RECIBIDO/RECEIVED: 29 OCTUBRE 2016 | ACEPTADO/ACCEPTED: 18 AGOSTO 2017 | PP. 115 - 127

Propuesta de mejora de un algoritmo criptográfico con la combinación de la esteganografía en imágenes

Proposal for improvement of a cryptographic algorithm with the combination of steganography in images

Pablo Martí Méndez Naranjo
Universidad Nacional de Chimborazo
Escuela Superior Politécnica de Chimborazo
(Ecuador)
pmendez@unach.edu.ec

Andrés Santiago Cisneros Barahona
Universidad Nacional de Chimborazo
(Ecuador)

Henry Mauricio Villa Yánez
Universidad Nacional de Chimborazo
(Ecuador)

Revista Cumbres Vol.3 Nº2
Versión impresa ISSN 1390-9541
Versión electrónica ISSN 1390-3365
http://investigacion.utmachala.edu.ec/revistas/index.php/Cumbres

RESUMEN

El presente trabajo de investigación integró dos campos relacionados con la seguridad: criptografía y esteganografía, lo que permitió incrementar la seguridad de la información. El algoritmo criptográfico seleccionado como base fue el Estándar de Encriptación Avanzada (AES), de acuerdo con el estudio realizado en base a los parámetros de comparación y para la técnica esteganográfica en imágenes se seleccionó la técnica del Bit Menos Significativo (LSB). El software utilizado para la investigación fue: Netbeans como ambiente de desarrollo, WinHex para comparar el código hexadecimal de las imágenes y IonForge ImageDiff para comparar las diferencias pixel a pixel entre imágenes. Se implementó el Prototipo II que utilizó la propuesta de mejora del algoritmo criptográfico denominado 2 Nuevo Estándar de Encriptación Avanzada (2NAES) y el Prototipo I que utilizó el algoritmo AES base, a los cuales se les combinó la técnica esteganográfica en imágenes LSB. Se comparó los resultados obtenidos analizando las características de los algoritmos y ejecutando criptoanálisis a los mensajes cifrados con el Prototipo I y con el Prototipo II. Se concluyó, que la propuesta de mejora del algoritmo criptográfico 2NAES con la combinación de la técnica LSB, mejoró la seguridad en comparación con el algoritmo criptográfico AES base debido a que el mensaje fue más difuso.

Palabras clave: criptografía, esteganografía, 2 Nuevo Estándar de Encriptación Avanzada (2NAES), Estándar de Encriptación Avanzada (AES), Bit Menos Significativo (LSB), criptoanálisis.

ABSTRACT

This work integrated two fields related to security: cryptography and steganography, which allowed to increase the security of information. The cryptographic algorithm selected as the basis was the Advanced Encryption Standard (AES), considering the results of a study based on the comparison parameters; for the steganographic technique in images, the Least Significant Bit (LSB) technique was selected. The softwares used for the study were Netbeans as a development environment; WinHex to compare the hexadecimal code of images; and, IonForge ImageDiff to compare pixel to pixel differences between images. We implemented Prototype II that used the proposed algorithm to improve the cryptographic algorithm called 2 New Advanced Encryption Standard (2NAES) and Prototype I that used the AES base algorithm. These prototypes were combined with the steganographic technique in LSB images. We compared the results obtained by analyzing the characteristics of the algorithms and executing cryptanalysis to messages coded with Prototype I and Prototype II. It was concluded that the proposed improvement of the 2NAES cryptographic algorithm with the combination of the LSB technique improved the security compared to the base AES cryptographic algorithm because the message was more diffuse.

Keywords: Cryptography, steganography, 2 New Advanced Encryption Standard (2NAES), Advanced Encryption Standard (AES), Least Significant Bit (LSB), cryptanalysis.

INTRODUCCIÓN

La seguridad de la información 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 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 & Kumar, 2013).

La criptografía y la esteganografía son dos campos en la seguridad informática: el primero hace referencia al mensaje, y el segundo término, a la forma de ocultar el mensaje tras un medio multimedia. Cada uno de estos campos por separado no asegura la información, pero si se combinan ambas técnicas para cifrar y ocultar el mensaje tras un medio multimedia, mejoraría el nivel de seguridad (Segura & Díaz, 2014).

La criptografía es la ciencia que utiliza algoritmos específicos para 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 tienen dos partes: la primera, convierte el mensaje original en criptogramas utilizando una clave y la segunda, convierte la información cifrada en el mensaje original con la clave respectiva (Sadaf, Shoaib, Anjum, & Dilbar, 2016). Cuando la información es transmitida a través de canales inseguros de comunicación es necesario asegurarla contra posibles accesos no autorizados utilizando la criptografía (Lennon, 2010). Por ejemplo, el cifrado por trasposición consiste en cambiar las posiciones de los caracteres, escribiendo al revés “criptografía y esteganografía” pasaría a ser “aífargotpirc y aífargonagetse”, lo cual es complejo de comprender si no se conoce el proceso con el cual se realizó el cambio.

Las principales propiedades de las que se ocupa la criptografía son: confidencialidad, integralidad, vinculación y autenticación (Saini & Verma, 2013). El origen cifra el mensaje utilizando una clave y el destino la descifra utilizando la clave dependiendo del tipo de criptografía utilizada ya sea simétrica o asimétrica (Sugandhi & Subba, 2016).

La esteganografía 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 integra el mensaje en el archivo multimedia y el receptor lo extrae para obtener el mensaje oculto (Saini & Verma, 2013). Existen varias técnicas para ocultar un texto o cualquier otro tipo de información, dentro de un archivo gráfico o de audio, asegurado por una clave conocida solo por la persona que ha creado ese archivo, pero que será el encargado de hacerla saber a quien quiera descubrir el contenido de esa información (Arribas del Pozo, 2014). El formato de imágenes más utilizado es el Windows Bitmap (BMP), cada pixel tiene un componente

RGB (Red-Green-Blue) y cada componente tiene 8 bits, utilizando la técnica esteganográfica LSB se reemplaza el bit menos significativo (Xu & Zhong, 2012).

En la investigación de Gaba y Kumar (2013), se mencionan 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 2 grandes áreas: la criptografía y la esteganografía. Se utiliza 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.

En la investigación de Kumar, Hemrajani y Kishore (2013), se mencionan 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. Las técnicas esteganográficas se basan en estrategias de embebido con menos consideraciones para el pre procesamiento. Una de las técnicas más utilizadas en la esteganografía es la del Bit Menos Significativo, debido a su alta capacidad de ocultación.

En la investigación de Saini y Verma (2013), se menciona 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.

MATERIALES Y MÉTODOS

Los instrumentos utilizados fueron: Netbeans (Netbeans, 2016) como IDE de desarrollo, WinHex (X-Ways, 2016) para comparar de forma visual las diferencias en el código hexadecimal de las imágenes, IonForge ImageDiff (IonForge, 2016) para comparar de forma visual las diferencias pixel a pixel de las imágenes esteganografiadas, Cryptool (Cryptool, 2016) para realizar pruebas de criptoanálisis a los mensajes cifrados.

La metodología que se utiliza es la siguiente:

- **Determinación e Implementación del algoritmo criptográfico base**: seleccionar un algoritmo criptográfico simétrico como base para la investigación
- **Determinación e Implementación de la técnica esteganográfica**: seleccionar una técnica esteganográfica como base para la investigación.
- **Creación e implementación de la propuesta de mejora del algoritmo criptográfico**: propuesta de mejora del algoritmo base
- **Integración de los algoritmos criptográficos y esteganográficos**: desarrollo del Prototipo I y Prototipo II para realizar las comparaciones de características y criptoanálisis.

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 2 escenarios son: Utilización de tamaños de clave de 128 bits, 192 bits, 256 bits. Tamaños de bloque de 128 bits. Utilización de imágenes BMP (Windows bitmap).

Escenarios

En el ambiente de pruebas se definen dos escenarios:

- **Escenario 1**: se utiliza el Prototipo I que incluye el algoritmo criptográfico AES que ha sido tomado como algoritmo base, con la combinación de la esteganografía en imágenes utilizando el método LSB.
- **Escenario 2**: se utiliza el Prototipo II que incluye la propuesta de mejora del algoritmo criptográfico desarrollado 2NAES, con la combinación de la esteganografía en imágenes utilizando el método LSB.

RESULTADOS Y DISCUSIÓN

Determinación e implementación del algoritmo criptográfico base

Luego de realizar la búsqueda de información de estudios primarios acerca de los algoritmos criptográficos simétricos más utilizados, se procede a seleccionar los algoritmos simétricos o de clave privada debido a sus características. Los algoritmos criptográficos simétricos seleccionados son: AES, DES, 3DES. Se procede con la síntesis para determinar el algoritmo criptográfico que será utilizado como base, para lo cual se realiza la comparación entre los algoritmos criptográficos simétricos utilizando los siguientes factores de seguridad y rendimiento, tomando como base con la información recopilada y la del artículo científico de Mathur y Kesarwani (2013).

De los resultados de la comparación realizada, se puede determinar que el algoritmo criptográfico simétrico AES es el más adecuado debido a sus ventajas en relación a los otros algoritmos ya que permite utilizar claves de 128 bits, 192 bits y 256 bits. Entre las principales ventajas se mencionan: tamaño de bloque variable, número de rondas depende de la clave que se utilice, es resistente al criptoanálisis diferencial, truncado diferencial, lineal, 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. Por lo que es utilizado como base para la elaboración e implementación de la propuesta de mejora del algoritmo criptográfico, a los cuales se combina la esteganografía en imágenes. Se procede con el desarrollo de la aplicación del algoritmo criptográfico AES base, para el proceso de cifrado y descifrado con las funciones definidas: AddroundKey, SubBytes, MixColumns, ShiftRows.

Determinación e Implementación de la técnica esteganográfica

Luego de realizar la búsqueda de información de estudios primarios acerca de los algoritmos esteganográficos más utilizados, se procede a seleccionar

la técnica Least Significant Bit (LSB) debido a sus características: es sencillo de implementar, es rápida, utiliza menos recursos, minimiza la variación en los colores, atenúa la distorsión de la imagen, no varía el tamaño de la imagen, puede utilizarse en imágenes a color y escala de grises. Posteriormente se procede con el desarrollo de la aplicación de la técnica esteganográfica LSB, para el proceso de embebido y extracción del mensaje.

Creación e implementación de la propuesta de mejora del algoritmo criptográfico

Para la propuesta de mejora del algoritmo criptográfico se ha considerado el algoritmo AES como base y se lo denominará 2NAES. Para mejorar la seguridad e incrementar la difusión del mensaje, se proponen las siguientes mejoras en el algoritmo criptográfico:

• Utilizar una **nueva función** que se ejecute en todas las rondas (ronda inicial, dentro de las rondas parciales y en la ronda final) denominado **SHIFTCOLUMNS**, en la cual se procede a realizar un desplazamiento hacia arriba cíclicamente de las columnas que conforman la matriz de estado actual. Cada columna se desplaza un número de posiciones diferentes. Como se muestra en la Figura 1, 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 1 se muestra la función ShiftColumns propuesta

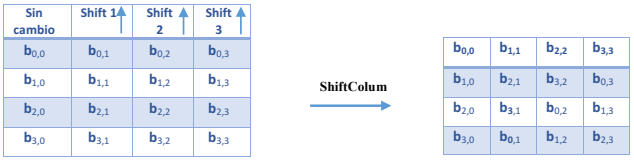

Figura 1. Función ShiftColumns

• Ejecutar 2 veces el algoritmo, para la primera ejecución se utiliza la clave ingresada por el usuario (clave A) y para la segunda ejecución se utiliza una segunda clave basada en la primera (clave B).

Para obtener la clave B se realiza el siguiente proceso:

- Se obtiene la clave ingresada por el usuario (clave A).
- Se invierte el orden de elementos de la clave A.
- Se realiza un ShiftRows de 3 posiciones hacia la izquierda de la clave A.
- Cada valor decimal de la clave A, se suma la posición en la que se encuentre.

Con las modificaciones definidas, se procede con el desarrollo de la aplicación de la propuesta de mejora del algoritmo criptográfico 2NAES, para el proceso de cifrado y descifrado.

Integración de los algoritmos criptográficos y esteganográficos

Cuando la esteganografía no asegura la información contenida en el mensaje secreto, se incluyen técnicas de encriptación que la aseguran (Islam, Siddiga, Uddin, Kumar, & Hossain, 2014), por lo que se integran los algoritmos definidos en los prototipos I y II:

Prototipo I

Se desarrolla el Prototipo I que integra el algoritmo criptográfico que es considerado como base y el método esteganográfico en imágenes. Se implementa el algoritmo AES base con sus funciones: AddRoundKey, SubBytes, ShiftRows, MixColumns y se lo combina la esteganografía en imágenes con la técnica de LSB.

Prototipo II

Para el Prototipo II se integra la aplicación con la propuesta de mejora del algoritmo criptográfico y la integración esteganográfica en imágenes. Se implementa la propuesta de mejora del algoritmo 2NAES con sus funciones: AddRoundKey, SubBytes, ShiftRows, **ShiftColumns** (**nueva función**), MixColumns. Además, el algoritmo 2NAES repite el proceso con una nueva clave generada a partir de la primera. Al algoritmo criptográfico 2NAES se combina la esteganografía en imágenes con la técnica de LSB.

Se procede con el desarrollo de la aplicación del Prototipo II, cuyo proceso de cifrado y embebido se resume en la Figura 2 y proceso de extracción y descifrado en la Figura 3

Cifrado y embebido – Extracción y descifrado

Para probar los procesos de cifrado y embebido – extracción y descifrado con el Prototipo I y Prototipo II desarrollados, con claves de 128 bits, 192 bits y 256 bits, se utilizan los siguientes datos:

Clave de 128 bits: }yl%OckF x){gI~o
Clave (192 bits): <E?<E?<E?<E?<E?<E?<E?<E?
Clave (256 bits): <E?<E?<E?<E?<E?<E?<E?<E?<E?<E?<E

Mensaje: La criptografia y la esteganografia son dos campos que se complementan basados en la seguridad informática: la primera encripta el mensaje y la segunda oculta el mensaje tras un medio multimedia. Cada una por separado no asegura el secreto, pero si se aplican ambas técnicas para cifrar y ocultar un mensaje, aumentan el nivel de seguridad.

Comparación de resultados criptográficos

El mensaje de prueba fue cifrado con el Prototipo I y Prototipo II con los diferentes tamaños de claves. Se comparan 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 1, cuyos caracteres pueden ser imprimibles y no imprimibles.

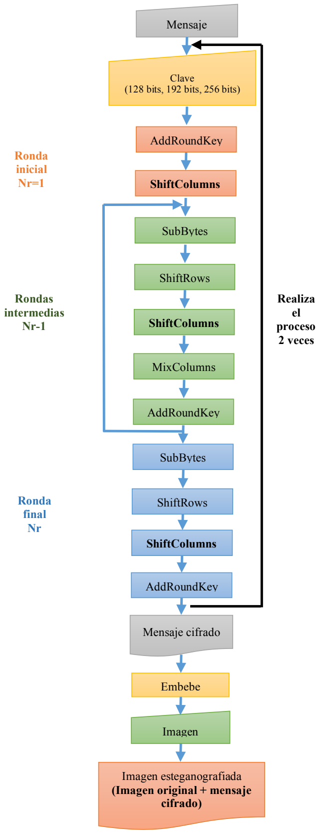

Figura 2 Proceso de cifrado y embebido

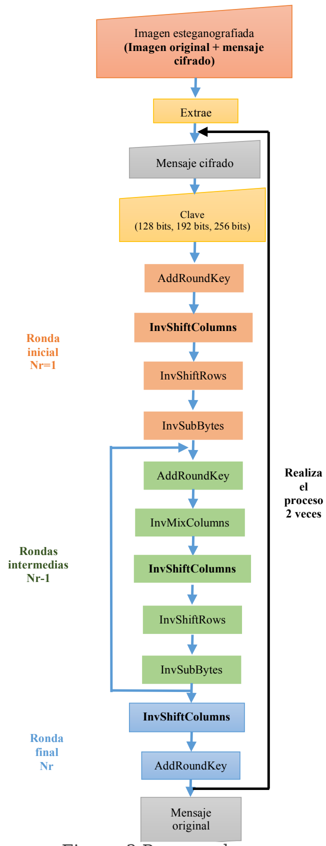

Figura 3 Proceso de extracción y descifrado

Tabla 1. Comparación de mensajes cifrados con Prototipo I y Prototipo II

Clave	Prototipo I	Prototipo II
128 bits	[illegible]	[illegible]
192 bits	[illegible]	[illegible]
256 bits	[illegible]	[illegible]

Comparación de resultados esteganográficos

Se comparan las imágenes “Base.bmp” y “Base_embebido.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. Se comparan los tamaños de las imágenes “Base.bmp “Base_embebido.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 manteniendo un tamaño de 1.440.054 bytes. Se utiliza el programa WinHex para determinar el código hexadecimal de las imágenes "Base. bmp" y "Base_embebido.bmp", 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 las imágenes, se determinan aproximadamente 1381 diferencias. Se utiliza 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 muestra en la parte superior la diferencia entre pixeles, como se muestra en la Figura 4

Figura 4 Diferencia en los pixeles entre las imágenes comparadas

Análisis de características de los algoritmos

Se compara el algoritmo AES base implementado en el Prototipo I y la propuesta de mejora del algoritmo 2NAES implementado en el Prototipo II, para los siguientes 4 indicadores de la variable dependiente definida: Número de claves utilizadas, Número de Rondas, Número de Funciones usadas por el algoritmo, Número de Funciones ejecutadas por el algoritmo. En la Tabla 2 se muestra los resultados de la comparación de los indicadores de análisis de características entre el Prototipo I y el Prototipo II.

Tabla 2. Resultados de comparación de indicadores

No.	Indicadores	Prototipo I			Prototipo II		
		Longitud de la clave					
		128 bits	192 bits	256 bits	128 bits	192 bits	256 bits
1	No. claves utilizadas	1	1	1	2	2	2
2	No. Rondas	10	12	14	20	24	28
3	No. funciones usadas por el algoritmo	4	4	4	10	10	10
4	No. funciones ejecutadas por el algoritmo	40	48	56	102	122	142

Ambiente de pruebas

Se compara el algoritmo AES base implementado en el Prototipo I y la propuesta de mejora del algoritmo 2NAES implementado en el Prototipo II, para los siguientes indicadores de la variable dependiente definida: entropía, histograma, n-grama, autocorrelación, fuerza bruta. Se realiza el criptoanálisis utilizando la herramienta Cryptool se comparan 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 2NAES implementado en el Prototipo II. Para las pruebas realizadas de criptoanálisis se utiliza un alfabeto extendido de 98 caracteres que incluyen: 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 realizados a los indicadores del 5 al 9 fueron:

· **Indicador 5: Entropía**

En la Tabla 3 se muestran los resultados de las pruebas de entropía para determinar el nivel de difusión existente en los mensajes.

Tabla 3. Caracteres diferentes y valores de entropía de mensajes cifrados

CLAVE	ALGORITMO	CARACTERES DIFERENTES	ENTROPÍA MÁXIMA	VALOR
128 bits	Prototipo I	67	6,61	5,87
	Prototipo II	73	6,61	6,02
192 bits	Prototipo I	71	6,61	5,96
	Prototipo II	72	6,61	6,00
256 bits	Prototipo I	68	6,61	5,90
	Prototipo II	70	6,61	5,96

· **Indicador 6: Histogramas**

En la Tabla 4 se muestran los resultados de las pruebas de histograma que relaciona el porcentaje de frecuencia con los valores contenidos en los mensajes cifrados.

Tabla 4. Número de caracteres del histograma de los mensajes cifrados

CLAVE	ALGORITMO	CARACTERES
128 bits	Prototipo I	116
	Prototipo II	148
192 bits	Prototipo I	125
	Prototipo II	126
256 bits	Prototipo I	125
	Prototipo II	125

· **Indicador 7: N-gramas**

En la Tabla 5 se muestran los resultados de las pruebas de N-grama que muestra el número y detalle de secuencia, frecuencia en porcentaje y frecuencia de los n-gramas contenidos en los mensajes cifrados.

Tabla 5. Resumen de n-gramas de los mensajes cifrados

CLAVE	ALGORITMO	N-GRAMA (MÁXIMO)
128 bits	Prototipo I	4
	Prototipo II	6
192 bits	Prototipo I	5
	Prototipo II	7
256 bits	Prototipo I	6
	Prototipo II	7

· **Indicador 8: Autocorrelación**

En la Tabla 6 se muestran los resultados de las pruebas de correlación que relaciona el número de caracteres que concuerdan con el desplazamiento de los mensajes cifrados

Tabla 6. Número de caracteres que concuerdan en la correlación

CLAVE	ALGORITMO	CARACTERES CONCUERDAN
128 bits	Prototipo I	4
	Prototipo II	6
192 bits	Prototipo I	3
	Prototipo II	4
256 bits	Prototipo I	3
	Prototipo II	4

· **Indicador 9: Fuerza bruta**

En la Tabla 7 se muestran los resultados de las pruebas de fuerza bruta que se basa en probar todas las combinaciones posibles de la clave de los mensajes cifrados

Tabla 7. Tiempo a descifrar mensajes por fuerza bruta

CLAVE	ALGORITMO	TIEMPO DESCIFRAR (AÑOS)
128 bits	Prototipo I	1,6x1025
	Prototipo II	1,7x1025
192 bits	Prototipo I	3,3x1044
	Prototipo II	3,4x1044
256 bits	Prototipo I	7,3x1063
	Prototipo II	7,4x1063

Comparando los resultados obtenidos en la presente investigación, con la de otros autores que han realizado investigaciones previas acerca de este tema: Gaba y Kumar (2013) no analizan los mensajes cifrados debido a que utilizan un algoritmo existente y se enfocan únicamente en los resultados con las imágenes esteganografiadas. Kumar, Hemrajani y Kishore (2013) plantea una mejora en el algoritmo criptográfico, sin embargo, se enfoca en la capacidad de mezcla de caracteres e intensidad de pixeles que contribuyen en el cifrado y no en el resultado de los mensajes cifrados. Saini y Verma (2013) proponen una mejora en el algoritmo criptográfico, pero no comparan los resultados en los mensajes, se enfocan en los resultados esteganográficos en relación con la calidad de la imagen. La presente investigación propone la integración de una nueva función que se integra en las rondas del algoritmo criptográfico, se utiliza otra clave generada en base a la primera, 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 determinan indicadores en base a las características y en base a criptoanálisis con los que se comparan el algoritmo criptográfico base con

la propuesta realizada. En otras investigaciones no se ha utilizado criptoanálisis para verificar la seguridad en los mensajes cifrados por los prototipos I y II ni se ha realizado una comparación pixel a pixel ni en base al código hexadecimal de las imágenes originales con las esteganografiadas para determinar los cambios visuales existentes.

CONCLUSIONES

Con la incorporación de la función propuesta ShifColumns en las rondas del algoritmo, repetición del proceso de cifrado y la generación de la clave B en función de la clave A que fueron utilizadas en el proceso del algoritmo 2NAES, el mensaje cifrado se difuminó más en comparación con el algoritmo AES base, demostrando así que es más seguro.

El Prototipo II es mejor debido a que utiliza un mayor número de claves, mayor número de rondas, mayor cantidad de funciones usadas y ejecutadas en comparación con el Prototipo I.

Los mensajes cifrados con el Prototipo II poseen mayor entropía, utilizan mayor cantidad de caracteres, gramas y caracteres que coinciden, y es más resistente contra fuerza bruta en comparación a los mensajes cifrados con el Prototipo I

REFERENCIAS BIBLIOGRÁFICAS

Arribas del Pozo, M. (2014). *Gestión de archivos*. España: Ediciones Nobel, S.A.

Cryptool. (2016). *About Cryptool 1.* Obtenido de https://www.cryptool.org/en/cryptool1

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

IonForge. (2016). *ImageDiff*. Obtenido de http://download.cnet.com/windows/ionforge/3260-20_4-6271082-1.html

Islam, R., Siddiga, A., Uddin, P., Kumar, A., & Hossain, D. (2014). *An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography*. Informatics, Electronics & Vision (ICIEV). IEEE.

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

Lennon, R. (2010). *Cryptography architecture for information security*. IBM Systems Journal (págs. 138-150). IEEE.

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

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

Sadaf, B., Shoaib, M., Anjum, M., & Dilbar, S. (2016). *Enhancing security of*

images by Steganography and Cryptography techniques. Innovative Computing Technology (INTECH). IEEE.

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

Segura, G., & Díaz, A. (2014). *Implementación del algoritmo esteganográfico LSB (Least Significant Bit) estándar en archivos de audio mp3*. Boletín UPIITA(ISSN 2007-6150).

Sugandhi, G., & Subba, C. (2016). *Efficient steganography using least significant bit and encryption technique*. Intelligent Systems and Control (ISCO), 10th. IEEE.

Xu, Q., & Zhong, S. (2012). *Blind Detection Algorithm for BMP Stego Images Based on Feature Fusion and Ensemble Classification*. Intelligent Human-Machine Systems and Cybernetics (IHMSC) (págs. 187-191). IEEE.

X-Ways. (2016). *WinHex: Computer Forensics & Data Recovery Software*. Obtenido de https://www.x-ways.net/winhex/