



**ESPE**  
UNIVERSIDAD DE LAS FUERZAS ARMADAS  
INNOVACIÓN PARA LA EXCELENCIA

**DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA**

**CARRERA DE INGENIERÍA EN ELÉCTRICA Y  
TELECOMUNICACIONES**

**TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL  
TÍTULO DE INGENIERÍA EN ELECTRÓNICA Y  
TELECOMUNICACIONES**

**TEMA: DESARROLLO Y ANÁLISIS DE UNA TÉCNICA  
ESTEGANOGRÁFICA PARA LA TRANSMISIÓN DE  
IMÁGENES EN ARCHIVOS DE AUDIO ORIENTADO A LA  
SEGURIDAD EN LAS REDES DE COMUNICACIÓN**

**AUTOR: BASTIDAS SOSA, CRISTINA ELIZABETH**

**DIRECTOR: ING. ACOSTA BUENAÑO, FREDDY**

**SANGOLQUÍ**

**2018**



DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA  
CARRERA DE ELECTRÓNICA Y TELECOMUNICACIONES

### CERTIFICACIÓN

Certifico que el trabajo de titulación, “DESARROLLO Y ANÁLISIS DE UNA TÉCNICA ESTEGANOGRÁFICA PARA LA TRANSMISIÓN DE IMÁGENES EN ARCHIVOS DE AUDIO ORIENTADO A LA SEGURIDAD EN LAS REDES DE COMUNICACIÓN” realizado por la señorita Cristina Elizabeth Bastidas Sosa con CI: 171819120-6 e ID: L00036139, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar a la señorita **CRISTINA ELIZABETH BASTIDAS SOSA** para que lo sustente públicamente.

Sangolquí, 08 de enero del 2018

ING. FREDDY ACOSTA BUENAÑO

[fracosta@espe.edu.ec](mailto:fracosta@espe.edu.ec)



**DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA  
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y  
TELECOMUNICACIONES**

**AUTORÍA DE RESPONSABILIDAD**

Yo, **CRISTINA ELIZABETH BASTIDAS SOSA**, con cédula de identidad N° 171819120-6, declaro que este trabajo de titulación “**DESARROLLO Y ANÁLISIS DE UNA TÉCNICA ESTEGANOGRÁFICA PARA LA TRANSMISIÓN DE IMÁGENES EN ARCHIVOS DE AUDIO ORIENTADO A LA SEGURIDAD EN LAS REDES DE COMUNICACIÓN**” ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas. Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

**Sangolquí, 08 de enero del 2018**

-----  
**CRISTINA ELIZABETH BASTIDAS SOSA**

**C.C: 171819120-6**



**DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA  
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y  
TELECOMUNICACIONES**

**AUTORIZACIÓN**

Yo, **CRISTINA ELIZABETH BASTIDAS SOSA**, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación **“DESARROLLO Y ANÁLISIS DE UNA TÉCNICA ESTEGANOGRÁFICA PARA LA TRANSMISIÓN DE IMÁGENES EN ARCHIVOS DE AUDIO ORIENTADO A LA SEGURIDAD EN LAS REDES DE COMUNICACIÓN”** cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

**Sangolquí, 08 de enero del 2018**

-----  
**CRISTINA ELIZABETH BASTIDAS SOSA**

**C.C: 171819120-6**

## DEDICATORIA

*Quiero dedicar mi tesis a las personas más importantes y especiales en mi vida, mis padres Nancy y Rafael, quienes gracias a su trabajo y dedicación, me brindaron todo su apoyo para lograr ser la persona que ahora soy. Quiero expresarles mis agradecimientos, mi admiración y amor profundo hacia ellos ya que, gracias a su entrega he logrado superar muchas pruebas en mi vida, levantarme ante las adversidades que se han presentado en el camino recorrido de nuestras vidas, así como lo hemos hecho y aspiro que sigan siendo mi fuerza, mi guía y ejemplo para seguir adelante con la bendición de Dios juntos como la familia que siempre hemos sido.*

*También quiero dedicar mi trabajo a mi hermana Paola ya que ha sabido demostrarme que los obstáculos no impiden lograr sus metas, que la responsabilidad, el respeto y la humildad son valores muy importantes en la vida. Gracias a sus consejos y apoyo durante todo el desarrollo de mi proyecto.*

*Cristina Elizabeth Bastidas Sosa*

## AGRADECIMIENTO

*A Dios por las bendiciones recibidas, por ser mi motor en los momentos de tristeza y ser la luz que ha guiado siempre mi camino.*

*A mi familia quienes siempre me han apoyado en los momentos difíciles y me dieron impulso para jamás rendirme.*

*A mi novio Edison por ser una persona incondicional, alegre, respetuosa y responsable que supo brindarme todo su apoyo en este proceso. Hemos pasado muchos momentos difíciles de nuestras vidas pero hemos sabido salir adelante y luchando juntos lograremos cumplir todos nuestros planes a futuro con la bendición de Dios y de nuestros padres. Gracias a sus consejos, su amor y apoyo incondicional en toda esta etapa que me han servido para no dejarme vencer y luchar por mi sueño de convertirme en una profesional.*

*A mi amiga Jessica que compartió junto conmigo muchas experiencias en este duro camino de nuestra formación profesional dentro y fuera del salón de clases. Gracias por que fue una ayuda indispensable durante todo el proceso de desarrollo de mi proyecto de tesis, éxitos en su vida.*

*A mi profesor, tutor y amigo Ing. Freddy Acosta por guiarme en el desarrollo de este proyecto para poder culminar este último paso de mi formación profesional, pero en especial por brindarme su amistad sincera, su confianza, su paciencia y por sus consejos en momentos difíciles, muchas bendiciones toda su familia y para él en su vida personal y profesional.*

*Cristina Elizabeth Bastidas Sosa*

## ÍNDICE DE CONTENIDO

CARÁTULA	
CERTIFICADO .....	ii
AUTORÍA DE RESPONSABILIDAD.....	iii
AUTORIZACIÓN.....	iv
DEDICATORIA .....	v
AGRADECIMIENTO.....	vi
ÍNDICE DE CONTENIDO .....	vii
INDICE DE TABLAS.....	x
ÍNDICE DE FIGURAS .....	xi
RESUMEN .....	xiv
ABSTRAC.....	xv
<b>CAPÍTULO 1 .....</b>	<b>1</b>
1. INTRODUCCIÓN.....	1
1.1 ANTECEDENTES .....	1
1.2 JUSTIFICACIÓN E IMPORTANCIA.....	2
1.3 ALCANCE DEL PROYECTO .....	2
1.4 OBJETIVOS.....	3
1.5 CONTENIDO DEL PROYECTO .....	4

<b>CAPÍTULO 2</b> .....	6
2. FUNDAMENTO TEÓRICO .....	6
2.1 Seguridad en la red informática actual .....	6
2.2 Tipos de ataques .....	7
2.3 Historia de la Esteganografía .....	8
2.4 Esteganografía terminología .....	11
2.5 Técnicas de Esteganografía.....	14
2.6 Formatos de audio digital.....	22
2.7 Imágenes Digitales .....	28
2.8 Formatos de imágenes digitales .....	36
2.9 Aplicaciones de la Esteganografía.....	41
<b>CAPÍTULO 3</b> .....	44
3. DISEÑO DEL PROGRAMA .....	44
3.1 Descripción general del programa.....	44
3.2 Medidas de Calidad de Imágenes.....	49
3.3 Medidas de Calidad de Audios.....	54
<b>CAPÍTULO 4</b> .....	56
4. IMPLEMENTACIÓN, PRUEBAS Y RESULTADOS .....	56



4.1 Implementación Esteganografía en audio.....	56
4.2 Pruebas realizadas .....	63
4.3 Análisis de resultados .....	64
<b>CAPÍTULO 5</b> .....	<b>85</b>
5.1 Conclusiones .....	85
5.2 Recomendaciones .....	87
5.3 Trabajos Futuros.....	87
<b>REFERENCIAS</b> .....	<b>89</b>

## INDICE DE TABLAS

<b>Tabla 1</b>	Clasificación de Técnicas Esteganográficas para archivos tipo audio.....	20
<b>Tabla 2</b>	Tabla comparativa de técnicas Esteganográficas y Criptográficas.....	21
<b>Tabla 3</b>	Características del Formato WMA.....	24
<b>Tabla 4</b>	Características del formato MP3.....	25
<b>Tabla 5</b>	Estructura del Formato WAV.....	26
<b>Tabla 6</b>	Descripción de Cabecera WAV.....	27
<b>Tabla 7</b>	Dimensiones de Imágenes Digitales.....	29
<b>Tabla 8</b>	Modos de Operación de Imágenes JPEG.....	37
<b>Tabla 9</b>	Tabla Comparativa entre Formatos Digitales de Imágenes.....	40
<b>Tabla 10</b>	Tipos de Marcas de Agua Esteganográficas según su robustez.....	41
<b>Tabla 11</b>	Tabla de Medidas de Satisfacción del Usuario.....	54
<b>Tabla 12</b>	Tiempo de duración de audios y Velocidad de bits.....	62
<b>Tabla 13</b>	Descripción de Escenarios de Pruebas de Audios Esteganográficos.....	64
<b>Tabla 14</b>	Tabla de resultados totales de encuestas MOS.....	68

## ÍNDICE DE FIGURAS

<b>Figura 1</b>	Porta del Libro de las Historias de Herodoto Esteganografía.....	8
<b>Figura 2</b>	Recado Telefónico donde fue aplicada la Técnica de Micro puntos .....	10
<b>Figura 3</b>	Modelo General de un Sistema Esteganográfico .....	13
<b>Figura 4</b>	Diagrama básico del proceso de esteganografia mediante imágenes.....	14
<b>Figura 5</b>	Técnica LSB implementada en imágenes RGB .....	15
<b>Figura 6</b>	Rangos de Frecuencia audibles .....	20
<b>Figura 7</b>	Ejemplo de un Proceso de digitalización de imágenes.....	28
<b>Figura 8</b>	Formatos de Imágenes 2D a) Imagen Vectorial b) Mapa de Bit .....	31
<b>Figura 9</b>	Tabla de Pixeles de una Imagen Binaria .....	32
<b>Figura 10</b>	Pixeles de una Imagen a Escala de Grises .....	33
<b>Figura 11</b>	Pixeles e una imagen RGB .....	34
<b>Figura 12</b>	Cubo RGB.....	34
<b>Figura 13</b>	Visión Estereoscópica .....	36
<b>Figura 14</b>	Estructura de Compresión JPEG2000 .....	38
<b>Figura 15</b>	Pantalla principal del Programa Esteganográfico .....	45
<b>Figura 16</b>	a)Ocultar imágenes B&N b)Recuperar imágenes B&N.....	45
<b>Figura 17</b>	Diagrama de Flujos de Inserción de Bits de Imágenes B&N .....	46
<b>Figura 18</b>	Diagrama de Flujo de Recuperación de Bits de Imagen B&N .....	47
<b>Figura 19</b>	a)Ocultar imágenes RGB b)Recuperar imágenes RGB.....	48
<b>Figura 20</b>	Diagrama de Inserción de bits de imagen RGB.....	48
<b>Figura 21</b>	Diagrama de Recuperación de Bits imagen RGB .....	49
<b>Figura 22</b>	Diagrama del sistema de medida de la similitud estructural (SSIM)...	52
<b>Figura 23</b>	Imagen e Histograma correspondiente .....	53

<b>Figura 24</b> Histogramas de color 3 canales RGB .....	53
<b>Figura 25</b> Selección de Audio Portador .....	56
<b>Figura 26</b> Selección de Imagen secreta .....	57
<b>Figura 27</b> Matriz de Pixeles de Imagen escogida para ser oculta .....	58
<b>Figura 28</b> Redimensionamiento de imágenes a ocultar, Tamaño de la matriz .....	58
<b>Figura 29</b> Matriz de pixeles convertidos a binarios .....	59
<b>Figura 30</b> Columna de bits que serán insertados en bit menos significativo.....	59
<b>Figura 31</b> Proceso de almacenamiento del archivo esteganográfico .....	59
<b>Figura 32</b> Interfaz de Recuperación de imágenes ByN.....	60
<b>Figura 33</b> Imagen recuperada RGB.....	61
<b>Figura 34</b> Diagrama de realización encuestas MOS .....	65
<b>Figura 35</b> Resultados encuesta MOS para imágenes 1 canal .....	66
<b>Figura 36</b> Resultados encuesta MOS para imágenes 3 canales .....	66
<b>Figura 37</b> Resultados encuesta MOS totales .....	67
<b>Figura 38</b> Grafica de Valores MSE de audios esteganográficos totales .....	69
<b>Figura 39</b> Grafica de Valores MSE de audios esteganográficos totales.....	70
<b>Figura 40</b> a) RMSE Promedio b) SSIM promedio del Primer Escenario .....	71
<b>Figura 41</b> MSE promedio de Audio portador del Primer Escenario.....	72
<b>Figura 42</b> a) RMSE Promedio b) SSIM promedio del Segundo Escenario .....	73
<b>Figura 43</b> MSE promedio de Audio portador del Segundo Escenario.....	74
<b>Figura 44</b> a) RMSE Promedio b) SSIM promedio del Tercer Escenario.....	75
<b>Figura 45</b> MSE promedio de Audio portador del Tercer Escenario .....	75
<b>Figura 46</b> a) Imagen Original 1 b) Imagen Recuperada 1 c) Histograma 1 .....	77
<b>Figura 47</b> a) Imagen Original 2 b) Imagen Recuperada 2 c) Histograma 2 .....	78

<b>Figura 48</b>	a) Imagen Original 3 b) Imagen Recuperada 3 c) Histograma 3 .....	79
<b>Figura 49</b>	a) Imagen Original 4 b) Imagen Recuperada 4 c) Histograma 4 .....	80
<b>Figura 50</b>	a) Imagen Original 5 b) Imagen Recuperada 5 c) Histograma 5 .....	81
<b>Figura 51</b>	a) Imagen Original 6 b) Imagen Recuperada 6 c) Histograma 6 .....	82
<b>Figura 52</b>	a)RMSE imágenes ByN b)RMSE imágenes RGB tres escenarios ....	83
<b>Figura 53</b>	a)SSIM imágenes ByN b)SSIM imágenes RGB tres escenario .....	84

## **RESUMEN**

A lo largo de la historia se ha presentado la necesidad de mantener oculta información muy importante de manera que sólo entidades autorizadas puedan tener acceso, de esta forma se han realizado estudios sobre el desarrollo de técnicas que buscan obtener una eficiente confidencialidad de datos. Algunos de los métodos implementados en la antigüedad han sido algoritmos sencillos de sustitución de caracteres, llegando hasta métodos matemáticos avanzados que permiten una optimización en los procesos y un cifrado de datos casi imposibles de descubrir. La esteganografía es uno de los diferentes métodos que existen para ocultar mensajes en un portador, con el objetivo de que pasen desapercibidos para terceros. Actualmente los portadores preferidos para implementar técnicas esteganográficas son archivos de tipo digital, ya sea video, imágenes o sonido. Por esta razón, el presente trabajo busca desarrollar una técnica de esteganografía para la transmisión de imágenes en archivos de audio, usando el algoritmo LSB, desarrollando un programa usando como herramientas el software Matlab que proporciona varias ventajas a través de su lenguaje de programación. Por último se evaluará la calidad de imagen oculta recuperada después de exponer el archivo de audio a varios escenarios, evaluando también la calidad de los audios portadores para determinar la efectividad y validez del algoritmo implementado.

### **PALABRAS CLAVE**

- **ESTEGANOGRAFIA**
- **LSB (LEAST SIGNIFICANTT BIT)**
- **SSIM(STRUCTURAL SIMILARITY INDEX)**
- **MSE(MEAN SQUARED ERROR)**

## **ABSTRAC**

History presented the need to keep hidden important information where only authorized entities can have access, studies have been conducted on the development of techniques that seek an efficient form of data confidentiality. The old methods implemented simple algorithms of substitution of bits, coming to use advanced mathematical methods, to optimize the processes and to provide an encryption of data almost impossible to discover. Steganography is a method to hide messages in a carrier, the main objective is to be unnoticed for third parties. Presently preferred carriers to implement steganographic techniques are digital type files, whether video, images or sound. For this reason, the present work seeks to develop a steganography technique for the transmission of images in audio files, using the LSB algorithm, developing a program using Matlab software as tools that provides several advantages through its programming language. Finally the image quality will be evaluated hidden recovered after exposing the audio file to various scenarios, also evaluating the quality of the audio carriers to determine the effectiveness and validity of the implemented algorithm.

### **KEYWORDS:**

- **STEGANOGRAPHY**
- **LSB (LEAST SIGNIFICANTT BIT)**
- **SSIM(STRUCTURAL SIMILARITY INDEX)**
- **MSE(MEAN SQUARED ERROR)**

# CAPÍTULO 1

## 1. INTRODUCCIÓN

### 1.1 ANTECEDENTES

Los consumidores de servicios digitales demandan un entorno cada vez más seguro para la transmisión de información, debido a la falta de medidas de seguridad en las redes informáticas y al crecimiento en los ataques que se han convertido en la principal amenaza a la privacidad. En Brasil y Rusia, por ejemplo presentan una tasa de detección de casi tres veces las tasas de detección de ataques del resto del mundo, donde se aplican nuevas técnicas de esteganografía y encriptación de datos a un nivel muy avanzado. (España Boquera M. C., 2003)

La esteganografía es una técnica usada para el ocultamiento de información dentro de otros objetos conocidos como portadores. En el año 2009 ya se desarrollaron estudios sobre esteganografía implementando la técnica esteganográfica LSB (Least Significant Bit) (Lerch-Hostalot & Megías, 2013), que incluía mensajes de texto en archivos de imagen con el objetivo de evaluar el método propuesto y permitir que la información en caso de ser interceptada no levante sospechas y llegue de manera segura al destinatario (Cantanhede, 2009). Por otro lado en la Universidad de las Fuerzas Armadas se han creado técnicas esteganográficas en imágenes mucho más robustas ante ataques estadísticos, mediante la combinación de dos métodos: la técnica de color reversible y búsqueda de bordes y texturas en la imagen. (Onofre, 2016)

Sobre la utilización de la esteganografía en audio se han implementado algunos algoritmos orientadas al uso de audio como portadores de archivos de datos (Rodríguez, 2016) (Cantanhede, 2009), que se han convertido en una pauta importante para el estudio de esta técnica, brindando mayor información para desarrollar más aplicaciones en el ámbito de las telecomunicaciones. (Casierra, 2009)



## **1.2 JUSTIFICACIÓN E IMPORTANCIA**

En el ámbito de las telecomunicaciones algún usuario que tenga acceso a las TIC's puede manipular o atacar cualquier tipo de información con relativa facilidad, pero aun así, aunque el usuario conozca la existencia de un mensaje oculto las probabilidades de que lo obtenga son muy bajas, debido a que no se conoce la técnica que se implementó al ocultar la información. El vertiginoso crecimiento de la tecnología día a día produce que los ataques informáticos sean más frecuentes y efectivos, permitiendo obtener información confidencial.

Es importante considerar las limitaciones que se derivan de los trabajos realizados sobre las técnicas esteganográficas aplicadas en archivos de imágenes (Onofre, 2016) y en audios (Rodriguez, 2016). La esteganografía en imágenes se basa en ocultar la información en cuadros de imagen RGB, pero la esteganografía en audio no es muy usada ni estudiada. Al trabajar con archivos de audio se debe tomar en cuenta muchos aspectos importantes como son la calidad del audio al ser enviada por la red que sufre un ligero cambio tomando en cuenta medidas subjetivas y objetivas para cumplir con un análisis de calidad auditivo mucho más dedicado y conocer la influencia de las técnicas esteganográficas tanto en su estructura como calidad auditiva.

Es importante analizar nuevas técnicas de esteganografía usadas para la transmisión de archivos multimedia y de esta forma poder disminuir los ataques a la privacidad en el entorno de las comunicaciones.

## **1.3 ALCANCE DEL PROYECTO**

Este proyecto se enfoca en el desarrollo y análisis de una técnica de esteganografía usada para la transmisión de imágenes ocultas en archivos de audio. Para este fin se desarrollará una herramienta de simulación en Matlab basada en el método de esteganografía del dominio espacial LSB (Least Significant Bit), ya que en este se tiene una gran capacidad de incrustación de la información con un bajo procesamiento matemático. Para esta manera transmitir información de forma segura e indetectable

y para aplicarlo en diferentes escenarios de la vida diaria evitando llamar la atención en la transmisión de un conjunto de datos ocultos, y no sólo evitar que otros lleguen a conocer la información oculta, sino que también evita que otros piensen que incluso no existe la información.

Determinar el desempeño de la transmisión de imágenes usando una técnica esteganográfica en un archivo de audio. Para esto se desarrollará una aplicación en Matlab con el método esteganográfico LSB. Principalmente tendrá una interfaz gráfica de entrada que permita tener una información general de la funcionalidad del programa, para después tener un menú donde se puede elegir el audio que será el archivo portador y también la imagen que será ocultada. Las pruebas se realizarán sobre diferentes escenarios que evaluarán con una encuesta MOS la calidad del audio, la medición del valor SSIM que determinará la similitud entre imágenes según el sistema visual humano y el error RMSE como una medida objetiva que probará el algoritmo utilizado sobre imágenes de uno y tres canales. Los resultados obtenidos permitirán disponer de una aplicación real para el desarrollo de sistemas de transmisión de datos multimedia, evaluar la calidad del audio e imagen y poder desarrollar trabajos futuros debido a la versatilidad del tema.

## **1.4 OBJETIVOS**

### **1.4.1 General**

- Desarrollar y analizar un algoritmo que permita la transmisión de imágenes en archivos de audio, con la utilización de técnicas estenográficas para proporcionar seguridad en sistemas de comunicación.

### **1.4.2 Específicos**

- Investigar y conocer las diferentes técnicas de esteganografía usadas en el envío de información oculta.

- Desarrollar un algoritmo para el envío de información oculta con la ayuda de la plataforma informática Matlab.
- Realizar pruebas sobre diferentes escenarios y analizar la calidad del audio recibido.

## 1.5 CONTENIDO DEL PROYECTO

El presente proyecto de grado está estructurado en cinco capítulos, cuyo contenido se describen a continuación:

**Capítulo 1. *Introducción:*** En este capítulo se detallan los antecedentes, justificación, alcance del proyecto y los objetivos principales, puntualizando los contenidos de cada capítulo para que el lector tenga una idea clara del tema del trabajo.

**Capítulo 2. *Fundamento Teórico:*** Aquí se describe el marco teórico en el que se basa la investigación, describiendo y estudiando de forma básica el concepto y técnicas principales referentes a la esteganografía. Además se abordará de manera resumida y puntual temas importantes para este trabajo como técnicas y herramientas, los parámetros fundamentales para el análisis de características de una imagen como desviación estándar, media e histogramas, métodos de detección de bordes y texturas basados en procesamiento de imágenes y por último métricas para evaluar la calidad de una imagen. Este capítulo permitirá comprender de mejor manera las técnicas usadas para el desarrollo del proyecto.

**Capítulo 3 *Diseño del Programa:*** Se detalla el método esteganográfico usado, es decir, el procedimiento que se utilizó para la inserción de imágenes de uno y tres canales (blanco y negro, RGB) en los archivos de audio, así como recuperación de ambos. También se presenta una breve explicación del software usado Matlab donde se diseña de la aplicación que desarrollará el tema propuesto.

**Capítulo 4 *Implementación, Pruebas y Resultados:*** Este capítulo expone los resultados obtenidos después de implementar los archivos de audio con esteganografía

a distintos escenarios, tanto para imágenes RGB y Blanco / Negro. Además describe las pruebas realizadas para evaluar la calidad de las imágenes recuperadas y audios portadores, y se verifica la efectividad de la técnica usada mediante el análisis de histogramas, SSIM, cálculos de errores y encuestas MOS.

**Capítulo 5 Conclusiones y Recomendaciones:** En este capítulo se presenta las conclusiones, recomendaciones finales obtenidas después de la recolección de datos sobre el algoritmo esteganográfico LSB implementado así como el programa desarrollado, describiendo también algunas propuestas de trabajos futuros en la línea de la esteganografía con archivos digitales.

## CAPÍTULO 2

### 2. FUNDAMENTO TEÓRICO

#### 2.1 Seguridad en la red informática actual

Un tema que en los últimos tiempos ha tomado gran relevancia para entidades y organizaciones mundiales es la confidencialidad de la información. El incremento de volumen de la información que ahora se maneja en los sistemas de comunicación actuales y las nuevas tecnologías que han aparecido con gran velocidad son las causas principales para los altos niveles de ataques, nuevas familias de malware, fallas de seguridad que tiene un impacto global no solo en el mundo corporativo sino en la información de los usuarios hogareños.

La mayoría de información que encontramos en la red es privada y de único interés para los propietarios de la misma, aquí es donde se deben buscar mecanismos, métodos y técnicas que garanticen que ésta información permanezca oculta para entidades o individuos que pretendan acceder a ella de manera no autorizada. (Tejada & García Dominguez, 2016)

La problemática de asegurar la confidencialidad de la información que así lo requiera ha venido evolucionando. Debido a que la información necesita ser constantemente transmitida mediante canales considerados inseguros, como lo es el internet, lo que provoca que esté en continuo peligro de ser capturada y se haga mal uso de ella. En los últimos años, Enjoy Safer Technology (ESET) ha debatido sobre cómo la web se convirtió en uno de los principales canales de propagación de códigos maliciosos, el crecimiento y profesionalización del crimeware, la importancia de las botnet (red de robots informáticos) para el mundo del ciber-crimen y la masificación del malware para dispositivos móviles. (ESET Enjoy Safer Technology, 2016)

Cada año la empresa ESET junto con sus especialistas en seguridad informática evalúa las nuevas tecnologías, los reportes de ataques, nuevas familias de malware o fallas de seguridad de impacto global, las ponen a prueba para entender cómo funciona y, en algunos casos, observan cómo se puede vulnerar la seguridad.

Durante 2015 se realizaron muchos reportes sobre vulnerabilidades en los wearables (dispositivos vestibles), en donde se desarrollaban casos que permitirían a un atacante robar y filtrar información desde el mismo dispositivo. Entre los medios que más usan los atacantes son las vulnerabilidades en las aplicaciones y en las tecnologías de comunicación, como por ejemplo Bluetooth, los códigos pin de seis dígitos. Los Smartphone utilizan tecnologías para comunicarse con otros equipos y cualquier falla de seguridad presentada en el protocolo permitiría a los atacantes leer en texto plano la información que se intercambia entre ellos. (ESET Enjoy Safer Technology, 2016)

## **2.2 Tipos de ataques**

Debido a que los métodos de ocultar información como la esteganografía se encuentran expuestos a diferentes ataques en los sistemas de comunicación, existen diferentes herramientas de software para obtener el mensaje secreto contenido en cualquier tipo de archivo digital; a continuación detallamos algunos ataques más comunes usados en la esteganografía actual. (Rodriguez, 2016)

- **Ataques estructurales**

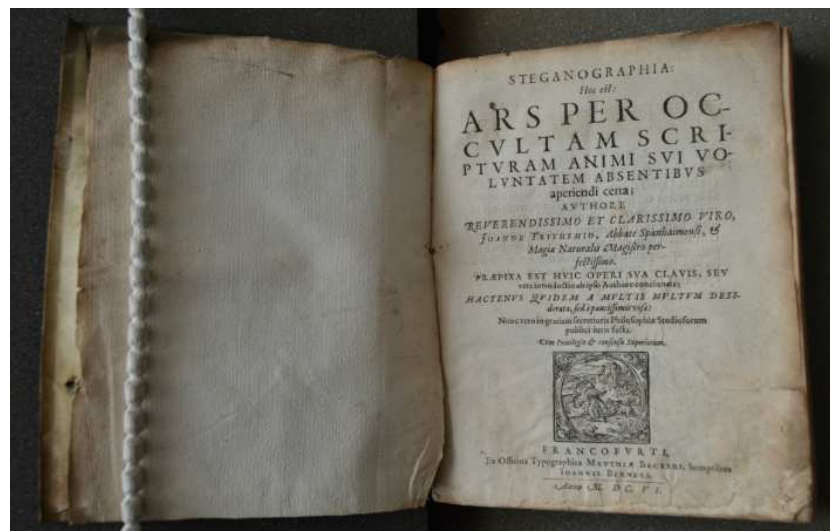
Los ataques estructurales compactan varias veces el archivo esteganográfico con el objetivo de eliminar todos los bits semejantes o redundantes ya que al momento de realizar esto el mensaje oculto llega a sufrir cambios, alteraciones y en ocasiones hasta pérdida completa siendo ininteligible.

- **Ataques estadísticos**

Como su nombre lo indica se basa en los procesos estadísticos en varios archivos con esteganografía, y así poder estimar en cual archivo elegido existe algún tipo de mensaje oculto. Se realiza la selección de archivos que son del mismo tipo para localizar cuál de ellos lleva la información oculta.

### 2.3 Historia de la Esteganografía

Una de las técnicas que permite enviar y entregar mensajes ocultos dentro de un objeto o contenedor, de manera que no se detecte su presencia y consigan pasar inadvertidos se llama esteganografía. Este método lleva años desarrollándose, como se puede observar en la Figura 1 el libro de las Historias de Herodoto presentaba varias anécdotas sobre esteganografía entre los años 484 y 430 a. C.



**Figura 1** Porta del Libro de las Historias de Herodoto Esteganografía

Fuente: (Yúbal, 2015)

## **Métodos clásicos**

Una de las posibles primeras manifestaciones de mensajes esteganográficos fue cuando Demeratus quería comunicar a la ciudad de Esparta que Xerxes tenía planes para invadir Grecia. Con el objetivo de evitar ser capturado por espionaje en los controles, escribió los mensajes en tablas que luego fueron cubiertas con cera, de forma que parecían no haber sido alteradas. Durante siglos otro de los métodos que solía usar es cuando generalmente a un esclavo tatuaban un mensaje en su cabeza afeitada dejando crecer el cabello y enviar así el mensaje oculto.

## **Esteganografía: Segunda Guerra Mundial**

### **Tinta invisible**

Las ideas e ingenio que surgieron en la Segunda Guerra Mundial ayudaron a desarrollar técnicas con las que pudieran enviar mensajes sin que sus rivales pudiesen interceptarlos. Por esta razón la esteganografía predominó usando tintas invisibles que normalmente se usa de la siguiente forma: primero escribían normalmente una carta, y después entre las líneas de esa carta se escribía otro texto donde se ocultaba la información importante. Era habitual el uso de vinagre, zumos de frutas o como hoy en día compuestos químicos especializados. Para hacer visible el mensaje oculto el papel era calentado.

### **Cifrado nulo (Null Cipher)**

Hoy en día el método de escritura de meta-información en un texto sigue siendo usado ya que es uno de los más sencillos al momento de ocultar información. Antiguamente se usaban algoritmos y claves para escribir un texto aparentemente inofensivo donde subyace la información realmente importante. Un ejemplo claro de ésta técnica es uno de los mensajes que eran enviados por espías alemanes durante la Segunda Guerra Mundial:



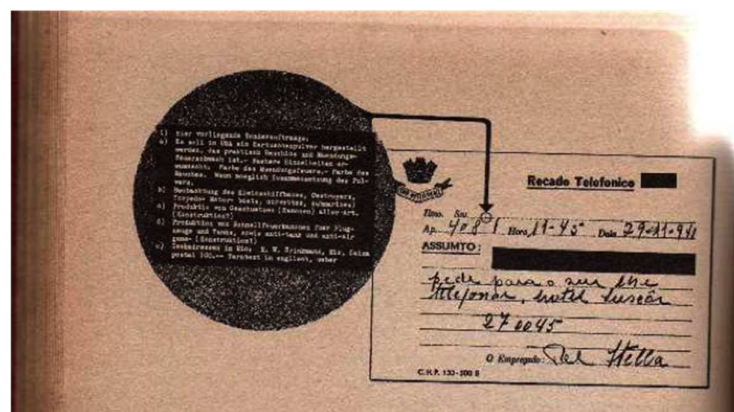
“Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by products, ejecting suets and vegetable oils.” (Master, 2004)

Si se extrae la segunda letra de cada palabra, obtendremos el mensaje que realmente ocultaron:

*Pershing sails from NY June 1.*  
 “Pershing navega desde Nueva York”

## Micropuntos

La tecnología de los Micropuntos fue usada durante la guerra fría y fue inventada por los alemanes. Esta técnica se basa en esconder puntos minúsculos en fotografías, tan pequeños que para el ojo humano e incluso para instrumentos ópticos básicos como lupas resultan invisibles, pero que forman un patrón de información significativa (Yúbal, 2015). Como se observa en la Figura 2 debido a la naturaleza analógica de esta técnica, resultaba fácilmente detectable para los servicios de inteligencia, pero a veces no siempre podían ser totalmente legibles.



**Figura 2** Recado Telefónico donde fue aplicada la Técnica de Micro puntos

**Fuente:** (Yúbal, 2015)

## **Esteganografía Digital**

En 1985 nace la esteganografía moderna junto con los avances tecnológicos en los ordenadores, Barrie Morgan y Mike Barney dos ingenieros empleados de una pequeña empresa estadounidense “Datotek” (empresa desarrolladora de equipos y software informáticos), aceptaron el reto de poder enviar información de forma segura a través de canales limitados de comunicación.

Durante años sus investigaciones crearon varios modelos esteganográficos, los desafíos y problemas que tuvieron que superar fueron el punto de partida para mejorar las herramientas modernas de ocultación de mensajes. Varios métodos existentes para ocultar información usan archivos digitales como imágenes, audio y vídeo, entre los más conocidos son el enmascaramiento y filtrado a través de marcas de agua en imágenes, los algoritmos y funciones matemáticas, y la inserción de información en el bit menos significativo de cada pixel ya son técnicas más estudiadas. (Tejada & García Dominguez, 2016)

### **2.4 Esteganografía terminología**

Del vocablo griego *steganos*, que significa encubierto con el sentido de oculto, y *graphos*, que significa escritura, nace el término esteganografía como una ciencia de ocultar mensajes en un objeto portador. El objeto portador puede ser cualquier contenido multimedia como imágenes, videos, audios, en este trabajo se enfoca el uso de imágenes ocultas sobre audios portadores.

Según la Real Academia Española la criptografía es conocida como el arte de escribir de forma enigmática, mientras que la esteganografía es el arte de escribir de forma oculta. La criptografía se basa en la imposibilidad de comprender el mensaje, en la esteganografía se desconoce totalmente la existencia de un mensaje. Ambas técnicas son distintas e independientes, pero pueden complementarse entre ellas para asegurar la información.

## Sistema Esteganográfico

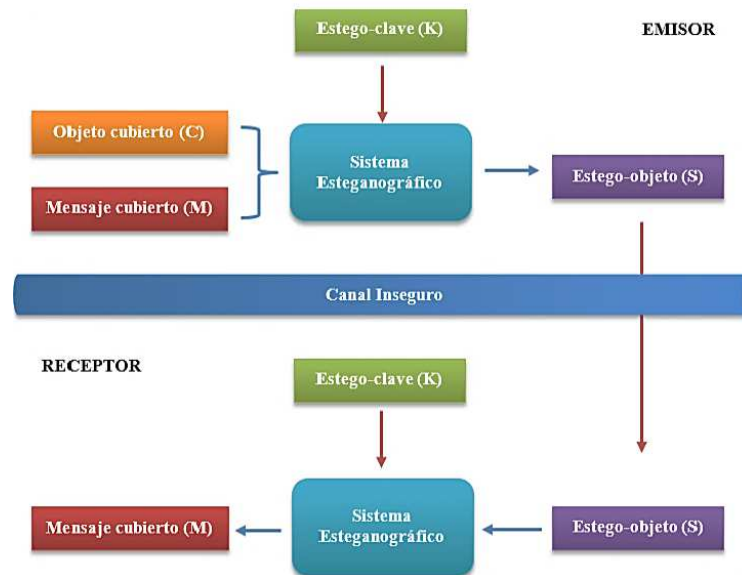
Un modelo esteganográfico se fundamenta en dos elementos básicos de un sistema de comunicación: emisor y receptor como se observa en la *Figura 3*, donde el emisor escoge un anfitrión, el cual puede ser transmitido por diferentes sistemas de comunicación sin levantar sospecha. (Checa, 2014)

Para entender mejor un sistema esteganográfico se detalla algunos elementos básicos:

- **Archivo encubridor o portador:** Es el archivo base donde se incrusta la información o mensaje oculto.
- **Mensaje oculto:** Son los datos secretos que se ocultan en el portador.
- **Algoritmo de ocultación:** Es el método esteganográfico que se implementa para ocultar la información secreta.
- **Archivo con esteganografía:** El archivo que contiene el mensaje secreto ya oculto en el portador.
- **Atacante:** Entidad que tiene por objetivo obtener la información secreta de manera ilegal.
- **Seguridad:** Herramientas usadas en el sistema esteganográfico para asegurar sus recursos.

Cuando seleccionamos un archivo portador, en el caso de esta tesis un audio, se selecciona una imagen que representa al mensaje secreto el cual será incrustado en el portador usando un algoritmo esteganográfico, para dar mayor seguridad al proceso de ocultamiento se asigna una clave que irá oculta junto con la información de la imagen secreta. Este archivo con esteganografía es enviado por algún sistema de comunicación emisor-receptor como se observa en la *Figura 3*.

Cuando el destinatario recibe el archivo esteganográfico, se realiza el proceso de recuperación de la imagen siempre y cuando conozca el método esteganográfico implementado y la clave correcta. La clave colocada no es siempre necesaria, pero debido a que existen varios atacantes y en la actualidad diversidad de software de estegoanálisis se recomienda adicionarla al mensaje para no ser descubierto o robado.



**Figura 3** Modelo General de un Sistema Esteganográfico

**Fuente:** (Rodríguez Mendoza, 2016)

Como se observa en el ejemplo de la Figura 4, se muestra un sistema esteganográfico usando imágenes como archivos portadores y archivos de texto como mensajes secretos, además que se inserta una contraseña de seguridad para hacer más robusta la transmisión del archivo esteganográfico final, mostrando claramente su estructuración y procedimiento de inserción y recuperación de la información.

### Características de un sistema esteganográfico

1. **Capacidad:** Es el número de bits que se puede esconder dentro del mensaje anfitrión.

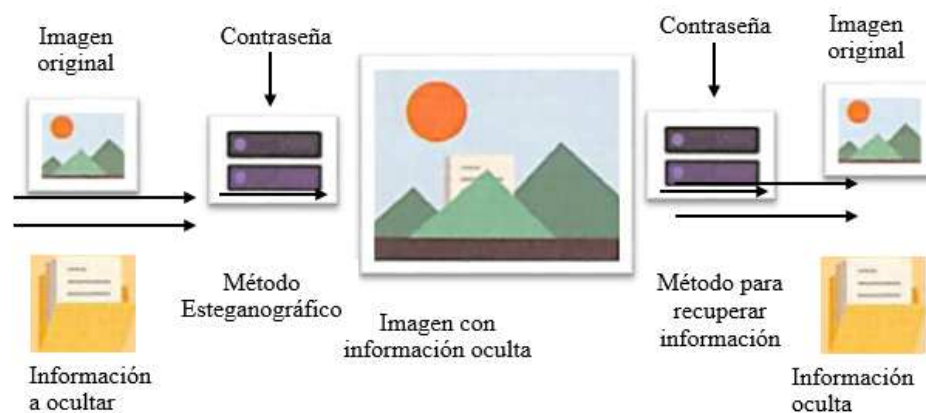
2. **Robustez:** Es la capacidad del sistema para poder someterse a diferentes escenarios ya sean adición de ruido, escalado, transformaciones, etc., sin perder el mensaje secreto escondido en el anfitrión.
3. **Invisibilidad:** Es la capacidad de que el mensaje secreto pase sin ser detectado en diferentes tipo de análisis.
4. **Seguridad:** Es la capacidad de que el mensaje secreto se enfrenta a diferentes ataques y que se encuentre libre de peligros y de riesgos. (Orbegozo, 2011)

## 2.5 Técnicas de Esteganografía

A continuación se presentan las diversas técnicas que favorecen la utilización de la esteganografía en varios ambientes. Algunos de los enfoques más conocidos de las técnicas que manejan con imágenes, audios y texto son la técnicas de inserción en el bit menos significativo - LSB, técnica de filtraje y enmascaramiento, algoritmos y transformaciones alemanas del esparcimiento por espectro, audio y video. (Cantanhede, 2009)

### *Esteganografía en imágenes*

En (Hamid, Yahya, Ahmad, & Al-Qershi, 2012) se describen seis técnicas existentes para la esteganografía en imagen las cuales a continuación se describen.



**Figura 4** Diagrama básico del proceso de esteganografía mediante imágenes.

**Fuente:** (Tejada & García Domínguez, 2016)

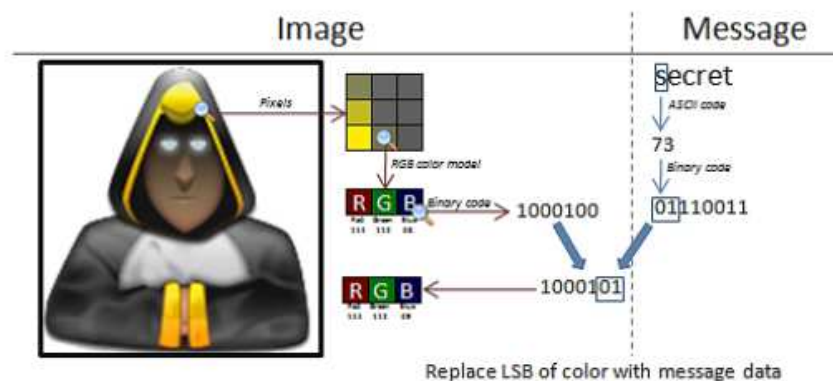
### 2.5.1 Esteganografía en el dominio espacial

Este tipo de esteganografía son muy usadas por su baja complejidad ya que incrustan la información secreta sustituyendo las partes insignificantes del objeto, directamente embebida en los valores de los pixeles de la imagen, es decir, se modifica ligeramente los pixeles para ocultar un mensaje.

#### A. Algoritmo de sustitución del Bit Menos Significativo (LSB)

LSB es el algoritmo esteganográfico más sencillo, su funcionamiento consiste en sustituir el bit menos significativo de la codificación de un pixel de una imagen o una muestra de audio por el bit del mensaje secreto a oculto, sin alterar el archivo portador.

El proceso LSB inicia transformando del mensaje secreto en un flujo de bits, a la imagen denominada portador se convierte en una matriz de bits, 8 bits para cada pixel de imágenes en escala de grises y 24 bits para imágenes RGB. En la Figura 5 se puede observar como los bits del mensaje son incrustados en el último bit de cada pixel RGB de la imagen. Esta técnica ofrece gran capacidad de incrustación de bits, los cambios realizados en la imagen portadora es mínima por lo que no es perceptible visualmente, sin embargo ya que la técnica es susceptible a detecciones con estego-analizadores, pérdidas de información ya sea por compresiones o recortes de la imagen portadora. (Onofre, 2016)



**Figura 5** Técnica LSB implementada en imágenes RGB

Con el objetivo de pasar desapercibidos y evitar la pérdida de información se desarrolló una mejora de la técnica usando el método *LSB matching* que funciona básicamente como LSB pero en lugar de sustituir el bit menos significativo se lo modifica cuando no coincide con el bit a ocultar. *LSB matching* entrega una imagen con bits embebidos que visualmente son imperceptibles y menos detectables estadísticamente. (Onofre, 2016)

Existen varios algoritmos basados en la técnica *LSB matching* entre los cuales se encuentran: *LSB Matching Revisited* (Mielikainen, 2006), *Lossless data hiding scheme based on lsb matching* (Quan & Zhang), *Very fast watermarking by reversible contrast mapping* (Coltuc & Chassery, 2007), entre otros.

### ***B. Diferencia de valores de pixeles***

Basándose en la vista de los seres humanos y tomando en cuenta que la misma es más sensible a variaciones de la imagen en zonas lisas mientras que en los bordes es más difícil que se detecte visualmente una alteración de cualquier imagen; se presenta la técnica llamada *Pixel Value Differencing* (PVD) la cual consiste en dividir a la imagen portadora en bloques de dos pixeles consecutivos para después evaluar la diferencia entre ellos y así poder determinar el número de bits que se pueden ocultar en el par de pixeles. En los bloques ubicados en los bordes de la imagen existe mayor diferencia entre pixeles, es aquí donde se tiene mayor capacidad de incrustación de bits, y cuando el área es de tipo lisa la diferencia se acerca a 0 y la capacidad para ocultar bits es muy baja. La principal ventaja es su baja susceptibilidad ataques comparada a LSB, sin embargo su principal desventaja es su alto nivel de procesamiento. (Onofre, 2016)

Una variación de esta técnica es la presentada en *Reversible Watermarking by Difference Expansion* (Tian, 2002) y en (Lerch Hostalot & Megías, 2014) donde se usa el principio de la diferencia de pixeles para clasificarlos como aptos para embeber información o no mediante la designación de un umbral y aquellos valores de

diferencia mayores al umbral indican que los píxeles pertenecen a zonas ruidosas por lo que son útiles para ocultar bits. (Onofre, 2016)

### ***C. Modificación de niveles de grises***

La ventaja que presenta este método es una gran capacidad de incrustación y una baja complejidad de procesamiento. La información secreta se incrusta realizando un mapeo del mensaje y luego se modifica el valor de los niveles de grises en los píxeles de las imágenes portadoras. Para ello se usan los números pares e impares y se selecciona mediante funciones matemáticas ciertos bits dentro de la imagen, los cuales se comparan posteriormente con el flujo de bits mapeado en la imagen. (Onofre, 2016)

### ***D. Esteganografía basada en la textura***

Esta técnica es muy utilizada cuando tanto el archivo portador como el mensaje son de tipo imagen. Su funcionamiento se basa en la sustitución de bloques de píxeles, consiste en dividir la imagen portadora y la imagen secreta en pequeños bloques del mismo tamaño. Cada bloque de la imagen secreta se asigna un patrón de textura y se compara con los bloques de la imagen portadora donde el objetivo es encontrar el más similar para reemplazarlo, creando finalmente una nueva imagen con la menor distorsión posible (Tiwari, Yadav, & Mittal, A Review on Different Image Steganography., 2014).

### ***E. Esteganografía basada en bordes***

Su funcionamiento se basa en la técnica *LSB*, aunque la información no se oculta en todos los píxeles de la imagen sino únicamente en aquellos que pertenecen a bordes. Es una de las técnicas menos usada debido a que su capacidad de incrustación de bits es baja, actualmente los 3 bits menos significativos son modificados de cada píxel.



### ***F. Ventajas y desventajas de técnicas del dominio espacial***

Se puede observar claramente las ventajas y desventajas de las técnicas en el dominio espacial (Onofre, 2016).

Entre las principales ventajas se encuentran:

- Gran capacidad de incrustación
- Menor degradación de la calidad de la imagen original
- Bajo procesamiento matemático

Entre las desventajas se encuentran:

- Susceptibilidad a pérdidas de información por manipulación de la imagen
- Más vulnerabilidad a ataques sencillos

#### **2.5.2 Esteganografía en el dominio de la transformada**

Método que ocultan la información secreta en un área significativa de la imagen que sirve como cubierta lo que los hace más robustos a ataques como compresión o adición de ruido. (Rodríguez Mendoza, 2016)

A diferencia de las técnicas usadas en el dominio del espacio, aquí la información secreta no se oculta directamente en el valor de los píxeles. Las imágenes son transformadas al dominio de la frecuencia, dominio wavelet, se incrusta la información secreta y posteriormente se puede volver a transformar al dominio del espacio. Un componente de la transformada puede abarcar varios píxeles de la imagen e incluso toda la imagen por lo que tiene la ventaja de mayor capacidad de incrustación y es más robusta ante pérdidas de información por recortes o compresiones de la imagen original. Pero es un tipo de técnica con una alta complejidad y mayor procesamiento matemático. (Onofre, 2016)

### **2.5.3 Esteganografía Spread Spectrum**

Esta técnica modula una señal de banda estrecha con una señal de banda ancha mediante un generador de ruido pseudo-aleatorio (técnicas spread spectrum). La señal modulada resultante se añade a la imagen portadora creando una estego-imagen robusta ante la detección y extracción (Tiwari, Yadav, & Mittal, A Review on Different Image Steganography., 2014, January).

De esta manera decrece la intensidad de la señal logrando una muy parecida al ruido, este procedimiento proporciona una alta calidad de la imagen, robustez ante ataques y su gran capacidad de incrustación de bits. (Onofre, 2016)

### **2.5.4 Esteganografía adaptativa**

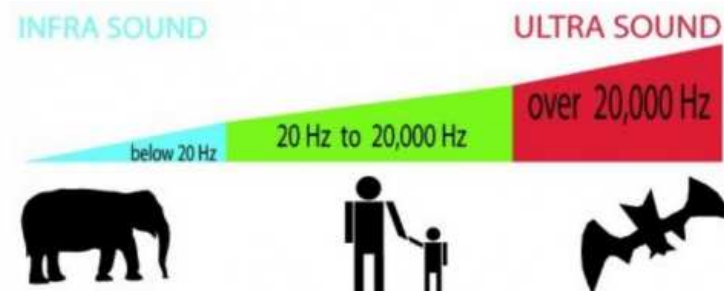
Esta técnica usa las características estadísticas de la imagen portadora, por lo cual también se la conoce como esteganografía basada en la estadística. La principal ventaja de este tipo de esteganografía es que no cambia las propiedades de la imagen con una distorsión visual insignificante para el sistema visual humano. (Onofre, 2016)

Existen dos métodos: seleccionar los píxeles adaptativos al azar dependiendo de la imagen portadora y seleccionar los píxeles con mayor desviación estándar en la imagen (Tiwari, Yadav, & Mittal, A Review on Different Image Steganography., 2014)

### ***Esteganografía en audios***

El oído humano es extremadamente sensible al cambio en los patrones del audio, la Figura 6 muestran los rangos de frecuencia audible, teniendo por debajo los infrasonidos y por encima los ultrasonidos. Para que los humanos puedan percibir un sonido, este debe estar comprendido en un rango de audición de 20 Hz a 20000Hz.

Al ocultar información en un archivo de tipo audio, un aspecto importante es conocer el medio por donde se va a transmitir el mensaje, puesto que no es lo mismo entre medios digitales o a través del medio ambiente físicos como bocinas.



**Figura 6** Rangos de Frecuencia audibles

**Fuente:** (Sonido: Características Físicas, 2016)

(Corona, 2015) Expone cuatro técnicas para ocultar información dentro de un fichero de sonido las cuales se detallan en la Tabla 1:

**Tabla 1**

*Clasificación de Técnicas Esteganográficas para archivos tipo audio*

<b>Técnica Esteganográfica</b>	<b>Funcionamiento</b>
<b>Codificación Low-Bit</b>	Esta técnica tiene un proceso de ocultamiento de bits similar a LSB que se usa en esteganografía con imágenes. Cuando se oculta cualquier tipo de información en un archivo de audio, ambos deben ser convertidos en binario para intercambiar los bits menos significativos del audio por los bits de la información secreta. Es importante que al trabajar con archivos tipo audio.wav los bits de cabecera no deben ser alterados ya que esta es la información más importante del audio, como la identificación del formato RIFF (Formato de Archivo de Intercambio de Recursos).
<b>Spread Spectrum</b>	Este método añade ruido aleatorio para ocultar la información

continua →

---

	final, desapercibida a la perfección. Oculta mensajes de baja señal dentro de otro mensaje de señal más alta. (Rodríguez Mendoza, 2016)
<b>Echo Data Hiding</b>	Este método usa el eco de un fichero de sonido para ocultar en éste información secreta. El eco se varía en tres parámetros: Amplitud Inicial, Offset, Decay Rate.
<b>Máscara perceptual</b>	Usa un sonido para ser ocultado tras otro de la misma frecuencia, debido a esta similitud en frecuencias, el sonido llega a ser imperceptible al oído humano.

---

Fuente: (Rodríguez Mendoza, 2016)

### **Criptografía y Esteganografía**

La criptografía ofrece distintos métodos y técnicas para afrontar el concepto de la confidencialidad, realiza una transformación del mensaje para hacer su significado ilegible ante ataques maliciosos. Por otro lado, en la esteganografía no se altera la estructura del mensaje secreto, en su lugar se oculta dentro de un portador. (Rodríguez Mendoza, 2016)

A continuación en la Tabla 2 se realiza una breve descripción de algunas características de estas dos técnicas, diferenciando los métodos aplicados entre ellas:

**Tabla 2**

*Tabla comparativa de técnicas Esteganográficas y Criptográficas*

<b>Características</b>	<b>Esteganografía</b>	<b>Criptografía</b>
<b>Método Aplicado</b>	LSB, Dominio espacial, Dominio Espectral.	Transposición. Substitución, RSA.
<b>Identificación a Simple Vista</b>	No, el mensaje es oculto en otro portador.	Sí, el mensaje es transformado para hacer ilegible. continua →

---

<b>Capacidad</b>	Difiere de las diferentes tecnologías su capacidad de ocultamiento.	Es alta, puesto que el mensaje requiere largos procesos de descifrado.
<b>Detección</b>	No es fácil de detectar, ya que para encontrar el contenido esteganográfico es difícil.	No es fácil de detectar, depende de la tecnología utilizada para generarse.
<b>Fortaleza</b>	Oculto el mensaje sin alterar el mismo, encubriendo la información.	Oculto el mensaje alterando éste, mediante la asignación de una clave
<b>Imperceptibilidad</b>	Alta	Alta
<b>Aplicabilidad</b>	Universal	Universal
<b>Robustez</b>	Sí	Sí

Fuente: (Rodríguez Mendoza, 2016)

## 2.6 Formatos de audio digital

El audio digital es la representación de señales sonoras mediante un conjunto de datos binarios. Un sistema completo de audio digital comienza habitualmente con un transceptor (micrófono) que convierte la onda de presión que representa el sonido a una señal eléctrica analógica. Tras el procesado analógico la señal se muestrea, se cuantifica y se codifica. (López Martín, 2015)

Los formatos de audio digital representan un conjunto de muestras digitales de la señal eléctrica analógica receptada, optimizando funcionamiento dependiendo la aplicación. Es importante tomar en cuenta que dichas muestras de audio tienen parámetros básicos que describen el sonido que representan son:

- **El número de canales:** 1 para mono, 2 para estéreo, 4 para el sonido cuadrafónico, etc.

- **Tasa de muestreo:** El número de muestras tomadas por segundo en cada canal.
- **Número de bits por muestra:** Habitualmente 8 o 16 bits.

En el presente trabajo se utilizar archivos de audios como portadores de la información secreta, es por esto, que es importante realizar un breve estudio de los formatos de audio digitales existentes explicando las ventajas que presenta cada uno con sus parámetros y composición.

(Cantanhede, 2009) Utiliza la esteganografía en audio e imagen con técnica LSB, en audio realiza una breve explicación de la técnica, sin embargo realiza una implementación sobre imágenes RGB.

(Casierra, 2009) Implementa un sistema esteganográfico insertando textos en señales de audio, realiza un breve estudio sobre frecuencias de audio del oído humano y evalúa la técnica implementada.

Otra de las investigaciones base para la realización de este trabajo es (Rodriguez, 2016) desarrollado en la Universidad de las Fuerzas Armadas Espe, donde implementa la técnica LSB para transmitir textos en archivos de audio mediante la utilización de una aplicación desarrollada en la plataforma Matlab, donde brinda información importante de cómo se tratan los archivos de audios digitales, su estructuración y técnicas para lograr que los cambios sean imperceptibles al oído humano.

Cuando se inició la digitalización del audio aparecieron variedad de formatos de audio donde cada sistema trataba un formato distinto. Los formatos de fichero muestran la estructura con la que el audio es almacenado. Cada vez aparecieron formatos más flexibles y eficientes, llegando a la actualidad donde se dividen en dos grupos, unos pocos usados de forma masiva y otros de usos muy reducidos.

***Los archivos de sonido con pérdida.***- Son aquellos que usan un algoritmo de compresión, permiten que la información ocupe menos espacio. Está representada por

menos cantidad de información esto hace que sea imposible reconstruir exactamente la información original del archivo. Estos métodos de compresión con pérdida son aplicados en la digitalización de en información, imágenes, audio, vídeo etc.

***Los archivos de sonido sin pérdida.***- Son aquellos que representan la información sin intentar utilizar menor cantidad de datos originales. Es posible un proceso de reconstrucción exacta del audio original. Pueden usar o no métodos de compresión.


### 2.6.1 WMA

Windows Media Audio es un formato de archivos de sonido con pérdida, desarrollado básicamente para el reproductor integrado en Windows, es muy parecido a MP3 pero también existe una versión sin pérdidas. Sin embargo a diferencia de los MP3, WMA posee una infraestructura para proteger el Copyright y así hacer más difícil el "tráfico P2P" (red de pares) de música.

Reduce el tamaño de archivos grandes, adapta a diferentes velocidades de conexión en caso de que se necesite reproducir en Internet en Tiempo Real (Romero García & Teran Figueroa, 2011). La Tabla 3 presenta las características principales de WMA:

**Tabla 3**

*Características del Formato WMA*

<b>Tipo de Audio</b>	<b>Características</b>	
	<b>Desarrollador</b>	Microsoft
	<b>Extensión</b>	.wma
	<b>Canales</b>	Estéreo, Mono
	<b>Frecuencia de muestreo</b>	48000 Hz, 44100 Hz

### 2.6.2 MP3

El formato MP3 nace a partir de la necesidad de los usuarios de intercambiar música por Internet, llegando a ser uno de los formatos más populares ya que puede almacenar hasta 100 archivos en un disco CD.


Es un formato de audio digital estándar de tipo audios con pérdida, ya que elimina el rango de frecuencias que el oído humano no escucha como se observó anteriormente en la Figura 6, es por esto, que la pérdida de información no es percibida por el oído humano. Una de sus principales ventajas es la versatilidad que tiene el formato mp3, ya que pueda ser reproducido en casi todos los reproductores de audio, su compatibilidad con todos los medios es garantizada y almacena música con buena calidad.

El formato de audio Mp3 permite seleccionar la calidad del audio que vamos a comprimir, la calidad de cd sería equivalente a 128 Kbps (Bit rate), pero podemos seleccionar la compresión entre los 8 Kbps y los 320 Kbps teniendo en cuenta que cuanto mayor sea la transmisión de datos (Kbps), mayor espacio ocupará el archivo. (Bousono, 2010)

En la Tabla 4 menciona algunas características:

**Tabla 4**

*Características del formato MP3*

Tipo de Audio	Características	
	<b>Desarrollador</b>	Microsoft
	<b>Extensión</b>	.mp3
	<b>Canales</b>	Estéreo, Mono
		Continua →



---

**Frecuencia de muestreo**    48000 Hz,44100 Hz

---

Fuente: (Rodríguez, 2016)

### 2.6.3 WAV

WAV o conocido como Microsoft Waveform, es uno de los más importantes formatos actualmente gracias a sus creadores Windows e IBM en 1995. Sus ventajas es la calidad de sonido bastante buena al ser grabado en 8 o 16 BYTES y sus múltiples aplicaciones en Multimedia. Sin embargo, su principal desventaja es que ocupa demasiado espacio para unos cuantos segundos de sonido.

El formato RIFF (Resource Interchange File Format) es un formato Windows para almacenar segmentos (chunks) de información multimedia, su descripción, formato, lista de reproducción, etc. El formato .WAV (WAVEform Audio File Format) se almacena dentro de un fichero con formato RIFF, definiendo unos segmentos concretos que puede contener. Por lo tanto es adecuado ver el formato general de un fichero RIFF y qué segmentos se definen para los ficheros .WAV. (López Martín, 2015)

Un archivo de Formato WAV está compuesto de las siguientes partes como se detalla en la Tabla 5:

**Tabla 5**

*Estructura del Formato WAV*

<b>Nombre del Campo</b>	<b>Tamaño del Campo (Bytes)</b>	<b>Descripción</b>
<b>ChunkID</b>	4	Formato WAV está
<b>ChunkSize</b>	4	compuesto de 2 partes:
<b>Format</b>	4	Formato y Datos.
<b>SubChunk1 ID</b>	4	Contiene la descripción del
<b>SubChunk1 Size</b>	4	sonido en los datos.
<b>AudioFormat</b>	2	Continúa →

<b>NumChannels</b>	2	
<b>SampleRate</b>	4	
<b>ByteRate</b>	4	
<b>BlockAling</b>	2	
<b>BitsPerSample</b>	2	
<b>SubChunk2 ID</b>	4	
<b>SubChunk2 Size</b>	4	Contiene El tamaño y los datos del archivo de audio
<b>Data</b>	SubChunk2Size	

Fuente: (Rodríguez, 2016)

La Tabla 6 presenta una breve descripción de cada uno de los campos que componen la cabecera de un archivo tipo WAV:

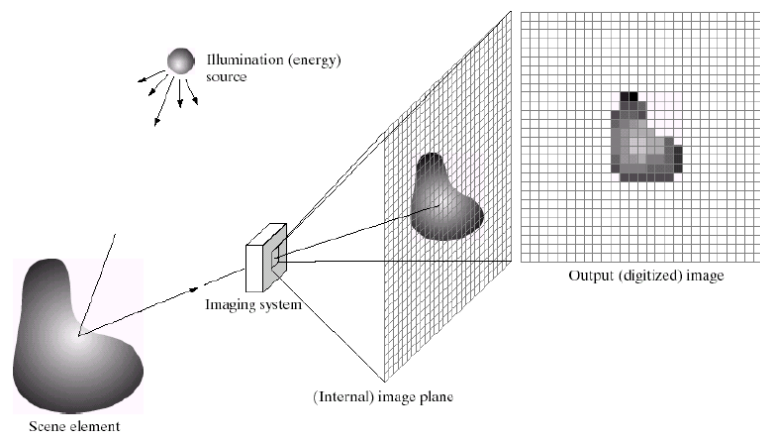
**Tabla 6**

*Descripción de Cabecera WAV*

<b>Nombre del Campo</b>	<b>Descripción</b>
<b>ChunkID</b>	Contiene RIFF en ASCII (52 49 46 46)
<b>ChunkSize</b>	36 + SubChunk2Size
<b>Format</b>	Contiene WAVE en ASCII (57 41 56 45)
<b>SubChunk1 ID</b>	Contiene fmt en ASCII (66 6D 74 20)
<b>SubChunk1 Size</b>	16 para PCM (modula la señal)
<b>AudioFormat</b>	PCM =1 (Identificador de PCM)
<b>NumChannels</b>	Mono=1, Stereo=2
<b>SampleRate</b>	8000,44100,etc.
<b>ByteRate</b>	$\text{SampleRate} * \text{NumChannel} * \text{BitsPerSample} / 8$
<b>BlockAling</b>	$\text{NumChannel} * \text{BitsSample} / 8$
<b>BitsPerSample</b>	8 bits=8; 16 bits=16; etc.
<b>ExtraParamSize</b>	Si está en PCM, este campo no existe.
<b>ExtraParams</b>	Para parámetros extra
<b>SubChunk2 ID</b>	Contiene DATA en ASCII (64 61 74 61)
<b>SubChunk2</b>	$\text{NumSample} * \text{NumChannels} * \text{BitsPerSample} / 8$
<b>Data</b>	Data del sonido

## 2.7 Imágenes Digitales

Actualmente para que una imagen analógico de cualquier tipo pueda ser manipulada por un ordenador debe ser convertirse a un formato adecuado, ahí nace la digitalización de imágenes. Este procedimiento de digitalización de imágenes se los realiza desde que se captura la señal luminosa mediante cualquier tipo de instrumento óptico, muestreo, cuantificación y codificación.



**Figura 7** Ejemplo de un Proceso de digitalización de imágenes

**Fuente:** (Sánchez Tirado, 2006)

El proceso consiste en dividir la imagen en pequeñas regiones llamadas píxeles o puntos, como se observa en la Figura 7 utilizando un esquema de subdivisión de cuadrícula rectangular más usado en el procesamiento de digital de imágenes. Cada punto de la matriz de valores de la imagen identifica el nivel de gris en ese punto. Los bits representan la intensidad de cada posición de la imagen, el color negro se representa mediante ceros, y la intensidad de blanco se representa por unos.

Al tratar con imágenes digitales es importante conocer las dimensiones de las imágenes, la Tabla 7 describe cada uno de ellos:

**Tabla 7***Dimensiones de Imágenes Digitales*

<b>Dimensiones</b>	<b>Características</b>
<b>Tamaño del Archivo</b>	Es la cantidad de memoria que ocupa una imagen en KB, MB, etc.
<b>Resolución de una imagen</b>	Es la cantidad de píxeles que describen a una imagen. Esta se mide en dpi=dots per inch o puntos por pulgada (ppp). Se usan para conocer la resolución de una escaneado o impresión de archivo.
<b>Resolución de bits</b>	Resolución o Profundidad de bits, es una cantidad de información que puede ser almacenada dentro de un bits: <i>1 bit:</i> Blanco / Negro <i>8 bits:</i> 256 colores <i>24 bits:</i> 16 000 000 colores

Fuente: Cristina Bastidas

**Clasificación de imágenes**

Por Dimensión:

**2.7.1 Imágenes 2D y 3D****Imágenes 2D**

Las imágenes en dos dimensiones se refieren a imágenes digitales cuadradas o rectangulares cuyas coordenadas de cada píxel es  $(x, y)$  filas y columnas respectivamente. Existen tres tipos básicos de imágenes en dos dimensiones que se presentan a continuación:

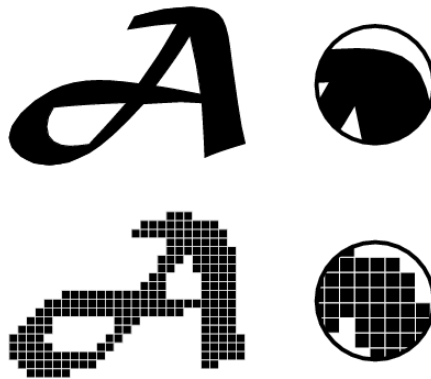
- **Imágenes de Mapa de Bits**

Conocidas también como BitMap o Imágenes Rraster, la Figura 8 presenta estas imágenes que están formadas por una cuadrícula o rejilla de puntos o píxeles. Cada pixel tiene asignado un valor de color y luminancia, creando así la ilusión de una imagen de tono continuo. Dependiendo de la paleta de colores el número de bits que se necesitan para definir cada píxel aumenta, mejorando la calidad de la imagen digital.

- **Imágenes Vectoriales**

Las imágenes vectoriales son representadas por fórmulas matemáticas pertenecientes a figuras geométricas tales como círculos, rectángulos o segmentos, por un círculo se forma por un centro, un radio y una ecuación como se observa en la Figura 8. El procesador convierte estas figuras geométricas en información matemática para que la tarjeta gráfica pueda interpretar. Conocidas también como Clipart las imágenes vectoriales permiten procesar archivos con muy poca información.

Una imagen vectorial está compuesta directamente con entidades matemáticas, mismas que pueden aplicar fácilmente transformaciones geométricas a la misma (ampliación, expansión, etc.), sin embargo las imágenes de mapa de bits, no se pueden exponer a dichas transformaciones ya que sufren pérdida de información conocida como distorsión.



**Figura 8** Formatos de Imágenes 2D a) Imagen Vectorial b) Mapa de Bit

Los formatos más habituales para imágenes vectoriales son:

- *Corel Draw (CDR)*: Los gráficos realizados están compuestos por líneas y planos que se sitúan en unas coordenadas concretas en la página.
- *Adobe Illustrator (AI)*: Sus características en la forma son muy similares a las CDR.
- *Encapsulated Postscript (EPS)*: Es formato muy flexible ya que trabaja con imágenes vectoriales y mapa de bits. Es uno de los mejores formatos para ser importados desde la mayoría de software de diseño.

- **Metaformatos**

Son un tipo de imágenes 2D mixtas donde se la información puede ser almacenada de forma gráfica vectorial o como mapa de bis.

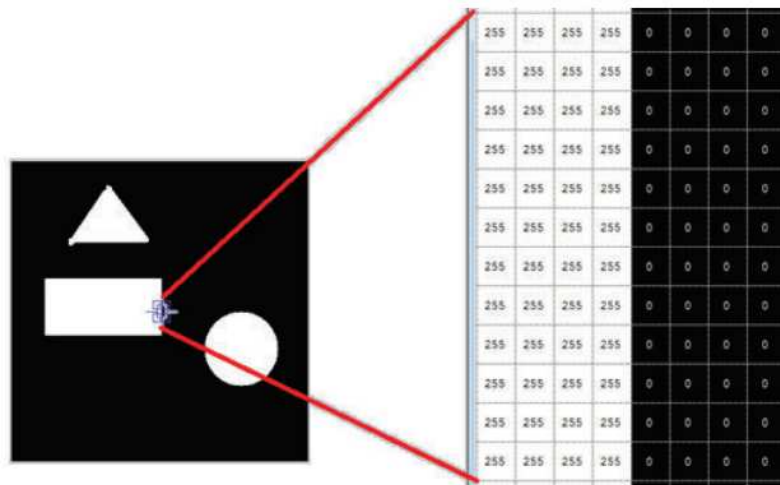
- BitMaps se usan los elementos fotográficos y las figuras irregulares
- Gráficos vectoriales los textos y dibujos

**Por Color:**

El modo de color de una imagen digital representa el número máximo de datos de color que se pueden almacenar, donde contiene la información sobre cada píxel de una imagen. Los principales modos de color utilizados en aplicaciones gráficas son:

### 2.7.2 Imágenes Binarias

Son imágenes que usan 1 bits por pixel para representar dos valores de color blanco o negro presentadas en la Figura 9. Debido a esto estas imágenes tienen un tamaño pequeño y no es posible trabajar con filtros ni capas.

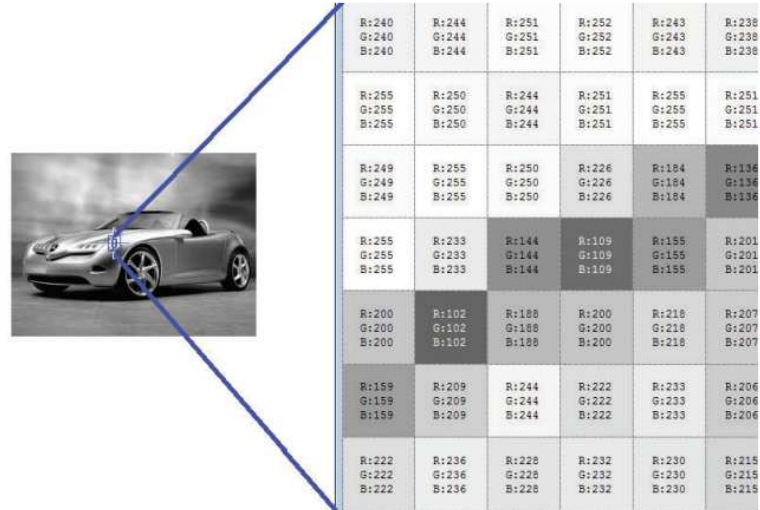


**Figura 9** Tabla de Píxeles de una Imagen Binaria

**Fuente:** (Cepeda Frías, 2016)

### 2.7.3 Imágenes a escalas de grises

En este caso las imágenes tienen 8 bits por cada píxel, donde el valor de 0 corresponde a Negro y el valor 255 es el color Blanco, estos dos colores van formando sombras grises para los valores intermedios como se observa en la Figura 10.



**Figura 10** Pixeles de una Imagen a Escala de Grises

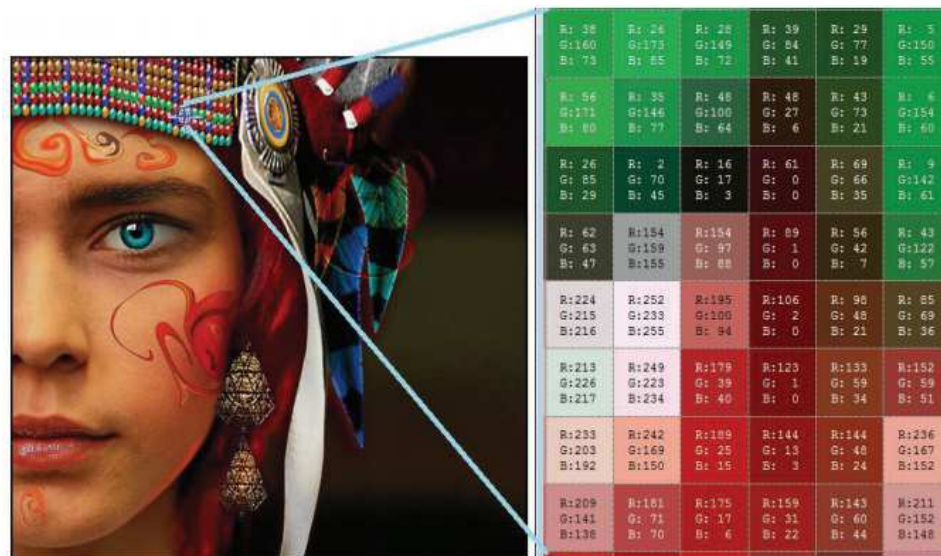
**Fuente:** (Cepeda Frías, 2016)

#### 2.8.4 Imágenes RGB a color

El Modelo de Color conocido como Rojo, Verde, Azul (RGB) mediante una combinación de una luz roja, verde y azul en diferentes proporciones genera los colores del espectro, por lo cual estos tres colores son conocidos como colores aditivos.

En un sistema RGB un pixel esta representa mediante la sintaxis decimal (R,G,B) o mediante la sintaxis hexadecimal #RRGGBB. En la Figura 11 se presenta un ejemplo done el color rojo puro especificará con un valor de (255,0,0) en notación RGB decimal y #FF0000 en notación RGB hexadecimal, mientras que el color rosa claro dado en notación decimal por (252,165,253) se corresponde con el color hexadecimal #FCA5FD. (Sánchez Tirado, 2006)

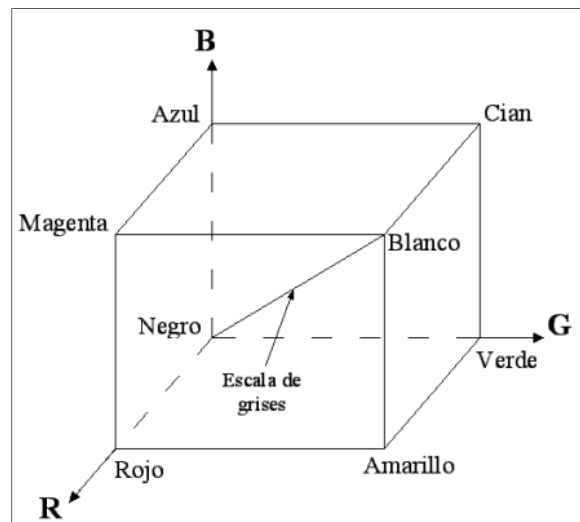




**Figura 11** Pixeles e una imagen RGB

**Fuente:** (Cepeda Frías, 2016)

El cubo RGB representa como se forman esta mezcla de tres colores. Como se observa en la Figura 12 cada uno de los ejes del cubo representa un color RGB, la proyección de un punto P contenido en el cubo sobre un eje indica la intensidad de luz con la que coopera el color de ese eje en la formación del color en ese punto (Jiménez Rosas, 2009).



**Figura 12** Cubo RGB

**Fuente:** (Jiménez Rosas, 2009)

Los valores que puede tomar cada componente del modelo RGB están determinados por el número de bits usado para representarlo, el cual, para imágenes fotográficas, es usualmente 8. Todos los modelos de color se pueden obtener a partir de la información que proporcionan dispositivos como escáners y cámaras, los cuales representan los colores utilizando el modelo RGB. (Jiménez Rosas, 2009)

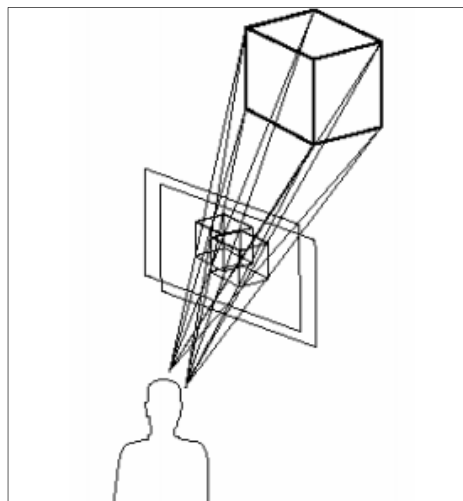
(Rodríguez Medina & Navas, 2015) Presenta una “Estudio, análisis, desarrolló y propuestas de algoritmos para la selección óptima de métodos de sustitución en aplicaciones esteganográficas”, donde trata imágenes RGB como portadores de información y se descomponen en Matlab en 3 planos de color, y así evaluar el comportamiento del algoritmo LSB implementado.

(Onofre, 2016) Presenta algo distinto, aquí se desarrolló un nuevo algoritmo de esteganográfico más robusta ante ataques estadísticos mediante la combinación de dos métodos: uno basado en transformaciones de color reversibles que modifican la imagen secreta a transmitir, para la obtención de un mosaico que luzca similar a una imagen portadora seleccionada previamente; y un método que busca las zonas más aptas (texturas y bordes) en el mosaico creado, para ocultar la información relevante requerida y recuperar la imagen secreta.

### **Imágenes 3D**

Para poder entender adecuadamente el concepto de Imágenes 3D, es importante definir el funcionamiento de la técnica conocida como Visión Estereoscópica remontándose al año 1838 donde el científico Charles Wheaststone describe este proceso como un acto innato de los seres humanos, que consiste en obtener una vista tridimensional de objetos percibidos mediante visión binocular. El cerebro humano es aquel que interpreta la realidad a partir de las imágenes que le proporcionan los ojos, sin embargo, existe una gran diferencia entre sí ya que por su separación, disparidad y paralaje entre las imágenes el cerebro percibe la profundidad como se detalla en la Figura 13.

El ojo humano funciona de manera análoga a una cámara fotográfica, así por ejemplo, la córnea se comporta como un filtro, el iris es el regulador de la intensidad de la luz, el cristalino actúa como lente y la retina se asimila a la película en la cual se forma la imagen. El conjunto de actividades realizadas por cada parte del ojo es lo que permite la formación de la imagen y el proceso de estereovisión se produce cuando el cerebro fusiona en una sola, la imagen recibida por cada ojo. (Cárdenas Quiroga, Morales Martín, & Ussa Caycedo, 2015)



**Figura 13** Visión Estereoscópica

**Fuente:** (Arévalo & Valencia, 2007)

## 2.8 Formatos de imágenes digitales

Poco a poco la compresión de imágenes se ha convertido en un área muy importante de aplicación investigativa y comercial, es así como comenzaron a desarrollarse una serie de estándares internacionales de compresión. Un estándar de compresión de imágenes principalmente permitir la interoperabilidad entre equipo y sistemas. Cada estándar describe una estructura para la representación de las imágenes comprimidas, el procedimiento para la descompresión y, posiblemente, un descompresor de referencia. En esta sección se describen los formatos archivos de imágenes GIF y PNG y los estándares de compresión JPEG y JPEG2000:

### 2.8.1 JPEG

Joint Photographic Experts Group conocido como JPEG fue formado en 1992 por miembros de la ISO (International Standards Organization) y la ITU-T (International Telecommunication Union), con el objetivo de crear un estándar de compresión de imágenes a color y en escala de grises.

JPEG permite la obtención de altas tasas de compresión cuando la calidad deseada de la imagen recuperada va de buena a muy buena, también permitir a los usuarios avanzados la manipulación de parámetros para lograr el equilibrio deseado entre tasa de compresión y calidad de la imagen y principalmente que el método de compresión no sea demasiado complejo para que pueda ser implementado tanto en software como en hardware en diferentes plataformas.

En la Tabla 8 se definen cuatro modos de operación en JPEG:

**Tabla 8**

*Modos de Operación de Imágenes JPEG*

<b>Modos de Operación</b>	<b>de Descripción</b>
<b>Modo Secuencial</b>	Realiza una compresión de cada componente del espacio de color de la imagen, mediante un barrido de izquierda a derecha y de arriba hacia abajo.
<b>Modo Progresivo</b>	Se comprime la imagen en varios barridos y al ser descomprimida con cada barrido se logra una imagen de mejor calidad.
<b>Modo Jerárquico</b>	Se comprime la imagen en varias resoluciones para que pueda ser ejecutada en diferentes dispositivos.
<b>Modo Sin Perdidas</b>	Se conserva una copia exacta de la imagen original, aunque

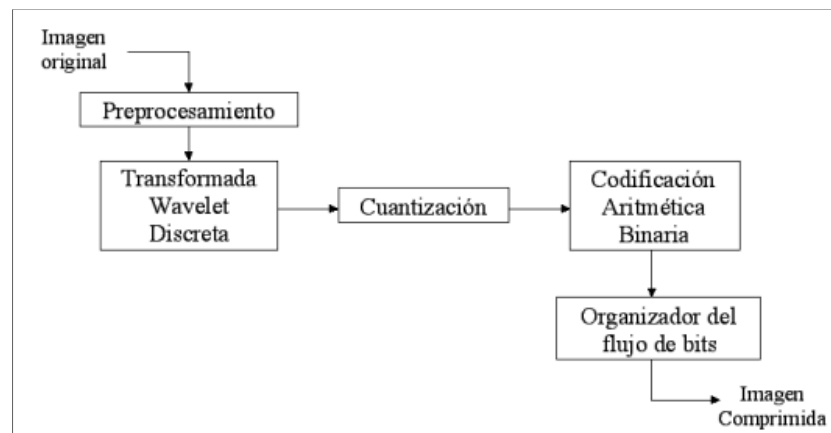
Continua →

la tasa de compresión no es tan buena como en la compresión con pérdidas. Sin embargo no se comprime tan bien como otros formatos que ya están disponibles como PNG.

Fuente: Cristina Bastidas

JPEG2000 es una mejora del formato de compresión anterior, este consta de once partes, la primera describe el sistema básico de compresión o núcleo en las modalidades de compresión con pérdidas y compresión sin pérdidas y las otras diez agregan características adicionales a la primera parte. (Morocho, Zambrano, Carvajal, & López, 2015)

La Figura 14 detalla el funcionamiento del Sistema de Compresión de JPEG2000, en la modalidad de compresión con pérdidas, sin embargo para compresión sin pérdidas es similar pero sin el bloque de Cuantización. Para el proceso de descompresión de la imagen se realiza siguiendo el diagrama de la Figura 14 en sentido inverso.



**Figura 14** Estructura de Compresión JPEG2000

Fuente: (Morocho, Zambrano, Carvajal, & López, 2015)

En (Morocho, Zambrano, Carvajal, & López, 2015) evalúa el algoritmo esteganográfico F5 para imágenes JPEG a color, determinando características de Invisibilidad, Robustez y Capacidad de Embebido en imágenes, comparado con el algoritmo LSB. Básicamente en este trabajo se ocultan una serie de bits de un mensaje

secreto dentro de coeficientes de la transformada discreta Coseno (DCT) de una imagen JPEG escogidas de manera aleatoria y emplea una matriz de embebido que minimiza el número de cambios necesarios para ocultar un mensaje de cierta longitud.

### **2.8.2 GIF**

Graphic Interchange Format o GIF es un formato de archivos gráficos comprimidos creado en 1987 por la compañía CompuServe Information Services. Básicamente comprime el número de colores o bits utilizando la técnica de compresión sin pérdidas LZW (Sánchez Tirado, 2006), que consiste en no detectar sólo las repeticiones de un color, sino en detectar las repeticiones de ciertas secuencias consiguiendo de esta forma reducir los archivos a un tamaño mucho menor que otros formatos.

La característica principal del GIF es que soporta paletas de 256 colores, y además de que soporta animaciones y transparencias. Esto no creará una distorsión de la imagen, como JPG, pero sí difuminará los colores bastante, haciendo que se vea ligeramente píxelado. Sin embargo, en una imagen GIF no se pierden líneas rectas como las del texto, como pasaría con un JPG.

### **2.8.3 PNG**

El formato de archivo PNG significa Portable Network Graphics, fue creado como una alternativa al formato GIF también se los conoce como PNG-not\_GIF.

Normalmente soporta transparencias a diferencia del GIF, maneja las transparencias con más elegancia y sin perder color porque soporta colores de 8-bits, y también de 24-bits, como JPG.

El PNG utiliza un algoritmo de compresión sin pérdida, por lo que reconstruye los datos de forma exacta a los originales. El problema con PNG es que si se tiene una imagen con muchos colores y píxeles, obtendremos un archivo más pesado que el JPG, por lo que no se usa con tanta frecuencia en la web.

Aunque GIF y PNG no son estándares de compresión, se mencionan debido a que al igual que los estándares, utilizan algunas de las técnicas de compresión descritas en las secciones anteriores. Mientras que GIF y PNG operan directamente sobre los píxeles y utilizan métodos de compresión sin pérdidas, JPEG y JPEG2000 pueden realizar compresión con pérdidas utilizando transformadas y Cuantificación.

La Tabla 9 detalla tres formatos de imágenes digitales y compara sus características más relevantes:

**Tabla 9**

*Tabla Comparativa entre Formatos Digitales de Imágenes*

	<b>JPG</b>	<b>GIF</b>	<b>PNG</b>
<b>Características</b>	Mapa de Bits Fotografías	Mapa de Bits Objetos Dibujados o Diseñados	Mapa de Bits
<b>Número de colores</b>	24 bits color 8 bits B/N	Hasta 256 colores	24 bits color
<b>Grado de Compresión</b>	Alto grado de compresión	de Formato de compresión	de Mayor compresión que el formato GIF (+10%)
<b>Admite Carga Progresiva</b>	Si	Si	Si
<b>Admite fondos transparentes</b>	No	Si	Si
<b>Permite Animación</b>	No	Si	No

Fuente: Cristina Bastidas

## 2.9 Aplicaciones de la Esteganografía

Siempre la esteganografía busca brindar seguridad en todos los ambientes, es por esta razón que las aplicaciones de la esteganografía orientada a la información digital y las comunicaciones se dividen en cuatro tipos:

- **Integridad y Autenticidad de los objetos**

Autenticidad consiste en identificar el origen o propietario real del objeto. El objetivo de estos procedimientos están orientados a garantizar la integridad de los objetos, detectar si han sido manipulados de algún modo.

Un ejemplo claro de este tipo de aplicación está en el campo de la Seguridad y Vigilancia frente a robots u otros delitos semejantes. Cuando una cámara de video registra las imágenes bajo vigilancia, es importante demostrar la autenticidad, usando métodos criptográficos como esteganográficos usando marcas de agua para detectar y localizar cambios realizados sobre la imagen real.

Las marcas de agua son técnicas esteganográficas que son insertadas en cualquier objeto, cuando sufre algún ataque o modificación el objeto las marcas son alteradas o se pierden completamente, evidenciando que la seguridad ha sido violada. Dependiendo de la robustez del procedimiento de verificación los tipos de marcas se clasifican en la Tabla 10:

**Tabla 10**

*Tipos de Marcas de Agua Esteganográficas según su robustez.*

<b>Marca de Agua</b>	<b>Descripción</b>
<b>Frágiles</b>	Su principal inconveniente es cuando la marca se destruye frente a ligeras manipulaciones.

Continua →



---

<b>Semifrágiles</b>	Sobreviven a un limitado tipo de manipulaciones y permite discriminar una alteración maliciosa y una intencionada consecuente de un proceso convencional.
<b>Robustas</b>	Primero se realiza un resumen a partir del objeto y los credenciales del autor usando por ejemplo funciones en un solo sentido. El resumen es insertado a modo de marca de agua robusta. Para verificar el procedimiento se compara la marca de agua extraída del objeto con un recalcu a partir del objeto original.

---

Fuente: Cristina Bastidas

- **Protección frente a copias ilícitas**

Otra de las aplicaciones de las técnicas esteganográficas es la protección de los derechos de propiedad intelectual donde las marcas de agua digitales son usadas actualmente. La existencia de equipos que permiten realizar copias de discos compactos han incrementado las ventas de discos de forma ilegal.

Al contrario de lo que sucede en las aplicaciones de autenticidad, en este caso los atacantes no desean manipular el objeto, sino eliminar la marca sin que ello repercuta negativamente sobre la calidad del objeto. Por esta razón, las marcas empleadas en este entorno son siempre marcas robustas.

- **Etiquetas, números de serie y huellas dactilares digitales**

En este caso las marcas de agua insertan tanto el origen como el receptor del objeto. El procedimiento consiste en números o datos de identificación únicos encubiertos en el objeto que se desea proteger y que permiten al poseedor de los derechos de propiedad intelectual, conociendo a identidad del cliente que violó el contrato o licencia de usos proporcionando el objeto a terceras partes. Los números de series son insertados de tal modo en el objeto que resulta imposible realizar una copia de serie.

Si se localiza una copia ilegal del objeto, inmediatamente se determina el cliente que cometió el delito. Con frecuencia los números de serie acompañan a programas informáticos y tienen como finalidad prevenir su distribución incontrolada. (España Boquera M. C., 2008)

- **Diferentes niveles de acceso a datos**

Consiste en proveer a los usuarios de múltiples niveles de acceso a la información. Estas técnicas pueden emplearse para crear canales ocultos de información complementaria accesibles sólo a determinados usuarios, ampliando de esta manera la cantidad de información transportada en los objetos. Por ejemplo, una película difundida en un canal de televisión digital podría incorporar bandas sonoras en múltiples idiomas. (España Boquera M. C., 2008)

## CAPÍTULO 3

### 3. DISEÑO DEL PROGRAMA

#### 3.1 Descripción general del programa

Para el desarrollo de la aplicación esteganográfica se buscó un entorno informático donde los archivos digitales (imágenes y audios) puedan ser manipulados de forma adecuada manteniendo su calidad y poder evaluar el algoritmo implementado obteniendo resultados más reales.

Matlab es un software matemático que ofrece todas esas características, es un entorno de desarrollo integrado con un lenguaje de programación propio (lenguaje M), que está disponible para las plataformas Unix, Windows y Apple Mac OS X. Permite manipular tanto vectores como matrices reales y complejas con funciones y fórmulas de variadas ramas de la matemática. Matlab se compone de un programa básico y un conjunto de *Toolbox* para labores más especializadas.

El programa parte con una pantalla principal como se observa en la Figura 15, donde se muestra información básica sobre el tema de trabajo y autor del programa, además de tres botones que direccionan a las siguientes pantallas:

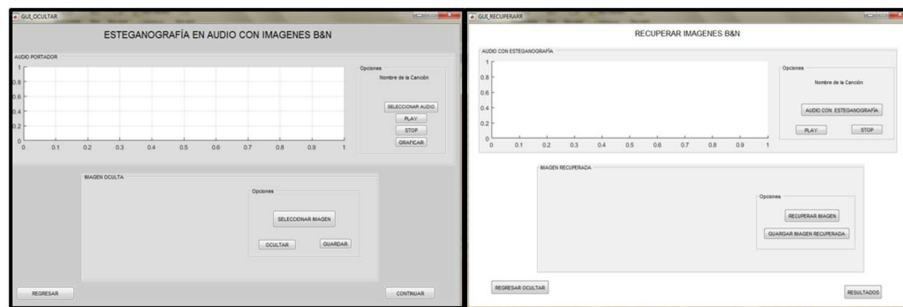
- *GUIDE OCULTAR B&N.*- para imágenes en Blanco y Negro-1canal
- *GUIDE OCULTAR RGB.*- para imágenes RGB-3 Canales
- *SALIR*



**Figura 15** Pantalla principal del Programa Esteganográfico

### 3.1.1 Ocultar Imágenes B&N

Al trabajar con imágenes en Matlab se presenta la ventaja de trabajar en forma de matricial, y dado que este software está orientado a aplicar toda su potencialidad de cálculo a las matrices, es que resulta una herramienta poderosa para la manipulación y procesamiento matemático; además de poder procesarse digitalmente las imágenes a través del *Toolbox de Procesamiento de imágenes* con el que cuenta (por ej. aplicar filtros, máscaras, etc.). (Rodríguez Medina & Navas, 2015)

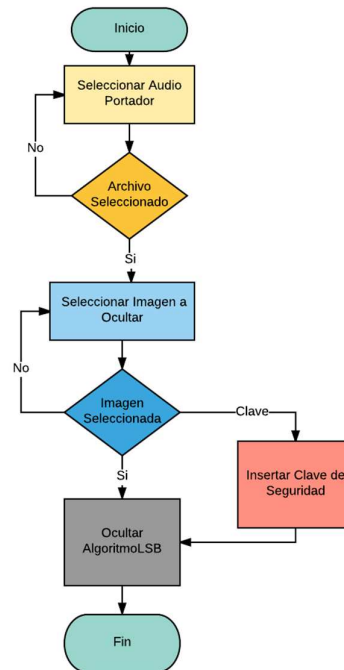


a)

b)

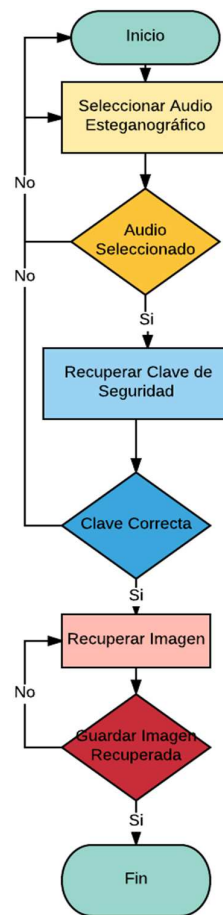
**Figura 16** a) GUIDE Ocultar imágenes B&N b) GUIDE Recuperar imágenes B&N

En la Pantalla *Ocultar B&N* en la Figura 16a se presenta un entorno amigable y fácil de usar para el usuario donde la selección de la imagen a ocultar fue de un grupo de imágenes obtenidas de una base de dato de uso libre (Pixabay, s.f.) y varios audios disponibles en la web de libre uso. El diagrama de flujo de la Figura 17 muestra el proceso de inserción de bits (píxeles de la imagen blanco y negro).



**Figura 17** Diagrama de Flujos de Inserción de Bits de Imágenes B&N

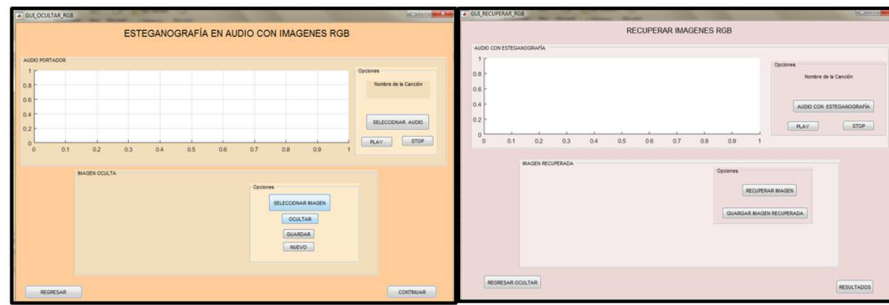
La Figura 16b muestra la pantalla *Recuperar B&N*, donde se selecciona el archivo esteganográfico y se obtiene la imagen oculta guardando la imagen recuperada para luego ser utilizada en el proceso de análisis de datos como se detalla en el diagrama de la Figura 18.



**Figura 18** Diagrama de Flujo de Recuperación de Bits de Imagen B&N

### 3.1.2 Ocultar Imágenes RGB

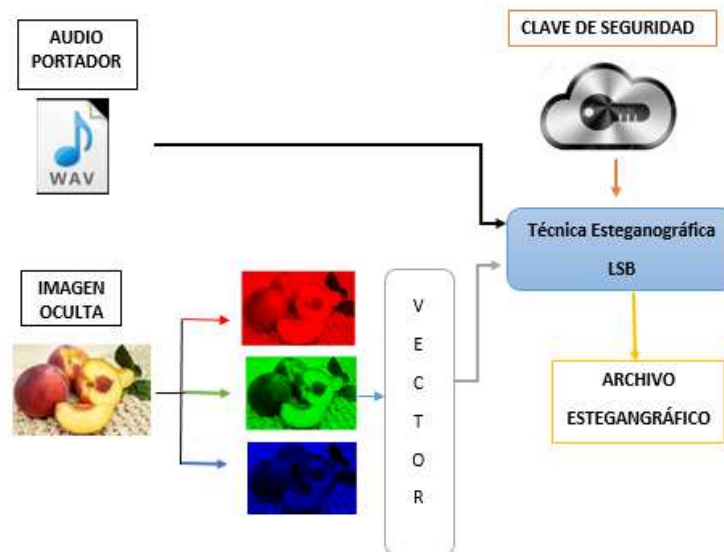
En la Figura 15 al seleccionar el *GUIDE Ocultar RGB* presenta una nueva pantalla donde muestra la interfaz gráfica para ocultar imágenes RGB en la Figura 19a y recuperar imágenes RGB en la Figura 19b.



a) b)

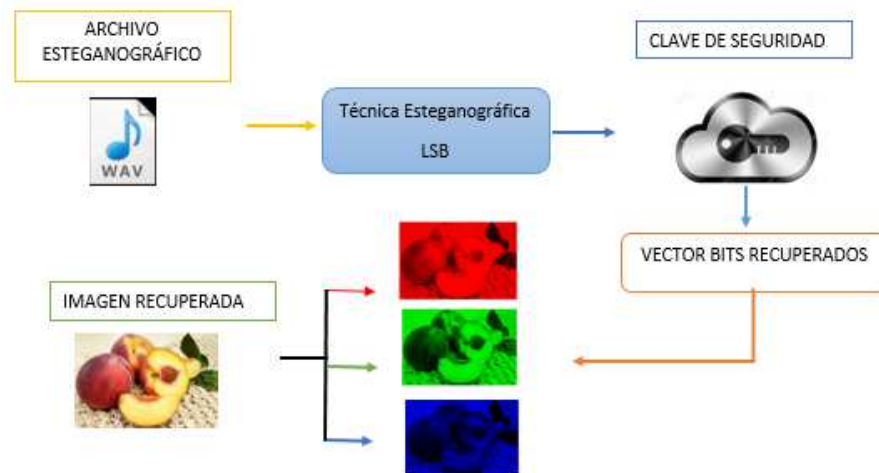
**Figura 19** a) GUIDE Ocultar imágenes RGB b) GUIDE Recuperar imágenes RGB

En el presente trabajo las imágenes RGB conocidas como imágenes de 3 canales son representadas en Matlab por una matriz de  $m \times n \times p$ , donde  $m, n$  representan el alto y ancho de la imagen respectivamente, y  $p$  el plano de color “1 Rojo”, “2 Verde” y “3 Azul” correspondientemente. El proceso de ocultamiento de bits es el mismo proceso demostrado en el diagrama de flujo de imágenes B&N de la Figura 17, sin embargo en este caso las imágenes son descompuestas en 3 planos de color donde cada plano contiene una matriz  $m \times n$  de pixeles que son codificados y convertidos en un solo vector de bits. Como se observa en el diagrama de la Figura 20 se realiza el proceso de inserción de bits RGB en el audio portador.



**Figura 20** Diagrama de Inserción de bits de imagen RGB

La Figura 21 detalla el proceso de recuperación de bits de la imagen RGB ocultos, los bits insertados usando la técnica LSB del último bit del vector de datos del audio son extraídos diferenciando cada canal (RGB) como fueron ubicados.



**Figura 21** Diagrama de Recuperación de Bits imagen RGB

### 3.2 Medidas de Calidad de Imágenes

Durante el desarrollo de técnicas de procesamiento digitales de imágenes es importante medir la calidad después de estar expuesto a manipulación e inserción de bits donde se adquieren distorsiones y ruido. Se han desarrollado varias medidas de calidad con el objetivo de estimar esta magnitud de manera, entre las más conocidas esta “La relación señal a ruido máxima PSNR” en conjunto con “Error medio cuadrático MSE”, que se consideran imprescindibles en el procesamiento y transmisión de imágenes. Estas dos medidas de calidad trabajando junto con “Índice de similitud estructural SSIM” son sencillas de calcular, tienen significados físicos precisos y son convenientes en el contexto de la optimización matemática son usadas en el presente trabajo con el objetivo de estimar un valor real de pérdida de información de bits para evaluar no solo el algoritmo LSB implementado sino el proceso esteganográfico imágenes y audios.



En este caso el hecho de que una imagen secreta sea incrustada en un audio portador y además el portador sea manipulado también ocasiona importantes modificaciones en la calidad de la imagen haciéndola más propensa a ataques estegoanalíticos visuales. Por este motivo es necesario medir la calidad visual de la imagen usando las métricas mencionadas.

Las medidas de calidad de la imagen pueden ser clasificadas según la disponibilidad de la imagen original (libre de distorsiones), la cual es comparada con la imagen distorsionada. Una de las ventajas En la mayoría de las aplicaciones prácticas no existe una imagen para comparar por lo cual se obtiene una calidad sin referencia, también existen referencias parcialmente disponibles, es decir solo se dispone de ciertas características extraídas de la imagen que ayudan en la evaluación de la calidad. (Onofre, 2016)

A continuación se describen las medidas de calidad de imágenes:

### **RMSE**

Es una medida objetiva de la calidad de la imagen mediante el cálculo de la raíz cuadrada de la diferencia cuadrática media entre los valores de los píxeles de la imagen distorsionada y la imagen referencia, este valor representa un error por lo que un menor valor demuestra mayor similitud de las imágenes y por ende mayor calidad (Wang, Bovik, Sheikh, & Simoncell, 2004)

Un criterio objetivo de calidad como el error medio cuadrático tiene en cuenta las diferencias entre la imagen original y la procesada o reconstruida. Sus valores se calculan según la *ecuación 1*:

$$RMSE = \frac{1}{m * n} \sum_{i=1}^m \sum_{j=1}^n (x_{orig.}(i,j) - x_{recon.}(i,j))^2 \quad (1)$$

Donde  $x_{orig.}$  es el valor de la imagen original,  $x_{recon.}$  es el valor de cada pixel de la imagen reconstruida,  $m$  es el número de columnas y  $n$  número de filas.

La distorsión presente en la imagen reconstruida debido al efecto de la compresión y/o modificación de bits con pérdidas puede ser calculada también utilizando la Relación Señal Ruido Máxima (PSNR) mediante la siguiente *ecuación 2*:

$$PSNR (db) = 10 \log_{10} \left( \frac{MAXp^2}{MSE} \right) \quad (2)$$

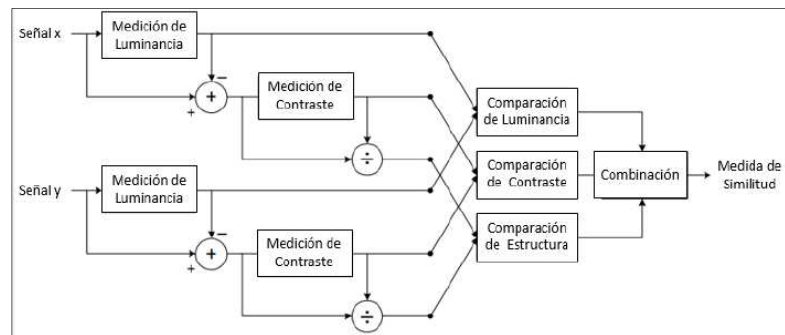
Donde RMSE es el error medio cuadrático obtenido en la Eq.1 y  $MAXp = (2^B - 1)$  donde B= es la profundidad de bits de la imagen. (Paz & Bosch, 2007)

Los parámetros estiman errores percibidos para cuantificar degradaciones en la imagen, pero no toman en cuenta el tipo de error y la calidad visual que produce. (Onofre, 2016)

## **SSIM**

La medida de calidad SSIM considera las degradaciones de la imagen como cambios en la información estructural que es lo que extrae la visión humana HSV (*Human Visual System*). El funcionamiento del sistema de medición SSIM se basa en tres comparaciones por separado: luminancia, contraste y estructura.

El sistema de medida mostrado en la Figura 22 funciona con la entrada de dos señales de imágenes x e y, una de ellas es una imagen libre de distorsiones, es decir, se supone como la medida de referencia de calidad perfecta con la que es comparada la otra señal ingresada. Finalmente, luego de la comparación de los tres parámetros se realiza una combinación para obtener un resultado final de similitud. (Onofre, 2016)



**Figura 22** Diagrama del sistema de medida de la similitud estructural (SSIM)

Fuente: (Wang, Bovik, Sheikh, & Simoncell, 2004)

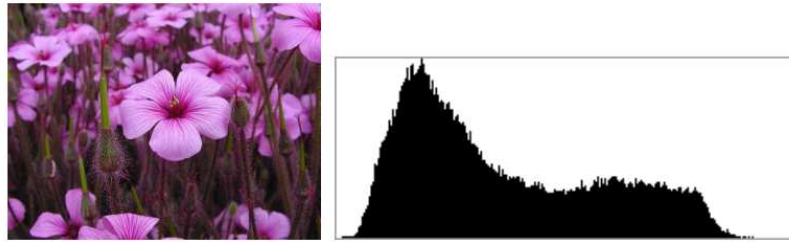
El índice de similitud estructural es una medida cuantitativa de la diferencia entre la imagen original y reconstruida en cuanto a sus luminancias, contrastes e información de estructura. Una forma simplificada de su expresión de acuerdo con es la siguiente *ecuación 3*:

$$SSIM(x, y) = \frac{(2\mu_x \mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (3)$$

Donde  $x$  es la imagen original,  $y$  es la reconstruida,  $\mu_x$  y  $\mu_y$  son los factores de luminancia y  $\sigma_x$  y  $\sigma_y$  son los valores de contraste y  $C_1$  y  $C_2$  son constantes. (Paz & Bosch, 2007)

## Histogramas

Son herramientas importantes en el análisis de imágenes, cada imagen tiene un propio histograma. Si una imagen tiene un buen contraste su histograma se extiende ocupando casi todo el rango de tonos como se observa en la Figura 23.

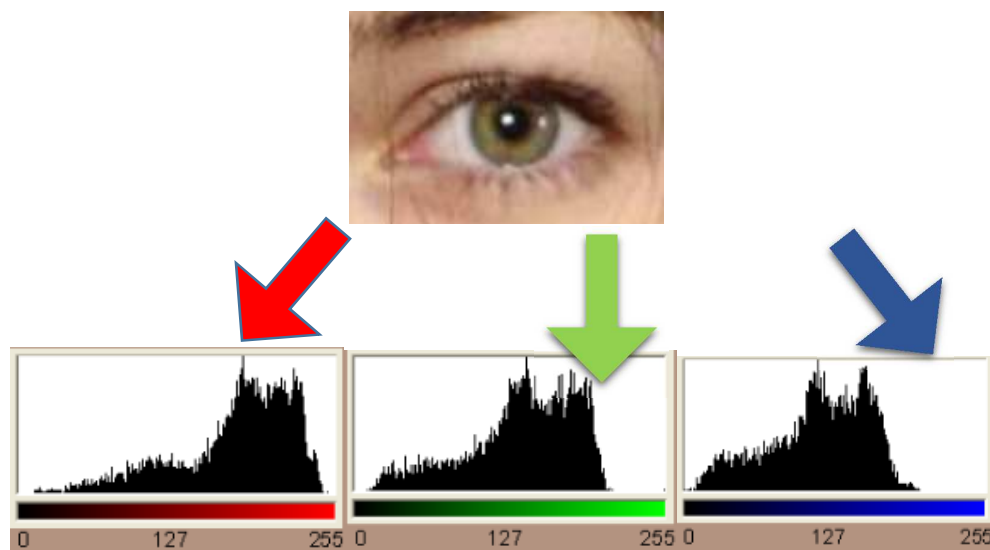


**Figura 23** Imagen e Histograma correspondiente

Los números que aparecen en el eje horizontal representan los niveles de gris que pueden aparecer en la imagen: a la izquierda está el valor más oscuro (negro) y en el extremo derecho el más claro (blanco). El resto de niveles se distribuyen uniformemente. Se ha puesto una escala con los tonos de gris correspondientes para facilitar la comprensión. En un histograma real habitualmente no encontrará numerado el eje vertical, ni la escala de tonos para el eje horizontal. La altura de cada barra representa el número de píxeles de la imagen que presentan ese nivel de gris concreto. (Atienza Vanacloig, 2015)

### Histogramas de color

En imágenes multicanal se puede obtener un histograma por cada canal como en la Figura 24 se observa la descomposición por color.



**Figura 24** Histogramas de color 3 canales RGB

### 3.3 Medidas de Calidad de Audios

#### Encuesta MOS

La calidad de la voz se establece a través de la opinión del usuario. La calidad de audio puede ser evaluada directamente (ACR = Absolute Category Rating), o en forma comparativa contra un audio de referencia (DCR = Degradation Category Rating). Con evaluaciones directas (del tipo ACR) se califica el audio con valores entre 1 y 5, siendo 5 “Excelente” y 1 “Malo”. El MOS (Mean Opinión Store) es el promedio de los ACR medidos entre un gran número de usuarios. (Joskowicz & Sotelo , 2013)

La metodología de evaluación subjetiva más ampliamente usada es la del MOS (Mean Opinión Score). (ITU-T, 1996)

En el presente trabajo se utiliza la encuesta MOS con medida subjetiva, ya que permite determinar la capacidad de un grupo de personas de detectar algún tipo de cambio en el archivo de audio portador con respecto al archivo original, sin embargo los datos obtenidos son subjetivos y el análisis depende de las condiciones del ambiente de la prueba y de las personas y su percepción.

La Tabla 11 detalla los niveles de medidas de satisfacción de los usuarios:

**Tabla 11**

*Tabla de Medidas de Satisfacción del Usuario*

<b>Satisfacción del Usuario</b>	<b>Factor R</b>	<b>MOS</b>
Muy Satisfecho	90	4.34
Satisfecho	80	4.03
Algunos usuarios insatisfechos	70	3,60
Muchos usuarios insatisfechos	60	3,10
Casi todos los usuarios insatisfechos	50	2,58

Fuente: Cristina Bastidas

### **Capacidad de Inserción de Bits**

La cantidad máxima de información que se puede ocultar en un audio depende de la capacidad de bits que este contenga, todo depende de la duración en minutos del archivo de audio. Para saber cuál es la cantidad de información que se puede ocultar en un archivo de audio se utiliza la *ecuación 4*: (Rodríguez, 2016)

$$\mathbf{Cantidad\ Bits} = \mathbf{Tiempo\ duración} * \mathbf{Velocidad\ de\ Transmisión} \quad (4)$$

## CAPÍTULO 4

### 4. IMPLEMENTACION, PRUEBAS Y RESULTADOS

#### 4.1 Implementación Esteganografía en audio

A continuación describiremos los procesos de inserción y recuperación de las imágenes en los archivos de audio.

##### 4.1.2 Inserción de la imagen

La Figura 17 detalla el proceso de implementación de la inserción de una imagen de un canal en un archivo de audio, una vez comprendido el diagrama de flujo de este proceso se describe el proceso de ocultamiento de pixeles en el audio:

1. Seleccionamos el audio portador, en el programa podemos reproducir/detener el audio, que ocuparemos para ocultar la imagen, graficar y observar la onda de la señal de audio como se observa en el ejemplo de la Figura 25.



**Figura 25** Selección de Audio Portador

2. Seleccionamos la imagen ya sea de uno y tres canales que será oculta en los audios usando la técnica esteganográfica LSB como en la Figura 26.



**Figura 26** Selección de Imagen secreta

3. Para poder ocultar las imágenes ByN o RGB dentro de los archivos de audio se realizan los siguientes pasos dentro del programa creado:

En la Figura 27 se lee la imagen escogida obteniendo el valor de cada pixel en una matriz  $m \times n$ , dada por el tamaño original de las imágenes que fueron obtenidas de una base de datos (Pixabay. (n.d.). (B. & GbR, Producer)):

```
image = imread('gato_negro.png');
```



```

im_tx =

    192    152    149     75     15     25     92    146    187    213
    119     63     46     36      7      7     48     88    132    201
     88    108     82     57    10    29     55     59     95     87
     82    169    188     64    15    38    127    174    137     62
     55    108    109     24     63     30     74    133     94     49
     41     55     80     33     24     32     61     70     60     51
     77    129    150     52     54     43    124     98     43     56
    104    146    148     58     35     65    185    188     85     91
    128    100    107     53     66     67    164    183    144    119
    144    101     88     98    119     93    103    134    145    155

```

**Figura 27** Matriz de Pixeles de Imagen escogida para ser oculta

4. Para facilitar el procesamiento de las imágenes que serán insertadas dentro de los audios portadores se modifica su tamaño a un valor genérico como en la Figura 28.

```
im_tx = imresize(image, [480 640]);
```

```

>> [r g b]=size(im_tx)

r =

    480

g =

    640

b =

     1

```

**Figura 28** Redimensionamiento de las imágenes a ocultar, Tamaño de la matriz

5. Los valores de pixeles anteriormente tomados son convertidos a binarios y colocados en una matriz de 480 x 640 como se ve en la matriz de la Figura 29.

```

>> im_bin

im_bin =

     0     0     0     0     0     0     1     1
     1     1     1     0     1     1     1     0
     0     0     0     1     1     0     1     0
     0     1     0     0     1     0     1     0
     1     1     1     0     1     1     0     0
     1     0     0     1     0     1     0     0
     1     0     1     1     0     0     1     0

```

**Figura 29** Matriz de pixeles convertidos a binarios

6. Finalmente en la Figura 30 colocamos la matriz en una columna continua, cuyos bits se colocaran en la última posición bits menos significativos del audio portador original.

```

>> im_bin_tx

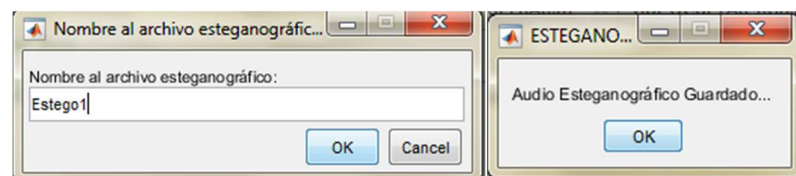
im_bin_tx =

     0
     1
     0
     0
     1
     1
     1
     0
     0
     0
     0

```

**Figura 30** Columna de bits que serán insertados en bit menos significativo

7. Nombramos el nuevo archivo de audio y guardamos como en la Figura 30, un nuevo audio con esteganografía.

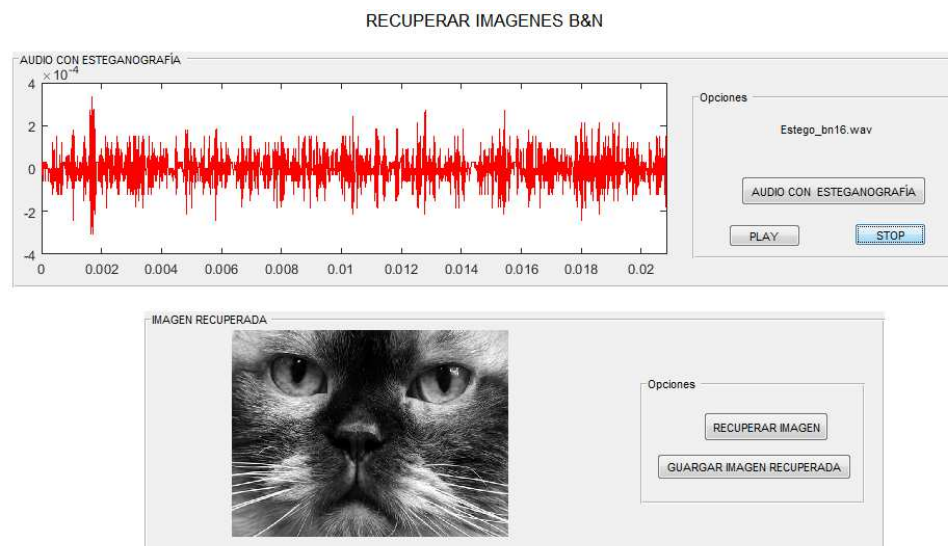


**Figura 31** Proceso de almacenamiento del archivo esteganográfico

### 4.1.3 Recuperación de la imagen

Una vez comprendido el diagrama de flujo del proceso de recuperación de imágenes RGB y ByN (ver Figura 18), detallamos el proceso de recuperación de las imágenes ocultas en el programa desarrollado:

1. Para la extracción de la imagen oculta, en la Figura 32 se muestra la interfaz de recuperación donde se selecciona el archivo de audio con esteganografía y se puede reproducir, detener y graficar la señal de audio con esteganografía.



**Figura 32** Interfaz de Recuperación de imágenes ByN

2. Para poder extraer la imagen en la Figura 32 seleccionamos el botón *Recuperar Imagen*. En el proceso de inserción de imagen secreta, una clave de seguridad fue incluida en todos los archivos de audio nuevos con esteganografía para que la información oculta no sea extraída o alterada por terceras personas. La clave de en un vector de 8 bits es insertada en cualquier parte del archivo, en este caso luego de la cabecera de los audios .WAV se coloca la clave para que si algún usuario desea recuperar la imagen oculta, primero debe extraer una clave correcta caso contrario el proceso de recuperación finaliza.

```
clave = bitget(datos(1:8),lsb,'uint64');
```

3. Si la clave original del programa es igual a la clave extraída de los archivos esteganográficos, se procede a recuperar la imagen:

```
if clave == [1 0 1 0 1 0 1 1]'
```

4. Es importante recuperar el tamaño del vector bits que fue oculta para extraer las imágenes de un canal ocultos en de los archivos de audio esteganográfico:

```
imre_bin(1:len) = bitget(datos(33:32 + len),lsb);
```

En el caso de imágenes RGB son tres vectores de información que fueron ocultos correspondientes a cada uno de los canales de color (Red, Green y Blue):

```
R_rx_bin(1:len) = bitget(datos(33:a),lsb);
G_rx_bin(1:len) = bitget(datos(a + 1:b),lsb);
B_rx_bin(1:len) = bitget(datos(b + 1:c),lsb);
```

5. Finalmente cumpliendo todos los requisitos se recupera la imagen como se observa en la *Figura 33* que muestra la interfaz de recuperación RGB:



**Figura 33** Imagen recuperada RGB

La cantidad de píxeles que se pueden ocultar en un archivo de audio depende de la capacidad de incrustación de bits que el archivo contenga, principalmente en base a la duración en minutos del archivo de audio.

En este caso para conocer la cantidad de píxeles que se pueden ocultar tomamos en cuenta el tiempo de duración de los audios y la velocidad de bits, como se ve en la tabla con un ejemplo; y con la ayuda de la *ecuación 4* calculamos:

A continuación en la Tabla 12 presenta un ejemplo de un par de audios con su velocidad de bits y duración de cada archivo:

**Tabla 12**

*Tiempo de duración de audios y Velocidad de bits*

<b>Audios</b>	<b>Tiempo de Duración</b>	<b>Velocidad de Bits</b>
<b>Audio 1 ByN</b>	2:45 min.	705 kbps
	165 seg.	
<b>Audio 2 RGB</b>	8:57 min.	705 kbps
	537 seg.	

Fuente: Cristina Bastidas

$$\mathbf{Cantidad\ Bits} = \mathbf{Tiempo\ duración} * \mathbf{Velocidad\ de\ Transmisión}$$

$$\mathbf{Cantidad\ Bits} = 165\ segundos * \frac{705 * 10^3\ bits}{segundos}$$

$$\mathbf{Cantidad\ Bits} = 116\ 325\ 000\ bits$$

Con el cálculo anterior obtuvimos 116 325 000 *bits* para incrustar en un archivo de audio de 2:45 *minutos*, para conocer la cantidad de píxeles solo dividimos para 8 y finalmente tenemos la cantidad máxima:

$$Píxeles = \frac{Cantidad\ de\ Bits}{8}$$

$$Píxeles = \frac{116\ 325\ 000\ bits}{8} = 14\ 540\ 625$$

## 4.2 Pruebas realizadas

Para medir la calidad de las imágenes recuperadas y evaluar el algoritmo esteganográfico implementado en los audios portadores, se realizaron 100 pruebas con imágenes obtenidas de una base de datos de uso libre (Pixabay. (n.d.). (B. & GbR, Producer)), seleccionadas de manera aleatoria 50 para imágenes de un canal (blanco y negro) y 50 para imágenes de tres canales (RGB).

Las imágenes fueron preestablecidas a un tamaño de 480x640 para facilitar su procesamiento, con extensión .PNG, ya que por su algoritmo de compresión permite la reconstrucción de imágenes sin pérdida de datos como se analizó en la Tabla 9. Los audios descargados gratuitamente en la web fueron escogidos especialmente con extensión .WAV debido a las ventajas de calidad de sonido alta y múltiples aplicaciones en multimedia.

Para la obtención de datos los audios portadores de imágenes RGB y ByN fueron expuestos a varias combinaciones entre ellos y diferentes escenarios de prueba:

- Un audio con varias imágenes secretas
- Varios audios con la misma imagen secreta
- Un audio con su correspondiente imagen secreta

Se exponen los archivos portadores con esteganografía a 3 escenarios ya que deben ser acoplados a situaciones cotidianas reales de cualquier usuario para así conocer las condiciones factibles donde compartir un archivo con información oculta sin sufrir daños o levantar sospecha, a continuación la Tabla 13 detallan sus características de prueba:

**Tabla 13***Descripción de Escenarios de Pruebas de Audios Esteganográficos*

<b>Escenario</b>	<b>Referencias</b>
<i>Primero</i>	Aquí los archivos de audio con esteganografía serán guardados sin realizar ningún tipo de cambio, modificación o movimiento. Serán extraídos después de un tiempo para evaluar sus resultados.
<i>Segundo</i>	La carpeta que contiene los audios con esteganografía serán compartidos para ser reproducidos varias veces durante un tiempo determinado, para después obtener esos archivos y recuperar las imágenes ocultas.
<i>Tercero</i>	Los audios esteganográficos serán comprimidos en un archivo .RAR y enviados por correo electrónico para evaluar las pérdidas que tiene al realizar estos dos procesos.

Fuente: Cristina Bastidas

### 4.3 Análisis de resultados

#### Evaluación de Calidad en Audios Portadores

Para medir la calidad obtenida de los archivos de audios esteganográficos determinamos que es importante realizar una evaluación subjetiva y objetiva, ya que al relacionar ambas medidas obtendremos resultados más cercanos tanto a la percepción de usuarios que son la base de la implementación de estas técnicas esteganográficas para no ser detectadas, como acorde con los resultados matemáticos sobre la estructura de los audios que las medidas objetivas nos brindan.

#### MOS - Mean Opinion Score

Se realizaron encuestas MOS como se observa en la Figura 34 cuya medida es en base a la detección o no de algún cambio en la calidad de los audios con imagen oculta por parte de los usuarios.



**Figura 34** Diagrama de realización encuestas MOS

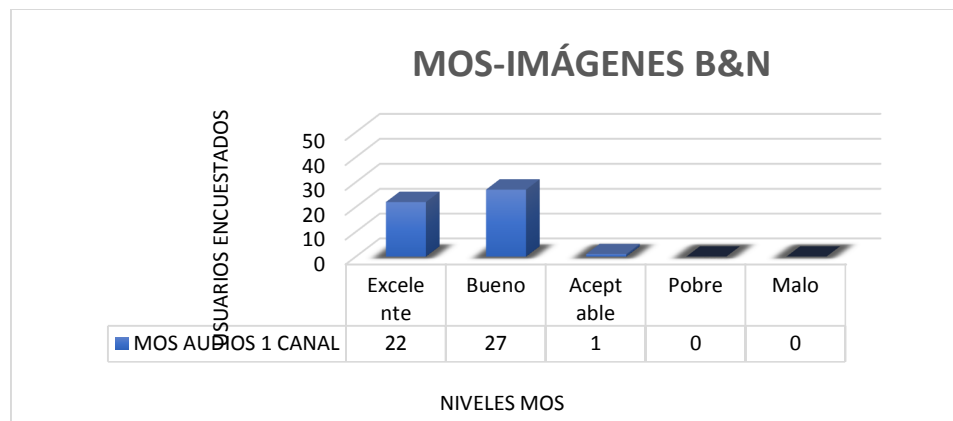
Para las encuestas MOS los audios fueron escogidos aleatoriamente de las diferentes combinaciones y escenarios a los que fueron expuestos durante 30 días, audios que fueron evaluados en 100 encuestas divididas equitativamente entre imágenes RGB y B&N:

### **Imágenes de un canal - B&N**

*PREGUNTA: Comparando con el audio original (AUDIO B&N 1), Califique la calidad del Audio Esteganográfico B&N A (con imagen oculta).*

Los resultados obtenidos en las encuestas MOS en audios portadores de imágenes de un solo canal fueron satisfactorios como se observa en la Figura 35, más del 50% usuarios pudieron notar que los audios tuvieron un mínimo cambio que no afectó a la calidad auditiva dando como resultado un valor promedio de  $MOS = 4,42$ , que según la Tabla 11 tiene un nivel de calidad *Muy Satisfactorio*.

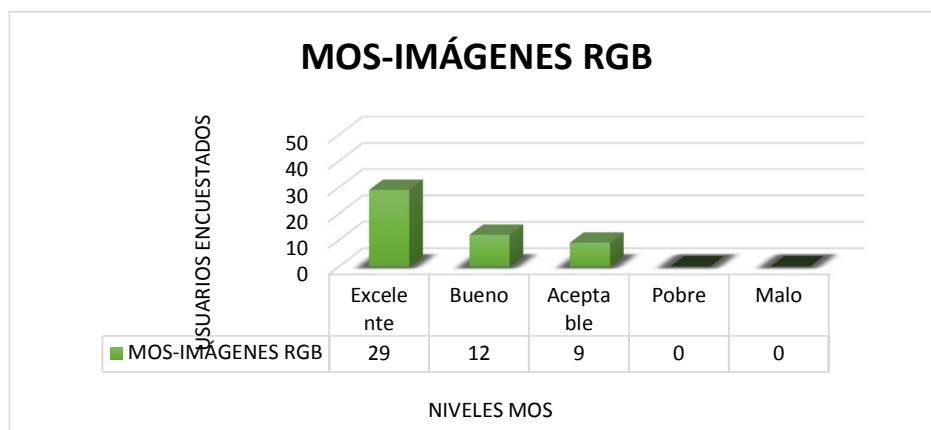




**Figura 35** Resultados encuesta MOS para imágenes 1 canal

### Imágenes de tres canales - RGB

En las encuestas MOS realizadas a los audios con imágenes de tres canales se obtuvieron resultados similares a las anteriores pruebas, debido a que la mayoría de los usuarios encuestados determinaron que la calidad del audio no vario en lo absoluto, 9 usuarios detecto baja calidad auditiva, sin embargo se obtuvo un valor promedio de  $MOS = 4,4$  con calidad auditiva *Muy Satisfactoria* según la Tabla 11, como se observa en la Figura 36.



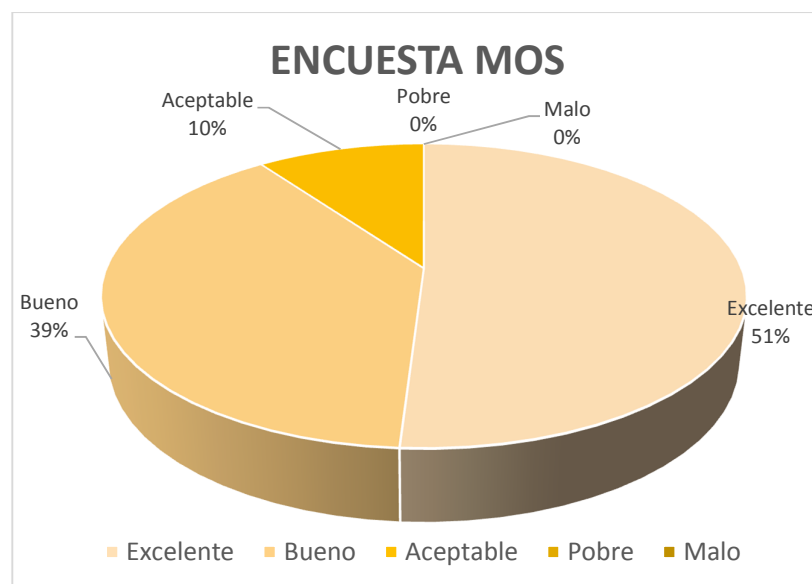
**Figura 36** Resultados encuesta MOS para imágenes 3 canales

Para las encuestas MOS en audios con imágenes RGB adicionalmente se añadió una pregunta donde el usuario debía mencionar si encontró algún tipo de cambio en el

audio y debía describirlo. Donde los comentarios más comunes que hicieron los usuarios fueron que:

- El volumen en los audios con imágenes ocultas se debilitan en algunas partes.
- El sonido se distorsiona y se hace molesto en comparación con el original.
- El audio es excelente no se nota cambios ni variaciones.

Finalmente se puede observar en la Figura 37 los datos totales de 100 encuestas MOS realizadas muestran que un 90% de usuarios determino que la calidad de los audios no disminuye, que son claros y sin mayores pérdidas, obteniendo un valor promedio de  $MOS = 4,41$  según los datos de la Tabla 14.



**Figura 37** Resultados encuesta MOS totales

**Tabla 14**

*Tabla de resultados totales de encuestas MOS*

<b>Tipo de Imágenes</b>	<b>Valor MOS</b>	<b>Satisfacción de Usuario</b>
<i>Un Canal</i>	4,42	Muy Satisfactorio
<i>Tres Canales</i>	4,40	Muy Satisfactorio
<i>Total</i>	4,41	Muy Satisfactorio

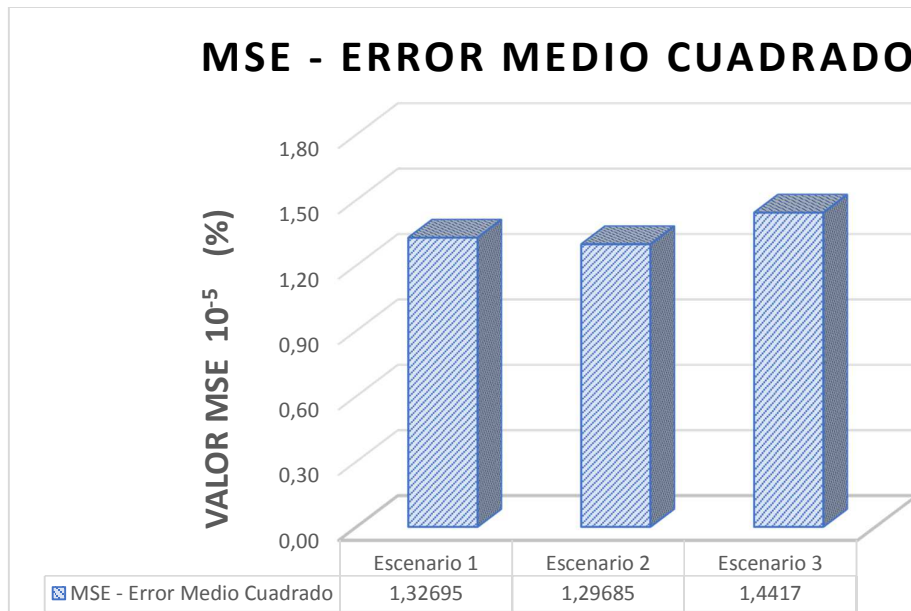
Fuente: Cristina Bastidas

La evaluación objetiva de la calidad en audio, imagen y video se han venido realizando usualmente mediante técnicas de evaluación de error MSE (Mean Square Error) y PSNR (Peak Signal to Noise Ratio).

Para validar los datos MOS obtenidos se realizaron medidas de 90 audios con esteganografía divididos 15 para cada uno de los escenarios propuestos donde se obtuvieron los valores de Señal Ruido y Porcentaje de error realizando un promedio en cada escenario.

### **MSE (Mean Square Error)**

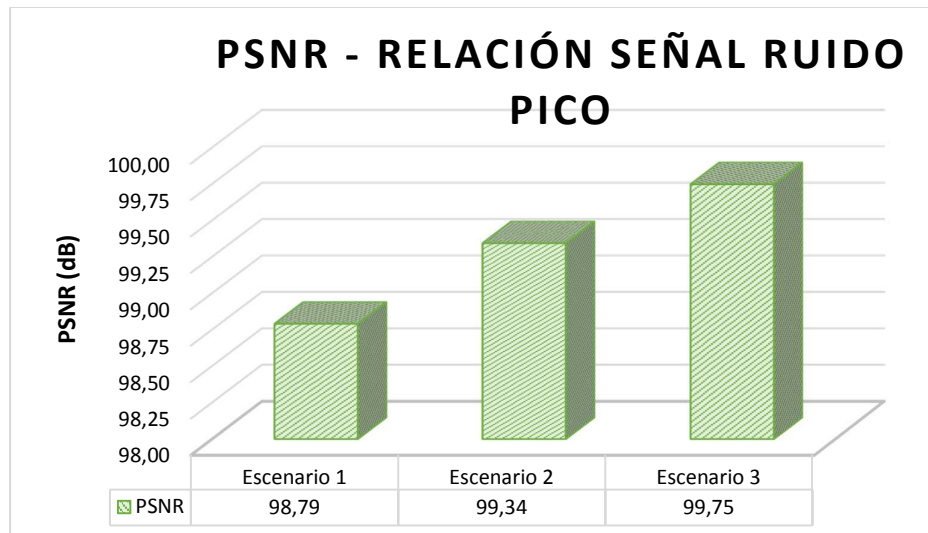
Los valores resultantes de MSE de los archivos con imágenes ocultas respecto al audio original de cada uno de los escenarios, obtuvieron un valor promedio muy bajo con un porcentaje menor al 2% de error en ambas pruebas tanto para imágenes de uno y tres canales. El error MSE obtenido en el tercer escenario tuvo un aumento mínimo con respecto a los otros dos, con un valor de pérdidas del 1,5% aproximadamente detallado en la Figura 38, debido a las condiciones a las que fueron expuestos los archivos de compresión y transmisión vía web.



**Figura 38** Grafica estadística de Valores MSE de audios esteganográficos totales

### PSNR

Finalmente obtenidos los valores MSE de cada escenario se determinó el valor pico de la relación Señal / Ruido (SNR) de dichos archivos esteganográficos en los tres escenarios, donde en la Figura 39 se puede observar que el ruido que se adhiere a los archivos de audio es mínimo ya que los valores Pico-SNR son altos, es así que no se puede considerar que existe daño alguno fuerte o pérdida alta en la calidad auditiva de los archivos.



**Figura 39** Grafica estadística de Valores MSE de audios esteganográficos totales

### Evaluación de Calidad de Imágenes

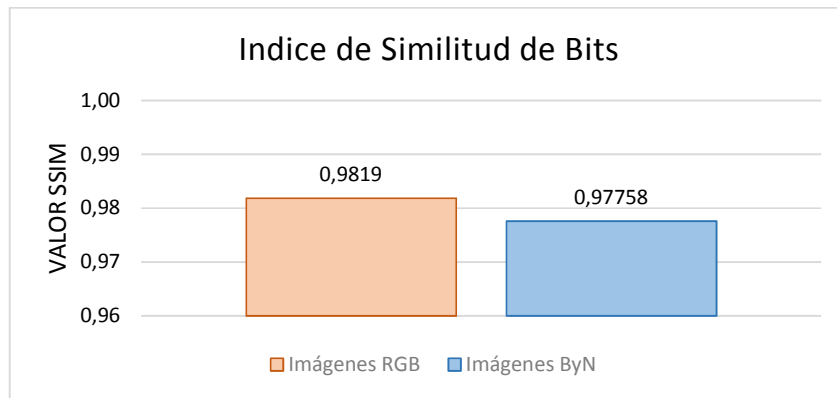
A continuación se mostrarán gráficos estadísticos de los valores de error (*RMSE*), Índices de Similitud de Estructura (*SSIM*), acompañados de Histogramas donde se muestra el comportamiento de los niveles de intensidad de color de ambos tipos de imágenes en cada uno de los escenarios de prueba indicados en la Tabla 12:

#### Primer Escenario

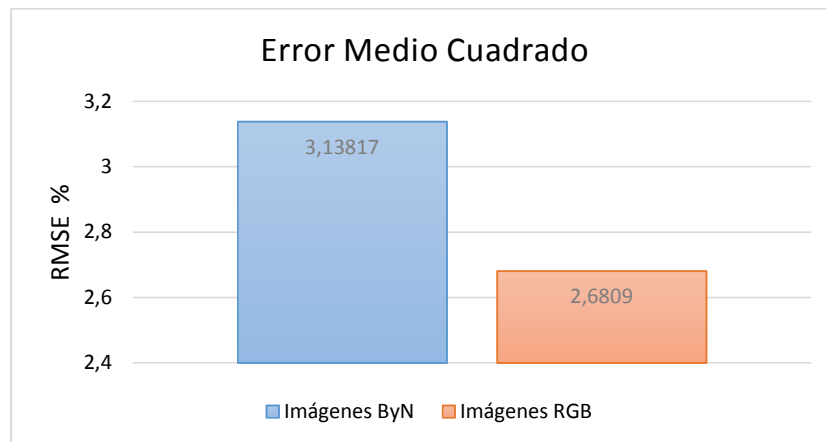
En el primer escenario se obtuvieron resultados muy satisfactorios debido a que los porcentajes de error *RMSE* entre las imágenes originales y las recuperadas, en la Figura 40b tienen valores muy pequeños menores al 3,5% aproximadamente, extendiendo una diferencia de error mínima de 3,2% en imágenes de un solo canal y 2,7% en imágenes de tres canales, sin embargo ambas imágenes tiene una calidad visual alta.

El índice *SSIM* permite medir la similitud de bits entre las imágenes recuperadas con las originales ocultas en los archivos de audios, el rango de esta métrica es de 0 a 1, donde 0 corresponde a una pérdida total de la similitud estructural y 1 corresponde a una copia exacta de la imagen original. Observando la Figura 41a ambos escenarios

muestran valores muy cercanos a 1, teniendo un 0,982 en imágenes de un canal y 0,978 en imágenes de tres canales, concluyendo que la similitud en ambas imágenes es de un 98% aproximadamente en ambos tipos de imágenes.



a)

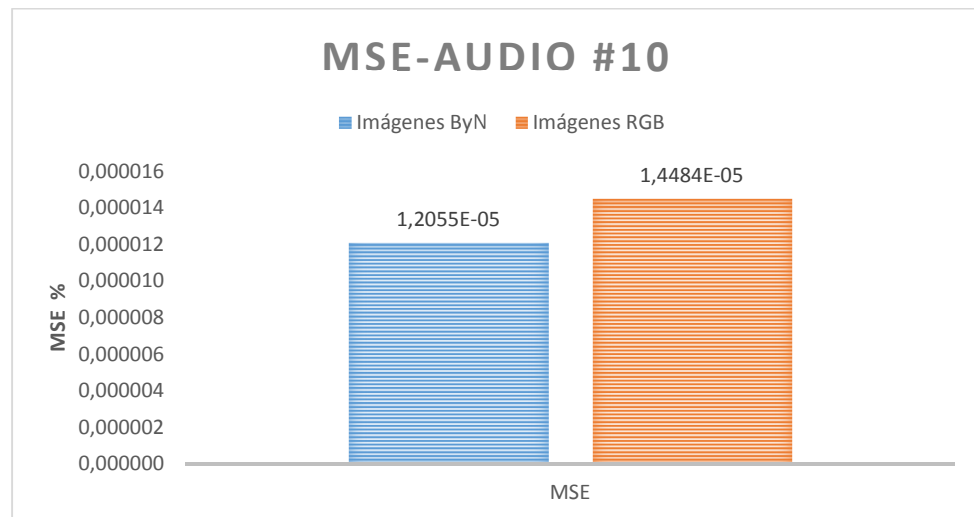


b)

**Figura 40** a) RMSE Promedio b) SSIM promedio del Primer Escenario

Ya que las imágenes en este primer escenario no sufrieron grandes cambios ni alteraciones a la calidad visual, es importante analizar los valores de porcentajes de error obtenidos en los audios con esteganografía y audios originales. Como podemos ver en la Figura 41, los audios que fueron usados como portadores de imágenes ocultas presentan valores muy bajos de error respecto a los originales, lo que determina que los cambios sufridos en el proceso esteganográfico y en la exposición a las

condiciones de este primer escenario no afectaron en casi nada a la calidad auditiva de los mismos, validando la objetividad de las técnicas esteganográficas.

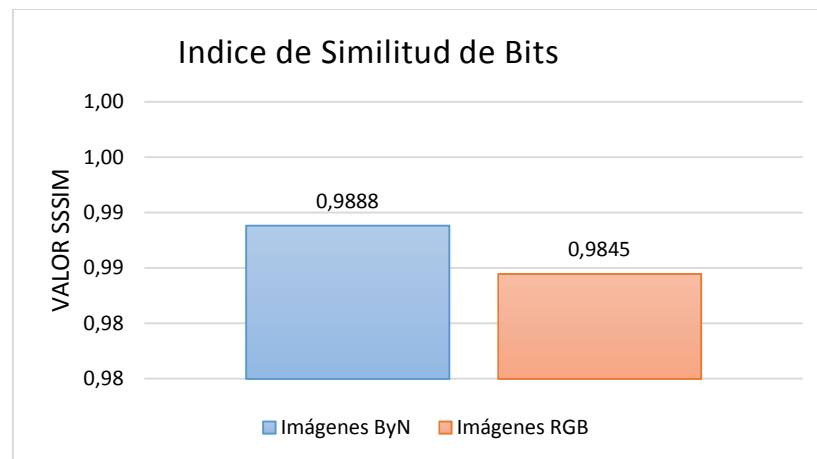


**Figura 41** MSE promedio de Audio portador del Primer Escenario

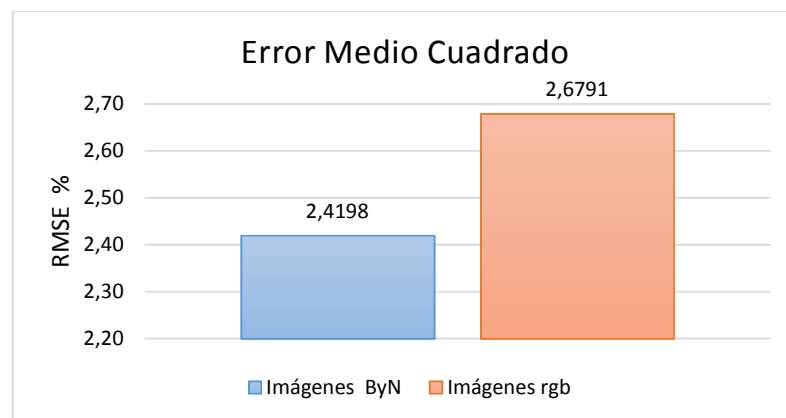
## Escenario 2

En el segundo escenario se obtuvieron resultados parecidos al primero debido a que los valores obtenidos de error RMSE en la Figura 42b fueron tan bajos como en el primer escenario, midiendo un 2,4% en imágenes de un solo canal y 2,8% en imágenes de tres canales aumentando significativamente pero no afectante en nada a la calidad visual de las imágenes.

Al obtener los índices de SSIM observados en la Figura 42a, en este escenario se evidenció de igual forma la alta similitud que se da entre imágenes recuperadas y originales con 98% muy cerca al 100% de similitud, evitando tener pérdidas de calidad en ambos experimentos.



a)



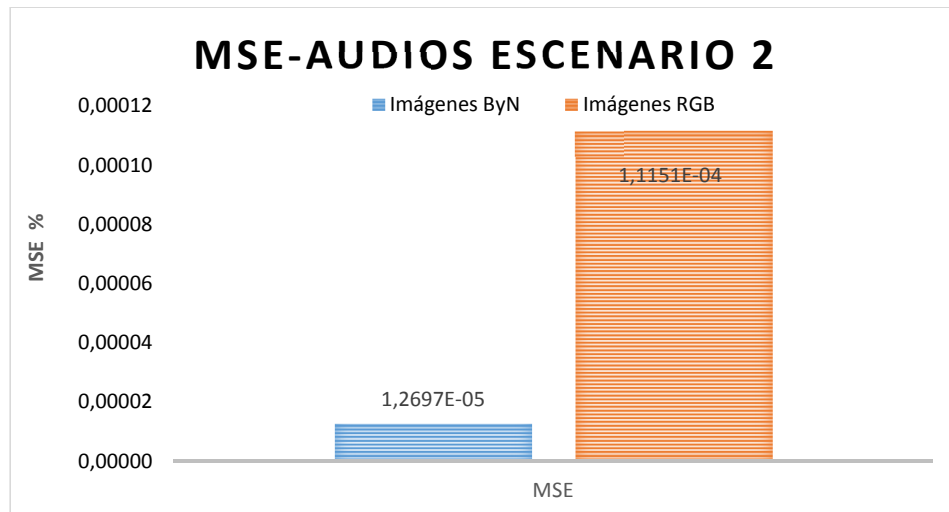
b)

**Figura 42** a) RMSE Promedio b) SSIM promedio del Segundo Escenario

En un grupo de pruebas de este segundo escenario se usaron la misma imagen en diferentes audios portadores, donde en las 5 pruebas obtuvieron los mismos valores de SSIM y RMSE teniendo el mismo comportamiento ya que es la misma información que se está ocultando en todas.

De igual manera al analizar los cambios que afectaron a la calidad auditiva, como se observa en la Figura 43 de los audios portadores de este grupo de pruebas en comparación con los audios esteganográficos, los valores de error en este segundo escenario fueron con un error mínimo.

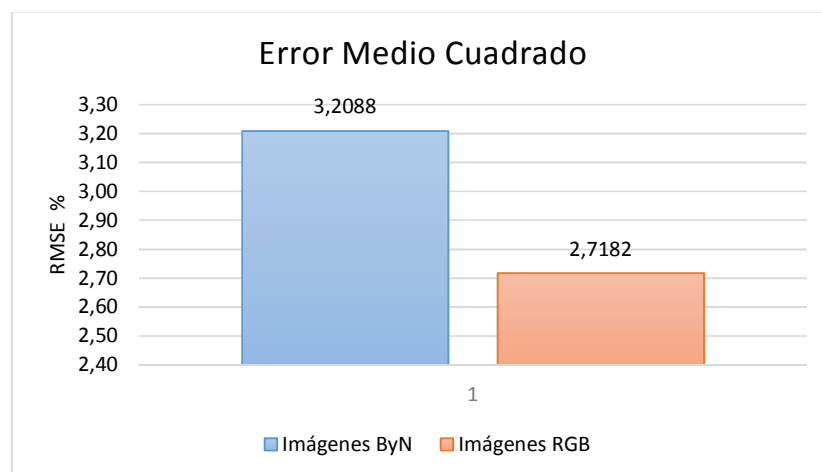


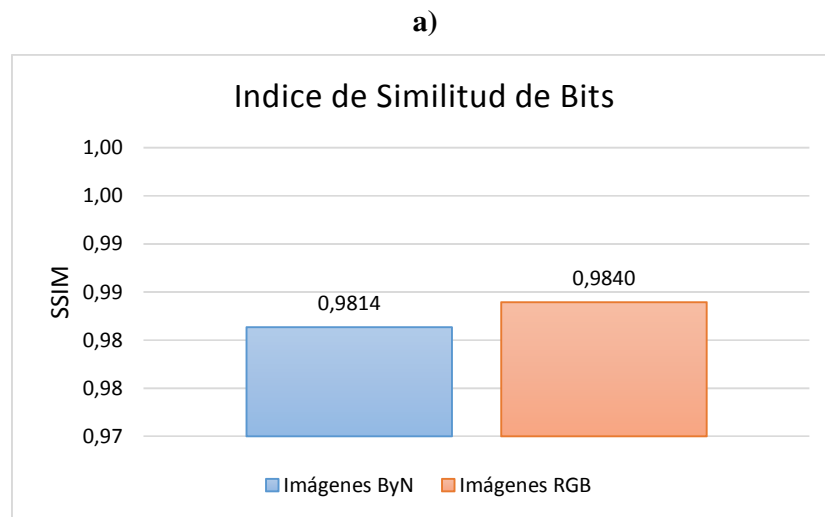


**Figura 43** MSE promedio de Audio portador del Segundo Escenario

### Escenario 3

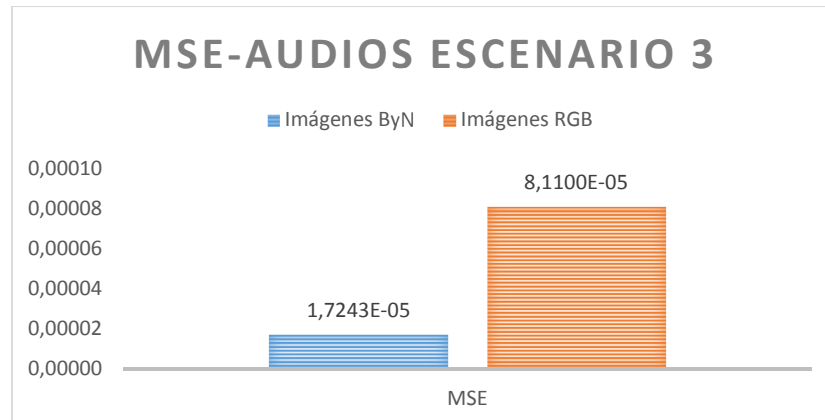
Para el tercer escenario a pesar de las condiciones de compresión y transmisión de audios esteganográficos vía correo electrónico, no se presentaron afectaciones ni cambios altos en la calidad de imágenes ocasionando grandes pérdidas en la calidad de las imágenes, al contrario hubieron aumentos significativos tanto de errores RMSE de 3,2% para imágenes de un canal y 2,7% en imágenes de tres canales como se ve en la Figura 44b, como la Figura 44a indica el índice SSIM obteniendo una similitud entre imágenes del 98%.





**Figura 44** a) RMSE Promedio b) SSIM promedio del Tercer Escenario

Finalmente al analizar los valores de errores de los audios portadores con audios originales los bajos valores de MSE presentados en la Figura 45 resultan porcentajes de errores tan bajos que no afectan en la calidad auditiva de los mismo.



**Figura 45** MSE promedio de Audio portador del Tercer Escenario

### Histogramas

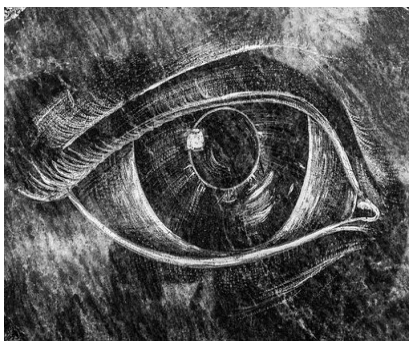
A continuación se presentan los histogramas de los dos mejores experimentos obtenidos en cada escenario con imágenes de un canal y tres canales donde se observa con más detalle el impacto de estos valores de SSIM y RMSE obtenidos anteriormente.

Todos los experimentos muestran tres imágenes, las imágenes originales usadas como información o mensaje secreto (ver Figuras literal a), las imágenes recuperadas después de ser expuesta a los procesos esteganográficos de ocultamiento y recuperación (ver Figuras literal b) en cada uno de los escenarios. Como se puede observar la calidad en las imágenes recuperadas comparadas con las originales es muy buena en todos los escenarios, no sufre de cambios o alteraciones bruscas, son imágenes claras nada borrosas y recuperadas en su totalidad.

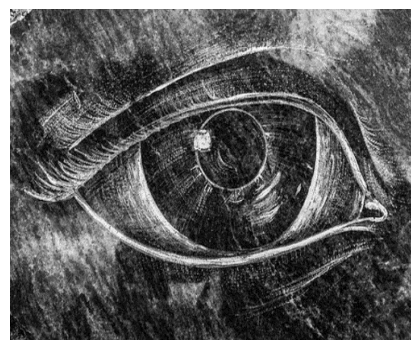
Los histogramas de imágenes ByN de las Figuras (46c,48c,50c) muestra dos curvas, la azul corresponde a los valores a la imagen original y la curva roja a la imagen recuperada, los histograma de la Figura (47c,49c,51c) presentan tres curvas correspondientes a los canales RGB, la curva de color rojo corresponde al canal R, la de color verde al canal G y la de color azul al canal B , el eje x tiene el número de valores de píxeles que en este caso están en el rango de 0 a 255, mientras que el eje y corresponde a las frecuencias de cada valor de píxel.

## Escenario 1

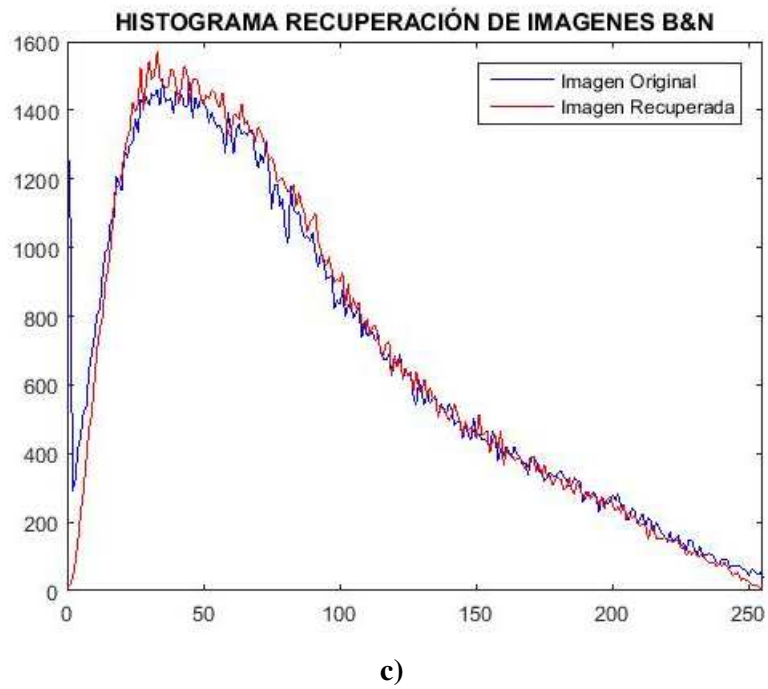
### Experimento 1



a)



b)



**Figura 46** a) Imagen Original 1 b) Imagen Recuperada 1 c) Histograma 1

## Experimento 2



**a)**



**b)**

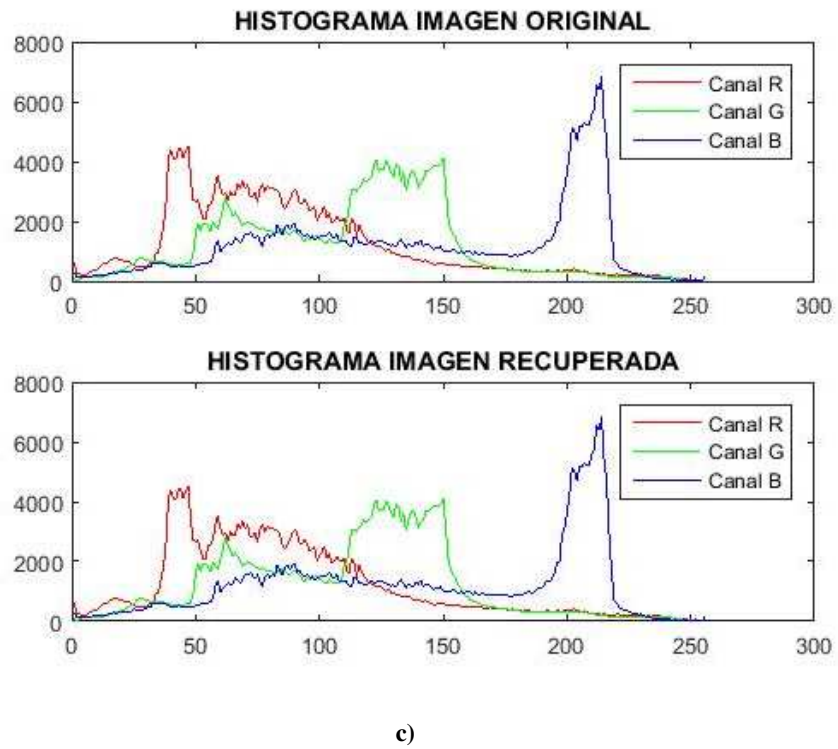


Figura 47 a) Imagen Original 2 b) Imagen Recuperada 2 c) Histograma 2

## Escenario 2

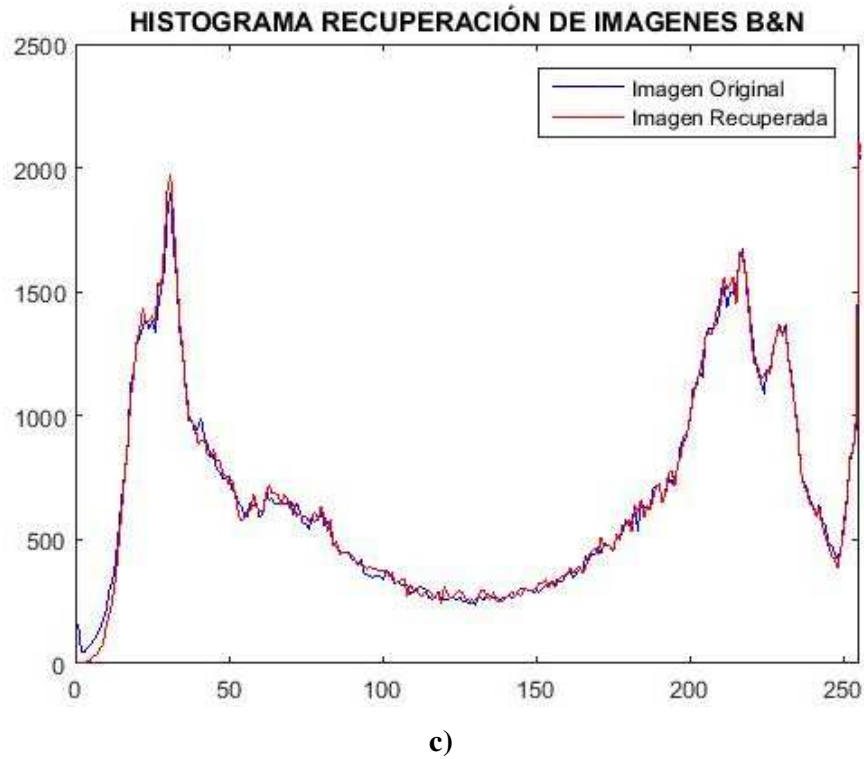
### Experimento 3



a)



b)

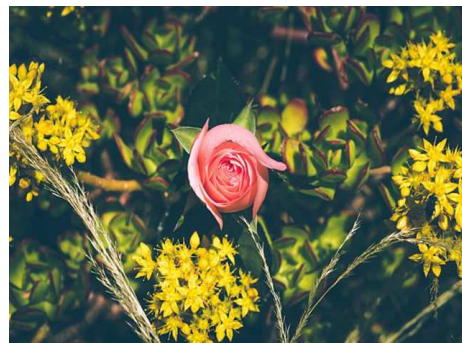


**Figura 48** a) Imagen Original 3 b) Imagen Recuperada 3 c) Histograma 3

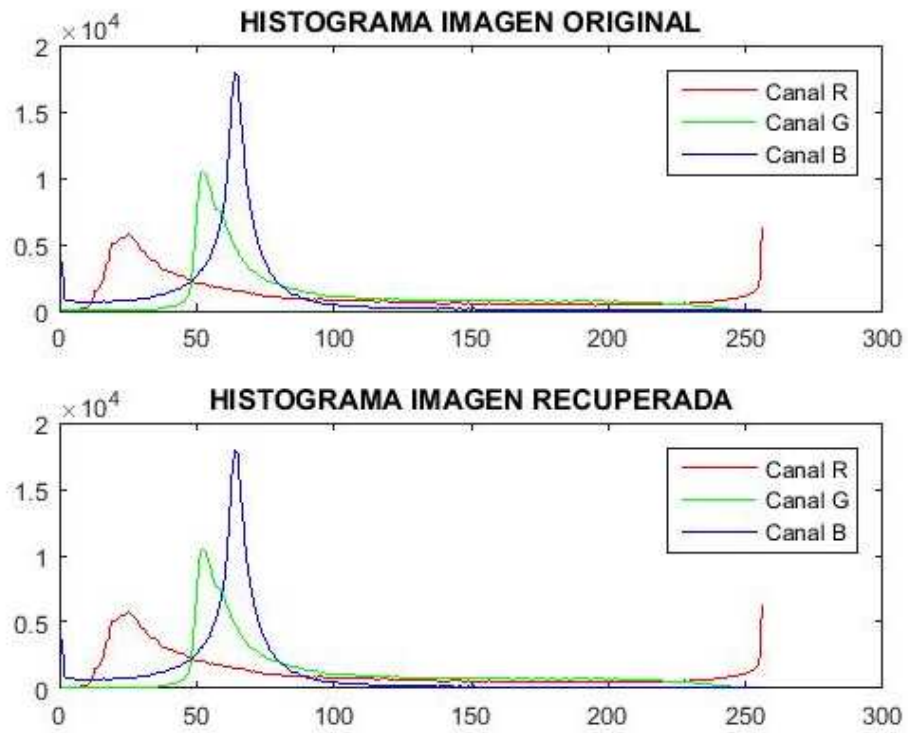
#### Experimento 4



**a)**



**b)**



**Figura 49** a) Imagen Original 4 b) Imagen Recuperada 4 c) Histograma 4

### Escenario 3

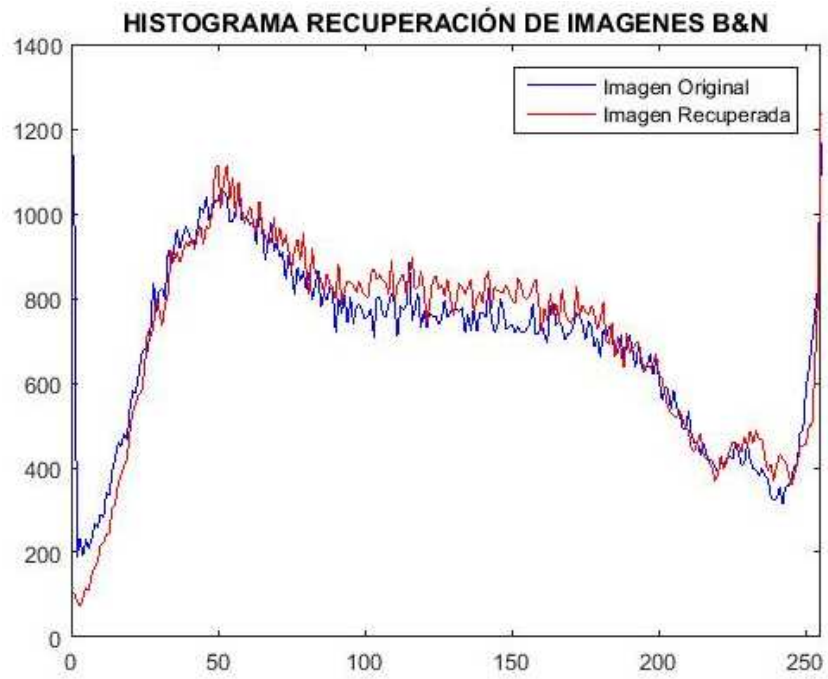
#### Experimento 5



a)



b)



**c)**

**Figura 50** a) Imagen Original 5 b) Imagen Recuperada 5 c) Histograma 5

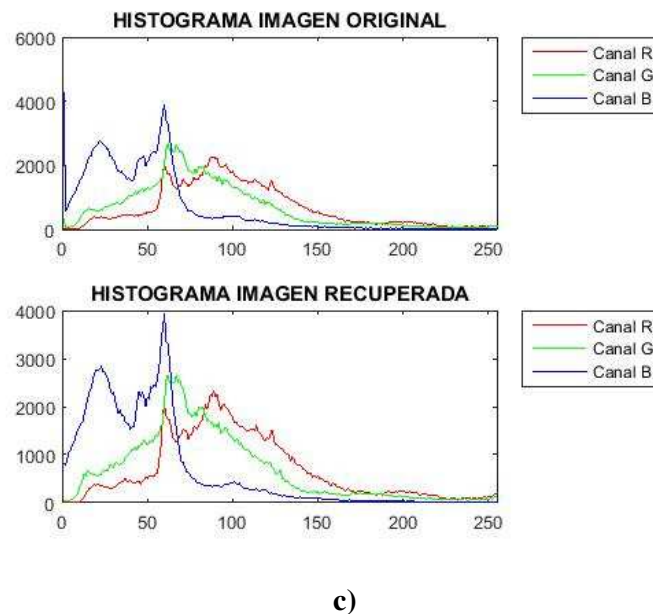
### Experimento 6



**a)**

**b)**





**Figura 51** a) Imagen Original 6 b) Imagen Recuperada 6 c) Histograma 6

### *Imágenes de un canal*

En el caso de los histogramas de las Figuras (46c,48c,50c) correspondientes a las imágenes de un solo canal las curvas de la imágenes recuperadas tiene gran similitud a las de la imágenes portadoras originales, sin embargo se puede observar que en las imágenes originales existen un grupo de valores muy cercanos al cero que son eliminados en los histogramas de las imágenes recuperadas realizando una pequeña variaciones en la curva en los valores más altos de pixeles, aunque ésta pérdida de valores no afecta visualmente a la calidad de las imágenes y son imperceptibles al sistema visual humano.

### *Imágenes de Tres canales*

A continuación el efecto de este proceso esteganográfico en las imágenes de tres canales es parecido al de las imágenes de una canal, en las Figuras (47c,49c,51c) se observa que el comportamiento de los tres canales de las imágenes recuperadas con

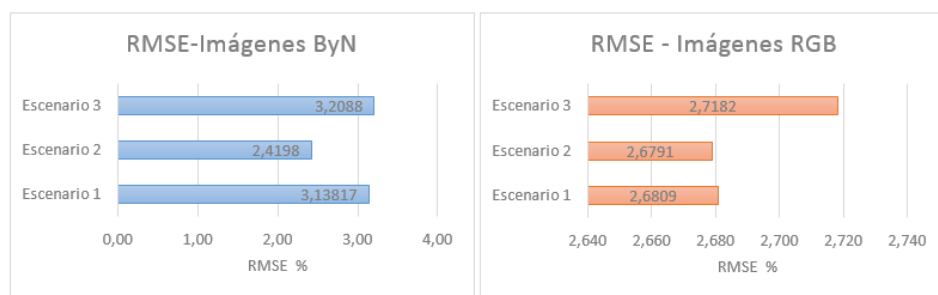
las imágenes originales son idénticas no se notan variaciones grandes que afecten la visibilidad de las imágenes o que permitan detectar algún cambio en las imágenes recuperadas. Algunas imágenes en este caso de tres canales también sufren una pérdida de esos grupo de valores muy próximos al cero en el canal B (*ver Figura 51c*) sin realizar cambios bruscos en los resultados de las imágenes recuperadas.

En la parte final del análisis de resultados de calidad de las imágenes recuperadas obtenidas, se realizaron gráficas estadísticas que determinan los valores de error RMSE e índices SSIM promedio de cada escenario en los dos experimentos imágenes de un canal y tres canales.

### ***RMSE (Root Mean Square Error)***

Según las mediciones RMSE promedio de los tres escenarios obtenidos en la Figura 52, se observa que para las imágenes de uno y tres canales, el tercer escenario muestra un incremento mínimo de error de 3,2% (*Figura 52 a*) y 2,7% (*Figura 52 b*) debido a los condiciones de este escenario a las que fueron expuestas.

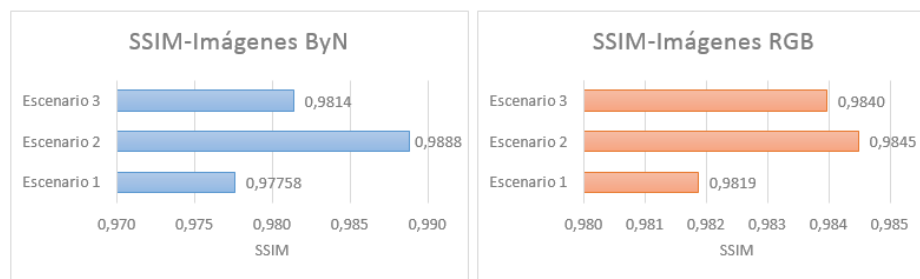
Con respecto a los otros dos escenarios correspondientemente los valores fueron igual de bajos y sin embargo los tres escenarios no muestran altas pérdidas de datos y se valida una muy buena calidad visible de las imágenes recuperadas.



**Figura 52** a) RMSE promedio de imágenes ByN b) RMSE promedio de imágenes RGB de los tres escenarios

### *SSIM (Structural Similarity Index Measurement)*

Se puede evidenciar en la Figura 53, que el promedio de los valores SSIM obtenidos en las 100 pruebas realizadas con respecto a la imagen secreta recuperada es de 0,98 cercano a 1, que indica que estructuralmente la similitud de imagen recuperada es muy cercana a la imagen original. En el caso de los segundos escenarios en ambos experimentos son los que mayor índice SSIM tienen en comparación a los otros escenarios, sin embargo este incremento no disminuye en la calidad de las imágenes de los otros escenarios.



**Figura 53** a) SSIM promedio de imágenes ByN b) SSIM promedio de imágenes RGB de los tres escenarios

## CAPÍTULO 5

### 5.1 Conclusiones

- Se desarrolló e implementó un algoritmo estenográfico en base al método de sustitución del último bit (LSB), ocultando imágenes de uno y tres canales en archivos de audio, evaluando la transmisión de estos archivos de audio y proporcionando seguridad ante ataques de terceros.
- Los archivos de audio .WAV utilizados para el proceso de estenografía tuvieron resultados muy positivos debido a que dichos formatos de audios en general no sufren ningún proceso de compresión y al ser insertadas las imágenes entregaron una alta calidad auditiva, además de ser un formato estándar de trabajo en la plataforma Matlab.
- Se evaluó la calidad de los audios con esteganografía usando encuestas MOS a 100 usuarios diferentes, donde un grupo de usuarios notaron ligeros cambios en la calidad auditiva, señalando que sufren pérdidas de volumen y cortes de sonido en algunas rangos, sin embargo más del 90% de usuarios concluyó que los archivos con imágenes ocultas son claros y no se nota ninguna pérdida en la calidad, con un valor promedio  $MOS = 4,41$  total en las encuestas se concluye que la calidad de los audios con esteganografía es muy buena.
- Es importante recordar que las encuesta MOS fueron usadas como una medida subjetiva que no presenta datos estadísticos reales sobre el comportamiento de los audios estenográficos en los diferentes escenarios propuestos, ya que los resultados van variando dependiendo el ambiente donde fueron reproducidos y la percepción de cada usuario que es distinto para cada uno. Es así que se obtuvieron valores de error MSE, consiguiendo valores ínfimos promedio bajo el 1,5% de error, resultados que no definen un nivel de pérdidas altas o modificaciones en los archivos de audio con esteganografía.

- Respecto al valor PSNR de los tres escenarios obtenidos de los audios con esteganografía en comparación con los archivos originales, se determinó que la adición de ruido y afectación que se da al realizar el proceso estenográfico con imágenes fue muy baja, ya que los valores PSNR obtenidos son 100 dB aproximadamente y se puede concluir que la calidad no es afectada en su totalidad.
- En una de las mediciones de calidad visual realizadas a las imágenes recuperadas en comparación con las imágenes originales, se tomó en cuenta la información estructural de la imagen basándose en el sistema visual humano usando el parámetro SSIM, obteniendo un valor de 0,99 aproximadamente para los dos tipos de imágenes (RGB y ByN), donde 1 corresponde a la copia exacta de la imagen original, obteniendo una calidad visual Muy Buena en los tres diferentes escenarios a los que los audios con esteganografía fueron expuestos.
- Al comparar los tres escenarios a los cuales estuvieron expuestos los archivos estenográficos los valores SSIM de 0,99 como índice de similitud y RMSE de 3% de error promedios aproximadamente no mostraron ningún aumento o disminución fuertes de valores, los cuales no permiten definir cuál es el mejor o peor escenario concluyendo que las condiciones de reproducción constante, compresión y envío vía correo electrónico no influyeron en grandes pérdidas de calidad en las imágenes recuperadas obteniendo cambios mínimos no perceptibles fácilmente a los usuarios.
- Los experimentos realizados tanto con imágenes de un canal (Blanco y Negro) y tres canales (RGB) no se presentaron grandes variaciones en las medidas de calidad tanto de audio (PSNR MSE) como en imágenes recuperadas (SSIM, RMSE) donde el número de canales de color no influyó en el proceso estenográfico ni en la alteración de la calidad de audio de los archivos portadores, sin embargo en el proceso de inserción de imágenes en los portadores las imágenes RGB tuvieron un procesamiento más complejo debido

a las 3 matrices de color que se deben ser ocultar la capacidad de incrustación de bits aumentada donde era necesario archivos de audio superiores a los 6 minutos de duración.

## 5.2 Recomendaciones

- Al implementar el algoritmo de esteganografía en los archivos de audio, se debe tomar en cuenta que la cabecera de los archivos describe la codificación de los audios utilizados, es por esta razón que no debe ser modificada o alterada, ya que los audios perderán calidad y sufrir cambios notorios a los usuarios al realizar la inserción de cualquier tipo de información (imágenes, texto, etc.).
- A pesar de que las encuestas MOS son medidas subjetivas cuyos resultados no son perfectos son necesarios para comprobar la precisión de los modelos de medidas objetivas MSE y PSNR, es por estas razones que es recomendable hacer unas evaluaciones tanto objetivas como subjetivas ya que debe existir una correlación entre ambos resultados.
- El tiempo a las que fueron expuestos los archivos con esteganografía no influyo en la evaluación de la calidad del audio, debido a que los tres escenarios tuvieron valores de error similar y no se concluye cuales condiciones afectaron más a los archivos, es recomendable hacer otro tipo de pruebas como son envió de los audios con esteganografía mediante implementación de nuevos escenarios.

## 5.3 Trabajos Futuros

Con la finalización del presente trabajo de investigación y debido a la versatilidad del tema sobre esteganografía se da paso a diferentes trabajos futuros relacionados al establecimiento de una vía de comunicación secreta entre dos partes, de modo que una tercera ubicada entre ambas no sea capaz de detectar la existencia de tal comunicación.

- Es así que un próximo desafío a realizarse sería exponer los archivos con esteganografía a escenarios bajo condiciones más reales y cotidianas, ayudándose de la implementación de una red inalámbrica en el campus de la Universidad usando un cualquier estándar de comunicación (802.11b, 802.16, etc.) donde mediante la medición de parámetros como paquetes perdidos, delay o jitter y el throughput evaluaremos la influencia en la calidad de los audios e imágenes recuperadas usando la técnica esteganográfica LSB y así conocer las condiciones factibles donde compartir un archivo con información oculta sin sufrir daños o levantar sospecha.
- El proceso de estego-análisis es una parte muy importante en lo que se refiere a pruebas de robustez ante ataques dirigidos, en lo que es esteganografía en audios como portadores no existen herramientas implementadas para realizar estas pruebas, es por esta razón que en base a la investigación realizada un trabajo futuro sería centrarse en detección de algoritmo LSB y ataques usando técnicas estadísticas usadas en imágenes acopladas a archivos portadores como audios.

## REFERENCIAS

- Rodríguez Medina, G., & Navas, S. (2015). Esteganografía: Sustitución LSB 1 bit utilizando Matlab. 859-854.
- Arévalo, C., & Valencia, V. (2007). *Modelo Tridimensional de la Historia Geológica del Volcán Cotopaxi*. Quito.
- Atienza Vanacloig, V. (2015). *El histograma de una imagen digital*.
- Bousono, C. (2010). *Sonido Digital*. Obtenido de <http://www.iescarlosbousono.com/wordpress/wp-content/uploads/2010/09/sonido-digital.pdf>
- Cantanhede, H. S. (2009). *Esteganografia em Audio e Imagem utilizando a tecnica LSB*. Catalao : Universidad Federl De Goiás.
- Cárdenas Quiroga, E. A., Morales Martín, L. Y., & Ussa Caycedo, A. (30 de julio de 2015). La estereoscopia, métodos y aplicaciones en diferentes áreas del conocimiento. *Revista Científica General José Mmaría Córdova*, 13(16), 201-219. Obtenido de <http://www.scielo.org.co/pdf/recig/v13n16/v13n16a10.pdf>
- Casierra, J. P. (2009). *Implementacao de im sistema esteganograficooarainsercao de textos emsinais de áudio*. Recife:Universidad Federal de Pernambuco.
- Cepeda Frías, G. L. (2016). *Creación de imágenes 3D utilizando el software de simulación Matlab*. Quito.
- Checa, E. (2014). *Implementación del Algoritmo Esteganografico F5 para imágenes JPEG a color*. Quito: Escuela Politecnica Nacional.
- Coltuc, D. &.-M. (Abril de 2007). Very fast watermarking by reversible contrast mapping. *IEEE Signal Proccess*, 14(14), 255-258.



- Corona, J. (2015). *Procedimiento de integración de la esteganografía al protocolo HTTP*. México.: Ciudad Universitaria.
- ESET Enjoy Safer Technology. (2016). *Tendencia 2016 (IN) SECURITY EVERYWHERE*.
- España Boquera, M. C. (2003). *Aplicaciones y Servicios de Comunicaciones de Servicios Avanzados de Telecomunicaciones*. Madrid: Ediciones Díaz de Santos.
- España Boquera, M. C. (2008). *Servicios Avanzados de Telecomunicaciones*. España: Díaz de Santos S.A. Obtenido de <https://books.google.com.ec/books?id=yTSoYCiXYAAC&printsec=frontcover#v=onepage&q&f=false>
- Hamid, N., Yahya, A., & Al-Qershi, O. (2012). *Image Steganography Techniques: An Overview*. International Journal of Computer Science and Security (IJCSS), 168-187.
- ITU-T, R. (1996). *Methods For Subjective Determination of Transmission Quality*.
- Jiménez Rosas, P. (2009). *Implementación de un Compresor-Descompresor de imágenes con JPEG200 en un DSP*. Mexico: Universidad Autónoma de Mexico.
- Joskowicz, J., & Sotelo, R. (2013). *Medida de la calidad de voz en redes IP*. Obtenido de <https://iie.fing.edu.uy/~josej/docs/Medida%20de%20la%20calidad%20de%20voz%20en%20redes%20IP.pdf>
- Kumar, A., & Pooja, K. ((2010)). *Steganography: A data hiding technique*.

- Lerch-Hostalot , D., & Megías, D. (Febrero de 2013). LSB matching steganalysis based on patterns of pixel differences and random embedding. *Computers & Security*, 192-206.
- López Martín, A. (2015). *Ingeniería en Ondas: Formatos de Audios Digitales*. Universidad de Valladolid.
- Master, D. (2004). *Introducción a la Esteganografía*. Obtenido de <https://radiosyculturalibre.com.ar/biblioteca/INFOSEC/death-master/Esteganografia.pdf>
- Megías, D. L.-H. (Febrero de 2013). LSB matching steganalysis based on patterns of pixel differences and random embedding. *Computers & Security*, 32, pp. 192-206.
- Morocho, E., Zambrano , A., Carvajal, J., & López, G. (2015). Análisis del Algoritmo Esteganográfico F5 para Imágenes JPEG a Color. *Revista Politecnica*.
- Onofre, G. (2016). “Desarrollo y análisis de una técnica esteganográfica en zonas ruidosas de la imagen mediante transformaciones de color reversibles” (tesis de pregrado). . Quito, Ecuador: Universidad de las Fuerzas Armadas ESPE.
- Orbegozo, I. (2011). *Técnicas de auto escalado de clouscomputing aplicadas al estegoanalysis*. Madrid: Universidad Complutesne De Madrid.
- Paz, J., & Bosch, A. (2007). La calidad en las imágenes de resonancia magnética comprimidas con JPEG2000.
- Pixabay. (n.d.). (B. & GbR, Producer). (s.f.). *Retrieved from Commons Creative*. Obtenido de <https://pixabay.com/es/>
- Rodriguez Mendoza, M. N. (2016). *Análisis de las técnicas de esteganografía para el ocultamiento de la información*. Quito: Universidad Central del Ecuador.

- Rodriguez, C. (2016). *Estudio y Desarrollo de una aplicación de esteganografía para enviar datos en archivos de audio, orientado a la seguridad en los sistemas de comunicación* (tesis de pregrado). Quito, Ecuador: Universidad de las Fuerzas Armadas ESPE.
- Romero García, J. L., & Teran Figueroa, J. E. (2011). *Análisis de formatos de audio y video para transmisión sobre demanda*. Mexico: Unidad Profesional "Adolfo López Mateos".
- Sánchez Tirado, S. A. (2006). *Integración de técnicas de manejo de la imagen digital para la web y la aplicación multimedia*. Quito.
- Sonido: Características Físicas*. (2 de Diciembre de 2016). Obtenido de <https://www.slideshare.net/margaprofe/sonido-caractersticas-fsicas>
- Tejada, C. E., & García Dominguez, A. (2016). Esteganografía: El arte de ocultar información. *ee' Revista de divulgación científica del COCyT*, 9-10.
- The origin of Modern Steganography*. (s.f.). Obtenido de <http://www.mikebarney.net/stego.html>
- Tiwari, A., Yadav, S., & Mittal, N. (2014). *A Review on Different Image Steganography*. International Journal of Engineering and Innovative Technology (IJEIT), 3(7), pp. 121-124.
- Tiwari, A., Yadav, S., & Mittal, N. (2014, January). *A Review on Different Image Steganography*. International Journal of Engineering and Innovative Technology (IJEIT), 3(7), pp. 121-124.
- Wang, Z., Bovik, A., Sheikh, H., & Simoncell. (2004). Image Quality Assessment: From Error Visibility to Structural Similarity. *IEEE Transactions on Image Processing*, 600-612.

Yúbal, F. (2015). *XATAKA*. Obtenido de <https://www.xataka.com/historia-tecnologica/cuando-una-imagen-oculta-mas-informacion-de-lo-que-parece-que-es-y-como-funciona-la-esteganografia>