ISSN 0798 1015

REVISTA ESPACIOS

Vol. 40 (Nº 38) Año 2019. Pág. 6

Experiencia de aplicación de criptografía para mejorar la seguridad en un método esteganográfico en imágenes

Cryptography application experience to improve security in a steganographic method in images

CUZCO, Raúl H. 1; MANTILLA, Carmen E. 2; MÉNDEZ, Pablo M. 3 y ÁVILA, Diego F. 4

Recibido: 03/07/2019 • Aprobado: 26/10/2019 • Publicado 04/11/2019

Contenido

1. Introducción
2. Metodología
3. Resultados
4. Conclusiones
Referencias bibliográficas

RESUMEN:
Esta investigación presenta una propuesta de mejora en la seguridad de mensajes transmitidos en imágenes, combina el método esteganográfico Least Significant Bit con el algoritmo criptográfico César. La imagen y datos a transmitir se ingresan en una aplicación web desarrollada en Java Netbeans y son visibles solo para el receptor, en la recepción se verifica la integridad de los datos con software. La aplicación en el caso de estudio produjo un incremento del 76.67% en el nivel de seguridad.
Palabras clave: Esteganografía, criptografía, seguridad telemática

ABSTRACT:
This research presents a proposal to improve the security of messages transmitted in images, combining the Least Significant Bit steganographic method with the César cryptographic algorithm. The image and data to be transmitted are entered into a web application developed in Java Netbeans and are visible only to the receiver, upon receipt the integrity of the data is verified with software. The application in the case study produced a 76.67% increase in the level of security.
Keywords: Steganography, Cryptography, Telematic security

1. Introducción

La tecnología avanza y con ello los ataques de los hackers a las empresas son cada vez más sofisticados, volviéndolas más vulnerables exponiendo la seguridad de su información privilegiada, debido a esto, es necesario implementar métodos de seguridad para preservar la confidencialidad e integridad de los datos compartidos, como pueden ser secretos comerciales o lanzamientos de nuevos productos, la esteganografía ofrece un gran potencial para reducir el riesgo de fuga. Aunque no es un sustituto para la criptografía, la esteganografía proporcionando seguridad y privacidad. (Díaz, 2010)

La esteganografía es una técnica que aplica métodos para ocultar mensajes dentro de un medio multimedia (Reza, 2017) . De esta manera no se sospecha que lleva almacenada información oculta, esto junto con los métodos de comunicación permite realizar intercambios ocultos. Se ha

utilizado desde hace mucho tiempo atrás por los terroristas cibernéticos para comunicarse, el FBI reveló que era la forma como se comunicaba Osama Bin Laden con los terroristas. (Inteco, 2012)

Actualmente, existen varios métodos esteganográficos que permiten ocultar información dentro de distintos tipos de medios digitales como imágenes, sonido y video, la cual pasa desapercibida por los usuarios, y al momento no existen procesos de seguridad en el análisis al enviar la imagen esteganografiada. Si bien es cierto existen diversas herramientas para ocultar información, la mayoría de ellas no incorporan mecanismos de seguridad que permitan encriptar el mensaje antes de ser ocultado fortaleciendo de esta manera la seguridad de la información en caso de que sea interceptada.

Varias investigaciones se enfocan en cifrar y ocultar mensajes utilizando diversas técnicas o métodos. Es de importancia citar algunas de relevancia:

Saini & Verma (2013) en la investigación "Securing multimedia colour imagery using multiple high dimensional chaos-based hybrid keys", proponen un método de cifrado eficiente para asegurar las imágenes en color multimedia. Se utilizan respuestas dinámicas complejas de múltiples sistemas caóticos de orden superior para llevar a cabo los procesos de barajado y difusión de los píxeles de imagen bajo el control de la clave secreta. Los resultados de la simulación validan que el método propuesto tiene un gran rendimiento de cifrado y practicabilidad.

Jung & Yoo (2014) , en su investigación proponen un método de ocultación de datos semi-reversible que utiliza la interpolación y la técnica de sustitución del bit 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. Los resultados de esta investigación destacan como ventaja la capacidad de transmitir gran cantidad de información manteniendo su alta calidad visual. Una de las desventajas es que no se pudo mejorar la seguridad durante la transmisión.

En la investigación realizada se evidencia que no se ha aplicado criptografía para mejorar la seguridad en la transmisión de información oculta en imágenes, por lo que en la presente investigación que tiene por objetivo el desarrollo de un método esteganográfico que incorpore técnicas criptográficas a fin de mejorar la seguridad de los mensajes transmitidos dentro de una imagen. A más de esto se pretende dar a conocer el campo de la esteganografía mediante el uso de software.

Dentro de los métodos esteganográficos, el más común es la ocultación de información dentro de imágenes digitales soportando varios formatos, mientras mayor resolución tenga la imagen se puede ocultar gran cantidad de datos logrando ser imperceptible al ojo humano. El método de Bit Menos Significativo (LSB), codifica un mensaje en bits y lo oculta en cada uno de los pixeles de la imagen portadora, pero una de sus debilidades son los ataques que han logrado detectar la presencia de información dentro de la imagen, pues este método se considera poco seguro (Jung & Yoo, 2014) , por lo que la propuesta incorpora César para la encriptación del mensaje dificultando el descifrado.

En el trabajo como primera fase se realizó un estudio de los métodos esteganográficos en imágenes, luego se realizó un estudio de algoritmos criptográficos como base para presentar la propuesta del método esteganográfico con criptografía implementado en una aplicación, también se presentan los resultados obtenidos y las conclusiones de la investigación.

1.1. Esteganografía

La esteganografía se encarga del estudio de un conjunto de métodos y técnicas para insertar un mensaje de forma segura dentro de un medio de multimedia como audio, video, imágenes y otros, de tal manera que dicha información solo pueda ser recuperada por un usuario legítimo que conozca el método determinado de extracción de la misma. (Perea, 2012)

Para el proceso esteganográfico se requiere el mensaje que se va a ocultar y el objeto para tapar el mensaje a enviar, que aplica una función estego (estego-función), que es algún tipo de método para que el mensaje pase desapercibido y luego viaje por un canal de transmisión inseguro, al llegar a su destino, el receptor aplica la estego-función y una clave esteganográfica (estego-clave), si lo tuviera para separar el camuflaje del mensaje oculto. (Iglesias, 2014)

Existen numerosos métodos y algoritmos utilizados para ocultar la información dentro de archivos multimedia, imágenes, audio y vídeo, que pueden ser de acuerdo al tipo de portador sobre el que actúan, el tipo de algoritmo en sí, por sus características y por el fin que persiguen. (Reza, 2017)

El método esteganográfico más común es el de ocultar información dentro de una imagen, estos se analizan exponiendo sus ventajas y desventajas como se describe en la Tabla 1.

Tabla 1
Ventajas y desventajas de
Métodos Esteganográficos

Método Esteganográfico	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 encargará 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 permiten 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.

Fuente: Elaboración propia [Autores]

Una vez analizadas las ventajas y desventajas de los métodos esteganográficos, se propone como base el método LSB, puesto que tiene una tasa de bits baja y no solamente se puede insertar en el último bit, sino que también permite la inserción en cualquier bit del byte, además en la complejidad computacional se logra mayor robustez con el nuevo método lo que le convierte en una fortaleza a la solución planteada.

1.2. Sustitución en LSB

En esteganografía existen diferentes métodos basados en la modificación de los bits menos significativos (LSB), esto consiste en tomar los pixeles de la imagen y hacer uso de los LSB de cado uno de ellos para incorporar el mensaje, alterándolos con el menor error posible, este método se puede aplicar a diferentes medios de multimedia como audio y video, aunque no es muy común. En imágenes la alteración es mínima, por no decir nula, pues el mensaje es insertado a lo largo de los pixeles de la imagen ya que se realiza en las áreas más ruidosas donde no atrae atención. (López, 2012)

1.3. Estegoanálisis

Así, cómo se debe realizar un proceso para incorporar la información a la imagen, también se debe realizar otro para obtener la información de ésta, entonces es necesario mencionar que es el estegoanálisis es una disciplina para descifrar mensajes ocultos por esteganografía, puede ser estegoanálisis manual que compara la imagen original y la imagen esteganografiada, pero el inconveniente es obtener la imagen original para realizar la comparación. Con el estegoanálisis estadístico se utiliza software especializado para comparar la frecuencia de distribución de colores en el caso de archivos de imágenes en donde se encuentra oculto el mensaje para ser descifrado. (Díaz, 2010)

En cuanto a los tipos de ataques contra la esteganografía la Tabla 2, presenta la clasificación que se puede considerar.

Tabla 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: Elaboración propia [Autores]

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. (García, 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 estegoanalísta 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): En este método, 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): El estegoanalísta oculta un mensaje utilizando un determinado algoritmo, se capturaran las firmas que deje el algoritmo, esto servirá como un patrón que permitirá detectar otras imágenes esteganografiadas con el mismo algoritmo.

Existen varias herramientas que permiten realizar estegoanálisis en imágenes, algunas de ellas se detallan a continuación: (Paz, 2014)

VSL (Laboratorio de Esteganografía Virtual). - Es una herramienta de diagramación compleja, contiene una interfaz sencilla de utilizar y está diseñada para ocultar imágenes digitales, también permite detectar mensajes ocultos dentro de una imagen.

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

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

1.4. Análisis de archivos de imágenes

En la Tabla 3, se presentan los formatos para imágenes más utilizados, con sus ventajas y desventajas, es importante mencionar que este estudio se realizó para probar en varios formatos el método propuesto. (Changir, 2017)

Tabla 3
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, que complica trabajar con esteganografía y la	La escasa paleta de colores

	capacidad de uso de transparencias.	
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

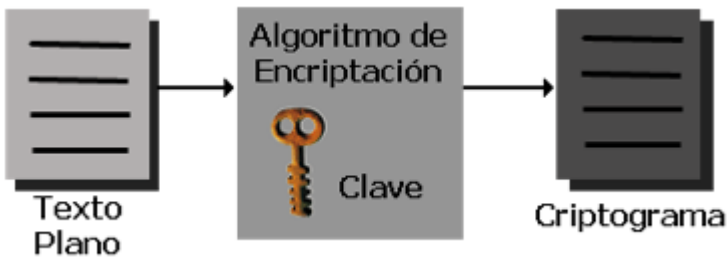
Fuente: Elaboración propia [Autores]

1.5. Criptografía

La Criptografía es el arte de escribir documentos mediante cifras o códigos secretos para proteger su confidencialidad contra ataques por personas que se dedican a interceptar, modificar, insertar información extra a la original, o el uso no autorizado de recursos de una red o sistemas informáticos evitando así que el intruso haga denegación de servicios. Su importancia radica, en que la información que lleva sea ilegible para la persona a la que no fue dirigida, pero de algún modo, el remitente pueda entenderla o descifrarla. (Galende, 1995)

La Figura 1, representa la forma como se encripta un mensaje en texto plano que se enviaría en la imagen esteganografiada, cumpliendo con el propósito de mejorar la seguridad del mensaje transmitido.

Figura 1
Proceso criptográfico sobre un texto plano



Fuente: Galende, 1995

Los métodos criptográficos pueden ser clásicos o modernos, los interés en este estudio son los clásicos que corresponden al conjunto de métodos que pueden ser por transposición o 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 por sustitución consiste en reemplazar las letras del mensaje original por otras. Según García (2004) algunas técnicas de cifrado por sustitución son: la matriz de Polibio, cifrado de Playfair y cifrado de César, este último presenta una simplicidad y compatibilidad con el método LSB.

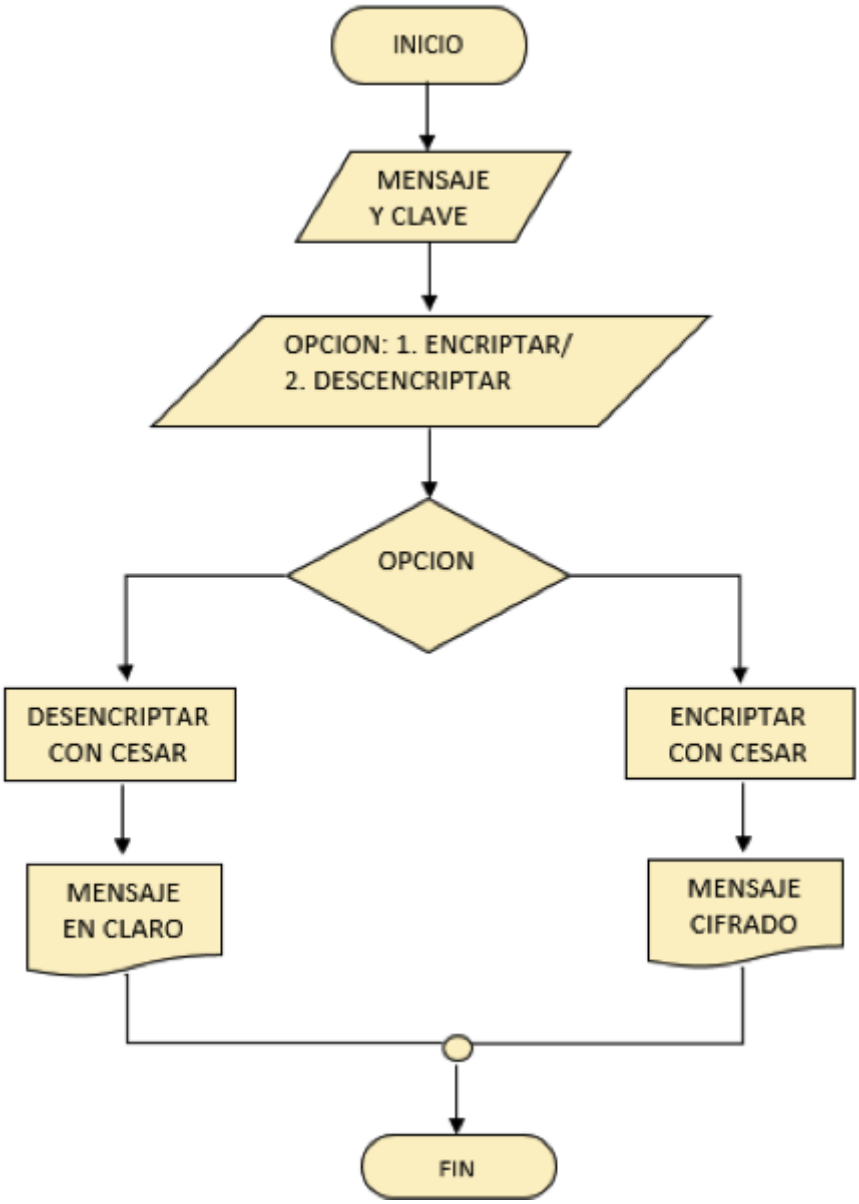
1.6. Cifrado de César

Esta técnica de cifrado es una de las más simples, el proceso consiste en mover cada letra del mensaje un determinado número de espacios en el alfabeto, logrando así un nuevo mensaje cifrado. Mientras mayor sea el número de espacios a recorrer en el alfabeto, mayor será el nivel de seguridad.

2. Metodología

Para mejorar el nivel de seguridad en la información se consideró implementar un nuevo procedimiento utilizando el método de César, pues existe un gran nivel de compatibilidad al momento de combinar con LSB, ya que no altera la imagen al momento que se inserta el mensaje encriptado. La Figura 2, ilustra el proceso de encriptación/desencriptación implementado con César para asegura el mensaje a ser transmitido.

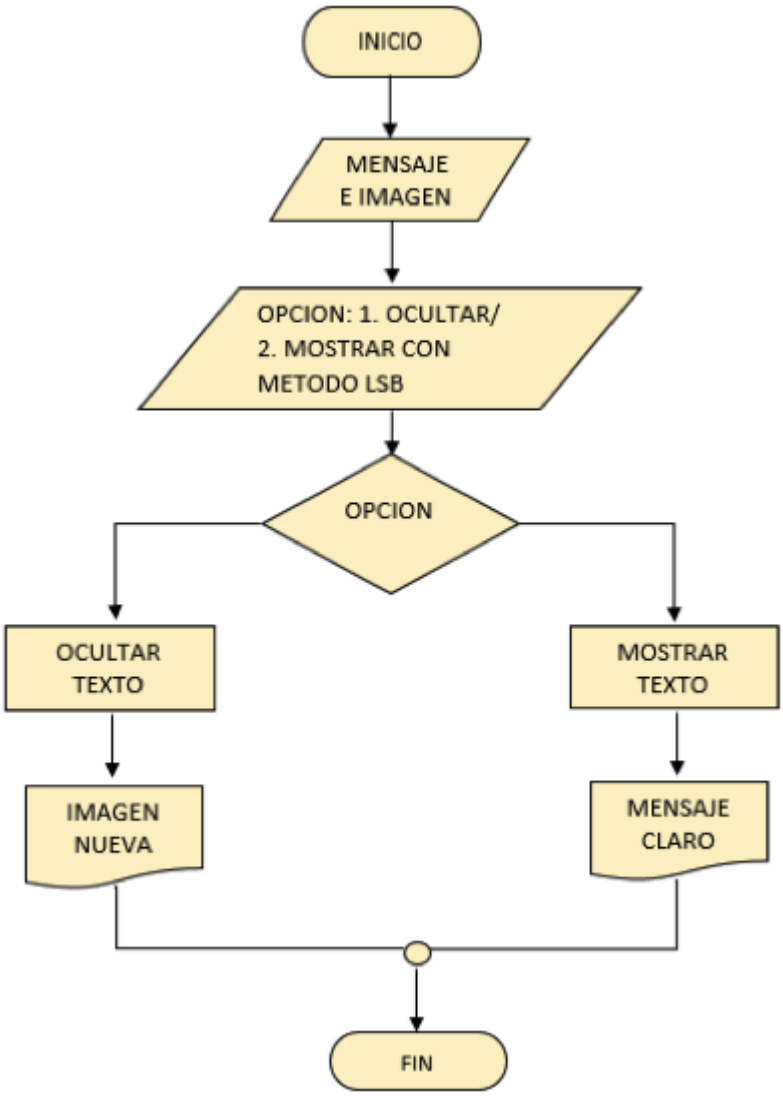
Figura 2
Diagrama de encriptación y desencriptación de mensaje



Fuente: Elaboración propia [Autores]

El proceso típico esteganográfico presenta las etapas de seleccionar la imagen o medio digital que servirá de portador, elaborar el mensaje o información que deseamos ocultar en el portador, ocultar el mensaje dentro de la imagen seleccionada y generar la nueva imagen o medio digital que contiene la información oculta. La Figura 3 muestra el diagrama de flujo para ocultar o mostrar el mensaje encriptado en una imagen utilizando LSB e integrarlo al mensaje encriptado.

Figura 3
Diagrama ocultar/mostrar
mensaje encriptado



Fuente: Elaboración propia [Autores]

En síntesis, para la propuesta de método se utilizó/obtuvo lo siguiente:

- Imagen base: imagen original en la que se insertará la información.
- Mensaje: información que se desea ocultar en la imagen.
- Número clave: elemento de seguridad para el proceso de encriptación del mensaje y que no pueda ser descifrada por terceros sin autorización.
- Algoritmo de César: proceso del algoritmo criptográfico.
- Algoritmo esteganográfico LSB (Bit Menos Significativo): sustitución del algoritmo LSB en los pixeles de la imagen con los bits de la información que va a ser insertada en la imagen.
- Imagen esteganografiada: fusión de la imagen base con la información oculta dentro de ella.

Para el proceso de ocultamiento se desarrolló una aplicación en Java en entorno gráfico de Netbeans integrando las herramientas y métodos seleccionados en el estudio, los parámetros más importantes requeridos al usuario antes del ocultamiento del mensaje en la imagen son: el número de desplazamientos a aplicar en el método de César, el mensaje que se desea enviar y la imagen portadora.

Para comparar las imágenes pixel a pixel se utilizó Guiffy Image Diff que permite determinar los cambios realizados en los componentes de cada pixel, para la verificación de la integridad de los datos se ejecutaron las herramientas HashMyFiles y FlexHEX, y para obtener el mensaje esteganografiado se utilizó la aplicación esteganografía básica disponible en la web.

Para validación de la propuesta, se tomó una muestra de 60 estudiantes de quinto semestre de la carrera de ingeniería en sistemas con conocimientos generales de criptografía. Se dividió en dos grupos de 30 estudiantes, uno para el grupo de control, el cual realizó la tarea de sustraer el mensaje sin el método propuesto y los otros 30 como el grupo experimental quienes realizaron la misma actividad con la propuesta de la investigación. Para ello se diseñó un conjunto de tareas y se les pidió a los sujetos de prueba que de una imagen con un mensaje oculto realizado con y sin el método propuesto extraiga el mensaje, los sujetos podían utilizar cualquier tipo de herramientas de criptoanálisis y estegoanálisis.

De acuerdo a esto, se estableció los niveles de seguridad, el nivel alto indica el número de estudiantes que no pudieron mostrar el mensaje en texto claro oculto dentro de la imagen por el lapso de más de 2 horas que duró la prueba, el nivel medio indica el número de estudiantes que lograron mostrar el mensaje claro en un tiempo de una hora y 45 minutos del tiempo que duró la prueba y el nivel bajo indica el número de estudiantes que mostraron el mensaje claro en un tiempo de una hora con 30 minutos.

2.1. Método propuesto

Antes de enviar el mensaje con el método propuesto, se ingresa el mensaje en la aplicación Esteganografía Básica, en el cual no existe ningún sistema de seguridad.

En la Figura 4 se presenta la interface desarrollada del método propuesto donde se integra LSB con el algoritmo César, también se puede observar los parámetros que se deben ingresar para este proceso.

De esta forma, se realiza el proceso de cifrado del mensaje original y posteriormente el proceso de embebido en la imagen.

Figura 4
Interface desarrollada de esteganografia con criptografia

Fuente: Elaboración propia [Autores]

3. Resultados

Al insertar la información en la imagen no se puede observar a simple vista la alteración realizada, cumpliendo con el principio de la esteganografía, por lo que se utiliza el programa Guiffy Image Diff para comparar pixel a pixel las imágenes (esteganografiada vs. Original), marcándose con color rojo los pixeles cuyos componentes fueron modificados con el algoritmo LSB, como se muestra en la Figura 5.

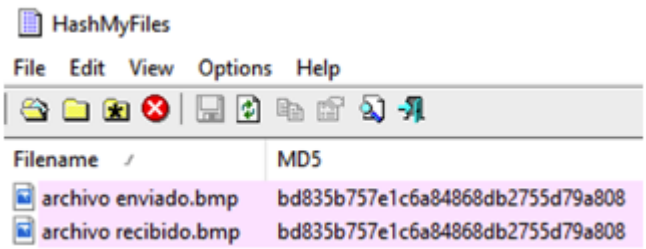
Figura 5
Pixeles modificados en la
imagen esteganografiada

Fuente: Elaboración propia [Autores]

3.1. Verificación de la integridad del mensaje transmitido con el método propuesto

Una vez receptado el mensaje se ejecutó el programa HashMyFiles para verificar el código MD5, que es un código único que tiene todo archivo para indicar si ha cambiado el momento de la transmisión. En la Figura 6 se puede observar que tanto el archivo del emisor como del receptor contiene el mismo MD5, por ende, el archivo no ha sufrido ningún cambio.

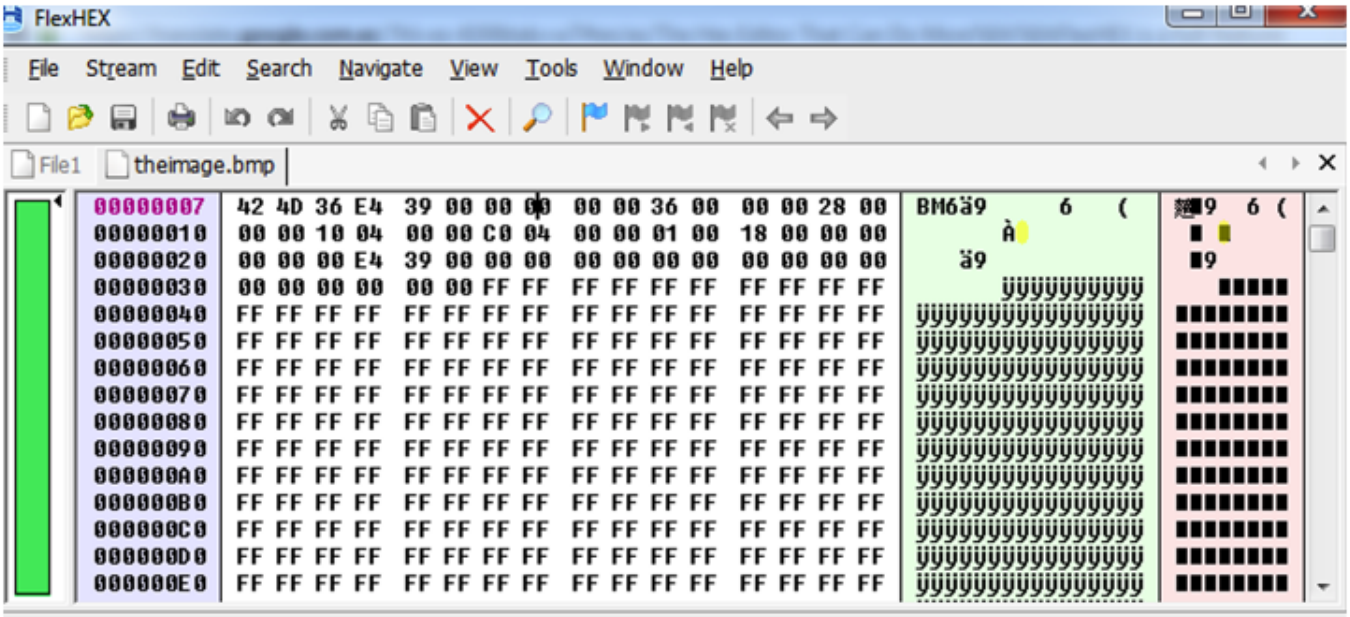
Figura 6
Verificacion de MD5



Fuente: Elaboración propia [Autores]

La herramienta FlexHEX permite visualizar el mensaje en código hexadecimal, comparando las dos imágenes para verificar su integridad, la Figura 7 muestra que debido a la encriptación no se puede identificar con facilidad el mensaje, dificultando la alteración del mismo y mejorando su seguridad.

Figura 7
Verificacion de integridad
del mensaje



Fuente: Elaboración propia [Autores]

3.2. Validación del método

Al finalizar las pruebas, del grupo de control un total de 30 estudiantes pudieron descifrar el mensaje, esto equivale a un nivel de seguridad bajo para preservar el mensaje oculto.

Los resultados obtenidos al aplicar el método esteganográfico con criptografía al grupo experimental se presentan en la Tabla 5, como se puede observar, 23 estudiantes no obtuvieron el mensaje, lo que representa el 76.67% de mejora en la seguridad respecto al grupo de control.

Tabla 5
Nivel de seguridad en el mensaje
con el método propuesto

Nivel Seguridad	Nº Estudiantes	Porcentaje de seguridad [%]
Alto	23	76.67
Medio	5	16.67
Bajo	2	6.66

Fuente: Elaboración propia [Autores]

4. Conclusiones

Del estudio se determinó al método esteganográfico LSB como base, ya que permite modificar cualquier bit del byte para ocultar el texto en la imagen y de los diversos algoritmos criptográficos existentes se seleccionó el cifrado de César por su gran compatibilidad con este, pues en las pruebas realizadas se observó que no hay cambios visibles en la imagen.

En el caso de este estudio el total del grupo de control pudo obtener el mensaje oculto de la imagen, y al realizar la misma tarea con la aplicación del método en el grupo experimental solo siete estudiantes pudieron descifrarlo, ya que se incrementa el nivel de seguridad en un 76.67%.

En el estudio se evidenció que de las herramientas esteganográficas disponibles, el método desarrollado mediante la aplicación web presenta la característica inusual para encriptación lo que le hace una herramienta confiable y robusta mejorando el nivel de seguridad en la transferencia de imágenes en cualquier formato.

Referencias bibliográficas

Changir, E. (2017). *Métodos de cifrado y políticas de seguridad*. Obtenido de http://loshermanosiutll.simplesite.com/

Díaz, J. (2010). Esteganografía y Estegoanálisis: Ocultación de Datos en streams de audio VORBIS. *Universidad Politécnica de Madrid*.

Galende, C. (1995). *La criptografía medieval*. Obtenido de http://pendientedemigracion.ucm.es/info/citechar/jornadas/II%20JORNADAS/jor02galende.pdf

García, D. (2004). *Análisis de herramientas esteganográficas*. Obtenido de Universidad Carlos III de Madrid: http://e-archivo.uc3m.es/bitstream/handle/10016/7119/PFC_David_Garcia_Cano_2004_201033204919.pdf?sequence=1

Iglesias, P. (2014). *#MundoHacker: Esteganografía, el arte de ocultar información sensible*. Obtenido de http://www.pabloyglesias.com/mundohacker-esteganografia/

Inteco. (2012). Obtenido de http://www.expresionbinaria.com/el-arte-de-ocultar-informacion-esteganografia/

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

López, M. (2012). *Esteganografía: para cifrar mensajes en imágenes.* Obtenido de https://www.unocero.com/2012/11/28/esteganografia-para-cifrar-mensajes-en-imagenes/

Paz, Á. (2014). *Herramienta para realizar técnicas de esteganografía y estegoanálisis.* Obtenido de http://www.gurudelainformatica.es/2014/08/herramienta-para-realizar-tecnicas-de.html

Perea, S. (2012). *Esteganografía: fotografías con firma invisibl.* Obtenido de http://www.xatakafoto.com/tutoriales/esteganografia-fotografias-con-firma-invisible

Reza, V. (2017). *Esteganografía.* Obtenido de https://prezi.com/8lp4ji-qayyu/esteganografia/

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

---

1. Profesor y profesional orientado a la Seguridad Informática. Ecuador. Escuela Superior Politécnica de Chimborazo. Ingeniero en Sistemas Informáticos. Magíster en Seguridad Telemática. rcuzco@espoch.edu.ec

2. Profesora y profesional orientada a la Seguridad Informática. Ecuador. Escuela Superior Politécnica de Chimborazo. Ingeniera en Electrónica y Computación. Magíster en Seguridad Telemática. carmen.mantilla@espoch.edu.ec

3. Profesor y profesional orientado a la Seguridad Informática. Ecuador. Universidad Nacional de Chimborazo. Ingeniero en Sistemas Informáticos. Magíster en Seguridad Telemática. pmendez@unach.edu.ec

4. Profesor y profesional orientado a Informática Aplicada. Ecuador. Escuela Superior Politécnica de Chimborazo. Ingeniero de Sistemas. Magíster en Informática Aplicada. diego.avila@espoch.edu.ec

---