Universidad de Buenos Aires

Facultades de Ciencias Económicas,

Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en

Seguridad Informática

Tema

Criptología

Título

Esteganografía,
Disciplina para ocultar información

Autor

Ing. Juan Miguel Sánchez Arteaga

Tutor

Dr. Pedro Hecht

Año de presentación

Cohorte 2017

Declaración jurada de origen de contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Juan Miguel Sánchez Arteaga
DNI: 95.760.575

Resumen

El presente trabajo recopila información de la esteganografía, disciplina para ocultar información. Proporciona una definición del tema, el propósito y la terminología utilizada. El documento repasa la historia y evolución, proporciona una clasificación lingüística y digital de acuerdo al tipo de esquema. Asimismo indica características de los algoritmos esteganográficos, una categorización de las técnicas esteganográficas y los requisitos para ocultar información. Además señala algunos programas informáticos que permiten incorporar un mensaje en otro para ocultarlo. También muestra el uso actual de la esteganografía desde el punto de vista legal e ilegal. Finalmente menciona de qué se trata el estegoanálisis, arte que se encarga de detectar la presencia de esteganografía.

Palabras clave: Esteganografía, estegoanálisis, información, mensaje, algoritmos, técnicas, clasificación, requisitos.

Tabla de contenidos

Agradecimiento

Cuando recibí la noticia de la admisión a la maestría, simplemente no creí, porque entre otras cosas, significaba vivir en la querida Argentina por algún tiempo. Para dar aquel paso, mi familia fue de gran ayuda. No existen palabras para agradecer el sacrificio que hicieron, pues este trabajo es apenas una pequeña retribución al esfuerzo que realizaron, pese al logro personal y profesional alcanzado.

También mi agradecimiento a los docentes y compañeros de cursada de la cohorte 2017. El nivel académico y profesional fue impresionante, permitiéndome aprender otra realidad que hasta ese momento desconocía.

"El tiempo de Dios es perfecto".

CAPITULO 1

1. Definición

1.1. Etimología

La palabra esteganografía proviene del griego *στεγανος* (steganos) que significa "cubrir", e *γραφος* (graphos) que significa “escritura”. Así, esteganografía significa literalmente “escritura encubierta” [1] [2].

1.2. Definición

La criptología es la disciplina científica que trata la escritura secreta, que los mensajes sean procesados de tal manera que dificulte o imposibilite la lectura de personas no autorizadas. Se divide por un lado en criptografía, que se define como el arte y la ciencia de transformar datos en una secuencia de bits que aparece como aleatoria y sin sentido para un atacante; por otro lado en criptoanálisis, que intenta identificar las debilidades de varios algoritmos criptográficos y sus implementaciones para explotarlos; y finalmente en la esteganografía [1] [2].

La esteganografía es el arte y la ciencia de ocultar información, hace que esos datos sean invisibles, escondiéndolos en algún portador, conocido también como portador (*cover*) [1], de tal manera que nadie, excepto el remitente y destinatario puedan detectar la existencia de la información [3].

De acuerdo a las definiciones presentadas, la esteganografía y la criptología podrían generar confusión, sin embargo, a diferencia de esta última, la esteganografía implica ocultar información, es decir, hacer parecer que no hay información oculta [4].

1.3. Clasificación

Dentro del ámbito de la ocultación de información, la esteganografía comparte lugar con otras técnicas y enfoques.

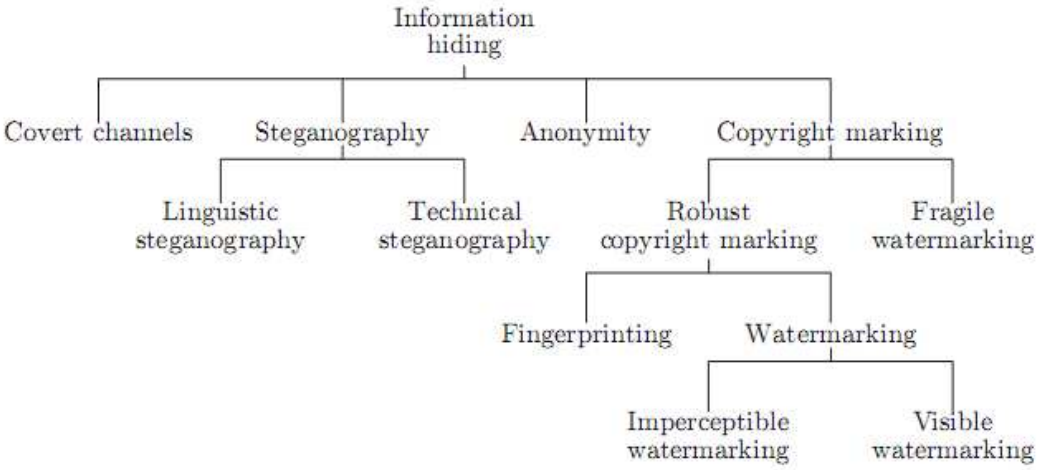

Ilustración 1: Clasificación de las técnicas de ocultación de información. Fuente [5]

1.4. Propósito

El objetivo de la esteganografía consiste en enlazar dos entidades en igualdad de condiciones para intercambiar mensajes ocultos, a través de un canal de comunicación inseguro, de tal manera que pase inadvertido por terceros que puedan tener acceso a dicho canal. Utiliza el concepto de "seguridad por oscuridad"; se refiere a que si nadie conoce la existencia de un mensaje oculto, nadie tratará de obtenerlo [6].

1.5. Terminología

La esteganografía al igual que otras disciplinas posee terminología propia que se describe a continuación [6].

Emisor: Entidad que enviará el mensaje por un canal a través de procedimientos predefinidos.

Receptor: Entidad inversa al emisor, realiza la operación contraria para reconstruir el mensaje.

Canal: Medio utilizado para transmitir un mensaje desde el emisor al receptor.

Portador: Cualquier tipo de dato susceptible de ser modificado para incorporar el mensaje a ocultar.

Embeber[1]: Es la acción de ocultar el mensaje dentro del portador. La recuperación posterior del mensaje oculto se conoce como extracción.

Estego-algoritmo: Denominación al algoritmo esteganográfico que indica la manera de realizar el procedimiento de incorporación del mensaje a ocultar.

Estego-clave: Denominación a una clave esteganográfica que define cómo aplicar el estego-algoritmo. Dentro del portador, ésta información podría indicar el lugar a partir del cual comienza a incorporarse el mensaje.

Estego-mensaje: Resultado del proceso de incorporar el mensaje a ocultar en un portador, en el que se aplica un estego-algoritmo, parametrizado por una estego-clave.

Esquema esteganográfico: Denominación al conjunto de componentes que permite la comunicación esteganográfica. Dentro de este esquema se encuentra la elección del tipo de portador, asimismo, los algoritmos para embeber y extraer el mensaje del portador y finalmente, la manera de transmitir el portador.

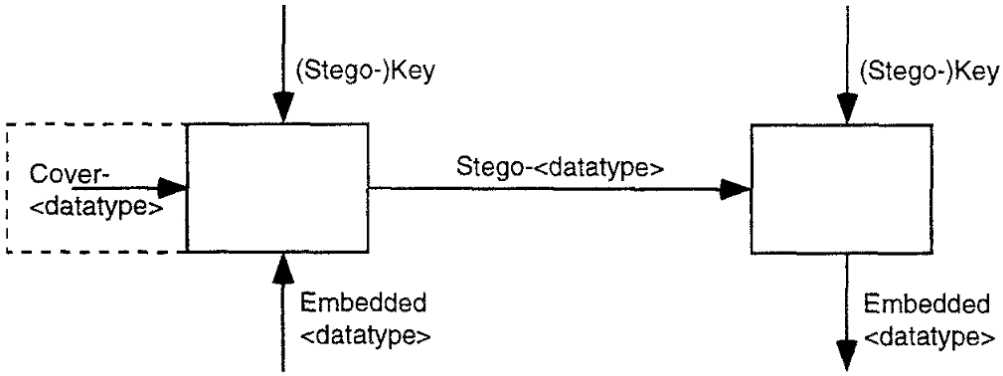

Ilustración 2: Esquema esteganográfico genérico acordado en el Primer Taller Internacional de ocultación de información. Fuente [7]

2. Historia y evolución

[1] Traducción literal de la palabra en inglés *embedded.* Proviene del verbo *embed* que significa incrustar, clavar, enterrar. https://dictionary.cambridge.org/es/translate/
Dentro del contexto esteganográfico y en el marco de este trabajo, la mejor traducción es "incorporar".

A continuación se presenta una evolución de las técnicas esteganográficas a través de la historia.

- **Tatuaje**

En 514 a. C., Darío I, rey de los persas, planea invadir Escitia a través de Tracia [8]. Construye un puente sobre el río Istros (hoy Danubio) y despliega un poderoso ejército. Los escitas al verse en inferioridad numérica deciden derribar dicho puente para aislar a los persas.

Histieo, tirano[2] de Mileto, impide el aislamiento del ejército al convencer a los jonios[3] no destruir el puente, ni rebelarse contra los persas, accionar del ateniense no por simpatía, sino por no estar preparados para enfrentarlos. El rey Darío I, lo premia con el título "consejero del rey" y compañero de la mesa Real, lo cual obliga acompañar al rey a Susa, capital persa de invierno.

Asimismo, Histieo logra que designen a un familiar suyo, Aristágoras, nuevo tirano de Mileto, maniobra que facilitaría posteriormente la rebelión contra los persas.

Al llegar el momento de la sublevación, Histieo debía comunicarse con Aristágoras, sin levantar la sospecha de los persas, sobre todo, que el mensaje no fuese interceptado en el camino por los puestos de guardia que controlaban a los viajeros. Entonces Histieo encuentra la solución en un esclavo, la cual fue afeitar su pelo, tatuar un mensaje en su cuero cabelludo, esperar a que crezca su cabello nuevamente y lo enviarlo a su familiar. El mensajero viajó desapercibido más de 2.400 Km, distancia existente entre Susa y Mileto.

---

[2] Tiranía: Desde la perspectiva de la Grecia antigua, el término tirano se refiere a un gobernante que ha accedido al poder de mediante la violencia, no por derecho, sino por la fuerza. https://es.wikipedia.org/wiki/Tiran%C3%ADa
Consulta: 03 10 2018.

[3] Jonio: Individuo perteneciente a la región de Jonia. En la antigua Grecia, Mileto era una gran metrópolis persa del Mar Egeo que formaba parte de dicho territorio.
https://es.wikipedia.org/wiki/Jonia
Consulta: 03 10 2018.

Finalmente, Aristágoras recibe al esclavo con la instrucción de rapar su cabello y leer el mensaje, que decía: “subleva Jonia”. Posteriormente esta acción desembocaría en las Guerras Médicas[4] [9].

Ilustración 3: Mapa invasión persa a Escitia sobre río Istros. Fuente [10]

- **Tablilla de cera**

Es una tableta de madera cubierta con una capa de cera. Para escribir y borrar se usa un estilete con raspador, respectivamente. Fue de gran utilidad para diferentes propósitos cotidianos, desde el periodo greco-romano hasta el siglo XIX [11].

[4] Guerras Médicas: Se conoce así a una fase de los conflictos entre griegos y persas que duró más de dos siglos. El historiador griego Heródoto, a través de su obra Historias, narra dichos enfrentamientos.
https://es.wikipedia.org/wiki/Guerras_m%C3%A9dicas
https://es.wikipedia.org/wiki/Her%C3%B3doto
https://es.wikipedia.org/wiki/Historias_(Her%C3%B3doto)
Consulta: 04 10 2018

En el siglo V, a. C., Demarato, griego exiliado en Persia, escribe en tabletas de madera, los planes persas de invadir Grecia; luego recubre con cera y envía las tablillas, de Susa a Esparta, sin ser detectado el mensaje en el trayecto. La información no fue descubierta durante un tiempo, incluso por sus receptores [12], hasta que Gorgo, esposa de Leónidas, vaticina el contenido real de dichas tablillas. Al leer el mensaje, los griegos pudieron armarse a tiempo y derrotar a los persas en las batallas de Termópilas, Salamina y Platea [13].

Ilustración 4: Tablillas de cera. Fuente [11].

- **Tinta invisible**

Llamada también "tinta simpática"[5], es un líquido que luego de aplicarse en alguna superficie concreta y secarse, se vuelve transparente, lo que permite ocultar información a la vista de los demás. Para recuperar dicha información, se requiere calor o alguna mezcla química que permita resaltar lo escrito.

El italiano Gayo Plinio Segundo, mejor conocido como "Plinio el Viejo", menciona en su obra "Historia Natural" que el líquido de una planta

[5] Definición Real Académia Española (RAE): "Composición líquida que tiene propiedad de que no sea visible con ella hasta el momento en que aplica el reactivo conveniente".
http://dle.rae.es/?id=Zo7qIdO
Consulta: 19 09 2018.

denominada Tithymalus puede usarse como tinta invisible [12]. Otros líquidos usados habitualmente han sido vinagre, zumos de frutas, orina y hasta semen, éste último utilizado por el MI6[6] en la Primera Guerra Mundial, ya que no reaccionaba a los vapores de yodo, técnica conocida en aquella época [14].

Asimismo, se conoce que el científico Giovanni Batista della Porta usaba huevos cocidos para esconder mensajes al mezclar alumbre y vinagre. Al escribir con dicha composición sobre la cáscara porosa, ésta se impregnaba en el huevo. Para leer el mensaje, bastaba con pelarlo [12] [15].

En la Segunda Guerra Mundial, la resistencia usaba activamente tinta simpática dentro de los campos de concentración nazi [16]. Además, las agencias de inteligencia alemana y estadounidense comprobaban que todas las cartas interceptadas no contengan tinta invisible; situación engorrosa, debido a la variedad de tintas y sustancias a comprobar [12].

- **Rejilla de Cardano**

A mediados del siglo XVI, el matemático italiano Girolamo Cardano inventa la 'tarjeta' que bautiza con su apellido. Se trata de una plantilla perforada en ciertos lugares, que al ser aplicada sobre un texto aparentemente trivial, permite descubrir letras o palabras del mensaje oculto. Únicamente quien posea una copia de la misma rejilla podrá conocer el mensaje. Por su parte, el texto que sirve para cubrir la información debe tener sentido para pasar desapercibido [15].

Por otro lado, para complicar más la detección, es posible que luego de encontrar una letra o palabra sea necesario rotar la plantilla 90 grados hacia la izquierda o derecha hasta volver a la posición original. Para recuperar el mensaje debe efectuarse el proceso inverso [17].

[6] MI6 (Servicio de Inteligencia Secreto): es la agencia de inteligencia exterior del Reino Unido.

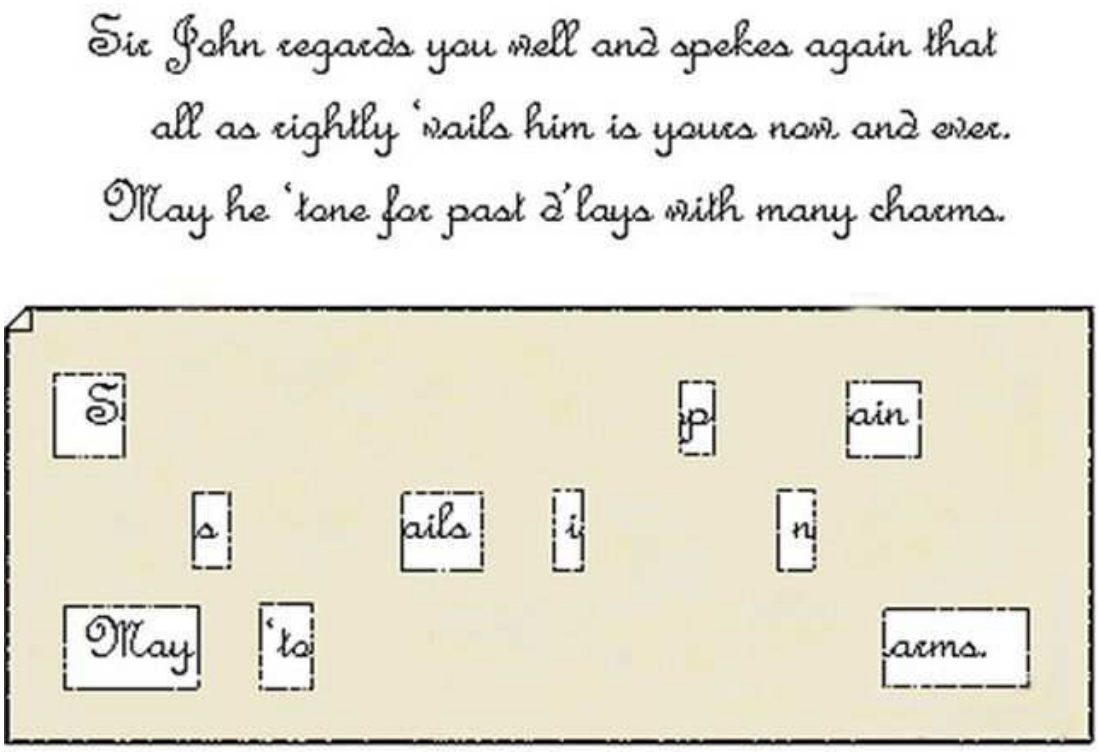

Ilustración 5: Reja de Cardano. Fuente [15]

- **Partituras musicales**

En el siglo XVII, el científico alemán Gaspar Schott, en su obra “Schola Steganographica” describe una manera de ocultar mensajes en partituras musicales, al asociar una letra del alfabeto con una nota del pentagrama. Si bien el resultado podía no producir una melodía agradable, el método funcionaba en papel [12].

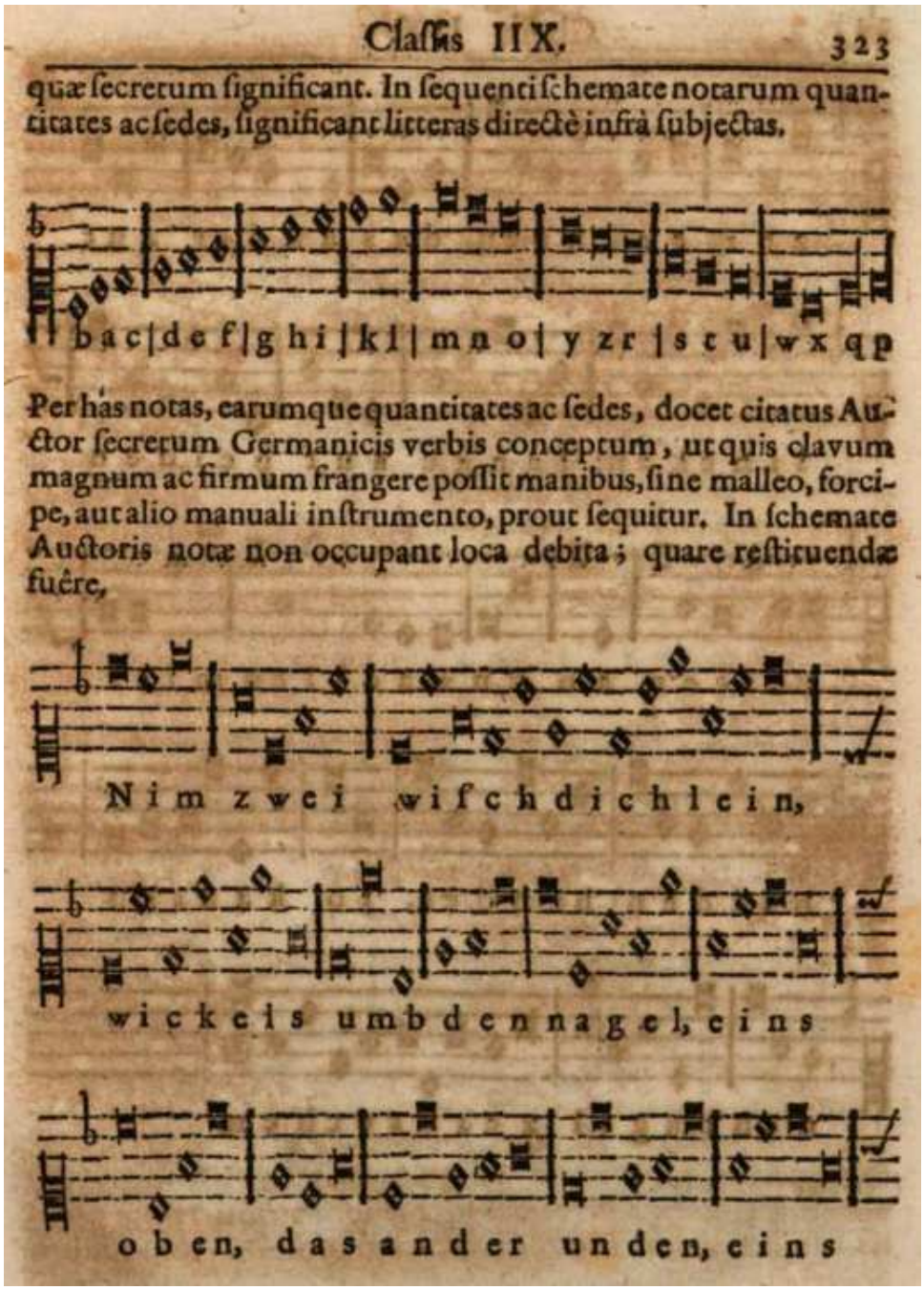

Ilustración 6: Asignación letra del alfabeto con nota musical. Fuente [18].

Las variaciones pueden ser diversas. Otro claro ejemplo para transmitir mensajes ocultos a través de partituras es utilizar una equivalencia de notas musicales y letras diferente, tal es el caso de la siguiente rueda.

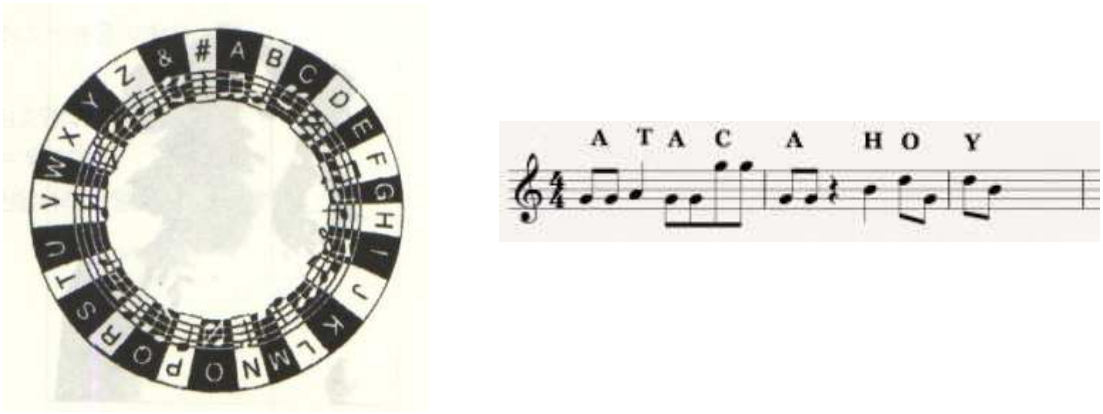

Ilustración 7: Otra asociación letra-nota musical. Fuente [19]

El célebre músico Johann Sebastian Bach compuso musicalmente su apellido a través del conocido “Motivo BACH”. En notación latina[7], se trata de la secuencia de notas Si bemol-La-Do-Si. De acuerdo a la notación musical alemana[8], la nota “Si bemol” se representa con la letra “B”, la nota “La” con la letra “A”, la nota “Do” con la letra “C” y la nota “Si” con la letra “H”. El motivo está presente en la parte final de su obra inconclusa “*Die Kunst der Fuge*” [20].

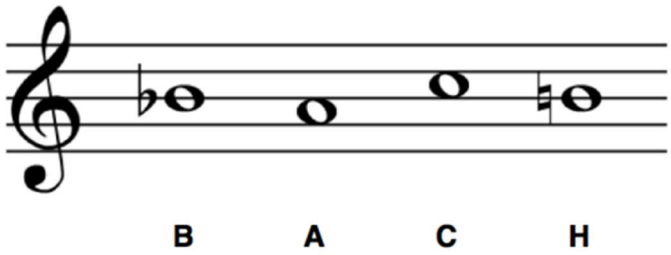

Ilustración 8: Motivo Bach. Fuente [20].

Si bien la asociación de notas musicales con letras del alfabeto correspondería a un cifrado por sustitución desde el punto de vista

[7] El sistema de notación musical latino, nombra las notas musicales a traves de las sílabas Do, Re, Mi, Fa, Sol, La y Si. El uso de sílabas facilita el solfeo, método de entrenamiento musical para enseñar entonación.
https://es.wikipedia.org/wiki/Sistema_de_notaci%C3%B3n_musical_latino
Consulta: 12 10 2018.

[8] La notación musical alemana, similiar al sistema de notación musical anglosajón, nombra las notas musicales por medio de letras del alfabeto. Existen ligeras variaciones de nomenclatura en algunas de las notas.
https://es.wikipedia.org/wiki/Sistema_de_notaci%C3%B3n_musical_anglosaj%C3%B3n
Consulta: 12 10 2018.

criptográfico, las partituras sirven como canal de encubrimiento y por ende cumple con el principio esteganográfico de pasar desapercibido, sobre todo ante no músicos.

- **Micropunto**

Técnica muy utilizada por el servicio militar alemán en la Primera y Segunda Guerra Mundial para ocultar información confidencial. Se trataba de la reducción fotográfica de textos a un tamaño menor a un milímetro de diámetro, para ser insertos dentro de un texto [12]. Dicha reducción, llamada microficha, se pegaba en algún punto de una letra o signo de puntuación, en una carta o sobre, la cual podía ser despegada por el receptor del mensaje para su lectura [21].

Este método fue descubierto en 1941 por los aliados, al percatarse del brillo inusual en la superficie del sobre de un presunto agente alemán [15].

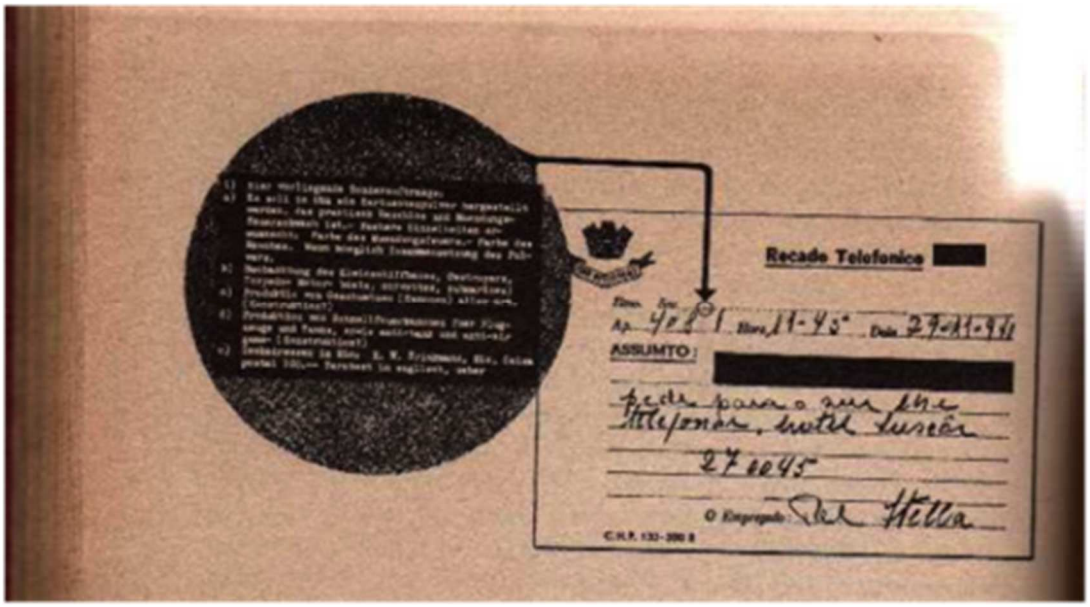

Ilustración 9: Reducción fotográfica de texto, micropunto alemán. Fuente [21]

- **Cifrado nulo**

Consiste en ocultar un mensaje a través de un texto aparentemente inofensivo. Durante la Primera Guerra Mundial, la Embajada alemana en Washington DC, enviaba mensajes por medio de telegramas a Berlín. Al

extraer el segundo carácter de cada palabra del párrafo siguiente se obtiene el mensaje oculto a comunicar [22].

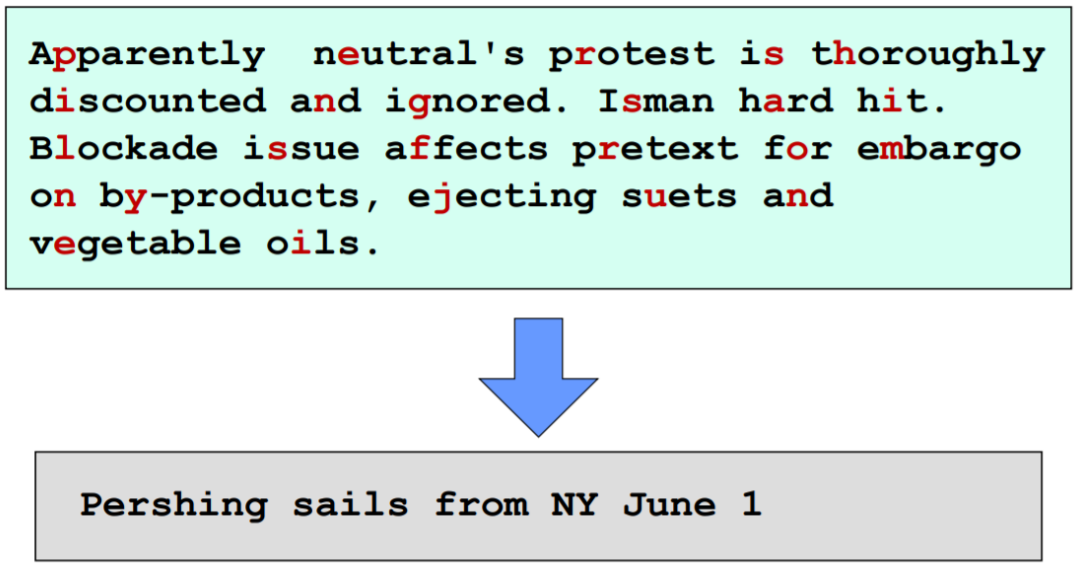

Ilustración 10: Mensaje secreto enviado por espía alemán usando cifrado nulo. Fuente [23]

CAPITULO 2

De acuerdo a la ilustración 11, la esteganografía se clasifica en dos grupos, la esteganografía digital que permite ocultar un mensaje en otro con ayuda de un computador y la esteganografía lingüística, que utiliza el lenguaje natural para enviar mensajes ocultos [24].

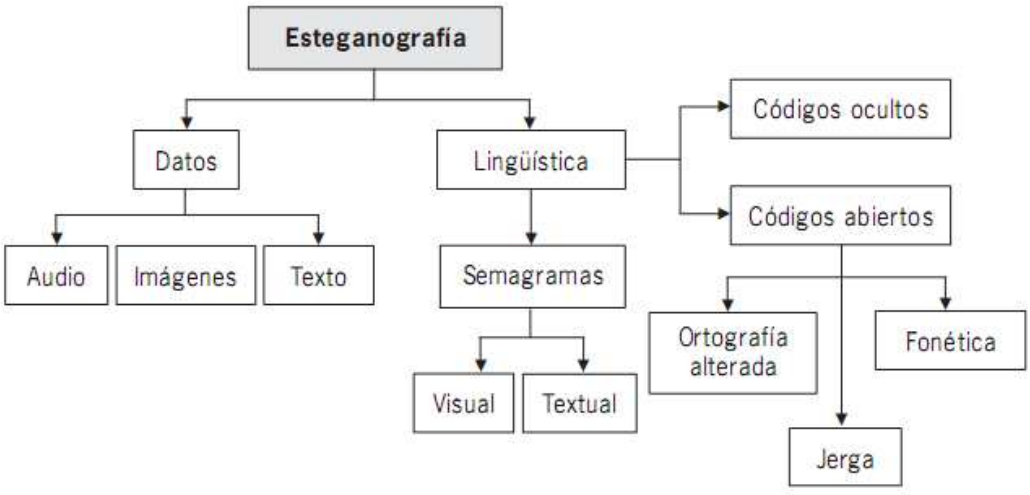

Ilustración 11: Clasificación de la Esteganografía. Fuente [24]

1. **Esteganografía Lingüística**

Se basa en la habilidad de las personas para comprender las palabras, el humor, los símbolos y ambigüedades que son propios del entendimiento del ser humano, equivalencia inexistente en los computadores. Si bien la Inteligencia Artificial ha dado pasos agigantados, aún dista que los computadores puedan reconocer caracteres en una imagen, por ejemplo el *captcha*, que es un método de autenticación para comprobar que quién se registra es un ser humano y no un robot.

- **Semagramas**

Los semagramas de texto consisten en pequeñas variaciones en la estructura de un documento, que aunque podrían ser visibles, no son fáciles de detectar. La técnica de ocultación se basa en la modificación horizontal o vertical de palabras y frases. Para el primer caso por ejemplo, se podría agregar espacios de tamaño fijo o variable entre palabras; para el segundo caso, modificar el tamaño del interlineado de un texto [12].

Por otro lado, los semagramas visuales, generalmente ocultan información objetos de uso cotidianos, tales como un garabato en una hoja, la posición de las manecillas del reloj en una imagen o la posición de los objetos en una mesa, debido a la poca atención que se presta a estos detalles [12].

- **Código abierto**

La esteganografía lingüística de código abierto oculta el mensaje en un texto legítimo, de manera que no es reconocible su existencia de inmediato. Se divide en ortografía modificada, jerga y fonética [24].

- **Ortografía modificada**

Se basa en cambiar la posición de las letras en una palabra, a fin de evitar la detección en programas de filtrado por palabras. Es posible conservar el significado de una palabra modificando su ortografía, con una cantidad infinita de variantes. Por ejemplo, la palabra “recursos humanos” podría

transmitirse como “*daareches umenos*”, “*direchs hoomans*” o “*dretsches humenos*” [24].

- **Fonética**

Es la ortografía por el sonido de las palabras, escribir lo que se escucha cómo se escucha [25]. La esteganografía lingüística resulta en utilizar los sonidos de un alfabeto diferente al habitual para comunicación. Por ejemplo, el alfabeto latín para los hablantes de árabe y viceversa [24].

Ilustración 12 : Esteganografía lingüistíca fonética. Fuente [24]

- **Jerga**

Se trata de la sustitución de expresiones por otras no tan comunes. El significado de las palabras, ya sean inventadas o no, son conocidas únicamente por el grupo de personas que entablan la comunicación y utilizan este lenguaje [12]. Las posibilidades de utilizar la jerga se limitan sólo por el vocabulario conocido por las partes que se comunican [24].

- **Códigos ocultos**

Emplean un método particular para ocultar el texto en el portador, el cual puede simular un comunicado relevante. La idea de esta técnica es que el portador no levante sospechas del mensaje que oculta en su interior [24].

2. Esteganografía Digital

La información secreta a ser transmitida puede ocultarse en diferentes medios. A continuación se especifica diferentes tipos de implementar esteganografía.

2.1. Esteganografía en imágenes

Se refiere a ocultar la información en archivos de imágenes a través de un mapa de bits, al cambiar el valor de ciertos bits que afecten lo menos posible la apariencia de la imagen.

Los colores que utiliza una imagen están representados por la cantidad de bits disponibles. Si posee 3 bytes significa que en la imagen existen los colores rojo, azul y amarillo, lo que produce toda una paleta de combinación de colores. Es recomendable utilizar imágenes en la escala de grises porque al cambiar el bit menos significativo en una imagen a color, podría no ser tan imperceptible el resultado, debido al nuevo color dentro de la paleta. En cambio en la escala de grises, la variación del color podría ser mínima. Se debe tener en cuenta que cada pixel se encontrará representado con 3 bytes en estos casos.

Existen varias técnicas para ocultar información. A través del bit menos significativo (LSB), consiste en codificar cada bit de la información a lo largo de la imagen, generalmente en zonas muy ruidosas para no llamar la atención, y luego reemplazar el último bit de cada byte por el bit del mensaje oculto.

Si al seleccionar 3 pixeles de una imagen se obtiene:

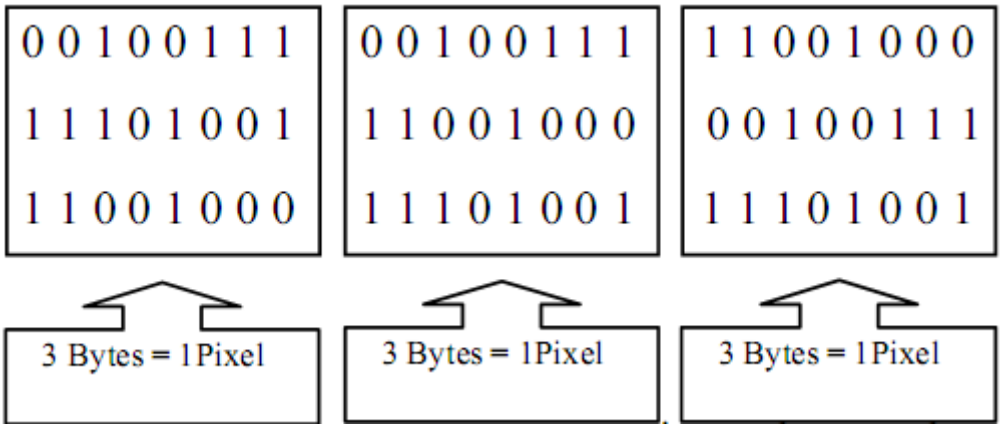

Ilustración 13: Pixeles de una imagen. Fuente [26]

Si se desea enviar de forma oculta la letra “C”, en código ASCII es 67, en binario es: 0 1 0 0 0 0 1 1. Al cambiar el valor por el bit menos significativo resultaría:

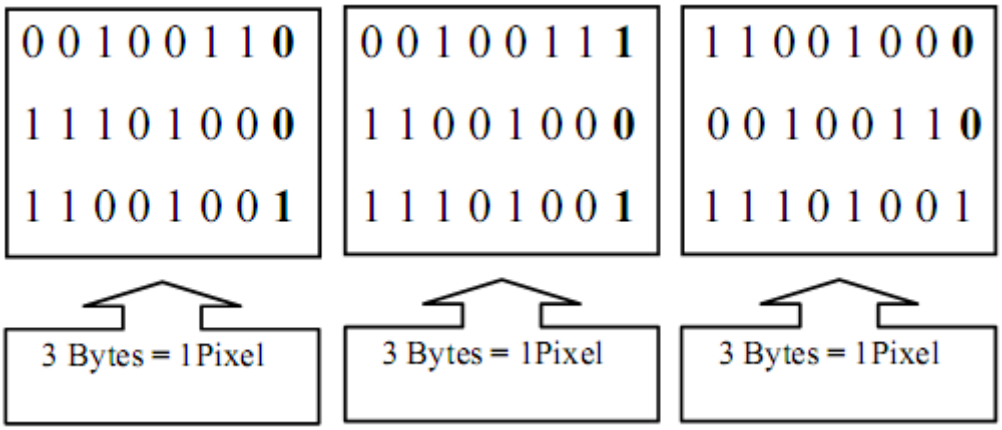

Ilustración 14: Información resultante al cambiar el LSB con el binario de la letra "C"

Este cambio es imperceptible para el ojo humano, no ocasiona ningún cambio ostensible en una imagen [26].

2.2. Esteganografía en audio

Los archivos de sonido también permiten ocultar información. A diferencia de los archivos de imagen, el ser humano sólo escucha un rango de frecuencia.

El formato .WAV es el más utilizado y recomendado para el almacenamiento de sonido; posee dos partes, el encabezado que contiene información del archivo, tales como la cantidad de canales, frecuencia de muestreo y tamaño de la muestra; y el sector de datos que es el sonido propiamente dicho, en forma de bits secuenciales.

En un archivo de sonido se puede extraer muestras de información de 8 bytes, por ejemplo: 45 23 120 31 128 44 76 89 y al convertirlos en binario resulta: 00101101 00010111 11110000 00011111 10000000 00101100 01001100 01011001.

A través de LSB, si se desea ocultar la información 200, que en binario equivale a 11001000, se reemplaza cada bit en el bit menos significativo de cada byte, así: 00101101 00010111 11110000 00011110 10000001 00101100 01001100 01011000. Al convertir a decimal se obtiene: 45 23 120 30 129 44 76 88, lo que evidencia una variación mínima comparada a los valores iniciales.

Otro caso puede apreciarse si se desea ocultar el mapa del aeropuerto de Burlington en un archivo de sonido, el sonido original con respecto al portador del mensaje se muestra de la siguiente manera:

Ilustración 15: Mapa del aeropuerto de Burlington. Fuente [26]

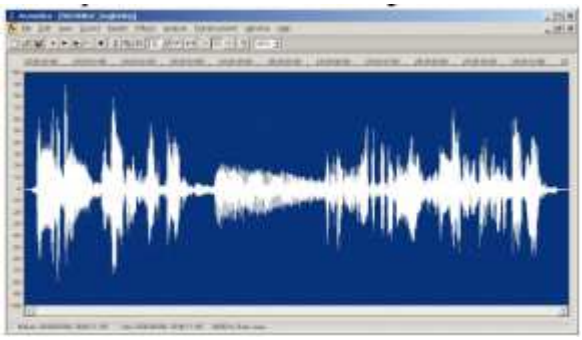

Ilustración 16: Archivo de sonido de encubierta. Fuente [26]

A continuación se muestra el espectro de sonido con la información oculta. Se aprecia una sutil diferencia respecto al archivo original, evidenciada en los círculos rojos [26].

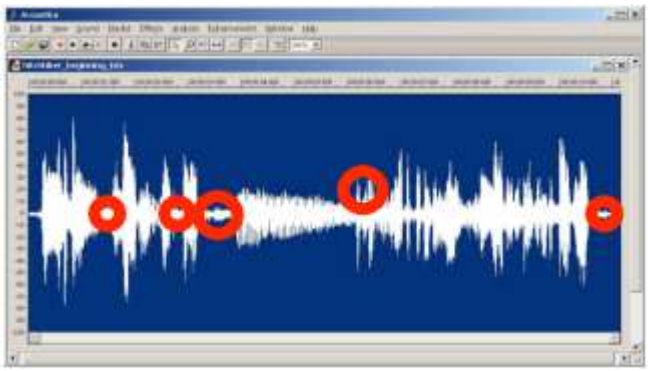

Ilustración 17. Archivo de sonido con mensaje oculto

2.3. Esteganografía en video

Los archivos de video generalmente son una colección de imágenes y sonidos, por lo que la mayoría de técnicas presentadas en imágenes y videos

y audio se puede aplicar a archivos de video. Usualmente se utiliza el método DCT que cambia ligeramente cada una de las imágenes del video hasta el punto que el ojo humano no lo perciba.

La ventaja de aplicar esteganografía en video es la gran cantidad de datos que puede ocultarse al interior por el hecho del flujo continuo de imágenes y sonido en movimiento. Cualquier distorsión pequeña puede pasar aparentemente desapercibida por el hombre [27].

2.4. Esteganografía en protocolos de comunicación UDP

Es posible crear canales ocultos en la mayoría de los protocolos de comunicación, mediante cierta manipulación del formato de los paquetes a enviar, a través del uso de campos reservados que no se validan, la reordenación de paquetes, etc.

El protocolo UDP se encuentra en el nivel de transporte y es un protocolo no orientado a la conexión, por lo que no es necesario que previamente se establezca una conexión entre dos entidades a nivel UDP. Cada paquete es independiente de los demás, además es un protocolo no es fiable porque no garantiza la entrega de información al destino, por lo que los datos pueden perderse, duplicarse o entregarse desordenados.

Ilustración 18: Paquete UDP. Fuente [12]

Mediante el campo puerto de origen se puede manipular el paquete UDP ya que permite indicar al receptor por qué puerto el emisor transmite información. Se puede utilizar para ocultar 16 bits por paquete UDP enviado. En muchas ocasiones el receptor no necesita conocer el puerto origen de transmisión, tal como en el establecimiento de una comunicación unidireccional de emisor a receptor [12].

2.5. Esteganografía en sistema de archivos

Los archivos utilizan bloques de almacenamiento, desde una perspectiva física. Debido a que el tamaño de un archivo no es un múltiplo exacto del tamaño del bloque, siempre hay un parte del bloque que no se usa y que está reservada para el archivo. Este espacio se conoce como fragmentación interna y también se usa para ocultar información. Una ventaja a destacar es que resulta invisible al sistema de archivos y a las herramientas de validación de archivos. Por otro lado, una desventaja es la portabilidad ya que si se realiza una copia del archivo con herramientas comunes, la información en el espacio de fragmentación interna se pierde. De igual manera si el archivo cambia de tamaño, para esos casos es preferible usar archivos que se conoce no variará en su longitud, tales como los archivos del sistema [12].

2.6. Esteganografía en formato de archivos

Esta técnica se denomina “End of File (EOF)” y consiste en añadir la información a ocultar al final de un archivo con estructura. Normalmente un sistema de ficheros carga e interpreta un formato de archivo y por ende lee los datos contenidos en la estructura definida, sin reconocer más allá del fin del fichero indicado en esa estructura. De esta manera se puede incorporar información sin que afecte el uso normal del mismo.

2.7. Esteganografía en borrado de información

Al borrar un archivo en el sistema de archivos, se elimina únicamente el enlace a los diferentes bloques que constituye dicho fichero, marcándose como disponibles. Hasta que no se sobrescriba en este espacio, la información permanece inalterada. Si bajo ciertas circunstancias es posible recuperar la información borrada, se puede catalogar este hecho como un mecanismo de ocultación de información.

CAPITULO 3

1. Características de algoritmos esteganográficos

Los estego-algoritmos poseen ciertos atributos que permiten determinar la fortaleza o debilidad de su utilidad [1].

1. Capacidad de incorporación

Es la cantidad de datos que puede ocultarse en el portador, en relación con el tamaño del mismo. La unidad de medida de este atributo es bit-por-bit (bpb). Un estego-algoritmo de estas características es ideal para ocultar una cantidad pequeña de datos, tal como un mensaje corto.

2. Invisibilidad

Cualquier dato oculto en el portador causa que el portador sea modificado. La invisibilidad mide la cantidad de distorsión del portador, por lo que es una medida cuantitativa. La mejor manera de medirla es mostrando el portador antes y después de la incorporación a diferentes observadores. El estego-algoritmo es calificado altamente invisible si ninguno de los observadores puede indicar la diferencia. Por lo tanto, la invisibilidad está vinculada a la percepción visual o auditiva del ser humano.

3. Indetectablilidad

Hace referencia a las propiedades estadísticas de los datos del portador. Si al examinarlo se compara con lo que se espera de ese archivo y se encuentra una diferencia importante, entonces genera sospechas de la presencia de información oculta. Un buen estego-algoritmo no debería modificar las propiedades estadísticas del portador. A diferencia de la invisibilidad, no depende de la percepción humana sino de las propiedades estadísticas de la información a ocultar.

4. Robustez

Es la capacidad del estego-algoritmo para mantener, sin cambios, los datos embebidos en el portador, incluso después que el portador haya sido sometido a varias modificaciones. Por ejemplo, si una imagen ha sido

sometida a ciertos cambios tales como filtros, rotación, ampliación, etc. Este atributo es importante cuando los datos ocultos consisten en derechos de autor, conocido como marca de agua.

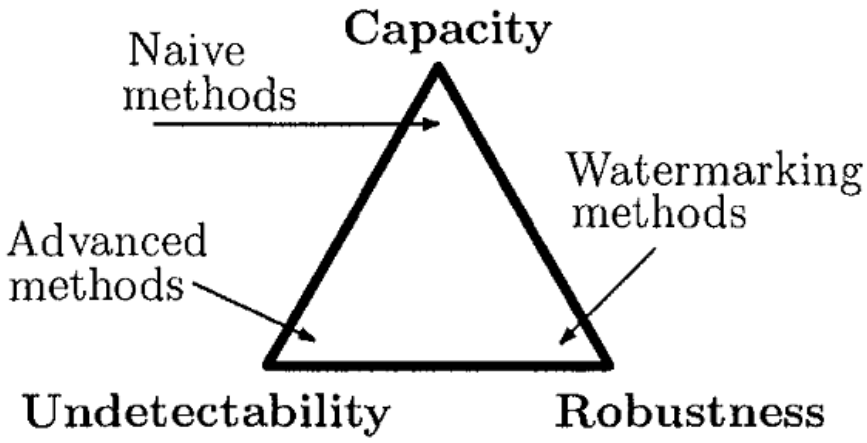

Ilustración 19: Relación estego-algoritmos. Fuente [1]

Habitualmente las técnicas de esteganografía que permiten ocultar mayor información (capacidad) son menos robustas y pasan desapercibidas (invisibilidad). Por el contrario, a mayor robustez normalmente se obtiene menor cantidad de información oculta [28].

2. Clasificación de técnicas esteganográficas

A continuación se enumeran algunas técnicas a través de la siguiente clasificación [29]:

2.1. Técnicas de Dominio Espacial

La información que se desea ocultar se inserta directamente de acuerdo a la intensidad de los píxeles. Es decir, algunos valores de los píxeles de la imagen cambian durante la ocultación de datos. Se subclasifica de la siguiente manera:

a) LSB (Least Significant Bit)

Este método reemplaza los bits menos significativos del objeto que servirá como encubridor conjuntamente con el mensaje oculto. Tiene baja complejidad computacional. Por lo tanto, para el ojo humano, la estego-imagen se verá idéntica a la imagen de portada. Aunque es un método

extremadamente fácil, es susceptible a la baja compresión y la manipulación de una imagen, como el escalamiento, la rotación, el recorte, etc. [30].

b) PVD (Pixel Value Differencing)

Esta técnica selecciona dos pixeles consecutivos en una imagen para esconder los datos. La información a ocultar está determinada al comprobar la diferencia entre ambos pixeles, se sustituye por otros similares en los que se incluye bits de datos a ocultar.

2.2. Spread Spectrum

En este método, la información oculta a transmitir se distribuye en un ancho de banda con frecuencia amplia.

La relación entre señal y ruido en cada banda de frecuencia debe ser tan pequeña a fin que sea difícil detectar la presencia de datos. Incluso si se eliminan partes de los datos de varias bandas, todavía existiría suficiente información en otras bandas para recuperar la información oculta. Por lo tanto, es difícil eliminar los datos por completo sin destruir por completo la cubierta. Esta técnica es muy robusta y es utilizada principalmente en comunicaciones militares.

2.3. Técnica estadística

Este método utiliza las propiedades estadísticas propias del objeto a usar como cubierta. Cuando las propiedades estadísticas del objeto cambian, se transfiere un “uno”, caso contrario el objeto no se modifica. [30].

2.4. Técnicas de Dominio Frecuencial

En esta técnica el mensaje secreto es incorporado en el dominio de frecuencia del portador. Es una forma más compleja de ocultar mensajes en una imagen debido a que usa diferentes algoritmos y transformaciones sobre esa imagen [29]. Los datos son incorporados en los coeficientes de cambio, transformados dentro del área de frecuencia mediante diversos métodos, tales como [30]:

2.4.1. Transformada Discreta de Fourier (DFT)

El proceso que transforma una señal digital definida en el dominio espacial a la misma señal en el dominio frecuencial se conoce como

DFT. En lugar de utilizar descomposición de senos y cosenos se utiliza la descomposición equivalente en exponenciales de números imaginarios [31].

2.4.2. Transformada Discreta de Coseno (DCT)

Es semejante a DFT porque toma un conjunto de puntos de dominio espacial y lo transforma en una representación equivalente en el dominio de frecuencias. Los vectores base se componen exclusivamente de funciones coseno muestreadas. Es la más usada en compresión de imágenes y videos. Produce coeficientes incorrelados, es decir, que no guarda relación lineal entre los valores. Los vectores base dependen únicamente del orden seleccionado de la transformada y no de la propiedades estadísticas de los datos de entrada [32].

La imagen se separa en sub-bandas con respecto a sus componentes de frecuencia (alta, media y baja) y así se obtiene los coeficientes DCT. Los coeficientes cuyo valor no supere un umbral dado, determinan las ubicaciones susceptibles para la incorporación de la información a ocultar [33].

2.4.3. Transformada Discreta Wavelet (DWT)

A diferencia de DFT y DCT, las cuales representan una señal en el dominio del espacio y en el dominio de frecuencia, respectivamente, DWT es capaz de proporcionar una representación para ambas interpretaciones simultáneamente. Como los senos y cosenos en la Transformada Discreta de Fourier, los wavelets son empleadas como funciones base para la representación de señales e imágenes. Cuando es aplicada a una imagen digital, se aplica un banco de filtrado proporcionando una matriz de coeficientes conocidos como coeficientes wavelets. Se obtiene tres matrices de aproximación llamadas sub-bandas de detalle horizontal, vertical y diagonal (HL, LH, HH). La sub-banda LL contiene la información más importante de la imagen, mientras que los detalles tienen valores próximos a cero [34].

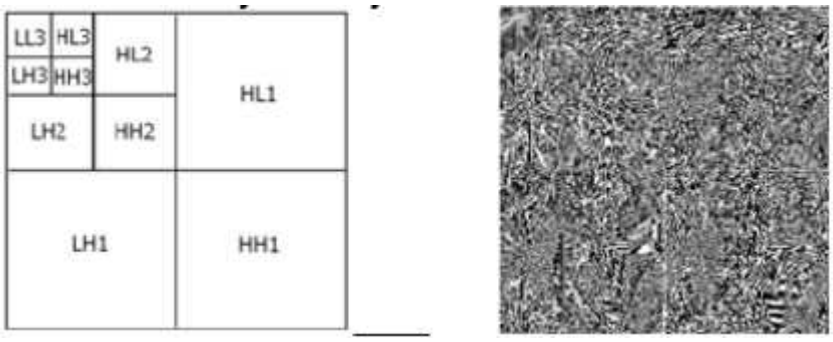

Ilustración 20: Descomposición imagen de tercer nivel DWT. Fuente [34]

La información a ocultar se incorpora en los coeficientes de detalle de la imagen para generar la menor distorsión posible en la estego-imagen [33].

2.5. Técnica de distorsión

En esta técnica, el mensaje oculto se almacena al distorsionar la señal. Una secuencia de modificaciones es aplicada a la cubierta a través de un codificador. Del lado del receptor, el decodificador mide las diferencias entre la cubierta original y la cubierta distorsionada para detectar la secuencia de modificaciones y recuperar el mensaje encubierto [29]. Los métodos de distorsión son menos seguros debido a que la cubierta original podría obtenerse para compararlo [30].

2.6. Enmascarado y filtrado

Este método se basa en el marcado de una imagen. Solo oculta la información cuando las marcas de agua son parte de la imagen. Esta técnica incorpora la información en las áreas más significativas en lugar de esconderla a modo de ruido. Las marcas de agua se pueden aplicar sin temor a la destrucción de la imagen ya que forman parte de la imagen. Este método se usa básicamente para imágenes de 24 bits y en escala de grises.

3. Requisitos para ocultar información

Las técnicas esteganográficas que permiten ocultar información deben cumplir algunos requisitos para que la esteganografía pueda aplicarse correctamente [35].

- La integridad de la información oculta después que ha sido incorporada en el estego-mensaje debe ser correcta. El mensaje secreto no debe cambiar de ninguna manera, así como la información adicional agregada, la pérdida de información o los cambios en la información secreta después que se ha ocultado. Si la información ocultada cambia durante la esteganografía, se anularía el proceso en este punto.
- El estego-mensaje debe permanecer sin cambios o casi sin cambios a simple vista. Si cambia significativamente y puede notarse, un tercero podría ver la existencia de dicha información y por lo tanto, intentaría extraerla o destruirla.
- Con respecto a la técnica de marca de agua, los cambios en el estego-mensaje no deben tener ningún efecto sobre la marca de agua resultante. Ante la manipulación de una copia ilegal de una imagen (por ejemplo, cambiar el tamaño, recortar o rotar) la marca de agua dentro de dicha imagen debe sobrevivir a estas manipulaciones, de lo contrario, terceros podrían quitarla fácilmente y romper la esteganografía en este punto.
- Finalmente, siempre se debe asumir que el atacante sabe que existe información oculta dentro del estego-mensaje.

CAPITULO 4

1. Herramientas actuales

En internet existen diversos programas que efectúan esteganografía. Los sitios web Info Sec Institute[9] [36] y Grey Campus[10] [37] proporcionan un

[9] InfoSec Institute es una fuente de capacitación en seguridad de la información. Enseñanza a profesionales de la seguridad de la información y de la información desde 1998 con amplia gama de cursos de capacitación relevantes.
https://resources.infosecinstitute.com/
Consulta: 09 11 2018

[10] Grey Campus es un proveedor líder de capacitación para profesionales que trabajan en las áreas de Gestión de Proyectos, Big Data, Ciencia de Datos, Gestión de Servicios y Gestión de Calidad.
https://www.greycampus.com/about-us
Consulta: 09 11 2018

listado actual de las diez mejores herramientas. En tal virtud, se proporciona las cinco aplicaciones coincidentes en ambos sitios web, las cuales aparecen en orden alfabético.

- **Camouflage**

Es una herramienta gratuita que se puede utilizar para ocultar un archivo en otro. Este es solo para Windows y el uso es extremadamente simple. La aplicación es fácil de usar, aunque se ha abandonado por algunas razones, sin embargo el software todavía está disponible para su uso y distribución gratuitamente. Se puede ocultar el archivo y enviar a cualquier lugar sin ser detectado [37].

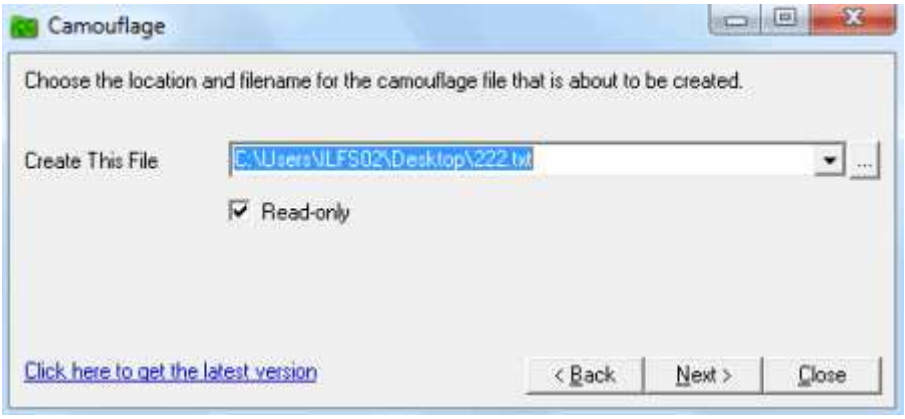

Ilustración 21 Camouflage. Fuente [38]

- **Hiden 'N' Send**

Permite ocultar cualquier tipo de archivo en un archivo de imagen .jpg. Es compatible con hash y cifrado de los datos. Por lo que añade una capa extra de seguridad. La interfaz de la herramienta es simple [36].

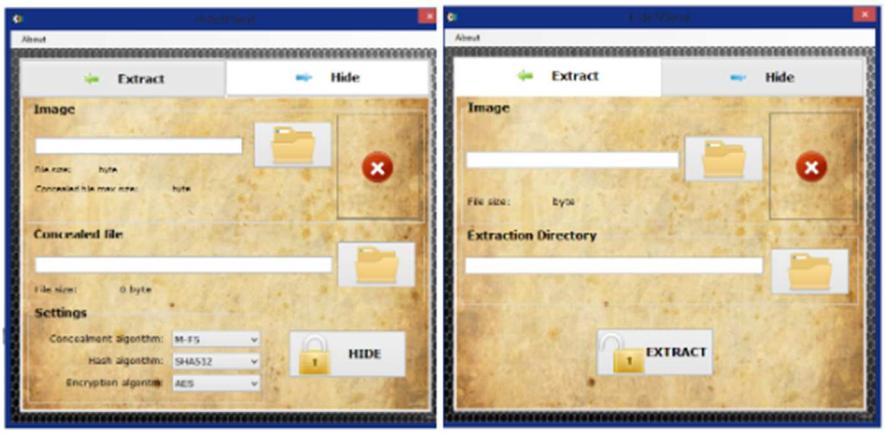

Ilustración 22. Hide 'N' Send. Fuente [37]

- **Image Steganography**

Es un software gratuito para ocultar información en archivos de imagen. Puede ocultar texto o archivos dentro de una imagen [36]. También muestra la capacidad del archivo de imagen portador. Asimismo, puede cifrar el archivo o el texto con contraseña [38].

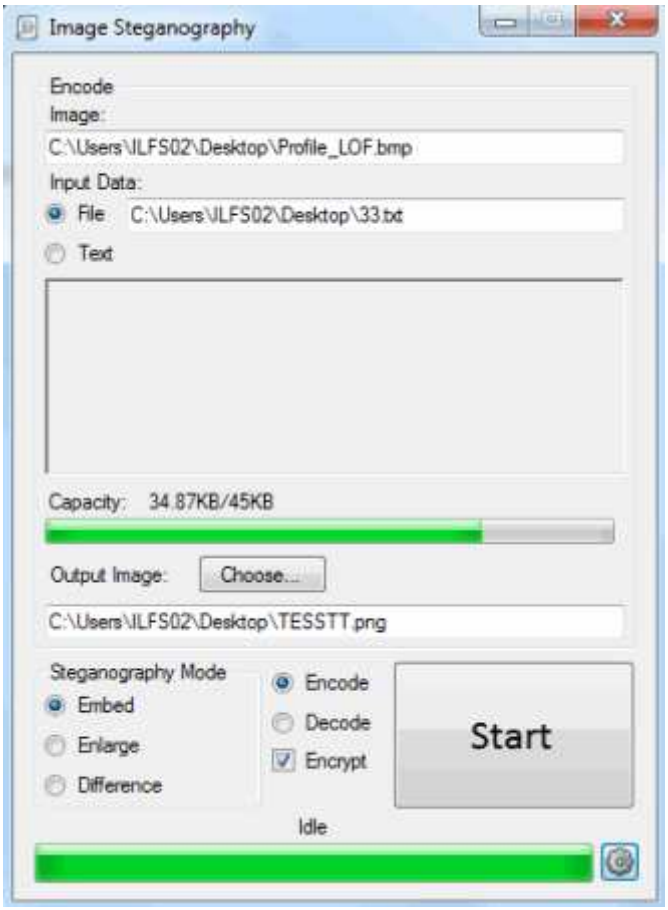

Ilustración 23: Image Steganography. Fuente [38]

- **Steghide**

Es un software de código abierto que funciona con líneas de comando, permite ocultar información en un archivo de imagen o audio. A pesar que fue desarrollada hace muchos años atrás funciona bien. Se ejecuta solo en versiones de 32 bits de Windows [36]. La herramienta puede ocultar datos en archivos JPEG, BMP, WAV y AU. Los datos embebidos están comprimidos, cifrados y etiquetados con *checksum*[11]. Los usuarios pueden elegir el

[11] Checksum (Suma de verificación): El propósito es proteger la integridad de los archivos al detectar cambios en su contenido, comprobando que no existan diferencias entre los valores obtenidos al hacer una verificación inicial y otra al final luego de haber compartido dichos datos. Generalmente se usa para verificar que un archivo compartido a un usuario es idéntico bit a bit facilitado por la fuente original.
https://blog-conocimientoadictivo.blogspot.com/2015/11/Que-es-el-CheckSum-Hash-MD5-SHA-1.html
Consulta: 09 11 2018

algoritmo de cifrado, aunque algoritmo predeterminado es Rijndael con clave de 128 bits, y *checksum* CRC32 [37].

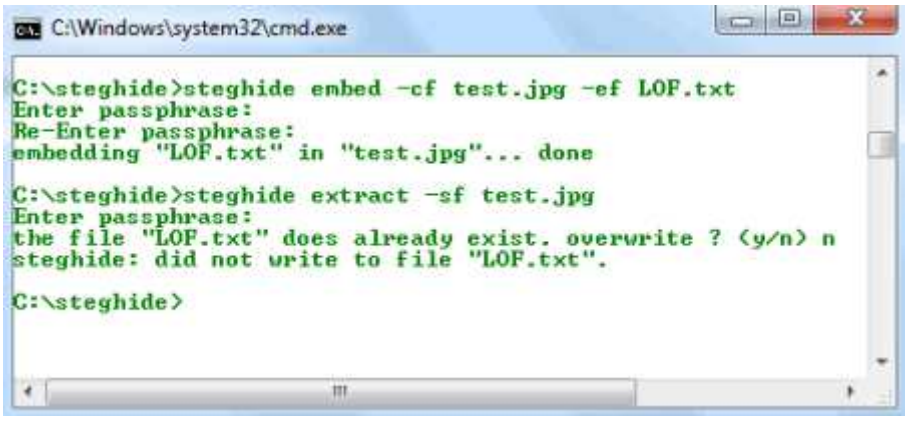

Ilustración 24: Steghide. Fuente [38]

- **Xiao Steganography**

Es un software gratuito que se usa para ocultar archivos en imágenes con formato .BMP o en archivos de audio con formato .WAV. La herramienta permite el cifrado de archivos, por lo tanto que puede seleccionarse entre varios algoritmos, tales como RC4, Triple DES, DES y hash SHA y MD5 [36].

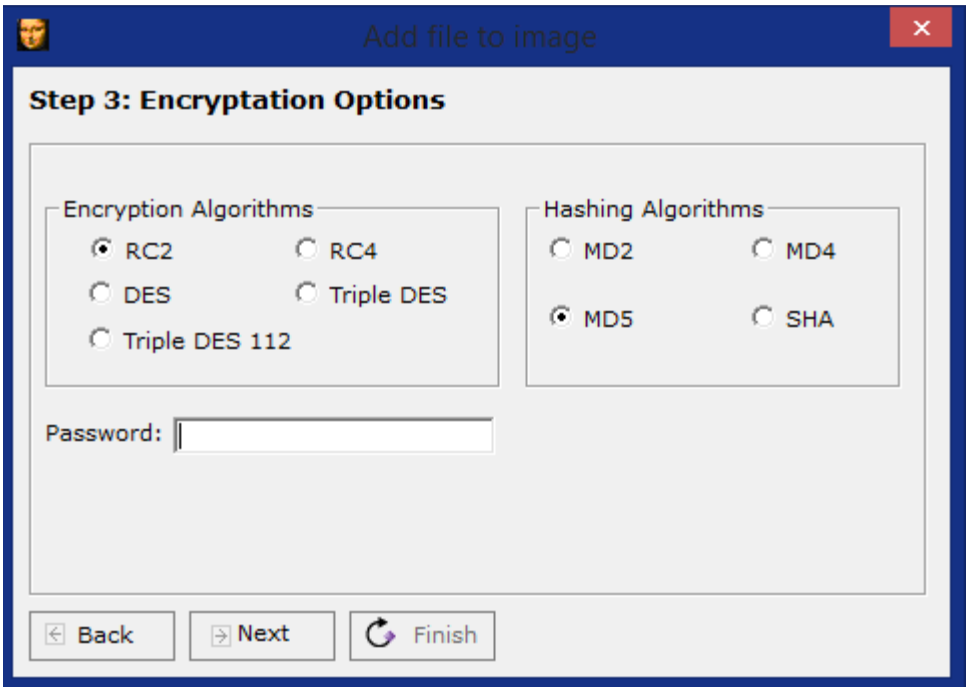

Ilustración 25: Xiao Steganography. Fuente [37]

- **VSL (Virtual Steganographic Laboratory)**

Se trata un software de código abierto de esteganografía y estegoanálisis de imágenes. Es una herramienta que utiliza diagramación gráfica de bloques [39]. A diferencia de otras herramientas, puede usar múltiples métodos esteganográficos y de estegoanálisis. También posee varias técnicas de distorsión que pueden ser usadas para probar la resistencia de los algoritmos esteganográficos ante cambios significativos en los archivos de imagen [40].

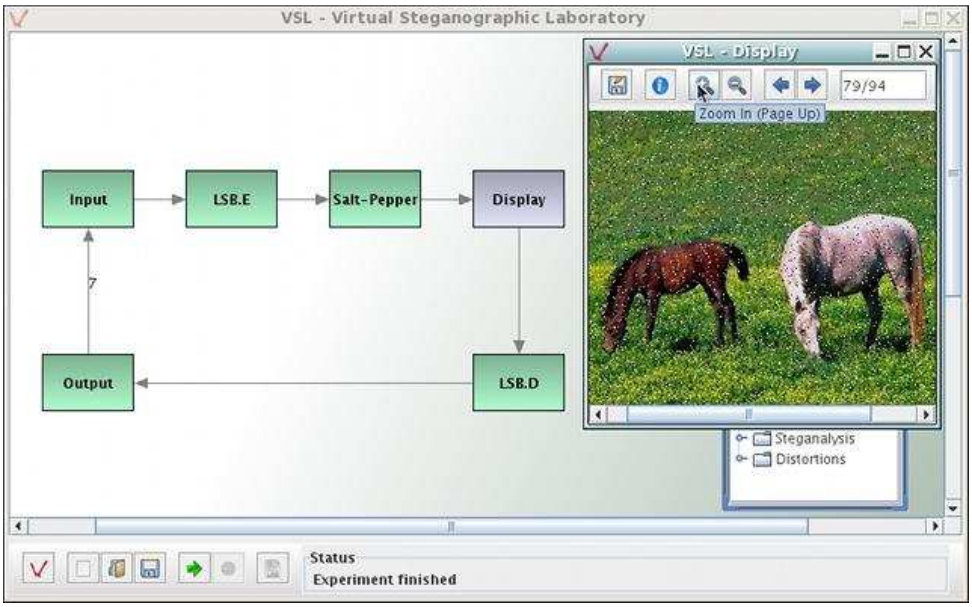

Ilustración 26: Virtual Steganographic Laboratory. Fuente [39]

El sitio web Hack Players proporciona un recopilatorio de herramientas de esteganografía y estegoanálisis clasificadas por categorías[12].

2. Esteganografía en la Seguridad Informática

Las técnicas esteganográficas tienen diversos usos, algunos legítimos y otros probablemente ilegales. Desde el punto de vista comercial, para la

[12] Recopilatorio de herramientas de esteganografía y estenoanálisis, disponible en https://www.hackplayers.com/2011/12/recopilatorio-de-herramientas-de.html
Consulta: 19 11 2018

protección de la propiedad, real e intelectual, el uso es muy fuerte. Las marcas de agua en los medios digitales están mejorando constantemente, principalmente para proporcionar marcas de agua robustas [41].

Por otro lado, el uso ilegitimo de la esteganografía, por ejemplo, para casos de pornografía infantil, donde fotos o videos se embeben dentro de archivos de imagen o sonido legales [41].

Un informe anual sobre delitos de alta tecnología enumera nueve tipos comunes de delitos informáticos: comunicaciones criminales, fraude, hacking, pagos electrónicos, juegos de azar y pornografía, acoso, delitos de propiedad intelectual, virus y pedofilia. En todas estas áreas se podría utilizar esteganografía [41].

Según el Washington Post, agentes federales encontraron al menos tres años de evidencia, "*que el grupo de Bin Laden incluyó comunicaciones secretas en correos electrónicos y sitios web mundanos*". Aún no hay evidencia directa de que los terroristas hayan usado estas tecnologías en la planificación de los ataques del 11 de septiembre de 2001 [42].

3. Estegoanálisis

El arte de detectar esteganografía se conoce como estegoanálisis. Es el proceso de identificación de la esteganografía mediante la inspección de varios parámetros en un medio-estego. El paso principal de este proceso es identificarlo, después determinar si ese medio contiene un mensaje oculto o no y luego intentar recuperar el mensaje. En el criptoanálisis, está claro que el mensaje interceptado está cifrado y ciertamente contiene el mensaje oculto porque el mensaje está codificado. En el caso del estegoanálisis esto puede no ser cierto. Los medios sospechosos pueden o no estar con un mensaje oculto. El proceso de estegoanálisis comienza debido a un flujo de información sospechoso [27].

Desde el punto de vista técnico, para los ordenadores es relativamente fácil detectar contenido esteganográfico, aunque tienen que ser configurados primero para buscarlos. La ventaja del uso de la esteganografía proviene del principio "una aguja en un pajar". Cada día, millones de imágenes, archivos de audio y documentos de texto son enviados en internet. Estos no levantan

sospechas y a diferencia de los mensajes cifrados, normalmente no son capturados para ser analizados. Compartir una colección de música presenta la oportunidad de incluir un mensaje corto en una de las canciones [24].

El principio de “una aguja en un pajar” sólo funciona si hay un “pajar”. Al compartir siempre fotos o canciones, la oscuridad del mensaje aumenta cuando se envía simplemente una foto o una canción más. No utilizar imágenes comunes o fuera de contexto, tampoco descargar imágenes de internet para ocultar información, porque un intruso podría descargar la misma imagen y comparar las dos digitalmente. Es decir, no se debe revelar las prácticas esteganográficas mediante una anomalía [24].

Conclusión

La Esteganografía ha estado presente hace muchos siglos atrás, desde la necesidad misma del ser humano en comunicarse con otros de manera privada. Bajo esa premisa, se ha puesto a prueba la inteligencia del hombre para diseñar diferentes formas para enviar mensajes indistintamente del medio. Por ejemplo, tatuar información en el cuero cabelludo de esclavos o la escritura de mensajes bajo la cera de tablillas propias de la época han sido maneras muy sencillas de transmitir información oculta sin que se enteren terceros. Algo muy ingenioso y sorprendente para el autor del presente trabajo fue el micropunto, tecnología sofisticada para los tiempos de la Primera y Segunda Guerra Mundial. Hasta que la citada manera de enviar información fuera detectada, muchos comunicados se transmitieron satisfactoriamente, pues en primera instancia, nadie pensaría que en un punto que forma parte de un documento, albergaría gran cantidad de información.

Actualmente las computadoras elaboran todo el proceso esteganográfico. En la red existen muchas herramientas que permiten realizar este arte, algunas de ellas han sido agregadas al presente trabajo. Hoy en día Internet es el medio generalizado para la comunicación. Cientos de miles de correos electrónicos son enviados en el mundo, muchos con información importante y otros tantos con información trivial. Y justamente esa trivialidad puede ser aprovechada para enviar información sin crear sospechas. Si entre dos personas es común compartir fotografías de las vacaciones de verano o el último disco del artista preferido, entonces enviar un archivo más con información oculta sería casi insospechado para un estegoanalista. Es como encontrar una aguja en un pajar. Si a esto se suma el uso de criptografía para cifrar esa información oculta, la comunicación efectiva entre las partes podría ser casi perfecta. Suena muy interesante, porque la criptografía no radica su fortaleza en ocultar la existencia del cifrado o en el algoritmo criptográfico, sino en sus claves de cifrado y descifrado, las cuales ambos entes previamente acordarán usar. Por su parte, la fortaleza de la esteganografía radica en desconocer la existencia de información oculta, si no se sabe dónde buscar, tampoco se sabe qué encontrar.

La Esteganografía y la Criptografía son creaciones del hombre, si son buenas o malas no es menester del autor en decidir y dar una respuesta, sin embargo, el autor piensa que todo radica en el uso que se quiera dar. La comunicación privada es un derecho, el problema está en las intenciones de esa privacidad. Si la finalidad atenta contra la seguridad ciudadana, contra la integridad de las personas, entonces mal podría culparse a estas "herramientas" sino al ser humano mismo. Por ejemplo, no existe documentación oficial que verifique y corrobore que se haya usado Esteganografía para la planeación de lo sucedido el 11 de septiembre de 2001, pero tampoco hay información que diga lo contrario, aunque de acuerdo a la información presentada en este documento, tampoco es imposible negarlo. Asimismo, otro uso ilegitimo de la esteganografía es la pornografía infantil, inaceptable bajo cualquier punto de vista en cualquier parte del mundo. Lamentablemente lo lucrativo que puede llegar a ser este vil negocio, hace que se utilicen técnicas para ocultar películas, fotos y videos de esta índole, en archivos "inofensivos" que sirven de encubierta.

Por otro lado, desde la legalidad, la esteganografía tiene gran utilidad. Por ejemplo, el uso de marcas de agua en fotografías es cada vez más común. La tecnología avanza siempre y lo que se busca es la robustez de las mismas para que no sean eliminadas ante un ataque de borrado. Asimismo el uso para propiedad intelectual. Por ejemplo, los discos de música de un artista o banda musical generados por una compañía disquera, que certifican la autenticidad del producto, aunque últimamente hayan perdido presencia en el mercado debido a nuevos modelos de negocio de compra y compartición, ahora vía streaming.

Finalmente, el motivo para elegir a la Esteganografía como tema de este trabajo se debe a que fue presentada sucintamente en una cátedra de la asignatura Criptografía, la cual generó gran interés e interrogantes. El autor concluye que la elección de este tema fue correcta, porque la presente investigación sumada a lo aprendido en la materia del postgrado, generó conocimiento y valor agregado en el autor. Aplicar ambas disciplinas para

mantener una comunicación “segura” podría ser otro tema de investigación. Los algoritmos criptográficos y las técnicas esteganográficas están a disposición en la red, por lo que elaborar una prueba de concepto que posible realizar, incluso para cualquier otro cursante de la maestría de Seguridad Informática.

Bibliografía

[1] D. Salomon, Coding for Data and Computer Communications, Springer, 2005.

[2] D. V. S. A. Joseph Raphael, *Cryptography and Steganography – A Survey.*

[3] K. A. N. P. Md. Khalid Imam Rahmani, *A Crypto-Steganography: A Survey,* vol. Vol5, (IJACSA) International Journal of Advanced Computer Science and Applications, 2014.

[4] D. B. D. G. S. M. &. P. D. Samir K Bandyopadhyay, *A Tutorial Review on Steganography,* 2008.

[5] R. J. A. a. M. G. K. Fabien A. P. Petitcolas, *Information Hiding - A Survey,* July 1999.

[6] P. A. Deymonnaz, *Análisis de vulnerabilidades esteganográficas en protocolos de comunicación IP y HTTP,* 2012.

[7] B. Pfitzmann, *Information Hiding Terminology.*

[8] «Arre caballo,» [En línea]. Available: https://arrecaballo.es/edad-antigua/primeros-jinetes/escitas-contra-persas/. [Último acceso: 03 10 2018].

[9] F. J. Tostado, «franciscojaviertostado.com,» 19 05 2014. [En línea]. Available: https://franciscojaviertostado.com/2014/05/19/el-tatuaje-que-origino-una-guerra/. [Último acceso: 03 10 2018].

[10] J. Sanz, «Historias de la Historia,» 12 08 2012. [En línea]. Available: http://historiasdelahistoria.com/2012/08/01/un-tatuaje-en-la-cabeza-el-pistoletazo-de-salida-de-las-guerras-medicas. [Último acceso: 04 10 2018].

[11] «Wikipedia,» 02 09 2018. [En línea]. Available: https://es.wikipedia.org/wiki/Tablilla_de_cera. [Último acceso: 04 10 2018].

[12] D. A. Muñoz, «Cript4you Aula Virtual,» 02 01 2014. [En línea]. Available: http://www.criptored.upm.es/crypt4you/temas/privacidad-proteccion/leccion7/leccion7.html. [Último acceso: 18 09 2018].

[13] M. L. E. G. d. C. Jesús Ortega, Intruducción a la Criptografía: historia y actualidad, Murcia: Universidad de Castilla-La Mancha, 2006, p. 21.

[14] «El Mundo,» 21 09 2010. [En línea]. Available: http://www.elmundo.es/elmundo/2010/09/21/internacional/1285079741.html. [Último acceso: 18 09 2018].

[15] C. Sánchez, «Hoja de Router, El Diario.es,» 12 09 2016. [En línea]. Available: https://www.eldiario.es/hojaderouter/seguridad/esteganografia-historia-tinta_invisible-mensajes_ocultos_0_557844630.html. [Último acceso: 19 09 2018].

[16] D. Master, «Introducción a la Esteganografía,» 2004. [En línea]. Available: https://radiosyculturalibre.com.ar/compartir/biblioteca/INFOSEC/death-master/Esteganografia.pdf. [Último acceso: 19 09 2018].

[17] «Wikipedia,» 05 11 2016. [En línea]. Available: https://es.wikipedia.org/wiki/Rejilla_de_Cardano. [Último acceso: 06 10 2018].

[18] G. Schott, Schola Steganographica, MDCLXXX.

[19] «Codificando Escarabajos,» 14 11 2010. [En línea]. Available: https://codificandoescarabajos.wordpress.com/2010/11/14/criptografia-musical/. [Último acceso: 19 09 2018].

[20] «Wikipedia,» 29 05 2015. [En línea]. Available: https://es.wikipedia.org/wiki/Motivo_BACH. [Último acceso: 12 10 2018].

[21] Y. FM, «Xataka,» 15 08 2016. [En línea]. Available: https://www.xataka.com/historia-tecnologica/cuando-una-imagen-oculta-mas-informacion-de-lo-que-parece-que-es-y-como-funciona-la-esteganografia. [Último acceso: 25 10 2018].

[22] G. Kessler, «FBI - Forensic Science Communications,» 06 2004. [En línea]. Available: https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/july2004/research/2004_03_research01.htm. [Último acceso: 26 10 2018].

[23] «Association for Computing Machinery,» 10 05 2015. [En línea]. Available: http://csus.acm.org/files/2015/ACM-Spring2015-Steganography.pdf. [Último acceso: 25 10 2018].

[24] D. Vitaliev, *Seguridad y privacidad digital para los defensores de los Derechos Humanos,* 2009.

[25] L. E. Santana, *Diferencia entre escritura fonética y ortografía fonética,* Santo Domingo, 2017.

[26] O. S. B. L. Angulo Carlos, *Una Mirada a la Esteganografía,* Pereira: Universidad Tecnológica de Pereira, 2007.

[27] P. J. L. G. Ronak Doshi, *Steganography and Its Applications in Security,* International Journal of Modern Engineering Research (IJMER), 2012.

[28] P. F. Iglesias, «Pablo Yglesias, #MundoHacker: Esteganografía, el arte de ocultar información sensible,» 28 04 2015. [En línea]. Available: https://www.pabloyglesias.com/mundohacker-esteganografia/. [Último acceso: 09 11 2018].

[29] D. V. Jasleen Kour, *Steganography Techniques - A Review Paper,* International Journal of Emerging Research in Management & Technology, 2014.

[30] P. K. Priyanka Sharma, *Review of Various Image Steganography and Steganalysis Techniques,* International Journal of Advanced Research in Computer Science and Software Engineering, 2016.

[31] J. D. Vico, *Esteganografía y Estegoanálisis: Ocultación de datos en streams de audio vorbis,* Universidad Politécnica de Madrid, 2010.

[32] J. L. M. N. H. P. Carlos Velasco, *Esteganografia en una imagen digital en el dominio DCT,* México, DF, 2007.

[33] D. B. R. R. Diego Renza, *Método de ocultamiento de pixeles para esteganografía de imágenes en escala de grises sobre imágenes a color,* ISSN:1794-9165 | ISSN-e: 2256-4314, 2016.

[34] M. G. A. H. R. P. J. R. Alejandro Padrón, *Ocultamiento de datos en imágenes digitales mediante BPCS,* Xalapa, 2008.

[35] P. D. S. L. a. R. P. Jonathan Cummins, *Steganography and Digital Watermarking,* 2004.

[36] P. Shankdhar, «Info Sec Institute,» 28 02 2018. [En línea]. Available: https://resources.infosecinstitute.com/steganography-and-tools-to-perform-steganography/#gref. [Último acceso: 09 11 2018].

[37] H. Passi, «Grey Campus,» 05 10 2018. [En línea]. Available: https://www.greycampus.com/blog/information-security/top-must-have-tools-to-perform-steganography. [Último acceso: 09 11 2018].

[38] A. Kumar, «List of Freeware,» [En línea]. Available: https://listoffreeware.com/list-of-best-free-steganography-software-for-windows/. [Último acceso: 09 11 2018].

[39] «VSL: Virtual Steganographic Laboratory,» 11 04 2013. [En línea]. Available: https://sourceforge.net/projects/vsl/?source=typ_redirect. [Último acceso: 09 11 2018].

[40] A. Paz, «Gurú de la Informática, Herramienta para realizar técnicas de esteganografía y estegoanálisis,» [En línea]. Available: https://www.gurudelainformatica.es/2014/08/herramienta-para-realizar-tecnicas-de.html. [Último acceso: 09 11 2018].

[41] S. Institute, *Steganography: Past, Present and Future,* 2001.

[42] S. Institute, *Hiding in Plain View: Could Steganography be a Terrorist Tool?,* 2001.