Desarrollo de un método esteganográfico para la ocultación de información en medios digitales

Martínez Pazmiño Ismael Alfonso

Departamento de Ciencias de la Computación

Carrera de Ingeniería de Sistemas e Informática

Trabajo de titulación, previo a la obtención del título de Ingeniero en Sistemas e Informática

PhD. Marcillo Parra, Diego Miguel

1 de Septiembre del 2021

Curiginal

Document Information

Analyzed document	TESISVF_Martinez_Ismael.docx (D110674358)
Submitted	7/22/2021 8:34:00 PM
Submitted by	Diego Marcillo Parra
Submitter email	dmmarcillo@espe.edu.ec
Similarity	0%
Analysis address	dmmarcillo.espe@analysis.urkund.com

Sources included in the report

W URL: https://doi.org/10.1109/ICCIACT46704.2019.8938486
Fetched: 7/22/2021 8:34:00 PM — 4

Firma:

DIEGO MIGUEL MARCILLO PARRA

Marcillo Parra Diego Miguel

DIRECTOR

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

CERTIFICACIÓN

Certifico que el trabajo de titulación, "**Desarrollo de un método esteganográfico para la ocultación de información en medios digitales**" fue realizado por el señor **Martínez Pazmiño Ismael Alfonso** el cual ha sido revisado y analizado en su totalidad por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 1 de Septiembre 2021

Firma:

Firmado electrónicamente por:
DIEGO MIGUEL
MARCILLO
PARRA

.....

Marcillo Parra Diego Miguel

C. C. : 1710802925

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

RESPONSABILIDAD DE AUTORÍA

Yo, **Martínez Pazmiño Ismael Alfonso**, con cédula de ciudadanía n° 1721727111, declaro que el contenido, ideas y criterios del trabajo de titulación: **Desarrollo de un método esteganográfico para la ocultación de información en medios digitales** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 1 de Septiembre 2021

Firma

ISMAEL ALFONSO MARTINEZ PAZMINO

Martínez Pazmiño Ismael Alfonso

C.C.: 1721727111

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

AUTORIZACIÓN DE PUBLICACIÓN

Yo **Martínez Pazmiño Ismael Alfonso,** con cédula de ciudadanía n°1721727111, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **Desarrollo de un método esteganográfico para la ocultación de información en medios digitales** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 1 de Septiembre 2021

Firma

ISMAEL
ALFONSO
MARTINEZ
PAZMINO

Martínez Pazmiño Ismael Alfonso

C.C.: 1721727111

Dedicatoria

Este trabajo está dedicado a mis padres, Ignacio y Marya, por brindarme todo su apoyo durante toda mi vida y, en especial, mis estudios universitarios, por saberme indicar lo que está bien, lo que está mal y sobre todo, enseñarme a ser una persona de bien.

A mi hermano Joel ya que como su hermano mayor, siento que es mi deber darle un buen ejemplo a seguir y permitirle aspirar a cosas grandiosas durante su vida.

A mis amigos Melany, Matias, Nicolás, Juan Sebastián, Mateo, José, Katty y Samantha, sé que siempre podré contar con su apoyo y amistad.

Al ingeniero Diego Marcillo por su apoyo durante la realización de este trabajo y ser un excelente docente.

Ismael Martínez

Agradecimiento

Agradezco a mis padres, Ignacio y Marya, a mi hermano Joel por apoyarme en todo lo que he necesitado para cumplir esta meta, ya que sin ellos este viaje pudo ser muy complicado y sobre todo, solitario.

Un agradecimiento especial a mi amiga Melany Palacios por siempre estar ahí y apoyarme en momentos en los que las cosas se veían difíciles y recordarme que siempre hay una solución. A todos mis amigos del colegio por ser maravillosas personas y un grupo muy unido, lo que me ha brindado maravillosos momentos a lo largo de los años.

Un agradecimiento especial al Ingeniero Diego Marcillo por guiarme durante el desarrollo de este trabajo.

A las maravillosas personas que conocí durante mi vida estudiantil por recordarme que en la universidad también se pasan momentos divertidos. A todos los Ingenieros del cuerpo docente, por enseñarme a ser excelente profesional y una persona con valores.

Ismael Martínez

Índice de contenido

Índice de tablas

Índice de figuras

Resumen

El rápido desarrollo de las ciencias computacionales junto con la creciente dependencia del internet, acentuada aún más por la pandemia del Covid-19, y el incremento de ataques informáticos, como por ejemplo el robo de información, han posicionado a la seguridad informática como una de las ciencias más importantes de nuestros tiempos. Una parte importante de la seguridad de la información es la confidencialidad, para este fin se puede optar por técnicas criptográficas o esteganográficas. El LSB es una técnica esteganográfica popular para ocultar información en medios no confidenciales, no obstante es fácilmente vulnerable. Por esta razón, el presente trabajo tiene como principal objetivo plantear un algoritmo esteganográfico que brinde más seguridad en comparación con el método LSB. Para poder llevar a cabo la construcción de este nuevo algoritmo se ha seguido una metodología de investigación de tres pasos propuesta por el autor. Cada uno de los pasos cubre una parte del proceso de desarrollo del trabajo, desde la investigación hasta la validación del algoritmo propuesto, de forma que permita cumplir con el objetivo planteado. Tras haber culminado la fase de evaluación, el algoritmo propuesto demostró ser más seguro que el algoritmo LSB hasta un 44%. No obstante, esta mejora se presenta al ocultar hasta 30 bytes de información, ya que cantidades mayores producen resultados adversos. Por lo tanto, a pesar de presentar mejoras notables, el algoritmo propuesto solo se considera eficiente en escenarios donde la información a ocultar no supere la cantidad descrita anteriormente.

Palabras clave:

- **SEGURIDAD INFORMÁTICA**
- **ESTEGANOGRAFÍA**
- **LSB**
- **MEJORA SOBRE LSB**
- **NUEVA PROPUESTA**

Abstract

The fast paced development of computer science, the ever growing user dependency of internet services and applications, accentuated by the Covid-19 pandemic, and the recent increase in cyber-attacks managed to put information security as one of the most important sciences of our times. An important part of information security is confidentiality, to achieve this there is a wide variety of cryptographic and steganographic techniques to choose from. LSB is a well-known steganographic technique used to hide information in non-confidential files, nevertheless, due to its simplicity, this technique is very easy to break. Due to this flaw, this study's main purpose is to present a new steganographic algorithm with enhanced security compared to the LSB algorithm, thus offering a new option to achieve information confidentiality with relevant security levels. To be able to build this new algorithm a three-step methodology proposed by the author was used. Each one of the methodology steps covers a part of the process of developing this study, from the preliminary investigation phase up to the evaluation of the proposed algorithm. After the evaluation phase finished, the desired results were achieved. The proposed algorithm showed an improvement of 44%. Nevertheless, this level of improvement is only present when hiding a maximum of 30 bytes, any more produces non favorable results. Thus, this algorithm is only suitable in scenarios where the information to be hidden is less or equal to 30 bytes.

Keywords:

- **INFORMATION SECURITY**
- **STEGANOGRAPHY**
- **LSB**
- **IPROVEMENT OVER LSB**
- **NOVEL ALGORITHM**

Capítulo I: Introducción

Antecedentes

Durante los últimos años se ha presenciado un incremento sustancial en el uso del internet, encontrándose que se ha evidenciado un crecimiento del 2 360% desde el año 2000 hasta el 2019 en latino américa y el caribe (Gonzáles, 2019). El rápido desarrollo del internet ha brindado paso a un mayor número de aplicaciones como: banca en línea, teletrabajo, e-commerce y video (Chen & Gong, 2012). Las oportunidades sin precedentes que ha brindado el acceso a internet, como el acceso a la información, trae consigo nuevos retos que se deben tener en consideración, entre ellos se puede destacar la necesidad creciente de mantener la seguridad de los datos y la privacidad de los usuarios (Abood, 2017; Morales & Robalino-Lopez, 2020).

En el año 2020, debido a la pandemia provocada por el SARS-COVID-2, la seguridad de la información se ha visto puesta a prueba debido a la creciente cantidad de ataques dirigidos a empresas y entidades gubernamentales que han migrado sus operaciones a sistemas que permiten la ejecución de la modalidad de teletrabajo. En el primer cuatrimestre del año 2020 se registraron 737 incidentes relacionados con malware de secuestro de datos y robo de información, además de la detección de 48,000 nuevas URLs malignas registradas (INTERPOL, 2020). Estos ataques, en algunos casos se han enfocado en la extracción de datos e información relevante, ya sea sobre actividades económicas empresariales e incluso datos relacionados al desarrollo de la vacuna contra el virus. Esta información es sumamente valiosa y los cibercriminales buscan obtener un gran redito económico apropiándose de esta información de forma ilegal (Gamba, 2020; INTERPOL, 2020).

Si bien existe una gran cantidad de estudios enfocados al impacto de las brechas de seguridad cuando se trata de información relacionada al área de la salud, poco se ha hablado del efecto que tienen pandemias como la actual y de la oportunidad que representa para los cibercriminales (Williams et al., 2020). Los ataques cibernéticos se han presentado particularmente problemáticos durante la pandemia del Covid-19 debido a su estrecha relación con la información confidencial de pacientes, a esto se agrega el hecho de que cerca del 90% de proveedores de salud han enfrentado brechas de seguridad en sus sistemas (Williams et al., 2020). Los ataques cibernéticos tienen una afectación económica de alrededor de 6 trillones de dólares (USD) alrededor del mundo para el año 2021, cifra que se ha duplicado desde el año 2015 donde la afectación económica bordeaba los 3 trillones de dólares (Williams et al., 2020).

Aunque los sistemas de seguridad pueden presentar brechas es importante que se mantenga la confidencialidad de la información a la que se podría acceder. Existen varios métodos propuestos por la comunidad científica para mantener la información segura y confidencial mediante el uso de criptografía y esteganografía (Abood, 2017).

La criptografía permite la creación de cadenas extensas de información codificada mediante funciones matemáticas complejas que dificulten su decodificación sin los datos necesarios para realizar este proceso. Existen diversos métodos como el RSA y ECDSA aunque hayan sido vulnerados, mediante la implementación de diversas técnicas la mejora del nivel de seguridad es considerable (Ayala et al., 2018; Salguero Dorokhin et al., 2019).

La esteganografía es el arte de ocultar información secreta en un medio que parecería irrelevante a simple vista y es tan antigua como la escritura misma (Kuksov, 2019). A diferencia de otros métodos para mantener la información asegurada como la criptografía, el objetivo de la esteganografía es lograr que la información pase desapercibida por personas a las que no está destinada (Kuksov, 2019). La esteganografía digital toma la ventaja de que casi cualquier objeto

digital puede contener información oculta ya que para el computador, es una únicamente una colección de bits (Kuksov, 2019). Entre las propuestas de la comunidad científica para mantener la seguridad de la información, el método esteganográfico LSB (Least Significant Bit) sigue siendo una de las técnicas más utilizadas para ocultar información en medios digitales y mantener la confidencialidad de la información (Jun et al., 2007).

Planteamiento del problema

La problemática que se aborda en esta investigación es la inseguridad que resulta en utilizar el método esteganográfico del bit menos significativo (LSB) como método preferente para el ocultamiento de información en medios digitales, más específicamente, en imágenes digitales, Thangadurai & Sudha Devi (2014) han realizado un estudio en el que se detalla el funcionamiento explícito y los principios del funcionamiento del método esteganográfico LSB y su contraparte el MSB (bit más significativo).

Debido al conocimiento público del funcionamiento del método de LSB se desata una constante búsqueda de mejora, tanto para sistemas esteganográficos como para sistemas de análisis diseñados específicamente para la detección de información oculta en los bits menos significativos de medios digitales como imágenes, texto y audio/video (Jun et al., 2007; Yang et al., 2017).

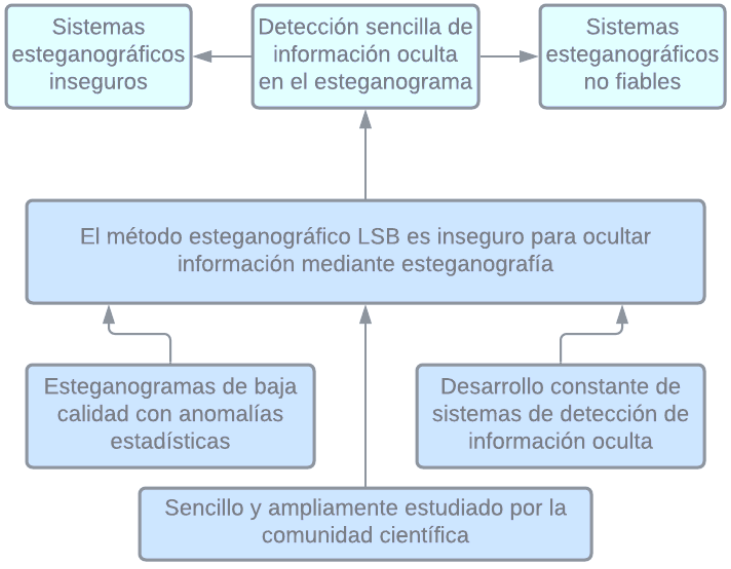
La técnica esteganográfica LSB se caracteriza, además, por producir esteganogramas de baja calidad, es decir, que aunque al ojo humano los cambios sean casi imperceptibles, análisis estadísticos como Peak Signal to Noise Ratio (PSNR) o Mean Square Error (MSE) pueden exponer de forma gráfica la agrupación de datos en una imagen, volviéndola sospechosa para los atacantes (Jois & Tejaswini, 2016).

Como consecuencia, al tomar en cuenta los efectos que conllevan el uso de métodos esteganográficos sobre los esteganogramas, las características estadísticas del mensaje no deben ser diferentes de las características estadísticas de los esteganogramas, ya que de ser el caso se facilita la revelación de información y por lo tanto el sistema esteganográfico se vuelve inseguro y no fiable (Westfeld & Pfitzmann, 2000).

La Figura 1 presenta una síntesis de las causas y consecuencias del problema que se ha identificado, dando relación a las causas descritas por los autores Jois & Tejaswini, 2016; Jun et al., 2007; Thangadurai & Sudha Devi, 2014; Yang et al., 2017 y las consecuencias como lo describen Westfeld & Pfitzmann, 2000.

Figura 1

Síntesis de causas y consecuencias resumidas en un árbol de problemas



En el presente trabajo se aborda la carencia de métodos alternativos para ocultar información en una imagen digital, puesto que para mejorar los sistemas esteganográficos existentes se necesitarán métodos más “diferentes” de aplicar la esteganografía digital. El objetivo es incrementar la seguridad de los sistemas esteganográficos, de tal forma que se

ofrezca una alternativa a los métodos LSB o MSB. Al ofrecer una nueva forma de usar la esteganografía en medios digitales se apunta a aumentar la seguridad y confidencialidad de la información almacenada en dispositivos digitales o que se transporte por la red, accesible para el corporativo e individuos.

Justificación

Como ya se ha establecido durante los antecedentes, en los últimos años se ha presenciado un incremento sustancial en el uso del internet (Chen & Gong, 2012) y con ello las oportunidades que se han presentado traen consigo nuevos retos relacionados con la seguridad y confidencialidad de los datos de los usuarios (Abood, 2017; Morales & Robalino-Lopez, 2020). La esteganografía y el estegoanálisis forman parte del núcleo de la seguridad para la transmisión de datos, convirtiéndose en un punto de gran interés en el área del ocultamiento de información (Jun et al., 2007). La esteganografía toma un papel sumamente importante en el área de la seguridad de la información ya que la mejor forma de mantener la confidencialidad de la información es mantenerla desapercibida u oculta en otros medios (Elkamchouchi et al., 2018). La criptografía, en cambio, se muestra bastante obvia al exponer datos explícitamente codificados a los atacantes(Elkamchouchi et al., 2018).

Aunque la esteganografía se muestre como una alternativa más segura que la criptografía debido a su capacidad de guardar información de forma discreta, la constante mejora de sistemas de análisis diseñados específicamente para la detección de información oculta en medios digitales realzan la preocupación de contar con técnicas y algoritmos esteganográficos ampliamente conocidos y utilizados como es el caso del LSB (Jun et al., 2007; Yang et al., 2017).

Es importante contar con nuevos medios para proteger la información ya que como se ha podido determinar, los ataques cibernéticos se han presentado particularmente problemáticos durante la pandemia del Covid-19 debido a su estrecha relación con la información confidencial de pacientes (Williams et al., 2020). Si la única forma de proteger y mantener la información privada de personal naturales u organizaciones depende de una técnica esteganográfica ampliamente conocida y vulnerada es de esperar que los datos no estén seguros y que por lo tanto se puedan provocar pérdidas y afectaciones que superen los 6 trillones de dólares (USD) alrededor del mundo (Williams et al., 2020). Es necesario plantear alternativas que se presenten más seguras y estables que puedan brindar una capa de seguridad extra y poner la seguridad de la información un paso adelante en la constante búsqueda de métodos seguros y sistemas de análisis para el robo de información encriptada u oculta en medios esteganográficos.

Objetivos

Objetivo General

Proponer un nuevo método esteganográfico mediante la implementación de un algoritmo de ocultación de información en medios digitales con la finalidad de brindar alternativas de mejora de seguridad al uso de LSB para esteganografía.

Objetivos específicos

OE1 Analizar la situación actual y las propuestas de la comunidad científica sobre los niveles de seguridad de los métodos esteganográficos disponibles mediante la revisión de la literatura sobre los niveles de seguridad de los métodos de seguridad disponibles.

OE2 Desarrollar un prototipo funcional mediante la implementación de un algoritmo esteganográfico seguro que evada los ataques comunes contra esteganogramas que usen la técnica LSB.

OE3 Validar el algoritmo propuesto mediante la utilización de los métodos de estegoanálisis estadísticos aplicados para vulnerar un esteganograma.

Alcance

La esteganografía digital se puede emplear en imágenes, audio, video y texto. Sin embargo, esta investigación se centra en la construcción de un algoritmo esteganográfico específico para la ocultación de información en imágenes digitales. Una vez se haya desarrollado el algoritmo, el mismo será evaluado para determinar su nivel de seguridad y su rendimiento computacional. Para esto se someterá al algoritmo a los métodos de estegoanálisis conocidos con la finalidad de determinar si es vulnerable. También se evaluará su rendimiento en tiempo de ejecución y uso de recursos computacionales.

Para delimitar de forma adecuada el alcance de la investigación se han planteado preguntas de investigación asociadas a los objetivos específicos como se muestra en la Tabla 1.

Tabla 1

Objetivos específicos y preguntas de investigación

Objetivos específicos	**Preguntas de investigación**
Analizar la situación actual y las propuestas de la comunidad científica sobre los niveles de seguridad de los métodos esteganográficos disponibles mediante la revisión de la literatura	**RQ1** ¿Cuál es la situación actual sobre la seguridad en sistemas de información? **RQ2** ¿Cuáles son las ventajas y desventajas de la utilización de métodos esteganográficos sobre algoritmos de encriptación?

sobre los niveles de seguridad de los métodos de seguridad disponibles.	**RQ3** ¿Qué métodos esteganográficos son los más utilizados en las propuestas de métodos esteganográficos de la comunidad científica?
Desarrollar un prototipo funcional mediante la implementación de un algoritmo esteganográfico seguro que evada los ataques comunes contra esteganogramas que usen la técnica LSB.	**RQ4** ¿Cuáles son las características que clasifican un algoritmo esteganográfico como seguro? **RQ5** ¿Es factible generar esteganogramas a partir de la representación en bytes de la información a ocultar y la generación de patrones en base a los mismos?
Validar el algoritmo propuesto mediante la utilización de los métodos de estegoanálisis estadísticos aplicados para vulnerar un esteganograma.	**RQ6** ¿Cuáles son los ataques esteganográficos más efectivos que se pueden utilizar para vulnerar un esteganograma? **RQ7** ¿El método propuesto resulta computacionalmente eficiente para ocultar información?

Hipótesis de trabajo

Para el presente trabajo se ha planteado la siguiente hipótesis que se ha de demostrar una vez se ha cumplido con los objetivos establecidos:

"El algoritmo propuesto mejora la seguridad ofrecida por los esteganogramas que resultan de la aplicación del método LSB."

Capítulo II: Marco Teórico

Ciberseguridad

Debido a que la información es uno de los activos más importantes de la sociedad contemporánea, la protección y defensa de la misma se ha vuelto un tema de crucial importancia que se toma en cuenta en las estrategias de seguridad nacional desarrolladas por los gobiernos y que se ha incorporado en el currículum de estudio de ciencias de la computación recomendado por la ACM (Ghernouti-Hélie, 2010; Suryotrisongko & Musashi, 2019). La ciberseguridad, también conocida como seguridad digital o seguridad de las tecnologías de información, es una ciencia joven cuyo principal enfoque es mantener la seguridad de la información digital en un mundo interconectado (Ghernouti-Hélie, 2010; Suryotrisongko & Musashi, 2019). Esta interconexión hace referencia a la interacción que se produce entre humanos, datos y la tecnología, en lo que se puede definir como: ciberespacio (Suryotrisongko & Musashi, 2019). El rápido crecimiento del ciberespacio ha traído gran crecimiento económico, el desarrollo de nuevas oportunidades y prosperidad, no obstante, este desarrollo también ha creado la oportunidad de que emerjan nuevos peligros y oportunidades criminales (Kriz, 2011).

En consecuencia al desarrollo acelerado del ciberespacio, la ciberseguridad se enfoca en mantener y proteger la información digital de los nuevos peligros que han nacido de este avance tecnológico, con la finalidad de no permitir que se amenace la existencia y desarrollo de una empresa, o bien de una nación (Ghernouti-Hélie, 2010). Para definir de forma más específica el propósito de la ciberseguridad, se han elaborado los siguientes objetivos (Ghernouti-Hélie, 2010):

- Reducir las vulnerabilidades y amenazas

- Limitar los daños o disfuncionalidad que se pueden presentar por una brecha de seguridad en un sistema de información
- Permitir que una organización vuelva a un estado previo a una afectación de seguridad, esto teniendo en cuenta un nivel aceptable de costos y retrasos en las operaciones.

Para que se pueda desarrollar correctamente las capacidades de la ciberseguridad en una organización es necesario que se entienda de forma clara los roles de los diferentes actores en el mundo de la ciberseguridad y las medidas más relevantes para incrementar los niveles de seguridad (Ghernouti-Hélie, 2010). De esta forma se facilita la identificación de estructuras organizacionales efectivas en cuanto a la seguridad informática y que a su vez permita determinar qué tipo de herramientas, conocimientos y procedimientos deben utilizarse para poder resolver los problemas relacionados con la ciberseguridad (Ghernouti-Hélie, 2010).

Actores en la ciberseguridad

Para que sea posible entender de forma más adecuada la importancia de desarrollar la ciberseguridad en cualquier institución, ya sea pública o privada, empresas o gobiernos, es necesario entender quiénes son los involucrados y qué rol cumplen dentro de este campo de estudio (Ghernouti-Hélie, 2010). Así, se tienen los siguientes roles claramente identificados (Ghernouti-Hélie, 2010):

- El protector: Empresas públicas / privadas o entidades gubernamentales encargadas de desarrollar sus capacidades de ciberseguridad
- El protegido: Puede ser una persona individual o en su efecto, empresas o inclusive gobiernos. Estas entidades son quienes están expuestas ante ataques de ciberdelincuentes y por lo tanto se les debe educar y proteger.

- El criminal: Pueden ser profesionales o bien novatos sin recursos, cualquiera que sea el caso, están en capacidad de hacer daños por diferentes motivos y son de quienes se debe proteger a diversas entidades en el ciberespacio.

Principios de la ciberseguridad

Para que el desarrollo de la ciberseguridad sea efectivo y tanto empresas como gobiernos se puedan beneficiar al máximo de la misma, y por lo tanto, cumplir con los objetivos que se proponen, es necesario que se sigan seis principios que ayudarán a adoptar las medidas de ciberseguridad (Kriz, 2011).

Los seis principios se describen a continuación:

1. *Los esfuerzos para mejorar los niveles de ciberseguridad deben apalancar la alianza público-privado y construirla a partir de iniciativas existentes y el compromiso de los recursos:* La cooperación entre entidades públicas y privadas ha mejorado los niveles de ciberseguridad de tal forma que que la implementación de medidas de ciberseguridad sean efectivas y adaptativas (Kriz, 2011).
2. *Los esfuerzos para mejorar la ciberseguridad deben reflejar la naturaleza global, interconectada y sin bordes de la infraestructura del ciberespacio:* Debido a que el ciberespacio es un dominio global que abarca varias ubicaciones geográficas y jurisdicciones nacionales es necesario que el desarrollo de la ciberseguridad se base en estándares aceptados globalmente, lineamientos de buenas prácticas y programas de seguros internacionales. Esto permitirá una mejora en los niveles de ciberseguridad, independientemente de la ubicación geográfica de dónde se las implemente (Kriz, 2011).

3. *Los esfuerzos para mejorar la ciberseguridad deben ser capaces de adaptarse rápidamente a amenazas emergentes, tecnologías y modelos de negocio:* El área de las tecnologías de información es sumamente dinámica y las relaciones entre los interesados evoluciona de forma constante. Los dispositivos que permiten conectarse al internet son modificados y mejorados continuamente. Los negocios se adaptan e incorporan nuevos modelos de negocio. Es un ambiente que motiva la dinámica y por lo tanto, los cibercriminales también hacen uso de métodos de vanguardia para perpetrar actos ilícitos (Kriz, 2011).
4. *Los esfuerzos por mejorar el ciberespacio deben estar basados en la gestión de riesgos:* La seguridad, ya sea dentro o fuera del ciberespacio, no es una meta que se pueda cumplir y estar 100% libres de riesgos. Siempre existirá la posibilidad de desastres naturales, crímenes, espionaje, guerras y diversos escenarios que representan una amenaza. Sin embargo, en todos estos escenarios se hace uso de la gestión de riesgos para poder identificar el riesgo, enfrentarlo y establecer pasos que permitan reducirlo a niveles tolerables (Kriz, 2011).
5. *Los esfuerzos por mejorar la ciberseguridad deben enfocarse en la concientización:* Todos los interesados y usuarios del ciberespacio deben tener conocimiento sobre los riesgos que involucra hacer uso del ciberespacio. Sin embargo, varios interesados no están conscientes de los riesgos y las herramientas que les permiten manejar los riesgos. Incrementar la conciencia sobre todos los aspectos negativos del ciberespacio es crítico para incrementar los niveles de ciberseguridad (Kriz, 2011).

6. *Los esfuerzos por mejorar la ciberseguridad deben enfocarse directamente en los malos actores y sus amenazas:* La ciberseguridad se trata de entender y mitigar las amenazas que se presentan en el ciberespacio, además de las vulnerabilidades y consecuencias. No obstante, debido a la dificultad que representa gestionar las amenazas a menudo se las ignora por completo. Las amenazas se pueden clasificar en cuatro grupos: Crímenes, espionaje industrial, espionaje de estado y guerra (Kriz, 2011).

Seguridad de la información

Debido a que en la actualidad las organizaciones dependen cada vez más de sistemas de información para poder ejecutar sus procesos de negocio de una forma rápida diferente a la manera tradicional, para que dichos sistemas se mantengan eficientes es necesario que se los proteja en contra de las amenazas del ciberespacio y que la seguridad de la información se mantenga (Alkhudhayr et al., 2019). Para lograr esto, los sistemas de información deben estar protegidos contra ataques activos y pasivos como por ejemplo: acceso ilegal a los datos, modificaciones no autorizadas de datos e interrupciones en el servicio (Alkhudhayr et al., 2019).

La seguridad de la información, por definición, tiene como objetivos mantener la confidencialidad, integridad y disponibilidad de los datos por cualquier medio, aunque por definición de la ISO, la seguridad de la información también abarca temas como el no repudio, identificación, autenticación y autorización (Alkhudhayr et al., 2019; Amankwa et al., 2014). Esta área de conocimiento no solo abarca los problemas técnicos relacionados con la seguridad sino que también incluye amenazas relacionadas con la interacción entre humanos y sistemas, no obstante, los profesionales e investigadores de esta temática se han enfocado ampliamente en cubrir aspectos técnicos como por ejemplo encriptación y firewalls, sin tomar en cuenta los

peligros ocasionados por los usuarios finales de los sistemas, debido a la carencia de conciencia sobre la seguridad de la información (Amankwa et al., 2014).

Confidencialidad de la información

La confidencialidad de la información se refiere a la protección de la misma, específicamente contra el acceso no autorizado, divulgación o robo (University of Delaware, 2020). En otras palabras la confidencialidad de la información se puede denotar como mantener la privacidad de la misma. Cuando se habla sobre confidencialidad existen dos categorías en las que se puede clasificar la información:

Pública: aquella información carente de medidas de confidencialidad se considera como pública o que no conlleva un riesgo que se conozca fuera del público objetivo (University of Delaware, 2020).

Secreta: la información que a la que se le ha aplicado medidas de confidencialidad es considerada como secreta y por lo tanto debe ser protegida para evitar efectos negativos sobre el propietario o agentes relacionados a esta información (University of Delaware, 2020).

Cuando se desee tratar la confidencialidad de la información es recomendable tener en cuenta el público al que se le puede divulgar la información, además de requisitos legales como leyes, regulaciones o contratos (University of Delaware, 2020). También es necesario considerar bajo qué circunstancias es seguro revelar información y si la divulgación de la misma no representa ningún riesgo (University of Delaware, 2020).

Métodos para mantener la confidencialidad de la información

La Universidad de Delaware (2020) recomienda las siguientes medidas para mantener la confidencialidad de la información física o digital:

Encriptación de archivos sensibles: mediante la encriptación de la información se puede proteger la información para que no sea leída o usada por aquellos que no están permitidos a hacerlo.

Gestionar el acceso a la información: La confidencialidad de la información está definida en gran medida por quienes tienen acceso a la misma. Es por esto que limitar el acceso de la información a aquellos que la necesitan. Es indispensable que estas personas también se autentiquen mediante contraseñas u otros factores de autenticación.

Asegurar de forma física documentos y dispositivos: el control del acceso a la información no solo se limita al control digital, también es indispensable controlar quién tiene acceso a dispositivos o copias físicas de la información.

Deshacerse de forma segura de los datos, dispositivos y copias físicas: Cuando la información ya no sirve ningún propósito para la organización esta debe ser eliminada de forma segura, teniendo cuidado que no sea posible recuperarla mediante ningún mecanismo.

Gestionar la recolección de datos: Es importante tener en cuenta que al momento de recolectar datos se deben guardar aquellos que sean estrictamente necesarios, esto es importante ya que en la medida de lo posible es necesario evitar la recolección de datos confidenciales que necesiten protección.

Gestionar la utilización de datos: Los riesgos relacionados con la confidencialidad se pueden reducir si aquellos datos o información confidencial es usada únicamente en escenarios específicos y únicamente cuando su uso ha sido aprobado por la autoridad a cargo.

Gestionar los dispositivos: La gestión de sistemas informáticos es un tema amplio y sumamente importante para la seguridad de la información. Mediante la protección de los dispositivos de cómputo el riesgo de que se divulgue información confidencial se puede reducir drásticamente.

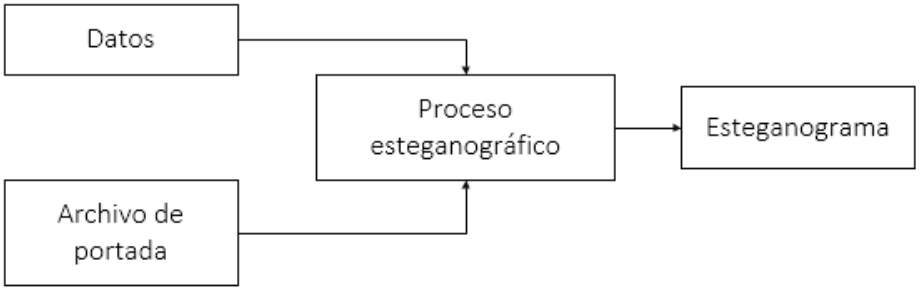
Esteganografía

La esteganografía puede ser definida como el arte de ocultar información considerada confidencial, y por lo tanto secreta, en un medio que parecería irrelevante a simple vista y es tan antigua como la escritura misma (Kuksov, 2019). A diferencia de otros métodos para mantener la confidencialidad de la información, como la criptografía, el objetivo de la esteganografía es lograr que la información pase desapercibida ya que la criptografía transforma los datos de tal forma que resultan en una forma ilegible, no obstante sospechosa, que delata la importancia de la información (Kuksov, 2019). Gracias al avance computacional, la esteganografía contemporánea tiene la ventaja de que casi cualquier elemento digital puede contener información oculta ya que para el computador, es una únicamente una colección de bits (Kuksov, 2019).

El proceso para generar un esteganograma se resume en utilizar un medio en el que se va a ocultar la información (portada), un mensaje y un algoritmo esteganográfico. El algoritmo ocultará en los datos de la imagen de portada la información que se desee, dando como resultado un esteganograma. En la Figura 2 se muestra un resumen del flujo que se efectúa para poder ocultar información en un medio digital.

Figura 2

Flujo esteganográfico básico



Formas de esteganografía digital

La esteganografía digital permite que se pueda esconder información en cualquier archivo almacenado en un computador, debido a que para una máquina no cambia el hecho de que se oculte información ya que a la final siguen siendo una secuencia de bits (Kuksov, 2019). De forma sencilla, la esteganografía se puede clasificar en tres grandes grupos:

Esteganografía basada en texto. Se oculta información en texto plano, no es usada debido a que las porciones de texto no tienen datos redundantes, reduciendo la efectividad de ocultar información por este medio (Thangadurai & Sudha Devi, 2014).

Esteganografía basada en imágenes. Es la más utilizada del grupo, se hace uso de imágenes que actúan como un baúl donde se almacena información confidencial por su gran volumen de datos redundantes que se pueden modificar (Thangadurai & Sudha Devi, 2014).

Esteganografía basada en audio/video. A diferencia de los otros dos tipos de esteganografía, esta es sumamente compleja debido a la estructura de un archivo de audio/video y por lo tanto no es tan común (Thangadurai & Sudha Devi, 2014).

Métodos para esteganografía en imágenes

Debido a que la esteganografía en imágenes es más común, sencilla y efectiva existen dos métodos generales para ocultar información en estos medios digitales:

Bit menos significativo (LSB). El método del bit menos significativo usa N bits de un canal RGB de un pixel, es decir hace uso de los bits de un color tomados desde la derecha hacia la izquierda para poder almacenar los bits de la información que se desea ocultar (Thangadurai & Sudha Devi, 2014).

Bit más significativo (MSB). El método del bit más significativo usa N bits de un canal RGB de un pixel, es decir hace uso de los bits de un color tomados desde la izquierda hacia la

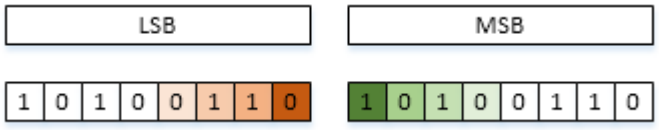
derecha para poder almacenar los bits de la información que se desea ocultar (Thangadurai & Sudha Devi, 2014).

El número de N bits que se reemplace en un pixel determinará la cantidad de información que se puede almacenar. Así, si se decide hacer uso de 4 bits más o menos significativos se tendrá más capacidad que si se decide utilizar únicamente un bit. Aunque es necesario recalcar que entre más bits se usen de un pixel más modificaciones tendrá la imagen y por lo tanto será más vulnerable contra el estegoanálisis (Thangadurai & Sudha Devi, 2014).

En la Figura 3 se muestra de forma gráfica el uso de los N bits menos significativos del canal rojo (Izq.) y los bits más significativos del canal Verde (Der.) que se usarían para ocultar información en un color de un píxel de una imagen.

Figura 3

Representación del LSB y MSB



Estegoanálisis

La esteganografía es una opción para poder mantener información oculta sin la necesidad de levantar sospechas, como pasa al hacer uso de la criptografía (Jie et al., 2010). El área de estudio dedicada al análisis de medios digitales para detectar información es conocida como el estegoanálisis, y como pasa con la criptografía y el criptoanálisis, la esteganografía y el estegoanálisis son dos caras de una misma moneda (Karampidis et al., 2018). Mientras que la esteganografía es el arte de lograr que un mensaje pase desapercibido y que su existencia no sea revelada a terceros, el estegoanálisis se encarga de analizar diversos medios para tratar de identificar esteganogramas (Karampidis et al., 2018; Knight, 2000).

El estegoanálisis, por su naturaleza se puede clasificar en dos categorías: el estegoanálisis pasivo y estegoanálisis activo (Karampidis et al., 2018). En el primer caso, el estegoanalista tratará de clasificar los medios de transporte en esteganogramas y los medios originales o inalterados (Karampidis et al., 2018). En el caso del estegoanálisis activo, el estegoanalista optará por métodos más sencillos, es decir, en vez de tratar de descubrir un esteganograma o el mensaje inscrito, el estegoanalista simplemente destruirá el mensaje al modificar una imagen (Knight, 2000). La destrucción de un esteganograma puede darse mediante técnicas sencillas como por ejemplo (Knight, 2000):

- Aplicación de difuminación: reduce el contraste entre pixeles y hace las transiciones entre colores más sutiles.
- Ruido: Se agregan pixeles al azar en la imagen. También pueden incluirse pixeles de colores similares al esteganograma original.

Métodos de estegoanálisis

En el mundo del estegoanálisis existen seis métodos principales que le permitirán al estegoanalista poder revelar información oculta o clasificar esteganogramas. La factibilidad de cada uno de estos métodos dependerá en gran medida de la cantidad de información que el estegoanalista posea para su análisis.

- **Solo estego**: En estos casos el único recurso disponible para el estegoanalista es lo que se sospecharía que es un esteganograma (Karampidis et al., 2018; Knight, 2000).
- **Portada conocida**: En este caso el medio original y el esteganograma están disponibles para analizar (Karampidis et al., 2018; Knight, 2000).

- **Mensaje conocido**: En estos casos el estegoanalista tiene en su control un mensaje que está oculto y lo podrá comprar con un esteganograma (Karampidis et al., 2018; Knight, 2000).
- **Ataque de selección de método esteganográfico**: en estos casos el estegoanalista posee el esteganograma y la herramienta de software utilizada para generarlo (Karampidis et al., 2018; Knight, 2000).
- **Ataque de selección de mensaje**: En estos casos el estegoanalista genera un esteganograma a partir de un mensaje arbitrario haciendo uso de una herramienta o un algoritmo. El objetivo es establecer los patrones de los esteganogramas que puedan ayudar a identificar el uso de una herramienta o algoritmo (Karampidis et al., 2018; Knight, 2000).
- **Ataque de estego conocido**: En estos casos el estegoanalista posee el medio original, el esteganograma y la herramienta o algoritmo usado para generar el esteganograma (Karampidis et al., 2018; Knight, 2000).

Técnicas de estegoanálisis

Como se ha revisado anteriormente, existen seis métodos o ataques que el estegoanalista puede utilizar para analizar un estego medio y cada uno de estos métodos varía dependiendo de la cantidad de información disponible. Sin embargo, también existen seis técnicas que podrá usar el analista dependiendo del método que ejecute (Karampidis et al., 2018). A continuación se realiza un resumen de estas seis técnicas (Karampidis et al., 2018):

- Estegoanálisis visual: Es la forma más sencilla de analizar un esteganograma. No obstante, la naturaleza de la esteganografía digital hace que este método sea muy ineficiente para el ojo humano. La transformación de una imagen a un

formato binario en el que solo se consideren los bits menos significativos puede ayudar a identificar la existencia en la manipulación de una imagen mediante un análisis visual.

- Estegoanálisis de firma: Esta técnica consiste en observar cualquier patrón repetitivo de un software de esteganografía. Estos patrones se los conoce como firma y pueden ayudar a determinar la presencia de mensajes ocultos en un medio. Por ejemplo, el software “Hiderman” agrega los caracteres “CDN” al final de un archivo cuando se ha ocultado información.
- Estegoanálisis estadístico: Son aquellas técnicas que se han desarrollado mediante el análisis del proceso de empotrado de mensajes en medios digitales y la determinación de datos estadísticos que se modifican tras empotrar información.
- Análisis de aspersión de espectro: Existe un método esteganográfico que oculta la información en ruido y el mismo es agregado a una imagen. En estos casos el ruido agregado se mantiene a bajos niveles de manera que es imperceptible al ojo humano. Para realizar estegoanálisis en estos casos se hace uso de una función de histograma de características – el cual es la transformada de Fourier del histograma de una imagen – este método mostró una efectividad del 94% en la identificación de esteganogramas.
- Estegoanálisis de transformación de dominios: Existen métodos esteganográficos más complejos que involucran ocultar información en los coeficientes de transformación de las imágenes de portada. Para esto se usan técnicas de transformación de dominios como por ejemplo: Transformación discreta de coseno, transformación discreta de onda y transformación rápida de

Fourier. En estos casos el análisis se efectúa mediante el entrenamiento de redes neuronales para la identificación de esteganogramas por sus características estadísticas, las cuales se obtienen tras aplicar las transformaciones de dominio mencionadas a un grupo de imágenes.

- Análisis universal (ciego): Debido a la cantidad de algoritmos existentes para ocultar información en medios digitales, varios investigadores han tratado de crear una forma de detección de esteganogramas independiente de la técnica esteganográfica empleada. Estos análisis son más complejos ya que se necesitan de técnicas de aprendizaje de máquinas e inteligencia artificial, además de un gran número de ejemplos para poder obtener un modelo que pueda identificar esteganogramas. La principal dificultad de obtener un modelo efectivo en la detección de esteganogramas es poder obtener las características relevantes del mismo.

Determinación de la calidad de un esteganograma

Para poder determinar la calidad de un esteganograma se lo puede comparar con la imagen original que se usó para ocultar información (Çataltaş & Tütüncü, 2017). En este caso, entre menor sea la diferencia se considera que un esteganograma es de mayor calidad. Para poder determinar la calidad de los esteganogramas se pueden usar diversas técnicas estadísticas para determinar un factor de similitud. La técnica más conocida y utilizada es el Error Promedio Cuadrático (MSE por sus siglas en inglés), el cual representa la diferencia promedio entre la imagen original y el esteganograma, un valor cercano a cero es indicador que las imágenes son muy similares (Çataltaş & Tütüncü, 2017). Otra técnica es la relación señal pico a ruido (PSNR por sus siglas en inglés), este es un término de ingeniería utilizado para identificar la proporción

entre el valor máximo de la exponenciación de una imagen elevado al promedio de sus diferencias, un valor alto usado con esta técnica indica una mayor similitud entre dos imágenes (Çataltaş & Tütüncü, 2017).

Estado del arte

Planteamiento de la revisión de literatura

El estado del arte se ha realizado bajo la metodología propuesta por Kitchenham (2004). En esta fase se realizó una breve descripción del problema de investigación para proporcionar un contexto para la búsqueda de estudios científicos; posteriormente se procedió a definir un objetivo de búsqueda y plantear preguntas de investigación para alinear la búsqueda en relación al problema de investigación y finalmente se definieron los criterios de inclusión y exclusión.

Conformación del grupo de control (GC) y extracción de palabras relevantes para la investigación.

El grupo de control permite a los investigadores eliminar y aislar las variables (Shuttleworth, 2010), en este caso se propusieron papers que se encuentren estrechamente relacionados con la problemática y la solución, de esta forma se llegó a conformar un grupo de control de cinco artículos, de igual manera de cada artículo se seleccionaron palabras clave para conformar la cadena de búsqueda. Esta información se muestra en la Tabla 2.

Tabla 2

Grupo de control

Título	Cita	Palabras Clave
Survey on LSB Data hiding techniques	(Jois & Tejaswini, 2016)	LSB Substitution, Steganography, data hiding, process, technique
An analysis of LSB based image steganography techniques	(Thangadurai & Sudha Devi, 2014)	Image steganography, LSB, analyze, technique, information security
A novel image steganography algorithm against statistical analysis	(Zhang & Tang, 2007)	LSB, statistical analysis, against, method, image steganography, technique, steganalysis, novel, algorithm
Analysis of Data Hiding with Multi-bit Image Steganography	(Qu et al., 2018)	LSB, data hiding, steganography, image-based steganography, evaluation
High secure digital image steganography based on 3D chaotic map	(Valandar et al., 2015)	Information security, enhance, security, method, steganalytic, lsb, image steganography

Una vez se encontró el grupo de control que brindará apoyo para la recopilación y determinación del estado del arte se procedió a establecer criterios de inclusión y exclusión que permitieron seleccionar los mejores candidatos a estudios primarios, los mismos pueden verse en la Tabla 3.

Tabla 3

Criterios de inclusión y exclusión establecidos para la revisión de literatura

Criterios de inclusión	**Criterios de exclusión**
Papers publicados después del 2019	Papers publicados antes del 2010
Publicados en conferencias	Papers que presenten métodos esteganográficos para medios digitales diferentes de imágenes
Papers que describan un nuevo método o algoritmo para ocultar información en una imagen digital, especialmente aquellos que se encuentren influenciados o estrechamente relacionados con la técnica LSB de esteganografía.	Papers que propongan algoritmos esteganográficos que dependan de algoritmos criptográficos previos a ocultar información
Papers que estudien y analicen la seguridad presentada por un algoritmo o método esteganográfico	Papers que detallen la aplicación de la esteganografía y no propongan nuevos métodos

Construcción y afinación de la cadena de búsqueda

Con las palabras clave que fueron obtenidas de los artículos científicos del grupo de control se conformó la cadena de búsqueda. En la siguiente tabla se puede observar las diferentes versiones de la cadena de búsqueda que se utilizó para realizar el estudio preliminar de literatura.

Las versiones 1 y 2 presentaban una gran cantidad de estudios, por lo que se consideran poco manejables y se procede a realizar los cambios correspondientes.

En las versiones 3, 4 y 5 se obtienen pocos resultados lo que no brinda suficiente espacio para analizar una cantidad importante de estudios, además los resultados no son relevantes para la investigación.

Por último la versión 6, a pesar de tener 111 estudios, cuenta con una gran cantidad de investigaciones relevantes y se tiene espacio para seleccionar los más adecuados. En la Tabla 4 se muestran las diferentes versiones de la cadena de búsqueda que se ha utilizado.

Tabla 4

Versiones de la cadena de búsqueda

Versión	**Cadena de búsqueda**	**Número de resultados**
1	(("analysis") AND (“steganography” OR “image steganography” OR “image-based steganography”) AND (“LSB” OR “LSB substitution”) AND (“method” OR “technique”))	377
2	(("steganalysis") AND (“image steganography” OR “image-based steganography”) AND (“LSB”) AND(“method” OR “technique”))	192
3	(“analysis” OR “steganalytic” OR “staganalysis”) AND (“steganography” OR “image steganography” OR “data hiding” OR	57

	“image-based steganography”) AND (“LSB” OR “LSB substitution”) AND (“method” OR “technique” OR “process”) AND (“enhance”) AND (“information security” OR “security”)	
4	(“steganography” OR “image steganography” OR “data hiding” OR “image-based steganography”) AND ("security issues" OR "information security" OR "vulnerabilities" OR "vulnerable") AND (“method” OR “technique” OR “process”) AND (“enhance”) AND (“LSB” OR “LSB substitution”)	27
5	((“image steganography” OR "data hiding" OR “image-based steganography”) AND (“LSB”) AND ("security issues" OR "information security") AND (“method” OR “technique” OR “algorithm”) AND ("enhanced security" OR "security" OR "against") AND ("analysis" OR "steganalysis"))	67
6	(“image steganography” OR "data hiding" OR “image-based steganography”) AND (“LSB”) AND ("security issues" OR "information security") AND (“method” OR “technique” OR “algorithm”) AND ("enhanced security" OR "security")	111

Para un mayor entendimiento de la cadena de búsqueda, las diferentes palabras claves se han organizado por contexto, esta organización se la muestra en la Tabla 5.

Tabla 5

Organización de palabras por contexto

Contexto	Palabras
Área de estudio	• Image steganography
	• Data hiding
	• Image-based steganography
Método de estudio	• LSB
Problema	• Security issues
	• Information security
Solución propuesta	• Method
	• Technique
	• Algorithm
Objeto de la solución propuesta	• Enhanced security
	• Security

Selección de estudios

Al aplicar la cadena de búsqueda en la base digital IEEE Xplore se obtuvo alrededor de ***111 artículos candidatos*** que están estrechamente relacionados con el tema; adicionalmente con esta cadena la mayor parte de los artículos del grupo de control apareció dentro de los artículos encontrados.

Al realizar un análisis rápido del título y resumen de los papers resultantes de la cadena de búsqueda, se han seleccionado 18 estudios que se presentan como buenos candidatos tras aplicar los filtros de inclusión y exclusión. Se dio lectura a los papers, reduciendo la selección a 8 papers candidatos, los cuales se listan en la Tabla 6.

Tabla 6

Estudios seleccionados

CÓDIGO	TÍTULO	CITA
EP1	An improved LSB embedding technique for image steganography	(Sugathan, 2017)
EP2	Improved detection of least Significant bit steganography algorithms in color and gray scale images	(Devi & Sharma, 2014)
EP3	An Image Steganography Algorithm using LSB Replacement through XOR Substitution	(Bhuiyan et al., 2019)
EP4	A novel steganography method based on matrix pattern and LSB algorithms in RGB images	(Nilizadeh & Nilchi, 2016)
EP5	A new method for image information hiding based on image scrambling and LSB technology	(Jie et al., 2010)
EP6	High secure digital image steganography based on 3D chaotic map	(Valandar et al., 2015)
EP7	A threshold-LSB based information hiding scheme using digital images	(Nayak & Bhagvati, 2013)

EP8	Who decides hiding capacity? I, the pixel intensity	(Amirtharajan et al., 2012)

Estado del arte

EP1 (Sugathan, 2017): An improved LSB embedding technique for image steganography

En el artículo “An improved LSB embedding technique for image steganography” el autor propone un algoritmo en base al método esteganográfico LSB el cual se centra en el direccionamiento de los bits para ocultar la información. Este método analiza los pixeles de la imagen en busca de tres pixeles consecutivos que permitan almacenar 1 byte de información, una vez encontrados, se analiza el 9no bit que determinará el orden en el que se almacena la información, reduciendo de esta forma la cantidad de alteraciones que se deben realizar sobre la imagen original.

EP2 (Devi & Sharma, 2014):Improved detection of least Significant bit steganography algorithms in color and gray scale images

En el artículo “Improved detection of least significant bit steganography algorithms in color and gray scale images”, los autores proponen un método que no modifica los principios del LSB, más bien calcula la diferencia existente entre el color original representado por un pixel y el color original de la imagen, de esta forma altera el resto de datos de cada pixel para reducir la distancia entre colores manteniendo así la calidad original de la imagen, volviendo más dificil la detección visual de la alteración de datos.

EP3 (Bhuiyan et al., 2019): An Image Steganography Algorithm using LSB Replacement through XOR Substitution

En el artículo "An Image Steganography Algorithm using LSB Replacement through XOR Substitution" los autores proponen un algoritmo que hace uso del método esteganográfico LSB, no obstante se diferencia en la aplicación de la operación lógica entre cada uno de los bits del mensaje a ocultar y el 7mo bit (de izquierda a derecha) de cada canal RGB, el resultado de esta operación se almacena en el 8vo bit. De esta forma no se cambian directamente los bits menos significativos, sino que para extraer la información es necesario realizar nuevamente la operación entre el séptimo y octavo bit.

EP4 (Nilizadeh & Nilchi, 2016): A novel steganography method based on matrix pattern and LSB algorithms in RGB images

En el artículo "A novel steganography method based on matrix pattern and LSB algorithms in RGB images" En este estudio se propone un nuevo algoritmo esteganográfico que combina los ya conocidos métodos de Patrón de Matriz (MP) y el Bit Menos Significativo (LSB). Estos dos métodos hacen uso del dominio espacial para ocultar información y sin embargo presentan formas diferentes de ocultar información. El método propuesto en este estudio hace uso del espectro azul de una imagen para ocultar el respectivo mensaje, ocultando con LSB 3 bits de información y otros cuatro bits haciendo uso del método MP. Este algoritmo recibe dos entradas siendo una únicamente texto que se oculta con el método MP y la otra entrada cualquier medio digital que se oculta con LSB. Se demuestra que este método mejora la capacidad de cargar información en una misma imagen de portada.

EP5 (Jie et al., 2010): A new method for image information hiding based on image scrambling and LSB technology

En el artículo “A new method for image information hiding based on image scrambling and LSB technology” los autores proponen un algoritmo que permite revolver los pixels de una imagen mediante una matriz la cual será oculta posteriormente mediante el método LSB en otra imagen. De esta forma se consigue una doble ocultación de información que previene que un atacante pueda descubrir los datos originales ocultos en la imagen cuyos pixeles han sido cambiados de orden.

EP6 (Valandar et al., 2015): High secure digital image steganography based on 3D chaotic map

En el artículo “High secure digital image steganography based on 3D chaotic map” los autores optan completamente por no usar el método LSB, proponiendo una alternativa creativa mediante el uso de mapas caóticos. Este método genera tres variables (x, y, z) lo que indicará qué pixel y en qué canal de color RGB se almacenará información. Este método evita ser detectado por los mecanismos de estegoanálisis conocidos en la actualidad, aunque representa una alternativa más compleja al clásico LSB.

EP7 (Nayak & Bhagvati, 2013): A threshold-LSB based information hiding scheme using digital images

En el artículo “A threshold-LSB based information hiding scheme using digital images” los autores proponen un método basado en claves que el usuario provee para generar números aleatorios los cuales representarán la posición donde se ocultará la información en la imagen de portada. Además, el usuario debe proveer dos valores que parametrizan la cantidad de información que se transportará por cada pixel, así al momento de ocultar información se

utilizará el método LSB para ocultar 3 o 2 bits de información dependiendo de la parametrización del usuario.

EP8 (Amirtharajan et al., 2012): Who decides hiding capacity? I, the pixel intensity

En el artículo "Who decides hiding capacity? I, the pixel intensity" los autores proponen un método en el cual los canales RGB actúan bien como un "indicador" o como almacenamiento de datos. En este método el menor valor de las tres capas actúa como indicador dejando las otras dos libres para ocultar información. En cuanto a los canales de designados para ocultar información, se calcula la cantidad de bits a almacenar mediante la intensidad del color. Si la intensidad es menor a 128 se considera 0. De esta forma si se tiene, por ejemplo, 00 se ocultará 1 bit, 01 ocultará 2 bits, 10 ocultará 3 bits y 11 ocultará 4 bits de información. Este método hace uso de la contraparte del LSB, el método del bit más significativo (MSB).

Caracterización del estado del arte

Tras analizar el estado del arte se ha notado que existen varios estudios destinados a encontrar una solución que incremente los niveles de seguridad de la esteganografía mediante la técnica LSB. La mayoría de estos estudios proponen incrementar las "capas" de seguridad al incluir más pasos para esconder datos en una imagen, como por ejemplo: la encriptación de la información previo al ocultamiento, uso de técnicas para barajar la información o incluso realizar el proceso varias veces, es decir, ocultar imágenes en otras imágenes. También existen estudios que toman ventaja del espacio de color RGB para usar sus características como medio de organizar y ocultar la información. En general, las alternativas para la solución a los problemas de seguridad son variados y proponen diversas técnicas que ayudan a que la información se mantenga confidencial, presentando así diversos métodos para evitar los ataques contra medios esteganográficos.

La propuesta plantea el desarrollo de un método esteganográfico que use los datos como base para poder crear esteganogramas. Al utilizar los datos mismos para crear un esteganograma, junto con patrones para distribuirlos a través de los distintos pixeles canales de color (Rojo, Verde y Azul), se crea una representación visual de los datos. Este esteganograma resultante puede reemplazar los pixeles de una imagen, realizando mínimas modificaciones a la misma y evitando así anomalías estadísticas notables en una imagen, o funcionar independientemente como un esteganograma que no requiere de una imagen portadora.

Definición de la investigación

Investigación aplicada tecnológica

La investigación es aplicada al área tecnológica ya que el planteamiento de un algoritmo esteganográfico encuentra una aplicación práctica en el área de la seguridad de la información tanto para sectores corporativos como para individuos.

Metodología propuesta

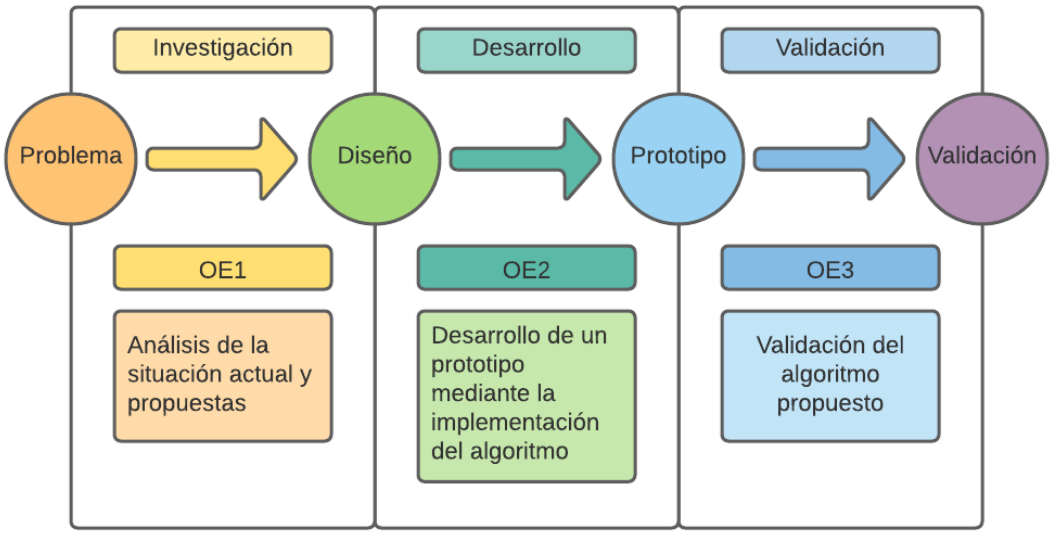
Para el desarrollo de esta investigación se ha planteado una metodología propia que consta de tres fases, en la Figura 4 se muestra una representación gráfica de la metodología.

Fase I - Investigación: Esta fase inicia con la identificación de la problemática que se va a tratar en torno a los problemas de seguridad relacionados a los métodos esteganográficos, para esto se analizará la situación actual y las propuestas de la comunidad científica mediante la revisión de la literatura sobre los niveles de seguridad de los métodos de esteganográficos disponibles. Una vez definida la problemática es preciso realizar el estudio del estado del arte para determinar las vulnerabilidades de estos métodos y poder establecer los puntos que se

mejorarán a través de la propuesta del estudio. Para el estudio del estado del arte se realizará una revisión preliminar de literatura.

Figura 4

Metodología propia utilizada en la investigación



Fase II - Desarrollo: Una vez que se ha determinado la solución en esta fase se diseñará un algoritmo enfocado a dar cumplimiento al objetivo general del proyecto, en base a lo que se ha encontrado en el estado del arte. Como siguiente paso se desarrollará un prototipo funcional que implemente el algoritmo elaborado.

Fase III - Validación: Finalmente, se realizarán pruebas sobre el prototipo desarrollado para evaluar el rendimiento y robustez del algoritmo en comparación del algoritmo base de LSB. Estas pruebas estarán enfocadas al cumplimiento del objetivo específico relacionado con la fase. Una vez que se ha determinado el rendimiento y robustez del algoritmo planteado, se procederá a reportar los hallazgos que se han obtenido.

Metodología de desarrollo

Las metodologías de desarrollo de software permiten a un equipo de trabajo producir productos de calidad mediante la gestión del proceso que implica la ejecución de un proyecto de desarrollo (Young, 2013). En el caso de las metodologías ágiles se prioriza la calidad del producto y del proceso ejecutado (Wynn, 2016). Cada organización decide qué metodología de desarrollo le resulta más conveniente ejecutar en vista de que ninguna de ellas brinda una completa protección ante fallos y problemas que puedan dificultar la realización de un proyecto, es así que algunas organizaciones consideran que trabajan mejor con metodologías más sistemáticas que siguen un ciclo de vida en cascada y otras optan por metodologías iterativas (Young, 2013).

Las metodologías ágiles se caracterizan por ser flexibles y disminuir los costos de desarrollo sin dejar de lado la calidad del producto entregado. La familia de metodologías ágiles se compone de marcos de trabajo como (Young, 2013):

- SCRUM: Enfocada en agregar características a un programa en intervalos cortos de tiempo (7 a 30 días), la concentración del equipo se mantiene con reuniones cortas. Cada equipo es auto suficiente, no obstante, existe un maestro de Scrum que se encarga de controlar la correcta ejecución de la metodología.
- XP: Enfocada en un desarrollo basado en pruebas, esta metodología prioriza el desarrollo por parejas brindando una constante revisión de código y mayor robustez al producto final, elevando los costos de desarrollo.
- Dynamic Systems Development Model: Es una metodología que especifica al Inicio del proyecto el costo, tiempo y calidad a lograr. Esta metodología prioriza las características del producto en: “Tiene qué”, “Debería tener”, “Podría tener”

y “No tiene”. Se espera que el cliente esté involucrado en la priorización de las características.

Estas metodologías, debido a su filosofía, están destinadas a equipos de trabajo que buscan mejorar la calidad de sus productos. No obstante, existen metodologías enfocadas a desarrolladores independientes, como la propuesta por Moyo & Mnkandla (2020), la cual adapta el proceso de gestión de un proyecto de software de tal forma que pueda ser ejecutado sin problemas o sobrecargas de trabajo por un único desarrollador incorporando, además, prácticas y guías para obtener un producto que cumpla con estándares de seguridad.

Herramientas

Para el desarrollo del presente trabajo se ha hecho uso principalmente de herramientas de software que permitiesen llevar a cabo la construcción de un prototipo funcional, además de otras que facilitaran el proceso de evaluación del algoritmo propuesto. Las herramientas que se utilizaron son gratuitas y open source.

Kotlin – Ktor

Ktor es un framework asíncrono para la creación de micro servicios, aplicaciones web, entre otros. Es sencillo de aprender, gratis y open source (JetBrains, 2020).

JavaScript – React

React es una librería de JavaScript creada para construir interfaces gráficas y que puede ser incorporada de forma gradual a una página web (FacebookInc, 2019).

Octave

Octave es descrito como un lenguaje de programación de alto nivel creado para computaciones numéricas (Eaton, 1998).

Open Stego

OpenStego es una solución esteganográfica que permite ocultar y retirar información de medios digitales (Vaidya, 2017).

Capítulo III: Desarrollo

Situación actual

El actual trabajo toma como inspiración una idea propuesta por el autor durante sus años de estudio en la universidad, la cual consiste en la generación de imágenes a partir de datos. Con la representación en bytes de la información que se quiere ocultar representando un valor para un canal y un pixel determinado. No obstante, este método tiene limitaciones, por ejemplo: debido a que una imagen generada por el algoritmo debe indicar la cantidad de datos que contiene, la información relevante se limita a 255 bytes por imagen ya que es el valor máximo que se puede asignar a un canal y la forma en la que se generan estas imágenes es estática y es siempre igual sin importar el mensaje (Martínez et al., 2021).

Por este motivo se ha planteado mejorar esta alternativa mediante la implementación de la generación pseudo aleatoria de patrones a partir de un dato específico y en vez de generar una imagen desde cero, utilizar un portador como se lo realiza normalmente con la esteganografía debido a que generar una imagen con valor simbólico es una tarea complicada y un atacante podría identificar claramente las imágenes generadas por el algoritmo original.

Diseño

Para el diseño del algoritmo, partiendo de la idea planteada por el autor, se consideró como punto de partida que la unidad básica para ocultar información en una imagen sería el byte. Además, se tomó en consideración de que para evitar ataques como chi cuadrado, la información debería ser oculta de forma aleatoria, sin embargo, seleccionar pixels aleatorios es algo que el algoritmo LSB ya realiza y representa un problema debido a que además de la información que se desea ocultar, se debe incorporar de alguna manera la cantidad de datos

que se deben retirar de la imagen; en ocasiones esto se realiza al guardar el número de bytes en la cabecera de la imagen, incorporando metadatos que no son los propios de la misma.

Interrogantes

Partiendo de estas consideraciones iniciales se plantean dos preguntas que guiarán el proceso de diseño del algoritmo:

- ¿Cómo se puede guardar un byte sin alterar en gran medida una imagen?
- ¿Qué forma de distribución aleatoria en la imagen es más eficiente que simplemente dispersar la información en varios pixeles?

Respuestas

Se empezará contestando la segunda pregunta puesto que de esta forma se tiene una idea más clara de lo que el algoritmo va a hacer y a la final facilita la presentación de una alternativa de cómo guardar un byte de información. Con la finalidad de evitar que el algoritmo disperse la información a ocultar a través de todos los pixeles disponibles de la imagen se decidió que lo mejor sería agrupar los pixeles en matrices más pequeñas a las que se les llamará cubos. La idea tras agrupar los pixeles en estos cubos es reducir la dispersión de datos a través de la imagen, tratando de disminuir el ruido inducido en la misma al ocultar datos. Un cubo es una agrupación de 9 pixeles que forma una matriz de 3*3, y, que al tomar en cuenta cada uno de los canales de color (RGB) se tiene una matriz de 3*3*3. Estos cubos concentran las alteraciones de la imagen en un área determinada, aumentando el ruido en una parte pequeña de la imagen y no a través de todo el espacio.

Se ha mencionado que una de las consideraciones para el algoritmo planteado es guardar información de forma aleatoria, para conseguir este propósito se requiere de una clave, provista por el usuario, que servirá de semilla para la generación de números aleatorios. Es así

que en vez de seleccionar pixeles aleatorios, ahora se seleccionan cubos aleatorios, los cuales a su vez tienen un orden aleatorio de las capas de color. Esto aumenta la seguridad en casos en los que un atacante tenga acceso al software usado para la encriptación o que haya logrado identificar de alguna forma que se ha usado este método específico para almacenar información ya que sin la clave usada como semilla se dificulta que obtenga los cubos en orden correcto y las capas de color en orden correcto. Una ventaja de usar estos cubos es que se puede “anular” uno de los mismos para marcar así el fin de los datos ocultos, evitando tener que agregar información en los metadatos de la imagen.

Si bien la selección de cubos y de capas para almacenar información se realiza de forma aleatoria, la forma en la que se guardan los datos en cada una de las capas no lo es. Así que para contestar la pregunta primera se tiene una respuesta bastante obvia: la forma más efectiva de ocultar un byte de información sin alterar una imagen es únicamente posible si el byte que se quiere ocultar ya está presente en la imagen. No obstante, encontrar un byte exactamente igual al que se quiere ocultar en un cubo resulta una tarea complicada ya que nada asegura que el cubo y capa correspondiente para el dato tenga un byte exactamente igual y además si lo tuviera sería complicado identificar en un grupo de 8 datos cuál es el que se requiere. Una forma de reducir la complejidad de identificar el dato que se necesita de un grupo de datos fue ignorar el pixel central del cubo ya que este funcionará como indicador. Se determinó que si el byte a ocultarse es un valor par, se modificará, de ser necesario, el valor central del cubo para que sea par y se lo ocultará en las esquinas del cubo, reemplazando el color original más similar al byte a ocultar (en estos casos un byte exactamente igual es el escenario ideal) y una vez oculto el dato se modificarían los restantes para ser impares. Lo mismo es cierto para datos impares, solo que en vez de ocultar la información en las esquinas se realiza en los pixeles no esquineros del cubo.

Con esto se imita el juego de “tres en raya”, así cuando el dato es par se busca en un patrón similar al de una “X” y cuando el dato es impar se busca en un patrón similar al de un círculo “O”. No obstante, como se mencionó anteriormente, encontrar un byte exactamente igual al que se desea ocultar en la imagen usando este método se vuelve una tarea casi imposible y por lo general se agregaba aún más ruido del deseado, además de que al tratar de ocultar dos bytes por capa las alteraciones en los colores del cubo eran sumamente notables debido a los cambios que se debían efectuar para poder identificar los datos que se ocultaron.

Así que como solución a las alteraciones desproporcionadas que provocaba ocultar un byte completo tratando de que sea lo más similar posible al color original, se decidió dividir cada byte a ocultar en cuatro grupos de dos bits, los cuales serían reemplazados en los bits menos significativos de cada color en cada plaza correspondiente, siguiendo el mismo principio del tres en raya explicado con anterioridad. Sin embargo, en estos casos ya no era necesario modificar por completo todos los datos de cada capa del cubo para identificar los datos ocultos, sino que basándose en la paridad o imparidad del valor central del cubo ya sería fácil identificar los valores relevantes. Sin embargo, es necesario que cada cubo pueda ser anulado para marcar el final de un mensaje. Para esto se estableció un patrón de dos caracteres representados por los bytes “00000000” y “10101010”, ocultos con el patrón par e impar respectivamente. Si una capa contiene estos dos caracteres se la considera como nula y si todas las capas de un cubo son nulas, se infiere que el mensaje ha sido recuperado en su totalidad.

Capacidad

Las decisiones técnicas que se han tomado en afán de reducir el ruido inducido en una imagen tienen implicaciones directas sobre la capacidad total de una imagen, que resulta reducida en comparación con el método LSB. En este caso, ya no se cuenta con *n* pixeles, dónde

n es la cantidad de cubos, puesto que el pixel central de cada cubo es ignorado para ocultar información y es usado de referencia. En adición, si las dimensiones de una imagen no permiten una división exacta de cubos, es inevitable tener columnas o filas enteras que no se usan para guardar información. En contraste con el método LSB, que permite ocultar n bits de información por pixel, dependiendo del ruido que se considere aceptable sobre una imagen, este método se limita a ocultar 2 bits por pixel, o dos bytes por capa, sumando un total de 6 bytes por pixel.

Flujograma del algoritmo

El algoritmo propuesto consta de tres procesos importantes los cuales se van a detallar a continuación, acompañado de un diagrama de flujo del algoritmo para brindar una visión más clara del mismo. Sin embargo, estos tres procesos se pueden resumir en:

1. *Pre procesamiento de la imagen*. Cuando el algoritmo recibe una imagen lo primero que realiza es extraer los cubos de la misma para poder ejecutar el proceso que se desee, es decir, ocultar o extraer información. En el caso de ocultar información, en este paso se determinará si la imagen cuenta con espacio suficiente para almacenar todos los datos que se desea ocultar. Es importante notar que un “cubo” tiene sus capas de color ordenadas de forma pseudo aleatoria, dependiendo de la semilla, al momento de su creación.
2. *Ocultación de información*. Una vez que se tenga todos los cubos y se haya comprobado que la imagen cuenta con la capacidad necesaria para ocultar información se procede a seleccionar los cubos que transportarán información de forma pseudo aleatoria. Ya que se tenga los cubos, se le entrega a cada uno un máximo de tres pares de bytes para que lo oculten en cada una de sus capas. En este proceso es importante notar que si un cubo recibe menos de tres pares

de bytes anulará las capas correspondientes, dejando válidas aquellas que contengan información. El último cubo de la serie anulará todas sus capas para marcar que es el fin del mensaje.

3. *Extracción de información*. Una vez que se tengan todos los cubos se los leerá de manera pseudo aleatoria, indicando a cada cubo que devuelva la información de cada una de sus capas, hasta encontrar aquel cubo que marque el final de la serie. Una vez que se tengan los bytes de información requeridos, se construirá el mensaje original y finalizará el proceso.}

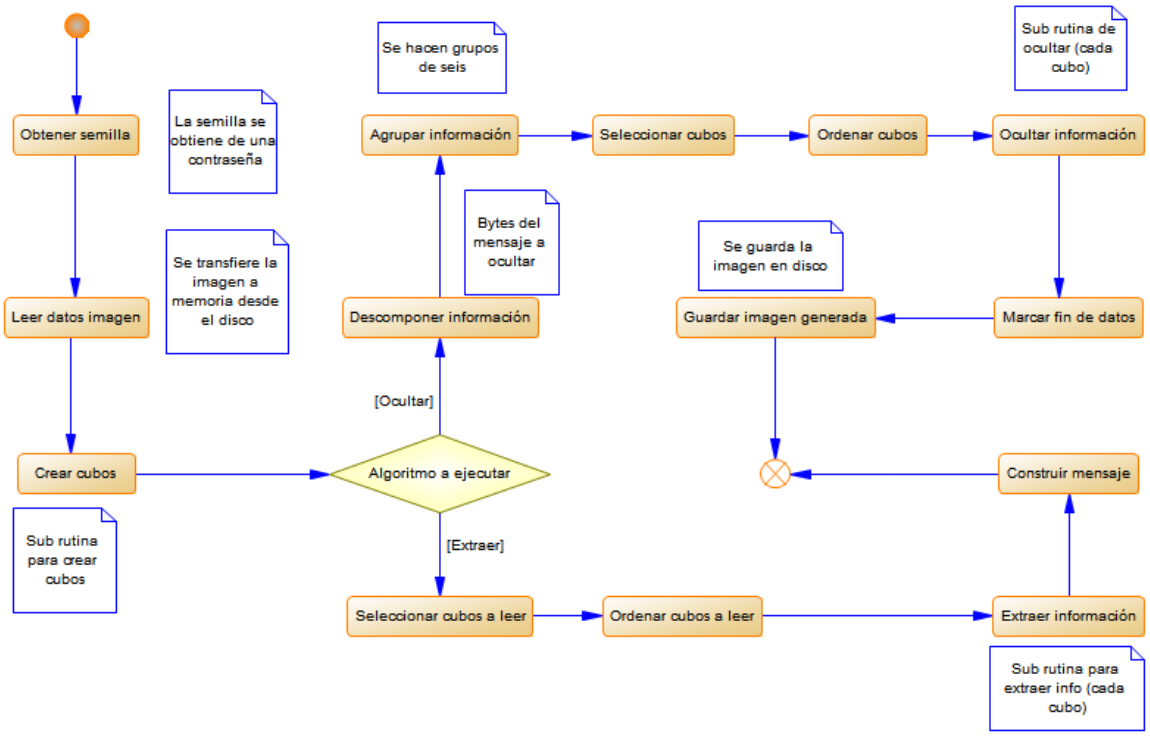
El flujo general del algoritmo se puede apreciar de forma gráfica en la Figura 5. Como se ha mencionado durante el diseño inicial del algoritmo, la aleatoriedad del mismo es una característica que aumenta la seguridad ante ataques que apunten a extraer la información oculta en un esteganograma. Para asegurar que sea posible obtener los mismos valores aleatorios en una serie generada a base de una semilla, el primer paso es obtener la "semilla" para generar esta secuencia. La "semilla" es un hash, o huella digital única, para una secuencia de caracteres proporcionada por el usuario, de esta forma se puede asegurar una secuencia pseudo aleatoria consistente para ocultar y retirar información de un esteganograma.

Posterior al establecimiento de la semilla necesaria para el algoritmo, se procede a leer la información de la imagen desde el disco, puesto que el prototipo (ver implementación) hace uso de una arquitectura cliente servidor y por lo tanto es necesario que la imagen sea escrita en disco. Una vez que la información de la imagen está disponible en memoria se procede a la construcción de los cubos que contendrán información, este proceso se puede ver de forma gráfica en la Figura 6. Los cubos, como se explicó con anterioridad, son unidades encargadas de retirar y ocultar información en la imagen original. Estas unidades tienen un orden lógico en sus canales de color RGB, el cual es establecido de forma aleatoria teniendo como base la semilla

provista de los primeros pasos del algoritmo. Es importante recordar que un cubo es una matriz que consta de un total de nueve pixeles, con dimensiones de tres pixeles de ancho por tres pixeles de largo. No obstante, el pixel central no almacena información, dando un total de ocho pixeles disponibles. Un cubo puede almacenar un máximo de 6 bytes, es decir, dos bytes por cada capa de color.

Figura 5

Flujograma del algoritmo

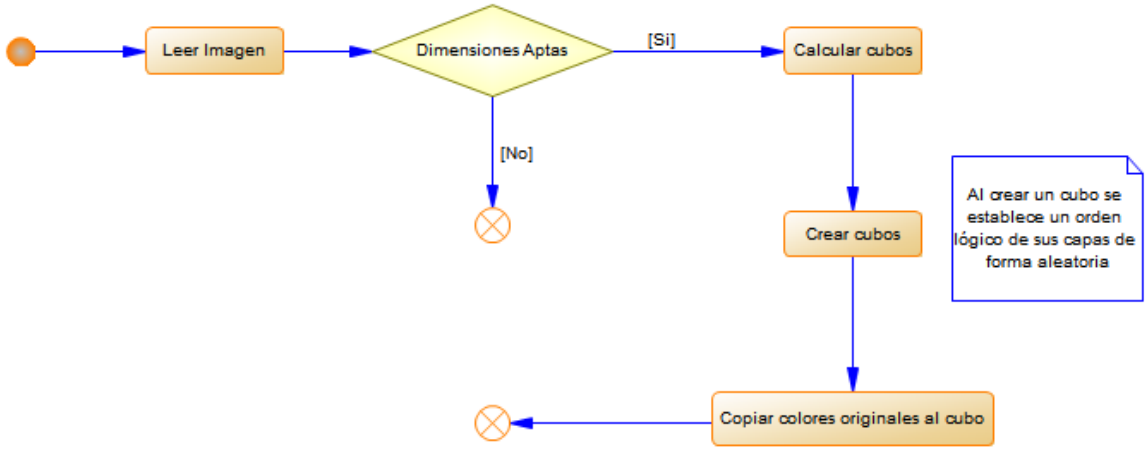


Una vez que el algoritmo ya tenga listos los cubos disponibles para ejecutar el resto de pasos, se procederá a ejecutar el proceso de ocultación o extracción según se requiera. En el caso de que se requiera ocultar información el primer paso es descomponer la información recibida en un listado de valores, más específicamente, en un listado de bytes. Posteriormente se agruparan en conjuntos de seis elementos, esto es debido a que los cubos tienen una capacidad máxima de seis bytes. Una vez finalizada la agrupación, se procederá a seleccionar los

cubos necesarios para ocultar información, la cantidad de cubos a seleccionar es igual a la cantidad de grupos a ocultar. Es importante notar que la selección de cubos es aleatoria y siempre se seleccionarán (n grupos + 1) cubos. Esto es porque el último cubo se usará para marcar el final de la secuencia de datos, y el resto de cubos se ordenarán nuevamente de forma aleatoria.

Figura 6

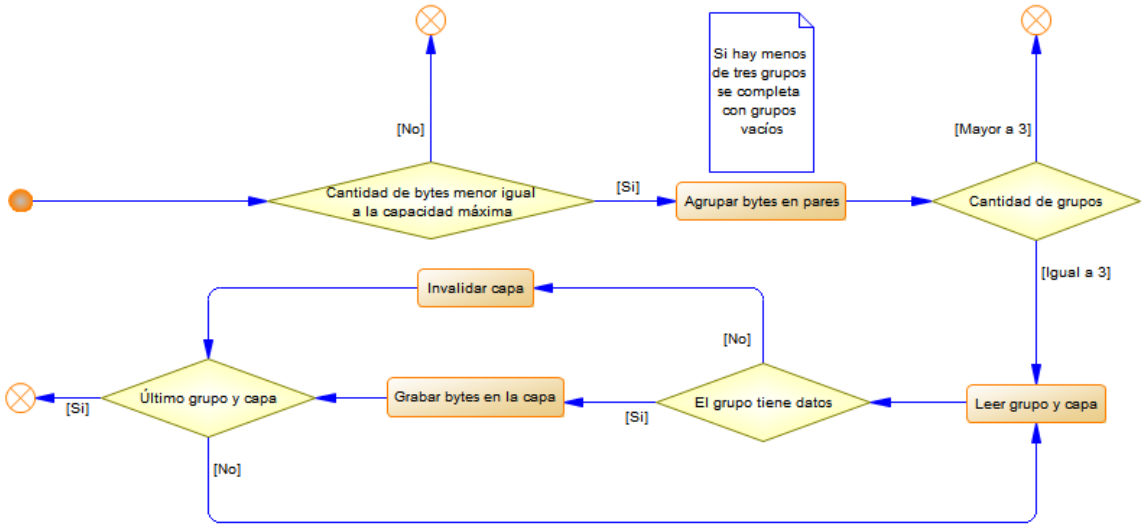
Flujograma para la creación de cubos



Es importante notar que cada cubo seleccionado ejecuta la sub rutina para ocultar información ilustrada en la Figura 7 con el conjunto de bytes que se le han asignado, hay que tener en cuenta las consideraciones que se utilizan para ordenar los datos en la capa.

Figura 7

Flujograma para ocultar datos



Como ya se ha descrito anteriormente, una primera iteración del algoritmo planteaba ocultar un byte completo en un lugar apropiado, pero esta alteración era sumamente notable y los resultados no eran remotamente aceptables. Por lo que se planteó dividir los bytes y ocultarlos siguiendo un patrón de tres en raya, para mantener una organización constante y que permitiese identificar fácilmente los datos cuando se requiera extraerlos, además de que esto evitaría modificar en mayor medida el algoritmo en su primera versión. Cada cubo oculta la información siguiendo el principio de tres en raya planteado originalmente y en el orden aleatorio en el que se organizan las capas al momento de su creación. Como se ha descrito anteriormente, los datos originales se separan en grupos de seis elementos que son asignados a cada cubo, pero ¿Qué pasa cuando hay menos de seis elementos? En estos casos se completan las plazas restantes con valores nulos, representados como 0. De esta forma se asegura una diferenciación concreta entre datos válidos, no válidos y cubos o capas anuladas.

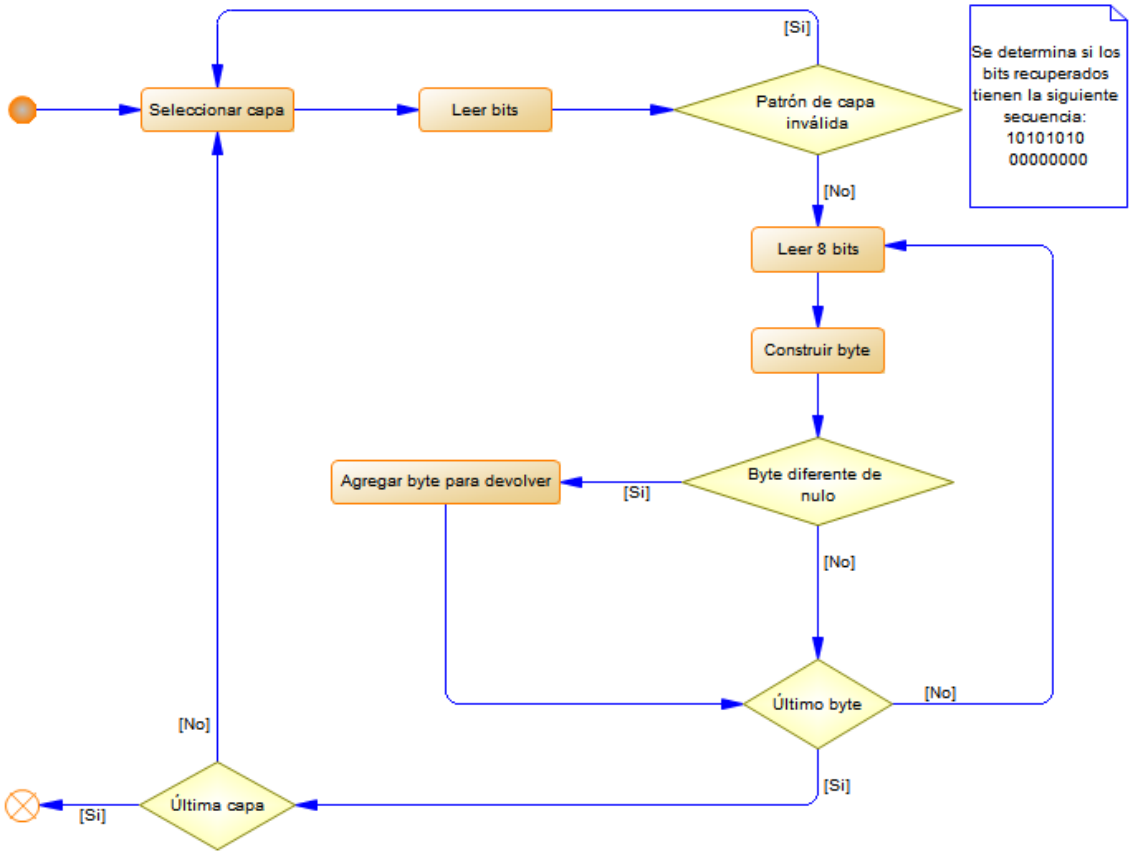
Una vez que cada cubo haya completado el proceso para ocultar la información que se le ha asignado, se procede a anular el último cubo de la selección original de cubos que se

mencionó en un principio. Esta “anulación” no es más que ingresar un patrón específico siguiendo el principio de tres en raya en cada una de las capas, este patrón de bits es el siguiente “1010101000000000”, con esto se podrá identificar cuando finaliza un mensaje sin la necesidad de agregar más información, a la cabecera de la imagen por ejemplo, como lo realizan otros algoritmos. Como paso final, se reemplazan los cubos modificados en la imagen original, para esto se usan las coordenadas del cubo en la imagen y se reemplazan los colores originales con los modificados y posteriormente se escribe la imagen en disco.

Una vez comprendida de mejor manera cómo se guardan los datos en una imagen, la explicación de cómo se extrae la información resulta más sencilla, ya que básicamente resulta ser el proceso inverso al usado para ocultar información, que también se ejecuta en cada uno de los cubos. Como se puede observar en la Figura 5, este proceso comienza con la selección y posterior reorganización de aquellos cubos de los que se extraerán datos, este proceso es similar al realizado al momento de ocultar información. Una de las principales diferencias es que al momento de retirar los datos no se conoce el número de cubos que se deben leer, es por esto que se usa un patrón para anular cubos, cuando se encuentra este patrón se detiene la búsqueda y los cubos seleccionados son sorteados de forma aleatoria para poder obtener, en orden correcto, los datos ocultos en primer lugar. Posteriormente, como se puede observar en el proceso detallado en la Figura 8, cada cubo busca en cada una de sus capas, dependiendo del principio del tres en raya, la información oculta. Cuando se extraen ocho bits es posible construir un byte y agregarlo a una lista que retornará el cubo para la construcción del mensaje oculto. Es importante notar que en estos casos si se encuentra un valor nulo, o 0, no se agregará a este listado, para evitar agregar datos basura en el mensaje original.

Figura 8

Flujograma para extraer información.



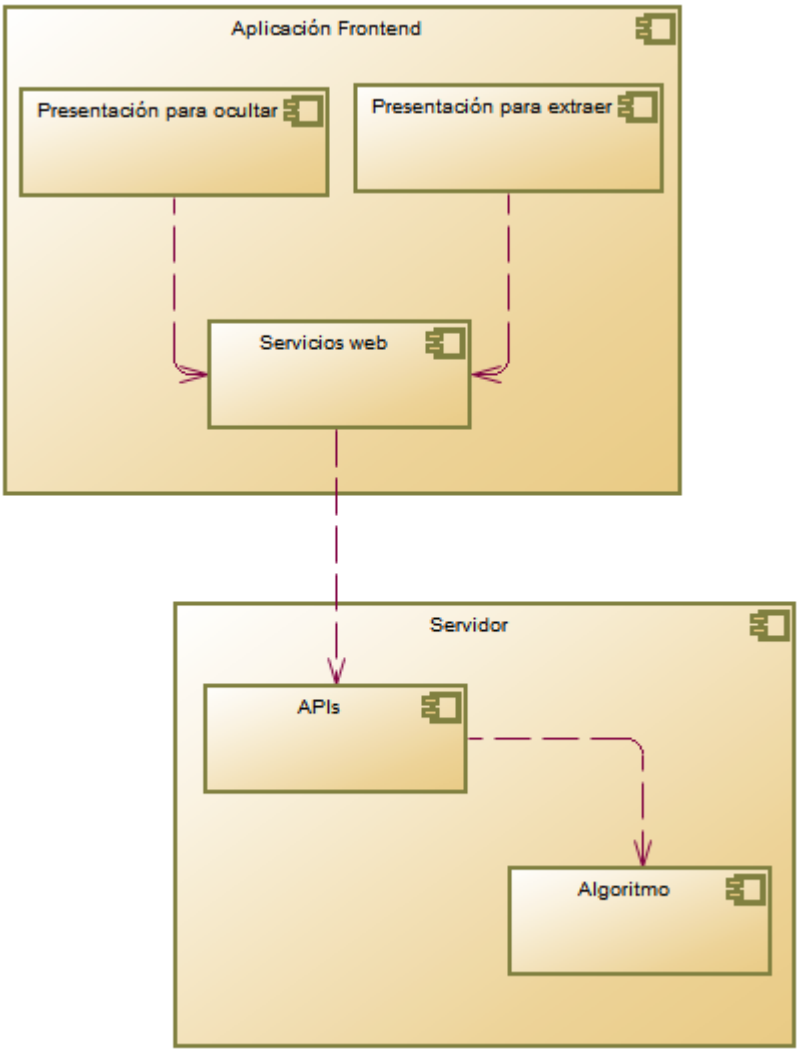
Como se puede observar el algoritmo planteado no resulta complejo, en comparación con otras alternativas elaboradas en base a principios matemáticos avanzados. Una de las principales ventajas es que al dividir el trabajo en cubos independientes, el proceso de ocultación y extracción se puede ejecutar en forma paralela para reducir el tiempo que se tarda en ejecutar las sub rutinas descritas en la Figura 7 y 8, ya que hay que recordar que cada una de estas es ejecutada por cada uno de los cubos seleccionados de la imagen.

Implementación

Para la implementación del prototipo que permitiese demostrar el funcionamiento del algoritmo de una manera más interactiva se utilizó una arquitectura cliente-servidor con los componentes descritos en la Figura 9. Para esto se han utilizado las herramientas descritas en secciones anteriores.

Figura 9

Diagrama de componentes de la aplicación



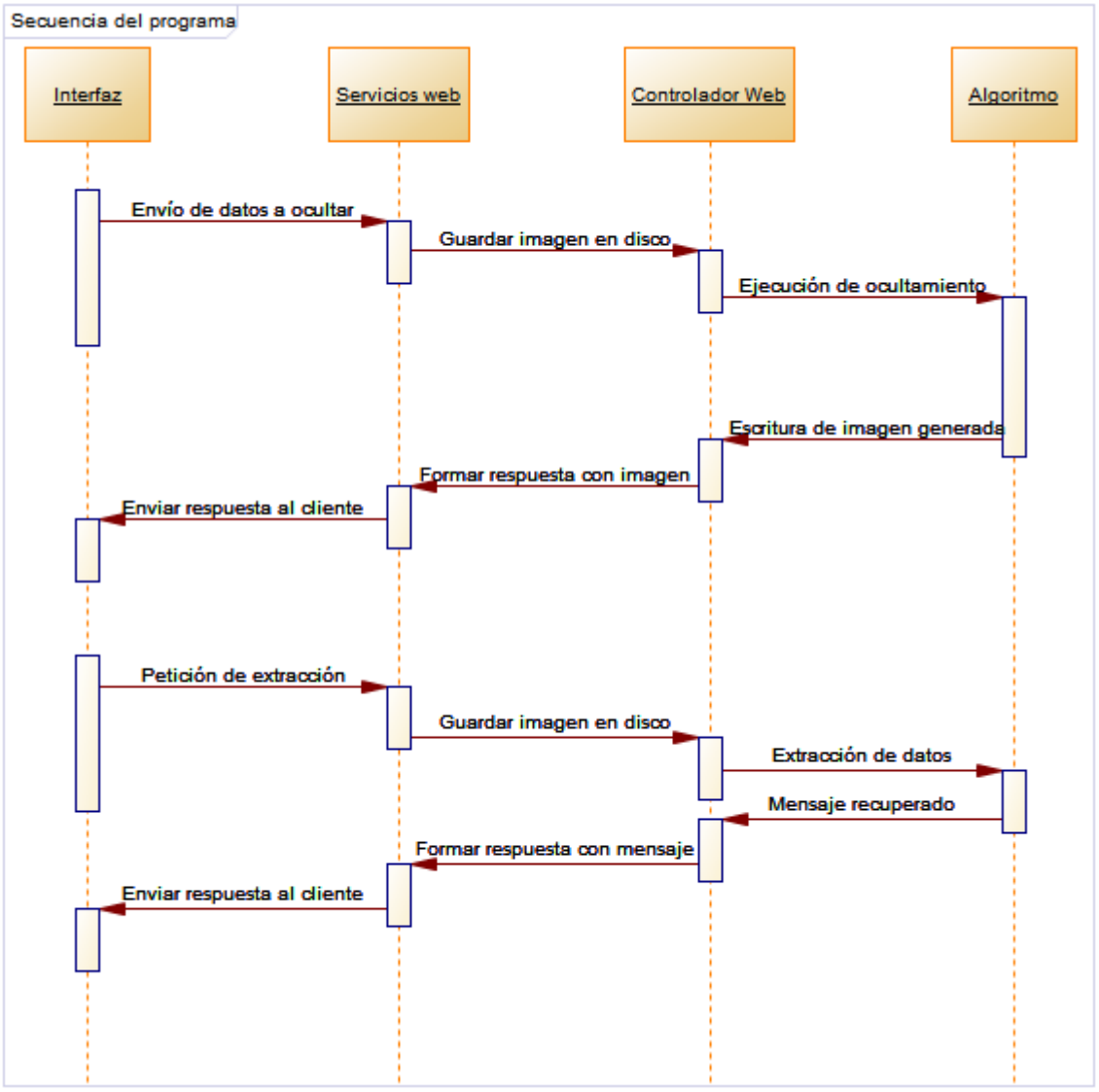
La implementación del prototipo se lo realizó siguiendo la metodología de desarrollo ágil propuesta por Moyo & Mnkandla (2020), permitiendo iterar rápidamente sobre varias versiones manteniendo la seguridad del código desarrollado. Esto permitió ajustar diversos aspectos, desde la interfaz de usuario, hasta el funcionamiento del algoritmo propuesto. Para poder entender cómo interactúan estos componentes se puede observar el diagrama de flujo detallado en la Figura 10. Como se puede notar, es una interacción sumamente simple y comprensible, ya que el trabajo más complejo es ejecutado por el algoritmo como se lo describe en la sección del diseño de la propuesta. El cliente (Interfaz) envía los datos necesarios para ocultar o retirar información, los cuales son básicamente una contraseña, un mensaje y una imagen. La única diferencia es que al enviar una petición de extracción se omite el mensaje y la imagen enviada debe ser la que se devolvió al usuario al momento de realizar el proceso de ocultación de datos.

Por lo general, los programas usados para esteganografía son herramientas instaladas de manera local en el equipo del usuario, lo que le puede facilitar la identificación del algoritmo esteganográfico al atacante y por ende a vulnerar o extraer información confidencial (Karampidis et al., 2018). Separando y simulando un servicio web para ocultar información imágenes brinda una nueva perspectiva al uso de estas herramientas, haciéndolas más accesibles y amigables para aquellas personas que quieren mantener su privacidad pero no quieren descargar herramientas en sus computadores.

Si bien usando este nuevo acercamiento se pueden producir nuevas interrogantes sobre la seguridad de la información que se transmite o recibe de los servidores, se debe recalcar que esas consideraciones no son parte del estudio y por lo tanto no se las ha tomado en cuenta como parte del objetivo de aumentar los niveles de seguridad que se pueden obtener al usar este método.

Figura 10

Secuencia del programa



En la Figura 11 se puede ver el prototipo en funcionamiento mostrando la interfaz en la cual el usuario puede ocultar información haciendo uso de los servicios que se ejecutan en un servidor remoto, la Figura 12 en cambio, muestra la interfaz que el usuario ve cuando desea extraer información de una imagen que actúa como transporte para datos confidenciales.

Figura 11

Interfaz del servicio para ocultar información

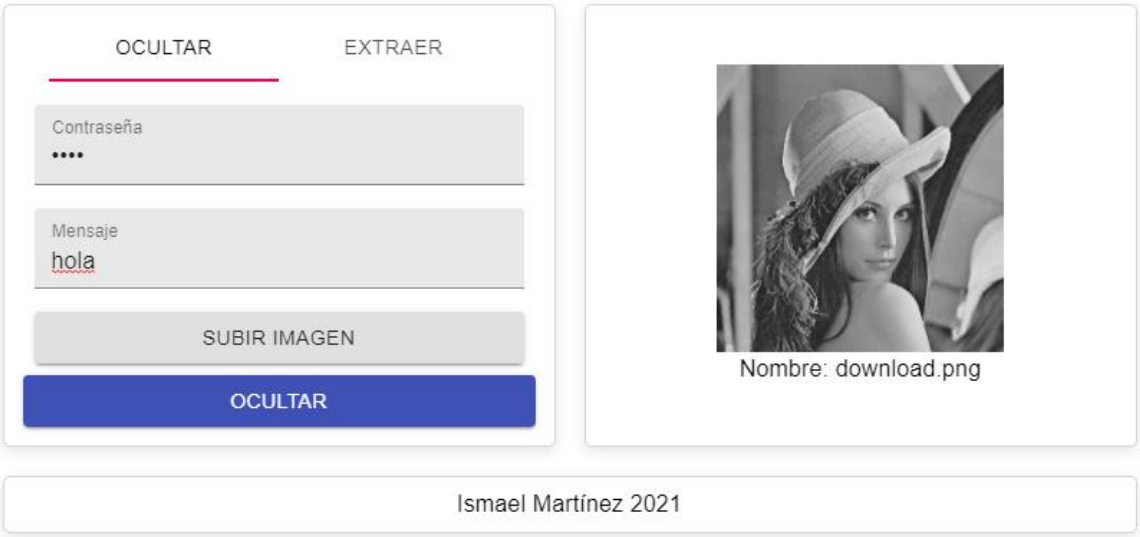


Figura 12

Interfaz del servicio para extraer información

Validación

Como se describió en partes anteriores, para la evaluación del método propuesto, se va a evaluar la calidad de los esteganogramas que resulten de la aplicación del mismo para ocultar información. Una de las métricas es el MSE, cuyo valor debe ser lo más cercano a cero posible, ya que valores mayores pueden delatar una alteración sustancial en la imagen y dar la impresión de que tiene información oculta. Otra de las métricas que se va a evaluar es el PSNR, este valor, en contraste con el MSE, debe ser un valor lo mayor posible, ya que matemáticamente es la inversa del MSE. Se puede asegurar entonces, que un valor diminuto de la métrica MSE resultará en valores más elevados al aplicar el PSNR. Para la evaluación del algoritmo se atravesaron dos fases: Experimentación y un análisis de casos específicos.

La primera fase se la realizó para obtener una visión general del rendimiento del algoritmo en comparación con el ya conocido LSB. La segunda fase, en cambio, se usó para determinar los rangos en los que el algoritmo propuesto presentaba mejores resultados que su contraparte, facilitando así, delimitar la utilidad y mejoras presentadas por esta nueva propuesta.

Experimentación

Componentes

Para este experimento de evaluación de la efectividad del método esteganográfico propuesto se va a hacer uso de las imágenes presentadas en las Figuras 13, 14 y 15. Estas imágenes son de diferentes dimensiones y como se puede observar, dos son a color y una de ellas está en escala de grises. La inclusión de una imagen a escala de grises resulta del estudio presentado por (Knight, 2000) en el que establece que estas presentan mejores resultados.

Para comparar los resultados del método LSB y el método propuesto se usará la aplicación Open Stego, la cual implementa un algoritmo de LSB aleatorizado, además de encriptación con contraseña para un mayor nivel de seguridad sobre la información. El uso de esta aplicación es conveniente ya que el método propuesto también tiene un grado de pseudo aleatoriedad determinado por la contraseña del usuario.

Para el análisis de la efectividad se compararan los valores de MSE y PSNR obtenidos al ocultar información con estos métodos, para esto se utilizará Octave y la librería “Image” la cual tiene diversos métodos para el procesamiento de imágenes.

Figura 13

Lena

Nota: Imagen distribuida en el paquete de procesamiento de imágenes *EBImage*, de Pau et al., 2010, 10.18129/B9.bioc.EBImage. LPGL.

Figura 14

Lena escala de grises

Nota: Imagen distribuida en el paquete de procesamiento de imágenes *EBImage*, de Pau et al., 2010, 10.18129/B9.bioc.EBImage. LPGL.

Figura 15

Casas

Nota: Imagen distribuida en el paquete de procesamiento de imágenes *EBImage*, de Pau et al., 2010, 10.18129/B9.bioc.EBImage. LPGL.

¿Qué se va a hacer?

Se ocultaran mensajes de las siguientes longitudes (bytes): 10, 100, 200, 300… 1000, en las Figuras 13, 14 y 15 haciendo uso de la aplicación Open Stego y el prototipo desarrollado.

Una vez finalizado el proceso de ocultación se calcularán los valores de MSE y PSNR para cada esteganograma, tomando como referencia la imagen original. Se compararán estos valores y se determinará la efectividad del método propuesto.

Resultados

Los resultados de las evaluaciones realizadas sobre las muestras disponibles comparándolas con el material original presentan dos conjuntos de resultados, uno referente a las medidas obtenidas con la métrica MSE y el otro conjunto referente a la métrica del PSNR. Como se puede observar en la Figura 16, los resultados de las pruebas se muestran favorables para el algoritmo propuesto, desafortunadamente, la mejora solo es notable con una cantidad reducida de información oculta, ya que a medida que la información crece en tamaño el rendimiento se degrada de forma constante y en gran medida.

Figura 16

Resultados del experimento

		Propuesto			LSB			Propuesto/LSB			Propuesto-LSB		
	Bytes	Lena	Lena e.grises	Casas	Lena	Lena e.grises	Casas	Relación			Diferencia		
MSE	10	0,0003	0,0011	0,0001	0,0005	0,0013	0,0001	44%	18%	28%	-0,00020	-0,00023	-0,00003
	100	0,0018	0,0049	0,0004	0,0009	0,0027	0,0002	-96%	-78%	-74%	0,00089	0,00213	0,00015
	200	0,0036	0,0104	0,0007	0,0013	0,0039	0,0003	-174%	-169%	-157%	0,00230	0,00656	0,00044
	300	0,0051	0,0147	0,0011	0,0016	0,0045	0,0003	-229%	-227%	-231%	0,00356	0,01023	0,00075
	400	0,0067	0,0187	0,0014	0,0021	0,0061	0,0005	-215%	-208%	-202%	0,00457	0,01261	0,00092
	500	0,0085	0,0225	0,0017	0,0023	0,0067	0,0005	-271%	-238%	-244%	0,00618	0,01585	0,00122
	600	0,0101	0,0271	0,0021	0,0026	0,0076	0,0006	-282%	-257%	-271%	0,00745	0,01950	0,00151
	700	0,0122	0,0323	0,0024	0,0030	0,0087	0,0007	-307%	-269%	-266%	0,00923	0,02353	0,00174
	800	0,0132	0,0361	0,0028	0,0031	0,0093	0,0007	-327%	-287%	-295%	0,01008	0,02675	0,00206
	900	0,0151	0,0403	0,0031	0,0034	0,0101	0,0007	-346%	-300%	-328%	0,01171	0,03026	0,00241
	1000	0,0166	0,0455	0,0034	0,0040	0,0121	0,0009	-315%	-275%	-293%	0,01263	0,03337	0,00255
PSNR	10	84,15	77,87	89,54	81,59	77,02	88,12	3%	1%	2%	2,55	0,85	1,42
	100	75,53	71,26	82,67	78,45	73,77	85,08	-4%	-4%	-3%	-2,92	-2,50	-2,41
	200	72,54	67,95	79,52	76,91	72,25	83,63	-6%	-6%	-5%	-4,37	-4,30	-4,10
	300	71,04	66,45	77,79	76,20	71,59	82,99	-7%	-8%	-7%	-5,17	-5,14	-5,20
	400	69,88	65,42	76,74	74,87	70,31	81,54	-7%	-7%	-6%	-4,99	-4,89	-4,80
	500	68,86	64,61	75,76	74,55	69,90	81,12	-8%	-8%	-7%	-5,69	-5,29	-5,36
	600	68,09	63,80	74,97	73,91	69,33	80,66	-9%	-9%	-8%	-5,82	-5,53	-5,69
	700	67,25	63,04	74,33	73,34	68,72	79,97	-9%	-9%	-8%	-6,09	-5,67	-5,63
	800	66,93	62,56	73,72	73,24	68,43	79,68	-9%	-9%	-8%	-6,30	-5,87	-5,96
	900	66,34	62,07	73,16	72,84	68,10	79,47	-10%	-10%	-9%	-6,50	-6,02	-6,31
	1000	65,92	61,55	72,80	72,10	67,29	78,73	-9%	-9%	-8%	-6,18	-5,74	-5,94

Si se analiza la relación que guarda el algoritmo propuesto con el algoritmo LSB, usando la métrica del MSE, se puede notar que cuando se almacenan 10 bytes el algoritmo propuesto

presenta una mejora del 28% ~ 44% en imágenes a color, mientras que en imágenes en escala de grises la mejora es de apenas el 18%. Sin embargo, cuando se almacenan datos desde los 100 bytes en adelante se puede notar un rendimiento menor, hasta en un 315%. Esto es una clara indicación de que el algoritmo propuesto no tiene un rendimiento aceptable con grandes cantidades de información. Los valores descritos anteriormente se pueden apreciar de mejor manera en la Figura 17.

Figura 17

Mejoras presentadas por el algoritmo

		Propuesto/LSB		
	Bytes	Relación		
MSE	10	44%	18%	28%
	100	-96%	-78%	-74%
	200	-174%	-169%	-157%
	300	-229%	-227%	-231%
	400	-215%	-208%	-202%
	500	-271%	-238%	-244%
	600	-282%	-257%	-271%
	700	-307%	-269%	-266%
	800	-327%	-287%	-295%
	900	-346%	-300%	-328%
	1000	-315%	-275%	-293%
PSNR	10	3%	1%	2%
	100	-4%	-4%	-3%
	200	-6%	-6%	-5%
	300	-7%	-8%	-7%
	400	-7%	-7%	-6%
	500	-8%	-8%	-7%
	600	-9%	-9%	-8%
	700	-9%	-9%	-8%
	800	-9%	-9%	-8%
	900	-10%	-10%	-9%
	1000	-9%	-9%	-8%

Al analizar de forma gráfica la evolución del rendimiento del algoritmo con la métrica MSE, se puede notar un patrón interesante. Al analizar el deterioro de una imagen en una escala macro, como se muestra en la Figura 18 y 19, el deterioro de los esteganogramas resultado del

algoritmo propuesto crece de una forma más notable y precipitada en contraste con el algoritmo LSB.

Figura 18

Patrón del deterioro de una imagen representado con la métrica MSE.

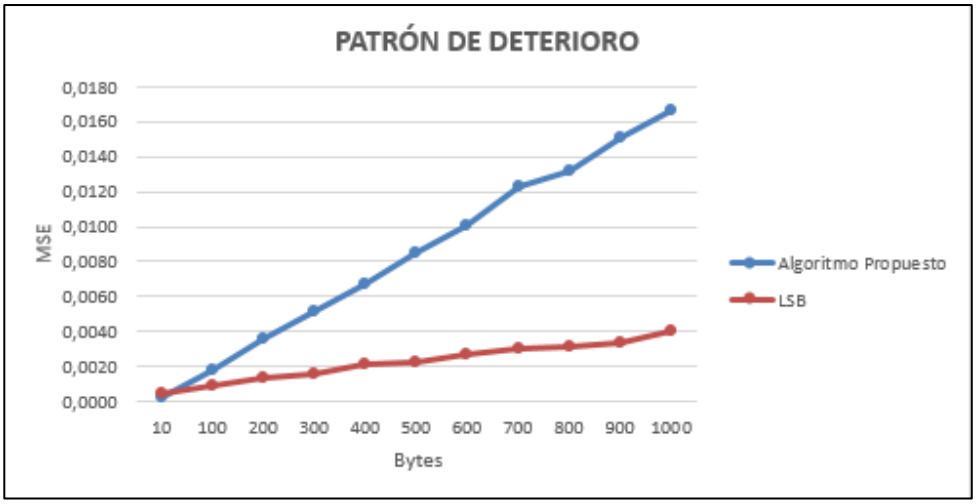
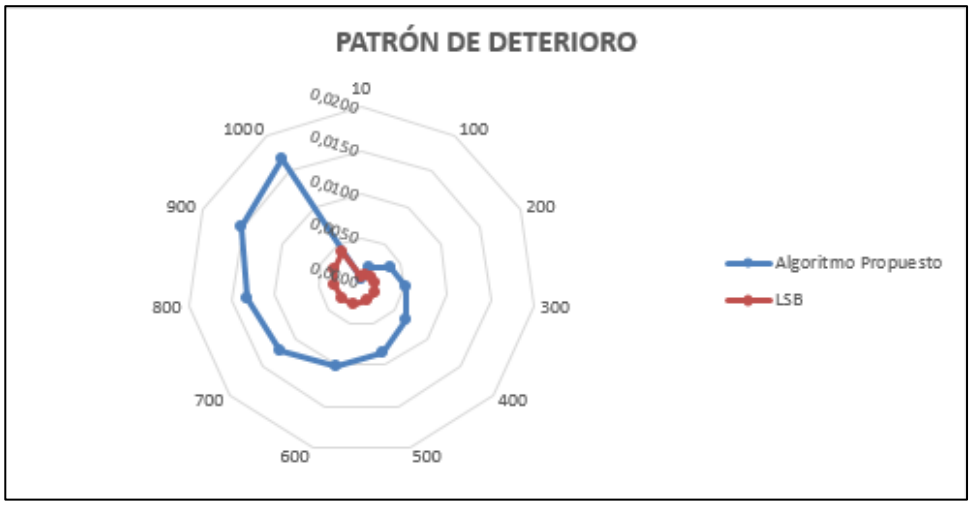


Figura 19

Patrón de deterioro de una imagen representado con la métrica MSE.



No obstante, analizando el comportamiento reflejado en las Figuras 20 y 21, al aplicar la métrica del PSNR no se observa una degradación notable del algoritmo propuesto en contraste

con el algoritmo LSB. Esto se da principalmente porque esta medida sigue una escala logarítmica, y sus valores se representan en decibeles.

Figura 20

Patrón de deterioro de una imagen representado con la métrica PSNR.

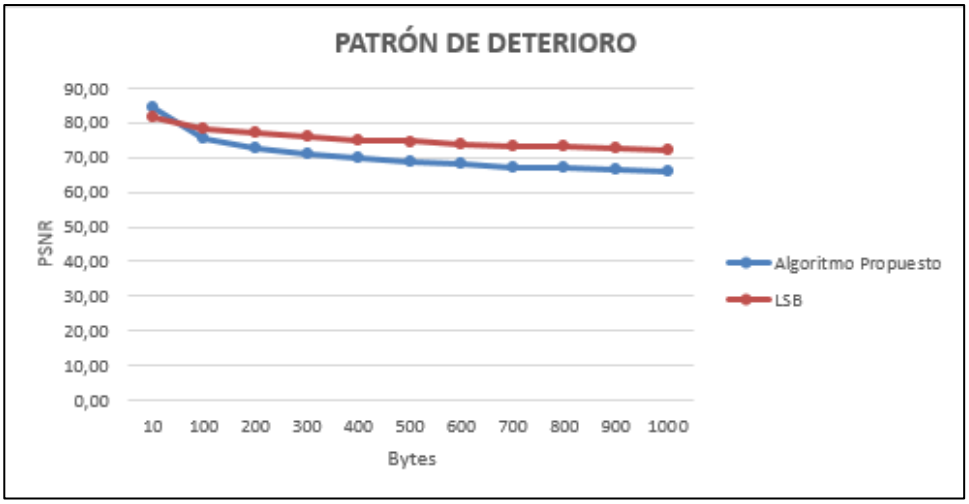
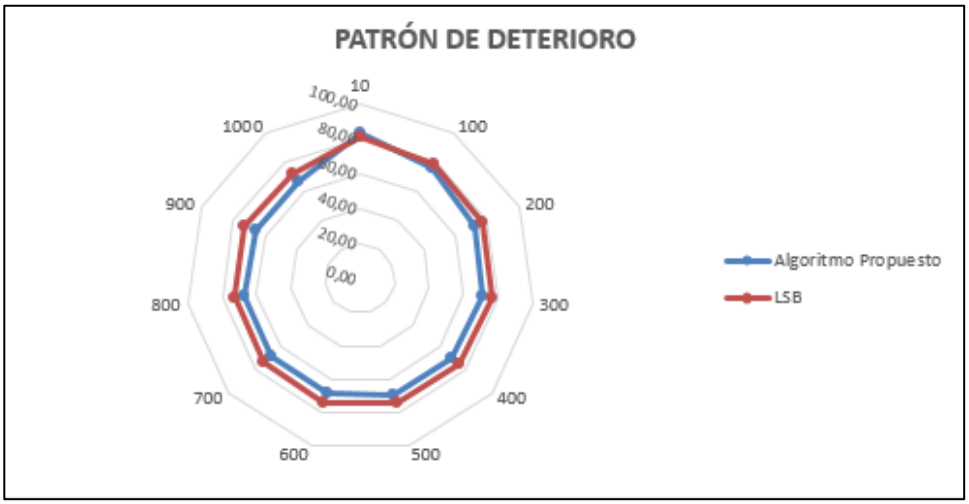


Figura 21

Patrón de deterioro de una imagen representado con la métrica PSNR.



Los patrones que se observan a través de las Figuras 18 a 21 se repiten a través de los resultados que se obtuvieron tras ocultar información en las Figuras 13, 14 y 15, por lo que es seguro determinar, en esta escala, que pasados los 100 bytes de información, el algoritmo no resulta de gran utilidad puesto que el deterioro de la imagen original resultará en

esteganogramas de baja calidad que podrían ser calificados de inmediato como portadores de información confidencial, vulnerando este método fácilmente.

Análisis por casos

Dados los resultados que se obtuvieron ocultando diferentes cantidades de bytes entre 10 y 1000 bytes, se determinó que sería necesario estudiar con más detalle otras cantidades de datos, más específicamente en el rango entre los 10 y 100 bytes debido a que con la primera cantidad de datos mencionada los resultados resultan favorables. Es así que se empezó un análisis por casos específicos limitando el rango de datos a ocultar entre los 10 y 50 bytes con la finalidad de determinar hasta qué punto el algoritmo muestra un mejor rendimiento que el algoritmo de LSB.

Figura 22

Resultados del análisis por casos.

		Propuesto/LSB		
	Bytes	Relación		
MSE	10	44%	18%	28%
	20	-6%	-14%	4%
	30	19%	-15%	6%
	40	-26%	-22%	-6%
	50	-22%	-27%	-25%
PSNR	10	3%	1%	2%
	20	0%	-1%	0%
	30	1%	-1%	0%
	40	-1%	-1%	0%
	50	-1%	-1%	-1%

Es así que se volvieron a ejecutar nuevamente las pruebas de la sección del experimento, pero esta vez, enfocándose únicamente en un rango más limitado. Tras efectuar estos análisis se logró detectar un nivel máximo de 30 bytes, como se puede observar en la Figura 22, lo que resultaría el límite más efectivo para ocultar información con este algoritmo.

Las Figuras 23 y 24 retratan cómo evoluciona el deterioro de la Figura 13 cuando se oculta información, pasados los 30 bytes se empieza a notar el patrón retratado en la Figura 18 y 19.

Figura 23

Deterioro de imagen a color representado con la métrica MSE.

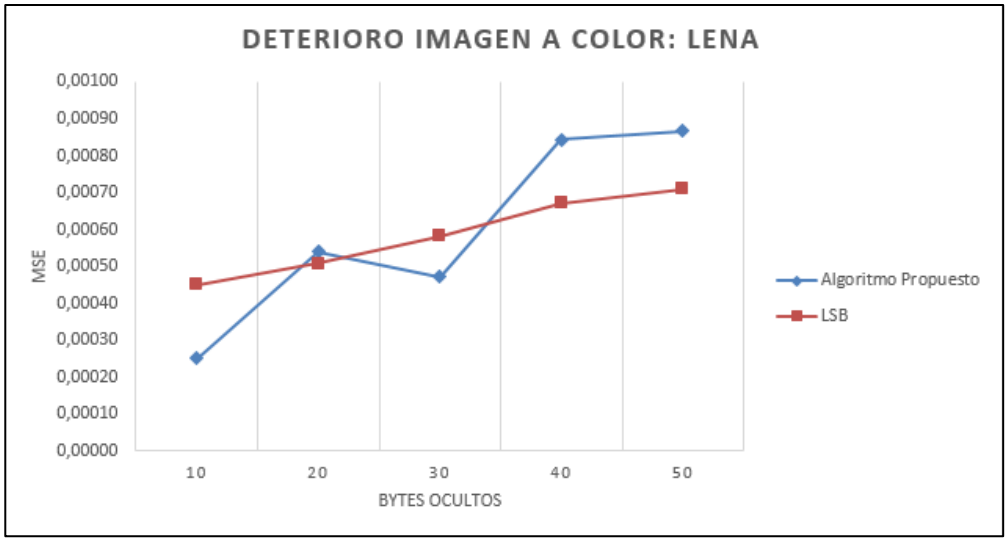
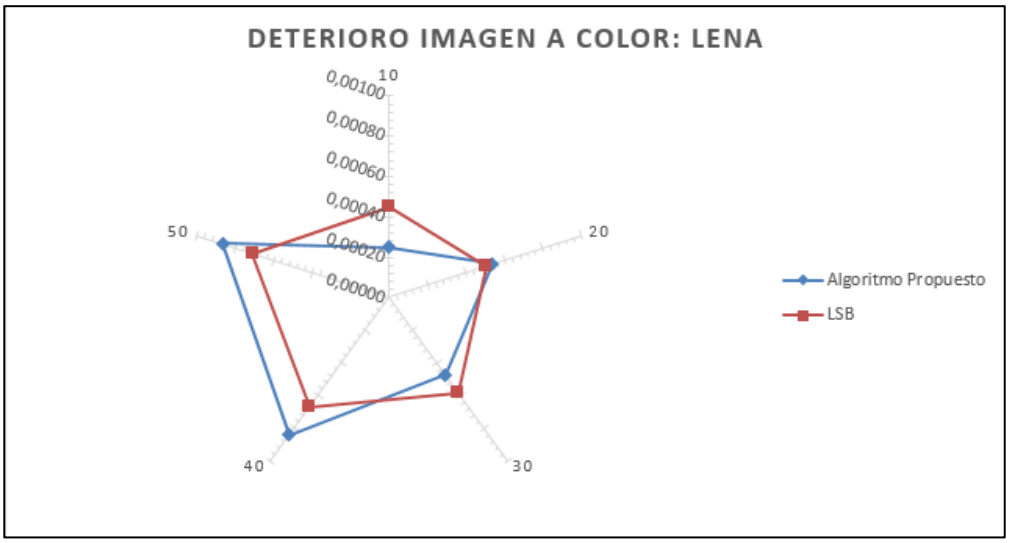


Figura 24

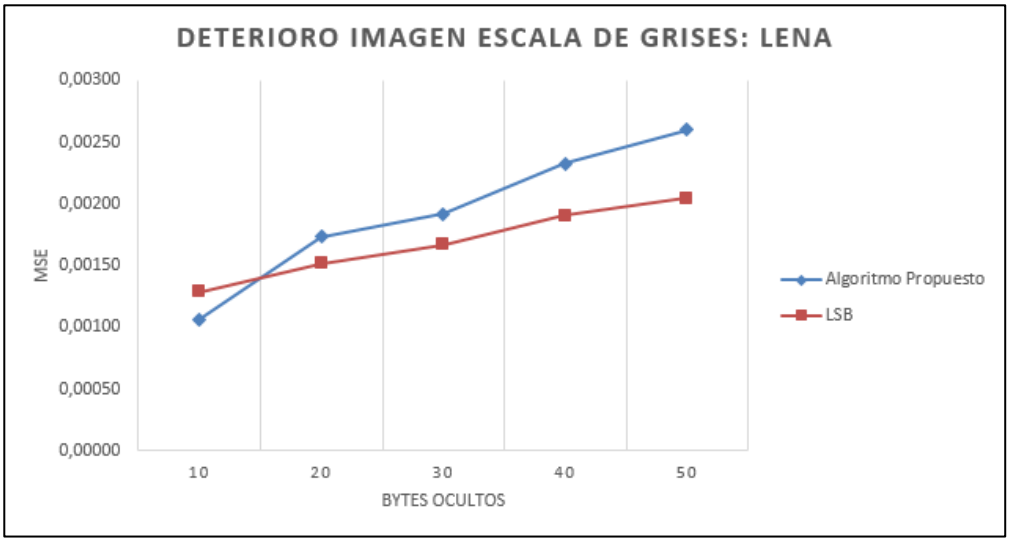
Deterioro de imagen a color representado con la métrica MSE.



Como se mencionó previamente, los resultados al ocultar información en una imagen a escala de grises no resulta favorable. Esto se puede ver claramente retratado en las Figuras 25 y 26, donde se puede observar cómo pasados los 10 bytes de información el deterioro es cada vez más notable, como se pudo observar en las Figuras 18 y 19.

Figura 25

Deterioro imagen en escala de grises representado por la métrica MSE.



Sin embargo, es interesante observar los resultados retratados en la Figuras 27 y 28 tras ocultar información en la Figura 15, puesto que la misma es a color y de mayores dimensiones que las Figuras 13 y 14 los valores obtenidos por la métrica de evaluación MSE siempre están por debajo que los valores obtenidos con el algoritmo LSB. No obstante, pasados los 30 bytes se vuelve a notar el deterioro ya identificado anteriormente. Esto puede brindar un poco de luz sobre las condiciones bajo las cuales el algoritmo propuesto puede resultar más efectivo que su contraparte.

Figura 26

Deterioro de imagen en escala de grises representado por métrica MSE.

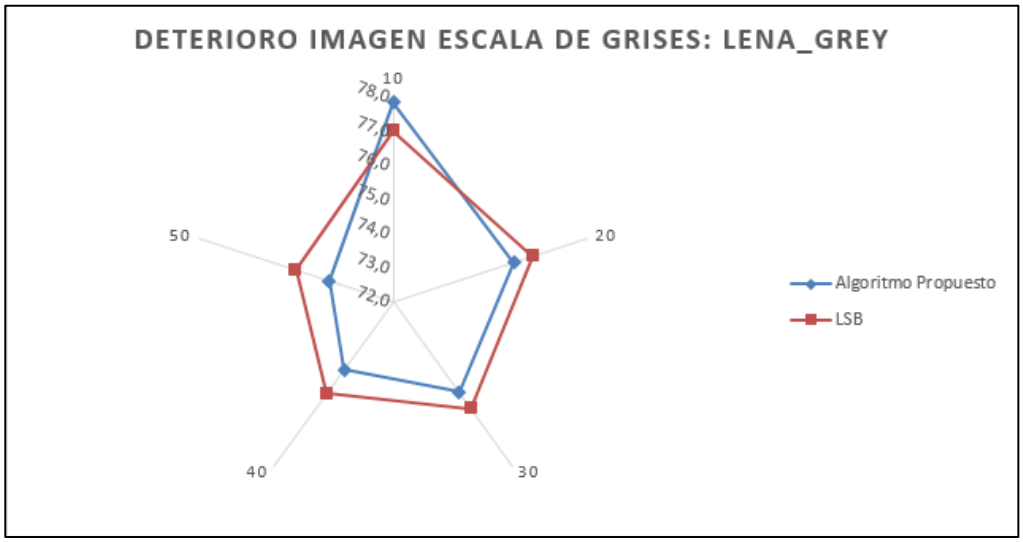


Figura 27

Deterioro de imagen a color representado con la métrica MSE.

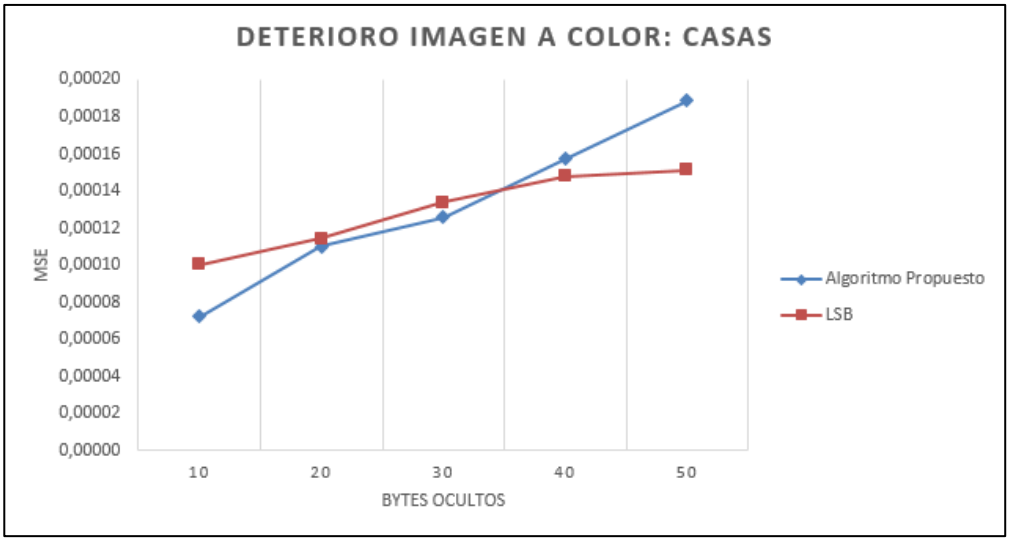
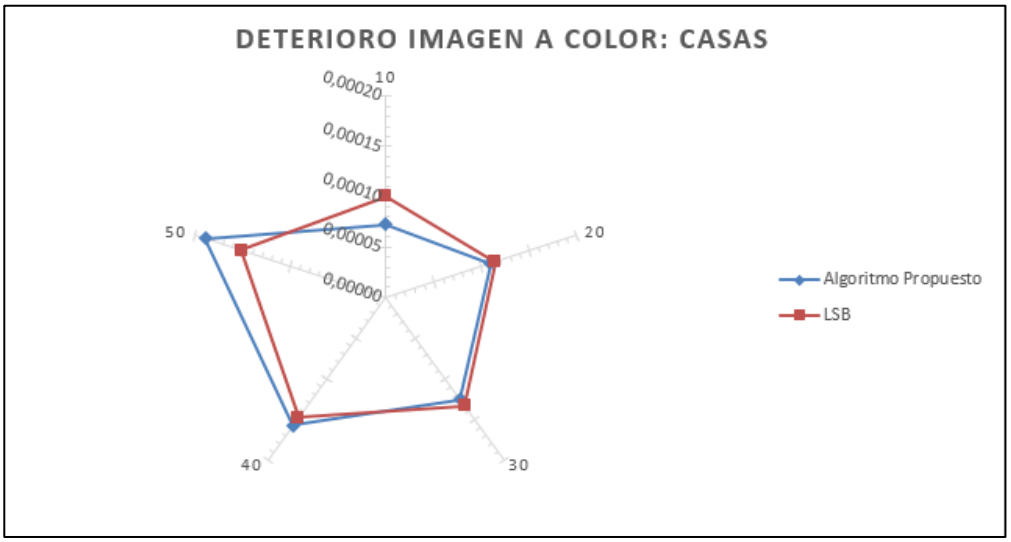


Figura 28

Deterioro de imagen a color representado con la métrica MSE.

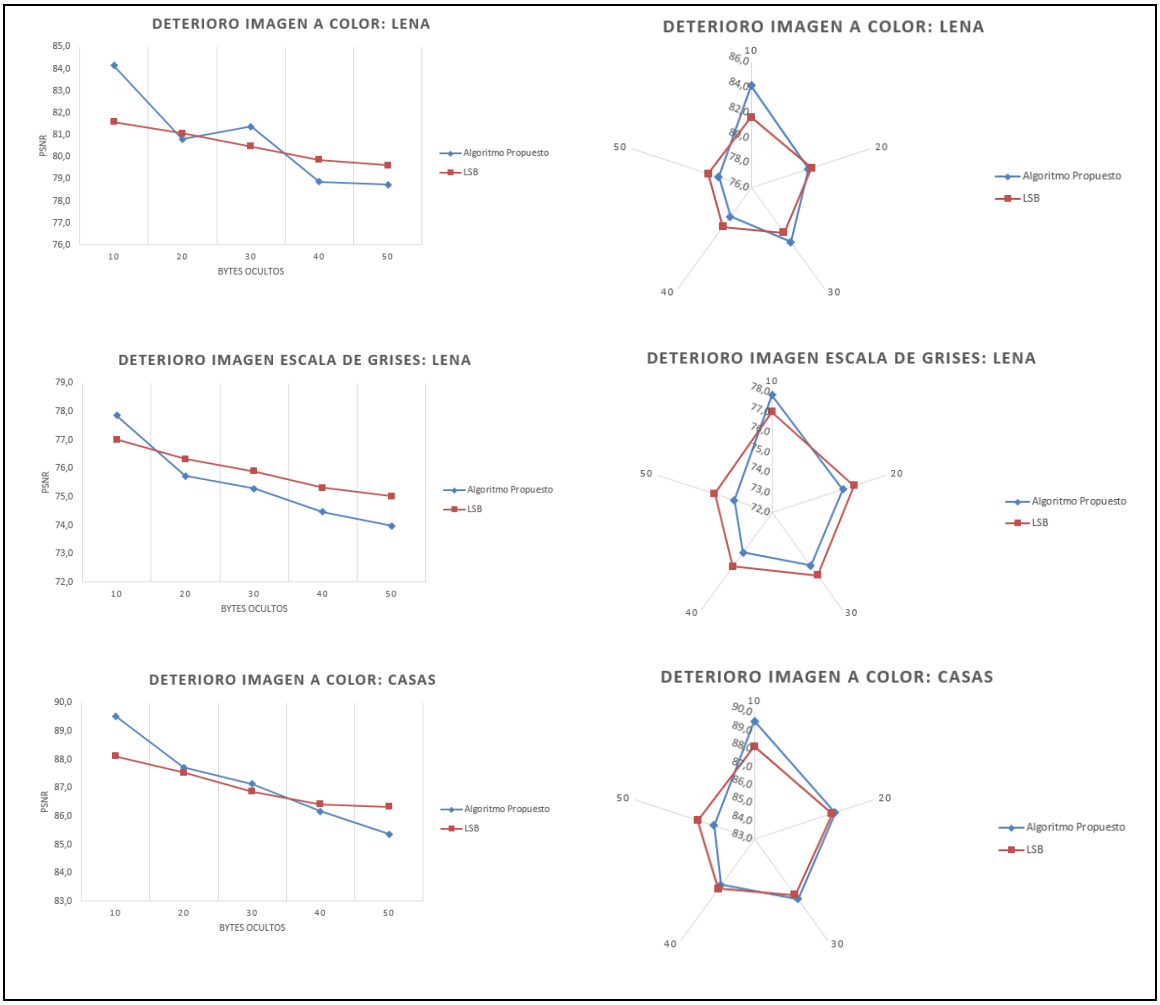


Cuando se analiza el comportamiento gráfico reflejado por los valores obtenidos por la evaluación de la métrica PSNR se nota claramente cómo representan, de forma invertida, los patrones observados al aplicar la evaluación de la métrica MSE como se puede ver en las Figuras 23 a 28. En esta escala no hay un ajuste logarítmico notable como se pudo observar en las Figuras 18 a 21.

Tras efectuar estos análisis se han observado mejoras de rendimiento bajo condiciones específicas lo que limita los usos prácticos del algoritmo y que aun así presentan nuevas posibilidades de mejora para el algoritmo. Aunque en ciertos casos las mejoras no sean tan sorprendentes, la simplicidad del algoritmo propuesto las vuelve valiosas puesto que puede ser fácilmente comprendido y por lo tanto mejorado y optimizado en futuros estudios sobre este tema.

Figura 29

Resultados métrica PSNR.



Capítulo IV: Conclusiones y Trabajos futuros

Tras haber realizado todo el proceso descrito por la metodología de investigación planteada y descrita en el Capítulo II, Figura 4, se han analizado los diferentes resultados obtenidos y por consiguiente se han sacado diversas conclusiones referentes con los objetivos planteados.

Conclusiones

OE1 Analizar la situación actual y las propuestas de la comunidad científica sobre los niveles de seguridad de los métodos esteganográficos disponibles mediante la revisión de la literatura sobre los niveles de seguridad de los métodos de seguridad disponibles.

La comunidad científica se encuentra trabajando constantemente en el desarrollo de nuevos algoritmos esteganográficos que mejoren su rendimiento, volviéndolos más seguros y difíciles de detectar. No obstante, la misma comunidad científica se dedica sin descanso a encontrar formas de vulnerar nuevas propuestas y métodos, desatando un círculo de mejora en ambas partes de la ecuación, tanto al ocultar información como al momento de vulnerarla.

Otra característica notable es la dependencia de fórmulas y métodos matemáticos complejos que permitan generar algoritmos más seguros, lo cual tiene sentido, pero hay que recordar que los recursos de hardware son limitados y que la seguridad informática debería ser accesible para todos los usuarios. Es así que dificultando la forma en la que trabajan ciertas propuestas, podría resultar más complicado que sean usados, por ejemplo, en sistemas embebidos o en dispositivos de bajos recursos de hardware.

OE2 Desarrollar un prototipo funcional mediante la implementación de un algoritmo esteganográfico seguro que evada los ataques comunes contra esteganogramas que usen la técnica LSB.

Los lenguajes de programación modernos facilitan mucho el desarrollo rápido de prototipos que pueden ser puestos a disposición de un público general en poco tiempo. En este caso, el desarrollo de una interfaz web y un servidor que llevara a cabo el proceso de ocultar o retirar información fue ejecutado en poco tiempo y de manera satisfactoria, pudiendo obtener un producto que demostrara cómo se puede utilizar un algoritmo esteganográfico de manera práctica e intuitiva.

Además, como se mencionó en el capítulo tercero, la mayoría de aplicaciones esteganográficas están disponibles al usuario de manera local, es decir, mediante la descarga del software. En caso de que un atacante pueda tener acceso al equipo, podrá, fácilmente, detectar que algoritmo ha usado para ocultar información, lo que elevará las sospechas de que en el equipo existen archivos esteganográficos, facilitando la vulneración de la confidencialidad de la información almacenada.

OE3 Validar el algoritmo propuesto mediante la utilización de los métodos de estegoanálisis estadísticos aplicados para vulnerar un esteganograma.

Como se demostró durante la evaluación del algoritmo propuesto durante las etapas finales del Capítulo III, el mismo presenta mejoras sobre el algoritmo LSB. No obstante, sus límites para ocultar información en imágenes lo vuelve una propuesta enfocada en casos de uso particulares. Es decir, en comparación con otros algoritmos, aquel que se ha propuesto en este trabajo estaría enfocado a guardar información crítica que no sea muy extensa. Por ejemplo, almacenar claves bancarias divididas en varias imágenes y entregadas a los responsables de cierto proceso, resultaría más seguro usando este método que el tradicional LSB. Adicional, por su sencillez, evitando cálculos matemáticos complejos y su facilidad para adaptarlo a un procesamiento en paralelo, lo vuelven un buen candidato para ser incorporado en sistemas embebidos que requieran ocultar información en archivos dentro de sus sistemas de

almacenamiento. Otra de las ventajas presentadas por este algoritmo, es la carencia de incorporar “rasgos” que lo identifiquen de forma sencilla como lo efectúan otros algoritmos. Estos “rasgos” son conocidos como firmas de método y pueden ir desde agregar información a la cabecera de un archivo, hasta agregar cadenas de caracteres únicas al final del mismo.

Trabajos futuros

Debido a los resultados que se han obtenido, el trabajo propuesto ha llegado a ser culminado con cierto grado de éxito. No obstante, queda espacio para mejorar. Es así que se ha planteado que en los trabajos futuros referentes a este tema se busque mejorar la capacidad del algoritmo, permitiendo ocultar más información en una imagen. Como se planteó en un principio la manera más óptima de ocultar información es buscando la coincidencia exacta de un byte de información en una imagen. Es por esto que una posible ruta a seguir sea la de incorporar un sistema de coordenadas personalizado que permita encontrar esta información y cambiar el paradigma de ocultar información a extraer datos de una imagen original, el principal objetivo sería almacenar este sistema de coordenadas en la imagen objetivo sin modificar más de lo necesario y sin dañar los datos que ya se han encontrado.

Bibliografía

Abood, M. H. (2017). An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms. *2017 Annual Conference on New Trends in Information and Communications Technology Applications, NTICT 2017*, 86–90. https://doi.org/10.1109/NTICT.2017.7976154

Alkhudhayr, F., Alfarraj, S., Aljameeli, B., & Elkhdiri, S. (2019). Information Security:A Review of Information Security Issues and Techniques. *2nd International Conference on Computer Applications and Information Security, ICCAIS 2019*, 1–6. https://doi.org/10.1109/CAIS.2019.8769504

Amankwa, E., Loock, M., & Kritzinger, E. (2014). A conceptual analysis of information security education, information security training and information security awareness definitions. *2014 9th International Conference for Internet Technology and Secured Transactions, ICITST 2014*, 248–252. https://doi.org/10.1109/ICITST.2014.7038814

Amirtharajan, R., Ramkrishnan, K., Vivek Krishna, M., Nandhini, J., & Balaguru Rayappan, J. B. (2012). Who decides hiding capacity? I, the pixel intensity. *Proceedings of the 2012 International Conference on Recent Advances in Computing and Software Systems, RACSS 2012*, 71–76. https://doi.org/10.1109/RACSS.2012.6212700

Ayala, W., Fuertes, W., Galarraga, F., Aules, H., & Toulkeridis, T. (2018). Software Application to Evaluate the Complexity Theory of the RSA and Elliptic Curves Asymmetric Algorithms. *Proceedings - 2017 International Conference on Software Security and Assurance, ICSSA 2017*, 87–93. https://doi.org/10.1109/ICSSA.2017.20

Bhuiyan, T., Sarower, A. H., Rashed Karim, M., & Maruf Hassan, M. (2019). An image steganography algorithm using LSB replacement through XOR substitution. *2019 International Conference on Information and Communications Technology, ICOIACT 2019*,

44–49. https://doi.org/10.1109/ICOIACT46704.2019.8938486

Çataltaş, Ö., & Tütüncü, K. (2017). Comparison of LSB image steganography technique in different color spaces. *IDAP 2017 - International Artificial Intelligence and Data Processing Symposium*. https://doi.org/10.1109/IDAP.2017.8090342

Chen, S., & Gong, G. Y. (2012). Study on internet traffic three-dimensional model. *Proceedings - 2012 International Conference on Control Engineering and Communication Technology, ICCECT 2012*, 741–746. https://doi.org/10.1109/ICCECT.2012.88

Devi, M., & Sharma, N. (2014). Improved detection of least Significant bit steganography algorithms in color and gray scale images. *2014 Recent Advances in Engineering and Computational Sciences, RAECS 2014*. https://doi.org/10.1109/RAECS.2014.6799507

Eaton, J. (1998). *About*. GNU Octave About. https://www.gnu.org/software/octave/about

Elkamchouchi, H., Salama, W. M., & Abouelseoud, Y. (2018). Data hiding in a digital cover image using chaotic maps and LSB technique. *Proceedings of ICCES 2017 12th International Conference on Computer Engineering and Systems*, *2018-Janua*, 198–203. https://doi.org/10.1109/ICCES.2017.8275302

FacebookInc. (2019). *Getting Started – React*. React Docs. https://reactjs.org/docs/getting-started.html

Gamba, L. (2020). *US claims Chinese hackers tried to steal COVID-19 data*. https://www.aa.com.tr/en/americas/us-claims-chinese-hackers-tried-to-steal-covid-19-data/1917970

Ghernouti-Hélie, S. (2010). A national strategy for an effective cybersecurity approach and culture. *ARES 2010 - 5th International Conference on Availability, Reliability, and Security*, 370–373. https://doi.org/10.1109/ARES.2010.119

Gonzáles, G. (2019, May 17). *Esto es Internet en 2019: 4.000 millones de usuarios, y páginas*

cuatro veces más pesadas que hace 10 años. https://www.genbeta.com/a-fondo/esto-internet-2019-4-000-millones-usuarios-paginas-cuatro-veces-pesadas-que-hace-10-anos

INTERPOL. (2020). *INTERPOL report shows alarming rate of cyberattacks during COVID-19*. Interpol. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19%0Ahttps://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19%0Ahttps://ww

JetBrains. (2020). *Ktor: Build Asynchronous Servers and Clients in Kotlin | Ktor Framework*. https://ktor.io/

Jie, A., Wu, S., & Zou, J. (2010). A new method for image information hiding based on image scrambling and LSB technology. *ICCASM 2010 - 2010 International Conference on Computer Application and System Modeling, Proceedings*, *4*. https://doi.org/10.1109/ICCASM.2010.5620600

Jois, A., & Tejaswini, L. (2016). Survey on LSB Data hiding techniques. *Proceedings of the 2016 IEEE International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2016*, 656–660. https://doi.org/10.1109/WiSPNET.2016.7566214

Jun, Z., Cox, I. J., & Doërr, G. (2007). Steganalysis for LSB matching in images with high-frequency noise. *2007 IEEE 9Th International Workshop on Multimedia Signal Processing, MMSP 2007 - Proceedings*, 385–388. https://doi.org/10.1109/MMSP.2007.4412897

Karampidis, K., Kavallieratou, E., & Papadourakis, G. (2018). A review of image steganalysis techniques for digital forensics. *Journal of Information Security and Applications*, *40*, 217–235. https://doi.org/10.1016/j.jisa.2018.04.005

Kitchenham, B. (2004). *Procedures for Performing Systematic Reviews*.

Knight, J. (2000). Steganalysis an Overview. *Style (DeKalb, IL)*, *Security 401*, 1–6.

Kriz, D. (2011). Cybersecurity principles for industry and government: A useful framework for efforts globally to improve cybersecurity. *2011 2nd Worldwide Cybersecurity Summit, WCS 2011*, 19–21.

Kuksov, I. (2019). *¿Qué es la esteganografía? | Blog oficial de Kaspersky*. https://www.kaspersky.es/blog/digital-steganography/18791/

Martínez, I., Fuertes, W., Palacios, M., Escudero, D., & Noboa, T. (2021). RSA Over-Encryption Employing RGB Channels through a Steganography Variant. *International Journal on Advanced Science, Engineering and Information Technology*, *11*(4), 1432. https://doi.org/10.18517/IJASEIT.11.4.13728

Martyn Shuttleworth. (2010, June 16). *Grupo de control científico*. https://explorable.com/es/grupo-de-control-cientifico

Morales, V., & Robalino-Lopez, A. (2020). Framework for the Evaluation of Internet Development. Case Study: Application of Internet Universality Indicators in Ecuador. *2020 7th International Conference on EDemocracy and EGovernment, ICEDEG 2020*, 291–296. https://doi.org/10.1109/ICEDEG48599.2020.9096781

Moyo, S., & Mnkandla, E. (2020). A Novel Lightweight Solo Software Development Methodology with Optimum Security Practices. *IEEE Access*, *8*, 33735–33747. https://doi.org/10.1109/ACCESS.2020.2971000

Nayak, D. K., & Bhagvati, C. (2013). A threshold-LSB based information hiding scheme using digital images. *Proceedings - 4th IEEE International Conference on Computer and Communication Technology, ICCCT 2013*, 269–272. https://doi.org/10.1109/ICCCT.2013.6749639

Nilizadeh, A., & Nilchi, A. R. N. (2016). A novel steganography method based on matrix pattern and LSB algorithms in RGB images. *1st Conference on Swarm Intelligence and Evolutionary*

Computation, CSIEC 2016 - Proceedings, 154–159. https://doi.org/10.1109/CSIEC.2016.7482107

Pau, G., Fuchs, F., Sklyar, O., Boutros, M., & Huber, W. (2010). EBImage-an R package for image processing with applications to cellular phenotypes. *Bioinformatics*, *26*(7), 979–981. https://doi.org/10.1093/BIOINFORMATICS/BTQ046

Qu, J., Song, Y., Wei, Y., & Song, J. (2018). Analysis of Data Hiding with Multi-bit Image Steganography. *Proceedings of 2018 IEEE 8th International Conference on Electronics Information and Emergency Communication, ICEIEC 2018*, 59–62. https://doi.org/10.1109/ICEIEC.2018.8473547

Salguero Dorokhin, É., Fuertes, W., & Lascano, E. (2019). On the Development of an Optimal Structure of Tree Parity Machine for the Establishment of a Cryptographic Key. *Security and Communication Networks*, *2019*. https://doi.org/10.1155/2019/8214681

Sugathan, S. (2017). An improved LSB embedding technique for image steganography. *Proceedings of the 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology, ICATccT 2016*, 609–612. https://doi.org/10.1109/ICATCCT.2016.7912072

Suryotrisongko, H., & Musashi, Y. (2019). Review of cybersecurity research topics, taxonomy and challenges: Interdisciplinary perspective. *Proceedings - 2019 IEEE 12th Conference on Service-Oriented Computing and Applications, SOCA 2019*, 162–167. https://doi.org/10.1109/SOCA.2019.00031

Thangadurai, K., & Sudha Devi, G. (2014, October 12). An analysis of LSB based image steganography techniques. *2014 International Conference on Computer Communication and Informatics: Ushering in Technologies of Tomorrow, Today, ICCCI 2014*. https://doi.org/10.1109/ICCCI.2014.6921751

University of Delaware. (2020). *Managing data confidentiality*. University of Delaware. https://www1.udel.edu/security/data/confidentiality.html

Vaidya, S. (2017). *OpenStego*. https://www.openstego.com/

Valandar, M. Y., Ayubi, P., & Barani, M. J. (2015, October 2). High secure digital image steganography based on 3D chaotic map. *2015 7th Conference on Information and Knowledge Technology, IKT 2015*. https://doi.org/10.1109/IKT.2015.7288810

Westfeld, A., & Pfitzmann, A. (2000). Attacks on steganographic systems breaking the steganographic utilities ezstego, jsteg, steganos, and s-tools–and some lessons learned. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *1768*, 61–76. https://doi.org/10.1007/10719724_5

Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity risks in a pandemic. In *Journal of Medical Internet Research* (Vol. 22, Issue 9, p. e23692). JMIR Publications Inc. https://doi.org/10.2196/23692

Wynn, M. G. (2016). *(PDF) Agile Processes and Methodologies: A Conceptual Study*. https://www.researchgate.net/publication/267706023_Agile_Processes_and_Methodologies_A_Conceptual_Study

Yang, W., Tang, S., Li, M., Cheng, Y., & Zhou, Z. (2017). Steganalysis of low embedding rates LSB speech based on histogram moments in frequency domain. *Chinese Journal of Electronics*, *26*(6), 1254–1260. https://doi.org/10.1049/cje.2017.09.026

Young, D. (2013). *Software development Methodologies - Brainvire*. https://www.researchgate.net/publication/255710396_Software_Development_Methodologies

Zhang, H. J., & Tang, H. J. (2007). A novel image steganography algorithm against statistical

analysis. *Proceedings of the Sixth International Conference on Machine Learning and Cybernetics, ICMLC 2007*, *7*, 3884–3888. https://doi.org/10.1109/ICMLC.2007.4370824