ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DESARROLLO DE UNA HERRAMIENTA DE USO DIDÁCTICO ESTEGANOGRÁFICA PARA ENVÍO DE TEXTO OCULTO Y CIFRADO EN ARCHIVOS DE AUDIO MP3.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

DIEGO ANDRÉS CHANGOLUISA SIMBAÑA
diego.changoluisa@epn.edu.ec

DIRECTOR: ING. WILLAMS FERNANDO FLORES CIFUENTES, MSc.
fernando.flores@epn.edu.ec

Quito, abril 2019

AVAL

Certifico que el presente trabajo fue desarrollado por Diego Andrés Changoluisa Simbaña, bajo mi supervisión.

_____

Ing. Willams Fernando Flores Cifuentes, MSc.
DIRECTOR DEL TRABAJO DE TITULACIÓN

DECLARACIÓN DE AUTORÍA

Yo Diego Andrés Changoluisa Simbaña declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Diego Andrés Changoluisa Simbaña

AGRADECIMIENTO

Agradezco a mis padres Rolando y Paulina por su apoyo incondicional y amor, a mi padre por enseñar a ser un profesional responsable y dedicado en la profesión que nos gusta realizar, a mi madre por enseñarme a cada día ser un mejor hombre y padre, a mis hermanos Jacqueline y Erick que de alguna forma estuvieron brindándome su apoyo.

Agradezco a Verónica por los consejos y ayuda que me brindo para culminar mi proyecto.

Gracias a mi director de tesis Ing. Fernando Flores, quien desde semestres bajos confió en mí y me otorgó la oportunidad de trabajar junto a él.

De igual manera agradezco a la Escuela Politécnica Nacional y mis profesores que supieron transmitir sus conocimientos y experiencias para mi formación personal y profesional.

DEDICATORIA

Quiero dedicar el presente proyecto a mi madre Paulina, mi padre Rolando y mi más preciado tesoro mi hija Lia Micaela quien a su corta edad supo preocuparse y brindarme el mayor impulso que se necesita, su amor incondicional, pues esto lo hago por ti, Te Amo mi pequeña Miki; quienes con su gran amor son mi motivación diaria para seguir siempre avanzando y cumpliendo mis metas.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE SEGMENTOS DE CÓDIGO

RESUMEN

En el presente proyecto de titulación se desarrolla una herramienta de uso didáctico esteganográfica para envío de texto oculto y cifrado en archivos de audio MP3.

En el primer capítulo se revisan brevemente los fundamentos teóricos de los diferentes métodos esteganográficos, además se revisa la técnica LSB (Least Significant Bit) de incrustación de datos para diferentes tipos de archivos, adicionalmente se estudian los elementos necesarios para el desarrollo de una aplicación GUIDE dentro del entorno de Matlab, así mismo se analizan los lenguajes de programación de Matlab y finalmente se revisa la información para el proceso de cifrado con la técnica de encriptación Triple DES.

El segundo capítulo presenta la metodología el cual trata sobre el diseño y la implementación de la herramienta de uso didáctico. Se analizan los requerimientos y se describen cada uno de los módulos para tener una perspectiva de las acciones que ejecuta la herramienta, posteriormente se instala el software de desarrollo necesario y luego se implementan los componentes de la herramienta.

En el capítulo tres se relatan las pruebas de funcionamiento de la herramienta de uso didáctico y se constata los resultados obtenidos. Las pruebas realizadas se dirigen a demostrar que la herramienta cumple con el alcance del proyecto técnico, además se dan explicaciones de los resultados.

En el cuarto capítulo se presentan las conclusiones y recomendaciones de acuerdo con el análisis de los resultados obtenidos al comprobar la herramienta.

PALABRAS CLAVE: Esteganografía, LSB, MP3, TripleDES, Matlab.

ABSTRACT

The present final career project develops a steganographic didactic use tool for sending ciphered and hidden text in MP3 audio files.

The first chapter briefly reviews the theoretical fundamentals of the different steganographic methods, in addition to reviewing the LSB (Least Significant Bit) technique of data incrustation for different file types, additionally studying the elements necessary for the development of a GUIDE application in Matlab's environment, as well as analyzing Matlab's programming languages and finally reviewing the information for the ciphering process with TripleDES encryption technique.

The second chapter presents the methodology, so it deals with the design and implementation of the didactic use tool. The requirements are analyzed and each one of the modules is described to have a perspective of the actions that the tool executes, finally the necessary development software is installed and then the components of the tool are implemented.

In the chapter three the didactic use tool performance tests are reported, and the results obtained are reflected. The tests carried out are aimed at demonstrating that the didactic use tool complies with the scope of the technician project, in addition explanations of the results are given.

The fourth chapter the conclusions and recommendations are presented according to the analysis of the results obtained when testing the didactic tool.

KEYWORDS: Steganography, LSB, MP3, TripleDES, Matlab.

CAPÍTULO 1

1. INTRODUCCIÓN

En la actualidad el problema de la privacidad y seguridad en redes de comunicación juegan un rol importante, ya que mediante intromisiones y herramientas para análisis de información se puede interceptar datos que podrían ser de suma importancia para una corporación o empresa.

Los avances tecnológicos y métodos de acceso no permitido en una red cada vez son más sofisticados, donde una mala política de seguridad podría exponer a los usuarios en el intercambio de mensajes o documentos confidenciales.

La palabra esteganografía tiene origen griego significa “encubrir escritura u ocultar”. Es la ciencia de ocultar información. Donde la meta de la criptografía es hacer que los datos sean indescifrables por un tercero, la meta de esteganografía es ocultar los datos de un tercero. En esteganografía la información puede ser oculta en medios portadores como imágenes, archivos de audio, archivos de texto y transmisiones de video y datos. Cuando el mensaje es oculto en la portadora una estego-portadora se forma por ejemplo una estego-imagen. Esteganografía y criptografía son estrechamente relacionados.

Criptografía mezcla mensajes para que no puedan ser entendidos. Esteganografía, por otra parte, ocultara el mensaje para que no se tenga conocimiento de su existencia.

Sin embargo, la esteganografía actual es significativamente más sofisticada, lo que permite al usuario ocultar información dentro de los archivos de imagen y audio. Estas formas de esteganografía usualmente son usadas conjunto con la criptografía para tenerla doblemente protegida.

1.1. Objetivos

El objetivo general del proyecto técnico es:

- Desarrollar una herramienta de uso didáctico esteganográfica para envío de texto oculto y cifrado en archivos de audio mp3.

Los objetivos específicos del proyecto técnico son:

- Analizar la información sobre los métodos esteganográficos, técnica Least Significant Bit (LSB)[1], lenguaje de programación MATLAB[2], estructura del formato MP3.
- Diseñar los módulos y componentes principales de la herramienta de uso didáctico.
- Implementar la aplicación y algoritmos diseñados para cumplir el método esteganográfico con archivos de audio mp3.
- Analizar los resultados de las pruebas realizadas con la herramienta de uso didáctica.

1.2. Alcance

La solución por desarrollarse tiene una aplicación demostrativa y didáctica donde la herramienta permitirá utilizar la técnica esteganográfica para el ocultamiento y recuperación del mensaje a incrustar.

El cual constará de un módulo principal, el cual mediante botones activará los siguientes módulos secundarios:

- Módulo de Ocultamiento del Mensaje
- Módulo de Obtención del Mensaje

En el primer módulo se tomará un archivo de audio MP3 que contenga las siguientes características:

[1] LSB: Es el bit que está más alejado a la derecha y tiene el menor valor en un número binario de múltiples bits.

[2] MATLAB: Es un entorno de computación numérica de paradigma múltiple y un lenguaje de programación patentado desarrollado por MathWorks.

- Tamaño mínimo 2.60 MB.
- Tamaño máximo 9,00 MB.
- Frecuencias de Muestreo estandarizada (32000, 44100, 48000) muestras/segundo.

Este archivo será cargado mediante la interfaz de usuario (Insertar Audio) donde se visualizará el espectro del audio cargado y la información obtenida mediante el uso de la dll (dynamic link library) LAME[3] la cual descompone el archivo y muestra todas las características que posee [1].

Una vez que el archivo de audio ya esté cargado, se habilitarán las opciones para incrustar el mensaje en el archivo de audio, las cuales pueden ser:

- Ingreso de Texto: el estudiante podrá ingresar por teclado el mensaje máximo de 2600 caracteres ASCII que se incrustarán en el archivo de audio mp3.
- Selección de Archivo: el estudiante mediante un botón podrá cargar el archivo de texto (formato .txt[4]) que cual contendrá como máximo 2600 caracteres en formato ASCII.

Se delimita el valor máximo de caracteres para realizar la técnica esteganográfica ya que se debe tomar en cuenta que el formato de audio MP3 ya está comprimido, por lo que el archivo de texto tendrá un tamaño máximo de 2,64 KB para audios de tamaño entre 2,60 - 9,00 MB, para mantener el archivo de audio intacto en tamaño y tiempo de duración, por lo que será imperceptible notar modificación alguna.

Se dispondrá de un cuadro de texto que el estudiante utilizará para el ingreso de la clave a utilizar en el proceso de encriptación.

[3] LAME: Es una herramienta educativa que se utiliza para aprender sobre la codificación de MP3. El objetivo del proyecto LAME es utilizar el modelo de código abierto para mejorar la psicoacústica, la configuración del ruido y la velocidad de MP3.

[4] TXT: Es un documento de texto estándar que contiene texto sin formato

Se tendrá un botón Guardar el cual incrustará el mensaje ingresado previamente por el estudiante, el cual creará el nuevo archivo de Audio MP3 con nombre en formato (ArchivodeAudioOriginal_estego.mp3).

Al finalizar el proceso de incrustación se activará el botón Comparación, el cual permitirá visualizar mediante un plot de espectrograma la diferencia de forma visual con el archivo original.

En la herramienta se tendrán botones de reproducción tanto para el audio original como para el estego-audio (MP3 modificado), donde el estudiante podrá identificar y constatar mediante la herramienta de uso didáctico si existe alguna diferencia al momento de su reproducción, tales como alteraciones o sobresaltos por la modificación del bit en el archivo MP3 al momento de su creación. [2]

Para el segundo módulo se tomará un archivo de audio MP3 con el mensaje incrustado (estego-audio)[5] el cual será cargado; en este módulo se añadirá un recuadro de texto donde el estudiante ingresará la clave de obtención del mensaje con el que fue encriptado, si en un caso la clave es incorrecta se procederá a mostrar un mensaje de clave inválida o mensaje corrupto. En el caso que la clave sea válida continuará con la obtención del mensaje para mostrarlo al estudiante. Cabe mencionar que habrá un producto final demostrable.

1.3. Marco Teórico

1.3.1. Definición

La palabra esteganografía es derivada de las palabras griegas “stegos” que significa “cubierta” y “graphos” que significa “escritura” [3]. Lo que define la como “escritura cubierta”.

[5] Estego-audio: Es el resultado de incrustar la información en la portadora

La esteganografía son datos ocultos dentro de datos. La cual es una técnica de cifrado que se puede utilizar junto con la criptografía como método extra seguro para proteger estos datos.

La criptografía con la esteganografía es básicamente proporcionar seguridad para la información. Usando la criptografía no se va a ocultar el mensaje, está transformando el mensaje (texto cifrado) tratando de ocultar el significado real del mensaje.

La esteganografía por su parte intentará ocultar el mensaje total insertándolo en imagen, audio o video.

Sin embargo, aunque persigan objetivos diferentes para que la esteganografía sea de mayor utilidad debe combinarse con la criptografía de modo que el mensaje que se desea ocultar sea cifrado robustamente y luego ser incrustado en el objeto portador. De modo, que, aunque se descubriese el patrón esteganográfico no se podrá llegar a conocer el mensaje intercambiado.

1.3.2. Terminología

Para poder continuar a más profundidad con el estudio de los aspectos técnicos que involucran las técnicas esteganográficas, analizados en el presente proyecto, es indispensable conocer, las definiciones de la terminología empleada, para poder facilitar el entendimiento y evitar confusiones.

- **Información incrustada o información oculta**, información que será enviada de forma oculta.
- **Portadora (Cover o Carrier),** se refiere al audio, imagen o video en donde se enviará la información incrustada.
- **Estego-objeto,** es el resultado de incrustar la información en la portadora.
- **Estego-clave,** hacer referencia a la clave que se usara en el proceso de incrustación por el algoritmo esteganográfico.

1.3.3. Tipos de esteganografía

Al igual que la criptografía, la esteganografía se divide en dos grandes grupos; la esteganografía clásica y la esteganografía moderna.

a) Esteganografía clásica

La primera descripción de la esteganografía se remonta a los griegos.

Donde Demaratus cuenta como se transmitió un mensaje a los griegos sobre las intenciones hostiles de Xerxes debajo de la cera de una tabla de escritura, y describe una técnica para puntear sucesivamente letras en un texto de portada con una tinta secreta. [3]

500 años A.C Histacios rapo la cabeza de su mensajero, escribió una nota incitando a Aristágoras de Mileto a rebelarse contra el rey de Persia. La desventaja del método era que debía esperar a que el cabello del mensajero creciese para por enviarlo hacia su destino.

Durante la guerra revolucionaria americana, las fuerzas británicas y americanas utilizaron variedad de tintas invisibles. La tinta invisible involucraba fuentes comunes como: leche, vinagre, jugo de frutas y orina para la escritura del texto oculto. Para descifrar los mensajes ocultos se requería de luz o calor.

En la segunda guerra mundial los alemanes introdujeron microdots.

Los microdots fueron documentos completos, fotos y planos de tamaño reducido y adjuntados a la documentación común en la que sería transportada.

En la figura 1.1 se observa la estructura de un microdot como este era reducido a un tamaño poco visible y enviado en un documento poco común.

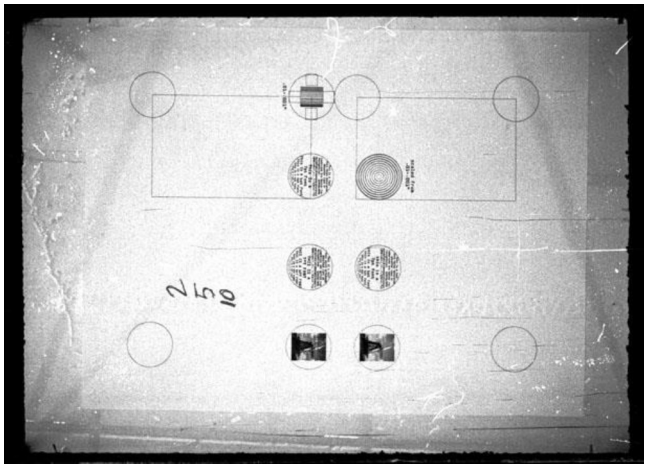


Figura 1.1 Estructura de un microdot. [4]

Aun en la actualidad se utiliza no tan comúnmente los cifradores nulos los cuales envían mensajes reales sin cifrar incrustados en el texto actual. Los mensajes ocultos eran difíciles de interpretar si no se conocía el mecanismo de ocultamiento.

Un ejemplo de mensaje inocente que contiene el cifrado nulo es:
Fishing freshwater bends and saltwater coasts rewards anyone feeling stressed. Resourceful anglers usually find masterful leapers fun and admit swordfish rank overwhelming any day. [5]

Tras tomar la tercera letra de cada palabra surge el siguiente mensaje:
Send Lawyers, Guns, and Money.

b) Esteganografía moderna

La esteganografía en la actualidad se refiere a la información de un archivo cualquiera que se encuentre oculto dentro de otro, normalmente multimedia, por ejemplo, el portador es una imagen digital, un video o archivo de audio.

Últimamente la esteganografía y particularmente las técnicas de incorporación de mensajes de copyright[6] en documentos, imágenes y archivos de audio han experimentado una notable demanda.

[6] **Copyright:** es el termino legal que se usa para describir los derechos que tiene el creador sobre trabajos artísticos y literarios.

Particularmente las técnicas conocidas como “marca de agua” (watermarking)[7] para ocultar mensajes de copyright para identificar números de serie o distinguir objetos específicos entre otros similares.

La importancia de estos métodos radica en que la protección de derechos de copyright de imágenes, álbumes y documentos escritos se han hecho cada vez más difíciles, donde para obtener alguno de estos simplemente se requiere navegar por la web y bajarlo.

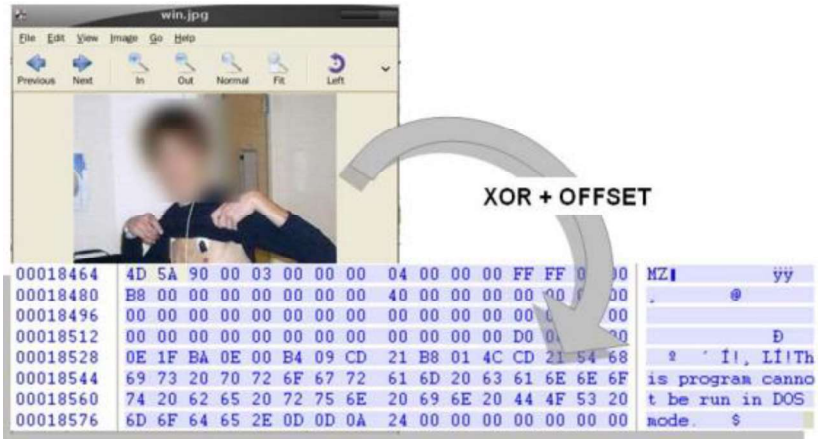


Figura 1.2 Ejemplo de esteganografía moderna en imágenes. [6]

1.3.4. Modelo Básico de esteganografía

El modelo básico de esteganografía se compone de portadora (Carrier), mensaje y clave de encriptación o password (estego-clave).

La portadora es comúnmente conocida como el objeto de cobertura, en donde el mensaje será incrustado y servirá para ocultar la presencia del mensaje. Básicamente, el modelo para la esteganografía se muestra en la Figura 1.3 [7].

El mensaje es la información que el transmisor desea enviar teniendo en cuenta que lo que se desea es la confidencialidad. Este puede ser texto plano, texto cifrado, o cualquiera que se pueda incrustar en un flujo de bits tales como marcas de copyright, comunicación encubierta, o un número serial.

[7] **Watermarking:** proceso de ocultar información digital dentro de una señal portadora.

Password es conocido como la estego-clave, la cual se asegura que solo el receptor el cual conoce la correspondiente llave de decodificación sea capaz de extraer el mensaje desde el objeto encubierto. El objeto encubierto con el mensaje secreto incrustado se lo denomina estego-objeto.

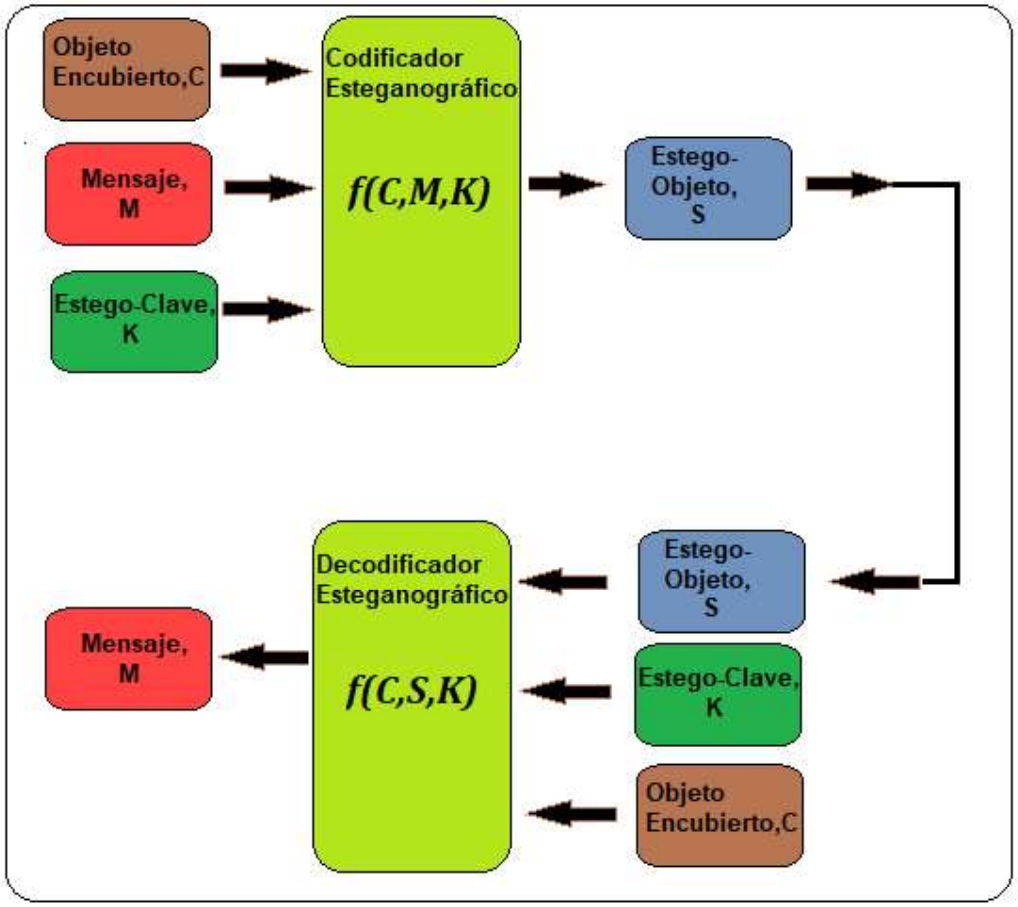


Figura 1.3 Modelo Básico Esteganografía

1.3.5. Clasificación de las categorías esteganográficas

La esteganografía se clasifica en tres categorías.

a) **Esteganografía pura:** Donde no se tiene estego-clave. Se basa en el supuesto de que ninguna otra parte tiene conocimiento de la comunicación. El problema con esta categoría es que no se obtienen ninguna seguridad, si el atacante conoce el método de esteganografía usado.

   La esteganografía pura puede ser definida como las variables (C, M, D y E) donde:

- **C:** El conjunto de posibles portadoras
- **M:** El mensaje secreto con |C|≥|M|
- **E:** CxM →C la función de incrustación
- **D:** C→M la función de extracción con la propiedad de D (E (c, m))= m para todos los m Є M y c Є C.

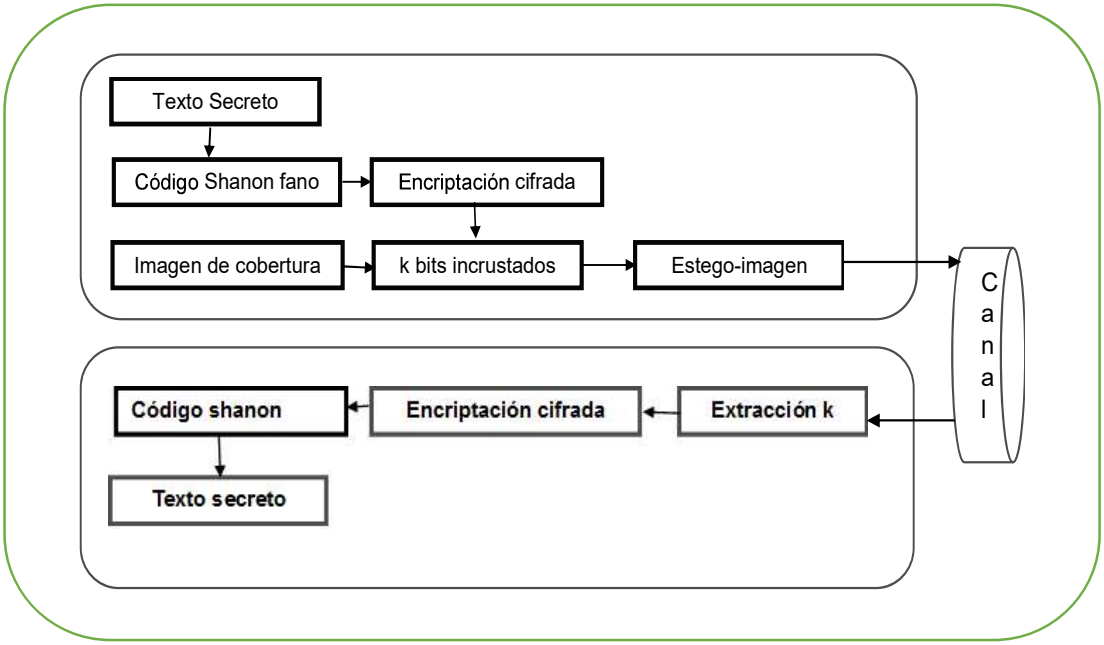


Figura 1.4 Esteganografía pura

b) **Esteganografía de clave secreta:** La estego-clave es intercambiada previa a la comunicación. El sistema es similar a un cifrador simétrico, donde el transmisor elige una cubierta e incrusta el mensaje secreto dentro de la portadora usando una llave secreta. Si la clave secreta utilizada en el proceso de incrustación es conocida por el receptor, este podrá realizar el proceso inverso y extraer el mensaje secreto.

La esteganografía de clave secreta puede ser definida como las variables (C, M, DK y EK) donde:

- **C:** Conjunto de posibles portadoras.
- **M:** El mensaje secreto.
- **K:** Conjunto de llaves secretas.

- **Ek:** CxMxK →C donde Dk (EK (c, m, k), k) =m para todos los m Є M, c Є C y k Є K.

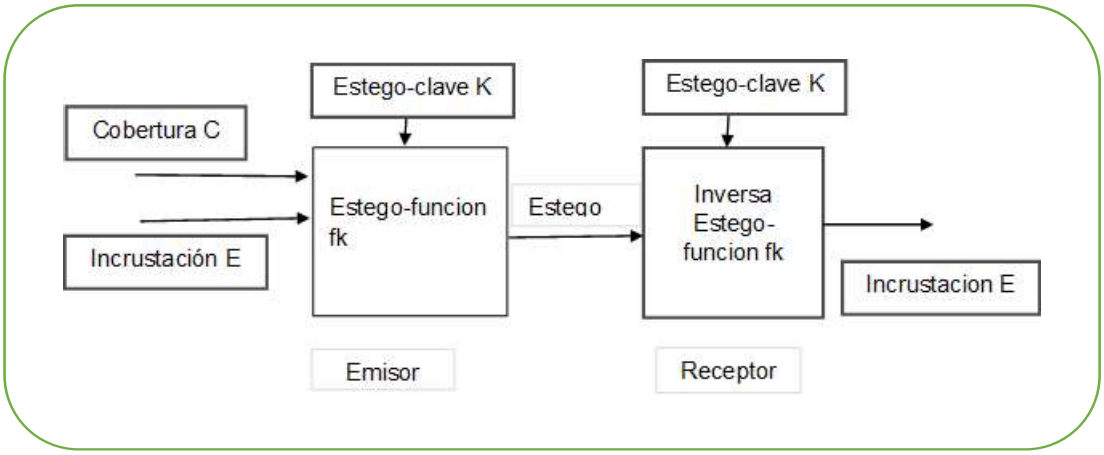


Figura 1.5 Esteganografía de clave secreta

c) **Esteganografía de clave pública:** La clave pública y privada son utilizadas para una comunicación segura. No depende del intercambio de una llave secreta esta requiere dos llaves, una que se denominara privada(secreta) y otra denominada pública: la clave pública es almacenada en base de datos públicas; mientras que la clave publica es utilizada para el proceso de incrustación. La clave privada se la utiliza para recuperar el mensaje secreto. Una forma de construir un sistema esteganográfico de clave publica es usar un sistema en encriptación de clave pública. El emisor y el receptor pueden intercambiar claves publica de algunos algoritmos criptográficos de clave publica antes de incrustar.

1.3.6. Características de un sistema esteganográfico

Las técnicas esteganográficas incrustan un mensaje dentro de una portadora. Por lo tanto, es relativo que cada característica dependa de la aplicación. [9]

Un esquema efectivo esteganográfico podría poseer las siguientes características deseadas [10]:

a) **Capacidad:** La noción de capacidad en el ocultamiento de datos indica el número total de bits ocultos y recuperados con éxito por el estego-sistema. [11]

b) **Robustez:** Se refiere a la capacidad de datos incrustados para permanecer intactos si el estego-sistema sufre una transformación. Como filtrado lineal y no lineal, adición de ruido aleatorio, y escalamiento, rotación y compresión suelta [12].

c) **Indetectable:** Un algoritmo de incrustación es indetectable, si una portadora con un mensaje incrustado es consistente con el modelo de la fuente con el cual se constituyó. Por ejemplo, si un método de esteganografía utiliza el componente de ruido de las imágenes digitales para incrustar el mensaje secreto, debe hacerlo sin realizar cambios estadísticos al ruido en la portadora.

   La indetectabilidad se ve afectada directamente por el tamaño de mensaje secreto y el formato del contenido de la portadora a cubrir [9].

d) **Invisibilidad (Transparencia perceptiva):** Este concepto se basa en las propiedades del sistema visual y auditivo humano. La información incrustada es imperceptible si un sujeto (humano promedio) no puede distinguir entre portadoras que contienen información oculta y aquellas que no lo hacen [12].

e) **Seguridad:** Se refiere a que tan seguro es el algoritmo, donde la información incrustada no está sujeta a eliminación después de ser descubierta por el atacante y depende de la información total sobre el algoritmo incorporado y la clave secreta [13] [14].

1.3.7. Clasificación de las Técnicas esteganográficas

Existen varios enfoques para clasificar los sistemas esteganográficos. Se los podría categorizar de acuerdo con el tipo de cubierta utilizada para la comunicación secreta o según las modificaciones de éstas aplicadas en el proceso de incrustación. Los métodos esteganográficos se los agrupa en 6 categorías, sin embargo, en algunos casos una clasificación exacta no es posible [15] [16] [17] [18].

La figura 1.6 presenta la clasificación esteganográfica.

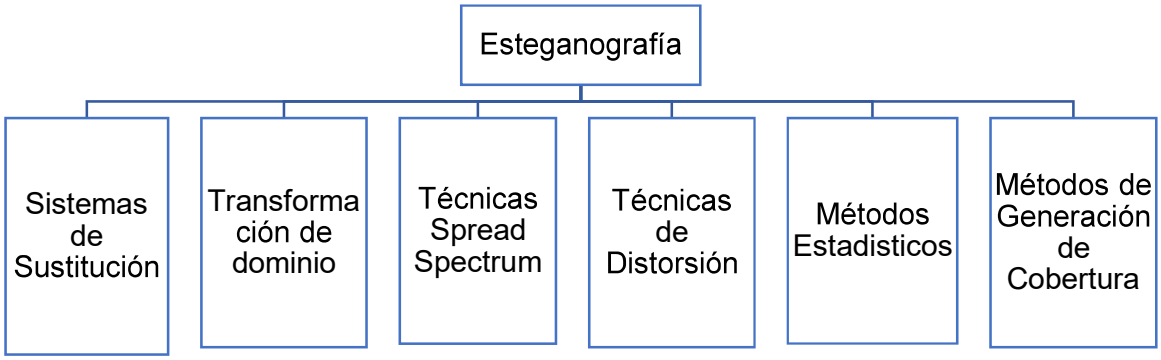


Figura 1.6 Clasificación Esteganográfica

1) Sistemas de sustitución.

Los sistemas básicos de sustitución intentan codificar información secreta sustituyendo partes insignificantes de la cubierta por bits de mensaje secreto. El receptor puede extraer la información si tiene conocimiento de las posiciones donde se ha incrustado la información secreta. Dado que solo se realizan modificaciones menores en el proceso de incrustación, el remitente asume que un atacante no las notará. Consiste en varias técnicas que se analizarán con más detalle en la siguiente subsección: [16], [17], [19], [20].

a) **Sustitución de bit menos significativa (LSB):** El proceso de inserción consiste en elegir un subconjunto de elementos $\{J_1 \ldots J_l\ (m)\}$ de cobertura y realizar la operación de sustitución $C_{ji} \leftrightarrow m_i$ entre ellos, donde intercambian el LSB de C_{ji} por m_i (m_i puede ser 1 o 0). En el proceso de extracción, se extrae el LSB del elemento de cobertura seleccionado y se alinea para reconstruir el mensaje secreto.

b) **Permutación Pseudorandómica**: Si se accede a todos los bits de cobertura en el proceso de incrustación, la cobertura es una de acceso aleatorio, y los bits de mensaje secreto se pueden distribuir aleatoriamente en toda la cobertura. Esta

técnica aumenta aún más la complejidad para el atacante, ya que no garantiza que los bits de mensaje subsiguientes estén incrustados en el mismo orden.

2) Técnicas de Transformación de Dominio

Estos métodos ocultan el mensaje en un área significativa de la cobertura del archivo el cual lo hace más robusto ante un ataque, como añadir ruido y proceso de compresión de archivos. Sin embargo, estos son más robustos a varios tipos de procesadores de señal y permanecen imperceptibles al sistema sensorial humano [21].

3) Técnicas Spread Spectrum (SS)

Las técnicas spread spectrum se definen como "Medio de transmisión en los cuales la señal ocupa un ancho de banda que excede el mínimo necesario para enviar la información". La expansión se realiza mediante código independiente de los datos, y es utilizada una recepción sincronizada con el código en el receptor para su envío y la posterior recuperación de datos [12] [13] [14] [21].

4) Técnicas de distorsión

Se requiere conocer la cubierta original para el proceso de decodificación. El transmisor aplica una serie de modificaciones en el objeto cubierta para poder obtener el estego-sistema. Se elige una secuencia de modificaciones de tal manera que se corresponda con el mensaje secreto específico para ser transmitido. El receptor constata la diferencia con la cubierta original para poder reconstruir la serie de modificaciones aplicadas por el transmisor, las cuales corresponderán al mensaje secreto.

5) Métodos estadísticos

Las técnicas de esteganografía estadística utilizan esquemas esteganográficos de "1-bits" existencia, el cual incrusta 1 bit de información en la portadora digital. Modificando el objeto cubierta y cambiando significativamente algunas características estadísticas.

6) Técnicas de generación de cubiertas

Estas técnicas después de agregar el mensaje oculto a una cubierta específica generan un objeto digital para que luego pueda ser utilizada como nueva cubierta y proteger la comunicación.

1.3.8. Audios Digitales

Los formatos de archivos de audio difieren a lo largo de una serie de ejes. Pueden ser gratuitos o propietarios, restringidos por plataforma o multiplataforma, comprimidos y no comprimidos, archivos de contenedor o archivos de audio simples y protegidos contra copia[8] o desprotegidos. Donde los detalles de un formato propietario y cómo se produce el formato no se hacen públicos y su uso está sujeto a patentes.

En simplicidad todos los formatos de audio se dividen en tres categorías principales las cuales se detallan en la tabla a continuación:

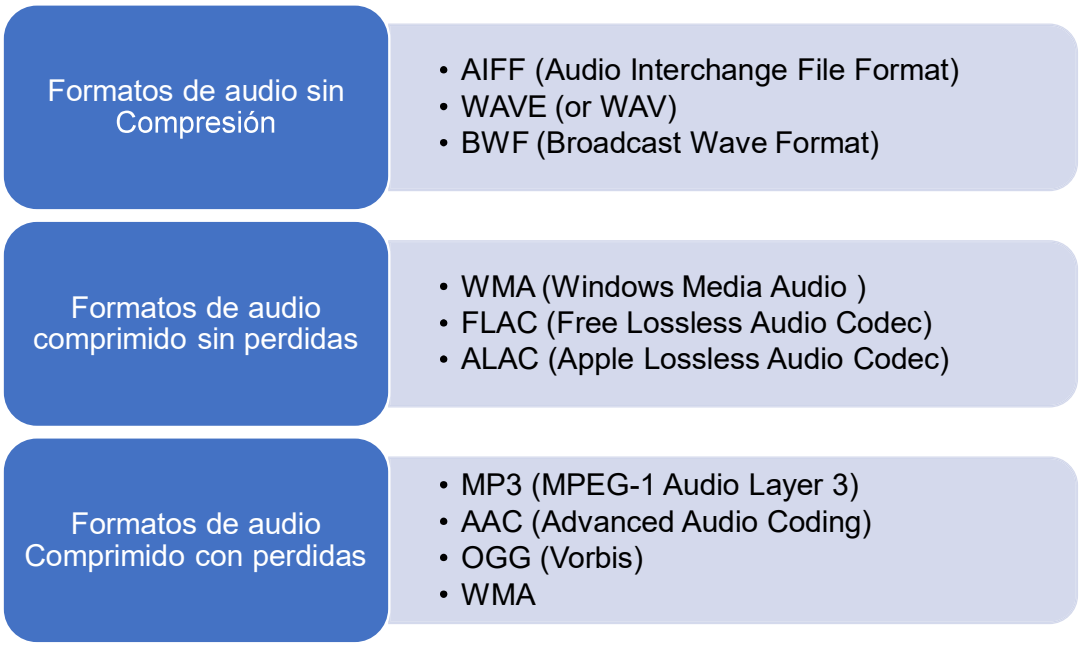


Figura 1.7 Categorías Audio digital

[8] La protección contra copia es más comúnmente conocida como gestión de derechos digitales o DRM

1) Formatos de audios sin compresión

El audio sin comprimir es exactamente lo que suena: ondas de sonido reales que se capturan y convierten a formato digital sin ningún procesamiento adicional. Como resultado, los archivos de audio sin comprimir tienden a ser los más precisos, pero como consecuencia ocupan demasiado espacio en disco, aproximadamente 34 MB por minuto para el estéreo de 24 bits a 96 kHz.

En este tipo de formato de audio el más conocido es WAV[9].

2) Formatos de audio comprimido sin pérdidas

La compresión sin perdidas es un método el cual reduce el tamaño del archivo sin ninguna pérdida de calidad entre el archivo original y el archivo resultante. El inconveniente que se tiene es que la compresión sin perdidas no será tan eficiente como una compresión con pérdidas, lo que significa que se puede tener archivos equivalentes de 2 a 5 veces más grandes.

3) Formatos de audio comprimido con pérdidas

La compresión con pérdidas es un tipo de compresión en la cual se pierde información durante el proceso de compresión. Dentro del contexto de audio, significa sacrificar calidad y fidelidad en el tamaño del archivo. Lo mejor de esto es que en la mayoría de los casos, al escucharlo no se notará diferencia alguna.

Sin embargo, si el audio es comprimido demasiado, se notará una diferencia notable como ruidos que serán cada vez más notables.

1.3.9. Formatos de Audio

En la actualidad existen varios formatos digitales, lo cual surgió debido a las diferentes plataformas de reproducción existentes, a continuación, se detalla algunos formatos más utilizados.

[9] WAV: Waveform Audio Format también llamado audio para Windows. Creado por Microsoft e IBM en 1991.

Tabla 1.1 Características de Formatos de audio más utilizados

Formato	Extensión	Aplicación	Desarrollador
WMA	.wma	Utilizado en el sistema Windows, pero reproducido sin ningún inconveniente en sistemas Mac	Microsoft.
AAC	.aac	Formato de compresión utilizado mayoritariamente por YouTube, Android, iOS, iTunes, consolas como Nintendo y Play Station	Bell Labs, Fraunhofer Institute, Dolby Labs, Nokia y Sony
MP3	.mp3	Formato de reproducción multiplataforma	Moving Picture Experts Group (MPEG)

a) Formato WMA

El formato WMA (Windows Media Audio) se refiere al formato de audio del archivo y como se codifica, es un formato de audio comprimido creado y popularizado por Microsoft.

La extensión de este archivo de audio funciona mediante el reproductor Windows Media Player usado comúnmente para música. Lo que significa que al ser Microsoft el propietario el formato presenta problemas de compatibilidad con otras plataformas.

Inicialmente fue desarrollado de forma similar a MP3 en casi todos sus aspectos, creando una mejor compresión y manteniendo el mismo nivel de calidad de sonido especialmente en Bitrates[10] bajos.

[10] Bitrate: Describe la velocidad a la que se transfieren los bits; mide la cantidad de datos que se transmiten en un periodo de tiempo determinado.

Existe desventajas dado que el formato WMA es propietario y está protegido por DRM[11], la compatibilidad puede ser un gran problema debido a la poca compatibilidad de otras plataformas o varios dispositivos convencionales, lo que hace que la ventaja de este formato también sea una desventaja en algunos casos.

b) Formato AAC

Un archivo con la extensión AAC es un archivo MPEG-2[12] Advanced Audio Coding. El cual es similar al formato de audio MP3, pero incluye algunas mejoras de rendimiento.

La idea primordial del algoritmo AAC es explotar las principales estrategias de codificación y así reducir drásticamente la cantidad de datos necesarios para transmitir audio digital de alta calidad. Posee frecuencias de muestreo entre 8 Hz y 96 KHz y número de canales entre 1 y 48. [22]
AAC es más capaz de codificar audio con flujos de pulsos complejos y ondas cuadradas que MP3 o Musicam[13].

c) Formato MP3

El formato MP3 se encuentra estandarizado por MPEG-1[14] Audio Layer 3. Fue lanzado en 1993 convirtiéndose en el formato de audio más popular del mundo par archivos de música.

El Principal propósito de MP3 es proveer una calidad de audio cercana a CD. MP3 puede comprimir una canción en un factor de entre 10 o 12. Por lo tanto, un archivo de sonido de 30 megabytes de un CD se reduce a 3 megabytes o menos.

---

[11] DRM (Digital Rights Management): es un enfoque sistemático de la protección de derechos de autor para medios digitales
[12] MPEG-2(Moving Picture Experts Group): es un estándar genérico ISO/IEC 13818-3 para codificación de imágenes en movimiento y audio asociado.
[13] Musicam: fue uno de los pocos códecs capaces de lograr una alta calidad de audio a velocidades de bits en el rango de 64 a 192 kbit / s por canal monofónico.
[14] MPEG-1: es un estándar para audio y video comprimido, publicado en la ISO/IEC 11172- Tecnología de la información- Codificación de imágenes en movimiento y audio asociado para medios de almacenamiento digital de hasta 1,5 Mbit/s

Una de las razones por la cual este tipo de formato se ha convertido en el más utilizado es debido a que elimina el rango de frecuencia que el oído humano no escucha, comprendido entre valores mayores a 20 KHz y menores a 20 Hz, logrando así que el archivo final con extensión mp3 ocupe menor tamaño en disco duro.

1.3.10. MPEG Audio Layer 3

Un archivo de audio MPEG se construye a partir de partes más pequeñas denominadas tramas. Generalmente las tramas son elementos independientes donde cada trama tiene su propio encabezado e información de audio.

Al no existir un encabezado de archivo se puede cortar cualquier parte del archivo MPEG y reproducirlo correctamente (esto debe realizarse en los límites de las tramas). Sin embargo, para la capa III, no es 100% correcto; debido a la organización interna de los datos en archivos del tipo MPEG layer III, las tramas a menudo dependen unas de otras y no pueden ser cortadas así.

Cuando se desea leer información sobre un archivo MPEG, generalmente resulta suficiente encontrar la primera trama, leer su encabezado y asumir que los otros cuadros son iguales. Pero no siempre puede ser este el caso.

Los archivos MPEG de Bitrate variable pueden usualmente usar un cambio de Bitrate, lo cual significa que el Bitrate cambia de acuerdo con el contenido de cada trama. De esta manera, se pueden utilizar Bitrates más bajos, tramas donde no se reducirá la calidad del sonido. Permitiendo hacer una mejor compresión manteniendo una calidad de sonido alta.

Los cuatro primeros bytes (32 bits) constituyen la cabecera de la trama donde los primeros once bits (o 12 dependiendo de la sincronización de la trama) de la cabecera de la trama siempre se configuran y se denominan “sincronización de trama”; por lo tanto, en el archivo se puede buscar la primera vez que se produce una sincronización de tramas.

Las tramas pueden tener un campo de verificación CRC[15].Donde el código CRC tiene una longitud de 16 bits, y de existir se indica que el encabezado de la trama continúa; después del campo CRC vienen los datos de audio, lo cual identifica que es realmente un método muy bueno para verificar la validez de la trama MPEG.

En las tablas a continuación, se indica una representación del contenido de la cabecera, donde los caracteres desde A hasta M se utilizan para indicar detalles de cada uno de los diferentes campos.

Tabla 1.2 Estructura de la Cabecera MP3

1 byte (8 bits)	1 byte (8 bits)	1 byte (8 bits)	1 byte (8 bits)
AAAAAAAA	**AAABBCCD**	**EEEEFFGH**	**IIJJKLMM**

a) Detalle de los campos de la cabecera MP3:

Tabla 1.3 Campo sincronización

Signo	Longitud (bits)	Posición(bits)	Descripción
A	11	(31-21)	Sincronización de Trama.

Tabla 1.4 Campo ID de versión MPEG

Signo	Longitud (bits)	Posición (bits)	Descripción
B	2	(20-19)	MPEG Audio versión ID 00 – MPEG versión 2.5[16] (extensión a futuro de MPEG 2). 01 – reservado. 10 – MPEG versión 2 (ISO/IEC 13818-3). 11 – MPEG versión 2 (ISO/IEC 11172-3).

[15]CRC (Código de Redundancia Cíclica):es un código de detección de errores usado frecuentemente en redes digitales y en dispositivos de almacenamiento para detectar cambios accidentales en los datos.

[16] MPEG Versión 2.5: no es un standard oficial; es una extensión utilizada para archivos de muy bajo bitrate.

Tabla 1.5 Campo descripción de la capa

Signo	Longitud (bits)	Posición(bits)	Descripción
C	2	(18-17)	00 – Reservado; 01 – Layer III 10 – Layer II; 11 – Layer I

Tabla 1.6 Campo Protección de bit

Signo	Longitud (bits)	Posición(bits)	Descripción
D	1	(16)	0 – Protegido por CRC (16 bits siguientes de la cabecera son CRC). 1 – No protegido.

Tabla 1.7 Índice de Bitrate

Signo	Longitud (bits)	Posición(bits)	Descripción
E	4	(15 - 12)	V - MPEG versión 1; L1 - Layer I; L2 - Layer II; L3 - Layer III

bits	V, L1	V, L2	V, L3
0000	free	free	free
0001	32	32	32
0010	64	48	40
0011	96	56	48
0100	128	64	56
0101	160	80	64
0110	192	96	80
0111	224	112	96
1000	256	128	112
1001	288	160	128
1010	320	192	160
1011	352	224	192
1100	384	256	224
1101	416	320	256
1110	448	384	320
1111	bad	bad	bad

- Free: significa que es un formato libre
- Bad: significa que no es un valor permitido

Cada trama puede ser creada por un Bitrate diferente por lo que los decodificadores Layer III deben soportar este método.

Tabla 1.8 Campo frecuencia de muestreo

Signo	Longitud (bits)	Posición(bits)	Descripción
F	2	(11-10)	Los valores están dados en Hz **bits** — **MPEG-1** **00** — 44100 **01** — 48000 **10** — 32000 **11** — reservado

Tabla 1.9 Campo Relleno

Signo	Longitud (bits)	Posición(bits)	Descripción
G	1	(9)	0- la trama no tiene relleno 1- la trama tiene relleno con un slot extra

El relleno es utilizado para ajustar el Bitrate. Por ejemplo, en Layer II a 44.1 Khz utiliza una cantidad de tramas de 418 bytes y otras de 417 bytes de longitud para obtener un bitrate exacto de 128kbps.

Para archivos de Layer II y Layer III se utiliza la siguiente formula

$$Longitud\ de\ Trama\ en\ Bytes = \frac{144 * Bitrate}{SampleRate + Relleno}$$

Ejemplo:

Layer III, BitRate= 128000, SampleRate= 441000, Relleno= 0

Tamaño de la Trama= 417 bytes

Tabla 1.10 Campo bit privado

Signo	Longitud (bits)	Posición(bits)	Descripción
H	1	(8)	El valor de campo es solo informativo

Tabla 1.11 Campo modo del canal

Signo	Longitud (bits)	Posición(bits)	Descripción
I	2	(7-6)	00 – Estéreo 01 – Joint estéreo (Estéreo) 10 – Canal dual (2 canales mono) 11 – Canal simple (mono)

Tabla 1.12 Campo modo de extensión

Signo	Longitud (bits)	Posición(bits)	Descripción
J	2	(5-4)	Es utilizado para unir información que no sirve para el efecto estéreo, comúnmente utilizados en Layer I y II

Tabla 1.13 Campo Copyright

Signo	Longitud (bits)	Posición(bits)	Descripción
K	1	(3)	0 – El audio no tiene derechos de autor 1 - El audio tiene derechos de autor

Tabla 1.14 Campo Original

Signo	Longitud (bits)	Posición(bits)	Descripción
L	1	(2)	0 – copia del medio original 1 – medio original

Al estar configurado el bit original indica que la trama se encuentra con un medio original.

Tabla 1.15 Campo Énfasis

Signo	Longitud (bits)	Posición(bits)	Descripción
M	2	(1-0)	00 – ninguno 01 – 50/15 ms 10 – reservado 11 – CCIT J.17

La indicación de énfasis permite indicar al decodificador que el archivo debe ser enfatizado, es decir, el decodificador debe "re-ecualizar" el sonido después la suprimir el ruido similar a como lo realiza Dolby[17]; por lo que rara vez se utiliza.

En la Figura 1.8 se muestra la estructura global de la cabecera MPEG-1 correspondiente a una trama de audio.

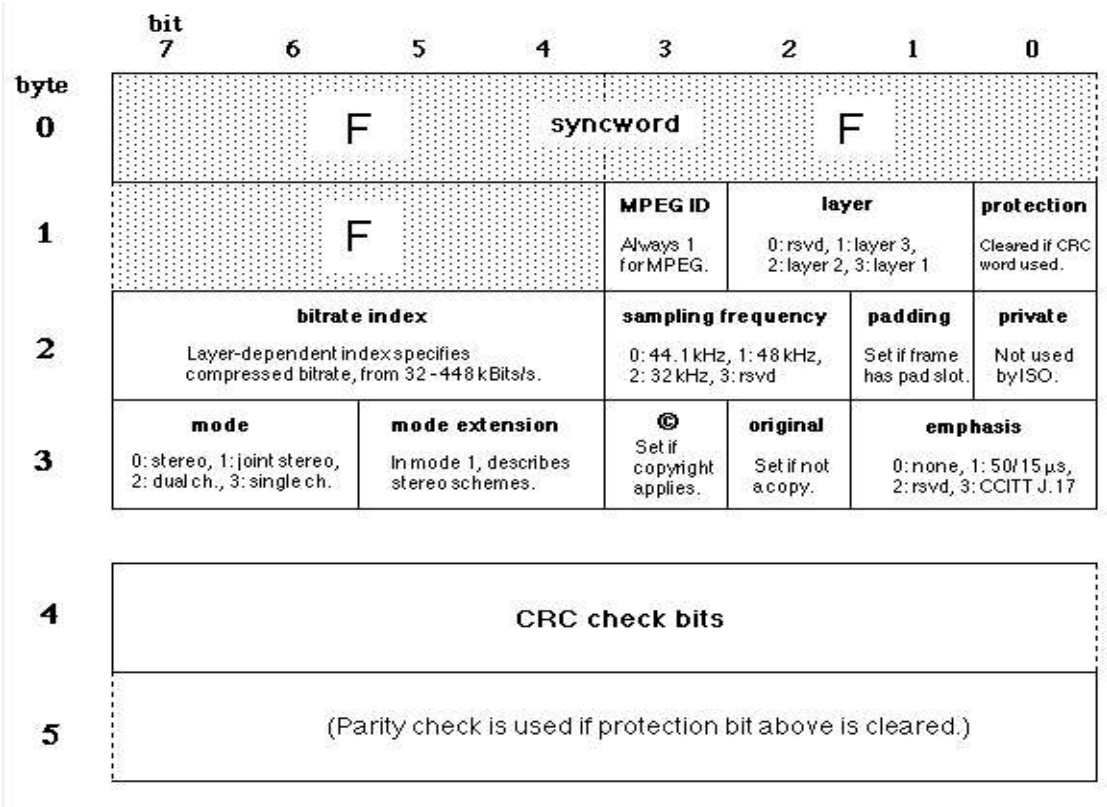


Figura 1.8 Cabecera de una trama de Audio MPEG-1. [23]

[17] Dolby: es una técnica de codificación de audio digital que permite reducir la cantidad de información necesaria para producir un audio de alta calidad.

1.3.11. MPEG Audio Tag ID3

El TAG-ID3[18] se utiliza para la descripción del archivo de audio MPEG; el cual contiene la siguiente información:

- Artista
- Título
- Álbum
- Año de publicación
- Género
- Espacio extra para comentarios

Tiene exactamente 128 bytes de longitud y se encuentra al final de los datos de audio (caso excepcional de la v1).

Tabla 1.16 TAG ID3v1

8 bytes	8 bytes	8 bytes	8 bytes
AAABBBBB	**BBBBBBBB**	**BBBBBBBB**	**BBBBBBBB**
BCCCCCCC	**CCCCCCCC**	**CCCCCCCC**	**CCCCCCCD**
DDDDDDDD	**DDDDDDDD**	**DDDDDDDD**	**DDDDEEE**
EFFFFFFF	**FFFFFFFF**	**FFFFFFFF**	**FFFFFFFG**

Tabla 1.17 Descripción del TAG ID3v1

Signo	Longitud (bytes)	Posición (bytes)	Descripción
A	3	(0-2)	Identificación del TAG. Podría contener el tag si este existe y es correcto.
B	30	(3-32)	Título
C	30	(33-62)	Artista
D	30	(63-92)	Álbum
E	4	(93-96)	Año
F	30	(97-126)	Comentarios
G	1	(127)	Género

[18] TAG-ID3: es un tipo de contenedor de metadato usado para almacenar información sobre un archivo MP3 dentro de este mismo.

Cabe mencionar que la versión del TAG ID3 más utilizado en la actualidad es la versión 2.3 la cual tiene una parte de sus datos antes de los datos binarios del audio. Cada TAG ID3v2 contiene uno o más fragmentos pequeños de información, llamados tramas. Estas tramas pueden contener cualquier tipo de información como los antes mencionados.

En la figura 1.9 se muestra un esquema de bloques de cómo puede ser el diseño típico de un etiquetado ID3v2 para un archivo de audio. [24]

Figura 1.9 TAG ID3v2

1.3.12. Métodos Esteganográficos en archivos de Audio

La estenografía en audio es más importante que otros medios esteganográficos (texto, imagen, video), debido a que se puede transportar información redundante en comparación de otros, por lo que se requiere un tipo de cobertura para ocultar el mensaje secreto; los cuales al ser unidos se convierten en un estego-objeto.

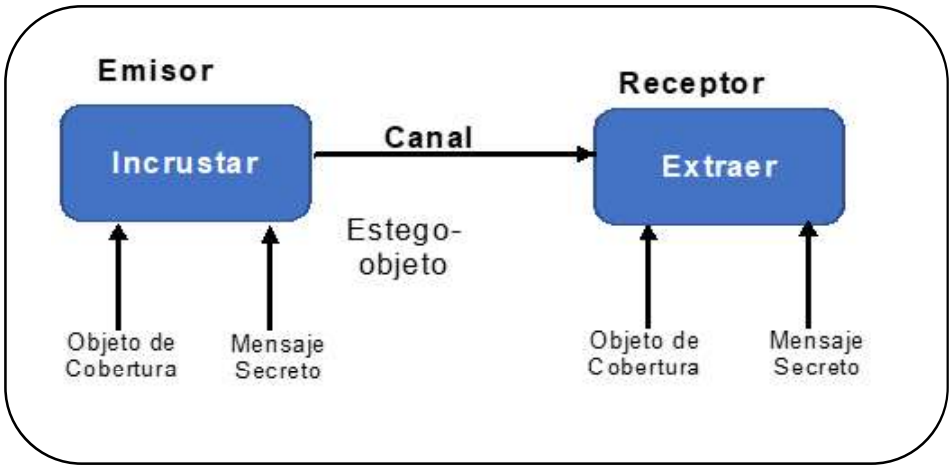


Figura 1.10 Diagrama de bloques para esteganografía en audio

Por lo que se propone la siguiente clasificación para los métodos esteganográficos en archivos de audio:

- Dominio Temporal
- Dominio Frecuencial
- Dominio de ondícula

a) Dominio Temporal

La conforman las siguientes técnicas:

1. **Low bit encoding:** también conocida con el nombre de Least Significant Bit (LSB), es una de las principales en el estudio de ocultamiento de información en señales de audio. Se basa en seleccionar un subconjunto de muestras de audio en las cuales se realiza la sustitución de los bits a ocultar por el valor de los bits originales.

2. **Echo Hiding:** es una técnica que incrusta información dentro de una señal de audio, su funcionamiento es encontrar "huecos" dentro del rango de precepción del sistema auditivo humano, en donde los datos pueden se ocultos, teniendo como objetivo una degradación mínima con respecto a los

datos originales, dificultando la percepción del cambio de audio para el oyente.

b) Dominio Frecuencial

Las principales técnicas de dominio frecuencial son:

1. **Tone insertion:** se encarga de conseguir la imperceptibilidad auditiva de tonos de baja amplitud, dentro de un espectro más grande. Por lo que el audio original es dividido en segmentos de 16 ms de duración, calculando la amplitud de cada muestra e incrustando únicamente un bit en el audio original.

2. **Phase Coding:** se encarga de incrustar información en la fase de la señal de audio, obteniendo un buen rendimiento respecto a la fidelidad del dato oculto. No obstante, una limitante es la poca capacidad de incrustación.

c) Dominio de ondícula

Conocido en inglés como Wavelet Domain, tiene propiedades de multi-resolución convirtiéndolo en un método apropiado para el análisis de frecuencia, al trabajar con coeficientes de ondículas, mediante una transformación inversa es posible reconstruir la estego-señal.

1.3.13. Método Least Significant Bit (LSB)

El algoritmo de bit menos significativo (LSB) se considera el método esteganográfico más simple para incrustar información en un archivo de audio digital [25].

Sustituye el bit menos significativo de cada muestra por uno del mensaje binario. Permitiendo que se codifique una gran cantidad de datos mediante este tipo de codificación.

La figura 1.11 ilustra cómo se codifica el mensaje “HEY” en una muestra de calidad de CD de 16 bits utilizando el método LSB.

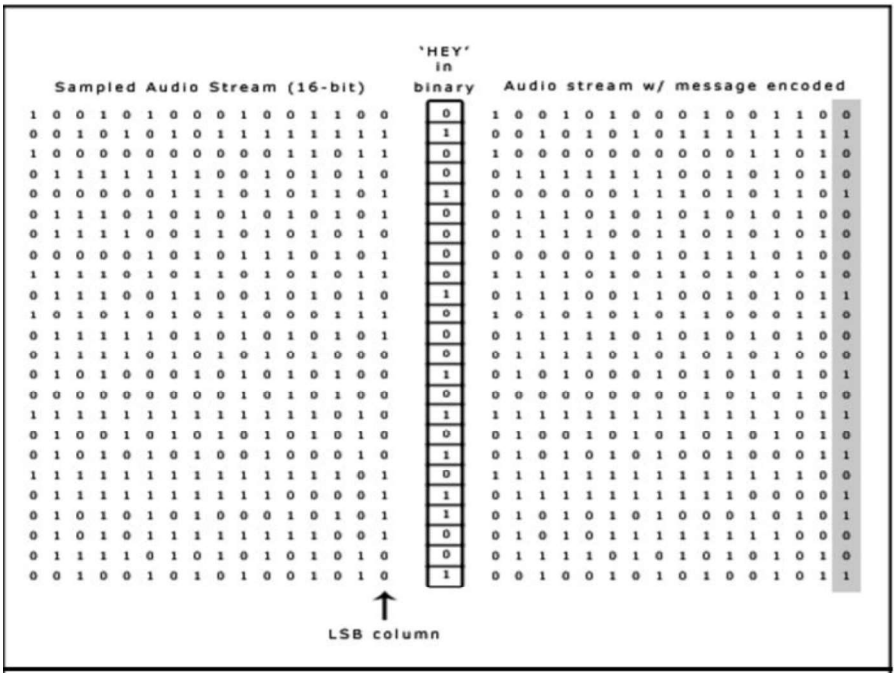


Figura 1.11 El mensaje “HEY” es codificado en una muestra con calidad de CD de 16-bit utilizando el método LSB [26].

En la codificación LSB, la velocidad de transmisión de datos ideal es de 1 kbps por khz. Sin embargo, en algunas implementaciones de este método, se toma los dos bits menos significativos de una muestra los cuales se reemplazan con dos bits del mensaje a ser enviado. Esto aumenta la cantidad de datos que se puede codificar, pero a consecuencia aumenta la cantidad de ruido resultante en el archivo de audio. Por lo tanto, se debe considerar el contenido de la señal antes de elegir la operación LSB a utilizar.

En el proceso de extracción del mensaje secreto de un archivo de sonido codificado mediante el método LSB, el receptor necesita acceso a la secuencia de índices utilizados en el proceso de incrustación. Por lo que normalmente, la longitud del mensaje secreto a codificar es menor que el número total de muestras en un archivo de sonido.

Entonces, se debe decidir cómo elegir el subconjunto de muestras que contendrán el mensaje secreto e indicar de esta decisión al receptor para realizar la correcta decodificación del mensaje.

1.3.14. Software MATLAB

El nombre 'Matlab' proviene de dos palabras: matrix y laboratory. Según The MathWorks (productor de Matlab), Matlab es un lenguaje informático técnico utilizado principalmente para cálculos numéricos de alto rendimiento y visualización. Integra la computación, la programación, el procesamiento de señales y los gráficos en un entorno fácil de usar, en el que los problemas y las soluciones se pueden expresar con notación matemática. El elemento de datos básicos es una matriz, que permite calcular fórmulas matemáticas difíciles, que se pueden encontrar principalmente en álgebra lineal.

Pero Matlab no es solo sobre problemas de matemáticas; puede ser ampliamente utilizado para analizar datos, modelado, simulación y estadísticas. El lenguaje de programación de alto nivel de Matlab encuentra implementación en otros campos de la ciencia como la biología, la química, la economía, la medicina y muchos más.

La característica más importante de Matlab es la fácil extensibilidad. Este entorno permite crear nuevas aplicaciones y convertirse en autor contribuyente. Ha evolucionado durante muchos años y se ha convertido en una herramienta de investigación, desarrollo y análisis.

Matlab también cuenta con un conjunto de bibliotecas específicas, llamadas toolboxes. Recopilan funciones listas para usar, que se utilizan para resolver problemas de áreas particulares.

El sistema Matlab consta de cinco partes principales.

1) Las herramientas de escritorio y el entorno de desarrollo son un conjunto de herramientas útiles al trabajar con funciones y archivos. Ejemplos de esta

parte pueden ser la ventana de comandos, el área de trabajo, el editor de bloc de notas y un mecanismo de ayuda muy extenso.

2) La librería de funciones matemáticas de Matlab es una amplia colección de funciones elementales como suma, multiplicación, seno, coseno, tangente, etc. Además de las operaciones simples, se puede calcular una aritmética más compleja, incluidas las inversas matriciales, las transformaciones de Fourier y las funciones de aproximación.

3) El lenguaje Matlab, que es un lenguaje de matricial de alto nivel con funciones, estructuras de datos y funciones de programación orientadas a objetos. Permite programar pequeñas aplicaciones, así como programas grandes y complejos.

4) El sistema de Matlab y sus gráficos, cuenta con amplias herramientas para visualizar gráficos y funciones. Contiene visualización bidimensional y tridimensional, procesamiento de imágenes, creación de interfaz gráfica de usuario e incluso animación.

5) Interfaces externas de Matlab. Esta librería permite escribir programas en C, C++ y Fortran, que se pueden leer y conectar con Matlab.

1.3.15. GUIDE (Graphical User Interface Development Enviroment)

Las GUI (también conocidas como interfaces gráficas de usuario o interfaces de usuario) permiten un control sencillo de las aplicaciones de software, lo cual elimina la necesidad de aprender un lenguaje y escribir comandos a fin de ejecutar una aplicación.

Las aplicaciones de MATLAB son programas autónomos que automatizan una tarea o un cálculo. Por lo general, la GUI incluye controles tales como menús, barras de herramientas, botones y controles deslizantes.

GUIDE almacena la interfaz en dos archivos:

- **Archivo .fig**: donde se encuentra la descripción de la parte gráfica completa
- **Archivo .m**: donde se puede encontrar el código que controla las acciones.

Las propiedades de cada objeto se guardan en el archivo .fig y se pueden configurar directamente desde la herramienta GUIDE, gracias al inspector de propiedades ya construido. Todas las acciones, generalmente llamadas "callbacks"[19] se pueden modificar y cambiar en el archivo .m. Cada componente tiene la propiedad "Tag"[20], la cual se utiliza al crear el nombre de la referencia callback.

1.3.16. Método Triple DES

DES (Data Encryption Standard o Estándar de Cifrado de Datos en español) fue desarrollado en la década de 1970 en IBM, basado en un diseño anterior de Horst Feistel.

En DES, tanto el tamaño del bloque como la longitud de la clave son de 64 bits cada uno. Se utilizan 8 bits para verificar la paridad, por lo que la longitud efectiva de la clave es de 56 bits.

Debido al tamaño pequeño de la clave, se identificó que era demasiado vulnerable a los ataques de fuerza bruta, por lo que en enero de 1999 DES fue públicamente rota en 22 horas 15 min. Por lo que se optó por una mejora en el cifrado de datos con la aparición del nuevo estándar Triple DES.

Triple DES fue desarrollado para abordar las obvias fallas en DES. Para lo cual, este método amplía el tamaño de la llave DES aplicando el algoritmo tres veces seguidas con tres llaves diferentes.

[19] Callback: función corta que debe obtener los datos necesarios para realizar su tarea.
[20] Tag: son etiquetas utilizadas dentro del ambiente GUIDE para determinar propiedades de un elemento.

El tamaño de la clave combinada es, por lo tanto, de 168 bits (3 veces 56), la cual va más allá del alcance de las técnicas de fuerza; donde no se ha descubierto fallas graves, y es utilizada en varios protocolos de internet. [27], [28]

En la figura se muestra diagrama de bloques del algoritmo Triple DES.

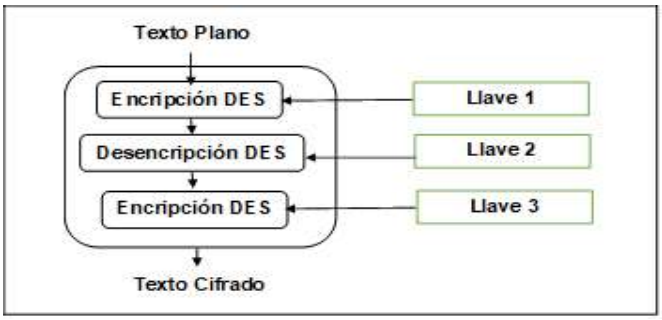


Figura 1.12 Algoritmo Triple DES.

CAPÍTULO 2

2. METODOLOGÍA

En este capítulo se presenta el diseño de la herramienta de uso didáctico esteganográfica a implementar. Donde se describen los módulos de la aplicación, requerimientos para el diseño, esquemas y desarrollo la interfaz GUI de la herramienta de uso didáctico. La cual será de utilidad para estudiantes de la carrera de Ingeniería en Electrónica y Redes de Información, que desean tener una base informativa sobre aplicaciones que se les puede dar a técnicas esteganográficas, creadas a partir de un lenguaje de programación interpretado MATLAB.

2.1. Diseño de la herramienta de uso didáctico esteganográfica

En esta sección se propone diseñar una herramienta de uso didáctico esteganográfica para el envío de texto oculto y cifrado en un archivo de audio MP3. Como pasos para conseguir este objetivo se describirán los módulos, requerimientos para el diseño, se realizarán esquemas de la interfaz y desarrollo la interfaz GUI.

2.1.1. Descripción de los módulos de la aplicación.

Debido a que no existe una herramienta de uso didáctico que permita verificar la utilidad de la técnica esteganográfica en archivos de audio MP3, se implementará dicha aplicación en una GUI de Matlab considerando los siguientes módulos.

1. **Módulo de Inicio:** El usuario de la herramienta en primer lugar deberá definir qué acción realizará para el proceso esteganográfico, ya sea ocultamiento u obtención del mensaje, debido que, este módulo contará con 2 botones permitiendo desplazarse a los diferentes módulos del proceso esteganográfico.

2. **Módulo de ocultamiento:** EL usuario deberá definir un archivo de audio de entrada con formato MP3, el cual servirá como cubierta del mensaje o archivo a ocultar.

   El usuario deberá definir si el mensaje a ocultar estará contenido en un archivo de texto (.txt) o si lo escribirá en el recuadro de texto que poseerá la

GUI, el programa le indicará al usuario si el tamaño de archivo podrá ser embebido en el audio seleccionado como cubierta.

En el programa el usuario podrá ingresar una clave de encriptación para cifrar el mensaje a enviar mediante la técnica 3DES, una vez realizados estos pasos secuencialmente el usuario podrá incrustar el mensaje dentro del archivo de audio; al finalizar la etapa de ocultamiento el programa le indicara al usuario de forma visual el audio final, el cual será almacenado en una carpeta de directorio para su previa reproducción, el usuario podrá utilizar la misma herramienta para reproducir tanto el archivo de audio original como el estego-audio.

3. **Módulo de obtención:** En este módulo de la herramienta se podrá realizar el proceso inverso para recuperar el mensaje, posteriormente luego de ser recuperado será almacenado en un archivo con el formato .txt.
   El módulo no permite la recuperación de audio, ya que la herramienta procurará que en el archivo no exista degradación, refiriéndose como degradación a saltos, distorsiones u otros aspectos que hagan notorio el cambio dentro del archivo MP3.

2.1.2. Requerimientos para el diseño de la aplicación, con los cuales se desarrollarán los módulos a implementarse.

En lo referente a la interfaz gráfica implementada, el programa está distribuido en interfaces que serán totalmente interactivas para el usuario. En total el programa se divide en tres ventanas principales de las cuales la ventana inicio invoca a otras 2 ventanas; en la ventana donde se lleva a cabo el proceso de ocultamiento los elementos de esta interfaz van apareciendo secuencialmente; según los requerimientos del proceso esteganográfico, similar en la ventana de obtención del mensaje.

Tomando en cuenta estas consideraciones, la herramienta debe cumplir con los siguientes requerimientos:

- Cargar el archivo de audio en el formato especifico de la aplicación (MP3) para los módulos ocultamiento y obtención del mensaje.
- Realizar el ocultamiento del mensaje, sea este ingresado mediante cuadro de texto de la herramienta o por un archivo en formato .txt cargado al presionar un botón.
- Dispondrá de un recuadro en donde el usuario ingresará la clave con la que se encriptará o desencriptará el mensaje correspondiente en cada módulo.
- Tendrá botones de reproducción para el audio original y el estego-audio.
- El estego-audio será guardado en una carpeta dentro del directorio del proyecto con formato ("Nombre_Audio_Original" +" _estego"), manteniendo la misma extensión; cabe mencionar que se realiza el cambio en el nombre del archivo solo para identificar el nuevo archivo creado.
- Al obtener el mensaje se lo podrá visualizarlo en un panel, donde posteriormente si se desea podrá guardase en un nuevo archivo con formato .txt.

Por lo que se ha considerado propicio definir cada una de las etapas del proceso esteganográfico, en varios archivos .m, evitando así una sobrecarga de código y pueda ser más comprensible al momento de corregir ciertos detalles del programa.

2.1.3. Esquema de la interfaz gráfica para la aplicación.

A continuación, se mencionará los archivos que componen la interfaz que componen la herramienta de uso didáctico

- CargarAudio.m
- CodificacionLSB.m
- ComparacionAudio.m
- DecodificacionLSB.m
- Decripcion3DES.m
- Deshabilitar.m
- Encripcion3DES.m

- HabilitaCodificacion.m
- HabilitaDecodificacion.m
- Inicio.m
- InsertarMensaje.m
- ObtenerMensaje.m
- TripleDES.m

Luego de haber descrito y analizado los requerimientos y componentes que serán parte de la herramienta, se puede realizar una vista general de los archivos principales que contendrá cada uno de los módulos como se muestra en la figura 2.1.

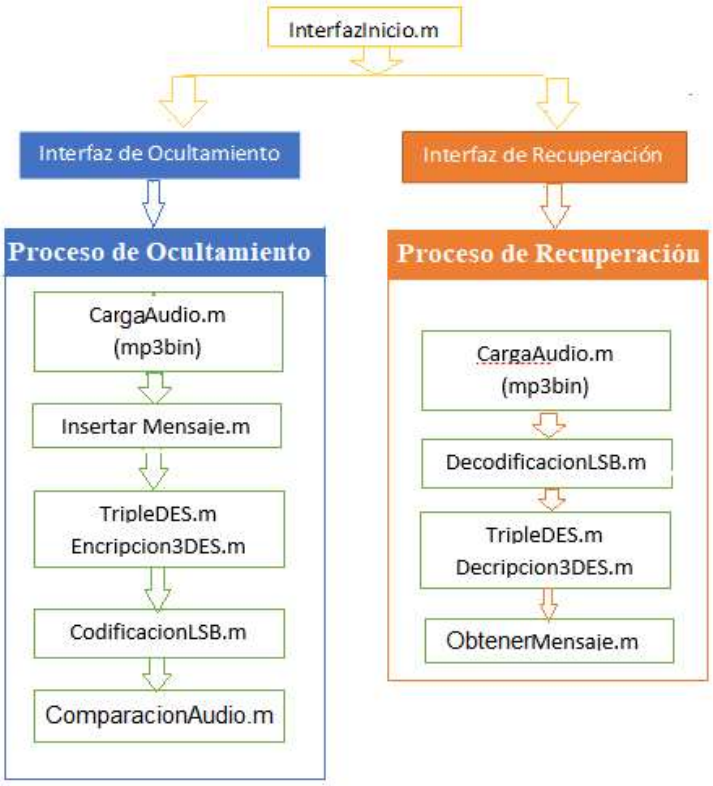


Figura 2.1 Esquema general de las funciones de la herramienta didáctica.

2.1.4. Diseño de las funciones que operan en la interfaz GUI.

En los siguientes aparatados se explica cómo opera cada una de las funciones mencionadas anteriormente.

2.1.4.1 Función InsertarMensaje.m

Esta función contiene el código con el que se programan todos los elementos que contiene el archivo InsertarMensaje,fig, el cual será utilizado como módulo de ocultamiento de mensaje esteganográfico.

Dentro de la función se han programado las siguientes tareas:

- Almacenar la información y ruta del archivo de audio que servirá como cubierta.
- Almacenar la ruta del archivo de texto que contiene la información oculta.
- Almacenar el mensaje ingresado por el usuario si este selecciono este tipo de entrada.
- Almacenar el nombre del estego-audio.
- Almacenar la clave ingresada por el usuario para poder encriptar el mensaje previo a su incrustación en el audio original.

2.1.4.2 Función CargarAudio.m

Esta función permite realizar el proceso de carga de audio, permitiendo obtener toda la información de este mediante la dll[21] Lame, la cual será utilizada en todo el proceso esteganográfico.

Como primer paso la función realiza la carga del archivo de audio mediante un cuadro de dialogo, donde el usuario seleccionará el archivo con formato específico, de no ser el caso, se enviarán banderas para mostrar cuadros de error en el proceso de selección; si se ha realizado correctamente el proceso de carga continua con una función interna la cual está ligada a Lame, utilizando binarios externos dentro de su respectivo proceso, permitiendo obtener la información total tanto de la cabecera como del tag ID3v2 que se encuentran en el audio MP3.

[21] Dll: es una librería la cual contiene código e información las cuales pueden ser utilizadas por varios programas al mismo tiempo.

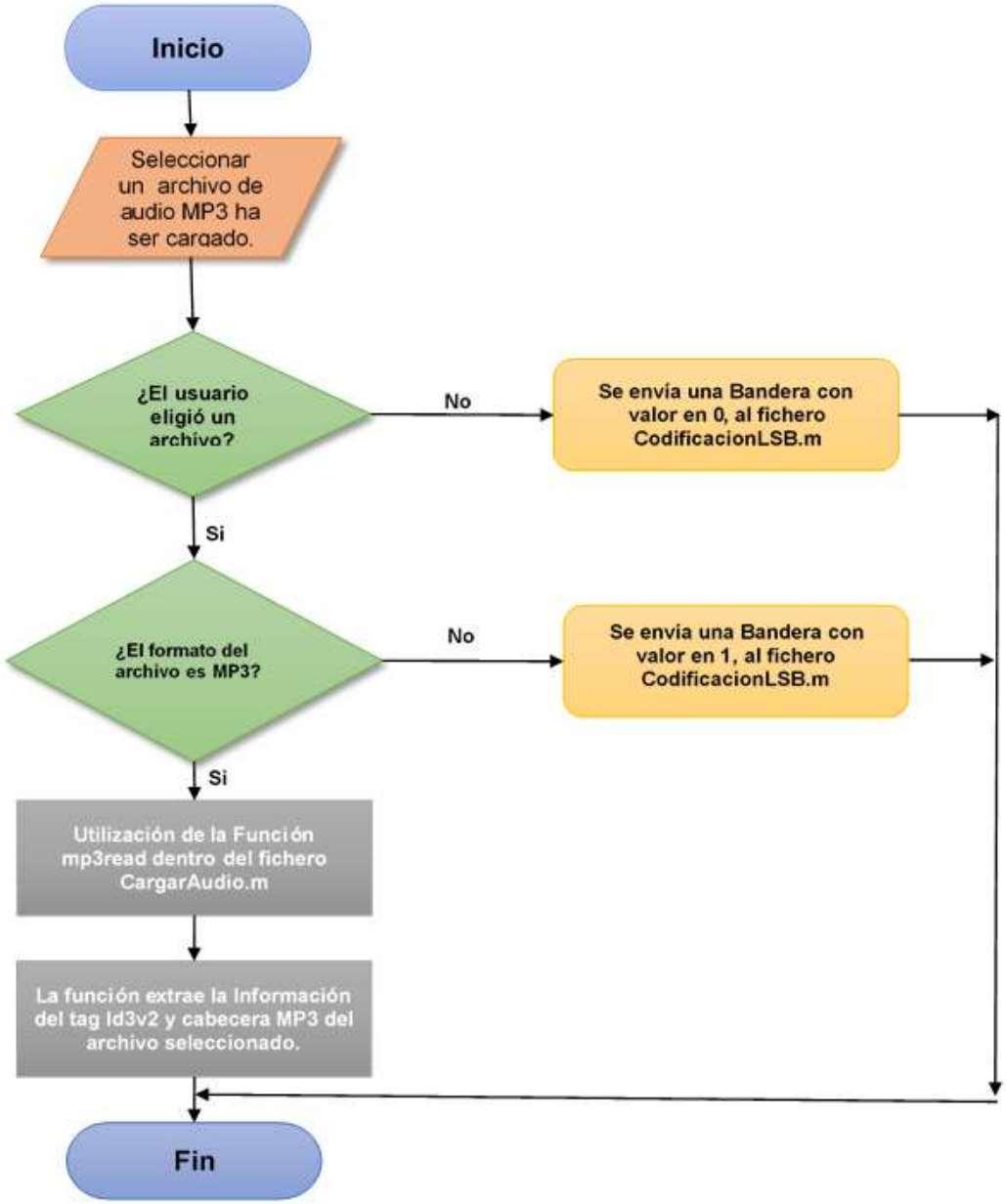


Figura 2.2 Diagrama de flujo para carga de audio, lectura de cabecera y tag Id3.

2.1.4.3 Función Encripcion3DES.m

La función Encripcion3DES.m recibe como parámetros de entrada las matrices de permutación inicial, pre-salida. selección de bit E, función permutación; texto y clave ingresados por el usuario.

Cabe mencionar que las tablas recomendadas para el proceso de encriptación dadas por la Federal Information Processing Standards en la publicación 46-3 el 25 de octubre de 1999 son las siguientes:

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Tabla 2.1 Tabla de Permutación Inicial

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Tabla 2.2 Tabla de Pre-Salida

Sea E una función que toma un bloque de 32 bits como entrada y produce un bloque de 48 bits como salida. Estos serán sobrescritos como 8 bloques de 6 bits cada uno, que se obtendrán seleccionando los bits en sus entradas en orden de acuerdo con la siguiente tabla:

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Tabla 2.3 Tabla Selección de Bit E

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Tabla 2.4 Tabla Función Permutación

Cabe indicar que las tablas que conllevan a las primitivas usadas por la técnica de encriptación Triple DES se las obtiene de las tablas antes mencionadas, por lo que cada función de selección S_1, S_2,..., S_8, toman un bloque de 6-bits como entrada y genera un bloque de 4-bits como salida, utilizando una tabla que contiene el S_1 recomendado por el estándar el cual se ilustra en la Tabla 2.5.

Fila No.	Número de Columna															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Tabla 2.5 Función primitiva S_1

Las cuales junto con la tabla función de permutación; generarán cada una de las funciones permutadas, las que ayudarán al cálculo de las diferentes llaves ilustrado en la Figura 2.3.

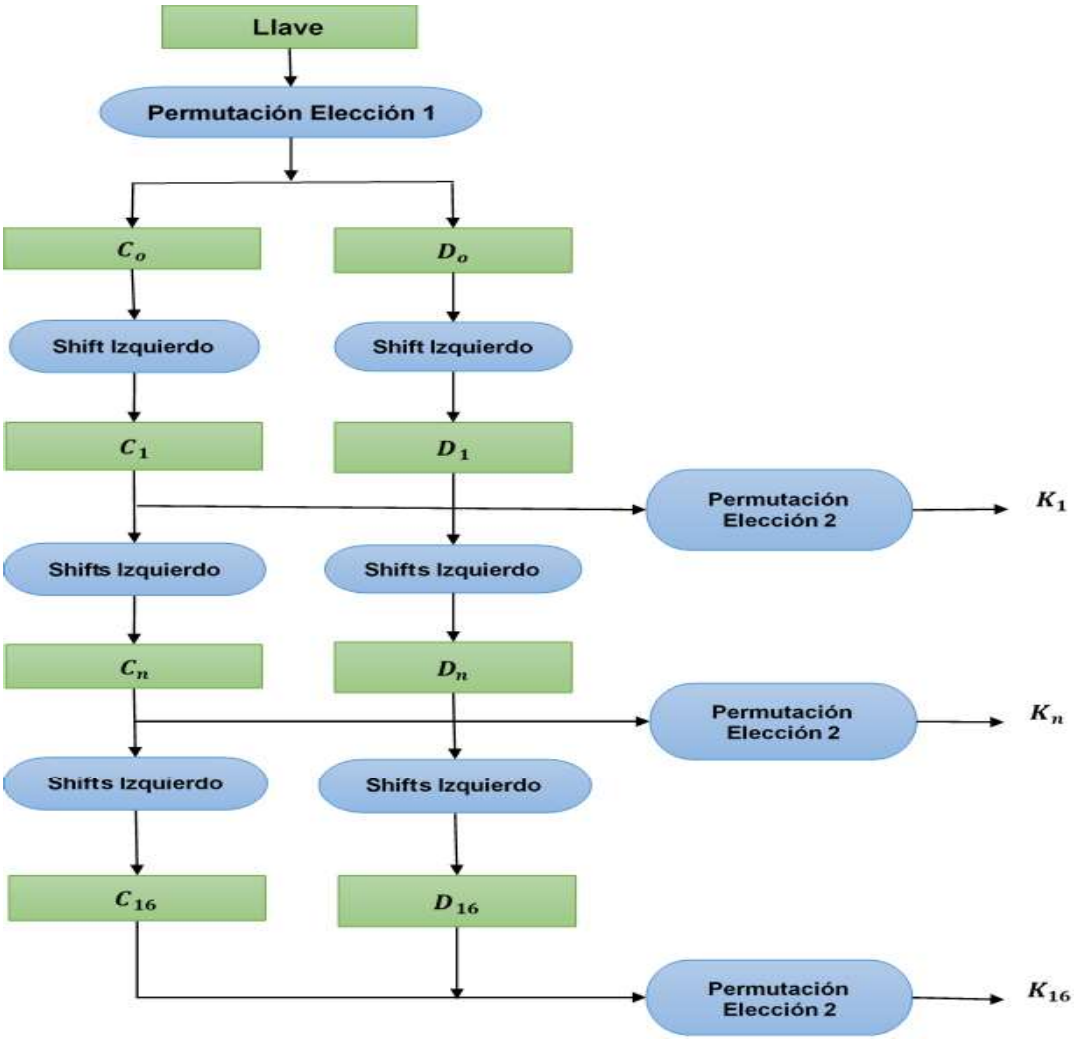


Figura 2.3 Calculo programado de las llaves [16]

2.1.4.4 Función CodificacionLSB.m

Esta función se encarga de realizar todo el proceso de ocultamiento de la información previamente encriptada y descrita en la sección 2.1.4.3.

Recibe como parámetros de entrada, la ruta completa del archivo de audio MP3 cargado, el cual será utilizado como cubierta, el texto del mensaje ya sea que el

usuario haya ingresado manualmente o cargado mediante el botón de la interfaz, la clave utilizada en el proceso de encriptación, el nombre de salida que tendrá el estego-audio.

Como primer paso se verifica si existe el directorio donde se guardará el estego-audio, luego se tomará la ruta del archivo de audio original el cual mediante la función fileread se procederá a descomponer en cabecera, tagid3, tamaño y cubierta; los cuales estarán codificados en unit8[22], uint32[23] y uint8 respectivamente.

- **Cabecera:** se toma en cuenta los valores de lectura para el archivo de audio en 4 Bytes, que corresponde a la cabecera del formato de audio descritos en la sección 1.3.10, en formato de codificación uint8.
- **TagID3:** asigna la lectura del archivo de audio en 128 Bytes, que corresponde a la estructura de este, en formato de codificación uint8.
- **Tamaño**: el cual servirá para indicar el tamaño de nuestro estego-audio, ya que se desea mantener el mismo tamaño al original, logrando que sea imperceptible la modificación de un archivo de audio; se codifica en uint32 propios de MPEG Audio Layer-3.
- **Cubierta:** esta variable nos servirá para incluir los bits del mensaje encriptado, teniendo en cuanta que devolverá una estructura con valores 0_L y 1_L, codificándolo en uint8 y así facilitar el proceso de incrustación del mensaje.

Teniendo los parámetros texto y clave se hace el llamado de la función TripleDES descritas anteriormente, luego se procede a concatenar una sola matriz de dimensiones mxn por cada uno de los caracteres del mensaje. Posteriormente se realiza conversiones en la matriz para colocarla en formato double con dimensión 1x[mxn].

Luego, de acuerdo con el parámetro clave, se creará una variable control que extraerá el módulo de los caracteres totales codificados en binario; cabe indicar que

[22] Uint8: se almacenan como enteros sin signo de 1 byte (8 bits).
[23] Uint32: se almacenan como enteros sin signo de 4 bytes (32 bits).

esta variable tiene 8 bits que serán incrustado en los primeros 8 bits de la variable cubierta.

Como siguiente punto en el proceso de embebido en los siguientes 17 bits de la cubierta se indicará el tamaño mensaje, obtenidos previamente de la matriz en la función encriptación, además se coloca los bits del mensaje en los subsiguientes bits de la cubierta hasta completarlos con los del mensaje.

Una vez hecho el proceso se procede a grabar el audio MP3 haciendo uso de la función Filewrite, la cual escribe la información en formato binario, siguiendo los pasos de lectura [cabecera, tagID3, tamaño, cubierta] permitiendo la creación del estego-audio.

Como último paso esta función activa el botón comparación el cual presenta, en una nueva ventana, la comparación visual en espectrograma de los dos archivos de audio (original y estego-audio), permitiendo en este caso identificar la diferencia y modificación de ambos archivos.

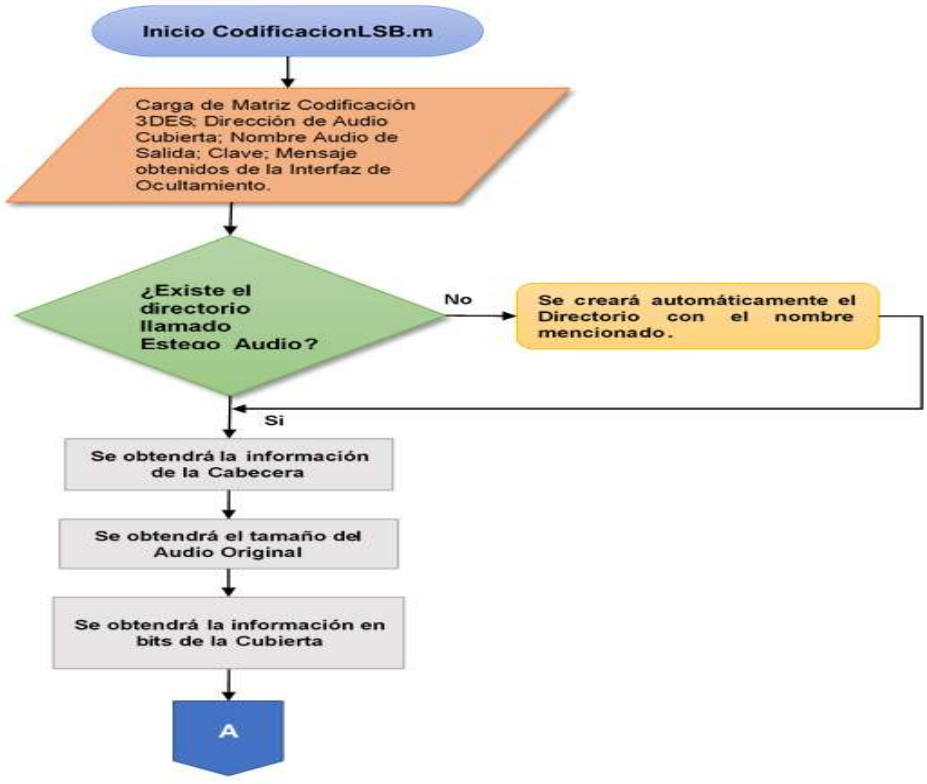


Figura 2.4 Diagrama de flujo de la función CodificacionLSB.m que permite ocultar información (1 de 2).

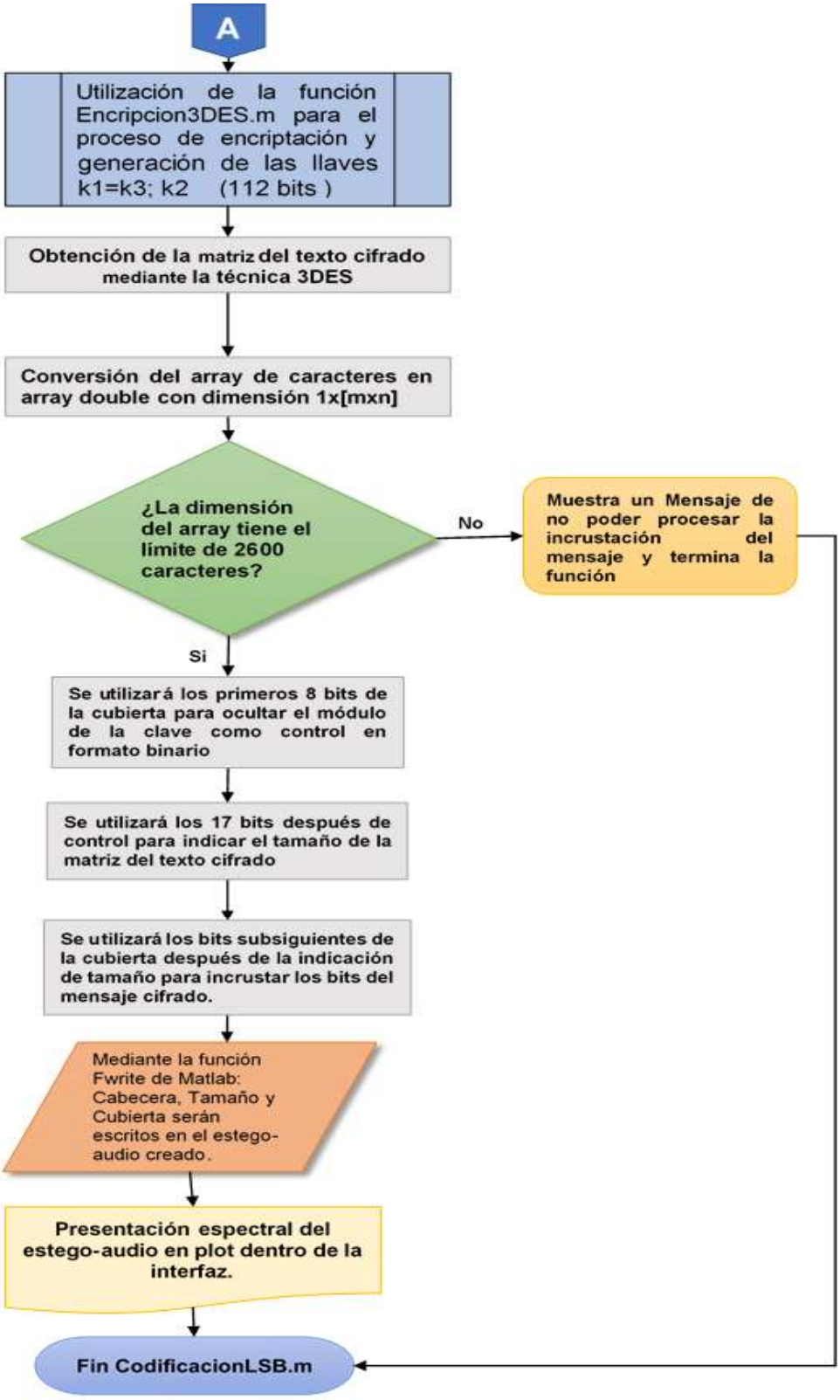


Figura 2.1.4 Diagrama de flujo de la función CodificacionLSB.m que permite ocultar información (2 de 2).

2.1.4.5 Función ComparacionAudio.m

Esta función permite la invocación de un GUIDE para la visualización de los espectros de frecuencia, el cual recibe como parámetros de entrada las rutas de los archivos de audio almacenadas en la función CodificacionLSB.m.

Como primer paso, esta función descompone los archivos de audio-original y estego-audio, de los cuales se obtendrán las componentes de frecuencia y datos correspondientes a cada uno.

Con los datos obtenidos de cada audio, se visualizarán sus espectros y así el usuario podrá notar de forma visual la modificación del estego-audio con el audio original.

Luego con las componentes de frecuencia, mediante la FFT[24] se calcula la potencia de cada señal. Donde la transformada rápida de Fourier puede ser utilizada en varios tipos de procesamiento de señales.

La FFT es de utilidad para leer señales como ondas de sonido o para cualquier tecnología de procesamiento de imágenes. Esta nos permite resolver varios tipos de ecuaciones, o mostrar varios tipos de actividad de frecuencia de manera útil.

Teniendo presente la utilidad de la FFT se representarán en un plot[25] las potencias, logrando mostrar la variación que se produce en el estego-audio, durante el proceso de incrustación de la información.

2.1.4.6 Función DecodificacionLSB.m

Esta función se encarga de recuperar el mensaje oculto mediante el proceso de incrustación, al utilizar el módulo de Ocultamiento previamente descrito.

---

[24] FFT (Fast Fourier Transform): es un algoritmo que reduce el tiempo de cálculo de $n2$ pasos a $n \cdot \log_2(n)$

[25] Plot: **crea** un gráfico de líneas 2D de los datos de Y frente a los valores correspondientes de X dentro de un ambiente GUIDE

Como parámetros de entrada recibe los valores de la dirección del archivo de audio MP3 (estego-audio), y la clave ingresada por el usuario.

Como primer paso, mediante la función Fileread se procederá a descomponer el audio MP3(estego-audio) en cabecera, tagID3, tamaño y cubierta; para posteriormente tomar la cubierta y extraer mediante la función bitget, propia de Matlab, los bits incrustados en el proceso de ocultamiento, indicando la posición correcta para extraer la variable control.

Como siguiente paso, realiza el cálculo de la semilla que identificará si cumple el control con la clave ingresada por el usuario, transformado cada carácter a un valor decimal y transformándolo a binario, para extraer su módulo respectivo y después compararlo con la variable de control extraído previamente.

Una vez constatado que cumple la condición de control se procede a seguir con la extracción de los bits dentro de la variable cubierta, teniendo en cuenta que se debe extraer la longitud del mensaje y el mensaje en sí; para luego armar una matriz tomando cada 8 bits de la extracción e interpretarla en formato decimal.

Una vez estructurada la matriz, se hace el llamado a la función DecripcionDES.m, la cual devuelve el texto desencriptado, para enviarlo como parámetro de salida en un vector que contiene el mensaje recuperado.

Se puede decir que la función es de suma relevancia dentro del proceso de recuperación del mensaje, porque al instante en que un bit recuperado cambie su valor, la información recuperada será inconsistente y presentará partes erróneas.

En la Figura 2.6 se presenta el diagrama de flujo con el que constan todos los pasos descritos que realiza esta función.

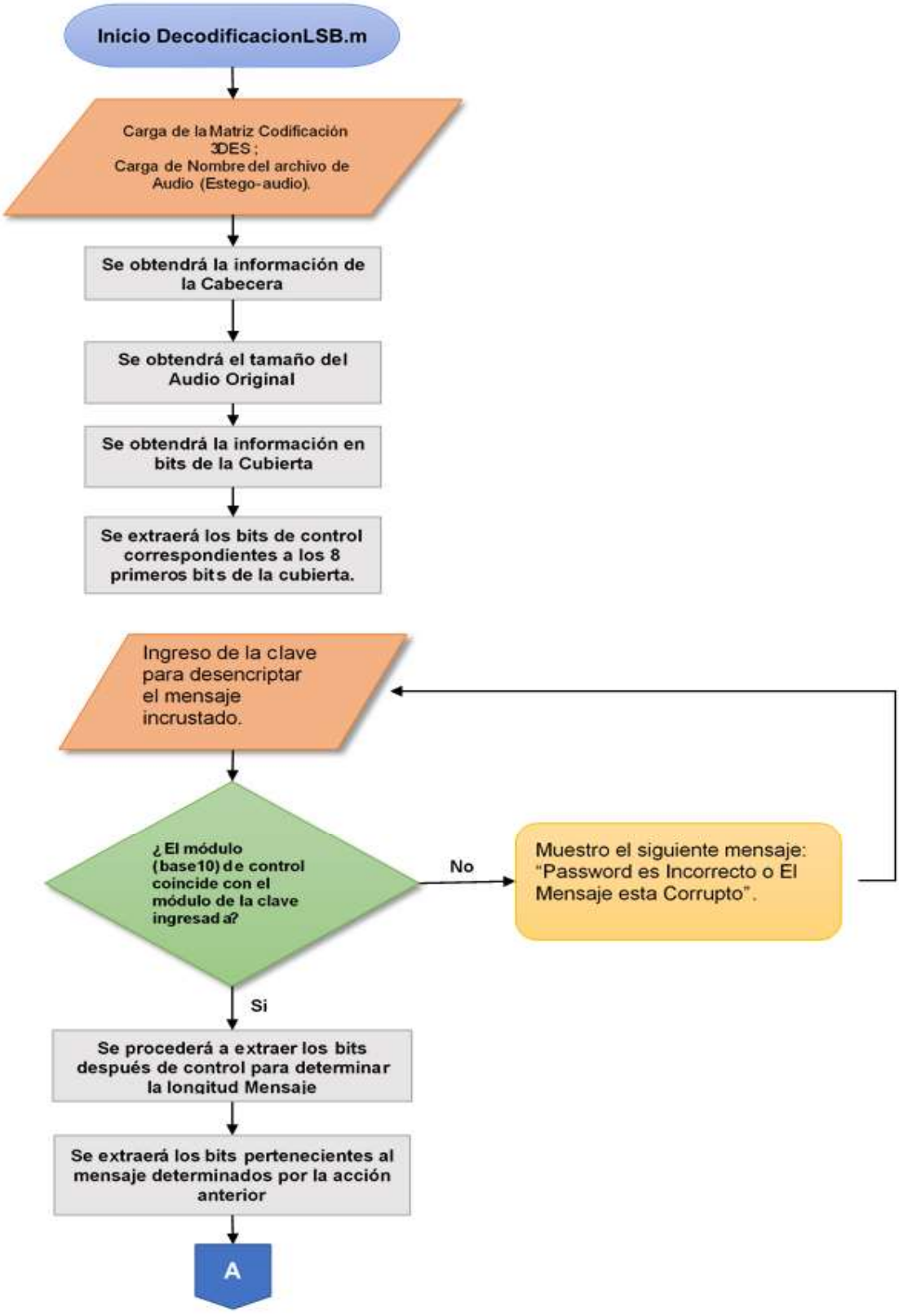


Figura 2.5 Diagrama de flujo de la función DecodificacionLSB.m que permite ocultar información (1 de 2).

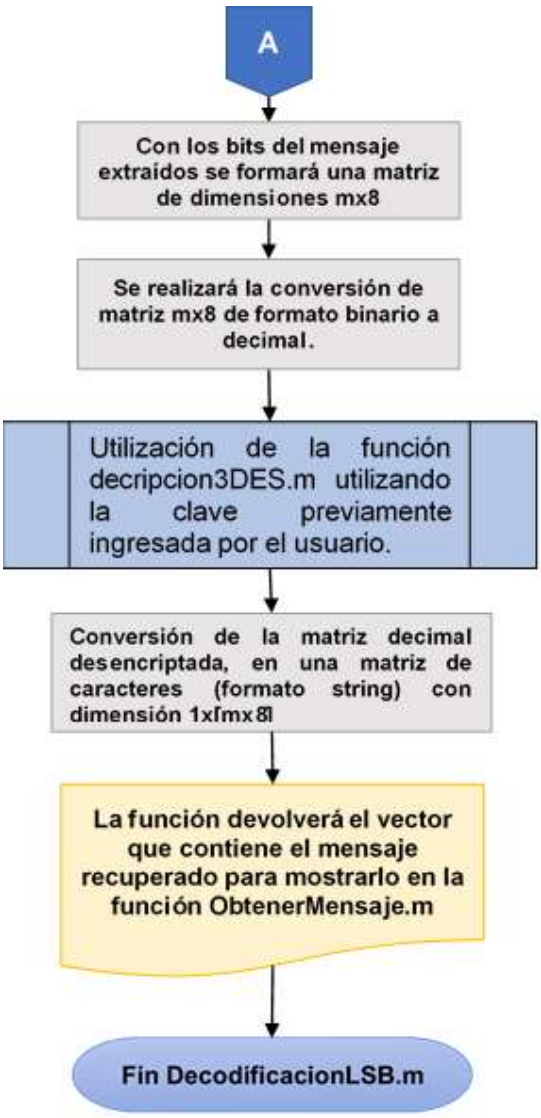


Figura 2.1.5 Diagrama de flujo de la función DecodificacionLSB.m que permite ocultar información (2 de 2).

2.1.4.7 Función Decripcion3DES.m

Esta función permite realizar el proceso de desencriptación de la matriz que contiene el mensaje oculto, para esto se recibe como parámetros de entrada la matriz y además la clave con la que fue encriptado el mensaje.

Como primer paso, esta función determina la longitud de la matriz de entrada; debe existir relación en la dimensión, ya que cada carácter es interpretado por un valor binario de 8 bits.

Luego de reestructurar la matriz inicial se procede a realizar el paso por cada una de las llaves que fueron generadas en el proceso de encriptación descritas en la sección 2.2.3.

Como parámetro de salida esta función devuelve un vector con los valores de los caracteres desencriptados, los cuales serán utilizados por la función DecodificacionLSB.m.

Figura 2.6 Diagrama de bloques del procedo de Desencriptación TripleDES. [16]

2.2 Implementación de las funciones que operan cada módulo de la interfaz GUI.

2.2.1. Implementación del Módulo Ocultamiento

Para la implementación de este módulo, las funciones fueron creadas en Matlab R2018a, correspondientes a cada etapa del proceso esteganográfico las cuales fueron detalladas en la sección 2.1.4.

a. Función CargarAudio.m

El segmento de Código 2.1 muestra el proceso de carga de audio, los cuales corresponden a la obtención de la ruta y lectura del archivo seleccionado por el usuario.

```
function file = CargarAudio()
message = 'Seleccione el Archivo de Audio.';
type = '*.mp3;';
[FileName,PathName] = uigetfile({[type]}, message);
if (FileName==0)
    file=0;
else
    [file.path,file.name,file.ext] = fileparts([PathName FileName]);
    if isequal((file.ext),['.mp3'])

    if ~isempty(strfind(type, file.ext))
        [file.data,file.fs,file.bitrate] = mp3read([PathName FileName]);
```

Código 2.1 Creación de la Función CargarAudio.

b. Función CodificacionLSB.m

En los siguientes segmentos de código se muestra el algoritmo de incrustación de los bits mediante la técnica LSB, se trata de la descomposición del archivo de entrada mp3in como se indicó en la sección 2.1.4.4.

```
function CodificacionLSB(mp3in, mp3out, texto, clav
%tecnicas LSB para ocultamiento en MP3%...%

if ~exist('Estego_Audio/')
    mkdir('Estego_Audio');
end

fid = fopen(mp3in,'r');
header = fread(fid,4,'uint8');
dsize  = fread(fid,1,'uint32');
[cubierta,len_cover] = fread(fid,inf,'uint8');
fclose(fid);
```

Código 2.2 Descomposición del archivo de audio MP3

Luego se hace la invocación a la función Encripcion3DES.m, con la que se realizará el proceso de encriptación del texto y clave como argumentos de entrada; para obtener las matrices en el proceso de incrustación.

```
bin   = Encripcion3DES(texto,clave)';
[m,n] = size(bin);
```

Código 2.3 Invocación de la función de Encriptación 3DES

También se puede observar, que se utiliza la función propia de Matlab llamada bitset la cual nos permite incrustar un bit en la posición indicada, para posteriormente incrustar el mensaje total dentro de la variable cubierta.

```
control = de2bi(mod(sum(double(clave)),256),8)';
disp(control);
cubierta(1:8) = bitset(cubierta(1:8),2,control(1:8));
cubierta(9:25) =bitset(cubierta(9:25),3,M(1:17));
t0=25+1;
t1=(len_msg+(t0-1));
for i=t0:t1
    e=bitset(cubierta(t0:t1),2,binx(1:len_msg)');
end
cubierta(t0:t1)=e;
```

Código 2.4 Función bitset para incrustación de bits

Y finalmente se utiliza la función de escritura binaria propia de Matlab, con la que se creará el estego-audio en el directorio indicado.

```
out=fopen(['Estego_Audio/' mp3out],'w');
fwrite(out,header,'uint8');
fwrite(out,dsize,'uint32');
fwrite(out,cubierta,'uint8');
fclose(out);
```

Código 2.5 Función Filewrite para escritura del estego-audio

c. Función Encripcion3DES.m

En los segmentos a continuación se detalla los parámetros de entrada, tratamiento de los datos y utilización de funciones que permiten realizar el proceso de encriptación del mensaje mediante la técnica 3DES.

```
function encrypt = Encripcion3DES(texto,clave)

global    iprt

dato = texto;
dato = double(uint8(dato))';
dato_length = length(dato);
adds = 8-mod(dato_length,8);
if adds ~= 0
    for i = 1:adds
        dato(dato_length+i) = 0;
    end
    dato_length = dato_length+adds;
end
```

Código 2.6 Parámetros de entrada y descomposición de datos para encriptación

Para la generación de llaves se realiza el método descrito en la sección 2.1.4.3, del cual se utilizan las matrices predefinidas por la FIPS[26] en la publicación 46-3, y en el Código 2.8 se establece el método de utilización de llaves K1=K3, K2.

```
function ki=gerkey(k)
mt = ...
    [1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16;
     1 1 2 2 2 2 2 2 1  2  2  2  2  2  2  1];
rt = ...
    [14 17 11 24  1  5  3 28 ...
     15  6 21 10 23 19 12  4 ...
     26  8 16  7 27 20 13  2 ...
     41 52 31 37 47 55 30 40 ...
     51 45 33 48 44 49 39 56 ...
     34 53 46 42 50 36 29 32];
kl = k(1:28);
kr = k(29:56);
k3 =  k(1:28);
for i = mt(1,1):mt(1,16)
    kl = mr(kl,mt(2,i));
    kr = mr(kr,mt(2,i));
    k3 = mr(k3,mt(2,i));
    k = [kl kr k3];
    for j = 1:48
        ki(i,j) = k(fix(rt(j)));
    end
end
```

[26] FIPS: FEDERAL INFORMATION PROCESSING STANDARDS descrito para el estándar TripleDES

Código 2.7 Generación de llaves método de encriptación 3DES

```
function nk = mr(k,n)

l = length(k);
k1 = k(n+1:l);
k2 = k(1:n);
k3 = k(n+1:l);
nk = [k1 k2 k3];
```

Código 2.8 Asignación de criterio de llaves para encriptación 3DES

2.2.2. Implementación del Módulo de Obtención

Para la implementación de este módulo, las funciones fueron creadas en base a la fase de ocultamiento teniendo en cuenta que son procesos similares, pero deben ser interpretados de diferente manera; no se detalla la función CargaAudio ya que es la misma utilizada en el proceso de ocultamiento.

a. Función DecodificacionLSB.m

El código a continuación muestra los parámetros de entrada, tales como el nombre del archivo de audio modificado(estego-audio) y la clave ingresada por el usuario; la función *bitget* permite extraer los bits indicados de la posición en la que fueron ocultos para así determinar la variable *control* como se muestra en el Código 2.9.

```
function out = DecodificacionLSB( mp3in, clave )


control = bitget(stego(1:8),2)';
disp(control);
```

Código 2.9 Extracción de bits incrustados en el estego-audio mediante la función bitget de Matlab

En el segmento de Código 2.10, se indica la forma en que se establece la matriz de dimensiones [mx8] de formato binario, la cual será reestructurada mediante el comando reshape y convertirla en decimal para ser almacenado en un array, el cual será enviado como parámetro de entrada en la función Decripcion3DES; el resultado devuelto por la función mencionada será convertido en caracteres, para enviarlo como parámetro de salida de la función.

```
    bin = reshape(dat',8,len/8);

    data_dencrypt=bi2de(bin','left-msb');
    stegodata=Decripcion3DES(clave,data_dencrypt);
    out = char((stegodata));
```

Código 2.10 Reestructuración de los bits extraídos del estego-audio

b. Función Decripcion3DES.m

En los segmentos a continuación se detalla el proceso de desencriptación de cada uno de los caracteres, teniendo en cuenta que se debe cargar las matrices descritas en la sección 1.3.16, con las que se recorrerán lazos para realizar las respectivas fases de la técnica TripleDES.

```
pwb = str2bin(keyuse,7,2);
pwb = rebit(pwb,iprt);
ki = gerkey(pwb);
ki=flipud(ki);

veces = (dato_length-mod(dato_length,8))/8;
for i = 0:veces-1
    for j = 1:8
        tempdata(j) = dato(8*i+j);
    end
```

Código 2.11 Proceso de desencriptación y manejo de las llaves

c. Función ObtenerMensaje.m

En el Código a continuación se detalla la utilización del botón GuardarMensaje, donde se indica la utilidad de las funciones propias de Matlab, las cuales nos

permiten la escritura del mensaje obtenido en un archivo de texto con extensión .txt.

```
if ~exist('Obtencion_de_Mensajes/')
    mkdir('Obtencion_de_Mensajes');
end
texto=char(get(handles.txtMensajeDeco,'String'));
filter = {'*.txt'};
[file, path] = uiputfile(filter,'Guardar Texto',['mensaje_' estegoAudio.name]);
nombre=[path file];
if(ischar(nombre))
    fid = fopen(nombre,'wt');
    t = cellstr(texto);
    fprintf(fid,'%s\n', t{:});
    fclose(fid);
end
```

Código 2.12 Guardado de mensaje en un archivo de texto

CAPÍTULO 3

3. RESULTADOS Y DISCUSIÓN

En este capítulo se relata acerca de las pruebas realizadas a la herramienta y se presentan los resultados obtenidos. Se realizaron pruebas a los diferentes módulos tales como ocultamiento y obtención, así como pruebas de carga y reproducción de cada audio, codificación y decodificación del mensaje mediante el método de encriptación escogido, además se verifica que la herramienta cumpla con el alcance del proyecto.

3.1. Pruebas de selección de Archivo.

Para realizar las pruebas de selección de archivo, se dividió el trabajo en dos partes, en la primera parte se hizo pruebas de selección del archivo de audio en formato especifico MP3, y en la segunda parte del trabajo, se hizo pruebas de control para la elección de archivos que no corresponden al formato determinado.

3.1.1. Pruebas selección de archivo en formato MP3.

Tomando en cuenta los parámetros de diseño, dentro de la herramienta se espera que por defecto la ventana de selección de archivos permita la elección del formato MP3. Una vez que se ha seleccionado el archivo con el formato correcto se espera la información correspondiente como:

- Ruta especifica del Archivo.
- Nombre del Archivo.
- Frecuencia de Muestreo.
- Tasa promedio de bits (bitrate).

En la Tabla 3.1 se muestran la información detallada de cada uno de los archivos cargados.

Tabla 3.1 Características de los archivos cargados

Nombre	Ruta	Frecuencia de Muestreo	Bitrate (Kbps)
evanescense - october	C:\Users\hp\Music\Audios\evanescense - october	44100	192
06-Africa Unite	C:\Users\hp\Music\Audios\Probado_OK \06-Africa Unite	44100	192
Major Lazer & DJ Snake Ft. MØ, J Balvin & Farruko - Lean On (Official Remix)	C:\Users\hp\Music\Audios\Probado_OK\ Major Lazer & DJ Snake Ft. MØ, J Balvin & Farruko - Lean On (Official Remix)	44100	128
SKA P 2000 Planeta Eskoria	C:\Users\hp\Music\Audios\ SKA P 2000 Planeta Eskoria	44100	128
let-it-go	C:\Users\hp\Music\Audios\ let-it-go	22050	96

Como se observa en la Tabla 3.1, las características de los archivos cargados mediante la herramienta de uso didáctico son constatadas ingresando a la ruta especifica en la que se encuentra cada uno de los archivos de audio.

3.1.2. Pruebas control para elección de archivos de distinto formato.

Las pruebas de elección de archivos de distinto formato, consisten en primer lugar, en verificar si el usuario decide escoger un formato distinto al determinado, seguido, al escoger un formato diferente envía una bandera para indicar que no es el formato indicado, y finalmente, muestra un mensaje al usuario indicando que no es el aceptado para trabajar con la herramienta, cabe mencionar que al mostrarse la ventana de selección; los tipos de archivos permitidos son:

- *.mp3.
- Todos los archivos.

En la Figura 3.1. se muestra una captura del mensaje informativo, seleccionando un archivo de video con formato mp4, el cual nos permite realizar la prueba y obtener el objetivo deseado.

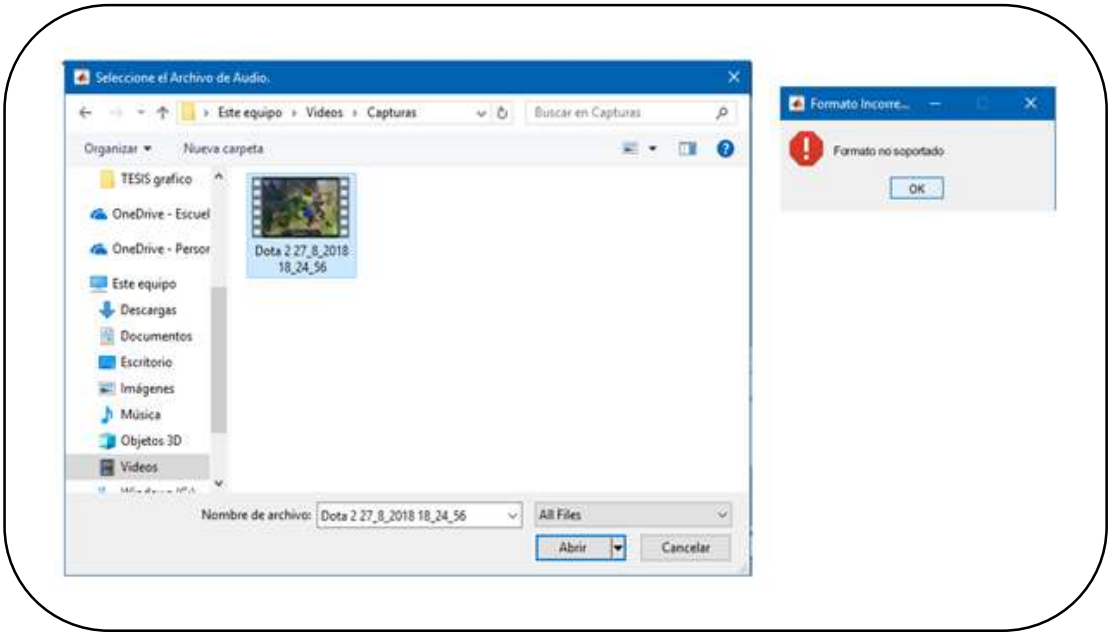


Figura 3.1 Control de selección de archivo con formato diferente a MP3

3.2. Pruebas de inserción de mensaje

Las pruebas de inserción de mensajes están enfocadas a verificar que no exista modificación alguna en el estego-audio, sea esta en tiempo de reproducción, frecuencia de muestreo y parámetros de copyright propios del archivo de audio original.

Verificar el tamaño máximo de caracteres que soporta la portadora, es decir, que el estego-audio no sufra ninguna modificación, mediante las opciones de ingreso de texto y selección de un archivo de texto con formato .txt, cada prueba será realizada independientemente y los resultados serán mostrados con capturas de pantallas.

3.2.1. Pruebas de inserción de mensaje mediante ingreso de texto

El objetivo de esta prueba es comprobar que los estego-audios creados no sufran ninguna modificación. Para la inserción del mensaje se utiliza la opción de ingresar texto, detallando a continuación el tamaño del texto para 3 diferentes audios:

a) Texto de 105 caracteres en formato ASCII

En la Figura 3.2 se muestra el mensaje ingresado por el usuario, además de la clave la cual será necesaria para encriptar el mensaje que se desea ocultar.

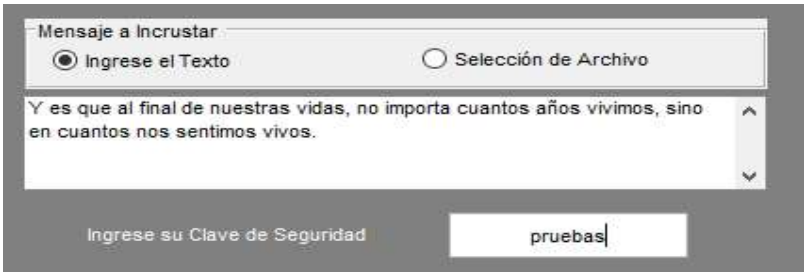


Figura 3.2 Ingreso de mensaje por el usuario en el recuadro de texto.

La Figura 3.3 muestra la comparación en detalles del audio original y estego-audio, tomadas de la vista de navegación dentro del ambiente Windows, cabe mencionar que se añade la palabra estego al nombre del archivo para identificarlo del audio original.

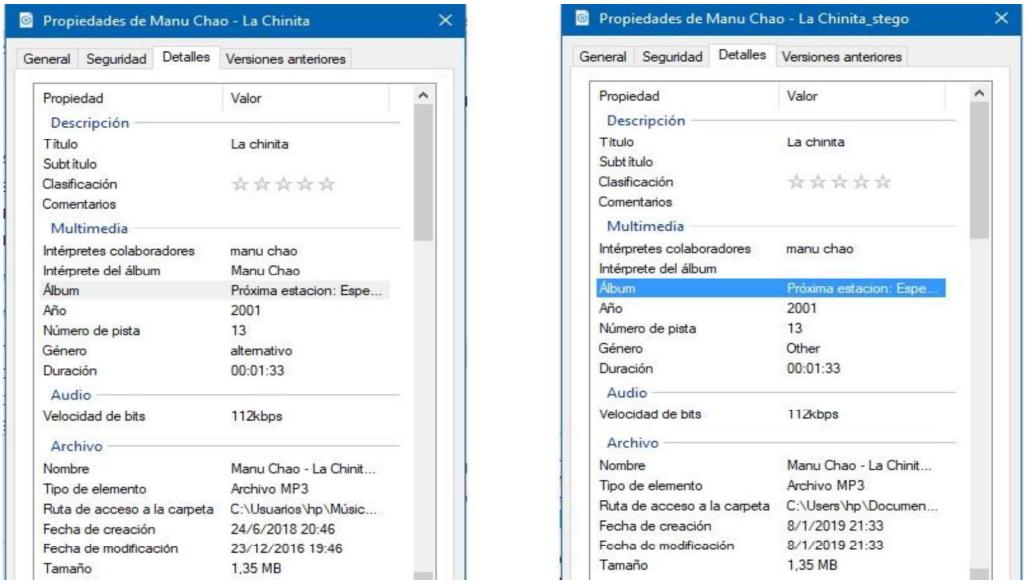


Figura 3.3 Comparación de características entre audio original y estego

b) Texto de 1184 caracteres en formato ASCII

En la Figura 3.4 se muestra el mensaje ingresado por el usuario, además de la clave la cual será necesaria para encriptar el mensaje que se desea ocultar.

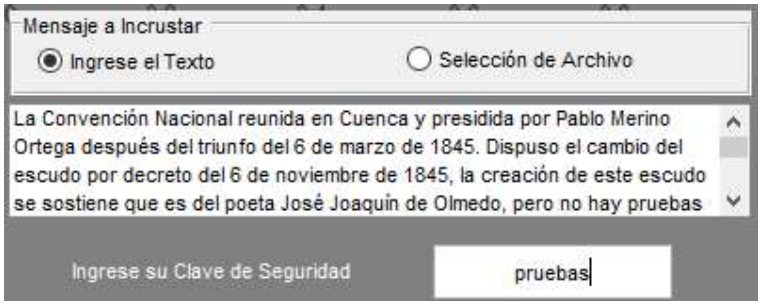


Figura 3.4 Ingreso de mensaje de 1184 caracteres por el usuario en el recuadro de texto

En la Figura 3.5 se puede observar la comparación en detalles del audio original y estego-audio, tomadas de la vista de navegación dentro del ambiente Windows.

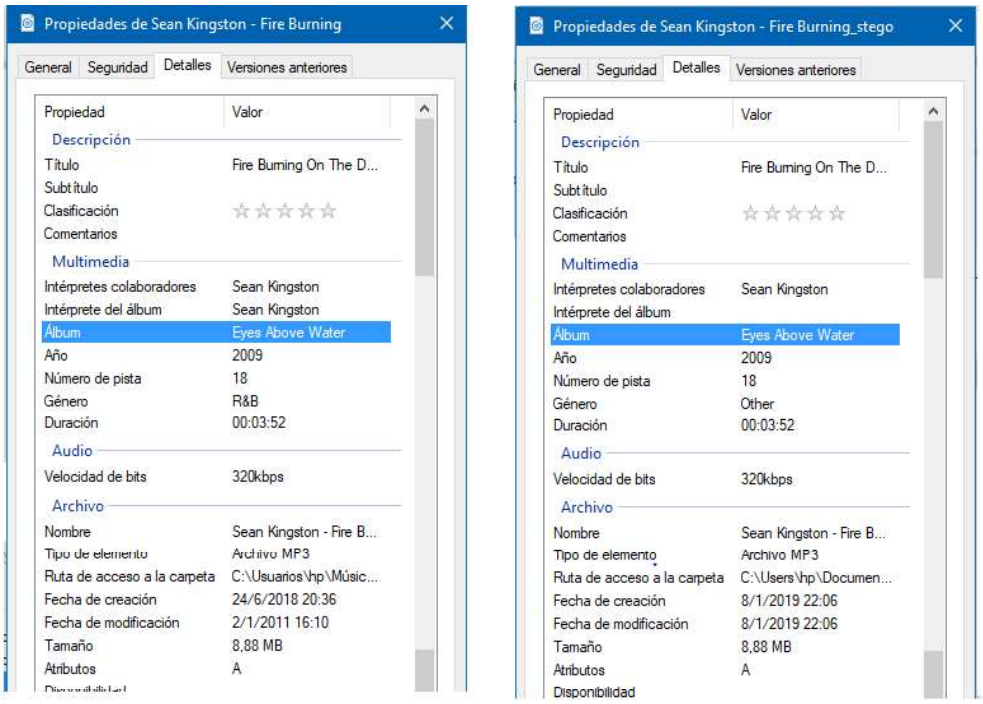


Figura 3.5 Comparación de características entre audio original y estego-audio para 1184 caracteres incrustados.

c) Texto de 1709 caracteres en formato ASCII

En la Figura 3.6 se muestra el mensaje ingresado por el usuario, además de la clave la cual será necesaria para encriptar el mensaje que se desea ocultar.

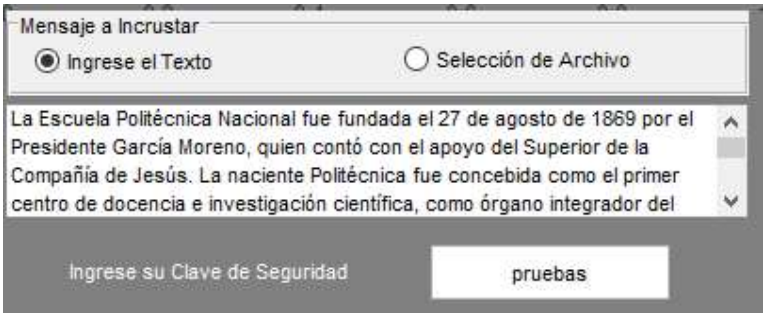


Figura 3.6 Ingreso de mensaje de 1709 caracteres por el usuario en el recuadro de texto

En la Figura 3.7 se muestra la comparación en detalles del audio original y estego-audio, tomadas de la vista de navegación dentro del ambiente Windows.

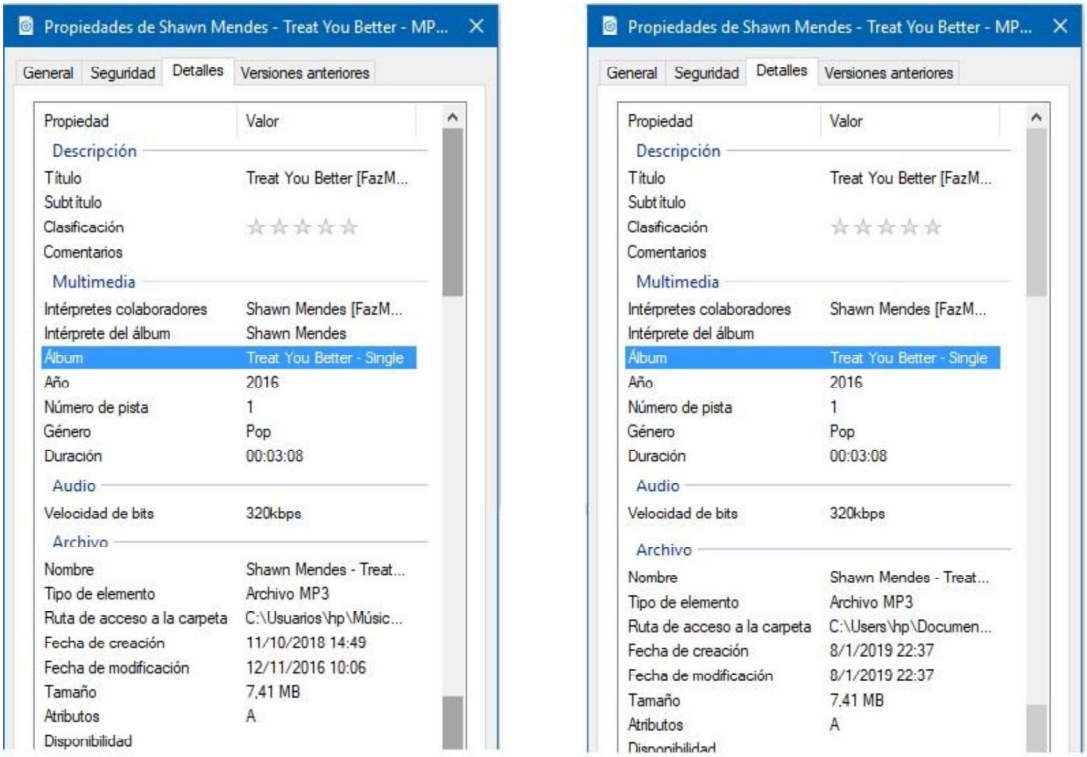


Figura 3.7 Comparación de características entre audio original y estego-audio para 1709 caracteres incrustados

3.2.2. Pruebas de inserción de mensaje mediante selección de archivo texto

Para realizar las pruebas de inserción mediante la selección de un archivo de texto, se seleccionarán archivos que contengan valores de caracteres diferentes a los mencionados en la sección 3.2.1. Para empezar, se selecciona la opción Selección de Archivo en la herramienta de uso didáctico, el cual nos permitirá habilitar la función de selección de este; es necesario mencionar que se han creado previamente los archivos de texto a ocultar, por lo que se ha de elegir 2 de diferente longitud de caracteres.

a) Archivo de texto con 2000 caracteres en formato ASCII

A continuación, en la Figura 3.8 se muestra los detalles de la selección del archivo de texto, el cual será tomado como mensaje a incrustar en el audio portadora dentro del proceso esteganográfico.

Figura 3.8 Selección del archivo de texto a incrustar en formato .txt

La Figura 3.9 muestra la comparación en detalles del audio original y estego-audio, tomadas de la vista de navegación dentro del ambiente Windows, esto para demostrar que se puede manejar una longitud mayor en caracteres para el mensaje a ser incrustado.

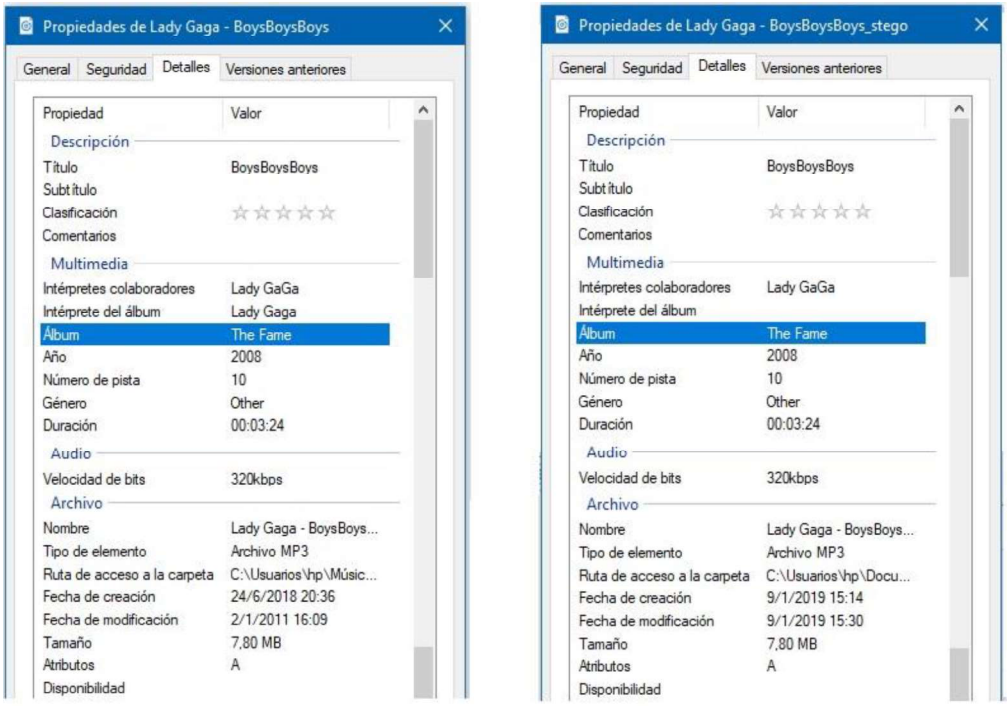


Figura 3.9 Comparación al incrustar 2000 caracteres desde un archivo de texto

b) Archivo de texto con 4035 caracteres en formato ASCII

En la Figura 3.10 se muestran los detalles de la selección del archivo de texto, el cual será tomado como mensaje para incrustarlo en el audio portadora siempre tratando de verificar que se cumpla el propósito esteganográfico.

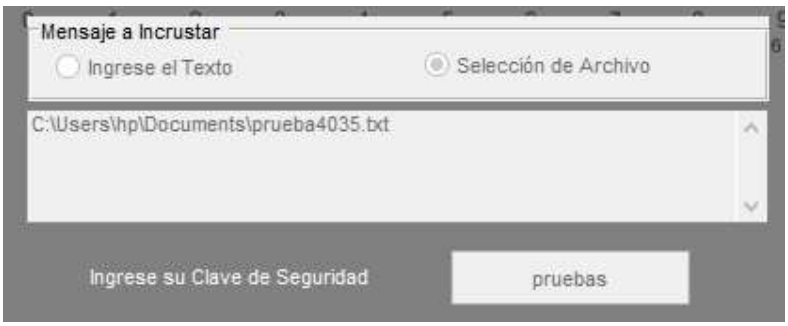


Figura 3.10 Selección del archivo de texto con 4035 caracteres a incrustar en formato .txt

En la figura 3.11 se puede observar que se puede incrustar un archivo de texto con 4035 caracteres de longitud sin que exista modificación del archivo de audio seleccionado para la prueba de ocultamiento.

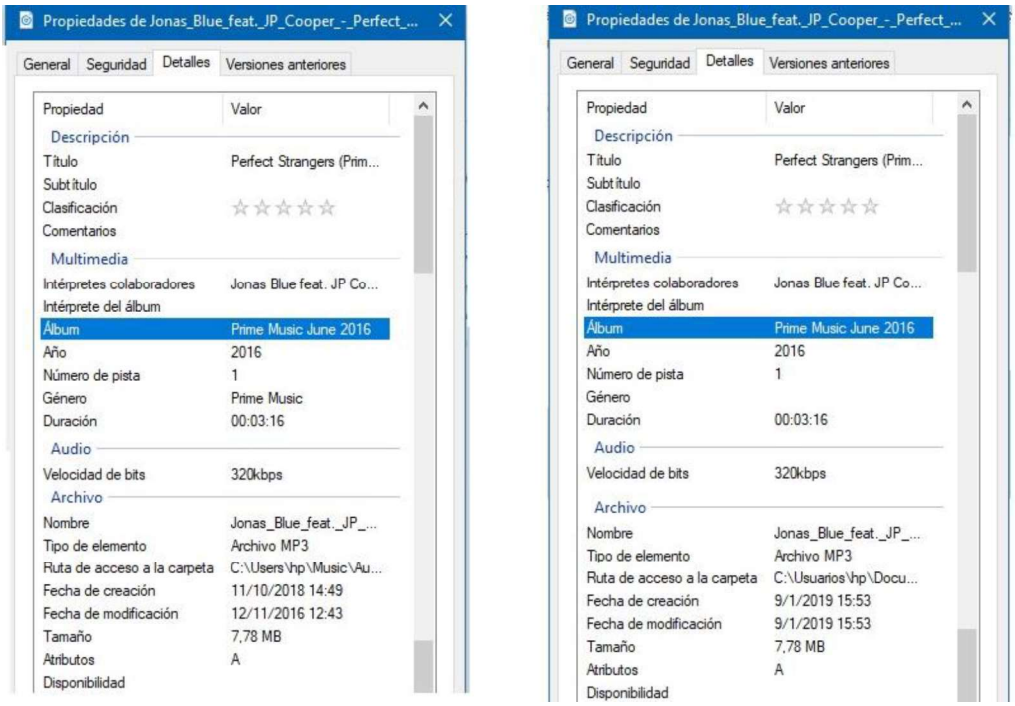


Figura 3.11 Comparación entre archivos al incrustar 4035 caracteres desde un archivo de texto

3.3. Pruebas de Encriptación del mensaje

Esta prueba está enfocada a verificar si la herramienta realiza las funciones descritas en el alcance del proyecto concernientes al proceso de encriptación de los mensajes que se incrustaran dentro del audio portadora. Para empezar con las pruebas, es necesario utilizar la función disp() propia de Matlab la cual nos permitirá observar la matriz de los caracteres antes de encriptar y la resultante del proceso de encriptación mediante la técnica TripleDES.

Después de haber concluido con las acciones anteriores, se procedió a realizar las pruebas de funcionamiento de la herramienta de uso didáctico, y se las muestra a continuación utilizando las diferentes opciones de incrustación del mensaje.

a) Encriptación mediante la opción de ingreso de texto.

El objetivo principal de esta prueba es verificar que se cumple el proceso de encriptación del mensaje que se desea enviar, por lo que en la Figura 3.12 se muestra la matriz del texto sin encriptar correspondientes al texto: "*No te aferres a lo que sea fue".*

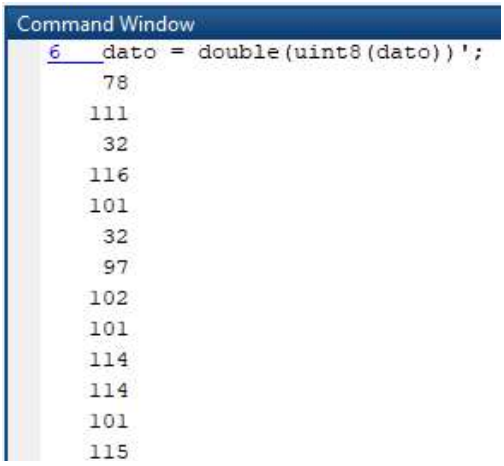


Figura 3.12 Obtención de formato decimal correspondiente a cada carácter ASCII

La imagen anterior corresponde a los valores en formato decimal de la tabla ASCII para cada carácter sin encriptar.

Luego de haber presionado el botón guardar de la herramienta, se hace la invocación de la función Encripcion3DES.m, la cual encriptará el mensaje mostrado en la Figura 3.13; con el mismo formato decimal donde se nota el proceso de encriptado.

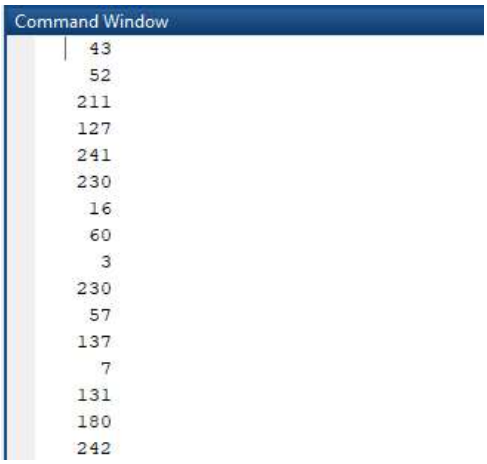


Figura 3.13 Obtención en formato decimal de los caracteres encriptados

Por lo tanto, se puede notar que el proceso de encriptación se cumple, ya que evaluando los 5 primeros números y comparándolos con el código ASCII corresponden a diferentes letras; cómo se puede ver en la tabla 3.2.

Tabla 3.2 Comparación de los caracteres encriptados con el alfabeto ASCII

Texto sin encriptar		**Texto encriptado**	
Numeración	**Carácter ASCII**	**Numeración**	**Carácter ASCII**
78	N	**43**	+
111	o	**52**	4
32	“espacio”	**211**	Ë
116	t	**127**	⌂
101	e	**241**	±

b) Encriptación mediante la opción de selección archivo de texto.

El objetivo de esta prueba es verificar que se cumple el proceso de encriptación al igual que el numeral anterior, por lo que en la Figura 3.14 se muestra la matriz del texto sin encriptar correspondientes al texto dentro del archivo .txt de 640 caracteres.

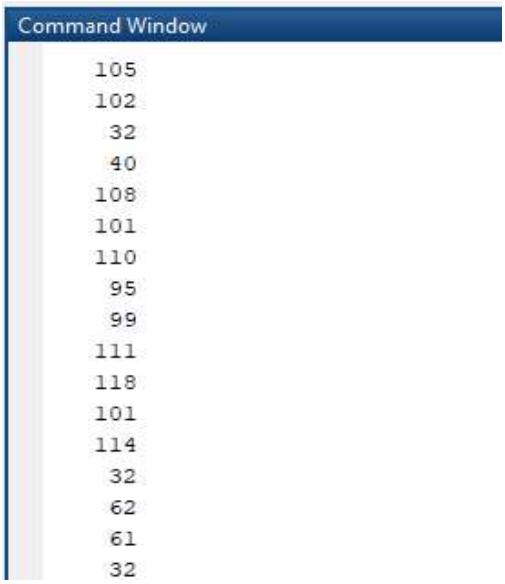


Figura 3.14 Obtención de formato decimal correspondiente a cada carácter ASCII dentro del archivo de texto seleccionado

Mientras que en la Figura 3.15, se muestra el texto encriptado por la función de encriptación, denotado en formato decimal.

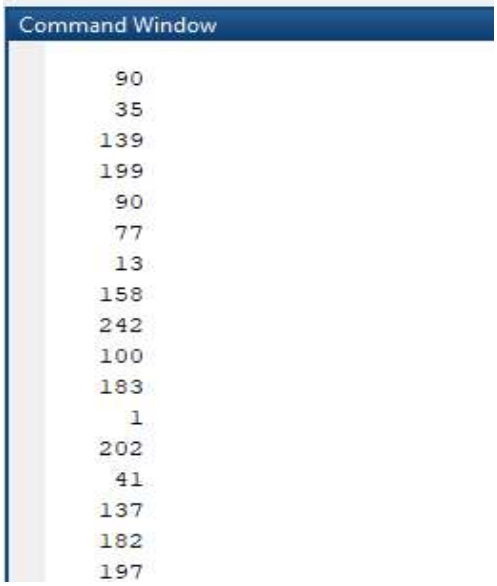


Figura 3.15 Obtención en formato decimal de los caracteres encriptados dentro del archivo de texto

Al evaluar los 6 primeros números y comparándolos con el código ASCII, se constata que corresponden a diferentes letras; mostrado en la tabla 3.3.

Tabla 3.3 Comparación de los caracteres encriptados con el alfabeto ASCII del archivo de texto seleccionado

Texto sin encriptar		**Texto encriptado**	
Numeración	**Carácter ASCII**	**Numeración**	**Carácter ASCII**
105	i	**90**	Z
102	f	**35**	#
32	“espacio”	**139**	Ï
40	(	**199**	Ã
108	l	**90**	Z
101	e	**77**	M

Con las pruebas realizadas, se constata que el proceso de encriptación mediante la técnica de cifrado TripleDES es satisfactoria, además, ayuda a brindar un nivel de seguridad adicional, lo cual es primordial para el proceso esteganográfico.

3.4. Pruebas de Reproducción del estego-audio

En relación con la prueba de reproducción de estego-audio, se inició la aplicación de audio Groove, la cual es propia del sistema operativo Windows 10, en la cual se comprobarán los audios creados en las secciones 3.2 y 3.3, refiriéndonos como comprobación a verificar que el tiempo de reproducción sea el mismo del audio original, no exista distorsión del audio, no existan espacios donde sea notorio la modificación del archivo mp3.

Por lo que se procederá a realizar una encuesta a un grupo de 10 personas, preguntando lo siguiente:

¿Respecto al audio original, como usted calificaría la calidad del audio con mensaje oculto?

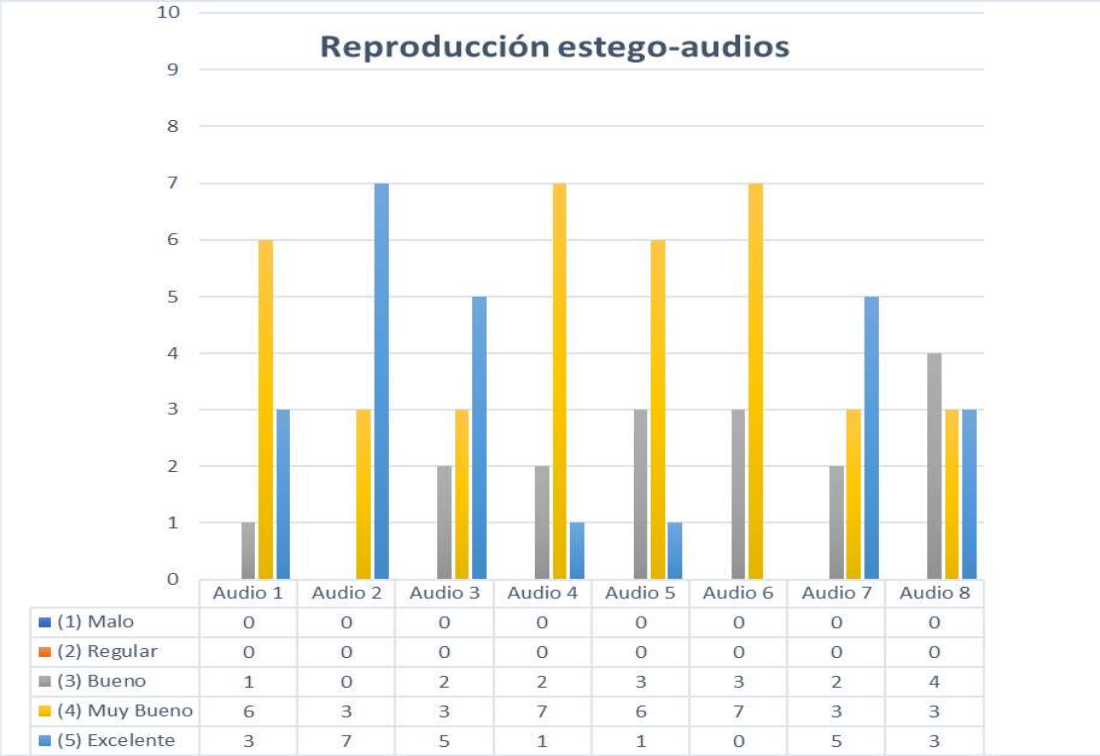
Teniendo como parámetros de calificación las opciones:

(1) Malo	(2) Regular	(3) Bueno	(4) Muy Bueno	(5) Excelente

Tabla 3.4 Ejemplo encuesta estego-audios

Audios	Calificación
Audio 1	Muy Bueno
Audio 2	Excelente
Audio 3	Excelente
Audio 4	Muy Bueno
Audio 5	Muy Bueno
Audio 6	Muy Bueno
Audio 7	Excelente
Audio 8	Bueno

Por lo que se detallara en la Figura 3.16; la calificación obtenida para cada audio dando los siguientes resultados:



	Audio 1	Audio 2	Audio 3	Audio 4	Audio 5	Audio 6	Audio 7	Audio 8
(1) Malo	0	0	0	0	0	0	0	0
(2) Regular	0	0	0	0	0	0	0	0
(3) Bueno	1	0	2	2	3	3	2	4
(4) Muy Bueno	6	3	3	7	6	7	3	3
(5) Excelente	3	7	5	1	1	0	5	3

Figura 3.16 Resultados de reproducción de estego-audios.

3.5. Pruebas de Desencriptación del mensaje

Para realizar el proceso de desencriptación del mensaje se procede a escoger un estego-audio previamente creado, se espera que mediante el uso correcto de la técnica 3DES y las matrices mencionadas en la sección 2.2.3 se desencripte el mensaje oculto en el audio portadora.

Por lo que se hará una captura de los bits transformados a formato decimal, que se extraen del estego-audio, dentro del proceso esteganográfico.

En la Figura 3.17 se muestra la captura de los bits en formato decimal antes de ser desencriptados.

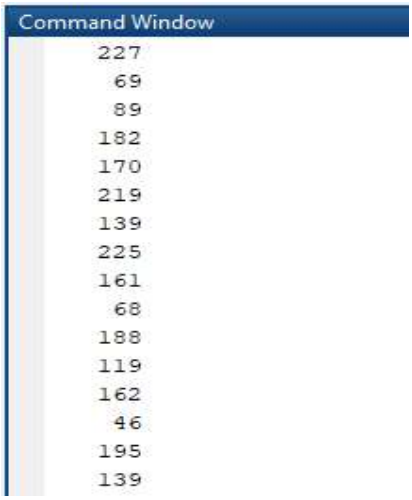


Figura 3.17 interpretación en formato decimal de los bits extraídos para su desencriptación

Luego a la matriz de bits extraídos se las envía como parámetros de entrada a la función Decripcion3DES.m para que nos devuelva una matriz en formato decimal con los valores que se muestran en la Figura 3.18.

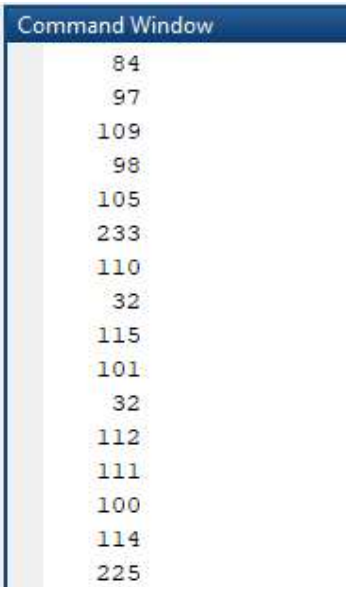


Figura 3.18 Desencriptación e interpretación de los bits en formato decimal

Tras evaluar los 8 primeros números y compararlos con el código ASCII, se constata que son diferentes letras; las cuales se muestran en la Tabla 3.5.

Tabla 3.5 Comparación entre los bits extraídos antes de desencriptar y luego de la desencriptación

Texto extraído sin desencriptar		Texto desencriptado	
Numeración	**Carácter ASCII**	**Numeración**	**Carácter ASCII**
227	Ò	**84**	T
69	E	**97**	a
89	Y	**109**	m
182	Â	**98**	b
170	¬	**105**	i
219	▮	**233**	Ú
139	Ï	**110**	n
225	ß	**32**	“espacio”

Los resultados obtenidos cumplen con la función de desencriptación y se los puede apreciar en la Figura 3.19, sin embargo, algunos caracteres con acento pueden no coincidir con su código ASCII, por lo que la herramienta procura hacer la conversión adecuada y así tener el texto que se insertó en la portadora sin ninguna modificación.

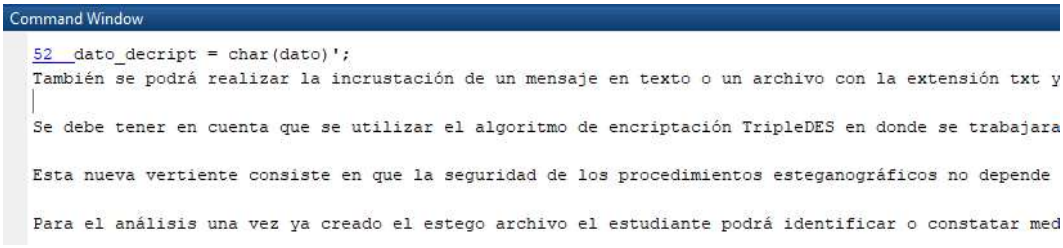


Figura 3.19 Correcta extracción del mensaje al proveer la clave correcta

En el caso, de tener una percepción de la clave, pero esta no sea correcta el mensaje aun seguirá encriptado como se muestra en la Figura 3.20 a continuación.

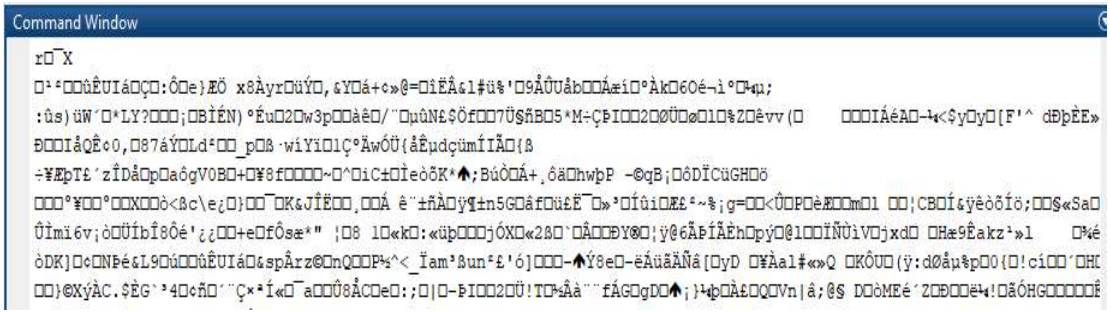


Figura 3.20 Texto cifrado luego de tratar de intuir la clave de encriptación

3.6. Pruebas de obtención del mensaje en el estego-audio creado

En este apartado se describen las diferentes pruebas realizadas para verificar el funcionamiento de la herramienta de uso didáctico. Se presentan pruebas para evaluar del desempeño y obtención del mensaje después de realizar el proceso de desencriptación. Posteriormente, al lograr obtener correctamente el mensaje se lo podrá visualizar en un cuadro de texto dentro de la herramienta.

Finalmente, de ser correcto el mensaje obtenido, se lo podrá guardar en un archivo de texto en formato .txt y constatar que el mensaje se ha recuperado sin ninguna alteración.

Los resultados obtenidos cumplen con la función de obtención del mensaje como se puede observar en la Figura 3.21, sin embargo, para el proceso de guardar el mensaje en un archivo de texto se procedió a utilizar funciones propias de Matlab.

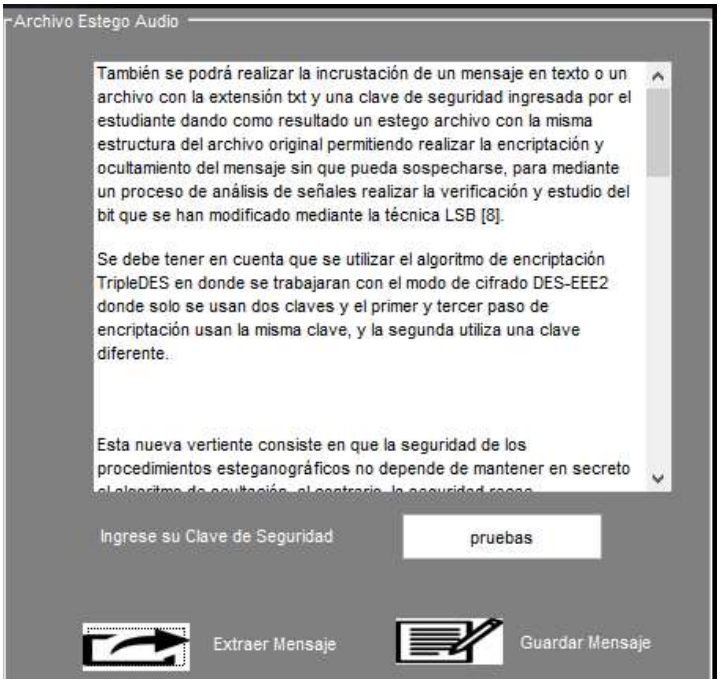


Figura 3.21 Visualización del proceso de extracción el mensaje dentro de la herramienta de uso didáctico.

Como se puede observar en la Figura 3.22, el archivo guardado contiene el mismo contenido del texto recuperado por lo que se puede indicar la prueba como satisfactoria.

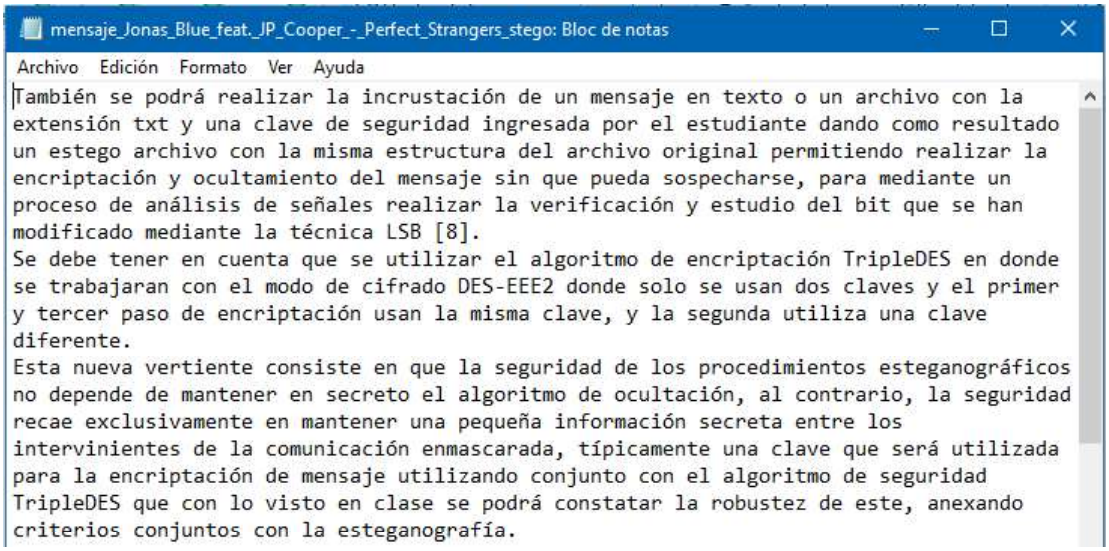


Figura 3.22 Visualización del Archivo de texto guardado con el mensaje correctamente extraído

3.7. Resultados.

- La funcionalidad básica de la herramienta de uso didáctico fue verificada en base a pruebas que consistieron en la carga de archivo de formato correcto y otra elegida por error en un formato diferente. Posteriormente, el funcionamiento de la herramienta fue validado en base a la carga del archivo de formato correcto, proceso de encriptación e incrustación del mensaje. Finalmente, obtenido el estego-audio se realizó la verificación el proceso de extracción y desencriptación del mensaje, para mostrarlo y guardarlo en un archivo con formato .txt.

- El mensaje máximo que puede ser incrustado en el archivo de audio mp3 como portadora es 2600 caracteres alfanuméricos, para archivos MP3 de tamaño mínimo 1.9Mb en adelante.

- En cuanto al consumo de los recursos computacionales de la herramienta se observó que el porcentaje de CPU que ocupa el software de simulación cuando se encuentra activo, durante el proceso de incrustación es de 41.3% y para el proceso de obtención es de 46.5% respectivamente; mientras que el consumo de memoria se mantiene en un valor del 0.5 %.

- En cuanto al desempeño de la herramienta de uso didáctica, se puede indicar que cumple con los objetivos planteados en el plan de titulación, cumpliendo los requerimientos y procesos dentro del ámbito esteganográfico.

CAPÍTULO 4

4. CONCLUSIONES Y RECOMENDACIONES

En este capítulo se presentan las conclusiones y recomendaciones obtenidas durante el desarrollo del trabajo de titulación.

4.1. Conclusiones.

- Es factible el envío de caracteres como mensaje en formato ASCII dentro de una portadora de audio con formato MP3, utilizando el método del dominio temporal, basada en la técnica esteganográfico LSB.
- Al realizarse la herramienta de uso didáctica esteganográfica en un lenguaje de programación propio como Matlab, permitió realizar el seguimiento progresivo de cada una de las funciones inmersas dentro del proceso esteganográfico, logrando así el objetivo planteado al inicio del proyecto.
- Los requerimientos de cada módulo permitieron tener una perspectiva de las acciones que deben realizarse al implementar las funciones de carga de audio, encriptación y desencriptación, incrustación y extracción, con los que se puede constatar el funcionamiento de los componentes que conforman la herramienta.
- El uso de funciones independientes para cada uno de los procesos; ya sean estos de incrustación u obtención del mensaje, permite la visualización de los errores en la escritura y formato dentro del IDE de Matlab, el cual provee herramientas para programar y crear interfaces gráficas.
- AL estudiar la técnica de encriptación DES como base, permitió elegir una secuencia de llaves adecuada en la implementación de las funciones encriptación y desencriptación mediante la técnica TripleDES la cual brindará seguridad adicional a la herramienta.
- Las pruebas realizadas tienen el objetivo de verificar que el funcionamiento de la herramienta de uso didáctico sea el correcto para cumplir con el alcance del proyecto. Se realizo pruebas a cada módulo y cada función dentro de la herramienta. Los resultados obtenidos demuestran que la

herramienta es funcional y puede ser utilizada en el ámbito educativo dentro de la materia de seguridades.

- Mediante la encuesta MOS realizada, la mayoría de personas no encontró ningún cambio en la calidad de audio respecto a el audio original, sin embargo, un pequeño grupo de personas percibió una ligera distorsión, mas no identificaron si existía ruido o sobresaltos en el audio creado.

4.2. Recomendaciones.

- Se debe tener muy en cuenta la estructura del formato MP3, ya que este es un formato de audio comprimido con pérdidas, por lo que, al realizar la descomposición del archivo y la estructuración de una trama para la incrustación de los bits del mensaje, esta debe tener una secuencia respecto a su cabecera de 4 Bytes. No obstante, también se deben analizar los 128 Bytes que posee el tag ID3, que con un correcto manejo y precisa reestructuración nos permite ampliar de forma significativa el tamaño de caracteres que se pueden incrustar en la portadora.
- Se recomienda hacer un seguimiento progresivo de cara matriz y dato que se extraiga dentro del entorno de Matlab, ya que de existir una inconsistencia de valores, dimensiones o conversión de tipo de datos generarán alertas, las cuales de no ser manejadas apropiadamente consumirán recursos de computación volviendo al ambiente de desarrollo lento.
- Dado que la ejecución del programa requiere gran cantidad de recursos computacionales, es recomendable utilizar un computador que tenga como mínimas características un procesador de 4 núcleos Intel o AMD, 6 GB de RAM dedicadas, sistema de 64 bits tanto de Matlab como en la versión de Windows a utilizar.
- Se debe tener en cuenta que el desarrollo de una aplicación tipo GUIDE en Matlab es muy limitado, por lo que, para tener una aplicación muy similar a lenguajes de programación de alto nivel se deben utilizar funciones o App propias de Matlab logrando así el uso adecuado de los recursos.

- Para realizar la descomposición de un archivo de audio MP3 es recomendable utilizar la dll LIME, la cual nos facilita el uso, manejo y extracción de información, exclusiva para archivos de audio en formato MP3.
- Se recomienda trabajar con una conversión de datos de información de 8 bits en la portadora MP3, para que sea menos perceptible la modificación del archivo de audio creado, ya que originalmente se trabaja con formato de datos dados en 16 bits.
- El presente Trabajo de Titulación podría ser usado como guía para el desarrollo de futuras aplicaciones, en las que se permita el ocultamiento de información en archivos de audio con formato digital, como Vosbis, Musepack o AAC, utilizando técnicas esteganográficas como echo-hiding, y pase-encoding.

5. REFERENCIAS BIBLIOGRÁFICAS

[1] H. Silva, «Esteganografia em Áudio e Imagem utilizando a técnica LSB,» UNIVERSIDADE FEDERAL DE GOIAS , Cataluña, 2009. [Online] Disponible en: https://dcc.catalao.ufg.br/up/498/o/Hugo2009.pdf .

[2] V. Navarro, «Esteganografía en contenido Multimedia,» Universitat Oberta de Catalunya, Catalunya, 2007. [Online] Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/929/1/40114tfc.pdf

[3] P. Dutta, D. Bhattacharyya y T. Kim, Data Hiding in Audio Signal: A Review, Korea: Theory and Application,Vol. 2, No. 2, 2009. [Online] Disponible en: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.617.550&rep=rep1&type=pdf

[4] E. Morocho, «Implementación del algoritmo esteganográfico f5 para imágenes jpeg a color, » Tesis Electrónica y Redes de Información (IER), Quito, 2014. [Online] Disponible en: http://bibdigital.epn.edu.ec/handle/15000/8062 .

[5] R. Petitcolas y J. Anderson, «On the limits of steganography.,» *IEEE Journal on Selected Areas in Communications,* vol. 16, nº 4, pp. 474-481, May 1998. [Online] Disponible en: https://www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf .

[6] G. Velásquez, «Análisis de técnicas de esteganografía aplicadas en archivos de audio e imagen,» *Polo del Conocimiento,* vol. 2, nº 1, pp. 54-67, 2017. [Online] Disponible en: https://polodelconocimiento.com/ojs/index.php/es/article/download/10/pdf .

[7] R. Chandramouli y N. Memon, «"Analysis of LSB BASed Image Steganographlhy Techniques",» de *Proceedings of the International Conference on Image Processing*, Greece, 2001. [Online] Disponible en: https://ieeexplore.ieee.org/document/6921751/ .

[8] G. Rodriguez y R. Navas, «Esteganografía: Sustitución LSB 1 bit utilizando Matlab,» de *XVIII Workshop de Investigadores en Ciencias de la Computación (WICC 2016, Entre Ríos, Argentina)*, Argentina, 2016.

[9] LAME, The LAME Project. [Online] Disponible en: http://lame.sourceforge.net/index.php

[10] A Petitcolas Fabien, « “History of Steganography”», [Online] Disponible en: https://www.petitcolas.net/steganography/history.html .

[11] A Siper, R Farley y C Lombardo, «"The Rise of Steganography",» de Proceedings of Student/Faculty Research Day, CSIS, Pace University, May 6th, 2005. [Online] Disponible en: http://csis.pace.edu/~ctappert/srd2005/d1.pdf

[12] «"ESTEGANOGRAFÍA, EL ARTE DE OCULTAR INFORMACIÓN ",» de Instituto Nacional de Tecnologías de la Comunicación. [Online] Disponible en: http://www.egov.ufsc.br/portal/sites/default/files/esteganografia1.pdf

[13] Muhalim Mohamed Amin et al., “Information hiding using Steganography”, 2003. [Online] Disponible en: https://www.researchgate.net/publication/4008787_Information_hiding_using_steganography

[14] Hamid.A.Jalab, A.A Zaidan, B.B Zaidan, “New Design for Information Hiding with in Steganography Using Distortion Techniques”, International Journal of Engineering and Technology (IJET)), Vol 2, No. 1, ISSN: 1793-8236, Feb (2010), Singapore.

[15] A.W. Naji, Shihab A. Hameed, B.B.Zaidan, Wajdi F. Al-Khateeb, Othman O. Khalifa, A.A.Zaidan y Teddy S. Gunawan, “ Novel Framework for Hidden Data in the Image Page within Executable File Using Computation between

Advance Encryption Standared and Distortion Techniques", International Journal of Computer Science and Information Security (IJCSIS), Vol. 3, No 1 ISSN: 1947-5500, P.P 73-78,3 Aug 2009, USA.

[16] Raymond G. Kamme," Federal Information Processing Standards Publication", U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, PUB 46-3, October 1999.

[17] Mahmoud Elnajjar, A.A Zaidan, B.B Zaidan, Mohamed Elhadi M.Sharif y Hamdan.O.Alanazi ," Optimization Digital Image Watermarking Technique for Patent Protection", Journal of Computing (JOC), Vol.2, Issue 2, ISSN: 2151-9617, P.P 142-148 February 2010, Lille, France.

[18] Alaa Taqa, A.A Zaidan, B.B Zaidan ,"New Framework for High Secure Data Hidden in the MPEG Using AES Encryption Algorithm", International Journal of Computer and Electrical Engineering (IJCEE),Vol.1 ,No.5, ISSN: 1793-8163, p.p.566-571 , December (2009). Singapore.

[19] B.B Zaidan , A.A Zaidan ,Alaa Taqa , Fazidah Othman ," StegoImage Vs Stego-Analysis System", International Journal of Computer and Electrical Engineering (IJCEE),Vol.1 ,No.5 , ISSN: 1793-8163, pp.572-578 , December (2009), Singapore.

[20] A.A.Zaidan, A.W. Naji, Shihab A. Hameed, Fazidah Othman y B.B.15 Zaidan, " Approved Undetectable-Antivirus Steganography for Multimedia Information in PE-File ",International Conference on IACSIT Spring Conference (IACSIT-SC09) , Advanced Management Science (AMS), Listed in IEEE Xplore and be indexed by both EI (Compendex) and ISI Thomson (ISTP), Session 9, P.P 425-429.

[21] A.A.Zaidan, B.B.Zaidan, M.M.Abdulrazzaq, R.Z.Raji, y S.M.Mohammed," Implementation Stage for High Securing CoverFile of Hidden Data Using

Computation Between Cryptography and Steganography", International Conference on Computer Engineering and Applications (ICCEA09), Telecom Technology and Applications (TTA), indexing by Nielsen, Thomson ISI (ISTP), IACSIT Database, British Library and EI Compendex, Vol.19, Session 6, p.p 482-489.

[22] A.W. Naji, A.A.Zaidan, B.B.Zaidan, Ibrahim A.S.Muhamadi, "New Approach of Hidden Data in the portable Executable File without Change the Size of Carrier File Using Distortion Techniques", Proceeding of World Academy of Science Engineering and Technology (WASET),Vol.56, ISSN:2070-3724, P.P 493-497.

[23] Hamdan. Alanazi, Hamid.A.Jalab, A.A.Zaidan, B.B.Zaidan, "New Frame Work of Hidden Data with in Non Multimedia File", International Journal of Computer and Network Security, 2010, Vol.2, No.1, ISSN: 1985-1553, P.P 46-54,30 January, Vienna, Austria.

[23] A.W.Naji, A.A.Zaidan, B.B.Zaidan, Ibrahim A.S.Muhamadi, "Novel Approach for Cover File of Hidden Data in the Unused Area Two within EXE File Using Distortion Techniques and Advance Encryption Standard.", Proceeding of World Academy of Science Engineering and Technology (WASET),Vol.56, ISSN:2070-3724, P.P 498-502.

[24] M.Abomhara, Omar Zakaria, Othman O. Khalifa, A.A.Zaidan, B.B.Zaidan, "Enhancing Selective Encryption for H.264/AVC Using Advance Encryption Standard ", International Journal of Computer and Electrical Engineering (IJCEE), ISSN: 1793-8198,Vol.2 , NO.2, Aprl 2010, Singapore.

[25] Md.Rafiqul Islam, A.W. Naji, A.A.Zaidan, B.B.Zaidan " New System for Secure Cover File of Hidden Data in the Image Page within Executable File Using Statistical Steganography Techniques", International Journal of

Computer Science and Information Security (IJCSIS), ISSN: 1947-5500, P.P 273-279, Vol.7 , NO.1, January 2010, USA.

[26] J. Herre ; M. Dietz, «" MPEG-4 high-efficiency AAC coding [Standards in a Nutshell]",» de IEEE Signal Processing Magazine, ISSN: 1558-0792, P.P 137-142, Volume: 25 , Issue: 3 , May 2008 . [Online] Disponible en: https://ieeexplore.ieee.org/document/4490211 .

[27] «"MPEG-1 Data Structures "» de Philips Interactive Media. [Online] Disponible en: http://andrewduncan.net/mpeg/mpeg-1.html .

[28] M. Nilsson y M. Mutschler, «" ID3v2 Programming Guidelines ",» de Dan O'Neill. [Online] Disponible en: http://id3.org/ID3v2Easy .

[29] Nematollahi, Mohammad Ali, Chalee Vorakulpipat, and Hamurabi Gamboa Rosales. "Audio Watermarking." Digital Watermarking. P.P 17-38. Springer Singapore, 2017.

[30] A.W. Naji, A.A.Zaidan, B.B.Zaidan, Ibrahim A.S.Muhamadi, "Novel Approach for Cover File of Hidden Data in the Unused Area Two within EXE File Using Distortion Techniques and Advance Encryption Standard.", Proceeding of World Academy of Science Engineering and Technology (WASET),Vol.56, ISSN:2070-3724, P.P 498-502, Aug 2009, USA.

[31] M. Abomhara, Omar Zakaria, Othman O. Khalifa, A.A.Zaidan, B.B.Zaidan, "Enhancing Selective Encryption for H.264/AVC Using Advance Encryption Standard ", International Journal of Computer and Electrical Engineering (IJCEE), ISSN: 1793-8198,Vol.2 , NO.2, April 2010, Singapore.

6. ANEXOS

ANEXO I. A	Instalación de la Herramienta de uso didáctico.
ANEXO I. B	Manual de Usuario.
ANEXO II.	Herramienta de uso didáctico esteganográfica (CD adjunto).
ANEXO III.A	Resultados de la encuesta para evaluar la calidad del estego-audio creado.
ANEXO III.B	Enlaces de la encuesta de la plataforma Google Forms

ANEXO I.A

GUÍA DE INSTALACIÓN DE LA HERRAMIENTA DE USO DIDÁCTICO

a. DOCUMENTACION DE USUARIO.

La herramienta de uso didáctico implementada en el capítulo dos, permite apoyar el estudio y obtención de conocimientos en materia de esteganografía, mediante la realización de ejemplos reales. Al usar esta herramienta, el usuario podrá crear estego-audios propios, extraer los mensajes que fueron ocultados en las mismos, constatando la utilidad y beneficio de usar técnicas esteganográficas.

b. REQUERIMIENTOS

Para la utilización de la herramienta el usuario debe poseer conocimientos previos, de no ser el caso, se recomienda la lectura de los tres primeros capítulos del este proyecto de titulación.

Como siguiente paso, el programa ha sido desarrollado y probado en un PC con las siguientes características:

- Matlab: Version R2018a (9.4.0.813654) 64-bit

Sistema Operativo	Windows Version Windows 10 (64 bit)
Memoria RAM	12 GB
Procesador	AMD A12-9720P RADEON R7, 12 COMPUTE CORES 4C+8G 2.7GHz
Tarjeta Gráfica	AMD Radeon R7 Graphics

Tabla A.1 Esquema de desarrollo de la Herramienta de uso didáctico

Por lo tanto, los requerimientos mínimos para el correcto desempeño de la aplicación se lo detallan en la siguiente tabla:

Sistema Operativo	Windows 10 Windows 7 Service Pack 1
Memoria RAM	**Minimo**: 4 GB; **Recomendado**: 8 GB Para ambientes múltiples, 4GB por core
Procesador	**Minimo**: Intel or AMD x86-64 **Recomendado:** procesador Intel or AMD x86-64 processor con 4 cores lógicos y AVX2
Tarjeta Gráfica	No requiere tarjeta gráfica específica, pero se recomienda una que soporte OpenGL 3.3 con 1GB GPU de memoria

Tabla A.2 Recomendaciones de Instalación.

c. INSTALACIÓN DE LA HERRAMIENTA

En la presente sección se describirá el proceso de instalación y utilización de recursos necesarios para el funcionamiento adecuado de la herramienta de uso didáctico esteganográfica para envío de texto oculto y cifrado en archivos de audio mp3.

En la Figura A.1 se muestra el instalador de la herramienta, cabe mencionar que al ser desarrollado en un ambiente de 64 bits se tendrá la herramienta para sistemas operativos de las mismas características.

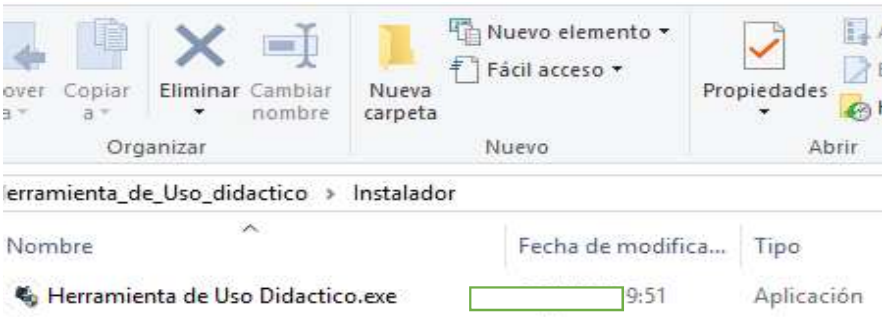


Figura A.1 Instalador de la Herramienta de uso didáctico.

Al realizar la instalación mediante el aplicativo .exe, se desplegará la siguiente pantalla mostrada en la Figura A.2.

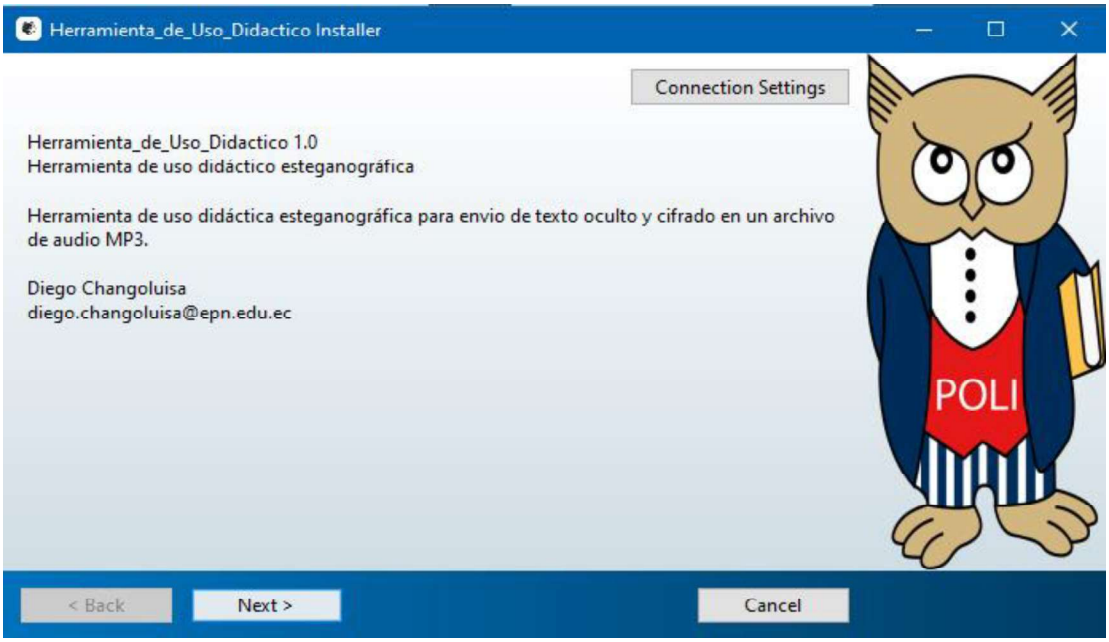


Figura A.2 Información del instalador de la Herramienta

Es recomendable realizar la instalación fuera del entorno predeterminado, y no activar la creación del atajo el escritorio que brinda el instalador, ya que se utilizarán dll y programas externos a la herramienta; posteriormente se instalará el Runtime de Matlab, para ordenadores que no tengan instalado el programa Matlab (Ver Figura A.3).

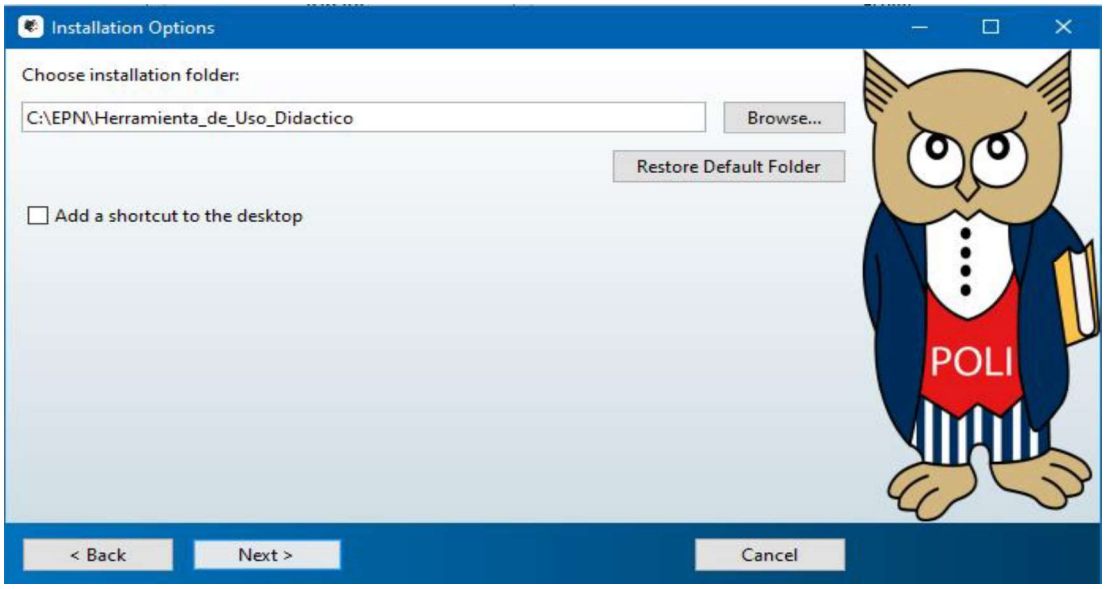


Figura A.3 Selección de la carpeta para la instalación de la herramienta

Luego de Finalizar la instalación correcta se mostrar un mensaje informativo (Ver Figura A.4).

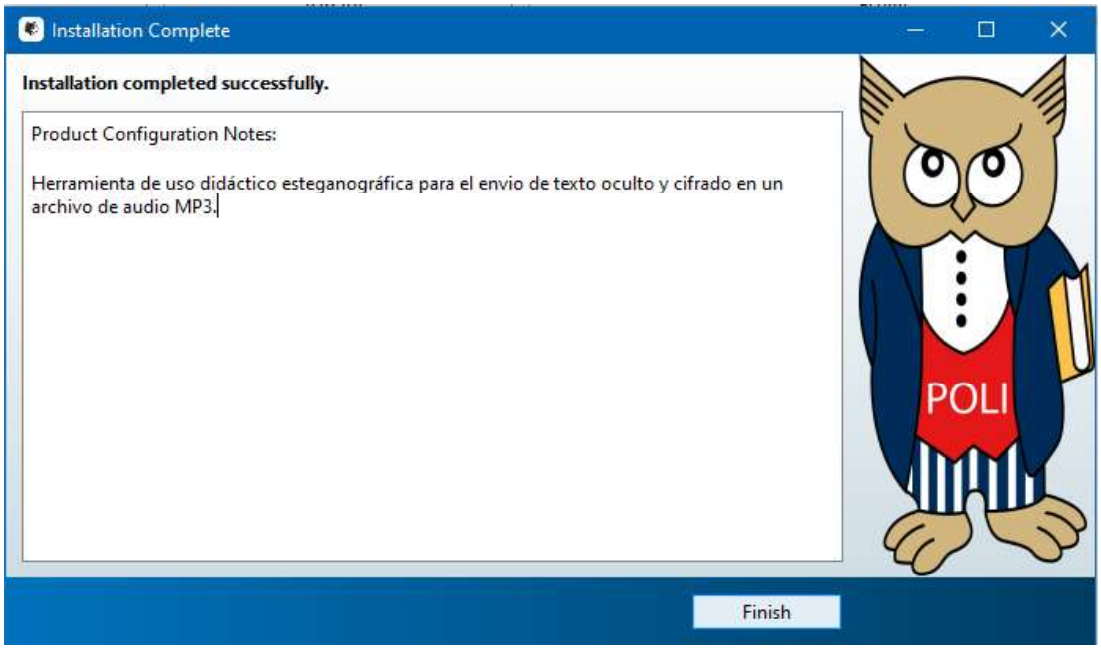


Figura A.4 Información de instalación correcta de la herramienta de uso didáctico

Para poder ejecutar la herramienta nos ubicaremos en la ruta en la cual fue instalado el programa. Dentro de la carpeta Herramienta_de_Uso_Didactico, iremos a > application donde encontraremos la información de la aplicación y en donde colocaremos la carpeta con el contenido necesario para su funcionamiento. Es indispensable aclarar que la carpeta con el contenido adicional se la puede obtener de la siguiente dirección:

- https://github.com/DiegoChangoluisa/binarioMP3

Se colocará la carpeta dentro del directorio en el que nos encontramos actualmente, para quedar tal cual la figura A.5.

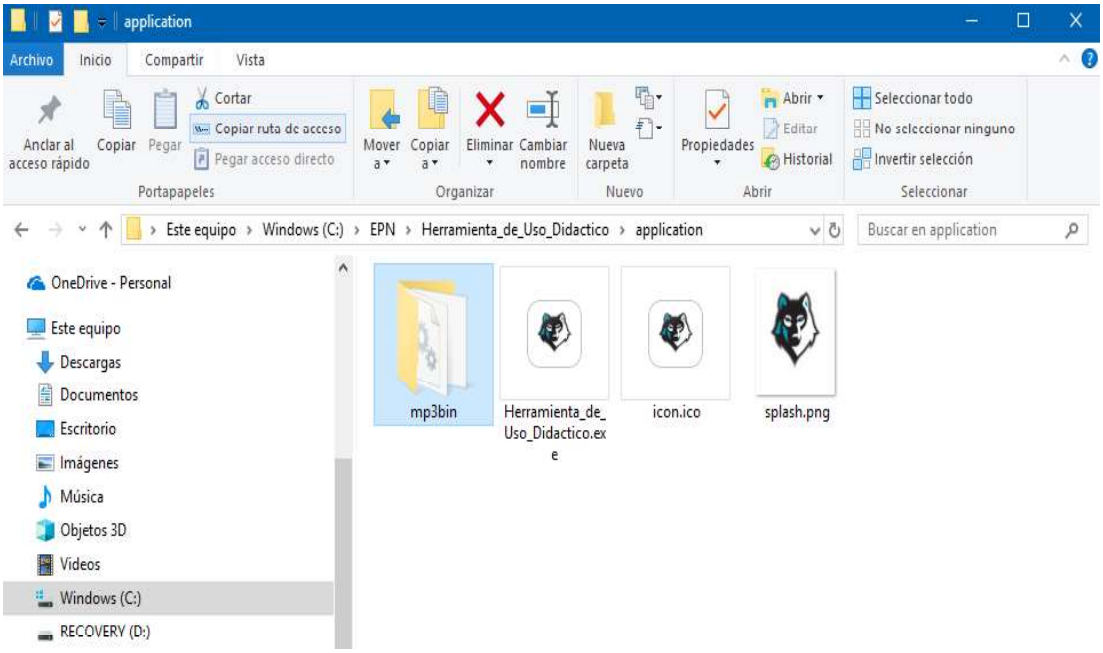


Figura A.5 Carpeta de la aplicación con los requerimientos necesarios para su correcta ejecución.

ANEXO I.B

MANUAL USUARIO

a. USO DE LA HERRAMIENTA

El programa ha sido desarrollado para realizar las tareas de la manera más intuitivas posibles, brindando al usuario la ventaja de conocer que realiza cada elemento de la interfaz. Sin embargo, a continuación, se detallará las tareas que se pueden efectuar en la interfaz, ayudando como referencia a usuarios inexpertos.

b. INTERFAZ DE INICIO

Al ejecutar la herramienta, al usuario se le despliega la ventana principal (ver Figura A.6), en la cual, existirán tres botones; el primero para el ocultamiento del mensaje, segundo para obtención del mensaje y por último el que permitirá salir al usuario de la herramienta.

Al seleccionar Ocultamiento del mensaje se desplegará una nueva ventana en al cual podrá ocultar el texto haciendo uso del método esteganográfico; si selecciona obtención del mensaje se desplegará una ventana, en la cual podrá realizar la obtención el cual ha sido incrustado y creado en el módulo de ocultamiento de mensaje; por último, si el usuario selecciona salir el programa será cerrado.

Figura A.6 Interfaz de Inicio de la Herramienta de uso didáctico

c. OCULTAMIENTO DE LA INFORMACIÓN

Al presionar el botón ocultamiento del mensaje en la interfaz de inicio, se despliega la ventana mostrada en la Figura A.7, al encontrarse allí el usuario notara que se encuentran habilitados los botones de carga de audio y atrás; en los cuales al presionar el primero se desplegara una ventana de navegación de archivos (Ver Figura A.8), donde debe cargar un archivo de audio en formato MP3. De no seleccionar un archivo mostrará el mensaje informativo (Ver Figura A.9).

Si el archivo seleccionado posee formato correcto, la herramienta despliega la información necesaria del archivo y habilitara los demás botones para continuar con el proceso esteganográfico, caso contrario le pedirá al usuario que seleccione el formato correcto.

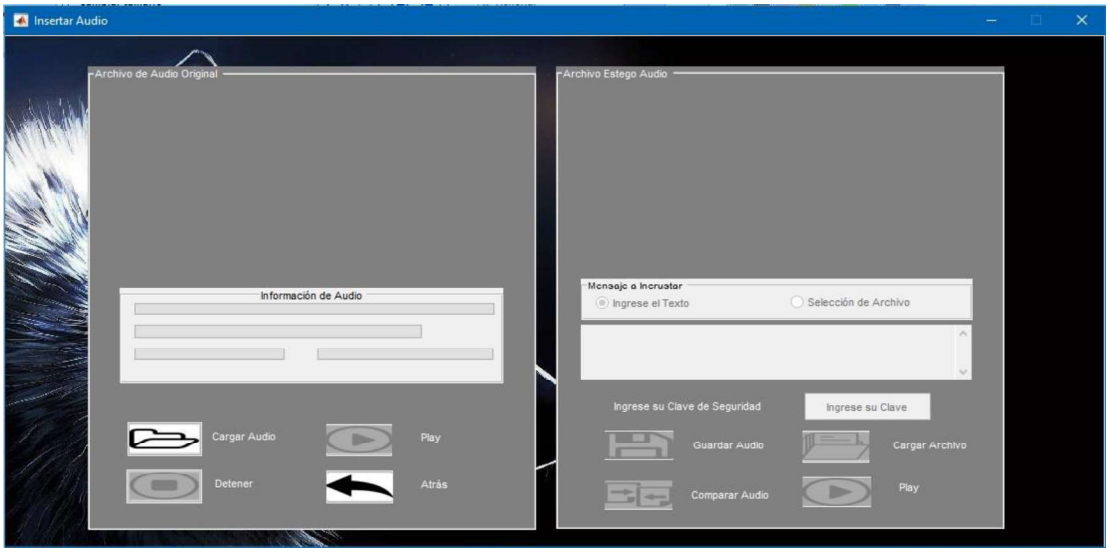


Figura A.7 Interfaz Ocultamiento del mensaje

Como se puede observar en la Figura A.10, los diálogos de error se dan cuando se ha seleccionado el formato incorrecto o no se ha cargado ningún archivo.

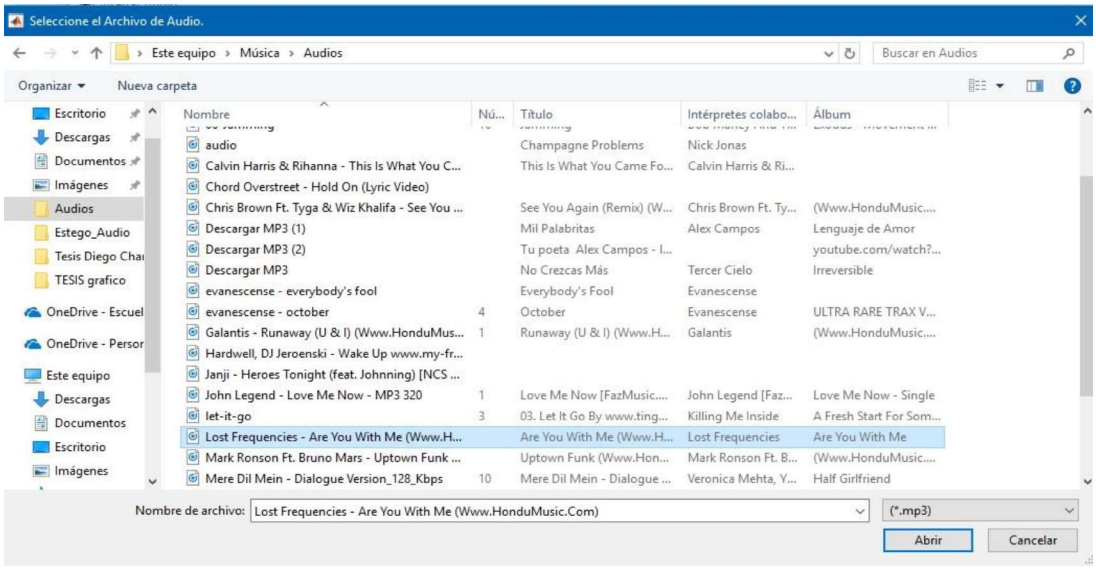


Figura A.8 Ventana de navegación para seleccionar el archivo portadora

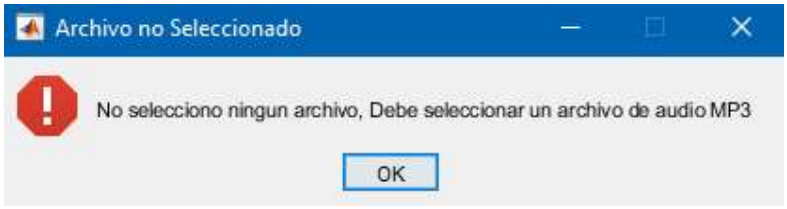


Figura A.9 Mensaje de Selección de archivo de audio MP3

En el panel de información del Audio, se visualizarán varias características que posee, entre ellas constan, ruta específica del archivo, nombre del archivo, frecuencia de muestreo, bitrate con el que fue codificado mostrado en la Figura A.11,

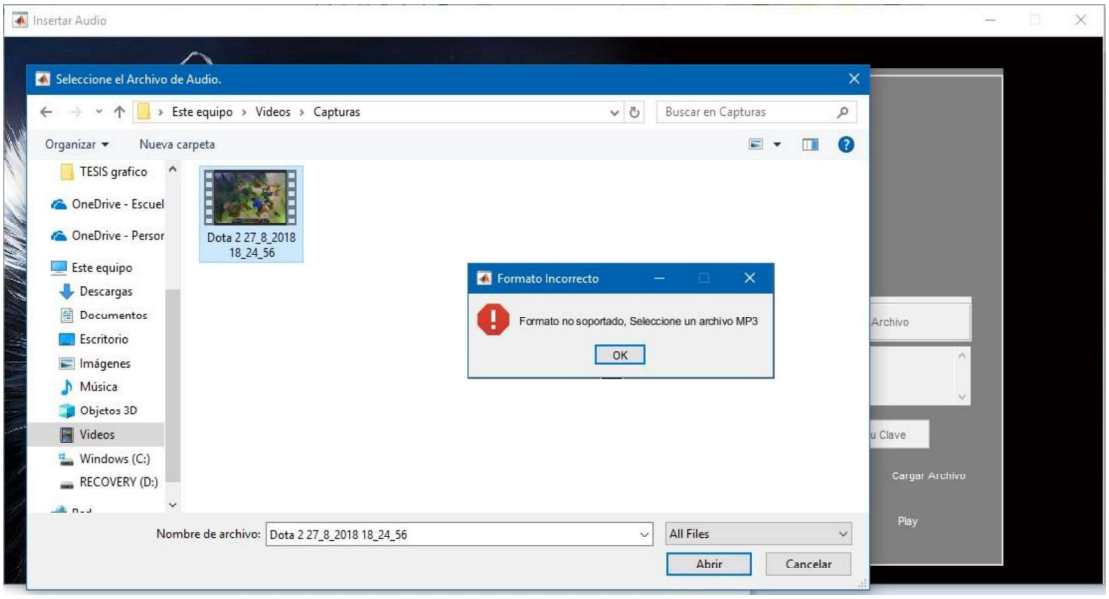


Figura A.10 Mensaje de error al seleccionar un archivo de formato diferente

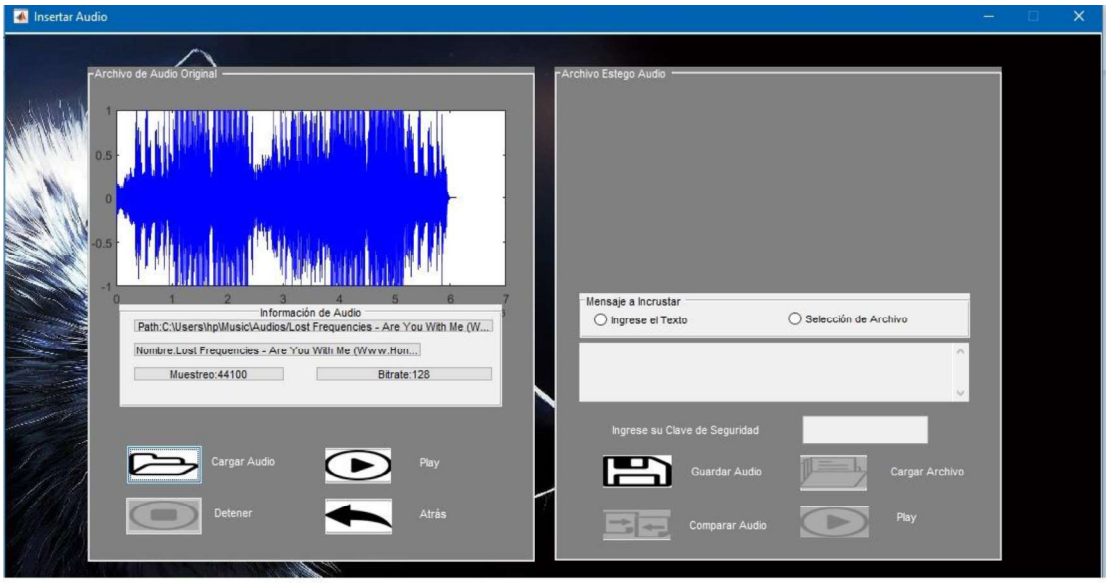


Figura A.11 Visualización de las características del archivo de audio y habilitación de botones del módulo ocultamiento

Una vez seleccionada la imagen, se habilita la opción para seleccionar la forma en que se incrustara la información, siendo esta, que el usuario escriba el mensaje en la interfaz de la herramienta o que seleccione un archivo de texto desde su ordenador (Ver Figura A.12)

Figura A.12 Selección del método de incrustación

Si selecciona "Ingrese el Texto", se habilita el cuadro de texto de la parte inferior en la cual el usuario podrá ingresar el texto que desee enviar mostrado en la Figura A.13.

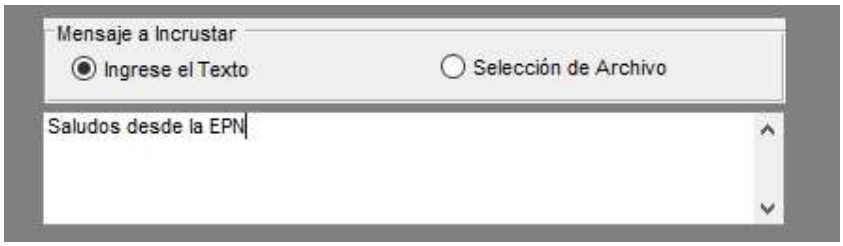


Figura A.13 Ingreso del mensaje por el usuario

Si selecciona la opción "Selección de Archivo", se habilita un botón de "Cargar Archivo" (Ver Figura A.14), al presionar el usuario el botón para cargar el archivo se despliega una ventana de navegación con la cual podrá navegar en el ordenador para seleccionar el archivo con formato .txt (Ver Figura A.15)

Figura A.14 Opción Selección de Archivo y habilitación del botón de Cargar Archivo

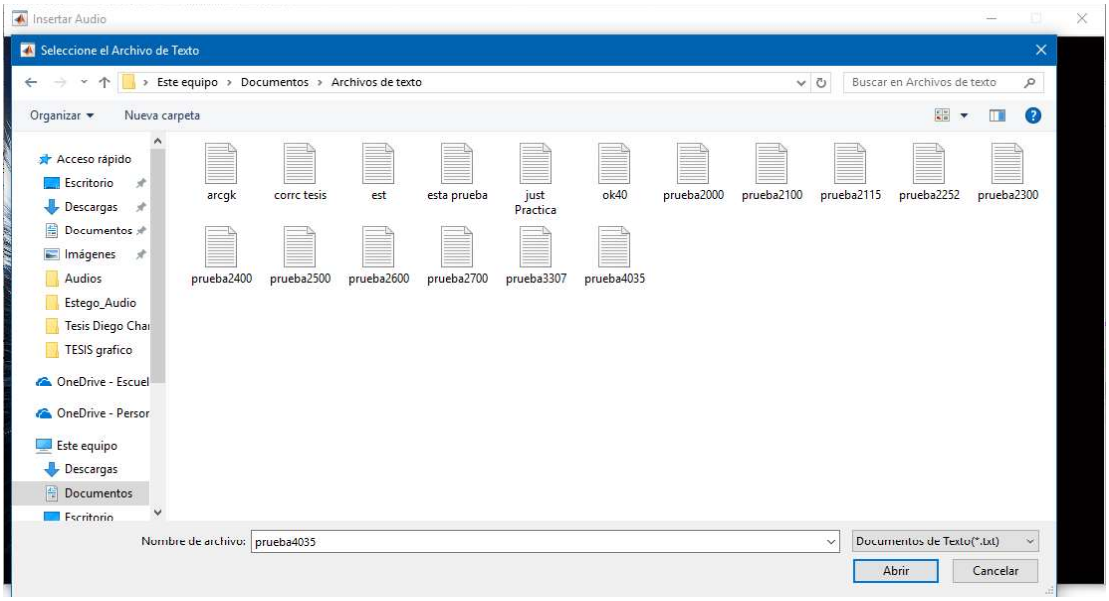


Figura A.15 Ventana de navegación para seleccionar el archivo a ocultar

Una vez ingresado el texto o seleccionado el archivo, el usuario debe proporcionar una clave la cual permitirá al algoritmo de encriptación cifrar el texto q se va a incrustar en la portadora.

Si el usuario no proporciona una clave, se indicar en un mensaje de dialogo que se debe ingresar una para continuar con el proceso de ocultamiento, como se muestra en la Figura A.16

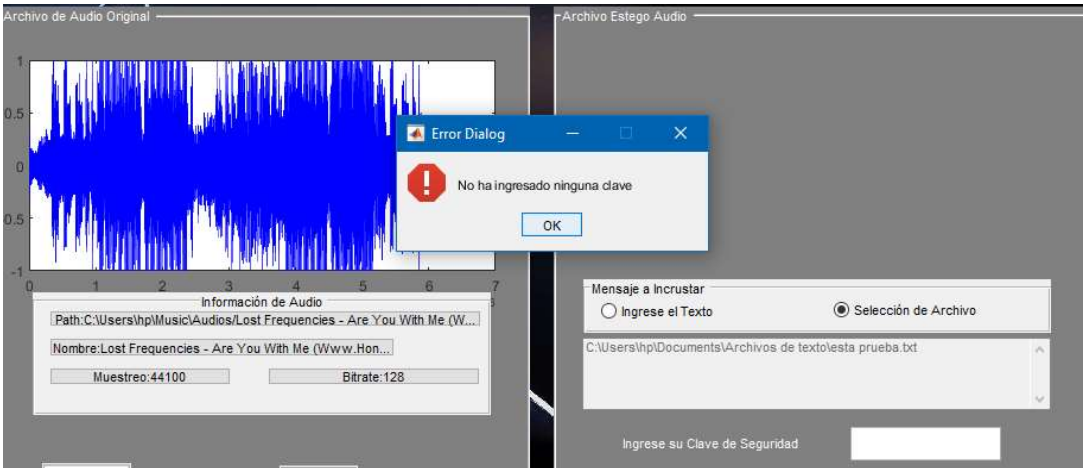


Figura A.16 Ventana de navegación para seleccionar el archivo a ocultar

Al presionar la casilla de clave se desplegará una ventana donde el usuario podrá ingresar la clave cumpliendo los requerimientos indicados en ella. (Ver Figura A.17).

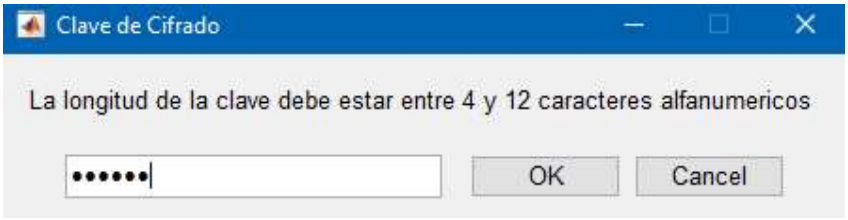


Figura A.17 Mensaje para ingresar la clave de cifrado.

Si la clave no cumple con los requisitos previsto para la encriptación se mostrará un mensaje de dialogo, en el cual se le indica al usuario la longitud que debe tener la clave (Ver Figura A.18).

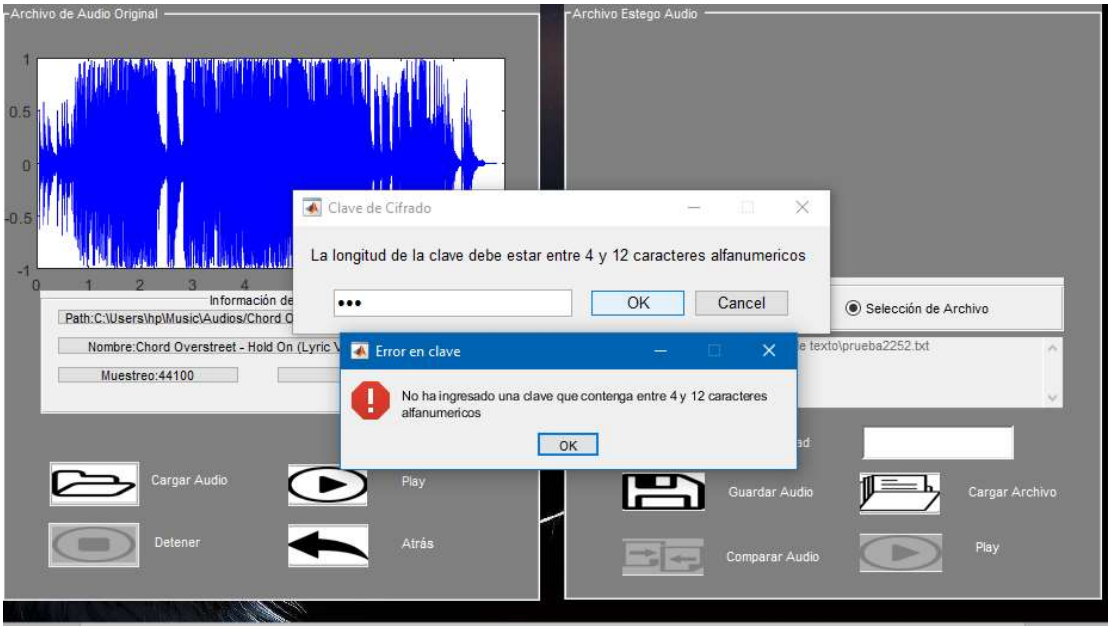


Figura A.18 Identificación de la longitud de la clave

Al cumplir todos los parámetros, para el ocultamiento del mensaje el usuario podrá presionar el botón “Guardar Audio” el cual permite crear el estego-audio; el cual será visualizado en un nuevo cuadro de espectrograma para poder notar la diferencia, además, se habilitan los botones de reproducción de este y el de comparación de Audio como se muestra en la Figura A.19.

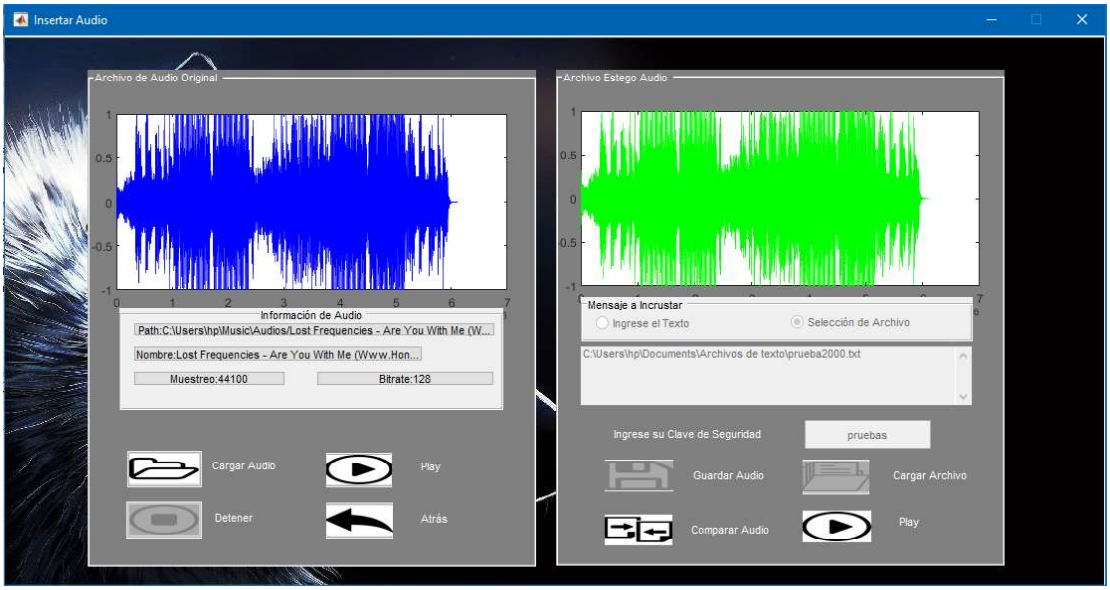


Figura A.19 Creación del nuevo estego-audio creado

Al presionar el botón de “Comparar Audio” se desplegará una nueva interfaz, en la cual, el usuario podrá identificar la diferencia de forma visual entre el audio original y el estego-audio, además, existirá una comparación respecto a las componentes de potencia de los audios mencionado, y la diferencia de valores en el campo datos del audio resultante (Ver Figura A.20).

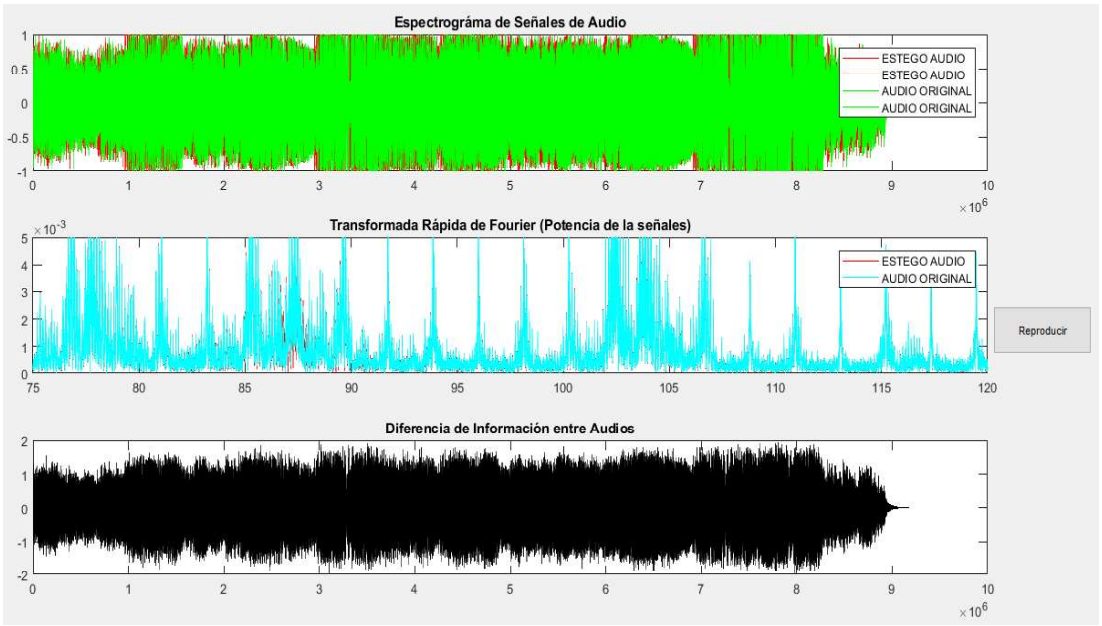


Figura A.20 Comparación entre audio original y estego-audio

Al presionar el botón reproducción, el usuario podrá escuchar el ruido que genera la información incrustada en el estego-audio.

d. OBTENCIÓN DE LA INFORMACIÓN OCULTA

Para la parte de obtención del mensaje oculto, desde la interfaz de inicio al presionar el botón “Obtención del Mensaje”, se desplegará la ventana mostrada en la figura A.21, allí el usuario visualizar una interfaz muy similar a la de ocultamiento del mensaje, pero con la diferencia que en el panel derecho servirá para la obtención del texto incrustado en el audio portadora. como en el paso anterior debe cargar un estego-audio MP3 desde el ordenador, al presionar el botón “Cargar Audio” se desplegar una ventana de navegación en la que podrá elegir el estego-audio MP3 deseado (Ver Figura A.22).

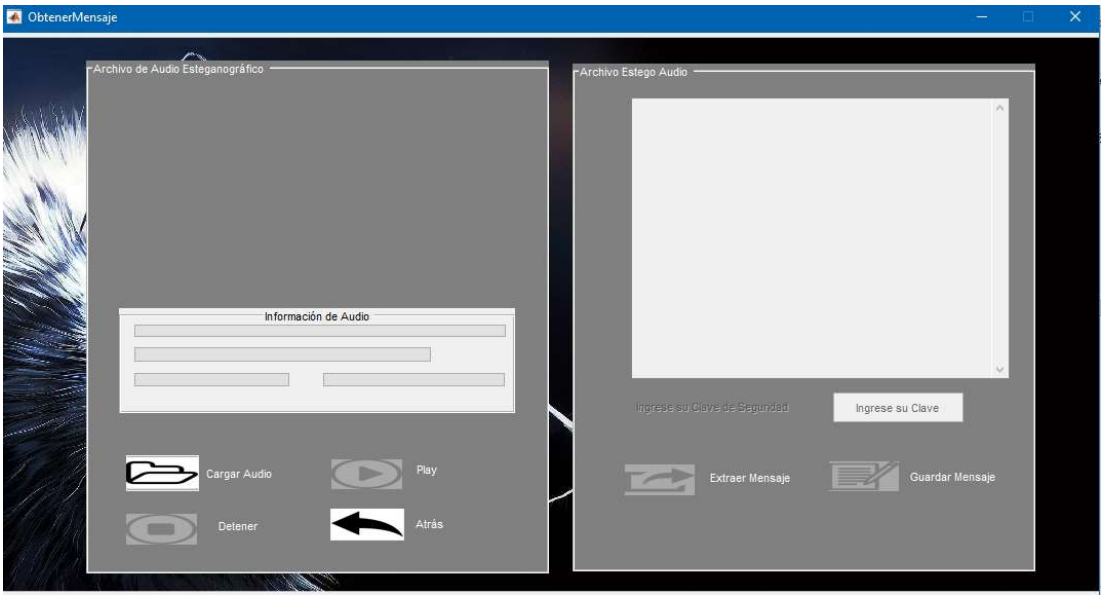


Figura A.21 Interfaz obtención del mensaje para realizar la recuperación del mensaje oculto

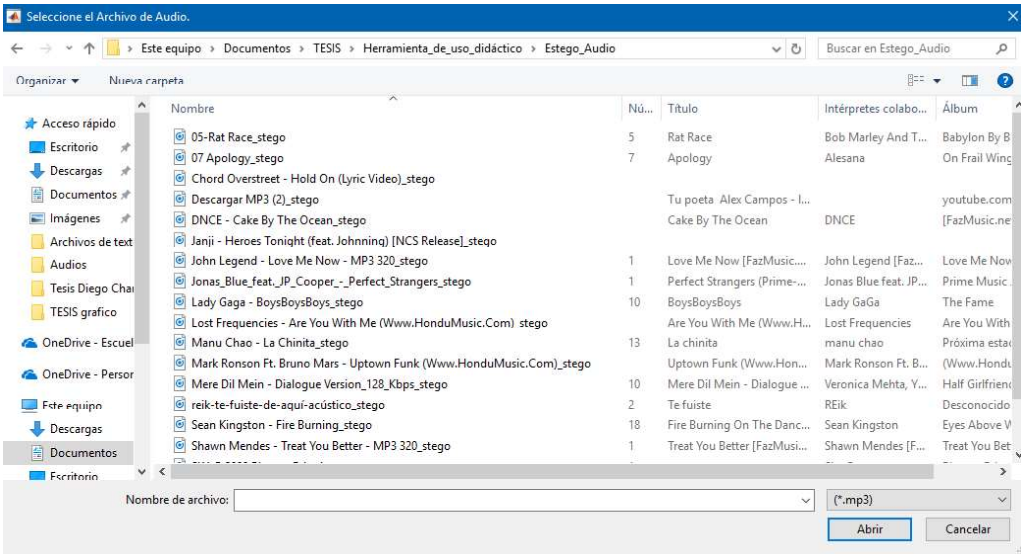


Figura A.22 Interfaz obtención del mensaje para realizar la recuperación del mensaje oculto

Una vez seleccionado el estego-audio, se lo presenta de la misma forma que en la interfaz de ocultamiento, donde, el usuario verificará la información que posee este archivo de audio; además se habilitará el cuadro de texto (Ver Figura A.23). en el cual el usuario podrá ingresar la clave con la que fue encriptado el mensaje. Cabe recalcar que de haber coincidencia de la clave con la que se encripto se mostrara un mensaje indicando que la clave es incorrecta o el archivo de audio se encuentra corrupto y no podrá visualizar la información (Ver Figura A.24)

Figura A.23 Cuadro de texto para ingresar la clave

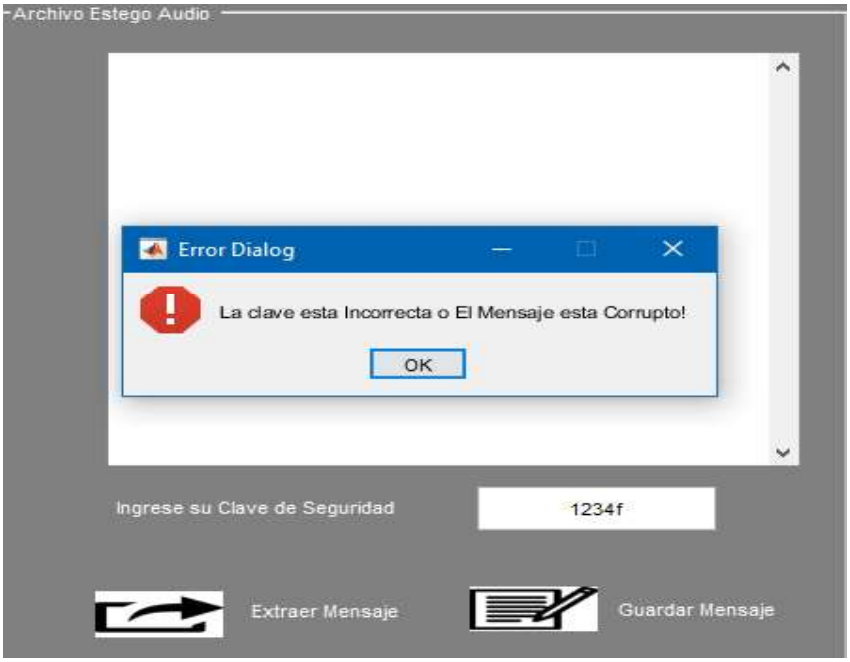


Figura A.24 Mensaje de notificación de clave incorrecta o mensaje corrupto

Al final el proceso de recuperación el mensaje será mostrado para que el usuario lo pueda visualizar; del mismo modo se habilitara el botón “Guardar Mensaje” (Ver Figura A.25), el cual al ser presionado mostrará un cuadro de dialogo, el cual permitirá al usuario guardar el contenido del mensaje recuperado, por defecto tiene el nombre de “archivo_de_audio.txt” (Ver Figura A.26).

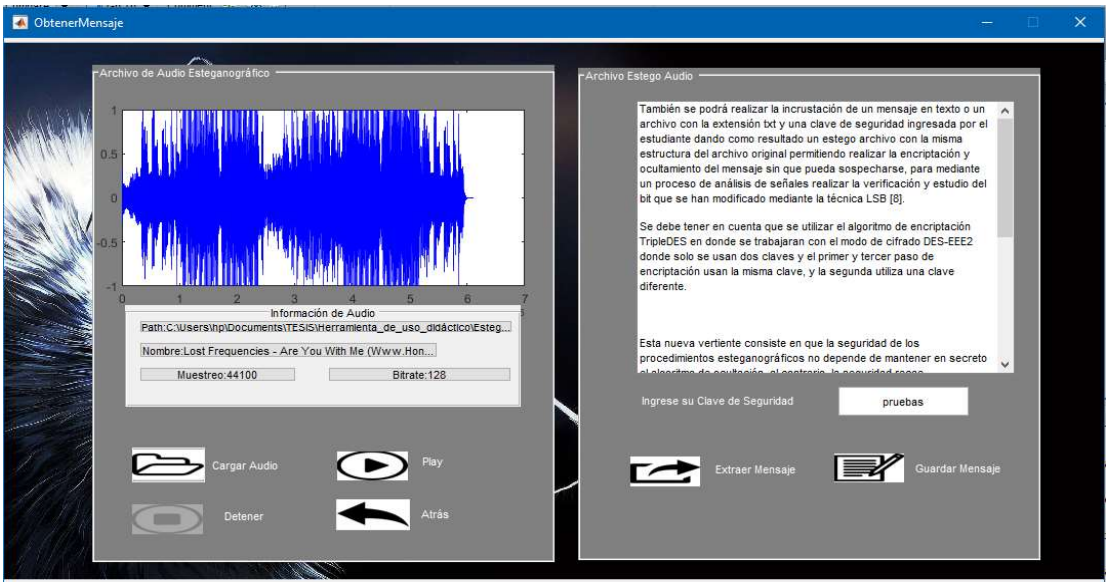


Figura A.25 Visualización del mensaje recuperado en la Interfaz

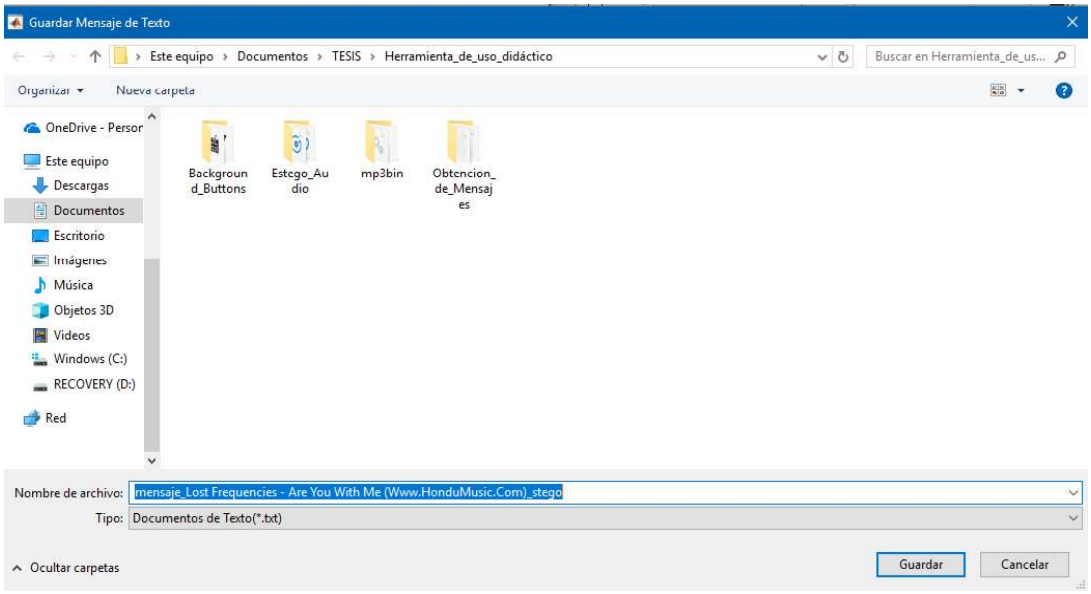


Figura A.26 Cuadro de dialogo para Guardar el mensaje recuperado en un archivo de texto

Al momento en que el usuario guarde el archivo, podrá verificar su contenido ubicándose en la carpeta del ordenador en la que lo guardo, constatando que el texto recuperado es legible (Ver Figura A.27).

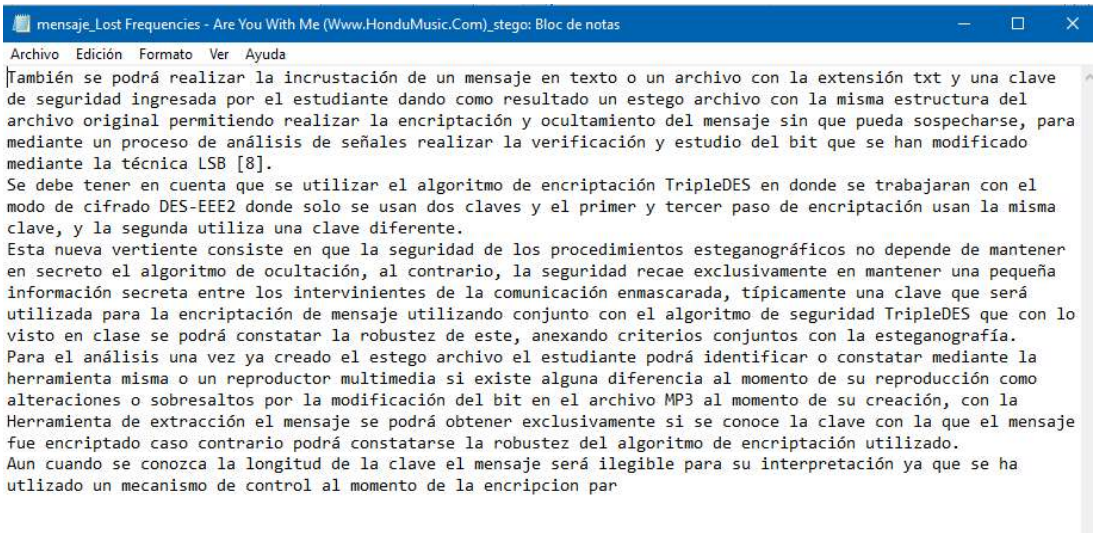


Figura A.27 Visualización del mensaje recuperado desde el archivo de texto guardado

ANEXO III.A

En la Tabla III.A se observa la valoración de las preguntas de la encuesta para determinar la calidad de los estego-audios creados.

(1) Malo (2) Regular (3) Bueno (4) Muy Bueno (5) Excelente

Tabla III.A Valoración de las preguntas de la encuesta

No. Encuesta	Audio 1	Audio 2	Audio 3	Audio 4	Audio 5	Audio 6	Audio 7	Audio 8
1	4	5	5	4	4	4	5	3
2	4	5	5	4	4	4	5	4
3	4	4	3	4	4	4	5	3
4	4	5	5	4	3	3	3	3
5	3	5	5	3	3	3	5	5
6	5	4	4	4	4	3	4	5
7	5	5	4	5	4	4	3	4
8	4	5	3	4	5	4	4	5
9	5	4	4	3	4	4	5	4
10	4	5	5	4	3	4	4	3

ANEXO III.B

En el Anexo III.C se incluyen los enlaces de la plataforma Google Forms de las encuestas realizadas a los 1o participantes para la valoración de la calidad de los estego-audios creados mediante la herramienta de uso didáctico.

- Preguntas: https://docs.google.com/forms/d/16oUnkPBb2hSe9r32mlhW3YGLuo-mCIKWcKErNg3LNVk/edit
- Respuestas: https://docs.google.com/forms/d/16oUnkPBb2hSe9r32mlhW3YGLuo-mCIKWcKErNg3LNVk/edit#responses

ORDEN DE EMPASTADO