UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

CENTRO UNIVERSITARIO UAEM ATLACOMULCO

"Sistema para la protección de derechos de autor en imágenes digitales utilizando marcas de agua mediante técnicas esteganográficas"

T E S I S

Que para obtener el Título de:

Ingeniero en Computación

Presenta:

Noé Alejandro López López

Director de Tesis:

Dr. en C. I. E. Everardo Efrén Granda Gutiérrez

Atlacomulco, México; Febrero del 2020

RESUMEN

En este trabajo se propone la investigación y desarrollo de un sistema para la protección de los derechos de autor en imágenes digitales. Dicho sistema utiliza un algoritmo basado en técnicas esteganográficas robustas, para la ocultación de una marca de agua dentro la imagen digital; posteriormente se aplican técnicas de estegoanálisis para sustraer la marca de agua oculta. La marca de agua puede ser un logotipo o firma digital que identifique al artista o empresa que quiera proteger dicha imagen. El sistema propuesto tiene como base cuatro criterios:

- Verificar: asegurarse que la imagen digital a proteger y la marca de agua a ocultar cumplen con las características para poder llevar a cabo el proceso esteganográfico.
- Cifrar: hacer uso de las técnicas esteganográficas para ocultar la marca de agua dentro de la imagen digital.
- Descifrar: hacer uso de técnicas de estegoanálisis para extraer la marca de agua oculta dentro de la estego-imagen.
- Evaluar: al ocultar la marca de agua dentro de la imagen el sistema debe dar como resultado una estego-imagen, la cual no se debe diferenciar con original a la percepción del ojo humano, además de que el sistema podrá extraer la marca de agua, aunque la estego-imagen haya sufrido modificaciones y como resultado la marca de agua podrá alterarse, pero no a tal grado de quedar irreconocible.

Se toman en cuenta dos formatos de imágenes: JPG (o JPGE) y PNG, los cuales son los más utilizados para la distribución de imágenes por su compatibilidad con la mayoría de los dispositivos para visualizarlas, por lo que son las más vulnerables a ser robadas y utilizadas sin dar crédito al autor. La marca de agua robusta es necesaria para verificar su autenticidad y reclamar sus derechos de autor cuando esta incumpla con la utilidad por la que fue creada y aunque esta sea modificada debe ser posible extraer la marca de agua oculta en ella.

Palabras clave: Imagen, Esteganografía, Autor, Marca de Agua, Algoritmo.

ABSTRACT

The research and development of a system for protection of copyright in digital images is proposed in this document. The system uses an algorithm based in robust steganography techniques to hide a watermark in the digital image; also, it uses stegonalysis techniques to extract the hidden watermark. The watermark could be a logo or digital signature that identifies the artist or company that wants to protect that image. The algorithm is based on four criteria:

- Evaluate: the system must assess whether digital image to protect and the watermark to hide, meet the characteristics to be able to carry out the steganographic process.
- Code: the system uses steganographic techniques to hide the watermark within digital image.
- Decode: the system uses stegoanalysis techniques to extract the watermark hidden within the stego-image.
- Performance: by hiding the watermark within the image, the system should give as a result an stego-image, which not differ from original to the perception of the human eye; in addition, the system may extract the watermark, although the stego-image has been modified and, as a result, the watermark may be altered but not to such a degree to look unrecognizable.

Two image formats were used: JPG (or JPGE) and PNG, which are the most used formats for image distribution due to their compatibility to be displayed in most devices; the latter is the reason of that these images are most vulnerable to be stolen and used without giving credit to the author. The robust watermark is necessary to verify the image authenticity and claim copyright when this fails to meet with the utility for the that was created and, although the image is modified, should be possible to extract the watermark hidden on it.

Keywords: Image, Steganography, Author, Watermark, Algorithm.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1 INTRODUCCIÓN

Las imágenes son interpretaciones visuales que se plasman en un archivo digital, como se hace mayormente en la actualidad, o en papel, lienzo, paredes u otro objeto físico como se ha hecho desde hace mucho tiempo. Las imágenes digitales se han convertido en uno de los archivos más utilizados hoy en día, en sus diferentes formatos; sus usos abarcan desde imágenes de gran importancia como las médicas o de grado militar, hasta las imágenes con fines artísticos o de entretenimiento. Una imagen digital está compuesta por un conjunto de pixeles; cada píxel es la combinación de tres colores en una escala RGB (Rojo, Verde y Azul), que de acuerdo con la intensidad de cada uno se fusionan y como resultado dan una tonalidad específica de color (Orea Flores, 2005).

Para algunas personas el crear estos archivos u objetos visuales es una profesión, ya que su creación es considerada una obra de arte; o bien, puede ser una imagen de gran importancia. Sin embargo, para que el autor obtenga el crédito por su obra, es necesario que este la marque con su firma, como lo hacen los artistas en sus pinturas, o le inserte una técnica que lo verifique como el autor auténtico de dicha obra. En imágenes digitales, usualmente es fácil borrar o disimular la zona donde el autor pone su marca o firma. Para cuestiones de derecho de autor, se han utilizado marcas de agua, las cuales son técnicas que han sido efectivas por mucho tiempo, pero en la actualidad y con el avance de la tecnología es posible, mediante herramientas de edición, sustituir u omitir la marca de agua que el autor le haya agregado a su imagen digital.

Hay algunas plataformas web donde los usuarios comparten imágenes, algunas protegidas con marcas de agua, las cuales la insertan en una parte significativa (Oliver, 2019). Si la imagen no es de gran importancia, o no importa que se perciba sobre la misma, la ponen en cualquier zona de la imagen; si es de gran importancia, o afecta la visibilidad de la imagen principal, la marca de agua se inserta en una zona de la imagen que no sea relevante. Sin embargo, por ello se dan casos de robo de derechos de autor, ya que la zona donde se inserta la marca de agua se puede recortar o remplazar con el uso de herramientas de edición de imágenes, por ejemplo Photoshop u otros softwares para el tratamiento de imágenes (Rodríguez Colín, 2006) (González Osorio, 2017).

Para el tratamiento de imágenes se han desarrollado algoritmos o técnicas que permiten el manejo de los datos de una imagen digital, como el realce de brillo, contraste o filtros para mejorar la calidad de una imagen. Estos algoritmos trabajan sobre el dominio espacial y las transformadas (Renza, et al., 2016), y es gracias al uso de estas técnicas que es posible ocultar información dentro de un archivo digital, pero principalmente enfocadas a las imágenes digitales. El uso de estas técnicas es conocido como esteganografía, que es el arte de ocultar información dentro de un objeto (Velasco Bautista, et al., 2007).

La esteganografía es una técnica de ocultamiento de información que se ha utilizado desde épocas medievales, ya que algunos emperadores y reyes utilizaban animales o esclavos para ocultar mensajes a personas infiltradas en otro reino enemigo y así planear una estrategia de ataque (Ruiz Tejeida, 2013).

Con el paso del tiempo, esta técnica ha ido evolucionando; por ejemplo, durante la Segunda Guerra Mundial, fueron utilizadas tintas invisibles para encubrir la información en notas o cartas aparentemente estándares e inofensivas; entre las fuentes más comunes para las tintas invisibles están la leche, el vinagre y la orina (Corona Falcon, 2015). Pero donde tuvo un mayor impacto fue cuando se implementó en los archivos digitales (imágenes, video, audio), los cuales son transferidos por medio de las tecnologías de comunicación, donde uno de los principales medios que ha resaltado en la actualidad es el internet, que es una de las herramientas más utilizadas para el intercambio de información.

Algunas personas confunden la esteganografía con la criptografía, pero realmente son diferentes, ya que la criptografía modifica el archivo de modo que este quede incomprensible para cualquier usuario que lo quiera leer, mientras que la esteganografía oculta información dentro de un archivo multimedia haciéndolo invisible para la percepción del ser humano y que no se pueda detectar a simple vista, por ejemplo: en las imágenes digitales, los archivos de audio, de video, entre otros (Soria Lorente, et al., 2016).

En este trabajo se utilizarán técnicas esteganográficas para insertar una marca de agua dentro de una imagen digital, y así poder comprobar los derechos de autor, al insertar una marca digital (logotipo, firma, entre otros) en la imagen, permitiendo verificar los créditos

del autor. Además, se busca que esta marca no sea borrada, aunque sea modificada por otros usuarios que tengan acceso a la imagen. Esta marca de agua debe pasar desapercibida por los demás y debe resistir diferentes modificaciones, como lo son el cambio de brillo o contraste.

2 PLANTEAMIENTO DEL PROBLEMA

La comunicación entre personas es indispensable para transmitir información; para ello se utilizan diferentes medios de comunicación. Hoy en día la información es transmitida, en su mayor parte, por los medios que nos ofrece las Tecnologías de la Información y Comunicación (TIC´s), ya que garantizan una comunicación más rápida, efectiva y fácil de entender; por ejemplo las redes sociales y páginas web, en las cuales los usuarios intercambian información por medio de archivos multimedia a otros usuarios que desean tener acceso a esta información (Campos Freire, 2008) (Renza, et al., 2016).

Algunos de los archivos multimedia más compartidos en estas plataformas son las imágenes digitales, las cuales tienden a ser las más vulnerables a ser hurtadas por algún usuario, para ser modificadas o utilizadas sin dar crédito al autor, ya sea con fines de lucro, para ocasionar un daño moral, o para atribuirse la autoría de la imagen indebidamente (Granda Tonato, 2015) (Orea Flores, 2005).

2.1 Definición del problema

El derecho de autor es el reconocimiento que se otorga al creador de obras literarias y artísticas, en virtud del cual goza de derechos de tipo personal, denominados derechos morales, pero también derechos de tipo económicos, denominados derechos patrimoniales (Instituto Nacional del Derecho de Autor, 2019). De aquí que, para preservar el derecho de autor, son muy importantes los aspectos legales y morales, puesto que el autor que da a conocer su obra busca obtener reconocimiento por su creación y/o recompensas económicas por el uso de esta.

Muchas personas, de manera intencional o no, utilizan obras que tienen derechos de autor y las modifican, de tal manera que el autor original pierde crédito por su obra y, por lo tanto, sus derechos han sido invadidos. Lo mismo pasa con las imágenes digitales, ya que en la actualidad es posible obtener una imagen de cualquier sitio web, y distribuirlo mediante las redes sociales y páginas de internet.

La mayor parte de las imágenes que se encuentran publicadas en sitios web o redes sociales no están acreditadas por su autor original, o ya están modificadas por los usuarios,

quitándole el crédito a su autor. Por otra parte, hay imágenes que si están protegidas por marcas de agua o leyendas sobre la figura, pero estas se denotan a simple vista y alteran la apariencia de la imagen, degradando su calidad y demeritando su estética; además, estos elementos son fáciles de eliminar con simplemente recortar el área donde se encuentra dicha marca y como consecuencia se pierde el crédito al autor.

Las técnicas de esteganografía y estegoanálisis son herramientas que se pueden utilizar para la edición de imágenes, antes de su publicación, de tal manera que se incorporen mecanismos para que se identifique a una imagen original de otras modificaciones no autorizadas por su autor, sin modificar la percepción visual o la estética de la imagen, mediante la edición de una marca de agua oculta a la vista.

2.2 Objetivos de investigación

Desarrollar un sistema mediante técnicas de esteganografía y estegoanálisis, para cifrar y descifrar una marca de agua, con la finalidad de ayudar en la protección de los derechos de autor de una imagen digital, aunque esta se haya sometido a modificaciones. Si se modifica alguna de las propiedades de la imagen, no se debe perder dicha marca de agua; de este modo el autor podrá ocultar un logotipo o firma que lo identifique dentro de la imagen digital, con el uso de las técnicas esteganográficas y así obtener como resultado una estego-imagen que tendrá la marca de agua oculta, no detectable a simple vista, y que no es posible de modificar por herramientas de edición convencionales.

Objetivos específicos:

- Aplicar técnicas de esteganografía y estegoanálisis para cifrar y descifrar una marca de agua; esta será la que el usuario lo considere, puede ser un logotipo o una imagen que lo identifique y lo acredite como autor autentico de una imagen digital.
- Estudiar las diferentes técnicas de la esteganografía para identificar cuál de ellas es la más adecuada para la ocultación de la marca de agua dentro de la imagen.
- Aplicar una marca de agua que no se detecte a simple vista, pero que al modificar la imagen no se pierda.

- Evaluar el desempeño del algoritmo en la identificación de imágenes alteradas, mediante la verificación de la marca de agua.
- Crear una interfaz de usuario que permita la utilización de las herramientas de esteganografía y estegoanálisis.

2.3 Preguntas de investigación

- ¿Como se puede crear una marca de agua para proteger los derechos de autor de una imagen digital?
- ¿Qué técnica de esteganografía es la más adecuada para el ocultamiento a simple vista de la marca de agua en la imagen?
- ¿Qué tipo de marca de agua es conveniente insertar en la imagen, de tal manera que no se altere significativamente?
- ¿Cuál técnicas de estegoanálisis puede utilizarse para reconocer la marca de agua oculta al momento de descifrarla?

2.4 Justificación

Una aplicación de este sistema es que puede ser utilizado para cifrar y descifrar una marca de agua de diseño propio, o una leyenda de texto, dentro de una imagen digital que acredite al autor auténtico de dicha imagen. La marca de agua no se degradará significativamente si la imagen sufre de modificaciones, ya que el sistema insertará una marca de agua "invisible" a la percepción de cualquier usuario, y si se quisiera modificar la estego-imagen esta marca de agua no tendría que alterarse a tal grado de quedar irreconocible, sino que se podrá reconocer al descifrarla de la imagen modificada. De este modo, potencialmente puede servir como herramienta para ayudar a la identificación de imágenes modificadas y, por lo tanto, a la preservación de los derechos de autor de las imágenes digitales.

Para lograr lo anterior, se pretenden aplicar algunas técnicas esteganográficas en la imagen para el ocultamiento de la marca de agua que acredite al autor de dicha obra, y ayudar en

la propagación o transferencia de dicha imagen de un usuario a otro, sin poner en riesgo a la marca de agua, ya que no será percibida por terceros.

Puesto que la marca de agua será difícil de detectar a simple vista, y puesto que si la imagen es modificada esta marca de agua no se perderá, se puede identificar una falsificación o alteración no autorizada de la imagen, y con ello se ayuda a proteger la integridad del derecho de autor, al no permitir que la imagen se acredite a otro autor. Esto beneficiará a los usuarios que tengan la necesidad de transferir una imagen por un medio no seguro, como lo son las redes sociales o páginas de internet y que no quieran perder los derechos de autor de su imagen digital.

Un ejemplo de potenciales usuarios de este tipo de herramientas puede ser el siguiente: si un fotógrafo quisiera dar a conocer una foto de un animal exótico a sus seguidores de Twitter para ganar reconocimiento, este tendrá que proteger su obra artística, ya que cualquiera que tenga acceso a dicha imagen puede modificarla y acreditársela, sin dar reconocimiento al autor original. Con el uso de este sistema, el usuario podría proteger su fotografía con el logotipo que lo representa oculto dentro de ella, y cuando esta sea utilizada por otra persona que no le de crédito, el podrá comprobar su autenticidad y reclamar sus derechos de autor ante las instancias que correspondan.

Para finalizar el ejemplo anterior, es necesario utilizar una técnica esteganográfica para que el sistema pueda ocultar la marca de agua dentro de una imagen digital que se desea proteger y que pase desapercibida a las personas que tengan acceso a esta imagen, pero además, el autor de la imagen debe poder descifrar dicha marca de agua oculta, aunque esta se modifique, por lo que en esta propuesta se utilizarán técnicas de estego-análisis, para comprobar la autenticidad de la imagen.

2.5 Impactos

- Científico. La generación de un algoritmo, basado en la herramienta esteganográfica DCT, aporta una herramienta para la esteganografía que permite cifrar y descifrar una marca de agua en imágenes digitales, e identificar si la imagen ha sufrido alteraciones.

- Tecnológico. Se creará una interfaz de usuario para el sistema que ayudará a cifrar y descifrar una marca de agua dentro de una imagen digital mediante el uso del algoritmo esteganográfico DCT.
- Social. Este algoritmo servirá como una herramienta para ayudar al creador de una imagen digital a proteger sus derechos de autor, insertando una marca de agua dentro de la imagen que acredite la autentificación de su obra, aunque esta sea modificada, por lo que se puede tener un impacto potencial en usuarios de diseño, dibujo artístico, fotografía, dibujos animados, logos comerciales, entre otros.

3 HIPÓTESIS

Mediante el diseño y desarrollo de un sistema que incorpora técnicas de esteganografía avanzada, se realizará, en una primer fase, el ocultamiento de una marca de agua con un tamaño de 150x150 pixeles como máximo, dentro de una imagen digital con formato jpg, de tamaño igual o menor de 1024x1024 pixeles; de tal forma que la marca de agua no modifique a simple vista la imagen original y no se altere ante modificaciones de la imagen, tales como corte de secciones de la misma o cambio de tonos, por lo que podrá ser reconocida por una segunda fase de estegoánalisis, en el mismo sistema, para determinar si la imagen ha sido modificada. Potencialmente, esto permitirá a un autor proteger su obra para preservar sus derechos de autor sobre la imagen digital, por medio de una herramienta para el ocultamiento de una marca de agua en su imagen digital, así como la identificación de alteraciones en la imagen original, con base en la verificación de la integridad de la marca de agua.

4 ESTADO DEL ARTE

4.1 Análisis de la literatura

El ocultar información dentro de una imagen digital mediante el uso de la esteganografía se ha convertido en herramienta efectiva para la transmisión de información, ya que esta información pasa desapercibida por las personas que visualicen dicha imagen (Soria Lorente, et al., 2013).

El diseño del sistema que se propone en este documento está enfocado al ocultamiento de una marca de agua que certifique los derechos de autor de una imagen, a su creador original, y que no se pierda cuando la imagen sea modificada, de tal manera que queda protegida aun cuando esta se sometida a alteraciones. Para ello es necesario tomar en cuenta los diferentes algoritmos y técnicas de ocultamiento que ofrece la esteganografía, pero lo más importante es considerar que esta debe ser una técnica esteganográfica robusta; es decir, que garantice que la marca de agua oculta este lo más integra al descifrarla con técnicas de estegoanálisis, aun después de que la imagen pase por ataques o modificaciones que la alteren (variación en la tonalidad de colores, recortes de secciones, cambios a la resolución o en su estructura, entre otros).

Las técnicas que más se acercan al objetivo de este trabajo son las técnicas del dominio de la frecuencia (Soria Lorente, et al., 2016), que son consideradas técnicas robustas por su gran resistencia a ataques. En algunos trabajos, los investigadores han experimentado con diferentes técnicas que abarca el ocultamiento de información en este domino, en las imágenes digitales, y sus resultados han sido muy eficientes en cuanto a la ocultación de información o incluso de otro archivo digital (Velasco Bautista, 2009) (Orea Flores, 2005).

La preferencia por el uso de las técnicas de esteganografía en el dominio de la frecuencia se debe a que el grado de modificación de las estego-imágenes es insignificante o muy poco, cuando se compara con las imágenes originales, pero en cuanto a resistencia a modificaciones, la información se ha logrado perder o distorsionar (Rodríguez Colín, 2006). Por ello, se deben considerar las investigaciones que se presentan en la Tabla 1, que es el resumen del estado del arte consultado para la presente propuesta, de tal manera

quesea posible determinar las técnicas que es más conveniente utilizar para obtener un resultado satisfactorio.

El sistema que se propone en este documento consiste en una interfaz de usuario a la que se le adapta y personaliza un algoritmo basado en técnicas de esteganografía en el domino de la frecuencia para obtener un resultado eficiente o que se cumpla el objetivo de la investigación mencionado con anterioridad; además, se adapta una herramienta de estegoanálisis, para determinar si una imagen previamente protegida ha sido alterada por una persona no autorizada.

Tabla 1 Matriz de Referencias

Autores, Titulo, fuente	Resumen	Metodología empleada	Áreas de oportunidad
A. Soria Lorente, et al., Algoritmo esteganográfico de clave privada en el dominio de la transformada discreta del coseno, Revista Cubana de Ciencias Informáticas, 2016.	La aplicación de esta técnica de clave privada para cifrar y descifrar la información dentro de una imagen digital garantiza que la esteganografía aplicada sea difícil de apreciar a simple vista pero fácil de descifrar.	Este tipo de esteganografía se garantiza una seguridad de nivel considerable, pero para aplicarla se necesitan procedimientos bastante complejos como la criptografía.	Relacionar esta técnica para la solución de otros tipos de esteganografía y determinar si sirve para el estegoanálisis de la mayoría de los formatos.
D. Renza, et. al., Método de ocultamiento de píxeles para esteganografía de imágenes en escala de grises, Revista Ingeniería y Ciencia, 2016.	En la aplicación de este método se puede ver que es posible ocultar información en imágenes y que sería muy complicado distinguir las imágenes en donde se emplearon la esteganografía, también menciona que es posible que la información oculta puede ser recuperada, pero en ocasiones no en su totalidad	Con la utilización de este tipo de ocultamiento garantiza que la información no será detectada a simple vista si no que será difícil detectar cual imágenes fueron sometidas a este proceso esteganográfico y cuáles no.	Determinar qué es lo que ocurre en el proceso de descifrado de información y determinar qué es lo que causa que los datos no se recuperen en su totalidad.
M. Ruiz Tejeida, Ocultamiento de información en documentos de formato abierto, Tesis de Maestria CINVESTAV , 2013.	Para el análisis de esteganografía se utilizan varias técnicas en las cuales se destaca la de LSB que es una técnica muy común dentro de la implementación para ocultar información, ya que toma un pixel de una imagen y lo convierte en una cadena de bits, en donde toma el bit menos significativo y lo modifica sin alterar visualmente a la imagen digital.	La técnica de LSB es una técnica eficaz para ocultar información dentro de las imágenes digitales, esta se divide en diferentes técnicas de acuerdo con el orden de pixeles distribuidos donde porta la información oculta, algunas son fáciles de cifrar y descifrar, pero otras no ya que aumenta la complejidad de ocultamiento.	Aplicar las diferentes técnicas de LSB y encontrar la más eficiente que garantice que la imagen sea difícil de identificar, pero fácil de descifrar.

J. M. Corona Falcón, Procedimiento de Integración de la Esteganografía al protocolo HTTP, Tesis de Licenciatura UNAM, 2015.	En la actualidad se manejan dos tipos de esteganografía las cuales son: clásica y moderna. La esteganografía clásica se refiere a los métodos simples que se utilizaban desde hace mucho tiempo y que en algunas partes del mundo se siguen utilizando, esta consta en tomar cualquier objeto portador y ocultar un mensaje, este objeto puede pasar desapercibido sin que nadie lo note hasta llegar el receptor destinado a leer el mensaje, y la esteganografía moderna es aplicada más a las imágenes digitales que se transmiten por medio de sitios web, redes o por otro medio, en estas insertan información oculta que a simple vista no se puede distinguir pero por medio de estegoanálisis se puede descifrar la información oculta.	Los dos tipos de esteganografía aplican en diferentes técnicas de ocultamiento de información que han funcionado para mantener una comunicación segura y sin ser detectada.	Encontrar un método que aplique en los dos tipos de esteganografía para su análisis.
G. E. Granda Tonato, Metodología para el Análisis Forense de Datos e Imágenes De Acuerdo a las Leyes del, Tesis de Licenciatura UPS, 2015.	Hay diferentes softwares que nos ofrecen una gran variedad de herramientas de esteganografía, estos tipos de softwares aplican varios algoritmos de ocultamiento de información, aunque hay pocos que también detectan indicios de esteganografía en imágenes, y en solo formatos especificados.	Se puede determinar qué tipo de estegoanálisis es el más conveniente utilizar para la mayoría de los formatos para detectar los indicios de esteganografía.	Analizar las diferentes herramientas que ofrece cada software y determinar cuál son las más convenientes para aplicar en la esteganografía
M. N. Rodríguez Mendoza, Análisis de las Técnicas de Esteganografía para el Ocultamiento de la Información, Ecuador: Tesis de Licenciatura, Universidad Central del Ecuador, 2016.	Hay diferentes técnicas y métodos que son muy efectivos en la aplicación de la esteganografía para el ocultamiento de información dentro una imagen digital una de ellas es la técnica de Spread Spectrum y LSB (el bit menos significativo), que son	La mayoría de las técnicas de esteganografía son métodos para obtener una comunicación segura entre un emisor y un receptor, con el fin de no comprometer a la información y que pase desapercibida	Analizar que técnicas son las convenientes para el ocultamiento de la información y determinar que herramientas utilizar para el estegoánalisis.

	técnicas que se utilizan con mayor frecuencia en la esteganografía.	por un medio no seguro como lo son las diferentes páginas de internet.	
R. H. Cuzco Naranjo, Propuesta de un Método Esteganográfico como Soporte al Proceso de Seguridad de Transferencia de Imágenes, Ecuador: Tesis de Maestría, Escuela Superior Politécnica de Chimborazo, 2017.	La implementación de un método esteganográfico en un método de criptografía aumenta el nivel de seguridad en la transferencia de imágenes, ya que con el método criptográfico se codifica el mensaje y con el esteganográfico se oculta dentro de una imagen para que no sea percibida por otros usuarios que no deban saber de dicha información oculta.	El uso de la esteganografía garantiza que la información no sea percibida por usuarios que no deban sospechar de que la información este oculta, pero se puede implementar un método de encriptación para aumentar la seguridad ya que es la información oculta la descubre un usuario intruso no podrá descifrarla ya que es necesaria una clave de desencriptación.	Considerar que es posible encontrarla información oculta pero que la decodificación de esta información será necesaria mediante otro algoritmo de desencriptación.
P. M. Méndez Naranjo, Nuevo Algoritmo Criptográfico con la Incorporación de la Esteganografía en Imágenes, Ecuador: Tesis de Licenciatura, Escuela Superior Politécnica de Chimborazo, 2015.	La seguridad de la información es muy importante ya que esto permite que no sea divulgada a personas no autorizadas y que a su vez tampoco la puedan manipular, una de las mejores formas de implementar la seguridad de la información es por medio de técnicas de esteganografía y si se quiere tener un nivel mucho más alto se puede incorporar métodos de encriptación para que la información se oculte dentro de una imagen digital y que además la información incrustada sea codificada dejando a la información inaccesible para un tercero.	Hay métodos esteganográficos que son muy complejos ya que ofrecen un nivel de seguridad muy alto y si además se agrega una técnica de encriptación es casi imposible poder descifrar el mensaje oculto dentro del archivo multimedia	Comprobar si es posible incorporar el algoritmo con un método de encriptación de datos
I. Redondo Chisvert, Desarrollo y Análisis de Algoritmos de Esteganografía, España: Tesis de Licenciatura, Universidad Politécnica de Madrid, 2017.	Existen diferentes métodos esteganográficos para la inserción de la información en imágenes digitales, en los cuales se adaptan de manera que no afectan demasiado visualmente a la imagen original, al momento de incorporar la información, también existen métodos para la extracción de la información, estos deben tener una	Los métodos de inserción y extracción de la información en imágenes digitales son algoritmos que permiten aplicar la esteganografía los diferentes formatos de imágenes digitales.	Verificar que métodos se pueden rescatar para implementar un mejor estegoánalisis más efectivo y que no dañe la información.

	eficiencia altamente segura, es decir, que no alteren o borren la información oculta.		
E. A. Morocho Checa, Implementación del Algoritmo Esteganográfico F5 para Imágenes JPEG a Color, Ecuador: Tesis de Licenciatura, Escuela Politécnica Nacional, 2014.	El algoritmo más utilizado y menos complejo es el LSB el cual toma el bit menos significativo, con la ayuda de esta técnica surgen otras técnicas más complejas ya que toman pieles de manera aleatoria, o el orden de los bits que se modifican para insertar la información.	El método LSB es una de las técnicas que se toman como base para generar nuevas técnicas más eficientes, y que brinden un mayor nivel de seguridad.	Determinar si el estegoánalisis de la técnica LSB se pueda implementar a sus técnicas descendentes.
A. Soria Lorente, R. M. Sánchez Reyes y A. M. Ramírez Aberasturis, Algoritmo Esteganográfico de Clave Privada, GIE Pensamiento Matemático, vol. III, nº 2, pp. 59-72, 2013.	El algoritmo esteganográfico de clave privada es uno de los sistemas esteganográficos más parecidos a lo que es la criptografía ya que para su descodificación es necesaria una clave, y aunque la información esta oculta no es posible identificarla con la ausencia de la clave que se utilizó para su cifrado.	Al encriptar la información queda de manera que no se entienda la información, con uso de un Estegosistemas con clave privada actúa como uno de encriptación ya que además de ocultar la información es necesaria una clave para poderla visualizar.	Implementar un sistema que analice las técnicas esteganográficas que son utilizadas con más frecuencia para el desarrollo de algoritmos para la ocultación de información.
I. Soria Solís, C. Castro Buleje, H. Calderón Vilca, C. Vargas Valverde, S. Pérez Quispe y A. Apaza Tarqui, Esteganografía en Imágenes Digitales Aplicando Autómatas Celulares Bidimensionales como Generadores Seudoaleatorios, Revista de Investigaciones de la Escuela de Posgrado, vol. VI, nº 1, pp. 66-77, 2017.	La Esteganografía permite la ocultación de información en imágenes, las cuales no se deben ver modificadas, hay técnicas que se pueden combinar para brindar una mayor eficiencia en la ocultación de datos dentro de una imagen, por ejemplo la técnica de LSB, donde se toman los valores de cada color RGB de cada pixel y se modifican dependiendo del bit a modificar, si es bien empleada la técnica, en la imagen resultante no se distinguirán las diferencias con la original a simple vista.	La combinación de técnicas esteganográficas nos permite obtener una nueva técnica que nos brinde una mejor seguridad de codificación de la información oculta.	Identificar que técnicas son compatibles entre sí (por ejemplo las basadas en LBS o las que trabajen con los coeficientes de matrices) y combinarlas de manera que se obtenga una mejor técnica de esteganografía.
A. Roman Gonzalez, C. J. Reynaga Cardenas y C. Ganvini Valcarcel, Método General para la Detección de Imágenes Alteradas Utilizando Técnicas de Compresión, Revista	Hay técnicas que nos permiten identificar si una imagen digital fue sometida a una alteración visual o en su estructura, una de ellas es mediante la función Rate-Distortion que está representada por una curva donde se	Con el uso de técnicas de detección de alteraciones dentro de una imagen digital, es posible determinar las zonas afectadas por el uso de softwares que modifique la imagen o	Comprobar si la técnica de detectar las imágenes distorsionadas pueda identificar las modificaciones hechas por técnicas de esteganografía con un nivel de seguridad alto

ECIPerú, vol. X, nº 1, pp. 14-23, 2013.	puede detectar donde exactamente se llevó a cabo la modificación de la imagen digital ya sea por la alteración grafica hecha por softwares o en su estructura de la información por medio de técnicas de esteganografía.	por métodos esteganográficos que manipulen la estructura de la información de la imagen.	
G. M. Velásquez Moreira, L. A. Molina Sabando y Í. B. Briones Véliz, Análisis de Técnicas de Esteganografía Aplicadas en Archivos de Audio e Imagen, Polo del Conocimiento, vol. II, nº 1, pp. 51-67, 2017.	La mayoría de las técnicas esteganográficas se basan en la aplicación a imágenes digitales, pero se pueden también implementar a otros tipos de archivos multimedia, ya que también están conformados por información hecha por bits, es decir que también son posibles objetos esteganográficos.	Algunas de las técnicas esteganográficas también se aplican en el ocultamiento de información en otros archivos multimedia además de las imágenes digitales.	Comprobar si existe una compatibilidad entre los estegosistemas de análisis para los diferentes archivos multimedia.
F. Sialer y I. Mejía, Comparación de Técnicas Esteganográficas de Dominio Espacial y Domino Frecuencial en Imágenes Digitales, Ingeniería: Ciencia, Tecnología e Innovación, vol. II, nº 2, pp. 41-49, 2015.	Las técnicas para la aplicación de esteganografía se dividen en dos dominios los cuales son: el dominio espacial y el de frecuencia. El primero se enfoca en el análisis de cada pixel de la imagen mientras que el otro se enfoca en el análisis los coeficientes de la imagen.	La implementación de las técnicas esteganográficas en las imágenes digitales, dependen del estegoánalisis que se desea aplicar además de que técnica es la más adecuada para el formato de la imagen.	Identificar cual técnicas, dentro del dominio del espacio o de las transformadas, es adecuada para implementar en cada caso de estegoánalisis.
J. Aguilar Santiago, Sistema Fotográfico para Aplicar Esteganografía y Cifrado en Rostros, México: Tesis de Licenciatura, Universidad de Guadalajara, 2017.	El uso de la esteganografía para mantener la información oculta es una de las herramientas que se puede implementar para poder proteger la información que se desea compartir, y que personas intrusas no se den cuenta de dicha información para no afectar la seguridad del usuario emisor y receptor. Aquí es posible codificar la información por medio de técnicas esteganográficas avanzadas o por medio de encriptación de la información.	Proteger la información combinando técnicas de esteganografía y encriptación ofrece un mayor nivel de seguridad para que los usuarios intrusos no puedan manipular dicha información.	Verificar si la información oculta y aparte encriptada está realmente segura, es decir que no cualquiera la pueda visualizar.

4.2 Derechos de Autor

Los derechos de autor son los que se adquieren cuando un artista crea una obra (fotografía, libro, animación, audio, entre otros) y quiere que este sea reconocido, hablando en términos legales se dice los derechos de autor son una construcción jurídica destinada a proteger la creación de formas, se dice que los derechos de autor tiene doble naturaleza; el derecho moral y el derecho patrimonial, el primero protege al autor que su nombre y obra no sean utilizadas de forma distinta a la que el autor desee, pero no tiene un fin económico, y la segunda si tiene como objetivo proteger al autor a obtener una compensación económica del uso y explotación de su obra (Colombet, 1997).

Los derechos de autor han cobrado mucha importancia con el paso del tiempo en diferentes partes mundo, ya que cada país ha tenido diferentes situaciones que los han obligado a crear y reforzar sus leyes, en especial las que protegen a las obras artísticas que implican imágenes, que son las más involucrados en problemas legales de derechos de autor, por ejemplo la reproducción de su obra, y que el sujeto u objeto que se utilice como modelo quiera apoderarse de la obra sin dar crédito al artista, entre otros (Lien Verbauwhede, 2006).

En diferentes sitios web y autores de obras experimentados en el ámbito artístico recomiendan diferentes técnicas para proteger los derechos de autor en imágenes, en las cuales se pueden destacar:

- Registrar las imágenes: Este proceso se hace en una institución de gobierno donde la imagen digital se debe registrar antes de que esta sea publicada, la imagen digital debe de contar por lo menos con una marca de agua de propiedad, esta puede ser el nombre de la empresa, artista o simplemente algo que identifique al autor, además de agregar el símbolo de copyright (©) que simboliza que la imagen ya está registrada legalmente (Alicea, 2011) (Cámara de Diputados del H. Congreso de la Unión, 2018).
- Publicar imágenes pequeñas o de baja resolución: Si la imagen no es de gran importancia se puede utilizar esta táctica que consiste en publicar imágenes que no sean de gran calidad, ya que no será de gran relevancia para los demás y así

evitar que sea usada, pero esta no protege al autor en términos legales (Agora Gallery, 2015).

- Agregar marcas de agua a las imágenes: Las marcas de agua es el método más popular para proteger una imagen, ya que no es una herramienta difícil de implementar, esta puede contener el nombre del autor, empresa, fecha, logotipo o cualquier información que autentifique al autor, esta técnica es muy efectiva para reclamación de derechos de autor ante autoridades legales (Alicea, 2011) (Agora Gallery, 2015) (Cámara de Diputados del H. Congreso de la Unión, 2018).

El uso de estas tácticas para la protección de derechos de autor no garantiza una protección en su totalidad, pues estas obras o imágenes digitales pueden ser modificadas, con el uso de softwares para el tratamiento de imágenes y quedar alteradas de tal manera de que pueden quedar desacreditadas por el autor original y perder todos sus derechos. Por ello es necesario el desarrollo de una nueva técnica que proteja los derechos de autor y que a su vez sea robusta a modificaciones de la imagen digital.

Para proteger los derechos de autor en imágenes hay varias técnicas, pero una de las que se han utilizado actualmente es la marca de agua, que tiene como objetivo proteger la imagen contra la manipulación o uso diferente para el cual fue creada (Lien Verbauwhede, 2006). Esto se realiza mediante la superposición de otra imagen difuminada o de texto, con la imagen original, por lo que usualmente se aprecia a simple vista.

El uso del término de marca de agua se utiliza comúnmente cuando se refiere al marcado de los billetes que se utiliza para comprobar que dicho billete es auténtico o falso, como se muestra a continuación en la Figura 1.

Figura 1 Marca de Agua de Seguridad en Billetes (BANXICO, 2018).

Pero para términos digitales las marcas de agua se dividen en tres grupos dependiendo su utilidad (M. Vargas, et al., 2016):

1) Marcas para proteger derechos de autor o autenticar.
2) Marcas para verificar la integridad de la imagen digital.
3) Marcas para insertar información o datos en la imagen.

En mayor parte, estas marcas de agua se utilizan en zonas o regiones dentro de la imagen, pero para una imagen con gran importancia como lo son las imágenes médicas o militares no se deben modificar de tal manera que se altere su estructura, por lo que la marca de agua debe pasar desapercibida al apreciar la imagen, por ello las marcas de agua las colocan en una zona insignificante o las hacen muy pequeñas, es por ello que las hacen vulnerables a que algún usuario que adquiera dicha imagen la pueda modificar como le plazca de tal manera que la marca de agua desaparezca, y por lo tanto le quitaría el crédito al autor original (M. Vargas, et al., 2016). Como se muestra en la Figura 2.

Figura 2 Marca de Agua en una Imagen Digital (WÍX, 2015).

4.3 Esteganografía

La esteganografía es el arte para ocultar información dentro de un objeto; es decir, que la información oculta dentro de un objeto portador pasa desapercibida por las personas que tengan en posesión cierto objeto y esta llega a su destinatario sin ser descubierta por los demás (Rodríguez Mendoza, 2016). Durante los últimos años se han realizado varios estudios donde se involucra el uso de la esteganografía, algunos por universidades nacionales y extranjeras, y otros por investigadores que han desarrollado varias técnicas para realizar la esteganografía en archivos multimedia, algunos temas que se destacan son:

- Tipos de esteganografía y su funcionamiento.
- La esteganografía en la comunicación.
- Metodologías empleadas a la esteganografía.
- Sistemas para el ocultamiento de información en imágenes.
- Detección de información oculta dentro de imágenes digitales mediante Software.
- Detección de imágenes digitales modificadas.
- Técnicas esteganográficas modernas y avanzadas aplicadas a imágenes digitales.

- Técnicas esteganográficas más utilizadas en la actualidad.

Tipos de esteganografía y su funcionamiento.

Durante su evolución, la esteganografía ha sufrido varios cambios, por lo cual se han desarrollado diversas técnicas que permiten la implementación de la esteganografía en diferentes áreas. Pero el objetivo de la esteganografía no ha cambiado: ocultar información dentro de un objeto para que esta no pueda ser identificada. Estas técnicas se pueden clasificar de la siguiente manera (Corona Falcon, 2015):

1) Esteganografía clásica: hay muchos antecedentes de la aplicación de esta técnica, desde imperios que se mandaban mensajes ocultos en la piel de animales, hasta en la actualidad que todavía hay personas que se comunican de esta manera, ocultando información dentro de artículos, libros, periódicos u otro medio escrito.
2) Esteganografía moderna: con el uso de la tecnología, este tipo de esteganografía es la más utilizada para ocultar información dentro de una imagen o archivo digital. Utiliza herramientas como la técnica *Least Significant Bit* (LSB, o en español: Bit Menos Significativo), y permite al usuario comunicarse con otro mediante el cifrado y descifrado de información, impidiendo que cualquier usuario pueda percatarse a simple vista de la información oculta, aunque este tenga en su poder la imagen contenedora.
3) Esteganografía Avanzada: emplea técnicas más avanzadas como las transformadas del espacio y del dominio de la frecuencia, que permiten ocultar la información de manera más eficaz que la esteganografía moderna, ya que hace uso de claves o contraseñas; teniendo cierto parecido con la criptografía (Rodríguez Mendoza, 2016).

La esteganografía depende de tres características principales para el proceso de ocultamiento de información, los cuales son (Cuzco Naranjo, 2017):

- Capacidad: que permita una mayor cantidad de información que pueda ser ocultada.
- Seguridad/Invisibilidad: que el nivel de probabilidad de la detección por un estegoanalista sea muy pequeño.

- Robustez: en esta característica implica la cantidad de alteraciones dañinas que el medio soporta antes de que se altere la información oculta.

Teniendo en cuenta las características anteriores se pueden generar algoritmos, que se basan en las siguientes metodologías (Cuzco Naranjo, 2017):

- La imagen digital existe y la ocultación de información no la modifica.
- La imagen digital existe y la ocultación produce alteraciones.
- La generación automática de la imagen incluye la información a ocultar.

Como ya se mencionó anteriormente, la esteganografía es confundida en algunas ocasiones con la criptografía, o que una sustituye a la otra, lo cual confunde a muchos al querer ocultar su información, pero es cierto que se puede trabajar con ambas técnicas agregándole a la información un nivel de seguridad más, ya que además que la información este oculta, también puede estar encriptada (Méndez Naranjo, 2015).

La esteganografía en la comunicación.

La esteganografía permite la comunicación entre dos o más personas a través de información oculta dentro de imágenes digitales; esta comunicación se puede clasificar a partir de un modelo general de la esteganografía, constituido de dos etapas (Rodríguez Mendoza, 2016):

1) La primera consta de un emisor, quien escoge una imagen digital que servirá como cubierta (C), lo cual permite que la transmisión de la información no sea detectada o que levante sospecha a terceros o usuarios que no deben saber de dicha información oculta; también consta de un mensaje secreto (M), que es la información que se inserta en dicha imagen, además de agregarle una estego-clave (K), que es la técnica que se aplica para el cifrado de la información , y como resultado se obtiene el estego-objeto (S), que es el objeto o imagen ya modificada con la información oculta, lista para ser transmitida por un canal público inseguro.
2) La segunda surge a partir de que el estego-objeto es adquirido por el receptor, el cual puede recuperar el mensaje oculto basándose en la técnica utilizada para el cifrado de la información oculta.

Para garantizar una comunicación sin que llame mucha la atención no se debe utilizar más de una vez la misma imagen como estego-objeto, ya que si se utiliza muchas veces la misma imagen posiblemente levante sospechas, poniendo en riesgo la información oculta o mensaje secreto. Otra forma de garantizar que la información oculta pase desapercibida por usuarios que no deben saber de dicha información, es utilizando la técnica esteganográfica adecuada para el tipo de imagen que se va a utilizar como objeto (Rodríguez Mendoza, 2016).

Con la ayuda de la esteganografía se garantiza una comunicación segura e imperceptible de los demás que tengan acceso a la imagen, ya sea por cualquier medio no seguro, se han dado casos donde la comunicación entre dos personas que comparten información relativamente importante utilizan estos métodos esteganográficos, y muchos aumentan la certeza de que su información no será expuesta por otra persona diferente al destinatario combinan la esteganografía otras técnicas como es la criptografía.

Metodologías empleadas a la esteganografía.

Un artículo de la revista Ingeniería y Ciencia llamado "Método de ocultamiento de píxeles para esteganografía de imágenes en escala de gris sobre imágenes a color", propone una metodología basada de un experimento, donde redacta que se utilizaron 10 imágenes a color y 10 imágenes a escala de grises, donde se adaptaron las dimensiones de las imágenes y durante las pruebas se observó que la imagen secreta tenía una relación de pixeles de 16:1, para esto fue necesario la utilización de un protocolo de pruebas del cual se obtuvo lo siguiente (Renza, et al., 2016):

1) La primera imagen secreta se oculta dentro de cada una de las imágenes huésped.
2) Ya una vez obtenido las estego-imágenes y claves, se obtienen las imágenes secretas recuperadas, para esto se calcula la calidad de las imágenes recuperadas.
3) Para cada imagen secreta se repiten los dos pasos anteriores.
4) Al acabar se obtienen las 10 estego-imágenes por cada imagen secreta, lo que quiere decir que se obtienen 100 estego-imágenes por cada método empleado.

Con el uso de este experimento se puede concluir que es posible el ocultamiento de una imagen digital dentro de otra imagen llamada huésped, y por medio de esta técnica es posible implementar el uso de claves para su cifrado y descifrado de las imágenes ocultas.

Métodos de extracción de información oculta en imágenes.

Existen varios algoritmos de estegoánalisis que permiten extraer la información oculta dentro de los archivos digitales, estos utilizan métodos que se basan en la esteganografía moderna y avanzada, algunos que se destacan por su eficiencia son:

1) JSteg: Este método trabaja con los coeficientes AC (Coeficientes resultantes de una matriz de 8x8), en lugar de la información de color que contiene cada pixel de la imagen digital, al aplicar este método se remplaza los bits menos significativos (LSB), de los coeficientes AC con aquellos datos que pertenecen a la información oculta (Giménez Aguilar, 2017). La implementación de este algoritmo tiene mejores resultados en las imágenes de formato JPEG.

2) F3: Este algoritmo también trabaja por medios de coeficientes solamente que, en lugar de sobrescribir los bits, hace un decremento en los valores de estos coeficientes y si al disminuir este valor da como resultado un 0 se tiene que volver a procesar el mismo bit de la información oculta con otro coeficiente (Giménez Aguilar, 2017).

3) F4: Este algoritmo es la mejora del F3, solo que aquí se utilizan los coeficientes negativos con el valor esteganográfico opuesto, es decir, que los valores negativos pares representan un 1 y los impares un 0; los valores positivos pares representan un 0 y los impares un 1 (Giménez Aguilar, 2017). Con la implementación de este algoritmo en una imagen digital los cambios hechos son muy pequeños de manera que no son visibles para la visión humana.

4) F5: Este es uno de los algoritmos recientes dentro del campo de la esteganografía, el cual trabaja en el dominio de la frecuencia con la DCT (Discrete Cosine

Transform), este algoritmo oculta los bits de la información dentro del coeficiente DCT de una imagen digital seleccionados de manera aleatoria. Las características principales de este algoritmo son las siguientes (Morocho Checa, 2014):

- Contiene un factor de calidad.
- Un archivo de entrada que es una imagen digital que puede ser de formato JPEG, BMP o GIF.
- El archivo digital (imagen digital, archivo de texto, entre otros) que contiene la información a ocultar.
- Una estego-clave.

5) DCT con clave privada: La implementación de una clave privada en un sistema esteganográfico garantiza que la información oculta no sea descifrada por cualquier persona o usuario, sino que solo va a ser posible que la información oculta sea visible para los usuarios que tengan la clave, este tipo de técnica es parecida al cifrado simétrico(donde la misma clave se usa para cifrar y descifrar el mensaje), solo que se diferencia en el proceso de inserción (Soria Lorente, et al., 2013).

Para que un sistema esteganográfico sea eficiente, debe tener un nivel de imperceptibilidad bueno; es decir, que este sistema debe generar un esteganograma inocente y que no levante alguna sospecha a simple vista. Una de las maneras de hacer esto posible es la utilización de una clave privada para ocultar la información dentro de una imagen (Soria Lorente, et al., 2016). Para el cifrado de información aplicando este método, se debe seguir una secuencia de pasos, los cuales son:

1. Se debe solicitar una clave de 64 bits al usuario. En esta, la secuencia binaria de la clave se emplean particiones en bloques de 16 bits, esto se hace para facilitar la clave secreta al usuario, con esto le facilita el cifrado y descifrado de la esteganografía aplicada.
2. Se modifica la secuencia binaria de la información oculta en bloques de 64 bits con el escaneo de zigzag y aplicando diferentes operaciones para obtener una cantidad de bloques de 64 bits.

3. Después segmentarlos en bloques de 8x8.
4. Convertir el dominio de la frecuencia con la DCT (Discrete Cosine Transform).
5. Se calcula la energía, esto quiere decir que la transformada de coseno discreta consigue concentrar la mayor parte de la información en pocos coeficientes transformados de cada una de estas matrices cuadradas anteriores, a lo que se dice que la transformada de coseno discreta consigue concentrar la mayor parte de la información de las matrices en pocos coeficientes transformados (Soria Lorente, et al., 2016).
6. Se seleccionan las matrices cuadradas de orden 8, donde la energía calculada es mayor que un umbral dado.
7. Se divide cada elemento de cada matriz de cuantificación que se da, con relación al factor de calidad.
8. Se realiza un escaneo del primer movimiento en zigzag.
9. Se insertan los elementos de la secuencia binaria en los bits menos significativos.
10. Multiplicar cada matriz resultante y aplicar la inversa de la DCT para construir la imagen con esteganografía.

Sistemas para ocultamiento de información en imágenes.

El constante uso de las imágenes digitales las ha convertido en el medio más vulnerable para ocultar información, con el propósito de se introduzca la información dentro de la imagen sin afectar la estructura. Por ello, es necesario utilizar dos procesos, que son: un mecanismo de incrustación y el otro que es de extracción o detección (Ruiz Tejeida, 2013). Las técnicas más utilizadas para ocultar información mediante esteganografía son

1) Bit Menos Significativo (LSB), es un método utilizado en imágenes donde cada píxel es representado por un valor de 8 bits, y dentro este valor se modifica un solo bit, que es el menos significativo. Ya que solo es un bit el que modifica en cada pixel de la imagen original, esta no tiene gran diferencia visual con la imagen modificada.

   Este método se puede implementar en las imágenes digitales, pero para obtener un mejor resultado se puede aplicar en autómatas celulares bidimensionales como

generadores de bits pseudoaleatorios, que impone el píxel que va a actuar como semilla además del orden de las filas y columnas (Soria Solís, et al., 2017).

2) Digital Invisible Ink Toolkit (DIIT) este método utiliza como base la técnica LSB para marcar imágenes de 24 bits (imágenes a color RGB), además de que se permite seleccionar que pixeles se van a modificar sin importar el orden. Cada una de estas variaciones se clasifican de la siguiente manera:
    - BlindHide o esconder "a ciegas", en este proceso se inicia de la esquina superior de la imagen y continúa línea por línea hacia abajo, modificando píxel a píxel con la técnica LSB.
    - HideSeek en esta técnica el mensaje oculto se distribuye de manera aleatoria, en ella es necesario saber en qué posición se va a empezar el análisis de descifrado si no se debe realizar todas las combinaciones necesarias para encontrar este píxel inicial, esta técnica brinda una mayor seguridad, aunque tarda un tiempo considerable al aplicar el estegoanálisis.
    - FilterFirst, en esta técnica es fácil de identificar los pixeles modificados ya que cambia el orden de estos y se puede visualizar por que modifica la imagen visualmente.
    - BattleSteg es una combinación de HideSeek y de FilterFirs, pero mejora la forma de ocultar la información, esta filtra la imagen modificando los bits más significativos y selecciona las posiciones aleatorias en donde se va a ubicar la información oculta, para descifrar la información es necesaria la contraseña igual que el HideSeek

Cada tipo de técnica que se deriva del LBS se aplica en diferentes casos, cada una maneja un grado de dificultad para el cifrado y descifrado de información oculta en los pixeles, estas técnicas son las más utilizadas para la esteganografía y que solo se modifica un solo bit, esto permite ocultar la información dentro de la imagen sin ser detectada a simple vista ya que no se modifica visualmente la imagen, en algunas técnicas como lo es DIIT se modifica el orden de los pixeles a modificar por lo cual brinda una mayor una seguridad y que no cualquiera pueda descifrar la información oculta. Para el desarrollo del sistema se debe considerar una técnica que sea capaz de pasar desapercibida la información oculta, lo cual cumplen estos sistemas de esteganografía, pero con el uso de estos sistemas no

garantiza que la información se altere o se pierda al modificar la imagen y por ello que estos sistemas no son del todo efectivos para ocultar información importante.

Detección de información oculta dentro de imágenes digitales mediante Software.

Para llevar a cabo la extracción de la información oculta por medio de técnicas esteganográficas, lo primero es verificar si el formato del archivo si es correcto, es decir que si se trata de un archivo valido, para ello se tienen que comprobar si hay contenido sospechoso en este archivo por medio de un análisis muy detallado (Granda Tonato, 2015). Para llevar a cabo este análisis se puede hacer uso de softwares encargados para el análisis de ficheros como lo son:

1) AccesData FTK Imager, que con la opción de Add Evidence Item se podrá llevar acabo el análisis del archivo multimedia donde nos muestra la información contenida en la cabecera de la imagen en forma de matriz.
2) XStegSecret, este software implementa técnicas esteganográficas, realiza ataque visual, estadísticos, este software solo detecta formatos BMP, GIF y JPEG, cuando se analiza una imagen con este software, da la opción si se quiere someter a un análisis RS-Atack para detectar modificaciones cuando se modifican los bits menos significativos aleatoriamente, es decir que hace uso de la técnica de esteganografía LBS, esta técnica tiene mayor precisión en la detección de esteganografía en imágenes BMP.
3) StegDetect, este software es de distribución libre de Linux, solo se aplica en imágenes con formato JPEG y al hacer el análisis lo que detecta es la técnica o herramienta que se utilizaron para realizar la esteganografía en la imagen.

La mayoría de estos softwares aplican la esteganografía básica, es decir, que es fácil identificar las imágenes que tengan indicios de esteganografía, por lo tanto, no son seguras para transmitir información, además de que se limitan a ciertos formatos de imágenes y para su descifrado hace el uso de técnicas que no recuperan la información en su totalidad.

Detección de imágenes digitales modificadas.

El método de detección de compresión de datos permite detectar si una imagen fue alterada o modificada. Tiene el fin de detectar si una imagen digital fue modificada visualmente o en su estructura de información, una de las maneras de que estas imágenes sean modificadas visualmente es mediante softwares(Paint, Photoshop, Corel Draw, entre otros) en los cuales los usuarios, aunque no tenga mucho conocimiento en esta área, son capaces de alterar la imagen (cambiándole el color, aplicándole filtros, agregándoles figuras, entre otras acciones), y la otra forma de modificar la imagen, es mediante la estructura de su información, en donde el usuario que aplique este tipo de alteración debe tener un poco más de conocimiento en el área de la esteganografía, en la cual permite que se ingrese información dentro de la imagen ocultándola y que esta no sea visible, en la mayoría de los casos.

El método para la detección de imágenes manipuladas es un método que sirve encontrar, de manera más eficiente y precisa, las imágenes digitales modificadas visualmente y a qué tipo de alteración se sometieron, para ello se utiliza una técnica de análisis, la cual es denominada "Análisis de Imágenes Utilizando la Curva Rate-Distortion". Este método es utilizado principalmente para la detección de alteraciones visuales, su análisis se refiere a la implementación de una función llamada RD (Rate-Distortion), mediante este análisis se obtiene una curva experimental, al graficarla se tiene que el eje horizontal es el tamaño de la imagen y en el eje vertical está representado por la distorsión calculada mediante la herramienta de MSE (Mean Square Error), en la curva se puede visualizar el lugar exacto donde se encuentra la distorsión y por medio de la técnica de la Función Estructura de Kolmogorov (KSF) aplicada la curva experimental, es posible recuperar una aproximación de la imagen original en la imagen modificada (Roman Gonzalez, et al., 2013).

Este tipo de análisis es capaz de detectar cualquier alteración dentro de las imágenes digitales, aunque sea una modificación insignificante es posible identificarla, lo cual la convierte en una herramienta eficiente para el estegoánalisis, ya que al modificar la estructura de la información dentro de la imagen se obtendrá una imagen modificada, que,

aunque no sea percibido visualmente, hay una alteración que es posible detectar mediante este método.

Técnicas esteganográficas modernas y avanzadas aplicadas a imágenes digitales.

Las imágenes digitales son gráficos creados mediante herramientas de la computadora mediante softwares que permiten diseñar gráficos, o también es posible crear gráficos por medio de dispositivos, como lo son las cámaras o sensores que permiten captar información y convertirla en un gráfico. Durante los últimos años la esteganografía es aplicada con más frecuencia en los gráficos creados mediante dispositivos o mejor dicho "fotografías" (Velásquez Moreira, et al., 2017). Las técnicas de imagen que se aplican en la esteganografía se clasifican en los siguientes dominios:

1) Dominio Espacial: Los métodos o técnicas en el dominio espacial modifican directamente los valores de los pixeles en la imagen huésped o la estego-imagen, como lo son los valores de color, en función de los valores de cada pixel de la imagen o datos de la información a ocultar, el método más común que entra dentro de este grupo es el llamado LSB, el uso de estas es muy sencillo y fácil de implementar (Renza, et al., 2016) (Rodríguez Colín, 2006) (Orea Flores, 2005) (Sialer & Mejía, 2015), está conformada por las siguientes técnicas en las siguientes técnicas.
    - Least Significant Bit (LSB): Este método modifica el bit menos significativo del valor de RGB de cada píxel de la estego-imagen por el valor de los bits de la información a ocultar, por ello es difícil distinguir la diferencia de la imagen original con la estego-imagen, esta es una de las técnicas más utilizada ya que no es tan compleja. Una de sus desventajas principales es que si la estego-imagen sufre un ataque o modificación la información se transformaría a algo diferente o se perdería (Rodríguez Medina & Navas, 2016) (Renza, et al., 2016).

    - RGB based Steganography: esta técnica está basada en los tres colores primarios; por sus siglas en ingles Red (R), Green (G), Blue (B). donde cada píxel está conformado por la combinación de cada uno de estos colores, por lo que se obtiene

un esquema del color resultante de 24 bits (8 bits por cada color primario), aplicando esta técnica los pixeles de la imagen RGB se pueden utilizar una capa o cobertura a través de un canal para indagar información en otros canales, estos valores son aleatorios y dependen de los pixeles que cuenta la imagen digital a utilizar.

En un trabajo de investigación hecho por José Aguilar Santiago donde propuso un sistema basado en la técnica RGB para la aplicación de esteganografía, este lo utilizó adaptándolo de manera que cada pixel es conformado por tres colores RGB, los cuales se convierte en tres subpixeles denominados PR, PG, y PB, estos obtienen un valor entero que esta entre 0 y 255, en donde estos valores los guarda en un arreglo para después calcularlos de acuerdo a su longitud y obtener un vector donde se queda almacenada la información codificada, después cada subpixel se divide entre 255 para obtener un valor que va de 0 a 1, estos valores se mezclan con la órbita caótica obtenida en el vector, después se aplica la técnica llamada difusión para generar las llaves de cifrado y por ultimo obtener las posiciones mediante un vector de posiciones (Aguilar Santiago, 2017).

- Pixel Value Differencing (PVD): esta técnica facilita la incorporación de información a las imágenes, además que la imagen modificada no se alcanzan a distinguir los cambios visuales al compararla con la original, ya que esta técnica se basa en insertar la información en una imagen de cobertura, es decir, que mediante la sustitución de valores en la diferencia de bloques de parejas de pixeles de la imagen digital con otros que sean similares, la desventaja de esta técnica es que solo se puede incrustar poca información ya que si se inserta mucha información la imagen se distorsiona y es fácil detectarla.

- Mapping Based Steganography: esta técnica también es llamada Pixel Mapping Method (PMM), y se basa en ocular datos en imágenes digitales que estén en escala de grises, la inserción de la información va en pixeles que se seleccionan por medio de funciones matemáticas que dependen del valor del pixel semilla.

- Método de ocultación de píxeles de bloque (BPHM): Este método está enfocado a la ocultación una imagen sobre otra imagen, ya que divide a la imagen a modificar en un número de bloques cuadrados, todos de igual tamaño, donde el número de bloques es igual al número de pixeles de la imagen a ocultar, después identifica el bloque que sea más compatible con cada pixel a ocultar, para la identificación de la imagen oculta es necesario contar con la clave de las posiciones del orden de ocultamiento de los pixeles en los bloques donde se ocultaron (Renza, et al., 2016).

2) Dominio de la Frecuencia: Esta se basa en ocultar la información en la imagen digital en coeficientes AC (Sialer & Mejía, 2015). Las técnicas que se utilizan en el domino de la frecuencia, o también conocidas como dominio de las transformadas por el uso de transformadas, modifican directamente los valores de los coeficientes de las transformadas para insertar la información a ocultar, este tipo de técnicas divide a la imagen en bloques donde calcula los coeficientes de cada uno con la transformada más adecuada; por ejemplo: DCT(Discrete Cosine Transform), DWT(Discrete Wavelet Transform), DFT(Discrete Fourier Transform), entre otros. Después en los coeficientes calculados se inserta la información a ocultar y por último para obtener la información oculta es necesario aplicar la inversa de la transformada que se haya utilizado para calcular los coeficientes (Renza, et al., 2016) (Rodríguez Colín, 2006) (Orea Flores, 2005).Este tipo de dominio utiliza técnicas más complejas y robustas ya que son más difíciles de percibir o detectar y evita que se pierda por completo la información, las técnicas que se utilizan con más frecuencia en este domino son:

- Transformada Discreta de Fourier (DFT, Discrete Fourier Transform): es una técnica que se basa en transformaciones matemáticas, con el fin de insertar la información en la imagen bidimensional, ya que las imágenes digitales se pueden interpretar como funciones bidimensionales discretas, estas se pueden obtener empleando sumatorias en lugar de integrales, en otras palabras, empleando la Transformada Discreta de Fourier, con la siguiente ecuación:

$$F(u,v) = \frac{1}{M \cdot N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \cdot e^{-j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)}$$

Figura 3 Transformada Discreta de Fourier de Dos Dimensiones

Donde M es el número de columnas (pixeles en el eje X) y N es el número de filas (pixeles en el eje Y). La Transformada Inversa de la Discreta de Fourier para dos dimensiones está dada de la siguiente manera:

$$f(x,y) = \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u,v) \cdot e^{j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)}$$

Figura 4 Transformada Inversa Discreta de Fourier de Dos Dimensiones

- Transformada Discreta del Coseno (DCT, Discrete Cosine Transform): La técnica de la transformada discreta del coseno es una de las más utilizadas dentro del dominio de la frecuencia para ocultar información, esta consiste en el cálculo de los coeficientes de una matriz de dos dimensiones (NxN) de pixeles, estos pueden representarse en funciones del coseno (Orea Flores, 2005):

$$p(x,y) = \frac{2}{N} \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} C(u)C(v)S(u,v) \cdot \cos\left[\frac{(2x+1)\pi u}{2N}\right] cos\left[\frac{(2y+1)\pi v}{2N}\right]$$

Figura 5 Transformada Discreta del Coseno

Donde:

$$S(0,0) = \frac{1}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} p(x,y)$$

Como resultado la ecuación general para S(f) es:

$$S(u,v) = \frac{2}{N} C(u)C(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} p(x,y) \cdot \cos\left[\frac{(2x+1)\pi u}{2N}\right] cos\left[\frac{(2y+1)\pi v}{2N}\right]$$

Figura 6 Transformada Discreta del Coseno Bidimensional de p(x, y).

Donde:

$$C(u), C(v)= \begin{cases} \sqrt{1/N} & u, v=0 \\ \sqrt{2/N} & 1 \leq u, v \leq N-1 \end{cases}$$

En esta las frecuencias, ya calculadas con la DCT, se van colocando en forma de zigzag empezando de la frecuencia más baja, que es la posición (1,1), hasta la frecuencia más alta, la posición (8,8) para el caso de la Figura 7 (Orea Flores, 2005).

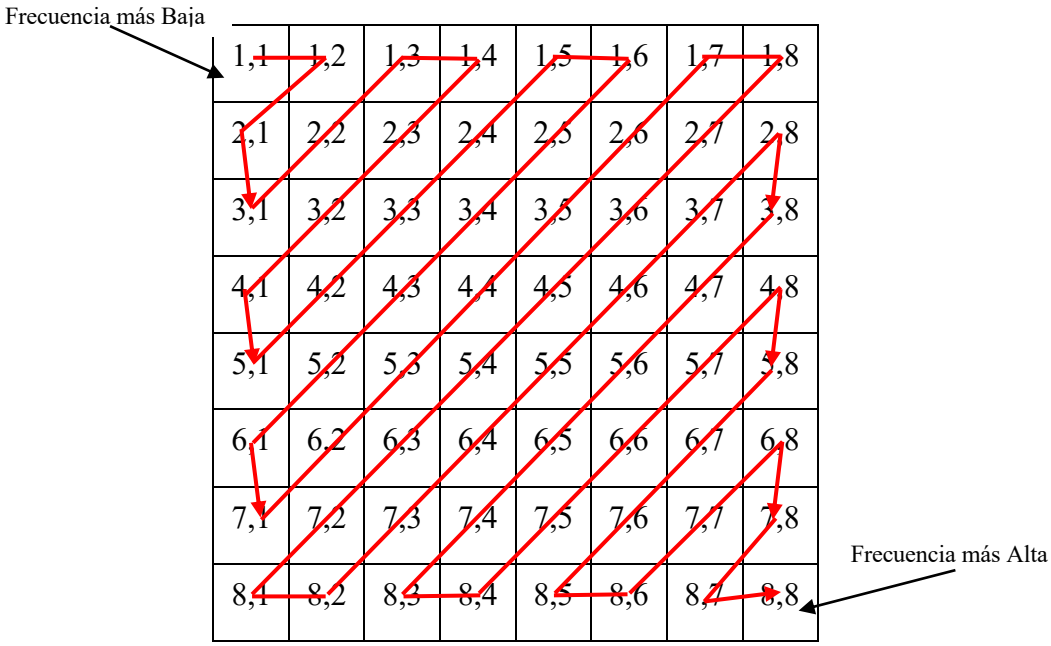

Figura 7 Posición de las Frecuencias

- Transformada Discreta de Wavelet (DWT, Discrete Wavelet Transform): esta técnica está basada en herramientas matemáticas que se utilizan para la descomposición de las imágenes y las transforma en pequeñas ondas, las cuales son llamadas ondículas con diferentes frecuencias. La discreta de una función wavelet forma parte de un grupo de wavelets llamados ortonormal, ya que la función f(t) como soporte finito puede ser reconstruida como la suma de

coeficientes wavelets discretos Wf(s, τ) multiplicados por las funciones de la base, la cual está definida como:

$$f(t) = \sum_{s} \sum_{\tau} W_f(s,\tau)\psi_{s,\tau}(t)$$

Figura 8 Transformada Discreta de Wavelet

La descomposición de una wavelet ortonormal no contiene información redundante y representa una señal de forma univoca, además que las bases son posibles con wavelets con factores de translación y dilatación discretos (Altamirano, 2012).

3) Técnicas de Distorsión: Estas técnicas se basan en encontrar diferencias entre la imagen original y la imagen distorsionada, utilizando una imagen de cobertura para el proceso de decodificación, por lo cual esta imagen de cobertura en necesaria ya que si no se tiene es casi imposible su extracción de información.
4) Enmascaramiento y Filtrado: Este utiliza técnicas parecidas a las marcas de agua que se utilizan en los documentos para protegerlos, solo que en este se crean mascaras en la imagen, es un poco más complejo que el LSB, solo que este busca que no se distingan los cambios visuales en la imagen con la máscara respecto a la original. Esta técnica no aplica en todos tipos de imágenes, donde presenta una mejor esteganografía es en imágenes de 24 bits o imágenes con escala de grises.

La implementación de estos dominios dentro de un sistema esteganográfico garantiza que el cifrado sea correcto y que en el descifrado no se vea afectada la información ya que hay técnicas que no garantizan que la información llegue correctamente al destinatario final.

5 MÉTODO

Para el desarrollo del sistema se tomó como base la metodología de cascada con retroalimentación, que se basa en que el producto evoluciona a través de una secuencia de pasos en forma lineal y permite interactuar con el paso anterior (Cataldi, 2000), este consiste en las siguientes secciones o pasos:

1. Análisis de Requisitos del Sistema.
2. Análisis de Requisitos del Software.
3. Diseño Preliminar.
4. Diseño Detallado.
5. Codificación y Pruebas.
6. Mantenimiento.

En la siguiente Figura 9 se puede ver cómo es el funcionamiento de la metodología de cascada para el desarrollo de software:

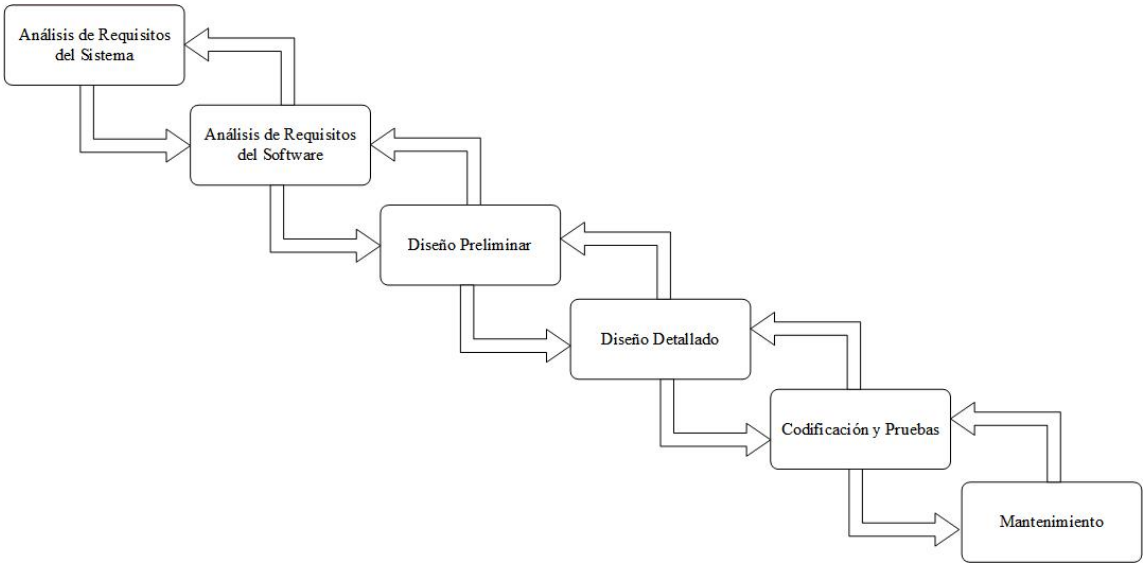

Figura 9 Metodología de desarrollo en cascada con retroalimentación

5.1 Requerimientos o especificaciones

El primer paso, de acuerdo con la metodología seleccionada para el desarrollo del sistema, consiste en el análisis de los requisitos del sistema y software. En este caso, el requisito principal es el objetivo de este trabajo: ocultar una marca de agua en una imagen mediante una técnica robusta de esteganografía. Como parte importante se contempla el diseño de la interfaz con la cual el usuario manipula el sistema para proteger su imagen digital. La codificación se apoya en los algoritmos de esteganografía y las herramientas que ofrece el lenguaje de programación Python 3.7. Las pruebas se realizan con los diferentes tamaños y formatos de imágenes, con lo cual se obtienen los resultados, en cuanto a determinar si es posible ocultar la marca de agua dentro de la imagen pasando desapercibida al ojo humano y que soporte los ataques que sufra esta imagen con el fin de que no se pierda la marca de agua.

El sistema está compuesto de la siguiente manera, como se muestra en Figura 10, donde la imagen es transmitida mediante un canal; este canal es el medio inseguro por el cual va a ser transmitida que son las diferentes paginas o redes sociales en el cual va a ser adquirida por el receptor; el receptor puede modificar la imagen, pero no se perderá por completo la marca de agua; el autor debe aplicar un estegoanálisis para descifrar la marca de agua oculta. Con el uso de este sistema el autor auténtico puede insertar una marca de agua casi inalterable, en cuestión de ataques a la imagen (distorsionar de manera significativa la estructura de la imagen, como cambio de tonalidades, modificación de tamaño, o recorte de zonas de la misma).

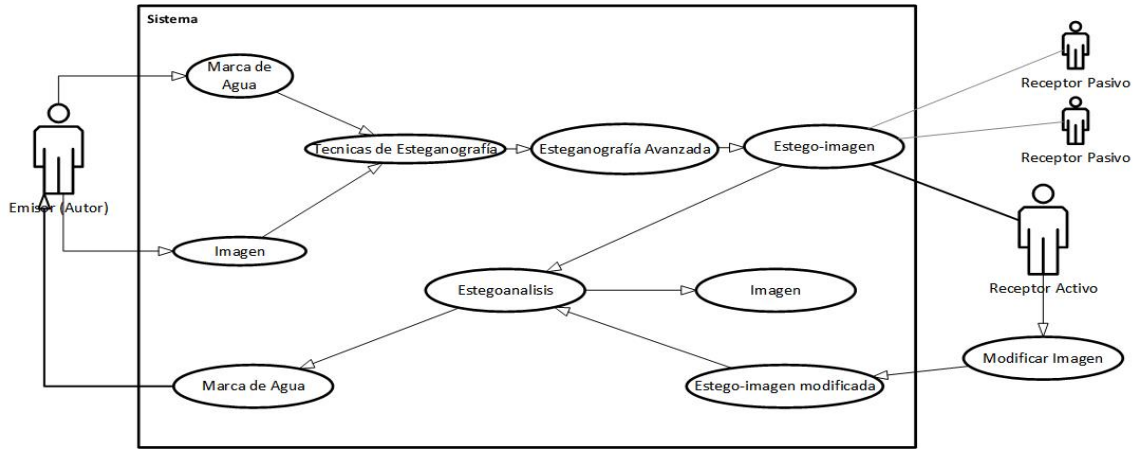

Figura 10 Diagrama de estados de uso aplicado al algoritmo esteganográfico.

El funcionamiento del sistema descrito se basa en el siguiente diagrama de la Figura 11.

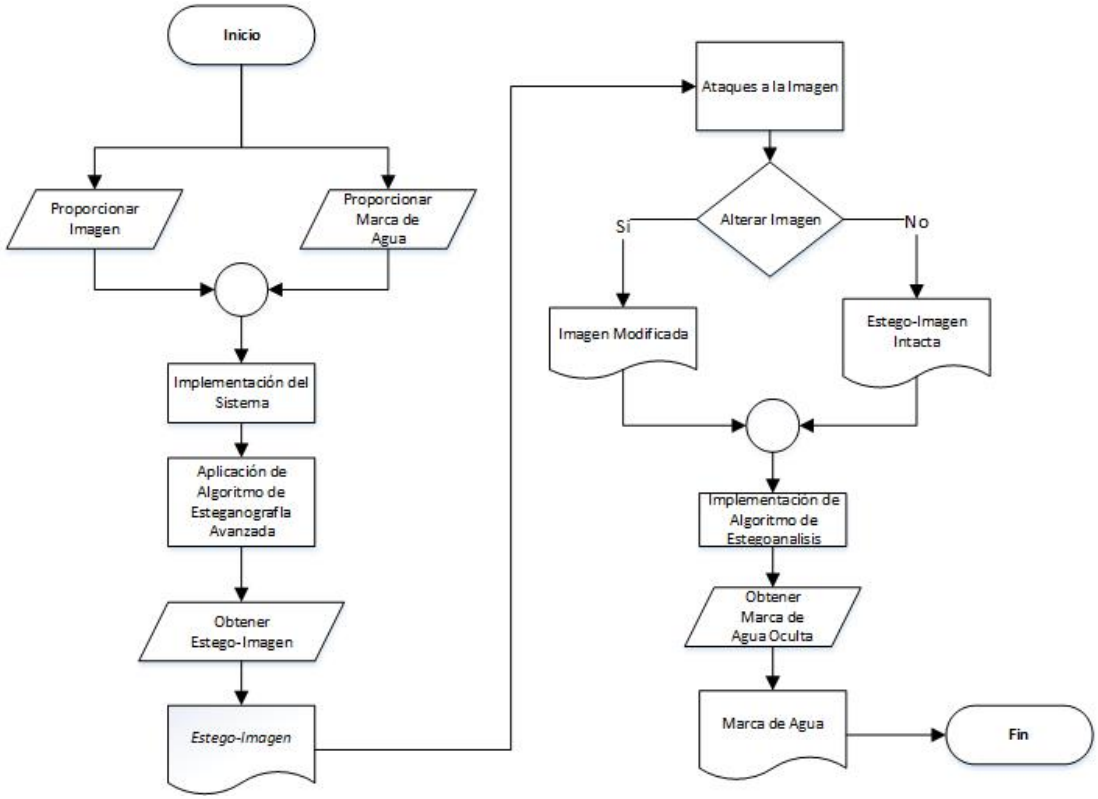

Figura 11 Diagrama de Flujo del Funcionamiento del Sistema

5.2 Diseño e implementación

Anteriormente ya se mencionaron los requerimientos del sistema y software, ahora de manera más detallada se muestra a continuación en la Figura 12 un diagrama, en la cual se muestra cómo debe estar integrada la interfaz con la que el usuario va a interactuar con este sistema, este debe contar con tres botones, donde el primer botón da la opción de llevar a cabo la protección de la imagen mediante la incrustación de una marca de agua, la segunda opción o botón tiene como función verificar la marca de agua oculta dentro de una estego-imagen, y por último el tercer botón permite que el usuario salga del sistema.

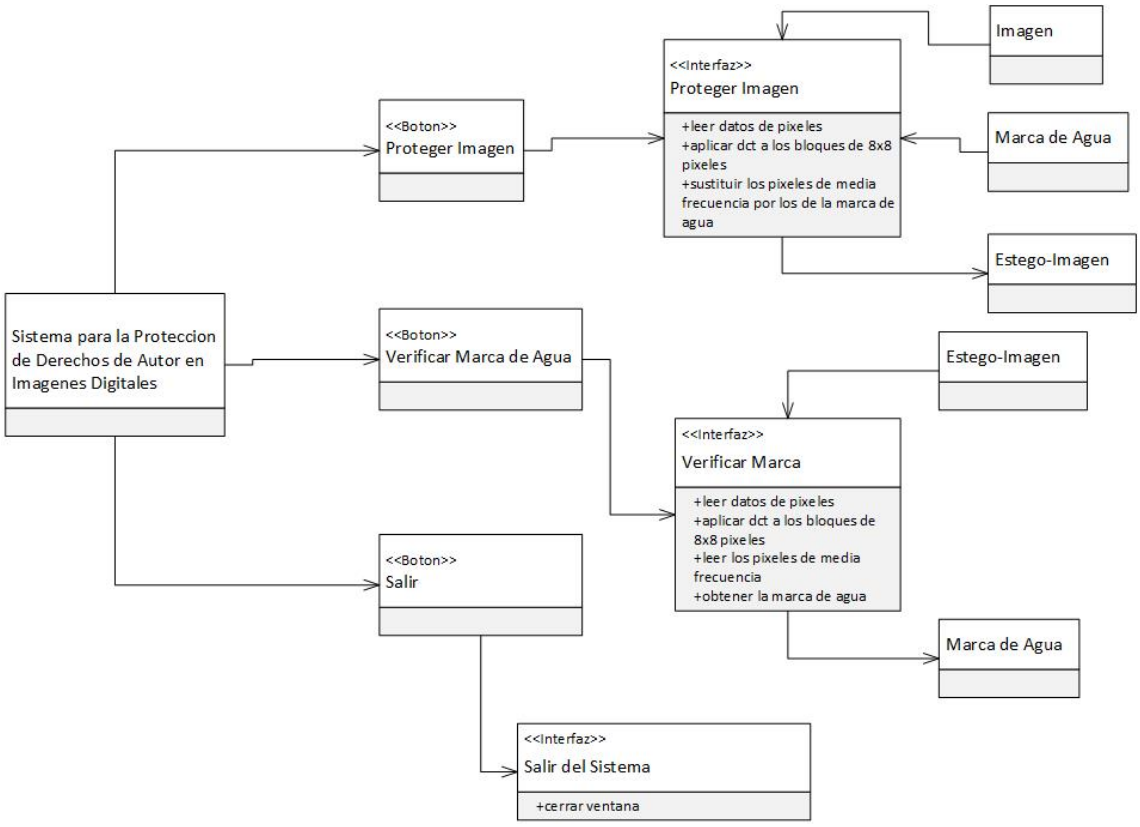

Figura 12 Diagrama UML para el sistema de protección de derechos de autor en imágenes digitales.

Cabe resaltar que, como se puede apreciar en la figura anterior, el sistema proporciona al usuario dos opciones relativamente importantes, las cuales son “Proteger Imagen”, y “Verificar Marca”; la primera consiste en proporcionarle al sistema la imagen digital a proteger y la marca de agua la cual se va a insertar dentro de la imagen, el proceso de esta opción se puede ver de manera más detallada en el diagrama de la Figura 13; y por otra parte, en la segunda opción el sistema decodifica la marca de agua que ya se haya ocultado con anterioridad con el uso de este sistema, este proceso se puede apreciar de manera más minuciosa en la Figura 14.

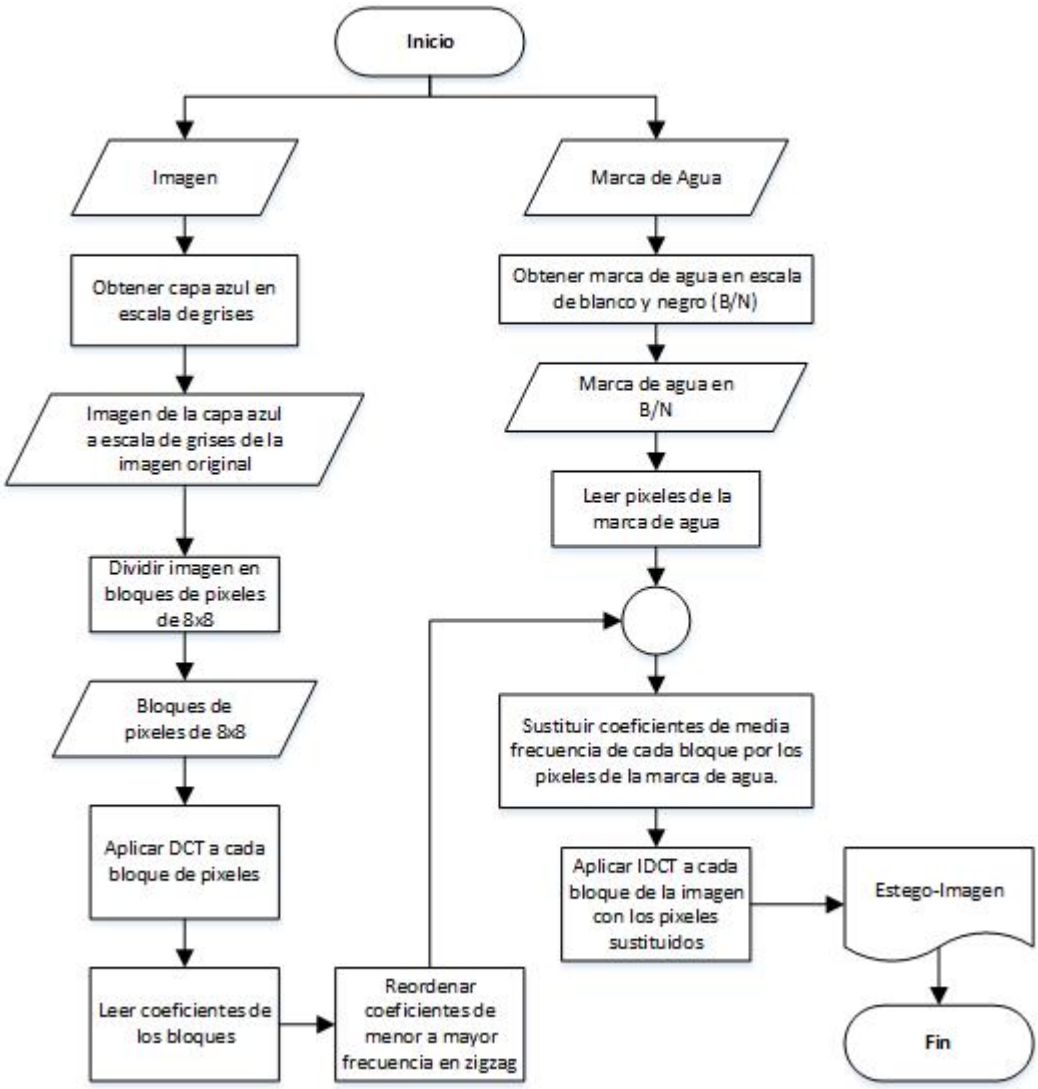

Figura 13 Diagrama del proceso de protección de la imagen digital.

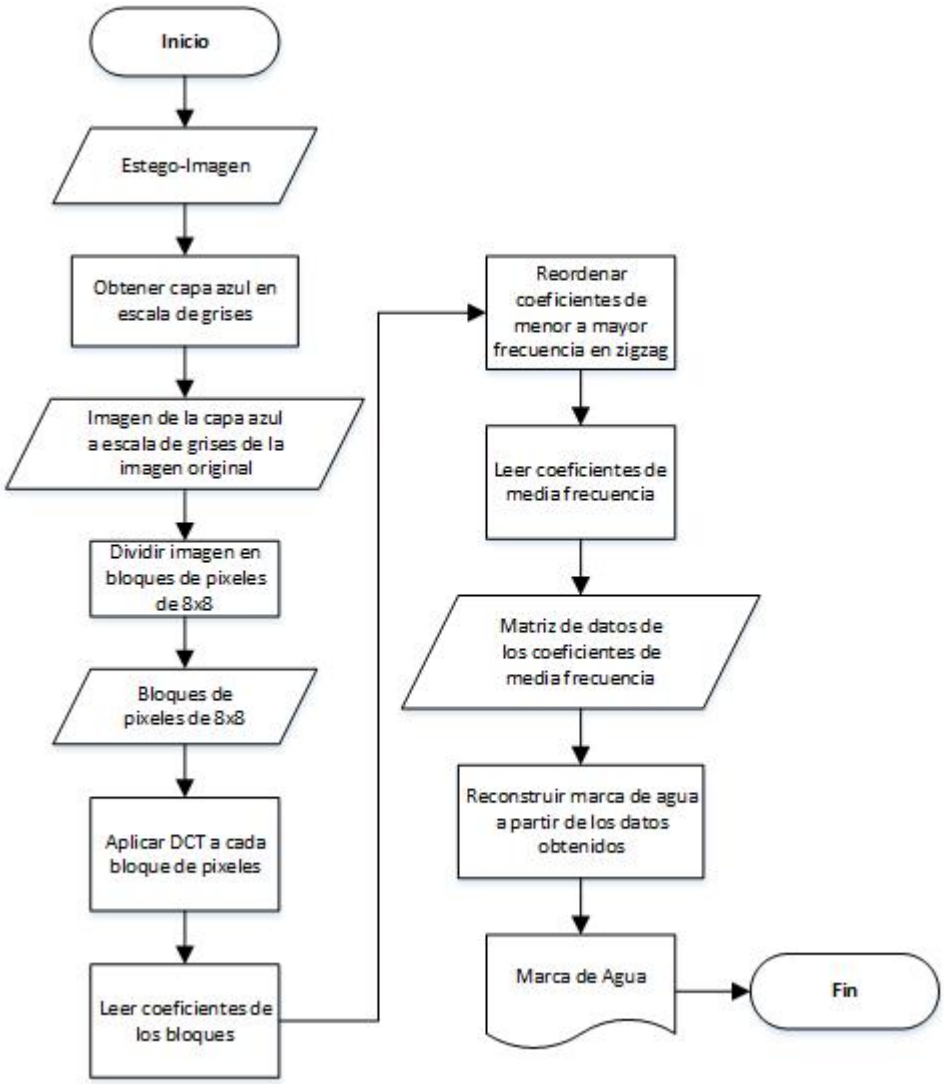

Figura 14 Diagrama del proceso de verificación de marca de agua.

De acuerdo con la metodología de cascada empleada para el desarrollo del sistema se debe hacer un diseño preliminar; este diseño está conformado como se especifica en la Figura 12. En esta figura se ilustra cómo está integrado el sistema: a) primero el usuario visualiza una interfaz, a esta le va a proporcionar dos elementos: la imagen y la marca de agua, b) después el control del sistema se encarga de validar estos dos elementos, c) ya que estén validados, se aplica la técnica esteganográfica robusta DCT a la imagen para ocultar la marca de agua, d) como resultado se obtiene una estego-imagen que después se verifica que para no tenga un grado de modificación muy notable comparada con la imagen

original (este se evaluara por medio de la comparación de pixel a pixel de la imagen y la estego-imagen y tener como resultado un promedio general o una diferencia absoluta), y e) la estego-imagen queda a disposición del usuario teniendo la posibilidad de guardarla.

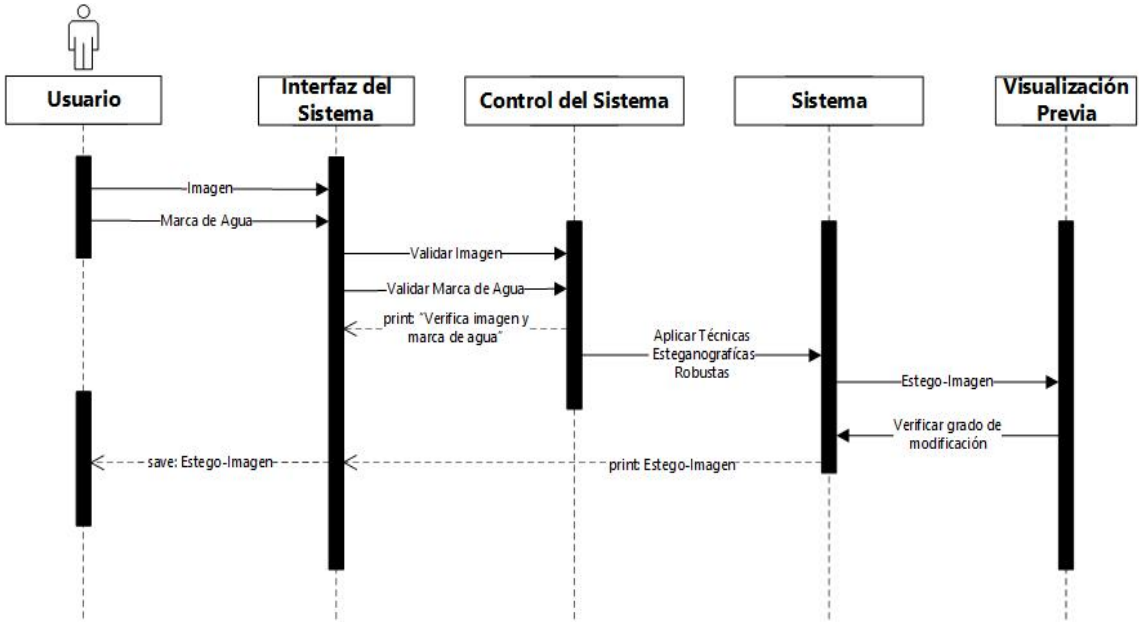

Figura 15 Diagrama de Secuencias del Diseño Preliminar del Sistema

5.3 Experimentación

El desarrollo de la interfaz y uso de algoritmos esteganográficos, para este sistema de protección de derechos de autor, fue realizado con el lenguaje de programación de Python 3.7, ya que es el leguaje más adecuado para la aplicación de algoritmos esteganográficos, es decir es el más indicado para el manejo de matrices de datos y hacer operaciones con estos mismos, además que trabaja eficientemente con el tratamiento de imágenes.

Cabe destacar que los principales paquetes de Python que se contemplan para el desarrollo de este sistema son OpenCV y NumPy. La paquetería de OpenCV (Open Source Computer Vision Library) es una herramienta para el tratamiento de imágenes digitales, la cual ayuda a trabajar de manera más flexible al sistema sobre la imagen a proteger mediante su gran variedad de funciones como lo son visualizar la imagen, aplicar

transformadas a la imagen, entre otras. Por otra parte tenemos la paquetería de NumPy, la cual su principal función es trabajar sobre matrices n-dimensionales, es decir que esta herramienta que es capaz de procesar datos multidimensionales, como los son las matrices de pixeles que conforman a una imagen digital que a su vez los pixeles pueden ser interpretados como datos. Con el uso combinado de estas dos paqueterías que nos ofrece Python se puede sacar mayor provecho y con ello poder trabajar con ellas para el desarrollo de este sistema, además que su mayor ventaja es que estas están bajo licencia BSD (Berkeley Software Distribution), es decir que son bajo una licencia de software libre (OpenCV, 2019) (NumPy, 2019).

Desarrollo del sistema

Lo primero que se debe de tener en cuenta para el desarrollo del sistema son el tipo de formato de las imágenes con las que se va a trabajar, como se mencionó anteriormente, para este sistema los formatos más adecuados y que son los más utilizados en la actualidad por las plataformas web, es el formato JPG seguido después por el formato PNG. Anteriormente también se mencionó que las imágenes con los formatos que se contemplan utilizar en este sistema están dadas por una matriz de pixeles, y que cada píxel está constituido por tres canales denominados RGB, que dependiendo del valor de cada uno de ellos forman un solo color al combinarlos. Para trabajar con la esteganografía en el dominio de las transformadas es necesario que la imagen este en escala de grises, ya que cada píxel está conformado por un solo valor entre 0 y 255, donde 0 representa el color negro y el 255 el color blanco y dependiendo del valor asignado a cada pixel este representara su tonalidad. Lo cual representa un conflicto ya que al pasar la imagen de color a escala de grises se modifican sus valores RGB y solo queda un solo valor, y al querer invertir la modificación los valores RGB se pierden o se modifican exageradamente. Es por ello que para que este sistema haga uso de la técnica esteganográfica DCT con imágenes a color, se propone utilizar un solo canal RGB de la imagen, que para este caso se contempla utilizar el canal azul (blue), que con base al sistema visual humano es el que menos se hace perceptible para el ojo humano; para esto

se debe obtener la máscara que conforma el color azul de la imagen y para ello se hace lo siguiente:

```
imagen=cv2.imread('C:\\Users\\Noe Alejandro\\Pictures\\pruebas\\Imagenes\\1024x1024.jpg')
b, g, r = cv2.split(imagen)  #Dividir canales
img1 = b                     #Obtener canal azul de la imagen
```

Figura 16 Obtener canal azul de una imagen a color con OpenCV

Mediante las herramientas del paquete de OpenCV es posible extraer un canal (ya sea R, G o B) de una imagen a color, como se muestra en la Figura 16; en este caso se debe obtener el canal azul; lo primero es leer la imagen, después dividir los canales RGB y de esos canales extraer el canal azul y por ultimo convertir dicho canal a una variable que es la cual se va a manipular para ocultar la marca de agua, esta capa es obtenida en escala de grises; cumpliendo así el requerimiento principal para poder trabajar con las técnicas esteganográficas en el dominio de la transformada.

```
############################Se calcula DCT de cada bloque de 8x8 de la imagen############

B=8
h,w= img1.shape
vis0[:h, :w]=img1
blocksV=h/B                          #Cantidad de bloques de 8x8 en Vertical
blocksH=w/B                          #Cantidad de bloques de 8x8 en Horizontal
for row in range (blocksV):
    for col in range (blocksH):
        currentblock = cv2.dct(vis0[row*B:(row+1)*B, col*B:(col+1)*B])
        Trans[row*B:(row+1)*B, col*B:(col+1)*B]=currentblock
#########################################################################################
```

Figura 17 Dividir imagen en matrices de 8x8 pixeles y obtener DCT de cada una.

Después de extraer la capa azul, a esta se le divide en bloques de 8x8 pixeles y se le calcula la DCT de cada bloque, como se muestra en la Figura 17; donde se puede observar que para crear los bloques se puede hacer mediante los ciclos *for* y la herramienta de OpenCV para calcular la DCT de cada bloque al mismo tiempo. Los resultados obtenidos son

conocidos como coeficientes, estos se clasifican de coeficiente de alta frecuencia a coeficientes de baja frecuencia, para fines del desarrollo de este sistema se tiene en cuenta reemplazar los coeficientes de media frecuencia para la inserción de la marca de agua, ya que las modificaciones en la zona de coeficientes de media frecuencia son casi imperceptibles para el ojo humano; la selección de estos coeficientes se hace por medio del escaneo zigzag, como se muestra en la Figura 7.

```
datoszigzag=[datosg[0],datosg[1],datosg[8],datosg[16],datosg[9],datosg[2],datosg[3],datosg[10],
             datosg[17],datosg[24],datosg[32],datosg[25],datosg[18],datosg[11],datosg[4],datosg[5],
             datosg[12],datosg[19],datosg[26],datosg[33],datosg[40],datosg[48],datosg[41],datosg[34],
             datosg[27],datosg[20],datosg[13],datosg[6],datosg[7],datosg[14],datosg[21],datosg[28],
             datosg[35],datosg[42],datosg[49],datosg[56],datosg[57],datosg[50],datosg[43],datosg[36],
             datosg[29],datosg[22],datosg[15],datosg[23],datosg[30],datosg[37],datosg[44],datosg[51],
             datosg[58],datosg[59],datosg[52],datosg[45],datosg[38],datosg[31],datosg[39],datosg[46],
             datosg[53],datosg[60],datosg[61],datosg[54],datosg[47],datosg[55],datosg[62],datosg[63]]
```

Figura 18 Escaneo Zigzag del bloque de 8x8

En la Figura 18 se muestra el reordenamiento de los coeficientes en zigzag de los bloques de 8x8, por medio del escaneo en zigzag se identifican los coeficientes de media frecuencia.

```
datoszigzag2=[datosg22[0],datosg22[1],datosg22[8],datosg22[16],datosg22[9],datosg22[2],datosg22[3],
              datosg22[10],datosg22[17],datosg22[24],datosg22[32],datosg22[25],datosg22[18],datosg22[11],
              datosg22[4],datosg22[5],datosg22[12],datosg22[19],datosg22[26],datosg22[33],datosg22[40],
              datosg22[48],datosg22[41],datosg22[34],datosg22[27],datosg22[20],datosg22[13],datosg22[6],
              datos22[0],datos22[1],datos22[2],datos22[3],datos22[4],datos22[5],datos22[6],datos22[7],
              datosg22[57],datosg22[50],datosg22[43],datosg22[36],datosg22[29],datosg22[22],datosg22[15],
              datosg22[23],datosg22[30],datosg22[37],datosg22[44],datosg22[51],datosg22[58],datosg22[59],
              datosg22[52],datosg22[45],datosg22[38],datosg22[31],datosg22[39],datosg22[46],datosg22[53],
              datosg22[60],datosg22[61],datosg22[54],datosg22[47],datosg22[55],datosg22[62],datosg22[63]]
```

Figura 19 Escaneo Zigzag del bloque de 8x8 con los coeficientes remplazados por los datos de la Marca de Agua.

Al identificar los valores de los coeficientes de media frecuencia, estos se remplazan por los valores de los datos de la marca de agua, como se muestra en la Figura 19, donde se toman 8 datos de la marca de agua y los inserta dentro de los datos de los coeficientes de

media frecuencia. Y después se vuelve a reordenar los coeficientes de tal manera de que queden en su orden original, como se muestra en la Figura 20.

```
matriznueva=[datoszigzag2[0],datoszigzag2[1],datoszigzag2[5],datoszigzag2[6],datoszigzag2[14],datoszigzag2[15],
             datoszigzag2[27],datoszigzag2[28],datoszigzag2[2],datoszigzag2[4],datoszigzag2[7],datoszigzag2[13],
             datoszigzag2[16],datoszigzag2[26],datoszigzag2[29],datoszigzag2[42],datoszigzag2[3],datoszigzag2[8],
             datoszigzag2[12],datoszigzag2[17],datoszigzag2[25],datoszigzag2[30],datoszigzag2[41],datoszigzag2[43],
             datoszigzag2[9],datoszigzag2[11],datoszigzag2[18],datoszigzag2[24],datoszigzag2[31],datoszigzag2[40],
             datoszigzag2[44],datoszigzag2[53],datoszigzag2[10],datoszigzag2[19],datoszigzag2[23],datoszigzag2[32],
             datoszigzag2[39],datoszigzag2[45],datoszigzag2[52],datoszigzag2[54],datoszigzag2[20],datoszigzag2[22],
             datoszigzag2[33],datoszigzag2[38],datoszigzag2[46],datoszigzag2[51],datoszigzag2[55],datoszigzag2[60],
             datoszigzag2[21],datoszigzag2[34],datoszigzag2[37],datoszigzag2[47],datoszigzag2[50],datoszigzag2[56],
             datoszigzag2[59],datoszigzag2[61],datoszigzag2[35],datoszigzag2[36],datoszigzag2[48],datosg[49],
             datoszigzag2[57],datoszigzag2[58],datoszigzag2[62],datoszigzag2[63]]
```

Figura 20 Matriz con los coeficientes con el orden original.

```
########################################IDCT#####################################
back02=np.zeros((h,w), np.float32)

for row in range (blocksV):
    for col in range (blocksH):
        currentblock = cv2.idct(Transdct3[row*B:(row+1)*B,col*B:(col+1)*B])
        back02[row*B:(row+1)*B,col*B:(col+1)*B]=currentblock
#################################################################################
```

Figura 21 Obtener IDCT de la matriz DCT con los datos ocultos.

Y para obtener la matriz IDCT que conformara como resultado final para la capa azul de la imagen original, con los datos de la marca de agua oculta, se hace el procedimiento de la Figura 21, donde se puede ver que es algo similar al cálculo de la DCT pero con la diferencia que en este caso se está calculando la inversa de la transformada discreta del coseno para cada bloque de 8x8.

6 RESULTADOS Y DISCUSIÓN

Interfaz del Sistema

Para la interacción de este sistema con el usuario y viceversa, se hizo uso de una interfaz GUI (Interfaz Gráfica de Usuario, o por sus siglas en inglés Graphical User Interface), es decir, es una interfaz que utiliza elementos gráficos, que en este caso se hizo uso de botones para poder llevar acabo la función del sistema, el cual se visualiza de la siguiente manera:

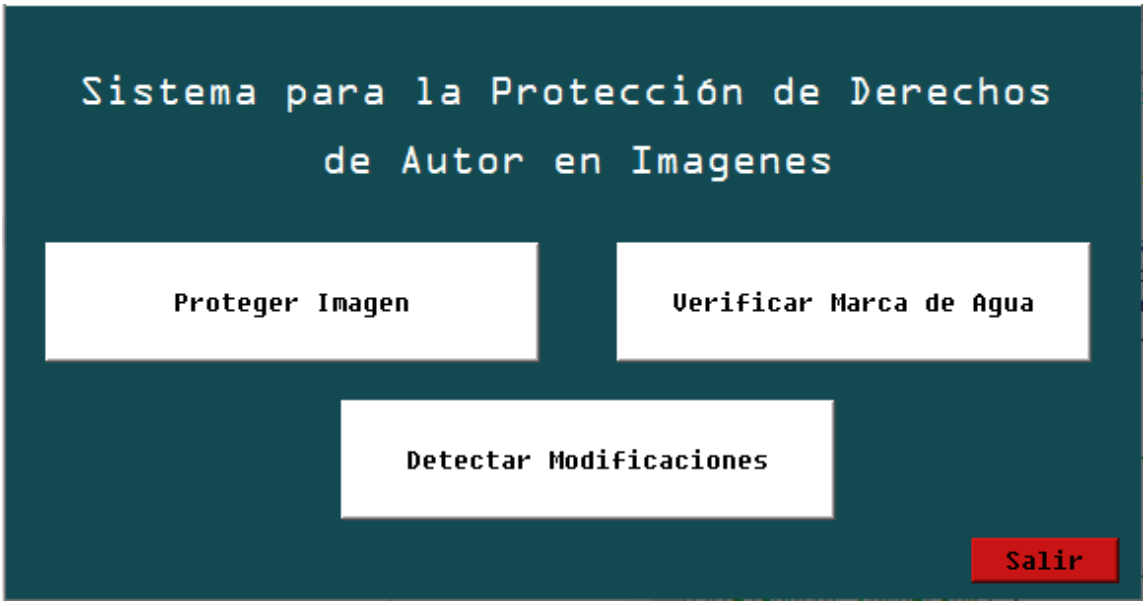

Figura 22 Ventana Principal del Sistema.

La primer ventana o ventana principal (Figura 22) muestra tres botones donde el usuario puede elegir la acción que desea realizar, la primer opción es dar clic al botón “proteger imagen”, donde se abrirá otra ventana la cual se muestra en la Figura 23 , la función de este es aplicar la esteganografía para ocultar la marca de agua dentro de la imagen a proteger; la segunda opción es dar clic al botón “verificar marca de agua”, donde se abrirá otra ventana la cual se muestra en la Figura 36, el cual tiene la función de ayudar al autor a verificar su marca de agua que le halla insertado a su imagen y así proteger la integridad

de sus derechos de autor sobre dicha imagen; el tercer botón abre una tercer ventana, como se muestra en la Figura 46, que le permite al autor calcular la diferencia entre su imagen protegida y aparentemente la misma imagen pero con indicios de modificación; y por último el cuarto botón de “Salir” el cual nos permite salir del sistema. Este último aplica para todas las ventanas del sistema.

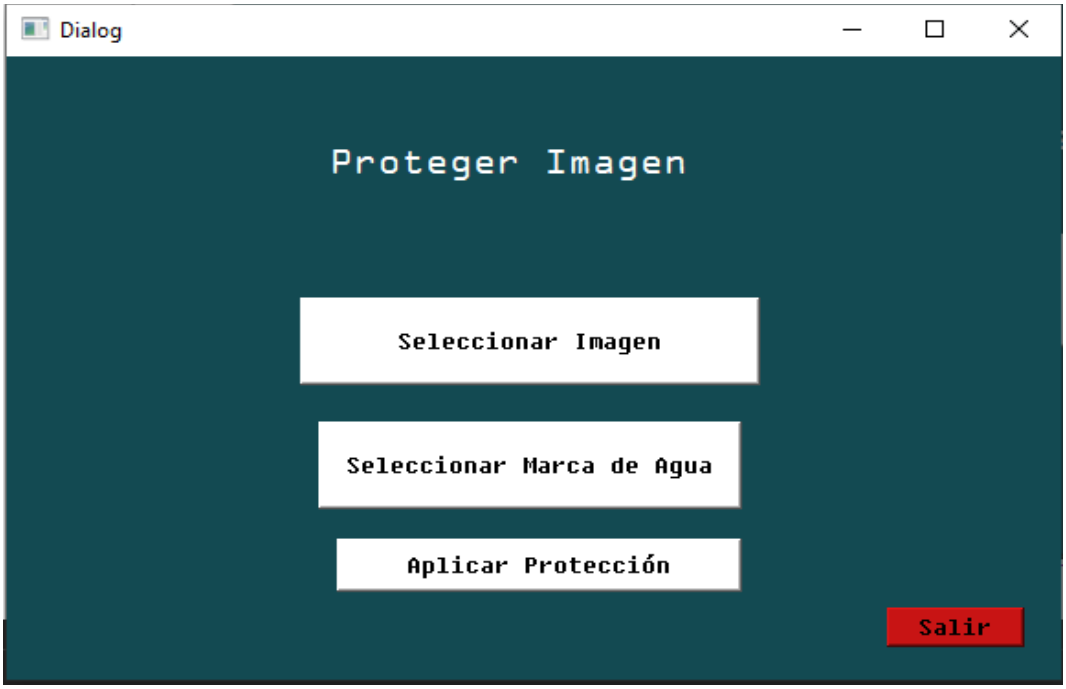

Figura 23 Ventana “Proteger Imagen”.

En la ventana de la Figura 23 , que nos aparece después de dar clic sobre el botón de “Proteger Imagen” en la ventana principal, la cual está conformada por cuatro botones los cuales cada uno cumple una función diferente, para el botón “Seleccionar Imagen a Proteger” su trabajo es desplegar otra ventana, como se muestra en la Figura 24 , donde el usuario tiene que seleccionar su imagen a proteger; para el botón “Seleccionar Marca de Agua” también se despliega otra ventana, como se muestra en la Figura 25, para que el usuario seleccione la imagen que utilizará como marca de agua para comprobar su autenticidad; para el botón “Aplicar Protección” pone en marcha el algoritmo

esteganográfico, en donde la marca de agua queda oculta dentro de la imagen; y por ultimo está el botón “Salir”, que al darle clic el sistema se cierra en automático.

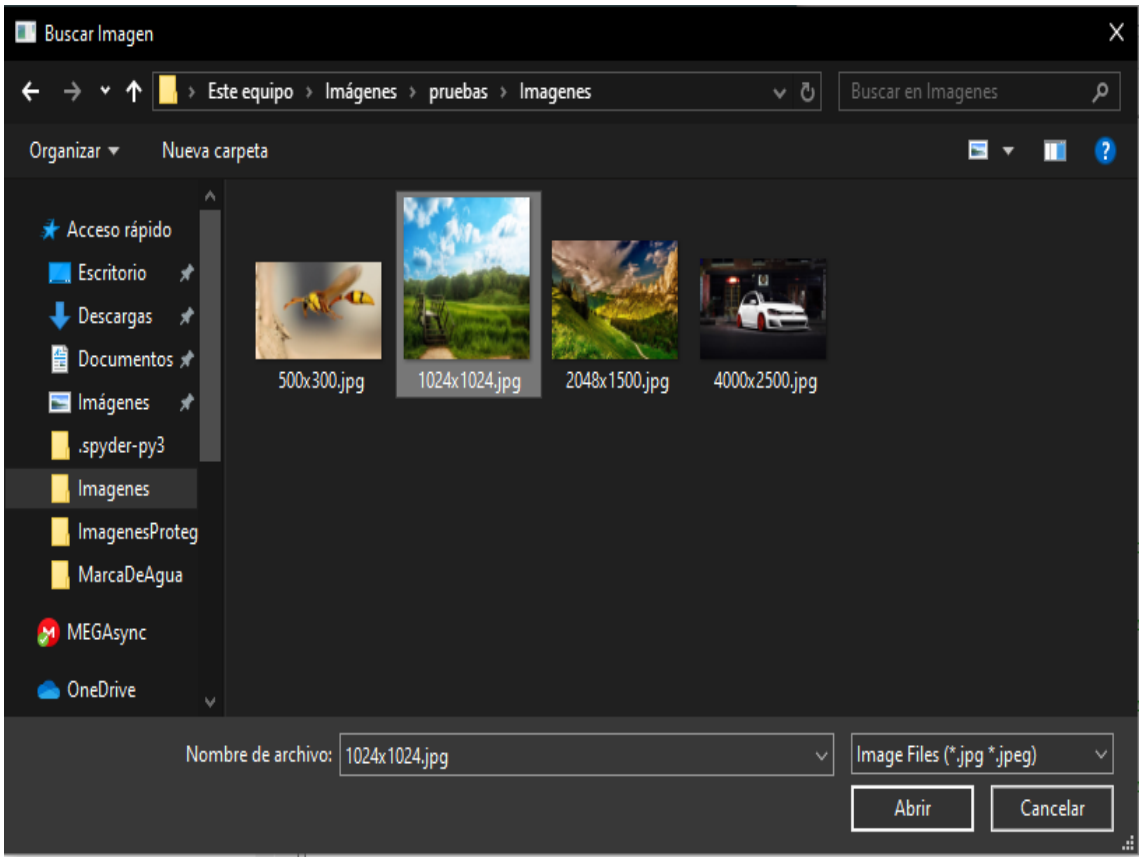

Figura 24 Ventana “Selecciona Imagen a Proteger”.

Para la protección de la imagen mediante la marca de agua el sistema trabaja de la siguiente manera:

- Se obtiene la capa azul del sistema RGB de cada pixel de la imagen a proteger y después este se convierte a escala de grises, como se muestra en la Figura 26.

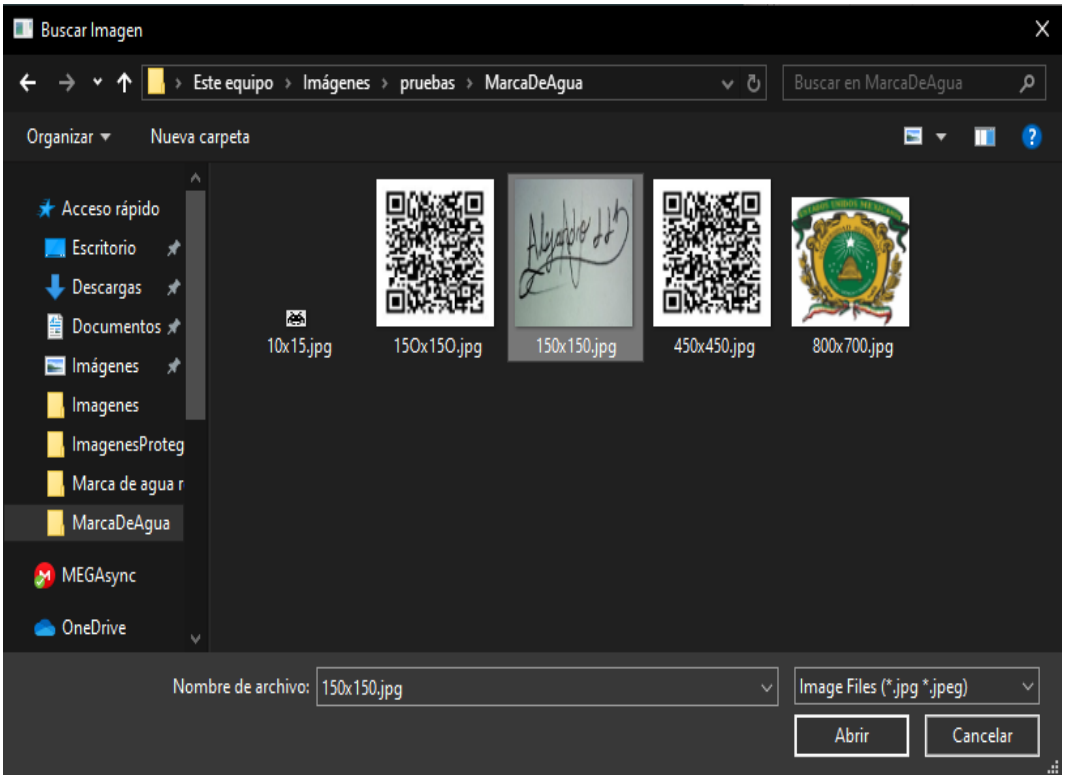

Figura 25 Ventana “Selecciona Marca de Agua”.

Figura 26 Capa Azul de la Imagen a Proteger.

- Después a esta imagen se le divide en bloques de 8x8 pixeles, en donde a cada bloque se le aplicara la Transformada Discreta del Coseno, como se muestra en la Figura 27.

Figura 27 División de la Imagen en Bloques de 8x8 y Aplicación de la DCT a cada Bloque.

- A la marca de agua se le aplicara un filtro donde quedará en escala de blanco y negro, como se muestra en la Figura 28, para insertarla y ocultarla dentro de la imagen.

Figura 28 Marca de Agua a Ocultar

- Esteganografía

Aquí es donde los coeficientes de media frecuencia de la transformada discreta del coseno, que se calcula de cada bloque 8x8, se remplazan por los datos de la marca de agua, para esto se leen los coeficientes y los datos de la marca de agua, como se muestran en la Figura 29 y la Figura 30.

```
Coeficientes DCT
[[ 2.0371249e+03 -2.7072148e+00 -1.8361522e+00 ...  5.7004509e+00
   2.3553839e+01  4.3396610e+01]
 [-2.8590178e-01 -5.1293242e-01  3.9991179e-01 ... -1.3781634e+01
  -2.1106384e+01 -2.0844803e+01]
 [ 3.9424813e-01 -1.9204450e-01  2.1338829e-01 ... -2.8304560e+01
   3.2966064e+01  7.8851776e+00]
 ...
 [ 1.4038136e+01  1.2648014e+01 -2.6942104e+01 ... -2.1132170e-01
   6.4936437e-02 -2.7234334e-01]
 [-3.8365784e+00 -6.8023186e+00 -2.6670494e+01 ...  5.8417477e-02
   3.2062143e-01 -4.2218536e-02]
 [-9.4591751e+00 -1.0144882e+01 -2.1721842e+01 ... -3.9481401e-01
   2.1016893e-01  3.7097910e-01]]
(48, 56)
```

Figura 29 Valores de los Coeficientes DCT de la Imagen a Proteger.

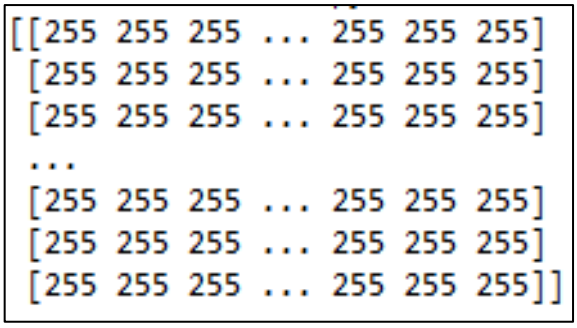

Figura 30 Fragmentos de Datos de la Marca de Agua a Ocultar.

Posteriormente, se remplazan los coeficientes de media frecuencia por los datos de la marca de agua, como se muestra en la Figura 31.

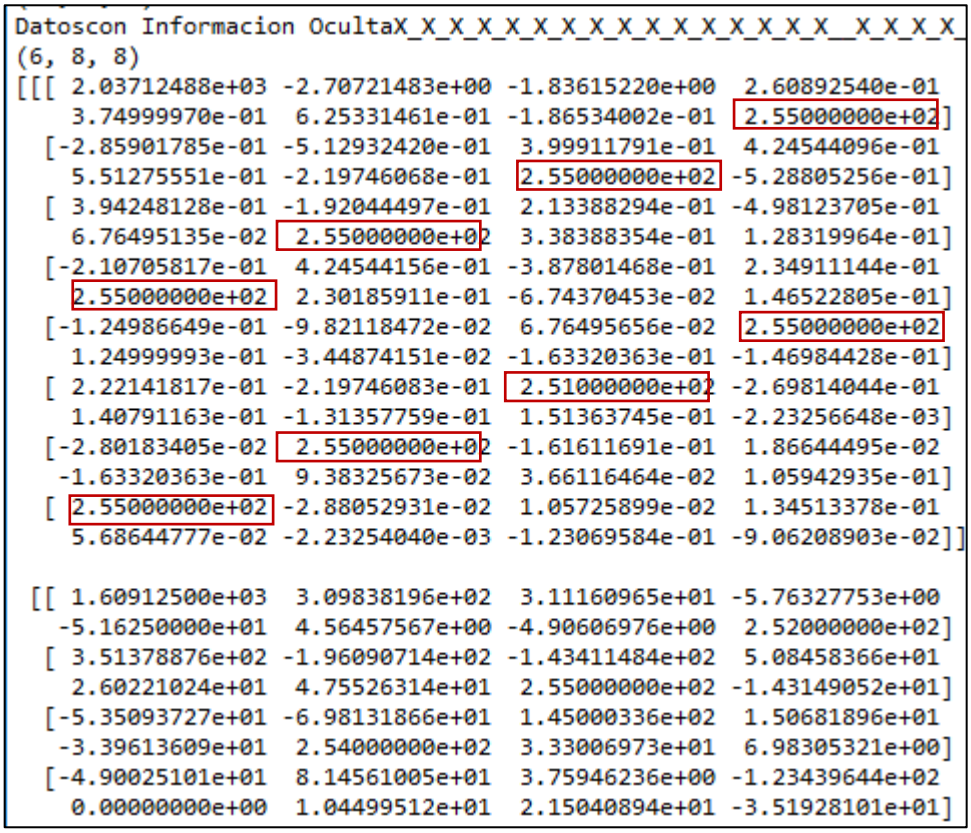

Figura 31 Valores de los Coeficientes de la Imagen a Proteger

con los Datos de la Marca de Agua Ocultos.

- Luego de insertar la marca de agua dentro de la imagen, se aplica la Inversa de la Transformada Discreta del Coseno para obtener la nueva capa azul de la imagen, la cual remplazara a la capa azul de la imagen original. Y como resultado se obtendrá la nueva imagen, o mejor dicho la estego-imagen, con la marca oculta (Figura 32).

Figura 32 Estego-imagen obtenida.

Con la imagen obtenida se hace una comparativa con la imagen original, con el fin de encontrar matemáticamente las diferencias entre ellas, como se muestra en la Figura 33.

```
Diferencia Maxima:    255
Diferencia Minima:     0
Diferencia Absoluta:  368.9027853012085
```

Figura 33 Cálculo de las Diferencias entre la Imagen Original y la Estego-imagen.

Y por último se abre una ventana donde el usuario elige la ruta o ubicación donde se guardará la estego-imagen, como se muestra en la Figura 34.

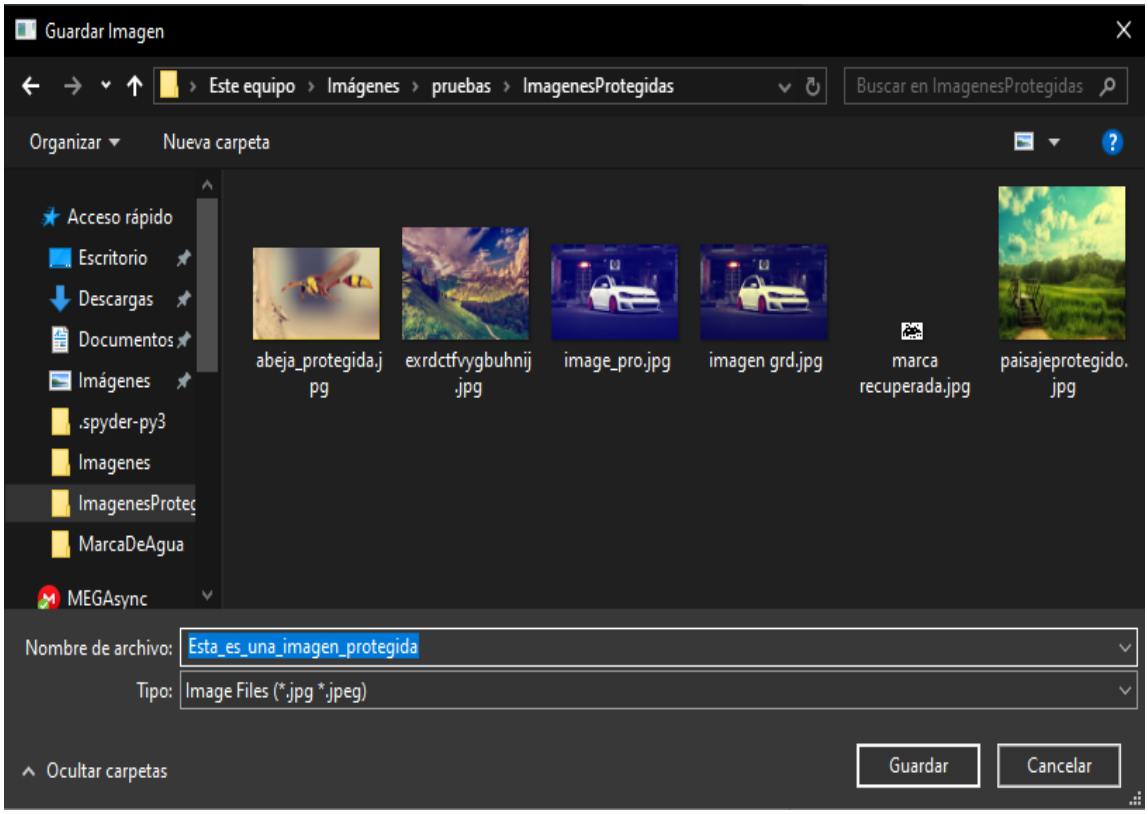

Figura 34 Ventana guardar estego-imagen.

Y para concluir se puede verificar que la imagen se haya guardado entrando a la ubicación donde se indicó que se guardará, como se muestra en la Figura 35.

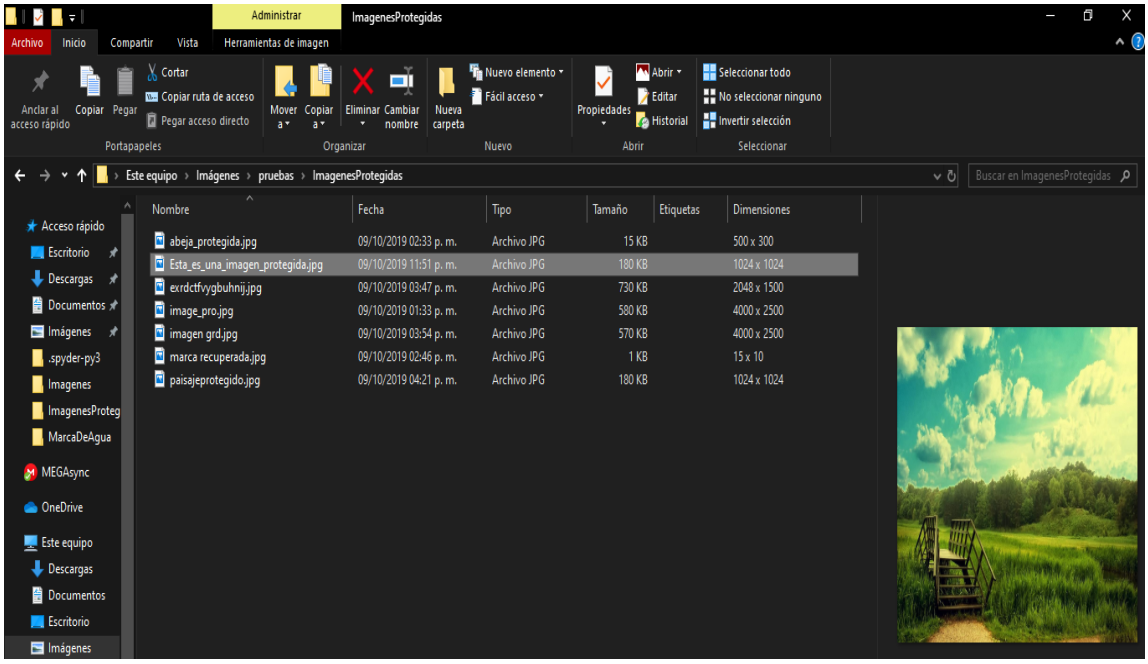

Figura 35 Verificar estego-imagen guardada.

La interfaz que se abre al dar clic en el botón “Verificar Marca de Agua” en la ventana principal se muestra en la Figura 36, en donde muestra tres botones que permiten al usuario verificar la marca de agua que esta oculta dentro la imagen.

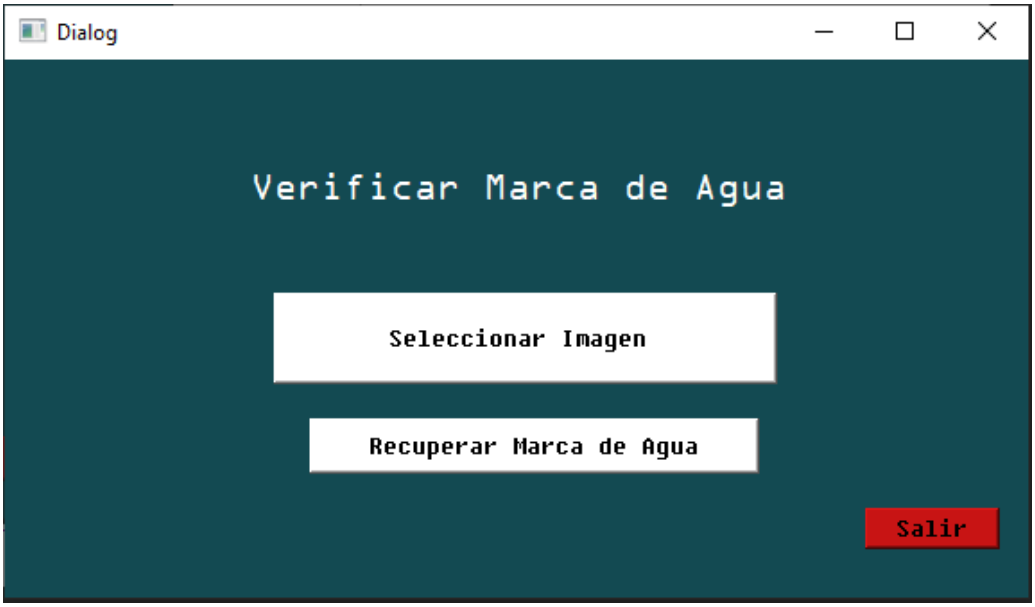

Figura 36 Ventana “Verificar Marca de Agua”.

Al dar clic en el botón “Seleccionar Imagen” se abre una ventana donde se indica que imagen es la que se quiere extraer la marca de agua, como se muestra en la Figura 37.

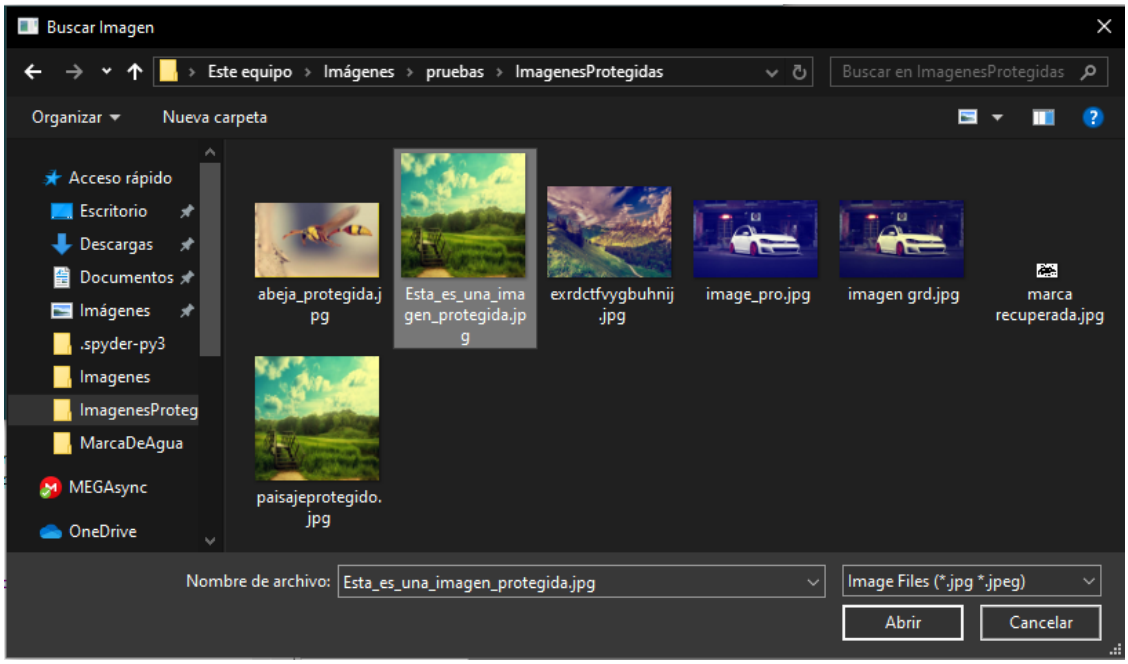

Figura 37 Ventana para seleccionar la estego-imagen.

Al darle clic al botón “Recuperar marca de Agua” el sistema empezará a hacer en estegoanálisis, pero para ello es necesario conocer las dimensiones de la imagen y marca de agua originales, por si la estego-imagen se haya redimensionado por alguna razón; para obtener esta información el sistema le pide al usuario que inserte las dimensiones de estas, como se muestra en las siguientes figuras.

Para obtener las dimensiones de la imagen son las ventanas de las Figuras 38 y 39.

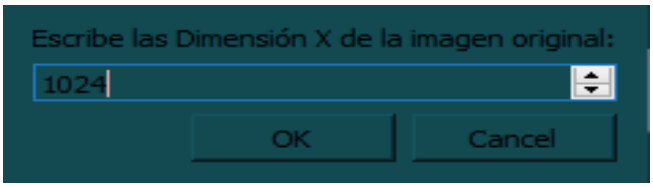

Figura 38 Obtención del valor de la dimensión horizontal de la estego-imagen.

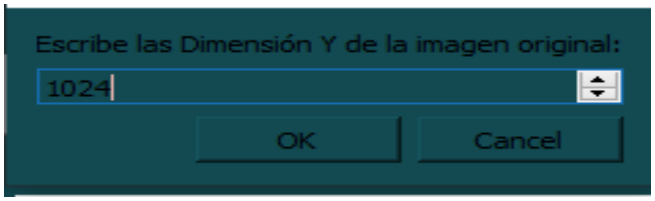

Figura 39 Obtención del valor de la dimensión vertical de la estego-imagen.

Para obtener las dimensiones (en pixeles) de la marca de agua son las ventanas de las Figuras 40 y 41.

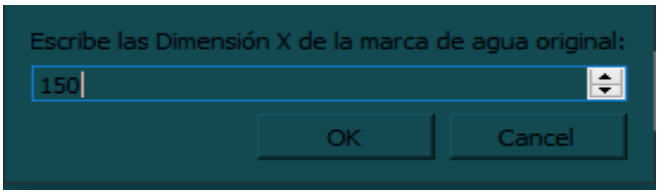

Figura 40 Obtención del valor de la dimensión horizontal de la marca de agua.

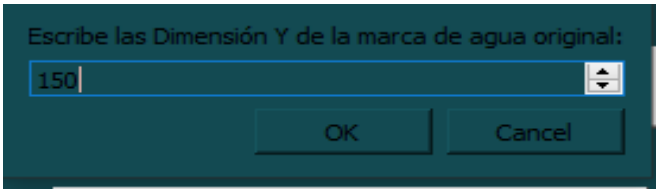

Figura 41 Obtención del valor de la dimensión vertical de la marca de agua.

Después de ingresar las dimensiones de la imagen original y marca de agua, el sistema recupera la marca de agua oculta, como se muestra en la Figura 42, pero al usuario se le muestra la misma marca de agua, pero en B/N para una mejor visualización, como la que se muestra en la Figura 43.

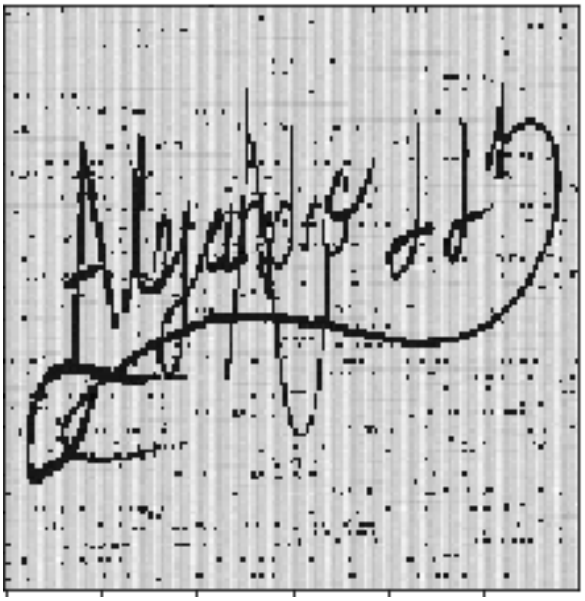

Figura 42 Marca de agua obtenida de la estego-imagen.

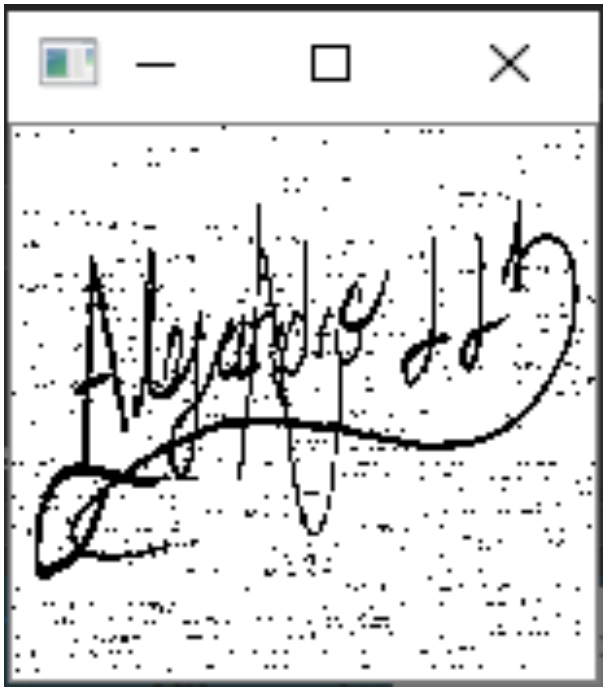

Figura 43 Marca de Agua obtenida en B/N.

Esta última será la que se guardará, ya que, al mostrar la marca de agua recuperada, esta solicitará al usuario una ubicación donde se guardará dicha marca mediante una ventana como se muestra en la Figura 44.

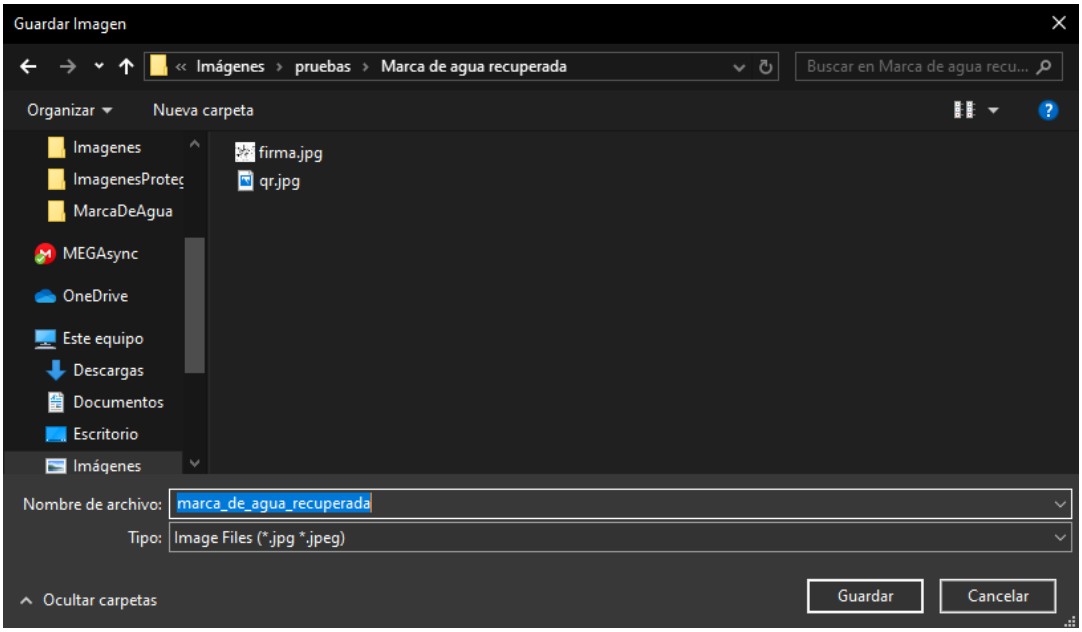

Figura 44 Ventana para guardar marca de agua recuperada.

Y para verificar que esta se haya guardado se puede ingresar a la dirección donde se indicó en el sistema que se guardaría, como se muestra en la Figura 45.

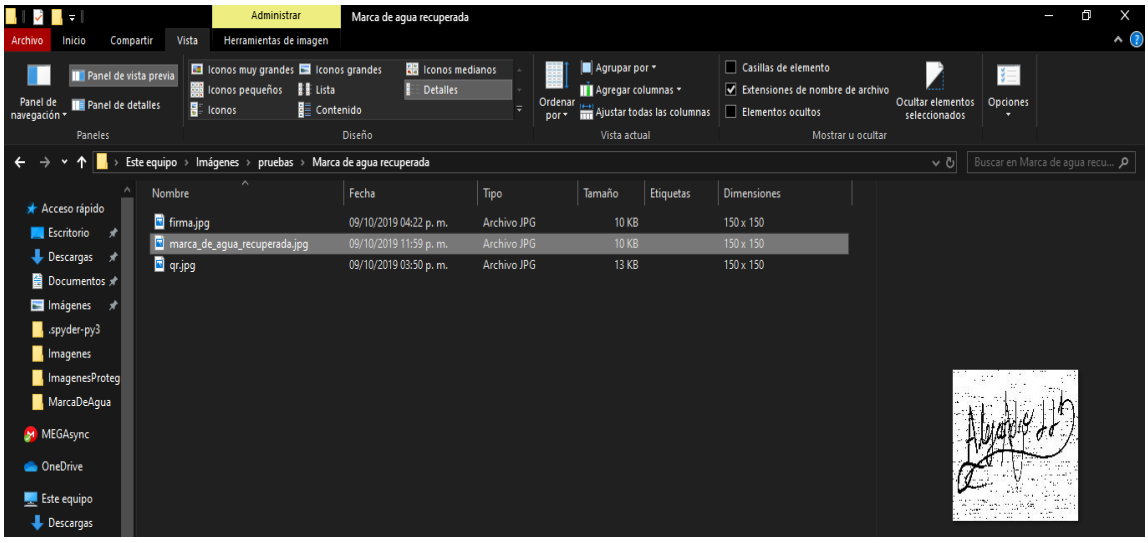

Figura 45 Verificar marca de agua guardada.

En la ventana principal, al darle clic al botón “Detectar Modificaciones” se abre la siguiente ventana que se muestra en la Figura 46.

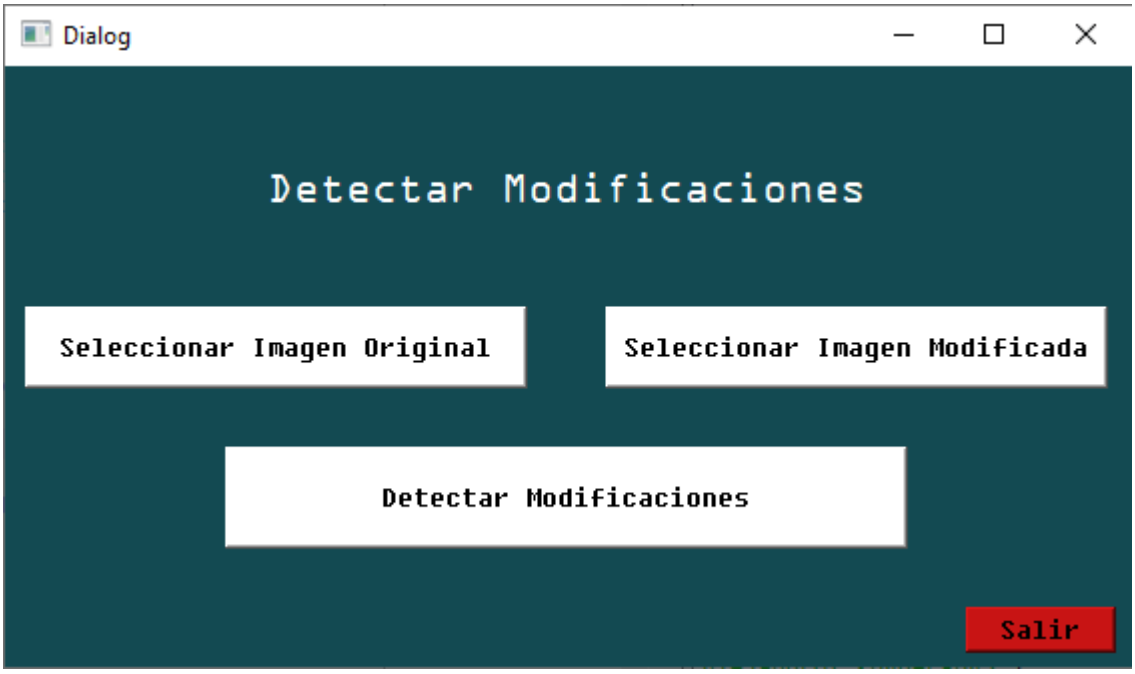

Figura 46 Ventana “Detectar Modificaciones”.

En esta ventana se muestran tres botones, el botón “Seleccionar Imagen Original”, que al darle clic permite al usuario seleccionar la imagen que el considere como su obra original mediante una ventana que se muestra en la Figura 47, el botón llamado “Seleccionar Imagen Modificada”, que también permite seleccionar la imagen que el usuario considere que tiene indicios de modificaciones como se muestra en la Figura 48, y por último, el botón “Detectar Modificaciones”, que permite al usuario calcular la diferencia absoluta que hay entre las dos imágenes seleccionadas, este cálculo se hace comparando pixel a pixel de cada una de las imágenes, y permite detectar si hay alguna alteración que se haya sufrido, ya sea mediante herramientas esteganográficas o simples alteraciones de color. Cabe resaltar que las imágenes a comparar deben ser de las mismas dimensiones, ya que si no lo son quiere decir que la imagen ya ha sido alterada en su tamaño.

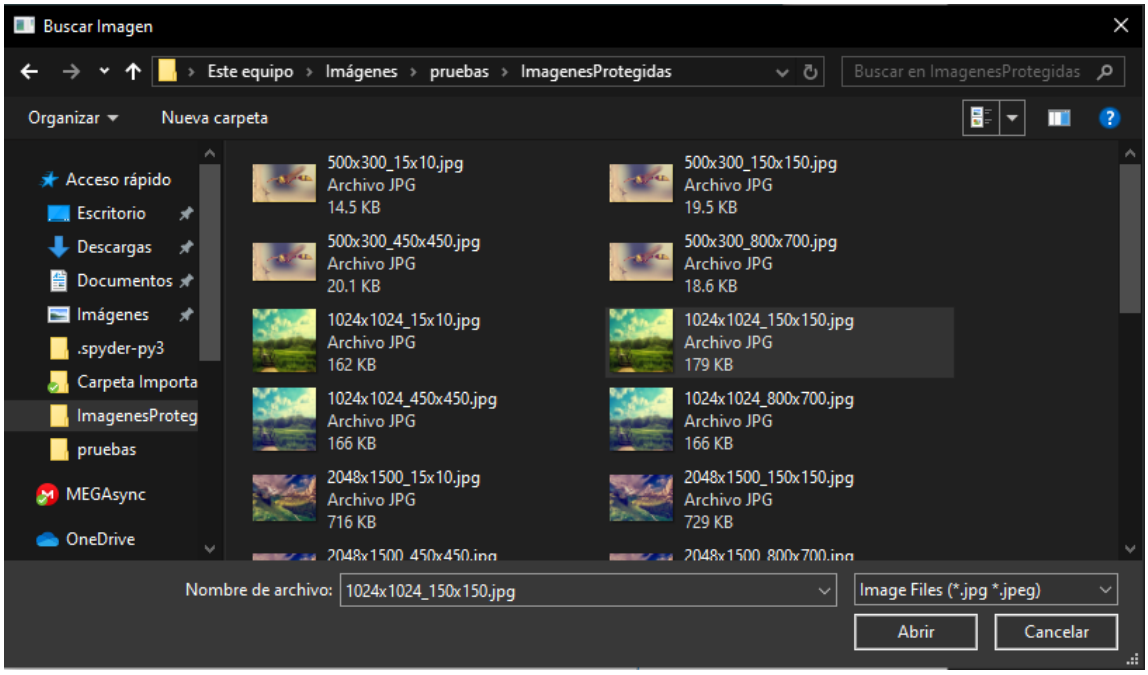

Figura 47 Ventana para seleccionar la imagen original protegida.

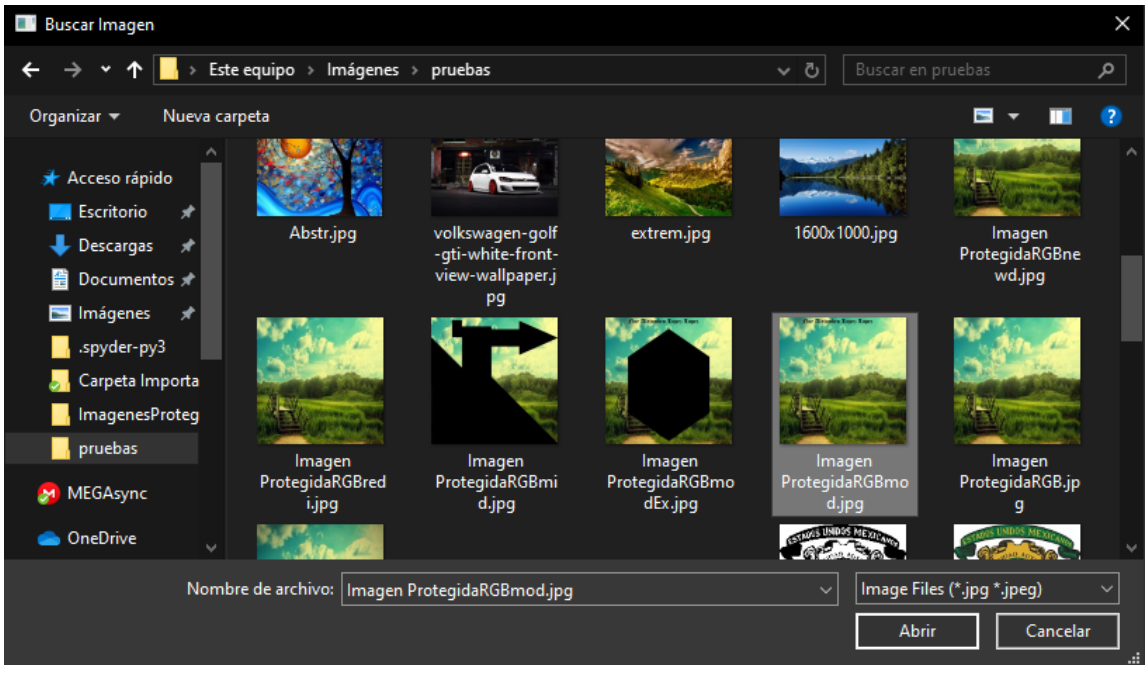

Figura 48 Ventana para seleccionar la imagen modificada.

Cuando el sistema empieza a detectar las modificaciones muestra las imágenes seleccionadas y por ultimo las modificaciones detectadas, como se muestra en las siguientes Figuras.

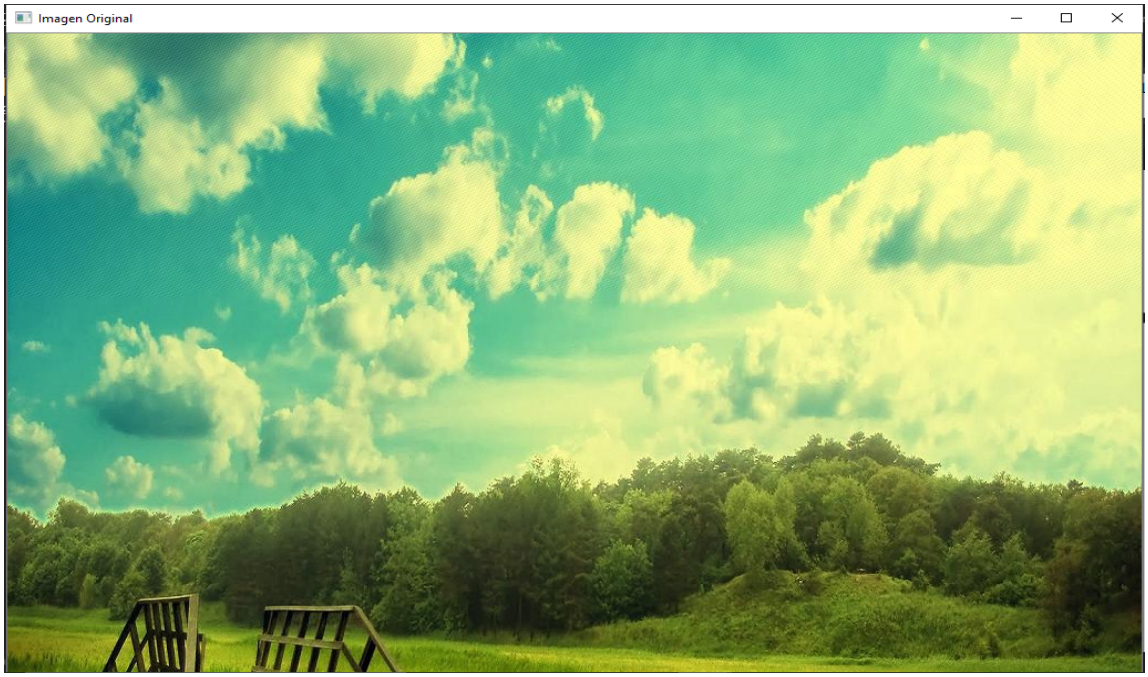

Figura 49 Visualización de la imagen original.

Figura 50 Visualización de la imagen modificada.

En la Figura 51 se visualiza las modificaciones encontradas y en la ventana de “Detectar Modificaciones” se muestra el cálculo de la diferencia absoluta entre las imágenes seleccionadas, como se muestra en la Figura 52.

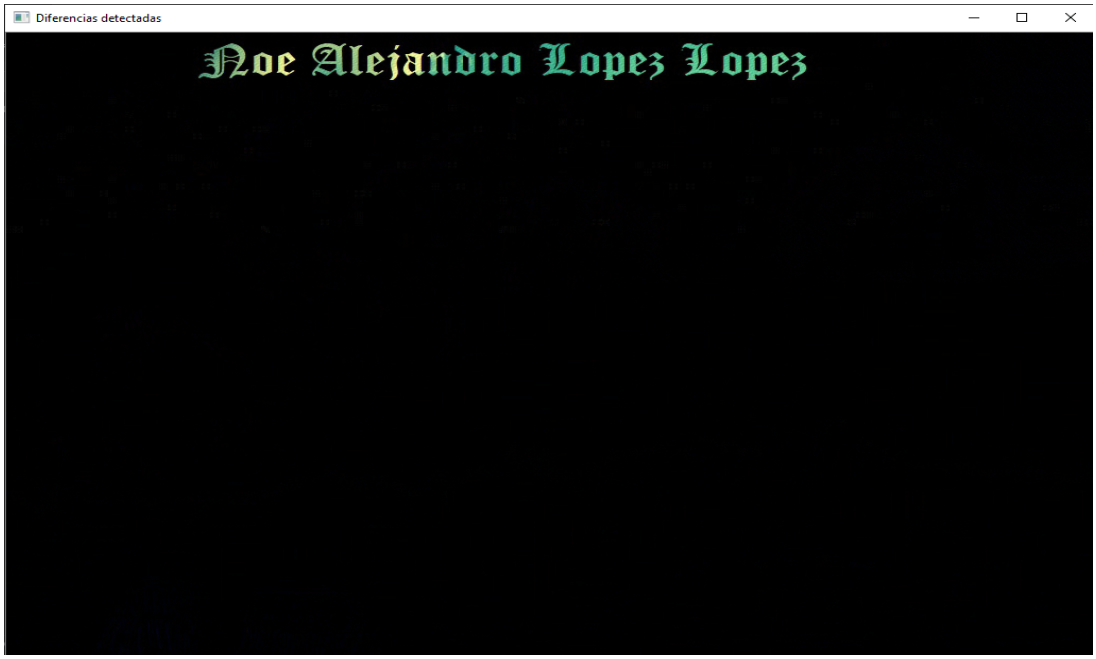

Figura 51 Visualización de las diferencias encontradas entre la imagen original y la modificada.

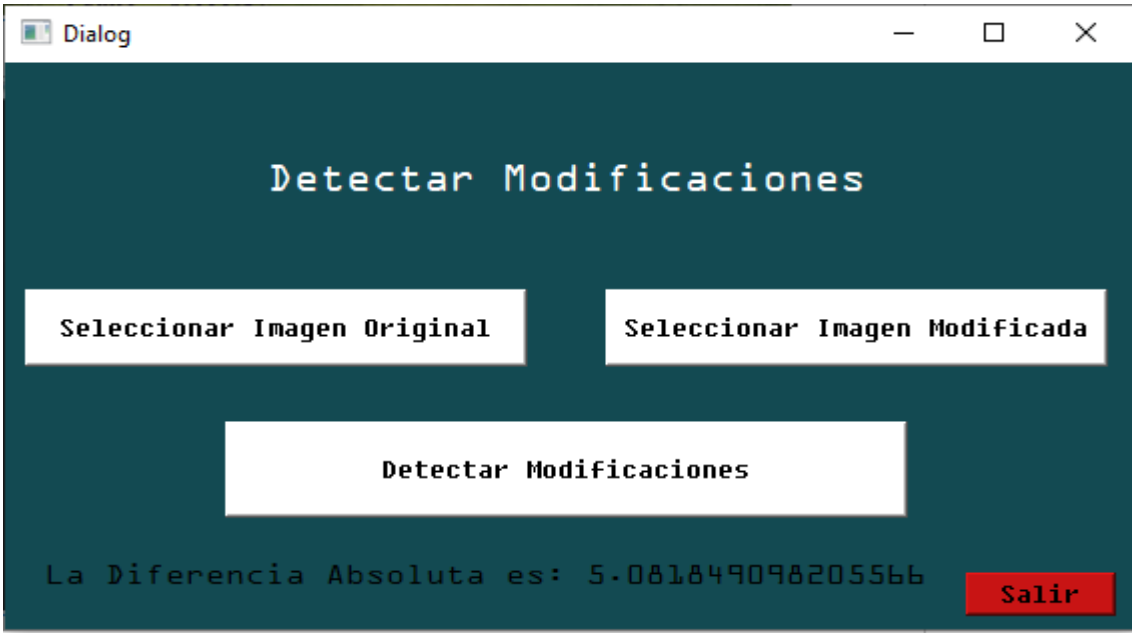

Figura 52 Diferencia Absoluta calculada.

Cuando el sistema detecta que las dimensiones son diferentes muestras un mensaje en la ventana, como se muestra en la Figura 53, y cuando detecta que en las imágenes no hay alteraciones el sistema también manda un mensaje de que no hay diferencia, como se muestra en a Figura 54.

Figura 53 Las dimensiones de las imágenes a comparar no son iguales.

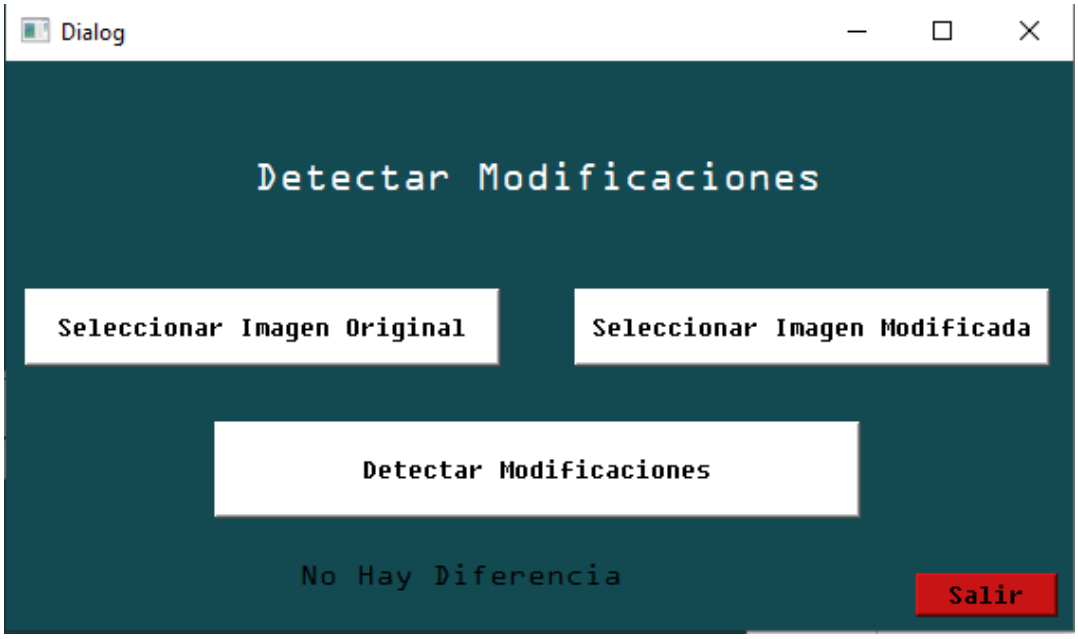

Figura 54 No se encuentra diferencia entre las imágenes seleccionadas.

La diferencia entre la imagen original y la estego-imagen obtenida por el uso del sistema se puede medir, comparando a estas, pixel por pixel y obtener una diferencia absoluta, esta nos sirve para encontrar cual dimensiones de imagen y marca de agua son las que afectan menos y cuales más. Para llevar a cabo estas pruebas se hará con las siguientes imágenes y marcas de agua que se muestran a continuación:

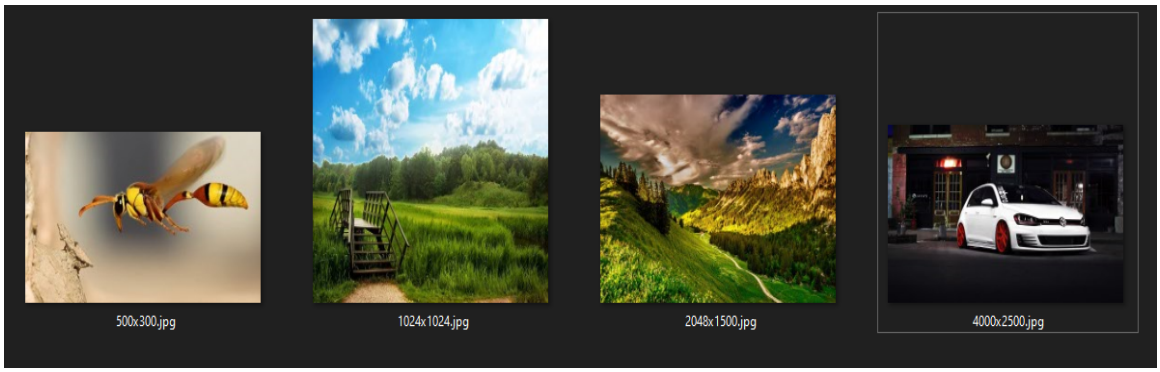

Figura 55 Imágenes Digitales a Proteger.

Figura 56 Marcas de Agua a Ocultar.

Cabe resaltar que las dimensiones de cada imagen y marca de agua son las mismas que se muestran en el nombre dado a cada una de ellas. Las diferencias absolutas que se obtuvieron al comparar las imágenes originales con las diferentes estego-imágenes resultantes al insertar las diferentes marcas de agua, se muestran en la Tabla 2.

Tabla 2 Diferencia Absoluta entre imagen original y estego-imagen.

Imagen Digital	Marca de Agua Oculta	Diferencia Absoluta entre la imagen original y la estego-imagen.
500x300.jpg	10x15.jpg	6.164111
500x300.jpg	150x150.jpg	9.226991
500x300.jpg	450x450.jpg	9.356275
500x300.jpg	800x700.jpg	9.038508
1024x1024.jpg	10x15.jpg	17.523016
1024x1024.jpg	150x150.jpg	19.118513
1024x1024.jpg	450x450.jpg	22.284642
1024x1024.jpg	800x700.jpg	22.273729
2048x1500.jpg	10x15.jpg	18.020137
2048x1500.jpg	150x150.jpg	24.222263
2048x1500.jpg	450x450.jpg	23.406362
2048x1500.jpg	800x700.jpg	23.124230
4000x2500.jpg	10x15.jpg	24.439531
4000x2500.jpg	150x150.jpg	25.572163
4000x2500.jpg	450x450.jpg	20.014317
4000x2500.jpg	800x700.jpg	20.945133

De acuerdo con los datos obtenidos de la diferencia absoluta, que se muestran en la Tabla 2, se pueden graficar los datos de cada imagen con las diferentes dimensiones de las marcas de agua, como se muestra a continuación en las siguientes figuras. Donde en la Figura 57 se muestra gráficamente los valores de las diferencias absolutas que el sistema calcula entre la imagen original, con dimensiones 500x300, y las diferentes estego-imágenes resultantes de la ocultación de las diferentes marcas de agua; de igual manera en la Figura 58 se tiene una gráfica, pero en este caso se muestra las diferencias absolutas que hay entre la imagen con dimensiones de 1024x1024 pixeles y sus respectivas estego-imágenes con diferentes marcas de agua ocultas dentro de ella; así mismo en la Figura 59, para la imagen con dimensiones de 2048x1500, y la Figura 60, para la imagen con una resolución de 4000x2500 pixeles.

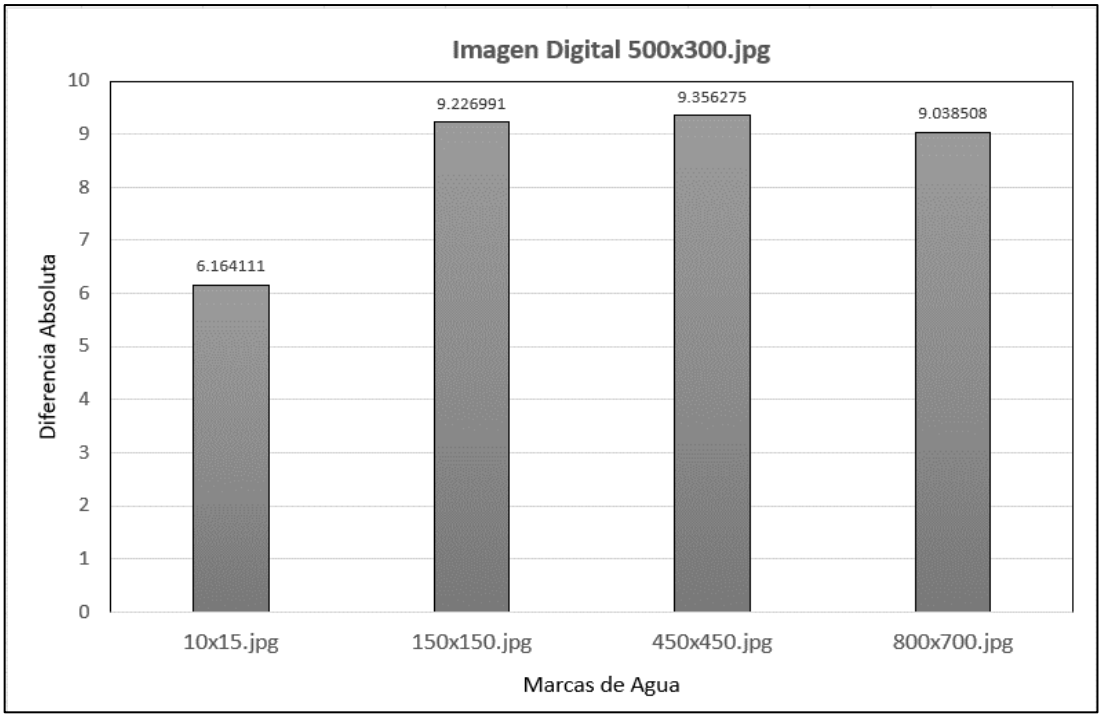

Figura 57 Grafica de diferencias absolutas de la imagen 500x300.jpg con las diferentes marcas de agua.

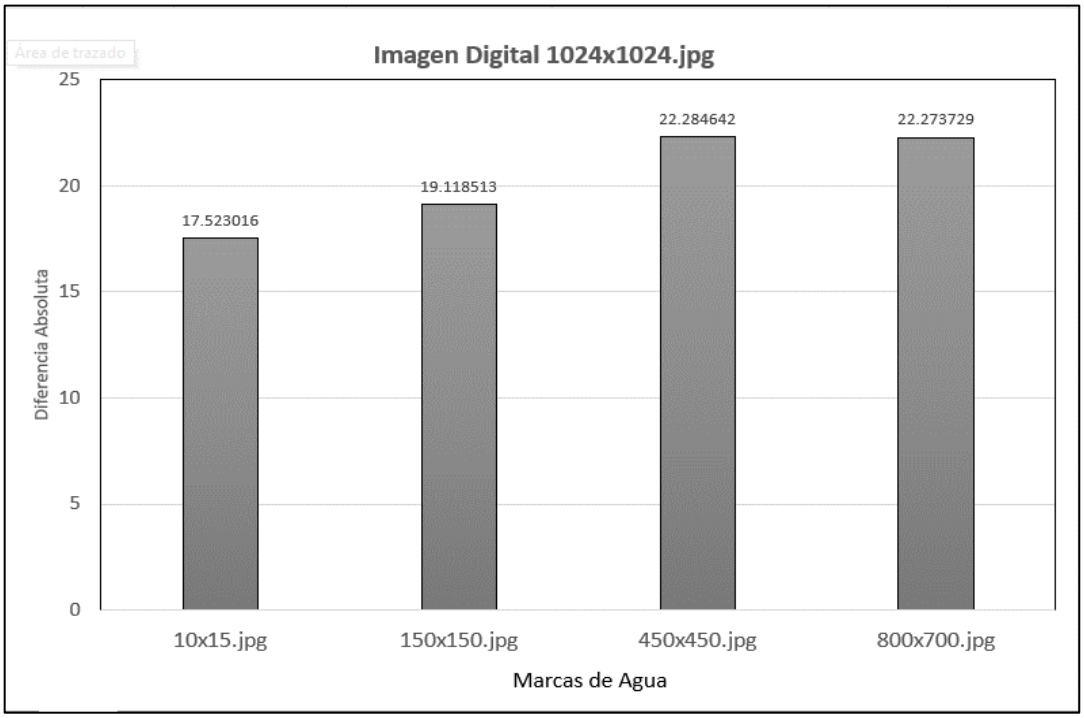

Figura 58 Grafica de diferencias absolutas de la imagen 1024x1024.jpg con las diferentes marcas de agua.

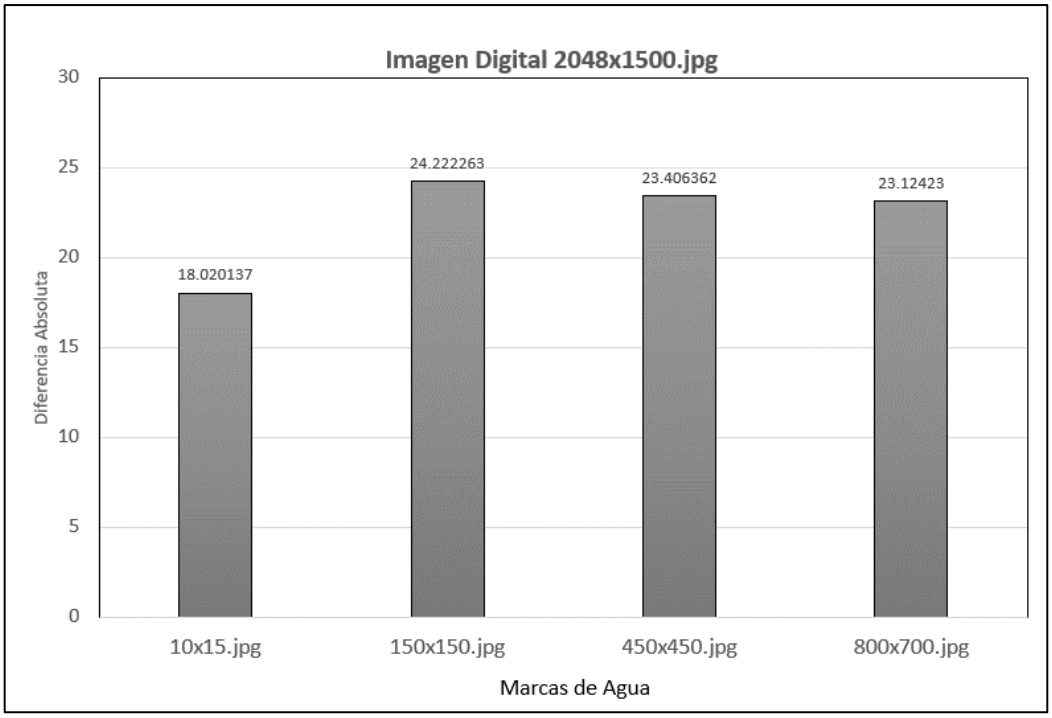

Figura 59 Grafica de diferencias absolutas de la imagen 2048x1500.jpg con las diferentes marcas de agua.

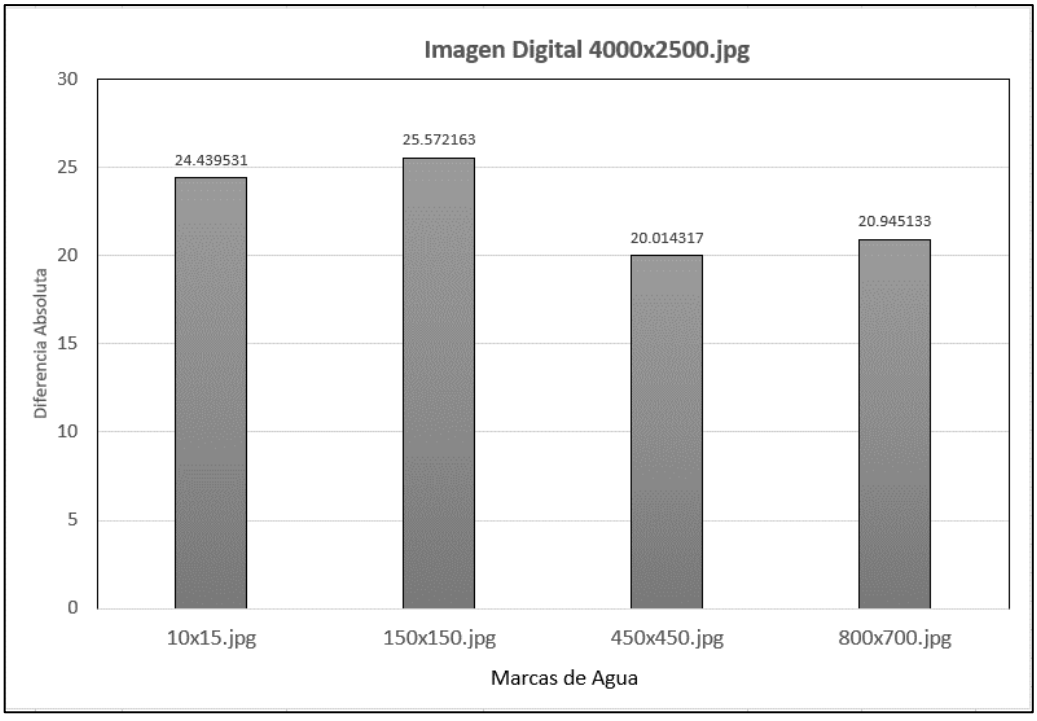

Figura 60 Grafica de diferencias absolutas de la imagen 4000x2500.jpg con las diferentes marcas de agua.

En estas se pueden identificar que tamaño de imagen y marca de agua es el más conveniente para aplicar la técnica esteganográfica DCT sin sufrir una alteración significativa. Pero también se debe considerar la integridad de la marca de agua, es decir, que sea reconocible al momento de verificar a marca de agua que se encuentra oculta dentro de la estego-imagen. En la Tabla 3 se pueden ver las diferencias absolutas que hay entre cada marca de agua original en B/N que se insertó en las imágenes digitales de la tabla anterior, con las marcas de agua recuperadas en B/N.

Tabla 3 Diferencias absolutas entre marcas de agua originales y marcas de agua recuperadas

Marca de Agua	Estego-imagen	Marca de Agua Recuperada	Diferencia Absoluta
10x15.jpg	500x300_15x10.jpg	Si	30.50
10x15.jpg	1024x1024_15x10.jpg	Si	22.02
10x15.jpg	2048x1500_15x10.jpg	Si	23.07
10x15.jpg	4000x2500_15x10.jpg	Si	22.02
150x150.jpg	500x300_150x150.jpg	No	-
150x150.jpg	1024x1024_150x150.jpg	Si	10.81
150x150.jpg	2048x1500_150x150.jpg	Si	183.75
150x150.jpg	4000x2500_150x150.jpg	Si	28.38
450x450.jpg	500x300_450x450.jpg	No	-
450x450.jpg	1024x1024_450x450.jpg	No	-
450x450.jpg	2048x1500_450x450.jpg	Si	134.12
450x450.jpg	4000x2500_450x450.jpg	Si	164.89
800x700.jpg	500x300_800x700.jpg	No	-
800x700.jpg	1024x1024_800x700.jpg	No	-
800x700.jpg	2048x1500_800x700.jpg	No	-
800x700.jpg	4000x2500_800x700.jpg	Si	142.60

Con los resultados obtenidos en la anterior tabla se puede denotar que no en todos los casos es posible recuperar la marca de agua, ya que el sistema solo puede reconstruir la marca de agua de acuerdo a las dimensiones de la marca original que el usuario le proporcione, y si la marca oculta no cumple con estas dimensiones, la marca de agua no se recuperara. La diferencia absoluta entre mayor sea su valor, más grado de modificación se hace visible, y de acuerdo con los resultados obtenidos con el uso de este sistema, las dimensiones de las marcas de agua más convenientes para insertar dentro de las imágenes digitales son las menores de 150x150, ya que son las que menos modificación sufren al aplicar el estegoanálisis. Cabe mencionar que las imágenes sufren un cambio relativamente considerable, esto se debe al tamaño de la marca de agua y de la imagen

digital, como se muestra en la Tabla 4 y en la gráfica de la Figura 61, donde se puede ver de manera más concreta las diferencias absolutas que hay entre las imágenes originales y sus respectivas estego-imágenes.

Tabla 4 Diferencias Absolutas entre las Imágenes Originales y sus Estego-imágenes.

Resolución de la Imagen	Diferencia Absoluta con la Marca 15x10	Diferencia Absoluta con la Marca 150x150	Diferencia Absoluta con la Marca 450x450	Diferencia Absoluta con la Marca 800x700
500x300	6.164111	9.226991	9.356275	9.038508
1024x1024	17.523016	19.118513	22.284642	22.273729
2048x1500	18.020137	24.222263	23.406362	23.124230
4000x2500	24.439531	25.572163	20.014317	20.945133

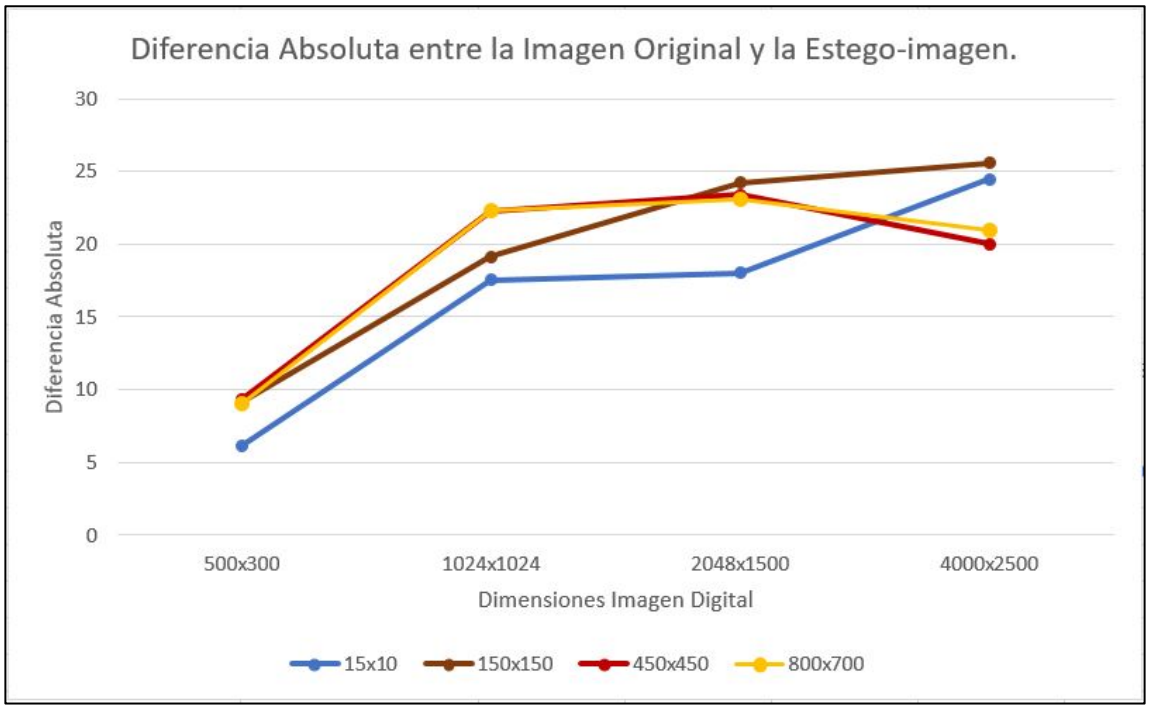

Figura 61 Diferencias Absolutas de las Imágenes Originales y las Estego-imágenes.

De acuerdo con los resultados de las diferencias absolutas que hay entre las imágenes originales y sus diferentes estego-imágenes resultantes, se puede deducir que las resoluciones recomendadas de las imágenes digitales que se deben utilizar para tener un buen resultado al hacer uso de este sistema deben ser no mayor a 1024x1024, ya que se hace uso de una dimensión mayor la estego-imagen se alterara demasiado, y quedara expuestos los indicios de esteganografía, por ejemplo en las siguientes figuras se puede

ver que en las imágenes utilizadas para este proceso de pruebas se pueden ver un poco modificadas pero entre más grande la resolución de la imagen se denotan más las modificaciones que sufren al ocultar la marca de agua.

Figura 62 Imagen con resolución de 1024x1024 *(García, 2011)*.

Figura 63 Estego-imagen con resolución de 1024x1024 y marca de agua oculta de 150x150.

Figura 64 Imagen con resolución de 4000x2500.

Figura 65 Estego-imagen con resolución de 4000x2500 y marca de agua oculta de 800x700.

Para verificar esta última afirmación, se prueba el sistema con diferentes imágenes a las anteriores, con dimensiones de 1024x1024 pixeles y marca de agua de 150x150 pixeles, y otra imagen de 2349x2592 pixeles con la misma marca de agua, las cuales se muestran a continuación:

Figura 66 Imagen con Resolución de 1024x1024 pixeles.

Figura 67 Imagen con Resolución 2349x2592 pixeles.

Figura 68 Marca de Agua de 150x150 pixeles.

Utilizando este sistema para la ocultación de la marca dentro de la imagen, se obtiene como resultado la siguiente estego-imagen:

Figura 69 Estego-imagen resultante de la imagen de 1024x1024 pixeles y marca de agua de 150x150 pixeles.

Y al recuperar la marca de agua con el uso de este sistema, se obtiene el siguiente la siguiente marca resultante:

Figura 70 Marca recuperada de la estego-imagen de 1024x1024 pixeles.

Para la segunda imagen de esta prueba los resultados visuales son los siguientes:

Figura 71 Estego-imagen resultante de la imagen de 2349x2592 pixeles y marca de agua de 150x150 pixeles.

Figura 72 Marca recuperada de la estego-imagen de 2349x2592 pixeles.

Calculando las diferencias absolutas entre las imágenes originales y las estego-imágenes se obtienen los siguientes resultados de la Tabla 5:

Tabla 5 Diferencias absolutas entre las imágenes y sus estego-imágenes.

Imagen	Marca de agua	Diferencia Absoluta (Imagen)
Cielo(1024x1024)	Firma(150x150)	20.87
Volcán(2349x2592)	Firma(150x150)	17.82

Gráficamente se visualiza de la Figura 73:

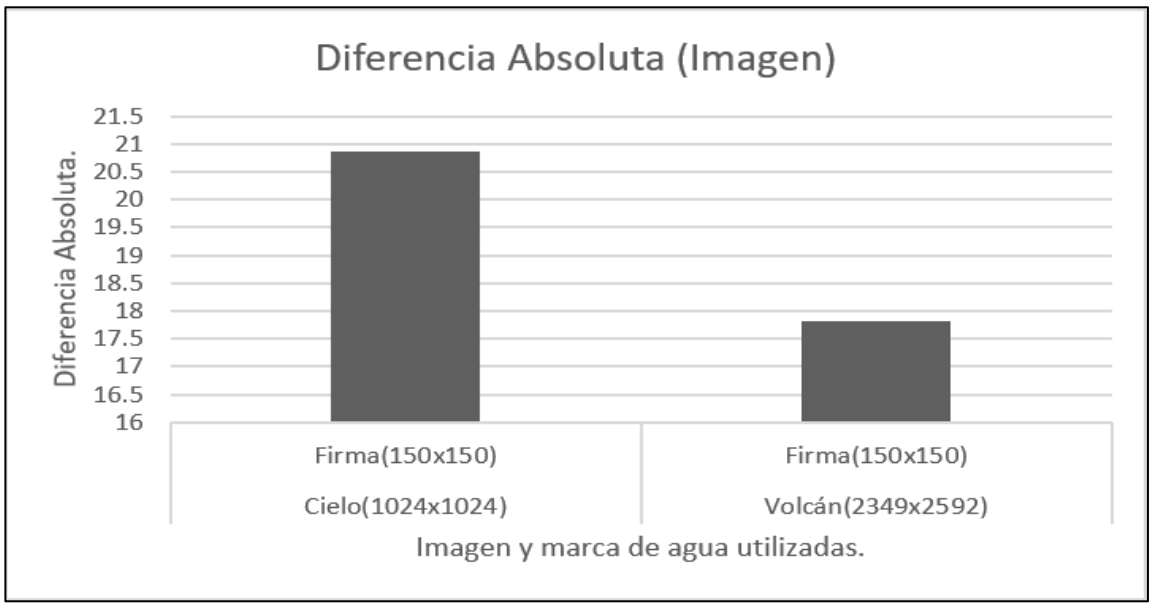

Figura 73 Grafica de las diferencias absolutas entre las imágenes y sus estego-imágenes.

Y para las marcas de agua se obtienen los siguientes resultados de la Tabla 6:

Tabla 6 Diferencias absolutas entre la marca de agua original y las recuperadas.

Imagen	Marca de Agua	Diferencia Absoluta (marca de agua)
Cielo(1024x1024)	Firma(150x150)	18.76
Volcán(2349x2592)	Firma(150x150)	50.74

Y gráficamente se visualiza en la Figura 74.

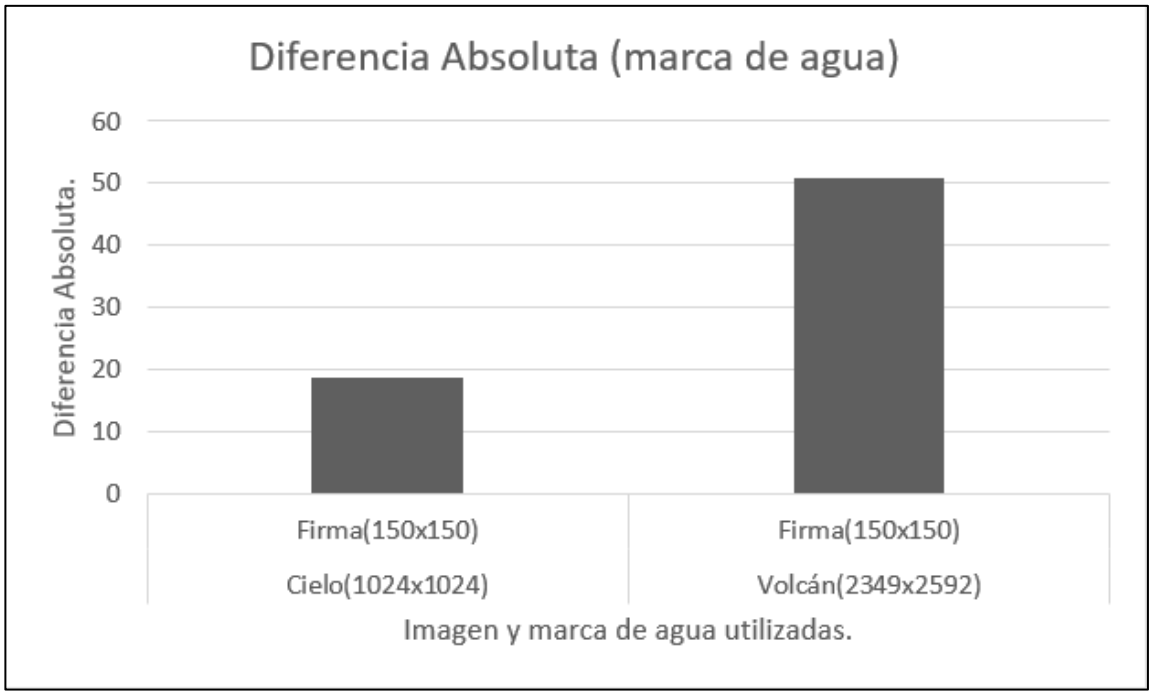

Figura 74 Grafica de las diferencias absolutas entre la marca de agua original y las recuperadas de las estego-imágenes.

De acuerdo con los últimos resultados la imagen de mayores dimensiones se ve menos afectada, pero la marca de agua se deteriora y se modifica más que en la imagen de baja resolución.

CONCLUSIONES

El objetivo principal de este trabajo consiste en realizar un sistema que le permita al usuario que quiera proteger sus derechos de autor de una imagen digital con una resolución no mayor a 1024x1024 pixeles y con formatos JPG, PNG o BMP, mediante una marca de agua oculta con dimensiones no mayores a 150x150 pixeles, dentro de la misma imagen sin que esta se altere visualmente, utilizando algoritmos y herramientas basados en la esteganografía. De acuerdo con la comparación de los resultados obtenidos y el objetivo de este proyecto de tesis, se puede concluir que se ha logrado cumplir dicho objetivo, pero con las especificaciones de las imágenes y marcas de agua establecidas con anterioridad, ya que, si se rebasa las dimensiones o se hace uso de formatos diferentes, el sistema deformará la imagen o no logrará satisfacer las expectativas del usuario.

Para la parte de ocultación de la marca de agua, se probó con los diferentes algoritmos esteganográficos, pero adaptándolos a los requerimientos de este proyecto, empezando desde los más simples como lo son los basados en la esteganografía moderna o los basados en el dominio del espacio, hasta los diferentes algoritmos basados en la esteganografía avanzada o dominio de las transformadas, donde haciendo un análisis se optó por utilizar el algoritmo basado en la DCT; para la parte de reconstrucción de la imagen, después de aplicar la esteganografía, fue necesario hacer un estegoanálisis basado en la IDCT, que daba como resultado una estego-imagen que cumplía con los requerimientos establecidos para este sistema.

En la parte de la recuperación de la marca de agua , se volvía aplicar la DCT y haciendo un análisis en zigzag para encontrar los pixeles de media frecuencia y basado en las dimensiones de la estego-imagen y marca de agua originales, que el sistema solicita al usuario cuando este quiere ejecutar esta opción , da como resultado una imagen que es la marca de agua, dependiendo de las modificaciones que haya sufrido la imagen, va a ser el grado de alteración que sufra la marca recuperada, pero si esta sufre demasiadas modificaciones el sistema no recuperara la marca de tal manera que sea reconocible a simple vista.

Además, el sistema también cumple con la parte de detección de indicios de modificaciones a la estructura de la imagen, pero cabe resaltar que el usuario que quiera detectar estas alteraciones debe contar con la imagen o estego-imagen originales.

Por último, es importante mencionar que este trabajo puede dar pauta para futuros proyectos, para el desarrollo de sistemas más sofisticados que hagan un análisis más minucioso y permita el uso de imágenes con alta resolución y no se delimite a una sola resolución o que permita el uso de formatos complejos como lo es Graphics Interchange Format (GIF) o Scalable Vector Graphics (SVG).

REFERENCIAS

Agora Gallery, 2015. *Agora Gallery Advice from the NYC art experts.* [En línea]
Available at: https://www.agora-gallery.com/advice/blog/2015/12/29/como-proteger-tu-arte-derechos-de-autor/?lang=es
[Último acceso: 07 Febrero 2019].

Aguilar Santiago, J., 2017. *"Sistema Fotográfico para Aplicar Esteganografía y Cifrado en Rostros".* México: Tesis de Licenciatura, Universidad de Guadalajara.

Alicea, S., 2011. *"Aprende Fotografía Digital".* [En línea]
Available at: http://www.aprendefotografiadigital.com/afd/2011/03/22/registro-derechos-de-autor/#axzz5eyGcM2Xg
[Último acceso: 8 Febrero 2019].

Altamirano, P., 2012. *"Aplicación de la Transformada Wavelet en Dos Dimenciones para el Análisis y Comprensión de Imágenes".* Ecuador: Tesis de Licenciatura, Escuela Politécnica de Ejercito.

BANXICO, 2018. *"BANXICO educa".* [En línea]
Available at: http://educa.banxico.org.mx/infografias_y_fichas/billetes_caracteristicas/billete-1000-banco-mexico.html
[Último acceso: 13 Enero 2019].

Cámara de Diputados del H. Congreso de la Unión, 2018. *"Ley Federal del Derecho del Autor".* [En línea]
Available at: http://www.diputados.gob.mx/LeyesBiblio/pdf/122_150618.pdf
[Último acceso: 8 Febrero 2019].

Campos Freire, D. F., 2008. "Las Redes Sociales Trastocan los Modelos de los Medios de Comunicación Tradicionales ". *Revista Latina de Comunicación Social,* XI(63), pp. 277-286.

Cataldi, Z., 2000. *"Una Metodología para el Diseño, Desarrollo y Evaluación de Software Educativo".* Argentina: Tesis de Maestria, Universidad Nacional de La Plata.

Colombet, C., 1997. *"Grandes Principios del Derecho de Autor y los Derechos Conexos en el Mundo".* Tercera ed. Madrid: UNESCO/CINDOC.

Corona Falcon, J. M., 2015. *"Procedimiento de Integración de la Esteganografía al protocolo HTTP".* México: Tesis de Licenciatura, Universidad Nacional Autonoma de México.

Cuzco Naranjo, R. H., 2017. *"Propuesta de un Método Esteganográfico como Soporte al Proceso de Seguridad de Tranferencia de Imágenes".* Ecuador: Tesis de Maestría, Escuela Superior Politécnica de Chimborazo.

García, M., 2011. *Horizontes.* [En línea]
Available at: http://horizontes-manuel.blogspot.com/search/label/paisajes%20naturales
[Último acceso: 10 11 2019].

Giménez Aguilar, M. d. M., 2017. *"Desarrollo y Análisis de Algoritmos de Esteganografía".* España: Tesis de Licenciatura, Universidad Politécnica de Madrid.

Gómez Espinoza, H. O., 2012. *"Aplicación de la Transformada Wavelet y el Método Level Set para el Filtrado y Segmentación de Imágenes".* Ecuador: Tesis de Licenciatura, Universidad Politécnica de Salesiana.

González Osorio, G. J., 2017. *"Reconocimiento de Objetos Utilizando OpenCV y Python en una Raspberry pi 2 en una Tlapaleria".* México: Tesis de Licenciatura, Universidad Autónoma del Estado de México.

Granda Tonato, G. E., 2015. *"Metodologia para el Análisis Forense de Datos e Imagenes De Acuerdo a las Leyes del Ecuador".* Ecuador: Tesis de Licenciatura, Universidad Politécnica Salesiana.

Instituto Nacional del Derecho de Autor, 2019. *Página oficial del Instituto Nacional del Derecho de Autor.* [En línea]
Available at: http://www.indautor.gob.mx/
[Último acceso: 03 04 2019].

Lien Verbauwhede, 2006. *OMPI Organización Mundial de la Propiedad Intelectual.* [En línea]
Available at: https://www.wipo.int/sme/es/documents/ip_photography.htm
[Último acceso: 7 Febrero 2019].

M. Vargas, L., Vera de Payer, E. & Di Gionantonio, A., 2016. "Marcas de Agua: una contribución a la seguridad de archivos digitales". *Revista Facultad de Ciencias Exactas, Fisicas y Naturales,* 3(1), pp. 49-54.

Méndez Naranjo, P. M., 2015. *"Nuevo Algoritmo Criptográfico con la Incorporación de la Esteganografía en Imágenes".* Ecuador: Tesis de Licenciatura, Escuela Superior Politécnica de Chimborazo.

Morocho Checa, E. A., 2014. *"Implementación del Algoritmo Esteganográfico F5 para Imágenes JPEG a Color".* Ecuador: Tesis de Licenciatura, Escuela Politécnica Nacional.

NumPy, 2019. *NumPy.* [En línea]
Available at: https://numpy.org/license.html
[Último acceso: 30 Agosto 2019].

Oliver, E., 2019. *DIGITAL TRENDS ES.* [En línea]
Available at: https://es.digitaltrends.com/fotografia/marcas-de-agua-para-fotos/2/
[Último acceso: 30 07 2019].

OpenCV, 2019. *OpenCV.* [En línea]
Available at: https://opencv.org/license/
[Último acceso: 30 08 2019].

Orea Flores, I. Y., 2005. *"Marcas de Agua Robustas en Imágenes Digitales con Formato BMP".* México: Tesis de Maestría, Instituto Politécnico Nacional.

Renza, D., Ballesteros L., D. M. & Rincón, R., 2016. Método de ocultamiento de píxeles para esteganografía de imágenes en escala de gris.. *Ingeniería y Ciencia,* XII(23), pp. 145-162.

Renza, D., Ballesteros L., D. M. & Rincón, R., 2016. "Método de Ocultamiento de Píxeles para Esteganografía de Imágenes en Escala de Gris Sobre Imágenes a Color". *Ingeniería y Ciencia,* XII(23), pp. 145-162.

Rodríguez Colín, R., 2006. *"Esquema de Marcas de Agua para Imágenes Médicas".* México: Tesis de Maestría, Instituto Nacional de Astrofísica, Óptica y Electrónica.

Rodríguez Medina, G. & Navas, G. S., 2016. *"Esteganografía: Sustitución LBS 1 Bit utilizando Matlab".* Argentina, RedUNCI.

Rodríguez Mendoza, M. N., 2016. *"Análisis de las Técnicas de Esteganografía para el Ocultamiento de la Información".* Ecuador: Tesis de Licenciatura, Universidad Central del Ecuador.

Roman Gonzalez, A., Reynaga Cardenas, C. J. & Ganvini Valcarcel, C., 2013. Método General para la Detección de Imágenes Alteradas Utilizando Técnicas de Compresión. *Revista ECIPerú,* X(1), pp. 14-23.

Ruiz Tejeida, M., 2013. *"Ocultamiento de información en documentos de formato abierto".* México: Tesis de Maestria, Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional.

Sialer, F. & Mejía, I., 2015. Comparación de Técnicas Esteganográficas de Dominio Espacial y Domino Frecuencial en Imágenes Digitales. *Ingeniería: Ciencia, Tecnología e Innovación,* II(2), pp. 41-49.

Soria Lorente, A., Cumbrera González, R. A. & Fonseca Reyna, Y., 2016. Algoritmo esteganográfico de clave privada en el dominio de la transformada discreta del coseno.. *Revista Cubana de Ciencias Informáticas.,* X(2), pp. 116-131.

Soria Lorente, A., Sánchez Reyes, R. M. & Ramírez Aberasturis, A. M., 2013. Algoritmo Esteganográfico de Clave Privada. *GIE Pensamiento Matemático,* III(2), pp. 59-72.

Soria Solís, I. y otros, 2017. Esteganografía en Imágenes Digitales Aplicando Autómatas Celulares Bidimensionales como Generadores Seudoaleatorios. *Revista de Investigaciones de la Escuela de Posgrado,* VI(1), pp. 66-77.

Velasco Bautista, C. L., 2009. *"Ocultamiento de Datos en Imágenes Digitales".* México: Tesis de Maestría, Instituto Politécnico Nacional..

Velasco Bautista, C. L., López Hernández, J. C., Nakano Miyatake, M. & Pérez Meana, H., 2007. "Esteganografía en una imagen digital en el dominio DCT". *Científica,* XI(4), pp. 169-176.

Velásquez Moreira, G. M., Molina Sabando, L. A. & Briones Véliz, Í. B., 2017. Análisis de Técnicas de Esteganografía Aplicadas en Archivos de Audio e Imágen. *Polo del Conocimiento,* II(1), pp. 51-67.

WÍX, 2015. *"WíXBlog".* [En línea]
Available at: https://es.wix.com/blog/2015/07/marcas-de-agua-e-imagenes/
[Último acceso: 13 Enero 2019].

ANEXOS : Código Fuente

Ventana Principal: sistema.py

```
import sys
from PyQt5 import uic, QtWidgets
from PyQt5.QtWidgets import QApplication
from Verificar import verificarmarca # Conectar con las clases de las
from Proteger import Estegano # otras clases de las ventanas.
from detectar import detectarM

qtCreatorFile = "VentanaPrincipal.ui" # Nombre del archivo .ui

Ui_MainWindow, QtBaseClass = uic.loadUiType(qtCreatorFile)
class Principal(QtWidgets.QMainWindow, Ui_MainWindow):

    def __init__(self):
        QtWidgets.QMainWindow.__init__(self)
        Ui_MainWindow.__init__(self)
        self.setupUi(self)

        self.protegerbtn.clicked.connect(self.proteger) #botones para
        self.verificarbtn.clicked.connect(self.verificar)#abrir ventanas
        self.detectarbtn.clicked.connect(self.detectar)
        self.salirbtn.clicked.connect(self.salir)

    def proteger(self):
        self.ventana=QtWidgets.QMainWindow()
        self.ui=Estegano() #abrir ventana proteger
        self.ui.setupUi(self.ventana)
        self.ventana.show()

    def verificar(self):
        self.ventana2=QtWidgets.QMainWindow()
        self.ui=verificarmarca() #abrir ventana verificar
        self.ui.setupUi(self.ventana2)
        self.ventana2.show()

    def detectar(self):
        self.ventana3=QtWidgets.QMainWindow()
        self.ui=detectarM() #abrir ventana detectar
        self.ui.setupUi(self.ventana3)
        self.ventana3.show()

    def salir(self):
        sys.exit(1) #cerrar ventana principal

if __name__ == '__main__':
app = QApplication(sys.argv)
win = Principal()
win.show()
sys.exit(app.exec_())
```

Ventana Proteger: Proteger.py

```
from PyQt5.QtGui import QImage, QPixmap
from PyQt5.QtWidgets import QFileDialog, QApplication
from PyQt5 import uic, QtWidgets
import cv2
import numpy as np
import sys
import scipy.misc

qtCreatorFile0 = "sistema.ui" # Nombre de la interfaz .ui

Ui_MainWindow, QtBaseClass = uic.loadUiType(qtCreatorFile0)

class Estegano(QtWidgets.QMainWindow, Ui_MainWindow):

  def __init__(self):
    QtWidgets.QMainWindow.__init__(self)
    Ui_MainWindow.__init__(self)
    self.setupUi(self)
    self.boton1.clicked.connect(self.abrirImagen)
    self.boton2.clicked.connect(self.abrirMarca)
    self.boton3.clicked.connect(self.DCT)
    self.botonSalir.clicked.connect(self.salir)

  def abrirImagen(self):
    filename, _ = QFileDialog.getOpenFileName(None, 'Buscar Imagen',
    '.', 'Image Files (*.jpg self.image =cv2.imread(filename)

  def abrirMarca(self):
    filename, _ = QFileDialog.getOpenFileName(None, 'Buscar Imagen',
    '.', 'Image Files (*.jpg self.marca =cv2.imread(filename)
  def DCT(self):
    if self.image is not None:
     imagen = self.image
     marca=self.marca
     B=8
     b, g, r = cv2.split(imagen) #Dividir canales
     img1 = b #Obtener canal azul de la imagen
     h,w= img1.shape #Se obtiene el valor de las dimensiones
     img1=img1[:h, :w]
     blocksV=h/B #Cantidad de bloques de 8x8 en Vertical
     blocksH=w/B #Cantidad de bloques de 8x8 en Horizontal
     vis0 = np.zeros((h,w),np.float32) #Matriz hxw con zeros
     Trans = np.zeros((h,w), np.float32) #Matriz hxw con zeros
     vis0[:h, :w]=img1
     blocksV=int(float(blocksV)) #Convertir el valor flotante a entero
     blocksH=int(float(blocksH)) #Convertir el valor flotante a entero
     ######Se calcula DCT de cada bloque de 8x8 de la imagen#######
     for row in range (blocksV):
       for col in range (blocksH):
        currentblock = cv2.dct(vis0[row*B:(row+1)*B, col*B:(col+1)*B])
        Trans[row*B:(row+1)*B, col*B:(col+1)*B]=currentblock


########MARCA DE AGUA#########################################
```

```
_,dst1=cv2.threshold(marca,110,255,cv2.THRESH_BINARY)
 cv2.imwrite('C:\\Users\\Noe
     Alejandro\\Pictures\\pruebas\\marcaxd.jpg',dst1)
 datosmarca = scipy.misc.imread('C:\\Users\\Noe
     Alejandro\\Pictures\\pruebas\\marcaxd.jpg')
 datosmarca = cv2.cvtColor(datosmarca, cv2.COLOR_BGR2GRAY)
 datosJ = datosmarca.ravel()
 datosJ5=int(len(datosJ)/5)
 datosmarca5=[]
 for xmm in range(datosJ5):
   datos55=datosJ[xmm*5:(xmm+1)*5]
   datosmarca5.append(np.array(datos55))
   datosgM=np.concatenate([datosmarca5])
 cv2.destroyAllWindows()
 ################################################################
 dg2 = np.zeros((h,w), np.float32)
 numaun=0
 for z in range (blocksV): #Y
  for zz in range(blocksH): #X
   dg=Trans[z*B:(z+1)*B, zz*B:(zz+1)*B]
    if len(dg)>0:
     datosg = dg.ravel() #convertir matriz a array
     if len(datosg)==64:
       datoszigzag2=[datosg[0],datosg[1],datosg[8],datosg[16],
           datosg[9],datosg[2],datosg[3],datosg[10],datosg[17],
           datosg[24],datosg[32],datosg[25],datosg[18],datosg[11],
           datosg[4],datosg[5],datosg[12],datosg[19],datosg[26],
           datosg[33],datosg[40],datosg[48],datosg[41],datosg[34],
           datosg[27],datosg[20],datosg[13],datosg[6],datosg[7],
           datosg[14],datosg[21],datosg[28],datosg[35],datosg[42],
           datosg[49],datosg[56],datosg[57],datosg[50],datosg[43],
           datosg[36],datosg[29],datosg[22],datosg[15],datosg[23],
           datosg[30],datosg[37],datosg[44],datosg[51],datosg[58],
           datosg[59],datosg[52],datosg[45],datosg[38],datosg[31],
           datosg[39],datosg[46],datosg[53],datosg[60],datosg[61],
           datosg[54],datosg[47],datosg[55],datosg[62],datosg[63]]
      if datosJ5>numaun:
        datosgMD=datosgM[numaun]
        datoszigzag2=[datosg[0],datosg[1],datosg[8],datosg[16],
                      datosg[9],datosg[2],datosg[3],datosg[10],
                      datosg[17],datosg[24],datosg[32],datosg[25],
                      datosg[18],datosg[11],datosg[4],datosg[5],
                      datosg[12],datosg[19],datosg[26],datosg[33],
                      datosg[40],datosg[48],datosg[41],datosg[34],
                      datosg[27],datosg[20],datosg[13],datosg[6],
                      datosg[7],datosg[14],datosgMD[0],datosgMD[1],
                      datosgMD[2],datosgMD[3],datosgMD[4],datosg[56],
                      datosg[57],datosg[50],datosg[43],datosg[36],
                      datosg[29],datosg[22],datosg[15],datosg[23],
                      datosg[30],datosg[37],datosg[44],datosg[51],
                      datosg[58],datosg[59],datosg[52],datosg[45],
                      datosg[38],datosg[31],datosg[39],datosg[46],
                      datosg[53],datosg[60],datosg[61],datosg[54],
                      datosg[47],datosg[55],datosg[62],datosg[63]]

        matriznueva=[datoszigzag2[0],datoszigzag2[1],datoszigzag2[5]
                  ,datoszigzag2[6],datoszigzag2[14],datoszigzag2[15],
```

```
                    datoszigzag2[27],datoszigzag2[28],datoszigzag2[2],
                    datoszigzag2[4],datoszigzag2[7],datoszigzag2[13],
                    datoszigzag2[16],datoszigzag2[26],datoszigzag2[29],
                    datoszigzag2[42],datoszigzag2[3],datoszigzag2[8],
                    datoszigzag2[12],datoszigzag2[17],datoszigzag2[25],
                    datoszigzag2[30],datoszigzag2[41],datoszigzag2[43],
                    datoszigzag2[9],datoszigzag2[11],datoszigzag2[18],
                    datoszigzag2[24],datoszigzag2[31],datoszigzag2[40],
                    datoszigzag2[44],datoszigzag2[53],datoszigzag2[10],
                    datoszigzag2[19],datoszigzag2[23],datoszigzag2[32],
                    datoszigzag2[39],datoszigzag2[45],datoszigzag2[52],
                    datoszigzag2[54],datoszigzag2[20],datoszigzag2[22],
                    datoszigzag2[33],datoszigzag2[38],datoszigzag2[46],
                    datoszigzag2[51],datoszigzag2[55],datoszigzag2[60],
                    datoszigzag2[21],datoszigzag2[34],datoszigzag2[37],
                    datoszigzag2[47],datoszigzag2[50],datoszigzag2[56],
                    datoszigzag2[59],datoszigzag2[61],datoszigzag2[35],
                    datoszigzag2[36],datoszigzag2[48],datosg[49],
                    datoszigzag2[57],datoszigzag2[58],datoszigzag2[62],
                    datoszigzag2[63]]
            matriznueva=np.array(matriznueva)
            matriznueva=matriznueva.reshape(8,8)
            dgx=matriznueva
          dg2[z*B:(z+1)*B, zz*B:(zz+1)*B]=dgx
          numaun=numaun+1
    ############### Se calcula la IDCT de cada bloque
    back0=np.zeros((h,w), np.float32)
    for row in range (blocksV):
     for col in range (blocksH):
      currentblock = cv2.idct(dg2[row*B:(row+1)*B,col*B:(col+1)*B])
      back0[row*B:(row+1)*B,col*B:(col+1)*B]=currentblock
    ###################################################################
    scipy.misc.imsave('SALIDAB.jpg', back0)
    imgmarca0 = scipy.misc.imread('SALIDAB.jpg')
    b2=imgmarca0
    imgSalidaColor = cv2.merge([r,g,b2])
    guardarimgpro, _ = QFileDialog.getSaveFileName(None, 'Guardar
                                        Imagen', '.', 'Image Files
    scipy.misc.imsave(guardarimgpro,imgSalidaColor)
    cv2.destroyAllWindows()
def salir(self):
    sys.exit(1)

if __name__ == '__main__':
app = QApplication(sys.argv)
win = Estegano()
win.show()
sys.exit(app.exec_())
```

Ventana Verificar: Verificar.py

```
import sys
from PyQt5 import uic, QtWidgets
from PyQt5.QtWidgets import QFileDialog,QApplication,QInputDialog

import cv2
import numpy as np
from matplotlib import pyplot as plt
import scipy.misc

qtCreatorFile1 = "Verificar.ui" # Nombre de la ventana principal.
Ui_MainWindow, QtBaseClass = uic.loadUiType(qtCreatorFile1)

class verificarmarca(QtWidgets.QMainWindow, Ui_MainWindow):
 def __init__(self):
   QtWidgets.QMainWindow.__init__(self)
   Ui_MainWindow.__init__(self)
   self.setupUi(self)
   self.selecbtn.clicked.connect(self.seleccionar)
   self.recuperarbtn.clicked.connect(self.recuperar)
   self.salirbtn.clicked.connect(self.salir)
 def seleccionar(self):
   filename, _ = QFileDialog.getOpenFileName(None, 'Buscar Imagen',
      '.', 'Image Files (*.jpg self.imagemarca =cv2.imread(filename)

 def recuperar(self):
   B=8
   imagen=self.imagemarca
   imgorigx, ok = QInputDialog.getInt(self, "getInt()", "Escribe las
     Dimención X de la imagen imgorigy, ok = QInputDialog.getInt(self,
     "getInt()", "Escribe las Dimención Y de la imagen
   yi1=int(imgorigy)
   xi1=int(imgorigx)
   dimen=(xi1,yi1)
   imagen1=cv2.resize(imagen, dimen)
   #-------------------------------Dividir Canales BGR de la Imagen---
   b, g, r = cv2.split(imagen1)
   imagen11=cv2.merge([r,g,b])

   #------------------------Tomar el Canal Azul para Sustraer la Marca
                               de Agua-------------------------------
   imgmarca0 = b
   h=imgmarca0.shape[0]
   w=imgmarca0.shape[1]
   blocksV=h/B #Cantidad de bloques de 8x8 en Vertical
   blocksH=w/B #Cantidad de bloques de 8x8 en Horizontal
   blocksV=int(float(blocksV)) #Se convierte el valor flotante a entero
   blocksH=int(float(blocksH)) #Se convierte el valor flotante a entero
   vis02=np.zeros((h,w), np.float32)
   DatosPixelEstego = np.zeros((h,w), np.float32)
   vis02[:h, :w]=imgmarca0
   xx2=0
   for row2 in range (blocksV):
    for col2 in range(blocksH):
     currentblock2 = cv2.dct(vis02[row2*B:(row2+1)*B,
```

```
                    col2*B:(col2+1)*B])
      DatosPixelEstego[row2*B:(row2+1)*B,
                   col2*B:(col2+1)*B]=currentblock2
    marcorigx, ok = QInputDialog.getInt(self, "getInt()", "Escribe las
      Dimención X de la marca marcorigy, ok = QInputDialog.getInt(self,
      "getInt()", "Escribe las Dimención Y de la marca
    y1=int(marcorigy)
    x1=int(marcorigx)
    datosJ=y1*x1
    datosJ5=datosJ/5
    datoszzmarca5=[]
    numaunzz=0
    for zyy in range (blocksV):
     for zzxx in range(blocksH):
      dgzz=DatosPixelEstego[zyy*B:(zyy+1)*B, zzxx*B:(zzxx+1)*B]
      datosgzz = dgzz.ravel()
      if datosJ5>numaunzz:
        datoszigzagzz=[datosgzz[0],datosgzz[1],datosgzz[8],
         datosgzz[16],datosgzz[9],datosgzz[2],datosgzz[3],datosgzz[10],
         datosgzz[17],datosgzz[24],datosgzz[32],datosgzz[25],
         datosgzz[18],datosgzz[11],datosgzz[4],datosgzz[5],
         datosgzz[12],datosgzz[19],datosgzz[26],datosgzz[33],
         datosgzz[40],datosgzz[48],datosgzz[41],datosgzz[34],
         datosgzz[27],datosgzz[20],datosgzz[13],datosgzz[6],
         datosgzz[7],datosgzz[14],datosgzz[21],datosgzz[28],
         datosgzz[35],datosgzz[42],datosgzz[49],datosgzz[56],
         datosgzz[57],datosgzz[50],datosgzz[43],datosgzz[36],
         datosgzz[29],datosgzz[22],datosgzz[15],datosgzz[23],
         datosgzz[30],datosgzz[37],datosgzz[44],datosgzz[51],
         datosgzz[58],datosgzz[59],datosgzz[52],datosgzz[45],
         datosgzz[38],datosgzz[31],datosgzz[39],datosgzz[46],
         datosgzz[53],datosgzz[60],datosgzz[61],datosgzz[54],
         datosgzz[47],datosgzz[55],datosgzz[62],datosgzz[63]]
        datoszzmarca=[datoszigzagzz[30],datoszigzagzz[31],
                  datoszigzagzz[32],datoszigzagzz[33],datoszigzagzz[34]]
        datoszzmarca5.append(np.array(datoszzmarca))
        numaunzz=numaunzz+1

   datosgMRE=np.concatenate([datoszzmarca5])
   datosgMRE2=datosgMRE.ravel()
   datosgMRE2=datosgMRE2.reshape(y1,x1)

   _,dst2=cv2.threshold(datosgMRE2,3,250,cv2.THRESH_BINARY)
   cv2.imshow('marca de agua recuperada',dst2)
   cv2.waitKey(0)
   cv2.destroyAllWindows()
   guardarmarcarec, _ = QFileDialog.getSaveFileName(None, 'Guardar
     Imagen', '.', 'Image Files scipy.misc.imsave(guardarmarcarec,dst2)
   cv2.destroyAllWindows()
 def salir(self):
    sys.exit(1)

if __name__ == '__main__':
app = QApplication(sys.argv)
win = verificarmarca()
win.show()
sys.exit(app.exec_())
```

Ventana Detectar: detectar.py

```
import sys
from PyQt5 import uic, QtWidgets
from PyQt5.QtWidgets import QFileDialog,QApplication,QInputDialog
import cv2
import numpy as np

qtCreatorFile3 = "Detectar.ui" # Nombre de la ventana principal.
Ui_MainWindow, QtBaseClass = uic.loadUiType(qtCreatorFile3)

class detectarM(QtWidgets.QMainWindow, Ui_MainWindow):
  def __init__(self):
   QtWidgets.QMainWindow.__init__(self)
   Ui_MainWindow.__init__(self)
   self.setupUi(self)
   self.selecIMGObtn.clicked.connect(self.seleccionarimgo)
   self.selecIMGMbtn.clicked.connect(self.seleccionarimgm)
   self.detecModbtn.clicked.connect(self.detectarmod)
   self.salirbtn.clicked.connect(self.salir)

  def seleccionarimgo(self):
   self.modabsLabel.setText("")
   filename, _ = QFileDialog.getOpenFileName(None, 'Buscar Imagen',
   '.', 'Image Files (*.jpg self.imagenoriginal =cv2.imread(filename)

  def seleccionarimgm(self):
   filename2, _ = QFileDialog.getOpenFileName(None, 'Buscar Imagen',
   '.', 'Image Files (*.jpg self.imagenmodificada=cv2.imread(filename2)

  def detectarmod(self):
   imgo=self.imagenoriginal
   imgm=self.imagenmodificada
   h=imgo.shape[0]
   w=imgo.shape[1]
   h2=imgm.shape[0]
   w2=imgm.shape[1]
   if h!=h2 and w!=w2:
    self.modabsLabel.setText("Las Dimenciones son Diferentes")

   if h==h2 and w==w2:
    dif_total=np.sum(cv2.absdiff(imgo, imgm))/((int(h*w))*3)
    dif_total0 = cv2.absdiff(imgo, imgm)

    if dif_total == 0:
      self.modabsLabel.setText("No Hay Diferencia")
    if dif_total != 0:
      difT=str(dif_total)
      self.modabsLabel.setText("La Diferencia Absoluta es: "+ difT)
      cv2.imshow('Imagen Original', imgo)
      cv2.waitKey(0)
      cv2.imshow('Imagen Modificada', imgm)
      cv2.waitKey(0)
      cv2.imshow('Diferencias detectadas', dif_total0)
      cv2.waitKey(0)
      cv2.destroyAllWindows()
```

```
 def salir(self):
   sys.exit(1)

if __name__ == '__main__':
app = QApplication(sys.argv)
win = detectarM()
win.show()
sys.exit(app.exec_())
```