnoses. <https://www.actualpacs.com/blog/2018/01/09/caso-real-rm-rodilla/> (accedido el 27 de abril de 2023)
- [32] Adobe. “Archivos de imagen”. Adobe Creative Cloud. <https://www.adobe.com/mx/creativecloud/file-types/image.html> (accedido el 5 de abril de 2023).
- [33] Adobe. “Archivos SVG”. Adobe Creative Cloud. <https://www.adobe.com/mx/creativecloud/file-types/image/vector/svg-file.html> (accedido el 5 de abril de 2023).
- [34] Adobe. “Archivos STL”. Adobe Creative Cloud. <https://www.adobe.com/mx/creativecloud/file-types/image/vector/stl-file.html> (accedido el 5 de abril de 2023).
- [35] Adobe. “Archivos EPS”. Adobe Creative Cloud. <https://www.adobe.com/mx/creativecloud/file-types/image/vector/eps-file.html> (accedido el 5 de abril de 2023).
- [36] Adobe. “Archivos GIF”. Adobe Creative Cloud. <https://www.adobe.com/mx/creativecloud/file-types/image/raster/gif-file.html> (accedido el 5 de abril de 2023).
- [37] Adobe. “Archivos PNG”. Adobe Creative Cloud. <https://www.adobe.com/mx/creativecloud/file-types/image/raster/png-file.html> (accedido el 5 de abril de 2023).
- [38] Adobe. “Archivos JPEG”. Adobe Creative Cloud. <https://www.adobe.com/mx/creativecloud/file-types/image/raster/jpeg-file.html> (accedido el 5 de abril de 2023).

- [39] Adobe. “Archivos DNG”. Adobe Creative Cloud. <https://www.adobe.com/mx/creativecloud/file-types/image/raw/dng-file.html> (accedido el 5 de abril de 2023).
- [40] ILCE. "Procesamiento de imágenes". Biblioteca digital. [http://bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen2/ciencia3/084/htm/sec\\_9.htm](http://bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen2/ciencia3/084/htm/sec_9.htm) (accedido el 6 de abril de 2023).
- [41] L. Hernández , J. Nazario. “Eliminación de ruido y segmentación de formas en imágenes médicas”. Universidad Nacional Autónoma de México UNAM. <http://www.ptolomeo.unam.mx:8080/xmlui/handle/132.248.52.100/171> (accedido el 27 de octubre de 2023).
- [42] Casasola Gómez Armando Iván, “Marcas de agua para archivos de vídeo”, México CDMX, Diciembre 2006.
- [43] Areyla Ekaterine Mejía Alba, “Galería de arte con marcas de agua”, México CDMX, 24 de Junio 2009.
- [44] Adobe. “Adobe Photoshop”. Adobe Creative Cloud <https://www.adobe.com/mx/products/photoshop.html>. (accedido el 24 de abril de 2023).
- [45] Watermark Pro. “Watermark Pro Signature y Logo”. Apple Inc. <https://apps.apple.com/mx/app/watermark-pro-signature-logo/id996776886> (accedido el 24 de abril de 2023).
- [46] Adobe. “Adobe Photoshop”. Adobe Creative Cloud <https://www.adobe.com/mx/products/photoshop.html> (accedido el 24 de abril de 2023).
- [47] J. Montero, “Criptografía Grado en Ingeniería Informática”. <https://silo.tips/download/criptografia-grado-en-ingeneria-informatica> (accedido el 25 de octubre de 2023).
- [48] W. Chengyou, Y. Zhang, X. Zhou. “Robust image watermarking algorithm based on ASIFT against geometric attacks.” Applied Sciences 8.3, pág. 410. (accedido el 20 de septiembre de 2023).
- [49] A. Eldayem, M. Mohamed, “A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine”. Egyptian Informatics Journal 14.1, pags. 1-13. (accedido el 20 de septiembre de 2023).
- [50] N. Athanasios, “Local distortion resistant image watermarking relying on salient feature extraction”. EURASIP Journal on Advances in Signal Processing 1, pág. 97. (accedido el 20 de septiembre de 2023).

- [51] A. Eldayem, M. Mohamed, “A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine”. Egyptian Informatics Journal 17.3, pags. 4-7. (accedido el 27 de septiembre de 2023).
- [52] E. Maida, J. Pacienza.“Metodologías de desarrollo de software [Tesis de Licenciatura, Universidad Católica Argentina]”. Biblioteca digital de la Universidad Católica Argentina. <http://bibliotecadigital.uca.edu.ar/repositorio/tesis/metodologias-desarrollo-software.pdf> (accedido el 11 de diciembre de 2023).
- [53] M. Frackiewicz. “IA en el procesamiento de imágenes y videos: Lenguajes y bibliotecas para aplicaciones de medios inteligentes”. TS2 SPACE.  
[https://ts2.space/es/ia-en-el-procesamiento-de-imagenes-y-videos-lenguajes-y-bibliotecas-para-aplicaciones-de-medios-inteligentes/#google\\_vignette&gsc.tab=0](https://ts2.space/es/ia-en-el-procesamiento-de-imagenes-y-videos-lenguajes-y-bibliotecas-para-aplicaciones-de-medios-inteligentes/#google_vignette&gsc.tab=0) (accedido el 11 de diciembre de 2023).