UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

CARRERA DE SOFTWARE

TRABAJO DE INTEGRACIÓN CURRICULAR
PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERO EN SOFTWARE

FORMA: PROYECTO DE INVESTIGACIÓN

TEMA:

COMPARACIÓN DE LAS HERRAMIENTAS ESTEGANOGRÁFICAS PARA OCULTAR INFORMACIÓN EN ARCHIVOS GRÁFICOS

AUTOR:

VELOZ BECERRA LUIS ALVARO

DIRECTOR:

Dr. HENRY VALLEJO

GUARANDA – ECUADOR

2023

TEMA DEL PROYECTO DE INVESTIGACIÓN

COMPARACIÓN DE LAS HERRAMIENTAS ESTEGANOGRÁFICAS PARA OCULTAR INFORMACIÓN EN ARCHIVOS GRÁFICOS.

AGRADECIMIENTO

Agradezco a Dios por la salud y vida que me brindo en todo momento, me supo guiar por un buen camino especialmente en mi formación académica, a mis padres por el apoyo incondicional que cada día me lo supieron dar con sus palabras, consejos y valores las cuales fueron un pilar fundamental para cumplir mis objetivos; también a mis hermanos y a toda mi familia que de una u otra manera influyeron para darme las fuerzas y no rendirme a pesar de las circunstancias las cuales fue de mucha ayuda para culminar con éxito esta importante etapa de mi vida.

A todos mis profesores que en el transcurso de mi vida estudiantil me brindaron sus enseñanzas las cuales contribuyeron para formarme como profesional, a mi tutor Dr. Henry Vallejo, por brindarme la oportunidad de realizar el presente trabajo de investigación y por sus valiosas orientaciones para llevarlo a cabo, a mis pares académicos Ing. Galuth García y Dr. Carlos Taco, por sus consejos y guías durante el desarrollo del proyecto.

DEDICATORIA

Dedico el proyecto de investigación a mi familia, en especial a mis padres ya que son un pilar fundamental en mi vida, porque siempre me acompañaron durante todo el transcurso de mi vida estudiantil, me apoyaron en todo sentido para que pudiera alcanzar esta etapa de mi vida, a mis hermanos que siempre estuvieron ahí cuando más los necesitaba ya que son mi inspiración para seguir adelante.

CERTIFICADO DE VALIDACIÓN

Dr. Henry Vallejo, Ing. Galuth García y Dr. Carlos Taco, en su orden Director y Pares Académicos del Trabajo de Integración Curricular "COMPARACIÓN DE LAS HERRAMIENTAS ESTEGANOGRÁFICAS PARA OCULTAR INFORMACIÓN EN ARCHIVOS GRÁFICOS" desarrollado por el señor Veloz Becerra Luis Alvaro.

CERTIFICAN

Que, luego de revisado el Trabajo de Integración Curricular en su totalidad, cumple con las exigencias académicas de la carrera SOFTWARE, por lo tanto, autorizamos su presentación y defensa.

Guaranda, 09 de junio del 2023

Dr. Henry Vallejo
Director

Ing. Galuth García
Par Académico

Dr. Carlos Taco
Par Académico

DERECHOS DE AUTOR

Yo, **Luis Alvaro Veloz Becerra** portador de la cédula de identidad **0250209640** respectivamente**,** en calidad de autor y titular de los derechos morales y patrimoniales del Trabajo de Titulación: **Comparación de las herramientas esteganográficas para ocultar información en archivos gráficos,** modalidad Trabajo de Integración Curricular, de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, concedemos a favor de la Universidad Estatal de Bolívar, una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservamos a mi favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizamos a la Universidad Estatal de Bolívar para que realice la digitalización y publicación de este trabajo de titulación el Repositorio Digital, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

El autor declara que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

Firmado electrónicamente por:
LUIS ALVARO VELOZ BECERRA

Luis Alvaro Veloz Becerra

CI. 0250209640

ÍNDICE DE CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCIÓN

En la actualidad, la falta de medidas de seguridad en la informática es un problema que está en crecimiento. El número de atacantes está aumentando y se están volviendo más organizados; todos los días obtienen habilidades especiales que les permiten obtener más beneficios. La esteganografía se basa en esconder un mensaje secreto dentro (o incluso sobre) algo que no es secreto. Puede ser casi cualquier cosa que quieras. Hoy en día, varios ejemplos de esteganografía tratan de incrustar un texto secreto dentro de una imagen. O esconder un mensaje o guión secreto en un documento de Word o Excel. (Ayudaley, 2021).

El objetivo principal de la investigación es obtener información con respecto a las herramientas que nos ayuda con el método esteganográfico que nos permite ocultar la información. Hallar nuevas alternativas de aprendizaje mediante la utilización de ejemplos demostrativos para facilitar la comprensión del tema de estudio. El presente estudio analizará algunas de las herramientas esteganográfícas para el ocultamiento de la información dirigidos especialmente a los archivos gráficos; se ofrecerá conocimiento útil sobre las técnicas de intervención adaptadas a la era digital, donde la información recopilada será específica, al incluir cuadros y tablas comparativas.

De esta manera es evidente el alto grado de investigación dentro de la esteganografía, por esta razón el trabajo de investigación consta de 4 capítulos: El capítulo I contiene la formulación general del proyecto donde se detalla el problema de investigación, los objetivos y la idea a defender del trabajo investigativo; en el capítulo II se presenta el marco teórico que es una revisión y sustento de todas las investigaciones, antecedentes o resultados existentes sobre la esteganografía; capítulo III detalla la metodología que se utilizará para resolver el problema de la investigación mediante la recopilación de datos utilizando diversas técnicas; y por último en el capítulo IV se exponen los resultados y discusión proporcionando la interpretación de los datos recopilados y analizados para posteriormente concluir sobre la investigación realizada.

RESUMEN

La esteganografía es la tecnología que nos ayuda a ocultar la información, la cual nos facilita enviar los archivos con un nivel alto de seguridad manteniendo la confidencialidad de los mensajes; por otra parte, contamos con diferentes herramientas esteganográficas que nos ayudan aplicar el proceso para ocultar la información donde podemos aplicarlos en diferentes tipos de archivos como imágenes, audios y videos. En el trabajo de investigación se realizó un análisis comparativo de las herramientas esteganográficas que fueron escogidas aleatoriamente utilizadas para archivos gráficos, mediante una investigación cualitativa y descriptiva. Se realizó una revisión bibliográfica donde se recolectó toda la información requerida de cada herramienta para su respectivo análisis, identificando el funcionamiento, las cualidades y debilidades. Por lo tanto, se pudo identificar la herramienta que cumple con los protocolos que sirven para proteger nuestros datos y garantizar el intercambio de información de una manera confidencial. También se identificó la herramienta que ofrecen más funciones para ocultar la información concluyendo con la más recomendada al ser actualizada, por lo tanto, al elegir una herramienta se debe considerar la importancia de la seguridad de la información y por ende generar nuevas alternativas de protección durante el envío/recepción de datos.

Palabras clave: Esteganografía, estegoanálisis, comunicación encubierta, mensaje secreto.

ABSTRACT

Steganography is the technology that helps us hide information, which makes it easier for us to send files with a high level of security while maintaining the confidentiality of messages; On the other hand, we have different steganographic tools that help us apply the process to hide the information where we can apply them to different types of files such as images, audios, and videos. In the research work, a comparative analysis of the steganographic tools that were chosen randomly used for graphic files was carried out, through a qualitative and descriptive investigation. A bibliographical review was carried out where all the information required of each tool was collected for its respective analysis, identifying the operation, qualities and weaknesses. Therefore, it was possible to identify the tool that complies with the protocols that serve to protect our data and guarantee the exchange of information in a confidential manner. The tool that offers more functions to hide the information was also identified, concluding with the most recommended when updated, therefore, when choosing a tool, the importance of information security must be considered and therefore generate new protection alternatives during sending/receiving data.

Keywords: Steganography, stegoanalysis, covert communication, secret message.

CAPÍTULO I

FORMULACIÓN GENERAL DEL PROYECTO

1.1. Descripción del Problema

La esteganografía es muy poco conocida y no aporta mucha información sobre el tema, esto no quiere decir que en la actualidad no se utilice, pero son cada vez más indispensables en el medio digital. Otra problemática que se tiene es al momento de enviar algún contenido, ya que existen 22 herramientas para realizar el método esteganográfico en archivos gráficos, pero se desconoce cuáles son las más factibles y seguras para compartir la información; estas herramientas se las puede localizar fácilmente en internet.

Según (El Universo, 2019) el mayor tráfico de datos a través de la red llega a las imágenes y vídeos que se comparten en las redes sociales, aunque al mismo tiempo se oculta el contenido del mensaje al ser almacenados.

El cifrado ocurre en Dropbox, Google Drive y Microsoft OneDrive, pero dichos servidores no van a tener la protección suficiente en todo el momento las cuales corren el riesgo de sufrir un ataque. Por esta razón existen muchos estudios sobre la esteganografía ya que es una herramienta útil para proteger información confidencial, pero también puede ser utilizada con fines ilegales, por lo que es importante entenderla para estar preparados para enfrentar cualquier situación.

1.2. Formulación del Problema

¿Cuáles son las herramientas más recomendadas que se pueden utilizar para ocultar la información en archivos gráficos de manera segura?

1.3. Preguntas de Investigación

¿Cuál es la importancia de la seguridad informática en el mundo tecnológico?

¿Qué características de las herramientas de esteganografía para el ocultamiento de información son las más relevantes?

¿Cómo inciden los algoritmos utilizados en dichas herramientas en la seguridad de la información?

1.4. Justificación

En la actualidad el uso de la esteganografía es de gran importancia debido al aumento de otras herramientas para ocultar la información, por otro lado analizar y comprender las funciones de dichas herramientas se vuelve cada vez más importante porque se puede detectar y prevenir actividades ilegales, cabe señalar que la esteganografía es un tema que mucha gente ignora y en ocasiones se puede confundir con la criptografía, pero con la investigación se puede ir expandiendo más información sobre el tema, a tal grado de conocer las ventajas y desventajas de los algoritmos de seguridad de la esteganografía y así poco a poco se lo puede utilizar a la par de la criptografía . Por esta razón en el trabajo de investigación se realiza un estudio de las diferentes herramientas esteganográficas para el ocultamiento de la información en archivos gráficos y así contribuir en temas vinculados a la seguridad informática.

Además, el presente proyecto aportará a la línea de investigación de la carrera de software, "Gestión De Tecnologías de la Información y Comunicación"; sublínea, "Valoración integral de las TIC´s para la toma de decisiones".

1.5. Objetivos: General y Específicos

OBJETIVO GENERAL:

Realizar un estudio comparativo de las diferentes herramientas de esteganografía para ocultar la información en archivos gráficos.

OBJETIVOS ESPECIFICOS:

- Determinar la importancia que tiene la seguridad informática en el mundo tecnológico.
- Evaluar las diferentes herramientas esteganográficas para determinar cuáles son las más usadas.
- Analizar los algoritmos de las herramientas esteganográficas.

1.6. Idea a Defender

El estudio de herramientas esteganográficas para archivos gráficos permitirá conocer las características más relevantes incluidos los algoritmos de cifrado de

cada una de estas y determinar cuál es la más idónea para compartir información de una manera segura y a la vez confidencial.

1.7. Variables (Operacionalización)

Según (Solís, 2020) la presente investigación utiliza el Método Bibliográfico Documental que se realiza con la información de documentos fundamentales obtenida de diferentes medios. La técnica que fue utilizada en el estudio es la Revisión Documental, que se efectuará mediante los siguientes pasos:

- **Búsqueda de información.** Pretende recolectar información necesaria referente al tema de estudio de la investigación utilizando diferentes fuentes secundarias disponibles. (Solís, 2020)
- **Selección de información (observación).** Permite realizar una clasificación de la información recolectada para poder diferenciarla, al compararla, de la más óptima y adecuada para la investigación. (Solís, 2020)
- **Análisis de información.** De la información lograda, permite determinar los resultados de la investigación. (Solís, 2020)

Operacionalización de las variables e indicadores

La variable que se va a emplear en el trabajo de investigación es de tipo cualitativo. De acuerdo con la idea a defender se determinan las siguientes variables:

- Herramientas esteganografícas
- Gráficos

Tabla 1: Variables e indicadores

Variable	Tipo	Concepto
Herramientas esteganográficas	Independiente	Diferentes herramientas esteganográficas utilizadas para ocultar la información.
Transportador del mensaje (Gráficos)	Dependiente	Portador de información ampliamente utilizado porque hay una gran cantidad de bits presentes en la representación digital de una imagen.

Fuente: Propia
Elaborado por: Alvaro Veloz

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes (académicos y artículos de investigación)

La esteganografía es una palabra derivada del griego steganos, "cubrir" u "ocultar", y graphos, "escribir", que implica el estudio y aplicación de técnicas que permiten ocultar un mensaje u objeto dentro de otro (llamado transportista) para que no se notara su existencia. Es decir, intenta establecer un canal de comunicación encubierto ocultando los mensajes en otros objetos para que los observadores que tienen acceso al canal no noten la comunicación. (Manrique, 2021)

Como explica Yúbal Fernández, la esteganografía existe desde hace siglos. Es el campo de la criptografía donde se estudian los patrones y se utilizan para ocultar mensajes en otros mensajes para que podamos ocultar información fácilmente, sin que los demás se den cuenta. (Fernandez, 2019)

Durante la Segunda Guerra Mundial, el sistema más utilizado consistía en microfilmar un mensaje y reducirlo al final de un pequeño punto para que sirviera como puntuación para un carácter en otro texto. La esteganografía se ha expandido y diversificado con la llegada de las computadoras. Uno de los métodos más comunes es incrustar mensajes en contenido multimedia, mezclando fragmentos del mensaje original con fragmentos de gráficos o archivos de sonido.

El archivo resultante será un archivo de imagen o audio completamente funcional que no despertará sospechas a primera vista, pero con el software adecuado se podrá extraer la información oculta. (Villagrán, 2019)

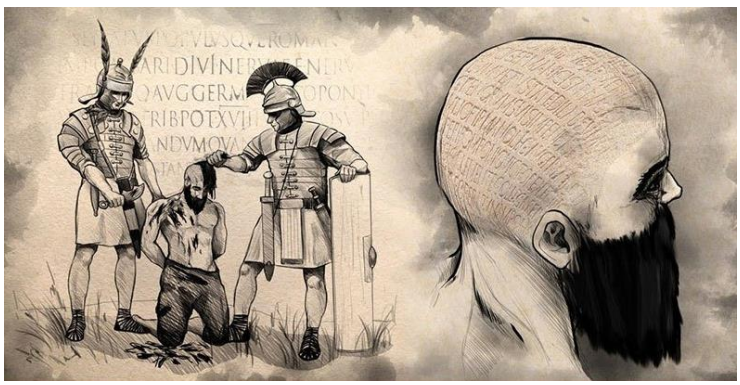
Origen y evolución

El origen de la esteganografía se encuentra en la historia de Heródoto. Escribe que esto ocurrió durante la revuelta jónica, un levantamiento de algunas ciudades griegas contra el dominio persa alrededor del año 500 a. C., cuando Histiaeus, el gobernante de Mileto, abandonó su ciudad para servir como rey persa. Quería

volver a Mileto bajo el gobierno de su yerno Aristágoras, por lo que planeó una rebelión en Jonia como pretexto para su regreso. Aquí es donde entra la esteganografía: rapó la cabeza del esclavo y tatuó un mensaje en el cuero cabelludo. (Blogger, 2019)

Histiaeus luego esperó a que el cabello del esclavo volviera a crecer y ocultó el mensaje antes de enviárselo a Aristágoras con instrucciones para que se afeitara la cabeza nuevamente y leyera el mensaje. Los textos ocultos le dicen que se levante contra los gobernantes persas, quienes iniciaron un levantamiento contra los conquistadores. Heródoto es conocido por sus historias fantásticas, por lo que no podemos estar seguros de su autenticidad, pero son los primeros registros de esteganografía que tenemos. Poco después, se registraron formas más complejas de esteganografía. En el siglo IV a. C., Eneas Tacticus menciona la técnica del piercing. Filón de Bizancio fue el primero en hablar sobre las tintas invisibles y escribió sobre ellas en el siglo III a. C. Su libro de cocina usa Galla para escribir el texto y una solución de sulfato de cobre para mostrarlo. (Blogger, 2019)

Figura 1: Transmisión del mensaje sobre la cabeza rasurada de uno de los criados y escribir sobre su piel el comprometedor mensaje.



Fuente: (Blogger, 2019)**.**

Nota. La figura 1 muestra como ocultaban los mensajes sobre la cabeza rasurada de uno de los criados y escribían sobre su piel.

El término esteganografía fue utilizado por primera vez en Steganographia por Johannes Trithemius. La palabra combinó la palabra griega steganos, que significa

oculto, y graphein, que significa escritura. Steganographia era un libro inteligente que se suponía que trataba sobre magia y ocultismo, pero usó criptografía y esteganografía para ocultar su tema real, que era criptografía y esteganografía. La Steganographia fue seguida por la Polygraphia, publicada por primera vez después de la muerte de Trithemius en 1518. Era un libro más simple sobre la esteganografía y su práctica. Otro desarrollo importante en la esteganografía ocurrió en 1605 cuando Francis Bacon desarrolló el Cifrado Bacon. Esta técnica utilizó dos tipos diferentes de fuentes para codificar un mensaje secreto en un texto aparentemente inocente. En los micropuntos se desarrollaron por primera vez en la segunda mitad del siglo XIX, pero no se utilizaron ampliamente en esteganografía hasta la Primera Guerra Mundial. Implican reducir un mensaje o imagen al tamaño de un punto, lo que permite a las personas comunicarse y transmitir información sin el conocimiento de sus oponentes. Ha habido muchos otros desarrollos y técnicas esteganográficas a lo largo de los años. La esteganografía todavía se practica hoy en día, y las pandillas de las prisiones a menudo usan versiones de baja tecnología y métodos digitales para ocultar datos en imágenes, audio y otros medios. (Ayudaley, 2021)

Estegoanálisis o detección de mensajes ocultos

El estegoanálisis es un campo de investigación relativamente nuevo, con solo unas pocas publicaciones que aparecieron antes de finales de la década de 1990. El estegoanálisis es el proceso de detección de esteganografía mediante el examen de las diferencias entre patrones de bits y tamaños de archivo inusualmente grandes. Es el arte de encontrar y entregar mensajes secretos inútiles. El propósito del análisis de llaves es detectar flujos de datos sospechosos, averiguar si hay mensajes ocultos codificados en ellos y, si es posible, recuperar los datos ocultos. (Ayudaley, 2021)

El hecho de que la esteganografía no siempre se pueda detectar hace que la esteganografía sea un tema de investigación en curso. Las limitaciones aumentan porque la esteganografía no es una técnica precisa. El software de esteganografía actual puede ocultar cualquier tipo de datos binarios en diferentes tipos de medios

de cobertura. Primero, nunca puedes predecir si hay un mensaje secreto; Es probable que el uso de la esteganografía por parte de terroristas y delincuentes aumente en el futuro, lo cual es un problema para los organismos encargados de hacer cumplir la ley. El análisis Stego debe desarrollarse aún más para luchar contra los terroristas de alta tecnología y los casos de espionaje industrial. (Ayudaley, 2021)

Tabla 2: Análisis comparativo entre la esteganografía y el estegoanálisis

Característica	Esteganografía	Estegoanálisis
Definición	Proceso de ocultar información en un medio de comunicación para que no sea aparente para el observador casual.	Proceso de detectar la presencia de información oculta y, si es posible, extraerla de un medio de comunicación.
Objetivo	Proteger la privacidad y seguridad de la información.	Detectar posibles amenazas o actividades ilegales.
Enfoque	Ocultar información.	Detectar información oculta.
Técnicas	Criptografía, modificación de bits, enmascaramiento, entre otras.	Análisis de patrones, correlación, comparación de tamaño de archivos, entre otras.
Herramientas	Esteganógrafos, software de codificación, protocolos de comunicación seguros.	Estegoanalizadores, software de decodificación, herramientas de análisis de archivos.
Aplicaciones	Comunicación segura, protección de datos confidenciales, marca de agua digital, entre otras.	Detectar malware, monitorear actividades ilegales en línea, protección de derechos de autor, entre otras.

Fuente: (Ayudaley, 2020)
Realizado por: Alvaro Veloz

La criptografía

La criptografía es la ciencia que se ocupa del cifrado de mensajes codificados y del desarrollo de sistemas de cifrado. Esto da como resultado el criptoanálisis, que se encarga de descifrar los mensajes codificados. La mayoría de las técnicas de encriptación utilizadas hoy en día tienen como objetivo ocultar información (como una contraseña que impide que se abra un documento) o autenticarla (como una

firma PGP en un correo electrónico exclusivo del autor de la carta). Los más utilizados por los usuarios tienen un sistema de encriptación que sirve para uno o ambos de los propósitos anteriores (Microsoft Office te permite proteger documentos con una contraseña que evita que personas no autorizadas los lean, WinZip te permite proteger archivos con contraseñas, etc.).

La esteganografía se enfoca en ocultar la presencia de información, mientras que la criptografía está más preocupada por la falta de acceso a la información. Cuando la esteganografía se usa correctamente, nadie más que los destinatarios sabrán que se está produciendo una comunicación encubierta. Esto la convierte en una técnica útil en situaciones en las que el contacto directo no es seguro. La tecnología de cifrado se utiliza preferentemente en situaciones en las que a los participantes no les importa que alguien descubra que se están comunicando, pero el mensaje en sí debe estar oculto e inaccesible para un tercero. (Berry, 2023)

Veamos algunos ejemplos para entender las diferencias. Si es un activista político que está encarcelado y necesita comunicarse con su organización, la logística puede ser un desafío. Las autoridades pueden monitorear todo lo que entra y sale de tu celda, por lo que probablemente tendrás que ocultar cualquier comunicación que se produzca. En esta situación, la esteganografía sería una buena opción. Esto puede ser difícil con los recursos que tiene, pero puede escribir una carta con un mensaje oculto que suene simple usando diferentes fuentes u otras técnicas esteganográficas.

Alternativamente, suponga que usted es un diplomático discutiendo detalles secretos con su país de origen. Es normal que los diplomáticos hablen con los funcionarios de su país, para que la comunicación en sí no despierte sospechas. Sin embargo, dado que el contenido de la conversación es de alto secreto, es posible que el diplomático desee utilizar el cifrado y hablar por una línea cifrada. Si espías o atacantes intentan espiar una conversación, solo pueden acceder al texto cifrado, no a lo que dice ninguna de las partes. Si un activista político usara encriptación para comunicarse con su organización, las autoridades probablemente lo detectarían. Los funcionarios vieron el texto encriptado y sabían que el activista

estaba tratando de enviar mensajes encriptados, por lo que probablemente dejarían de enviarlo e interrogarían al activista al respecto. Por lo tanto, en tal escenario, la esteganografía sería más apropiada. En contraste, los países anfitriones a menudo monitorean a los diplomáticos. Si un diplomático intentara enviar mensajes ofuscados esteganográficamente a su país, podrían ser interceptados, analizados y descubierto el contenido. En esta situación, la criptografía es más apropiada, porque incluso si los espías saben que te estás comunicando, no pueden averiguar de qué se trata.

Tabla 3: Relación entre la criptografía y la esteganografía.

	Criptografía	**Esteganografía**
Definición	Técnica de seguridad que cifra los datos para proteger su confidencialidad.	Técnica de seguridad que oculta los datos para proteger su confidencialidad.
Objetivo	Proteger los datos para que solo puedan ser leídos por personas autorizadas.	Ocultar los datos para que no sean detectados por personas no autorizadas.
Proceso	Cifra los datos mediante una clave de cifrado y los descifra mediante una clave de descifrado.	Oculta los datos en un archivo o medio de comunicación sin cambiar aparentemente el archivo o medio.
Seguridad	Ofrece una seguridad alta al proteger los datos con una clave de cifrado que solo es conocida por el emisor y el receptor.	Ofrece una seguridad media al depender de que el algoritmo de ocultación no sea descubierto.
Ejemplos de uso	Protección de contraseñas, transacciones bancarias, comunicaciones gubernamentales, etc.	Ocultación de mensajes dentro de imágenes, audios o videos, protección de información personal, entre otros.
Combinación	La criptografía y la esteganografía pueden ser combinadas para maximizar la seguridad de los datos.	La combinación de ambas técnicas permite proteger los datos mediante el cifrado y la ocultación.

Fuente: (Incibe, 2019)
Realizado por: Alvaro Veloz

2.2. Científico (bases teóricas en la que fundamenta la investigación)

Esteganografía

La esteganografía es considerada la base teórica de la seguridad de la información, debido a que en el proceso de movimiento de la información es necesario proteger u obtener garantías de que la información no caiga en manos de terceros no autorizados, un autor la define como “arte”. Ocultar información en imágenes, archivos de audio o canales ocultos utilizando métodos y técnicas informáticas

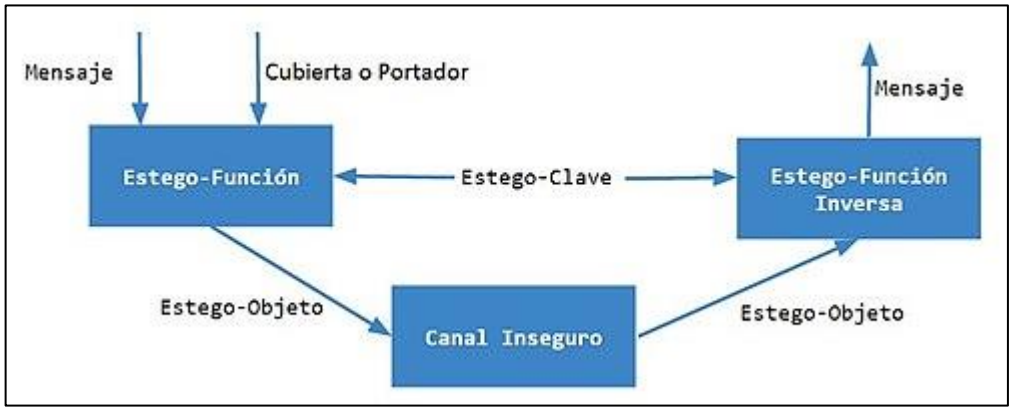
La esteganografía es ocultación y engaño es una forma de comunicación secreta y puede implicar el uso de cualquier medio para cifrar mensajes. Forma de cifrado porque no implica cifrar datos ni usar una clave, sino que es una forma de ocultar datos y se puede hacer de forma inteligente. Mientras que la criptografía es la ciencia que permite la privacidad en gran medida, la esteganografía es la práctica que permite el secreto y el engaño. La ocultación de datos se refiere a dos áreas, esteganografía y marca de agua. Hay tres problemas principales con la ocultación de datos, la capacidad, la seguridad y la solidez. La capacidad se refiere a la cantidad de información que se puede ocultar, la seguridad se refiere a la incapacidad del rastreador para detectar la información oculta y la robustez se refiere a la cantidad de modificaciones que un medio de enmascaramiento puede soportar antes de que la información oculta se vea comprometida. (enfasys, 2023)

En general, la ocultación de datos ocurre a través de los siguientes procesos:

- Detección de bits redundantes en el entorno de la máscara. Los bits redundantes son aquellos que se pueden editar independientemente de la calidad de la superposición.
- A continuación, seleccionamos un subconjunto de bits redundantes para reemplazarlos con información de mensajes privados. El medio de fase se crea reemplazando los bits redundantes seleccionados con bits de mensaje.

La edición de bits redundantes puede cambiar las propiedades estadísticas del entorno de la máscara. Como resultado, el análisis estadístico puede revelar contenido oculto.

Figura 2: Proceso de la esteganografía



Fuente: (Yglesias, 2020)

Nota. La figura 2 muestra el proceso para ocultar la información de forma que no se levanten sospechas.

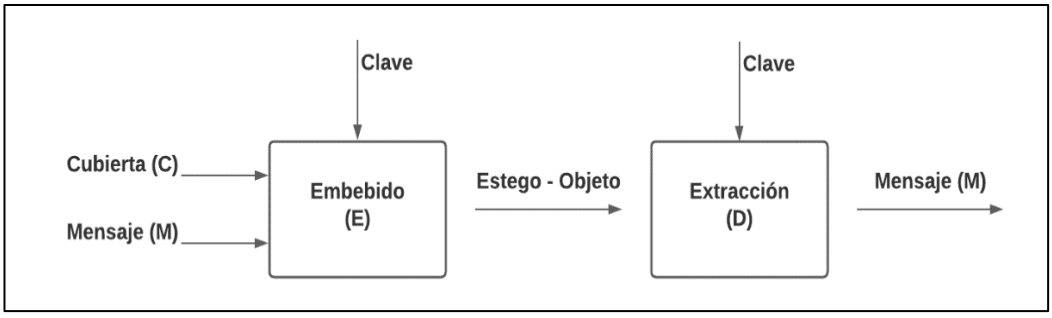
Tipos de esteganografía

Los principales tipos de esteganografía son:

Pura

La esteganografía pura no requiere el intercambio de un cifrado como un stego - key. Se asume que ninguna otra parte tiene conocimiento de la comunicación. (Ayudaley, 2021)

Figura 3: Proceso de la esteganografía pura



Fuente: (E, 2015)
Elaborado por: Alvaro Veloz

Nota. La figura 2 muestra el proceso de la esteganografía pura donde no requiere el intercambio de un cifrado como un stego-key.

De clave secreta

Aquí la clave secreta (stego) se intercambia antes de la comunicación. Esto es más susceptible a la interceptación. La esteganografía de clave secreta toma un mensaje de cobertura e incrusta el mensaje secreto dentro de él mediante el uso de una clave secreta (stego-key). Solo las partes que conocen la clave secreta pueden revertir el proceso y leer el mensaje secreto. (Ayudaley, 2021)

Figura 4: Proceso de la esteganografía secreta

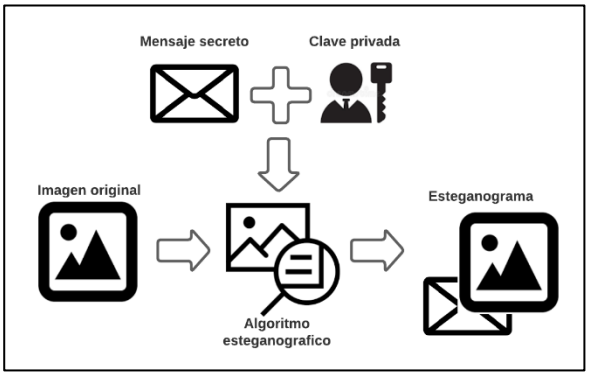
Fuente: (E, 2015)
Elaborado por: Alvaro Veloz

Nota. En la figura 4 nos muestra el proceso de la esteganografía secreta ya que toma un mensaje de cobertura e incrusta el mensaje secreto dentro de él mediante el uso de una clave secreta (stego-key).

De clave pública

En este caso se utiliza una clave pública y una clave privada para una comunicación segura. El remitente utilizará la clave pública durante el proceso de codificación y solo la clave privada, que tiene una relación matemática directa con la clave pública, puede descifrar el mensaje secreto. (Ayudaley, 2021)

Figura 5: Proceso de la esteganografía de clave pública



Fuente: (Lorente, 2013)
Elaborado por: Alvaro Veloz

Nota. En la figura 3 nos muestra el proceso de la esteganografía de clave privada por lo tanto se utiliza una clave pública y una clave privada para una comunicación segura.

Técnicas esteganográficas

Existen muchas técnicas para ocultar información. A continuación, explicamos las más habituales.

Enmascaramiento

En este caso la información se oculta dentro de una imagen digital usando marcas de agua donde se introduce información, como el derecho de autor, la propiedad o licencias. El objetivo es diferente de la esteganografía tradicional, lo que se pretende es añadir un atributo a la imagen que actúa como cubierta. De este modo se amplía la cantidad de información presentada. (Ayudaley, 2021)

Algoritmos de la compresión de datos

Esta técnica oculta datos basados en funciones matemáticas que se utilizan a menudo en algoritmos de la compresión de datos. La idea de este método es ocultar el mensaje en los bits de datos menos importantes. (Ayudaley, 2021)

Métodos de sustitución

Una de las formas más comunes de hacer esto es alterando el bit menos significativo (LSB). En archivos de imagen, audio y otros, los últimos bits de información en un byte no son necesariamente tan importantes como los iniciales. Por ejemplo, 10010010 podría ser un tono de azul. Si solo cambiamos los dos últimos bits a 10010001, podría ser un tono de azul que es casi exactamente igual. Esto significa que podemos ocultar nuestros datos secretos en los dos últimos bits de cada píxel de una imagen, sin cambiar la imagen de forma notable. Si cambiamos los primeros bits, lo alteraría significativamente. El método del LSB funciona mejor en los archivos de imágenes que tienen una alta resolución y usan gran cantidad de colores. En caso de archivos de audio, favorecen aquellos que tienen muchos y diferentes sonidos que poseen una alta tasa de bits. (Ayudaley, 2021)

Además, este método no altera en absoluto el tamaño del archivo portador o cubierta (por eso es «una técnica de sustitución»). Posee la desventaja de que el tamaño del archivo portador debe ser mayor al mensaje a embeber; se necesitan 8 bytes de imagen por cada byte de mensaje a ocultar; es decir, la capacidad máxima de una imagen para almacenar un mensaje oculto es de su 12,5%. Si se pretende emplear una mayor porción de bits de la imagen (por ejemplo, no solo el último, sino los dos últimos), puede comenzar a ser percibido al ojo humano la alteración general provocada. (Ayudaley, 2021)

Tabla 4: Cuadro comparativo de las técnicas de la esteganografía

Aspectos	Enmascaramiento	Compresión de datos	Métodos de sustitución
Definición	Técnica de ocultamiento de información en señales de audio o video	Reducción del tamaño de un archivo sin perder información	Técnica de codificación de información mediante la sustitución de caracteres, números o símbolos
Objetivo	Ocultar información en una señal de audio o video	Ahorrar espacio de almacenamiento y acelerar la transmisión de datos	Proteger la información mediante su cifrado
Principales características	Añade una señal de enmascaramiento a la señal original, la información oculta no es perceptible por el oído o el ojo humano	Reduce el tamaño de archivo, utiliza diferentes tipos de algoritmos, existen compresiones con y sin pérdida	Sustituye caracteres, números o símbolos por otros mediante una clave de cifrado, se pueden utilizar sustituciones mono alfabéticas o poli alfabética
	Técnicas de esteganografía, como enmascaramiento	Formatos de compresión de imágenes como JPG, PNG,	Cifrado César, cifrado de Vigenère, cifrado de sustitución poli

Ejemplos	de sonido y enmascaramiento de imagen	formatos de compresión de audio como MP3, formatos de compresión de vídeo como MPEG	alfabética, cifrado de sustitución mono alfabética
Ventajas	Oculta información de forma efectiva, sin afectar la calidad de la señal original	Permite almacenar y transmitir datos en menor espacio de almacenamiento, mejora la velocidad de transmisión, permite enviar datos a través de redes con menor capacidad de ancho de banda	Protege la información de posibles ataques externos, cifra la información para que solo pueda ser leída por aquellos que poseen la clave de cifrado
Desventajas	La información oculta puede ser revelada mediante técnicas de análisis de frecuencia y otras técnicas avanzadas de estegoanálisis	Puede haber pérdida de calidad en los datos comprimidos con pérdida, los archivos comprimidos pueden ser más difíciles de editar	Si la clave de cifrado es débil o se comparte, la información puede ser vulnerada, la sustitución mono alfabética es más vulnerable a ataques de frecuencia

Fuente: (Ayudaley, 2021)
Realizado por: Alvaro Veloz

Nota. En la tabla 4 se detalla las ventajas y desventajas de las técnicas esteganográficas

Esteganografía según el medio

Dependiendo de la naturaleza del objeto de cobertura (objeto real en el que se incrustan datos secretos), la esteganografía se puede dividir en varios tipos. Exploremos cada uno de ellos.

- **Documentos**

Según (Ayudaley, 2021) la esteganografía de texto oculta información dentro de los archivos de texto. Implica cosas como cambiar el formato de texto existente, cambiar palabras dentro de un texto, generar secuencias de caracteres aleatorias o usar gramáticas libres de contexto para generar textos legibles. Varias técnicas utilizadas para ocultar los datos en el texto son:

- Método basado en formato
- Generación estadística y aleatoria
- Método lingüístico

- **Imágenes**

Ocultar los datos tomando el objeto de portada como imagen se conoce como esteganografía de imagen. En la esteganografía digital, las imágenes son una fuente de cobertura ampliamente utilizada porque hay una gran cantidad de bits presentes en la representación digital de una imagen. Hay muchas formas de ocultar información dentro de una imagen. (Ayudaley, 2021) Los enfoques comunes incluyen:

- Inserción de bits menos significativa
- Enmascaramiento y filtrado
- Codificación de patrón redundante
- Cifrar y dispersar
- Codificación y transformación del coseno

- **Video**

En la esteganografía de video puede ocultar tipos de datos en formato de video digital. La ventaja de este tipo es que se puede ocultar una gran cantidad de datos en su interior y el hecho de que es un flujo de imágenes y sonidos en movimiento. Puedes pensar en esto como la combinación de esteganografía de imagen y esteganografía de audio. (Ayudaley, 2021) Dos clases principales de video esteganografía incluyen:

- Incrustar datos en video sin comprimir y comprimirlos más tarde
- Incrustar datos directamente en el flujo de datos comprimido

- **Audio**

Según (Ayudaley, 2021) en la esteganografía de audio, el mensaje secreto está incrustado en una señal de audio que altera la secuencia binaria del archivo de audio correspondiente. Ocultar mensajes secretos en digital es un proceso mucho más difícil en comparación con otros, como la esteganografía de imágenes. Los diferentes métodos de esteganografía de audio incluyen:

- Codificación de bits menos significativos
- Codificación de paridad
- Codificación de fase
- Espectro ensanchado
- Este método oculta los datos en archivos de sonido WAV, AU e incluso MP3.

- **Otros archivos**

Uno de los métodos más fáciles de implementar es el de inyección o agregado de bytes al final del archivo. Esta técnica consiste, esencialmente, en agregar o adosar al final de un archivo, de cualquier tipo, otro archivo que será el contenedor del «mensaje a ocultar», también de cualquier tipo. Esta metodología es la más versátil, pues permite usar cualquier tipo de archivo como portador (documentos, imágenes, audio, vídeos, ejecutables, etc.) y añadir al final del archivo contenedor el «paquete enviado», que es otro archivo, también de cualquier tipo. (Ayudaley, 2021)

Tipos de ataques a la esteganografía

Los ataques a la esteganografía son técnicas utilizadas para detectar, desenmascarar o incluso destruir información oculta dentro de archivos esteganográficos. Los ataques a la esteganografía se pueden clasificar en dos tipos principales:

1. **Ataques pasivos:** En este tipo de ataque, el objetivo es detectar la existencia de información oculta en un archivo esteganográfico sin modificar el archivo. Los ataques pasivos se basan en técnicas de análisis que buscan detectar patrones, anomalías o características distintivas en el archivo esteganográfico que sugieran la existencia de información oculta. (CIBERSEGURIDAD, 2022)

Algunos ejemplos de ataques pasivos son:

- Análisis visual: Examinar la imagen esteganográfica con el fin de detectar patrones de ruido o variaciones que podrían indicar la presencia de información oculta.
- Análisis estadístico: Utilizar técnicas estadísticas para detectar patrones o características distintivas en el archivo esteganográfico.

2. **Ataques activos:** En este tipo de ataque, el objetivo es modificar el archivo esteganográfico para degradar o eliminar la información oculta. Los ataques activos pueden ser más complejos y peligrosos que los pasivos, ya que pueden destruir la información oculta o incluso dañar la integridad del archivo original. (CIBERSEGURIDAD, 2022)

   Algunos ejemplos de ataques activos son:

   - Ataques de alteración: Modificar el archivo esteganográfico de manera que se degraden o eliminen la información oculta.
   - Ataques de eliminación: Eliminar completamente la información oculta del archivo esteganográfico.

Tabla 5: Descripción sobre los ataques a la esteganografía.

Tipo de ataque	Descripción	Ejemplos
Ataque pasivo	Se basa en la observación y análisis del archivo esteganográfico sin modificarlo	Análisis visual, análisis estadístico
Ataque activo	Implica la modificación del archivo esteganográfico con el objetivo de degradar o eliminar la información oculta	Ataques de alteración, ataques de eliminación

Fuente: (CIBERSEGURIDAD, 2022)
Realizado por: Alvaro Veloz

Nota. En la tabla 5 nos muestra la descripción sobre los tipos de ataques a la esteganografía.

Estegoanálisis

El estegoanálisis, trata de romper las técnicas esteganográficas. El estegoanálisis tiene varios objetivos:

- **Detección:** Detecta contenido oculto en medios portadores, de varias formas:
  - Visual o Auditiva
  - Estructural
  - Estadística (Entropía, etc.)
- **Extracción:** Elimina la información oculta del medio portador.
- **Confusión:** Altera e introduce nueva información para dejar inservible la información oculta.
- **Deshabilitación:** Elimina la información oculta.

Si la esteganografía logra cualquiera de estos objetivos, la esteganografía se considera un fracaso. Por lo tanto, el éxito es enorme si sabe que el transportista tiene información oculta. Sin embargo, está claro que lo óptimo e ideal es saber cuál es el mensaje oculto del soporte de datos portátil y, si estuviera encriptado, poder descifrarlo. Tenga en cuenta que JUBSAC se centra en el objetivo esteganográfico, es decir. Detectar información oculta en imágenes. El análisis esteganográfico de una imagen es un proceso complejo, porque se pueden considerar tantos parámetros al hacer un algoritmo esteganográfico que el análisis esteganográfico es bastante laborioso y difícil. Además, el análisis generalmente no es útil para otro algoritmo, porque cada aplicación es diferente en función y origen.

Proceso del Estegoanálisis

1. **Extracción del archivo portador:** En primer lugar, se extrae el archivo portador que se sospecha contiene información oculta, ya sea una imagen, audio, video, archivo de texto, entre otros.
2. **Análisis del archivo portador:** Una vez extraído el archivo portador, se realiza un análisis exhaustivo del mismo en busca de cualquier indicio de información oculta. Este análisis puede involucrar el uso de herramientas de software especializadas que permitan detectar patrones y características que puedan indicar la presencia de información oculta.

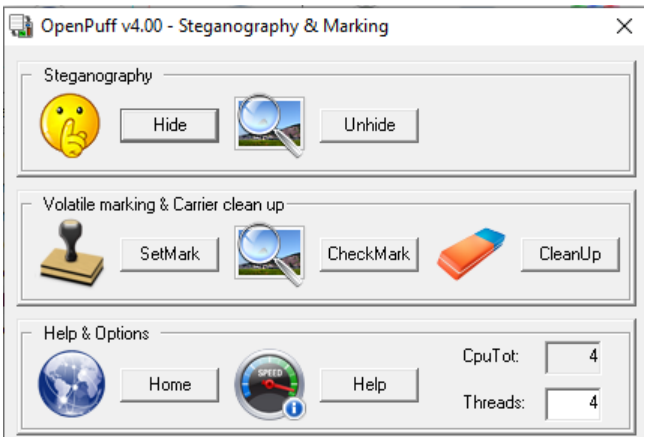
3. **Extracción de la información oculta:** Si se detecta información oculta en el archivo portador, se procede a su extracción utilizando herramientas especializadas de esteganografía o mediante la realización de técnicas de análisis forense digital. Es importante destacar que la extracción de la información oculta debe realizarse de manera cuidadosa para evitar dañar o corromper los datos.
4. **Análisis de la información extraída:** Una vez extraída la información oculta, se realiza un análisis adicional para determinar su significado y su importancia en el contexto en el que se encuentra. Este análisis puede involucrar la identificación de patrones, el uso de técnicas de análisis de datos y la revisión de otras fuentes de información para contextualizar los datos extraídos.
5. **Presentación de resultados:** Finalmente, los resultados del proceso de estegoanálisis se presentan en un informe que incluye los detalles del archivo portador, la información oculta detectada y cualquier otra información relevante. Este informe puede ser utilizado para tomar medidas de seguridad adicionales y mejorar la protección de la información en el futuro.

Herramientas para el análisis de la esteganografía en imágenes

Las herramientas para el análisis esteganográfico son programas o software que se utilizan para detectar la presencia de información oculta en archivos mediante técnicas de esteganografía. Algunas de las herramientas más comunes para el análisis esteganográfico incluyen:

1. **OpenPuff:** Es un software de esteganografía de código abierto que permite ocultar información en diferentes tipos de archivos, como imágenes, audio y vídeo. OpenPuff utiliza una técnica de esteganografía conocida como "esteganografía de archivos múltiples", lo que significa que puede ocultar varios archivos dentro de un archivo esteganográfico. OpenPuff también incluye funciones de cifrado y autenticación para proteger la información oculta. (Ephesos Software, 2023)

Figura 6: Interfaz de la herramienta OpenPuff



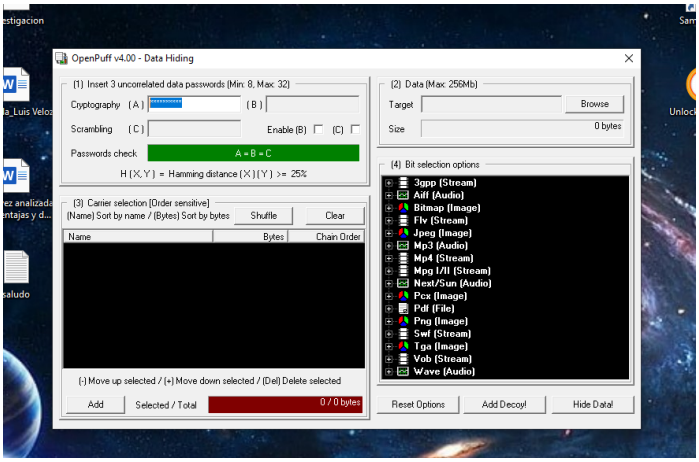
Fuente: (Oliboni, 2019)

Nota. La figura 6 nos muestra todas las funciones de la herramienta OpenPuff.

Procedimiento para cifrar un mensaje

1. Abrir el programa, se mostrará la interfaz con todas las opciones disponibles como se muestra en la **figura 6**.
2. Damos clic en Hide (esconder), se configurará una contraseña la cual será cifrada la información.

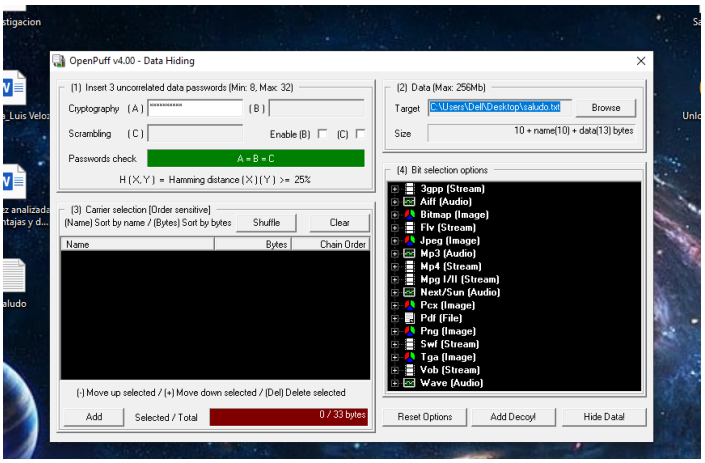
Figura 7: Configuración de una contraseña



Fuente: Captura de pantalla herramienta OpenPuff
Elaborado por: Alvaro Veloz

3. Añadimos un archivo de texto.

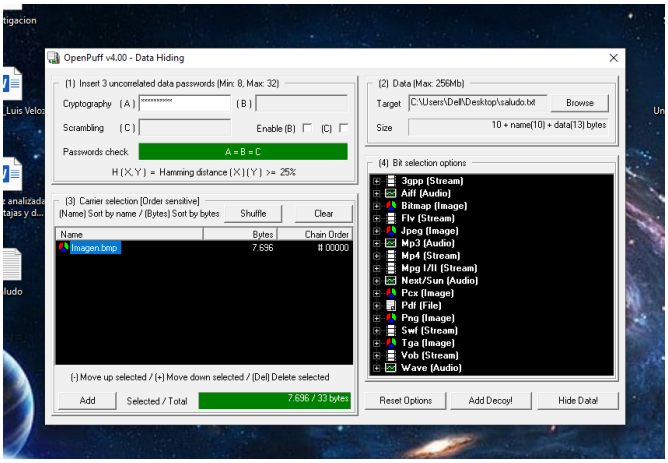
Figura 8: Añadir archivo de texto



Fuente: Captura de pantalla herramienta OpenPuff
Elaborado por: Alvaro Veloz

4. Añadimos el portador del mensaje.

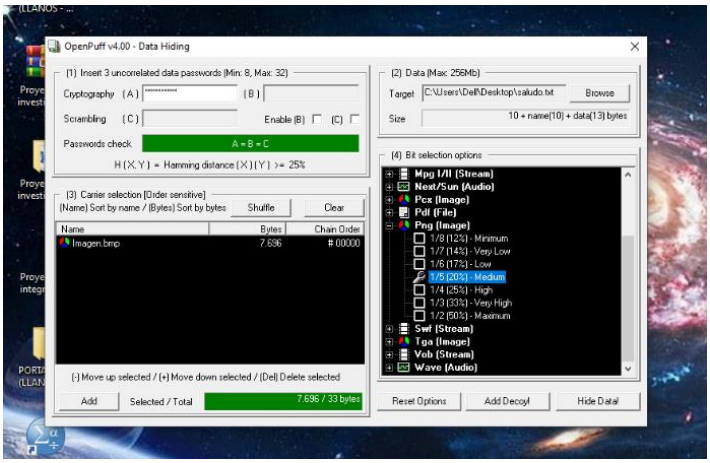
Figura 9: Añadir el portador del mensaje



Fuente: Captura de pantalla herramienta OpenPuff
Elaborado por: Alvaro Veloz

5. Elegimos el formato y damos clic en Hide Data (Ocultar Datos).

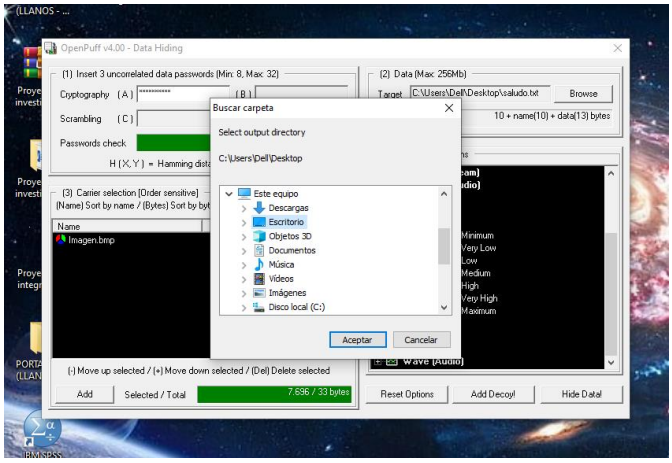
Figura 10: Ocultar Datos según el formato



Fuente: Captura de pantalla herramienta OpenPuff
Elaborado por: Alvaro Veloz

6. Por último, seleccionamos la carpeta de destino donde se guardará el archivo.

Figura 11: Carpeta de destino donde se guardará el archivo

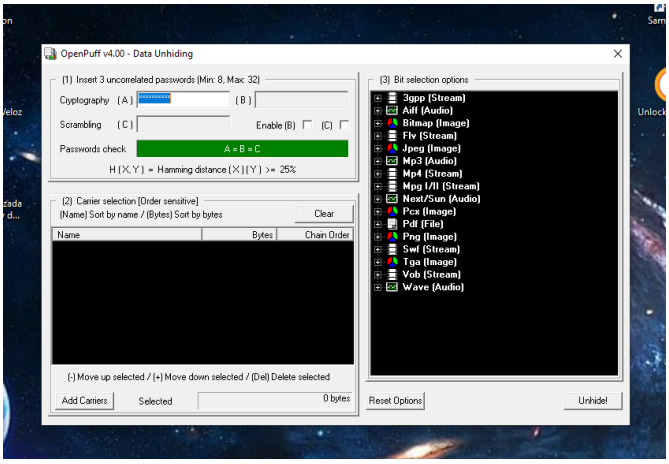


Fuente: Captura de pantalla herramienta OpenPuff
Elaborado por: Alvaro Veloz

Procedimiento para descifrar un mensaje

1. Abrir el programa OpenPuff. **Figura 6**
2. Se da clic en Unhide (mostrar), se escribirá la contraseña con la cual fue guardado el mensaje.

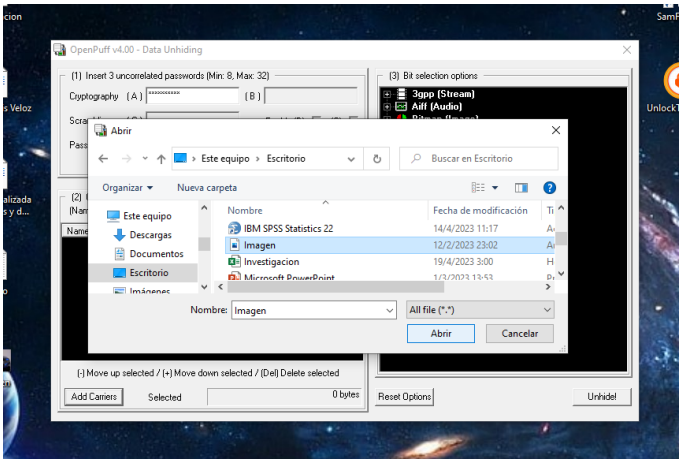
Figura 12: Escribir la contraseña



Fuente: Captura de pantalla herramienta OpenPuff
Elaborado por: Alvaro Veloz

3. Damos clic en Add Carriers (añadir transportista), añadimos el archivo a descifrar.

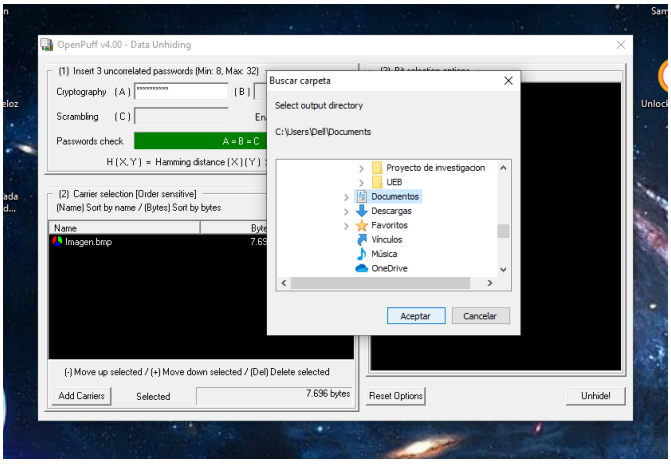
Figura 13: Añadir el archivo a descifrar



Fuente: Captura de pantalla herramienta OpenPuff
Elaborado por: Alvaro Veloz

4. Damos clic en Unhide (mostrar), seleccionamos la carpeta donde se exportará el mensaje oculto.

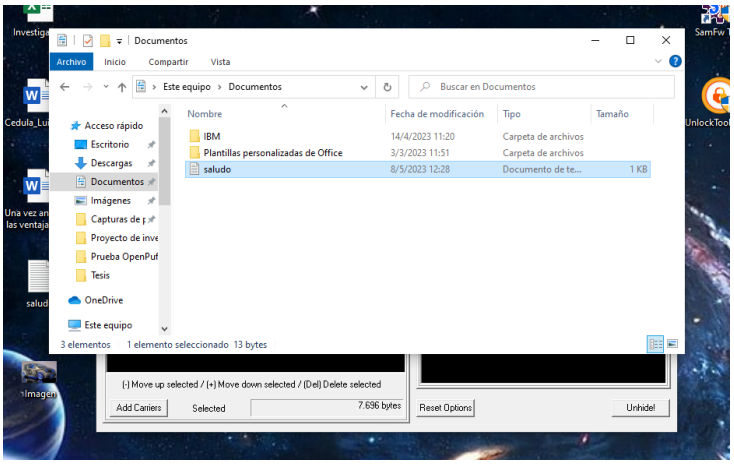
Figura 14: Carpeta donde se exportará el mensaje oculto



Fuente: Captura de pantalla herramienta OpenPuff
Elaborado por: Alvaro Veloz

5. Se muestra el mensaje que se mantuvo oculto en el archivo.

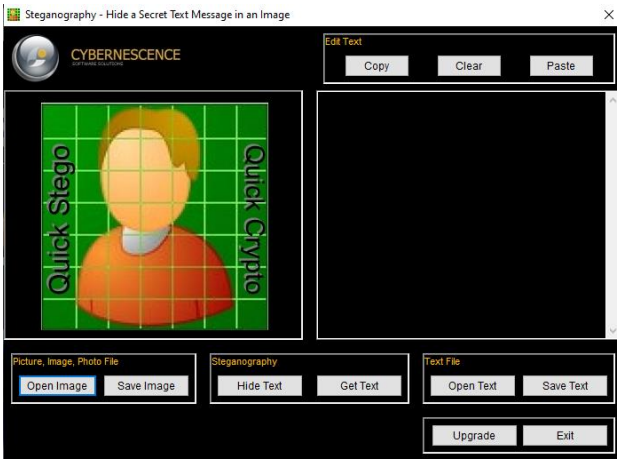
Figura 15: Mensaje que se mantuvo oculto en el archivo



Fuente: Captura de pantalla herramienta OpenPuff
Elaborado por: Alvaro Veloz

2. **QuickStego:** Es un software de esteganografía fácil de usar que permite ocultar información en archivos de imagen. QuickStego utiliza una técnica de esteganografía conocida como "LSB" (Least Significant Bit), que oculta información en los bits menos significativos de los píxeles de una imagen. QuickStego también incluye funciones básicas de cifrado y compresión. (ESGEEKS, 2019)

Figura 16: Interfaz de la herramienta QuickStego

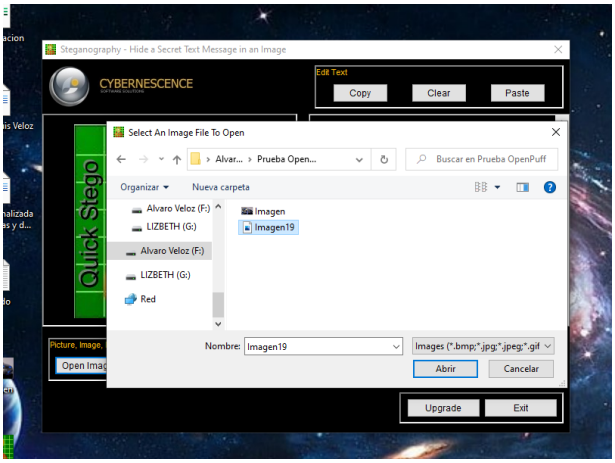


Fuente: (QuickCripto, 2020)

Procedimiento para cifrar un mensaje

1. Abrir el programa, se mostrará la interfaz con todas las opciones disponibles como se muestra en la **figura 16.**
2. Se da clic en Open Image (abrir imagen), elegimos la imagen que nos ayudara como transportador.

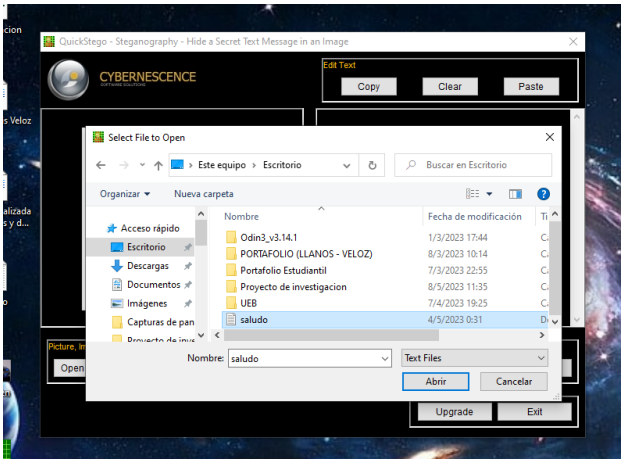
Figura 17: Imagen que nos ayudara como transportador



Fuente: Captura de pantalla herramienta Quickstego
Elaborado por: Alvaro Veloz

3. Se da clic en Open text (abrir texto), escogemos el archivo que será oculto en la imagen.

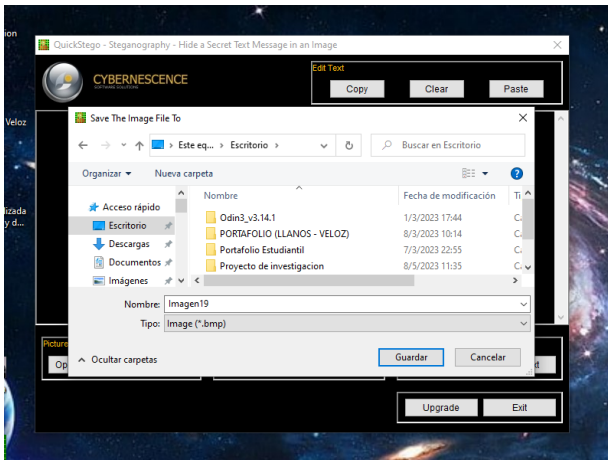
Figura 18: Archivo que será oculto en la imagen



Fuente: Captura de pantalla herramienta Quickstego
Elaborado por: Alvaro Veloz

4. Damos clic en Save Image (guardar imagen), seleccionaremos la carpeta donde se guardará el archivo.

Figura 19: Carpeta donde se guardará el archivo

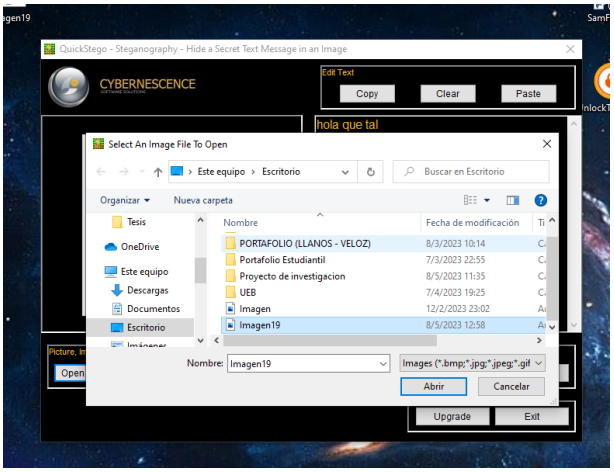


Fuente: Captura de pantalla herramienta Quickstego
Elaborado por: Alvaro Veloz

Procedimiento para descifrar un mensaje

1. Abrimos el programa QuickStego. **Figura 16**
2. Damos clic en Open Image (abrir imagen), seleccionamos el archivo a descifrar.

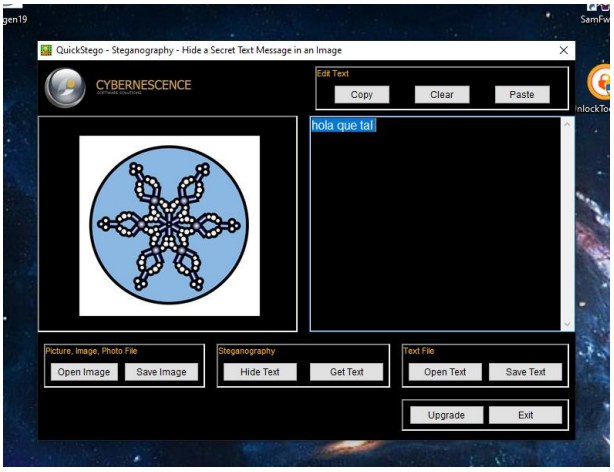
Figura 20: Archivo a descifrar



Fuente: Captura de pantalla herramienta Quickstego
Elaborado por: Alvaro Veloz

3. Se mostrará el mensaje oculto a lado izquierdo del programa.

Figura 21: Mensaje oculto



Fuente: Captura de pantalla herramienta Quickstego
Elaborado por: Alvaro Veloz

3. **Xiao Steganography:** Es un software de esteganografía que permite ocultar información en archivos de imagen. Al igual que QuickStego, Xiao Steganography utiliza la técnica de esteganografía LSB para ocultar información en los bits menos significativos de los píxeles de una imagen. El software incluye funciones básicas de cifrado y compresión para proteger la información oculta. (Bhatia, 2019)

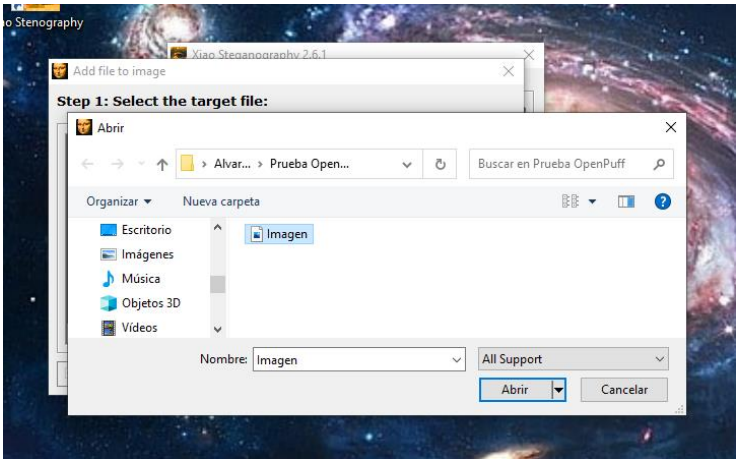
Figura 22: Interfaz de la herramienta Xiao Steganography

Fuente: (Bhatia, 2019)

Procedimiento para cifrar un mensaje

1. Abrir el programa, una vez abierto el programa se mostrará todas las opciones disponibles como se muestra en la **figura 22.**
2. Damos clic en Add Files (agregar archivo), seleccionamos la imagen que nos ayudara como transportador.

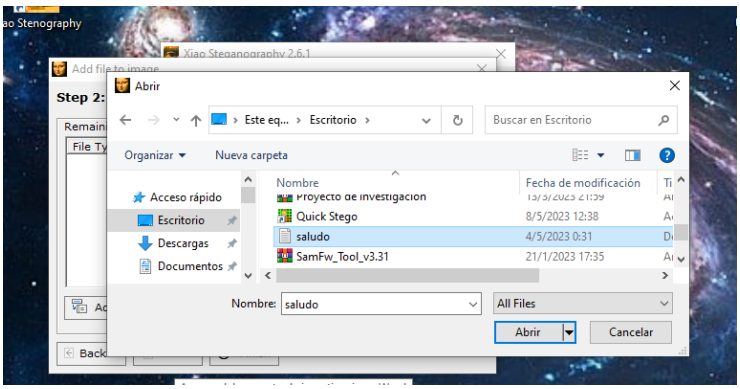
Figura 23: Imagen que nos ayudara como transportador



Fuente: Captura de pantalla herramienta Xiao Steganography
Elaborado por: Alvaro Veloz

3. Seleccionamos el archivo que se ocultara en la imagen.

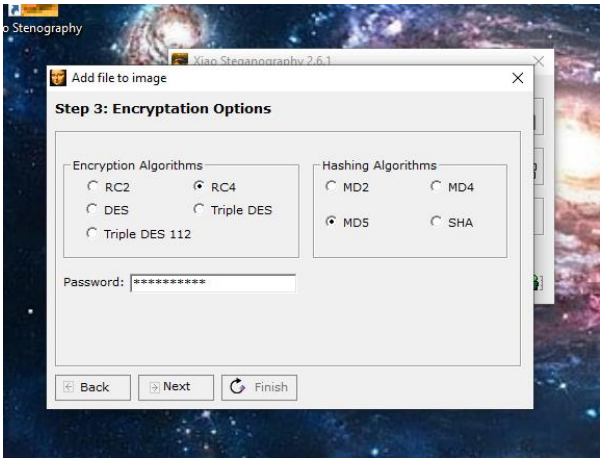
Figura 24: Archivo que se ocultara en la imagen



Fuente: Captura de pantalla herramienta Xiao Steganography
Elaborado por: Alvaro Veloz

4. Seleccionamos el algoritmo de encriptación y la clave.

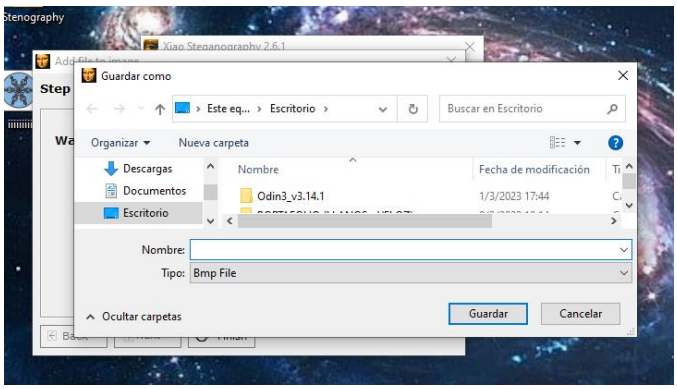
Figura 25: Algoritmo de encriptación y la clave



Fuente: Captura de pantalla herramienta Xiao Steganography
Elaborado por: Alvaro Veloz

5. Escogemos la carpeta donde se guardará el archivo.

Figura 26: Carpeta donde se guardará el archivo

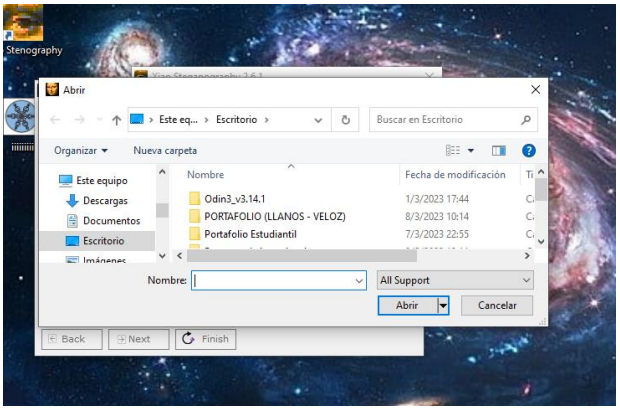


Fuente: Captura de pantalla herramienta Xiao Steganography
Elaborado por: Alvaro Veloz

Procedimiento para descifrar un mensaje

1. Abrimos el programa Xiao Steganography. **Figura 22**
2. Damos clic en Extract Files (extraer archivo), seleccionamos el archivo a descifrar.

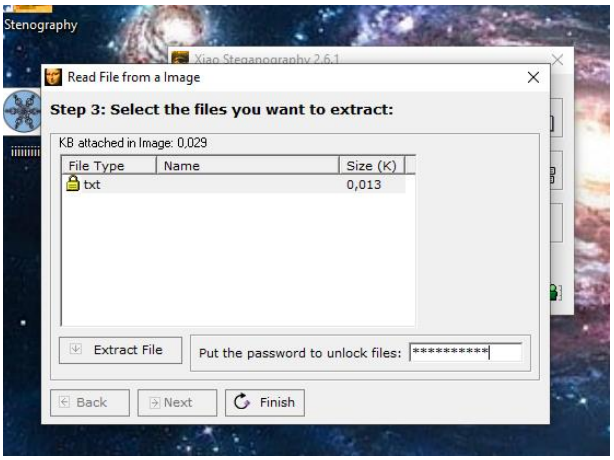
Figura 27: Archivo a descifrar



Fuente: Captura de pantalla herramienta Xiao Steganography
Elaborado por: Alvaro Veloz

3. Escribimos la contraseña con la que fue guardado el archivo y extraemos el mensaje.

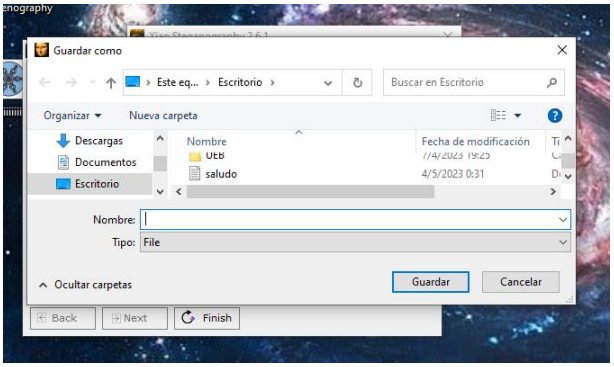
Figura 28: Extracción del mensaje



Fuente: Captura de pantalla herramienta Xiao Steganography
Elaborado por: Alvaro Veloz

4. Seleccionamos la carpeta donde se guardará el mensaje extraído del archivo.

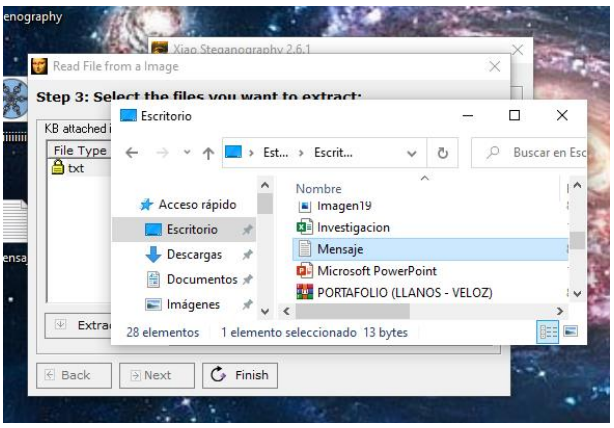
Figura 29: Carpeta donde se guardará el mensaje extraído



Fuente: Captura de pantalla herramienta Xiao Steganography
Elaborado por: Alvaro Veloz

5. Se muestra el mensaje extraído del archivo.

Figura 30: Mensaje extraído



Fuente: Captura de pantalla herramienta Xiao Steganography
Elaborado por: Alvaro Veloz

Tabla 6: Cuadro comparativo de las herramientas a estudiar

Aspecto	OpenPuff	QuickStego	Xiao Steganography
Desarrollador	Cosimo Oliboni	CyberSpy Software	X-Ways Software Technology AG
Licencia	Gratis	Gratis	Versión gratuita y de pago
Tipo de archivo	Permite ocultar en todo tipo de archivo	Sólo permite en archivos de imagen y audio	Permite ocultar en imágenes, audio y video
Seguridad	Cifrado AES	Cifrado RSA y AES	Cifrado AES
Ocultamiento	Múltiples capas de ocultamiento	Capacidad para ocultar sólo un mensaje por archivo	Capacidad para ocultar múltiples mensajes por archivo
Interfaz gráfica	Sí	Sí	Sí
Estabilidad	Estable	Estable	Estable

Fuente: (ESGEEKS, 2019)
Realizado por: Alvaro Veloz

Los formatos de imágenes más empleados por las herramientas esteganográficas y por los usuarios en general, son:

JPG o JPEG: Joint Photographic Experts Group (Grupo conjunto de expertos en fotografía).

BMP: Windows BitMaP (Mapa de bits de ventana).

GIF: Graphics Image Format (Formato de imágenes gráficas).

PNG: Portable Network Graphics (Gráficos portables en red). Y las técnicas usadas por los programas de esteganografía son las ya mencionadas, sobre el Dominio del Espacio y el Dominio de las Transformadas:

LSB: Bit menos significativo.

DCT: Transformada Discreta del Coseno.

DFT: Transformada Discreta de Fourier.

DWT: Transformada Discreta Ondulada.

¿Cómo funciona la esteganografía digital?

La esteganografía digital funciona ocultando información de manera que no despierte sospechas. Una de las técnicas más populares es la esteganografía de bits menos significativos (LSB). En este tipo de esteganografía, el ocultador de información incrusta la información secreta en las piezas menos significativas del archivo multimedia. (Ayudaley, 2021)

Por ejemplo, en un archivo de imagen, cada píxel consta de tres bytes de datos correspondientes a los colores rojo, verde y azul (algunos formatos de imagen especifican un cuarto byte adicional, o "alfa"), para la transparencia.

La esteganografía LSB cambia el último bit de cada byte para ocultar un bit de datos. Entonces, para ocultar un megabyte de datos con este método, necesita archivos de imagen de ocho megabytes. (Ayudaley, 2021)

Dado que cambiar el último bit del valor de un píxel no provoca un cambio visualmente perceptible en la imagen, un espectador humano no puede notar la diferencia entre la imagen original y la alterada esteganográficamente.

El mismo modelo se puede aplicar a otros medios digitales (audio y video), donde los datos se ocultan en las partes del archivo que causan el menor cambio en la salida de audio o visual. (Ayudaley, 2021)

Otra técnica esteganográfica menos popular es la sustitución de palabras o letras. Aquí, el remitente del mensaje cifrado oculta el texto organizándolo en un texto mucho más grande, colocando las palabras en ciertos intervalos.

Aunque este método de reemplazo es fácil de usar, puede hacer que el texto se vea extraño e inapropiado, ya que las contraseñas pueden no coincidir muy bien con sus frases de destino. (Ayudaley, 2021)

Existen otros tipos de esteganografía, como ocultar una partición completa en un disco duro o incrustar información en la sección de encabezado de archivos y paquetes de red. La eficacia de estos métodos depende de la cantidad de datos que puedan ocultar y de lo fácil que sea detectarlos. (Ayudaley, 2021)

2.3. Conceptual

- **La esteganografía:** Es el arte o ciencia de comunicar de manera oculta un mensaje, camuflando la información entre otro conjunto de datos para que pase desapercibida. Hoy día suele utilizarse para esconder información en todo tipo de archivos tales como fotos, videos o audio. (Villagrán, 2002)
- **La criptografía:** Es el desarrollo de un conjunto de técnicas que permiten alterar y modificar mensajes o archivos con el objetivo de que no puedan ser leídos por todos aquellos usuarios que no estén autorizados a hacerlo. Hoy en día, en pleno auge de las comunicaciones digitales, funciona como la base para cualquier proceso de seguridad informática. (NIC, 2018)
- **Seguridad de la información:** Es el conjunto de medidas y técnicas utilizadas para controlar y salvaguardar todos los datos que se manejan dentro

de la organización y asegurar que los datos no salgan del sistema que ha establecido la organización. Es una pieza clave para que las empresas puedan llevar a cabo sus operaciones, ya que los datos que maneja son esenciales para la actividad que desarrollan. (27001:2013,2021)

- **Estegoanálisis:** Es la técnica para descubrir e inutilizar información oculta en archivos digitales. (Española, 2006)
- **Algoritmos de cifrado:** son las instrucciones, fórmulas y técnicas de encriptación predeterminadas que usa su computadora para convertir texto sin formato en texto sin formato, comúnmente conocido como encriptación. (International IT, 2002)
- **Algoritmos hash:** Es un algoritmo matemático que convierte todos los datos entrantes en una serie de caracteres de salida de longitud fija o variable, según el algoritmo hash que utilicemos. (López, 2022)

2.4. Legal

LEY DE COMERCIO ELECTRONICO, FIRMAS Y MENSAJES DE DATOS (LEY DE COMERCIO ELECTRONICO, 2002)

Art. 9.- Protección de datos. - Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente. No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato. El consentimiento a que se refiere este artículo podrá

ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.

Art. 10.- Procedencia e identidad de un mensaje de datos. - Salvo prueba en contrario se entenderá que un mensaje de datos proviene de quien lo envía y, autoriza a quien lo recibe, para actuar conforme al contenido del mismo, cuando de su verificación exista concordancia entre la identificación del emisor y su firma electrónica, excepto en los siguientes casos:

a) Si se hubiere dado aviso que el mensaje de datos no proviene de quien consta como emisor; en este caso, el aviso se lo hará antes de que la persona que lo recibe actúe conforme a dicho mensaje. En caso contrario, quien conste como emisor deberá justificar plenamente que el mensaje de datos no se inició por orden suya o que el mismo fue alterado; y,

b) Si el destinatario no hubiere efectuado diligentemente las verificaciones correspondientes o hizo caso omiso de su resultado.

Art. 12.- Duplicación del mensaje de datos. - Cada mensaje de datos será considerado diferente. En caso de duda, las partes pedirán la confirmación del nuevo mensaje y tendrán la obligación de verificar técnicamente la autenticidad del mismo.

Art. 13.- Firma electrónica. - Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.

Art. 14.- Efectos de la firma electrónica. - La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba en juicio.

Art. 15.- Requisitos de la firma electrónica. - Para su validez, la firma electrónica reunirá los siguientes requisitos, sin perjuicio de los que puedan establecerse por acuerdo entre las partes:

a) Ser individual y estar vinculada exclusivamente a su titular;
b) Que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta ley y sus reglamentos;
c) Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado;
d) Que, al momento de creación de la firma electrónica, los datos con los que se creare se hallen bajo control exclusivo del signatario, y,
e) Que la firma sea controlada por la persona a quien pertenece.

Art. 16.- La firma electrónica en un mensaje de datos. - Cuando se fijare la firma electrónica en un mensaje de datos, aquélla deberá enviarse en un mismo acto como parte integrante del mensaje de datos o lógicamente asociada a éste. Se presumirá legalmente que el mensaje de datos firmado electrónicamente conlleva la voluntad del emisor, quien se someterá al cumplimiento de las obligaciones contenidas, en dicho mensaje de datos, de acuerdo a lo determinado en la ley.

Art. 17.- Obligaciones del titular de la firma electrónica. - El titular de la firma electrónica deberá:

a) Cumplir con las obligaciones derivadas del uso de la firma electrónica;
b) Actuar con la debida diligencia y tomar las medidas de seguridad necesarias, para mantener la firma electrónica bajo su estricto control y evitar toda utilización no autorizada;
c) Notificar por cualquier medio a las personas vinculadas, cuando exista el riesgo de que su firma sea controlada por terceros no autorizados y utilizada indebidamente;
d) Verificar la exactitud de sus declaraciones;
e) Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización,

salvo que el destinatario conociere de la inseguridad de la firma electrónica o no hubiere actuado con la debida diligencia;

f) Notificar a la entidad de certificación de información los riesgos sobre su firma y solicitar oportunamente la cancelación de los certificados; y,

g) Las demás señaladas en la ley y sus reglamentos.

Art. 18.- Duración de la firma electrónica. - Las firmas electrónicas tendrán duración indefinida. Podrán ser revocadas, anuladas o suspendidas de conformidad con lo que el reglamento a esta ley señale.

Art. 19.- Extinción de la firma electrónica. - La firma electrónica se extinguirá por:

a) Voluntad de su titular;

b) Fallecimiento o incapacidad de su titular;

c) Disolución o liquidación de la persona jurídica, titular de la firma; y,

d) Por causa judicialmente declarada.

La extinción de la firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso.

Art. 22.- Requisitos del certificado de firma electrónica. - El Certificado de firma electrónica para ser considerado válido contendrá los siguientes requisitos:

a) Identificación de la entidad de certificación de información;

b) Domicilio legal de la entidad de certificación de información;

c) Los datos del titular del certificado que permitan su ubicación e identificación;

d) El método de verificación de la firma del titular del certificado;

e) Las fechas de emisión y expiración del certificado;

f) El número único de serie que identifica el certificado;

g) La firma electrónica de la entidad de certificación de información;

h) Las limitaciones o restricciones para los usos del certificado; e,

i) Los demás señalados en esta ley y los reglamentos.

Art. 25.- Suspensión del certificado de firma electrónica. - La entidad de certificación de información podrá suspender temporalmente el certificado de firma electrónica cuando:

a) Sea dispuesto por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta ley;
b) Se compruebe por parte de la entidad de certificación de información, falsedad en los datos consignados por el titular del certificado; y,
c) Se produzca el incumplimiento del contrato celebrado entre la entidad de certificación de información y el titular de la firma electrónica.

La suspensión temporal dispuesta por la entidad de certificación de información deberá ser inmediatamente notificada al titular del certificado y al organismo de control, dicha notificación deberá señalar las causas de la suspensión.

La entidad de certificación de información deberá levantar la suspensión temporal una vez desvanecidas las causas que la originaron, o cuando mediare resolución del Consejo Nacional de Telecomunicaciones, en cuyo caso, la entidad de certificación de información está en la obligación de habilitar de inmediato el certificado de firma electrónica.

CAPITULO III

METODOLOGÍA

3.1. Tipo de Investigación

El trabajo de investigación es de tipo informativo y explicativo, cuyo objetivo fue presentar la información más relevante de diversas fuentes confiables sobre el tema a tratar. Se centra en analizar y seleccionar información de estas fuentes, aquello que es relevante para la investigación, organizando la información para cubrir todo el tema, reduciendo las ideas y después mostrarlas en un reporte final que a la vez sea fluido y esté claramente escrito.

3.2. Enfoque de la investigación

El enfoque de la investigación es cualitativo, puesto que se realizó estudios de diferentes fuentes fiables de un tema determinado, en este caso, todo lo referente las herramientas esteganográficas, para proponer nuevos conceptos de comprensión y medición de dicha información recolectada.

3.3. Métodos de Investigación

En el trabajo de investigación se utilizó el método bibliográfico documental que se realiza con la información de documentos fundamentales obtenida de diferentes medios.

3.4. Técnicas e instrumentos de Recopilación de Datos

La técnica que se utilizó en el trabajo de investigación es la Revisión Documental, que se efectuó mediante los siguientes pasos:

- **Búsqueda de información.** Pretende recolectar información necesaria referente al tema de estudio de la investigación utilizando diferentes fuentes secundarias disponibles.
- **Selección de información.** Permite realizar una clasificación de la información recolectada para poder diferenciarla, al compararla, de la más óptima y adecuada para la investigación.

- **Análisis de información.** De la información lograda, permite determinar los resultados de la investigación.

3.5. Universo, Población y Muestra

En la presente investigación que se llevó a cabo su población estará conformada por las 22 herramientas esteganográficas que nos ayudaran a validar los datos presentados en el trabajo, también podremos definir la muestra a través de un muestreo aleatorio donde se escogió 3 herramientas con las que se realizó el estudio comparativo.

Los criterios de inclusión y exclusión para la delimitación poblacional son los siguientes:

- Investigaciones realizadas sobre las herramientas esteganográfícas, sus técnicas y métodos a nivel nacional.
- Investigaciones realizadas sobre esteganografía, sus técnicas y métodos a nivel internacional.
- Investigaciones conformadas de los últimos años.

3.6. Procesamiento de la información

En el trabajo de investigación se realizó un estudio sobre las principales técnicas y métodos de la esteganografía para el ocultamiento de información en archivos gráficos para lo cual se utilizó una matriz con sus parámetros y Excel para procesar la información, por lo tanto, se propone:

- Difundir el tema de la esteganografía en el ámbito nacional en centros educativos de tercer nivel y superiores, como complemento de estudio de la seguridad de la información.
- Robustecer el tema de la esteganografía con el análisis de las diferentes técnicas esteganográficas que enfaticen la necesidad de conocer cómo actúa en las imágenes y poder así prevenir sus ataques.

CAPITULO IV

RESULTADOS Y DISCUSIÓN

4.1. Análisis, Interpretación y Discusión de Resultados

Algoritmos de seguridad

Tabla 7: Cuadro comparativo del funcionamiento de dichas herramientas

Funcionalidad	QuickStego	OpenPuff	Xiao Steganography
Algoritmos de esteganografía	LSB (Least Significant Bit)	Varios algoritmos, incluyendo Blowfish, AES, y Twofish	LSB (Least Significant Bit)
Encriptación	No	Sí, con varios algoritmos, incluyendo Blowfish, AES, y Twofish	No
Autenticación	No	Sí, con contraseña y firma digital	No
Ocultamiento de archivos dentro de otros archivos	No	Sí, utilizando contenedores de datos	No

Fuente: (ESGEEKS, 2019)
Realizado por: Alvaro Veloz

La tabla 7 resume el funcionamiento de las herramientas esteganográficas donde se puede conocer los algoritmos esteganográficos, la encriptación, la autenticación y la ocultación de archivos dentro de otros archivos entre las características más relevantes de las 3 herramientas evaluadas.

Tabla 8: Cuadro comparativo de los algoritmos de seguridad que manejan las herramientas a estudiar.

Tecnología de seguridad	Tipo de cifrado	Longitud de clave	Ventajas	Desventajas
AES	Simétrico	128, 192 o 256 bits	Altamente seguro, ampliamente utilizado, implementación eficiente, resistentes a los ataques de fuerza bruta y criptoanálisis.	Requiere una clave segura, puede ser vulnerable a los ataques de canal lateral si no se implementa adecuadamente.
Blowfish	Simétrico	Variable, típicamente 64-448 bits	Seguro, implementación eficiente, ampliamente utilizado.	Menos seguro que AES, la implementación incorrecta puede ser vulnerable a ciertos ataques.
LSB	Esteganográfico	Variable	Útil para ocultar datos de manera discreta sin afectar significativamente la calidad perceptible de los archivos de imagen o audio.	No es una técnica de cifrado segura, los datos ocultos se pueden recuperar fácilmente mediante el uso de herramientas en línea.

Fuente: (OpenPuff Steganography, s.f.)
Realizado por: Alvaro Veloz

OpenPuff

- OpenPuff ofrece la mayor variedad de algoritmos de seguridad y encriptación, incluyendo Blowfish, AES y Twofish, que son conocidos por ser seguros y

robustos. Además, cuenta con opciones de autenticación mediante contraseñas y firma digital.

QuickStego

- QuickStego, por otro lado, utiliza el algoritmo LSB (Least Significant Bit), que es el método más simple y básico para ocultar datos en imágenes. No cuenta con encriptación ni autenticación para proteger los datos ocultos.

Xiao Steganography

- Xiao Steganography utiliza el mismo algoritmo LSB (Least Significant Bit) para ocultar datos en imágenes. No cuenta con opciones de encriptación ni autenticación.

En resumen, OpenPuff ofrece la mayor variedad de algoritmos de seguridad y opciones avanzadas de encriptación y autenticación, lo que aumenta su nivel de seguridad. QuickStego y Xiao Steganography como lo muestra en la **tabla 7** y en la **tabla 8**, por otro lado, utilizan el algoritmo LSB (Least Significant Bit), que es menos seguro que otros algoritmos más avanzados.

Tipo de cifrado

Tabla 9: Cuadro comparativo del tipo de cifrado de las herramientas esteganográficas

Software	Tipo de cifrado	Fortaleza del cifrado
OpenPuff	Cifrado AES de clave simétrica con 256 bits	Muy seguro, ampliamente utilizado
QuickStego	Algoritmo de cifrado simple y no especificado	No se conoce la fortaleza del cifrado
Xiao Steganography	Algoritmo de cifrado de clave simétrica personalizado (posiblemente cifrado Vigenère)	Menos seguro que AES utilizado por OpenPuff

Fuente: Propia
Realizado por: Alvaro Veloz

En resumen, OpenPuff utiliza el cifrado AES de clave simétrica con 256 bits, que se considera muy seguro. QuickStego utiliza un algoritmo de cifrado simple y no se proporcionan detalles sobre la fortaleza del cifrado. Por último, Xiao

Steganography utiliza un algoritmo de cifrado de clave simétrica personalizado, que se cree que es un cifrado Vigenère, que es menos seguro que el cifrado AES utilizado por OpenPuff como se muestra en la **tabla 9**.

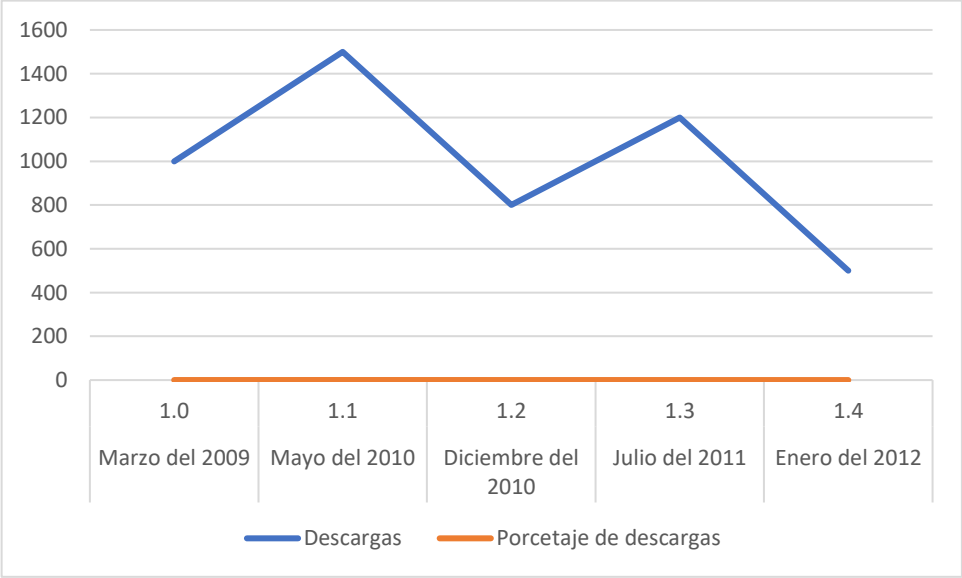
Resumen estadístico de las diferentes herramientas

Tabla 10: Resumen estadístico de la herramienta OpenPuff sobre las descargas de los usuarios

Año de creación	Versión del software	Descargas	Porcentaje de descargas
Marzo del 2009	1.0	1000	20%
Mayo del 2010	1.1	1500	30%
Diciembre del 2010	1.2	800	16%
Julio del 2011	1.3	1200	24%
Enero del 2012	1.4	500	10%
Total		5000	100%

Fuente: (OpenPuff Steganography, s.f.)
Realizado por: Alvaro Veloz

Figura 31: Ponderación grafica sobre el estado de las descargas de OpenPuff



Fuente: (OpenPuff Steganography, s.f.)
Realizado por: Alvaro Veloz

La **tabla 9 y figura 9** muestran que durante el periodo 2009 - 2012 hubo un total de 5000 descargas para las cinco versiones del software. Se observa que la versión

1.1 fue la más descargada con un 30% en el año 2009, la misma que decayó en el año 2012 hasta un 10 %.

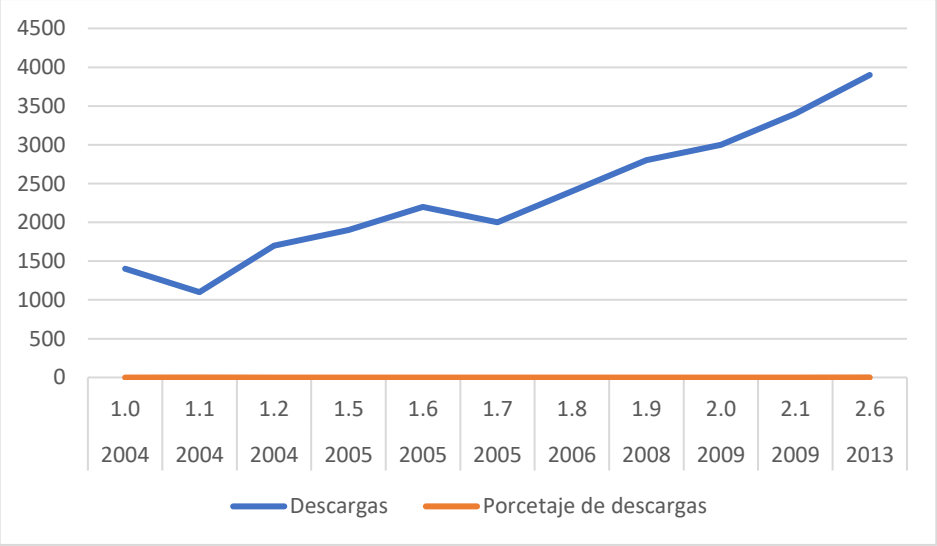
Quickstego

Tabla 11: Resumen estadístico de la herramienta Quickstego sobre las descargas de los usuarios.

Año de creación	Versión del software	Descargas	Porcentaje de descargas
Marzo del 2004	1.0	1400	5%
Mayo del 2004	1.1	1100	4%
Noviembre del 2004	1.2	1700	7%
Mayo del 2005	1.5	1900	7%
Julio del 2005	1.6	2200	9%
Noviembre del 2005	1.7	2000	8%
Julio del 2006	1.8	2400	9%
Marzo del 2008	1.9	2800	11%
Abril del 2009	2.0	3000	12%
Diciembre del 2009	2.1	3400	13%
Julio del 2013	2.6	3900	15%
Total		25800	100%

Fuente: (QuickCripto, 2020)
Realizado por: Alvaro Veloz

Figura 32: Ponderación grafica sobre el estado de las descargas de Quickstego



Fuente: (QuickCripto, 2020)
Realizado por: Alvaro Veloz

La **Tabla 10 y figura 10** muestran que durante el periodo 2004 - 2013 hubo un total de 25800 descargas para las once versiones del software. Se observa que la versión 2.6 fue la más descargada con un 15% en el año 2013, la misma que decayó en el año 2004 hasta un 4 %.

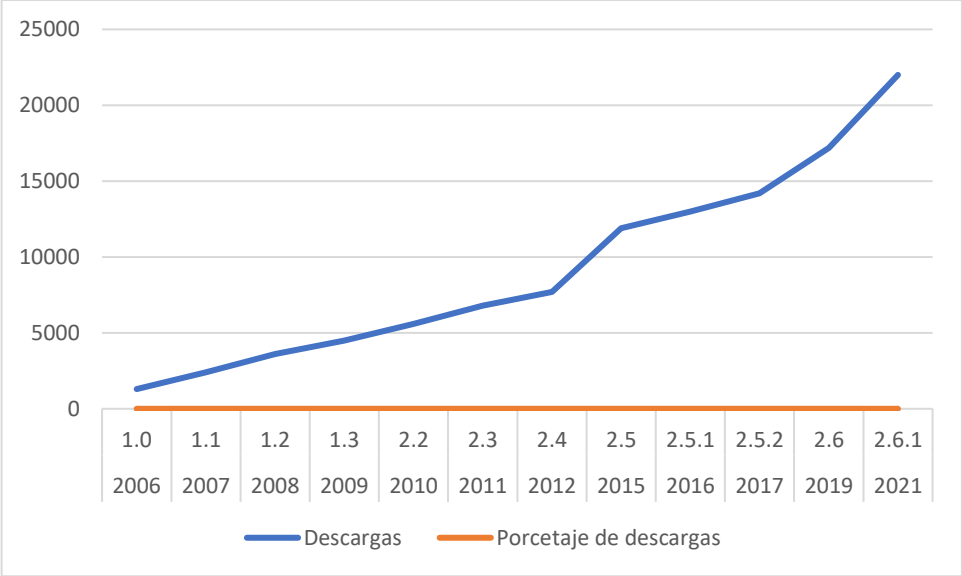
Xiao Steganography

Tabla 12: Resumen estadístico de la herramienta Xiao Steganography sobre las descargas de los usuarios.

Año de creación	versión del software	Descargas	Porcentaje de descargas
2006	1.0	1300	1%
2007	1.1	2400	2%
2008	1.2	3600	3%
2009	1.3	4500	4%
2010	2.2	5600	5%
2011	2.3	6800	6%
2012	2.4	7700	7%
2015	2.5	11900	11%
2016	2.5.1	13000	12%
2017	2.5.2	14200	13%
2019	2.6	17200	16%
2021	2.6.1	22000	20%
Total		110200	100%

Fuente: (Softonic, 2018)
Elaborado por: Alvaro Veloz

Figura 33: Ponderación grafica sobre el estado de las descargas de Xiao Steganography



Fuente: (Softonic, 2018)
Elaborado por: Alvaro Veloz

La **tabla 11 y figura 11** muestran que durante el periodo 2006 - 2021 hubo un total de 110200 descargas para las doce versiones del software. Se observa que la versión 2.6.1 fue la más descargada con un 20% en el año 2021, la misma que decayó en el año 2006 hasta el 1 %.

Cuadro resumen de las herramientas esteganográficas

Tabla 13: Resumen de las herramientas esteganográficas que estudiamos en el trabajo de investigación.

Características	OpenPuff	Quickstego	Xiao Steganography
Tipo de herramienta	Herramienta de esteganografía, que permite ocultar información en archivos de imagen, audio o video.	Herramienta de esteganografía, que permite ocultar información en archivos de imagen.	Herramienta de esteganografía, que permite ocultar información en archivos de imagen.
Funcionamiento	Utiliza técnicas de cifrado y ocultamiento de datos para esconder información en archivos portadores. Además, cuenta con la opción de añadir contraseña y/o cifrado a los datos ocultos.	Utiliza técnicas de cifrado y ocultamiento de datos para esconder información en archivos de imagen. Además, cuenta con la opción de añadir contraseña a los datos ocultos.	Utiliza técnicas de ocultamiento de datos para esconder información en archivos de imagen. Además, cuenta con la opción de añadir contraseña a los datos ocultos.
Interfaz	Cuenta con una interfaz gráfica de usuario (GUI) intuitiva y fácil de usar.	Cuenta con una interfaz gráfica de usuario (GUI) sencilla y fácil de usar.	Cuenta con una interfaz gráfica de usuario (GUI) sencilla y fácil de usar.
Plataformas compatibles	Es una herramienta multiplataforma, compatible con Windows, Mac OS y Linux.	Es una herramienta para Windows.	Es una herramienta para Windows.
Licencia	Es un software libre y gratuito, distribuido bajo la licencia GPL v3.	Es un software libre y gratuito, distribuido bajo la licencia GPL v2.	Es un software libre y gratuito, distribuido bajo la licencia GPL v3.
Ocultamiento	Alto	Bajo	Moderado
Detección	Alto	Bajo	Moderado
Protección de clave	Moderado	Bajo	Bajo

Protección de datos	Moderado	Bajo	Bajo
Seguridad en red	No aplicable	No aplicable	No aplicable
Formatos de imagen compatibles	BMP, JPG, PNG, GIF, ICO, TIF, WMF, EMF	BMP, JPG, GIF	BMP, JPG, PNG, GIF, TIF, ICO
Velocidad de procesamiento	Variable	Rápido	Rápido
Usabilidad de la herramienta	Compleja	Sencilla	Moderada
Tipo de archivo de entrada	Cualquier tipo de archivo	Imagen BMP, GIF, JPEG, PNG	Imagen BMP
Tamaño máximo del archivo a ocultar	Sin límite	20 MB	64 MB

Fuente: Página web oficial de cada herramienta esteganográfica
Elaborado por: Alvaro Veloz

Descripción de la herramienta OpenPuff:

- **Ocultamiento:** La herramienta ofrece un alto nivel de ocultamiento de datos, lo que significa que los datos pueden ser escondidos en una imagen de manera muy efectiva y es difícil de detectar.
- **Detección:** La herramienta ofrece un alto nivel de detección de datos ocultos, lo que significa que los datos ocultos pueden ser descubiertos sólo con técnicas avanzadas de análisis forense.
- **Protección de clave:** La herramienta ofrece un nivel moderado de protección de clave, lo que significa que la seguridad de la clave utilizada para ocultar los datos es razonablemente fuerte y difícil de comprometer.
- **Protección de datos:** La herramienta ofrece un nivel moderado de protección de datos, lo que significa que los datos ocultos están protegidos por contraseña y cifrado, y pueden ser accedidos sólo por personas autorizadas.
- **Seguridad en red:** La herramienta no es aplicable a la seguridad en red, ya que no está diseñada para transferir datos a través de una red.
- **Formatos de imagen compatibles:** La herramienta es capaz de ocultar datos en los siguientes formatos de imagen: BMP, JPG, PNG, GIF, ICO, TIF, WMF, EMF.
- **Velocidad de procesamiento:** La velocidad de procesamiento de la herramienta OpenPuff puede variar según el tamaño de los datos a ocultar y la complejidad de la técnica de esteganografía utilizada. En general, el proceso puede ser más lento que en otras herramientas debido a la implementación de medidas de seguridad adicionales.

Es importante tener en cuenta que OpenPuff es una herramienta de esteganografía avanzada que utiliza técnicas más complejas que otras herramientas más simples. Esto puede aumentar el tiempo de procesamiento, pero también puede ofrecer una mayor seguridad y ocultación de datos. Además, la velocidad de procesamiento también puede verse afectada por la capacidad del hardware utilizado.

- **Usabilidad de la herramienta:** La herramienta OpenPuff se considera compleja en términos de usabilidad, ya que tiene una amplia variedad de

opciones y configuraciones avanzadas. Además, su interfaz gráfica puede ser menos intuitiva que otras herramientas esteganográficas.

Es importante destacar que la complejidad de la herramienta también puede ser una ventaja, ya que permite una mayor personalización y control sobre el proceso de ocultación de datos. Sin embargo, para usuarios con poca experiencia en esteganografía, puede resultar difícil de usar.

- **Tipo de archivo de entrada:** OpenPuff admite cualquier tipo de archivo como entrada, incluyendo imágenes, audio, video, documentos y archivos comprimidos.
- **Tamaño máximo del archivo a ocultar:** La cantidad máxima de datos que se pueden ocultar en un archivo depende del tamaño del archivo de entrada y de la cantidad de bits menos significativos que se utilicen para ocultar los datos. En el caso de OpenPuff, no hay un límite máximo en cuanto a la cantidad de datos que se pueden ocultar.

Es importante tener en cuenta que ocultar una gran cantidad de datos en un archivo puede disminuir la calidad del archivo resultante y hacer que sea más fácilmente detectable. Además, la capacidad de ocultación de datos de OpenPuff también dependerá de los algoritmos de seguridad y de esteganografía utilizados.

Descripción de la herramienta Quickstego

- **Ocultamiento:** La herramienta ofrece un nivel bajo de ocultamiento de datos, lo que significa que los datos pueden ser escondidos en una imagen, pero es relativamente fácil de detectar.
- **Detección:** La herramienta ofrece un nivel bajo de detección de datos ocultos, lo que significa que los datos ocultos pueden ser descubiertos con técnicas simples de análisis forense.
- **Protección de clave:** La herramienta ofrece un nivel bajo de protección de clave, lo que significa que la seguridad de la clave utilizada para ocultar los datos es débil y puede ser comprometida fácilmente.

- **Protección de datos:** La herramienta ofrece un nivel bajo de protección de datos, lo que significa que los datos ocultos no están protegidos por contraseña o cifrado, y pueden ser accedidos por cualquier persona que tenga acceso a la imagen.
- **Seguridad en red:** La herramienta no es aplicable a la seguridad en red, ya que no está diseñada para transferir datos a través de una red.
- **Formatos de imagen compatibles:** La herramienta es capaz de ocultar datos en los siguientes formatos de imagen: BMP, JPG y GIF.

Es importante tener en cuenta que QuickStego no es compatible con formatos de imagen más modernos, como PNG o TIF. Además, como la herramienta no ha sido actualizada en varios años, puede no ser compatible con las últimas versiones del sistema operativo Windows.

- **Velocidad de procesamiento:** La herramienta QuickStego tiene una velocidad de procesamiento rápida, lo que significa que el tiempo de ocultación y extracción de datos es relativamente rápido.

Es importante tener en cuenta que el tiempo de procesamiento también dependerá del tamaño de la imagen y de los datos que se estén ocultando. Además, la velocidad de procesamiento puede verse afectada por la capacidad del hardware utilizado.

- **Usabilidad de la herramienta:** La herramienta QuickStego se considera sencilla en términos de usabilidad, ya que su interfaz gráfica es intuitiva y fácil de usar, lo que hace que sea una buena opción para usuarios sin experiencia previa en esteganografía.

Es importante tener en cuenta que la simplicidad de la herramienta también puede ser una desventaja en términos de personalización y control sobre el proceso de ocultación de datos. Además, QuickStego no tiene tantas opciones avanzadas como otras herramientas más complejas, lo que puede limitar su utilidad en ciertos casos.

- **Tipo de archivo de entrada:** QuickStego admite varios tipos de archivo de imagen como entrada, incluyendo BMP, GIF, JPEG y PNG.
- **Tamaño máximo del archivo a ocultar:** La cantidad máxima de datos que se pueden ocultar en una imagen depende del tamaño de la imagen y de la cantidad de bits menos significativos que se utilicen para ocultar los datos. En el caso de QuickStego, se puede ocultar un archivo de hasta 20 MB en una imagen BMP, GIF, JPEG o PNG.

Es importante tener en cuenta que la cantidad máxima de datos que se pueden ocultar en una imagen depende del tipo de archivo de entrada y del algoritmo utilizado por la herramienta esteganográfica. Además, es importante recordar que ocultar una gran cantidad de datos en una imagen puede disminuir la calidad visual de la imagen resultante y hacer que sea más fácilmente detectable.

Descripción de la herramienta Xiao Steganography

- **Ocultamiento:** La herramienta ofrece un nivel moderado de ocultamiento de datos, lo que significa que los datos pueden ser escondidos en una imagen de manera efectiva, pero pueden ser detectados por técnicas de análisis forense.
- **Detección:** La herramienta ofrece un nivel moderado de detección de datos ocultos, lo que significa que los datos ocultos pueden ser descubiertos con técnicas de análisis forense.
- **Protección de clave:** La herramienta ofrece un nivel bajo de protección de clave, lo que significa que la seguridad de la clave utilizada para ocultar los datos es débil y puede ser comprometida fácilmente.
- **Protección de datos:** La herramienta ofrece un nivel bajo de protección de datos, lo que significa que los datos ocultos no están protegidos por contraseña o cifrado, y pueden ser accedidos por cualquier persona que tenga acceso a la imagen.
- **Seguridad en red:** La herramienta no es aplicable a la seguridad en red, ya que no está diseñada para transferir datos a través de una red.
- **Formatos de imagen compatibles:** La herramienta es capaz de ocultar datos en los siguientes formatos de imagen: BMP, JPG, PNG, GIF, TIF y ICO.

Es importante tener en cuenta que, aunque Xiao Steganography es compatible con una amplia variedad de formatos de imagen, también es importante considerar la seguridad de la herramienta. Se recomienda evaluar la seguridad y la confiabilidad de cualquier herramienta antes de utilizarla para ocultar información confidencial.

- **Velocidad de procesamiento:** La herramienta Xiao Steganography tiene una velocidad de procesamiento rápida, lo que significa que el tiempo de ocultación y extracción de datos es relativamente rápido.

Es importante tener en cuenta que el tiempo de procesamiento también dependerá del tamaño de la imagen y de los datos que se estén ocultando. Además, la velocidad de procesamiento puede verse afectada por la capacidad del hardware utilizado.

- **Usabilidad de la herramienta:** La herramienta Xiao Steganography se considera moderadamente fácil de usar, ya que su interfaz gráfica es intuitiva y tiene opciones sencillas para la ocultación de datos. Sin embargo, también tiene algunas características avanzadas que pueden ser un poco más difíciles de entender.

Es importante destacar que Xiao Steganography tiene varias opciones avanzadas, como la capacidad de utilizar múltiples métodos de ocultación de datos y la encriptación de archivos, lo que lo hace una herramienta muy útil para usuarios con experiencia en esteganografía y criptografía.

- **Tipo de archivo de entrada:** Xiao Steganography solo admite imágenes BMP como archivo de entrada.
- **Tamaño máximo del archivo a ocultar:** La cantidad máxima de datos que se pueden ocultar en una imagen BMP depende del tamaño de la imagen y de la cantidad de bits menos significativos que se utilicen para ocultar los datos. En el caso de Xiao Steganography, se puede ocultar un archivo de hasta 64 MB en una imagen BMP.

CONCLUSIONES

- La seguridad informática es un aspecto crucial en el mundo tecnológico actualmente, es por ello que el aumento de la digitalización y la interconexión de dispositivos, la protección de la información se ha vuelto más compleja y necesaria que nunca. Por lo tanto, es fundamental que las empresas y los usuarios adopten medidas de seguridad efectivas para proteger sus datos y prevenir amenazas cibernéticas, como el robo de identidad, el malware y los ataques de phishing.
- Se concluye que la herramienta OpenPuff es la mejor opción para ocultar datos entre múltiples portadores y su capacidad para utilizar claves de cifrado personalizadas debido a su algoritmo AES, en cambio QuickStego y Xiao Steganography son más fáciles de usar y tienen interfaces de usuario más intuitivas, pero utilizan cifrados más débiles y tienen limitaciones en cuanto a los tipos de archivos en los que se pueden ocultar datos.
- También se concluye que la unión de la estenografía y criptografía generan un resultado con mayor nivel de seguridad comparado con el promedio; siendo eficiente en cuanto a su tiempo de ejecución, logrando que a los ojos de un atacante sean imperceptibles los cambios realizados sobre la imagen original.
- Se concluye que la herramienta más utilizada por los usuarios es Xiao Steganography con un total de 110200 descargas para las doce versiones del software que fueron lanzadas al mercado desde su creación.

RECOMENDACIONES

- Se recomienda utilizar la esteganografía ya que es una forma segura y confiable de compartir información, es por ello que, al ocultar un mensaje dentro de una imagen, puede mantener su privacidad y confidencialidad de una manera que no es posible esconderlos con otros métodos más convencionales. Sin embargo, tenemos que tener en cuenta que la esteganografía puede ser costosa y requiere cierta habilidad técnica para usarla correctamente.
- Después de analizar las necesidades de seguridad y privacidad se recomienda utilizar la herramienta esteganográfica OpenPuff porque ofrece la mayor variedad de algoritmos de seguridad y encriptación, incluyendo Blowfish, AES y Twofish, que son conocidos por ser seguros y robustos. Sin embargo, es importante tener en cuenta que el tamaño máximo del archivo de destino no puede exceder los 256 Megabytes, pero no hay duda de que OpenPuff será una excelente opción para proteger los datos.
- Se recomienda realizar un estudio completo de las diferentes técnicas y métodos existentes de la esteganografía en el ocultamiento de información para los diferentes medios digitales.

BIBLIOGRAFÍA

27001:2013, I. (11 de Marzo de 2021). *ISOTools Excellence*. Obtenido de ISOTools Excellence: https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/

Ayudaley. (13 de Mayo de 2020). Obtenido de Ayudaley: https://ayudaleyprotecciondatos.es/2020/05/13/estaganografia/

ayudaley. (17 de Marzo de 2021). Obtenido de ayudaley: https://ayudaleyprotecciondatos.es/2021/03/17/esteganografia/

Ayudaley. (17 de Marzo de 2021). Obtenido de Ayudaley: https://ayudaleyprotecciondatos.es/2021/03/17/esteganografia/

Berry, P. (3 de Mayo de 2023). *surveillancepackages.* Obtenido de surveillancepackages: https://es1.surveillancepackages.com/difference-between-steganography-and-cryptography-22a4

Bhatia, N. (2019 de Enero de 2019). Obtenido de https://www.ijsrcsams.com/images/stories/Past_Issue_Docs/ijsrcsamsv8i1p158.pdf

BITBUCKET. (s.f.). Obtenido de BITBUCKET: https://www.atlassian.com/es/git/tutorials/what-is-git

Blogger. (11 de Febrero de 2019). Obtenido de Blogger: https://destejiendo.blogspot.com/2018/02/breve-historia-de-la-esteganografia-1.html

CIBERSEGURIDAD. (4 de Febrero de 2022). Obtenido de CIBERSEGURIDAD: https://ciberseguridad.com/amenzas/ciberataques-activos-pasivos/

E, M. (Septiembre de 2015). Obtenido de file:///C:/Users/Dell/Downloads/3509.pdf

El Universo. (2019). Obtenido de El Universo: https://www.eluniverso.com/vida-estilo/2015/08/03/nota/5051431/encriptar-seguridad-nube-mas-compleja-efectiva/

El Universo. (2019). Obtenido de El Universo: La esteganografía es muy poco conocida y no aporta mucha información sobre el tema, lo que no quiere decir que no se utilice sin conocer su existencia, pero son cada vez más indispensables en el medio digital. Otra problemática que se tiene es al momento

enfasys. (25 de Enero de 2023). Obtenido de enfasys: https://www.enfasys.net/2023/01/25/esteganografia-el-ciberataque-de-la-imagen-en-blanco/

Ephesos Software. (2023). Obtenido de Ephesos Software: https://es.ephesossoftware.com/articles/windows/openpuff-professional-strength-steganography-by-hiding-data-in-photos-more-windows.html

ESGEEKS. (2019). Obtenido de ESGEEKS: https://esgeeks.com/mejores-herramientas-esteganografia/

Española, E. R. (2006). *Real academia española* . Obtenido de Real academia española: https://www.rae.es/dhle/estegoan%C3%A1lisis

Fernandez, Y. (15 de Agosto de 2019). Obtenido de https://www.xataka.com/historia-tecnologica/cuando-una-imagen-oculta-mas-informacion-de-lo-que-parece-que-es-y-como-funciona-la-esteganografia

Incibe. (10 de Julio de 2019). Obtenido de Incibe: https://www.osi.es/es/actualidad/blog/2019/07/10/sabias-que-existen-distintos-tipos-de-cifrado-para-proteger-la privacidad#:~:text=La%20criptograf%C3%ADa%20es%20una%20t%C3%A9cnica, encargan%20de%20cifrar%20los%20mensajes

International IT. (28 de Septiembre de 2002). Obtenido de International IT: https://www.internationalit.com/post/cu%C3%A1les-son-los-principales-tipos-de-cifrado-para-la-transferencia-segura-de-archivos?lang=es#:~:text=Los%20algoritmos%20de%20cifrado%20son,indescifrable%2C%20com%C3%BAnmente%20conocido%20como%20cifrado.

LEY DE COMERCIO ELECTRONICO, F. Y. (17 de abril de 2002). Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf

López, A. (19 de Julio de 2022). *Redes Zone*. Obtenido de Redes Zone : https://www.redeszone.net/tutoriales/seguridad/criptografia-algoritmos-hash/

Lorente, A. S. (1 de Octubre de 2013). Obtenido de file:///C:/Users/Dell/Downloads/Dialnet-AlgoritmoEsteganograficoDeClavePrivada-5991687.pdf

Manrique, F. (4 de 11 de 2021). *Trentia*. Obtenido de Trentia: https://www.trentia.net/evolucion-de-la-estenografia-desde-sus-origenes-hasta-la-era-digital/

Mayans, L. S. (Julio de 2000). Obtenido de https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnwyMDE0c2NqaW1lbmV6Y29yb25hZXJuZXN0b3xneDozNmQyYjBkNDJmYzZjZTli

NIC. (Marzo de 2018). Obtenido de NIC: https://nic.ar/es/enterate/novedades/que-es-criptografia

Oliboni, E. C. (19 de Julio de 2019). Obtenido de https://es.wikipedia.org/wiki/OpenPuff

OPENPUFF. (2019). Obtenido de OPENPUFF: https://embeddedsw.net/doc/OpenPuff_Help_EN.pdf

OpenPuff Steganography. (s.f.). Obtenido de OpenPuff Steganography: https://embeddedsw.net/OpenPuff_Steganography_Home.html

QuickCripto. (2020). Obtenido de QuickCripto: http://quickcrypto.com/free-steganography-software.html

softonic. (2018). Obtenido de softonic: https://xiao-steganography.en.softonic.com/?ex=DINS-635.1

softonic. (2019). Obtenido de softonic: https://xiao-steganography.en.softonic.com/?ex=DINS-635.0

Solís, L. D. (2020). *investigalia*. Obtenido de investigalia: https://investigaliacr.com/investigacion/metodos-y-tecnicas-de-investigacion-cualitativa/

Villagrán. (3 de Septiembre de 2019). *VSAntivirus*. Obtenido de VSAntivirus: http://www.vsantivirus.com/esteganografia.htm

Yglesias, P. (13 de Marzo de 2020). Obtenido de https://error595.wordpress.com/2020/03/13/stego/

ANEXOS

- **Anexo 1:** Cronograma (Gantt)

Actividades	F. Inicio	F. Final	Sem1	Sem2	Sem3	Sem4	Sem5	Sem6	Sem7	Sem8	Sem9	Sem10
Revisión bibliográfica sobre la esteganografía	10-Ene	14-Ene										
Definir los objetivos para la investigación	15-Ene	17-Ene										
Establecer las variables con las que se va a trabajar en la investigación	23-Ene	31-Ene										
Definir las herramientas para realizar el estudio comparativo	6-Feb	8-Feb										
Análisis de las herramientas esteganográficas	8-Feb	13-Feb										
Realizar las prácticas con dichas herramientas	20-Feb	27-Feb										
Analizar los algoritmos de las que trabajan dichas herramientas.	6-Mar	20-Mar										
Establecer las ventajas y desventajas de las mismas	21-Mar	7-Abr										
Definir la herramienta más recomendable para transmitir los mensajes de forma secreta	10-Abr	24-Abr										

- **Anexo 2:** Presupuesto Ejecutado

Recurso	Cantidad	Precio Unitario	Total
Internet (por mes)	6	$25	$ 150.0
Computadora	1	$380	$ 380.0
Carpetas	2	$0.75	$1.50
Esferos	1	$0.50	$0.50
Resma de papel	1	$4.50	$4.50
		Total	$536.5

DR. HENRY VALLEJO BALLESTEROS EN CALIDAD DE DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR,

CERTIFICA

Que el trabajo de integración curricular denominado "**COMPARACIÓN DE LAS HERRAMIENTAS ESTEGANOGRÁFICAS PARA OCULTAR INFORMACIÓN EN ARCHIVOS GRÁFICOS**", presentado por Veloz Becerra Luis Álvaro estudiante de la **carrera de Software** pasó el análisis de coincidencia no accidental en la herramienta URKUND, reflejando un **porcentaje de similitud del 5%**, como se puede evidenciar en el documento adjunto.

Ouriginal by Turnitin

Document Information

Analyzed document	Estudio de las herramientas esteganograficas 1.docx (D167178333)
Submitted	5/16/2023 6:10:00 PM
Submitted by	
Submitter email	luveloz@mailes.ueb.edu.ec
Similarity	5%
Analysis address	hvallejo.ueb@analysis.urkund.com

Guaranda, 17 de mayo del 2023

Atentamente,

Dr. Henry Vallejo B. MsC.
Director