Análisis del Algoritmo Esteganográfico F5 para Imágenes JPEG a Color

Morocho E.*; Zambrano A.*; Carvajal J.*; López G.*

**Escuela Politécnica Nacional, Facultad de Ingeniería Eléctrica y Electrónica, Quito, Ecuador*
e-mail: { enriquembmw, jose.zambrano;jorge.carvajal;gabriel.lopez}@epn.edu.ec

Resumen: El presente trabajo se basa en el análisis del algoritmo esteganográfico F5 para imágenes JPEG a color, determinando características de Invisibilidad, Robustez y Capacidad de Embebido en imágenes, comparado con el algoritmo LSB. Se presenta el Estegoanálisis visual, estadístico R-S, Chi cuadrado del algoritmo F5 y LSB.

Palabras clave: Esteganografía, Estegoanálisis, JPEG, Algoritmo F5, Algoritmo LSB, Estego-Imagen.

Abstract: This investigation is based on the analysis of the steganography algorithm F5 for JPEG color images, determining invisibility characteristics, performance, and capacity of the embed process in comparison with the LSB algorithm. It is presented the visual steganography analysis, statistics R-S, Chi square from the algorithm F5 and LSB.

Keywords: Steganography, JPEG, F5 algorithm, LSB algorithm, Steganalysis, Stego-Image

1. INTRODUCCIÓN

Históricamente la Esteganografía es una técnica muy antigua que data del año 474 A.C. y que goza de trascendental importancia en la actualidad ya que desde el punto de vista informático, la Esteganografía es el conjunto de métodos y técnicas para hacer pasar desapercibido o camuflar un mensaje.

La Esteganografía se puede ver muy relacionada con la criptografía, pero se diferencia en que esta última, cifra o codifica los mensajes dejándolos ininteligibles, para esto la Esteganografía trata de ocultar el envío del mensaje dentro de un portador de apariencia normal, sin transmitirlo necesariamente cifrado.

Tomando en cuenta esta definición y considerando que en la actualidad se ha incrementado mucho las restricciones al acceso de manera libre a la información, se están ideando nuevas maneras para lograr ocultamiento de información importante dentro de archivos que son muy comunes como las imágenes.

El algoritmo F5 es relativamente nuevo en el campo de la Esteganografía, el cual fue introducido por los investigadores alemanes Pfitzmann y Westfeld en el 2001 mientras que el algoritmo LSB es ampliamente difundido

Técnicas y Requerimientos para la Esteganografía [1]

Existen básicamente tres tipos de técnicas Esteganográficas dentro de las cuales se tiene: pura, de clave secreta y de clave pública. El sistema de Esteganografía pura se caracteriza por no requerir un intercambio previo de información como por ejemplo, claves compartidas, por lo tanto no se necesita información para iniciar el proceso de comunicación y la seguridad de este sistema, solo depende de la discreción. En la Fig 1. se muestra el sistema.

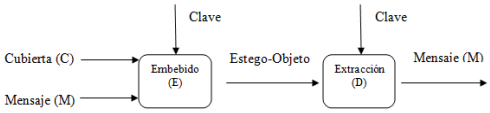

Figura 1. Sistemas de Esteganografía Pura.

Un sistema de Esteganografía de clave secreta, Fig. 2, es muy parecido a un sistema de cifrado simétrico, en el cual el emisor selecciona una cubierta e incrusta el mensaje secreto en la cubierta haciendo uso de una clave secreta. Si el receptor conoce la clave secreta, este puede obtener el mensaje oculto.

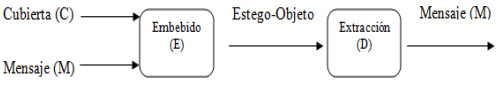

Figura 2. Sistemas de Esteganografía de Clave Secreta.

La Esteganografía de clave pública no requiere del intercambio de una clave secreta. Este sistema requiere de dos claves, una privada (secreta), la cual es usada en el proceso de inserción del mensaje secreto y la otra pública, la cual es almacenada en una base de datos pública. La clave secreta es usada para reconstruir el mensaje.

Los requerimientos fundamentales para la Esteganografía son: invisibilidad el cual está relacionado a la calidad de la estego-imagen resultante luego del proceso de ocultamiento por parte del sistema esteganográfico. La robustez Se refiere al grado de inmunidad que presenta la información oculta ante las diferentes manipulaciones que pueda sufrir el objeto utilizado como cubierta. Entre las manipulaciones más comunes se encuentran el filtrado, re-muestreo y el recorte de áreas o secciones no deseadas y por último la capacidad de Embebido que representa la cantidad de bits de información secreta que pueden ser embebidos dentro de la imagen que se usará como cubierta. Se debe tener en consideración que el nivel de invisibilidad no es proporcional a la capacidad de embebido por lo que, estas dos características deben ser tomadas muy en cuenta por los algoritmos de Esteganografía

2. DESCRIPCIÓN DE LOS ALGORITMOS ESTENOGRÁFICOS

2.1 LSB Least Significant Bit

Es el algoritmo más fácil de implementar, por lo cual es muy utilizado para realizar Esteganografía con imágenes y archivos de audio.

En el método LSB normal, el proceso de embebido, consiste en sustituir x-bits de información secreta, por los x-bits, menos significativos, usados para representar el valor de un píxel de la imagen que se utilizará para cubierta. En el proceso de extracción, se toman los x-bits menos significativos de cada píxel de la estego-imagen y se reconstruye la información secreta como se muestra en la Fig. 3.

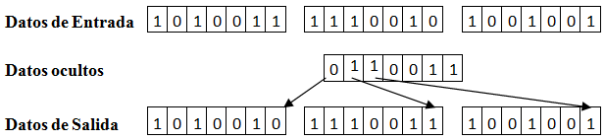

Figura 3. Descripción del Algoritmo Esteganográfico LSB.

OpenStego es un software de código abierto desarrollado en Java que permite la ocultación de información dentro de imágenes haciendo uso del algoritmo esteganográfico LSB.
Las imágenes de entrada que acepta el programa pueden ser de cualquier formato, entre tanto que las estego-imágenes producidas por el programa solo tienen el formato bmp, formato elegido por el creador del programa porque no tiene pérdidas de información.

El programa permite guardar la estego-imagen generada, la cual tendrá el formato bmp sin importar cuál sea su formato original.

Además el programa permite elegir cuantos bits menos significativos se van a utilizar de cada pixel para reemplazarlos con bits de información oculta, en este caso se va a escoger el mínimo que es 1 bit, esto para asegurar que la estego-imagen producida no sea distorsionada.

2.1 Algoritmo Esteganográfico F5

El algoritmo trabaja en el dominio de la frecuencia con los coeficientes de la transformada discreta Coseno (DCT). El algoritmo oculta los bits del mensaje dentro de coeficientes DCT de una imagen JPEG escogidos de manera aleatoria y emplea una matriz de embebido que minimiza el número de cambios necesarios para ocultar un mensaje de cierta longitud. De acuerdo a la descripción del algoritmo F5 [8], acepta las siguientes entradas:

- Un factor Q de calidad para la estego-imagen (por defecto = 75).
- Un archivo de entrada que puede ser JPEG, BMP, TIFF o GIF.
- El nombre del archivo de salida.
- Un archivo que contiene la información a ocultar.
- Un password de usuario (estego-clave) que será usado como semilla para un Generador Pseudo-aleatorio de Números (GPAN).
- Un comentario puede ser insertado de manera opcional en la cabecera de la imagen JPEG.

Además el proceso de embebido, del algoritmo F5, tiene la siguiente estructura:

- En el proceso de compresión de la imagen JPEG, se detiene antes de la cuantificación de los coeficientes.
- Calcula la tabla de cuantificación correspondiente al factor de calidad Q y se comprime la imagen mientras se almacenan los coeficientes DCT cuantificados.
- Calcula la capacidad estimada, sin la matriz de embebido mediante la siguiente Ecuación.

$$C = h_{DCT} - \frac{h_{DCT}}{64} - h(0) - 0{,}51 * h(1) \qquad (1)\ [9]$$

h_{DCT} : Número de todos los coeficientes DCT.
$h(0)$: Número de todos los coeficientes AC iguales a cero.
$h(1)$: Número de todos los coeficientes AC con valor absoluto igual a 1.
$\frac{h_{DCT}}{64}$: Número de todos los coeficientes DC.
$-0{,}51 * h(1)$: Perdida estimada durante el proceso de contracción, el cual se describirá más adelante.

Para determinar la mejor matriz de embebido se utiliza la capacidad C y la longitud de la información a ocultar.

Asimismo la estego-clave es utilizada para generar una semilla para el Generador de Números Pseudo-aleatorio, con

el cual se genera un camino aleatorio que sirve para colocar los bits de la información oculta. Durante el proceso de embebido, los coeficientes iguales a cero y los coeficientes DC son omitidos.

Determinar el valor de k, el cual se calcula utilizando la capacidad estimada y la longitud del mensaje a ocultar. Cabe mencionar que el valor de k y la longitud del mensaje deben ser encriptados usando un cifrador de flujo.

La información a ocultar es dividida en segmentos de k-bits los cuales se intenta embeberlos dentro de los siguiente 2^k-1 coeficientes. Los coeficientes cero son omitidos para mantener el histograma de coeficientes AC intacto. Ahora se aplica un hash a los actuales k-bits del mensaje dentro del actual grupo de 2^k-1 coeficientes. S*i* el valor del hash es cero, significa que los k-bits se embebieron sin realizar ningún cambio. Si el valor es j, se decrementa en uno el valor absoluto del coeficiente c_j. Si el nuevo valor de c_j no es cero, significa que los k-bits de información a ocultar han sido embebidos realizando un solo cambio; caso contrario, si el valor de c_j es cero, se dice que ha ocurr*ido una contracción, c_j es posteriormente* removido de la lista y se toma el siguiente coeficiente para realizar el proceso nuevamente.

Este proceso se realiza hasta que la lista de coeficientes distintos de cero o la lista de bits del mensaje se termine. Si la lista de coeficientes finaliza antes que la *lista de bits del mensaje*, significa que el algoritmo F5 no ocultó la totalidad del mensaje y debe emitir un mensaje de error advirtiendo el tamaño máximo de la información a ocultar [6].

El algoritmo F5 esta implementado en el software computacional Matlab y el esquema que componen la interfaz gráfica se presenta en la Fig 4. Se ha considerado conveniente definir cada una de las etapas del algoritmo F5, en varios archivos .m, para evitar una sobrecarga de código y pueda ser más legible a la hora de corregir ciertos detalles del programa, el programa acepta diferentes formatos de imagen pero antes de comenzar las etapas de sub-muestreo las estandariza al formato BMP.

3. ESTEGOANÁLISIS [17, 18]

El Estegoanálisis es la técnica que estudia los métodos que permitan la detección de mensajes ocultos usando Esteganografía. Dichos mensajes pueden estar ocultos en diferentes tipos de medio, como pueden ser: imágenes digitales, ficheros de vídeo, los ficheros de audio o incluso un simple texto plano.

En el Estegoanálisis considera que un sistema ha sido vulnerado con detectar la existencia de información oculta. Existe diferentes tipos de Estegoanálisis para imágenes y dentro de las más importantes se tiene Estegoanálisis Visual y Estadístico

El primer ataque consiste en lograr identificar de manera visual partes sospechosas de una imagen, siempre y cuando se disponga de la imagen original. Este proceso se lo puede realizar sin modificar la imagen con lo cual no se asegura que el Estegoanálisis tenga el éxito deseado, ya que la mayoría de algoritmos esteganográficos intentan pasar desapercibidos visualmente.

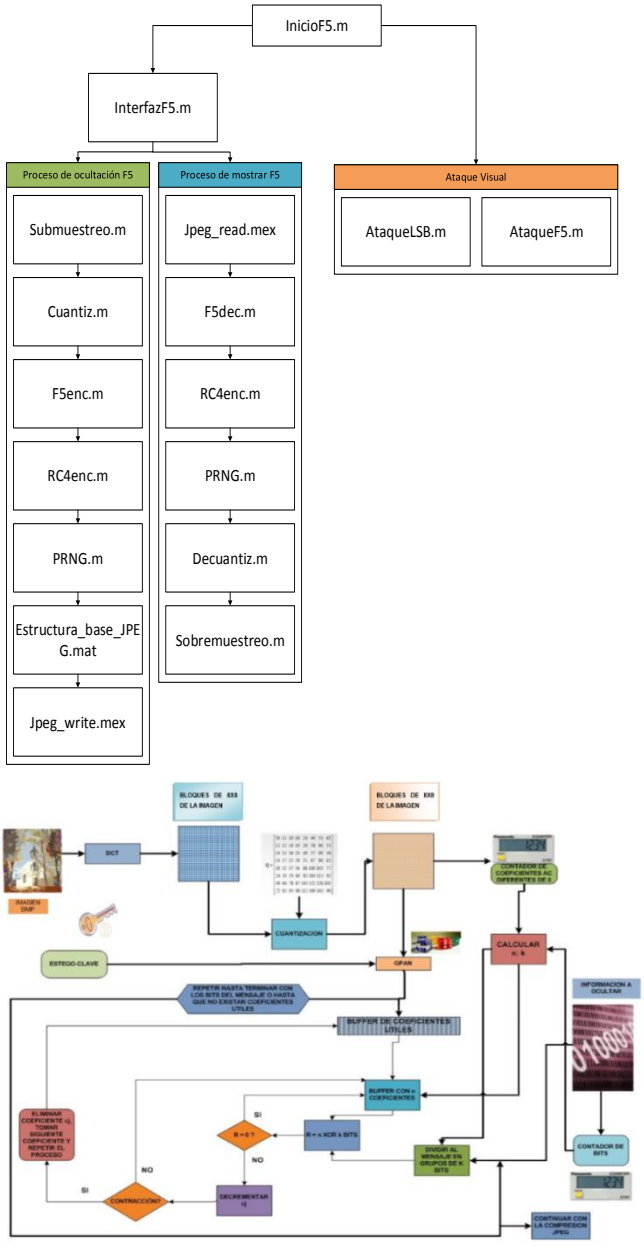

Figura 4. Esquema del algoritmo implementado F5.

Si a la estego-imagen se la somete a algún proceso y nuevamente se realiza la inspección visual se puede obtener un resultado exitoso, [21] donde los investigadores someten a un ataque visual a varios algoritmos Esteganográficos. De manera general, un ataque visual consiste en las etapas mostradas en la Fig 5.

Figura 5. Esquema de una ataque visual

El estegoanálisis Estadístico consiste en el cotejo de la frecuencia de distribución de los colores de una estego-imagen, la cual puede ser dividida en dos grupos de datos, el grupo de datos de la imagen al cual se refiere básicamente a los valores que toman los píxeles para formar los diferentes colores que conforman la imagen y el grupo de datos del mensaje oculto el cual, por lo general, se distribuye de manera aleatoria.

Un ejemplo de este tipo ataque se denomina Chi-cuadrado [21, 19] Este tipo de ataques aparecen en la literatura académica como métodos esteganográficos sobre imágenes en las que se hayan aplicado algoritmos esteganográficos que modifican el bit menos significativo.

Este tipo de ataques posibilita la comparación entre las propiedades estadísticas de la estego-imagen con las propiedades estadísticas supuestas de la imagen original. Como se puede notar, este tipo de ataque es ampliamente utilizado porque no necesita de la imagen original

Entre otro tipo se tiene el ataque estadístico R-S [26] que permite estimar además el tamaño aproximado del mensaje oculto. El método deja de ser efectivo cuando la imagen original es ruidosa de por sí, reduciendo también su efectividad cuando los bits de mensaje no son distribuidos de forma aleatoria en la imagen portadora, aunque existen variaciones del algoritmo para solventar esta última debilidad.

4. PRUEBAS Y ANÁLISIS

Para las pruebas se realiza la ocultación de información en diferentes fotografías que poseen características distintas tanto en tamaño como en la distribución de colores. Con esto se pretende obtener variedad de posibilidades para realizar el análisis.

Las imágenes mostradas desde la Fig. 6 hasta la Fig. 9 han sido seleccionadas para ser utilizadas como cubierta para ocultar un mensaje y realizar diferentes ataques de Estegoanálisis que permitirán demostrar las ventajas o desventajas de cada uno de los algoritmos esteganográfico LSB y F5. Por otra parte dichas imágenes presentan las mismas dimensiones en píxeles, el formato de las imágenes son bmp.

Figura 6. Imagen bmp paisaje 256x256 [25]

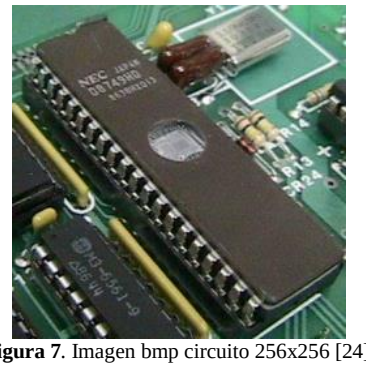

Figura 7. Imagen bmp circuito 256x256 [24]

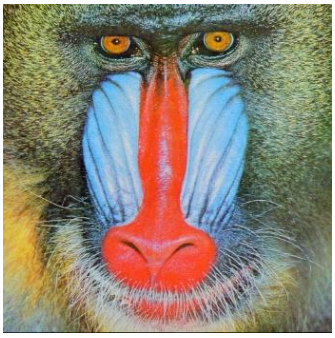

Figura 8. Imagen bmp Mandrill 256x256 [3]

Figura 9. Imagen bmp mural 256x256 [7]

Se ha escogido una imagen de prueba el cual va a ser ocultado en todas las imágenes usando los algoritmos Esteganográficos LSB y F5, para luego realizar los respectivos ataques de Estegoanálisis. Para esto se ha seleccionado la imagen de la Fig. 10 llamada button-css que tiene un tamaño de 300 bytes.

Figura 10. Imagen png button-css 80x15

4.1 LSB Ataque Visual con el algoritmo LSB

En la Fig. 11 se muestra el ataque visual a las imágenes utilizadas como cubierta y a las respectivas estego-imágenes LSB, se debe mencionar que algunas de las imágenes originales han sido transformadas al formato bmp, esto para facilitar el análisis y la efectividad del ataque.

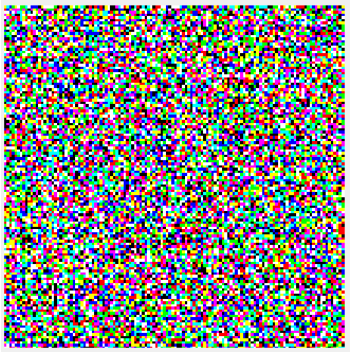

Figura 11. Ataque Visual a la Imagen Original circuito.bmp sin información Oculta

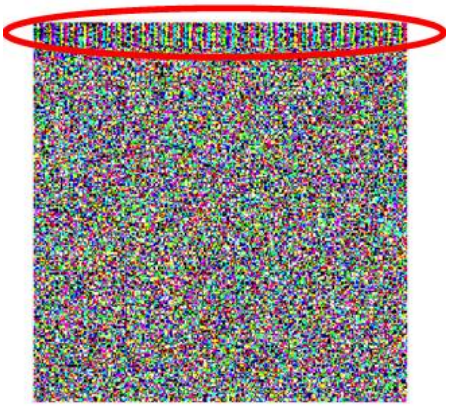

Figura 12. Ataque Visual a la Estego-Imagen circuito.bmp con información oculta

Como se puede apreciar en la Fig. 11 correspondiente el ataque visual a la imagen original usada de cubierta, se produce un resultado homogéneo en la imagen generada, pero si se analiza las figuras correspondientes al ataque visual realizado a las estego-imágenes LSB, se puede notar una ligera distorsión en la parte superior de la imagen generada, lo cual significa que la información ha sido ocultada en esa parte y además esa información permite tener una ligera idea del tamaño de la información oculta ya que se puede apreciar que ocupa alrededor de un 2% a 3% de la imagen.

4.2 LSB Ataque Visual con el algoritmo F5

En las figuras se analiza el ataque visual a las imágenes anteriores pero se ha ocultado la información mediante el algoritmo F5. Cabe mencionar que el algoritmo F5 trabaja sobre imágenes bmp, las imágenes usadas como cubierta también han sido modificadas a este formato, usando un factor Q=75 y un submuestreo horizontal 4:2:2 esto para asegurar una calidad aceptable en las imágenes producidas..

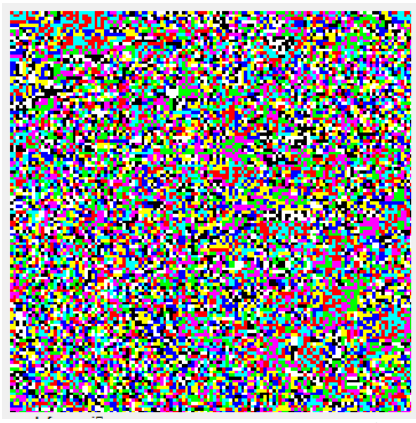

Figura 13. Ataque Visual a la Imagen circuito.bmp sin información Oculta.

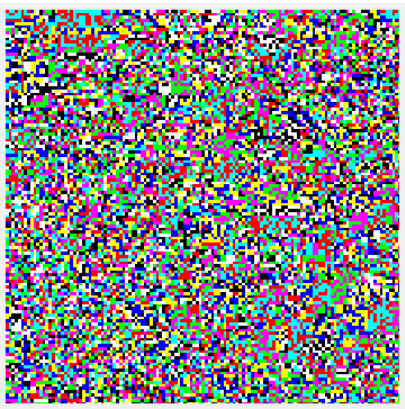

Figura 14. Ataque Visual a la Estego-Imagen circuitoF5.bmp con información Oculta.

En las Fig. 13 y 14 se aprecia los resultados producidos por los ataques visuales los cuales tienen una consistencia homogénea tanto para la imagen original y la estego-imágen, con lo cual se observa que el algoritmo F5, la información oculta permanece inadvertida si se aplica Estegoanálisis visual.

4.3 Ataque Estadístico R-S

En la tabla I se presentan los resultados obtenidos al analizar las imágenes originales y las estego-imágenes utilizando el ataque estadístico R-S.

Tabla 1. Ataque R-S a Imágenes y Estego-Imágenes

Imagen	Formato anterior	Ataque R-S a imagen original (%)	Tamaño aproximado Información Oculta (Bytes)	Ataque R-S a estego-imagen LSB (%)	Tamaño aproximado Información Oculta (Bytes)	Ataque R-S a estego-imagen F5 (%)	Tamaño aproximado Información Oculta (Bytes)
Circuito.bmp (256x256)	png	1,54046	378,58	3,34239	156,20	0,63558	821,43
Paisaje.bmp (256x256)	jpg	13,03667	3203,89	14,5277	3570,34	1,97762	486,02
Mural.bmp (256x256)	jpg	3,92196	963,86	4,59064	1128,19	1,33992	329,30
Mandril.bmp (256x256)	bmp	4,2484	1044,09	9,7068	2385,54	2,32711	571,91

Los resultados obtenidos del ataque R-S a las imágenes originales, se tiene que una de las cuatro imágenes están dentro del umbral apropiado para una imagen sin

información oculta el cual está entre 1 % – 3 %, para las imágenes que no cumplen con este valor se puede decir que se ha dado un falso positivo, en estos casos depende de la cantidad de información que se está ocultando dentro de estas imágenes que por lo visto no alcanza el umbral mínimo permitido que como se observa varía de acuerdo al tamaño y la cantidad de detalles que posee la imagen, cabe mencionar que la información oculta se refiere a un tamaño aproximado que brinda la función RS.

Si ahora se analizan los resultados del ataque R-S a las estego-imágenes que ocultan información con el algoritmo LSB, se muestra que cuatro de las cuatro imágenes han sobrepasado el umbral permitido para que una imagen se considere sin información oculta, con lo cual se puede observar la precisión del ataque R-S para la detección de información oculta cuando se usa el algoritmo esteganográfico LSB. Por otro lado se observa que el tamaño aproximado de la información oculta varia de una imagen a otra y que el resultado que más se aproxima se lo encuentra en la imagen circuito.bmp, estas variaciones se deben a los tamaños y cantidad de detalles que poseen las imágenes.

Si ahora se observan los resultados obtenidos del ataque-RS a las estego-imágenes que ocultaron información con el algoritmo F5, se tiene que tres de las cuatro imágenes están dentro del umbral permitido para una imagen sin información oculta, con lo cual se puede concluir que el ataque R-S no es eficiente para detectar información oculta empleando al algoritmo F5.

4.4 Ataque Estadístico Chi-Cuadrado

En la Fig. 15 se presentaran los resultados obtenidos al realizar el ataque Chi-Cuadrado a las diferentes imágenes cubierta y estego-imágenes. Los resultados se muestran en el siguiente orden: estego-imagen LSB (izquierda), imagen original (centro) y estego-imagen F5 (derecha).

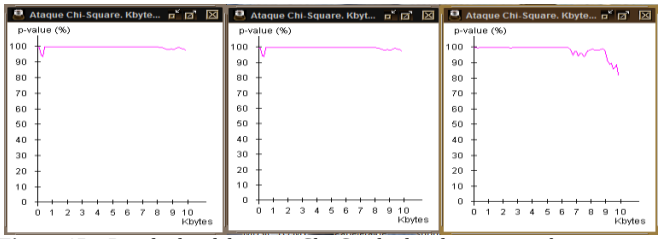

Figura 15. . Resultados del ataque Chi-Cuadrado a la imagen cubierta circuito.bmp y sus respectivas estego-imágenes

El ataque Chi-Cuadrado, en el eje X se representa el tamaño posible de la información oculta y en el eje Y se representa la probabilidad de que la imagen contenga información oculta.
Se presentaron resultados variados y en algunos casos no ayudan a clarificar si la imagen en realidad posee o no información oculta.

Se dio el caso que ninguna de las imágenes posee información oculta descartando las estego-imágenes que en realidad si poseen información oculta. Estos resultados se presentan de esta manera ya que las imágenes utilizadas como cubierta tienen una resolución alta con la cual se podría ocultar archivos más grandes al utilizado como ejemplo en este análisis, cabe mencionar que no se debe exagerar en los tamaños de la información que se oculta porque precisamente lo que buscan los algoritmos de Esteganografía es pasar inadvertidos ante cualquier algoritmo de Estegoanálisis.

En la Fig. 15 la imagen original aparece con altas probabilidades de contener información oculta, lo cual hará sospechar de todas las imágenes obtenidas a partir de esta. En los casos en los que los ataques de Estegoanálisis presentan resultados tan contradictorios es mejor cerciorarse por todos los métodos posibles para así obtener un resultado verídico y eliminar los falsos positivos que son muy comunes a la hora de realizar Estegoanálisis

5. CONCLUSIONES

Al realizar una comparación entre el algoritmo LSB y F5 para Esteganografía muestra que el algoritmo F5 tiene mayores ventajas en cuanto Invisibilidad, Robustez y Capacidad

Con el algoritmo esteganográfico implementado no se pretende tener un sistema irrompible sino más bien un referente para saber cómo funciona el algoritmo de Esteganografía, que componentes influyen en la calidad de la estego-imagen obtenida, que factores influyen en la capacidad de una determinada imagen, para ocultar cierta cantidad de información y obtener un conocimiento general de una de las diferentes técnicas que existen para detectar si una imagen contiene o no información oculta.

Los análisis realizados a las diferentes imágenes con información oculta, se puede evidenciar que por ejemplo, en los ataques visuales realizados a aquellas imágenes que emplean el método LSB secuencial, se presenta una distorsión (franja) en cierta parte de la estego-imagen evidenciando así donde ha sido ocultada la información, cosa que con las estego-imágenes F5 no se produce. Ahora en lo referente a los ataques estadísticos en cambio, se han analizado ciertas propiedades específicas de las estego-imágenes que como se ha visto en los resultados no se ven afectadas al utilizar el algoritmo F5

De acuerdo a los resultados obtenidos en las pruebas de Estegoanálisis se concluye que en ocasiones no es suficiente utilizar un solo método para determinar si una imagen contiene o no información oculta y como se pudo apreciar los ataques de Estegoanálisis más efectivos para detectar Esteganografía LSB son el ataque visual y el ataque R-S.

Una imagen posee un rango variado en lo referente altamaño máximo de información que puede ocultar, esto dependerá del tamaño de la imagen, de la cantidad de variaciones de color que presente la imagen y principalmente del factor de calidad Q seleccionado para la imagen de salida.

Dada la sensibilidad del algoritmo F5 ante el cambio en el valor de un pixel en la estego-imagen, este algoritmo

soportaría mínimas o casi nulas modificaciones o alteraciones en la estego-imagen, dado que si esto ocurre el mensaje oculto no podrá ser recuperado.

REFERENCIAS

[1] Z. K. AL-Ani, A.A.Zaidan, B.B.Zaidan y Hamdan.O.Alanazi, «*Overview: Main Fundamentals for Steganography*,» 2010. [En línea]. Available: http://arxiv.org/ftp/arxiv/papers/1003/1003.4086.pdf. [Último acceso: Febrero]

[2] M. C. España Boquera, «*Aplicaciones y Servicios de Comunicaciones*,» de Servicios Avanzados de Telecomunicaciones, Madrid, Ediciones Díaz de Santos, 2003, p. 72.

[3] «Bilsen,» [En línea]. Available: http://www.bilsen.com/aic/tests/mandrill/mandrill.bmp. [Último acceso: Abril 2014].

[4] «Bilsen,» [En línea]. Available: http://www.bilsen.com/aic/tests/frymire/frymire.bmp. [Último acceso: Abril 2014].

[5] CyberScience Laboratory, «*Steganography Analysis and Research Center*,» Febrero 2006. [En línea]. Available: http://www.sarc-wv.com/products/stegalyzerss/stegalyzerss_csl_report.pdf. [Último acceso: Noviembre 2013].

[6] J. Fridrich, M. Goljan y D. Hogea, «*Steganalysis of JPEG Images: Breaking the F5 Algorithm*,» pp. 4-5

[7] «Flickr,» [En línea]. Available: http://www.flickr.com/photos/sirqitous/7114886543/sizes/o/in/photostream/. [Último acceso: Abril 2014].

[8] K. Hempstalk, «*Digital Invisible Ink Toolkit*,» 2005. [En línea]. Available: http://diit.sourceforge.net/doco.html#whatarethealgorithms.

[9] Herra L., Tipantuña C, «*Revisión del Estado del Arte de los Estándares de Codificación y Compresión de Audio MPEG y sus Aplicaciones* », Revista Politécnica, ISSN:1390-0129, Volumen 35, febrero,2015

[10] ITU-T, «REC-T.81,» *de Information Technology-Digital Compression and Coding of Continuous-Tone Still Images-Requirements and Guidelines*, ITU-T, Ed., 1992.

[11] kriptópolis, «*Esteganografía: Doble Uso*,» [En línea]. Available: http://www.kriptopolis.org/esteganografia-doble-uso. [Último acceso: Noviembre 2013].

[12] Mathworks, «Mathworks-PSNR,» 2013. [En línea]. Available: http://www.mathworks.es/es/help/vision/ref/psnr.html. [Último acceso: Febrero 2013].

[13] A. Muñoz, «*StegSecret. A simple steganalysis tool*,» [En línea]. Available: http://stegsecret.sourceforge.net/SpanishManual.pdf. [Último acceso: Noviembre 2013].

[14] «Picasa,» [En línea]. Available: https://picasaweb.google.com/lh/photo/ByLJLQymUIuqKbqSlBCxqtMTjNZETYmyPJy0liipFm0. [Último acceso: Abril 2014].

[15] N. Provos, «*Steganography Detection with Stegdetect*,» 2004. [En línea]. Available: http://www.outguess.org/detection.php. [Último acceso: Octubre 2013].

[16] M. Raggo, «*Spy-Hunter*,» [En línea]. Available: http://www.spy-hunter.com/stegspy. [Último acceso: Octubre 2013].

[17] G. H. Schaathun, «*Main Approaches to Steganalysis*,» de Machine Learning in Image Steganalysis, John Wiley & Sons, 2012, pp. 19-22

[18] B. Si, «*Steganalysis*,» Athabasca University, 25 Julio 2004. [En línea]. Available:http://io.acad.athabascau.ca/~grizzlie/Comp607/steganalysis.htm. [Último acceso: Octubre 2013].

[19] C. Stanley, «*Pairs of Values and the Chi-squared Attack*,» 2005

[20] M. Węgrzyn, «*Virtual Steganographic Laboratory for Digital Images (VSL)*,» 2011. [En línea]. Available: http://vsl.sourceforge.net/. [Último acceso: Octubre 2013].

[21] A. Westfeld, «*F5—A Steganographic Algorithm*,» 2001. [En línea]. Available:https://f5steganography.googlecode.com/files/F5%20Steganography.pdf. [Último acceso: Marzo 2013].

[22] Wetstone Technologies, «Stego *Suite Discover the Hiden*,» Wetstone Technologies,[Enlínea].Available:http://www.wetstonetech.com/product/1. [Último acceso: Noviembre 2013].

[23] «Wikimedia,» [En línea]. Available: http://upload.wikimedia.org/wikipedia/commons/0/0d/D8749.png. [Último acceso: Abril 2014].

[24] «Wikimedia,» [En línea]. Available: http://upload.wikimedia.org/wikipedia/commons/e/ea/LinuxOnAir_Logo.png. [Último acceso: Abril 2014].

[25] [En línea]. Available: http://3.bp.blogspot.com/_fQ-vK4KVXVE/Rdthlo2PDdI/AAAAAAAAABo/UvDfax2llvo/s400/DSC03695.JPG. [Último acceso: Abril 2014].

[26] X. Zhang, S. Wang y K. Zhang , «*Steganography with Least Histogram Abnormality*,» Shanghai University, Shanghai