UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TITULO DEL TRABAJO DE TITULACIÓN

APLICACIÓN DE TÉCNICAS FORENSE, PARA VERIFICAR LA AUTENTICIDAD DE IMÁGENES USANDO ESTEGOANÁLISIS Y METADATOS.

AUTOR

Neira Alejandro, Jeancarlos Josue

PROYECTO DE INTEGRACIÓN CURRICULAR.

Previo a la obtención del grado académico en
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR

ING. LÍDICE HAZ LÓPEZ

Santa Elena, Ecuador

Año 2024

TRIBUNAL DE SUSTENTACIÓN

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Ing. José Sánchez Aquino, Mgt.
DIRECTOR DE LA CARRERA

Ing. Lidice Haz López, Mgt.
TUTOR

Ing. Jaime Orozco Iguasnia, Mgt.
DOCENTE ESPECIALISTA

Ing. Marjorie Coronel Suárez. Mgt.
DOCENTE GUÍA UIC

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por **NEIRA ALEJANDRO JEANCARLOS JOSUE**, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 03 días del mes de diciembre del año 2024

TUTOR

Firmado electrónicamente por:
LIDICE VICTORIA HAZ LOPEZ

ING. LÍDICE VICTORIA HAZ LÓPEZ, Msi.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Jeancarlos Josue Neira Alejandro**

DECLARO QUE:

El trabajo de Titulación, Aplicación de técnicas forense, para verificar la autenticidad de imágenes usando estegoanálisis y metadatos, previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 03 días del mes de diciembre del año 2024

EL AUTOR

Jeancarlos Josue Neira Alejandro

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado Aplicación de técnicas forense, para verificar la autenticidad de imágenes usando estegoanálisis y metadatos, presentado por el estudiante, **Jeancarlos Josue Neira Alejandro** fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 7%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.

TUTOR

LIDICE VICTORIA HAZ LOPEZ

ING. LÍDICE HAZ LÓPEZ

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **JEANCARLOS JOSUE NEIRA ALEJANDRO**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de artículo profesional de alto nivel con fines de difusión pública, dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, a los 03 días del mes de diciembre del año 2024

EL AUTOR

Jeancarlos Josue Neira Alejandro

AGRADECIMIENTO

Expreso mi mayor agradecimiento a todas las personas que me ayudaron de manera correcta en la realización de este proyecto.

En primer lugar, a mis padres y familia, llenos de paciencia y perseveración participes del camino que he recorrido en mi carrera. Con su apoyo, comprensión y amor que fue esencial para mantenerme enfocado en todo el transcurso.

a mi tutora Ing. Lídice Haz López, por su paciencia, ardua orientación y apoyo a lo largo de este gran proceso. Sus conocimientos y consejos fueron primordiales para dar forma adecuadamente a mi proyecto.

Por último, agradezco a todas las personas que se han involucrado directa o indirectamente con la cooperación de mi carrera, los cuales me proporcionaron seguridad para cada paso que daba en la institución.

Esta lucha y culminación no hubiera sido dable sin la ayuda de cada uno de ustedes. Gracias por todo.

Jeancarlos Josue, Neira Alejandro

DEDICATORIA

Dedico este trabajo a mi familia, amigos y a todas las personas que son mi motivo de inspiración y apoyo desde un inicio de la carrera

A mis padres, cuyo apoyo y amor fue inquebrantables en todo el trayecto de mi vida, su sacrificio me ha ofrecido las bases para alcanzar todas mis metas propuestas a lo largo de estos 4 años de esfuerzo. A ustedes les dedico este gran logro en mi vida con mucha gratitud y mucho cariño.

A mis amigos, mis hermanos de otra madre que me apoyaron con su empatía en este gran proceso, les agradezco por estar siempre a mi lado con su gran apoyo leal.

Este trabajo esta dedicado a cada uno de ustedes como muestra de mi agradecimiento y afecto.

Jeancarlos Josue, Neira Alejandro

ÍNDICE GENERAL

Contenido

INDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El proyecto se centra en el desarrollo de una aplicación móvil forense diseñada para verificar la autenticidad e integridad de imágenes digitales en formato JPEG/JPG. La aplicación combina tres técnicas principales: estegoanálisis, análisis de nivel de error (ELA) y la extracción de metadatos. Mediante el uso de algoritmos especializados como LSB y Chi-cuadrado, se detectan manipulaciones y datos ocultos en las imágenes. El análisis de nivel de error permite visualizar alteraciones evidentes, mientras que la extracción de metadatos proporciona información adicional como el dispositivo utilizado y la fecha de creación. La aplicación sigue un modelo incremental, incorporando funcionalidades clave como la carga de imágenes, análisis estegoanalítico y generación de reportes detallados. Los resultados obtenidos de las pruebas confirman la eficacia de la herramienta enfrentándose con imágenes esteganográficas, siendo esta una solución forense que contribuye en los resultados de una investigación pericial, jurídica y auditorias.

Palabras clave: Estegoanálisis, Metadatos, Autenticidad.

ABSTRACT

The project focuses on the development of a forensic mobile application designed to verify the authenticity and integrity of digital images in JPEG/JPG format. The application combines three main techniques: steganalysis, error level analysis (ELA) and metadata extraction. Using specialized algorithms such as LSB and Chi-square, manipulations and hidden data in images are detected. Error level analysis allows to visualize obvious alterations, while metadata extraction provides additional information such as the device used and the creation date. The application follows an incremental model, incorporating key functionalities such as image upload, steganalytic analysis and generation of detailed reports. The results obtained from the tests confirm the effectiveness of the tool when dealing with steganographic images, making this a forensic solution that contributes to the results of expert investigations, legal investigations y audits.

Keywords: Steganalysis, Metadata, Authenticity.

INTRODUCCIÓN

En la actualidad, la autenticidad de las imágenes digitales se ha convertido en un aspecto crucial debido al aumento de manipulaciones y falsificaciones en el ámbito digital. En este contexto, el proyecto "Aplicación de Técnicas Forenses para Verificar la Autenticidad de Imágenes Usando Estegoanálisis y Metadatos" podría considerarse como una contribución significativa a la informática forense. Este enfoque busca proporcionar una herramienta especializada para evaluar la integridad de las imágenes digitales, lo cual es vital en áreas como investigaciones legales, auditorías digitales y ciberseguridad.

Las imágenes digitales, además de ser ampliamente utilizadas, poseen características que las convierten en un medio ideal para el ocultamiento de datos, donde los métodos de incrustación y detección juegan un papel crucial. Este proyecto emplea técnicas como el estegoanálisis (LSB y Chi-cuadrado), el análisis de nivel de error (ELA) y la extracción de metadatos para identificar alteraciones y detectar datos ocultos en formatos JPEG/JPG.

El propósito principal es desarrollar una aplicación móvil que, mediante la integración de estas técnicas forenses, permita analizar imágenes de manera intuitiva y eficiente. Siguiendo una metodología incremental, se garantiza que cada fase del desarrollo se enfoque en implementar funcionalidades clave que aseguren resultados precisos y confiables.

Este proyecto busca fortalecer la confianza en los análisis periciales y contribuir a la promoción de una cultura de seguridad digital, ofreciendo una solución accesible y adaptada a los desafíos de un mundo donde la manipulación de imágenes es cada vez más frecuente.

El presente informe se presenta de la siguiente manera:

El capítulo I, presenta los antecedentes, descripción del proyecto, justificación, alcance y la metodología del proyecto.

El capítulo II de la propuesta, contiene el marco contextual, marco teorico, marco conceptual y el marco legal

El capítulo III abarca el análisis de requerimientos, el diseño de la propuesta, desarrollo y prueba.

Finalmente tenemos las conclusiones, recomendaciones las bibliografías y anexos.

CAPÍTULO 1. FUNDAMENTACIÓN

1.1 Antecedentes

En la era actual, la tecnología se ha convertido en un aspecto clave de todos los días. El acceso a internet ha dado lugar a una amplia gama de áreas, desde la comunicación hasta la educación o el entretenimiento, pero también el uso de las nuevas tecnologías que van saliendo a la luz, con el transcurso de los años la tecnología ha llevado a la aparición de nuevas amenazas en línea como el espionaje digital o el robo de información confidencial. [1]

En lo que cabe la historia, la esteganografía data de los años 474 A.C. la cual tiene una importancia en la actualidad, es un conjunto de métodos y técnicas para pasar desapercibidos o camuflar mensajes en una imagen, video o audio, está relacionada un poco con la criptografía, la cual es una técnica de cifrado o codificado dejando los mensajes ininteligibles, pero la técnica de esteganografía trata de ocultar el envío de datos dentro de un portador que aparenta no estar alterado de ninguna manera y que tenga una apariencia normal, sin ser necesario cifrar el mensaje. [2]

En la red o en el internet existen intercambio de datos como lo es la pornografía infantil, esta es un delito extremadamente grave, y muchos otros delitos también pueden llevarse a cabo en el mundo del internet. Existen investigadores especializados que están trabajando arduamente para indagar, detener y procesar a los responsables de transmitir este tipo de contenido, el cual a menudo se oculta utilizando técnicas como la esteganografía, que puede ser empleada tanto para fines legítimos como ilegales, se estima que hay aproximadamente 400 páginas o herramientas de acceso libre en la internet que utilizan esteganografía, y muchas de ellas son empleadas para el tráfico de imágenes que pueden ocultar información sensible o dañina. [3]

La seguridad en el envío de información a través de canales de comunicación inseguros es fundamental para reducir la vulnerabilidad frente a posibles ataques cibernéticos, esto incluye hackeos o tráfico de información prohibida [4]. La esteganografía oculta información dentro de varios tipos de medios multimedia como documentos, audios, imágenes, videos, entre otros, es una herramienta útil en este contexto, sin embargo, también existen métodos como es el estegoanálisis, la cual permiten detectar la presencia de mensajes ocultos en estos medios que estén utilizando técnicas de esteganografía [4].

Un sistema esteganográfico se considera comprometido cuando se logra identificar la existencia de información oculta en imágenes u otros archivos multimedia, lo que evidencia una brecha en su seguridad. [5]

La investigación realizada por [6], el cual tiene como objetivo ocultar la información en las zonas más difíciles de modelar de la imagen. La problemática del proyecto se presenta cuando se desea ocultar información únicamente en unas zonas concretas de la imagen, es cómo comunicar al receptor del mensaje (de la imagen) en qué zonas debe leer y en qué zonas no. Si se desarrolla un procedimiento para identificar las zonas ruidosas, estas pueden cambiar (dejar de ser ruidosas) al ocultar información, por lo que el receptor puede acabar leyendo en zonas donde no hay mensaje e ignorando zonas donde sí lo había. El método propuesto usa cada pareja que supera el umbral para ocultar un bit. Concretamente se oculta alterando el píxel de la izquierda, es decir, el etiquetado como a de la pareja (ab). Para ello, se usa el LSB de a como bit de información, dejándolo tal y como está si su valor es igual al del bit del mensaje que se quiere ocultar y modificándolo si su valor no coincide.

Los experimentos se han diseñado para verificar que, marcando con umbrales superiores a los establecidos por las herramientas de estegoanálisis, el método presentado no se detecta. A continuación, se muestra una comparativa de imágenes con diferentes zonas ruidosas para la ocultación de información [6]:

Figura 1: Imagen lemma a escala grises

Figura 2: Imagen lemma, zonas de ocultación 1

Figura 3: Imagen lemma, zona de mejor ocultación

Por otro lado, el proyecto [7], indica que un portador imagen puede ser utilizado para ocultar, a la vista de intrusos, cualquier mensaje u objeto software (archivo), codificándolo con sutiles cambios en los colores de los píxeles (sus componentes RGB) que no pueden ser percibidos por el ojo humano; de tal forma que el Portador que contiene el mensaje, o "Estegoportador". El objetivo de este proyecto es exponer la implementación de la técnica esteganográfica de Sustitución LSB 1 bits desarrollado en Matlab, haciendo uso de herramientas disponibles para el procesamiento de 1LSB: Least Significant Bit imágenes. El que resulta ser de bastante utilidad a los fines de desarrollar una herramienta de Esteganografía aplicada.

Por último, el proyecto [8], explica que el creciente y abrumante avance de la tecnología de redes y dispositivos digitales interconectados como smartphones, hacen que la evidencia o rastro digital juegue un papel importante en los procesos legales en la última década, el objetivo es implementar los algoritmos estegoanalíticos y de análisis de nivel de error (ELA) mediante el uso de herramientas open source de informática forense que

permitan garantizar la integridad de los archivos de imágenes. Este proyecto evaluará la manipulación digital de los archivos de imágenes y determina la integridad de los mismos, utilizando como metodología de mejores prácticas en el examen forense de tecnología digital (ver figura 4). Los resultados obtenidos fue la incrustación exitosa sin afectar su apariencia visual de la imagen original, compresión de datos al examinar la metadata y la variación del hash por la incrustación.

Figura 4: Procedimiento técnico de la metodología forense [8]

Por todo lo expuesto anteriormente, se propone el desarrollo de una aplicación móvil forense, capaz de verificar la autenticidad de imágenes, usando una técnica de estegoanálisis, análisis de nivel de error (ELA) y metadatos. Este software utiliza métodos accesibles y eficientes para la detección de manipulación digital, permitiendo la identificación de posibles alteraciones en imágenes. Además, se verifica la autenticidad de las imágenes a través de la validación y consistencia de los metadatos. El objetivo es proporcionar una herramienta de computación forense para profesionales e investigadores en el campo de la ciberseguridad.

1.2 Descripción del Proyecto

El proyecto se centra en el desarrollo de una aplicación móvil de técnicas forenses, para verificar la autenticidad de imágenes usando estegoanálisis, ELA y metadatos. El objetivo principal es una aplicación exclusiva para dispositivos Android que aplique la técnica estegoanalíticas como, chi-cuadrado ELA y metadatos.

El método chi-cuadrado es un algoritmo aplicado sobre imágenes en la que se haya aplicado algoritmos esteganográfico que modifican el bit menos significativo (LSB) en [37] podremos apreciar mejor el concepto. Al modificarse una imagen en los LSB y ser escaneado por chi-cuadrado podemos esperar que cada par de valores sea diferente ya que si una imagen sin modificaciones tendría que tener una pila de valores de bits más frecuente y "estable". [9]

Por otro lado, la técnica ELA es una técnica forense es usada para la detección de manipulaciones o esteganografía en imágenes como JPG/JPEG, formato más común en dispositivo móviles y que son el formato automático al realizar una fotografía, además de la comparación de los metadatos de las imágenes para una mayor credibilidad de las imágenes analizadas por la aplicación.

El método de análisis de nivel de error ELA [10] identifica las áreas de una imagen que haya sido modificada o alterada, ya que las compresiones no uniformes en una imagen modificada revelan inconsistencias que en el análisis se puede detectar. Además del método ELA en la aplicación forense, se integra un analizador de los metadatos de imágenes para la verificación de cualquier inconsistencia o cambio no autorizado que puedan comprometer la integridad de las imágenes receptadas.

La aplicación está diseñada para ser utilizada por profesionales, como personal en el área de peritaje informático y otras ramas relacionadas con la ciberseguridad y análisis forense digital. Sin embargo, también se busca que sea accesible para usuarios comunes o personas interesadas en verificar la autenticidad de imágenes digitales en situaciones cotidianas. De esta manera, se ofrecerá una herramienta versátil que podrá emplearse tanto en contextos profesionales como por el público en general, ampliando su alcance y utilidad.

El proyecto seguirá una metodología incremental, la cual permite el desarrollo de software en fases, permite asegurar la entrega de versiones funcionales en cada incremento. De igual forma facilitará la implementación y pruebas del método estegoanalíticos, también añadiendo una técnica de extracción de metadatos para una investigación más exhaustiva de la imagen para aumentar la integridad y veracidad de ella.

1.1 Objetivos del Proyecto

1.1.1 Objetivo General

Desarrollar una aplicación forense que combine técnicas de estegoanálisis y validación de metadatos para verificar la integridad y autenticidad de imágenes en formato JPG/JPEG

1.1.2 Objetivos Específicos

- Analizar los metadatos en la aplicación móvil, para verificar imágenes JPEG/JPG.
- Desarrollar un sistema de validación de metadatos, diseñado exclusivamente para verificar la autenticidad de imágenes en formato JPEG/JPG.
- Implementar un algoritmo de estegoanálisis para detectar las manipulaciones y ocultamientos en imágenes.
- Validar la efectividad y precisión de la aplicación mediante pruebas exhaustivas con conjuntos de datos específicos de imágenes.

1.3 Justificación

En la actualidad, el creciente uso de los dispositivos móviles y de las redes sociales han facilitado la creación, manipulación y distribución de imágenes digitales, debido a este incremento de uso de las tecnologías y métodos que se usan para la ocultación de información, lo cual da paso también al riesgo de alteraciones fraudulentas en fotografías, que pueden usarse con fines ilícitos, como por ejemplo: la distribución de contenido falsos o la manipulación de pruebas en investigaciones donde se tenga como evidencia los archivos de imagen [1]. Ante este escenario, la necesidad de herramientas forenses avanzadas para la verificación de la integridad de las imágenes es crucial, en especial en

dispositivos móviles, cuyo caso es donde se almacena y procesa gran cantidad de contenido visual. La tecnología de estegoanálisis y el análisis de nivel de error (ELA) han demostrado ser técnicas eficientes para detectar la manipulación oculta en imágenes, así proporcionando un mecanismo robusto para garantizar la autenticidad de las mismas [11].

La fiabilidad de las imágenes en un proceso judicial, juegan un papel muy importante. La integridad de estas imágenes proporciona una base sólida para la toma de decisiones judiciales, ya que de alguna manera se puede confiar en que la evidencia es exacta y que no haya sido manipulada de manera fraudulenta en el transcurso de la o las investigaciones. Asimismo, la confianza en los resultados de la investigación, al mantener la integridad de las imágenes, se genera confianza en los resultados de la investigación forense sobre esteganografía en ellas. Los informes y conclusiones basados en evidencia visual confiable y que no sea manipulada tiende a tener un mayor grado de credibilidad y pueden influir vastamente en el transcurso de la investigación o en el proceso judicial legal [8].

Al pasar una imagen por varios métodos estegoanalíticos se podrá verificar que la imagen mantenga la integridad de sí misma, asi podríamos obtener varios beneficios, como garantizar la autenticidad de imágenes compartidas en redes sociales o medios digitales donde se transmita una gran cantidad de imágenes. Otro beneficio es la detección o identificación de imágenes malintencionadas que tengan como fin dañar al usuario o causar otro mal como el tráfico de información confidencial.

De igual manera beneficia a la integridad de la cadena de custodia, tanto que el registro de la evidencia muestra a todas las personas que han tenido acceso a ella, y de las acciones realizadas sobre ella. Al garantizar la integridad de la imagen de igual forma se conserva la integridad de la cadena de custodia, lo que fortalece la validez legal de la evidencia y evita la pérdida o alteración accidental de los datos de una imagen como prueba implementando un hash único para cada archivo imagen.

Mayormente las herramientas o software que usualmente se usan para el análisis esteganográfico requieren de un dispositivo de escritorio o laptop, algunas herramientas requieren un sistema operativo diferente como el Linux para el análisis de imágenes o métodos estegoanalíticos, los cuales, si bien son muy útiles en el área forense o de investigaciones, suelen ocupar mucho espacio o pueden no ser muy prácticos en

diferentes entornos donde la movilidad es crucial. Los dispositivos móviles aparte de ser portátiles y de un peso ligero, ofrecen una ventaja de estar siempre al alcance del usuario, facilitando así el acceso de inmediato a herramientas que desee usar el investigador.

Esto convierte a los teléfonos o tabletas que son de fácil traslado en plataformas ideales para la implementación de una aplicación forense, que permitirá realizar análisis estegoanalíticos directamente desde un dispositivo móvil, eliminando la dependencia de equipos de gran tamaño y dando así una mejor accesibilidad a herramientas para investigaciones.

El desarrollo de una aplicación forense de este tipo es fundamental para minimizar delitos graves como el espionaje y la fuga de información confidencial. A través de técnicas como el estegoanálisis, es posible que se pueda identificar el mal uso de las imágenes para la ocultación de datos sensibles, que de otra manera pasarán desapercibidos. Esto resulta particularmente relevante en entornos corporativos gubernamentales, donde la filtración de información podría tener consecuencias devastadoras. Al poder detectar estos actos de manera temprana, la aplicación no solo protege la integridad de los archivos JPG/JPEG sino que también contribuye a la seguridad de la información, evitando daños a futuro a organizaciones o individuos.

El proyecto "aplicación de técnicas forense, para verificar la autenticidad de imágenes usando estegoanálisis y metadatos" se alinea al Plan de creación de oportunidades, según el eje del objetivo:

Objetivo 10.- Garantizar la soberanía nacional, integridad territorial y seguridad del Estado [12].

Política 10.1. - Fortalecer al estado para mantener la confidencialidad, integridad y disponibilidad de información frente a amenazas provenientes de ciberespacio y proteger su infraestructura critica [12].

1.4 Alcance

El presente proyecto se enfoca en verificar la integridad de las imágenes digitales mediante el uso de una técnica estegoanalítica, técnica ELA y análisis de metadatos. La metodología empleada de incremento seguirá las fases claves: análisis, diseño, codificación y prueba dentro de cada incremento.

El proyecto abarca el desarrollo de una aplicación móvil forense que analiza las imágenes en formatos JPG y JPEG, los más comunes para la distribución de imágenes en redes sociales y plataformas digitales.

Incremento 1: Página de registro de usuarios

- Objetivo: Establecer una base sólida para la gestión de usuarios.
- Detalles:
    - Crear una pantalla para que los usuarios puedan registrarse e iniciar sesión.
    - Implementar roles de usuario, como administrador y usuario regular.
    - Incorporar una funcionalidad de inicio de sesión persistente para evitar autenticaciones repetitivas.

Incremento 2: Página de investigaciones

- Objetivo: Ofrecer un espacio organizado para gestionar casos de análisis.
- Detalles:
    - Crear una sección para ver opciones como crear nuevos casos, editar casos existentes, y acceder a información sobre esteganografía y estegoanálisis.
    - En la página de editar casos, listar los casos iniciados con opciones para eliminarlos o ver los casos finalizados.

Incremento 3: Página de añadir imágenes

- Objetivo: Incorporar una funcionalidad para el manejo y almacenamiento de imágenes relacionadas con los casos.
- Detalles:
    - Habilitar la carga de imágenes desde el dispositivo del usuario.
    - Almacenar las imágenes en Firebase y guardar datos relevantes (URL, hash, metadatos, ID del usuario) en la base de datos.
    - Mostrar las imágenes subidas por el usuario, organizadas según el caso de investigación.

Incremento 4: Página de estegoanálisis

- Objetivo: Analizar imágenes en busca de datos ocultos.

- Detalles:
    - Permitir al usuario seleccionar una imagen para detectar esteganografía.
    - Implementar un botón de "Analizar Imagen" que indique el porcentaje de detección de esteganografía y genere un gráfico de líneas.
    - Añadir un botón para generar reportes del análisis chi-cuadrado.

Incremento 5: Página de análisis ELA

- Objetivo: Detectar manipulaciones en imágenes mediante ELA.
- Detalles:
    - Diseñar una sección que permita seleccionar una imagen y aplicar ELA.
    - Mostrar la imagen original y la imagen filtrada lado a lado, resaltando posibles alteraciones.
    - Indicar el porcentaje de manipulación de la imagen.
    - Incorporar un botón para generar reportes del análisis.

Incremento 6: Página de metadatos

- Objetivo: Extraer y visualizar los metadatos de las imágenes.
- Detalles:
    - Permitir al usuario seleccionar una imagen y extraer sus metadatos.
    - Mostrar los resultados en una tabla sencilla de interpretar.
    - Añadir un botón para generar reportes de los metadatos.

Incremento 7: Página de reportes de investigación

- Objetivo: Centralizar los resultados y reportes generados durante la investigación.
- Detalles:
    - Diseñar una página para que los usuarios puedan visualizar reportes completos de las investigaciones realizadas.

1.5 Metodología de Investigación

1.5.1 Diseño de la Investigación

Por la poca información que se llega a obtener sobre la aplicación del análisis de nivel de error (ELA) para la verificación de la integridad de imágenes en dispositivos móviles, se

optó por usar la metodología de investigación exploratoria [13]. A partir de la revisión de estudios y proyectos relacionados con el proyecto propuesto, se identificó patrones y características claves, lo que llevó a comparaciones tanto similitudes y diferencias. Esta revisión proporcionaría una base sólida para el desarrollo y la implementación de soluciones adaptadas al contexto móvil y verificación de imágenes.

Algunas propuestas relacionadas al proyecto son, el tema proveniente de Colombia titulado "aplicación de la técnica error level analysis y metadatos para el estudio forense de imágenes producidas por dispositivos móviles" [14] que muestra una vista más cercana a lo que es el proyecto a diferencia que no desarrolla una aplicación móvil en sí. Otro proyecto relacionado es "Análisis de la integridad de imágenes usando métodos estegoanalíticos y análisis de nivel de error ELA" [8] cuyo proyecto podría ser guía para el buen uso de la técnica ELA.

Además de la metodología exploratoria se empleará la metodología descriptiva [15]. Este enfoque permitirá describir minuciosamente las técnicas utilizadas para el análisis de imágenes, la metodología se centra en aspectos como el porcentaje del grupo objetivo que utiliza la marca en una ubicación concreta o la característica de las personas que utilizan un servicio concreto [16]. Como el proyecto se centra en un tipo de imágenes específica, va a especificar cómo es el análisis de esta.

1.5.2 Variables del Estudio

Se pretende encontrar las imágenes con esteganografía utilizando la metodología incremental para garantizar el óptimo desarrollo de la aplicación.

Variable independiente: integración de técnicas estegoanalíticas, ELA y metadatos.

Variable dependiente: verificación de la autenticidad de las imágenes (JPG/JPEG).

1.5.3 Hipótesis

La aplicación de técnicas basadas en estegoanálisis, ELA y análisis de metadatos permite verificar de manera efectiva la autenticidad de las imágenes digitales, mejorando la precisión en la detección de manipulaciones.

1.5.4 Población y Muestra

La población objeto del estudio se tomó de la Universidad Estatal Península de Santa Elena, en el periodo académico 2024-2. Específicamente en la facultad de Sistemas y Telecomunicaciones, 5to semestre y 4to semestre para poder obtener información sobre el conocimiento de las técnicas y métodos esteganográfico.

Semestre	Estudiantes
4to	**31**
5to	**25**
total	**56**

Tabla 1: Estudiantes por semestre.

Rango de edad	Estudiantes		Total
	Femenino	**Masculino**	
18-30	6	8	**14**
31-40	0	3	**3**
Total	6	11	**17**

Tabla 2: Número de estudiantes intervenidos para la encuesta

1.5.5 Recolección y procesamiento de información

1.5.5.1 Técnicas y Herramientas de Recolección de Información

En este apartado se detallará de manera puntuada las técnicas e instrumentos para la recolección de información que sé utilizaran para la realización de este proyecto.

Técnica: Fuentes bibliográficas, estado del arte, encuestas.

Instrumentos: El cuestionario de preguntas es dirigida a un grupo de estudiantes de la facultad de Sistemas y Telecomunicaciones de la universidad Estatal Península de Santa Elena. El cuestionario se utiliza para poder comprender a fondo el panorama actual y

conocimiento en relación al tema investigado. Y así poder asegurar que la investigación se base en una comprensión sólida y actualizada de las prácticas en el uso de la tecnología relevantes. Por otra parte, se usan bases de datos indexadas como Google Schoolar para acceder a recursos bibliográficos que sirven como guía y análisis con relación a la problemática tratada en esta investigación.

1.5.5.2 Procesamiento de la Información

En este trabajo se presentan gráficos estadísticos descriptivos que reflejan las respuestas de cada pregunta planteada en la encuesta aplicada a los estudiantes antes mencionados (ver Anexo 1). Los resultados obtenidos se analizarán detalladamente para proporcionar una visión clara y precisa de los hallazgos de esta investigación, facilitando la comprensión de los patrones y tendencias observados.

1.6 Metodología del Proyecto

Para llevar a cabo un desarrollo de un software es esencial seguir con un método que pueda guiar al del proyecto desarrollo de una aplicación móvil de técnicas forenses, para verificar la autenticidad de imágenes usando estegoanálisis y metadatos. El método que se escogió es el método incremental.

El modelo incremental combina la forma secuencial e iterativo a través de prototipos funcionales, es decir, cada evolución del proyecto se considera un incremento. El primer incremento contiene elementos básicos del proyecto, hasta seguir con los siguientes incrementos para mejorar la funcionalidad, priorizando los requerimientos más importantes [17].

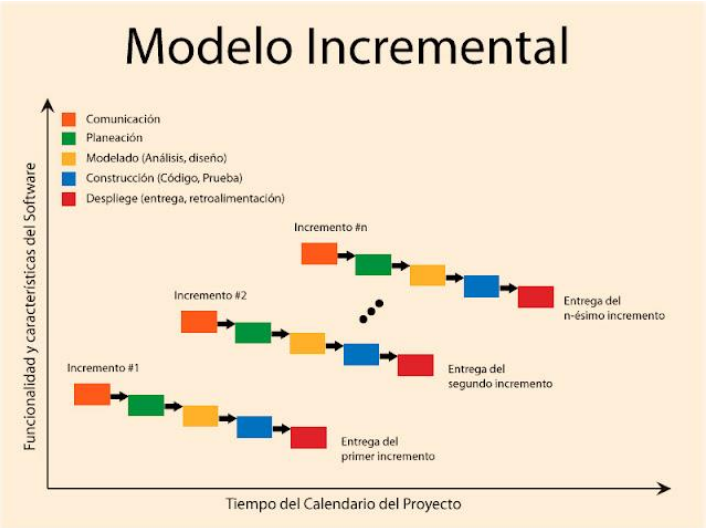


Figura 5: Modelo Incremental [18]

Los incrementos realizados en este proyecto son:

Incremento 1

- Página de registro de usuarios

Incremento 2

- Página de registro de investigaciones

Incremento 3

- Página de imágenes

Incremento 4

- Página de estegoanálisis

Incremento 5

- Página de análisis ELA

Incremento 6

- Página de metadatos

Incremento 7

- Página de reporte de investigación

CAPÍTULO 2. MARCO REFERENCIAL

2.1 Marco Contextual

2.1.1 La evolución de la ciberseguridad y la importancia de la autenticidad digital.

El desarrollo de la tecnología, especialmente la expansión de las redes y el internet, ha generado la necesidad de proteger los entornos digitales, tanto en dispositivos de escritorios como portátiles. Desde la creación de ARPANET y la adopción del protocolo TCP/IP la creciente conectividad ha facilitado el intercambio masivo de información pero también ha expuesto las redes a vulnerabilidades y ataques y en respuesta a estos riesgos la ciberseguridad ha emergido como una disciplina esencial dedicada a proteger los sistemas y datos frente a amenazas en un mundo cada vez más interconectado siendo un hito importante en este ámbito el desarrollo de Reaper considerado el primer programa antivirus que fue diseñado como una versión mejorada de autorreplicación del programa Creeper el cual es reconocido como el primer virus informático del mundo y que se movía a través de ARPANET eliminando las copias de Creeper marcando así el inicio de la lucha contra el malware en la historia de la informática. [19]

2.1.2 Principales amenazas a la autenticidad de las imágenes en el entorno digital.

En el entorno digital, las imágenes son vulnerables a diversas amenazas que pueden comprometer su autenticidad. Entre las principales amenazas que se puede realizar en imágenes encontramos la manipulación mediante software de edición, las alteraciones de metadatos y la inserción de datos ocultos a través de técnicas esteganográficas [20]. Estas acciones no solo afectan a la integridad de las imágenes, sino que también pueden usarse para fines ilícitos como la falsificación de pruebas la difusión de desinformación o la ocultación de actividades delictivas ya que la facilidad con la que se pueden modificar las imágenes plantea un desafío considerable para garantizar la veracidad en contextos judiciales y de investigación. [21]

2.1.3 Rol de la informática forense en la verificación de la autenticidad de imágenes.

La creciente sofisticación de técnicas de manipulación plantea una amenaza importante para la integridad de las imágenes digitales, especialmente en ámbitos sensibles como la justicia y la seguridad. En un contexto judicial, como por ejemplo la autenticidad de las

imágenes presentadas como evidencia es fundamental para garantizar un proceso justo. Si la imagen ha sido adulterada, la credibilidad de la evidencia se ve gravemente comprometida, lo que esto podría afectar a las decisiones importantes en casos judiciales. [22]

Uno de los ejemplos que se podría poner como prueba para identificar algún delito informático es la de investigaciones relacionadas con la pedofilia, pornografía y abuso infantil. Ya que se encuentran como evidencia: agendas con direcciones, conversaciones virtuales, software de edición de imágenes, software de conectividad con cámaras digitales, imágenes, videos, software de juegos, historia de navegación de browsers y metadatos de directorios e imágenes. [23]

2.1.4 Importancia del estegoanálisis en la autenticidad de imágenes.

Uno de los métodos más eficientes en el análisis forense de imágenes es el estegoanálisis, que se enfoca en detectar la información oculta dentro de las imágenes a través de técnicas de esteganografía, o detecta si tiene algún tipo de modificación dentro de la imagen, sea en los pixeles o metadatos. El esteganálisis permite identificar patrones anómalos en los datos de la imagen que indican la presencia de mensajes ocultos o modificaciones encubiertas dado que la esteganografía puede ser utilizada para ocultar información maliciosa malintencionada o sensible por lo que la aplicación de técnicas de estegoanálisis es crucial para asegurar que las imágenes no hayan sido manipuladas con propósitos ilegales en este contexto la capacidad de detectar información oculta en una imagen resulta fundamental para mantener la integridad de la misma en entornos donde la seguridad de la información es prioridad tanto en empresas grandes como en empresas pequeñas. [24]

2.1.5 Importancia de la autenticidad de los metadatos en las imágenes

Los metadatos juegan un papel esencial en la autenticación de imágenes. Son la información asociada a un archivo de imagen, que incluye detalles como la fecha de creación, dispositivos con el que fue capturada la imagen, la ubicación geográfica, entre otros tipos de datos. Los datos contenidos en las imágenes permiten rastrear su origen y detectar posibles modificaciones dado que la manipulación o eliminación de los metadatos puede ser un indicio claro de alteraciones o modificaciones en la imagen por lo cual el análisis de los metadatos constituye una herramienta esencial para la

autenticación de archivos además el uso adecuado de los metadatos no solo facilita la verificación de la integridad del archivo sino que también permite contextualizar la imagen en su entorno original lo que resulta particularmente útil en el ámbito de investigaciones forenses y auditorías de seguridad. [25]

2.1.6 Área donde puede ser utilizada el aplicativo.

Investigaciones forenses y judiciales: la autenticidad de las imágenes es fundamental en la presentación de pruebas digitales en un juicio. El aplicativo permitiría verificar si las imágenes presentadas como evidencia haya sido alteradas o manipuladas.

Ciberseguridad: en este campo, el análisis forense de imágenes es vital para detectar actividades delictivas como espionaje, filtraciones de información., o las manipulaciones de imágenes con fines desinformativo.

Medios de comunicación y redes sociales: las imágenes compartidas a través de plataformas sociales y medios digitales son frecuentemente manipuladas. El aplicativo puede ser usada para poder verificar la autenticidad de fotografías que circulan en estos entornos.

Áreas de auditoria: las auditorias digitales requieren la verificación de la autenticidad de diversos documentos e imágenes. La aplicación podría ser empleado para garantizar que las imágenes usadas en procesos de auditoria no hayan sido alteradas, mejorando la transparencia y la confianza en los procesos.

Periodismo de investigación: los periodistas usan el aplicativo para validar la autenticidad de las imágenes que publican, especialmente en casos sensibles donde las fotos pueden ser manipuladas con fines engañosos. Esto podría ayudar a proteger la integridad de la información y aumentar la credibilidad de los reportajes.

2.2 Marco Teórico

2.2.1 Integración de estegoanálisis y metadatos

La integración de técnicas de estegoanálisis y análisis de metadatos constituye una metodología avanzada y robusta para garantizar la autenticidad y la integridad de las imágenes digitales. El estegoanálisis se especializa en la detección de alteraciones ocultas en el contenido visual de las imágenes, como mensajes incrustados mediante técnicas de

esteganografía. Por otro lado, los metadatos actúan como una fuente de información complementaria, proporcionando datos sobre el origen, la configuración de la cámara, la ubicación geográfica y las modificaciones realizadas en la imagen. [21]

Esta combinación permite realizar un análisis integral desde dos enfoques distintos pero complementarios:

- Estegoanálisis como núcleo de detección visual: Identifica patrones irregulares y anomalías derivadas de la inclusión de información oculta en el contenido binario de la imagen. Esto incluye cambios en el bit menos significativo (LSB), análisis de nivel de error (ELA) y detección de ruido o artefactos.
- Análisis de metadatos como prueba de contexto y trazabilidad: Verifica detalles como fechas de creación, ubicación GPS, tipo de dispositivo, y posibles manipulaciones al comparar metadatos originales con su estado actual. La ausencia o modificación de estos datos puede ser un indicio de intentos de manipulación.

Cuando estas técnicas se aplican conjuntamente, ofrecen una evaluación más completa, permitiendo:

- Identificar falsificaciones digitales que podrían pasar desapercibidas con solo un análisis visual.
- Corroborar la congruencia entre el contenido visual y los metadatos para descartar manipulaciones o alteraciones en contextos forenses o judiciales.
- Detectar casos de desinformación o contenido malicioso que utilicen imágenes aparentemente legítimas.

2.2.2 Identificación y comparación de imágenes en ambientes forenses

El estudio destaca que los hashes perceptuales son herramientas clave para el análisis rápido y robusto de imágenes, permitiendo detectar contenido específico incluso si este ha sido modificado, gracias a la resiliencia de los algoritmos utilizados. Estos hashes pueden ser configurados con umbrales ajustables, lo que es fundamental para equilibrar precisión y sensibilidad, dependiendo de si se busca un reconocimiento exacto o variantes modificadas. Aunque el trabajo actual se enfoca en imágenes RGB, se sugiere extender el análisis a formatos como RGBA, implementar variantes de algoritmos para mejorar la

identificación y explorar tamaños de hash más grandes para manejar imágenes con mayor detalle. La propuesta de utilizar estos hashes en bases de datos especializadas para instituciones judiciales y de seguridad, como complemento a los hashes criptográficos, resalta su potencial en la lucha contra el contenido multimedia ilegal o sensible, subrayando la necesidad de continuar investigando para mitigar falsos positivos y definir aplicaciones prácticas en contextos forenses y de investigación. [26]

2.2.3 Software de esteganografía del bit menos significativo para distribuir archivos en varias imágenes digitales

El proyecto revisa diversas técnicas de esteganografía y ramas de la seguridad informática, como la criptología, con el objetivo de mejorar la técnica del bit menos significativo (LSB). Mediante algoritmos diseñados para particionar, embeber y extraer archivos, se logra incrementar la capacidad de ocultamiento sin comprometer la integridad ni la confiabilidad de la información. Este proceso consiste en dividir el archivo en fragmentos proporcionales a la capacidad de las imágenes portadoras, lo que dificulta la captura de información por terceros y amplía las posibilidades de seguridad. [27]

Además, se desarrolló una solución web que integra estos algoritmos, facilitando la interacción del usuario mediante la carga y procesamiento de archivos en un servidor. El resultado es una herramienta que extiende el uso de la técnica LSB al permitir ocultar archivos más grandes en múltiples imágenes, garantizando tanto la integridad como la confidencialidad de los datos embebidos. Este enfoque abre nuevas posibilidades en la implementación de alternativas de seguridad basadas en esteganografía, fortaleciendo la protección de información sensible en entornos digitales. [27]

2.2.4 ¿Cuándo son necesarias las peritaciones de nuestras imágenes o vídeos?

En los procesos judiciales, la autenticidad de las imágenes presentadas es fundamental para demostrar la veracidad de las pruebas. Las imágenes pueden ser manipuladas fácilmente utilizando diversas herramientas digitales, lo que hace crucial contar con métodos que validen su integridad como el análisis de errores de nivel (ELA) que es una técnica ampliamente utilizada para detectar posibles modificaciones en imágenes JPEG, por ejemplo, se espera que todas las áreas de la imagen tengan un nivel de error similar debido a la compresión. [28]

Si una parte de la imagen presenta un nivel de error significativamente distinto, esto puede ser indicativo de alteraciones. Esta técnica permite a los peritos informáticos identificar modificaciones, lo que es esencial para los procesos judiciales donde la exactitud y la fiabilidad de las pruebas visuales son esenciales como también lo son las herramientas especializadas utilizadas en este análisis ya que proporcionan a los peritos la información necesaria para verificar si una imagen ha sido editada, ayudando a garantizar la integridad de las pruebas presentadas en un juicio. [28]

2.3 Marco Conceptual

2.3.1 Análisis forense informático

Se considera que el análisis forense informático consiste en l aplicación de técnicas científicas y analíticas especializadas a una infraestructura tecnológica que permite identificar, preservar, analizar y presentar datos que sea validos dentro de un proceso legal. El conocimiento del informático forense abarca aspectos no solo del software, sino también del hardware, redes seguridad, hacking, cracking, recuperación de información. [29]

Perito informático: el perito informático es una persona especializada en la informática y en las nuevas tecnologías. En la gran mayoría de países modernos la limitación de jueces y tribunales sobre cuestiones como la especialización del perito informático hace necesaria la presencia de estos profesionales. Que sirven para ofrecer sus conocimientos y resolver casos relacionados con la tecnología de la forma más adecuada posible. [30]

Principios del peritaje:

Objetividad: el perito debe ser objetivo, debe observar los códigos de ética profesional.

Autenticidad y conservación: durante la investigación, se debe conservar la autenticidad e integridad de los medios probabilísticos.

Legalidad: los peritos deben ser precisos en sus observaciones, opiniones y resultados, conocer la legislación respecto de sus actividades pericia y cumplir con los requisitos establecidos por ella.

Idoneidad: los medios probatorios deben ser auténticos, ser relevantes y suficientes para el caso.

Inalterabilidad: en todos los casos, existirá una cadena de custodia debidamente asegurada que demuestre que los medios no han sido modificados durante la pericia.

Documentación: deberá establecer por escrito los pasos dados en el procedimiento pericial.

Estos principios deben cumplirse en todas las pericias y por todos los peritos involucrados.

2.3.2 Imágenes digitales

Hoy en día se ha aumentado el uso de las imágenes digitales, así como los otros medios como texto, imagen, sonido y video, tanto en el ámbito comercial como en la índole personal. Durante los últimos 25 años, dos fueron los fenómenos que afectaron directamente el avance grafico de la informática. Por un lado, el mundo editorial empleo sistemas computarizados para agilizar su producción. Por eso se requirió desarrollar formatos de imagen digital y programas de diseño editorial, tan o más eficientes que los procesos fotomecánicos. A su vez, el internet resulto ser un medio francamente gráfico y dinámico en la aplicación de propuestas multimedia. [31]

Imágenes de mapa de bits: las imágenes de mapa de bits (bitmaps o imágenes raster), están formadas por una rejilla de celdas. Cada celda se denomina píxeles, se les asigna un color y luminancia propios. Por eso, cuando se ve todo el conjunto de celdas, se puede observar la ilusión de una imagen de tono continuo.

Técnica similar a la de los pintores neo-impresionistas del siglo XIX. Por ejemplo, por Georges Seurat en su pintura:

Figura 6: : Un domingo por la tarde en la Grande Jatte [31]

Aquí se muestra una aplicación de la obra de Seurat para revelar la técnica del puntillismo que el pintor utilizaba para pintar.

Imágenes vectoriales: las imágenes vectoriales no están formadas por pixeles, por lo que no es válido aplicar a ellas el concepto en textos anteriores. Al no estar compuesta por pixeles, a la imagen vectoriales se las puede agrandar o achicar sin que se produzca una pérdida de calidad o el tan molesto pixelado. Se trata de imagen "dibujadas" digitalmente a partir de un editor de gráficos como puede ser el Adobe Ilustrator o el más hogareño Corel Draw. La cual se usa habitualmente para crear iconos, formas, logotipos. [32]

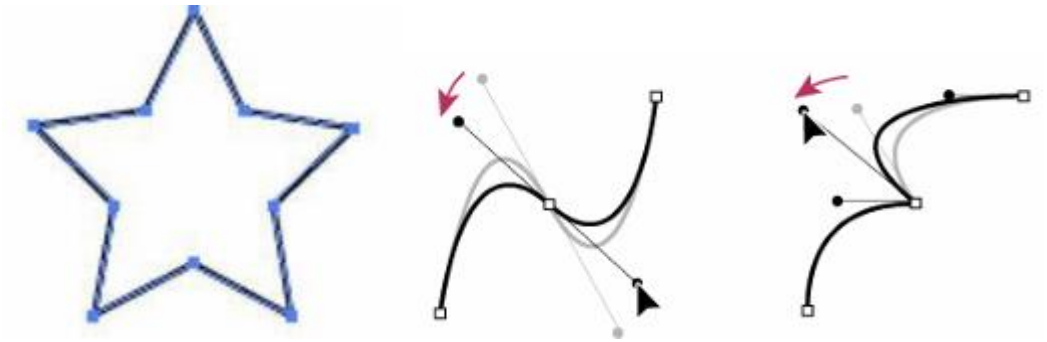


Figura 7: : Imagen vectorial, se trabaja con nodos y tensores [32]

Falsificación de imágenes

Las falsificaciones se pueden clasificar en varios tipos:

- Alteraciones que cambian el contenido: splicing y cpy-move
- Las que preservan el contenido: las manipulaciones comunes de imágenes digitales como remuestreo, compresión, mejora, de contraste, desenfoque, y nitidez no causa alteraciones de información y generalmente no tiene una alteración maliciosa

Métodos activos, son los que extraen cierta información de una imagen; o incrustan información útil sobre la imagen bajo análisis. En ambos casos, la información extraída o incrustada se usa durante la verificación: esquema basados en criptografía, en marca de agua y en esteganografía. Métodos pasivos, también llamados métodos forenses, no requieren información previa sobre la imagen que está siendo analizada. [33]

2.3.3 Metadatos

Los metadatos son información estructurada que describe, explica, localiza o hace más fácil de recuperar, utilizar o manejar una fuente de información. A los metadatos a menudo se les llama datos que se usan para describir otros datos. Es el uso más tradicional del término. [34]

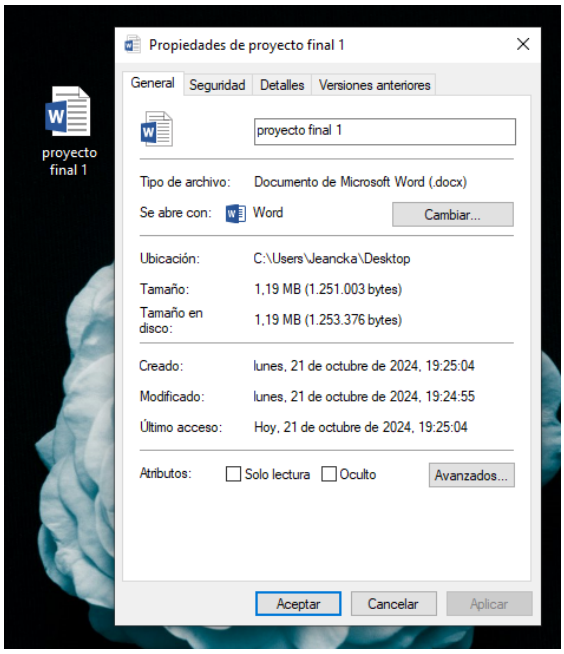


Figura 8: metadatos generales de un documento Word.

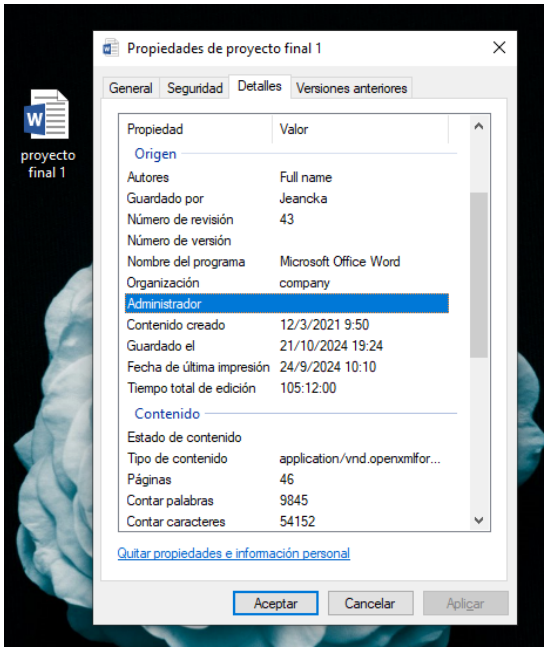


Figura 9: detalles de metadatos de un documento Word

Precisamente, los metadatos son los “datos que hablan cerca de los datos”, en el sentido de que describen el contenido de los archivos o la información que estos traen.

Los metadatos tienen una serie de aplicaciones que resultan útiles en el trabajo cotidiano. Algunas de ellas son [35]:

Búsqueda y análisis: los metadatos al portar información sobre contenido de los datos, ayuda a la hora de clasificarlos y encontrar el tipo de información al no necesitar consultar el dato en sí. Precisamente este es su uso más común: agilizar la consulta de buscadores.

Estandarización: mediante los metadatos pueden definirse criterios fijos y comunes ara identificar los documentos, eliminando errores e inconsistencia, de manera que se facilita si manejo cotidiano y la compatibilidad si necesitas sacarlos de tu empresa y enviarlos a clientes, proveedores u otros agentes externos.

Gestión de cambios: gracias a los metadatos es fácil localizar alteraciones que se haga en los datos originales, por lo que te resultara sencillo controlar el progreso de un proyecto y las distintas versiones que se hayan haciendo de él.

Rapidez de desarrollo: al poder acceder de forma más inteligente a los datos, los metadatos permiten a los creadores trabajar con más agilidad reduciendo el tiempo invertido en el abastecimiento de material, por lo tanto, incrementar su producción y la rentabilidad para tu empresa.

Mejora de informes: los metadatos permitirán gestionar informes de más calidad, de que repercutirá en el análisis más fiable de los procesos y, por lo tanto, contribuirá a la aplicar correctamente las medidas de corrección que se necesiten.

Evaluación: en forma de metadatos se puede incluir una valoración sobre la calidad del contenido de un documento, que resulta de gran utilidad a la hora de decidir si merece la pena utilizarlo o no para el proyecto que tenga en marcha.

Verificación: los metadatos de un documento se pueden utilizar para la verificación de la veracidad de él, la comparación de un archivo con otro que haya sido manipulado se podría comprobar por medio de los metadatos y sus diferencias, sabiendo cual es la verdadera o la más reciente.

Metadatos en imágenes

Los metadatos son información adicional incrustad en los archivos de imágenes digitales que registran detalles sobre las condiciones en las que se capturo la imagen. Esta información puede incluir fecha y hora de la captura, el uso o no del flash, la distancia al objeto y el tiempo de exposición, la apertura del obturador entre algunos casos, datos de ubicación GPS. Los metadatos complementan el contenido principal de la imagen y facilitan su organización y búsqueda en bibliotecas digitales. Las imágenes digitales son almacenadas en una gran variedad de formatos como TIFF, JPEG, PSD. Algunos de los distintos contenedores de metadatos para distintos formatos son: EFD Exif, TIFF, Adobe XMP, e IPTC-IIM. La especificación Exif es la más utilizada para identificación de la fuente por ser el contenedor de metadatos más común en las cámaras digitales. [38]

Los metadatos juegan un papel crucial en la verificación forense de la autenticidad de una imagen, ya que puede contener información valiosa como las antes mencionadas, elementos difíciles de interferir del contenido visual de la imagen por si sola. Sin embargo, los metadatos son vulnerables a alteraciones. Algunos programas de edición de imágenes pueden modificar o eliminar accidentalmente los metadatos, lo que plantea desafíos para su uso en análisis forense. a pesar de estas limitaciones si los metadatos están presentes y se verifica su autenticidad, son una herramienta de gran utilidad pata los análisis forenses. [36]

Nombre	Descripción
Exif Data	Es una aplicación online que presenta datos Exif de una forma ordenada. Se puede subir una imagen desde el ordenador o usar una URL. Admite varios tipos de archivos (JPG, TIFF, RAW, PNG, SMP entre otras), con un límite de 20 MB.
ExtractMetadata	Con esta herramienta se puede extraer los metadatos online de varios formatos de archivo, no solo imagen, sino también documentos Word, PDF, OpenOffice, entre otras

Jeffrey´s Exif Viewer	Ofrece una información completa en su plataforma online, la cual es compatible con una amplia variedad de formatos de archivos.
Metapicz	Ofrece la información muy ordenada, limpia y completa. Se puede cargar las imágenes desde el ordenador o introduciendo la dirección URL de la imagen.
Camera Summary	Extrae metadatos de imágenes y esta no los guardará al momento de analizarla. Sin embargo, en esta herramienta habría que subir solamente la imagen desde el ordenador, debe tener formato JPG/JPEG y peso limitado de 1.5 MG.
Online Exif Viewer	Es una herramienta para extraer metadatos sencilla, pero que ofrece una gran cantidad de información. Solo sirve para archivos de imagen, los cuales se cargan desde el ordenador o URL.
Verexif	Esta herramienta no solo se puede visualizar los metadatos de las imágenes, sino también se puede quitar los metadatos online.
Metadato.org	El extractor de metadatos online que permite visualizar y extraer datos de cualquier imagen, con posibilidad de exportarlos a un fichero .csv.
Get-Metadata	Permite extraer metadatos de diferentes ríos de archivos
TheExifer	Permite cargar varios tipos de archivos de formato de imagen desde el ordenador, drive, Dropbox o Flickr de manera sencilla y rápida. Permite ver, eliminar o incluso editar los metadatos mostrados.

Metashield Clean-up Online	Esta herramienta es compatible con varios tipos de archivos, documentos, imágenes, audio y videos, entro otro formato como PDF, ZIP o RTF. No solo permite extraer los metadatos del archivo subido, sino también podría ser eliminados.

Tabla 3: Herramientas online para ver y editar los metadatos de tus archivos

2.3.4 Esteganografía

La esteganografía es el arte y ciencia de ocultar información, hace que esos datos sean invisibles, escondiéndolos en algún portador, de tal manera que nadie, excepto el remitente y destinatario puedan detectar la existencia de la información [37]. El objetivo de la esteganografía consiste en enlazar dos entidades en igualdad de condiciones para intercambiar mensajes ocultos, a través de un canal de comunicación inseguro, de tal manera que pase inadvertido por terceros que puedan tener acceso a dicho canal. Utiliza el concepto de "seguridad por oscuridad", se refiere a que, si nadie conoce la existencia de un mensaje oculto, nadie tratara de obtenerlo. [38]

La esteganografía al igual que otras disciplinas tiene terminologías propias:

- Emisor: entidad que envía el mensaje por un canal a través de procedimientos predefinidos.
- Receptor: entidad inversa al emisor, realiza la operación contraria para reconstruir el mensaje.
- Canal: medio utilizado para transmitir un mensaje desde el emisor al receptor.
- Portador: cualquier tipo de dato susceptible de ser modificado para incorporar el mensaje a ocultar.
- Embeber: es la acción de ocultar el mensaje dentro del portador. La recuperación posterior del mensaje oculto se conoce como extracción.
- Estego-algoritmo: denominación al algoritmo esteganográfico que indica la manera de realizar el procedimiento de incorporación del mensaje a ocultar.
- Estego-clave: denominación a una clave esteganográfica que define como aplicar el estego-algoritmo. Dentro del portador, esta información podría indicar el lugar a partir del cual comienza a incorporar el mensaje.

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

Esquema esteganográfico: denominación al conjunto de componentes que permite la comunicación esteganográfica. Dentro de este esquema se encuentra la elección del tipo del portador, asimismo, los algoritmos para embeber y extraer el mensaje del portador y finalmente, la manera de transmitir el portador. [39]

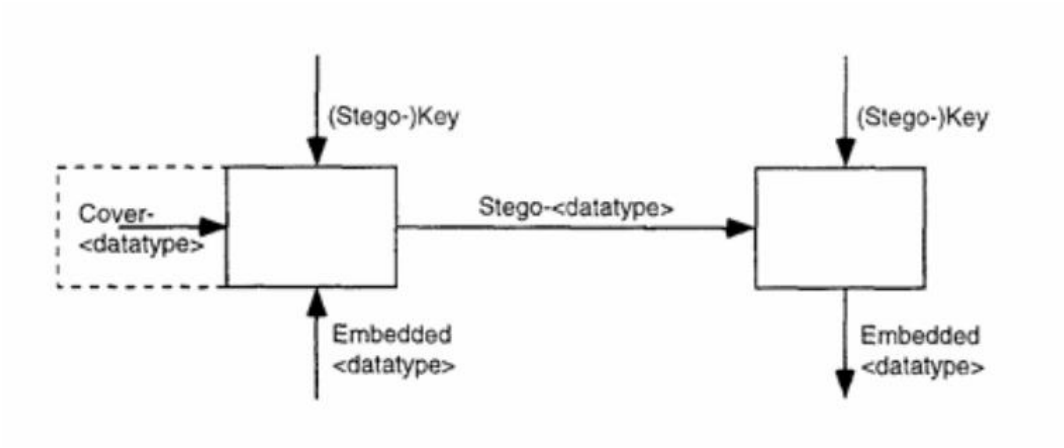


Figura 10: Esquema esteganográfico genérico acordado en el primer taller internacional de ocultación de información. [39]

Tipos de esteganografía [40]

- **Esteganografía Simple:** En este enfoque, el mensaje oculto se integra en un mensaje anfitrión sin la necesidad de utilizar claves de intercambio. El principal desafío es que la seguridad es nula si el atacante conoce el método de ocultación utilizado.
- **Esteganografía con clave secreta:** Similar al modelo anterior, pero en este caso, el mensaje se oculta utilizando una clave privada, lo que proporciona mayor seguridad, ya que tanto el emisor como el receptor comparten la misma clave y no es necesario transmitirla.
- **Esteganografía con clave pública:** Este método emplea un par de claves, una privada y otra pública. La clave pública se usa para ocultar el mensaje, mientras que la clave privada es necesaria para recuperarlo. En este caso, es esencial transmitir la clave pública a través de un medio seguro.

Esteganografía en imágenes:

- **LSB** (Least Significant Bit): Es uno de los métodos más comunes para ocultar información en una imagen, y generalmente consiste en insertar cada bit del mensaje dentro del bit menos significativo de los píxeles de la imagen, lo que permite esconder datos de manera sutil sin alterar visiblemente la imagen.
- **DCT** (Transformada Discreta del Coseno) y DWT (Transformada Discreta de Wavelet): Son técnicas esteganográficas que emplean funciones matemáticas dentro de algoritmos de compresión para ocultar datos. Por ejemplo, en las imágenes JPEG se utiliza la DCT para comprimir la imagen, lo que también puede ser aprovechado para insertar información oculta sin afectar significativamente la calidad visual de la imagen.
- **Spread Spectrum**: Este método se distingue por su robustez frente a ataques estadísticos, especialmente cuando se aplica a imágenes en formato JPEG. La información oculta se distribuye de manera uniforme en toda la imagen, lo que hace que sea difícil de detectar sin alterar las propiedades estadísticas de la imagen.

2.3.6 Estegoanálisis

El estegoanálisis es una ciencia que estudia la detección (ataques pasivos) y/o anulación (ataques activos) de información oculta en distinto formatos (texto, imagen, audio, video), así mismo, puede detectar o localizar información útil dentro de la misma. El estegoanálisis se puede definir como el arte de descubrir y hacer a los mensajes ocultos inútiles para una comunicación efectiva. [41]

Todas las técnicas de esteganografía en imágenes digitales pueden ser representadas por la fórmula dada en la imagen #

$$C = p + t$$

Figura 11: Formula que representa la esteganografía

Tomando en cuenta el umbral de la perceptibilidad de la visión humana en una imagen, *t* es la cantidad de información en la imagen que puede ser manipulada sin causar una distorsión perceptible. La otra porción de información, que si es modificada provocara

una distorsión, es representada por *p*. Finalmente *C,* es alguna imagen con potencial para ser cubierta del mensaje secreto. [42]

El tamaño de t está disponible tanto para el usuario del sistema esteganográfico como para algún atacante que espera poder destruir la información en *t*. siempre y cuando *t* se mantenga en las regiones imperceptibles, existe alguna *t'* que puede ser usada por el atacante $C'' = p + t'$, donde no existe una diferencia perceptible entre *C* y *C''*, este ataque puede ser para reemplazar o remover las regiones que ocupan *t*. si se agrega información extra al medio digital, esta puede sufrir mayores distorsiones y puede remover o sobrescribir la información oculta en la cubierta (área donde se oculta la información), haría a la información más robusta pero eso también provocaría la aparición de marcas, que advertirían la presencia de un mensaje oculto. Algunas degradaciones o distorsiones ocurren durante el proceso, pero estas no son fácilmente detectadas por el sistema de visión humana. [42]

En la siguiente lista se muestra algunos ataques que puede realizar el estegoanalista:

- **Ataque de estego-objeto:** solo los estego-objetos están disponibles para el análisis.
- **Ataque a una cubierta conocida:** tanto la cubierta como el estego-objeto están disponibles para ser analizado.
- **Ataque de mensaje conocido:** en algún punto, el mensaje oculto puede ser conocido por el atacante. Analizando el estego-objeto para encontrar patrones que correspondan con el ocultamiento del mensaje, esto puede ser de beneficio para futuros atacantes en contra de este sistema. Aún con el mensaje, esto puede ser muy difícil y probablemente esto sea equivalente al ataque de estego-objeto.
- **Ataque de esto elegido:** tanto la herramienta esteganográfica y el estego-objeto son conocidos.
- **Ataque de mensaje elegido:** el estegoanalista genera un estego-objeto mediante una herramienta o algún algoritmo esteganográfico, usando un mensaje elegido. El objeto de este ataque es determinar los patrones correspondientes en el estego-objeto, que puedan señalar el uso de herramientas o algoritmos esteganográficas específicos.

- **Ataque de estego conocidos:** el algoritmo esteganográfico es conocido y tanto la cubierta original como el estego-objeto están disponibles.

Entre las técnicas de estegoanálisis más comunes se encuentran:

LSB (Least Significant Bit)

El método LSB (Least Significant Bit) es uno de los más utilizados en el campo de la esteganografía para ocultar información dentro de una imagen digital. Este enfoque consiste en modificar los bits menos significativos de los píxeles de la imagen, lo que permite insertar datos ocultos sin alterar visualmente la imagen de manera significativa. En términos de esteganografía, este método es efectivo porque los cambios en los bits menos significativos son casi imperceptibles para el ojo humano. Sin embargo, su simplicidad también implica que es vulnerable a métodos de detección como el análisis de histograma y técnicas estadísticas que buscan anomalías en los datos pixelados. Dado que la modificación solo afecta a los bits menos importantes de los píxeles, las imágenes siguen siendo visualmente intactas, pero la información oculta puede ser extraída con herramientas especializadas. La detección del LSB se basa en la observación de patrones inusuales o la repetición de valores en los bits modificados. [43]

Análisis de Nivel de Error (ELA)

El Análisis de Nivel de Error (ELA, por sus siglas en inglés) es una técnica utilizada en el campo de la forensia digital para detectar alteraciones en las imágenes. Funciona evaluando las diferencias de compresión entre las regiones de la imagen que deberían ser homogéneas, lo que permite identificar áreas que han sido modificadas. Este análisis es particularmente útil cuando se trabaja con imágenes JPEG, ya que las zonas que han sido alteradas o modificadas digitalmente, por lo general, presentan un nivel de error diferente al de las zonas originales de la imagen. ELA puede identificar anomalías en la compresión de la imagen, revelando áreas donde se han producido cambios o inserciones de información. La aplicación de esta técnica es fundamental para verificar la autenticidad de las imágenes en procesos legales y de investigación, ya que permite detectar manipulación sin necesidad de conocer los métodos específicos utilizados para alterarlas. [44]

Algoritmos Basados en Inteligencia Artificial

El uso de algoritmos basados en inteligencia artificial (IA) en el análisis de esteganografía ha ganado relevancia debido a su capacidad para mejorar la precisión y automatización de la detección de información oculta. Las redes neuronales y los sistemas de aprendizaje automático (machine learning) son herramientas eficaces para reconocer patrones complejos y sutiles en los datos de las imágenes. Estos sistemas pueden ser entrenados para identificar huellas digitales de inserciones de datos, incluso en contextos donde las técnicas tradicionales de esteganografía, como LSB, podrían pasar desapercibidas. La capacidad de los algoritmos basados en IA para procesar grandes volúmenes de datos y adaptarse a diferentes métodos de ocultación de información los convierte en una herramienta poderosa para la detección de esteganografía, proporcionando una solución más precisa y eficiente en comparación con los métodos manuales o heurísticos. [45]

Chi-Cuadrado

El test de Chi-cuadrado es una técnica estadística ampliamente utilizada en el análisis de imágenes digitales para detectar alteraciones o manipulaciones. Este test evalúa la dispersión de los datos entre diferentes categorías o grupos y compara la frecuencia observada con la frecuencia esperada en función de un modelo teórico. En el contexto del análisis de imágenes, el test de Chi-cuadrado se utiliza para identificar discrepancias entre las características estadísticas de la imagen original y las posibles manipulaciones. Si se han realizado modificaciones en la imagen, como la inserción de información oculta a través de técnicas como LSB, el test de Chi-cuadrado puede revelar patrones inusuales que indican la presencia de alteraciones. [9]

El uso de Chi-cuadrado en el estegoanálisis es una forma efectiva de evaluar la "normalidad" de las imágenes y detectar signos de manipulación sin la necesidad de conocer el algoritmo exacto que se utilizó para modificar la imagen. Esta herramienta es útil cuando se busca realizar un análisis más exhaustivo de las características estadísticas de las imágenes para detectar cualquier alteración. [9]

2.3.7 Composición y formato de imagen

La composición de las imágenes va de acuerdo a su color:

Imágenes monocromáticas, están formadas por pixeles blancos y negros puros. No se incluyen tonalidades intermedias (grises) ni colores.

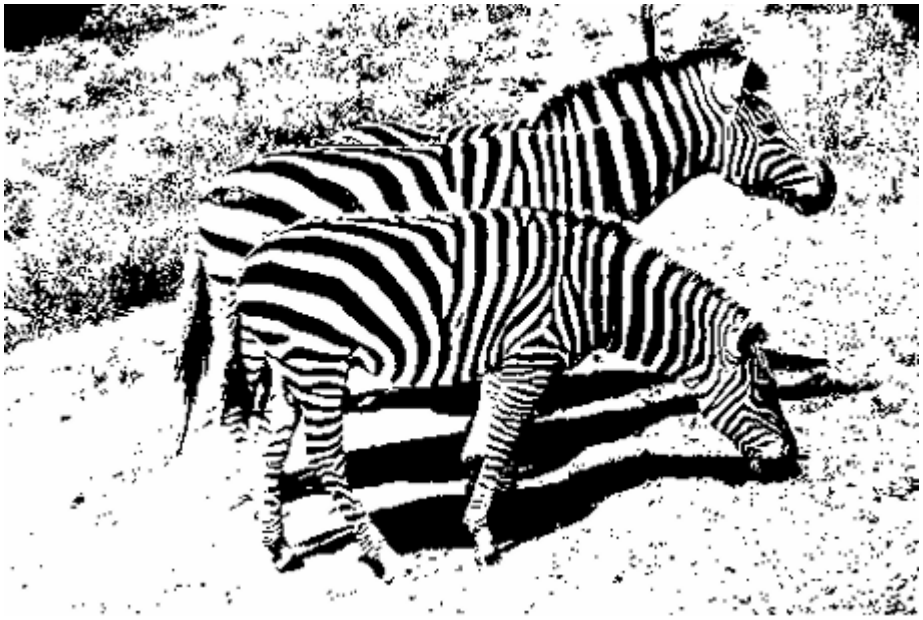


Figura 12: Imagen monocromática

Imagen escala de grises, tienen tonos blancos, negros y grises de hasta 259 tonos. No hay color.

Figura 13: Imagen escala de grises

Imagen duotono, como su nombre indica, se refiere a imágenes que emplean dos colores de tinta.

Figura 14: Imagen duotono.

Imagen color, contiene varios colores, puede ser RGB o CMYK.

Figura 15: imagen a color

La compresión de imágenes

La mayoría de formatos de imágenes se realizan de dos tipos: LOSSY (con perdida) y LOSSLESS (sin perdida). Las imágenes con una compresión sin perdida (LOSSLESS) son capaces de reconstruir la imagen a su estado original. No se producen perdidas. Por el contrario, las imágenes con una compresión con perdida (LOSSY) se aproxima a la imagen original, aunque no es exactamente igual (en muchas ocasiones está perdida no

es apreciable). Obviamente, las imágenes con esta compresión ocupan menos espacio. [46]

Pero existen diferentes maneras de compresión y cada una de ellas será apropiada para diferentes situaciones. Los formatos más conocidos son .jpg, .gif, .png, .bmp, .psd, .webp. Los siguientes ejemplos son sacados del trabajo [46]

- **Formato de imagen .jpeg / .jpg:**

  Esta extensión es una de las más usadas, sobre todo en internet, en fotografías o en gráficos web. Es un formato de imagen con pérdidas, y pesa poco. Aunque en resoluciones pequeñas puede aumentar notablemente su pixelación, nos ofrece un excelente equilibrio entre peso/calidad. Al guardad una imagen como .jpg, podemos elegir el grado de compresión: alto, medio, bajo. Cuando más compresión, más perdida. Se recomienda usar el formato de imagen .jpeg o .jpg para imprimir archivos en alta resolución (pero con una baja compresión para evitar demasiadas perdidas)

- **Formato de imagen .gif:**

  Este formato sin perdida se usa casi exclusivamente para web y que permite crear pequeñas animaciones. Últimamente ha adquirido gran popularidad gracias a los memes. A pesar de que gif es un formato de imagen sin perdida, se puede guardar en un formato reducido para menguar su tamaño. Se recomienda usar el formato de imagen .gif para animaciones web como banners, memes o iconos. Este formato, además permite guardar imágenes con un fondo transparente.

- **Formato de imagen .png:**

  Este formato es sin perdida y se puede añadir una transparencia con degradado al fondo (.gif solo permite una transparencia pura). Es muy común actualmente y es ideal para gráficos web como iconos. Funciona muy bien con una paleta de color reducida. Con .png también se puede guardar fotografías con una calidad alta, no obstante, se recomienda usar .jpeg en estos casos porque con .png el tamaño será mucho mayor

- **Formato de imagen .tiff / .tif:**

  Este formato es sin perdida y ofrece mucha calidad de fotografías, aunque suele ser bastante pesado. También se usa para escanea en alta calidad. Sin embargo, no se recomienda en gráficos web, ya que está optimizada para imprimir.

- **Formato de imagen .bmp:**

  El formato de imagen .bmp es un archivo de mapa de bits sin perdida y fue desarrollado para Windows. Es por ello que guarda una gran cantidad de información y eso lo convierte en un archivo bastante pesado. Sin embargo, debido al auge de internet, este tipo de formato de imagen ha ido perdiendo popularidad durante los últimos años a favor de .jpeg.

- **Formato de imagen .psd:**

  Este formato fue creado por Adobe Photoshop y puede ser abierta por este programa. Los archivos .psd son editables con capas y ajustes de imagen. Es usado mayoritariamente para imágenes en mapa de bits, aunque también tiene opciones para crear vectores. Con Photoshop se puede explorar a muchos otros formatos de imagen una vez se haya terminado de editar o de crear

- **Formato de imagen .eps:**

  Este formato pude incluir tanto vectores como imágenes rasterizadas o mapa de bits. Se recomienda usar este archivo de imagen únicamente para evitar el proyecto a la imprenta o para enviárselo al cliente. Se genera trabajando archivos en Ilustrator.

- **Formato PDF:**

  Es un formato de almacenamiento para documentos digitales independiente de plataformas de software o hardware. Este formato es de tipo compuesto (imagen vectorial, mapa de bits y texto). Es un formato universal y se puede pedir en imprentas como archivo final. Es por ello que se recomienda guardar en .pdf antes de llevar a imprimir o para subir archivos o documentos “cerrados” a un correo o una web.

- **Formato de imagen .webp:**

  Este formato tiene por objetivo reducir al máximo el tamaño de las imágenes en la web. Según Google, las imágenes y los gráficos en formato WebP son, más o menos un 30 por ciento más pequeñas que los archivos PNG O JPEG y tiene la misma calidad de imagen. Mientras que estos formatos se basan en métodos de compresión distintos -PNG, sin perdida, y JPG, con perdida, WebP permite ambas posibilidades. Gracias a la flexibilidad, el formato es adecuado tanto para fotografías como para imágenes y gráficos pequeños. Por sus características de compresión (con y sin perdida) y por otras propiedades centrales que ofrece el formato WebP (transparencia, animaciones) se ha ido posicionando en los últimos años.

2.3.8 Ciberseguridad

El término ciberseguridad se definió como la habilidad de proteger y defender las redes o sistemas de los ciberataques. Con el fin de evitar el acceso, uso, alteración, modificación o destrucción no autorizada de la información almacenada electrónicamente. Como existen nuevos entornos de nuevas tecnologías, han surgido nuevas herramientas para detectar malware avanzado o para poder encontrar anomalías e incidentes de seguridad dentro de millones de eventos de diversas bitácoras o, incluso, en miles de millones de paquetes de red, pero el reto de tener una estrategia de ciberseguridad es mucho mayor que la adquisición e implementación de nuevas herramientas, se vuelve muy importante fortalecer, entre otras, las capacidades de detectar que estamos siendo víctimas de un ataque avanzado; de analizar su estructura y comportamiento para poder contenerlos y remediarlos; así como de analizar los efectos o el impacto que se haya tenido. [47]

2.3.9 Evolución de las ciber amenazas

Los conceptos y la normativa se han ido configurando para responder a unas ciberamenazas cada vez más orientadas a destruir, alterar y sustraer la información y a quebrantar o interrumpir a disponibilidad de los servicios. Para entender una aproximación practica a este fenómeno el CCN-CERT (Centro Criptológico Nacional Computer Emergency Response Team, es un organismo español, creado en 2006) establece una priorización por agentes de la amenaza, según sus motivaciones [48]:

Crimen Cibernético	Descripción
Ciberespionaje	Ciberataques realizados para obtener secretos de estado, prioridad industrial, propiedad intelectual, información comercial sensible o datos de carácter personal. Es uno de los ataques que causan una mayor preocupación a CCN.
Ciberdelito/cibercrimen	Actividad que emplea las redes y sistemas como medio, objetivo o lugar del delito. Se les aplican todas las figuras delictivas del crimen tradicional pero adaptadas al ciberespacio. Normalmente su motivación es el rendimiento económico y sus objetivos con víctimas que dispongan de a vulnerabilidad adecuada y con capacidad financiera para tender sus demandas.
Ciberactivismo	Activismo digital antisocial. Persigue el control de redes o sistemas (sitios web) para promover su causa o defender su posicionamiento político o social.
Ciberterrorismo	Actividades dirigidas a causar pánico o catástrofes en las redes y sistemas o utilizando estas como medio.
Uso de internet por los terroristas	Actividad de los grupos terroristas que utilizan internet como soporte de comunicaciones y coordinación, para atención de información de posibles objetivos en tareas de propaganda,

	radicalización o financiación de sus actividades.
Ciberconflicto/ciberguerra/guerra	Operación dirigida por un estado para desestabilizar otros Estados y polarizar a la población civil. Incluye una gran variedad de herramientas como diplomacia y acciones de inteligencia tradicional, instrumentalización del crimen organizado, operaciones psicológicas, propaganda, desinformación y ciberataques.

Tabla 4: Tabla de Crimenes Cibernético

2.4 Marco Legal

2.4.1 Importancia de la regulación de la ciberseguridad y el análisis de malware

El auge de los crímenes digitales o ciberataques ha puesto en jaque a los usuarios de internet, sitios web, empresas y corporaciones, generando perdida por miles de millones de dólares al año. Debido a esto es importante estar al tanto de las amenazas que se pueden conseguir día a día en la web o con solo encender el computador o el dispositivo, sin embargo, no basta con ello, se debe de tener un conocimiento mínimo de como contrarrestar dichas amenazas y tener las herramientas mínimas para no ser víctimas de robo de información, fraude o estafa. Por lo antes expuesto, es por esto que la seguridad informática y el análisis de cualquier malware o virus tiene tanta importancia, no solo desde el punto de vista de resguardo de información, sino también económico, la inversión de tiempo para el adiestramiento y programas de protección son la única manera de hacerle frente a los cibercriminales y evitar mayores pérdidas monetarias en el futuro. [49]

El Instituto Nacional de Ciberseguridad (INCIBE), ha publicado su balance de ciberseguridad relativo al año 2023, donde se refleja el incremento del 24% de los incidentes respecto al año anterior. En total, se gestionaron desde el CERT de INCIBE 83.517 incidentes de ciberseguridad, de los cuales más de 58 mil afectaron a la ciudadanía

(usuarios de internet) y el resto de infectados sobrepasaron los 22 mil a empresas privadas (incluidas pymes, micropymes y autónomos). Además, se identificaron 183.077 sistemas vulnerables. [50]

2.4.2 Normativas internacionales

2.4.2.2 Convenio Internacional sobre Cibercriminalidad (Budapest)

El Convenio Internacional sobre Cibercriminalidad, conocido también como el Convenio de Budapest, es un tratado internacional diseñado para abordar el ciberdelito y establecer mecanismos de cooperación judicial y policial en la lucha contra los crímenes informáticos. Fue adoptado en Budapest, Hungría, el 23 de noviembre de 2001, y es el primer tratado internacional que establece normas comunes para el combate de delitos cibernéticos.

El Convenio de Budapest es relevante en términos de cómo se manejan y protegen las pruebas digitales. Además de la cooperación internacional, este tratado aborda el delito de falsificación de documentos electrónicos (lo que incluye la alteración de imágenes), un tema clave en la investigación. Si alguna de las imágenes analizadas forma parte de una investigación judicial, el cumplimiento de este convenio es esencial para asegurar la validez y la cadena de custodia de la evidencia digital.

Además, el convenio también resalta la importancia de la seguridad en la recolección de evidencias, lo cual es esencial en el contexto de la esteganografía, donde la integridad de los datos ocultos debe ser preservada durante la recolección, análisis y presentación en juicio.

Los siguientes artículos del convenio pueden ser relevantes para el proyecto propuesto [51]:

Artículo 4 - Ataques a la integridad de los datos

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.

2. Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.

Artículo 7 - Falsificación informática

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Las Partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal.

Artículo 8- Fraude informático

Las Partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante:

- la introducción, alteración, borrado o supresión de datos informáticos;
- cualquier interferencia en el funcionamiento de un sistema informático;

con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

2.4.3 Normativas Nacionales

2.4.3.1 Ley de Protección de Datos Personales

La Ley de Protección de Datos Personales de Ecuador, conocida también como la Ley Orgánica de Protección de Datos Personales (LOPDP), regula el tratamiento de datos personales y establece los derechos y garantías para las personas sobre sus datos personales. Esta ley es relevante para tu proyecto de tesis, que involucra la manipulación y análisis de imágenes, ya que muchas veces las imágenes pueden contener datos personales que deben ser protegidos y tratados de manera legal.

Algunos de los artículos más relevantes para el proyecto son [52]:

Artículo 7- Tratamiento legítimo de datos personales

Establece que los datos personales deben ser procesados de manera legal, justa, transparente y respetando la finalidad específica para la que fueron recolectados. Prohíbe el uso de los datos más allá de lo estrictamente necesario para el propósito inicial.

Artículo 8- Consentimiento

Estipula que cualquier tratamiento de datos personales requiere el consentimiento previo, explícito e informado de la persona propietaria de esos datos, salvo excepciones contempladas en la ley. El consentimiento puede ser revocado en cualquier momento.

Artículo 12- Derecho a la información

Define los derechos de Acceso, Rectificación, Cancelación y Oposición. Estos derechos permiten a los titulares de los datos consultar qué información personal se está procesando, solicitar modificaciones o la eliminación de datos incorrectos o innecesarios y oponerse a su uso.

2.4.3.2 COIP

El Código Orgánico Integral Penal (COIP) de Ecuador regula los delitos, sanciones y procedimientos relacionados con la actividad criminal, incluyendo aquellos vinculados al uso indebido de sistemas informáticos y tecnológicos. Algunos artículos relevantes incluyen [53]:

Artículo 212 – Suplantación de identidad

Tipifica el uso de datos personales o credenciales ajenas para acceder a sistemas informáticos, redes o servicios con fines fraudulentos o ilegales.

Artículo 345 – Sabotaje

Regula la penalización por dañar sistemas informáticos, redes o bases de datos mediante software malicioso o cualquier medio que impida su funcionamiento normal.

Artículo 190 – Apropiación fraudulenta por medios electrónicos

establece que comete un delito quien se apropie de dinero, bienes o recursos ajenos utilizando tecnologías electrónicas o sistemas informáticos, con el propósito de engañar o generar beneficios indebidos. Esto incluye técnicas como fraudes en transacciones, uso indebido de plataformas digitales, o manipulación de datos para obtener ganancias de manera ilícita.

Artículo 232 – Ataque a la integridad de sistemas informáticos

Tipifica como delito cualquier acción que, sin autorización, altere, dañe, elimine, deteriore o interfiera en el funcionamiento de sistemas informáticos, bases de datos o redes electrónicas

2.4.4 Aspectos éticos

2.4.4.1 Implicaciones éticas de la manipulación de imágenes.

La manipulación de imágenes plantea serias cuestiones éticas, ya que puede usarse para alterar la percepción de la realidad, influir en opiniones o dañar la reputación de personas y organizaciones. Este acto puede ser intencionado para desinformar, falsificar evidencia en contextos legales, o crear contenido engañoso. Las implicaciones éticas radican en el respeto a la verdad, el derecho a la privacidad y la confianza social. Manipular imágenes sin el consentimiento adecuado o para fines fraudulentos compromete principios como la integridad, la transparencia y la responsabilidad.

2.4.4.2 Implicaciones éticas del análisis de imágenes.

El análisis de imágenes también plantea dilemas éticos, especialmente cuando se trata de investigar contenido sensible o privado sin el consentimiento adecuado. Esto incluye el uso de herramientas avanzadas para identificar alteraciones o extraer información que no estaba destinada a ser compartida. Es esencial garantizar que estas prácticas respeten la privacidad, no violen derechos individuales y se apliquen únicamente con fines legítimos, como investigaciones legales o seguridad. La recopilación y el análisis de datos visuales deben alinearse con estándares éticos que aseguren el respeto a los derechos humanos y la no discriminación.

CAPÍTULO 3. PROPUESTA

3.1 Análisis de requerimientos

3.1.1 Requerimientos funcionales

Código	Registro e inicio de sesión
RF01	Implementar un sistema de registro de usuarios.
RF02	Implementar un sistema de autenticación de usuarios.
RF03	Permitir a los usuarios ver una lista de investigaciones creadas previamente asociadas a su cuenta.
RF04	Habilitar la opción para crear una nueva investigación desde la lista principal.

Tabla 5: Requerimientos funcionales- registro e inicio de sesión

Código	Gestión de investigaciones
RF05	Registrar cada investigación creada, incluyendo una descripción, fecha de inicio, y estado (en progreso o terminada).
RF06	Guardar los análisis realizados durante una investigación y asociarlos con el ID de usuario y de la investigación.
RF07	Permitir a los usuarios ver una lista de investigaciones creadas previamente asociadas a su cuenta.
RF04	Permitir a los usuarios finalizar una investigación y bloquear nuevos análisis en la misma.

Tabla 6: Requerimientos funcionales - gestión de investigaciones

Código	Opciones de menú principal
RF08	Incluir un botón de información sobre la aplicación con una guía de usuario accesible.
RF09	Ofrecer un botón para salir y regresar al listado de investigaciones sin perder el progreso.
RF10	Proveer una opción para finalizar una investigación desde su página.

Tabla 7: Requerimientos funcionales - opción de menú principal

Código	Análisis forense
RF11	Realizar **análisis LSB** para detectar posibles datos ocultos en los bits menos significativos de las imágenes cargadas.
RF12	Extraer y visualizar los bits LSB (R) y los segundos bits menos significativos (S) de una imagen.
RF13	Implementar un módulo para aplicar **Error Level Analysis (ELA)**, generando una versión visual del análisis con áreas destacadas que muestren posibles manipulaciones.
RF14	Extraer y mostrar los metadatos de las imágenes, incluyendo datos como fecha de captura, ubicación, dispositivo, cámara, etc.
RF15	Habilitar la posibilidad de generar reportes de cada análisis (LSB, ELA y metadatos) en formato PDF.
RF16	Visualizar reportes previos generados, filtrados por ID de usuario e ID de investigación.

Tabla 8: Requerimientos funcionales - análisis forense

Código	Gestión de imágenes
RF17	Permitir la subida de imágenes JPG/JPEG a Firebase Storage desde el dispositivo móvil del usuario.
RF18	Habilitar la opción de eliminar imágenes almacenadas en la base de datos, se podrá eliminar la imagen sola o todos los reportes asociados.
RF19	Facilitar el acceso a imágenes almacenadas en la base de datos para realizar nuevos análisis.

Tabla 9: Requerimientos funcionales - gestión de imágenes

Código	Usabilidad
RF20	Mostrar gráficos o indicadores visuales para representar el progreso de los análisis realizados.
RF21	Permitir la navegación intuitiva entre las páginas de análisis, reportes y gestión de imágenes.

Tabla 10: Requerimientos funcionales - usabilidad

3.1.2 Requerimientos Técnicos

Código	Plataforma y tecnologías
RT01	Desarrollar la aplicación en **Ionic** y Angular para asegurar compatibilidad multiplataforma
RT02	Implementar Firebase como servicio de backend para autenticación, base de datos en tiempo real, y almacenamiento de imágenes y reportes.
RT03	Configurar Firebase Firestore para almacenar datos de imágenes, y metadatos

Tabla 11: Requerimientos Técnicos - plataforma y tecnologías

Código	Compatibilidad
RT04	Asegurar la compatibilidad con dispositivos Android, desde la versión **10 (API nivel 29)** en adelante.
RT05	Adaptar la interfaz para pantallas de diferentes resoluciones y tamaños, asegurando una experiencia óptima en dispositivos móviles y tabletas.
RT06	Garantizar que los análisis puedan realizarse en imágenes de un tamaño máximo de 5 MB, optimizando tanto el procesamiento como el almacenamiento.

Tabla 12: Requerimientos Técnicos - compatibilidad

Código	Integración de análisis
RT07	Implementar algoritmos para el análisis LSB y la extracción de bits significativos (R y S) basados en estándares forenses.
RT08	Desarrollar un algoritmo para el análisis ELA que resalte áreas manipuladas visualmente y lo integre a la interfaz.
RT09	Utilizar bibliotecas específicas para la extracción de metadatos, como **ExifTool** o soluciones similares, adaptadas a la arquitectura móvil.

Tabla 13: Requerimientos Técnicos - integración de análisis

Código	Seguridad
RT10	Proteger la comunicación entre la aplicación y Firebase mediante el uso de protocolos seguros como **HTTPS**.
RT11	Implementar reglas de acceso en Firebase Storage, restringiendo el acceso a imágenes y datos solo a usuarios autenticados.
RT12	Encriptar la información sensible almacenada en Firebase, como los datos de usuario y análisis.

Tabla 14: Requerimientos Técnicos - seguridad

3.2.3 Requerimientos Operativos

Código	Gestión de usuarios
RO01	Permitir el acceso simultáneo de múltiples usuarios a la aplicación sin afectar el rendimiento.
RO02	Registrar las acciones realizadas por cada usuario (inicio de sesión, subida de imágenes, generación de reportes) en un log para auditoría.

Tabla 15: Requerimientos Operativos - gestión de usuario

Código	Rendimiento
RO03	Optimizar la carga de las páginas de análisis y reportes para que el tiempo de respuesta no exceda los 5 segundos.
RO04	Asegurar que el análisis de imágenes (LSB, ELA y metadatos) se complete en menos de 10 segundos para imágenes de hasta 5 MB.

Tabla 16: Requerimientos Operativos – rendimiento

Código	Documentacion
RO05	Proveer documentación para el uso de la aplicación.
RO06	Incluir una guía de usuario accesible desde la aplicación.

Tabla 17: Requerimientos Operativos – documentación

3.2 Diseño de la propuesta

3.2.1 Arquitectura del sistema

La arquitectura Modelo-Vista-Controlador (MVC) es un patrón de diseño utilizado para estructurar aplicaciones de software, promoviendo la separación de responsabilidades entre los componentes principales. Este enfoque divide la aplicación en tres partes: el Modelo, que gestiona los datos y la lógica de negocio. La Vista, que se encarga de la presentación y la interacción con el usuario. Y el Controlador, que actúa como intermediario, procesando las solicitudes del usuario, coordinando la interacción entre el Modelo y la Vista. Al utilizar MVC en nuestra aplicación móvil forense, se facilita el mantenimiento y la escalabilidad del software, permitiendo que cada componente sea desarrollado y actualizado de manera independiente, lo que mejora la eficiencia en el desarrollo y asegura una mayor flexibilidad en la implementación de nuevas funcionalidades [54].

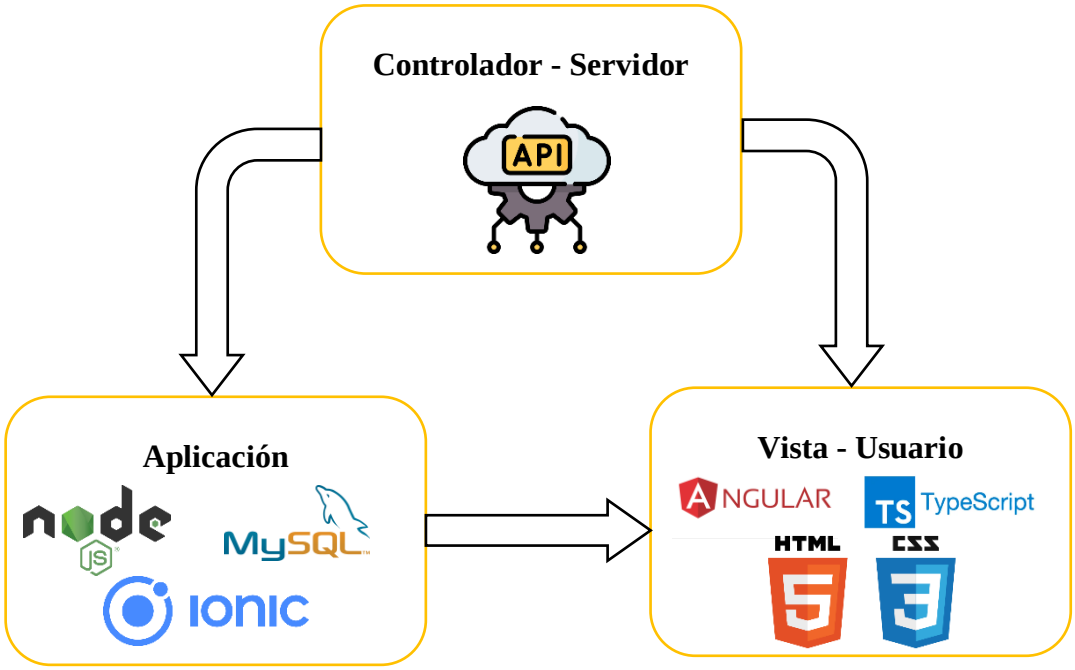


Figura 16: Arquitectura del sistema

3.2.2 Diagrama de caso de uso

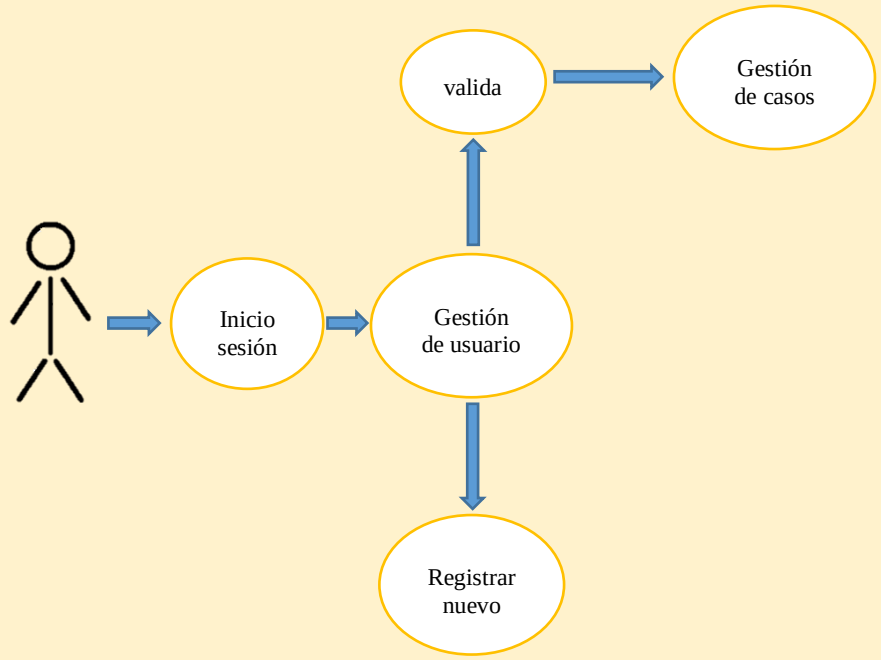
Caso de uso inicio de sesión - creación	
Actor	Cliente
Descripción	Ingresar a la aplicación con su usuario y contraseña o registrar nuevo usuario
Flujo básico	1. Se muestra en pantalla de la aplicación el apartado de login / inicio sesión 2. El cliente procede a ingresar sus credenciales (usuario, contraseña). 3. Se verifica las credenciales ingresadas 4. Si existe el cliente en la base de datos se deja ingresar a gestionar los casos de ese usuario. 5. Si en caso contrario no existe, no permitirá ingresar hasta que se registre
Código	Ver código fuente 1
	

Tabla 18: Caso de uso inicio de sesión – creación

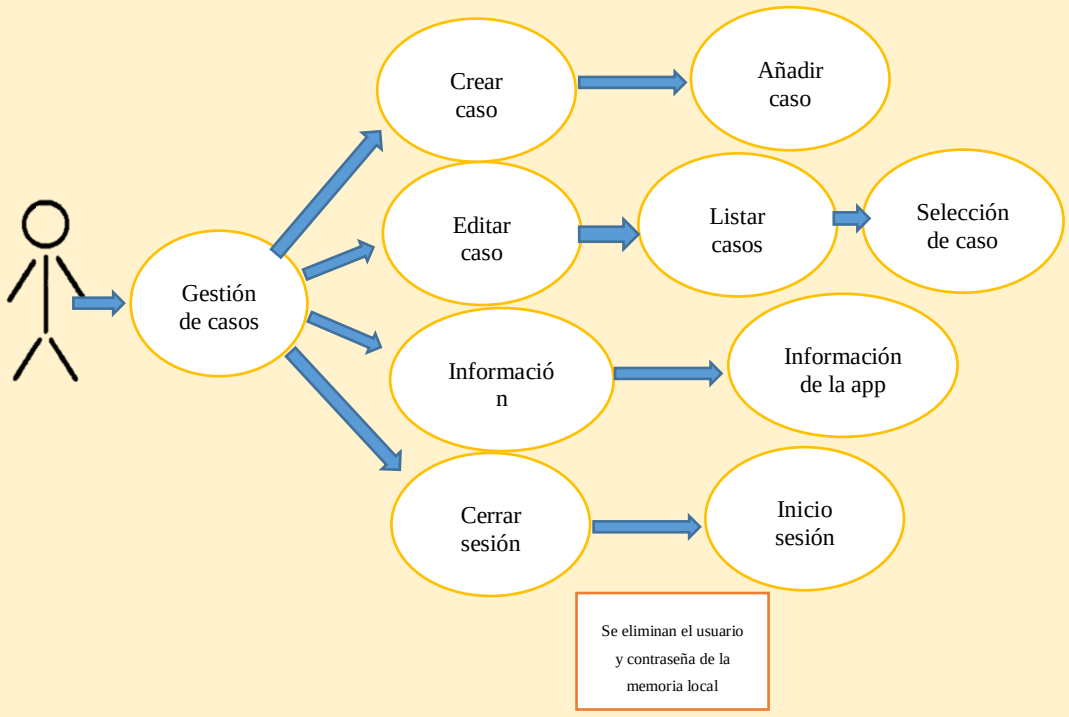
Caso de uso gestión de casos	
Actor	Cliente
Descripción	Registrar un nuevo caso, listar casos iniciados, ver información de aplicación, cerrar sesión.
Flujo básico	1. Se muestra en pantalla 4 opciones, nuevo caso, editar caso, información, cerrar sesión. 2. Si el cliente no tiene casos iniciados o es nuevo, deberá ingresar un nuevo caso para dar uso de las herramientas. 3. En caso de que tenga casos iniciados, se verá una lista de casos en la pantalla de casos. 4. Si desea información sobre la aplicación o sobre la esteganografía podrá ir al apartado de información. 5. Por último se muestra una pantalla de cerrar sesión.
código	Ver código fuente 2
	

Tabla 19: Caso de uso gestión de casos

Caso de uso pantalla principal	
Actor	Cliente
Descripción	Visualiza todas las opciones para hacer pruebas estegoanalíticas y opciones para visualizar los reportes generados por el cliente.
Flujo básico	1. Se muestra en pantalla 3 botones y un menú, dentro del menú existen 10 opciones. 2. Opción 1 - Analizar Imagen (ver código fuente 4) 3. Opción 2 - Integridad de Imagen (ver código fuente 5) 4. Opción 3 – Extraer Metadatos (ver código fuente 6) 5. Opción 4 – Ver/Subir Imágenes (ver código fuente 7) 6. Opción 5 – Estadísticas (ver código fuente 8) 7. Opción 6 – Reportes estegoanálisis (ver código fuente 9) 8. Opción 7 – Reportes de Integridad (ver código fuente 10) 9. Opción 8 – Reporte de metadatos (ver código fuente 11) 10. Opción 9 – Información (ver código fuente 12) 11. Opción 10 – salir 12. Botón 1 – Información, si entra en esta página vera una guía de cómo usar la app. 13. Botón 2 – Terminar el caso, si en caso de que ya no quiera o no necesite analizar más imágenes puede terminar el caso y ver un lista de todos los reportes realizados. 14. Botón 3 – salir del caso, se dirige directamente a la pantalla de gestión de casos
código	Ver código fuente 3

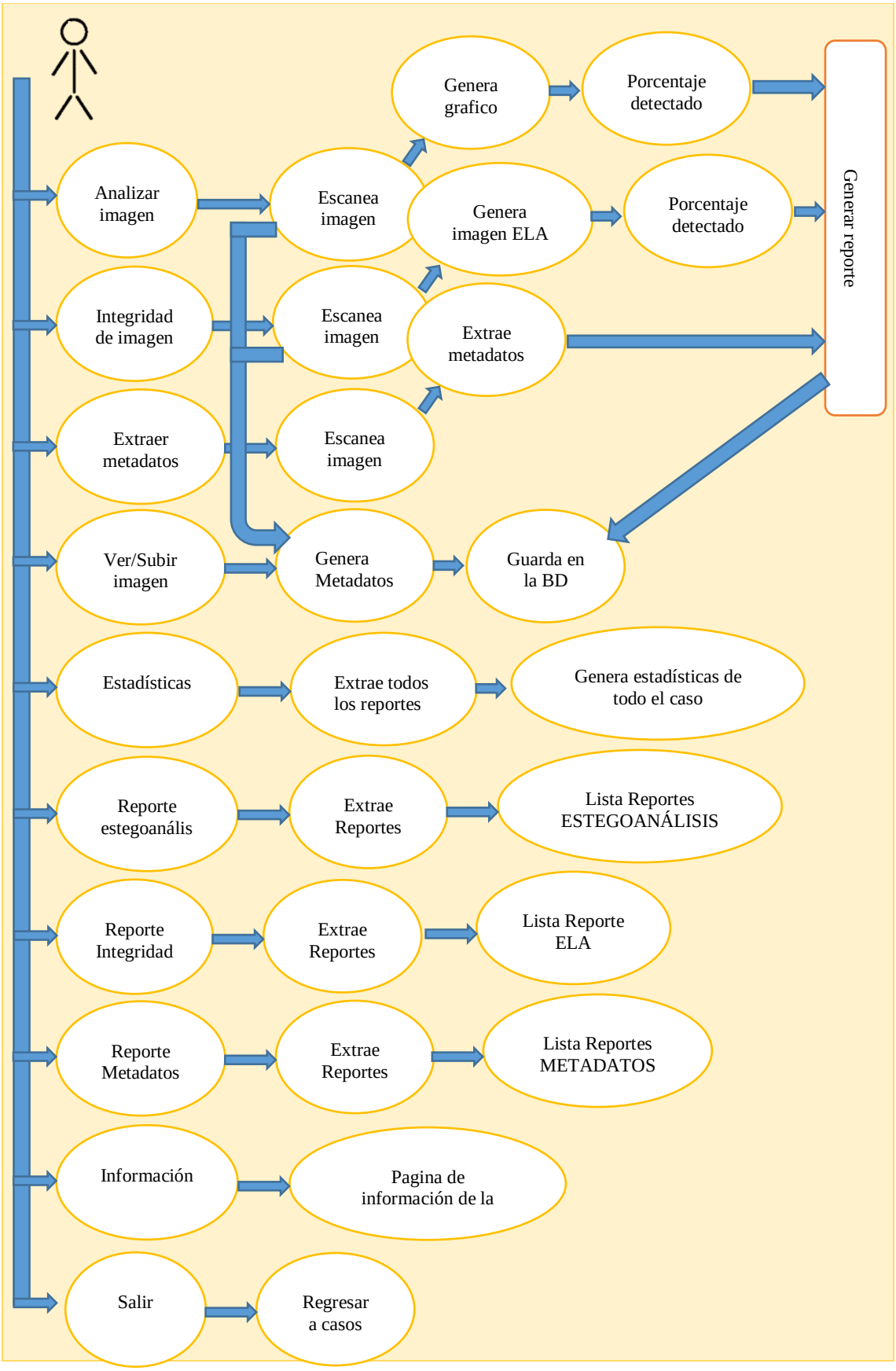

Analizar imagen
Integridad de imagen
Extraer metadatos
Ver/Subir imagen
Estadísticas
Reporte estegoanális
Reporte Integridad
Reporte Metadatos
Información
Salir
Escanea imagen
Escanea imagen
Escanea imagen
Genera Metadatos
Genera grafico
Genera imagen ELA
Extrae metadatos
Guarda en la BD
Porcentaje detectado
Porcentaje detectado
Generar reporte
Extrae todos los reportes
Genera estadísticas de todo el caso
Extrae Reportes
Lista Reportes ESTEGOANÁLISIS
Extrae Reportes
Lista Reporte ELA
Extrae Reportes
Lista Reportes METADATOS
Pagina de información de la
Regresar a casos

Tabla 20: Caso de uso pantalla principal

3.2.3 Modelo de datos

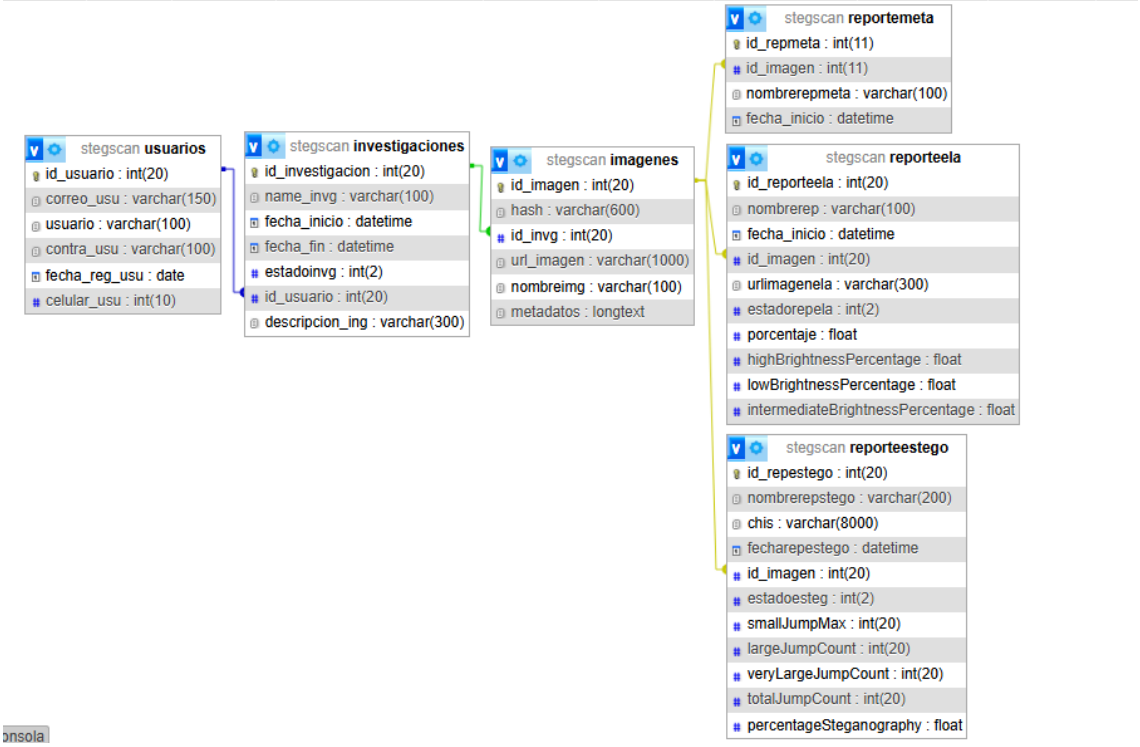


Figura 17: Modelo de datos

La base de datos "stegscan" está diseñada para una aplicación móvil forense enfocada en el análisis de imágenes en formato JPG/JPEG. Su estructura relacional permite gestionar usuarios, investigaciones, imágenes y reportes generados a partir de distintos análisis (metadatos, ELA y estegoanálisis).

Propósito General:

Proveer una solución para almacenar y gestionar de manera eficiente los datos relacionados con el análisis forense de imágenes. La base de datos soporta el flujo de trabajo de la aplicación, desde el registro de usuarios e investigaciones, hasta la generación y consulta de reportes técnicos.

3.2.4 Diseño de Interfaces

3.2.4.1 Página de registro de usuarios

Inicio de sesión / Registro de usuario / Éxito al registrar usuario

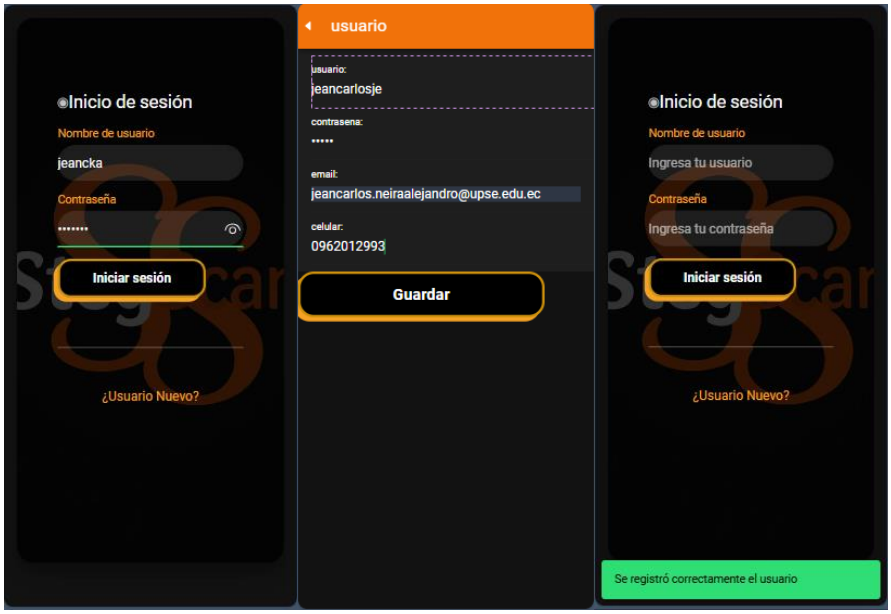


Figura 18: Inicio de sesión / Figura 19: Registro de usuario / Figura 20: Éxito al registrar usuario

3.2.4.2 Pagina de registro de casos

Gestión de casos / Registro caso / Editar caso

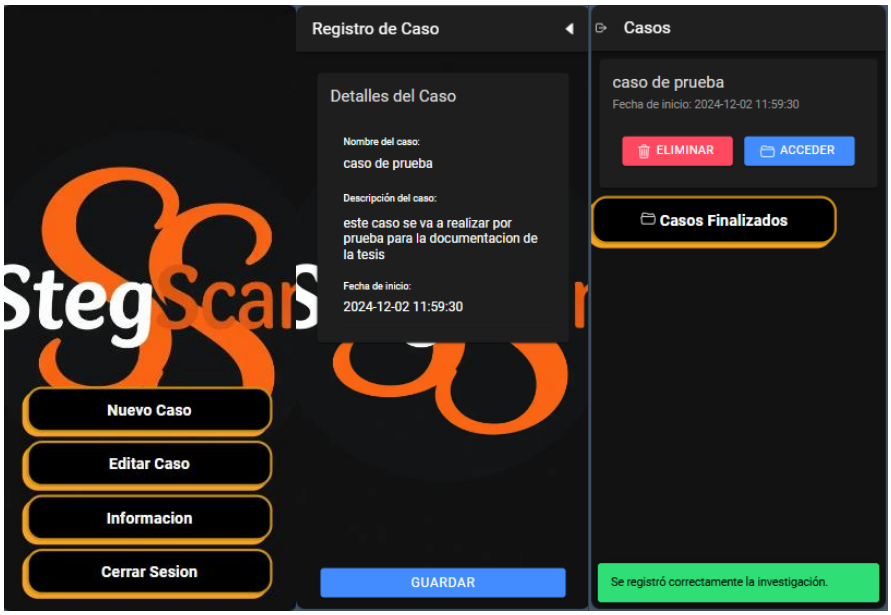


Figura 21: Gestión de casos / Figura 22: Registro caso / Figura 23: Editar caso

3.2.4.3 Pantalla principal dentro del caso

Menú del caso

Figura 24: Pantalla principal dentro del caso / Figura 25: Menú del caso

3.2.4.4 Página de insertar y enlistar imágenes

Insertar-enlistar imagen / Selección de imagen / Verificación en la lista

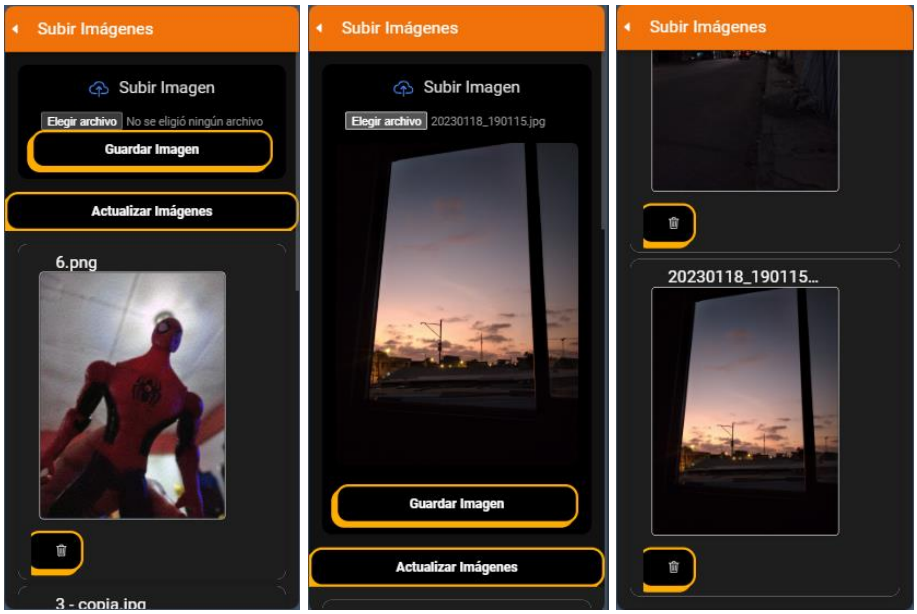


Figura 26: Pagina de insertar y enlistar imágenes / Figura 27: Selección de imagen / Figura 28: Verificación en la lista

3.2.4.4 Página de estegoanálisis

Estegoanálisis / Inserción de imagen y analizar / Resultados de estegoanálisis / Generar reporte

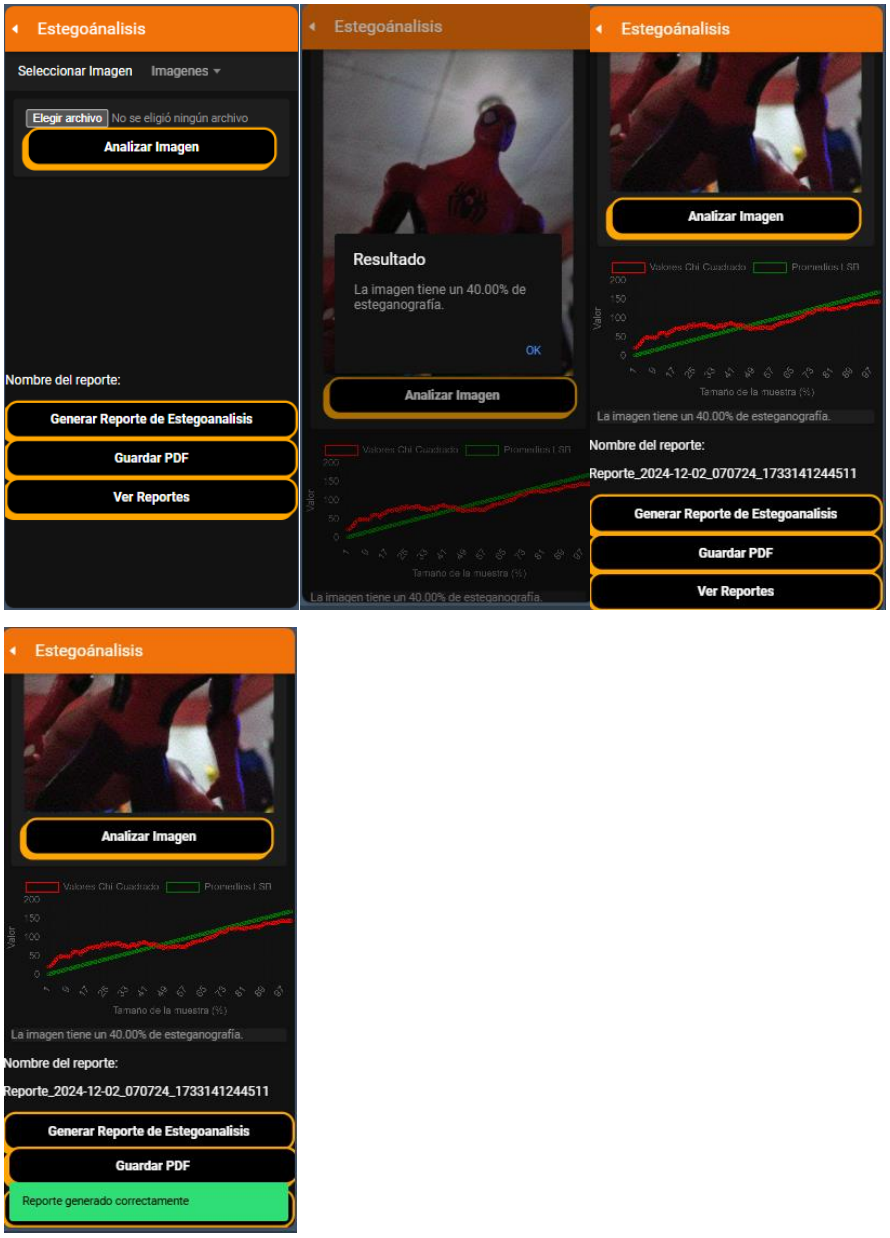


Figura 29: Página analizar imagen - Estegoanálisis

Figura 30: Inserción de imagen y analizar

Figura 31: Resultados de estegoanálisis

Figura 32: Generar reporte

Ver anexo reporte

3.2.4.5 Página de análisis ELA

Integridad de imagen / Inserción de imagen / Imagen con filtrado / Resultados del análisis / Generar reporte de la integridad

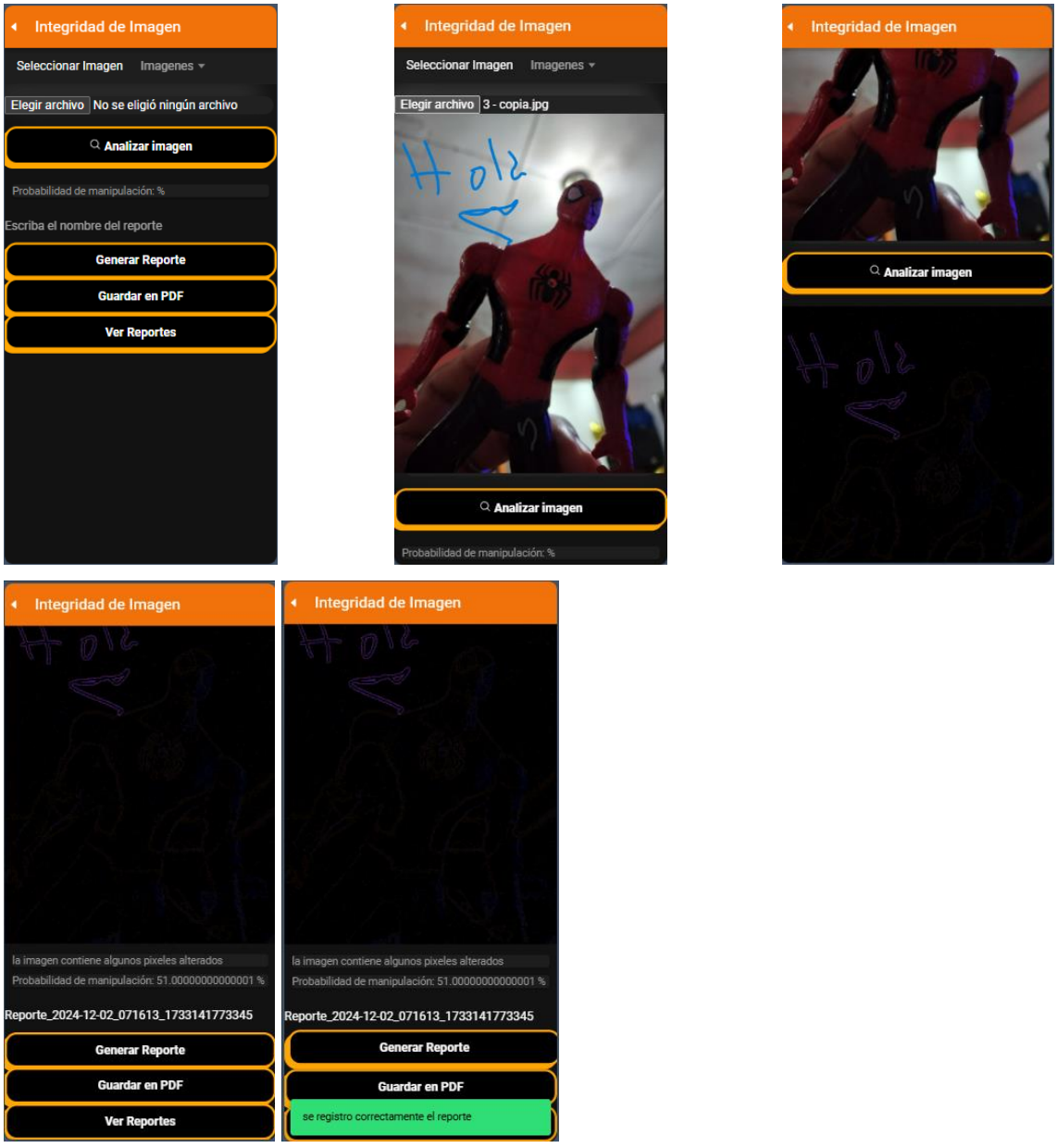


Figura 33: Pagina Integridad de imagen / Figura 34: Inserción de imagen / Figura 35: Imagen con filtrado / Figura 36: Resultados del análisis / Figura 37: Generar reporte de la integridad

Ver anexo reporte

3.2.4.6 Página de metadatos

Extraer metadatos / Inserción de imagen / Metadatos extraídos / Generar reporte metadatos

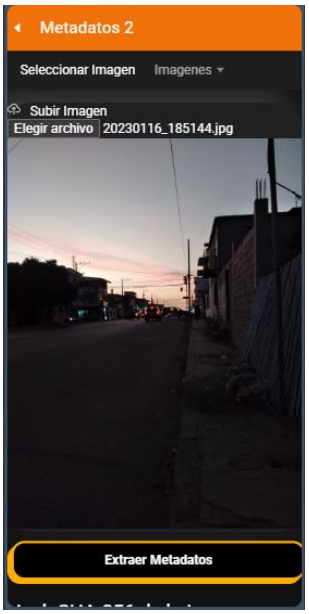


Figura 38: Pagina extraer metadatos / Figura 39: Inserción de imagen / Figura 40: Metadatos extraídos / Figura 41: Generar reporte metadatos

Ver anexo reporte

3.2.4.7 Página de reportes de investigación

Página reporte estegoanálisis / Página de reporte de integridad / Verificación de las dos imágenes / Página de reportes de metadatos

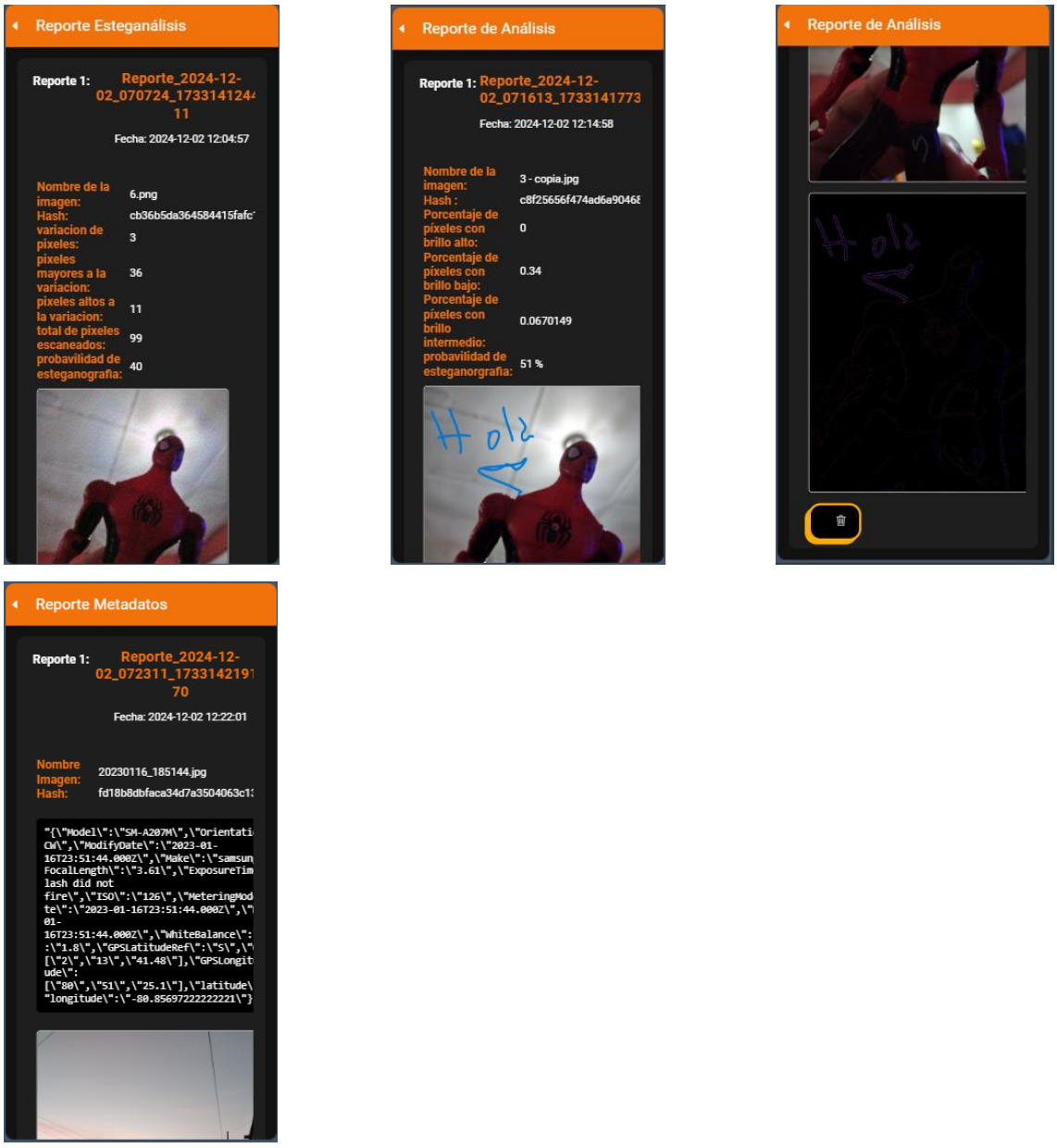


Figura 42: Pagina reporte estegoanálisis / Figura 43: Página de reporte de integridad / Figura 44: Verificación de las dos imágenes / Figura 45: Página de reportes de metadatos.

3.3 Desarrollo y prueba

3.3.1 Descripción del funcionamiento del código estegoanalítico [55]

El algoritmo analyzeImage analiza una imagen para detectar posibles indicios de esteganografía utilizando valores de Chi-Cuadrado y análisis de LSB (Least Significant Bit). Aquí están sus principales etapas y componentes:

- Validación inicial
    - Verifica que se haya seleccionado una imagen válida (local o URL).
    - Si la imagen no es válida, muestra un mensaje de error.
- Carga de la imagen
    - Carga la imagen en un objeto Image y utiliza un lienzo (Canvas) para procesarla.
    - Extrae los datos de la imagen (ImageData) como matriz de píxeles.
- Cálculo de Chi-Cuadrado y análisis LSB
    - Método calculateChiSquare:
        - Divide la imagen en bloques para obtener una muestra.
        - Calcula valores observados (frecuencia de píxeles) y valores esperados (promedios pares e impares).
        - Calcula el valor de Chi-Cuadrado para medir la desviación entre los valores observados y esperados.
        - Analiza los bits menos significativos (LSB) de los píxeles para detectar patrones anómalos.
- Análisis de saltos en Chi-Cuadrado
    - Calcula las diferencias entre valores consecutivos de Chi-Cuadrado.
    - Identifica y clasifica saltos como "pequeños", "grandes" o "muy grandes".
    - Usa estos datos para determinar un porcentaje de probabilidad de esteganografía.
- Decisión final
    - Si el porcentaje de esteganografía supera un umbral (25%), marca la imagen como alterada.
    - Muestra el resultado con un mensaje y un gráfico de los valores analizados.

3.3.2 Descripción del funcionamiento del código análisis de nivel de error (ELA)

Flujo Principal

- performELA(file):
    - Compara los píxeles de la imagen original y comprimida.
    - Calcula diferencias RGB escaladas por un factor (scale).
    - Clasifica píxeles en tres categorías según brillo:
        - Alto: Brillo > 200.
        - Intermedio: 100 < Brillo ≤ 200.
        - Bajo: 50 < Brillo ≤ 100
    - Genera una nueva imagen con las diferencias resaltadas y calcula métricas de manipulación. .

Métricas Calculadas

1. Porcentajes de Brillo:
    - % de píxeles con brillo alto, intermedio y bajo.
2. Relación Alto/Bajo:
    - Mide la proporción de áreas altamente manipuladas respecto a áreas poco manipuladas.
3. Porcentaje Final:
    - Ajusta el porcentaje de alteraciones detectadas según las métricas.

Clasificación de Manipulaciones

- Basado en los valores calculados:
    - Alta manipulación: Si brillo alto > 5% o relación alto/bajo > 1.5.
    - Posible manipulación: Si brillo bajo o intermedio supera ciertos límites.
    - Sin alteraciones significativas: Si brillo bajo < 0.01%.

Resultados Visuales

- Genera una nueva imagen procesada (ELA) con las alteraciones resaltadas.
- Guarda la imagen procesada como un archivo ela_image.jpg.

3.3.3 Descripción del funcionamiento del código de extracción de metadatos

El código extrae metadatos de una imagen cargada utilizando exifr como método principal. Si falla, emplea un método alternativo para obtener información básica del archivo (nombre, tamaño, tipo y última modificación). Además, genera un hash SHA-256 del archivo como identificador único. Según el éxito o fallo de la extracción, muestra mensajes al usuario y actualiza la interfaz para generar reportes.

3.3.4 Pruebas

Pruebas de estegoanálisis

Datos del experimento			
Título del experimento:	Prueba de esteganografía en archivo 1	Realizado por:	Jeancarlos Josue Neira Alejandro
No. Prueba:	A-01	Fecha inicio:	1/12/2024
Tipo prueba:	Experimental	Fecha fin:	1/12/2024
Detalles del experimento			
Objetivo del experimento:	Detectar qué porcentaje de esteganografía que contiene la imagen	Modulo:	Analizar Imagen-Esteganografía
Nivel complejidad prueba:	Medio	Tiempo ejecución:	5 minutos
Descripción de la imagen			
Tipo de imagen:	JPG/JPEG	Inserción de esteganografía en la imagen	SI

Tamaño de la imagen:	781 KB (800.164 bytes) Imagen1	Tipo de esteganografía	LSB con CriptoStego.
Evaluación de la imagen			
Procedimientos		Descripción del procedimiento	
• Entrar al apartado de análisis de imágenes. • Ingresar imagen a escanear o buscar en la base de datos por el nombre de la imagen. • Dar al botón “Analizar Imagen” • Esperar a que se cargue la imagen en la base de datos y haga los cálculos. • Visualiza el porcentaje de esteganografía en la imagen • Visualiza el grafico de líneas de chi-cuadrado de la imagen • Generación de el nombre del reporte automático • Dar en el botón de generar reporte • Esperar a que se guarde en la base de datos • Dar en el botón “Guardar pdf” para poder visualizar a más detalle el reporte		Anexo 4.2 - Escaneo de la imagen 1 y generación de reporte	
Resultados esperados		Resultados obtenidos	

Se visualice un porcentaje de esteganografía dependiendo de qué tan variado este el análisis chi-cuadrado, visualizar que el porcentaje este acorde a la gráfica mostrada, llegar a una conclusión dependiendo de del porcentaje y la grafica	El porcentaje visualizado fue un **54.9 %** de probabilidad de esteganografía. Acorde a la gráfica se muestra una variación drástica en los parámetros chi-cuadrado, esto indica que tiene esteganografía.
Conclusión	Valido ■
Cuando una imagen es cambiada o modificada en los LSB con el método chi-cuadrado que genera una estadística evaluando si existe una diferencia significativa entre una distribución observada de datos y una distribución esperada.	Invalido ☐
	No concluyente ☐

Tabla 21: Pruebas de estegoanálisis P1

Datos del experimento			
Título del experimento:	Prueba de esteganografía en archivo 2	Realizado por:	Jeancarlos Josue Neira Alejandro
No. Prueba:	A-02	Fecha inicio:	1/12/2024
Tipo prueba:	Experimental	Fecha fin:	1/12/2024
Detalles del experimento			
Objetivo del experimento:	Detectar qué porcentaje de	Modulo:	Analizar Imagen-Esteganografía

	esteganografía que contiene la imagen		
Nivel complejidad prueba:	Medio	Tiempo ejecución:	5 minutos
Descripción de la imagen			
Tipo de imagen:	JPG/JPEG	Inserción de esteganografía en la imagen	No
Tamaño de la imagen:	1,97 MB (2.067.007 bytes) Imagen2	Tipo de esteganografía	NULL
Evaluación de la imagen			
Procedimientos		Descripción del procedimiento	
• Entrar al apartado de análisis de imágenes. • Ingresar imagen a escanear o buscar en la base de datos por el nombre de la imagen. • Dar al botón “Analizar Imagen” • Esperar a que se cargue la imagen en la base de datos y haga los cálculos. • Visualiza el porcentaje de esteganografía en la imagen • Visualiza el grafico de líneas de chi-cuadrado de la imagen		Anexo 5.2 - Escaneo de la imagen 2 y generación de reporte	

• Generación de el nombre del reporte automático • Dar en el botón de generar reporte • Esperar a que se guarde en la base de datos • Dar en el botón "Guardar pdf" para poder visualizar a más detalle el reporte	
Resultados esperados	Resultados obtenidos
Se visualice un porcentaje de esteganografía dependiendo de qué tan variado este el análisis chi-cuadrado, visualizar que el porcentaje este acorde a la gráfica mostrada, llegar a una conclusión dependiendo de del porcentaje y la grafica	El porcentaje visualizado fue un **8.7 %** de probabilidad de esteganografía. Acorde a la gráfica se muestra que no hay una variación drástica de los valores chi-cuadrado, esto indica que no tiene esteganografía.
Conclusión	Valido ■
El análisis de imágenes originales suele tener una variación de los parámetros chi-cuadrado si mucha distorsión. Lo cual indicar que una imagen es original.	Invalido ☐
	No concluyente ☐

Tabla 22: Pruebas de estegoanálisis P2

Datos del experimento			
Título del experimento:	Prueba de esteganografía en archivo 3	Realizado por:	Jeancarlos Josue Neira Alejandro
No. Prueba:	A-03	Fecha inicio:	1/12/2024

Tipo prueba:	Experimental	Fecha fin:	1/12/2024
Detalles del experimento			
Objetivo del experimento:	Detectar qué porcentaje de esteganografía que contiene la imagen	Modulo:	Analizar Imagen-Esteganografía
Nivel complejidad prueba:	Medio	Tiempo ejecución:	5 minutos
Descripción de la imagen			
Tipo de imagen:	JPG/JPEG	Inserción de esteganografía en la imagen	Si
Tamaño de la imagen:	750 KB (768.070 bytes) Imagen3	Tipo de esteganografía	LSB – con CriptoStego
Evaluación de la imagen			
Procedimientos		Descripción del procedimiento	
• Entrar al apartado de análisis de imágenes. • Ingresar imagen a escanear o buscar en la base de datos por el nombre de la imagen. • Dar al botón “Analizar Imagen” • Esperar a que se cargue la imagen en la base de datos y haga los cálculos.		Anexo 6.2 - Escaneo de la imagen 3 y generación de reporte	

<table>
<tr><td>

- Visualiza el porcentaje de esteganografía en la imagen
- Visualiza el grafico de líneas de chi-cuadrado de la imagen
- Generación de el nombre del reporte automático
- Dar en el botón de generar reporte
- Esperar a que se guarde en la base de datos
- Dar en el botón “Guardar pdf” para poder visualizar a más detalle el reporte

</td><td></td></tr>
<tr><td>Resultados esperados</td><td>Resultados obtenidos</td></tr>
<tr><td>Se visualice un porcentaje de esteganografía dependiendo de qué tan variado este el análisis chi-cuadrado, visualizar que el porcentaje este acorde a la gráfica mostrada, llegar a una conclusión dependiendo de del porcentaje y la grafica</td><td>El porcentaje visualizado fue un 47.2 % de probabilidad de esteganografía.

En esta ocasión en el porcentaje y en la gráfica se muestran fluctuaciones grandes en varios parámetros del análisis chi-cuadrado, esto indica que si tiene esteganografía.</td></tr>
<tr><td>Conclusión</td><td>Valido ■</td></tr>
<tr><td rowspan="2">Siendo la misma imagen que en la prueba 2 pero con esteganografía concluimos que por el análisis de chi-cuadrado podemos observar y detectar fluctuaciones en imágenes.</td><td>Invalido □</td></tr>
<tr><td>No concluyente □</td></tr>
</table>

Tabla 23: Pruebas de estegoanálisis P3

Datos del experimento			
Título del experimento:	Prueba de esteganografía en archivo 4	Realizado por:	Jeancarlos Josue Neira Alejandro
No. Prueba:	A-04	Fecha inicio:	1/12/2024
Tipo prueba:	Experimental	Fecha fin:	1/12/2024
Detalles del experimento			
Objetivo del experimento:	Detectar qué porcentaje de esteganografía que contiene la imagen	Modulo:	Analizar Imagen-Esteganografía
Nivel complejidad prueba:	Medio	Tiempo ejecución:	5 minutos
Descripción de la imagen			
Tipo de imagen:	JPG/JPEG	Inserción de esteganografía en la imagen	No
Tamaño de la imagen:	2,05 MB (2.151.529 bytes) Imagen4	Tipo de esteganografía	NULL
Evaluación de la imagen			
Procedimientos		Descripción del procedimiento	
• Entrar al apartado de análisis de imágenes.		Anexo 7.2 - Escaneo de la imagen 4 y generación de reporte	

• Ingresar imagen a escanear o buscar en la base de datos por el nombre de la imagen. • Dar al botón “Analizar Imagen” • Esperar a que se cargue la imagen en la base de datos y haga los cálculos. • Visualiza el porcentaje de esteganografía en la imagen • Visualiza el grafico de líneas de chi-cuadrado de la imagen • Generación de el nombre del reporte automático • Dar en el botón de generar reporte • Esperar a que se guarde en la base de datos • Dar en el botón “Guardar pdf” para poder visualizar a más detalle el reporte	
Resultados esperados	Resultados obtenidos
Se visualice un porcentaje de esteganografía dependiendo de qué tan variado este el análisis chi-cuadrado, visualizar que el porcentaje este acorde a la gráfica mostrada, llegar a una conclusión dependiendo de del porcentaje y la grafica	El porcentaje visualizado fue un **23.4 %** de probabilidad de esteganografía. En la gráfica resultante de chi-cuadrado no se muestra ni un valor fuera de lo común y el porcentaje no es tan alto, por lo tanto, podría concluir que en esta imagen no tiene esteganografía.
Conclusión	Valido

Las imágenes originales pueden dar a veces falsos positivos dependiendo de qué tan fluctuada este la imagen, pero visualizando el grafico de chi-cuadrado se podría llegar a una conclusión.	Invalido ☐ No concluyente ☐

Tabla 24: Pruebas de estegoanálisis P4

Datos del experimento			
Título del experimento:	Prueba de esteganografía en archivo 5	Realizado por:	Jeancarlos Josue Neira Alejandro
No. Prueba:	A-05	Fecha inicio:	1/12/2024
Tipo prueba:	Experimental	Fecha fin:	1/12/2024
Detalles del experimento			
Objetivo del experimento:	Detectar qué porcentaje de esteganografía que contiene la imagen	Modulo:	Analizar Imagen-Esteganografía
Nivel complejidad prueba:	Medio	Tiempo ejecución:	5 minutos
Descripción de la imagen			
Tipo de imagen:	JPG/JPEG	Inserción de esteganografía en la imagen	Si

Tamaño de la imagen:	37,1 MB (38.937.654 bytes) Imagen5	Tipo de esteganografía	¿? (inyección esteganográfica desconocida) – con Quickstego
Evaluación de la imagen			
Procedimientos		Descripción del procedimiento	
• Entrar al apartado de análisis de imágenes. • Ingresar imagen a escanear o buscar en la base de datos por el nombre de la imagen. • Dar al botón "Analizar Imagen" • Esperar a que se cargue la imagen en la base de datos y haga los cálculos. • Visualiza el porcentaje de esteganografía en la imagen • Visualiza el grafico de líneas de chi-cuadrado de la imagen • Generación de el nombre del reporte automático • Dar en el botón de generar reporte • Esperar a que se guarde en la base de datos • Dar en el botón "Guardar pdf" para poder visualizar a más detalle el reporte		Anexo 8.2 - Escaneo de la imagen 5 y generación de reporte	
Resultados esperados		Resultados obtenidos	

<table>
<tr><td>Se visualice un porcentaje de esteganografía dependiendo de qué tan variado este el análisis chi-cuadrado, visualizar que el porcentaje este acorde a la gráfica mostrada, llegar a una conclusión dependiendo de del porcentaje y la grafica</td><td>El porcentaje visualizado fue un 39.4 % de probabilidad de esteganografía.

Las variaciones de chi-cuadrado se ven un poco constantes, pero si se nota pequeñas fluctuaciones, sumando el porcentaje de probabilidad de esteganografía, podríamos indicar que si contiene.</td></tr>
<tr><td>Conclusión</td><td>Valido ■</td></tr>
<tr><td rowspan="2">Siendo la misma imagen que en la prueba 4 pero con esteganografía hecha con la herramienta de QuickStego el cual no está claro que método de inyección de esteganografía usa, se puede verificar el porcentaje de esteganografía contiene también dependiendo del gráfico.</td><td>Invalido ☐</td></tr>
<tr><td>No concluyente ☐</td></tr>
</table>

Tabla 25: Pruebas de estegoanálisis P5

3.4 Resultados de la investigación.

El desarrollo de la aplicación móvil para verificar la autenticidad e integridad de imágenes a través de técnicas forenses resultó en una herramienta integral diseñada para profesionales en el ámbito de la informática forense, como peritos informáticos y especialistas en ciberseguridad, pero intuitiva para ser utilizada por cualquier persona. La aplicación implementa funcionalidades clave, como el análisis de metadatos y el uso de métodos estegoanalíticos, incluido el análisis de nivel de error (ELA) y la detección de manipulación por medio de algoritmos especializados como LSB y chi-cuadrado. Estas herramientas permiten identificar alteraciones en imágenes digitales, y determinar la presencia de datos ocultos en formatos JPEG/JPG.

La funcionalidad principal se centra en el análisis de imágenes, donde los usuarios pueden cargar imágenes desde Firebase, aplicar técnicas de estegoanálisis y obtener un informe detallado sobre la posible manipulación y autenticidad de las imágenes. La integración

con Firebase no solo garantiza un almacenamiento seguro y eficiente, sino que también permite el acceso de manera rápida y confiable.

El impacto positivo de la aplicación se evidencia en varios aspectos. Los profesionales pueden contar con una herramienta para garantizar la autenticidad de imágenes utilizadas en investigaciones judiciales, peritajes informáticos y análisis de ciberseguridad. La implementación de técnicas forenses avanzadas reduce significativamente el riesgo de manipulación de información visual y mejora la confianza en los resultados presentados en contextos legales y técnicos.

3.4.1 Resultados de la encuesta

El objetivo de esta encuesta es verificar el conocimiento sobre la esteganografía o ediciones de imágenes, por eso se realizó esta encuesta a 17 estudiantes de la universidad estatal península de Santa Elena del periodo académico 2024-2.

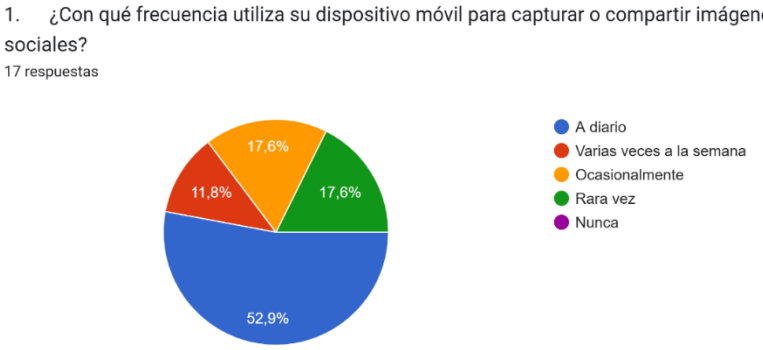


Figura 46: Encuesta - Pregunta 1

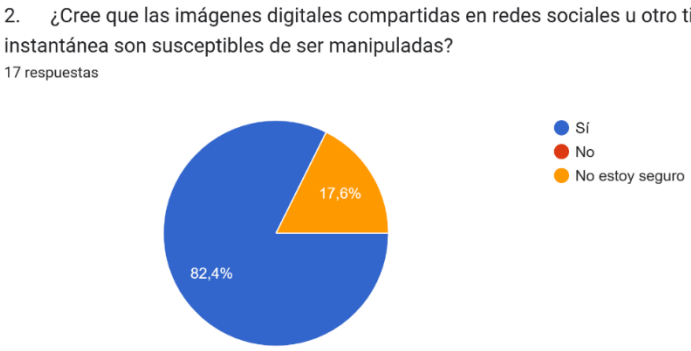


Figura 47: Encuesta - Pregunta 2

3. ¿Ha utilizado alguna vez software para editar imágenes digitales?

17 respuestas

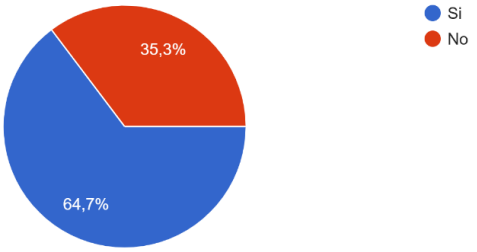


Figura 48: Encuesta - Pregunta 3

4. ¿Ha oído hablar del término "esteganografía" y su uso para ocultar información en imágenes digitales?

17 respuestas

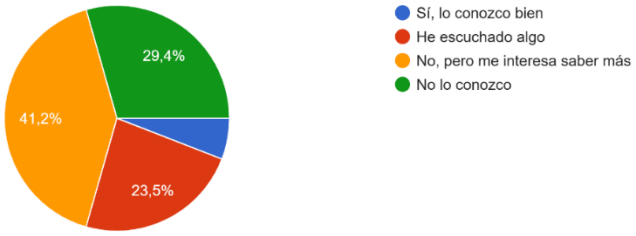


Figura 49: Encuesta - Pregunta 4

5. ¿Cree que la manipulación de imágenes digitales puede influir negativamente en la reputación o la privacidad de una persona?

17 respuestas

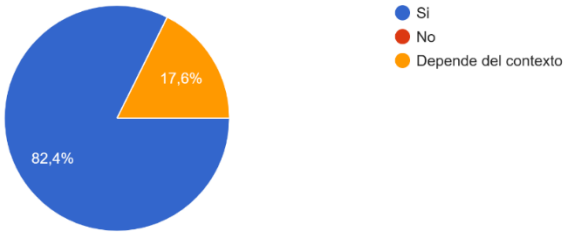


Figura 50: Encuesta - Pregunta 5

6. ¿Cuán confiable le parecen las imágenes que circulan en redes sociales en cuanto a su autenticidad y veracidad?

17 respuestas

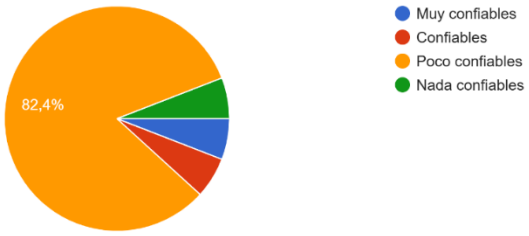


Figura 51: Encuesta - Pregunta 6

7. ¿Qué tan preocupante le parece el riesgo de que imágenes manipuladas se utilicen para difundir información falsa o engañosa?

17 respuestas

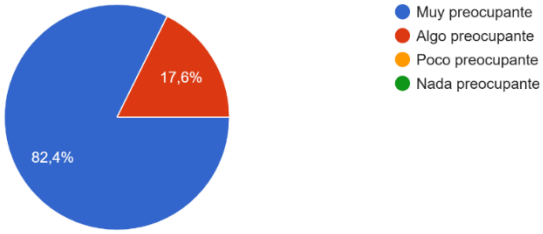


Figura 52: Encuesta - Pregunta 7

8. ¿Cuál considera que es el mayor riesgo asociado con la manipulación de imágenes digitales en el ámbito de la ciberseguridad?

17 respuestas

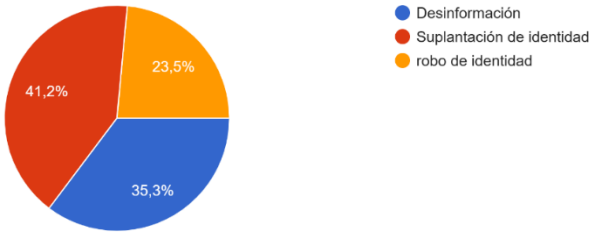


Figura 53: Encuesta - Pregunta 8

9. ¿Ha oído hablar de técnicas como el estegoanálisis o el análisis de metadatos para detectar manipulación en imágenes?

17 respuestas

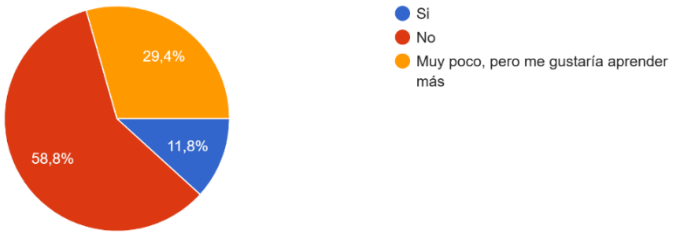


Figura 54: Encuesta - Pregunta 9

10. ¿Estaría dispuesto a usar una aplicación móvil para verificar la autenticidad de las imágenes que comparte o recibe?

17 respuestas

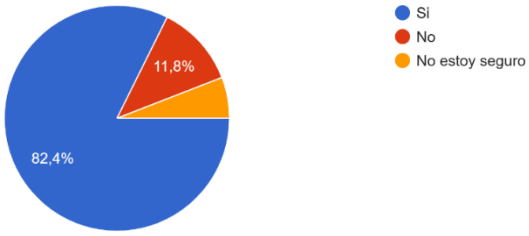


Figura 55: Encuesta - Pregunta 10

CONCLUSIONES

- El desarrollo de la aplicación móvil de análisis forense para validar imágenes fue primordial en la detección de manipulaciones y datos ocultos. Con la integración de tres técnicas principales: estegoanálisis (LSB y Chi-cuadrado), análisis de nivel de error (ELA) y extracción de metadatos, la herramienta brinda un enfoque práctico y completo para analizar imágenes en formato JPEG/JPG. Esto permite a los usuarios de smartphone identificar alteraciones o rastros de ocultamiento de forma más precisa y accesible.
- La implementación del estegoanálisis Chi-cuadrado destacó por su efectividad para detectar variaciones de bits en los LSB que oculta datos en las imágenes digitales. Estas técnicas ofrecen un análisis detallado que facilita la identificación de patrones sospechosos y asegura que los usuarios puedan tomar decisiones fundamentadas.
- El análisis de nivel de error (ELA) se convirtió en una pieza clave para evidenciar alteraciones en imágenes. Esta técnica permite a los usuarios visualizar de manera sencilla las áreas modificadas, haciendo que el análisis de posibles manipulaciones sea más claro y directo.
- La funcionalidad de extracción de metadatos complementó el análisis forense al proporcionar información técnica adicional de las imágenes, como la fecha de creación, el dispositivo usado, o detalles de edición. Aunque sencilla, esta función agrega un valor significativo al análisis general, más cuando se extrae o genera un hash único de la imagen para mayor credibilidad.
- La aplicación, diseñada para profesionales como peritos informáticos y auditores digitales, facilita tareas relacionadas con la validación de imágenes en investigaciones judiciales, auditorías corporativas y procesos de seguridad digital.
- Se implementaron pruebas para verificar la funcionalidad de la aplicación, logrando analizar sin ningún inconveniente las imágenes con y sin esteganografía dando una mayor validez a la aplicación
- La elaboración de reportes detallados dentro de la aplicación genera mayor validez en la aplicación, pudiendo ver a detalle la imagen, metadatos y resultados de los escaneos de las técnicas estegoanalíticas.

RECOMENDACIONES

- Sería útil ampliar la funcionalidad de la aplicación, incluyendo métodos adicionales de estegoanálisis, como algoritmos basados en inteligencia artificial o análisis de patrones en frecuencia. Esto podría aumentar la capacidad de detección de manipulaciones más complejas.
- Es recomendable que los usuarios cuenten con una guía o tutorial dentro de la misma aplicación. Esto les permitiría entender fácilmente cómo funcionan las tres técnicas implementadas y sacarles el máximo provecho en sus análisis diarios.
- Agregar un módulo para generar reportes automáticos con los resultados obtenidos podría facilitar el trabajo de los profesionales. Estos reportes podrían incluir detalles del análisis y capturas de las áreas alteradas, listos para ser presentados como evidencia o documentos oficiales.
- Explorar la compatibilidad de la aplicación con formatos de imagen adicionales, como PNG, TIFF o BMP, ampliaría su uso en distintos contextos donde los usuarios trabajan con diferentes tipos de archivos.
- Se sugiere implementar un sistema de actualización continúa basado en las necesidades de los usuarios. Esto podría incluir encuestas o mecanismos de retroalimentación que permitan identificar áreas de mejora o nuevas funciones deseadas.
- Incluir notificaciones o alertas que guíen al usuario durante el proceso de análisis podría mejorar aún más la experiencia, asegurando que no se pasen por alto posibles manipulaciones o errores en los resultados.
- Finalmente, sería interesante promocionar la aplicación entre instituciones, empresas y organismos judiciales para que adopten esta herramienta en sus procesos. Una estrategia de difusión adecuada posicionaría la app como una solución confiable y accesible dentro del campo de la informática forense.

BIBLIOGRAFÍA

[1] Guaña-Moya, Javier. "Usos Y Aplicaciones de La Esteganografía En La Era Digital Uses and Applications of Steganography in The..." ResearchGate, unknown, 29 June 2023, www.researchgate.net/publication/380018269_Usos_y_aplicaciones_de_la_esteganografia_en_la_era_digital_Uses_and_applications_of_steganography_in_the_digital_age. Accessed 14 Sept. 2024.

[2] Morocho E; Zambrano A; Carvajal J; López G. "Vista de Análisis del Algoritmo Esteganográfico F5 para Imágenes JPEG a Color," Epn.edu.ec, 2024. https://revistapolitecnica.epn.edu.ec/ojs2/index.php/revista_politecnica2/article/view/602/pdf (accessed Sep. 14, 2024).

[3] Luis Sifuentes "Análisis comparativo de técnicas de esteganálisis en imágenes digitales LSB" https://revistas.ulima.edu.pe/index.php/CIIS/article/download/5522/5225/. Accessed 14 Sept. 2024.

[4] P. Méndez; H Villa, A Cisneros "Nuevo algoritmo para la detección de bordes en imágenes para esteganografía" Universidad Nacional de Chimborazo, 11 de abril 2017 https://publicaciones.ucuenca.edu.ec/ojs/index.php/maskana/article/download/1449/pdf/4411. Accessed 14 Sept. 2024.

[5] Tomás Pevný, P. Bas, and J. Fridrich, "Steganalysis by Subtractive Pixel Adjacency Matrix," ResearchGate, Jul. 2010. https://www.researchgate.net/publication/40653276_Steganalysis_by_Subtractive_Pixel_Adjacency_Matrix (accessed Sep. 14, 2024).

[6] Lerch Hostalot, Daniel and D. Megías, "Esteganografía en zonas ruidosas de la imagen," Rua.ua.es, 2014, doi: https://doi.org/978-84-9717-323-0. Accessed 15 Sept. 2024. (accessed Sep. 14, 2024).

[7] R. Medina and N. G. Sergio, "Esteganografía: sustitución LSB 1 bit utilizando Matlab," Unlp.edu.ar, Jun. 2016, doi: http://sedici.unlp.edu.ar/handle/10915/53221. (accessed Sep. 14, 2024).

[8] S. Angie, “Análisis de la integridad de imágenes usando métodos estegoanalíticos y análisis de nivel de error ELA,” Upse.edu.ec, 2024, doi: https://doi.org/UPSE-TTI-2024-0005. (accessed Sep. 15, 2024).

[9] J. Dias. “esteganografía y estegoanálisis: ocultación de datos en streams de audio voris”. Madrid, sep. 2010. https://oa.upm.es/5353/2/TESIS_MASTER_JESUS_DIAZ_VICO.pdf

[10] Dejan Raković, “Error level analysis (ELA),” ResearchGate, 2023. https://www.researchgate.net/publication/373404409_Error_level_analysis_ELA (accessed Sep. 23, 2024).

[11] A. Nagm, M. Moussa, Rasha Shoitan, and H. I. Abdulwakel, “Detecting image manipulation with ELA- CNN integration: a powerful framework for authenticity verification,” ResearchGate, Aug. 08, 2024. https://www.researchgate.net/publication/382949014_Detecting_image_manipulation_with_ELA-_CNN_integration_a_powerful_framework_for_authenticity_verification (accessed Sep. 17, 2024).

[12] “Plan de Creación de Oportunidades 2021-2025 – Secretaría Nacional de Planificación,” Planificacion.gob.ec, 2021. https://www.planificacion.gob.ec/plan-de-creacion-de-oportunidades-2021-2025/ (accessed Sep. 24, 2024).

[13] M. Paz, M. Garcia. “Capitulo 3. Los métodos de investigacion”. https://www.ucm.es/data/cont/media/www/pag-135806/12%20metodologc3ada-1-garcia-y-martinez.pdf (accessed Sep. 24, 2024).

[14] Alberto, “Aplicación de la Técnica Error Level Analysis y metadatos para el estudio forense de imágenes producidas por dispositivos móviles.,” Unad.edu.co, 2017, doi: https://repository.unad.edu.co/handle/10596/12037

[15] Orlando Z. “Revista Científica General José María Córdova.”, Bogotá, 2006, Available: https://www.redalyc.org/pdf/4762/476259067004.pdf

[16] M. Benassini, “INTRODUCCIÓN A LA INVESTIGACIÓN DE MERCADOS.” Available: https://clea.edu.mx/biblioteca/files/original/89fd306f47a32a187ffcd3fa1f116370.pdf (accessed Sep. 24, 2024).

[17] José S.,” Aplicación del Modelo Incremental Para el Desarrollo del Sistema de Información Docente”, Mexico, Jun. 08, 2018. http://ri.uaemex.mx/bitstream/handle/20.500.11799/99005/TESIS+Aplicaci%F3n+del+Modelo+Incremental+Para+el+Desarrollo+del.pdf;jsessionid=9F21DCE9CF05CEFF5209918973232196?sequence=1

[18] “Modelo Incremental,” Blogspot.com, 2017. https://isw-udistrital.blogspot.com/2012/09/ingenieria-de-software-i.html (accessed Dec. 02, 2024).

[19] R. Leiva, “Vista de Evolución tecnológica y ciberseguridad,” Publicacionesacague.cl, 2024. https://publicacionesacague.cl/index.php/tica/article/view/157/173 (accessed Oct. 05, 2024).

[20] D. Renza, D. M. Ballesteros L., and R. Rincón, “Método de ocultamiento de píxeles para esteganografía de imágenes en escala de gris sobre imágenes a color,” Ingeniería y Ciencia, vol. 12, no. 23, pp. 145–162, Feb. 2016, doi: https://doi.org/10.17230/ingciencia.12.23.8

[21] W. Amilcar, “Análisis forense y antiforense de imágenes digitales mediante metadatos y esteganografía.pdf,” figshare, Apr. 2023, doi: https://doi.org/10.6084/m9.figshare.22584031.v1.

[22] A. Blanco, “Trabajo Fin de Máster.” Available: https://reunir.unir.net/bitstream/handle/123456789/2828/arnedo%20blanco.pdf

[23] “Evidencias digitales en la investigación informática forense.” Accessed: Oct. 02, 2024. [Online]. Available: http://cimogsys.espoch.edu.ec/direccion-publicaciones/public/docs/books/2024-01-22-174703-evidencias_digitales.pdf

[24] J. Diaz, “esteganografía y estegoanálisis: ocultación de datos en streams de audio voris” Sep. 2010, TESIS_MASTER_JESUS_DIAZ_VICO.pdf (upm.es) (accessed Oct. 05, 2024).

[25] “Metadatos Y La Prueba Pericial,” Peritos Judiciales Informaticos Sevilla Valencia Barcelona Madrid Málaga Canarias, Jun. 28, 2021. https://tecnoperitaciones.com/metadatos-y-la-prueba-pericial/ (accessed Dec. 02, 2024).

[26] B. Constanzo, A. Haydée, M. Castellote, and Info-Lab Laboratory, "Identificación y comparación de imágenes en ambientes forenses," ResearchGate, Jun. 06, 2019. https://www.researchgate.net/publication/338554842_Identificacion_y_comparacion_de_imagenes_en_ambientes_forenses (accessed Dec. 02, 2024).

[27] A. Felipe, G. Camacho, and J. Nieto, "SOFTWARE DE ESTEGANOGRAFÍA DEL BIT MENOS SIGNIFICATIVO PARA DISTRIBUIR ARCHIVOS EN VARIAS IMÁGENES DIGITALES." Accessed: Dec. 02, 2024. [Online]. Available: http://polux.unipiloto.edu.co:8080/00001130.pdf

[28] "Peritaciones informáticas de imágenes y vídeos," GlobátiKa Peritos Informáticos, Jun. 28, 2024. https://peritosinformaticos.es/certificacion-de-no-manipulacion-de-imagenes/ (accessed Dec. 02, 2024).

[29] I. Hidalgo, S. Yasaca, L. Lema, B. Hidalgo, "INFORMÁTICA FORENSE." Available: http://cimogsys.espoch.edu.ec/direccion-publicaciones/public/docs/books/2019-09-19-133251-70%20Libro%20Informatica%20Forense.pdf

[30] J. Sampaoli, "Peritaje informático: marco teórico-practico", Available: https://repositorio.uca.edu.ar/bitstream/123456789/523/11/peritaje-marco-tecnico-practico.pdf

[31] C. Andrés Ordoñez, S. Pasante, and L. Hispánicas, "FORMATOS DE IMAGEN DIGITAL." Available: https://www.revista.unam.mx/vol.6/num5/art50/may_art50.pdf

[32] "Imágenes vectoriales y mapa de bits." Accessed: Oct. 22, 2024. [Online]. Available: https://perio.unlp.edu.ar/catedras/wp-content/uploads/sites/125/2020/05/Im%C3%A1genes-vectoriales-y-mapa-de-bits.pdf

[33] D. Kelsey, A. Ramírez, and G. Cátedra, "Esquemas de Seguridad para Imágenes Digitales." Accessed: Oct. 16, 2024. [Online]. Available: https://ccc.inaoep.mx/~kramirez/Esquemas%20de%20Seguridad%20para%20Imagenes%20Digitales.pdf

[34] P. Pajares, "METADADES I PROCESSOS." Available: https://arxiversvalencians.org/wp-content/uploads/2020/04/revista2009_raventos.pdf (accessed Oct. 21, 2024).

[35] Docunecta, “Qué son los metadatos: definición, tipos y ejemplos,” Docunecta.com, Dec. 15, 2020. https://www.docunecta.com/blog/que-son-los-metadatos (accessed Oct. 22, 2024).

[36] D. Arenas, “técnicas de identificación de la fuente de adquisición en imágenes digitales de dispositivos moviles”, Madrid, 2015, https://docta.ucm.es/entities/publication/20a265fc-8c43-4a06-aaff-280f77401423 (accessed Oct. 07, 2024).

[37] J. Sánchez, “Esteganografía, Disciplina para ocultar información.”, Cohorte 2017, Available: http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1765_SanchezArteagaJM.pdf

[38] P. A. Deymonnaz, “Análisis de vulnerabilidades esteganográficas en protocolos de comunicación IP y HTTP,” Unlp.edu.ar, 2021, doi: http://sedici.unlp.edu.ar/handle/10915/124855.

[39] “Information hiding terminology,” Lecture notes in computer science, pp. 347–350, Jan. 1996, doi: https://doi.org/10.1007/3-540-61996-8_52

[40] A. GUEVARA, “Clasificación de tipos y herramientas de Esteganografía,” Scribd, 2022. https://es.scribd.com/document/565049637/Clasificacion-de-tipos-y-herramientas-de-Esteganografia (accessed Dec. 02, 2024).

[41] C. De Ciencia, Y. Tecnología, and J. Pineda, “desarrollo de algoritmos estegoanalíticos usando descomposición en mapa de bits de segmentación compleja y transformación Wavetel”, Accessed: Oct. 18, 2024. [Online]. Available: https://www.repositorioinstitucionaluacm.mx/jspui/bitstream/123456789/642/3/JaimeRamirezPineda_ISET.pdf

[42] Sakura Sonomi Amamia, “ESTEGOANALISIS.pdf,” Scribd, 2024. https://es.scribd.com/document/632458110/ESTEGOANALISIS-pdf (accessed Oct. 18, 2024).

[43] Daniel Lerch Hostalot, “Esteganografía LSB en imágenes y audio,” Daniellerch.me, 2016. https://daniellerch.me/stego/intro/lsb-es/ (accessed Oct. 08, 2024).

[44] "ELA (Error Level Analysis)," CRIMIBLOG, Dec. 18, 2017. https://javier97rf.wordpress.com/2017/12/18/ela-error-level-analysis/ (accessed Oct. 08, 2024).

[45] E. Kuchumova, Sergio Mauricio Martínez-Monterrubio, and J. A. Recio-Garcia, "STEG-XAI: explainable steganalysis in images using neural networks," Multimedia Tools and Applications, vol. 83, no. 17, pp. 50601–50618, Nov. 2023, doi: https://doi.org/10.1007/s11042-023-17483-3.

[46] M. Vila. "Formatos de imagen", febrero, 2020, https://openaccess.uoc.edu/bitstream/10609/150089/2/FormatosDeImagen.pdf

[47] Scitum, "QUÉ ES LA CIBERSEGURIDAD?" Available: https://resources.scitum.com.mx/wp-content/uploads/2018/02/WP-QUE-ES-LA-CIBERSEGURIDAD-resources.pdf

[48] J. Candau, "ciberseguridad. Evolución y tendencias", Accessed: Oct. 22, 2024. [Online], https://dialnet.unirioja.es/descarga/articulo/8175398.pdf

[49] G. Suárez and J. Luis, "MUNDO ACTUAL." Available: https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8668/IMPORTANCIA%20DE%20LA%20SEGURIDAD%20INFORM%C3%81TICA%20Y%20CIBERSEGURIDAD%20EN%20EL%20MUNDO%20ACTUAL.pdf?sequence=1

[50] "Los incidentes de ciberseguridad de 2023, gestionados por INCIBE, aumentan en un 24% respecto al año anterior | INCIBE | INCIBE," Incibe.es, Apr. 24, 2024. https://www.incibe.es/incibe/sala-de-prensa/los-incidentes-de-ciberseguridad-de-2023-gestionados-por-incibe-aumentan-en (accessed Oct. 22, 2024).

[51] CCH, "Convenio cibercriminalidad," 2005. Available: http://documentostics.com/documentos/convenio_cibercriminalidad.pdf

[52] "LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES." Available: https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

[53] "CÓDIGO ORGÁNICO INTEGRAL PENAL, COIP." Available: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

[54] J. Mestras, “Estructura de las Aplicaciones Orientadas a Objetos El patrón Modelo-Vista-Controlador (MVC) Programación Orientada a Objetos Facultad de Informática,” 2008. Available: https://www.fdi.ucm.es/profesor/jpavon/poo/2.14.mvc.pdf

[55] “jeancarlosneira/StegScan: Aplicación de estegoanálisis con chi-cuadrado, ELA, metadatos,” *GitHub*, 2024. https://github.com/jeancarlosneira/StegScan (accessed Dec. 03, 2024).

ANEXOS

Anexo 1. Encuesta realizada a estudiantes de la universidad estatal península de Santa Elena de la facultad de sistemas y telecomunicaciones, periodo académico 2024-2.

Universidad Estatal Península de Santa Elena **Facultad de Sistemas y Telecomunicaciones** **Carrera de Tecnologías de la Información**	
Encuesta dirigida a los estudiantes de 4to y 5to semestre de T.I.	
Objetivos: Evaluar el conocimiento sobre esteganografía o edición de imágenes en un ambiente de "estudiante".	
1.	**¿Con qué frecuencia utiliza su dispositivo móvil para capturar o compartir imágenes en redes sociales?** **A diario__ Varias veces a la semana__ Ocasionalmente__ Rara vez__ Nunca__**
2.	**¿Cree que las imágenes digitales compartidas en redes sociales u otro tipo de mensajería instantánea son susceptibles de ser manipuladas?** **Sí__ No__ No, estoy Seguro__**
3.	**¿Ha utilizado alguna vez software para editar imágenes digitales?** **Si__ No__**
4.	**¿Ha oído hablar del término "esteganografía" y su uso para ocultar información en imágenes digitales?** **Sí, lo conozco bien__ He escuchado algo__ No, pero me interesa saber más__ No lo conozco__**
5.	**¿Cree que la manipulación de imágenes digitales puede influir negativamente en la reputación o la privacidad de una persona?** **Si__ No__ Depende del contexto__**

6.	**¿Cuán confiable le parecen las imágenes que circulan en redes sociales en cuanto a su autenticidad y veracidad?** **Muy confiables__ Confiables__ Poco confiables__ Nada confiables__**
7.	**¿Qué tan preocupante le parece el riesgo de que imágenes manipuladas se utilicen para difundir información falsa o engañosa?** **Muy preocupante__ Algo preocupante__ Poco preocupante__ Nada preocupante__**
8.	**¿Cuál considera que es el mayor riesgo asociado con la manipulación de imágenes digitales en el ámbito de la ciberseguridad?** **Desinformación__ Suplantación de identidad__ Robo de identidad__ Otro: __**
9.	**¿Ha oído hablar de técnicas como el estegoanálisis o el análisis de metadatos para detectar manipulación en imágenes?** **Si__ No__ Muy poco, pero me gustaría aprender más__**
10.	**¿Estaría dispuesto a usar una aplicación móvil para verificar la autenticidad de las imágenes que comparte o recibe?** **Si__ No__ No estoy seguro__**

Resumen:	Recolección de información para determinar el conocimiento de imágenes con esteganografía o modificadas.
Responsable:	Jeancarlos Josue Neira Alejandro

Anexo 2

Link de códigos del proyecto: [jeancarlosneira/StegScan: Aplicación de estegoanálisis con chi-cuadrado, ELA, metadatos]

Anexo 3

Reporte 1 estegoanálisis

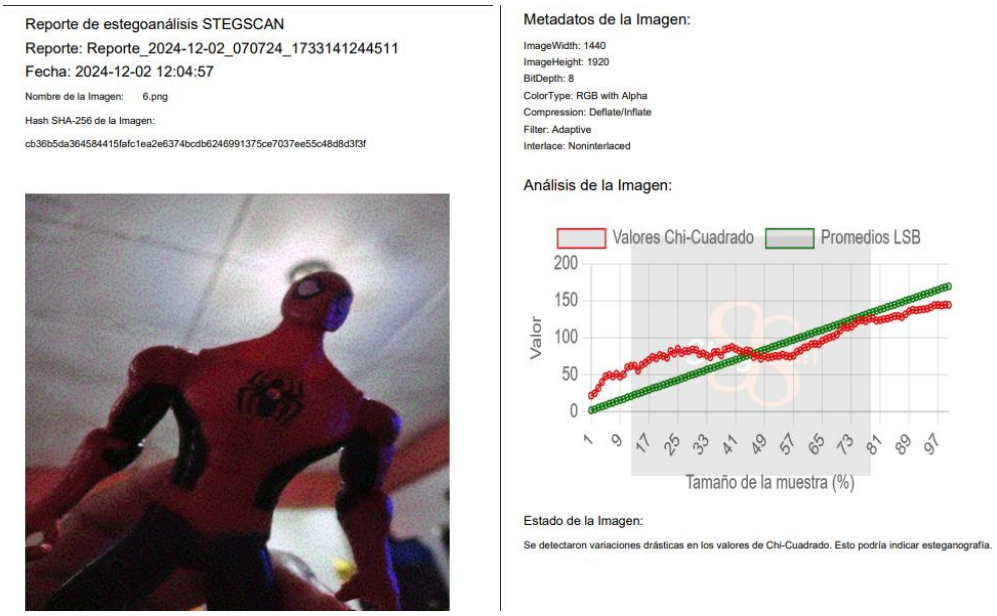


Figura 56: Reporte 1.1 estegoanálisis / Figura 57: Reporte 1.2 estegoanálisis

Reporte 2 ELA

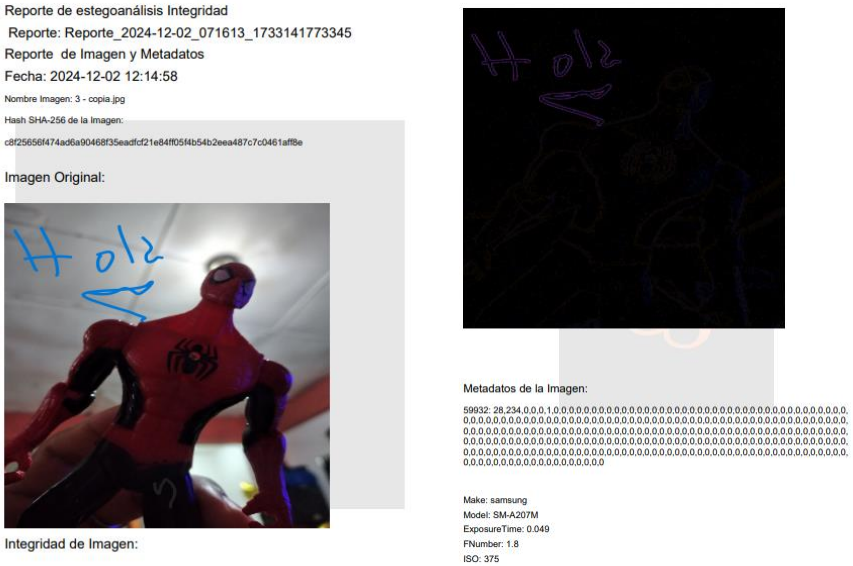


Figura 58: Reporte 2.1 ELA

Figura 59: Reporte 2.2 ELA

0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0

Make: samsung
Model: SM-A207M
ExposureTime: 0.049
FNumber: 1.8
ISO: 375

DateTimeOriginal: Sun Jan 08 2023 23:22:31 GMT-0500 (hora de Ecuador)
CreateDate: Sun Jan 08 2023 23:22:31 GMT-0500 (hora de Ecuador)
ApertureValue: 1.8
MeteringMode: Unknown
Flash: Flash did not fire
FocalLength: 3.61
SubSecTimeOriginal: 00
SubSecTimeDigitized: 00
WhiteBalance: Auto
Padding: 28,234,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0

GPSLatitudeRef: S
GPSLatitude: 2,13,43.47
GPSLongitudeRef: W
GPSLongitude: 80,51,21.3596
latitude: -2.2287416666666666
longitude: -80.85593322222222

Estado de la Imagen:
porcentaje de pixeles modificados:0.000%
probabilidad de contener alteraciones:51.00000000000001%

Figura 60: Reporte 2.3 ELA

Reporte 3 metadatos

Reporte: Reporte_2024-12-02_072311_1733142191370
Reporte de Metadatos
Fecha y hora: 2024-12-02 12:22:01
Nombre de la Imagen: 20230116_185144.jpg
Hash SHA-256 de la Imagen:
fd18b8dbfaca34d7a3504063c134fbe076048debae3fc86e1de76637dba79285

Metadatos de la Imagen:
Model: SM-A207M
Orientation: Rotate 90 CW
ModifyDate: Mon Jan 16 2023 18:51:44 GMT-0500 (hora de Ecuador)
Make: samsung
FNumber: 1.8
FocalLength: 3.61
ExposureTime: 0.01
Flash: Flash did not fire
ISO: 126
MeteringMode: Unknown
CreateDate: Mon Jan 16 2023 18:51:44 GMT-0500 (hora de Ecuador)

FNumber: 1.8
FocalLength: 3.61
ExposureTime: 0.01
Flash: Flash did not fire
ISO: 126
MeteringMode: Unknown
CreateDate: Mon Jan 16 2023 18:51:44 GMT-0500 (hora de Ecuador)
DateTimeOriginal: Mon Jan 16 2023 18:51:44 GMT-0500 (hora de Ecuador)
WhiteBalance: Auto

ApertureValue: 1.8
GPSLatitudeRef: S
GPSLatitude: 2,13,41.48
GPSLongitudeRef: W
GPSLongitude: 80,51,25.1
latitude: -2.228188888888889
longitude: -80.85697222222221

Figura 61: Reporte 3.1 metadatos / Figura 62: Reporte 3.2 metadatos

Anexo 4

Anexo 4.1 Imagen1

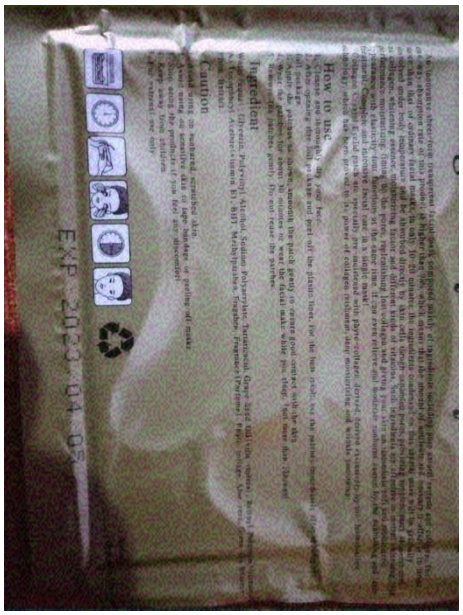


Figura 63: Imagen 1 para pruebas

Anexo 4.2 Prueba esteganográfica 1

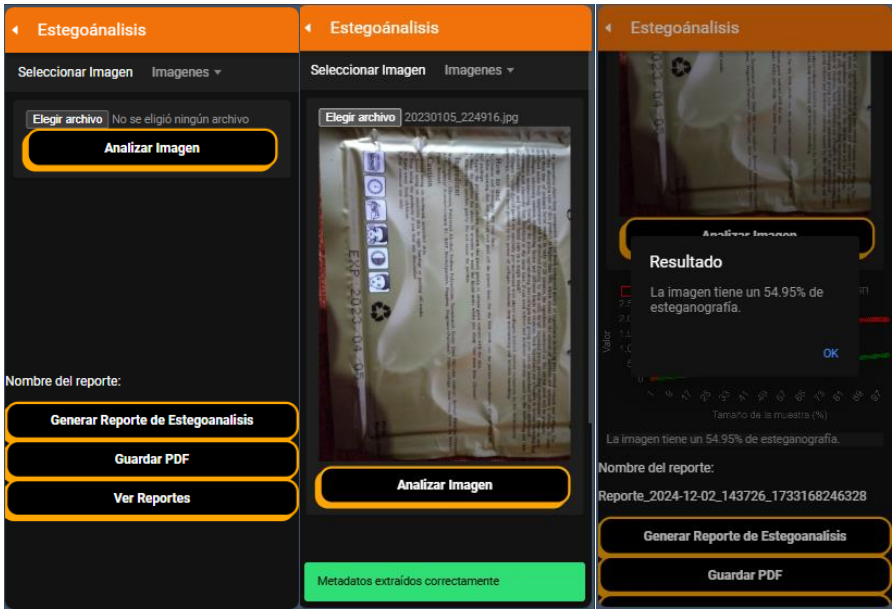


Figura 64: Prueba esteganográfica 1.1 / Figura 65: Prueba esteganográfica 1.2 / Figura 66: Prueba esteganográfica 1.3

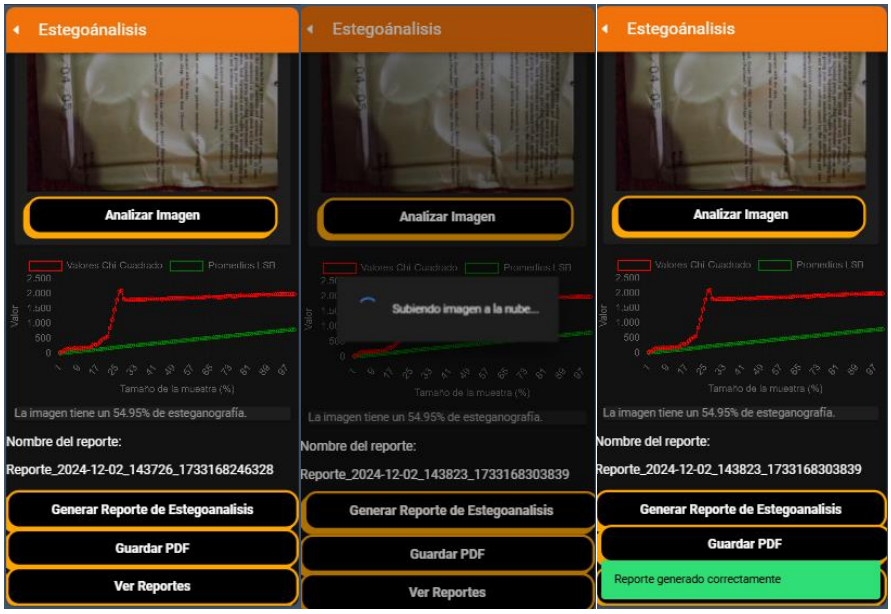


Figura 67: Prueba esteganográfica 1.4 / Figura 68: Prueba esteganográfica 1.5 / Figura 69: Prueba esteganográfica 1.6

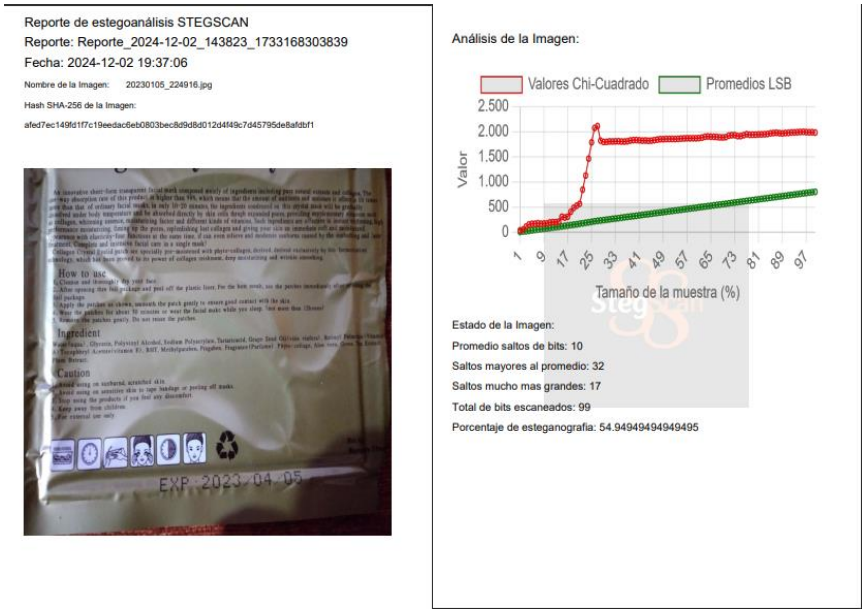


Figura 70: Prueba esteganográfica 1.7 / Figura 71: Prueba esteganográfica 1.8

Anexo 5

Anexo 5.1 Imagen2

Figura 72: Imagen 2 para pruebas

Anexo 5.2 Prueba esteganográfica 2

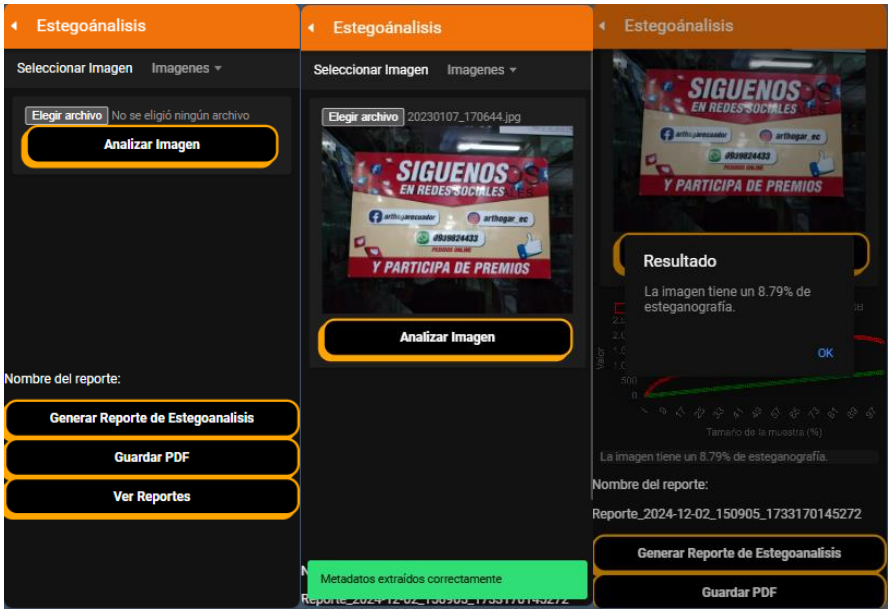


Figura 73: Prueba esteganográfica 2.1 / Figura 74: Prueba esteganográfica 2.2 / Figura 75: Prueba esteganográfica 2.3

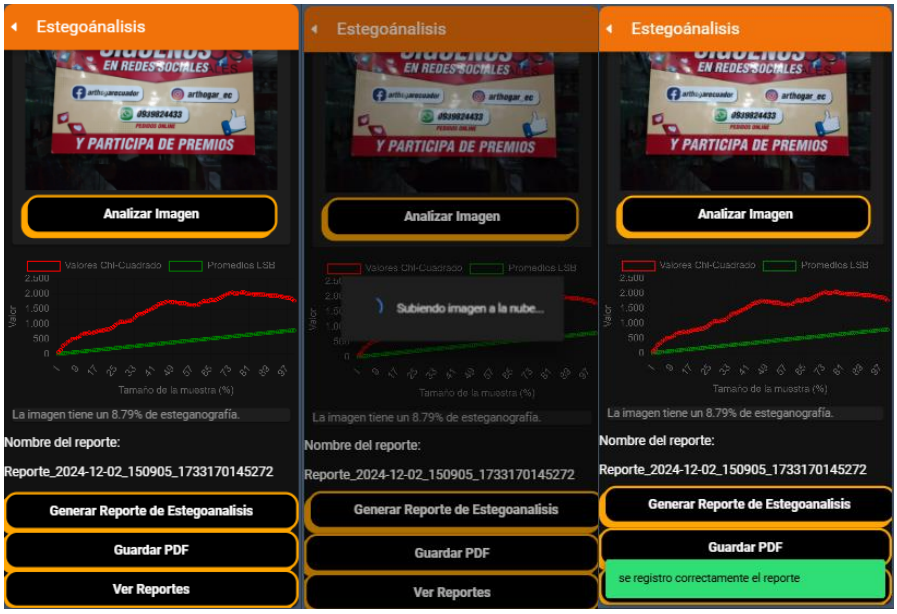


Figura 76: Prueba esteganográfica 2.4 / Figura 77: Prueba esteganográfica 2.5 / Figura 78: Prueba esteganográfica 2.6

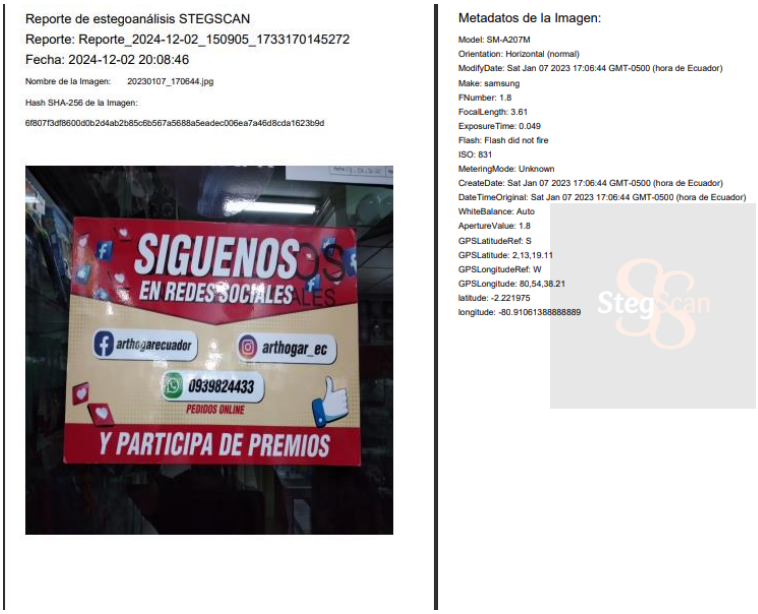


Figura 79: Prueba esteganográfica 2.7 / Figura 80: Prueba esteganográfica 2.8

Figura 81: Prueba esteganográfica 2.9

Anexo 6

Anexo 6.1 Imagen3

Figura 82: Imagen 3 para pruebas

Anexo 6.2 Prueba esteganográfica 3

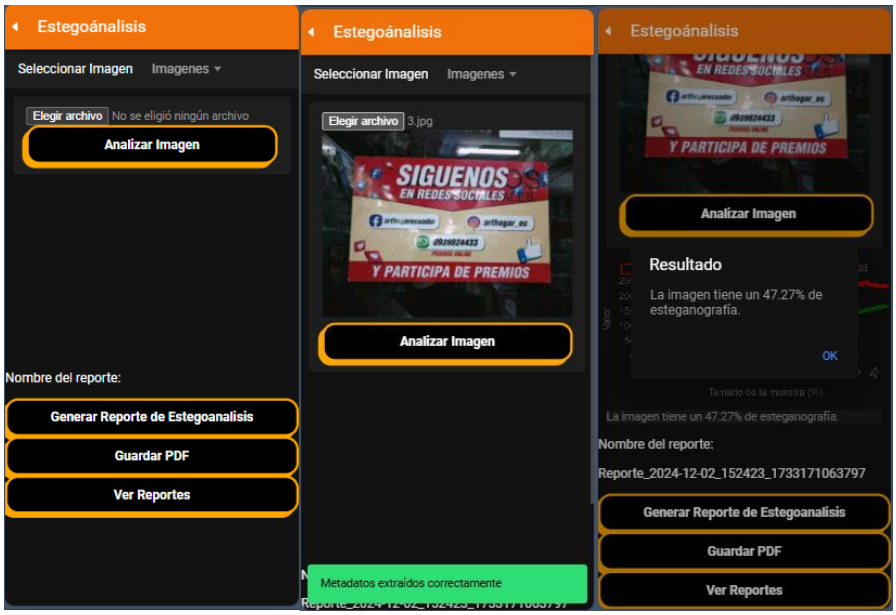


Figura 83: Prueba esteganográfica 3.1 / Figura 84: : Prueba esteganográfica 3.2 / Figura 85: Prueba esteganográfica 3.3

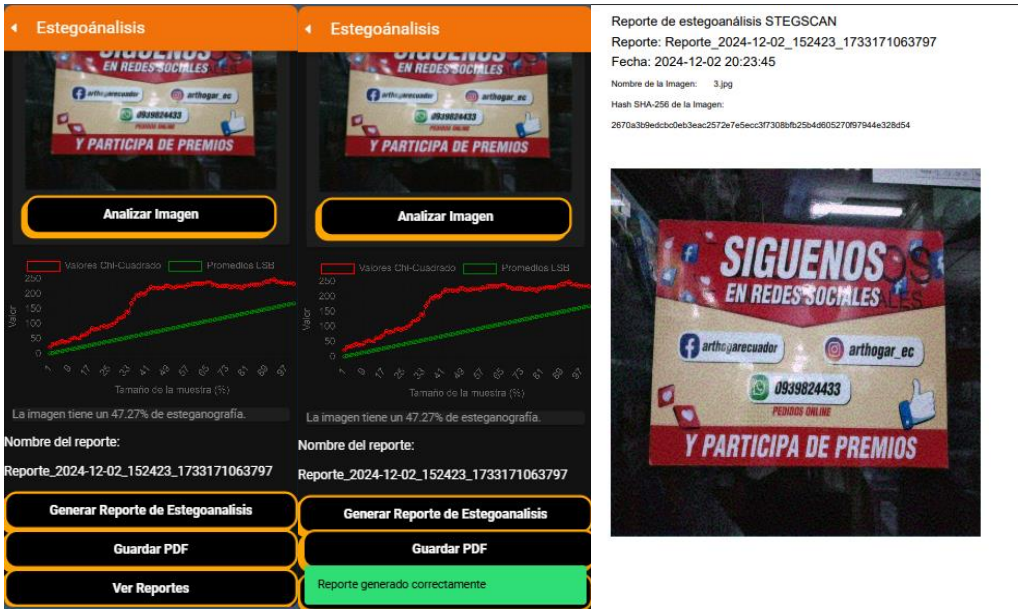


Figura 86: Prueba esteganográfica 3.4 / Figura 87: Prueba esteganográfica 3.5 / Figura 88: Prueba esteganográfica 3.6

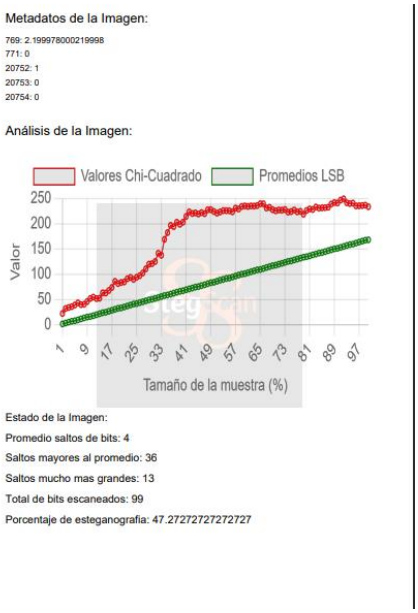


Figura 89: Prueba esteganográfica 3.7

Anexo 7

Anexo 7 Imagen4

Figura 90: Imagen 4 para pruebas

Anexo 7.2 Prueba esteganográfica 4

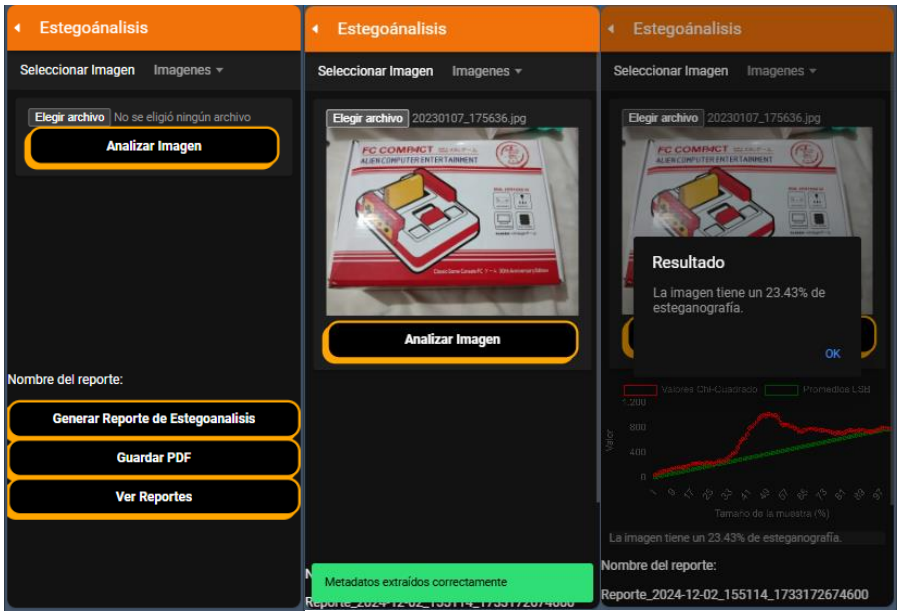


Figura 91: Prueba esteganográfica 4.1 / Figura 92: Prueba esteganográfica 4.2 / Figura 93: Prueba esteganográfica 4.3

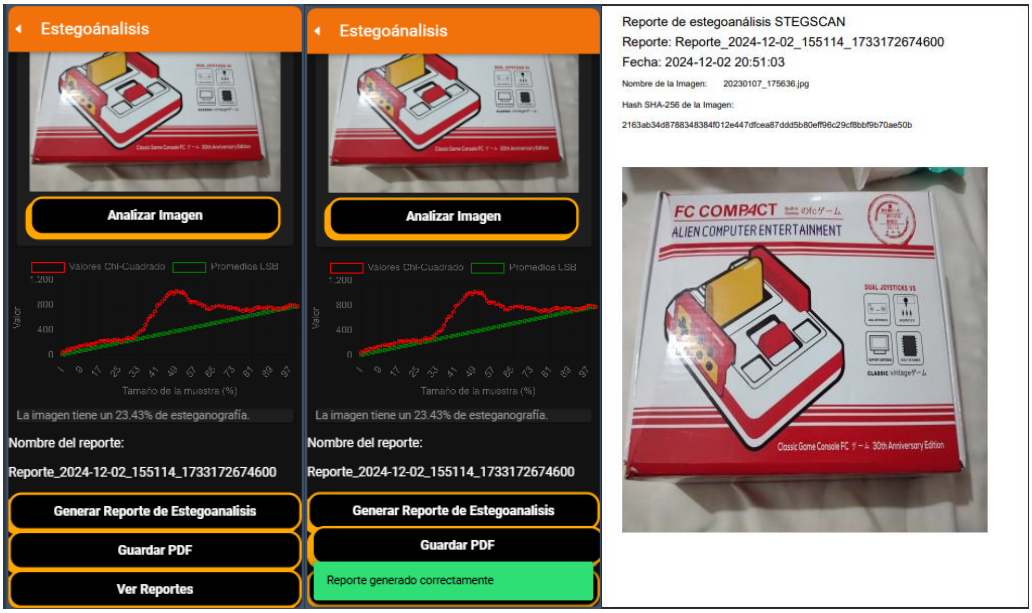


Figura 94: Prueba esteganográfica 4.4 / Figura 95: Prueba esteganográfica 4.5 / Figura 96: Prueba esteganográfica 4.6

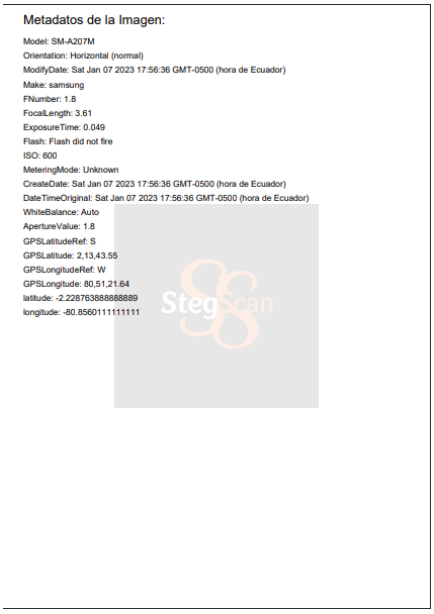


Figura 97: Prueba esteganográfica 4.7 / Figura 98: Prueba esteganográfica 4.8

Anexo 8

Anexo 8.1 Imagen5

Figura 99: Imagen 5 para pruebas

Anexo 8.2 Prueba esteganográfica 5

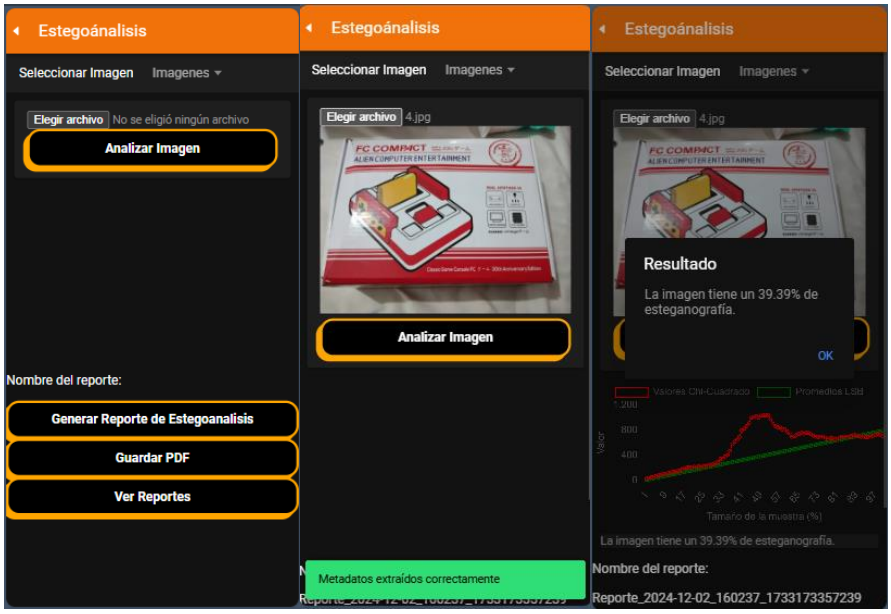


Figura 100: Prueba esteganográfica 5.1 / Figura 101: Prueba esteganográfica 5.2 / Figura 102: Prueba esteganográfica 5.3

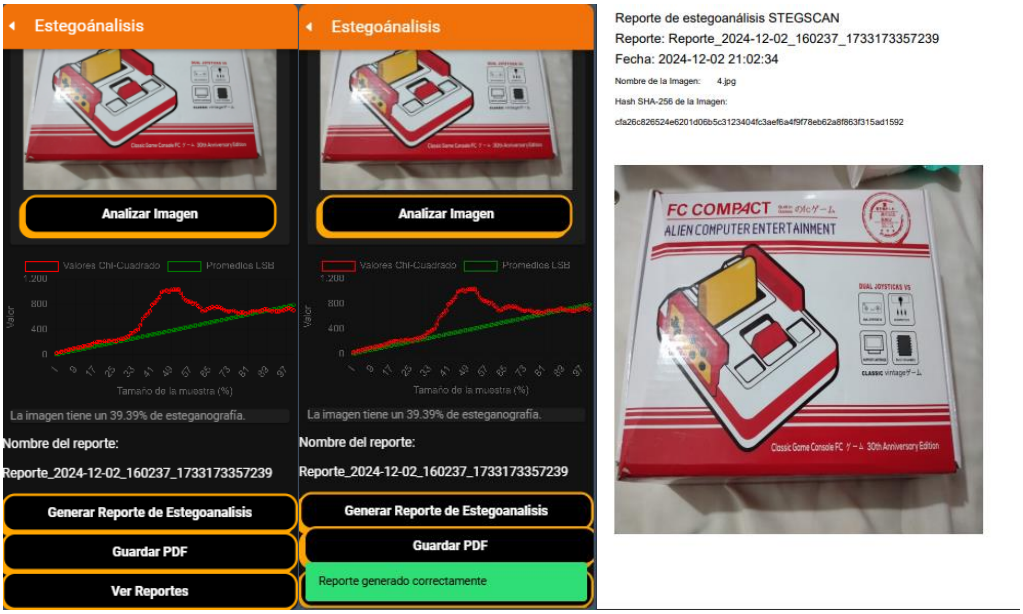
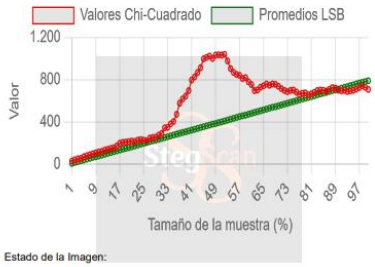


Figura 103: Prueba esteganográfica 5.4 / Figura 104: Prueba esteganográfica 5.5 / Figura 105: Prueba esteganográfica 5.6

Metadatos de la Imagen:

nommbre: : 4.jpg
size: : 1982917
type: : image/jpeg
ultima_modificacion: 2024-12-02T20:40:09.273Z

Análisis de la Imagen:



Estado de la Imagen:

Promedio saltos de bits: 19

Saltos mayores al promedio: 30

Saltos mucho mas grandes: 13

Total de bits escaneados: 99

Porcentaje de esteganografia: 39.39393939393939

Figura 106: Prueba esteganográfica 5.7

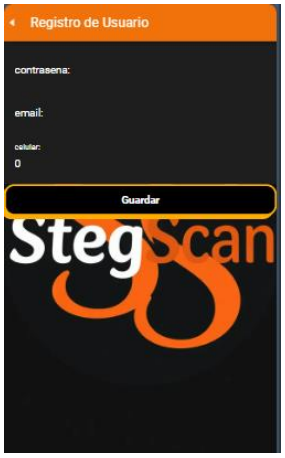
MANUAL DE USUARIO

El siguiente manual está organizado de acuerdo a la secuencia de ingreso del usuario y consecutivo con las funciones de la aplicación.

- **Ingreso a la aplicación**

En esta pantalla el usuario deberá digitar el nombre de usuario y su clave correspondiente y presionar el botón “Iniciar sesión” tal como muestra en la ilustración siguiente, los datos que se ingresan son los previamente ya registrados o pueden registrar nuevos usuarios.

En caso de no estar registrado deberá presionar sobre el botón registrarse el cual despliega una ventana en la que puede realizar el ingreso de su información, con el fin de otorgarle un usuario y contraseña para que pueda ser registrado.

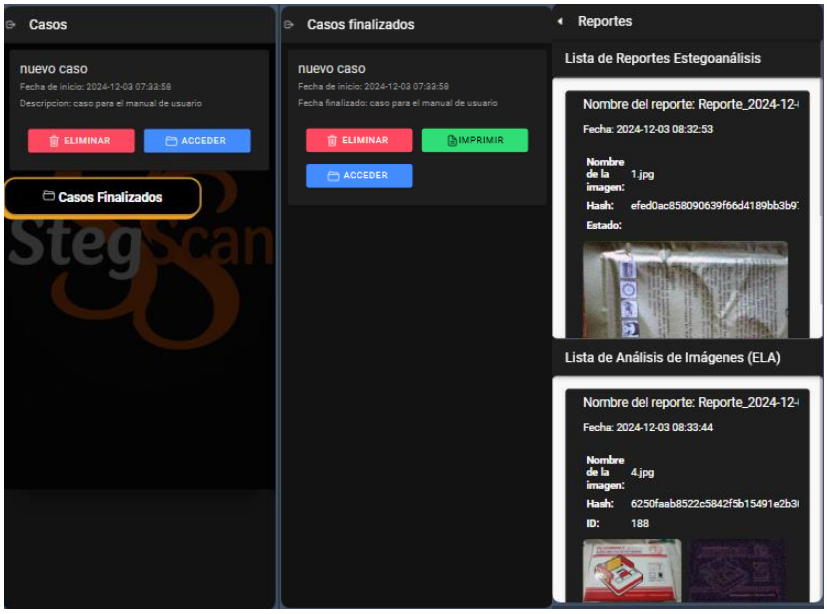


- Registro de casos o edición de casos.

Una vez realizado con éxito el inicio de sesión se redireccione a la pantalla de casos, donde habrá 4 botones:

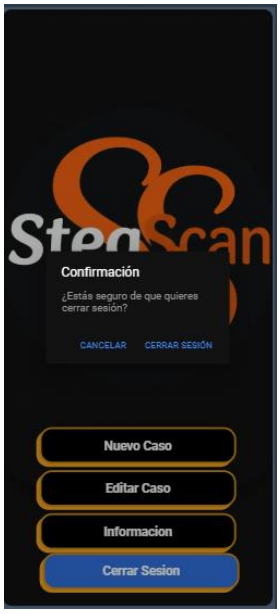
Nuevo caso- al momento de presionar el botón de crear caso o nuevo caso se dirige a una pantalla para registrar un nuevo caso, al ingresar los datos y aplastar el botón de guardar se guardaría el caso en la base de datos.

Editar caso- al aplastar el botón de editar caso podemos observar una lista de los casos guardados con una breve descripción y también encontramos un botón que dice casos finalizados, el cual alberga casos ya finalizados y enlista los reportes generados.



Información- en esta pantalla se observará información o introducción de esteganografía, sobre lo que se trata la aplicación.

Cerrar sesión- al dar click en este botón se abrirá una alerta de cerrar sesión y dos opciones de cerrar sesión y cancelar, al cerrar sesión se eliminaran los datos de usuario del almacenamiento local.

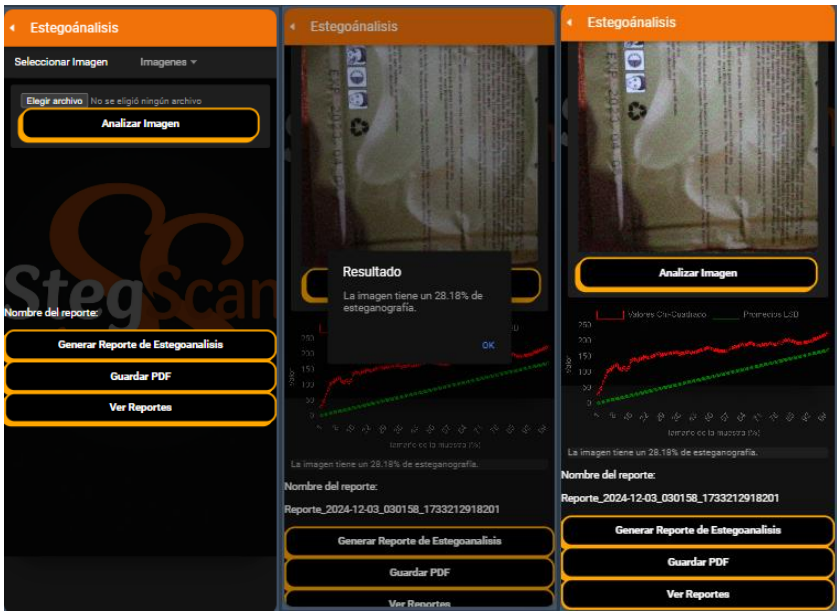


- Acceder a un caso

Al acceder a un caso se dirigirá a una página donde podremos observar varias opciones como información, terminar el caso y salir del caso, en el menú se puede obtener varias opciones como Analizar imagen, Integridad de Imagen, Extraer Metadatos, Ver/Subir Imagen, Estadísticas, Reportes Estegoanálisis, Reportes Integridad, Reporte de Metadatos, Información, salir.

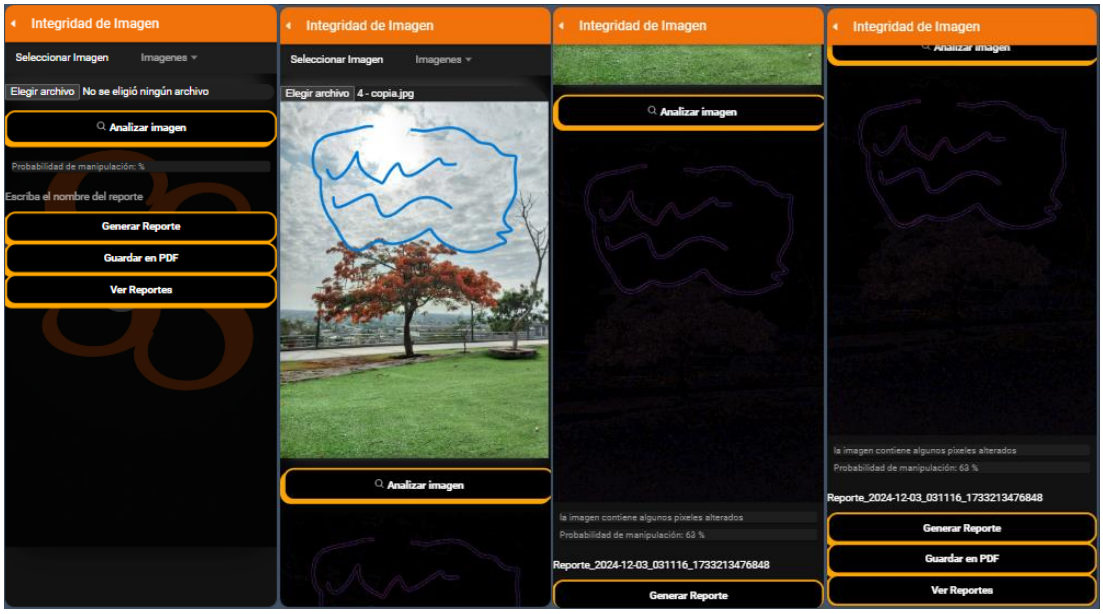
Análisis Imagen-

En esta página se procederá a analizar la imagen, la cual se puede cargar del almacenamiento local o buscar en la base de datos del usuario, cuando la imagen este cargado y aplaste el botón de Analizar imagen se puede observar la probabilidad de que contenga esteganografía, en el botón generar reporte se puede guardar el reporte de el escaneo de la imagen en la base de datos, al aplastar guardar pdf se descargara un pdf con toda la información del escaneo de la imagen, y el botón ver reportes se redirigirá a la página de los reportes generados.

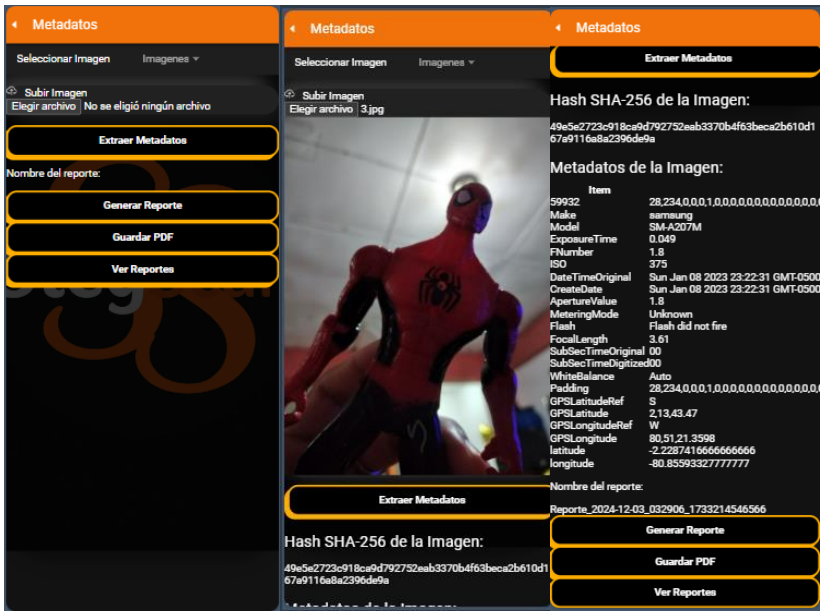


Integridad de imagen-

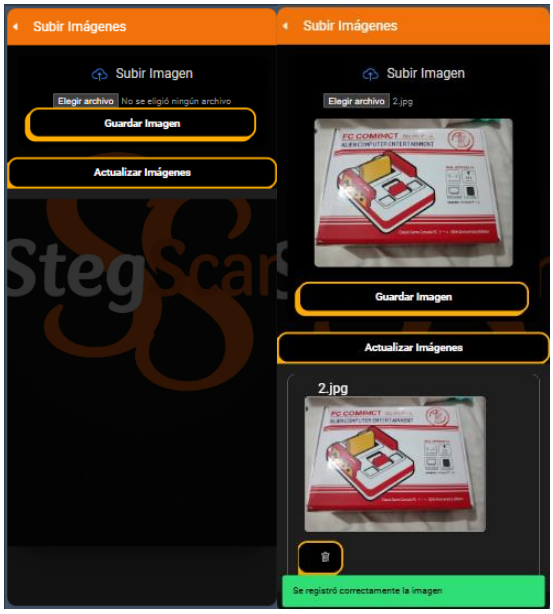
En esta página podemos escanear una imagen y generar una imagen con filtros específicos para poder ver las partes de la imagen modificada, tiene la opción de ingresar imagen localmente y escanear una imagen de la base de datos, se mostrara la imagen y al momento de aplastar el botón de analizar imagen se procederá escanear la imagen y generara un filtro para ver si contiene modificaciones o ediciones, se visualizara también la probabilidad de contener modificaciones de la imagen y otro botón para poder generar reporte el cual guarda todos los datos del análisis y de la imagen, también esta le botón de guardar el pdf que se podrá descargar el pdf en el dispositivos, y el botón ver reportes visualiza una lista de reportes de integridad de imágenes.



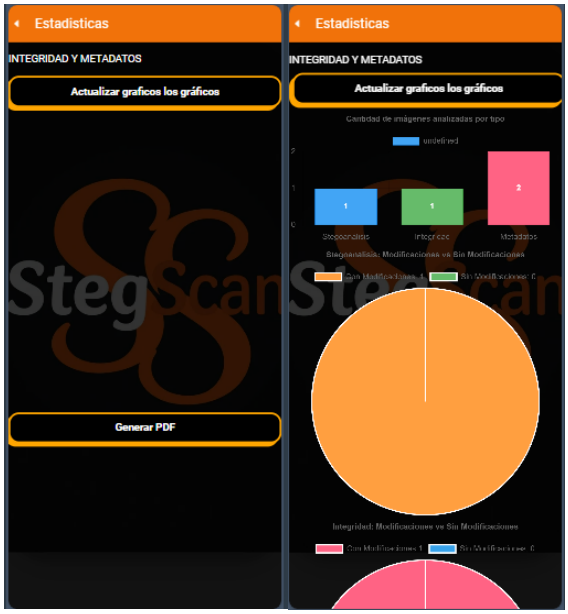
Extraer metadatos- en la pantalla de metadatos también se podrá seleccionar una imagen local o de la base de datos, al momento de seleccionar la imagen se podrá extraer los metadatos de la imagen y guardarlos en la base de datos, el botón de generar reporte guarda todo el dato del reporte generado en la base de datos para postrarlos en reportes de metadatos y también se puede generar pdf el cual se descargaría.



Ver/subir imagen- en la pantalla se podría subir imagen y observar imágenes, al momento de cargar la imagen y aplastar el botón de guardar imagen se guarda en la base de datos y se enlista.



Estadísticas- En la pantalla se puede observar un botón para actualizar gráficos y al presionarlo se generará gráficos de las cantidades de reportes generados en cada método estegoanalítico y más abajo se observa la comparación de imágenes con y sin modificaciones.



- Reportes

En esta página se puede visualizar los reportes generados de cada método estegoanalítico

Reporte Esteganálisis

Reporte 1: Reporte_2024-12-03_033330_1733214810843

Fecha: 2024-12-03 08:32:53

Nombre de la imagen:	1.jpg
Hash:	efed0ac858090639f66d4189bb3b
variacion de pixeles:	4
pixeles mayores a la variacion:	31
pixeles altos a la variacion:	9
total de pixeles escaneados:	99
probavilidad de esteganografia:	28.1818

Reporte de Análisis

Reporte 1: Reporte_2024-12-03_033347_1733214827845

Fecha: 2024-12-03 08:33:44

Nombre de la imagen:	4.jpg
Hash :	6250faab8522c5842f5b15491e2
Porcentaje de pixeles con brillo alto:	0.011
Porcentaje de pixeles con brillo bajo:	22.38
Porcentaje de pixeles con brillo intermedio:	2.15451
probavilidad de esteganorgrafia:	99 %

Reporte Metadatos

Reporte 1: Reporte_2024-12-03_033420_1733214860628

Fecha: 2024-12-03 08:34:14

Nombre Imagen:	5.png
Hash:	218a093a297449ace56deaed2292ee6e55

"{\"ImageWidth\":\"1440\",\"ImageHeight\":\",\"BitDepth\":\"8\",\"ColorType\":\"RGB wit Alpha\",\"Compression\":\"Deflate\/Inflate lite\":\"Adaptive\",\"Interlace\":\"Noninted\"}"