ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

PROPUESTA DE UN MÉTODO ESTEGANOGRÁFICO COMO SOPORTE AL PROCESO DE SEGURIDAD DE TRANSFERENCIA DE IMÁGENES.

RAÚL HUMBERTO CUZCO NARANJO

Trabajo de Titulación modalidad: Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGISTER EN SEGURIDAD TELEMÁTICA

Riobamba – Ecuador

Octubre 2017

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, denominado: **"Propuesta de un método esteganográfico como soporte al proceso de seguridad de transferencia de imágenes"**, de responsabilidad del Sr. Raúl Humberto Cuzco Naranjo, ha sido minuciosamente revisado y se autoriza su presentación.

Tribunal:

Dr. Juan Vargas Guambo; M.Sc.
PRESIDENTE _____
FIRMA

Ing. Iván Hidalgo Cajo; M.Sc.
DIRECTOR DE TESIS _____
FIRMA

Ing. Cristhy Jiménez Granizo M.Sc.
MIEMBRO DEL TRIBUNAL _____
FIRMA

Ing. Byron Hidalgo Cajo M.Sc.
MIEMBRO DEL TRIBUNAL _____
FIRMA

Riobamba, Octubre 2017

DERECHOS INTELECTUALES

Yo, Raúl Humberto Cuzco Naranjo soy responsable de las ideas, doctrinas y resultados expuestos en este trabajo de titulación y el patrimonio intelectual del mismo pertenece a la Escuela Superior Politécnica de Chimborazo.

RAÚL HUMBERTO CUZCONARANJO
No. Cédula 060311880-3

DEDICATORIA

A mis Padres que, sin su ayuda, su apoyo incondicional y su gran amor no podría alcanzar mis sueños. A mi esposa que es uno de mis pilares fundamentales para lograr cumplir una meta más en mi vida profesional.

Raúl

AGRADECIMIENTO

Quiero agradecer primeramente a Dios por darme las oportunidades para seguirme capacitándome y desarrollarme como profesional.

A mi tutor de tesis Ing. Iván Hidalgo por compartir sus conocimientos adquiridos durante su vida profesional para poder desarrollar este trabajo de investigación al Ing. Byron Hidalgo e Ing. Cristhy Jiménez por la ayuda incondicional para cumplir el objetivo de esta nueva meta en mi vida.

Raúl

CONTENIDO

Páginas

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

RESUMEN

En el trabajo de investigación se realizó el estudio de una propuesta de un método esteganográfico para mejorar el nivel de seguridad en la transferencia de imágenes, el método propuesto se basa tanto, en el método Esteganográfico Least Significant Bit (LSB) como en el método criptográfico de César en donde se ha logrado demostrar que al unificar los dos métodos se logra un nivel de seguridad confiable puesto que con el método criptográfico logramos encriptar el mensaje y a la vez lo ocultamos dentro de una imagen logrando así que pase desapercibido por el ojo del ser humano. Se ha desarrollado una aplicación web del método investigado con el lenguaje de programación Java Netbeans. Con la elaboración del prototipo se demuestra que aumenta el nivel de seguridad en un 80% con respecto a otros métodos esteganográficos en las transferencias de imágenes. Se recomienda fomentar la investigación sobre estos temas para incentivar sobre las medidas de seguridad que se debe tener para momento de enviar los mensajes dentro de las imágenes.

Palabras clave: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>, <SEGURIDAD TELEMÁTICA>, <MÉTODO CRIPTOGRÁFICO CESAR> <MÉTODO ESTEGANOGRÁFICO> <ENCRIPTAR> < LEAST SIGNIFICNAT BIT (LSB)>

ABSTRACT

In this research it was developed a study of a proposal of steganography method to improve the security level in the image transfer, the proposed method is based on steganography method Least Significant Bit (LSB) as well Cesar's cryptographic method, where it has been demonstrated, by unifying both methods, it was achieved reliable security level because with cryptographic method it gets encrypted message and at the same time it is hidden into an image and it passed unnoticed to the human eye. It was developed a web application of the research method with Java Netbeans programming language. With the development of the prototype shows the security level increase about 80%. It is recommended to encourage research topics to motivate security measures that it should have at the moment of sending messages into the images.

Key words: <Technology and Engineering Science> < Telematics' Security> <Cesar's Cryptographic Method> <Steganography Method> <Encrypt> <Least Significant Bit (LSB)>

CAPÍTULO I

1 INTRODUCCIÓN

El mundo y la tecnología avanzan, y con ello también las técnicas de seguridad utilizadas para preservar la confidencialidad e integridad de los datos compartidos por los diferentes usuarios.

La esteganografía es el arte de ocultar datos dentro de otros datos. El objetivo, en general, es ocultar los datos de tal forma que los piratas no sospechen del medio en que se comunican. La esteganografía es también un medio de almacenar información basada en la idea de mantener oculta su existencia, que junto con los métodos de comunicación existentes se puede utilizar para llevar acabo intercambios ocultos.

Los gobiernos están interesados en este tipo de comunicación, específicamente cuando se emplea para los siguientes propósitos: los que apoyan la seguridad nacional.

La esteganografía ofrece un gran potencial tanto para las empresas que pueden tener problemas similares con respecto a los secretos comerciales o información de lanzamientos de nuevos productos. En donde se puede establecer una comunicación a través del ocultamiento de información reduciendo en gran medida el riesgo de fuga que está en tránsito. La esteganografía también puede mejorar la privacidad individual, aunque no es un sustituto para la criptografía, la esteganografía proporciona un medio de comunicación privado.

En la actualidad existen varios métodos disponibles de esteganografía, donde cada una utiliza las limitaciones que tienen los diferentes formatos de las imágenes digitales para su respectiva ocultación de información. Esto quiere decir que mientras más nítida sea la imagen mayor cantidad de datos se puede transmitir.

1.1 Problema de Investigación

1.1.1 Planteamiento del problema

Con el avance de la tecnología muchas instituciones públicas y privadas utilizan los medios computarizados para enviar gran parte de su información, como por ejemplo formularios, documentos personales, trámites institucionales, etc. Sin embargo, no toda la información que se envía es comprobada en cuanto a su autenticidad e integridad. El ser humano no está en capacidad de determinar a simple vista si la información es auténtica o si ha sido adulterada; lo cual nos llevaría a una toma de decisión equivocada.

Debido a este problema, surge la necesidad de crear un método de ocultamiento de objetos que, al ser enviado junto con la información importante, permita comprobar que la información fue recibida de manera íntegra y confiable.

La esteganografía es la disciplina en la que se estudian y aplican los métodos que permiten que se oculten mensajes u objetos dentro de otros, a estos objetos se les conoce portadores de modo que pase desapercibida su existencia. Es una mezcla entre artes y técnicas que una vez combinadas las dos conforman la práctica de ocultar y enviar información sensible en un portador que pueda pasar desapercibido.

La esteganografía se derriba de dos palabras griegas steganos y graphos que significan escritura oculta, en términos informáticos, es la disciplina que estudia el conjunto de métodos cuyo propósito es la ocultación de información estos pueden ser mensajes u objetos, dentro de otros denominados archivos contenedores, normalmente multimedia («El Arte de ocultar información», 2012).

Para el desarrollo Esteganográfico existen numerosos métodos que se utilizan para ocultar la información dentro de archivos multimedia como documentos, imágenes, audio, vídeo como, por ejemplo: El método de sustitución, modificación de paleta de colores de una imagen, ocultación en el dominio transformada, Spread Spectrum, etc.

En la actualidad existen algunas investigaciones relacionadas con la seguridad de multimedia en imágenes como lo describimos a continuación:

- La investigación "Securing multimedia colour imagery using multiple high dimensional chaos-based hybrid keys" donde el autor propone un método de cifrado eficiente para asegurar las imágenes en color multimedia. Respuestas dinámicas complejas de múltiples sistemas caóticos de alto orden (Saini & Verma, 2013)
- La investigación "Steganographic method based on interpolation and LSB substitution of digital images" propone un método de ocultación de datos semi-reversible que utiliza la interpolación y la técnica de sustitución menos significativo. En donde en primer lugar, los métodos de interpolación se utilizan para aumentar la escala de la imagen y la cubierta hacia abajo antes de ocultar los datos secretos para una mayor capacidad y calidad. En segundo lugar, el método de sustitución LSB se utiliza para incrustar datos secretos. El resultado de esta investigación tuvo como ventaja que se puede transmitir gran cantidad de información manteniendo su alta calidad visual y una de las desventajas es que no se pudo mejorar la seguridad al momento de transmitir. (Jung & Yoo, 2014)

  Con la presente propuesta de trabajo de investigación se pretende realizar un método esteganográfico para mejorar la seguridad en el envío y recepción de mensajes ocultos por medio de imágenes.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cuál es la mejora en el nivel de seguridad al implementar un nuevo método esteganográfico para enviar mensajes ocultos dentro de imágenes?

1.3 SISTEMATIZACIÓN DEL PROBLEMA

¿Cuáles son los métodos que existen actualmente al momento de utilizar esteganografía?
¿Qué ventajas y desventajas poseen los métodos esteganográficos existentes?
¿Cuáles son los pasos que debe contener un nuevo método esteganográfico para enviar un mensaje oculto en imágenes?
¿Cómo contribuiría al nivel de seguridad al implementar el nuevo método Esteganográfico?

1.4 JUSTIFICACIÓN DE LA INVESTIGACIÓN

1.4.1 Justificación teórica

La esteganografía permite que los mensajes se puedan ocultar atrás de un medio multimedia que puede ser documentos, imágenes, video, etc.; de tal forma que pasen de una manera desapercibida y segura.

La presente investigación se justifica teóricamente, ya que se propone crear un nuevo método de seguridad de envío de imágenes, basado en el uso de métodos esteganográficos.

1.4.2 Justificación metodológica

La justificación metodológica se sustenta en el análisis de las ventajas y desventajas que poseen los métodos actualmente existentes, para en base a este análisis, elaborar un conjunto de pasos que puedan ser aplicados dentro de un nuevo método de seguridad esteganográfico.

1.4.3 Justificación práctica

El método esteganográfico que se pretende desarrollar será implementado a través de una aplicación informática que será la encargada de aplicar los pasos resultantes del método creado. Con esto, se está demostrando la justificación práctica de la propuesta.

Adicionalmente, es importante señalar que la validación del método propuesto se llevará a cabo confrontado los resultados del nivel de seguridad utilizando un método existente vs el nivel obtenido al aplicar el método propuesto.

1.5 OBJETIVOS

1.5.1 Objetivo general

Proponer un método esteganográfico como soporte al proceso de seguridad de transferencia de imágenes.

1.5.2 Objetivos específicos

- Analizar las ventajas y desventajas de los diferentes métodos esteganográficos de transferencia de imágenes existentes.
- Crear un nuevo método esteganográfico a partir de los métodos analizados.
- Implementar un prototipo de aplicación Web para el nuevo método.

1.6 HIPÓTESIS

La implementación de un nuevo Método Esteganográfico permitirá mejorar la seguridad en la transferencia de imágenes.

CAPÍTULO II

2.1 ESTEGANOGRAFÍA

2.1.1 Antecedentes

Del griego steganos y graphos en donde nace el término esteganografía que es el arte de escribir de forma oculta.

Aunque Criptografía y Esteganografía parecieran términos equivalentes no es así puesto que la criptografía se encarga de escribir de forma enigmática el mensaje dificultando el entendimiento, mientras que la esteganografía se encarga de ocultar el mensaje de forma segura dentro de un medio de multimedia (audio, video, imágenes, etc.), en donde pasa por desapercibido dicho mensaje.

La esteganografía se encarga del estudio de un conjunto de métodos y técnicas con el objetivo de insertar información dentro de otro archivo de tal manera que dicha información solo pueda ser recuperada por un usuario legítimo que conozca el método determinado de extracción de la misma.

En los últimos años han causado mucho interés los métodos Esteganográficos debido a que son utilizados por organizaciones. Esta disciplina se lleva empleando desde la antigüedad. Con el presente trabajo de investigación se pretende dar a conocer en el campo de la esteganografía mediante el uso de un software para este método.

Historia y orígenes

Los primeros indicios que describen la utilización de varias técnicas que estas técnicas datan de los tiempos de Herodoto en la Grecia antigua. La historia describe como fue enviado un mensaje a Esparta para avisar de que Xerxes tenía la intención de invadir Grecia, de forma que pasara oculto ante cualquier inspección y que no levantará sospecha.(María Jesús Villagrán, 2006.)

La forma de enviar los mensajes mediante unos tablones cubiertos de cera (Gráfico 1-2). Para camuflar el mensaje se escribía directamente a la tabla y se cubría el tablón con cera y encima de esto se volvía a escribir para ocultar el primer mensaje. A simple vista sólo podía observarse el escrito sobre la cera, pero si se retiraba, podía leerse el mensaje oculto en la madera.

Gráfico 1-2 Tablilla para escribir mensajes ocultos grabado en la madera

Fuente: https://www.drivehq.com/web/pgarciab/Documentos/Esteganografia.pdf

Durante la segunda guerra mundial se usaron los microfilmes, en los puntos de las i's o en signos de puntuación para enviar mensajes. Los prisioneros usan i, j, t y f para ocultar mensajes en código morse. Pero uno de los sistemas más ingeniosos se conoce con el nombre de "Null Cipher". Este último consiste en enviar un mensaje, de lo más común posible, y elegir cierta parte de él para ocultar el mensaje («Ciberseguridad GITS Informática: Criptografía y Esteganografía, Privacidad y Delitos Informáticos», s. f.).

Un ejemplo es el texto siguiente: Actividad molesta indignado gobierno opresor en donde descifrando se obtendría el siguiente mensaje (amigo).

Queda expuesto que la esteganografía ha estado presente desde hace mucho tiempo atrás en nuestra civilización en donde ha sido tradicionalmente empleada por algunas organizaciones como es el caso de agencias militares y de inteligencia, los criminales y la policía.

Ahora bien, en la época moderna la esteganografía emplea canales digitales como es el caso de imagen, video, audio con el propósito de alcanzar el objetivo. Si es bien se logra identificar el objeto contenedor, pero es imposible identificar el algoritmo empleado.

2.1.2 Definiciones y fundamentos teóricos

Gracias a los avances que ha tenido la tecnología especialmente en la computación y al uso más frecuente del Internet, ha ido creciendo el uso de la esteganografía de una manera notable. Con la realización de cálculos que nos proporcionan los equipos de cómputo, permite ocultar información de una manera rápida y eficiente, por otra parte, con el uso del internet ha permitido el intercambio de información entre usuarios.

La esteganografía moderna se base en esconder datos binarios en los bits de los archivos digitales (audio, video, imágenes, etc.) los bits que componen dicho texto a ocultar se introduce en el archivo portador procurando que el nuevo mensaje incrustado cause la menor distorsión posible.

Algunas otras definiciones sobre esta ciencia se muestran a continuación:

- La esteganografía es el arte o ciencia de comunicar mensaje de una manera oculta , insertando la información entre otro conjunto de datos para que no sea vista a simple vista (María Jesús Villagrán, s. f.)
- La Esteganografía es una técnica que permite ocultar mensajes y archivos dentro de otros medios.(Perea, 2012).
- La esteganografía es la disciplina en la que se estudian y aplican técnicas que permiten el ocultamiento de mensajes u objetos, dentro de otros normalmente multimedia, llamados portadores, de modo que no se perciba su existencia.(«Ciberseguridad GITS Informática: Criptografía y Esteganografía, Privacidad y Delitos Informáticos», s. f.)

Hoy en día cuando se realiza una conversación de esteganografía terminamos refiriéndonos a la ocultación de información dentro de un medio digital (audio, video, imágenes, etc.) por lo que el archivo portador se ve a simple vista del humano, pero ignoran con que método se está utilizando para ocultar dicha información.

La esteganografía ha adquirido un gran interés porque ya no solo se usa para enviar mensajes de amor, sino que son utilizados con fines muy diferentes por organizaciones terroristas y criminales entre otras. Según diarios de Estados Unidos informaron que el FBI y la CIA descubrieron que Bin Laden usaba esteganografía para comunicarse con sus oficiales.(«El Arte de ocultar información», 2012)

En el Gráfico 2-2 nos muestra que la esteganografía siempre utiliza dos elementos primero que es el mensaje que se va a ocultar y el segundo es el objeto para tapar el mensaje a enviar, la función estego que es algún tipo de método para que el mensaje pase desapercibido dentro del camuflaje en este caso es dentro de la imagen. La imagen viajara por un canal de transmisión inseguro pudiendo ser interceptado por otro receptor. El objetivo es que el intruso, no pueda darse cuenta que dentro del camuflaje tiene un mensaje oculto. Una vez llegado a su destino el recepto aplicara la estogo-función y la estego-clave si lo tuviera separando así el camuflaje del a imagen y poder ver el mensaje oculto.(Pablo F. Iglesias, 2014).

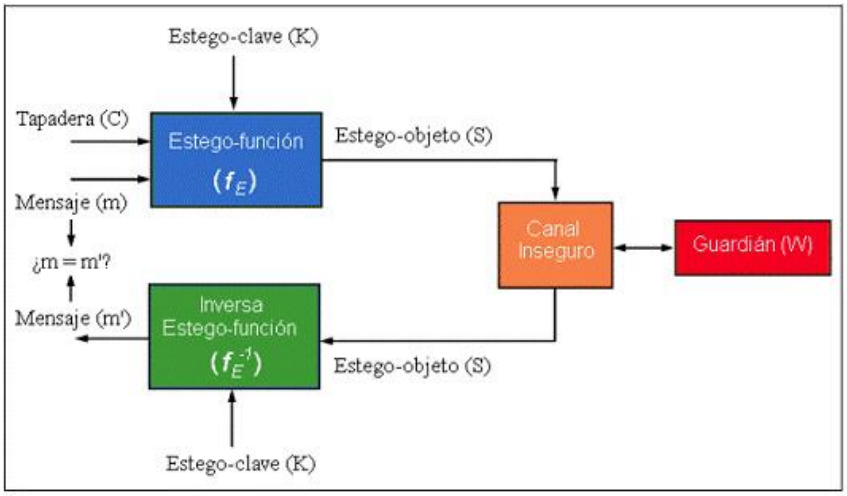

Gráfico 2-2 Proceso de un método esteganográfico

Fuente: https://www.pabloyglesias.com/mundohacker-esteganografia/

2.1.3 Características principales de esteganografía

Dentro de Esteganografía dependerá de 3 características esenciales en el proceso de ocultación de mensajes Gráfico 3-2.

1. **Capacidad** (técnica esteganográfica en donde permite mayor cantidad de información que puede ser ocultada).
2. **Seguridad/Invisibilidad** (nivel de probabilidad de detección por un estegoanalista).
3. **Robustez** (involucra la cantidad de alteraciones dañinas que el medio puede soportar antes de que se pierda la información oculta).

Considerando estas características la búsqueda de un procedimiento concreto de ocultación en un medio puede ayudarse teniendo en cuenta 3 grandes líneas de creación de algoritmos esteganográficos(Pablo F. Iglesias, 2014):

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

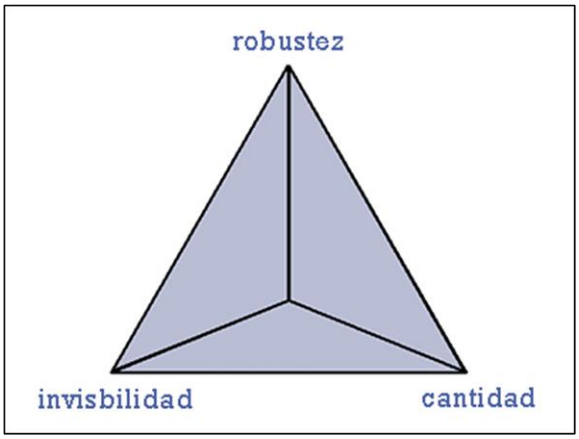

Gráfico 3-2 Características de Esteganografía

Fuente: https://www.pabloyglesias.com/mundohacker-esteganografia/

2.1.4 Beneficios

El objeto de la esteganografía es esconder mensajes existentes dentro de un medio de comunicaciones que van dirigidos entre dos entidades el cual pase desapercibida.

Unas de las principales ventajas de la esteganografía es que me permite la comunicación oculta el cual me muestra su gran valor y aplicación al momento de enviar gran cantidad de información.

En cuanto al límite de un algoritmo esteganográfico no contiene límites, el grado o el estándar que utilice al momento de ocultar el mensaje puesto que un intruso si desea descifrar lo que tiene oculto deberá saber con qué tipo de algoritmo está codificado.

2.1.5 Principios

La primera definición de un esquema de esteganografía fue dada por (Gustavus J. Simmons, 1983) el cual describe a continuación.

En una cárcel dos prisioneros, A y B desean comunicarse confidencialmente para escapar. El problema es que al momento de intercambiar los mensajes se lo debe hacer por medio del guardia W. El personaje W puede leer modificar o incluso puede enviar el mismo los mensajes. Si el guardia descubre que existe algún mensaje para escapar dejara de transmitir los mensajes. En esta prueba de laboratorio se debe establecer un canal de comunicación encubierto(Manuel López Michelone, s. f.).

El uso de la esteganografía permite comunicarnos por medio de un canal encubierto con la ventaja que no puedan detectar. La estrategia que sigue la esteganografía es poder solucionar el problema de los dos prisioneros en donde enviaran la información sin que sean detectados entre los mensajes que permite ser recibido por el guardia.(Manuel López Michelone, s. f.).

El problema de los prisioneros y el guardián se encuentra representado en el Gráfico 4-2

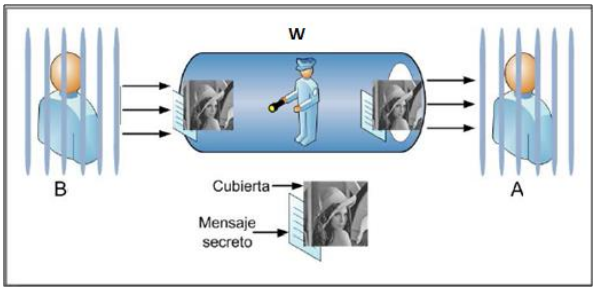

Gráfico 4-2 Esquema de prisioneros

Fuente: Raúl Cuzco, 2016

Este modelo es generalmente aplicable en situaciones de comunicaciones esteganográficas, donde los prisioneros **A** y **B** representan dos partes de la comunicación (emisor y receptor) deseando intercambiar información secreta, así mismo **W** representa un sujeto con posibilidad de leer y posiblemente alterar los mensajes enviados entre emisor y receptor.

2.1.6 Métodos esteganográficos

Existen numerosos métodos y algoritmos utilizados para ocultar la información dentro de archivos multimedia imágenes, audio y vídeo.(Víctor Reza, s. f.)

- Tipo de portador sobre el que actúan (vídeo, audio o texto, principalmente).
- Tipo de algoritmo en sí (ocultación en LSB1, variaciones estadísticas, cambios en la ordenación de los elementos...)
- Por sus características (capacidad, robustez, imperceptibilidad).
- Por el fin que persiguen

2.1.6.1 Modificación de la paleta de colores de una imagen

Con este método las imágenes basadas en paletas de colores como es los formatos (BMP y GIF), se componen de un conjunto de colores determinados. En donde se le asigna a cada color un vector y un índice en cual forma así una paleta de colores el cual apunta a ese pixel en lugar de incluirlo. Una vez obtenida la paleta se puede modificar los propios vectores del color usando diversas técnicas de sustitución como es el caso de Bit Menos Significativo (LSB o Least Significant Bit) ya que al momento de cambiar los colores aparece en la paleta de forma irrelevante.

Con esta técnica ofrece bastante capacidad para cambiar los vectores de colores debido a que existe N cantidad de colores en la imagen entonces va existir N! para poder manipularlos.

Al momento de modificar la imagen hay que tener cuidado ya que primero se debería ordenar la paleta de forma que los colores estuviesen indexados agrupados por similitud o cualquier otro criterio del estilo. Un algoritmo más elaborado es el propuesto en (Kuslu & Yalman, 2016) donde los autores realizan el estudio de un método de alta capacidad basado en la modificación de la paleta de colores de imágenes monocromas partiendo del histograma, emparejando así los colores más utilizados (picos) con los colores no utilizados (ceros), modificando los colores no utilizados dependiendo de los bits a ocultar. Estos emparejamientos se pueden realizar de diferentes formas, por lo que los autores estudian las diferentes posibilidades, permitiendo elegir la que proporcione mayor capacidad.

2.1.6.2 Métodos de sustitución

Sustitución en LSBs:

En esteganografía existen diferentes métodos basados en la modificación de los bits menos significativos o LSBs. Este método consiste en coger los pixeles de la imagen y hacer uso del bit menos significativo de cado uno de ellos y alterarlo provocando así el error menos posible, con este método se puede aplicar en diferentes medios de multimedia con es el caso de audio y video, aunque no es lo más común. La alteración de la imagen es mínima por no decir nula y el mensaje se encuentra insertado a lo largo de los pixeles de dicha imagen. Este método consiste en insertar cada bit del mensaje en toda la imagen retirando el bit menos significativo e insertando cada bit de la información, esto se lo realiza en las áreas más ruidosas donde no atrae la atención.

Como por ejemplo tenemos el valor (1 1 1 1 1 1 1 1) es un número binario de 8 bits. Por lo cual el bit ubicado más a la derecha se le llama "bit menos significativo" (LSB) porque de menor peso, es decir alterándolo cambia en la menor medida posible el valor total del número representado.

Al momento de ocultar la letra "A". Si se tiene una imagen con píxeles con formato RGB (3 bytes), la representación seria la siguiente (3 píxeles, 9 bytes):(Manuel López Michelone, s. f.)

(1 1 0 1 1 0 1 0) (0 1 0 0 1 0 0 1) (0 1 0 0 0 0 1 1)
(0 0 0 1 1 1 1 0) (0 1 0 1 1 0 1 1) (1 1 0 1 1 1 1 1)
(0 0 0 0 1 1 1 0) (0 1 0 0 0 1 1 1) (0 0 0 0 0 1 1 1)

El mensaje a cifrar es ‘A’ cuya representación ASCII es **(1 0 0 1 0 1 1 1)**, entonces los nuevos píxeles alterados serían:

(1 1 0 1 1 0 1 **1**) (0 1 0 0 1 0 0 **0**) (0 1 0 0 0 0 1 **0**)
(0 0 0 1 1 1 1 **1**) (0 1 0 1 1 0 1 **0**) (1 1 0 1 1 1 1 **1**)
(0 0 0 0 1 1 1 **1**) (0 1 0 0 0 1 1 **1**) (0 0 0 0 0 1 1 1)

Observar que se ha sustituido el bit del mensaje (letra A, marcados en negritas) en cada uno de los bits menos significativos de color de los 3 píxeles. Fueron necesarios 8 bytes para el cambio, uno

por cada bit de la letra A, el noveno byte de color no se utilizó, pero es parte del tercer pixel (su tercera componente de color).

Los métodos estudiados aquí son los siguientes:

1. Simple LSB: El método consiste en reemplazar los bits del mensaje original en cada uno de los bits menos significativos de los pixeles de la imagen original dando así una misma imagen con su mensaje oculto.

2. Optimal LSB: El presente método es similar al anterior, pero tras ocultar unos ciertos números de bits, el bit (x+1)-esimo menos significativo es modificado con la finalidad de que el valor final del píxel sea en lo posible el más cercano al valor original sin afectar al mensaje subliminal. Como por ejemplo tendríamos:

Pixel original

$Po= 1100101_2=201_{10}$

Bits a ocultar

111_2

Pixel final

$Pf=11001111_2=207_{10}$

Modificando el 4° bits menos significativo

$Pf=11000111_2=199_{10}$

3. Método PVD (Pixel-Value Differencing): Este método permite un esquema de alta imperceptibilidad a la imagen el cual es proporcionado mediante la selección de dos píxeles consecutivos que se encarga de diseñar una tabla de rango de cuantificación para determinar la carga útil por el valor de la diferencia entre los píxeles consecutivos. Ofreciendo así trasmitir una gran cantidad de datos manteniendo la consistencia de la imagen.(Tseng, Leng, Tseng, & Leng, 2013)

4. Método MBNS (Multiple-Based Notational System): Una vez estudiado los métodos anteriores el concepto de MBNS es similar al método PVD, este método se encuentra basado en el Sistema de Visión Humano para determinar la capacidad subliminal de cada píxel de la imagen original. Los datos que se insertan se transforman en una serie de símbolos en un sistema de notación con múltiples bases. Las bases específicas utilizadas son determinados por el grado de variación local de las magnitudes de los píxeles de una imagen de modo que los píxeles en las zonas ocupadas pueden potencialmente transportar datos más ocultos.

Estudiados los métodos PVD y MBNS se puede ver que como resultados finales que la información pasa más desapercibida puesto que mantienen mejor las características de la imagen original, también tienen una capacidad subliminal menor que los métodos Simple LSB y Optimal LSB, que, a cambio de una menor calidad final de imagen, ofrecen mayor capacidad de ocultación. Un caso especial de modificación de los LSB, que se incluye como un tipo de algoritmo diferente que llama degradación de imágenes.

Paridad de bloques (imagen):

Según este método se basa en dividir la imagen portadora en diferentes bloques o segmentos de un determinado tamaño. Especificando una ordenación arbitraria de los mismos, si la paridad de bloque coincide con el bit de mensaje subliminal a ocultar no se hace nada; si no coincide se modificará el bit menos significativo de algún elemento del bloque. El receptor lo único que tiene que realizar es calcular la paridad de los bloques siempre y cuando manteniendo el mismo orden que envió el emisor.

2.1.6.3 Ocultación en el dominio transformado

Modificación de los coeficientes frecuenciales:

Con los estudios de los métodos que actúan en el dominio temporal suelen ser poco robustos, esto implica que puede llegar hasta el punto de perder toda la información oculta si el estego-objeto es procesado mediante alguna técnica básica de procesamiento de señales. Mientras que los métodos que incluyen la información oculta en el dominio recíproco de las frecuencias suelen ser más robustos. Esto se debe a que se puede elegir con mayor certeza las zonas menos propensas a sufrir modificaciones importantes y hacer que los cambios realizados permanezcan imperceptibles.

Unos de los métodos consisten en dividir la señal en bloques y para cada uno de los bloques escoger dos elementos que vendría hacer el coeficiente de frecuencia A y B que tengan un valor cercano. Si el elemento A tiene un valor mayor que el elemento B, el bloque codificará un 0, si caso contrario B es mayor que A, el bloque codificará un 1.

Cabe destacar que, para transmitir el mensaje subliminal deseado, los valores de A y B se modificarán ligeramente para ocultar el bit que corresponda del mensaje subliminal. Por su parte el receptor, deberá utilizar la misma división en segmentos, la misma ordenación, y los mismos elementos dentro de cada segmento, para poder recuperar la información subliminal.(Jesús Díaz Vico, 2010)

Phase coding (audio)

Con el presente método es aplicado solamente a las señales acústicas debido a la insensibilidad del sistema auditivo humano. Este funciona alterando significativamente la fase de la señal original de la misma manera divididas en segmentos. Cada segmento es modificado acorde al bit del mensaje subliminal. Esto quiere decir cuanto mayor sea la modificación introducida en la fase de los segmentos mayor será la robustez del método, pero se irá disminuyendo su imperceptibilidad.

Del mismo modo, cuantos más cortos sean los segmentos, más alta será la capacidad, disminuyendo también su imperceptibilidad.

Inserción de eco (audio)

El método estudiado se puede aplicar de igual manera solo a señales acústicas por las propiedades que tiene el sistema auditivo humano. Esto quiere decir si tenemos dos señales con la misma frecuencia, pero la del mensaje subliminal debe ser de menor amplitud el cual será imperceptible para el oído humano.

2.1.6.4 Spread Spectrum

Este método es utilizado principalmente en las telecomunicaciones, tradicionalmente se utilizan como métodos de marcas de agua por lo tanto ofrecen alta robustez y poca capacidad subliminal, en algunas ocasiones no se preocupan por su imperceptibilidad, puesto que se usa como marcas de propiedad intelectual.

En esta técnica utilizan un código para extender el espectro, que es independiente de los datos, y para la recuperación de datos se usa una recepción sincronizada del código en el lado del receptor («T-UCE-0011-261.pdf», s. f.)

Estos métodos pueden ser adaptados para proporcionar una alta capacidad subliminal con la disminución de la robustez por lo que pueden ser utilizados como métodos esteganográficos.

En el método propuesto por P. Bassia propone una protección de derecho de autor de una señal de audio mediante el procesamiento del dominio. La fuerza de modificaciones de la señal de audio está limitada por la necesidad de producir una señal de salida que es perceptualmente similar a la original. El presente método lo que requiere el uso de una señal original incrustado una marca de agua con una clave el cual el único que conoce es el propietario de copyright. («P. Bassia, I. Pitas, and N. Nikolaidis. Robust audio waterm arking in the time domain, 2001.», s. f.) .

2.1.6.5 Esteganografía Estadística

En estos métodos una de las ventajas que ofrece es que tiene mayor robustez, pero tiene baja capacidad subliminal esto puede ir en contra de los métodos esteganográficos puros, pero de la mismo forma que la técnica de Spread Spectrum, se puede adaptar para tener mayor capacidad y menos robustez.

Estos métodos suelen ofrecer baja capacidad subliminal, pero una mayor robustez, algo que puede ir en contra de los principios de los métodos esteganográficos puros, pero, de igual forma que en el caso de las técnicas de Spread Spectrum, se pueden adaptar para tener mayor capacidad y menor robustez. El método Patchwork, estudiado por W. Bender, D. Gruhl, N. Morimoto, and Aiguo Lu en donde fue uno de los primeros métodos esteganográficos pertenece a este tipo de métodos. Este método es aplicado en un dominio espacial y aplica un método estadístico para cargar un mensaje a través de patrones. En donde la imagen se divide en bloques y cada bloque en dos conjuntos A y B si en el conjunto A se desea guardar un 1 el brillo del pixel se incrementará y del conjunto B el brillo del pixel disminuirá mientras que para ocultar un 0 seria de manera inversa con respecto al anterior.

Para la recuperación del mensaje se utilizará las mismas divisiones de bloques y conjuntos de la imagen, calculara la diferencia de ambos conjuntos y la diferencia si es positivo recuperara un 1 y si es negativo un 0.

2.1.6.6 Esteganografía sobre texto

Para el manejo de estos métodos esteganográficos sobre texto es muy delicado ya que casi cualquier cambio que se realice puede llamar la atención donde su capacidad subliminal es muy baja. Por otra parte, tanto en la esteganografía de imágenes como de audio se basa en la manipulación de las señales por lo que en los métodos esteganográficos vistos hasta el momento no tiene nada que ver con lo estudiado anteriormente.

Es importante destacar que cuando nos referimos a texto no es nada que ver con escanear y almacenar en imágenes por tal motivo los métodos esteganográficos sobre texto se pueden clasificar en tres tipos(David García Cano, 2004).

- Métodos de Inserción de blancos
- Los métodos sintácticos
- Los métodos semánticos.

Método de inserción de blancos. - consiste en insertar espacios en blanco entre palabras y al final de cada línea.

Método Sintácticos. - Consiste en cambiar los signos de puntuación o alterar el orden de las frases que se está enviando al receptor con el fin que pase desapercibido el mensaje

Método Semántico. - Es el encargado de cambiar las palabras por sinónimos con el fin que pase desapercibido el mensaje.

2.1.7 Tipos de ataque contra la esteganografía

El Estegoanálisis es una disciplina para descifrar mensajes ocultos por esteganografía. Dentro de esta disciplina se utiliza dos tipos:

- Estegoanálisis Manual
- Estegoanálisis Estadístico

Estegoanálisis Manual. - Consiste en buscar a simple vista diferencias entre la imagen original y la imagen esteganografiada. El gran inconveniente es obtener la imagen original para realizar la comparación.

Estegoanálisis Estadístico. - Se encarga de la comparación de frecuencia de distribución de colores, esto se da en el caso de archivos de imágenes en donde se encuentra oculto el mensaje para ser descifrado. Esta técnica necesita emplear software especializado.

En cuanto a los tipos de ataques, se puede considerar la siguiente clasificación (Tabla 1-2):

Tabla 1-2 Tipo de ataques y sus consecuencias

Tipo de Ataque	Consecuencia
Activo	Solo analiza la información.
Pasivo	Modifica la información accidentalmente hasta dañarle completamente.
Malicioso	Cambia la información a su antojo provocando una reacción del receptor

Fuente: Raúl Cuzco, 2016

Los ataques pasivos a la vez se pueden clasificar de acuerdo a la información de la que disponga el estegoanalísta como se detalla a continuación. (David García Cano, 2004)

- **Stego-only attack (Un solo Ataque):** Este método se puede usar cuando el atacante dispone de solo un objeto en este caso puede ser de una imagen para su estudio.

- **Known cover attack (Ataque Cubierta Conocida):** Este método se utiliza cuando el estegoanalista dispone de la imagen original y también de la imagen con el mensaje oculto, pero en ningún caso dispone del algoritmo utilizado para enmascarar la información.

- **Known message attack (Ataque Mensaje Conocido):** Este método donde el atacante deduce el mensaje que están enviando sin saber cuál es el algoritmo utilizado para el enmascaramiento.

- **Chosen stego attack (Ataque Estego Elegido):** Este método consiste en que el atacante conoce el algoritmo utilizado y tiene en su poder la imagen con su texto oculto.

- **Chosen message attack (Ataque Mensaje Elegido):** Este método consiste en que cuando el estegoanalista oculta un mensaje utilizando un determinado algoritmo el cual ira capturando firmas que deje el algoritmo en donde permitirá detectar otras estego-imágenes con el mismo algoritmo.

2.1.8 Herramientas para análisis esteganográficos en imágenes

Existen varias herramientas que permite realizar Estegoanálisis en imágenes algunas de ellas se detallan a continuación:(Paz Álvaro, s. f.)

VSL (Laboratorio de Esteganografía Virtual). - Es una herramienta de Diagramación compleja contiene una interfaz sencilla de utilizar está diseñado para ocultar imágenes digitales, también nos permite detectar mensajes ocultos dentro de una imagen controlando a la vez su robustez.

STEGHIDE. - Es un programa que nos permite ocultar datos en varios tipos de imágenes y archivos de audio, unas de las características principales es el cifrado de datos incrustados y la compresión de los mismos a la vez permite la verificar la integridad de los datos extraídos.

STEGSPY. - Esta herramienta detecta la esteganografía y también que programa se utilizó para ocultar el mensaje en las últimas versiones, una de las características principales de esta herramienta nos identifica la ubicación del contenido oculto dentro de la imagen.

2.1.9 Archivos de imágenes

En esteganografía es común ocultar mensajes utilizando imágenes que pueden pasar desapercibidos por los atacantes, Existen varios tipos de formatos para imágenes, algunos de los más utilizados son los siguientes:(David García Cano, 2004)

Windows BitMap (BMP). - La principal característica de este formato es que la imagen se forma de una parrilla de pixeles de modo que no sufre pérdida de calidad y resulta muy adecuado para su manipulación.

Graphics Image Format (GIF). - Fue diseñada para comprimir imágenes digitales reduciendo la paleta de colores a 256 colores como máximo y a la vez admite gamas de menor número de colores; permitiendo optimizar el tamaño del archivo que contiene la imagen.

Joint Photographic Experts Group (JPEG). - A diferencia del formato GIF este admite una paleta hasta 16 millones de colores, es utilizado para publicar imágenes en la web, pero la desventaja es que al momento de la compresión se va perdiendo o reduciendo la calidad de la imagen.

Tagged Image File Format (TIFF). - Almacena imágenes de muy buena calidad utilizando cualquier profundidad de 1 a 32 bits, este tipo de formatos es muy considerado para trabajos de edición o impresión de imágenes.

Portable Network Graphics (PNG). - El presente formato nace a partir de un problema de patente del algoritmo LZW (Lempel-Ziv-Welch) el cual pretende sustituirle a GIF como estándar, PNG cubre todas las características de GIF con un algoritmo que no permite la pérdida de información y con una paleta decolores superior a los 256 bits, logrando así una altísima calidad en el uso de capas y transparencia.

En la Tabla 2-2 se describen las ventajas y desventajas de cada uno de los formatos de imágenes(EULINS CHANGIR, s. f.).

Tabla 2-2 Ventajas y desventajas de los formatos de imágenes

Formatos	Ventajas	Desventajas
Windows BitMap(BMP)	Es sencillo e indicado para trabajar con esteganografía	El tamaño del archivo es muy grande.
Graphics Image Format (GIF)	La enorme compresión el cual nos complica trabajar con esteganografía y la capacidad de uso de transparencias.	La escasa paleta de colores
Joint Photographic Experts Group (JPEG)	La calidad a la hora de representar fotografías (con su paleta de 16 bits y su alta compresión).	La pérdida de calidad e información al momento de realizar una compresión.
Tagged Image File Format (TIFF)	Se obtiene una muy buena calidad	El tamaño que ocupa. Debido a lo específico de este tipo de fichero, no es prácticamente usado para esteganografía
Portable Network Graphics (PNG)	Se trata de un formato libre	No permite el uso de animaciones

***Realizado por*:** Raúl Cuzco, 2016

2.2 CRIPTOGRAFÍA

2.2.1 Antecedentes

La palabra Criptografía se deriva del griego "kryptos" que significa oculto, y "Graphia" que significa escritura, según definiciones consultadas es el arte de escribir documentos mediante cifras o códigos secretos el cual protege su confidencialidad.

Desde hace mucho tiempo atrás la criptografía se ha convertido en una técnica o un conjunto de las mismas que nos ayudan a la mantener protegida la información contra ataques por personas que se dedican a interceptar modificar e incluso insertar información extra a la original.

Otros de los usos que se puede hacer con la criptografía es evitar el uso no autorizado a recursos de una red o a los sistemas informáticos evitando así que el intruso haga denegación de servicios.

En el Gráfico 5-2 representa como actúa la criptografía en un texto plano.

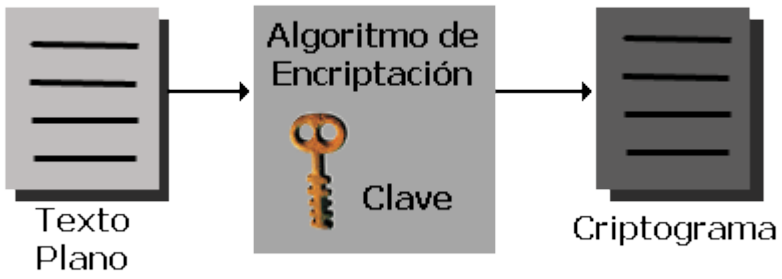

Gráfico 5-2 Proceso de Criptografía sobre un texto plano

Realizado por: http://www.segu-info.com.ar/criptologia/criptologia.htm

2.2.2 Historia y origen

La criptografía nace a partir que el hombre necesita enviar información confidencial a otros individuos ya sea por motivos diplomáticos, comerciales, etc., por lo que surge la información secreta que se trata de conservar su integridad hasta que llegue a un individuo o una comunidad completa.

En el año 500 A.C. los griegos utilizaron un método de encriptación el cual consistía de un cilindro llamado "scytale" alrededor del cual enrollaban una tira de cuero. Una vez escrito el mensaje se desenrollaba el cuero y se veía una lista de letras sin sentido. El mensaje enviado solo se podía leerse al enrollar el cuero nuevamente en un cilindro de igual magnitud.(Seguridad de la Información, s. f.)

Durante el imperio de Roma emplearon un sistema de cifrado el cual consistía en reemplazar la letra a encriptar por otra letra distanciada a tres posiciones más adelante. Durante su reinado estos mensajes nunca fueron desencriptados («Seguridad Informática / Criptología», s. f.)

La Criptografía es la disciplina que se encarga de estudiar cómo transformar un mensaje de texto en un mensaje encriptado, mediante alguna técnica que impida que el mensaje real sea descifrado por terceros. («Criptografía», 2014).

2.2.3 Métodos criptográficos

En la actualidad existen dos grupos de métodos criptográficos: Métodos Clásicos y Métodos modernos.

Métodos Clásicos. - Corresponde al conjunto de métodos que pueden ser clasificados en métodos de transposición y de sustitución.

El Método de Transposición consiste en cifrar el mensaje, cambiando simplemente el orden de las letras mediante algún patrón como, por ejemplo, escribiendo primero las letras múltiplos de tres y luego las letras restantes dando como resultado un conjunto de palabras sin significado o sentido aparente. El mensaje real sólo podrá ser descifrado por quien conozca o reciba el patrón de intercambio utilizado en el mensaje.

El Método de Sustitución consiste en reemplazar las letras del mensaje original por otras. Algunas técnicas de cifrado por sustitución se listan a continuación:

- **Cifrado de Cesar. -** Esta técnica de cifrado es una de las más simples y se basa en reemplazar cada letra del texto original por otra letra que se encuentra desplazando un número fijo de

posiciones más adelante o más atrás en el alfabeto. Por ejemplo, si se desea cifrar la frase "**ESTO ES UN MENSAJE"** utilizando un alfabeto de 2 posiciones hacia adelante el resultado será el siguiente:

Abecedario normal:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

Abecedario cifrado:

c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b

Mensaje cifrado: **GUVQ GU WP OGPUCLG**

- **Cifrado de Polibio. -** Este método consiste en representar en una matriz de 5 X 5 todo el alfabeto en donde la letra I /J se representaría en una sola posición, una vez obtenida la matriz se reemplazará cada letra por sus coordenadas escribiendo primero la fila y luego la columna es decir la letra A tomará el valor de 11 y así sucesivamente.

La matriz de Polibio se encuentra representada en la Gráfico 6-2:(David Garcia Cano, 2004)

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I / J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Gráfico 6-2 Tabla de Polibio

Fuente: http://www.taringa.net/posts/ciencia-educacion/19329301/Aprende-Criptografia-Cifrado-Polibio-con-este-Post.html

Ejemplo

Mensaje Original: HOLA MUNDO

Mensaje Encriptado: 23343111 3245551434

- **Cifrado de Playfair. -**Este método consiste en crear una matriz de 5X5 en donde se colocará el alfabeto luego de colocar la clave del mensaje en este proceso se debe ingresar las letras que no se encuentren repetidas.

Es un sistema de encriptación bastante bueno, las posibles claves que puede tener es de las permutaciones de 25 elementos lo que nos permite obtener un número muy grande que no se puede derrotar con algoritmos de fuerza bruta.

CAPÍTULO III

3 METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Diseño de estudio

Para el diseño de esta investigación es de tipo no experimental Transversal en donde luego de estudiar los conceptos básicos de la esteganografía y los métodos existentes, se desarrolló un proceso esteganográfico que fue evaluado para medir o determinar el nivel de seguridad al transferir mensajes ocultos en este tipo de archivos.

Para la investigación la muestra se tomó a los estudiantes de quinto semestre de la escuela de Ingeniería en Sistemas de la Escuela Superior Politécnica de Chimborazo que se encontraban tomando la asignatura de Criptografía en donde se valida que la propuesta del método mejora el nivel de seguridad en la transmisión de mensajes dentro de una imagen.

3.2 Tipo de estudio

La presente investigación es de tipo aplicativo y experimental.

Aplicativo: La investigación se basa en conocimientos existentes de investigaciones previas respecto a métodos esteganográficos para establecer nuevos procesos que permitan mejorar los métodos existentes.

Experimental: Se basa en pruebas realizadas en laboratorios en donde se observan los objetos más importantes para el estudio de la investigación y captación de los fenómenos a primera vista. En otras palabras, observar cómo el uso de un nuevo método esteganográfico para transferencia de imágenes puede mejorar el nivel de seguridad de los métodos ya existentes.

3.3 Población

La población para validar la propuesta está constituida por los estudiantes de quinto semestre de la Escuela de Ingeniería en Sistemas de la ESPOCH que, a la fecha de la validación, se encontraban recibiendo la asignatura de Criptografía.

3.4 Muestra

La muestra para la investigación será tomada según la siguiente formula.

$$n = \frac{N * Z_{\propto}^{2} p * q}{d^{2} * (N-1) + Z_{\propto}^{2} * p * q}$$

Dónde:

N= Número de la población

Z=Nivel de Confianza

p=Probabilidad de éxito

q=Probabilidad de fracaso

3.5 Métodos de investigación

El método principal que se utilizado en la presente investigación es el método científico en donde se siguieron las etapas principales de manera sistemática para obtener un conocimiento fiable. Las etapas del método científico son:

- Planteamiento del problema
- Formulación de Hipótesis
- Levantamiento de la información
- Análisis de resultados comprobación de Hipótesis
- Presentación de resultados

Además del método científico se utilizó el método analítico-sintético para en base del análisis de los resultados establecer las conclusiones respectivas.

3.6 Técnicas

Las técnicas que se utilizaron son las siguientes:

Búsqueda de información: Permitió obtener toda la información que sea necesaria para elaborar el marco teórico de la investigación utilizando fuentes tanto primarias como secundarias disponibles.

Pruebas: Se realizaron pruebas al prototipo desarrollado bajo escenarios de laboratorios.

Observación: Se observó la participación de los sujetos diseñadas para la validación de la propuesta.

3.7 Instrumentos

Los instrumentos que se han utilizado en el presente estudio son los siguientes:

Netbeans: Es un Entorno de Desarrollo Integrado (IDE) de código abierto, este programa permite desarrollar aplicaciones en Java como, por ejemplo: J2SE, web, aplicaciones móviles entre otras (Gráfico 7-3).

La presente aplicación se utilizó como una plataforma de programación para la elaboración del prototipo de la aplicación propuesta.

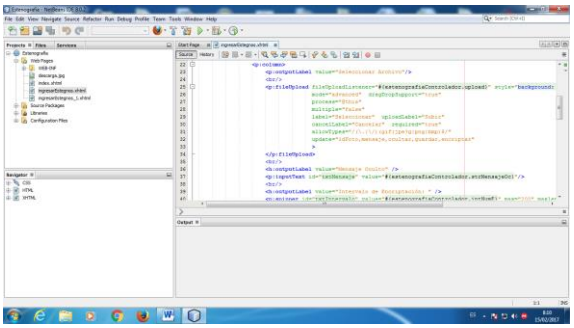

Gráfico 7-3 Pantalla de Netbeans

Realizado por: *Raúl Cuzco, 2016*

HashMyFiles: Es una aplicación que nos va a permitir calcular los MD5 Y SHA-1 de varios archivos a la vez (Gráfico 8-3). En nuestra investigación se realizó las pruebas de seguridad ya que nos permitió comparar MD5 tanto del emisor como del receptor.

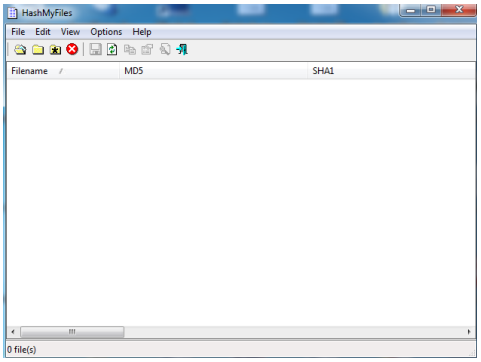

Gráfico 8-3 Pantalla de HashMyFiles

Realizado por: *Raúl Cuzco, 2016*

FlexHEX: Es una herramienta que nos permite editar archivos binarios, se puede inspeccionar, modificar, buscar o reemplazar datos binarios, ASCII o UNICODE (Gráfico 9-3).

Con esta herramienta nos permite ver si los archivos del emisor y receptor fueron modificados en formato binario.

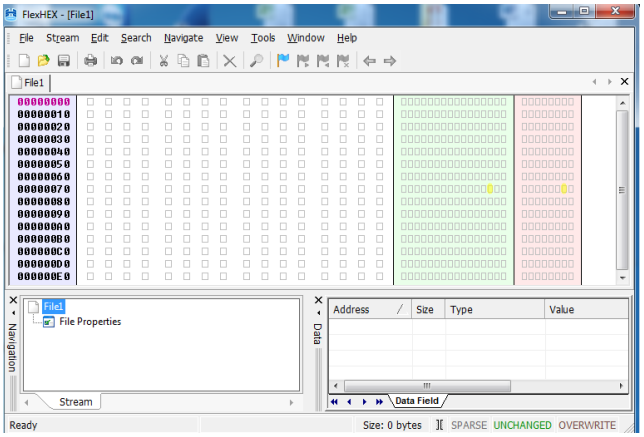

Gráfico 9-3 Pantalla de FlexHEX

Realizado por*: Raúl Cuzco, 2016*

3.8 Aplicación del método

Durante el proceso de transferencia de imágenes existe una gran preocupación por las alteraciones que éstas pueden sufrir, sin que el usuario se dé cuenta de ello y por ende atente o vulnere la seguridad de los sistemas informáticos.

La propuesta del presente trabajo de investigación es la elaboración de un método esteganográfico en el que mejora considerablemente la seguridad en la transmisión de imágenes, tomando como base las principales características de los métodos existentes, pero a la vez superando las debilidades que pueden presentar.

3.8.1 Procedimientos

Como primer punto debemos conocer los métodos esteganográficos existentes para lo cual se realiza un breve resumen mediante un cuadro con sus respectivas ventajas y desventajas como se describe en la Tabla 3-3.

Tabla 3-3 Ventajas y desventajas de Métodos Esteganográficos

Métodos Esteganográficos	Ventajas	Desventajas
Patchwork	Utiliza la distribución Gaussiana, la información se esconde en forma de parches aleatoriamente.	Oculta muy poca información y para ocultar la información se debe tener registrado donde se encuentra la información para su recuperación.
Codificación por textura de bloques	Busca regiones con patrones similares entre la imagen y la información a ocultar.	Es realizado necesariamente por un operador humano quien se encargara de escoger las regiones fuente y destino.
Codificación de tasa de bits elevada	Está diseñada para tener un mínimo impacto en la percepción de la imagen. Existe un mayor control sobre las imágenes.	Es muy sensible sobre las modificaciones en la imagen.
LSB(Bits menos significativo)	Tiene una alta tasa de bits de inserción tiene una baja complejidad computacional	Tiene poca robustez
Codificación de fase	Las modificaciones en las fases permite tener una transmisión encubierto de información	Tiene un nivel medio de robustez, si la trasmisión sufre un ataque en medio de la trasmisión la información no se recupera en su totalidad.

***Realizado por*:** Raúl Cuzco, 2016

Una vez analizada las ventajas y desventajas de los métodos esteganográficos se propone realizar con el método LSB puesto que tiene una tasa de bits baja y no solamente se puede insertar en el último bit, sino que también se puede insertar en cualquier bit del byte, con respecto a la complejidad computacional se logra mejorar su robustez con el nuevo método planteado para así convertirle en una fortaleza con el nuevo método planteado.

3.9 Variables e indicadores

Tomando en cuenta la hipótesis de trabajo planteada: La implementación de un nuevo Método Esteganográfico permitirá mejorar la seguridad en la transferencia de imágenes, se determinan las siguientes variables (Tabla 4-3):

Variable Independiente: Método Esteganográfico

Variable Dependiente: Seguridad en la Transmisión de imágenes

Operacionalización Conceptual

Tabla 4-3 Conceptualización de las variables

VARIABLE	TIPO	CONCEPTO
Método Esteganográfico	v. independiente	Es una serie de pasos sucesivos, conducen a una meta.
Seguridad en la Transmisión de imágenes	v. dependiente	Nivel de protección de los datos utilizando esteganografía.

Realizado por: Raúl Cuzco, 2016

Operacionalización Metodológica

Tabla 5-3 Operacionalización de variables

VARIABLE	CATEGORIA	INDICADOR	TÉCNICA	INSTRUMENTO / FUENTE
Método Esteganográfico	Envió y Recepción	- Complejidad - Recursos - Utilizados	Búsqueda de información - Pruebas - Observación	Netbeans
Seguridad en la transmisión de imágenes	Envío y Recepción	- Nivel de complejidad - Cantidad de líneas de código - Nº clave	- pruebas - Observación - Análisis	- HashMyfiles - Netbeans

Realizado por: Raúl Cuzco, 2016

3.10 Análisis de las variables

En el presente trabajo de investigación se propone una propuesta de un método esteganográfico que mejora el nivel de seguridad en la transmisión de imágenes.

3.10.1 Indicadores de la variable independiente

Para la comprobación de la hipótesis se aplicará la propuesta de método esteganográfico para cifrar un mensaje en una imagen y posteriormente someter esta imagen a prueba para determinar si es posible o no desencriptar el mensaje.

3.10.2 Indicadores de la variable dependiente

Para determinar si mejora la seguridad con el método propuesto se analizará los resultados obtenidos en la prueba, respecto a si los sujetos de prueba lograron o no descifrar el mensaje encriptado.

CAPÍTULO IV

4 RESULTADOS Y DISCUSIÓN

4.1 Procedimiento general

El presente trabajo de investigación tiene como propósito dar a conocer los diferentes métodos esteganográficos con el fin de conocer los niveles de seguridad de cada uno de los estudiados.

A través del estudio lo que se pretende es crear una propuesta de un método esteganográfico para mejorar el nivel de seguridad en la transmisión de mensajes dentro de una imagen.

Para mejorar los niveles de seguridad, se estudian los métodos criptográficos básicos con el fin de implantar en un método esteganográfico el más apropiado o aquella que presenten las mayores ventajas en cuanto a seguridad y facilidad de implementación.

Para la validación de la propuesta se realizó pruebas con los estudiantes de Quinto Semestre de la Escuela de Ingeniería en Sistemas de la ESPOCH que se encuentran cursando la asignatura de Criptografía. La prueba consiste básicamente en tratar de descifrar un mensaje, que se encuentra en el interior de una imagen y determinar el tiempo o esfuerzo empleado por los sujetos de prueba.

4.2 Presentación de resultados

Los resultados obtenidos demuestran de una manera directa que el uso de la propuesta ayuda a mejorar la seguridad de la información brindando así confiabilidad, disponibilidad e integridad.

4.3 Demostración de la hipótesis

A continuación, se presenta de manera sistematizada la demostración de la hipótesis

4.3.1 Planteamiento

La implementación de un nuevo Método Esteganográfico permitirá mejorar la seguridad en la transferencia de imágenes.

4.3.2 Población

La población que se utiliza para el presente estudio son los estudiantes de Quinto Semestre de la Escuela de Ingeniería en Sistemas de la Escuela Superior Politécnica de Chimborazo que se encuentran cursando la materia de Criptografía, ya que son las personas que tienen conocimientos acerca de seguridad informática.

4.3.3 Selección del nivel de significación

Para el estudio de la investigación se va utilizar un nivel de significación de ∞=0.05

4.3.4 Descripción de la muestra

Para el estudio se ha tomado de la población una muestra en este caso la población es de 50 y la muestra se obtendrá con la siguiente formula

$$n = \frac{N * Z_{\propto}^2 p * q}{d^2 * (N-1) + Z_{\propto}^2 * p * q}$$

Dónde:

N=50

Z=1.96

p=0.05

q=0.95

d=0.05

$$n = \frac{50 * 1.96^2 \ * 0.05 * 0.95}{0.05^2 * (50-1) + 1.96^2 \ * 0.05 * 0.95}$$

n =30

Una vez realizado los cálculos correspondientes obtenemos que la muestra de nuestra población es de 30 estudiantes que se encuentran cursando la materia de criptografía.

4.3.5 Especificación del estadístico

Con respecto a la distribución para la población se realizó con Chi Cuadrado en donde determinaremos que con la propuesta obtendremos mayor seguridad en las imágenes, con un nivel de significancia de 5%, se crea una tabla con los datos obtenidos al grupo experimental.

4.4 Comprobación

En la Tabla 6-4 nos presenta un resumen con los 30 estudiantes que es la muestra sacada para la realización de la prueba a los estudiantes quinto semestre que se encuentran cursando la materia de Criptografía de la Escuela de Ingeniería en Sistemas de la ESPOCH.

Tabla 6-4 Datos obtenidos de la muestra tomada

NIVEL SEGURIDAD	Nº ESTUDIANTES
ALTO	23
MEDIO	5
BAJO	2

Realizado por: Raúl Cuzco, 2016

De la misma manera se realiza la prueba con toda la población para demostrar que no existe mayor alteración como se demuestra en la Tabla 7-4

Tabla 7-4 Datos obtenidos de toda la población

NIVEL SEGURIDAD	Nº ESTUDIANTES
ALTO	43
MEDIO	5
BAJO	2

Realizado por: Raúl Cuzco, 2016

Una vez realizada la prueba se describe de cada uno de los niveles de seguridad:

El nivel alto nos indica el número de estudiantes que no pudieron descifrar el mensaje encriptado que se envió dentro de una imagen por el lapso de más de 2 horas

El nivel medio indica el número de estudiantes que cifraron el mensaje en un tiempo de una hora y 45 minutos.

El nivel bajo indica el número de estudiantes que cifraron el mensaje en un tiempo de una hora con 30 minutos

4.5 Indicadores de Variables

Una vez realizado las diferentes pruebas en el laboratorio nos arroja resultados y aplicando el programa HashMyFiles verificamos el nivel de seguridad del archivo por lo que nos muestra un MD5 que es un código único que tiene todo archivo y podemos verificar si han sufrido algún cambio al momento de la transmisión de la imagen.

Como nos muestra en el Gráfico 10-4 podemos observar que tanto el archivo del emisor como del receptor contiene el mismo MD5 por ende podemos sacar la conclusión que el archivo no ha sufrido ningún cambio.

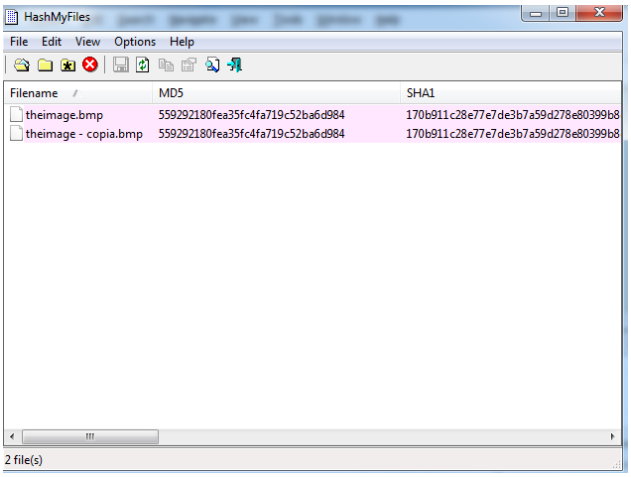

Gráfico 10-4 Autenticación de archivos

Realizado por: *Raúl Cuzco, 2016*

Otra manera de verificar si existió o no alguna alteración de los datos en el transcurso de envió de la imagen se lo puede realizar con la herramienta FlexHEX, que nos permite alterar la información que se lleva dentro de la imagen, gracias a la encriptación no nos permite identificar el mensaje para que pueda ser alterado como nos representa en el Gráfico 11-4.

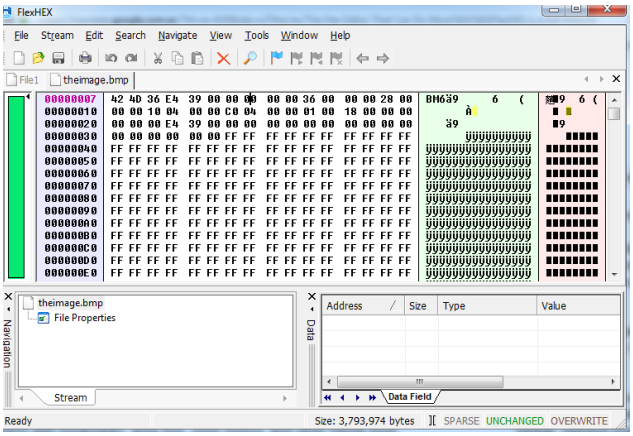

Gráfico 11-4 Demostración con FlexHEX

Realizado por: *Raúl Cuzco, 2016*

4.6 Conclusión de la hipótesis

Comprobación de la Hipótesis General

Hipótesis Nula H_0: El método esteganográfico implementado no permite descifrar el texto claro que se envía dentro de una imagen.

Hipótesis alternativa Ha: El método esteganográfico implementado permite descifrar el texto claro que se envía dentro de una imagen.

Fórmula para el Chi-Cuadrado muestra:

$$X^2 = \frac{(A_1 - D_1)^2}{D_1} + \frac{(A_2 - D_2)^2}{D_2} + \frac{(A_3 - D_3)^2}{D_3} = \sum_{J=1}^{K} (A_J - D_J)^2 / D_J$$

Donde:

X^2 = Ji cuadrada la cual agrupa en categorías las observaciones.

A = Porcentaje antes de la aplicación de nuestra propuesta

D = Porcentaje después de la aplicación de la propuesta

J = El *número* de opciones que se tiene dependerá la cantidad de frecuencias que se repite las variables.

La distribución chi-cuadrada depende de desviaciones independientes, grados de libertad y no puede ser negativa.

Interpretación de resultados

Variable Independiente

- *Método Esteganográfico*

Variable dependiente:

- *Seguridad en la Transmisión de imágenes*

Resolvemos la ecuación de tabla final de total de la matriz (Tabla 8-4):

Tabla 8-4 Tabla de resultados con una muestra de 30

NIVEL SEGURIDAD	Nº ESTUDIANTES	Fo	Fe
ALTO	23	23	16,9
MEDIO	5	5	2,5
BAJO	2	2	6,4

***Realizado por**: Raúl Cuzco, 2016*

$$X^2 = \frac{(A_1 - D_1)^2}{D_1} + \frac{(A_2 - D_2)^2}{D_2} + \frac{(A_3 - D_3)^2}{D_3} = \sum_{J=1}^{K} (A_J - D_J)^2 \ / \ D_J$$

$$x^2 = \frac{(23-10)^2}{10} + \frac{(5-10)^2}{10} + \frac{(2-10)^2}{10}$$

$$x^2 = 25.8$$

De la misma manera se realiza la prueba con toda la población obteniendo los siguientes resultados (Tabla 9-4).

Tabla 9-4 Tabla de resultados con toda la población

NIVEL SEGURIDAD	Nº ESTUDIANTES	Fo	Fe
ALTO	35	35	20.16
MEDIO	10	10	2.67
BAJO	5	5	8.71

Realizado por: *Raúl Cuzco, 2016*

$$X^2 = \frac{(A_1 - D_1)^2}{D_1} + \frac{(A_2 - D_2)^2}{D_2} + \frac{(A_3 - D_3)^2}{D_3} = \sum_{J=1}^{K} (A_J - D_J)^2 \; / \; D_J$$

$$x^2 = \frac{(35-16.67)^2}{16.67} + \frac{(10-16.67)^2}{16.67} + \frac{(5-16.67)^2}{16.67}$$

$$x^2 = 31$$

- Nivel de Significación

95% de confianza = 5% de error ⇒ 0,05

- Grados de libertar mediante la fórmula:

df = (r-1)

Para el valor crítico de ji – cuadrado, podremos determinar los valores en la campana de Gauss descrita en la Gráfico 12-4:

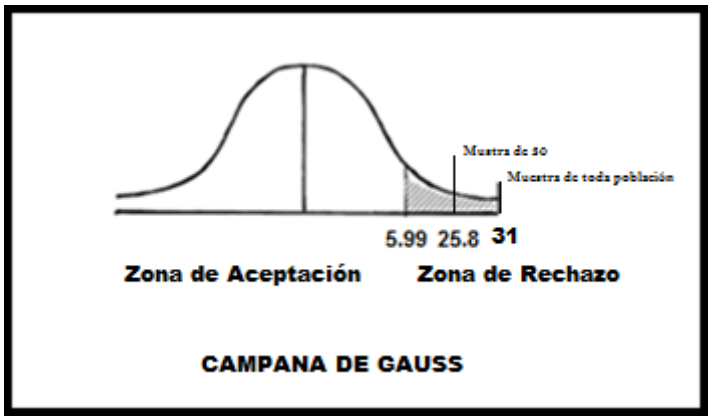

Gráfico 12-4 Campana de Gauss

Realizado por: *Raúl Cuzco, 2016*

Una vez calculada el valor de chi-cuadrado nos dan como resultados, para la muestra de 30 obtenemos X2=25.8 y para toda la población tenemos que X2= 31, concluimos que tanto para la muestra como para la población tiene una pequeña alteración, pero siempre va hacer mayor que (5.99) con df= (3-1) =2 al 95% confianza se acepta la hipótesis H0 y se rechaza el H1 por lo que nos indica que mejora considerablemente la seguridad con el nuevo método propuesto.

CAPÍTULO V

5 PROPUESTA

5.1 Introducción

En el presente capítulo se presenta propuesta de un método esteganográfico en el que permita mejorar la seguridad en la transferencia de imágenes.

5.2 Objetivos

Con el método propuesto se pretende:

- Obtener mayor seguridad al momento del envío y recepción de un mensaje oculto dentro de una imagen en cualquier formato.
- Enviar la imagen de manera íntegra y confiable, para la persona o usuario correspondiente.

5.3 Descripción del escenario con el método propuesto STEGOCESARF5

En la actualidad al momento de enviar un mensaje dentro de una imagen no existe niveles de seguridad dando facilidad a que se produzcan ataques generando así alteración de dicho mensaje provocando grandes fraudes a causa de este cambio.

Con el nuevo método propuesto lograremos dar mayor seguridad en la transferencia de imágenes generando así confiabilidad integridad al momento de recibir dicho mensaje.

Para la elaboración del método propuesto denominado STEGOCESARF5 se utiliza el algoritmo de cesar que consiste en remplazar cada letra del mensaje por otra de un alfabeto que contiene las letras, se desplaza de acuerdo a un número X de posiciones. Generalmente mientras más grande sea el número de desplazamiento se estará proporcionando mayor nivel de seguridad. El proceso de encriptar y desencriptar se encuentra representado en el Gráfico 13-5.

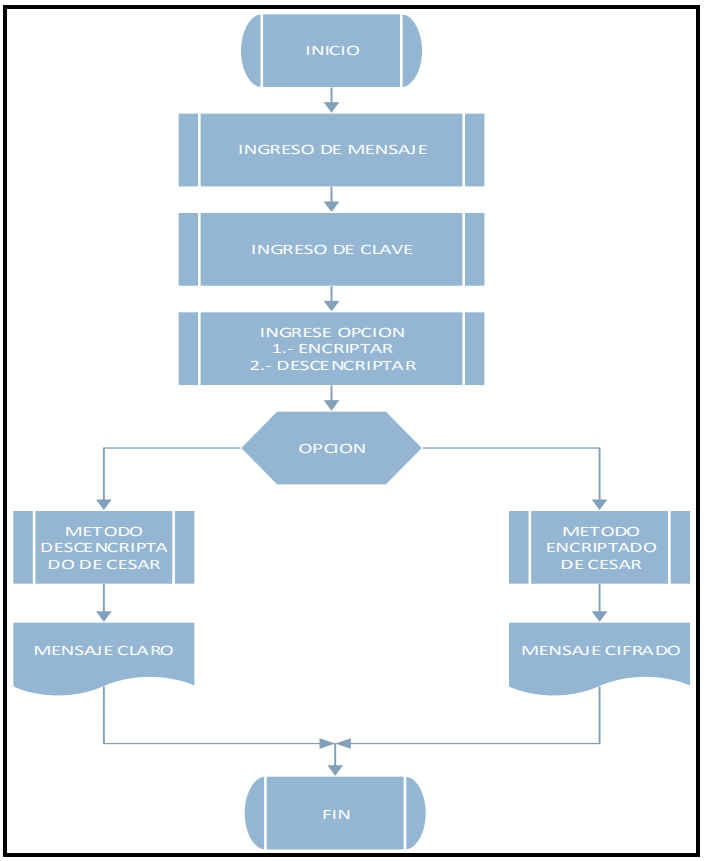

Gráfico 13-5 Diagrama de Encriptación y Desencriptación de mensaje

Realizado por: *Raúl Cuzco, 2016*

Una vez realizado la encriptación se procede a la ocultación del mensaje dentro de una imagen, durante este proceso se utilizará el método de bit menos significativo el cual al integrarse con el mensaje encriptado permitirá obtener mayor seguridad. Esta etapa se muestra en el Gráfico 14-5.

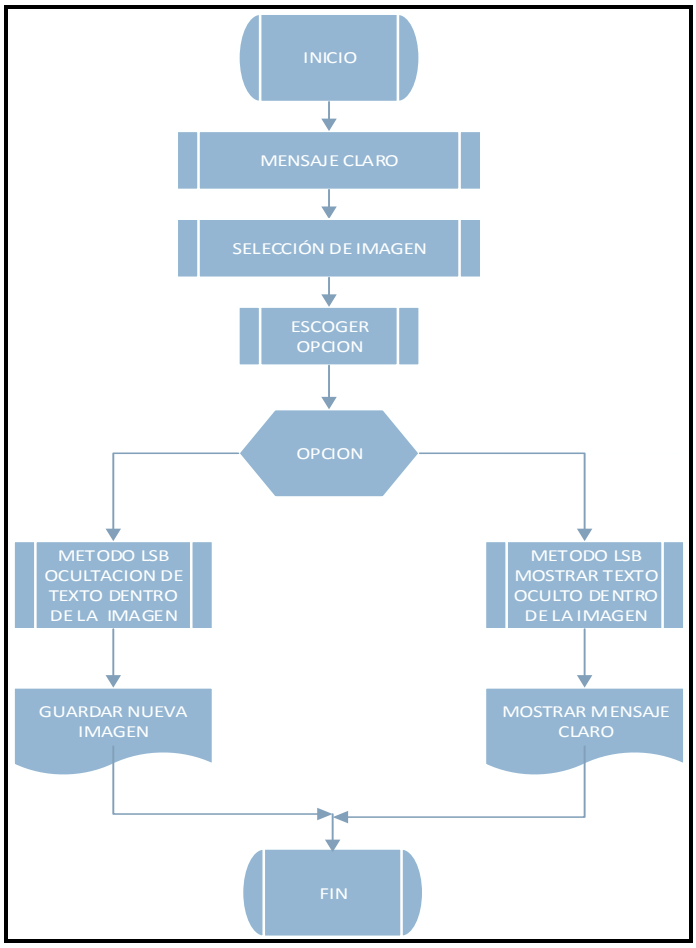

Gráfico 14-5 Diagrama de ocultar y mostrar imagen

Realizado por: *Raúl Cuzco, 2016*

En síntesis, la propuesta de método STEGOF5 consiste en las siguientes etapas o procesos.

- Selección de imagen a utilizar.
- Ingreso de mensaje a ocultar.
- Ingreso de numero clave para el proceso de encriptación del mensaje.
- Ejecución del algoritmo de cesar.
- Ejecución del algoritmo esteganográfico.
- Creación de la nueva imagen con el mensaje oculto.

Cabe mencionar que el usuario puede manipular uno de los parámetros más importantes antes del ocultamiento del mensaje en la imagen. El usuario podrá determinar el número de desplazamientos a aplicar en el método de cesar, el mensaje que se desea modificar y la imagen que será la encargada de ocultarlo.

La propuesta del método esteganográfico es implementada mediante una aplicación o sistema de ocultamiento, desarrollada en el lenguaje de programación Java a través del entorno grafico de netbeans e integrando las herramientas y métodos seleccionados durante la fase de estudio teórico de la presente investigación.

Con la finalidad de comprobar la mejora en el nivel de seguridad, se descargó la aplicación denominada esteganografía básica que no permite establecer ningún nivel de seguridad durante la encriptación por otra parte, se desarrolló la aplicación que permite configurar los parámetros de seguridad antes de la encriptación.

En el Gráfico 15-5 nos presenta un sistema que no brinda ningún nivel de seguridad como se presenta a continuación.

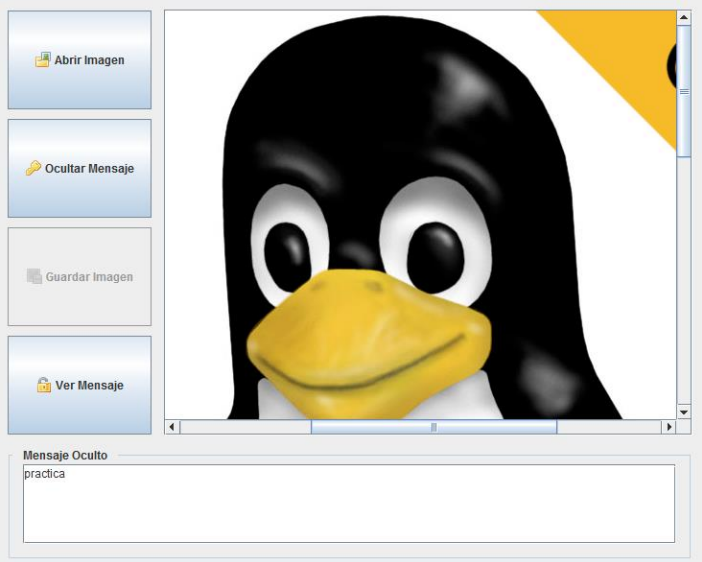

Gráfico 15-5 Sistema sin proceso de encriptación

Realizado por: *Raúl Cuzco, 2016*

En la Gráfico 16-5 muestra en mensaje encriptado y a la vez el número de desplazamiento que se realizó tanto para la encriptación como la descencriptacion.

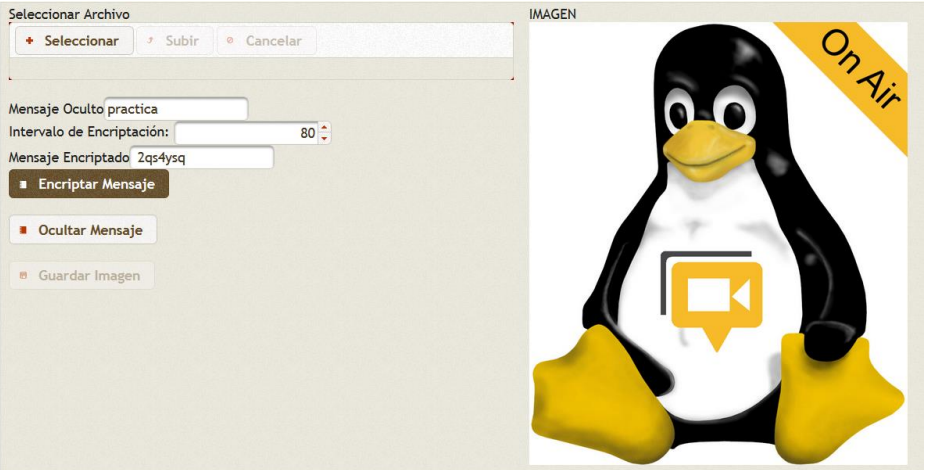

Gráfico 16-5 Sistema con proceso de encriptación

Realizado por: *Raúl Cuzco, 2016*

CONCLUSIONES

- Mediante el análisis de los diferentes métodos esteganográficos se logró identificar el más robusto, para implantar en la nueva aplicación, en este estudio el método LSB fue el seleccionado ya que debido a sus características permite no solo ocultar siguiendo un patrón, sino que se puede seguir otras opciones como alterar en cualquier otro bit del byte logrando así otra forma de ocultar el texto dentro de la imagen.

- Con la combinación de uno de los algoritmos esteganográficos y criptográficos se ha logrado crear un nuevo método logrando así mejorar el nivel de seguridad en las transferencias de imágenes.

- La esteganografía en la antigüedad se enviaba solo texto hoy en día se utiliza para enviar archivos he incluso para enviar imágenes dentro de otra imagen.

- Existe diversos algoritmos criptográficos que se puede combinar con los métodos esteganográficos y así mejorar el nivel de seguridad de la información.

- De la misma forma que se va priorizando la seguridad de la información en la esteganografía va apareciendo nuevos programas que le vulneran la seguridad en dichos sistemas.

- Los resultados del análisis realizado permitieron demostrar que mientras mayor sea la dificultad del algoritmo esteganográfico a implantar mayor va hacer el nivel de seguridad de la información

- Una de las principales fortalezas del método desarrollado es la inclusión de un método criptográfico para incrementar el nivel de seguridad. Esta característica es inusual en otras herramientas esteganográficas disponibles.

- Mediante las pruebas realizadas se pudo comprobar que al utilizar el método propuesto se mejoró en un 85% el nivel de seguridad en la transferencia de imágenes haciendo de ésta una herramienta confiable y robusta.

RECOMENDACIONES

- Fomentar la investigación sobre estos temas para incentivar sobre las medidas de seguridad que se debe tener para momento de enviar los mensajes dentro de las imágenes.

- Profundizar esta temática con el fin de llenar vacíos y profundizar con nuevos conocimientos para fortalecer dicho tema.

- Incentivar para futuros estudios, esta temática desde nivel de pregrado el cual nos ayudará a tomar conciencia sobre la importancia de la seguridad de la información y por ende generar nuevas alternativas de protección durante el envío/recepción de información.

BIBLIOGRAFÍA

Ciberseguridad GITS Informática: Criptografía y Esteganografía, Privacidad y Delitos Informáticos. (s. f.). Recuperado 25 de febrero de 2016, a partir de http://www.gitsinformatica.com/criptografia.html

Criptografía. (2014, enero 26). Recuperado a partir de https://infosegur.wordpress.com/unidad-4/criptografia/

David García Cano. (2004). *ANÁLISIS DE HERRAMIENTAS ESTEGANOGRÁFICAS*. UNIVERSIDAD CARLOS III DE MADRID, MADRID. Recuperado a partir de http://e-archivo.uc3m.es/bitstream/handle/10016/7119/PFC_David_Garcia_Cano_2004_201033204919.pdf?sequence=1

El Arte de ocultar información: Esteganografía. (2012, febrero 24). Recuperado a partir de http://www.expresionbinaria.com/el-arte-de-ocultar-informacion-esteganografia/

EULINS CHANGIR, H., HERNANDEZ. (s. f.). METODOS DE CIFRADO Y POLITICAS DE SEGURIDAD. Recuperado 18 de febrero de 2017, a partir de http://loshermanosiutll.simplesite.com/

Díaz Vico, Jesús (2010). *Esteganografia y EstegoAnalisis: Ocultación de Datos en STREAMS DE AUDIO VORBIS*. Universidad Politecnica de Madrid, Madrid.

Jung, K.-H., & Yoo, K.-Y. (2014). Steganographic method based on interpolation and LSB substitution of digital images. *Multimedia Tools and Applications*, *74*(6), 2143-2155. https://doi.org/10.1007/s11042-013-1832-y

Kuslu, M., & Yalman, Y. (2016). Contemporary Approaches on Reversible Data Hiding Methods: A Comparative Study. *International Journal of Applied Mathematics, Electronics and Computers*, *4*(1), 1-9.

Manuel López Michelone. (s. f.). Esteganografía: para cifrar mensajes en imágenes. *unocero*. Recuperado a partir de https://www.unocero.com/2012/11/28/esteganografia-para-cifrar-mensajes-en-imagenes/

María Jesús Villagrán. (s. f.). Orígenes de la esteganografía. *VSantivirus*. Recuperado a partir de http://www.vsantivirus.com/esteganografia.htm

P. Bassia, I. Pitas, and N. Nikolaidis. Robust audio waterm arking in the time domain, 2001. (s. f.). Recuperado a partir de http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.54.3896&rep=rep1&type=pdf

Pablo F. Iglesias. (2014, diciembre 11). #MundoHacker: Esteganografía, el arte de ocultar información sensible. Recuperado 1 de marzo de 2016, a partir de http://www.pabloyglesias.com/mundohacker-esteganografia/

Paz Álvaro. (s. f.). Herramienta para realizar técnicas de esteganografía y estegoanálisis. *Herramienta para realizar técnicas de esteganografía y estegoanálisis.* Recuperado a partir de http://www.gurudelainformatica.es/2014/08/herramienta-para-realizar-tecnicas-de.html

Perea, S. (2012, diciembre 7). Esteganografía: fotografías con firma invisible. Recuperado 25 de febrero de 2016, a partir de http://www.xatakafoto.com/tutoriales/esteganografia-fotografias-con-firma-invisible

Saini, J. K., & Verma, H. K. (2013). A hybrid approach for image security by combining encryption and steganography (pp. 607-611). IEEE. https://doi.org/10.1109/ICIIP.2013.6707665

Seguridad de la Información. (s. f.). Seguridad Informatica / Criptología. Recuperado 9 de marzo de 2016, a partir de http://www.segu-info.com.ar/criptologia/criptologia.htm

Tseng, H.-W., Leng, H.-S., Tseng, H.-W., & Leng, H.-S. (2013). A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number, A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number. *Journal of Applied Mathematics, Journal of Applied Mathematics*, *2013*, *2013*, e189706. https://doi.org/10.1155/2013/189706, 10.1155/2013/189706

Victor Reza. (s. f.). ESTEGANOGRAFIA. Recuperado 19 de febrero de 2017, a partir de https://prezi.com/8lp4ji-qayyu/esteganografia/