APLICACIONES DE LA ESTEGANOGRAFÍA EN LA SEGURIDAD INFORMÁTICA

HÉCTOR FABIO VILLA ESTRADA

JUAN CAMILO JARAMILLO PÉREZ

UNIVERSIDAD TECNOLÓGICA DE PEREIRA

FACULTAD DE INGENIERÍAS

PROGRAMA INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

PEREIRA

2015

APLICACIONES DE LA ESTEGANOGRAFÍA EN LA SEGURIDAD INFORMÁTICA

HÉCTOR FABIO VILLA ESTRADA

JUAN CAMILO JARAMILLO PÉREZ

Trabajo de grado para optar al título de

Ingeniero de Sistemas y Computación

Director

Ing. Omar Ivan Trejos Buriticá

UNIVERSIDAD TECNOLÓGICA DE PEREIRA

FACULTAD DE INGENIERIAS

PROGRAMA INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

PEREIRA

2015

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

Firma del jurado

ÍNDICE

Contenido

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

En la presente investigación se pretende hacer un recorrido histórico de las principales aplicaciones de la esteganografía a la seguridad de la información. Métodos empleados por los griegos para comunicarse en medio de las guerras de modo secreto, el siglo XIV y las técnicas utilizadas por los prisioneros de la Santa Inquisición, los conflictos religiosos presentados en la Inglaterra del siglo XVI y las diferencias entre las hijas del rey Enrique VIII. El primer libro que utilizó en su vocablo la palabra esteganografía y las razones por las que la iglesia católica no lo aceptó, se describen además, métodos utilizados para ocultar información en partituras de música así como los utilizados por africanos para escapar de la esclavitud española. El siglo XX y la llegada de la segunda guerra mundial fueron fundamentales para la aplicación de técnicas esteganográficas.

La esteganografía moderna proporciona nuevos medios por los cuales transmitir información. La era moderna de la esteganografía utiliza recursos como imágenes, archivos de audio o video para ocultar información. Los campos de aplicación de la disciplina se expanden, además de los conflictos bélicos se tiene en cuenta técnicas de espionaje industrial, filtrado de información de carácter privado, implementación de software espía y las marcas de agua digitales para garantizar los derechos de autor.

CAPÍTULO I
1. GENERALIDADES

1.1 INTRODUCCIÓN

La esteganografía ha estado presente en nuestra civilización por muchas décadas, el arte de ocultar mensajes sin ser detectados ha despertado gran interés por entidades militares, de inteligencia o personas civiles con diferentes propósitos. La facilidad de encriptar información sin ser detectada en diferentes medios como imágenes digitales, archivos de audio o videos ha aportado técnicas para mejorar la seguridad de la información.

En este proyecto se pretende dar a conocer cómo la esteganografía se ha involucrado desde hace muchos años en la historia de la humanidad, desde la perspectiva de las tácticas militares hasta nuestro diario vivir, donde hoy en día se hace más evidente en transacciones comerciales con el proceso de firmas digitales e incluso en la clasificación de contenidos que pueden ser vistos por determinadas personas.

1.2 ANTECEDENTES

1.2.1 TRABAJOS DE INVESTIGACIÓN

Tesis 1:

Nombre del autor:

Diego Fiori de Carvalho

Nombre del artículo:

ESTEGANOGRAFIA EM VÍDEOS COMPRIMIDOS MPEG-4

Fecha de publicación:

2008

Resumen:

“La esteganografía en videos digitales posibilita el ocultamiento de un gran volumen de información cuando es comparada con las técnicas en imágenes. Sin embargo, esta tarea no es trivial cuando se aplica a videos comprimidos porque la inserción de información oculta puede adicionar ruido dificultando una perfecta recuperación de la misma durante la decodificación. Este trabajo presenta una técnica para la esteganografía en videos comprimidos, denominada MP4Stego, que explora las estructuras y tecnología de video estándar MPEG-4 con el fin de proceder con la recuperación de información sin perdida y presentar una mayor capacidad de inserción de datos ocultos. Entre los beneficios de esta técnica están: La capacidad de ocultación de grandes cantidades de datos; la capacidad de reproducir estos videos con datos ocultos en reproductores no especializados

(ayudando a dar la ilusión de que se trata de un video común), su inmunidad, hasta el momento, las técnicas de análisis en esteganografía".[1]

Discusión:

Con el objetivo de investigar algunas de las aplicaciones de la esteganografía en el campo de la seguridad de la información, resulta conveniente estudiar las técnicas utilizadas para el ocultamiento de información, en este caso se presenta un método para ocultar datos en videos comprimidos MPEG-4, la gran ventaja de este tipo de video es la gran eficiencia en la compresión de datos, esto posibilita guardar grandes cantidades de información donde la esteganografía puede tener un papel importante dependiendo del tipo de información que se desee guardar.

Tesis 2:

Nombre del autor:

Alexandre Henrique Afonso Campos

Nombre del artículo:

ESTEGANOGRAFIA DO PONTO DE VISTA DA TEORIA DOS CÓDIGOS

Fecha de publicación: 2014

Resumen:

"La esteganografía se convirtió en un tema muy importante en el estudio de seguridad de la información. Cuando se relaciona con la Teoría de Códigos, que fue bien desarrollada, la investigación sobre este tema aumentó rápidamente. En este trabajo, vamos a introducir a la esteganografía y vamos a demostrar cómo la

[1] Diego Fiori de Carvalho. Esteganografia Em Vídeos Comprimidos MPEG-4. Disponible en: < http://www.teses.usp.br/teses/disponiveis/55/55134/tde-08062009-143448/ > [citado el 15 de Octubre de 2015]

Teoría de Códigos puede ayudar en su estudio; códigos perfectos estarán relacionados con tipo de stegoscheme y vamos a ver el efecto de los códigos de papel húmedo en esteganografía".[2]

Discusión:

Uno de los problemas a los que se enfrenta la esteganografía es que al momento de aplicar la técnica se ingresen datos que no corresponden a la información original (ruido), al momento de decodificar la información se pueden perder o recibir datos incorrectos. La Teoría de códigos busca resolver este problema, es decir, trata de detectar y corregir este tipo de errores en la transmisión de la información. Es conveniente entonces, estudiar algunas de las ventajas y desventajas de la aplicación de la esteganografía y mitigar los posibles errores.

Tesis 3:

Nombre del autor:

Samuel Oliveira de Azevedo

Nombre del artículo:

SISTEMA DE AGENTES POLIGÍNICOS PARA ESTEGANÁLISE DE IMAGENS DIGITAIS

[2] Alexandre Henrique Afonso Campos. Esteganografia Do Ponto De Vista Da Teoria Dos Códigos. Disponible en: < http://www.bdtd.ufu.br//tde_busca/arquivo.php?codArquivo=5481 > [citado el 15 de Octubre de 2015]

Fecha de publicación:

2007

Resumen:

“En este trabajo, se propone un sistema multi-agente para el estogoanálisis en imágenes digitales, basado en la metáfora de abejas polínicas. Este enfoque tiene como objetivo resolver el problema del autómata de estogoanálisis para medios digitales, con el caso de estudio para imágenes digitales. La arquitectura del sistema está diseñado no sólo para detectar si un archivo es o no sospechoso de tener un mismo mensaje oculto, sino también para extraer el mensaje o información al respecto. Varios experimentos fueron realizados cuyos resultados confirmaron una mejora sustancial (67% a 82% de accesos) con el uso del enfoque multi-agente, que no se observó en otros de los sistemas tradicionales. Una aplicación actualmente en curso con el uso de la técnica es detección de falla en datos digitales producidos por los sensores que capturan las emisiones cerebrales en animales pequeños. La detección de tales anomalías se puede utilizar para probar las teorías y las imágenes de pruebas complementarias durante el sueño, proporcionada por las áreas visuales del cerebro en la corteza cerebral”.[3]

Discusión:

[3] Samuel Oliveira de Azevedo. Sistema De Agentes Poligínicos Para Esteganálise De Imagens Digitais. Disponible en: < http://repositorio.ufrn.br:8080/jspui/handle/123456789/17965 > [citado el 15 de Octubre de 2015]

Es de importancia esta tesis en la participación de nuestro proyecto, ya que es muy importante conocer las diferentes aplicaciones de la esteganografía en la seguridad de la información, en este caso por medio del estogoanálisis permite la detección de información oculta. La esteganografía es un campo abierto a diferentes materias, los métodos heurísticos por ejemplo, son utilizados como herramienta adicional en la búsqueda de información representada en "*anomalías*" que pueden presentar las imágenes digitales.

Tesis 4:

Nombre del autor:

Jinnett Pamela Carrión Casierra

Nombre del artículo:

IMPLEMENTAÇÃO DE UM SISTEMA ESTEGANOGRÁFICO PARA INSERÇÃO DE TEXTOS EM SINAIS DE ÁUDIO

Fecha de publicación:

2009

Resumen:

"El arte de esconder un mensaje dentro de otro objeto se conoce como Esteganografía. Son técnicas convencionales detalladas para ocultar mensajes que propone un nuevo enfoque. Este nuevo método de esteganografía en dos pasos combina un texto completo cifrado a través de un criptosistema estándar, esto seguido de la inmersión de datos cifrados en un archivo de audio. El trabajo se centra en la inclusión de textos breves en archivos con formato wav. La entrada de los datos es realizada por los componentes que resultan de la transformación

de la señal por las transformadas de Wavelet. El objetivo es introducir datos casi transparente, de modo que la detección por terceros sea poco probable, como también para asegurar que la recuperación prácticamente no altere los datos. Los audios se descomponen en doce niveles por la elección de una madre Wavelet, los datos se encriptan y ocultan en los diferentes niveles de acuerdo a la discreción del usuario. Para una mejor dispersión de datos en cada nivel se utilizan contraseñas alfanuméricas de tamaño proporcional a la cantidad de caracteres introducidos en cada uno de los niveles. La implementación computacional se realizó en Matlab y las simulaciones se hicieron con archivos de audio con tamaños diferentes, obteniendo de esta manera la tasa de cambio porcentual del archivo de sonido. La esteganografía basada en este esquema, puede ser desarrollada en aplicaciones de negocio para garantizar la autenticidad de los archivos, así como protección de los derechos de autor a los archivos digitales".[4]

Discusión:

La esteganografía puede ser utilizada tanto para descifrar información como para ocultar mensajes depende del uso que se le quiera dar, esta investigación resulta importante en la realización de nuestro proyecto ya que describe una de las técnicas que mediante las transformadas de Wavelet ayudan en la inserción de información en archivos de audio. Una de las características importantes que debe tener cualquier sistema esteganográfico es prevenir que se puedan alterar los datos, en este trabajo se describe como se oculta esta información, el tipo de contraseñas que son utilizadas en la encriptación así como las diferentes aplicaciones en el que este tipo de sistemas puede resultar útil.

[4] Jinnett Pamela Carrión Casierra. Implementação De Um Sistema Esteganográfico Para Inserção De Textos Em Sinais De Áudio. Disponible en: < http://repositorio.ufpe.br:8080/xmlui/handle/123456789/5409 > [citado el 15 de Octubre de 2015]

1.3 DESCRIPCIÓN GENERAL DEL PROBLEMA

La esteganografía como aparece en [1] busca ocultar información en diferentes medios de transmisión de datos, desde la antigüedad se ha visto el desarrollo de esta técnica, buscando guardar en secreto mensajes que sólo podían ser relevados a un grupo de personas que supieran la técnica que se estaba usando, haciendo uso de diferentes canales de comunicación se lograban esconder tácticas, secretos, estrategias ante los ojos de las demás personas.

En este trabajo se explicará la importancia de este término en la actualidad y los aportes que ha hecho a la historia esta técnica, ya que, forma parte importante en lo que concierne con seguridad informática, tomado de [2] “la esteganografía, bien usada, resulta prácticamente imposible de descubrir, e incluso entonces, si de nuevo se han utilizado técnicas avanzadas y cruzadas (diferentes estegos en diferentes fuentes necesarios para comprender el mensaje), posiblemente sea casi indescifrable.”. Así pues, la esteganografía está presente en cualquier lugar de la web pero pasa desapercibida para nosotros.

1.4 JUSTIFICACIÓN DEL PROYECTO

Teniendo en cuenta los pasos agigantados que está dando la tecnología, queremos dar un aporte mediante nuestro trabajo, sobre cómo opera la seguridad de la información “detrás de cámaras”, cómo funciona esta técnica, cuáles herramientas existen en el momento y de qué manera nos pueden servir.

De esta forma, es importante conocer la historia, cómo llegó a tomar importancia la esteganografía que tiene en este momento y qué importancia tendrá en el futuro debido a que cada vez son más los negocios vía Internet, mensajes secretos de gobierno e incluso consultas que hacemos diariamente a entidades bancarias.

Por lo tanto la esteganografía hace parte fundamental de la seguridad de la información, si bien de [3] podemos tomar que no existe un sistema el cual sea 100% seguro, siempre habrá un riesgo presente y por esto se debe implementar seguridad, es decir, de cualquier modo esta práctica logra fortalecer la seguridad en un sistema de información.

En resumidas cuentas la esteganografía permite transmitir información de manera imperceptible, enviar cantidades razonablemente altas de información, no ser necesariamente robusta ante modificaciones y a través de un medio diseñado para transmitir otro tipo de información [4], otorgando de esta manera, una capacidad enorme a esta disciplina.

Haciendo hincapié en [5] “Si bien la esteganografía suele confundirse con la criptografía, por ser ambas parte de los procesos de protección de la información, son disciplinas bastante distintas, tanto en su forma de implementar como en su

objetivo mismo.” es importante establecer las diferencias entre estas disciplinas, del mismo modo, se explicará cómo pueden complementarse, dando un nivel de seguridad extra a la información.

1.5 OBJETIVOS DEL PROYECTO

1.2.2 OBJETIVO GENERAL

Presentar los avances de la esteganografía en diferentes áreas del conocimiento a lo largo de la historia de la humanidad y la manera como ha incidido en la seguridad de la información.

1.2.3 OBJETIVOS ESPECÍFICOS

- Agrupar los principales avances que la esteganografía ha aportado a la humanidad a través del tiempo.
- Explicar de qué manera esta técnica incide en la seguridad de la información.

1.6 MARCO REFERENCIAL

1.2.4 MARCO TEÓRICO

“La seguridad ha pasado de utilizarse para perseverar los datos clasificados del gobierno en cuestiones militares o diplomáticas, a tener una aplicación de dimensiones inimaginables y crecientes que incluye transacciones financieras, acuerdos contractuales, información personal, archivos médicos, comercio y negocios por Internet, domótica, inteligencia ambiental y computación ubicua. Por ello, se hace imprescindible que las necesidad de seguridad potenciales sean tenidas en cuenta y se determinen para todo tipo de aplicaciones.”[6], es allí donde se quiere enfocar este proyecto, en la necesidad de la humanidad de tener bajo

llave sus datos y para esto es necesario conocer de forma detallada el concepto de seguridad de información o seguridad informática partiendo de los 4 niveles básicos de seguridad los cuales se muestran en la Tabla 1 [7].

Nivel	**Especificación**
Aplicación	Es lo que ve el usuario. Es el nivel más complejo y el menos fiable. La mayor parte de los fraudes informáticos ocurren en este nivel.
Middleware	Implicados los sistemas de gestión de BD y la manipulación del software.
Sistema operativo	Se trata la gestión de ficheros y las comunicaciones.
Hardware	Es el nivel menos complejo y más fiable. Características de seguridad en las CPU y en el hardware (ejemplo, para evitar desbordamientos de búffer o pila).

Tabla 1. Niveles básicos de seguridad

De esta manera, podemos enmarcar este proyecto en el nivel de aplicación de los niveles básicos de seguridad de la información, ya que, es dónde debemos ocultar dicha información por sus antecedentes de elevados número de fraudes informáticos que se presentan a través de la web.

Según [8] el 80% de los fraudes bancarios son el 80% de los ciberdelitos y Colombia es uno de los 4 países más afectados en Latinoamérica; un estudio realizado en República Dominicana arrojó los siguientes resultados:

Figura 1. Cantidad de reclamaciones de transacciones fraudulentas de usuarios de los servicios financieros en República Dominicana. Fuente: El autor

Si se observa la figura anterior no existe duda de que los avances tecnológicos hacen que la inseguridad en la Internet aumente notoriamente año tras año, el aumento entre octubre de 2010 y octubre de 2013 asciende a unos 549 casos reportados de transacciones fraudulentas a través de la red.

1.7 MARCO CONCEPTUAL

Esteganografía: Del griego *steganos* (oculto) y *graphos* (escritura), la esteganografía se puede definir como la ocultación de información en un canal encubierto con el propósito de prevenir la detección de un mensaje oculto [9].

Criptografía: Es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet [10].

Objeto contenedor: Se trata de la entidad que se emplea para portar el mensaje oculto [9].

Estego-objeto: Se trata del objeto contenedor más el mensaje encubierto [9].

Adversario: Son todos aquellos entes a los que se trata de ocultar la información encubierta [9]**.**

Estego-análisis: Ciencia que estudia la detección (ataques pasivos) y/o anulación (ataques activos) de información oculta en distintas tapaderas, así como la posibilidad de localizar la información útil dentro de la misma (existencia y tamaño) [9].

1.8 DISEÑO METODOLÓGICO

A continuación se describe como se llevará a cabo la investigación, los métodos utilizados y las técnicas utilizadas para la recolección de información.

1.2.5 FORMA DE INVESTIGACIÓN

Uno de los objetivos de la presente investigación es reunir los avances más significativos que la esteganografía ha contribuido a la humanidad, consideramos que es una investigación básica ya que la recolección de información es la base para profundizar en los conocimientos existentes y es indispensable para lograr dicho objetivo. Es importante además conocer los antecedentes para generar nuevos criterios que contribuyan al crecimiento de la investigación.

1.2.6 TIPO DE INVESTIGACIÓN

La esteganografía es un tema que ya se ha venido trabajando hace algún tiempo, en el campo de la informática se han hecho algunas aplicaciones. La presente investigación es de carácter descriptivo ya que se pretende explicar de qué manera esta técnica incide en la seguridad de la información además de los principales avances y aportes que ha hecho a la humanidad y en especial a las ciencias de la computación, lo que desafía a identificar las propiedades más importantes del tema estudiado.

1.3 METODO DE INVESTIGACIÓN

En la presente investigación se pretende partir de la recolección de información para así proceder a la deducción y análisis de los datos, por esta razón se recurre a métodos de investigación teóricos que sirvan como medio para identificar y analizar las propiedades más importantes de la esteganografía como base para contribuir al avance y estudio del tema en cuestión.

1.3.1 FUENTES, TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Tanto las fuentes como las técnicas e instrumentos de recolección de la información se consideran importantes en el desarrollo de la investigación, se obtiene información de fuentes secundarias como libros, documentos y estadísticas de investigaciones ya hechas por otros investigadores teniendo en cuenta la normatividad legal vigente para evitar el plagio de información. Después de la recolección de información se procede al análisis del contenido adquirido, si es necesario se hace uso de herramientas como videos o audios que permitan un mejor entendimiento y si sirvan como aporte ante posibles inquietudes que surjan en la realización de la investigación.

1.9 ESQUEMA TEMÁTICO

RESUMEN

CAPÍTULO I

1. GENERALIDADES

1.1 INTRODUCCIÓN

1.2 ANTECEDENTES

1.3 DESCRIPCIÓN GENERAL DEL PROBLEMA

1.4 JUSTIFICACIÓN DEL PROYECTO

1.5 OBJETIVOS DEL PROYECTO

1.6 MARCO REFERENCIAL

1.7 MARCO CONCEPTUAL

1.8 DISEÑO METODOLÓGICO

1.9 ESQUEMA TEMÁTICO

CAPÍTULO II

2. ESTADO DEL ARTE

CAPÍTULO II
2. ESTADO DEL ARTE

Actualmente la esteganografía se encuentra muy ligada con delitos informáticos del presente, en un reciente artículo [11] el cual ha sido muy controversial por la popularidad de este crimen que data del año 2010 explica como hace unos años el FBI logró después de varios años de investigación detener a varios espías rusos que hacían contacto a través de fuentes públicas (blogs, periódicos, foros, redes sociales), logrando pasar información sin ser percibida por las personas que diariamente utilizaban esta red de comunicación a la vista de todos, algo para tener en cuenta, es que toda la red de espías no fue descubierta hasta que uno de los detenidos señaló al resto de implicados en este delito.

Figura 2. En dónde se ve la esteganografía. Fuente: el autor

De esta manera, se puede ver como la esteganografía llevada a un nivel más alto se vuelve casi imposible de descubrir incluso para organismos especializados, a continuación se detallará el estado del arte de esta disciplina, lo que se ha alcanzado hasta el momento aplicando este arte y de qué manera ha cambiado la historia de la seguridad de la información, obligando a muchas personas a reforzar su conocimiento sobre este tema, para el mejoramiento de seguridad de transacciones en su negocio y/o vida diaria, para evitar los tan distinguidos fraudes informáticos.

Figura 3. Deep Web. Fuente: el autor

“En la última década, se ha observado una intensa labor de investigación relacionada con la esteganografía y sus métodos de detección (esteganálisis). Esto ha sido provocado por dos hechos: primero, empresas interesadas en DRM (Digital Rights Management) y en segundo lugar, la utilización de los métodos

esteganográficos por terroristas por ejemplo para la planificación de los ataques a Estados Unidos el 11 de septiembre de 2001. Los organizadores utilizaron imágenes para ocultar instrucciones, que posteriormente se publicaron en Internet.”. Según este fragmento tomado de [12] en el atentado realizado el 11 de septiembre, uno de los principales atentados de la historia de la humanidad, fue posible gracias a la esteganografía, transmitiendo imágenes con información acerca del delito puestas en imágenes de pornografía infantil, con el fin de dar pistas de cómo iban a ser ejecutadas estas instrucciones.

“Es importante comentar la conciencia y la forma de pensar que tienen las personas y las sociedades en general. A los gobiernos nunca les han hecho demasiada gracia la criptografía, esteganografía, etc. y, en general, cualquier método que pueda suponer datos fuera de su control. Gracias a los ordenadores personales y al software libre en gran medida, técnicas antes reservadas a unos pocos están ahora al alcance de cualquiera, hasta de las peores personas.” [13].

Figura 4. Atentado torres de gemelas. Fuente: el autor.

Muchos de los acosos informáticos, se logran ejecutar gracias al desconocimiento de esta técnica de los grandes gobiernos e incluso de personas que hacen uso de la internet como principal medio de comunicación, su principal contacto con su trabajo o incluso hasta su principal ingreso cuando de dinero se trata, también es importante saber que esta técnica y el conocimiento que se puede adquirir sobre ella en cualquier lugar de la internet no es privado para ninguna persona, depende de cada persona el uso que le quiera dar a esta disciplina.

Así pues, se puede ver cómo la esteganografía, en su mayoría de veces es usada con fines negativos para la sociedad y que oculta macabras situaciones, otro ejemplo “el caso de la "Operation Twins", que culminó en 2002 con la captura de delincuentes relacionados con "Shadowz Brotherhood", una organización pedófila responsable de la distribución de pornografía infantil mediante esteganografía.” [14].

Y es que esta técnica siendo bien usada podría generar grandes problemas o desarrollos para la humanidad, según un reciente proyecto que habla sobre un informe Federal publicado en el 2006 por parte de EEUU [15], la esteganografía es tildada como una de las principales amenazas crecientes en la web, de las cual se espera un crecimiento exponencial en los próximos años –el cual se está viendo en este momento- y es tanto la importancia que hoy muestran los gobiernos que una de las soluciones que plantean es “para mitigar los riesgos asociados a esta técnica es conocer la evolución de la esteganografía y, en consecuencia, predecir su desarrollo futuro.” [15], de esta disciplina que se empezó a ganar popularidad a partir del año 1980.

“Ya no es tan necesario desplazar agentes secretos a otros países, falsificar pasaportes o disfrazarse para no ser reconocido. Ya no hay que jugarse el pellejo colándose en la noche esquivando sistemas de alarma y seguridad en la sede presidencial o alguna empresa tecnológica para robar documentos. No solo la guerra se libra en internet, sino en sus aspectos más "2.0".”[16].

Se conoce de un grupo llamado APT29 los cuales usan redes sociales, más concretamente twitter, para lograr los objetivos, mediante una aplicación llamada “Hammertoss” la cual genera códigos que conducen a imágenes que han pasado por el proceso de ocultación para posteriormente ejecutar instrucciones en el ordenador que se quiere espiar, a continuación una imagen que muestra cómo se realiza este proceso.

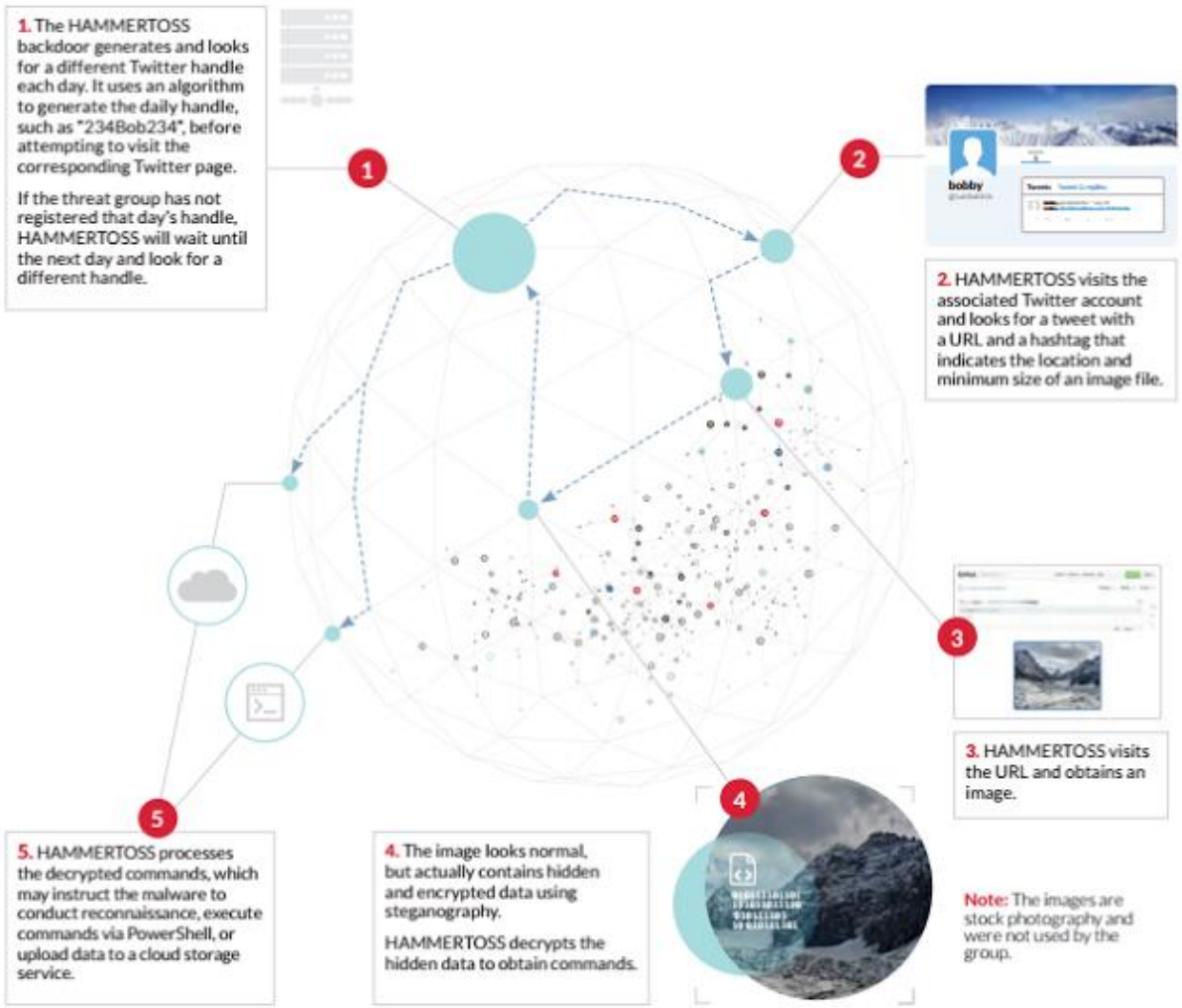

Figura 5. Herramienta Hammertoss. Fuente: el autor

Este proceso finaliza cuando la víctima sin ninguna aprobación está trasmitiendo información de su computadora a la nube de una persona que puede consultar todo lo que realiza.

El malware es un técnica esteganográfica que es utilizada en la actualidad con frecuencia. La capacidad de ocultar programas sofisticados dentro de publicidad por ejemplo, con el objetivo de robar información importante o en ocasiones

buscan objetivos codiciosos como robo de cuentas bancarias o se conocen casos en los que toda la producción de una compañía se ha tenido que parar por culpa de estos virus.

La capacidad de obtener paquetes de información que viajan por la red se ha ido perfeccionando por parte de terceros que buscan acceder a información privada con el fin de infectar computadores y robar información o también como una herramienta de comunicación entre organizaciones criminales.

Figura 6. Virus informáticos. Fuente: el autor.

Cada día aparecen nuevos tipos de virus informáticos, se observa con normalidad que los exploradores de internet son sometidos por este tipo de malware. Adware

es tipo de programa cuya tarea consiste en mostrar mensajes publicitarios por medio de ventanas emergentes y de esta forma robar la atención del usuario. Lo que se desconoce es que este tipo de avisos la mayoría de veces contienen ocultos programas especializados capaces de robar información del ordenador o causar serios daños en el mismo.

Dado que la naturaleza de la esteganografía proviene de investigaciones hechas por entes no criminales, hasta el momento no se sabe en qué cantidad se ha extendido el malware en internet. Lo que se hasta el momento se ha podido tener conocimiento se obtiene de ataques como por ejemplo el robo de datos financieros al Departamento de Justicia de los Estados Unidos en 2008 como lo indica [17].

Archivos Ejecutables

En la actualidad, los mecanismos de esteganografía se enfrentan a un reto y es que la cantidad de información que se puede ocultar en un medio digital como una fotografía, archivo de audio o video se encuentra limitada. Un equipo de investigación hindú liderado por dos científicos informáticos Rajesh Kumar y G. Sahoo, ha desarrollado un algoritmo que es capaz de ocultar información en archivos ejecutables mediante técnicas de esteganografía, de esta manera poder almacenar ocultar grandes cantidades de información en archivos ejecutables según [18].

En estudios realizados anteriormente, solo se podía encubrir cierta cantidad de información, lo que se convertía en una falencia de utilizar estos mecanismos, según los autores se elimina esta limitación además de poder utilizar esta tecnología en diferentes tecnologías como computadoras, teléfonos inteligentes y cualquier otro dispositivo en el que usuario desee ocultar información.

Cuando se oculta gran cantidad de información en archivos de audio, imágenes o video, el tamaño de dicho archivo se ve afectado en gran medida que podría levantar sospechas, motivando a terceros a buscar que la información contenida en el archivo.

Los archivos ejecutables por lo general si su tamaño incrementa no genera tanta desconfianza en el usuario, estos a la vez contienen muchos información basura lo que se puede aprovechar para adjuntar gran cantidad de información importante que se desee ocultar sin levantar ningún tipo de sospecha.

Seguridad de la Información

La seguridad de la información ha sido un tema que en los últimos años se le ha puesto más importancia debido a los constantes ataques y pérdida de información clasificada para algunos países. En el 2010, Bradley Manning, analista de inteligencia del ejército estadounidense pudo filtrar a Wikileaks, miles de documentos clasificados sobre la guerra en Afganistán como indica [19]. Este hecho fue tan grave que llevo a ejecutar reformas estructurales en cuanto al sistema de seguridad de la información en aquel país.

La Agencia Nacional de Seguridad (ANS) del gobierno de los Estados Unidos, encargada de toda la seguridad de la información, donde anteriormente laboraba Edward Joseph Snowden un consultor estadounidense a quien se le atribuye hizo públicos documentos secretos sobre varios programas de la NSA organización que más tarde reconoció la imposibilidad de identificar el número exacto de documentos filtrados por Snowden, llevo a crear una Orden Ejecutiva con el fin de volver a reestructurar el sistema de seguridad de la información en EEUU.

Gracias a los avances tecnológicos y a nuevos métodos para ocultar y en este caso filtrar información, a llevando a países como Estados Unidos que se ha visto envuelto en escándalos por espionaje, a tomar medidas para mejorar la seguridad de la información. En la actualidad es un tema al que la mayoría de organizaciones, no solo las que forman parte del gobierno, ha puesto especial atención y obligado a blindarse contra perdida de información y cumplir con rigurosas normas de seguridad.

CAPÍTULO III
3. ANTECEDENTES DE LA ESTEGANOGRAFÍA

La necesidad de ocultar información sin que sea detectada utilizando algún tipo de “cubierta” ha sido un problema o mejor aún un reto al que muchas personas a través de la historia se han preocupado en resolver ingeniando métodos o técnicas para dar solución. Estas técnicas han sido empleados para transportar algún tipo de información con el objetivo de que ésta no sea detectada. Los principales escenarios en los que se ha utilizado la esteganografía han sido en la guerra, política y actualmente en el campo informático que se ha encontrado especial utilidad. A continuación se pretende hacer un recorrido histórico desde la esteganografía clásica hasta la era moderna donde se utilizan medios digitales.

3.1 ESTEGANOGRAFÍA CLÁSICA

La esteganografía no es un tema actual, ya se ha venido trabajando desde hace mucho tiempo, en la antigüedad por ejemplo, el uso de la esteganografía en un contexto de guerra era vital para decidir el rumbo de la misma, un mensaje que no fuera detectado por el enemigo podía cambiar las reglas del juego, ya fuera para defenderse de un futuro ataque o como motivo para proceder en las operaciones de guerra.

El origen de la esteganografía no se sabe muy bien, pero las primeras aplicaciones de esta disciplina datan desde antes del siglo XV [20] en la Grecia Antigua, época en la que eran muy comunes las guerras con fines territoriales o religiosos. La esteganografía ha venido en constante evolución hasta los tiempos modernos. La principal diferencia es que para la época antigua no se utilizaban medios digitales comparada con la época actual.

"La esteganografía clásica o pura se puede definir como todo aquel conjunto de métodos de ocultación, que se mantienen en secreto, que permiten esconder un mensaje aprovechándose de un canal específico o tapadera, habitualmente la tapadera utilizada es desconocida para el potencial atacante." [21]

La base de la estenografía radica en que el posible atacante no conozca el medio que sirve como cubierta para proteger el mensaje. Desde la antigüedad se ha demostrado el éxito al utilizar este tipo de métodos sin que el enemigo sepa cómo o por medio de qué mecanismo se transporta la información.

3.1.1 La Guerra en la Antigua Grecia

A continuación se presenta detalladamente las principales aplicaciones de la esteganografía en la antigüedad y quienes han sido los principales interesados o ingeniosos que se han tomado la tarea de concebir nuevos métodos o "trucos" para transportar información sin que ésta sea revelada.

Uno de los principales referentes de la esteganografía clásica es Heródoto de Helicarnaso, fue un historiador que vivió aproximadamente en el siglo V antes de Cristo en Grecia [22]. A él se le atribuyen los primeros aportes en cuanto a narraciones donde cuenta implícitamente se aplicaba la técnica de la esteganografía. Escribió un libro llamado "historias" donde en varias ocasiones describe ejemplos en los que se utilizaba esta técnica para transportar mensajes sin que fueran interceptados.

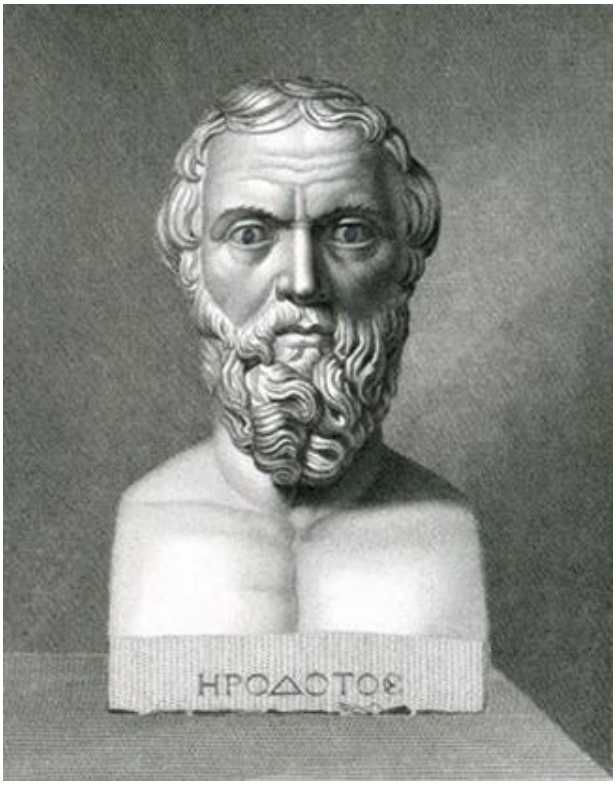

Figura 7. Herótodo, historiador griego. Fuente: el autor.

La guerra en la Antigua Grecia se convirtió en el escenario apropiado para que Heródoto realizara su trabajo como historiador. Las antiguas polis griegas en ocasiones entraban en guerra por cuestiones políticas, religiosas o comerciales. Por ejemplo la guerra presentada entre Atenas y Esparta duró alrededor de 30 años. No era muy conveniente que se presentaran este tipo de disputas entre los mismos griegos quienes en ocasiones se olvidaban de sus diferencias para unirse como aliados y luchar contra su principal enemigo, el rey Jerjes, rey del Imperio Persa, como lo describe [23].

Este tipo de guerras eran muy comunes para la época, donde el imperio Persa buscaba someter a Grecia y formar un solo imperio, las pequeñas ventajas sobre el enemigo podían ser fundamentales para obtener la victoria. Heródoto describe en su libro “historias”, como se transmitió tal vez el mensaje más importante, sin

que fuese descubierto, en la Antigua Grecia. Cuenta en su libro, que Demarato un antiguo rey de Esparta fue obligado a abandonar Grecia, acusado de medismo, ya que el aceptaba la supremacía de los Persas. Demarato obligado a vivir en Persia se enteró que el rey Jerjes estaba planificando un futuro ataque a Grecia rearmando su ejército.

No se tiene gran certeza cuál fue la razón por la que Demarato ingenió un método para transmitir un mensaje sin que los persas se dieran cuenta y pudieran interceptarlo, fue un reto para él, ya que las requisas por parte de los guardias eran constantes sin embargo pudo filtrar el mensaje y de esta forma los griegos prepararse para el ataque y obtener la victoria.

El método empleado por Demarato consistía en escribir el mensaje en tablas de madera las cuales recubría con cera. Ya que en la época no existía papel ni otra herramienta más practica como las que existen en la actualidad, la técnica usada consistía en escribir directamente sobre la madera y luego taparla con la cera hasta que no se pudiera observar el mensaje. Cuando el mensaje logró llegar a los griegos, luego de pasar por muchos puestos de control, simplemente retiraron la cera y el mensaje quedó descubierto. Esta técnica para transportar un mensaje sin que fuese detectado fue tal vez lo que salvó a Grecia de que fuera sometida por Persia.

La siguiente figura describe una tablilla de madera donde se escribía en mensaje oculto bajo la cera.

Figura 8. Tablilla con mensaje oculto. Fuente: el autor

Heródoto describe otro modelo de esteganografía en su mismo libro, en esta ocasión hace referencia a Histieo, fue un general ateniense, quien planeaba derrocar del poder al rey de los persas. Para lograr este objetivo solicitó la ayuda de su yerno Aristágoras como lo describe [22], con el reto de diseñar un método para transportar la información sin que fuera descubierto, decide hacer rapar la cabeza a uno de sus esclavos para que de esta forma se le grave o “tatúe” un mensaje en su testa. Una vez hecho esto, esperaba que el cabello volviera a crecer y poder trasladarse sin levantar sospechas. Este mecanismo tuvo éxito, sin embargo no es muy eficaz si se necesita resolver el problema en corto tiempo. La antigua Grecia deja grandes aportes a la esteganografía que han servido de base para que más adelante se generaran nuevas metodologías y técnicas para transportar mensajes ocultos con diversos fines.

Alrededor de dos mil años después de que Heródoto describió en su libro *“historias”* hechos tan importantes para la evolución de la esteganografía, surge en la cultura china un mecanismo ingenioso para ocultar información.

3.1.2 Antigua China

Una de las civilizaciones más antiguas de la humanidad, donde el régimen de gobierno por muchos años fue basado en las dinastías. Para la época era común que se presentaran guerras en campañas de conquista. Esta cultura se destaca por sus aportes a la escritura como un medio de comunicación, en ocasiones era necesario transmitir mensajes muy importes, para esto escribían sobre seda muy fina que luego comprimían hasta formar una especie de esfera, una persona debía ingerir la pelota y trasladarse hasta el receptor del mensaje como lo menciona [22]. Fue un mecanismo incómodo para la persona que tenía que transportar el mensaje, pero se lograba objetivo, evitando la detección del mensaje.

3.1.3 Siglo XIV

Uno de los acontecimientos que marcó esta época fue la llamada Santa Inquisición, el nacimiento de movimientos impulsados por la iglesia católica con el objetivo de castigar la herejía, muchas veces castigada con la pena de muerte. El hereje era aislado de la comunidad y su familia era marcada como infame durante muchas generaciones como menciona [24]. La necesidad de comunicación para los prisioneros siempre ha sido un reto, especialmente en esta época la Inquisición era muy estricta en lo que se le entrega al prisionero, los mecanismos de control eran rigurosos para evitar el contacto del hereje con la sociedad. En el siglo XV Giovanni Battista della Porta un famoso filósofo e investigador italiano, describe en una de sus obras más importantes *“Magia Naturalis”* un método poco convencional, pero que arrojó muy buenos resultados. El mecanismo, sustenta [3],

consiste en utilizar un huevo duro para ocultar el mensaje que se desea entregar al prisionero. Aprovechando las características permeables de la cascara del huevo, se preparaba una mezcla de sustancias que fuera capaz de atravesar la corteza del huevo para posteriormente transcribir el mensaje. De esta manera y sin levantar sospechas de los guardas, los huevos se entregaban al prisionero quien al retirar el recubrimiento observaba el mensaje. Esta gran idea daría fuerza para el resurgimiento de uno de los aportes más significativos para la esteganografía, las llamadas “tintas invisibles” que más adelante se describen.

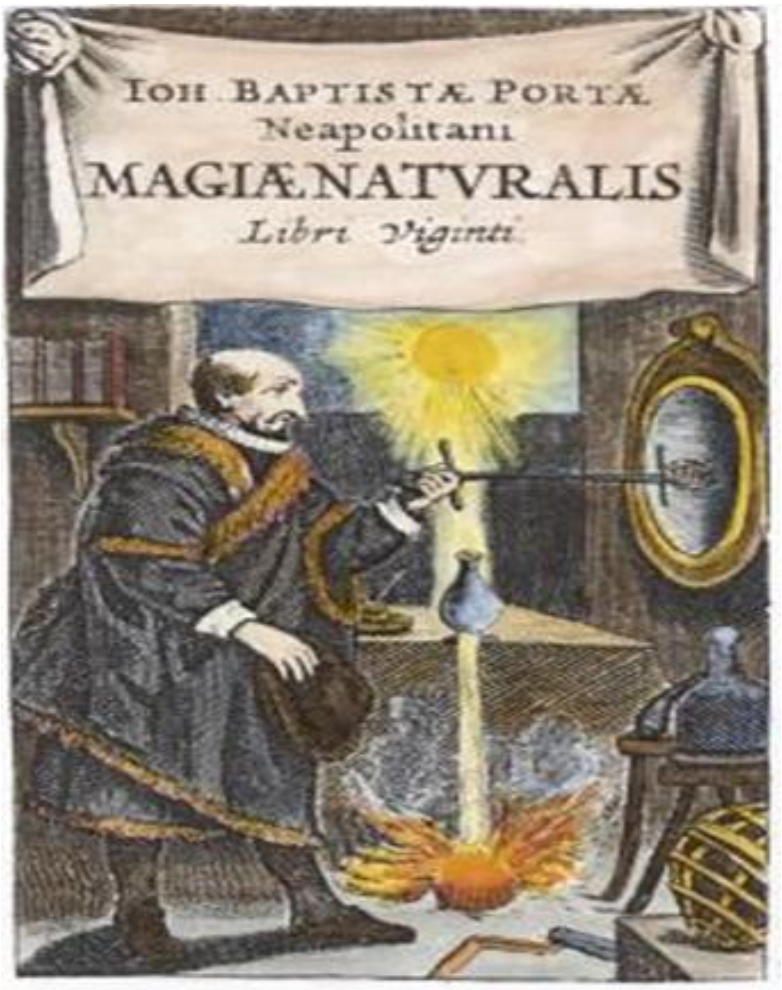

Figura 9. Portada Magia Naturalis. Fuente: el autor

Aunque el uso de tintas invisibles no es algo que para le época fuera nuevo, ya se había implementado desde mucho antes de la inquisición, se tenía conocimiento del aprovechamiento de jugos cítricos como la naranja o el limón para transcribir mensajes que no fueran perceptibles por el ojo humano. La única manera de descifrarlos era por medio de la exposición al calor o la luz.

Plinio el Viejo fue un escritor y naturalista italiano el siglo I antes de Cristo como lo indica [22]. Este escritor describe en una de sus obras más significativas que sobreviven hasta el día de hoy como recado del Imperio Romano cómo podía utilizarse la leche de algunas plantas como tinta invisible. La obra se llama *"Naturalis historia"* y abarca temas como astronomía, botánica, agricultura, entre otros.

3.1.4 Siglo XVI

Figura 10. Enrique VIII y su hija Isabel I. Fuente: el autor

El uso de tintas invisibles fue tenido en cuenta siglos más adelante, pero es necesario hacer una pausa en esta parte del tiempo, este siglo fue un periodo de auge económico para Europa y de muchos conflictos religiosos en Inglaterra. La esteganografía juega un papel importante en esta época. El rey Enrique VIII quien para la época era el soberano de toda Inglaterra y quien en su intento por tener un hijo heredero de su trono, se casó en repetidas ocasiones hasta conseguir su objetivo como lo indica [25]. De sus pruebas fallidas nacieron dos hijas, María I e Isabel I, quienes más tarde tendrían diferencias de poder. Surgieron conspiraciones entre nobles católicos de la época y María I. Acuerdos secretos entre estas dos partes con el fin de derrocar a la reina vigente Isabel I, fue la razón para que se creara un mecanismo de comunicación privado evitando a toda costa que la reina Isabel I se enterara de este delito, de ser así correrían el riesgo de ser condenados.

La esteganografía jugó un papel fundamental, el camuflaje de mensajes en diferentes medios se transformó en un proceso peligroso tanto así que dependían vidas del éxito en la implementación del mismo. No cabe duda que el éxito del mismo depende de tan ingeniosa sea la idea, en este caso para los conspiradores fue una excelente herramienta ya que es casi nulo el número de personas que sospecharía de la transmisión de mensajes por este medio. Diferentes mecanismos se han utilizado, desde mensajes ocultos en tablillas de madera o utilizar la tinta invisible extraída del jugo de cítricos hasta transportar mensajes en barriles de cerveza, son ejemplo de la creatividad de la personas para obtener beneficios de esta herramienta

3.1.4.1 Primer Libro

El siglo XVI es la época en que se empieza a tener en cuenta la palabra Esteganografía en el vocablo de algunos interesados en esta disciplina. Para

entonces aparece el primer libro que especificaba algunos mecanismos empleados hasta la época de cómo se pueden ocultar mensajes dentro de otros objetos sin que sean descubiertos. Johannes Trithemius fue un monje alemán considerado el precursor de la criptografía moderna, se le relaciona con el ocultismo ya que fue mago y alquimista como lo indica [26]. Su obra más importante se tituló *"Steganographia"*.

Este libro se caracterizó porque se trataban temas como la ocultación de información y sortilegios diabólicos que no fueron muy bien vistos por la iglesia católica. Antes de convertirse en monje, Trithemius demostró gran inclinación por las ciencias ocultas y esto no fue impedimento para ingresar al monasterio, todo lo contrario impulsó la vacación por este tipo de disciplinas.


STEGANOGRAPHIAE
Hoc est:
ARS PER OC
CVLTAM SCRIPTV
RAM ANIMI SVI VO
LVNTATEM ABSENTIBVS
aperiendi certa;
AVTHORE
REVERENDISSIMO ET CLARISSIMO VIRO,
IOANNE TRITHEMIO, Abbate Spanhelmensi, &
Magia Naturali: Magistro per-
fectissimo,
PRAEFIXA EST HVIC OPERI SVA CLAVIS, SEV
HACTENVS QVIDEM A MVLTIS MVLTVM DE-
siderata, sed à paucissimis visa:
publicitati facta.
DARMSTADII,
IOANNIS BERNERI, Bibliop. Francof.
ANNO M. D. C. XXI.

Figura 11. Portada Steganographia

El libro se considera como maldito ya que describe rituales satánicos para invocar espíritus lo que la Santa Inquisición no observó de buena manera y acusó a Trithemius de mentiroso y fabulador según [26]. Sin dudas es una de las obras más enigmáticas de todos los tiempos, su contenido guarda secretos que hasta en la actualidad resultan difíciles de descifrar.

Muchos intentos fallidos han tratado interpretar los mensajes escritos en el libro, pero solo hasta 1996 un investigador alemán llamado Thomas Ernst logró descifrar el contenido del código como lo especifica [26].

3.1.5 Siglo XVII

Después de dar paso a esta disciplina, muchos investigadores mostraron su interés en el tema, se daba lugar entonces a un nuevo siglo donde aparecen grandes científicos y físicos de los que hoy todavía se habla como Isaac Newton, Rene Descartes o Galileo Galilei que abrieron puertas para que el surgimiento de nuevos matemáticos y con ellos nuevos métodos o técnicas que son consideradas como parte de la Esteganografía. Fue declarado como periodo barroco, esto por la influencia en las artes visuales o arte barroco, para el periodo otro tipo de disciplinas como la pintura, la arquitectura, la escultura o la música eran también de gran importancia, principalmente en la Europa Occidental. La música instrumental hacia auge en aquella época por ende la necesidad de componer partituras era primordial. Para entonces aparece un físico matemático llamado Gaspar Schott quien describe en su libro llamado “Schola Steganographica” nuevos métodos de Esteganografía, en este caso utilizando partituras musicales como lo indica [21]. Generalmente una partitura es escrita para establecer lo que los músicos deben interpretar en sus instrumentos musicales, Gaspar Schott

describe en su libro una técnica muy ingeniosa donde cada letra equivale a una nota musical, esto por supuesto, para ocultar mensajes dentro de las partituras.

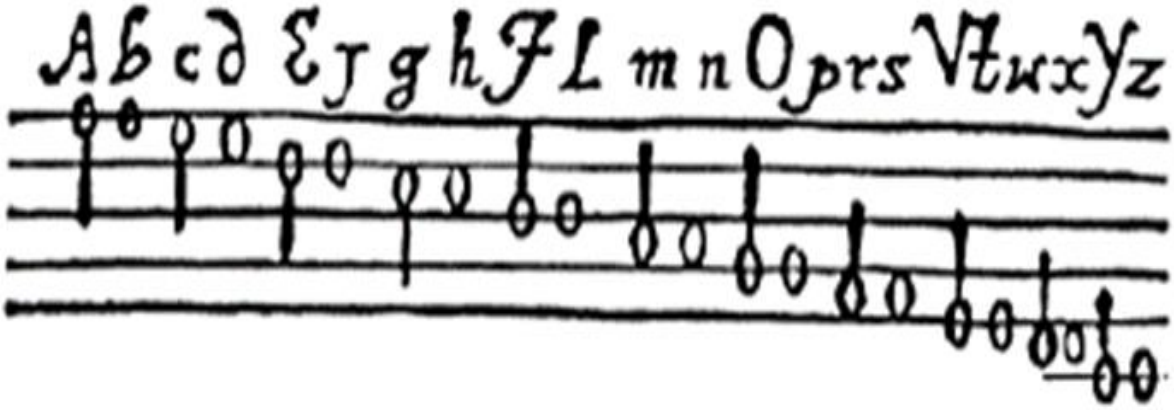

Figura 12. Partitura Musical. Cada letra corresponde a una Nota. Fuente: el autor.

Lo que se buscaba en este tipo de mecanismo era ocultar el mensaje, no se buscaba crear una melodía atractiva al oído. Se han encontrado nuevas variantes a esta metodología como por ejemplo contar el número de veces en que una nota se repite. No solo en las partituras musicales se ha encontrado un medio para ocultar mensajes, hoy en día es muy común reemplazar letras del alfabeto por figuras o imágenes de esta manera formar palabras sin que sea evidente la información que se quiere transmitir.

3.1.6 Esclavitud en África

Para nadie es un secreto que durante muchos años la cultura africana se ha visto sometida a la esclavitud. El siglo XIX fue un periodo de exploraciones por parte de los españoles en territorio africano, uno de los objetivos fue trasladar personas al continente americano para ser esclavizados. En la ruta se necesitaban métodos de comunicación, para lo cual, los africanos contaban con la ventaja de ser ricos

en cultura, tradiciones, música y muchos medios que les proporcionaban sacar ventaja ante los sometimientos de los españoles.

Figura 13. Telas con patrones. Fuente: el autor.

Crearon un método que consistía en tejer en vestidos o telas una serie de patrones como lo indica [21], este patrón solo lo identificaban la negritudes que buscaban refugiarse de quienes los buscaban someter. Los mensajes secretos por lo general eran para ocultarse o saber cuáles eran las rutas indicadas para trasladarse.

3.1.7 Segunda Guerra Mundial

La comunicación en las guerras es tan indispensable que gracias a esta se puede desestabilizar la misma o tal vez perderla si no se cuentan con medios seguros para transmitir información. La Segunda Guerra Mundial estimuló para que se ingeniaran nuevos mecanismos de esteganografía.

El siglo XX fue Alemania liderado por Adolf Hitler y con ayuda de algunos países vecinos cuyo objetivo ambicioso por conquistar la economía y la política de todo el planeta dio como resultado millones de muertos, mientras que Inglaterra, Francia y la Unión Soviética trataban de defender sus intereses como lo indica [27]. Estados Unidos entró a la guerra un par de años más tarde lo que sería determinante para el rumbo de la misma.

La esteganografía se convierte en un factor importante y determinante dentro del conflicto. Tanto en la Primera como en la Segunda Guerra Mundial se utilizaron mecanismos sofisticados que sirvieron de apoyo en batallas donde este tipo de ventajas eran fundamentales para inclinar la balanza a favor de quienes los implementaban.

3.1.7.1 Cifrado Nulo

Una de las técnicas que también tuvo éxito tanto en la primera como en la segunda guerra mundial fue el cifrado nulo. Los alemanes se han destacado por ingeniar métodos esteganográficos que se convierten en retos para sus adversarios. En este caso implementan un mecanismo que consistía en escribir un párrafo que a simple vista no tenía importancia pero si se retiraba una letra cada dos o cinco letras se podía formar un mensaje el cual podía ser una orden de ataque las coordenadas para un bombardeo. Durante la Primera Guerra Mundial

se pudo interceptar un mensaje enviado por un espía alemán como lo describe [22].

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

A simple vista puede ser un mensaje sin mucha importante pero las autoridades estadounidenses analizaron el mensaje y pudieron identificar que si se retira la segunda letra de cada palabra se puede formar la siguiente frase:

“Pershing sails from NY June 1”

Era una orden para que el comandante de las fuerzas estadounidenses Pershing saliera de la ciudad de Nueva York el primero de junio.

El método tuvo éxito durante varios años una vez descubierto sirvió de referencia para la decodificación de futuros mensajes interceptados.

3.1.7.2 Micropunto

Una de las técnicas más famosas usadas durante la segunda guerra mundial. Los alemanes diseñaron un mecanismo que era capaz de reducir el contenido de una hoja de papel a una microficha o Micropunto de menos de un milímetro de diámetro lo que facilitaba el camuflaje del mensaje. En el punto de la letra “i”

podía estar oculto el mensaje. Una vez la carta llegaba a su destinatario el Micropunto podía ser despegado de la carta y el mensaje leído.

Este método fue descubierto dos años después de iniciada la guerra justo cuando Estados Unidos entraba en la lucha, al parecer fue un opositor el encardo de revelar el mecanismo que era casi imperceptible por el ojo humano. Fueron muchos mensajes que se lograron transmitir con este mecanismo que llegó a ser considerado como “la obra maestra del espionaje enemigo” como lo indica [22].

Figura 14. Ejemplo de la utilización del Micropunto. Fuente: el autor

3.1.7.3 Codetalkers

Los Codetalkers o locutores claves era un término generalmente usado para referirse a los soldados norteamericanos que provenían de la una región indígena estadounidense cuyo papel en la guerra era transmitir mensajes militares secretos utilizando su propio lenguaje nativo. Estos mensajes eran transmitidos generalmente utilizando un teléfono o una radio y el reto principal era que los mensajes no fueran descifrados. También se les conoce con el nombre de Navajos y su papel fue fundamental en la Segunda Guerra Mundial ya que gracias a su lenguaje que en realidad pertenecía a un grupo pequeño de indígenas era muy difícil de descifrar para el enemigo.

Figura 15. Navajos Transmitiendo Mensaje en su Lenguaje. Fuente: el autor.

El uso de este mecanismo representó para los Estado Unidos una gran ventaja considerando que solo un grupo minoritario conocía la estructura del lenguaje, puede ser considerado como una técnica de esteganografía donde se oculta el mensaje en un medio conocido por pocos.

La esteganografía jugó un papel fundamental en la segunda guerra mundial, métodos tan sofisticados que duraban meses, incluso años en descifrar el mecanismo. Al final, Estados Unidos y los aliados lograron la victoria a costa de desastres y muchas muertes pero rescatando los avances en métodos para la seguridad de la información.

3.2 ESTEGANOGRAFÍA MODERNA

Durante la Segunda Guerra Mundial los avances en tecnología se vieron suspendidos ya que todo el dinero estaba destinado a sustentar el conflicto. Con el fin de la guerra se pudieron observar nuevamente avances en telecomunicaciones, tecnología, educación, entre otras áreas. La esteganografía en consecuencia también se benefició, la información que se oculta actualmente está dirigida a un grupo de personas y el ambiente cambia de ser conflictivo (guerra) a un entorno donde el manejo de la información y la seguridad de los datos se convierten en el principal reto para los que emplean esta disciplina.

Gracias al avance de las tecnologías actuales, las aplicaciones esteganográficas se han podido extender a sectores como protección de propiedad intelectual, política, ocultación de virus informáticos, así como también se sigue usando en comunicaciones en el sector militar. La era de los computadores ha llegado y con ella miles de oportunidades y medios de comunicación que nos simplifican las tareas. Lo que antes era imposible hoy es posible gracias a la capacidad de

comunicación que nos ofrece la tecnología. Lo que antes tardaba días, semanas o hasta años, hoy tarda segundos. La tecnología se ha convertido en parte esencial de nuestras vidas, la necesidad de estar constantemente en contacto con nuestros seres queridos y compartir con ellos información se ha convertido en una costumbre.

Cada día son más las personas que interactúan con los medios electrónicos, todos los días aumenta la demanda y con ella aumentan los requisitos de infraestructura para dar soporte y servicio a los usuarios. Con la llegada de Internet la oportunidades no solo de comunicación sino también de negocio ha aumentado de forma exponencial, cada día son más las empresas que desean hacerse conocer ante el mundo por medio de la red. Los arquitectos de redes se han enfrentado a un monstruo y es poder garantizar que las comunicaciones se establezcan de forma confiable y segura.

El manejo de información es fundamental para cualquier empresa moderna, el área de sistemas en cualquier organización es vital para el funcionamiento de la misma. En una empresa muchas veces se manejan datos de carácter privado, es decir, se tiene que garantizar que esa información sólo puede accesible por la empresa. Siempre que existan datos importantes van a existir terceros que quieren acceder a de ellos. Para nadie es un secreto que las redes permiten que una persona con conocimientos en informática puede acceder desde cualquier sitio a información privada dependiendo de los protocolos de seguridad que las mismas empresas implementen.

Mecanismo como la ocultación de malware puede ser utilizado para extraer información importante de la compañía, el objetivo es hacerle creer a cualquier empleado por medio de promociones a publicidad falta en internet que se trata de algo inofensivo y motivándola a descargar e inmediatamente este software

encontrar puntos débiles en el sistema para hospedarse y extraer información importante. Este tipo de mecanismo es considerado una técnica esteganográfica que se puede convertir en una amenaza peligrosa para cualquier empresa.

Figura 16 Spyware Método Esteganográfico. Fuente: el autor.

Spyware es un tipo de malware que generalmente utiliza medios publicitarios para hacerle creer al usuario que se trata de algo inofensivo, sin saber que una vez instalado en el computador puede llevar tareas de espionaje o hasta dejar inútil el mismo. Se han conocido casos en los que se han utilizado este tipo de software malicioso para extraer información de conversaciones diplomáticas de alto nivel de gobiernos en todo el mundo.

Ejemplo de esto son los constantes ataques en compañías israelís donde ejecutivos utilizan software espía para extraer información importante de la competencia, se conocen casos donde se ha perdido información militar clasificada, planos de motores y en ocasiones la producción de una compañía se ha visto obligada a detener por culta de software malintencionado.

La esteganografía moderna no depende en mantener en secreto un algoritmo de ocultación y tampoco del objeto que se utilizar para ocultar la misma, sino que se centra en mantener una cantidad mínima de información secreta entre los que intervienen en la comunicación como lo indica [21].

Algunas de las técnicas esteganográficas utilizadas actualmente para controlar la piratería informática y derechos de autor se describen a continuación.

3.2.1 Marcas de Agua sobre Papel

Antes de hablar sobre las marcas de agua digitales y sus aplicaciones en la informática es necesario hablar sobre las marcas de agua sobre papel. Aunque es una técnica que actualmente es muy utilizada pero ya se venía empleando desde finales del siglo XIII cuando se empezaba a elaborar el papel como indica [29]. Durante el proceso de fabricación del papel y cuando este aún se encuentra húmedo, se emplea una especie de cilindro el cual tiene adherido una rejilla con la señal o la marca que se desea emplear, en muchos casos se utilizan dibujos, escudos o alguna señal que hace distintivo el papel.

En la actualidad esta técnica es usada por ejemplo, en el papel de los billetes, el objetivo principal de utilizar esta técnica es evitar que los billetes sean falsificados,

aunque también se utiliza cuando se desea dar cierta validez a algún libro o estudio impreso en papel además de dotar al libro de información como año en que se elaboró o el lugar de procedencia del mismo.

Figura 17. Marca de agua sobre billete de 50 euros. Fuente: el autor.

Una de las principales aplicaciones de las marcas de agua que también se conocen como filigranas es en los billetes para evitar que estos sean falsificados, este método consiste en ocultar información ya que estas marcas nos son muy visibles. La marca aparece solo si se observa el billete a contraluz. Se considera es una técnica esteganográfica ya que utiliza un objeto para ocultar información.

3.2.2 Marcas de Agua Digitales

La era digital ha llegado y la necesidad de manejar información por la red es vital para cualquier persona o compañía, toda la información almacenada en libros y en documentos importantes tienden a convertirse en archivos digitales. La necesidad de las personas de ser reconocidos como los autores originales de todos estos trabajos es un reto para el cual se proponen las marcas de agua digitales como solución.

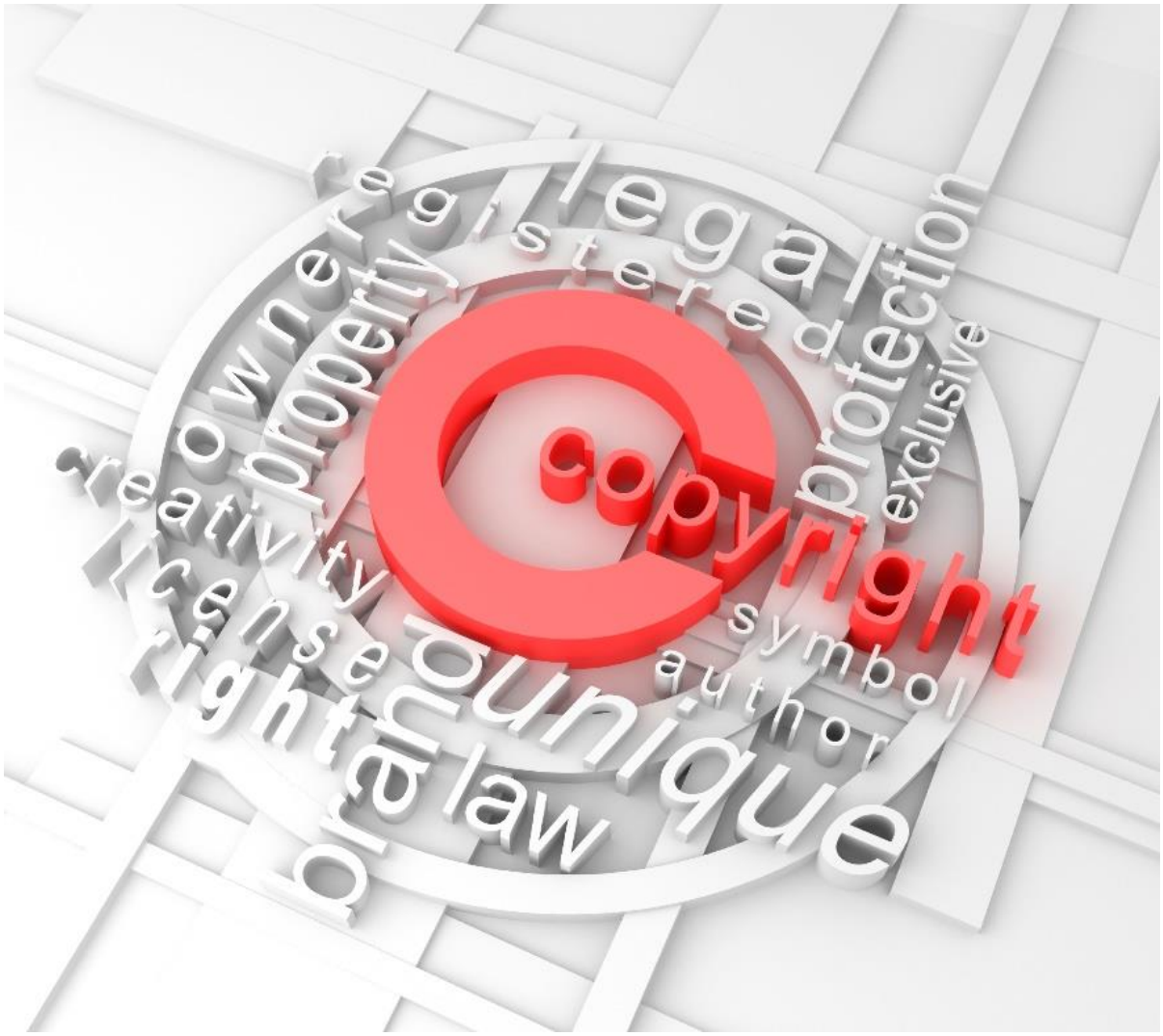

Figura 18. Copyright: Derecho de copia. Fuente: el autor.

Esta técnica esteganográfica se creó básicamente como solución a los derechos de copia o copyright de archivos como documentos, imágenes, audio, video. La idea principal de este método es crear una marca que sea inseparable de todos estos archivos donde se pueda conservar información como autor, propietario, distribuidor y evitar el plagio de esta información. Las principales características de esa técnica es que debe ser invisible a la persona que quiera observar su contenido, al momento de implementar esta técnica se debe proteger el contenido que se quiere proteger, es decir, no se debe degradar la información.

Básicamente esta herramienta consiste en insertar un código directamente al archivo ya sea una imagen, audio o video como lo indica [30]. Este código funciona como un identificador que está asociado al autor, en ocasiones se utilizan otros medios como huellas digitales para reforzar la seguridad del sistema. Este modelo debe ser invisible a terceros que quieran hacer plagio del contenido pero deber ser accesible mediante generalmente el uso de un algoritmo y una contraseña.

3.2.3 Estudios Actuales

Uno de los estudios actuales más importantes que se han hecho sobre esteganografía, es el artículo publicado por Cristian Cachin en el 2004 llamado An Information-Theoretic Model for Steganography donde propone un sistema de esteganografía perfecto, incluye toda la formulación matemática de las condiciones que un estegosistema debería tener, plantea un problema de prueba de hipótesis donde compara una objeto de inocente y un objeto con información oculta donde la discriminación entre los dos objetos es lo que se plantea como hipótesis para luego por medio de pruebas determinar su validez [28].

3.2.4 Tendencias Esteganográficas

A pesar que es una técnica utilizada desde la antigüedad, hoy en día se sigue empleando especialmente por empresas interesadas en Gestión de Derechos Digitales que buscan proporcionar seguridad y derechos de autor a todos sus proyectos.

Un hecho que marcó al mundo y a los Estados Unidos de Norteamérica fue los atentados terroristas del 11 de Septiembre de 2001 como se menciona en capítulos anteriores de este trabajo, cometidos por miembros de la red yihadista Al Qaeda. Este grupo utilizaban imágenes publicadas en internet para ocultar mensajes que les sirvieron para la planificación de dichos atentados.

Por hechos como este, es que los organismos de defensa de muchos países han mostrado preocupación por implementar métodos que permitan la detección de este tipo de amenazas (estego-análisis).

Lastimosamente la esteganografía se ha visto envuelta en delitos como pornografía infantil, planificación de ataques terroristas, espionaje, delitos de derechos de autor, entre otros, donde se han empleados técnicas que a juicio de la sociedad no deberían aplicarse.

CAPÍTULO IV
4. ESTEGANOGRAFÍA

De [31] podemos tomar una clara definición de lo que es la esteganografía “La esteganografía es la disciplina en la que se estudian y aplican técnicas que permiten el ocultamiento de mensajes u objetos dentro de otros, llamados portadores, de modo que no se perciba su existencia.”. Así pues, podemos partir desde este punto para tratar de exponer las capacidades que tiene esta técnica al momento de salvaguardar información, de diferentes formas la esteganografía puede llevar información de un punto a otro a través de medios informáticos que están a disposición de cada uno de nosotros, como lo son: correos electrónicos, los cuales si no están protegidos adecuadamente podrían revelar mucha información de la empresa o persona que haga uso de él, correo físico, el cual al ser interceptado podría revelar su contenido fácilmente tan solo con romper el sobre, transmisiones por redes sociales, las cuales, si se comparte información por este medio, ningún detalle está a salvo de la mirada de los curiosos; de esta manera, se quiere exponer esta técnica, la cual, sea por cual sea el medio de transmisión, la información siempre estará a salvo de las personas que usan estos medio de comunicación.

4.1 TIPOS DE ESTEGANOGRAFÍA

Queriendo explicar esta disciplina de la mejor forma posible, se desglosará este capítulo del trabajo en las formas conocidas de esteganografía y posteriormente, se mostrarán herramientas que pueden servir para el desarrollo de esta idea, la cual, cada día tiene más desarrollo.

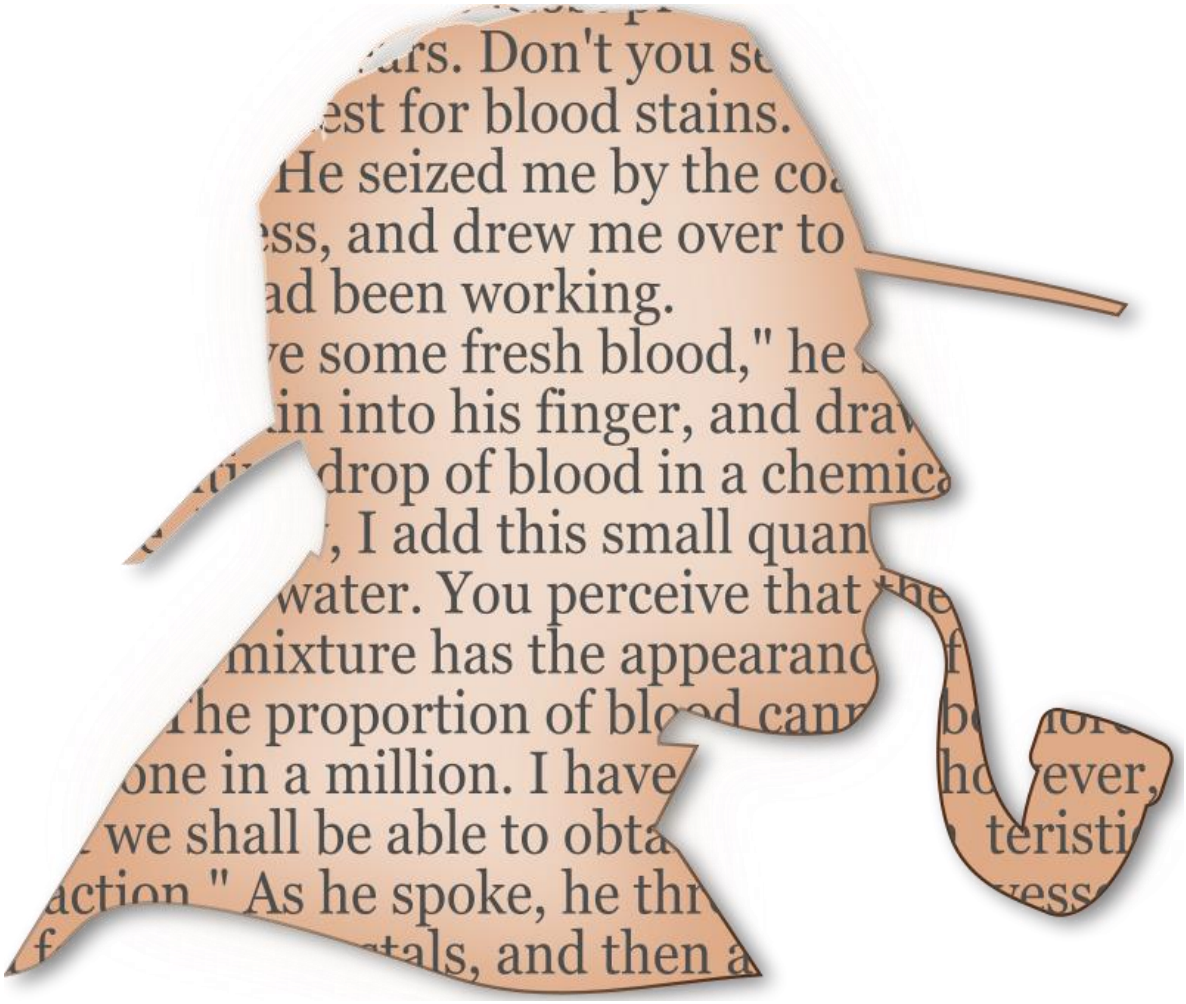

Figura 19. Esteganografía en imágenes. Fuente: el autor.

4.1.1. Esteganografía pura

De acuerdo con la definición puntual que nos ofrecen en [32] “La fortaleza del sistema recae en los algoritmos de ocultación y extracción de la información, que sólo el emisor y el receptor del mensaje deberían conocer.”, este tipo de esteganografía es seguro siempre y cuando el medio por el cual se transmite el mensaje sea inexperto en las habilidades de esteganografía, pero en medios más avanzados se requiere el uso de este método combinado con criptografía, ya que, si no se combina podría resultar desastroso para el objetivo que se busca.

Un ejemplo claro de esto ocurre en una cárcel, cuando dos prisioneros planean escapar, pero sus notas tienen que pasar necesariamente por el guardia de seguridad quien las revisa antes de entregarlas, su plan lo realizan mediante notas al parecer indefensas, las cuales al ser puestas a contraluz, revelaban el mensaje oculto, este es un claro ejemplo de la aplicación de la esteganografía pura, cuando el medio que transporta el mensaje, omite los mensajes ocultos que puede contener los ficheros que transporta.

Figura 20. Problema de los prisioneros. Fuente: el autor

4.1.2. Esteganografía de clave privada

“Fruto de la combinación de esteganografía pura con criptosistemas simétricos. Se asume que un atacante podría conocer los algoritmos de ocultación y extracción de la información. Por este motivo, el mensaje se cifra utilizando un cifrado simétrico antes de ocultarlo. De esta manera, incluso si el atacante intercepta la

transmisión y logra extraer la información aún tendrá que enfrentarse al criptoanálisis del criptosistema utilizado.” [33] como bien se mencionó anteriormente para evitar el fracaso a la hora de transmitir mensajes, es necesario agregar otro nivel de seguridad más a el mensaje oculto y es aquí donde la esteganografía gana gran fortaleza frente a otras técnicas de ocultamiento de información; tan sólo se agrega un nuevo parámetro al estego-algoritmo el cual es comúnmente conocido como “estego-clave”, la “estego-clave” debe ser socializada entre el emisor y el receptor antes de la comunicación, puede llegar a ser desde que metro de la cinta se debe leer, cada cuántas revoluciones de cassette se debe capturar una letra o incluso que intensidad de luz es la óptima para poder ver el mensaje, de esta manera se tiene infinidad de formas de esconder y es por esto que es casi imposible descifrar el contenido de la comunicación si no se cuenta con la “estego-clave”.

4.1.3. Esteganografía de clave pública

Por último, este tipo de esteganografía utiliza dos claves y su principal característica es que no requiere un intercambio previo de estego-clave. Requiere de dos claves, una secreta que se utiliza al momento de realizar la inserción del mensaje secreto y una pública, la cual se guarda en las bases de datos públicas. La estego-clave se usa para reconstruir el mensaje

4.2 ESTEGO-ALGORITMOS

Después de conocer los tipos de esteganografía, se mostrará el principal y más conocido estego-algoritmo y se mostrará cómo se realiza el proceso interno del ocultamiento de mensajes secretos, para de esta forma saber cómo funciona esta disciplina que ha mostrado tantos avances en los últimos años.

4.1.4. Inserción en el bit menos significativo (LSB Least Significant Bit)

Captado de [34] “Este es el método moderno más común y popular usado para esteganografía y también es uno de los llamados métodos de sustitución.”. Como su nombre lo indica este tipo de estego-algoritmo hace uso del bit menos significativo o de menos importancia dentro de la cadena de bits de 32 ó 64 bits, dependiendo de la arquitectura que estemos utilizando y alterarlo, estas técnicas son aplicables tanto a audio como a video. Es bastante eficaz en imágenes a blanco y negro o que tienen un gran peso, ya que, pueden ser modificadas sin verse afectados sus pixeles, si por el contrario son imágenes con una paleta de color de 8 bits, este se podría ver afectado debido a su baja resolución o lo que se traduciría en este caso, poco espacio para albergar nuestro mensaje.

El ejemplo dado por [35] nos muestra cómo se puede ocultar la letra “A” en tan solo tres píxeles de imagen. Para este caso se analiza en una imagen que cuenta con un formato RGB (3 bytes), estos tres píxeles estarían representados en su forma original de la siguiente manera:

(1 1 0 1 1 0 1 0) (0 1 0 0 1 0 0 1) (0 1 0 0 0 0 1 1)

(0 0 0 1 1 1 1 0) (0 1 0 1 1 0 1 1) (1 1 0 1 1 1 1 1)

(0 0 0 0 1 1 1 0) (0 1 0 0 0 1 1 1) (0 0 0 0 0 1 1 1)

El mensaje a cifrar es ‘A’ cuya representación ASCII es (1 0 0 1 0 1 1 1), entonces los nuevos píxeles alterados serían:

(1 1 0 1 1 0 1 **1**) (0 1 0 0 1 0 0 **0**) (0 1 0 0 0 0 1 **0**)

(0 0 0 1 1 1 1 **1**) (0 1 0 1 1 0 1 **0**) (1 1 0 1 1 1 1 **1**)

(0 0 0 0 1 1 1 **1**) (0 1 0 0 0 1 1 **1**) (0 0 0 0 0 1 1 1)

Si bien se observa en cada píxel se están afectando 3 de cada 24 bits, lo que equivale al 12.5% de la imagen, la cual lograría pasar desapercibidamente cualquier control propuesto, debido a su poca cantidad de ruido.

De esta manera, podemos ocultar información en diferentes formatos de imágenes, si para el mismo ejemplo, utilizamos un formato CMYK, sólo necesitaríamos dos pixeles para ocultar la letra “A” lo cual nos daría un menor desperdicio de bytes a la hora de transferir imágenes con contenidos ocultos. Este algoritmo ofrece una gran ventaja sobre los demás, porque no afecta el tamaño de la imagen.

En conclusión, al usar este tipo de estego-algoritmo, es imprescindible saber que únicamente se puede ocultar 1 bit por cada 8 bits que tenga la imagen, si el mensaje que se quiere ocultar es muy grande, este tamaño debe ser directamente proporcional al tamaño de la imagen. Si en vez de un bit se quieren usar dos en la cadena de bits, es más fácil ser descubiertos debido a la mayor cantidad de ruido que se puede generar y que ya no pasará de forma inadvertida ante el ojo humano.

Otro ejemplo de este algoritmo se ve reflejado en la siguiente imagen:

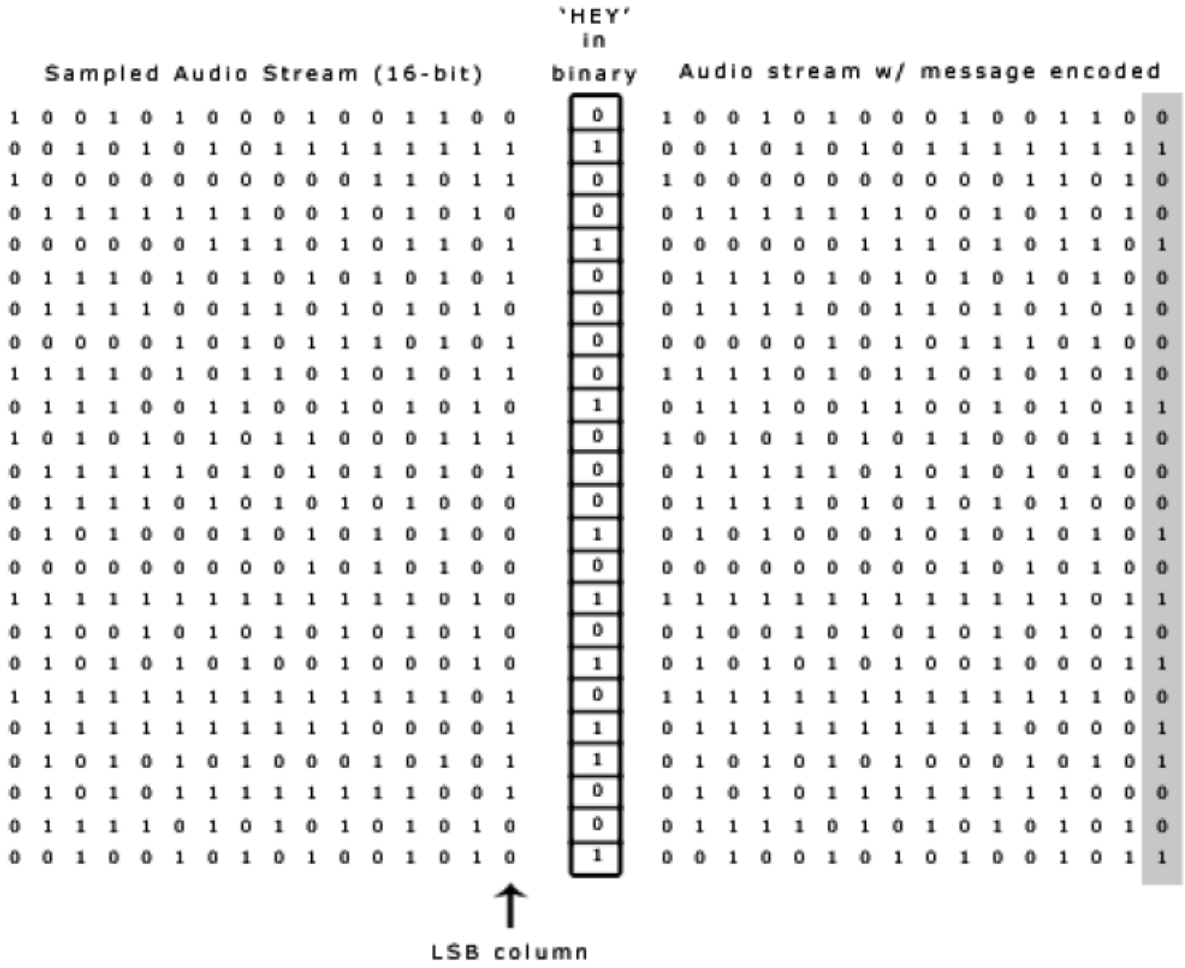

Figura 21. Palabra ‘HEY’ en LSB. Fuente: el autor.

En la anterior imagen, se codificó la palabra ‘HEY’ en un audio de 16 bits mediante la técnica del bit menos significativo, se puede observar que sólo se afecta 1/16 parte de la pista de audio lo cual pasaría inadvertido al oído humano.

4.3 EJEMPLOS DE ESTEGANOGRAFÍA

Miles de personas muestran cada vez más interés en el esteganografía como medio de protección para el traspaso de sus mensajes a través de las redes públicas o ya bien sea para ocultar los secretos más importantes de sus negocios a los ojos de personas que tienen intereses comunes sobre ellas, en la web se pueden encontrar muchas y diversas herramientas que permiten la fácil aplicación de esta técnica de ocultamiento.

A continuación se mostrarán varias formas de aplicar el concepto, en software que es aplicable a Windows y también formas para desarrollar la disciplina en software libre

Tomado de [36] “DeepSound es una herramienta gratuita para Windows diseñada especialmente con ese fin, el de ocultar archivos e información dentro de ficheros Mp3 con un cifrado AES de 256 bits.”

Después de instalar el software lo más importante es tener el medio portador, el cuál puede ser un archivo con extensión .mp3, ya que, DeepSound oculta mensajes en canción en formato .mp3.

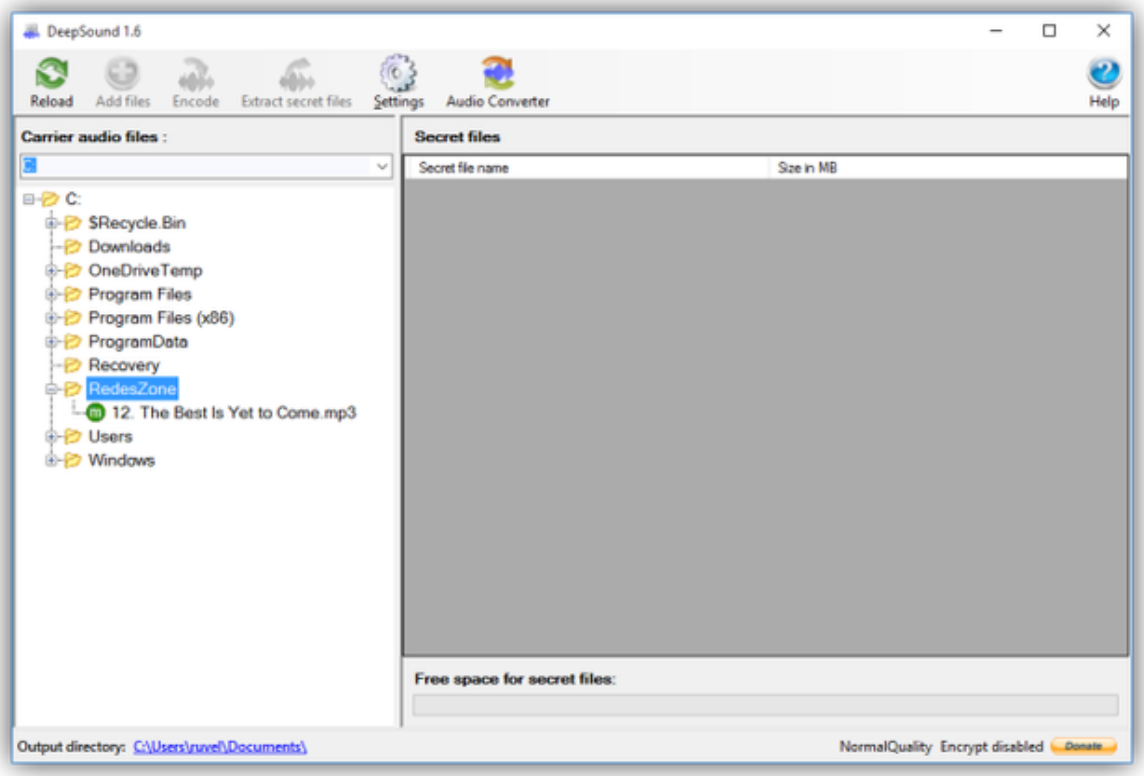

Figura 22. Encontrar medio portador para el mensaje que se requiere transmitir mediante esteganografía. Fuente: el autor.

Cuando se realiza la descarga, lo primero que se encuentra es esta pantalla, donde se puede observar que es una interfaz muy amigable con el usuario, con gran facilidad para entender cómo debe ser el proceso para ocultar el mensaje y sin muchas opciones que puedan dificultar el desarrollo del propósito.

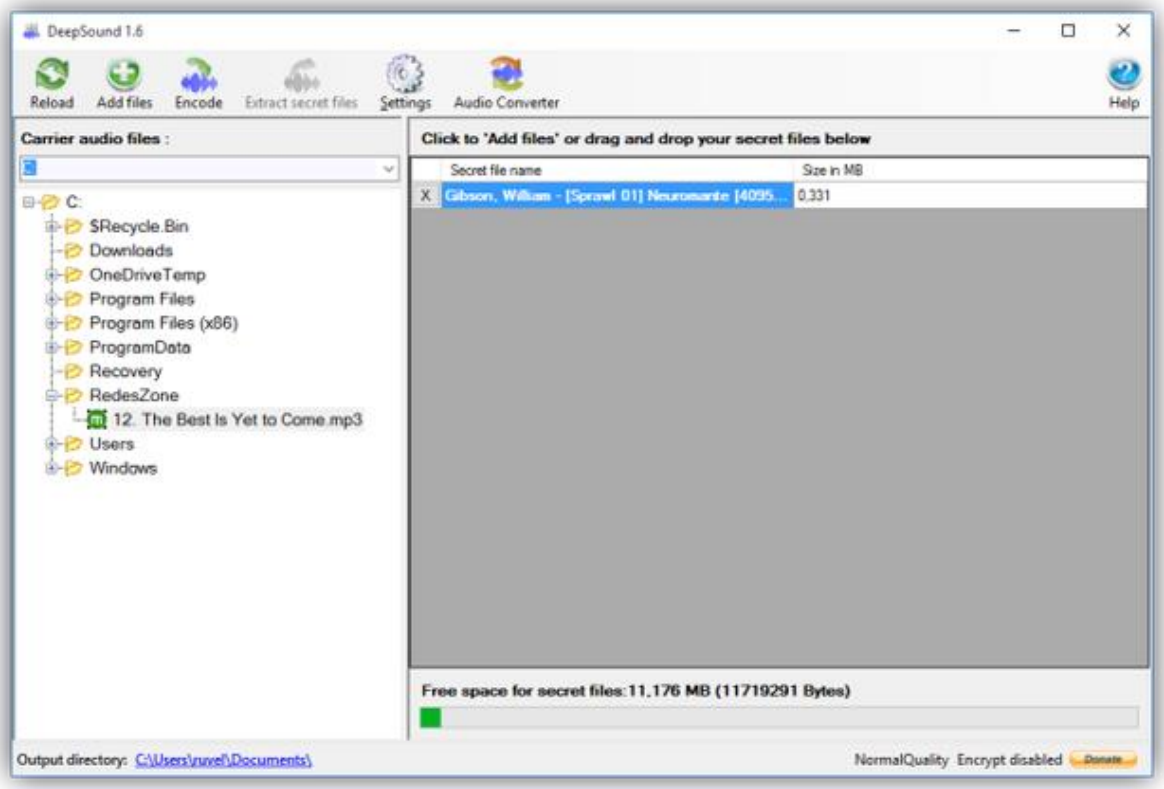

Figura 23. Añadir archivo portador. Fuente: el autor.

El primer paso es encontrar en el directorio la carpeta que contiene la canción portadora del mensaje que queremos transmitir.

Una vez identificado el archivo portador, el paso a seguir es buscar la opción “add files” en el menú superior y hacer clic en ella, de esta forma el archivo quedará listo en la zona derecha de la pantalla, a la espera de el mensaje que queremos ocultar.

Después de añadir el archivo portador, nuevamente se selecciona en el explorador de archivos, el mensaje que queremos ocultar, puede ser uno o varios, la herramienta permite ocultar los mensajes que se requieran. Para hacer un buen

uso de la esteganografía y de la herramienta se debe tener en cuenta el tamaño del mensaje que se pretende ocultar, no es posible que una canción de 3:40 minutos pese alrededor de 20 MB, esto podría levantar sospechas, para esto el artículo recomienda realizar cargas pequeñas al archivo de audio para pasar desapercibido ante las personas que puedan ver el mensaje primero.

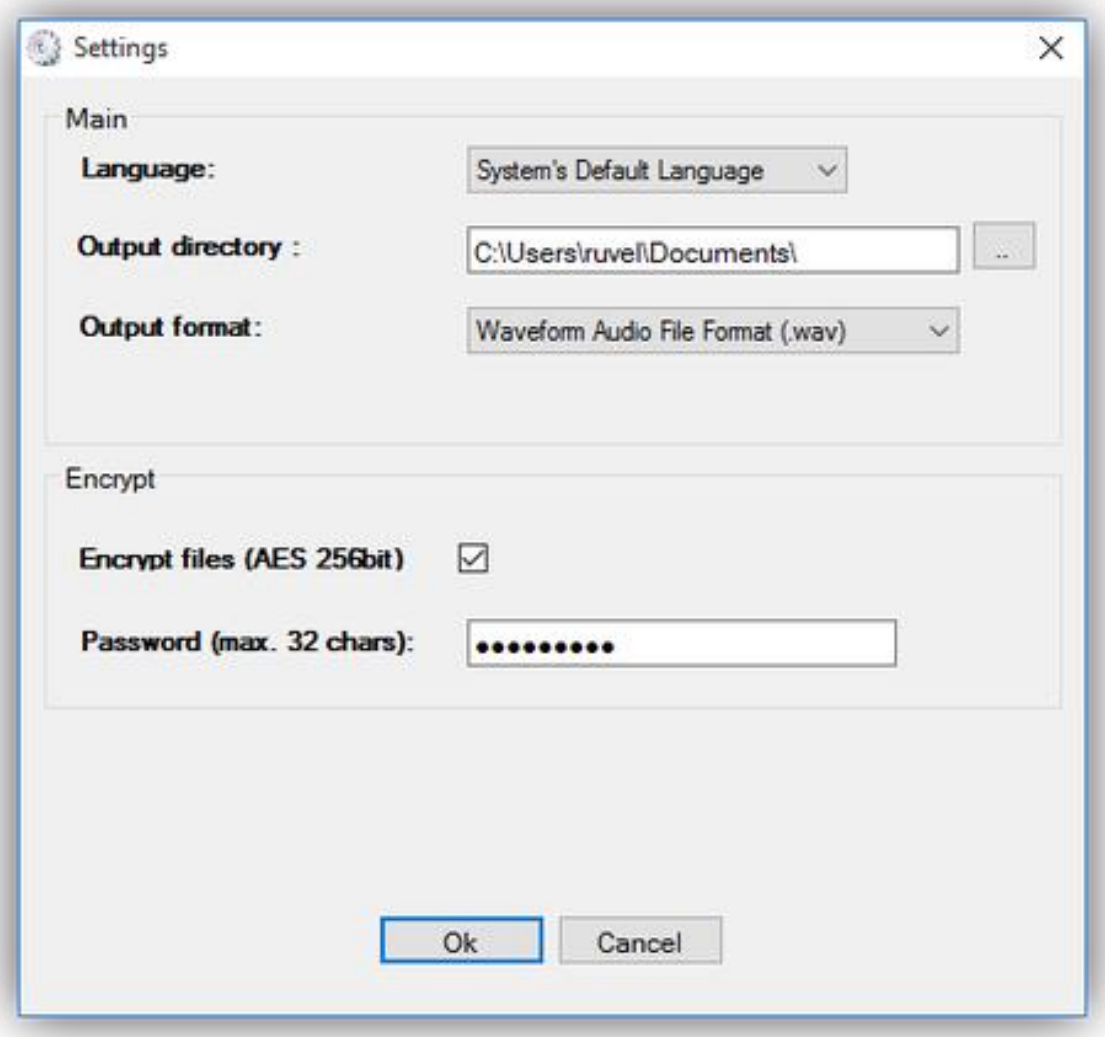

Figura 24. Codificación del archivo. Fuente: el autor.

En el siguiente paso, sólo resta hacer clic en el botón “encode” de la barra superior de la plataforma, en esta parte el software solicitará la extensión del output, lo más recomendable por el autor es formato .wav, porque es un tipo de archivo de mayor tamaño y no tendrá problemas en ocultar archivos de mayor envergadura.

Adicionalmente y muy importante es la contraseña de encriptación que recibirá nuestro archivo, es el “plus” de seguridad que ofrece esta herramienta, con una contraseña de hasta 32 caracteres, que hará más difícil el descubrimiento de nuestro mensaje, si es descubierto.

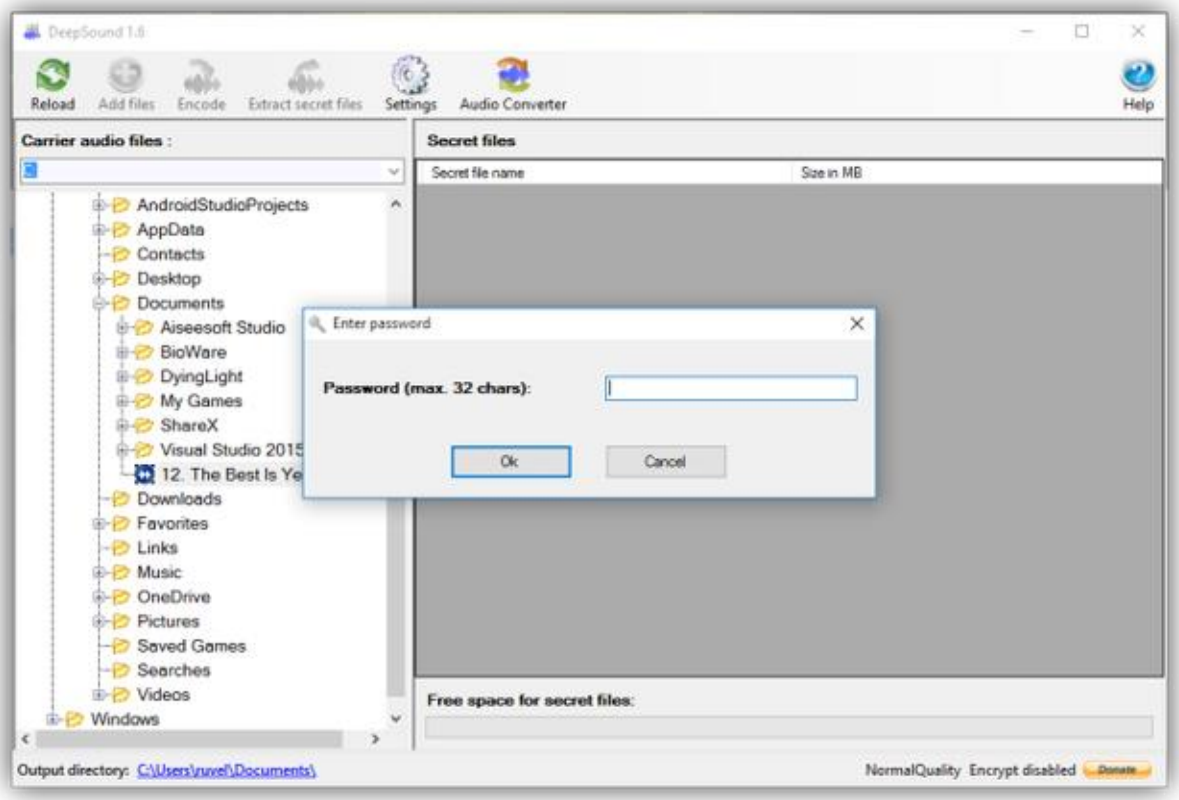

Figura 25. Descodificación del archivo portador. Fuente: el autor.

El paso siguiente y final lo realiza el receptos del mensaje, con el “DeepSound” deberá seleccionar la canción portadora y opromir el botón “Extract Secret Files” para descomprimir los archivos en su disco duro.

El archivo que oculta el mensaje, puede ser reproducido sin ningún problema en el reproductor, sólo la persona “objetivo” sabe que este archivo contiene un mensaje secreto y para descifrarlo necesita, la misma versión del software que se utilizó para realizar la encriptación y además la contraseña que utilizó la persona que realizo el proceso de ocultamiento, de esta manera vemos que el mensaje queda con una seguridad muy fuerte y además oculto a los ojos de las demás personas.

En [37] se puede apreciar una forma mucho más fácil de realizar la esteganografía, sin necesidad de instalar ningún tipo de software, solamente mediante líneas de código, gracias al enorme potencial del software libre, de esta forma.

En este caso, ocultaremos archivos de información en una imagen con extensión .png, primero que todo se abre el terminal y se debe comprimir el archivo que se quiere ocultar de la siguiente forma:

```
rar a archivocomprimido.rar loqueocultare.txt
```

Figura 26. Comprimir archivo que se quiere ocultar. Fuente: el autor.

Se pueden utilizar varias extensiones de compresión como los son .zip .rar. 7z .tar.7z entre otros.

Para el siguiente paso se debe tener el medio portador con una extensión .png y se concatena con el archivo que se comprimió anteriormente.

```
cat imagen.png archivocomprimido.rar > nuevaimagen.png
```

Figura 27. Concatenar imagen con mensaje secreto. Fuente: el autor.

De esta manera, el archivo “nuevaimagen.png” será el contenedor del archivo comprimido que esconde el mensaje, lo mejor de todo, es que, si se abre este archivo directamente desde el directorio, únicamente mostrará la imagen y no habrá pistas de lo que oculta; una vez transmitido el mensaje lo único que resta por hacer es renombrar el archivo de la siguiente forma:

```
mv nuevaimagen.png nuevaimagen.rar
```

ó

```
cp nuevaimagen.png nuevaimagen.rar
```

Figura 28. Renombrar archivo. Fuente: el autor.

Al renombrar el archivo, se logrará extraer todo el contenido de la imagen, revelando de esta manera el o los mensajes ocultos que se lograron transmitir bajo la fachada de una inofensiva imagen, al igual que un audio, se debe justificar el tamaño del archivo, sería demasiado evidente una imagen con mucho peso, pero que la calidad sea en muy baja resolución.

CAPÍTULO V
5. CONCLUSIONES, RECOMENDACIONES Y REFERENCIAS BIBLIOGRÁFICAS

5.1 CONCLUSIONES

- El presente trabajo de investigación hace un registro histórico de los eventos más importantes que han trascendido la esteganografía como mecanismo de seguridad de la información en la actualidad.
- En la antigüedad el principal escenario para la aplicación de mecanismos esteganográficos eran conflictos bélicos, en la actualidad se ha expandido el campo de aplicación de esta disciplina.
- En la esteganografía clásica principalmente el mensaje oculto se trataba de texto, en la actualidad se pueden ocultar archivos utilizando como medio portador otro archivo.
- La esteganografía moderna acepta algoritmos mucho más complicados ya que se puede aprovechar la potencia de los cálculos realizados por un computador.
- La esteganografía moderna ha dado paso al estego-análisis creado para tratar de prevenir y protegerse de los ataques realizados por herramientas esteganográficas.
- La seguridad de la información se ha visto vulnerada por métodos esteganográficos que han obligado a la creación de mecanismos de defensa.
- La esteganografía combinada con otras metodologías puede formar llaves inquebrantables de seguridad de la información que se quiere portar.

5.2 RECOMENDACIONES

- Se recomienda mejorar la identificación de trabajos esteganográficos haciendo énfasis en libros que se han dedicado por completo al tema.
- Se recomienda fomentar los estudios investigativos a cerca de esta temática, de modo que estos sirvan como ejemplo y soporte teórico que lo fundamenten y le den validez.
- Se recomienda incentivar este tipo de investigaciones con el fin de identificar en esta temática los vacíos o saturación del conocimiento que existen en la actualidad.
- Para futuras investigaciones y al Programa Ingeniería de Sistemas y Computación se recomienda estimular al estudiante de pregrado hacia la investigación con el fin de fortalecer capacidades que permitan mejorar la realización de sus proyectos de grado.

5.3 REFERENCIAS BIBLIOGRÁFICAS

[1] Esteganografía, el arte de ocultar información sensible (Disponible en http://www.pabloyglesias.com/mundohacker-esteganografia/. Consultado el: 09 de septiembre de 2015).

[2] Esteganografía, el arte de ocultar información sensible (Disponible en http://www.pabloyglesias.com/mundohacker-esteganografia/. Consultado el: 14 de septiembre de 2015).

[3] Seguridad de la información (Disponible en http://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion. Consultado el: 14 de septiembre de 2015).

[4] Criptografía, criptoanálisis, criptología y encriptación (Disponible en http://www.gitsinformatica.com/criptografia.html. Consultado el: 14 de septiembre de 2015).

[5] Criptografía, criptoanálisis, criptología y encriptación (Disponible en http://www.gitsinformatica.com/criptografia.html. Consultado el: 14 de septiembre de 2015).

[6] Javier Areitio. Importancia de la seguridad. Seguridad de la información: Redes, informática y sistemas de información. Paraninfo, 2008. P. 2.

[7] Javier Areitio. Importancia de la seguridad. Seguridad de la información: Redes, informática y sistemas de información. Paraninfo, 2008. P. 5.

[8] Fraudes bancarios son el 80% de los ciberdelitos (Disponible en http://www.diariolibre.com/noticias/fraudes-bancarios-son-el-80-de-los-ciberdelitos-FLDL477561. Consultado el: 16 de septiembre de 2015).

[9] Esteganografía, El Arte de Ocultar Información (Disponible en http://www.egov.ufsc.br/portal/sites/default/files/esteganografia1.pdf. Consultado el: 16 de octubre de 2015).

[10] Que es la Criptografía (Disponible en http://www.informatica-hoy.com.ar/seguridad-informatica/Criptografia.php. Consultado el: 16 de octubre de 2015).

[11] Esteganografía, el arte de ocultar información sensible (Disponible en http://www.pabloyglesias.com/mundohacker-esteganografia/. Consultado el: 14 de noviembre de 2015).

[12] Esteganografía, una técnica que suscita interés (Disponible en http://es.blastingnews.com/tecnologia/2014/12/esteganografia-una-tecnica-que-suscita-interes-00218643.html. Consultado el: 14 de noviembre de 2015).

[13] David García Cano, Análisis de herramientas esteganográficas, Universidad Carlos III de Madrid Escuela Politécnica Superior, Diciembre 2004. P 14.

[14] Esteganografía, una técnica que suscita interés (Disponible en http://es.blastingnews.com/tecnologia/2014/12/esteganografia-una-tecnica-que-suscita-interes-00218643.html. Consultado el: 14 de noviembre de 2015).

[15] Esteganografía, una técnica que suscita interés (Disponible en http://es.blastingnews.com/tecnologia/2014/12/esteganografia-una-tecnica-que-suscita-interes-00218643.html. Consultado el: 14 de noviembre de 2015).

[16] Hammertoss, APT que usa esteganografía y Twitter para recibir comandos (Disponible en: http://blog.elevenpaths.com/2015/08/hammertoss-apt-que-usa-estaganografia-y.html. Consultado el: 15 de noviembre de 2015).

[17] This emerging malware sends secret messages and is practically impossible to detect. (Disponible en: http://qz.com/238561/this-emerging-malware-sends-secret-messages-and-is-practically-impossible-to-detect/ . Consultado el: 16 de Noviembre de 2015).

[18] Nueva técnica permite ocultar información en archivos ejecutables. (Disponible en: http://www.tendencias21.net/Nueva-tecnica-permite-ocultar-informacion-en-archivos-ejecutables_a6496.html Consultado el: 16 de Noviembre de 2015).

[19] La (in)seguridad de los sistemas TIC que tratan información clasificada. (Disponible en: http://www.blog.rielcano.org/la-inseguridad-de-los-sistemas-tic-que-tratan-informacion-clasificada/ Consultado el: 16 de Noviembre de 2015).

[20] El Arte de ocultar información: Esteganografía. (Disponible en: http://www.expresionbinaria.com/el-arte-de-ocultar-informacion-esteganografia/. Consultado el: 10 de Noviembre de 2015).

[21] Curso de privacidad y protección de comunicaciones digitales. (Disponible en: http://www.criptored.upm.es/crypt4you/temas/privacidad-proteccion/leccion7/leccion7.html. Consultado el: 10 de Noviembre de 2015).

[22] Esteganografía: el arte de pasar inadvertido. (Disponible en: http://www.editorialterracota.com.mx/pdf/Criptografia.pdf. Consultado el: 10 de Noviembre de 2015).

[23] La Guerra en la Antigua Grecia. (Disponible en: http://www.historiasimple.com/2009/07/la-guerra-en-la-antigua-grecia.html. Consultado el: 10 de Noviembre de 2015).

[24] Sobre la herejía y la Inquisición. (Disponible en: http://www.sindioses.org/sociedad/inquisicion.html. Consultado el: 12 de Noviembre de 2015).

[25] Inglaterra Siglo XVI. (Disponible en: http://www.inglaterra.net/inglaterra-siglo-xvi Consultado el: 12 de Noviembre de 2015).

[26] Un códice ocultista de hace 500 años Desvelado. (Disponible en: http://www.vopus.org/es/gnosis-gnosticismo/dimension-desconocida/esteganografia-de-trithemius--codice-desvelado.html. Consultado el: 12 de Noviembre de 2015).

[27] La Segunda Guerra Mundial. (Disponible en: http://www.resumendehistoria.com/2011/02/la-segunda-guerra-mundial-resumen.html . Consultado el: 12 de Noviembre de 2015).

[28] An Information-Theoretic Model for Steganography (Disponible en: https://www.zurich.ibm.com/~cca/papers/stego.pdf . Consultado el 15 de Noviembre de 2015).

[29] El Estudio De Las Marcas De Agua Del Papel Como Material Para Determinar La Datación Y Procedencia De Las Fuentes Histórico-Musicales, Y Su Grado De Fiabilidad. (Disponible en: http://digital.csic.es/bitstream/10261/36557/1/Ezquerro-2000-El%20estudio%20de%20las%20marcas%20de%20agua....pdf . Consultado el: 16 de Noviembre de 2015).

[30] Marcas de Agua en el Mundo Real. (Disponible en: http://digital.csic.es/bitstream/10261/8864/1/Marcas_de_agua_en_el_mundo_real.pdf . Consultado el: 16 de Noviembre de 2015).

[31] Juan Antonio Cano Salado, Borja Moreno Fernández, Pascual Javier Ruiz Benítez. 2 de junio de 2011. P. 4.

[32] Juan Antonio Cano Salado, Borja Moreno Fernández, Pascual Javier Ruiz Benítez. 2 de junio de 2011. P. 5.

[33] Juan Antonio Cano Salado, Borja Moreno Fernández, Pascual Javier Ruiz Benítez. 2 de junio de 2011. P. 5.

[34] Esteganografía: para cifrar mensajes en imágenes (Disponible en https://www.unocero.com/2012/11/28/esteganografia-para-cifrar-mensajes-en-imagenes/. Consultado el: 10 de noviembre de 2015).

[35] Esteganografía: para cifrar mensajes en imágenes (Disponible en https://www.unocero.com/2012/11/28/esteganografia-para-cifrar-mensajes-en-imagenes/. Consultado el: 10 de noviembre de 2015).

[36] DeepSound: Cómo ocultar información en archivos de música al estilo Mr. Robot (Disponible en http://www.redeszone.net/2015/10/31/deepsound-como-ocultar-informacion-en-archivos-de-musica-al-estilo-mr-robot/ Consultado el: 16 de noviembre de 2015).

[37] Esteganografía en Linux - Ubuntu (Disponible en http://xombra.com/index.php?do/articulos/nota/320/op/5/t/esteganografa-linux-ubunt Consultado el: 16 de noviembre de 2015).