Revista Ciencia UNEMI
Vol. 10, Nº 25, Diciembre 2017, pp. 134 - 147
ISSN 1390-4272 Impreso
ISSN 2528-7737 Electrónico

Evaluación de la propuesta algorítmica criptográfica con la incorporación de la esteganografía en imágenes

Pablo, Méndez-Naranjo[1*]; Andrés, Cisneros- Barahona[2]; Henry, Villa-Yánez[3]; Diego, Caiza- Méndez[4]

Resumen

El presente trabajo de tipo aplicativo, cuasi experimental, integró dos campos de la seguridad: la criptografía que cifra el mensaje y la esteganografía que oculta el mensaje tras un medio multimedia, lo cual fortalece el nivel de seguridad. El software utilizado para la investigación fue: *Netbeans* como ambiente de desarrollo, *Beyond Compare*, para comparar el código hexadecimal de las imágenes, Ion *Forge Image Diff* para comparar las diferencias entre imágenes pixel a pixel y Cyptool para las pruebas de criptoanálisis. El algoritmo criptográfico utilizado como base fue el AES (*Advanced Encryption Standard*) y para la técnica esteganográfica en imágenes se seleccionó LSB (*Least Significant Bit*). Se implementó y evaluó nuevas funciones que fueron incluidas en el Prototipo II, y se compararon los resultados obtenidos ejecutando criptoanálisis a los mensajes cifrados entre el Prototipo II que utiliza el nuevo algoritmo criptográfico denominado NAES y el Prototipo I que utiliza el algoritmo AES base, a los cuales se les incorporó la técnica esteganográfica en imágenes LSB. Se concluyó, que el nuevo algoritmo criptográfico NAES con la incorporación de la técnica LSB mejoró la seguridad, en comparación con el algoritmo criptográfico AES base, ya que el mensaje es más difuso.

Palabras Clave: Advanced Encryption Standard (AES); criptoanálisis; criptografía; esteganografía; Least Significant Bit (LSB); New Advanced Encryption Standard (NAES).

Evaluation of the cryptographic algorithmic proposal with the incorporation of steganography into images

Abstract

The present study was quasi experimental, applicative and integrated two fields of security: the cryptography that encrypts the message and the steganography that hides the message behind a multimedia medium, which strengthens the level of security. Netbeans was the software used for the research as a development environment, Beyond Compare to compare the hexadecimal code of the images, Ion Forge Image Diff to compare the differences between pixel to pixel images and Cyptool for the cryptanalysis tests. The AES (Advanced Encryption Standard) cryptographic algorithm was used as the basis and LSB (Least Significant Bit) was selected for the steganographic technique in images. New functions that were included in Prototype II were implemented and evaluated, and results obtained by running cryptanalysis were compared to the encrypted messages between Prototype II, that uses the new cryptographic algorithm named NAES, and Prototype I, that uses the AES base algorithm, to which incorporated the steganographic technique into LSB images. It was concluded that the new cryptographic algorithm NAES with the incorporation of the LSB technique improved the security, in comparison with the AES cryptographic algorithm, since the message is more diffuse.

Keywords: Advanced Encryption Standard (AES); cryptanalysis; cryptography; steganography; Least Significant Bit (LSB); New Advanced Encryption Standard (NAES).

Recibido: 18 de diciembre de 2016.
Aceptado: 1 de septiembre de 2016.

[1]Universidad Nacional de Chimborazo, Ecuador. pmendez@unach.edu.ec - https://orcid.org/0000-0002-3967-3718

[2]Vicerrectorado Académico de la Universidad Nacional de Chimborazo, Ecuador. ascisneros@unach.edu.ec

[3]Universidad Nacional de Chimborazo, Ecuador. villa@unach.edu.ec

[4]Consejo Nacional Electoral, Ecuador. diegomix07@hotmail.com

*Autor para correspondencia pmendez@unach.edu.ec

I. INTRODUCCIÓN

La seguridad en la transmisión de información, a través de canales inseguros, es de vital importancia en las comunicaciones, por lo que surge el término de seguridad informática, para brindar una mayor confianza de la información, ya que existen intrusos que desean acceder a ella para conocerla y/o utilizarla con propósitos maliciosos, por lo que se propone mejorar los algoritmos criptográficos y combinar sus fortalezas con las técnicas de esteganografía (Gaba y Kumar, 2013). La criptografía y la esteganografía son dos campos en la seguridad informática: la primera cifra el mensaje y la segunda oculta el mensaje tras un medio multimedia. (Segura y Díaz, 2014)

Al utilizar la criptografía y la esteganografía de forma separada existe la posibilidad que el intruso pueda distinguir el mensaje de origen, por lo que si se las fusiona se puede mejorar la privacidad y seguridad de la información (Sethi y Kapoor, 2016). El término criptografía proviene del griego kryptos (oculto) y graphos (escritura), lo que etimológicamente significa "escritura oculta"; es la ciencia que utilizando algoritmos específicos permite convertir los datos originales en criptogramas, que son enviados por un canal inseguro, en el que únicamente el destinatario puede descifrar los datos y obtener el mensaje original.

Los criptosistemas son muy útiles para proteger la información secreta, consiste en dos partes, la primera parte es el cifrado que convierte el mensaje original o datos en otra forma llamada forma cifrada, que no puede ser accesible por tercera persona en ausencia de información clave y la segunda parte es el descifrado que es el proceso de volcado de cifrado y convierte la información cifrada en forma original con la ayuda de información clave (Bukhari et al.., 2016).

Las principales propiedades de las que se ocupa la criptografía son: confidencialidad, integralidad, vinculación, autenticación (Saini y Verma, 2013).

El algoritmo Advanced Encryption Standard (AES) es un tipo de criptografía simétrica que usa la misma clave (128 bits, 192 bits o 256 bits) para el cifrado y descifrado, por lo que el receptor debe conocer la clave con la que fue cifrado el mensaje para poder descrifrarlo y obtener el mensaje original (Nurhayati y Ahmad, 2015). AES tiene 10 rondas para llaves de 128 bits, 12 rondas para llaves de 192 bits y 14 rondas para llaves de 256 bits (Ferguson et al.., 2000)

El criptoanálisis es un proceso para encontrar fallas en algoritmos criptográficos y usar estas debilidades, para descifrar el texto cifrado sin conocer la clave secreta (Comunidad OWASP, 2009). Por otro lado, el criptoanálisis se realiza al proceso criptográfico y se considera roto el criptosistema cuando se descifra el mensaje.

El término esteganografía proviene del griego steganos (cubierto) y graphos (escritura), lo que etimológicamente significa "escritura cubierta", es la ciencia de ocultar información con técnicas específicas dentro de un archivo multimedia, evitando la revelación de la información oculta para que pasen inadvertidos, el emisor embebe el mensaje en el archivo multimedia y el receptor lo extrae para obtener el mensaje oculto. (Saini y Verma, 2013). Con el fin de lograr una transmisión en cubierto entre el remitente y destinatario; ayuda a potenciar la seguridad informática ya que puede ser usada por instituciones policiales, militares y de inteligencia. En la esteganografía se puede utilizar como portador varios tipos de archivos, los más comunes son las imágenes, audios y videos.

Al momento de realizar el proceso estenográfico se destacan tres parámetros fundamentales son la capacidad, la imperceptibilidad y robustez (Jabbar et al.., 2013) los cuales permitirán tener una técnica eficiente al momento de ocultar información y cumplir con la idea fundamental de la esteganografía, la cual es poder enviar información de una manera imperceptible entre el emisor y receptor. (Rodríguez et al., 2014). En el presente trabajo de investigación se ha utilizado una imagen de tipo mapa de bit (BMP).

Existen varias técnicas utilizadas para ocultar la información dentro de archivos multimedia como: documentos, imágenes, audio, vídeo, otros, por ejemplo: basada en paleta de colores, técnica de sustitución LSB (Bit Menos Significativo), basada en coeficientes .JPEG, entre otros (Muñoz, 2014).

El presente trabajo de tipo aplicativo, cuasi experimental, integró dos campos de la seguridad informática: la criptografía que cifra el mensaje y la esteganografía que oculta el mensaje tras un medio multimedia. Aplicando el nuevo algoritmo criptográfico AES e integrando la esteganografía en imágenes, se presenta el proceso de cifrado y embebido con el Prototipo I y Prototipo II y realiza una comparación.

II. DESARROLLO

1. Estado del Arte

En investigaciones previas, se realizan propuestas de integración de la criptografía con la esteganografía:

Saini y Verma (2013), mencionan que debido a la necesidad que existe de asegurar la información antes de que sea transmitida, existen varios algoritmos de criptografía que han sido desarrollados para cumplir este fin. En la investigación, primero cifra la imagen con una nueva versión del algoritmo criptográfico y lo combina con la esteganografía para mejorar el nivel de seguridad contra posibles ataques.

Gaba y Kumar (2013), dan cuenta que debido al crecimiento de las redes y el avance de la tecnología es necesario incrementar la complejidad en la protección de información para que tengan seguridad, para lo que existen dos grandes áreas: la criptografía y la esteganografía. La criptografía altera la estructura de los datos y la esteganografía oculta la información detrás de un medio multimedia. Además, utilizan el algoritmo criptográfico CES para el intercambio de información usando la técnica de pre proceso que comprende reducir el tamaño del texto y luego alterarlo utilizando una clave, lo que permite ocultar una mayor cantidad de información con técnicas esteganográficas para proteger la misma.

Kumar et al.. (2013), aluden que debido a la evolución de las tecnologías de internet y sus aplicaciones requieren de un alto nivel de seguridad en los datos sobre canales de comunicación. La esteganografía en imágenes es una técnica digital para ocultar información atrás de una imagen. La técnica del Bit Menos Significativo (Least Significant Bit - LSB), es una de las más populares debido a su capacidad y alta capacidad de ocultación. Las técnicas esteganográficas se basan en estrategias de embebido con menos consideraciones para el pre procesamiento, sin embargo, el algoritmo original no provee el pre procesamiento requerido para una mayor seguridad, no ofrecen flexibilidad, robustez y alto nivel de seguridad. Se plantea una técnica de esteganografía en imágenes basado en DES (Data Encryption Standard) usando la fortaleza de mapeo s-box y clave secreta.

Sharma y Srivastava (2017), utilizan la criptografía y esteganografía, en la primera etapa utilizan el algoritmo AES y luego ocultan sus resultados con la ayuda de Haar Discrete Wavelet Transform y alpha blending para que exista una mayor imperceptibilidad y confiabilidad en la información, la implementación la realizan en MATLAB.

Manjula y Shivakumar (2016), el mensaje se cifra primero con el algoritmo criptográfico simétrico AES y se codifica mediante el método de criptografía pública Eliptical Curve Cryptography (ECC), este doble cifrado de datos se comprime con Lempel Ziv Welch (LZW) técnica para reducir la capacidad de residencia de datos secretos, combinando la criptografía simétrica y la asimétrica el resultado es más resistente a los ataques visuales y estadísticos.

Nurhayati y Ahmad (2016), diseñó una aplicación que utiliza la técnica del Bit Menos Significativo (LSB) del mensaje cifrado con el algoritmo AES, por lo que el mensaje no es fácil de entender a terceras personas no autorizadas, mejorando la seguridad de la información al combinar la criptografía y la esteganografía.

2. Metodología

Materiales y Métodos

La presente investigación puede clasificarse de dos tipos: aplicativa y experimental. El diseño es del tipo cuasi experimental, ya que se escogió el algoritmo criptográfico que fue utilizado como base para la creación del nuevo algoritmo criptográfico, al cual se incorporó la esteganografía en imágenes para mejorar la seguridad, además los datos de prueba fueron generados por el autor de esta investigación. Se utilizó el método científico, de acuerdo a ello el trabajo consta de varias etapas, tratadas de manera sistemática y coherente, para obtener un conocimiento válido desde el punto de vista científico.

Los instrumentos utilizados fueron: Netbeans (Netbeans, 2016) como IDE de desarrollo, Beyond Compare (Scooter Software, 2016) para comparar de forma visual las diferencias en el código hexadecimal de las imágenes, IonForge ImageDiff (ionForge, 2014) para comparar de forma visual las diferencias pixel a pixel de las imágenes esteganografiadas. Además, Cryptool (Cryptool, 2015) con el objetivo de realizar pruebas de criptoanálisis a los mensajes cifrados.

Algoritmo criptográfico base

Se realizó la búsqueda de información de estudios

primarios acerca de los algoritmos criptográficos simétricos más utilizados y se procedió a seleccionar los algoritmos simétricos o de clave privada debido a sus características. En base a la comparación realizada en la investigación de Mathur y Kerwani (2013), donde comparan las características de los algoritmos con base a: tipo de cifrado, tipo de clave, longitud de la clave, tamaño de bloque, número de rondas, seguridad, resistencia a criptoanálisis, tiempo requerido para determinar todas las posibles claves (con 50 billones de claves por segundo), para lo que se estableció que el algoritmo criptográfico simétrico AES es el más adecuado, debido a sus ventajas en relación a los otros algoritmos, además permite utilizar claves de 128 bits, 192 bits y 256 bits (Méndez, 2016)

Entre las principales ventajas del algoritmo criptográfico seleccionado se mencionan: tamaño de bloque variable, número de rondas depende de la clave que se utilice, es resistente al criptoanálisis diferencial, truncado diferencial, lineal, por lo que es una de las principales ventajas en comparación con los otros, el tiempo requerido para determinar todas las posibles claves (con 50 billones de claves por segundo) es mucho mayor, por lo que lo hace más seguro y resistente en comparación con los otros. Esto justificó su utilización como base para la elaboración e implementación del nuevo algoritmo criptográfico, a los cuales se incorpora la esteganografía en imágenes.

Determinación de la técnica esteganográfica

Luego de realizar la búsqueda de información de estudios primarios acerca de los algoritmos esteganográficos más utilizados, se procedió a seleccionar la técnica Least Significant Bit (LSB) debido a sus características: sencillo de implementar, rápido, utiliza menos recursos, minimiza la variación en los colores, distorsión de la imagen se mantienen al mínimo, no varía el tamaño de la imagen, puede utilizarse en imágenes a color y escala de grises.

Implementación del algoritmo criptográfico base

Esta parte sirvió para el desarrollo de la aplicación del algoritmo criptográfico AES base, el proceso de cifrado y descifrado con las funciones definidas: AddroundKey, SubByte, MixColumns, ShiftRows.

Creación e implementación del nuevo algoritmo criptográfico

Para la creación del nuevo algoritmo criptográfico se consideró el algoritmo AES como base y denominó NAES. Para mejorar la seguridad e incrementar la difusión del mensaje, se propuso las siguientes mejoras en el algoritmo criptográfico, modificando las principales funciones que proporcionan la principal fuente de difusión en el cifrado AES:

Función 1: AddRowRoundKey

Utilizar una nueva función ADDROWROUNDKEY, que se ejecuta en la ronda inicial en lugar de la función ADDROUNDKEY, en la cual los cuatro bytes de cada fila se realizan un $\oplus$ (or exclusivo XOR) con cada columna de la subclave calculada de la ronda, durante el cálculo de subclaves. Como se muestra en la Figura 1.

Función 2: MixRows

Utilizar una nueva función MIXROWS, en la cual los cuatro bytes de cada fila son multiplicados dentro del Campo de Galois por una determinada matriz. Como se muestra en la Figura 2.

Función 3: ShiftColumns

Utilizar una nueva función SHIFTCOLUMNS, en la cual se realizó un desplazamiento hacia arriba, cíclicamente, de las columnas que conforman la matriz de estado actual. Cada columna se desplazó un número de posiciones diferentes. Como se muestra en la Figura 3, los bytes en cada columna del Estado son rotados de manera cíclica hacia arriba. El número de lugares que cada byte es rotado difiere para cada columna:

- La primera columna no sufre cambio
- La segunda columna rota hacia arriba una posición
- La tercera columna rota hacia arriba dos posiciones
- La cuarta columna rota hacia arriba tres posiciones

En la Figura 3 se muestra la función ShiftColumns propuesta.

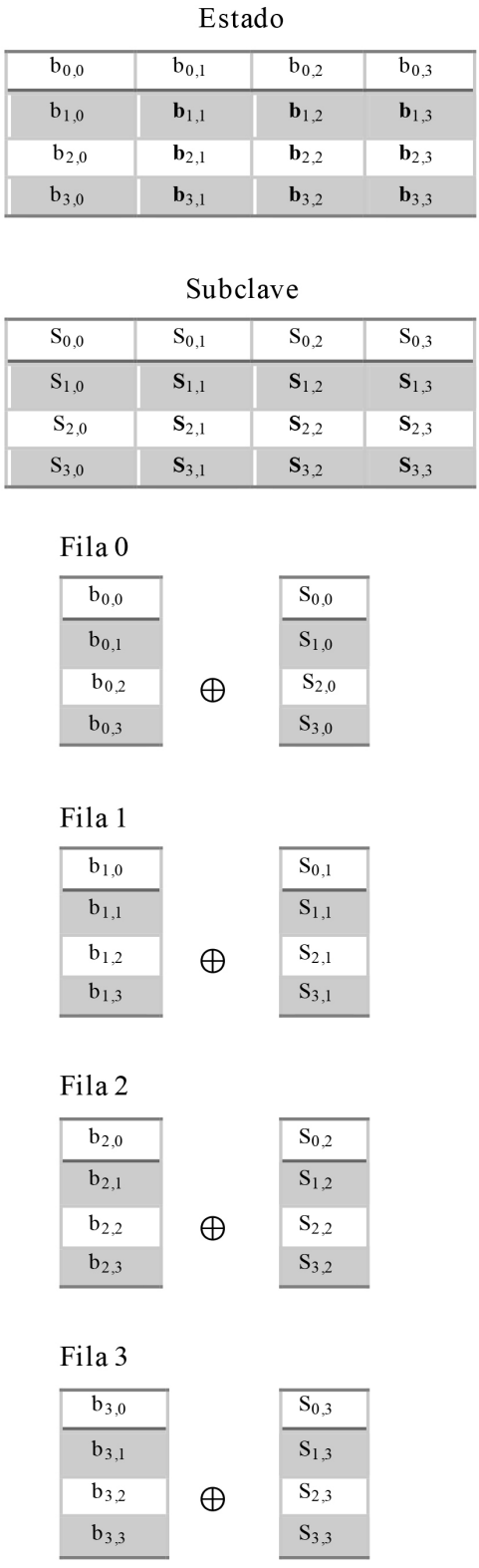

Figura 1. Función AddRowRoundKey

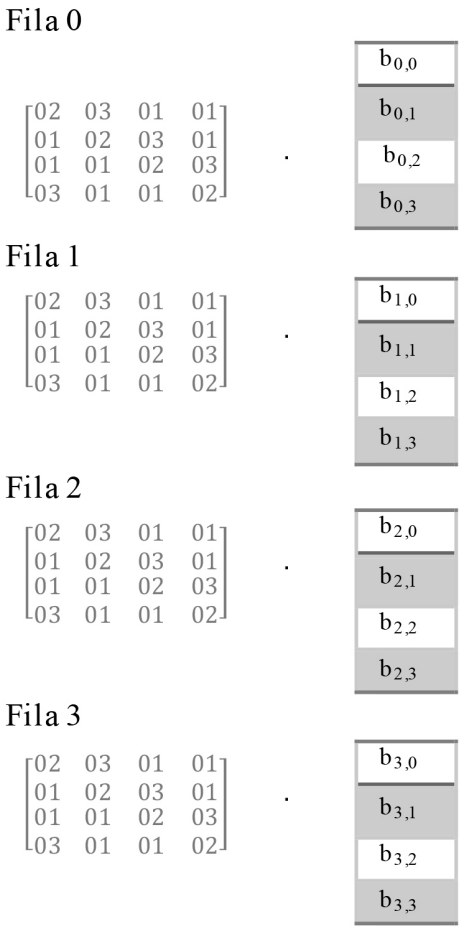

Figura 2. Función MixRows

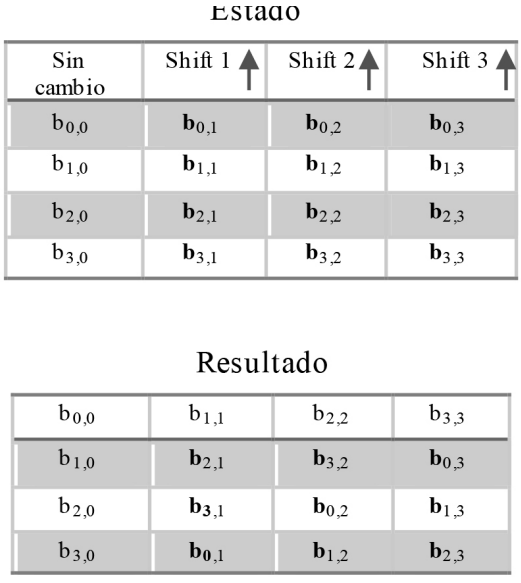

Figura 3. Función ShiftColumns

Se procedió con el desarrollo de la aplicación del nuevo algoritmo criptográfico NAES, cuyo proceso de cifrado y descifrado se muestra en la Figura 4 y Figura 5, de acuerdo con el número de rondas (Nr).

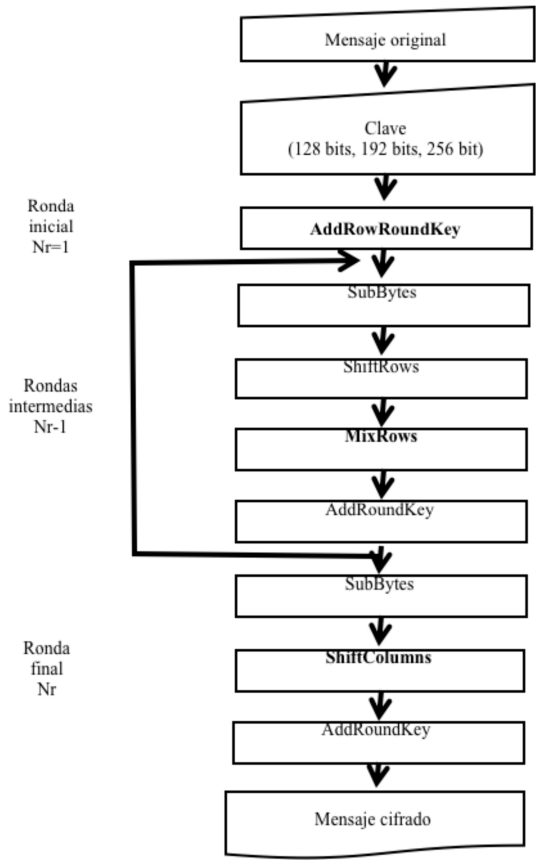

Figura 4. Proceso de cifrado y embebido NAES

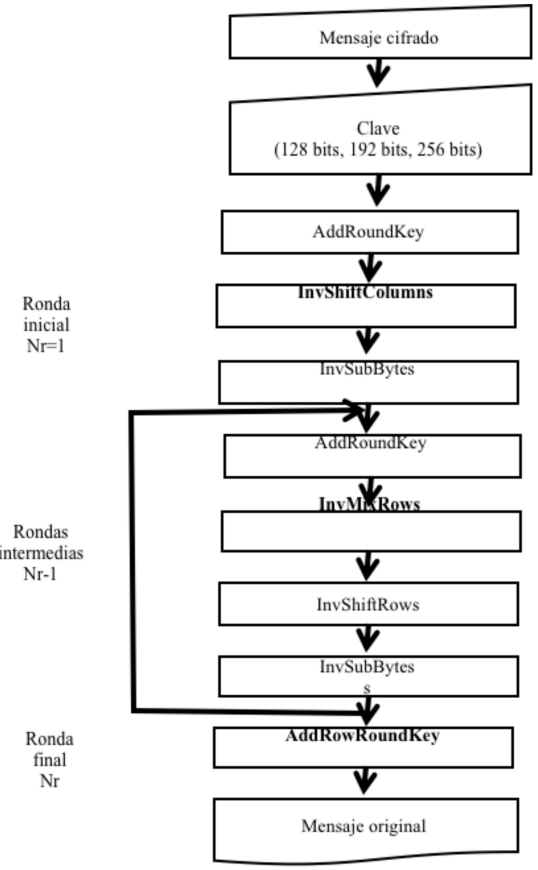

Figura 5. Proceso de extracción y descifrado NAES

Implementación del algoritmo esteganográfico en imágenes

Se procedió con el desarrollo de la aplicación de la técnica esteganográfica LSB, para el proceso de embebido y extracción del mensaje.

Integración de los algoritmos criptográficos y esteganográficos

Prototipo I

Para el Prototipo I se integró la aplicación con el algoritmo criptográfico que es considerado como base y la integración esteganográfica en imágenes. Se implementó el algoritmo AES base con sus funciones: AddRoundKey, SubBytes, ShiftRows, MixColumns. Al algoritmo criptográfico AES base se incorporó la esteganografía en imágenes, con la técnica de LSB.

Se procedió con el desarrollo de la aplicación del Prototipo I, cuyo proceso de cifrado y embebido se resume en la Figura 6 y el proceso de extracción y descifrado en la Figura 7, de acuerdo al número de rondas (Nr).

Prototipo II

Para el Prototipo II se integró la aplicación con el nuevo algoritmo criptográfico y la integración esteganográfica en imágenes. Se implementó el nuevo algoritmo NAES con sus funciones: AddRoundKey, AddRowRoundKey (nueva función), SubBytes, ShiftRows, ShiftColumns (nueva función), MixColumns, MixRows (nueva función). Al algoritmo criptográfico NAES se incorporó esteganografía en imágenes con la técnica de LSB. Se procedió con el desarrollo de la aplicación del Prototipo II, cuyo proceso de cifrado y embebido se resume en la Figura 8 y proceso de extracción y descifrado en la Figura 9, de acuerdo al número de rondas (Nr).

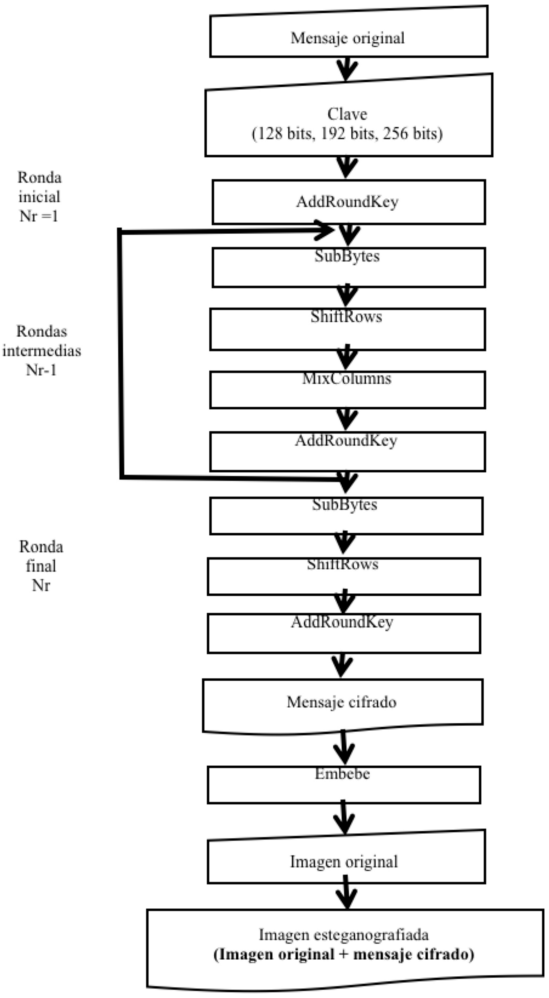

Figura 6. Proceso de cifrado y embebido P. I

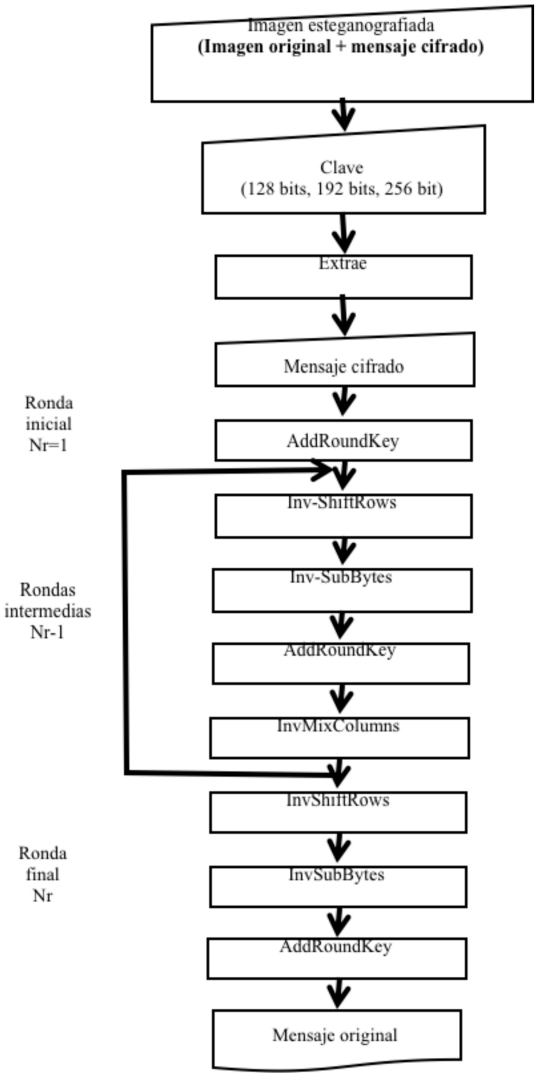

Figura 7. Proceso de extracción y descifrado P. I

Ambiente de pruebas

Se establece un ambiente de pruebas común en el que comparten los escenarios para el cifrado/embebido y extracción/descifrado. Las condiciones del ambiente de pruebas para los dos escenarios fueron: Utilización de tamaños de clave de 128 bits, 192 bits, 256 bits. Tamaños de bloque de 128 bits. Utilización de imágenes BMP.

Escenarios

En el ambiente de pruebas se definieron dos escenarios:

- Escenario 1: En el primer escenario se utilizó el Prototipo I (algoritmo criptográfico AES, con la incorporación de la esteganografía en imágenes utilizando el método LSB).
- Escenario 2: En el segundo escenario se utilizó el Prototipo II (nuevo algoritmo criptográfico desarrollado NAES, con la incorporación de la esteganografía en imágenes utilizando el método LSB).

3. Resultados

Cifrado y embebido

Para probar el proceso de cifrado y embebido con el Prototipo I y Prototipo II desarrollados, con claves de 128 bits, 192 bits y 256 bits, se utilizaron los datos de la Tabla 1.

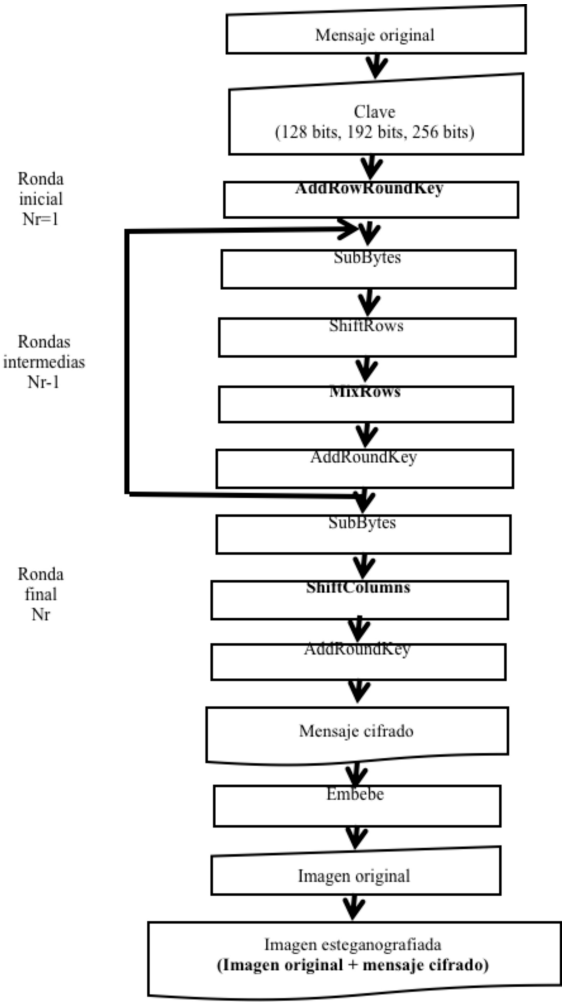

Figura 8. Proceso de cifrado y embebido P. II

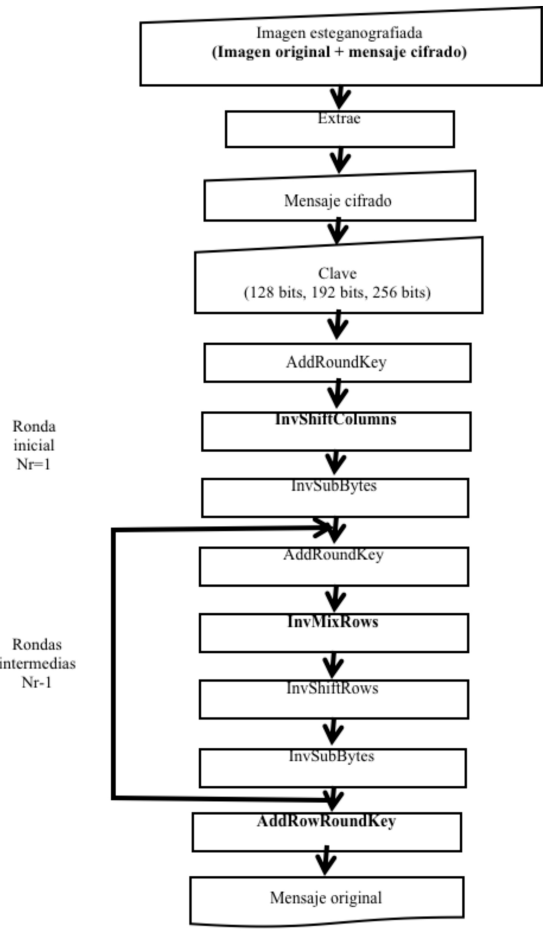

Figura 9. Proceso de extracción y descifrado P. II

Tabla 1. Datos para ejecución de cifrado y embebido

Datos para ejecución de cifrado y embebido	
Clave (128 bits):	kW]Ld5$\|E@Q^$iq"
Clave (192 bits):	kW]Ld5$\|E@Q^$iq"kW]Ld5$|
Clave (256 bits):	kW]Ld5$\|E@Q^$iq"kW]Ld5$\|E@Q^$iq"
Mensaje:	La esteganografía trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia. Es decir, procura ocultar mensajes dentro de otros objetos y de esta forma establecer un canal encubierto de comunicación, de modo que el propio acto de la comunicación pase inadvertido para observadores que tienen acceso a ese canal. Y la criptografía se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

Comparación de resultados criptográficos

Se compararon los mensajes cifrados que fueron generados con el Prototipo I y con el Prototipo II con claves de 128 bits, 192 bits y 256 bits, los cuales se muestran en la Tabla 2.

Tabla 2. Comparación de mensajes cifrados con Prototipo I y Prototipo II

Comparación de mensajes cifrados con Prototipo I y Prototipo II		
Clave	**Prototipo I**	**Prototipo II**
128 bits		
192 bits		
256 bits		

Comparación de resultados esteganográficos

Se compararon las imágenes "Original.bmp" y "Final.bmp", utilizada y generada por el Prototipo I y Prototipo II con claves de 128 bits, 192 bits y 254 bits, en las cuales no se puede apreciar una diferencia a simple vista, como se muestra en las Figura 10 y Figura. 11.

Figura 10. Imagen "Original.bmp"

Figura 11. Imagen "Final.bmp"

Se compararon los tamaños de las imágenes "Original.bmp "Final.bmp", con el Prototipo I y Prototipo II con claves de 128 bits, 192 bits y 256 bits, demostrando que con la técnica esteganográfica LSB no existe variación de las mismas, como se muestra en la Tabla 3.

Tabla 3. Tamaños de las imágenes

Tamaños de las imágenes			
Nombre de Imagen	**Tamaño (bytes)**	**Tamaño en disco (bytes)**	**Tamaño (MB)**
Original.bmp	4.305.654	4.305.992	4,10
Final.bmp	4.305.654	4.305.992	4,10

Se utilizó el programa Beyond Compare, para determinar el código hexadecimal de las imágenes "Original.bmp" y "Final.bmp", utilizada y generadas por el Prototipo I y Prototipo II con claves de 128 bits, 192 bits y 256 bits. Al comparar los dos archivos hexadecimales de la imagen original "Original.bmp" y la imagen esteganografiada "Final.bmp" generada por el Prototipo I y II con claves de 128 bits, 192 bits y 256 bits, se determinó diferencias marcadas con color rojo, como se muestra en la Figura 12.

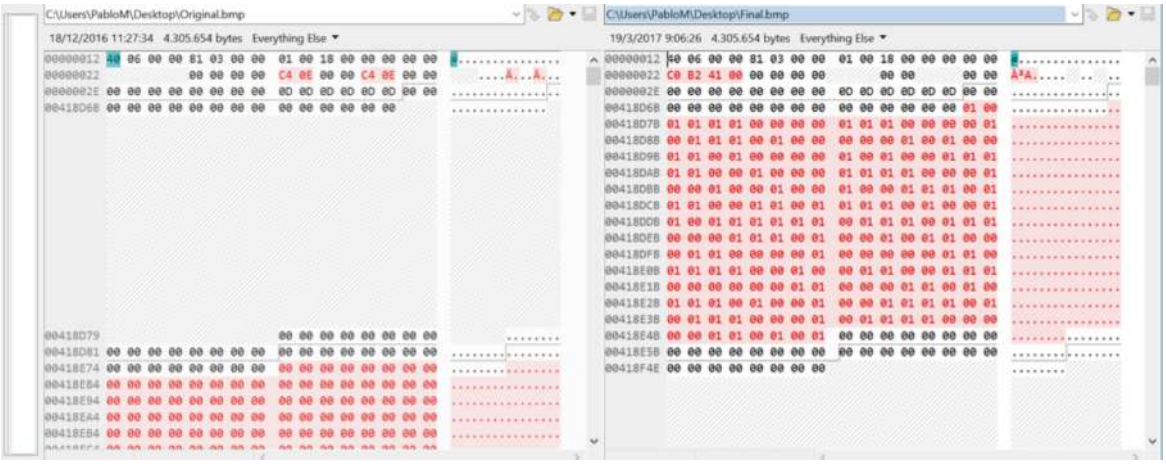

Figura 12. Comparación de código hexadecimal de las imágenes

Se utilizó el programa ionForge imageDiff para comparar las dos imágenes y comprobar que la información del mensaje cifrado con claves de 128 bits, 192 bits y 256 bits con el Prototipo I y Prototipo II, se encuentra dentro de la imagen esteganografiada. Luego de comparar las imágenes, se evidenció la diferencia de los pixeles modificados que corresponden al 0,10%, los cuales son representados con color rojo en la parte superior de la imagen, como se muestra en la Figura 13.

Figura 13. Diferencia en los pixeles entre las imágenes comparadas

Pruebas

Para la comprobación de la hipótesis se realizaron las pruebas en base al criptoanálisis de los mensajes cifrados con el algoritmo AES base implementado en el Prototipo I y del nuevo algoritmo desarrollado NAES implementado en el Prototipo II, para 4 indicadores de la variable dependiente (seguridad): Entropía, Histograma, Autocorrelación, Fuerza bruta.

Ambiente de pruebas

Se comparó el algoritmo AES base implementado en el Prototipo I y el nuevo algoritmo NAES implementado en el Prototipo II, para los siguientes indicadores de la variable dependiente definida: entropía, histograma, autocorrelación, fuerza bruta.

Se realizó el criptoanálisis utilizando la herramienta Cryptool se compararon los mensajes cifrados con llaves de 128 bits, 192 bits y 256 bits por: Algoritmo criptográfico AES base implementado en el Prototipo I, Algoritmo criptográfico NAES implementado en el Prototipo II. Para las pruebas realizadas de criptoanálisis se utilizó un alfabeto extendido de 98 caracteres que incluyó: letras mayúsculas, letras minúsculas, espacios, números, puntuación, diéresis, para lo cual se configuran las opciones de texto en el programa Cryptool.

Criptoanálisis

Los resultados de las pruebas de criptoanálisis realizado a los indicadores se muestran a continuación:

Indicador 1: Entropía

Se realizaron las pruebas de entropía para determinar el nivel de difusión existente en los mensajes cifrados con el Prototipo I y Prototipo II con claves de 128 bits, 192 bits y 256 bits, como se muestra en la Tabla 4.

Tabla 4. Caracteres diferentes y valores de entropía de mensajes cifrados

Caracteres diferentes y valores de entropía de mensajes cifrados				
Clave	**Algoritmo**	**Caracteres diferentes**	**Entropía máxima**	**Valor**
128 bits	Prototipo I	89	6,61	6,26
	Prototipo II	90	6,61	6,28
192 bits	Prototipo I	87	6,61	6,24
	Prototipo II	86	6,61	6,24
256 bits	Prototipo I	89	6,61	6,25
	Prototipo II	92	6,61	6,30

Como se puede observar, en la Tabla 4, la entropía que representa el nivel de desorden del mensaje es más alto en el Prototipo II en comparación con el Prototipo I, el nivel de entropía es directamente proporcional a la seguridad, mientras mayor es el nivel de entropía más seguro es el mensaje cifrado debido a que es más difuso.

Indicador 2: Histogramas

Se realizaron las pruebas de histograma que relacionan el porcentaje de frecuencia con los valores contenidos en los mensajes cifrados con el Prototipo I y Prototipo II con claves de 128 bits, 192 bits y 256 bits, como se muestra en la Tabla 5.

Tabla 5. Número de caracteres del histograma de los mensajes cifrados

Número de caracteres del histograma de los mensajes cifrados		
Clave	**Algoritmo**	**Caracteres**
128 bits	Prototipo I	254
	Prototipo II	221
192 bits	Prototipo I	215
	Prototipo II	244
256 bits	Prototipo I	236
	Prototipo II	267

Como se puede observar, la cantidad de caracteres en el histograma en mayor en el Prototipo II en comparación con el Prototipo I, por lo que el mensaje en más variado.

Indicador 3: Autocorrelación

Se realizaron las pruebas de correlación que relacionan el número de caracteres que concuerdan en relación al desplazamiento de los mensajes cifrados con el Prototipo I y Prototipo II con claves de 128 bits, 192 bits y 256 bits, como se muestra en la Tabla 6.

Tabla 6. Número de caracteres que concuerdan en la correlación

Número de caracteres que concuerdan en la correlación		
Clave	**Algoritmo**	**Caracteres que concuerdan**
128 bits	Prototipo I	6
	Prototipo II	6
192 bits	Prototipo I	5
	Prototipo II	7
256 bits	Prototipo I	5
	Prototipo II	11

Como se puede observar, existe una mayor cantidad de caracteres que concuerdan en el Prototipo II en comparación con el Prototipo I, por lo que el mensaje tiene mayor variedad en su combinación.

Indicador 4: Fuerza bruta

Se realizaron las pruebas de fuerza bruta, que se basa en probar todas las combinaciones posibles de la clave, para determinar los mensajes cifrados con el Prototipo I y Prototipo II con claves de 128 bits, 192 bits y 256 bits, como se muestra en la Tabla 7.

Tabla 7. Número de caracteres del histograma de los mensajes cifrados

Número de caracteres del histograma de los mensajes cifrados		
Clave	**Algoritmo**	**Tiempo descifrar (años)**
128 bits	Prototipo I	$2{,}0x10^{25}$
	Prototipo II	$2{,}1x10^{25}$
192 bits	Prototipo I	$4{,}0x10^{44}$
	Prototipo II	$4{,}4x10^{44}$
256 bits	Prototipo I	$9{,}3x10^{63}$
	Prototipo II	$9{,}8x10^{63}$

Como se puede observar, los tiempos para determinar la clave por fuerza bruta son muy altos en el Prototipo II en comparación con el Prototipo I, por lo que es más seguro.

Comparando los resultados obtenidos en la presente investigación, con la de otros autores que han realizado investigaciones previas acerca de este tema, se menciona:

- Se propone la integración de nuevas funciones que se integran en las rondas del algoritmo, lo cual permite mayor difusión en el mensaje y se realizan pruebas comparativas de las características de los algoritmos y utilizando claves de 128 bits, 256 y 512 bits.
- Se realiza la comparación pixel a pixel y en base al código hexadecimal de las imágenes originales con las esteganografiadas, para determinar los cambios realizados.
- Se utiliza criptoanálisis para los mensajes cifrados por los prototipos I y II, para verificar que la propuesta realizada mejora la seguridad.

III. CONCLUSIONES

- Se utilizó el algoritmo criptográfico AES, debido a que es el más adecuado por sus ventajas, permite utilizar claves de 128 bits, 192 bits y 256 bits, tamaños del bloque variables, número de rondas variables, resistente al criptoanálisis diferencial, truncado diferencial, lineal y posee fortaleza contra fuerza bruta, por lo que es más seguro y resistente.
- De las técnicas esteganográficas existentes en la actualidad, se seleccionó la técnica esteganográfica LSB en imágenes debido a que es una de las más utilizadas por sus ventajas porque es sencilla de implementar, rápida, utiliza menos recursos, minimiza la variación en los colores que se crea la incrustación, la distorsión de la imagen se mantiene al mínimo y puede utilizarse en imágenes a color y escala de grises.
- Con la incorporación de las funciones propuestas en las rondas del algoritmo, el mensaje cifrado

se difuminó más en comparación con el algoritmo AES base, demostrando así que es más seguro.

- Los mensajes cifrados con el Prototipo II poseen mayor entropía, utilizan mayor cantidad de caracteres y se requiere un mayor tiempo para obtener la clave y con ella el mensaje original utilizando fuerza bruta, en comparación a los mensajes cifrados con el Prototipo I.
- Para trabajos futuros de investigación se podría considerar para el proceso de cifrado el uso de diferentes tamaños de bloque para las claves, modificar el orden de las funciones establecidas o incorporar nuevas funciones en las diferentes rondas del algoritmo con la finalidad de obtener nuevos resultados con mensajes más difusos. Se pueden utilizar o combinar técnicas esteganográficas para embeber la información cifrada en elementos multimedia que pasen desapercibidos, mejorando la seguridad de la información.

IV. REFERENCIAS

Bukhari, S., Shoaib, M., Anjum, M., y Dilbar, S. (2016). *Enhancing security of images by Steganography and Cryptography techniques*. Innovative Computing Technology (INTECH) p. 531-534. IEEE.

Comunidad OWASP. (2009). *Cryptanalysis*. Obtenido de https://www.owasp.org/index.php/Cryptanalysis

Cryptool. (2015). *About CrypTool* 1. Obtenido de https://www.cryptool.org/en/cryptool1

Ferguson, N., Kelsey, J., Lucks, S., Schneier, B., Stay, M., Wagnew, D., y Whiting, D. (2000). Improved Cryptanalysis of Rijndael. FSE 2000, p. 213–230.

Gaba, J., y Kumar, M. (2013). Implementation of steganography using CES technique. IEEE Second International Conference on Image Information Processing (ICIIP) p. 395-399. Shimla: IEEE.

ionForge. (2014). *ionForge* Releases imageDiff As Free Standalone Software. Obtenido de http://www.gamasutra.com/view/news/96796/ionForge_Releases_imageDiff_As_Free_Standalone_Software.php

Jabbar, A., Alaa, A., Sahib, S., y Zamani, M. (2013). *An Introduction to Image Steganography Techniques*. Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference on (p. 5). IEEE.

Kumar, M., Hemrajani, N., y Kishore, A. (2013). Security Improvisation in Image Steganography using DES. Advance Computing Conference (IACC). Ghaziabad: IEEE.

Manjula, Y., & Shivakumar, K. (2016). *Enhanced secure image steganography using double encryption algorithms*. 3rd International Conference on Computing for Sustainable Global Development (INDIACom) (p. 705-708). New Delhi: IEEE.

Mathur, M., y Kesarwani, A. (2013). Comparison Between DES, 3DES, RC2, RC6, Blowfish and DES. *Procedings* of *National* Conference of New Horizons in IT (p. 143-148).

Méndez, P. (2016). N*uevo algoritmo criptográfico con la incorporación de la esteganografía en imágenes*. Escuela Superior Politécnica de Chimborazo.

Muñoz, A. (2014). *Canales subliminales. Esteganografía*. Obtenido de http://www.criptored.upm.es/crypt4you/temas/privacidad-proteccion/leccion7/leccion7.html

Netbeans. (2016). N*etBeans IDE - The Smarter and Faster Way to Code*. Obtenido de https://netbeans.org/features/index.html

Nurhayati, & Ahmad, S. (2016). Steganography for inserting message on digital image using least significant bit and AES cryptographic algorithm. 4th International Conference on Cyber and IT Service Management (p. 1-6). Bandung: IEEE.

Rodríguez, M., Navas, S., y Eterovic, J. (2014). *Aplicación del filtro de Canny en la esteganografía digital*. WICC 2014 XVI Workshop de Investigadores en Ciencias de la Computación p. 806-811.

Saini, J., y Verma, H. (2013). A hybrid approach for image security by combining encryption *and steganography*. *IEEE Second International Conference on Image Informatio*n *Processing* (ICIIP) (p. 607-611). Shimla: IEEE.

Scooter Software. (2016). Beyond compare. Obtenido de http://www.scootersoftware.com/index.php

Segura, G., y Díaz, A. (2014). *Implementación del algoritmo esteganográfico LSB (Least Significant Bit) estándar en archivos de audio mp3*. Obtenido de http://www.boletin.upiita.ipn.mx/index.php/ciencia/215-cyt-numero-33/109-implementacion-del-algoritmo-esteganografico-lsb-least-significant-bit-estandar-en-archivos-de-audio-mp3

Sethi, P., y Kapoor, V. (2016). A Proposed Novel Architecture for Information Hiding in Image Steganography by Using Genetic Algorithm and Cryptography. International Conference onn Computational Science (p. 61-66). India: Elsevier.

Sharma, V., & Srivastava, D. (2017). *Comprehensive Data Hiding Technique for Discrete Wavelet Transform-Based Image Steganography Usin*g Advance Encryption Standard. Computing and Network Sustainability. 12, p. 353-360. Singapore: Springer.