
# DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

## CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

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

**TEMA: ANÁLISIS DEL MÉTODO ESTEGANOGRÁFICO COMO SOPORTE A LA SEGURIDAD DE LA INFORMACIÓN MEDIANTE LA OCULTACIÓN DE INFORMACIÓN SECRETA DENTRO DE UN VIDEO**

**AUTOR: HERRERA ARCENTALES, XAVIER EDUARDO**

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

**SANGOLQUÍ**

**2018**

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

CERTIFICACIÓN

Certifico que el trabajo de titulación, **"ANÁLISIS DEL MÉTODO ESTEGANOGRÁFICO COMO SOPORTE A LA SEGURIDAD DE LA IFORMACIÓN MEDIANTE LA OCULTACIÓN DE INFORMACIÓN SECRETA DENTRO DE UN VIDEO"**, realizado por el señor XAVIER EDUARDO HERRERA ARCENTALES 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 al señor **XAVIER EDUARDO HERRERA ARCENTALES** para que lo sustente públicamente.

Sangolquí, 20 de febrero de 2018.

**Ing. Freddy Acosta B.**
**DIRECTOR**


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

AUTORÍA DE RESPONSABILIDAD

Yo, **XAVIER EDUARDO HERRERA ARCENTLAES** con cedula de identidad **Nº 1716750144** declaro que este trabajo de titulación **"ANÁLISIS DEL MÉTODO ESTEGANOGRÁFICO COMO SOPORTE A LA SEGURIDAD DE LA IFORMACIÓN MEDIANTE LA OCULTACIÓN DE INFORMACIÓN SECRETA DENTRO DE UN VIDEO"** 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, 20 de febrero de 2018.

**XAVIER EDUARDO HERRERA ARCENTALES**
**C.C. 1716750144**


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

AUTORIZACIÓN

Yo, **XAVIER EDUARDO HERRERA ARCENTALES** autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación **"ANÁLISIS DEL MÉTODO ESTEGANOGRÁFICO COMO SOPORTE A LA SEGURIDAD DE LA IFORMACIÓN MEDIANTE LA OCULTACIÓN DE INFORMACIÓN SECRETA DENTRO DE UN VIDEO"** cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Sangolqui, 20 de febrero de 2018

XAVIER EDUARDO HERRERA ARCENTALES
C.C. 1716750144

# DEDICATORIA

***A mis padres, José Xavier y Cristina, quienes con su esfuerzo, amor y paciencia supieron guiarme por el camino de los valores, la perseverancia y han sido siempre un ejemplo y modelo a seguir.***

***A mis hermanos y familia en general, quienes a lo largo de mi vida han sabido estar en todo momento brindándome un apoyo incondicional e impulsándome a seguir adelante.***

***Xavier Euardo Herrera Arcentales***

# AGRADECIMIENTO

***A Dios por haberme dado la vida, la sabiduría para lograr mis objetivos y la oportunidad de crecer como un hombre de bien.***

***A mis padres y hermanos por su apoyo incondicional, la confianza y la fuerza que siempre supieron brindarme para no decaer y lograr mis objetivos.***

***A mi familia que ha sabido cómo darme el apoyo y la fuerza para seguir adelante y no dejarme vencer.***

***A mis maestros por la paciencia, conocimientos brindados y sobre todo por su amistad brindada durante el transcurso de mi vida estudiantil dentro de la Universidad.***

***A mis amigos que se convirtieron en la familia adicional y con quienes poco a poco hemos luchado para conseguir una meta más en nuestras vidas, una más a la lista de nuestras vidas.***

# ÍNDICE DE CONTENIDOS

# ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

# ÍNDICE DE ECUACIONES

# RESUMEN

La seguridad en la información hoy por hoy dentro de las comunicaciones es una ciencia cada vez más rigurosa en cuanto al manejo y procesamiento necesario para realizar una transferencia de datos o de información. Por esta razón y con el pasar de los años se han ido creando nuevas técnicas o mecanismos de seguridad de la información como son por ejemplo: marcas de agua, la criptografía, la esteganografía y muchas más, las cuales nos permiten tener un grado de seguridad y confianza al momento de transmitir información importante. En el presente proyecto de investigación busca manejar el método de la esteganografía con el fin de brindar seguridad en la información mediante sus múltiples características y beneficios pero ahora sobre un sistema un poco más complejo como es el video, para ello se procederá a manejar herramientas que permitan separar un video en sus dos componentes básicas, audio e imágenes. Una vez obtenidas estas dos secciones se procederá a ocultar un texto secreto dentro del audio e incrustar una imagen secreta dentro de la secuencia de imágenes propias del video, una vez oculta la información se volverá a unir las dos secciones para obtener un estego-video y posterior a ello lograr extraer la información oculta. Por último se verifica la eficiencia de los métodos utilizados mediante pruebas subjetivas (MOS) y subjetivas mediante el uso de herramientas estadísticas.

**Palabras clave:**

- ESTEGANOGRAFÍA
- ESTEGO-VIDEO
- FRAMES DE UN VIDEO
- AUDIO DE UN VIDEO
- INFORMACIÓN OCULTA

# ABSTRACT

Information security today in communications is an increasingly rigorous science regarding the handling and processing necessary to carry out a data or information transfer. For this reason and over the years have been created new techniques or information security mechanisms such as: watermarks, cryptography, steganography and many more, which allow us to have a degree of security and confidence when transmitting important information. In this research project seeks to manage the method of steganography in order to provide information security through its many features and benefits but now on a slightly more complex system such as video, it will proceed to handle tools that allow to separate a video in its two basic components, audio and images. Once these two sections have been obtained, a secret text will be hidden inside the audio and a secret image will be embedded within the sequence of the video's own images, once the information is hidden, the two sections will be merged again to obtain a video-stego and After that, extract the hidden information. Finally, the efficiency of the methods used by subjective (MOS) and subjective tests will be verified through the use of statistical tools.

**KEYWORDS:**

- STEGRANOGHAPHY
- STEGO-VIDEO
- VIDEO FRAMES
- AUDIO OF A VIDEO
- HIDDEN INFORMATION

# CAPÍTULO I

# INTRODUCCIÓN DEL PROYECTO DE INVESTIGACIÓN

## 1 Introducción del proyecto de investigación

### *1.1 Resumen del proyecto*

La seguridad en la información  al realizar una transferencia de datos e información, es uno de los temas muy cruciales y de mayor importancia dentro del ámbito de las comunicaciones. Por esta razón y con el pasar de los años se han ido creando nuevas técnicas o mecanismos de seguridad de la información como son por ejemplo: marcas de agua, la criptografía, la esteganografía y muchas más, las cuales nos permiten tener un grado de seguridad y confianza al momento de transmitir información importante.

En el presente proyecto se va a manejar el método de la esteganografía con el fin de brindar seguridad en la información mediante sus múltiples características y beneficios, para ello se proceder a manejar herramientas que permitan dividir a un video en audio e imágenes. Una vez obtenidas estas dos secciones procederemos a ocultar un texto secreto dentro del audio e incrustar una imagen secreta dentro de la secuencia de imágenes propias del video, una vez oculta la información se volverá a unir las dos secciones para obtener un Estego-Video, después se realizará el proceso de decodificación con el fin de recuperar en su mayoría la información oculta que se encuentra dentro del mismo.

### *1.2 Antecedentes y justificación del proyecto*

La necesidad de ocultar información en especial en la que se maneja el ámbito de las comunicaciones es un factor que se ha venido desarrollando desde hace mucho tiempo atrás, sus inicios se dan en la antigua Grecia en donde se utilizaba el cabello de los esclavos para poder ocultar mensajes tatuados en sus cabezas. Un ejemplo en el cual se puede evidenciar el proceso de ocultación de información son los jeroglíficos del antiguo Egipto, aunque ellos no se crearon con fines militares, suelen ser unos de los primeros ejemplos de escritura oculta de la historia. Según expertos, existan jeroglíficos no estándares los cuales se utilizaban para exagerar el dramatismo de un relato y por ende complicar su lectura. Otro ejemplo de escritura oculta es la escritura con tinta invisible la cual era fabricada con elementos caseros como vinagre, zumo de limón, leche, etc.

Si avanzamos en el tiempo podemos encontrar que la escritura oculta o la ocultación de información comienzan a evolucionar e involucrarse en ámbitos militares, es así como esta técnica refleja un punto importante en la historia dentro de la Segunda Guerra Mundial, en donde se utilizaban los periódicos para el envío de señales o mensajes ocultos mediante la realización de marcas en ciertas letras, que aunque por si solas pasaban inadvertidas en conjunto trasmitan una amplia cantidad de información. Durante el año de 1499 el escritor Francesco Colonna genera la primera escritura oculta dentro de su libro "Sueño de Polífilo" en el cual se puede obtener la frase <<*Poliam frater Franciscus Columna peramavit*>> ('El hermano Francesco Colonna ama

apasionadamente a Polia') tomando solamente la primera letra de los treinta y ocho capítulos que lo contiene.

Existen varios métodos conocidos para lograr la ocultación de la información, entre ellos los más usados son: el proceso de marca de agua, la técnica de la criptografía y la técnica de la esteganografía.

Dentro de la Universidad de las Fuerzas Armadas ESPE existen dos investigaciones realizados en los cuales se maneja las diferentes técnicas de esteganografía, es así el caso de ocultar una imagen dentro de otra utilizando las zonas ruidosas de la imagen mediante transformaciones de color reversibles (Onofre, 2016). Y el estudio orientado a la seguridad en los sistemas de comunicación utilizando técnicas de esteganografía para ocultar texto dentro de archivos de audio. (Rodríguez, 2016)

Conocidos estos preliminares el presente proyecto de investigación se enfoca al desarrollo de un sistema de seguridad de la información basado en métodos de esteganografía con el fin de ocultar información secreta como texto e imágenes dentro de un video.

## *1.3 Objetivos de la investigación*

### 1.3.1 *Objetivo general*

Analizar el método esteganográfico como soporte a la seguridad de la información mediante la ocultación de información secreta como texto e imágenes dentro de un video.

### *1.3.2 Objetivos específicos*

- Investigar sobre los métodos esteganográficos más óptimos para ocultar información dentro de un medio multimedia (video).
- Realizar un pre-procesamiento sobre el video original con el fin de obtener sus componentes de audio e imágenes.
- Insertar como información secreta un texto sobre los datos del audio obtenido después de la separación del video.
- Insertar como información secreta una imagen dentro de los frames de imágenes obtenidas del video.
- Aplicar métodos esteganográficos con el fin de recuperar la información oculta en un gran porcentaje.
- Verificar la eficiencia de los métodos utilizados mediante pruebas subjetivas (MOS) en una muestra de 15 personas y pruebas subjetivas mediante el uso de herramientas estadísticas.

# CAPITULO II

# MARCO TEÓRICO

## 2 Marco teórico

### *2.1 Procesamiento de señales*

Definiremos en un inicio a una señal como un parámetro que es capaz de variar en función del tiempo o del espacio y que sigue ciertas características definidas por su condición, sean éstas analógicas o digitales. Cualquier señal se encuentra expuesta a ser parte de un sistema, lo que implica que cada una puede ser sometida a modificaciones para obtener como resultado una señal de salida (Ver Figura 1).

Esta acción operar con una señal de entrada para obtener como resultado una señal de salida se puede definir como el procesamiento de una señal, en donde, a más de realizar operaciones con las señales de ingreso permite realizar análisis sobre dichas señales y que en su inicio comenzó con manejo de señales exclusivamente analógicas. (Moher, 2007)

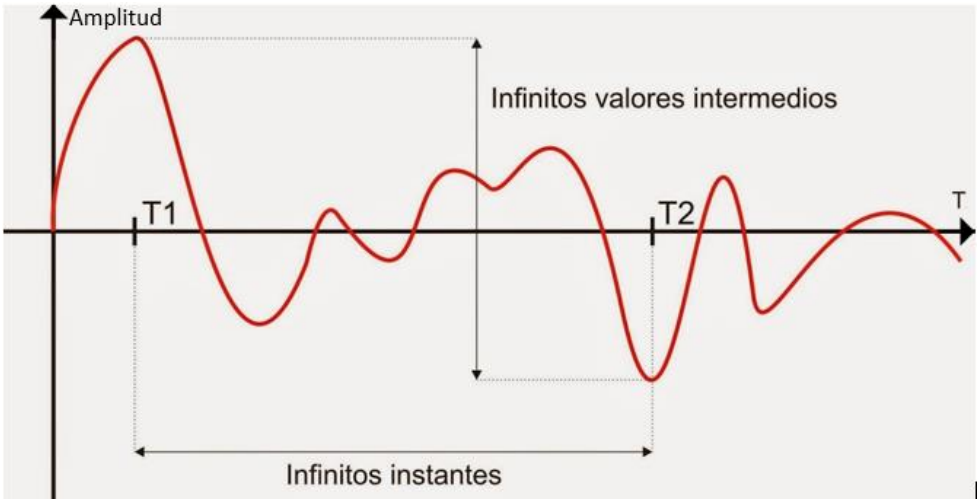
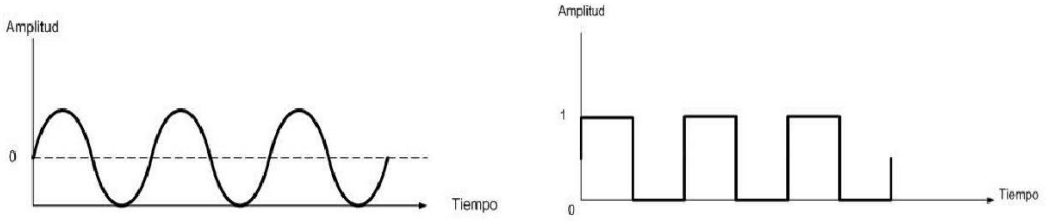



***Figura 1*** Señal analógica.

Fuente: (Shannon, 1949)

Con el nacimiento de la tecnología digital, el hombre se vio en la necesidad de crear una herramienta la cual le permita manejar y procesar las señales analógicas que existían de una manera más sencilla, entonces es ahí donde aparecen las señales digitales las cuales son la representación codificada de una señal analógica (Ver Figura 2). (Moher, 2007). Dentro del área de las comunicaciones, el procesamiento de señales analógicas es fundamental al momento de transmitir información de una sitio a otro, es por eso que las comunicaciones manejan como criterio fundamental tres pasos para realizar el procesamiento de señales al Muestreo, Cuantificación y Codificación. (Roden, 2018, Fifth Edition)




(a) (b)

***Figura 2.*** (a) Señal analógica. (b) Señal digital. Digitalización de una señal analógica.

Fuente: (Shannon, 1949)

### 2.1.1 Muestreo

El muestreo de una señal se puede definir como la cantidad de veces que se mide el valor de la señal analógica en un período de tiempo determinado, comúnmente se suele realizar cada un segundo como se puede observar en la Figura 3. (Moher, 2007)

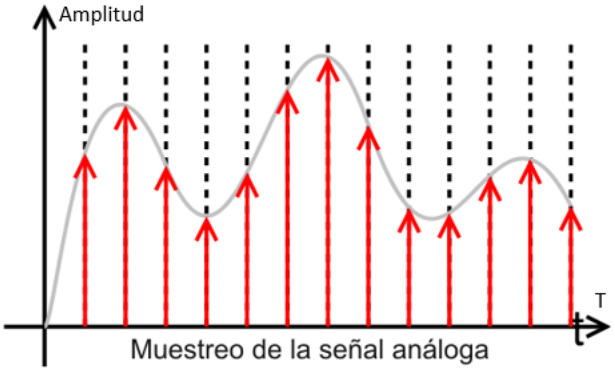



***Figura 3*** Muestreo de una señal analógica.

Fuente: (Shannon, 1949)

En este primer paso para digitalizar las señales analógicas surge el teorema de Nyquist (Ver Ecuación 1), el cual indica que para no perder la información de una señal

las veces que debemos muestrear la misma debe ser al menos el doble de la frecuencia máxima que posee esa señal. (Moher, 2007)

$$Fm \geq 2 * Fs$$

***Ecuación 1*** Ecuación del teorema de Nyquist

Donde Fs corresponde a la frecuencia propia de la señal analógica y Fm la frecuencia resultante del teorema. El teorema de Nyquist da la seguridad de no perder datos al momento de realizar el proceso de codificación de la señal analógica.

### 2.1.2 Cuantificación

El segundo paso que se requiere para lograr la digitalización de una señal sin que se pierda la mayor cantidad de información es el uso de la cuantificación que no es más que el número de símbolos requeridos para guardar una medida de una señal (Ver Ecuación 2). (Moher, 2007). Estas medidas son codificadas de acuerdo a un conjunto de bits, siguiendo la siguiente formula:

$$Nivel\ de\ cuantificación = 2\text{^}nbits$$

***Ecuación 2*** Ecuación para determinar el nivel de cuantificación de una señal

Donde nbits representa la longitud en bits que representaremos cada nivel de cuantificación obtenido. Mientras mayor sea el número de bits (nbits) que se empleen en la cuantificación se obtiene una menor pérdida de información de la señal analógica que queremos digitalizar. (Roden, 2018, Fifth Edition). Se puede observar un ejemplo de representación de la cuantificación de una señal en la Figura 4 a continuación.

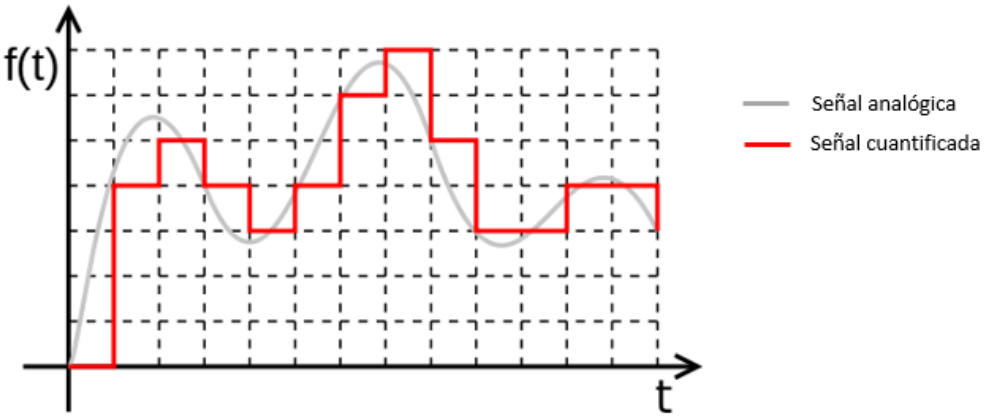



***Figura 4*** Señal cuantificada de acuerdo al nivel de cuantificación.

Fuente: (Shannon, 1949)

### 2.1.3 Codificación

Una vez que tenemos las medidas de la cuantificación de la señal, se procede a realizar el último paso de la digitalización de una señal análoga, este paso es la codificación, en donde el proceso que se realiza consiste en simplemente representar las medidas obtenidas del procedo de cuantificación de la señal mediante un código binario de 1 y 0 (Ver Figura 5) (Roden, 2018, Fifth Edition).

Una vez que se tiene un vector de valores de 1 y 0 se puede decir que la señal análoga se encuentra ya digitalizada y al momento de tener la señal digital (Ver Figura 5), ésta permite ser manipulada, en el caso puntual del presente proyecto de investigación se utilizará la señal digitalizada para modificar sus datos y ocultar información secreta dentro del contenido del audio de un video. (Moher, 2007).

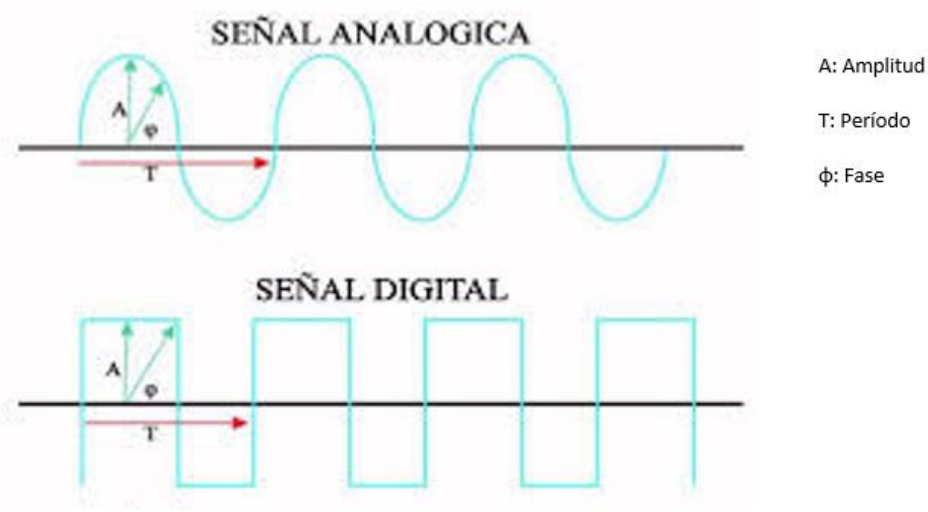



***Figura 5*** Señal digitalizada

Fuente: (Shannon, 1948)

La combinación de estos tres pasos para digitalizar una señal de tipo analógica es conocida como conversión analógica-digital (Ver Figura 6), hoy en día con el avance tecnológico existen conversores análogos-digitales y viceversa, un conversor digital-análogo se obtiene mediante el proceso inverso al mencionado con anterioridad, es decir, se cuenta con un vector de 1 y 0, el cual mediante los niveles de cuantificación se obtiene

una señal parecida a la análoga resultante y después de aplicar el teorema de Nyquist a la inversa, se obtiene la señal análoga. (Moher, 2007)

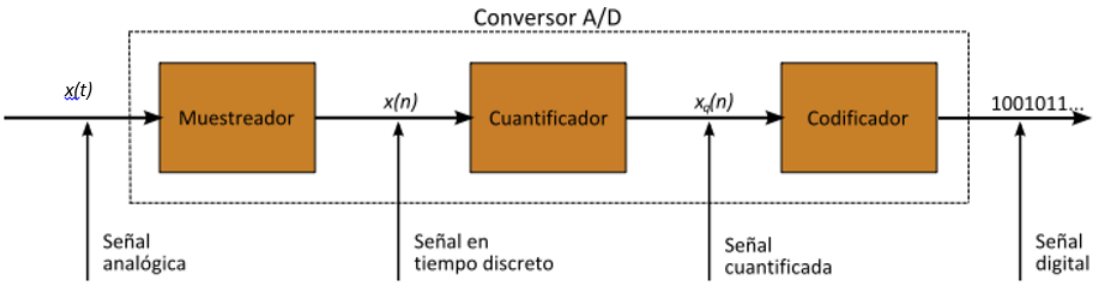



***Figura 6*** Diagrama de bloques de un Conversor Análogo – Digital. Procesamiento Digital de Señales

Fuente: (Shannon, 1949) (Shannon, 1948)

## 2.2 Información

### *2.2.1 Etimología*

El término información tiene un amplio desarrollo a lo largo de la historia, dentro del griego proviene del término “informationis”, éste término era utilizado para indicar o compartir un “concepto” o una “idea”. Así también el término de información proviene del sustantivo latino que da un significado a la frase “dar forma a la mente”, “instruir” o “enseñar”.

### *2.2.2 Definición*

Los conceptos antes mencionados dan como resultado que la información puede ser definida como la agrupación de datos ya supervisados y ordenados con el fin de ser transmitidos y compartidos con diferentes medios receptores ya sea de manera auditiva o visual, el motivo esencial de compartir la información es el de establecer modelos de pensamiento humano. Este mensaje es un recurso que otorga un sentido o significado a la realidad, es decir, que permite la interacción con otras personas o medios receptores y crear así una comunidad capaz de expresar ideas, emociones, etc. (Carvajal Gámez, 2008)

El receptor de la información tiene la capacidad de interpretar el mensaje que recibe de la manera que mejor le convenga; obviamente la percepción de la información que se recibe depende de cada individuo que obtiene esa información.

La información se caracteriza por cuatro conceptos primordiales que son: Los datos, el orden, la veracidad y el valor. Los datos de la información hacen referencia a los detalles, hechos, números y más parámetros recopilados y codificados, los cuales puedan ser almacenados para su uso futuro. El orden de la información es de suma importancia puesto que permite que la información transmitida tenga sentido y de esa manera se evita tener malos entendidos en caso de la comunicación verbal o errores en la recopilación de la información hablando de manera tecnológica. La veracidad de la información implica que los datos obtenidos deber provenir de fuentes confiables, esto permite que la información obtenida y que posteriormente pueda ser compartida sea válida y no genere dudas de su contenido. Y por último el valor de la información no es

más que reconocer por medio del medio receptor si aquellos datos transmitidos han sido útiles para él o las personas que recibieron dicha información. (Carvajal Gámez, 2008)

## 2.3 Transmisión de la información

La biodiversidad de nuestro planeta afirma que todas las especias tienen la facultad de comunicarse mediante la transmisión de información para su supervivencia; la diferencia que radica en los seres humanos es que se presenta la capacidad que tiene el hombre para discriminar la información que recibe y utilizarla a su conveniencia.

Cabe mencionar que existe una diferencia entre el concepto de transmisión de la información y la comunicación, siendo la comunicación un proceso bilateral en donde prevalece en el carácter recíproco entre emisor y transmisor lo que les convierte en interlocutores al tener la oportunidad de intercambiar constantemente sus roles; por otro lado, la transmisión de la información tiene un carácter unidireccional y estático en cuanto a los roles del emisor y receptor. Este proceso humano es utilizado para transmitir ideas, sentimientos, opiniones, diferentes puntos de vista sin necesidad de realizar interacción entre los extremos del sistema de comunicación. (Carvajal Gámez, 2008)

Como ejemplos básicos de transmisión de la información podemos mencionar la charla de un expositor en una conferencia, en donde solo el expositor es quien transmite las ideas y conocimientos que tiene, mientras que el público presente hace el papel de receptor solamente.

Los procesos empleados para compartir información han ido cambiado a lo largo de la historia de acuerdo al crecimiento y el avance tecnológico, es así que este proceso tiene sus inicios desde sistemas precarios como son las señales de humo, palomas mensajeras, o el uso de mensajeros para transmitir un mensaje, hasta llegar a las tecnologías de última generación que es el uso de sistemas celulares, microondas, comunicaciones satelitales, etc., que han permitido que la interconexión entre personas sea mucho más fácil. (Carvajal Gámez, 2008)

En la actualidad, la transmisión de la información ha evolucionado en una gran magnitud de tal manera que ahora es posible reemplazar cualquier tipo de proceso de transmisión empleado en la antigüedad por la manipulación de señales eléctricas con el fin de compartir la información que se tiene por cualquier medio físico o digital existente al momento. Con el crecimiento de las naciones y el deseo de poder que ha tenido el ser humano se vio en la necesidad de buscar métodos y formas en las cuales se podría transmitir la información de una manera segura y sin que sea vulnerada por extraños y es ahí de donde nace el concepto que se muestra en el presente proyecto de investigación, este concepto es la Seguridad de la Información.

## 2.4 Seguridad de la información

### *2.4.1 Ocultación de la información*

Una vez que la humanidad ha entendido la importancia del manejo de la información, busca también la oportunidad de enviar mensajes ocultos con el fin de que

el resto de personas no descubra la información que quiere transmitir, comienza a buscar métodos en los cuales la información enviada no puede ser intervenida o vulnerada por agentes externos.

Es entonces que desde hace mucho tiempo atrás el proceso de ocultar la información ha existido, algunos ejemplos prácticos en los cuales se ha utilizado métodos de ocultación de información se puede mencionar los siguientes: Escritura con “tinta invisible” fabricada con elementos de cocina como vinagre, zumo de limón, leche, etc., otro ejemplo claro es la ocultación de mensajes en libros como es el caso reconocido del libro “Sueño de Polífilo” escrito por Francesco Colonna en el año 1499 en donde se logra obtener la frase oculta ‘Poliam frater Franciscus Columna peramavit‘ (‘El hermano de Francesco Colonna ama apasionadamente a Polia’) solamente tomando la primera letra de los treinta y ocho capítulos que lo contiene. (Ver Figura 7).

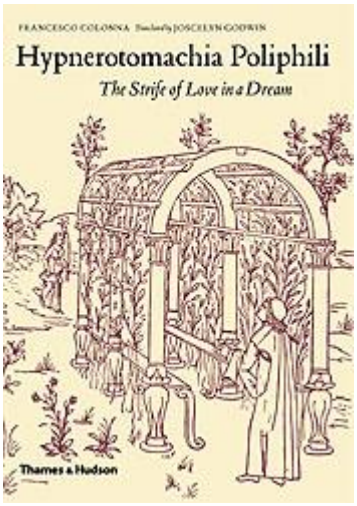



***Figura 7*** Portada del libro “Sueño de Polifilo”

Fuente: (Onofre, G., 2016)

Dentro del ámbito militar es en donde se ha utilizado con mayor frecuencia el término de ocultación de información, como por ejemplo, si nos remontamos a la época de la Segunda Guerra Mundial los grupos militares utilizaban los medios de comunicación en especial los periódicos de la época para el envío de señales ocultas que contenían mensajes secretos con sus planes de batalla y que no debían ser interceptados por sus adversarios, la metodología utilizada para ocultar información en esa época dentro de un periódico consistía en realizar marcas en ciertas letras, éstas marcas correspondían a puntos, líneas o algún tipo de señal que aunque por si solas pasaban inadvertidas en conjunto trasmitían formaban un patrón el cual contenía información oculta. (Carvajal Gámez, 2008)

Durante el transcurso de los años y el crecimiento del desarrollo tecnológico, los diferentes métodos para ocultar información han ido incrementando y mejorando, teniendo hoy en día como los principales métodos para ocultar información a la criptografía, el uso de marcas de agua y la esteganografía.

### *2.4.2 Métodos para ocultar información*

Existen una gran cantidad de métodos para ocultar información, en el presente proyecto de investigación mencionaremos los más utilizados en la actualidad y que han tenido resultados efectivos con sus propósitos.

Los métodos para ocultar información más utilizada son la criptografía, el uso de marcas de agua y la esteganografía, siendo éste el método que nos centraremos para el desarrollo del presente proyecto de investigación.

#### 2.4.2.1 *Criptografía*

Comenzaremos con la definición del método de la criptografía, ya que éste método es uno de los pioneros en éste ámbito. La criptografía es una técnica que viene dándose de mucho tiempo atrás, aproximadamente hace unos 4000 años en donde nace esta palabra proveniente de dos vocablos griegos que son, “kripto” que significa oculto y “graphos” que significa escritura. Por ende podemos definir a la criptografía como la ciencia que estudia lo relacionado a la escritura oculta. (Gambhir & Sibaram, 2016)

El objetivo principal que presenta éste método para ocultar información es el de compartir información siempre y cuando el emisor y receptor conozcan la manera única de extraer la información. Realizando una analogía para entender la criptografía, se lo puede asociar con un ejemplo básico como el uso de un cofre en donde la información que se requiere ser compartida va dentro del cofre y se utiliza un candado como medio de seguridad para evitar de que un tercero obtenga el mensaje oculto, el cofre solamente puede ser abierto por 2 llaves la que tiene el emisor y la que tiene el receptor, éstas llaves deben ser las mismas caso contrario el receptor no podrá recuperar el mensaje, determinando que solamente ellos serán los únicos que pueden abrir el candado y tomar el mensaje.

En el medio tecnológico sucede de manera igual a la analogía del cofre y el candado, en donde si una persona quiere transmitir información a otra sin que esta sea detectada por un tercero, ocupa un método para ocultar información, la encripta mediante una llave la cual conoce solamente el emisor y receptor, quienes serán los únicos que podrán extraer la información secreta. La característica principal de la criptografía es el uso de la encriptación como medio de seguridad o llave. (Gambhir & Sibaram, 2016)

La encriptación de la información es la ciencia que permite convertir datos en otros completamente distintos con el fin de que no se comprenda o no se logren visualizar los datos que se están enviando. La encriptación puede ser tomada también como el cifrado de información, el cual es una técnica en donde el mensaje que se transmite se encuentra desordenado de tal manera que la persona que lo intercepta no le encuentra un sentido. Esta es una medida adicional debido a que así como incrementan los conocimientos en cuanto a tecnología las maneras de vulnerar mensajes son mucho más óptimas, esta variación antes mencionada lo que permite es realizar el trabajo de un interceptor mucho más complicado y de esa manera la información se mantenga un poco más segura.

Uno de los primeros ejemplos del uso de la criptografía se remonta tiempo atrás en el antiguo Egipto en donde los jeroglíficos representaban las historias de su pueblo y sus misterios, esas imágenes talladas en los murales tenían el objetivo de dar un sentido de dramatismo al contar la historia de los pueblos egipcios, presentaban una dificultad al momento de interpretarlas debido al confuso sistema de imágenes y símbolos que en el transcurso de esas épocas eran solamente entendidas por el mismo pueblo de Egipto,

éste tipo de escritura se lo puede apreciar en la Figura 8 que se presenta a continuación. (Gambhir & Sibaram, 2016)

***Figura 8*** Murales con jeroglíficos egipcios.

Fuente: (Gambhir & Sibaram, 2016)

Unos siglos más tarde el cifrado de los mensajes evolucionó de tal manera que los Griegos crearon un instrumento llamado “Escítalo” (Ver Figura 9) el cual consistía en un cilindro, por lo general de madera, en el que se envolvía una tela. Una vez envuelta se procedía a escribir mensaje a lo largo de cada una de las generatrices del cilindro, para después enviarlo con un mensajero al receptor. El mecanismo funcionaba de tal manera que si no se contaba con un cilindro del mismo diámetro con el que se escribió en su inicio no se podría comprender el mensaje descrito. (Gambhir & Sibaram, 2016)

***Figura 9*** Ejemplo de un “escítalo” utilizado para enviar mensajes ocultos.

Fuente: (Gambhir & Sibaram, 2016)

Otro ejemplo memorable del uso de la criptografía es dentro del ámbito militar transcurrido durante la Segunda Guerra Mundial en donde gracias a la histórica máquina “Enigma” sus comunicaciones eran prácticamente indescifrables. Gracias al trabajo del personal militar estadounidense incluido el personal manejado por Alan Turing se pudo descifrar las tácticas militares de Japón. La máquina “Enigma” se puede considerar como una versión actualizada del “escítalo”, ya que ésta máquina operaba de manera casi automática formando códigos aleatorios para transmitir la información. El descubrimiento de los mensajes ocultos enviados por los militantes enemigos de Estados Unidos, el grupo de trabajo comandado por Alan Turing trabajó casi sin descanso por varios meses y lograr entender el funcionamiento de dicha máquina y así poder interceptar las comunicaciones enemigas. (Gambhir & Sibaram, 2016)

Con el paso del tiempo, el arte de la criptografía poco a poco se fue convirtiendo en un modelo matemático gracias a estudios realizados en el año de 1948 por Claude Shannon sobre las teorías de la información, escribe un libro llamado “Una teoría

matemática de la comunicación" (Shannon, A mathematical theory of communication, 1948) en donde demuestra que todas las fuentes de información pueden ser medibles. Posterior a ello, un año después escribe su investigación conocida como "La Teoría de las Comunicaciones Secretas", que permite definir a la criptografía como una ciencia. (Shannon, 1949). Y fue gracias al crecimiento de la tecnología, el nacimiento de la computadora en donde se puede validar que lo expuesto en su momento por Claude Shannon era correcto, así también los métodos algorítmicos de cifrado que se desarrollaban eran cada vez más complejos por lo que la seguridad en la información fue creciendo notablemente.

#### *2.4.2.2 Marca de agua*

Otro método de para ocultar información son las marcas de agua, éste método surge con la era digital y el mundo del internet, como se conoce, en internet se puede encontrar gran cantidad de información, es por ello que se utilizaron las marcas de agua como protección de los derechos de copia y propiedad intelectual de archivos de audio, documentos, etc., éste método facilita la identificación del creador, fuente, propietario o distribuidor de la información. La característica principal con la que cuenta este método es el que la marca es insertada directamente en el contenido de la información multimedia, esta información multimedia puede ser imágenes, audio o video sin problema. (Vargas, Elizabeth, & Di Gionantonio, 2016)

La diferencia que presenta el método de marca de agua con respecto al anterior descrito es que la información oculta es embebida dentro de la información lo que la

convierte en imperceptible, mientras que en la criptografía la información secreta es visible más incomprensible debido al cifrado que utiliza. A su vez, se diferencia con el método que vamos a detallar en el apartado siguiente, en la esteganografía la información secreta se encuentra relacionada con el objeto portador, lo cual lo convierte en un método prácticamente invisible e impredecible como se lo puede evidenciar en la Figura 10. (Coltuc, 2007)

Entre las propiedades más destacadas que presenta el método de marcas de agua se puede encontrar como principal la robustez, lo cual implica que la marca debe encontrarse presente en la información oculta así ésta sea expuesta a modificaciones, ampliaciones, etc., la resistencia a manipulaciones hace referencia a la característica de la robustez y lo que busca es que la marca presente resistencia a ataques hostiles realizados por terceros.

La imperceptibilidad es una propiedad única de la marca de agua puesto que la misma tiene como función básica la de ser un sistema totalmente imperceptible o transparente a la vista humana siempre y cuando se logre manejar una característica de degradación lo cual implica que la información secreta o marca insertada sea difícil de reconocer o apreciar.

El manejo de este tipo de proceso de ocultar información conlleva consigo un costo computacional que va de acuerdo al nivel de procesamiento que se requiera y de las aplicaciones que se le quiere dar a un sistema, es decir, que como en toda tecnología mientras más exacta o perfecta se intenta que sea, él costo computacional se incrementa. (Coltuc, 2007)

Por último la propiedad de la probabilidad de error en marcas de agua, este parámetro trata en su mayor parte del tiempo ser cada vez más bajo, es decir, que mientras mejor sea el proceso que se realice se podrá tener un mayor porcentaje de fallos al momento de intentar detectar la información que se encuentra oculta. (Vargas, Elizabeth, & Di Gionantonio, 2016)

***Figura 10*** Ejemplo del uso de la técnica de marcas de agua en imágenes.

Fuente: (Vargas, E., Di, G., 2016)

### *2.4.2.3 Esteganografía*

El presente proyecto de investigación se centra en el estudio y manejo de este método para ocultar información, el cual a través de la historia ha tenido variantes que han sido utilizadas con el fin de ocultar la información.

Etimológicamente la palabra esteganografía está compuesta por dos palabras griegas: *Steganos,* que significa oculto o secreto, y *Graphos, q*ue quiere decir texto o

dibujo. Lo cual nos da un significado básico de esteganografía como la ciencia que estudia el manejo de textos o dibujos ocultos. (Cole, 2003)

Al ser la esteganografía también un método para ocultar la información es fácilmente confundido con el método de la criptografía, y a pesar de que ambas ciencias tienen como fin evitar que la información que poseen no sea detectada, la criptografía utiliza el cifrado de la información que desea transmitir impidiendo que ésta pueda ser legible o sea detectada con facilidad a pesar de encontrarse a la vista de todos, éste proceso a pesar de ser bastante óptimo da el presentimiento de que existen datos ocultos dentro de la información transmitida por el mismo hecho de encontrarse a la vista de todos. (Gambhir & Sibaram, 2016)

Por su parte la esteganografía no se preocupa en cifrar la información que va a transmitir, simplemente se encarga de hacerla imperceptible para terceras personas a quienes no va dirigida la información. Conociendo estas simples pero claras diferencias entre ambas ciencias se puede definir que la esteganografía no es un tipo de criptografía, son técnicas completamente distintas que en ciertas ocasiones pueden complementarse entre ellas para obtener mejores resultados.

Dentro de la historia de la esteganografía han existido cientos de métodos utilizados, de los cuales los que tuvieron mayor significado podemos destacar los siguientes: En la Grecia antigua se utilizaba la cera de las velas para cubrir la información oculta de los textos escritos en tablas de madera, mencionado en el libro “Las Historias de Herodoto” entre los años 484 y 430 a.C.

Existieron también métodos más radicales como por ejemplo utilizar a un grupo de personas llamadas mensajeros, quienes eran afeitados las cabezas en su totalidad con el fin de que el mensaje que iban a transportar sea tatuado en ella, para poder enviar un mensaje tenían que esperar a que el cabello volviera a crecer y así llevar el mensaje. Una vez que los mensajeros llegaban a su destino eran rapados nuevamente para obtener el mensaje. En sus tiempos a pesar de ser un método radical era bastante efectivo ya que el mensaje no lo conocía ni el propio mensajero, él solamente se encargaba de transportar el mensaje consigo. (Gambhir & Sibaram, 2016)

Así como los ejemplos mencionados anteriormente existen muchos casos más en donde se aplicó la esteganografía como método para ocultar información y poder ser transmitida con la mayor seguridad posible. Cabe recalcar que en tiempos atrás los medios de comunicación con los que se contaba eran mucho más simples e incluso tenían sus limitaciones, como por ejemplo correo, teléfono analógico, etc. en donde la intercepción de los mensajes por terceros no tenía tanta influencia como lo es hoy en día debido al desarrollo de la tecnología en especial con la aparición de la computadora y el desarrollo de las telecomunicaciones.

Existen algunas técnicas que son utilizadas por parte de la esteganografía para lograr el objetivo de ocultar información, las técnicas que maneja la esteganografía son: *Watermaking* o Marca de Agua y *Fingerprinting* o Huellas dactilares. Si hablamos de los sistemas de *Watermaking*, éstos se encargan de realizar una modificación pequeña sobre los bits de la información a ser transmitida lo cual permite que el resultado obtenido sea

en su mayoría igual al original, éste método es utilizado en la actualidad con mucha frecuencia para el manejo de “firmas digitales” y el impedimento de la piratería.

Por su parte el Fingerprinting es utilizado en su mayoría para el manejo de identificación ya sea de usuarios, redes, productos. Éste método ayuda a mantener a que un producto ofrecido sea único. (Villa & Jaramillo, 2015)

Así como existen algunos modos para ocultar información, dentro la esteganografía existe a su vez diferentes métodos para utilizar esta técnica de ocultación de la información:

- **Métodos clásicos:** Éstos métodos son considerados como los inicios de la esteganografía con los ejemplos antes mencionados como son la escritura en tablas cubiertas con cera, los tatuajes con mensajes ocultos en las cabezas de los mensajeros o el manejo de tintas “invisibles” como vinagre, los cuales fueron conocidos como las primeras manifestaciones de la esteganografía en la historia.

- **Cifrado Nulo:** éste método es utilizado comúnmente en textos ya desde tiempo atrás y ha perdurado hasta nuestros tiempos ya que posiblemente, sea uno de los métodos esteganográficos más sencillos pero efectivos que existe. El cifrado nulo consiste en escribir un texto inofensivo aparentemente pero que el receptor de la información mediante un mecanismo conocido únicamente por el emisor y receptor del texto o

mensaje se puede obtener la información relevante del mismo. Éste tipo de método fue utilizado comúnmente durante la II Guerra Mundial ya que los militares necesitaban enviar mensajes con frecuencia a sus compañeros en batalla y más aún si se trataba de mensajes por parte de los infiltrados en tropas enemigas.

- **Tinta Invisible:** Al igual que el método anterior, éste método fue utilizado con frecuencia durante los conflictos de la Segunda Guerra Mundial, en especial dentro de los campos de prisioneros nazis. El modo de uso consistía en primero redactar una carta normal y una vez finalizada, se escribe el mensaje oculto entre líneas de la carta original con la “tinta invisible” que por lo general era el vinagre, zumos de fruta o en ocasiones la orina servía para realizar la escritura. La persona que recibía la carta debía calentar el papel y la escritura oculta se tornaba visible.

- **Micro puntos:** Como su nombre lo indica éste método se basaba en el uso de minúsculos puntos sobre una imagen, estos puntos eran imperceptibles por el ojo humano e incluso difícilmente perceptibles por instrumentos ópticos. Los puntos resultaban en parte ser invisibles pero que en conjunto formaban un patrón con la información enviada. Sin embargo no fue uno de los métodos más acertados para la esteganografía ya que durante la Guerra Fría éstos eran fácilmente detectables por parte de los expertos.

En la actualidad los métodos esteganográficos están ligados en su totalidad a la tecnología y al manejo de datos basándose en ocultar la información binaria dentro de las matrices de bits que conforman un fichero multimedia. Todo fichero puede ser representado por una cantidad de bits que pueden ser añadidos, modificados mediante algoritmos y así obtener un fichero resultante o estego-resultado, hablando directamente de la esteganografía como método de ocultación de la información. El fichero resultante o estego-resultado debe parecerse en su mayoría a la original una vez que contenga la información adicional que se quiere transmitir. (García Cano, 2004)

Los ficheros o medios portadores más utilizados para la técnica de la esteganografía son las imágenes ya que las características que poseen y el manejo computacional que requieren son mucho más simples y accesibles que el manejo con archivos de audio o archivos de video. A continuación detallaremos los formatos más utilizados en cuanto a imágenes se refiere:

- *Windows BitMap (BMP)*
- *PC Paintbrush (PCX)*
- *Graphics Image Format (GIF)*
- *Joint Photographic Experts Group (JPEG)*
- *Tagged Image File Format (TIFF)*
- *Portable Network Graphics (PNG)*

Para representar una imagen en un ordenador existen varias formas, sin embargo todas tienen un factor en común: tienen que representar colores mediante bits, bien sea

cada punto, vectores o matrices. La calidad de la imagen es un factor sumamente importante ya que gracias a la profundidad del color se obtendrá un resultado mucho más cercano a la realidad. Como todo procesamiento de información tiene como objetivo principal el lograr manejar la información sin que ésta se vea comprometida; hablando de la seguridad de la información, el objetivo principal es el de que la información que se encuentra oculta no logre ser vulnerada por terceros, ya que en caso de que eso suceda, el sistema implementado no cumple con el objetivo fundamental, por ende el método no es válido. (Villa & Jaramillo, 2015)

## 2.5 Imágenes como medio portador dentro de la esteganografía

Como se mencionó anteriormente, las imágenes son los medios digitales más utilizados para realizar el proceso de la esteganografía gracias al manejo de un modelo de colores llamado “Modelo RGB”.

Este modelo de colores RGB (“Red, Green, Blue”, en inglés), los colores se describen mediante un valor cuyo rango va desde 0 hasta 255. Mediante la combinación de los valores se tiene una gama de colores, una combinación de 256 x 256 x 256, un total de 16’777.216 posibles colores (Ver Tabla 1). (Onofre, 2016)

**Tabla 1**

*Tabla de colores primarios RGB*

| COLOR | R | G | B |
|---|---|---|---|
| Blanco | 255 | 255 | 255 |
| Rojo | 255 | 0 | 0 |
| Verde | 0 | 255 | 0 |
| Azul | 0 | 0 | 255 |
| Negro | 255 | 255 | 255 |

Una imagen puede ser analizada mediante una “cuadricula” en donde cada una de sus celdas tiene la forma de un número binario de 8 dígitos, es decir, un vector de “1” y “0” los cuales en conjunto forman a un número decimal entre 0 y 255 que correspondería al código de colores mostrado en la Tabla 1, cada una de las celdas formadas por la matriz tienen por nombre pixeles. (Onofre, 2016)

Un pixel puede ser definido como la unidad más pequeña y homogénea en color que conforma una imagen digital, la manera de visualizar un pixel es realizar un acercamiento profundo a una imagen mediante un software de edición, la característica principal de un pixel es que tiene en forma de un cuadrado. (Ver Figura 11)

Con la definición de pixel y lo mencionado anteriormente sobre el manejo de los datos, se puede tener una idea de la manera en la cual se utilizan los bits de una imagen

para poder ésta ser manipulada y tener cabida dentro de la técnica de la esteganografía mediante la modificación de un solo bit de cada valor de celda, por lo general este cambio se realiza en el bit menos significativo, ya que como su nombre lo indica es un bit que no modifica en su totalidad la información que se transmite.


***Figura 11*** Mapa de bits. Visualización de la composición de pixeles de una imagen
Fuente: (Villa, Jaramillo, 2015)

Ocultar información dentro de una imagen requiere de dos partes fundamentales, la primera debe ser la información a ser ocultada o el mensaje secreto que se quiere esconder; y la segunda se requiere de una imagen “portadora” la cual será quien aloje la información que se pretende esconder.

El desarrollo computacional para realizar el objetivo requerido necesita ser capaz de manipular los bits de la imagen portadora para colocar el mensaje, los sectores de la imagen portadora en los que es más óptimo ocultar información se le conoce como “zonas

ruidosas", que son las áreas en las cuales no se atrae la atención de la persona que observa la imagen.

El método básico de esteganografía es el uso del bit menos significativo (LSB o *Least Significant Bit*, en sus siglas en inglés), sin embargo también es el más vulnerable al momento de manipular la imagen, lo que quiere decir que es posible que la información escondida se pierda para siempre. (Arora & Pratap Singh, 2016)

La esteganografía maneja una serie de técnicas que permiten que éste método sea uno de los más eficientes para ocultar la información.

### 2.5.1 Técnicas de Esteganografía en Imágenes

- **Uso de claves:** Esta técnica se basa en el uso de codificadores que pueden ser establecidas para cada una de las diferentes etapas del mensaje a ocultar, estas claves son conocidas también como "llaves" lo cual permite que solo las personas que conocen dichas claves puedan tener acceso a la información oculta, esto permite que el método tenga un grado de seguridad más alto de lo normal.

- **Esteganografía en capas:** La técnica de utilizar capas para ocultar la información se trata de realizar el procesamiento de las imágenes con una secuencia establecida, es decir, que para ocultar la siguiente porción de la información se requiere del resultado del anterior procesamiento. Ésta técnica puede ser nombrada también como proceso de iteraciones. La eficiencia que presenta ésta

técnica se basa en que para encontrar el mensaje oculto se debe tener una secuencia establecida de decodificación ya que si no es así la información oculta no podrá ser encontrada.

- **Adición de ruido:** Además de modificar los bits necesarios para ocultar la información, se puede agregar algunos bits aleatorios dentro de la información de la imagen portadora, lo cual permite que si el atacante logra recuperar información oculta, ésta no sea real por la adición de ruido que se tiene.

Mediante ésta combinación de técnicas se puede manejar un correcto y seguro sistema de esteganografía y así lograr una mayor seguridad de la información. Y conjuntamente con las técnicas de la criptografía se puede conseguir que cualquier información sea oculta y pase inadvertida y así lograr el objetivo principal de este proyecto de integración. (Onofre, 2016)

## 2.6 Audio como medio portador dentro de la esteganografía

Al igual que en el apartado anterior, otro medio en el cual la información puede ser oculta, es el audio, a pesar de ser una señal analógica en su origen, ésta señal puede ser digitalizada en bits para de esa manera utilizar la información digital que posee y a su vez ser utilizada con diferentes aplicaciones, en este caso en específico, ser el medio por el cual se va a transmitir información oculta. (Rodríguez, 2016)

Antes de continuar con el método esteganográfico usado en audio, realizaremos unas definiciones cortas, pero que nos ayudarán a comprender el medio en el cual se inserta la información oculta. Primero podemos decir que el sonido es la variación de la presión ambiental que se propaga en forma de onda a través del aire. (Rossmann, 2014). Las formas de onda presentan tres características sumamente importantes y que son las que definen a una onda, amplitud, longitud de onda, período y frecuencia. (Ver Figura 12). La amplitud se define como la distancia máxima que pude alcanzar una onda con respecto a su posición de equilibrio. La longitud de onda es la distancia que existe entre dos puntos que se encuentran en el mismo estado de vibración (crestas o valles), una cresta es el punto en donde la amplitud de la señal es máxima y por encima de su eje de equilibrio; por el contrario, un valle representa el lugar donde la amplitud igual es máxima pero que se encuentra por debajo del eje de equilibrio. El período va de la mano de la longitud de onda, pues es el tiempo que requiere la onda en viajar una longitud de onda. La frecuencia, representa la cantidad de variaciones u oscilaciones que presenta una onda en un período de tiempo. (Rossmann, 2014)

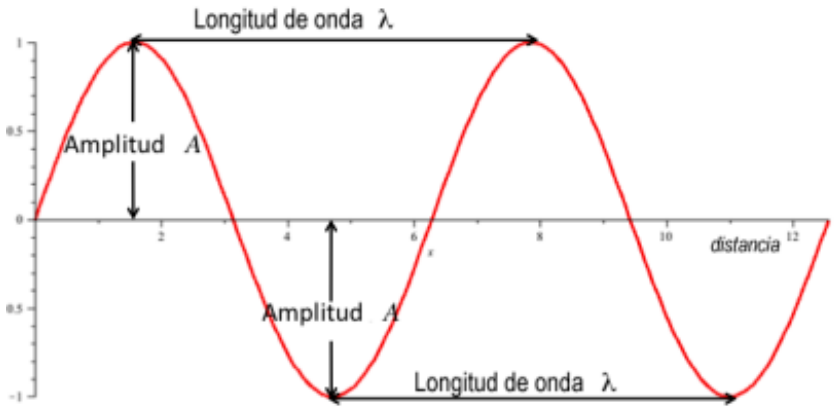



***Figura 12*** Elementos de una onda.

Fuente: (Rossman, 2014)

Una vez que tenemos claro los conceptos básicos que conforman una onda o un audio, como se puede observar las ondas son señales analógicas que viajan por el medio llamado aire, para lo cual estas señales de audio requieren de ser sometidas a un procesamiento en el cual se pueda representar esa señal de audio de manera digital para poder ser manipulada y estudiada. Por ello se utilizan las técnicas expuestas en el apartado de “Procesamiento de Señales” expuesto en el presente proyecto de investigación en donde se puede comprender el procedimiento que se requiere para digitalizar una señal de audio analógica. (Moher, 2007)

Una vez que la señal de audio es digitalizada, es decir, que la podemos tener en forma de bits, “1” y “0”, entran los métodos o técnicas que serán expuestas más adelante con el fin de cumplir en este caso el objetivo principal de la esteganografía que es el de compartir de una manera segura un mensaje hacia un receptor y si un mensaje transmitido genera sospecha o inclusive es detectado por un tercero, el sistema ha

fallado, por lo que hace que la técnica de esteganografía sea más complicada de efectuar en archivos de audio que en imágenes.

El proceso de esteganografía en audio consiste básicamente en utilizar el archivo de audio como portador de la información secreta que puede ser cualquier tipo de archivo, ya sea texto plano, imagen y otro archivo de audio como lo expuesto en (Rodríguez, 2016). Lo importante es entender el manejo correcto de la información tomando en cuenta uno de los principios fundamentales en los archivos de audio, que es el manejo de bits redundantes, estos bits son aquellos que como su nombre lo indica es la información que se encuentra duplicada en una porción de información y que su modificación no afecta la calidad del archivo portador y a su vez no compromete la técnica de la esteganografía. (Tayel, Gamal, & Shawky)

Así como en las imágenes, los archivos de audio también cuentan con diferentes técnicas utilizadas para lograr el objetivo de la esteganografía, cada uno cuenta con diferentes características las cuales aportan para mejorar las técnicas.

### 2.6.1 Técnicas de Esteganografía en Audio

- **Codificación del Bit Menos Significativo (LSB):**

  Ésta técnica es el más simple, así como se lo expuso en el presente proyecto de investigación en el apartado 2.5, sin embargo, es la técnica más eficiente en cuanto a la degradación de calidad de información oculta, ya que es la que menos altera la información del medio portador.

- **Codificación de Paridad:**

  Ésta técnica es robusta en comparación a la anterior mencionada ya que permite que el remitente obtenga la información secreta con más de una opción en la codificación de la información oculta. Se basa en el manejo de algoritmos que analizan la paridad de una secuencia de bits colocando la información secreta dentro de un bit de paridad que no siempre es el mismo y dependerá de la porción de información que se encuentre procesando.

- **Codificación de fase:** La codificación de fase dentro de un archivo de audio consiste en realizar el cambio de fase a un segmento del audio original o audio portador, y ser reemplazado por la fase codificada de la información secreta que se requiere transmitir. A pesar de ser una técnica muy eficiente, se debe tener cuidado ya que al crear un cambio de fase sumamente pronunciado dará como origen el término de dispersión de fase notable, lo cual permitirá a terceros notar con facilidad que existe algún tipo de información dentro del audio portador.

- **Amplio Espectro:** Conocido también en el área de las telecomunicaciones como *"Spread Spectrum (SS)"*, éste método es muy utilizado en cuando a comunicaciones se refiere, ya que no interactúa directamente con la señal de audio original sino que a su vez crea un algoritmo que es capaz de transmitir la información oculta a través del espectro en frecuencia de las señales. En este caso, de una señal de audio. Se asimila bastante al manejo de la técnica del Bit

Menos Significativo (LSB). Lo que caracteriza a esta técnica es que al manejar una señal independiente a la real, al conjugarse con ella, el resultado ocupa un mayor ancho de banda al que tenía originalmente.

Con el paso del tiempo y el crecimiento de las plataformas de reproducción, existe una variedad muy amplia de formatos digitales para archivos de audio, a continuación detallaremos algunas de las características que presentan estos formatos:

### 2.6.2 Formatos de Audio

- **Formato WAV:** (*Waveform Audio File*), éste formato fue desarrollado por la empresa Microsoft en conjunto con IBM, se caracteriza por no manejar ningún tipo de compresión de datos lo cual permite que sea de alta calidad. El formato WAV es uno de los más utilizados a nivel profesional ya que actualmente permite el manejo de una gran variedad de codec's. Su extensión es **.WAV**, maneja mono canales y canales estéreo y cuenta con una frecuencia de muestreo entre los 22050 Hz a 44100 Hz. (Rodríguez, 2016)

- **Formato WMA:** (*Windows Media Audio*), éste tipo de formato de audio fue desarrollado también por la empresa Microsoft con la diferencia de que éste formato si maneja compresión de datos, lo cual tiene como ventaja la de ocupar menos espacio de almacenamiento, en otras palabras, se puede tener muchos

más archivos de audio con extensión **.wma** que .wav, el contra que maneja éste tipo de formato es que al comprimir la información la calidad del audio disminuye, aunque la pérdida de información no es notoria muchas veces al oído humano al momento de procesar esa información se evidencia que los datos no se encuentran completos. maneja mono canales y canales estéreo y cuenta con una frecuencia de muestreo entre los 44100 Hz a los 48100 Hz. (Rodríguez, 2016)

- **Formato MP3:** El formato MP3 nació con la necesidad de almacenar mayor cantidad de archivos de audio con el mismo tamaño en disco, en ese entonces el uso del CD (*Compact Disk)* era mucho más frecuente y la idea de almacenar sin problema una cantidad de 100 archivos dentro de un CD era casi imposible, hasta que apareció el MP3. El formato se encargó de eliminar las porciones de información que eran irrelevantes para el oído humano, como por ejemplo los rangos de frecuencia mayores a 20 kHz y menores a 20 Hz, al eliminar esas frecuencias, los archivos tenían un tamaño menor lo cual permitió manejar un almacenamiento de una cantidad grandiosa de información. (Rodríguez, 2016)

Existe una gran variedad de formatos de audio que se utilizan actualmente mucho depende de las características que se requieren a nivel profesional, dependiendo también de los diferentes sistemas operativos y muchos otros factores.

Las técnicas estaganográficas en imágenes se basan en el manejo de algoritmos utilizando transformadas de Fourier o la transformada de cosenos; a su vez, la

esteganografía en audio se basa en la transformada wavelet, éste tipo de transformadas generan un costo computacional bastante grande, pero ayudan a mejorar la calidad de la esteganografía.

## 2.7 Video como medio portador dentro de la esteganografía

En el presente apartado nos centraremos en las propiedades y características que tiene un archivo de video para ayudar al manejo del método esteganográfico. El manejo de un audio como medio portador es un reto para el procesamiento de imágenes. (Mendoza, 2008)

### 2.7.1 Historia del Video

En éste apartado revisaremos un poco sobre el recorrido que ha tenido el video desde sus inicios hasta la fecha de hoy. La creación del cine o del video se dio de una manera exclusivamente experimental hasta que los hermanos Lumiere dieron con la creación del “Cinematógrafo”, el cinematógrafo utilizaba una película de 35 milímetros de ancho que al momento de girarla mediante una sistema logra capturar cada escena como una sola imagen y que al momento de ser proyectada, el hecho de transmitir una imagen tras otra genera una sensación de movimiento en el ojo humano. (Ver Figura 13)

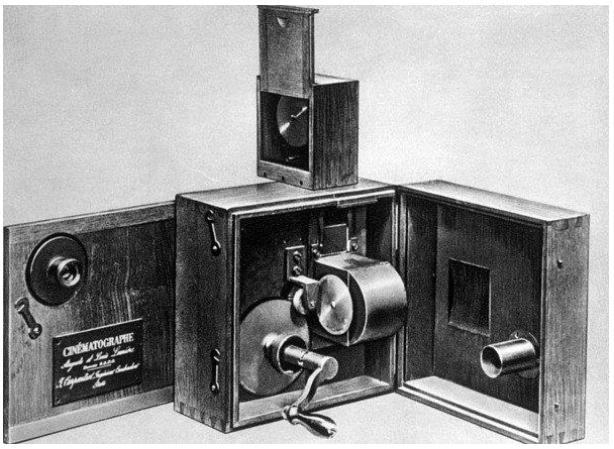



***Figura 13*** Cinematógrafo diseñado para la proyección de secuencias de imágenes

Fuente: (García Cano, D., 2004)

La creación del “cinematógrafo” dio como consecuencia varios estudios y avances científicos para comprender por qué el ojo humano no puede visualizar cada imagen de manera independiente sino que asimila la secuencia de imágenes como una secuencia en movimiento. Es así que Peter Mark Roget, en 1824 realiza una publicación de un estudio científico llamado “Persistencia de la visión”, en donde se establece que el ojo humano es capaz de retener una imagen durante una fracción de segundo después de que la persona haya visto la imagen y es por eso que se explica el motivo por el cual el ojo humano permite visualizar una secuencia en movimiento a partir de un grupo de imágenes. Y así se dan los inicios de los videos en el área de la ciencia de la cinematografía.

En base a lo expuesto con anterioridad, se puede generar un concepto, el video es la tecnología del procesamiento, grabación, almacenamiento, transmisión de una secuencia de imágenes que representan el movimiento.

Los videos manejan dos términos fundamentales, incluso para el área de la cinematografía, estos términos son; luminancia y crominancia. La luminancia corresponde a una variación de voltaje en la amplitud de la señal que va desde los -0.3 V a los 0.7 V. Y la crominancia que es la señal que es capaz de dar los diferentes tonos de colores.

Los videos también manejan un dato importante, que es su resolución, la resolución de un video es básicamente el tamaño de una imagen, si hablamos de un video analógico el tamaño se lo mide en líneas realizando un barrido horizontal o vertical, por el contrario el tamaño de un video digital se mide por pixeles, es decir, se mide el tamaño de la imagen digital que se muestra en ese momento.

Antes de que existan los videos, la única manera de mostrar imágenes era simplemente mediante fotografías, con el paso del tiempo se pudo observar que si se juntan varias fotografías con diferentes escenas y se las hace pasar a una velocidad moderada, el ojo humano lo visualiza como un movimiento continuo y sin cortes, es así como la definición de video fue creciendo.

### *2.7.2 Componentes del Video*

Los archivos de video cuentan con dos componentes fundamentales, las imágenes y el audio.

#### *2.7.2.1 Componente Audio*

En un principio retomando el concepto del audio, el audio de un video se maneja con la característica que debe tener sincronismo con lo que se visualiza en la secuencia de imágenes.

En la actualidad la digitalización de la información han permitido que el procesamiento, sincronismo, creación y edición de videos sea mucho más fácil, así como también los diferentes métodos expuestos en el apartado 2.6 del presente proyecto de investigación en donde se presenta las características y técnicas utilizadas para realizar el método de esteganografía en audio.

#### *2.7.2.2 Componentes Frames*

Otro componente fundamental de un video son los frames, estos frames no son más que la secuencia de imágenes que con la frecuencia de muestreo de dichas imágenes presentan una sensación de movimientos continuos. Ahora con la tecnología y las diferentes técnicas de procesamiento de imagen como las mostradas en el apartado 2.5 del presente proyecto un video puede ser transformado en imágenes para de esa manera utilizar las diferentes técnicas con imágenes que puedan ser requeridas.

En el presente proyecto de investigación se realiza ese proceso, para transformar un video y manipular los frames necesarios para nuestro método de esteganografía. (Illescas Robalino & Villamarín Zapata, 2011)

### 2.7.3 Formatos de Video

Al igual que las imágenes y los archivos de audio, los videos en la actualidad también cuentan con varios formatos que pueden ser utilizados. A continuación se presentará algunos de los formatos más utilizados en la actualidad. (Illescas Robalino & Villamarín Zapata, 2011)

- **Formato AVI:** (*Audio Video Interleaved*), su nombre en español tiene como traducción Audio y Video intercalado. Es el formato estándar para almacenar video en digital. Éste formato presenta una alta calidad de imagen y de sonido sin embargo el tamaño de los archivos es bastante grande por lo que se necesita una gran cantidad de almacenamiento. (Ite.educacion.es, s.f.)

- **Formato MPEG:** (*Moving Pictures Expert Group*), éste es el formato estándar para la compresión de archivos de video digital. Admite diversos tipos de códec's de video como son: MPEG-1 (Calidad CD), MPEG-2 (Calidad DVD), MPEG-3 (Calidad orientada para audio MP3) y MPEG-4 (Utilizado para videos en la web). (Ite.educacion.es, s.f.)

- **Formato MOV:** Para ir a la par con los formatos anteriores presentados, el formato MOV fue diseñado por la empresa Apple. Utiliza un códec de video propio el cual maneja una serie de actualizaciones en tiempos cortos, estas actualizaciones permiten que el manejo de videos en internet sea efectivo por motivo de su calidad

y peso. Lo que le caracteriza principalmente, es que el formato MOV fue diseñado para admitir *streaming*. (Ite.educacion.es, s.f.)

- **Formato WMV:** La empresa Microsoft también creó un formato de audio que maneja una alta calidad de imagen y a su vez bajo peso en almacenamiento, el formato WMV en la actualidad viene integrada dentro de Windows y es capaz de manejar *streaming*. (Ite.educacion.es, s.f.)

Al describir los formatos de video más utilizados, surge un término que es bastante utilizado en el área de las comunicaciones y la transmisión de la información, el *streaming*. La definición de *streaming* se basa en la manera más óptima para descarga y reproducción de archivos de video en línea, el *streaming* permite que la conexión con el servidor remoto de algún cliente que tenga un video en internet sea mucho más rápida. (Illescas Robalino & Villamarín Zapata, 2011)

El *streaming* tiene un proceso definido para funcionar correctamente, el cual detallaremos a continuación:

- Primero se realiza la conexión al servidor, el reproductor del cliente envía el archivo seleccionado a través del servidor remoto.
- Maneja un buffer, el buffer no es más que un almacenamiento dentro del servidor del cliente.

- Comienza la reproducción del video, una vez que el buffer se ha llenado con la información requerida, comienza a transmitir la información. Hasta que la descarga esté completa.

## 2.8 Aplicaciones de la esteganografía

Al tratarse de una medida de seguridad para la información, la esteganografía puede tener varias aplicaciones en las cuales sus métodos pueden ser parte del diario vivir, a continuación se presentarán algunas de las aplicaciones que actualmente tiene la esteganografía:

### *2.8.1 Aplicaciones Militares*

La seguridad de la información en el campo militar es de suma importancia ya que la información transmitida de un campo militar a otro debe ser confidencial. El uso más frecuente de medidas o técnicas de seguridad de la información se da principalmente en zonas de guerra. Si bien es cierto la tecnología militar en un principio no contaba con técnicas modernas para sus comunicaciones, hoy por hoy con el crecimiento de la tecnología utilizan con frecuencia implementos que son capaces de manejar técnicas como la esteganografía y la criptografía para transmitir su información. (Sugathan, 2016)

### 2.8.2 *Derechos de autor*

Esta aplicación es utilizada con mucha frecuencia en el ámbito de las artes como música, películas, animaciones, etc., en donde el requerimiento más importante es conseguir la autorización del autor para poder ocultar su información dentro de algún trabajo realizado. Se utiliza estos métodos con el fin de evitar que los trabajos realizados por un artista se vean comprometidos en algún caso de copia o piratería. (Sugathan, 2016)

### 2.8.3 *Aplicaciones Médicas*

Aunque dentro de la medicina no se tiene un panorama claro de cómo podría tener un uso efectivo de la esteganografía, a mi parecer ésta técnica puede ser utilizada para mantener la confidencialidad de los resultados médicos de un cliente determinado, de tal manera que solamente el médico tratante y el paciente puedan tener acceso a esa información. (Sugathan, 2016)

# CAPITULO III

# METODOLOGÍA DEL PROYECTO DE INVESTIGACIÓN

## 3 Metodología

### 3.1 Descripción general del proyecto de investigación

El presente proyecto de investigación consiste en el uso de la técnica de la esteganografía en base a la combinación de un método utilizando el bit menos significativo para incluir la información en el audio y otro método basado en la detección de zonas ruidosas o puntos clave de una imagen en la cual puede ser embebida la información que queremos ocultar.

Con el fin de obtener seguridad en la información mediante la técnica de ocultación de información conocida como esteganografía se tomará en cuenta dos definiciones importantes que se van a manejar a lo largo del presente proyecto de investigación, las cuales son: (Suarez, Carvajal, & Carreto, 2015)

- Información oculta: corresponde en este caso a un texto y una imagen que se quiere ocultar.
- Video anfitrión: hace referencia al video original en el cual se va a incluir la información.

- EEstego-Video: corresponde al video en el cual ya se encuentra incluida la información oculta.

Estas definiciones las podremos observar de una manera más amplia en la Figura 14.

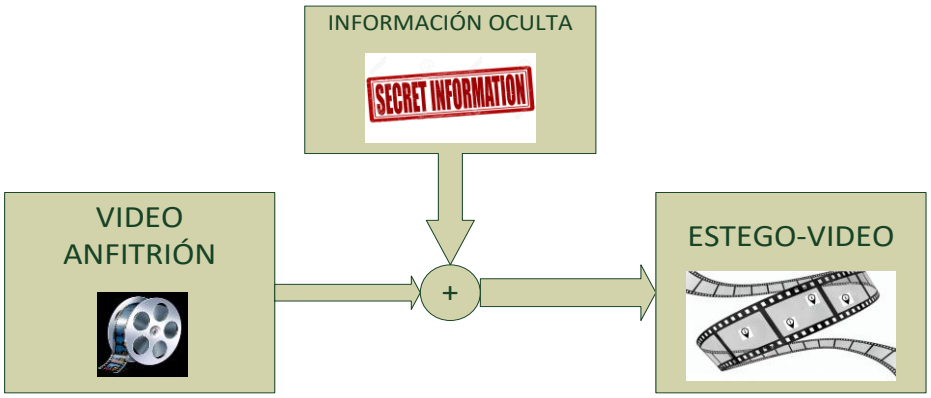



***Figura 14*** Diagrama de bloques del método de la esteganografía aplicada en video

## 3.2 Extracción de componentes del video

A continuación se presenta en detalle el desarrollo del método esteganográfico a ser utilizado para ocultar información dentro de un video para lo cual primero se realiza un procesamiento al video anfitrión mediante una herramienta computacional (VLC, FFmpeg, etc) la cual nos permitirá separarlo en sus dos principales componentes multimedia: audio e imágenes, de tal manera que este proceso permita trabajar sus dos componentes de manera independiente. (FFmpeg, s.f.) (Kempf, s.f.)

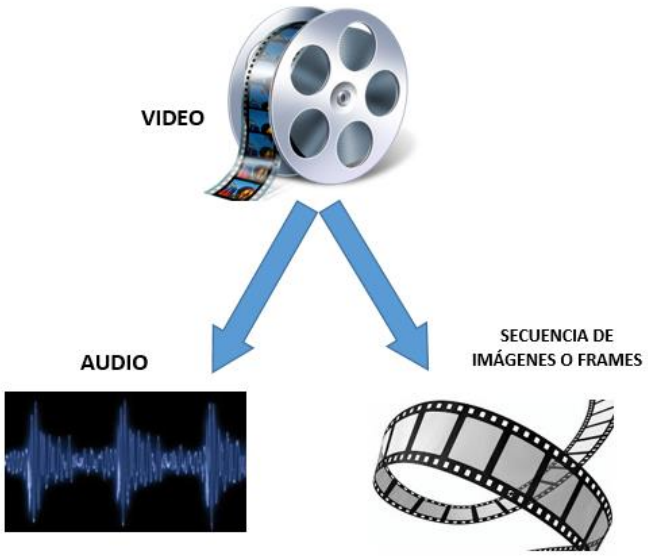



***Figura 15*** Componentes básicos de un video

Como se expuso con anterioridad un video no es más que una serie de imágenes consecutivas que por efecto del movimiento hacen parecer ante el ojo humano una secuencia sin cortes, es ahí que se manejará los frames o imágenes del video para en ellos tener como información oculta otra imagen cualesquiera; por su parte otra de las componentes multimedia de un video es su audio, en el cual se ocultará un mensaje de texto. (Ver Figura 15)

Para lograr este objetivo de separar las componentes del video se ha tomado como herramienta computacional a MATLAB ya que es una herramienta computacional y de procesamiento sumamente fuerte y con características excepcionales en cuando al manejo de señales, en este caso, señales de audio e imágenes.

### 3.2.1 Procesamiento del audio

Para poder ocultar la información secreta dentro de un audio debemos lograr acceder a la información que existe en el mismo de tal manera que mediante el uso de alguna técnica esteganográfica de inserción de información permita incluir un mensaje de texto secreto sin que este distorsione al audio y no pueda ser detectado por algún tipo de atacante.

La herramienta computacional MATLAB brinda la opción de extraer el audio de un video mediante el uso de la función: *audioread* para realizar un mejor manejo del audio en MATLAB es recomendable utilizar el formato .wav por las características que lo conforman.

Una vez que el audio se encuentra separado del video se procede con la codificación del mismo, puesto que como se expuso en el presente proyecto de investigación para manipular o en este caso incluir información dentro de un elemento multimedia como el audio se requiere que el mismo se encuentre digitalizado para lo cual se expondrá el procesamiento fundamental de una señal analógica para convertirla en digital mediante los pasos: muestreo, cuantificación y codificación, en el caso puntual del presente proyecto de investigación se utilizará el proceso hasta la cuantificación de la señal puesto que el proceso de codificación por lo general es utilizado para realizar transmisión de información por canales simulados o reales.

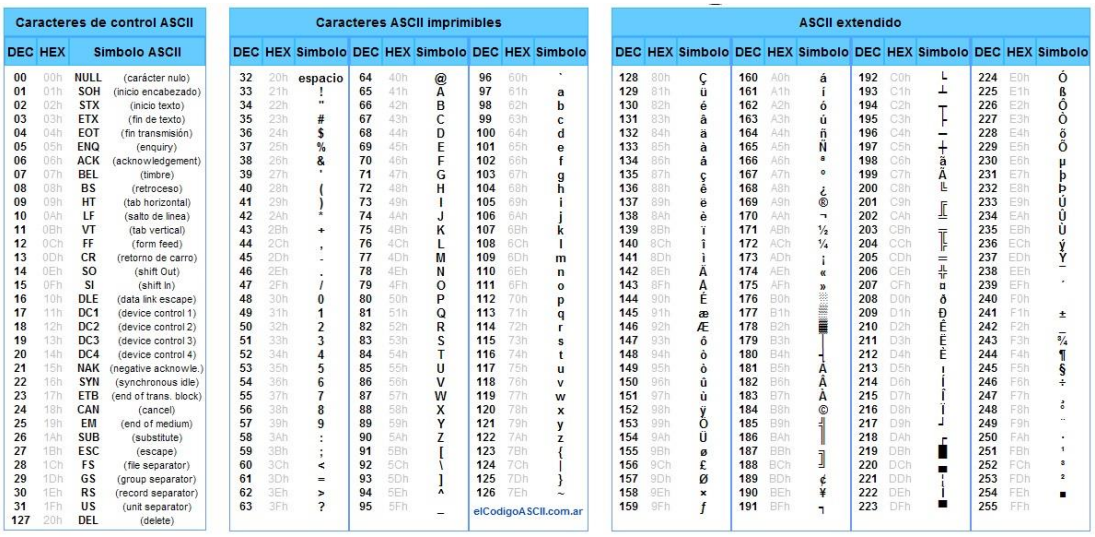
El muestreo de la señal se lo realiza basándose en el teorema de Nyquist, en donde se basa en el uso del doble de la frecuencia fundamental de la señal analógica para tomar valores de dicha señal.

Después de obtener las muestras de la señal, se procede con la cuantificación de la señal con el fin de evitar la pérdida de la información, para ello se ubica niveles de cuantificación que corresponden a la fórmula $2^n = niveles.$ Para lograr un procesamiento confiable evitando un alto porcentaje de pérdidas de la señal se debe aumentar el valor de n para que existan más niveles de referencia. En el caso del presente proyecto de investigación se realizó pruebas con diferentes niveles de cuantificación en donde se encontró que el nivel más óptimo para evitar una gran pérdida de información y sin que se distorsione la señal original de audio fueron 128 niveles.

El resultado final de los procesos anteriores nos da como resultado un vector de audio en valores decimales en el cual se va a embeber la información secreta, en este caso la información a ocultar es un texto que tiene que ser convertido a bits en su primera fase para poder manejarlo y ocultarlo dentro del audio.

Una vez que se tiene el texto en forma de bits y el audio en matriz decimal después de la cuantificación se utilizará la técnica esteganográfica del bit menos significativo (LSB) y mediante el uso de aplicaciones propias de la herramienta computacional MATLAB, se utilizará la función *bitset* la cual nos permite incluir el vector de bits necesarios dentro de otro vector que será el portador.

La transformación de un texto a bits, puede ser aplicado mediante el manejo de código ASCII (Ver Figura 16).



**Caracteres de control ASCII**

| DEC | HEX | Simbolo ASCII | |
|---|---|---|---|
| 00 | 00h | NULL | (carácter nulo) |
| 01 | 01h | SOH | (inicio encabezado) |
| 02 | 02h | STX | (inicio texto) |
| 03 | 03h | ETX | (fin de texto) |
| 04 | 04h | EOT | (fin transmisión) |
| 05 | 05h | ENQ | (enquiry) |
| 06 | 06h | ACK | (acknowledgement) |
| 07 | 07h | BEL | (timbre) |
| 08 | 08h | BS | (retroceso) |
| 09 | 09h | HT | (tab horizontal) |
| 10 | 0Ah | LF | (salto de linea) |
| 11 | 0Bh | VT | (tab vertical) |
| 12 | 0Ch | FF | (form feed) |
| 13 | 0Dh | CR | (retorno de carro) |
| 14 | 0Eh | SO | (shift Out) |
| 15 | 0Fh | SI | (shift In) |
| 16 | 10h | DLE | (data link escape) |
| 17 | 11h | DC1 | (device control 1) |
| 18 | 12h | DC2 | (device control 2) |
| 19 | 13h | DC3 | (device control 3) |
| 20 | 14h | DC4 | (device control 4) |
| 21 | 15h | NAK | (negative acknowle.) |
| 22 | 16h | SYN | (synchronous idle) |
| 23 | 17h | ETB | (end of trans. block) |
| 24 | 18h | CAN | (cancel) |
| 25 | 19h | EM | (end of medium) |
| 26 | 1Ah | SUB | (substitute) |
| 27 | 1Bh | ESC | (escape) |
| 28 | 1Ch | FS | (file separator) |
| 29 | 1Dh | GS | (group separator) |
| 30 | 1Eh | RS | (record separator) |
| 31 | 1Fh | US | (unit separator) |
| 127 | 20h | DEL | (delete) |

**Caracteres ASCII imprimibles**

| DEC | HEX | Simbolo | DEC | HEX | Simbolo | DEC | HEX | Simbolo |
|---|---|---|---|---|---|---|---|---|
| 32 | 20h | espacio | 64 | 40h | @ | 96 | 60h | ` |
| 33 | 21h | ! | 65 | 41h | A | 97 | 61h | a |
| 34 | 22h | " | 66 | 42h | B | 98 | 62h | b |
| 35 | 23h | # | 67 | 43h | C | 99 | 63h | c |
| 36 | 24h | $ | 68 | 44h | D | 100 | 64h | d |
| 37 | 25h | % | 69 | 45h | E | 101 | 65h | e |
| 38 | 26h | & | 70 | 46h | F | 102 | 66h | f |
| 39 | 27h | ' | 71 | 47h | G | 103 | 67h | g |
| 40 | 28h | ( | 72 | 48h | H | 104 | 68h | h |
| 41 | 29h | ) | 73 | 49h | I | 105 | 69h | i |
| 42 | 2Ah | * | 74 | 4Ah | J | 106 | 6Ah | j |
| 43 | 2Bh | + | 75 | 4Bh | K | 107 | 6Bh | k |
| 44 | 2Ch | , | 76 | 4Ch | L | 108 | 6Ch | l |
| 45 | 2Dh | - | 77 | 4Dh | M | 109 | 6Dh | m |
| 46 | 2Eh | . | 78 | 4Eh | N | 110 | 6Eh | n |
| 47 | 2Fh | / | 79 | 4Fh | O | 111 | 6Fh | o |
| 48 | 30h | 0 | 80 | 50h | P | 112 | 70h | p |
| 49 | 31h | 1 | 81 | 51h | Q | 113 | 71h | q |
| 50 | 32h | 2 | 82 | 52h | R | 114 | 72h | r |
| 51 | 33h | 3 | 83 | 53h | S | 115 | 73h | s |
| 52 | 34h | 4 | 84 | 54h | T | 116 | 74h | t |
| 53 | 35h | 5 | 85 | 55h | U | 117 | 75h | u |
| 54 | 36h | 6 | 86 | 56h | V | 118 | 76h | v |
| 55 | 37h | 7 | 87 | 57h | W | 119 | 77h | w |
| 56 | 38h | 8 | 88 | 58h | X | 120 | 78h | x |
| 57 | 39h | 9 | 89 | 59h | Y | 121 | 79h | y |
| 58 | 3Ah | : | 90 | 5Ah | Z | 122 | 7Ah | z |
| 59 | 3Bh | ; | 91 | 5Bh | [ | 123 | 7Bh | { |
| 60 | 3Ch | < | 92 | 5Ch | \ | 124 | 7Ch | \| |
| 61 | 3Dh | = | 93 | 5Dh | ] | 125 | 7Dh | } |
| 62 | 3Eh | > | 94 | 5Eh | ^ | 126 | 7Eh | ~ |
| 63 | 3Fh | ? | 95 | 5Fh | _ | | | |

elCodigoASCII.com.ar

**ASCII extendido**

| DEC | HEX | Simbolo | DEC | HEX | Simbolo | DEC | HEX | Simbolo | DEC | HEX | Simbolo |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 128 | 80h | Ç | 160 | A0h | á | 192 | C0h | └ | 224 | E0h | Ó |
| 129 | 81h | ü | 161 | A1h | í | 193 | C1h | ┴ | 225 | E1h | ß |
| 130 | 82h | é | 162 | A2h | ó | 194 | C2h | ┬ | 226 | E2h | Ô |
| 131 | 83h | â | 163 | A3h | ú | 195 | C3h | ├ | 227 | E3h | Ò |
| 132 | 84h | ä | 164 | A4h | ñ | 196 | C4h | ─ | 228 | E4h | õ |
| 133 | 85h | à | 165 | A5h | Ñ | 197 | C5h | ┼ | 229 | E5h | Õ |
| 134 | 86h | å | 166 | A6h | ª | 198 | C6h | ã | 230 | E6h | µ |
| 135 | 87h | ç | 167 | A7h | º | 199 | C7h | Ã | 231 | E7h | þ |
| 136 | 88h | ê | 168 | A8h | ¿ | 200 | C8h | ╚ | 232 | E8h | Þ |
| 137 | 89h | ë | 169 | A9h | ® | 201 | C9h | ╔ | 233 | E9h | Ú |
| 138 | 8Ah | è | 170 | AAh | ¬ | 202 | CAh | ╩ | 234 | EAh | Û |
| 139 | 8Bh | ï | 171 | ABh | ½ | 203 | CBh | ╦ | 235 | EBh | Ù |
| 140 | 8Ch | î | 172 | ACh | ¼ | 204 | CCh | ╠ | 236 | ECh | ý |
| 141 | 8Dh | ì | 173 | ADh | ¡ | 205 | CDh | ═ | 237 | EDh | Ý |
| 142 | 8Eh | Ä | 174 | AEh | « | 206 | CEh | ╬ | 238 | EEh | ¯ |
| 143 | 8Fh | Å | 175 | AFh | » | 207 | CFh | ¤ | 239 | EFh | ´ |
| 144 | 90h | É | 176 | B0h | ░ | 208 | D0h | ð | 240 | F0h | |
| 145 | 91h | æ | 177 | B1h | ▒ | 209 | D1h | Ð | 241 | F1h | ± |
| 146 | 92h | Æ | 178 | B2h | ▓ | 210 | D2h | Ê | 242 | F2h | ‗ |
| 147 | 93h | ô | 179 | B3h | │ | 211 | D3h | Ë | 243 | F3h | ¾ |
| 148 | 94h | ö | 180 | B4h | ┤ | 212 | D4h | È | 244 | F4h | ¶ |
| 149 | 95h | ò | 181 | B5h | Á | 213 | D5h | ı | 245 | F5h | § |
| 150 | 96h | û | 182 | B6h | Â | 214 | D6h | Í | 246 | F6h | ÷ |
| 151 | 97h | ù | 183 | B7h | À | 215 | D7h | Î | 247 | F7h | ¸ |
| 152 | 98h | ÿ | 184 | B8h | © | 216 | D8h | Ï | 248 | F8h | ° |
| 153 | 99h | Ö | 185 | B9h | ╣ | 217 | D9h | ┘ | 249 | F9h | ¨ |
| 154 | 9Ah | Ü | 186 | BAh | ║ | 218 | DAh | ┌ | 250 | FAh | · |
| 155 | 9Bh | ø | 187 | BBh | ╗ | 219 | DBh | █ | 251 | FBh | ¹ |
| 156 | 9Ch | £ | 188 | BCh | ╝ | 220 | DCh | ▄ | 252 | FCh | ³ |
| 157 | 9Dh | Ø | 189 | BDh | ¢ | 221 | DDh | ¦ | 253 | FDh | ² |
| 158 | 9Eh | × | 190 | BEh | ¥ | 222 | DEh | Ì | 254 | FEh | ■ |
| 159 | 9Fh | ƒ | 191 | BFh | ┐ | 223 | DFh | ▀ | 255 | FFh | |

***Figura 16*** Tabla de caracteres del código ASCII

Fuente: (Ite.educacion.es, s.f.)

El código ASCII no es más que la representación de un carácter en base a un código que puede ser entendido por la máquina. A su vez los caracteres de texto pueden ser representados de manera binaria directamente mediante (Ver Figura 17).

| LETRA | LETRA EN BINARIO | LETRA | LETRA EN BINARIO |
|---|---|---|---|
| A | 01000001 | a | 01100001 |
| B | 01000010 | b | 01100010 |
| C | 01000011 | c | 01100011 |
| D | 01000100 | d | 01100100 |
| E | 01000101 | e | 01100101 |
| F | 01000110 | f | 01100110 |
| G | 01000111 | g | 01100111 |
| H | 01001000 | h | 01101000 |
| I | 01001001 | i | 01101001 |
| J | 01001010 | j | 01101010 |
| K | 01001011 | k | 01101011 |
| L | 01001100 | l | 01101100 |
| M | 01001101 | m | 01101101 |
| N | 01001110 | n | 01101110 |
| O | 01001111 | o | 01101111 |
| P | 01010000 | p | 01110000 |
| Q | 01010001 | q | 01110001 |
| R | 01010010 | r | 01110010 |
| S | 01010011 | s | 01110011 |
| T | 01010100 | t | 01110100 |
| U | 01010101 | u | 01110101 |
| V | 01010110 | v | 01110110 |
| W | 01010111 | w | 01110111 |
| X | 01011000 | x | 01111000 |
| Y | 01011001 | y | 01111001 |
| Z | 01011010 | z | 01111010 |

***Figura 17*** Tabla de códigos binarios de letras.

Fuente: (Ite.educacion.es, s.f.)

Hay que tener en cuenta que para escribir un solo carácter en binario se requiere de una secuencia de 8 bits de 1 o 0, es decir, que para transformar a binario la palabra “Hola”, se requiere de 8 bits * 4 letras = 32 bits.

En el presente proyecto de investigación se realizó el proceso de manejar el texto como: “*mensaje de prueba”*, el vector en binario del mensaje quedaría de la siguiente manera representado como una matriz de 17x8 ya que cada una de las filas corresponde

a una letra del texto y se incluyen también los espacios entre palabras que cuentan también con una representación en binario. (Ver Tabla 2).

**Tabla 2**

*Matriz de Texto convertido a bits*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 |
| 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 |
| 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 |
| 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |

Una vez obtenidos los valores en binario de cada uno de los caracteres de texto se procede a la incrustación de los bits dentro de la señal de audio digitalizada. Éste proceso se lo puede comprender mejor en base al diagrama de bloques mostrado a continuación en la Figura 18:

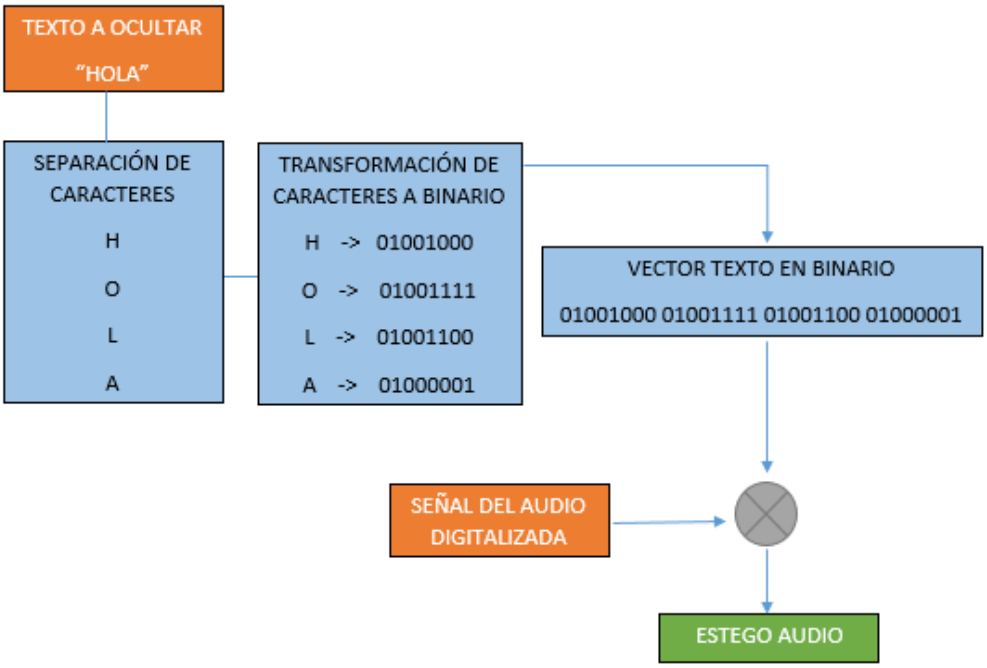
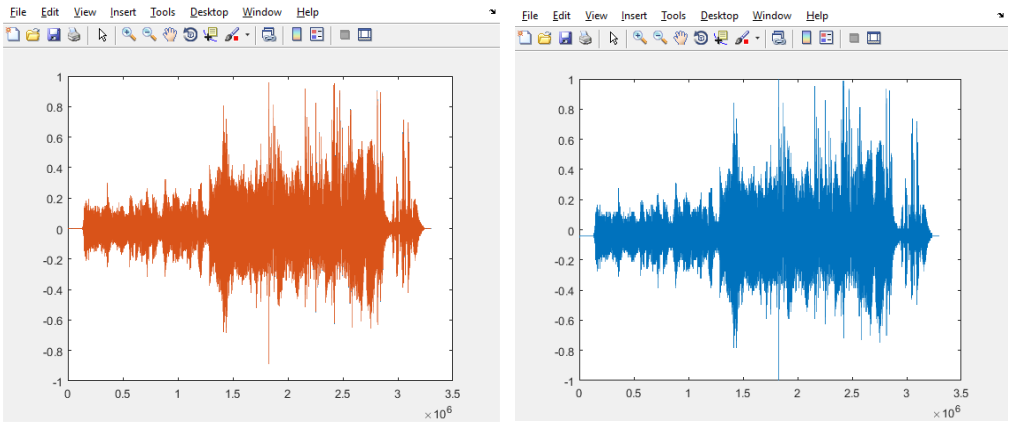



***Figura 18*** Diagrama de bloques del proceso para transformación y ocultación del texto dentro del audio

En donde se evidencia que la señal de audio original y el Estego-Audio no reflejan modificaciones evidenciables dentro de su señal visible. (Ver Figura 19)



(a) (b)

***Figura 19*** (a) Señal de audio original. (b) Señal del Estego-Audio

### 3.2.2 Procesamiento de los frames

Una vez realizado el procesamiento de la sección del audio se procede con la etapa del procesamiento de los frames. Para ello lo primero que se realizó en el presente proyecto de investigación mediante el uso de la herramienta MALTAB es separar los frames de todo el video original.

Mediante una función propia de MATLAB llamada *VideoReader*, se pueden obtener todos los frames de un archivo de video, la función *VideoReader* tiene la característica de manejar codec's de video MPEG-1 y MPEG-4.

Al ser un video una secuencia de imágenes, se puede utilizar cada una de ellas para realizar un procesamiento diferente, lo cual podría tornarse como una ventaja de utilizar un video como medio portador para ocultar información ya que es capaz de almacenar en su interior una cantidad grande de información, sin embargo, se debe tomar en cuenta la complejidad del procesamiento e inclusive se puede tener como consecuencia tamaño de videos resultantes sumamente elevados, lo cual complicaría realizar el proceso de ocultar información ya que a su vez dejaría en evidencia de que dentro de ese archivo se encuentra más información de la que realmente existe.

En el presente proyecto de investigación se utilizó un video con las siguientes características: (Ver Figura 20)

- Duración: 01:14 min
- Ancho del fotograma: 1280 pixeles
- Alto del fotograma: 720 pixeles
- Velocidad del fotograma: 24 frames/segundo aproximadamente

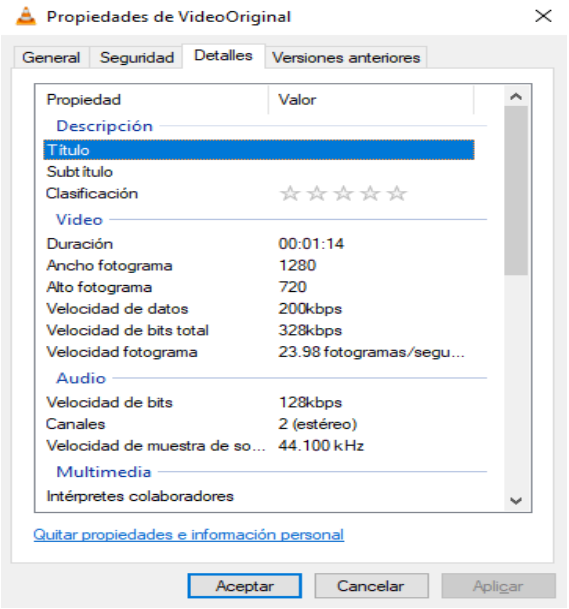



***Figura 20*** Propiedades del video original

Con esas características y mediante el procesamiento que realiza MATLAB, tenemos como resultado un total de 1795 frames obtenidos del video original. Este total se obtiene realizando la siguiente operación:

$$Frames\ Totales = duración\ video\ en\ segundos * número\ de\ fotogramas/segundo$$

$$Frames\ Totales = 74\ seg * 23.98\ fotogramas\ /\ seg$$

$$Frames\ Totales \simeq 1775\ fotogramas$$

***Ecuación 3*** Cálculo de fotogramas totales de un video

Una vez obtenidos los frames se realizó el proceso de selección de los frames que van a ser utilizados como portadores y además de la imagen secreta para el propósito del presente proyecto de investigación.

El método de esteganografía se lo realizó en 3 experimentos escogiendo diferentes imágenes secretas como se puede observar en la Figura 19. Siendo la (a) *Imag1* la que se escogió como Imagen Secreta de acuerdo a los parámetros de relación señal a ruido en imágenes PSNR, error cuadrático RMSE y mediciones de similitud en imágenes SSIM descritos más adelante.

(a) (b) (c)

***Figura 21*** Experimentos realizados. (a) Imag1 (b) Imag2 (c) Imag3

Y como imágenes portadoras se escogieron las siguientes:

***Figura 22*** Imagen Portadora de la información secreta a ser ocultada

(a) (b)

(c)

***Figura 23*** Imágenes portadoras de las características utilizadas para la esteganografía (a) Imagen portadora del canal R. (b) Imagen portadora del canal G. (c) Imagen portadora del canal B.

Las imágenes seleccionadas para ser portadoras corresponden a imágenes iniciales o finales de una escena, es decir, que representan el cambio de escena dentro del video, esta selección se realizó debido a que en el transcurso del video, si se escoge un frame que se encuentra por la mitad de una secuencia de frames al momento de poner información dentro puede existir el inconveniente de que la información oculta sea visible para el ojo humano ya que en una secuencia de imágenes iguales si se presenta un cambio de color en la imagen, éste cambio puede ser notado.

Es por eso, que se escogió los cambios de escena para realizar la incrustación de la información ya que en esos momentos por el mismo hecho de cambiar de escena el ojo humano no percibirá algún cambio que se realice en ese momento. De esa manera se genera un bloque de seguridad extra aparte del uso de la esteganografía para evitar que la información oculta sea visualizada y extraída por terceros.

## 3.3 Obtención del Estego-Video

### 3.3.1 Incrustación de la información

#### 3.3.1.1 Texto en Audio

Como se mencionó con anterioridad en el apartado 3.2.1, para poder ocultar un texto dentro de una señal de audio, se procedió principalmente con la digitalización del texto a ocultar.

El código ASCII (Ver figura 16), fue creado en 1963 por parte del Comité Estadounidense de Estándares (ASA), ahora conocido como (ANSI), este tipo de código

fue creado principalmente para realizar el intercambio de información y evolución de los códigos utilizados por la telegrafía.

El código ASCII se maneja a través de 7 bits para poder representar cada uno de los caracteres del alfabeto latino y se creó debido a que las computadoras solo entienden números, es decir, que la definición básica del código ASCII es la representación numérica de un carácter.

El texto mensaje de prueba, mediante fórmulas de MATLAB se transforma a bits teniendo como resultado un vector en binario el cual será incrustado bit a bit dentro de la información del audio utilizando cómo método principal el uso del Bit menos significativo (LSB). Como resultado obtendremos una señal de audio la cual será llamada como *Estego-Audio*. (Rodríguez, 2016)

#### *3.3.1.2* **Imagen en Frames**

Una vez que tenemos escogidos los frames portadores nos centraremos en utilizar uno de ellos, el cual será el que brindará sus características para que la imagen secreta llegue a convertirse en ella. Para lograr este objetivo comenzaremos con la creación de una Imagen Mosaico, ésta imagen se consigue dividiendo en bloques a la imagen secreta y la imagen portadora. Para el presente proyecto de investigación se utilizan bloques de 8x8 para los bloques, con el fin de manejar porciones más pequeñas a la imagen y lograr manejar la distribución de color con más precisión. El análisis del manejo de la cantidad de bloques a ser requeridos para el proceso fue realizado en (Onofre, 2016), en donde

se tiene como resultado que el utilizar bloques de 8x8 genera la mejor calidad de imagen posible. Éste proceso se lo puede observar a detalle en el diagrama de bloques de la Figura 24.

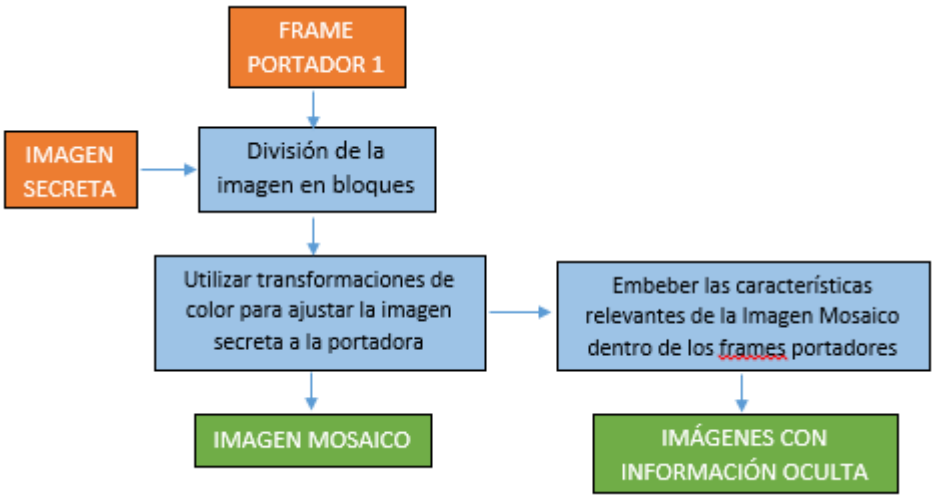
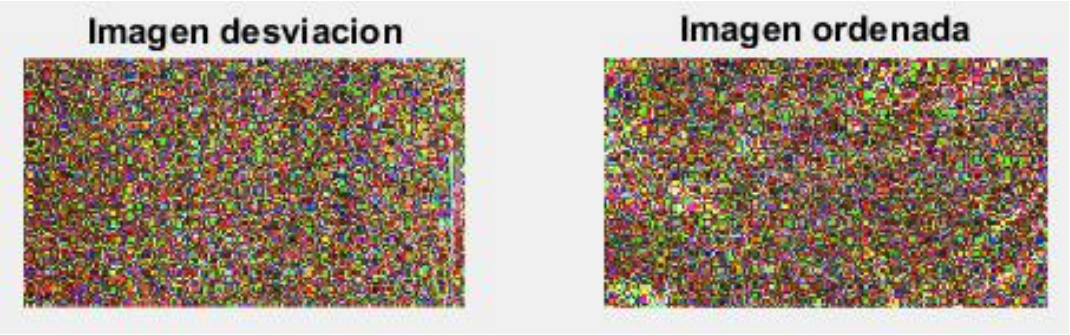



***Figura 24*** Diagrama de bloques del procesamiento para ocultar una imagen

Para lograr que la imagen secreta se parezca en su mayoría a la imagen portadora se utiliza como parámetros fundamentales la desviación estándar y la media, tanto de la imagen secreta como portadora y se ordena cada uno de los fragmentos del bloque de mayor a menor de acuerdo a los valores obtenidos en las desviaciones estándar, las posiciones iniciales de cada uno de los bloques van a ser la información que se vaya a ocultar. (Ver Figura 25). En el estudio realizado en (Onofre, 2016) se evidencia que el manejo de los datos de los canales RGB por separado dan mejores resultados que utilizar el promedio de las desviaciones estándar según lo expresado en (Ya-Lin, 2014).

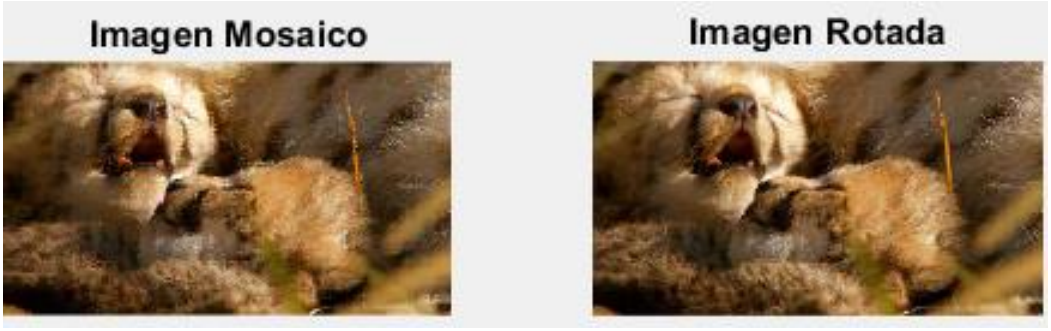



(a) (b)

***Figura 25*** (a) Imagen de desviaciones estándar. (b) Imagen ordenada por su desviación estándar.

El método que se realiza en el presente proyecto de investigación utiliza procesos de transformaciones de color la imagen secreta o mejor dicho los colores de la imagen secreta lleguen a convertirse en los colores de la imagen portadora y así reemplazar a la imagen portadora; para lograr aquello se utiliza las variaciones y cálculos de las desviaciones estándar y las medias de cada bloque según lo expuesto en (Onofre, 2016).

Una vez que tenemos ya realizadas las transformaciones de color necesarias de la imagen secreta basándonos en las características de la imagen portadora, y con el fin de mejorar la calidad de la imagen resultante o Imagen Mosaico como será llamada en el proyecto de investigación, se realiza la rotación de los bloques de la Imagen Mosaico en 0°, 90°,180° y 270°. El grado de rotación lo da el valor mínimo calculado del error RMSE con respecto al valor del bloque que tenga la portadora. (Ver Figura 26).




(a) (b)

***Figura 26*** (a) Imagen Mosaico. (b) Imagen rotada. Para mejorar la calidad de imagen

La imagen mosaico dentro del proyecto de investigación correspondería a la imagen secreta convertida en la portadora, la imagen rotada será la versión mejorada de la Imagen Mosaico la cual reemplazará a la portadora al momento de armar nuestro Estego-Video.

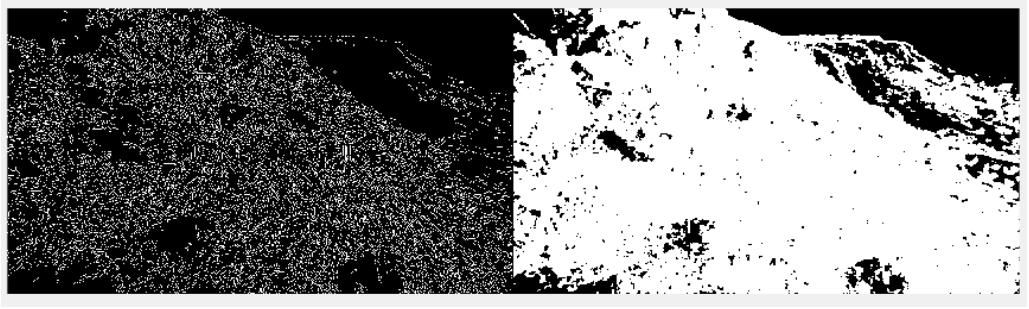
Ahora debemos ocultar la información requerida para poder realizar el proceso inverso en el lado del receptor y de esa manera poder recuperar la información secreta, la información que se va a ocultar son los valores correspondientes a desviaciones estándar, medias, etc., para ello ocuparemos lo definido en el proyecto de investigación de (Onofre, 2016) con una variación, en vez de utilizar una sola imagen para ocultar la información mediante el uso de iteraciones, nosotros contamos con cientos de imágenes que pueden dar lugar a ser portadoras de información y es ahí donde entrar el resto de imágenes anteriormente seleccionadas como portadoras.

Primero debemos realizar la detección de bordes y texturas de las imágenes portadoras de la información con el fin de obtener los mapas de bordes, que nos

permitirán reconocer las ubicaciones más óptimas de cada una de las imágenes para poder ocultar la información en ellas, se utiliza éste método ya que se busca sectores de la imagen donde la variación de tonos en color pasan inadvertidos. Los diagramas de bordes que tenemos de nuestras imágenes portadoras se pueden visualizar en las Figuras 27, 28 y 29 mostradas a continuación:

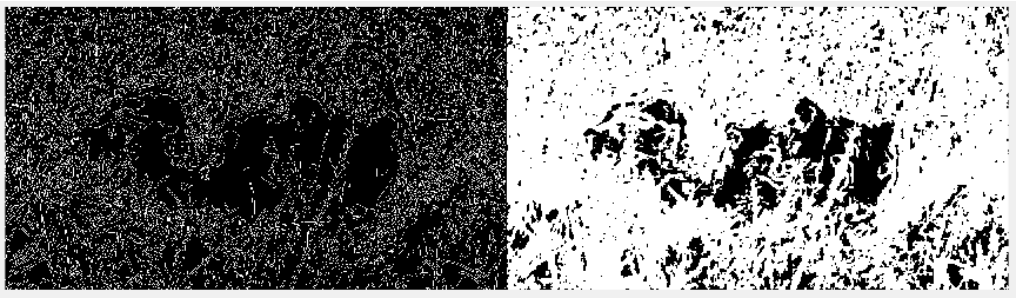
(a) (b)

***Figura 27*** (a) Diagrama de bordes Imagen Portadora 1 (b) Diagrama de texturas Imagen Portadora 1



(a) (b)

***Figura 28*** (a) Diagrama de bordes Imagen Portadora 2 (b) Diagrama de texturas Imagen Portadora 2



(a) (b)

***Figura 29*** (a) Diagrama de bordes Imagen Portadora 3 (b) Diagrama de texturas Imagen Portadora 3

Una vez que ya contamos con nuestros diagramas de bordes y texturas, así como también las posiciones en las cuales la información puede ser ocultada, procedemos a ocultar sobre cada una de nuestras imágenes portadoras la información necesaria, en el presente proyecto de investigación se ha optado por utilizar una imagen portadora por cada canal RGB, teniendo como resultado stego-imágenes. (Ver Figuras 30, 31 y 32)

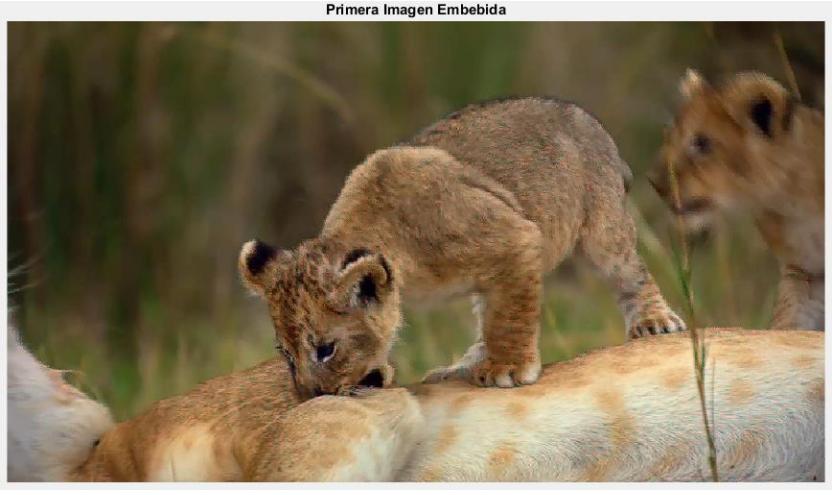



***Figura 30*** Primera imagen embebida de información


***Figura 31*** Segunda imagen embebida de información


***Figura 32*** Tercera imagen embebida de información

Una vez que se tiene creada la Estego-Imagen con la Imagen Secreta y se tiene el resto de información oculta se procede a la creación del Estego-Video, para ello se detalla a continuación.

### 3.3.2 Formación del Estego-Video

Como se mencionó en los apartados anteriores, los componentes necesarios para formar un video, son los frames y el audio, después de realizar los procesos correspondientes de incrustación de información tanto en el audio como en las imágenes seleccionadas como portadoras, tenemos que formar nuestro Estego-Video con la información oculta.

Para ello se utilizó una aplicación de acceso libre llamada *ImageToAvi*, (Ver Figura 33) la cual nos permite unificar todos los frames necesarios e incluso incluir archivos de audio y tener como resultado un archivo de video en formato .avi. (Softonic.com, 2007)


***Figura 33*** Programa para generar archivos de video. ImageToAvi

El programa ImageToAvi, puede ser descargado gratuitamente desde el navegador de preferencia y su forma de uso no es compleja. (Ver Figura 34)

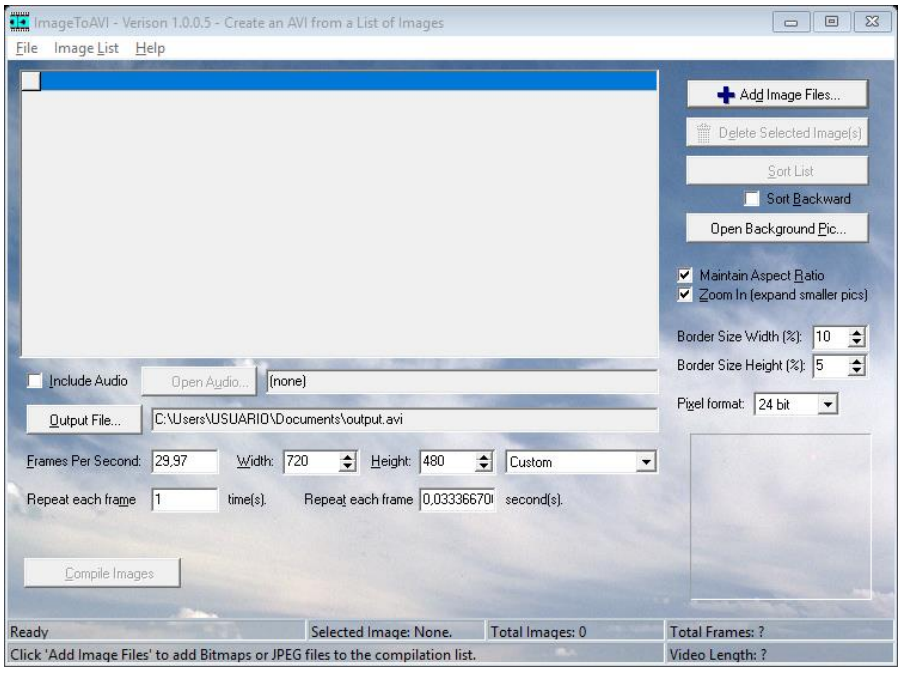



***Figura 34*** Página principal de ImageToAvi.

Se debe escoger principalmente los frames requeridos para crear el archivo de video, para ello damos click en *Add Image Files*, se ubica la carpeta en la cual se encuentran los frames que van a pertenecer al Estego-Video, obviamente reemplazando las imágenes seleccionadas como portadoras por aquellas que contienen la información oculta en su interior.

Para que sea mucho más fácil, se creó una sola carpeta con todos los frames que van a ser incluidos dentro del Estego-Video con el fin de no perder ningún frame que pueda perjudicar a la recuperación de la información oculta dentro de nuestro Estego-Video.

Lo importante de la aplicación ImageToAvi es que aparte de agregar toda la información necesaria como audio e imágenes, también nos permite configurar parámetros como: cantidad de frames por segundo, tamaño de los frames, etc. Lo cual nos permite acercarnos mucho más a las características que presenta el video original. (Ver Figura 35).

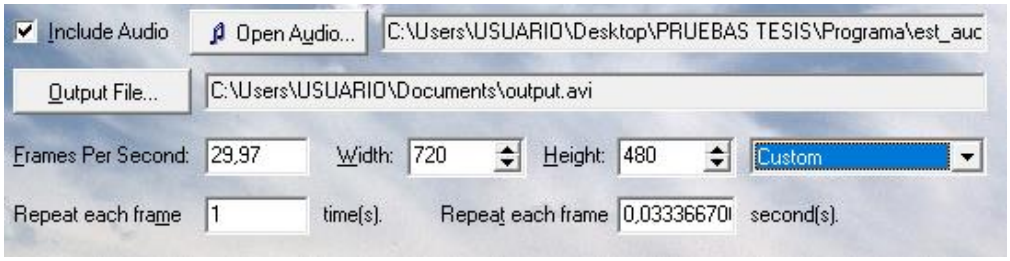



***Figura 35*** Parámetros de configuración para creación del Estego-Video

Una vez que tenemos definidos todos los parámetros necesarios para poder realizar nuestro Estego-Video, por último le damos a compilar y se espera un tiempo prudente hasta que la aplicación cree el Estego-Video.

Después de terminar la compilación del video nuevo, tenemos nuestro Estego-Video con la afirmación de que no se divisa en que frames se encuentra la información oculta, eso se debe a que por la velocidad de frames por segundo, no permiten que se perciba por el ojo humano las variaciones en los pixeles de las Stego-Imágenes.

## 3.4 Extracción de Información del Estego-Video

Después de tener nuestro Estego-Video armado y transmitido, nos queda como segunda parte de este proyecto de investigación trabajar en el inverso a lo realizado con anterioridad para poder obtener nuestra información oculta, tanto a nivel de audio como de video.

Para ello así como se realizó en el video original, necesitamos separar a nuestro Estego-Video en sus dos componentes fundamentales, audio y frames, en este caso los llamaremos Estego-Audio y Stego-Frames. La división de estas dos componentes lo realizaremos mediante la herramienta computacional MATLAB.

### 3.4.1 Extracción de Información del Estego-Audio

Una vez que tenemos separadas las componentes, éstas serán trabajadas independientemente así como para el proceso de incrustación de información.

El Estego-Audio para ser parte de un video es una señal digital y para poder obtener su información es necesario realizar el proceso de digitalización de una señal analógica, es decir, que el Estego-Audio se someterá al procesamiento de señales mediante el muestro de la señal, la cuantización y la codificación de la señal.

Después de realizar este proceso ya contamos con un vector binario que corresponde a la información digital de nuestro archivo de audio, entonces utilizamos la función de la herramienta computacional MATLAB, **bitget**, y de esa forma extraemos la información necesaria. (Rodríguez, 2016)

Para ello debemos recordar que el receptor de la información secreta necesita conocer la posición del vector del cual requiere extraer la información, ya que si no es así, la información recuperada no correspondería a la secreta y se perdería dicha información.

Después de extraer la información necesaria, tenemos un vector en binario el cual lo debemos someter al proceso inverso de la codificación de un mensaje de texto para poder obtener la información, es decir, que utilizaremos las funciones inversas para que en grupos de 8 bits del vector recuperado transformarlo a decimal y a su vez transformarlo a caracteres, y así obtener como resultado el mensaje:

```
>> TextoEnAudioRec
Su mensaje recuperado es:
mensaje de prueba
```

A continuación en la Figura 36 se muestra un diagrama de bloques general con el proceso de recuperar el texto oculto.

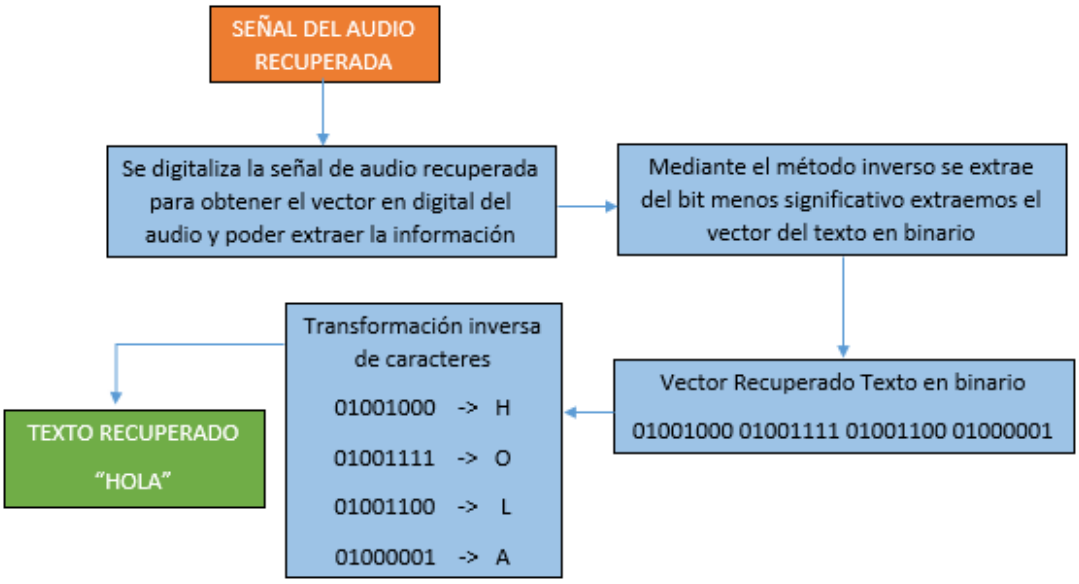



***Figura 36*** Diagrama de bloques del proceso de recuperación del texto oculto dentro del audio

### 3.4.2 Extracción de Información del Stego-Frames

De la misma manera que se realizó con el Estego-Audio para obtener el mensaje oculto dentro del mismo, tenemos que realizar el proceso inverso a la incrustación de la información para obtener la imagen secreta que se ocultó dentro del Estego-Video.

A continuación se detalla el proceso que se realizó con los Stego-Frames para lograr recuperar la imagen secreta mediante el diagrama de bloques expuesto en la Figura 37.

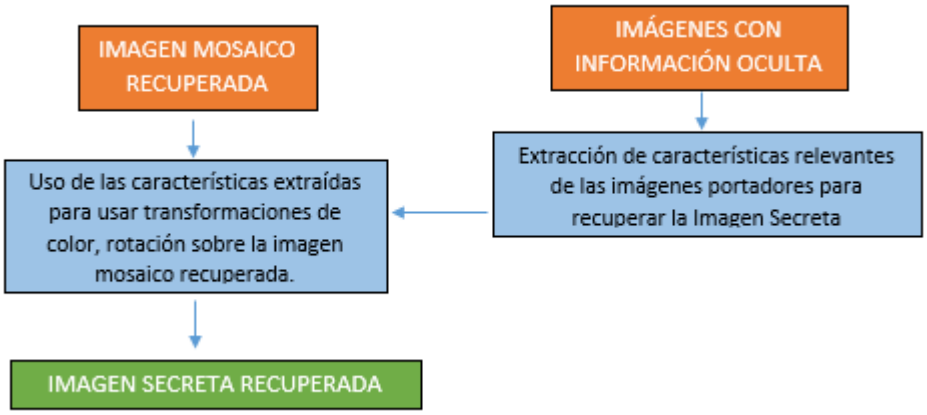



***Figura 37*** Diagrama de bloques general del proceso para recuperar la imagen oculta

Una vez que tenemos separados los Stego-Frames del Estego-Video mediante el uso de la herramienta de MATLAB, VideoReader, lo primero que se requiere hacer es recuperar la información oculta de las imágenes portadoras que contienen las características necesarias para recuperar nuestra imagen secreta. Es decir, que de las imágenes portadoras vamos a obtener los valores de desviaciones estándar, medias, número de iteraciones y cantidad de pixeles utilizados para realizar la transformación de la Imagen Secreta en la Imagen Portadora.

Una vez que tenemos identificados los pixeles que fueron modificados en el proceso de incrustación de la información, realizaremos el proceso inverso a la técnica explicada en (Coltuc, 2007) y aplicada dentro del manejo de la esteganografía en imágenes en (Onofre, 2016) para obtener nuestra imagen secreta. (Ver Figura 38).

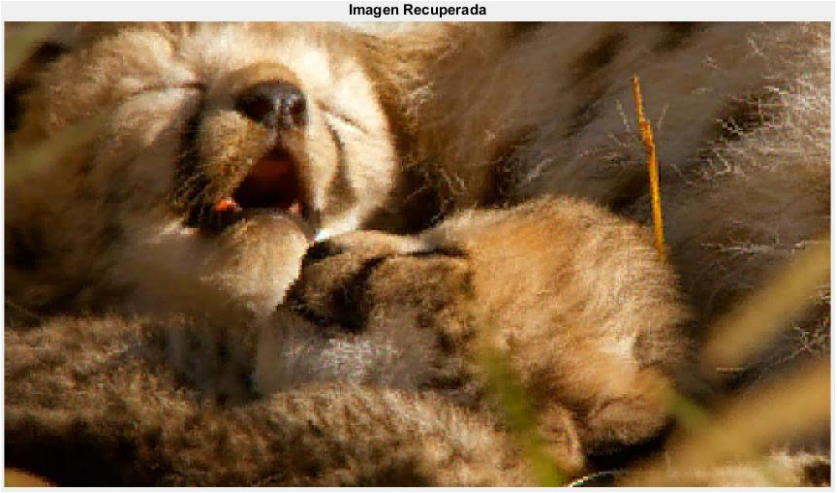



***Figura 38*** Imagen recuperada del Estego-Video

Como debemos continuar con el proceso inverso a la incrustación de la información, la imagen recuperada la sometemos a un proceso de re-rotación de bloques, esto lo realizamos con el objetivo de poder manejar los bloques en la posición en la que se encontraba la imagen secreta. Este resultado lo tomaremos como Imagen Rerotada o a su vez representa la Imagen Mosaico Recuperada (Ver Figura 39).

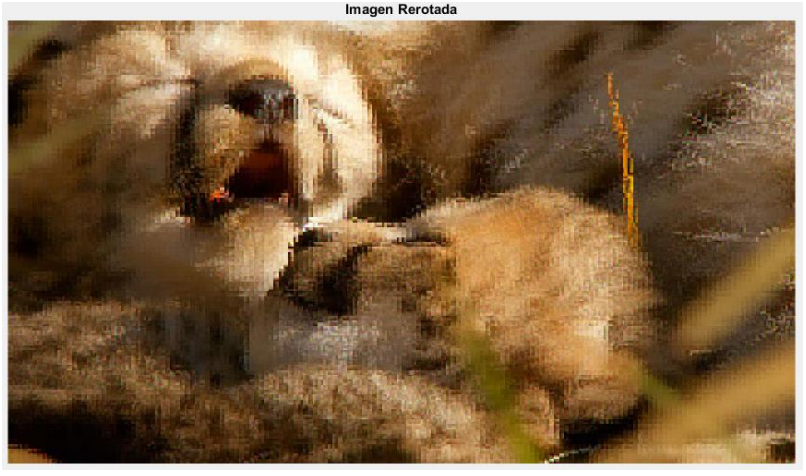



***Figura 39*** Imagen re-rotada o Imagen Mosaico Recuperada

Una vez que se tiene la Imagen Mosaico recuperada, utilizamos las características de las medias, coeficientes de desviación estándar y la adición de los residuos que pueden haber existido en cada uno de los bloques y de esa manera podremos obtener el valor de cada uno de los pixeles originales.

El último paso que requerimos es re ordenar los bloques de acuerdo a las posiciones iniciales que se obtuvieron al inicio de la incrustación de la información para que de esa forma poder obtener nuestra Imagen Secreta Recuperada. (Ver Figura 40).


***Figura 40*** Imagen Secreta Recuperada.

# CAPITULO IV

## ANÁLISIS DE RESULTADOS OBTENIDOS

### 4 Análisis de Resultados Obtenidos.

Cómo se pudo observar en el apartado anterior, se logró recuperar la información secreta tanto del audio como de los frames del Estego-Video, sin embargo la Imagen Secreta Recuperada no cuenta con una calidad de imagen efectiva, la imagen resultante presenta un nivel de pixelado bastante promitente, uno de los posibles factores y el más probable sería la pérdida de información al momento de recuperar la información.

Se intentó recuperar la información con una alta calidad de imagen mediante la manipulación de la información extraída del Estego-Video, sin embargo no se tuvo una respuesta favorable.

Es por ello que como solución adicional al proyecto se investigó sobre diferentes formas de recuperar la calidad de una imagen y es así que se encontró que es factible la restauración de una imagen en cierto porcentaje mediante el uso de filtros, en este caso se utilizarán dos clases de filtros para poder mejorar en un porcentaje la calidad de la imagen secreta recuperada. (Blanes & Gorricho)

Los filtros utilizados para lograr este objetivo son: filtro Wiener y el filtro de Mediana. Los filtros Wiener conforman parte de los filtros lineales de mínimos cuadrados, los cuales

son utilizados con frecuencia para la predicción, interpolación, filtrado de señal y ruido entre otras aplicaciones. El filtro Wiener se basa en ajustar su estructura tiempo-frecuencia a las características tiempo-frecuencia de la señal que se desea eliminar y de esa manera lograr una reducción del ruido. (Vettorazzi Gonzales, 2007)

Y por su lado el filtro de mediana, utilizado comúnmente para la disminución del ruido “pepper”, a diferencia del filtro anteriormente mencionado, el Filtro de Mediana es un filtro del dominio del espacio no de la frecuencia, y corresponde a la rama de los filtros no lineales. Éste tipo de filtro se utiliza con frecuencia en el procesamiento digital de imágenes para reducir el ruido en imágenes, la manera de trabajar del filtro de mediana se basa en recorrer cada uno de los pixeles de la imagen y el valor que este posee se lo reemplaza por la mediana de los pixeles vecinos. (Vettorazzi Gonzales, 2007)

Como se puede observar a continuación en la Figura 37. Al aplicar el filtro Wiener se logra disminuir la característica de pixelado de la Imagen Secreta Recuperada. Sin embargo se notó que al aplicar este filtro la Imagen Secreta Recuperada presenta ruido conocido como “sal y pimienta” es decir que a simple vista se puede observar como si la imagen estuviera llena de pequeños puntitos. (Ver Figura 41).

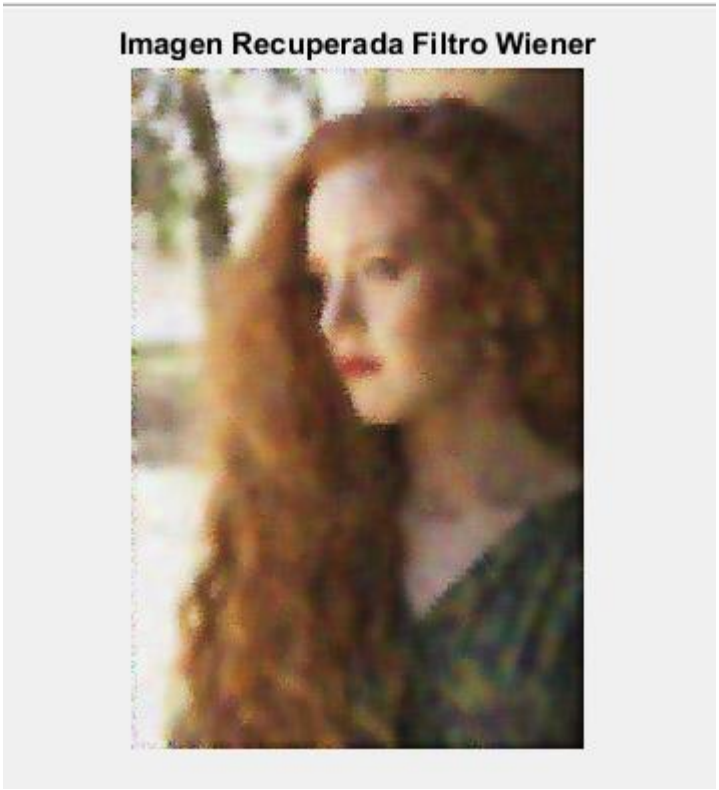



***Figura 41*** Imagen Recuperada Filtro Wiener

A su vez tenemos la imagen Secreta Recuperada aplicada el filtro de mediana solamente, y como se puede visualizar en la figura 38., la diferencia entre la Imagen Secreta Recuperada y la Imagen Secreta Recuperada pasada por el filtro de mediana son casi las mismas, y esto se debe a que el filtro de mediana como se expuso anteriormente se centre en disminuir el tipo de ruido conocido como “sal y pimienta”, (Ver Figura 42). (Blanes & Gorricho)

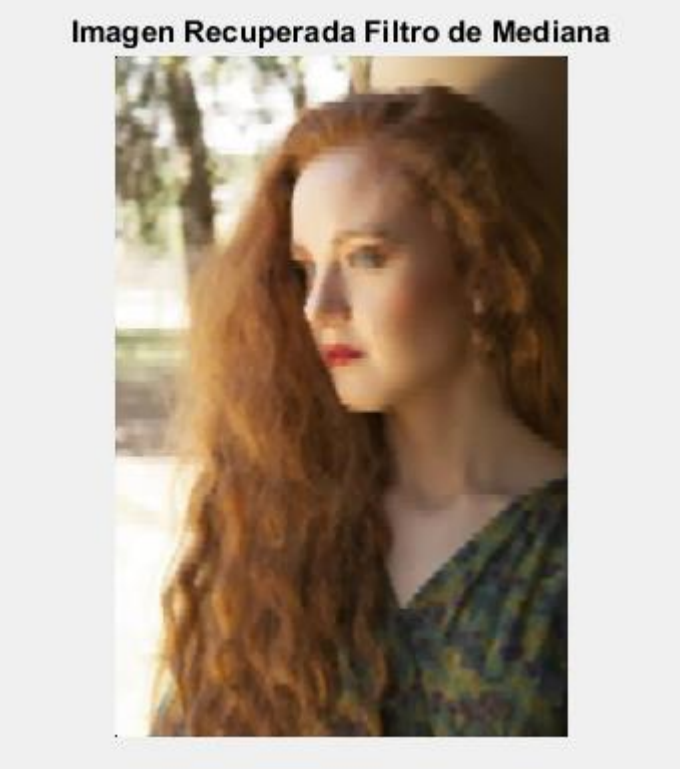



***Figura 42*** Imagen Recuperada Filtro de Mediana

Al visualizar ambos resultados después de aplicar los filtros Wiener y de Mediana, no se tendría definido completamente cual podría ser la mejor opción de Imagen Secreta Recuperada, es por ello que como opción adicional se realizó la combinación de ambos filtros y así visualizar si se cuenta con una mejoría en la imagen.

Se aplicó primero el filtro Wiener, ya que por sí solo representa una modificación a la Imagen Secreta Recuperada evitando la característica de pixelado sea visible. Como resultado se obtuvo una imagen con característica de pixelado menor, sin embargo, se ganó una característica de “Sal y pimienta” que presentó puntos a lo largo de toda la imagen, y es ahí en donde entra el filtro de Mediana ya que, como se explicó con

anterioridad, éste filtro se encarga de eliminar el ruido tipo “sal y pimienta” de las imágenes. (Blanes & Gorricho)

Una vez aplicados ambos filtros tenemos como resultado la Imagen Secreta Recuperada que se muestra en la Figura 43:

***Figura 43*** Imagen Recuperada Combinación Filtro Wiener y Mediana

Si bien es cierto, la Imagen Secreta Recuperada no cuenta con una calidad de imagen óptima se ha tomado como resultado válido ya que a pesar de presentar una baja calidad, es visible el diseño de la Imagen, es decir, que puede ser comparada con respecto a la Original.

A continuación se realizará el análisis de comparación entre las dos imágenes, la Imagen Secreta Original y la Imagen Secreta Recuperada con la combinación de los filtros Wiener y de Mediana.

## 4.1 PSNR (*Peak Signal to Noise Ratio*)

El valor de PSNR representa la manera de medir la cantidad de ruido que tiene una imagen con respecto a otra. En el presente proyecto de investigación mide la cantidad de ruido comparando la Imagen Secreta Recuperada con respecto a la Imagen Secreta.

**Tabla 3**

*Valores PSNR obtenido de los experimentos realizados*

| Imag Secrt | psnrSR | psnrS |
|---|---|---|
| Imag1 | 28,127 | 26,614 |
| Imag2 | 27,546 | 26,125 |
| Imag3 | 27,782 | 25,856 |
| Promedio | 27,818 | 26,198 |

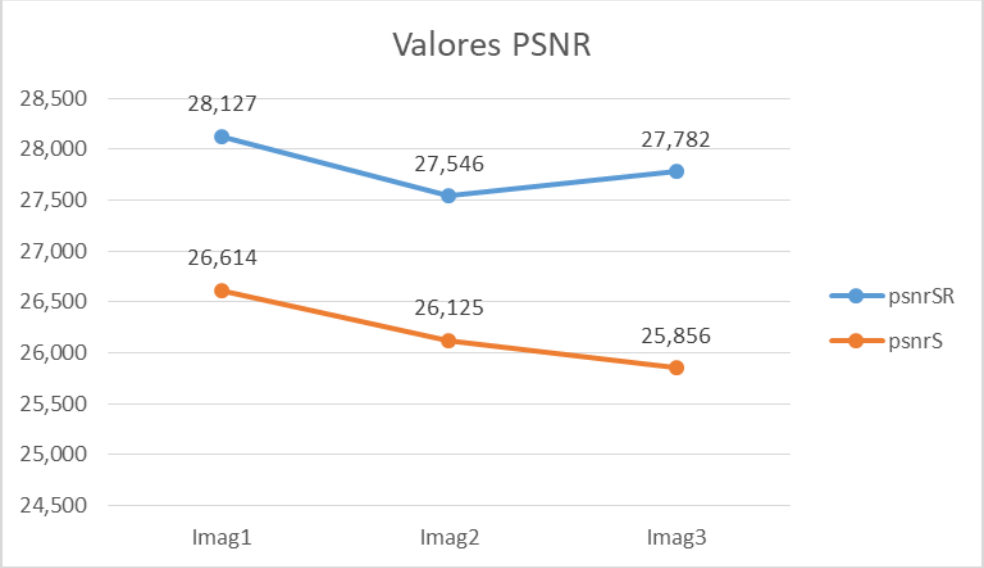



***Figura 44*** Gráfica de valores PSNR obtenidas de los 3 experimentos realizados

Como se puede observar en la Figura 44, se obtiene un valor más alto en PSNR de la Imag1, por lo cual permite que sea la imagen más óptima para el manejo de la esteganografía.

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

El valor RMSE es utilizado para medir la calidad de una imagen con respecto a otra. En el presente proyecto de investigación se mide la calidad de la Imagen Secreta Recuperada con Respecto a la Imagen Secreta Original.

**Tabla 4**

*Valores PSNR obtenidos los experimentos realizados*

| Imag Secrt | rmseSR | RmseS |
|---|---|---|
| Imag1 | 10,002 | 12,326 |
| Imag2 | 10,256 | 10,172 |
| Imag3 | 12,153 | 14,813 |
| Promedio | 10,804 | 12,437 |

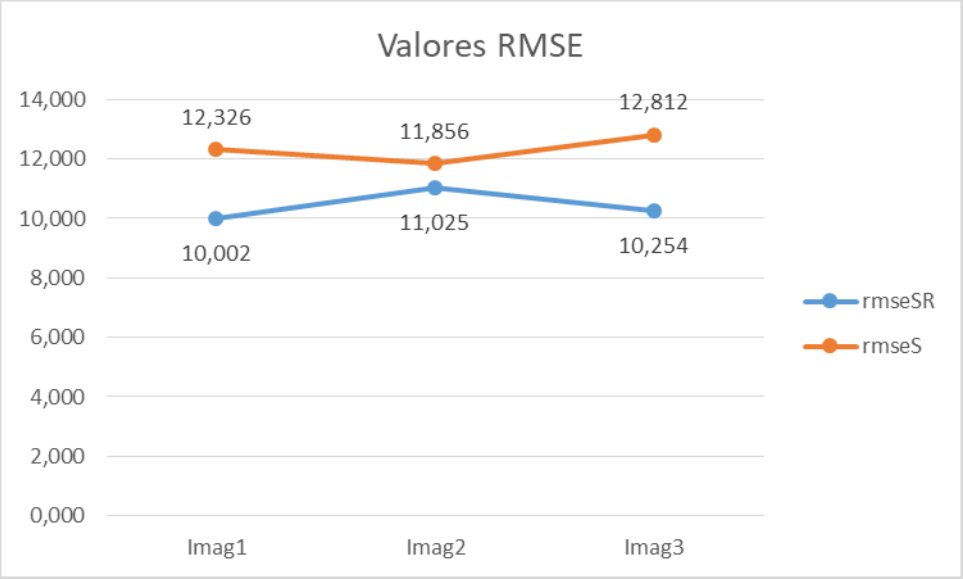



***Figura 45*** *Gráfica de valores RMSE obtenidas de los 3 experimentos realizados*

Como se puede observar en la Figura 45, los valores de RMSE que corresponden a las tres imágenes analizadas, se evidencia que el error RMSE más bajo corresponde a la Imag1, sin embargo también se visualiza que los tres experimentos realizados no tienen una diferencia pronunciada en cuanto al error RMSE, por tal motivo se podría

tomar cualquiera de las tres imágenes analizadas para realizar el método propuesto de esteganografía.

## 4.3 MSSIM (*Mean Structural Similarity Index*)

Las medidas anteriormente utilizadas evalúan los errores que pueden presentar las imágenes obtenidas en un sistema como una medida objetiva, es ahí en donde aparece el parámetro de medida conocida como SSIM, éste parámetro hace referencia al sistema visual humano, es decir que compara dos imágenes basándose en el rango de la métrica de 0 a 1, en donde 0 corresponde a que existe una pérdida total de la similitud de la imagen final con respecto a otra, y 1 corresponde a que la imagen resultante puede ser tomada en cuenta como una copia exacta de la imagen original.

**Tabla 5**

*Valores SSIM obtenidos los experimentos realizados*

| Imag Secrt | ssimRS |
|---|---|
| Imag1 | 0,899 |
| Imag2 | 0,870 |
| Imag3 | 0,892 |
| Promedio | 0,887 |

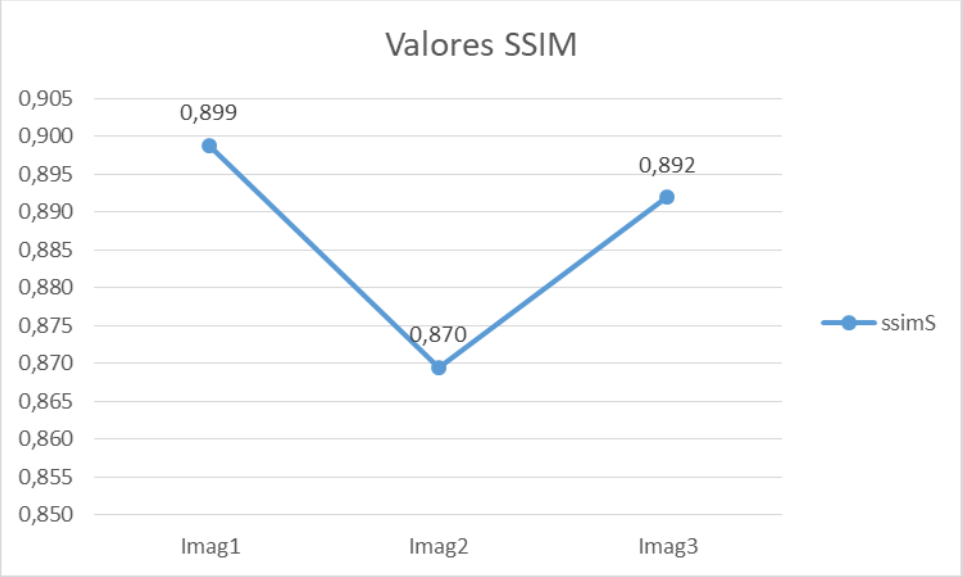


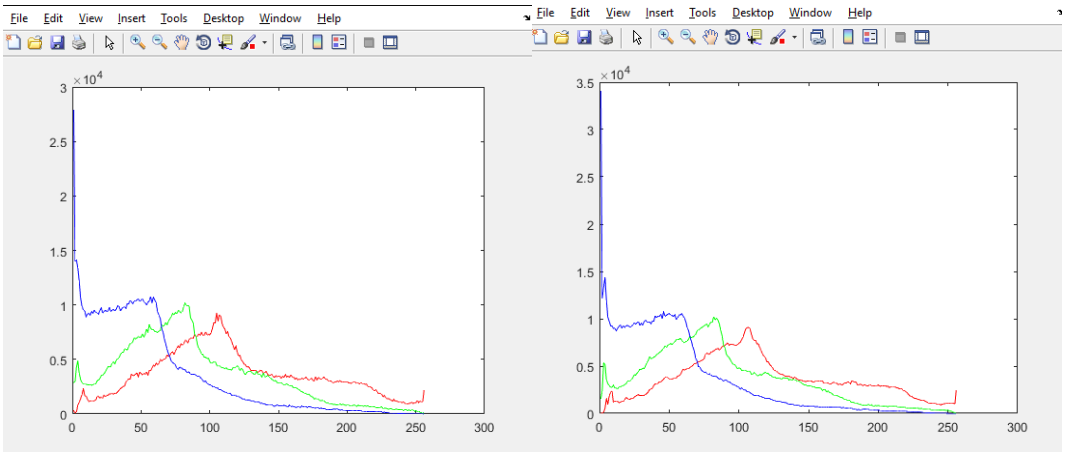

***Figura 46*** Gráfica de valores SSIM obtenidas de los 3 experimentos realizados

Como se visualiza en la Figura 45, se obtiene como resultado que la imagen con un mejor resultado visual de similitud de imagen SSIM es la Imag1 ya que presenta el valor SSIM más alto de las tres imágenes analizadas.

En base a los resultados obtenidos del análisis de la calidad de una imagen se encuentra determinada por los parámetros analizados de PSNR, RSME y SSIM mediante el cálculo de errores se obtuvo que la imagen con mejor resultado fue la Imag1, la cual será ocupada dentro del proyecto de investigación actual.

Aparte de los análisis de los errores anteriormente mencionados, existe también una manera de medir y comprobar el rendimiento del método de esteganografía propuesto, para ello se utiliza el análisis mediante histogramas, en donde se puede evidenciar las gráficas de los canales RGB tanto de la Imagen Secreta Original como de la imagen Secreta Recuperada y de esa manera determinar si el método de

esteganografía ha sido óptimo o no. A continuación se presentan los histogramas obtenidos del experimento que tuvo mejor resultado del método de esteganografía propuesto por (Onofre, 2016). Como se mencionó anteriormente las gráficas de los histogramas representan cada canal de una imagen (RGB), en el eje x se tiene como medida el número de valores de pixeles entre 0 y 255; y en el eje y se encuentra la respuesta en frecuencia de cada valor de pixel. (Ver Figura 47).




(a) (b)

***Figura 47*** Histogramas: (a) Imagen Secreta Original. (b) Imagen Secreta Recuperada

Como se puede evidenciar en los histogramas presentados en la Figura 47, el rendimiento del método de esteganografía propuesto en (Onofre, 2016) es visualmente muy eficiente debido a que la Imagen Secreta Recuperada obtenida como resultado es prácticamente igual a la Imagen Secreta Original, obviamente si analizamos los valores de RMSE y SSIM de la Imagen Secreta Recuperada podemos evidenciar que en cuanto a la calidad de imagen, el resultado obtenido no es el óptimo a pesar de haber incrustado la Imagen Recuperada dentro de una serie de filtros para mejorar la calidad de la imagen.

Una vez analizados los resultados obtenidos en cuanto a la Imagen Secreta Recuperada, se procederá a analizar mediante una encuesta MOS que consiste en la obtención de medidas subjetivas sobre la calidad de lo que se está evaluando por parte de un grupo de personas encuestadas, en este caso se encuestó a una población de 15 personas mediante la herramienta de encuestas generada por la empresa “Google” con el fin de obtener muestras y observaciones acerca del Estego-Video generado en el presente proyecto de investigación. Las personas encuestadas deben visualizar el Estego-Video y evaluarlo en base a las preguntas realizadas a continuación:

- Pregunta 1: ¿La calidad del video es óptima?

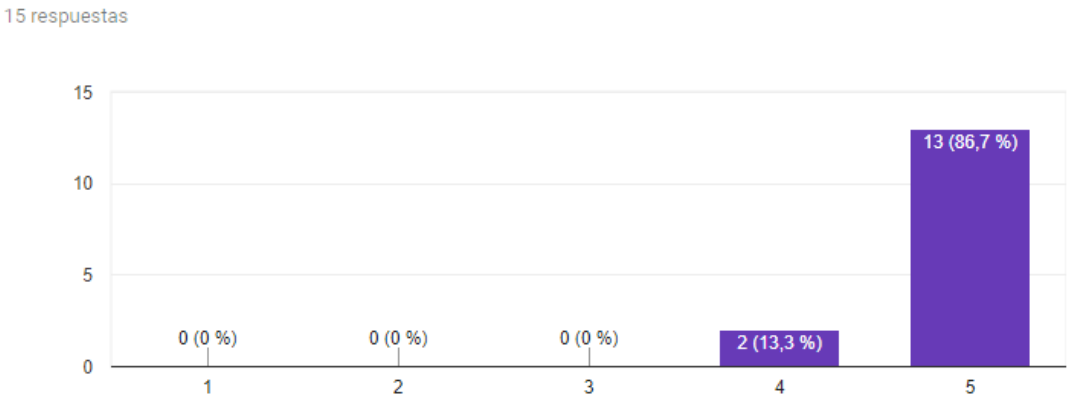



***Figura 48*** Resultado de encuesta MOS a la Pregunta 1

Cómo se puede evidenciar en la Figura 48, de una población de 15 personas encuestadas, el **86,7%** de la población calificó al Estego-Video con una calidad de Muy

Bueno y un **13,3%** calificó como Buena. Lo cual nos da como resultado que el proyecto de investigación cuenta con una eficiencia óptima en cuanto a ocultar la información.

- Pregunta 2: ¿Ha notado algún cambio perceptible en el transcurso del video?

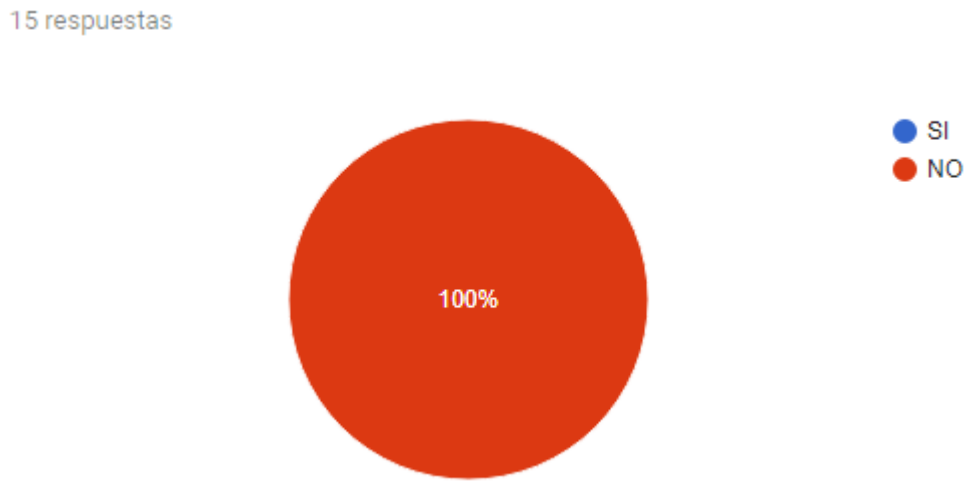



***Figura 49*** Resultado de encuesta MOS a la Pregunta 2

Cómo se puede evidenciar en la Figura 49, de una población de 15 personas encuestadas, el **100,0%** de la población no notó ningún tipo de distorsión o cambio dentro del Estego-Video, lo cual permite asegurar que la información que se encuentra oculta es imperceptible por un usuario visualmente.

- Pregunta 3: Evalúe la calidad del audio del video.

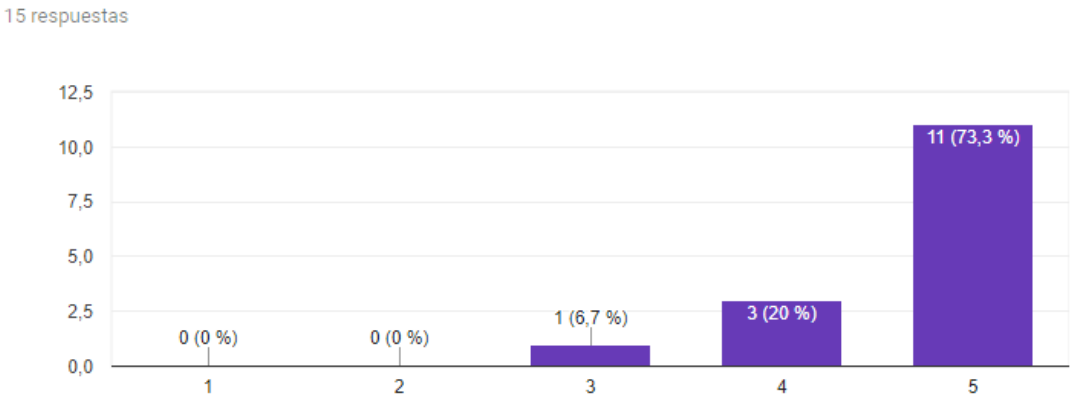



***Figura 50*** Resultado de encuesta MOS a la Pregunta 3

Cómo se puede evidenciar en la Figura 50, de una población de 15 personas encuestadas, el **73,3%** de la población calificó al audio del Estego-Video con una calidad de Muy Bueno y un **20,0%** calificó el audio como Bueno y un **6,7%** calificó el audio como Bueno. Lo cual nos da como resultado que se puede evidenciar un ligero ruido en el audio del Estego-Video, sin embargo se puede decir que el sistema es lo bastante óptimo para ser imperceptible.

- Pregunta 4: ¿Creería usted que dentro del video se encuentra algún tipo de información oculta?

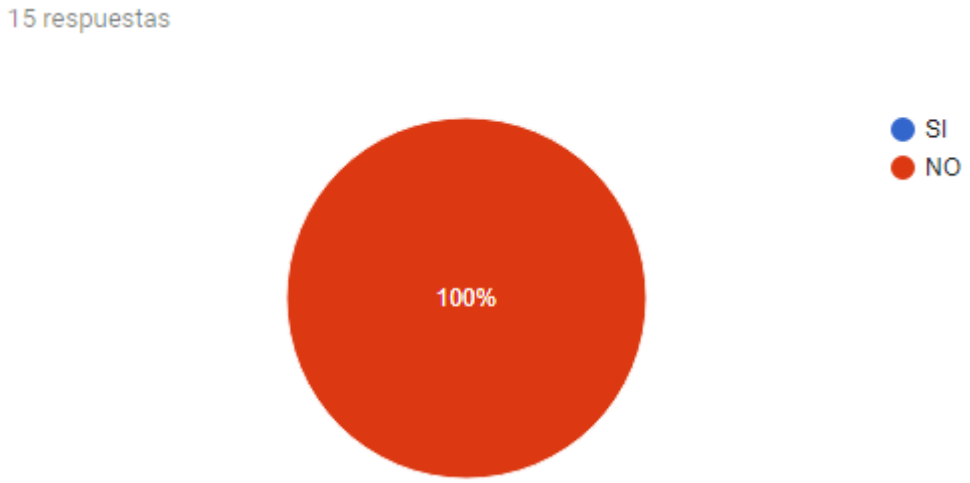



***Figura 51*** Resultado de encuesta MOS a la Pregunta 4

Cómo se puede evidenciar en la Figura 51, de una población de 15 personas encuestadas, el **100,0%** de la población no pudo intuir que dentro del Estego-Video existía información oculta. Lo cual permite asegurar que a pesar de tener un ligero ruido en la señal de audio, éste puede ser confundido como una falla en la calidad del audio, más no que se encuentra información dentro del video.

A pesar de tener esos resultados se puede decir que el objetivo del presente proyecto de investigación ha tenido un resultado muy bueno ya que se logró realizar el objetivo principal que es el de ocultar información dentro de un video sin que éste sea alterado o que la información oculta sea percibida tanto visual como auditivamente.

# CAPITULO V

# CONCLUSIONES Y RECOMENDACIONES

## 5 Conclusiones y Recomendaciones

- Se logró insertar como información secreta un texto sobre los datos del audio extraído del video original así como también se logró insertar como información secreta una imagen dentro de los frames obtenidos del video original mediante el uso de la técnica del bit menos significativo en el procesamiento de un audio.

- Se logró combinar las porciones con información oculta para obtener como resultado un Estego-Video, el cual se pudo crear en base a aplicaciones de procesamiento y creación de videos como es ImageToAvi.

- Se logró separar un archivo de video con extensión .avi en sus dos componentes principales, audio e imágenes, se lo realizó mediante un algoritmo propuesto en la herramienta computacional la cual nos permitió tener el manejo de los datos de una manera mucho más práctica que el uso de funciones como ffmpeg que pueden ser utilizadas también como herramienta para procesamiento de videos.

- Se evidenció que el Estego-Video obtenido tiene una gran calidad en cuanto a la percepción visual humana corresponde, ya que no se puede evidenciar que existe información oculta dentro del video al verlo o escucharlo.

- Se aplicó métodos esteganográficos inversos con el fin de recuperar la información oculta dentro del Estego-Video, en cuanto al texto incluido se lo pudo recuperar en su totalidad, por otro lado, la imagen secreta obtenida se logró recuperar también pero perdiendo calidad de imagen.

- Se verificó que el método esteganográfico permite ocultar información dentro de un medio sin que éste sea percibido, y mediante el análisis de los diferentes valores estadísticos como son RMSE, PSRN y SSIM que permiten validar la calidad y eficiencia del método utilizado.

- Se presenta un mayor costo computacional para desarrollar procesamiento sobre archivos multimedia como videos, imágenes o audio ya que aquello influye en el tiempo de implementación del algoritmo por lo que se recomienda en trabajos futuros optimizar el código de MATLAB y evitar tiempos altos en el procesamiento.

- Se recomienda utilizar como imágenes secretas, imágenes que cuenten con el tamaño del frame del video ya que al momento de realizar el reajuste del tamaño de imagen se puede perder bastante información.

- Si bien es cierto, los diferentes métodos para ocultar información ayudan con muchos fines de seguridad de la información también existe un mal uso de este tipo de técnicas, en donde se utiliza la información oculta con fines destructivos o

que hacen daño a las personas. Por ello se recomienda que el manejo de estas técnicas para ocultar información se debe realizar únicamente con fines de estudio y de manejo ético de la información.

# CAPITULO VI

# LÍNEAS DE TRABAJOS FUTUROS

## 6 Líneas de Trabajos Futuros

- Una vez culminado el presente proyecto de investigación se puede dar paso a diferentes trabajos posteriores ya que se tiene un campo amplio de investigación por el mismo hecho de tener diversos medios multimedia para ser trabajados.

- Como trabajo futuro principalmente se propone el hecho de mejorar la sección de la recuperación de la información con el fin de mejorar la calidad de la imagen secreta recuperada.

- Se propone como trabajo futuro el estudio e implementación de filtros correctivos de imagen con el fin de lograr obtener un resultado más óptimo al momento de recuperar la información.

- En cuanto a la porción de audio como trabajo futuro se propone el de buscar métodos más simples para realizar el procesamiento de la señal análoga con el fin de que el costo computacional sea menor y el tiempo de ejecución de las pruebas mejoren.

- Por último se propone como trabajo futuro el manejar diferentes formatos de video y probar el método esteganográfico con el fin de evidenciar que formato es el más óptimo para realizar el proceso de ocultar información.

- Una vez culminado el trabajo de investigación se propone como trabajo futuro el combinar diferentes métodos de ocultación de la información, como por ejemplo el uso de la criptografía y la esteganografía en conjunto para mejorar la eficiencia de ocultar información.

# CAPITULO VII

## 7 Bibliografía

Amirtharajan, R., Subrahmanyam, R., Prabhakar, P. J., Kavitha, R., & Bosco Balaguru, J. (s.f.). *MSB over hides LSB - A dark communication with integrity.* Thanjavur, India: SASTRA University.

Arora, A., & Pratap Singh, M. (2016). Image Steganography Using Enhanced LSB substiturion Technique. *Fourth International Conference on Paralllel, Distributed and Grid Computing (PDGC)*, (pág. 4). Kurukshetra, India.

Blanes, J. S., & Gorricho, J. L. (s.f.). *Técnicas de Evaluación de la Calidad de la Imagen. Tendencias y métricas basadas en bordes.*

Carvajal Gámez, B. E. (2008). *Técnica de Inserción de Información en Video aprovechando el mismo Ancho de Banda.* México D.F.

Cole, E. (2003). *Hiding_in_Plain_Sight_Steganography.* Indianapolis: Wiley Publishing, Inc.

Coltuc, D. &. (2007). Very fast watermarking by reversible contrast mapping. *IEEE Signal Proccess*.

FFmpeg. (s.f.). *About FFmpeg*. Obtenido de http://ffmpeg.org/about.html

Gambhir, A., & Sibaram, K. (2016). Integrating RSA Cryptography & Audio Steganography. *International Conference on Computing, Communication and Automation (ICCCA)* (pág. 4). Greater Noida, India: Galgotias University.

García Cano, D. (2004). *Análisis de herramientas estaganográficas.* Leganés.

Illescas Robalino, M. A., & Villamarín Zapata, D. F. (2011). *Implementación de un transmisor de pruebas de tv digital terrestre isdb-tb, para la emisión de aplicaciones interactivas.* Sangolquí-Ecuador.

Ite.educacion.es. (s.f.). *Diseño de materiales multimedia. Web 2.0*. Obtenido de Vídeo y animaciones: http://www.ite.educacion.es/formacion/materiales/107/cd/video/pdf/video01.pdf

Kempf, J.-B. (s.f.). *VLC engine relicensed to LGPL*. Obtenido de https://www.videolan.org/press/lgpl-libvlc.html

Mendoza, L. E. (2008). *Low-complexity methods for image and video.* Vancouver.

Moher, s. H. (2007). *Analog & digital communications. Second edition.* John wiley & sons, inc.

Onofre, G. (2016). *Desarrollo y análisis de una técnica esteganográfica en zonas ruidosas de la imagen mediante transformaciones de color reversibles.*

Roden, M. S. (2018, Fifth Edition). *Analog and Digital Communication Systems.* Designsoft, Inc.

Rodríguez, C. (2016). *Estudio y desarrollo de una aplicación de esteganografia para enviar datos en archivos de audio, orientado a la seguridad en los sistemas de comunicación.*

Rossmann, M. R. (2014). El espectro de frecuencias. *Cultura, ciencia y tecnología. Asdopen-unmsm*.

Shannon, C. E. (1948). *A mathematical theory of communication.*

Shannon, C. E. (1949). *Comunication theory of secrecy systems.*

Softonic.com. (2007). *Softonic.com*. Obtenido de Softonic.com: https://imagetoavi.softonic.com/

Suarez, J. C., Carvajal, B. E., & Carreto, C. (2015). *Transmisión de Video simultáneo en ancho de banda limitado aplicando esteganografía.*

Sugathan, S. (2016). *An Improved LSB Embedding Technique for Image Steganography.* India: Siemens Healthcare Pvt. Ltd.

Tayel, M., Gamal, A., & Shawky, H. (s.f.). *A Proposed Implementation Method of an Audio Steganography Technique.* Egypt: Alexandria University.

Vargas, L., Elizabeth, V. D., & Di Gionantonio, A. (2016). Marcas de agua: una contribución a la seguridad de archivos digitales. *Revista FCEFYN*, 6.

Vettorazzi Gonzales, J. A. (2007). *Restauración de imágenes distorsionadas mediante técnicas de procesamiento digital y comparación entre dos métodos de restauración.* Guatemala.

Villa, H. F., & Jaramillo, J. C. (2015). *Aplicaciones de la esteganografía en la seguridad informática.* Pereira.

Ya-Lin, L. &.-H. (2014). A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations. *IEEE Transactions on circuits and systems for video technology*.

Yingnan, Z., Minqing, Z., Xiaoyuan, Y., Guo, D., & Liu, F. (2017). Novel Video Steganography Algorithm Based on Secret Sharing and Error-Correcting Code for H.264/AVC. *Tsinghua science and technology*, 12.

Yuan-Hui Yu, C.-C. C.-C. (2017). Hiding secret data in images via predictive coding. 16.