ISSN 1870-4069

Análisis de calidad en imágenes esteganográficas aplicando el algoritmo LSB en códigos QR embebidos

Rodrigo Hernández Moncayo, José Martin Flores Albino,
Víctor Manuel Landassuri Moreno, Saturnino Job Morales Escobar,
Ivone Rodríguez Pérez

Universidad Autónoma del Estado del México,
Maestría en Ciencias de la Computación,
México

rhernandezm403@alumno.uaemex.mx,
{jmfloresa, vmlandassurim, sjmoralese,
irodriguezp} @uaemex.mx

Resumen. Se presenta un estudio del efecto en la imagen esteganográfica al embeber un Código de Respuesta Rápida (Quick Response Code) en otro código QR por medio de la técnica esteganográfica de sustitución del Bit Menos Significativo (LSB). Se plantea su aplicación como marca de agua donde en la primera parte se calculan los parámetros para inserción de un código QR en otro código QR, basados en la versión del código contenedor y del código QR oculto. En la segunda parte, se presenta el efecto en la calidad de imagen del código QR usado como cubierta dependiente del bit usado para ocultar el segundo código QR. Se presenta también el cálculo de las métricas de calidad de imagen, similitud y fidelidad visual para observar su comportamiento. Los resultados permiten observa que el código QR embebido puede recuperarse usando desde el LSB hasta el 5to bit.

Palabras clave: Esteganografía, algoritmo LSB, código QR embebido.

Quality Analysis in Steganography Images Using the LSB Algorithm in Embedded QR Codes

Abstract. A study of the effect on the steganographic image when embedding a Quick Response Code (QR Code) is presented using the steganographic technique of replacing the Less Significant Bit (LSB). The application as watermark is proposed where the first part calculates the parameters for inserting a QR code into another QR code based on the container version code and the hidden QR code. The second part presents the effect on the image quality of the QR code used as a bit-dependent cover used to hide the second QR code. Also is shown the metrics of image quality similarity, and visual fidelity to observe its behavior. The result indicates that the embedded QR code can be retrieved using from the LSB to the 5th bit.

Keywords: Steganography, LSB algorithm, embedding QR code.

1. Introducción

La esteganografía es el arte y la técnica de ocultar información en un medio que la hace imperceptible al observador. Esta técnica es eficaz para ocultar información que se transmite por un canal de mensajes con alta densidad de datos digitales; por ejemplo, textos, imágenes y voz [1].

Los elementos del proceso esteganográfico relacionan a un objeto portador o cubierta, que es algún medio digital y el mensaje oculto o secreto que se embeberá en el portador, creando así el llamado estego objeto, que es la mezcla del portador y del mensaje oculto y la llave o clave esteganográfica que orienta para recuperar el mensaje oculto [2].

La esteganografía es una herramienta para reducir la vulnerabilidad latente en medios digitales. Da seguridad entre emisor y receptor al incorporar información secreta y hacerla imperceptible para otros observadores. Se ha aplicado en la autenticación de documentos digitales, como: pasaportes, identificaciones de nacionalidad y licencias para conducir. En este tipo de aplicaciones, el mensaje secreto funciona como una marca de agua embebido en los documentos sensibles, siendo un recurso para validar su autenticidad [3].

Actualmente, los Quick Response Codes (códigos QR), son ampliamente usados para la identificación rápida de productos y para facilitar el acceso a información en el espacio digital. Son imágenes digitales que, al ser explorada, por la cámara de un teléfono inteligente, extraen la información codificada. Los códigos QR se utilizaron por primera vez en 1994 por Denso Wave, empresa del grupo Toyota. Desde 2011, y debido al uso general de la tecnología móvil, los códigos QR son extensamente usados como un medio de rápido acceso a la información [4].

Los códigos QR son imágenes que pueden duplicarse al copiarse a través de la captura de imagen en pantalla de un dispositivo móvil o al tomarles una fotografía, y la imagen reproducida podrá ser explorada para decodificar la información que contiene. Lo anterior hace que los códigos QR sean un medio para difundir rápida y fácilmente información. Por otro lado, hay casos donde se necesita autenticar el origen del código QR, siendo ahora la facilidad de reproducirlo y el acceso a la información vayan en contra de validar la originalidad del código QR.

Se propone así en este trabajo analizar la posibilidad de aprovechar que los códigos QR son imágenes digitales y con técnicas esteganográficas agregar una imagen digital de otro código QR como marca de agua, y así permita su validación, siendo un medio para comprobar el origen del código QR.

Este artículo presenta una serie de experimentos sobre el efecto del algoritmo esteganográficos LSB (The Least Significant Bit), para incrustar o embeber en un código QR un segundo código QR. Se analiza también el efecto en la calidad de la imagen esteganográfica para cuantificar su alteración. Existen diversos factores que impacta en la calidad de la estego imagen, entre estos la carga de datos del mensaje oculto y el algoritmo esteganográfico usado.

Para cuantificar el efecto del algoritmo esteganográfico se usa el Error Cuadratico Promedio (Mean Square Error, MSE) y la Tasa de Ruido a Señal, (Peak Signal to Noise Ratio, PSNR).

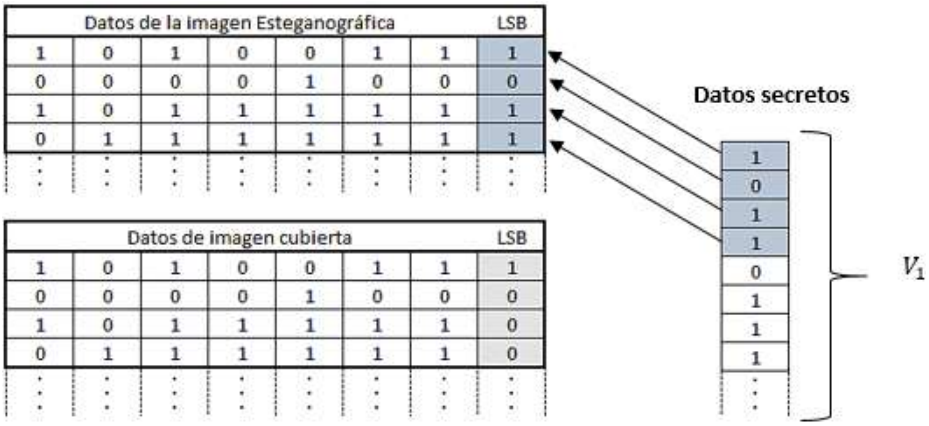

Fig. 1. Algoritmo esteganográficos Least Significant Bit.

A continuación, se presentan el método esteganográfico del bit menos significativo que se aplicará en imágenes con código QR, se dará la descripción de los códigos QR basados en la versión y sus parámetros de capacidad de información que puede contener.

1.1. Algoritmo esteganográfico the Least Significant Bit (LSB) y métricas de calidad de imagen

El algoritmo de sustitución del bit Menos Significativo (LSB) es la herramienta clásica para ocultar información en imágenes. Es una técnica del dominio espacial y se implementa al variar ligeramente el valor de los pixeles de la imagen cubierta para incorporar la información secreta [5].

En las imágenes en escala de grises cada píxel de la imagen es un elemento de una matriz, tomando valores en el intervalo de 0 a 255, siendo necesarios 8 bits por píxel. En las imágenes a color se usan 3 cadenas de N-bits/color (Red, Green, Blue), donde N es el número de bits para el color o profundidad de color (N= 8, 16 o 32 bits) [6].

Se muestra en la Fig. 1, el algoritmo LSB, donde los bits que representan a los pixeles de la imagen secreta se apilan ordenadamente en un vector V_1. Se realiza una comparación entre los bits menos significativos (LSB) de los píxeles de imagen cubierta y los bits del vector V_1. Si coinciden los bits, no se modifica el bit LSB de la imagen cubierta; en caso contrario, se sustituye el bit LSB de la imagen cubierta por el valor del bit de la imagen secreta. Al utilizar este método la información de la imagen secreta queda embebida en la información de la imagen cubierta, generando la estego imagen que es la imagen cubierta con la imagen secreta incorporada.

Para imágenes en tonos de la imagen secreta afecta al bit LSB de los pixeles de la imagen cubierta que sean necesarios para la cantidad de bits de la imagen secreta. En imágenes a color (RGB), los bits de la imagen secreta se reparten en los bits LSB de cada canal de color de la imagen cubierta [7].

El algoritmo LSB tiene la característica de ser un algoritmo reversible lo que permite recuperar el mensaje oculto de manera exacta, donde la llave será la información del algoritmo LSB y el tamaño de la imagen secreta. Para medir el efecto en la imagen estego se han propuesto diversos índices como referencia al cambio en la imagen estego.

Cualidades esteganográficas: En la esteganografía se definen tres cualidades: Capacidad, Robustez y la Imperceptibilidad. Al realizar el proceso esteganográfico se busca balancear estás cualidades. La Capacidad mide la cantidad de información que puede ser incrustada en un medio esteganográfico o carga útil, se mide en bits por píxel (bpp). La Robustez es la medida de la resistencia a los ataques realizados por sistemas de estegoanálisis.

La Imperceptibilidad mide el grado de indetectabilidad de la información secreta por un observador. Para valorar el efecto esteganográfico en imágenes como medio de ocultación de la información, se suelen utilizar índices que permiten valorar el grado de cambio en el medio de manera que el proceso genere estego objetos con el mínimo de distorsión, con la máxima carga y robustez. En este trabajo se calculan los Índice de Calidad de Imagen (IQAM), el Error Cuadrático Medio (MSE) la Relación de Señal a Ruido (PSNR) y la Fidelidad de la Información Visual (VIF) [8, 9].

Los algoritmos esteganográficos deben de mantener un equilibrio es sus parámetros, que permitan mantener la eficiencia y seguridad de estos y lograr que, al aumentar la imperceptibilidad no se sacrifique la robustez o al aumentar la robustez no se limite la capacidad.

Fidelidad de la información Visual (Visual Information Fidelity): Este modelo retoma algunos conceptos de la teoría de la información como el modelado de escenas naturales (NSS) y el sistema visual humano (HVS). Para su aplicación en esteganografía, toma la imagen de portada (*C*) para cuantificar su información, y la imagen estego (*S*) para saber la cantidad de información que puede ser extraída. Al combinarlas se puede medir la degradación que puede sufrir la imagen estego [10]. Este índice (ir a las referencias para los detalles) se representa por medio de la ecuación (1):

$$VIFF(S_k, \mathrm{C_b}) = \frac{\sum_K \sum_b \log_2 \left(1 + \frac{g_{k,b}^2 * \left(\sigma_{\mathrm{k,b}}\right)^2}{\left(\left(\sigma_{k,b}^d\right)^2 - g_{k,b}^2 * \left(\sigma_{k,b}^r\right)^2 + {\sigma_N}^2\right)} \right)}{\sum_k \sum_b \log_2 \left(1 + \frac{\left(\sigma_{k,b}^r\right)^2}{{\sigma_N}^2} \right)}. \quad (1)$$

Error Cuadrático Medio (Mean Square Error): Para medir el error que hay entre dos conjuntos de datos y el cálculo se realiza promediando la intensidad al cuadrado de la imagen original (*C*) y los pixeles de la estego imagen (*S*) donde *M* y *N* son filas y columnas respectivamente [6]. Este cálculo servirá también en la métrica PSNR la cual está definida por la ecuación 2:

$$MSE = \frac{1}{M\ xN} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(C_{i_j} - S_{i_j} \right)^2. \quad (1)$$

Un MSE igual a 0 indica que las imágenes son idénticas.

Métrica Relación Señal a Ruido Pico (PSNR): Esta métrica se usa para observar las distorsiones que existen entre la imagen original y la imagen estego, además puede indicar si existe un grado de distorsión mayor al momento de realizar la compresión en una imagen y se define por la siguiente ecuación (3):

$$PSNR = 10xlog_{10}\left(\frac{255^2}{MSE}\right), \tag{2}$$

donde las unidades de PSNR son decibelios (dB). Para la ecuación (3) se toma 255 por ser la intensidad máxima para un píxel. La clasificación PSNR para una imagen se realiza con el siguiente criterio: $PSNR$ < 30 dB es no aceptable, $PSNR$ entre 30 a 40 dB es aceptable y $PSNR$ > 40 dB es muy buena [6].

Índice de Calidad de Imagen Universal (UIQI): La métrica UIQI tiene la capacidad para medir la pérdida de información ocurrida durante los procesos que impliquen la degradación de la imagen tomando como base tres índices: pérdida de correlación, distorsión de luminancia y distorsión de contraste. El rango de evaluación en la calidad de imagen es dinámico, va de -1 a 1, entre más cercano es a 1 mejor será la calidad de la imagen evaluada. En la ecuación (4) se define esta métrica [11]:

$$\text{UIQI} = \frac{4\sigma\text{CS}}{\sigma^2 c + \sigma^2 s} \times \frac{\bar{C}\,\bar{S}}{C^{-2}\,S^{-2}}. \tag{4}$$

Índice de Semejanza Estructural (SSIM): La métrica SSIM [8], determina la similitud que existe entre una imagen estego y la original y se determina por la ecuación (5):

$$SSIM(s,y) = \frac{\left(2\mu_x\mu_y + c_1\right)\left(2\sigma_{x_y} + c_2\right)}{(\mu_x{}^2 + \mu_y{}^2 + c_1)(\sigma_x{}^2 + \sigma_y{}^2 + c_2)}. \tag{5}$$

Cuando c1 = 0 y c2 = 0, SSIM se vuelve igual a Q como un caso especial. Mientras el resultado de SSMI se acerque a 1, el rendimiento será mejor.

1.2. Código de respuesta rápida, QR (Quick Response Code)

Los códigos Quick Response (QR) fueron creados por la compañía Denso Wave Inc. para facilitar el acceso instantáneo de información al codificarla para que sea recuperada por medios ópticos. Están normados en el estándar ISO/ EEC18004:2006 y es de acceso libre.

El código QR es una imagen de dos dimensiones que codifica información por medio de puntos oscuros sobre un fondo claro. Los patrones de imagen codifican ciertas estructuras que facilitan la identificación de parámetros para la interpretación, almacenamiento y corrección de errores en la información [12].

En la Tabla 1 se resumen el tipo de formato (numéricos, alfanuméricos, binario y Kanji), capacidad límite y caracteres que admite el código QR para su implementación en el Modelo 1 y 2 que son los más frecuentes.

Tabla 1. Tipos Datos y capacidad límite que admite el código QR [13].

Formato	Capacidad de datos	Caracteres
Numérico	7089 caracteres	0-9
Alfanumérico	4296 caracteres	0-9, A-Z (mayúsculas) espacio $ % ‘+ -, /:
Binario	2953 bytes	Codificación por defecto: ISO 8859-1 (QRC 2005)
Kanji	1817 caracteres	Desplazamiento JIS X 0208

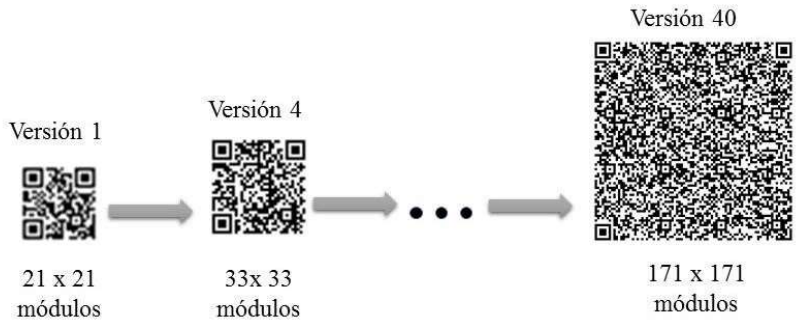

Fig. 2. Ejemplo de diferentes versiones código QR [4].

La versión para un código QR depende del tamaño de la matriz de puntos de imagen (módulos). El Modelo 1, va de la versión 1 hasta la versión 14; al Modelo 2 pertenecen de la versión 15 hasta la 40. La versión corresponde a la dimensión de la matriz del código QR y está relacionado con su capacidad de caracteres de información que soporta. Las versiones van de $n \times n$, donde $n = 17 + 4 \cdot i$, donde i=1, …, 40. Así que la versión 1, es un QR de tamaño 21×21; la versión 2, es un QR de tamaño 25×25, respectivamente.

Otro factor que está relacionado con la capacidad de datos de un código QR, es el nivel del factor de corrección de errores (ECC). Aquí se usa una codificación tipo Reed-Solomon y se especifican cuatro niveles: L (7%), M (15%), Q (20%) y H (30%), entre más alto el nivel de corrección de errores, mayor es la capacidad para recuperar la información por deterioro de la imagen, pero reduce la capacidad de datos de información.

El tamaño menor de los códigos QR corresponde a la versión 1, de 21×21 módulos, se le suman 2 módulos de margen a los lados, dando 25 × 25 módulos del código QR, cada módulo es de 4 píxeles, por lo que la imagen tiene una dimensión de 100 × 100 píxeles. Al imprimirlo a 100 pixeles por cm (100 ppcm.) el código QR será de 1 cm de ancho y 1 cm de alto.

Para la distancia de detección se recomienda la regla de 1:10, tal que la distancia de detección de un código de versión 1 es de al menos 10 cm. En la Fig. 2, se observa el código QR en versión 1 la cual es la versión mínima, al ir aumentando su capacidad van también aumentando sus módulos y su complejidad, como se observa en la versión 40 [4].

Tabla 2. Relación entre Imagen oculta e imagen cubierta.

Versión código QR oculto	Módulos	Módulos + margen: N	$2\sqrt{2}N$	Módulos sin margen	Módulos por versión	Versión de la imagen cubierta
1	21	25	71	67	69	13
2	25	29	83	79	81	16
3	29	33	94	90	93	19
4	33	37	105	101	101	21
5	37	41	116	112	117	25
6	41	45	128	124	125	27
7	45	49	139	135	137	30
8	49	53	150	146	149	33
9	53	57	162	158	161	36
10	57	61	173	169	169	38
11	61	65	184	180	-	-

1.3. Revisión de la literatura sobre el tema esteganografía y códigos QR

Los métodos esteganográficos se han utlizado para embeber información en códigos QR, como por ejemplo en [14] se presenta un resumen de diferentes trabajos relacionados sobre el tema, mostrando como se utiliza un código QR como imagen de portada y otro código QR oculto embebido y encriptado por medio de una clave secreta.

La lectura del código QR oculto se lleva a cabo por medio de un lector modificado. Además, presenta el uso de las técnicas esteganográficas en el dominio de frecuencia por medio de la Transformada Wavelet Discreta Haar, debido a que han mostrado robustez a ataques de estegoanálisis. Otra técnica utilizada es la LSB en su forma de sustitución o secuencial, por mostrar una gran capacidad de carga útil.

Así mismo presenta formas para encriptar la información utilizando métodos tipo AES (Estándar Avanzado de Encriptación) y por el método de tipo RSA (Rivest, Shamir y Adleman). Masoud Alajmi et. al. en [15] proponen un sistema utilizando un código QR como portada con información común y encriptación AES o RSA, para una imagen oculta. Utilizan la reversibilidad del algoritmo LSB y modifican el mensaje en código ASCII a binario para realizar el proceso esteganográfico con el objetivo de que al ser atacado el sistema el mensaje secreto sea confundido con ruido.

2. Desarrollo

2.1. Dimensiones para embeber un código QR en otro código QR.

La esteganografía ha tenido un interés particular como medio para ocultar él envió de información por medios sin que despierten sospecha. Está claro que existe la posibilidad de que un mensaje oculto se vea como una falla de seguridad; sin embargo, podría ser un medio para transmitir información confidencial. Entonces es un debate permanente el temor que tienen algunos agentes a lo que se les oculta y el derecho a la confidencialidad de la comunicación.

Tabla 3. Cálculo de formato físico para código QR.

Versión código QR oculto	Módulos más margen	Píxeles (4 p/m)	Dimensión (100 ppcm)	Módulos con imagen oculta	Píxeles	Dimensión (cm.×cm.)
1	25	100	1	73	292	2.92
2	29	116	1.16	85	340	3.4
3	33	132	1.32	97	388	3.88
4	37	148	1.48	105	420	4.2
5	41	164	1.64	121	484	4.84
6	45	180	1.8	129	516	5.16
7	49	196	1.96	141	564	5.64
8	53	212	2.12	153	612	6.12
9	57	228	2.28	165	660	6.6
10	61	244	2.44	173	692	6.92

Desde este punto de vista, el explorar la posibilidad de incrustar información en un código QR, dado su uso general en el ciberespacio, ya presenta por sí mismo un tema de interés. El aporte de este trabajo es definir la estructura de la imagen cubierta y la imagen estego utilizando códigos QR y su importancia al implementarlas en un sistema esteganográfico, ya que al realizar los cálculos de capacidad de los dos elementos se puede aprovechar de forma eficiente la carga útil.

Así al utilizar los códigos QR como elementos de un sistema esteganográfico se debe tomar en cuenta su versión, los niveles de corrección, además de la capacidad de información que es posible almacenar. También es requisito conocer el tamaño mínimo por pixeles que debe contener, para evitar que la lectura sea errónea al ocultar o extraer información, además en el caso del algoritmo LSB al medir los niveles de degradación pasando por los distintos bits que componen una imagen es posible conocer que tan eficiente puede ser el código QR en sus niveles de corrección.

Al ser el algoritmo LSB reversible en la imagen secreta se puede implementar como una marca de agua, dotando entonces a estos elementos de un nivel especial de seguridad, que pudiera aplicarse para autentificar la procedencia y autoría de distintos elementos que interactúan en el entorno social, tales como: documentos públicos y privados, medicamentos, ropa, artículos domésticos etc. Las marcas de aguas digitales buscan esconder una serie de bits dentro de un medio digital para identificar autoría, distribuidores, documentos, e imágenes, etc.

El diseño debe permitir que sea invisible, para evitar su manipulación. Al implementar una marca de agua eficaz se deben de contemplar tres parámetros: la capacidad, la robustez y la imperceptibilidad, en el presente trabajo se abordarán y se pondrán a prueba dos áreas, a) la capacidad y b) la imperceptibilidad, estas características son similares a las esteganográficas descritas en la sección 1.1 [13]. Para la implementación esteganográfica en la imagen del QR cubierta y del código QR oculto se convirtieron las imágenes a tonos de gris. Como se explicó en la sección 1.1.

El algoritmo LSB, incorpora la información del código QR oculto en los bits menos significativos de los valores de tono de gris de los píxeles código QR de cubierta.

Tabla 4. Parámetros de las imágenes de Código QR.

Imagen Oculta				**Imagen Portada**			
Version	Modulos	ECC	Alfanumerico	Versión	Módulos	ECC	Alfanumerico
1	21 x21	L	41	13	69 x 69	L	619
10	57x 57	H	174	13	69x69	H	269
				38	169 x169	H	1591

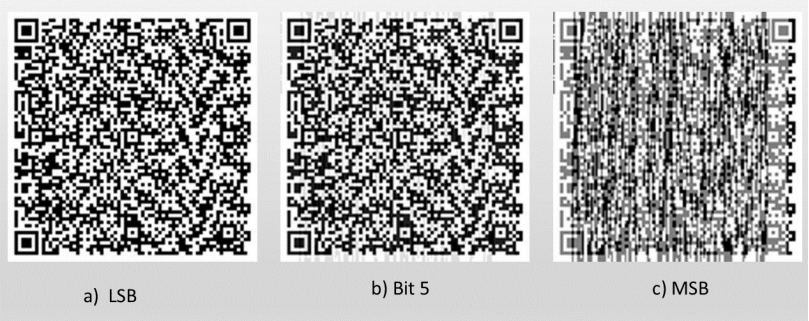

Fig. 3. Aplicación de esteganografía a imágenes con código QR.

Esto provoca que a lo más el cambio de tono de los pixeles del código QR cubierta sea de $\pm\ 1/255$, esto es menos del 0.4% en el tono del píxel, lo que hace que sea difícilmente perceptible de forma visual, ya que el ojo humano puede detectar en promedio sólo 30 tonos de gris.

Lo que implica que el cambio tonal deber ser de poco más de 8 en el cambio para el bit menos significativo para hacerlo perceptible. La imagen del código QR secreto en capacidad, es la versión 1 que cuenta con 21×21 módulos, más 2 módulos en el margen de zona de silencio, lo que da una imagen de dimensiones de 25×25 módulos, que está relacionado con su tamaño físico al usar 4x4 píxeles para cada módulo (100×100 pixeles) y una resolución de 100 píxeles por centímetro.

Para estimar el número de píxeles que se requieren de la imagen del código QR cubierta, se considera una matriz cuadrada de píxeles en el intervalo {0, 255}, es decir, equivalente a 8 bits. Se usa el bit LSB de cada 8 para guardar por sustitución un bit de información de la imagen oculta.

De forma general, si la cantidad de datos de la imagen cubierta de $N\times N$ es N^2, y el número de datos de la imagen oculta de tamaño $M\times M$ es M^2, la relación entre estos números es dada (6). Para el cálculo de la imagen cubierta se parte de la versión y el número de módulos que se ocultan, se suman dos módulos por lado de margen, se aplica la formula (6):

$$N^2 = \frac{M^2}{8} \text{lo que implica: } 2\sqrt{2}N = M\ . \tag{6}$$

El resultado es el módulo total para la imagen cubierta, se le restan 2 módulos de margen por lado y el resultado es el número de módulos mínimo para la imagen cubierta, finalmente se selecciona la versión que tenga igual o mayor número de módulos [16]. Este proceso se representa en la Tabla 2.

Tabla 5. Resultados para las métricas UIQI, SSMI, VIF y PSNR.

Conjunto A (imágenes QR versión 1 incrustada en QR versión 13 y ECC L)					**Conjunto B (imágenes QR versión 1 incrustada en QR versión 13 y ECC H)**			
Bit	UIQI	SSMI	VIF	PSNR	UIQI	SSMI	VIF	PSNR
1	0.99999	1	0.9893	51.56	1	1	0.9893	51.5367
2	0.99996	0.9999	0.9639	45.5394	1	0.9999	0.964	45.5161
3	0.99983	0.9998	0.9001	39.5188	0.9998	0.9997	0.9003	39.4955
4	0.99932	0.999	0.7901	33.4982	0.9993	0.999	0.7905	33.4749
5	0.99729	0.9958	0.6451	27.4776	0.9973	0.9957	0.6458	27.4543
6	0.98927	0.9826	0.4755	21.457	0.9892	0.9822	0.4764	21.4337
7	0.95793	0.9246	0.2864	15.4364	0.9576	0.9229	0.2868	15.4131
8	0.84256	0.6776	0.0964	9.41581	0.8414	0.6716	0.0933	9.39253

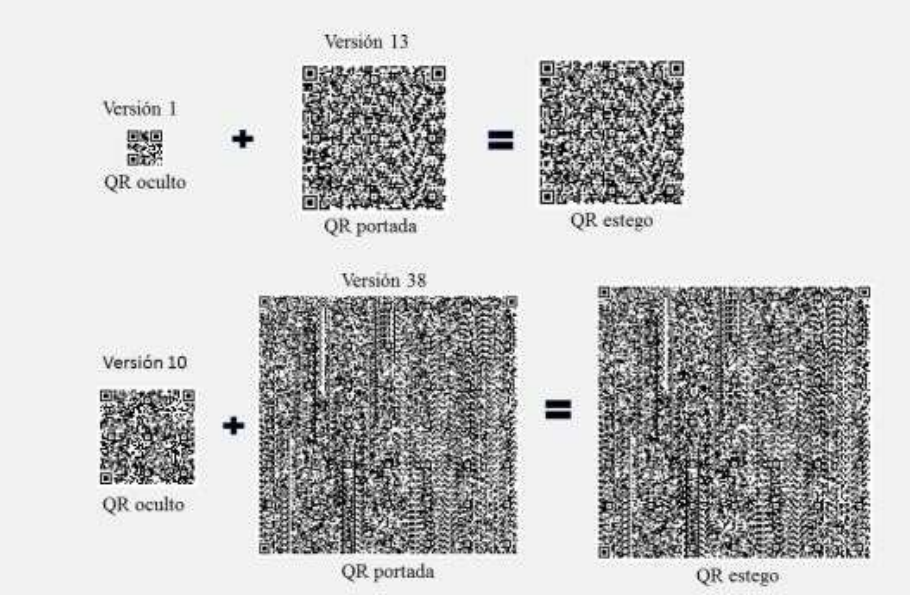

Fig. 4. Cambios en las imágenes estego del conjunto A al cambiar los bits a) LSB, b) 5to. bit y c) MSB.

Como se puede apreciar en la primera fila, si se quiere ocultar un código QR de versión 1 se necesita un código QR cubierta de versión 13. La Tabla 3 nos muestra el tamaño físico del código QR oculto y de cubierta.

Por ejemplo, de la primera línea, un código QR oculto de versión 1 de 21+4=25 módulos con una resolución de 4 píxeles por módulo, si se imprime a una resolución de 100 píxeles por cm, el código mide 1 cm por lado.

Un código QR correspondiente a una versión 13 de 73 módulos (69 módulos más 4 módulos de margen) son suficientes para incluir los datos de imagen del código QR oculto, puesto con 4 píxeles por módulo dan 292 píxeles que a una resolución de 100 ppcm. tendrá un tamaño de 2.92 cm × 2.92 cm.

Tabla 5. Resultados para las métricas UIQI, SSMI, VIF y PSNR.

Conjunto A (imágenes QR versión 1 incrustada en QR versión 13 y ECC L)					**Conjunto B (imágenes QR versión 1 incrustada en QR versión 13 y ECC H)**			
Bit	UIQI	SSMI	VIF	PSNR	UIQI	SSMI	VIF	PSNR
1	0.99999	1	0.9893	51.56	1	1	0.9893	51.5367
2	0.99996	0.9999	0.9639	45.5394	1	0.9999	0.964	45.5161
3	0.99983	0.9998	0.9001	39.5188	0.9998	0.9997	0.9003	39.4955
4	0.99932	0.999	0.7901	33.4982	0.9993	0.999	0.7905	33.4749
5	0.99729	0.9958	0.6451	27.4776	0.9973	0.9957	0.6458	27.4543
6	0.98927	0.9826	0.4755	21.457	0.9892	0.9822	0.4764	21.4337
7	0.95793	0.9246	0.2864	15.4364	0.9576	0.9229	0.2868	15.4131
8	0.84256	0.6776	0.0964	9.41581	0.8414	0.6716	0.0933	9.39253

2.2. Calidad de imagen del uso del algoritmo LSB y códigos QR

Las pruebas se llevaron a cabo en imágenes con código QR con contenido codificado por textos alfanuméricos. Se eligió este tipo de información porque es comúnmente utilizada tanto en medios digitales como en impresos. El programa utilizado para la creación de las imágenes con código QR fue codificado en lenguaje Python, usando la librería QR Code [17].

Para las pruebas, se implementaron las configuraciones indicadas en la Tabla 2, lo que representa modificar el número de versión, el factor de corrección y valor de pixeles por cada cuadro. Las imágenes están en formato PNG, los datos de las imágenes creadas para el proceso esteganográfico están divididas en imágenes ocultas y de portada. Se implementó el algoritmo LSB codificado en Matlab según la descripción de la sección 2.1.

Las imágenes con código QR de la Tabla 4 muestran el efecto de usar el LSB hasta el bit más significativo (MSB) para ocultar la información. El propósito de insertar los bits de la imagen secreta en bits de mayor peso que el LSB es para medir como se altera la imagen de cubierta al insertar la imagen secreta.

La aplicación del algoritmo esteganográfico LSB se da por medio de los siguientes pasos: Primero se elige el código QR oculto y el código QR cubierta de acuerdo con los valores de la Tabla 2, para responder a las características de carga útil que se calcula en la imagen cubierta de acuerdo con la ecuación (6) y en formato PNG, este formato se utilizó para evitar perdida de datos por compresión.

En el segundo paso se realiza el proceso de reemplazo de los bits con el algoritmo LSB para crear una estego imagen que contiene la imagen oculta, pero además de usar el LSB se aplica el algoritmo esteganográfico en bits más significativos. Este proceso se realizó para crear estego imágenes para cada uno de los 8 bits que se tienen en la imagen cubierta.

En la Fig. 3 se muestra el resultado del proceso de aplicación del algoritmo LSB para dos imágenes a ocultar de acuerdo con las propiedades de la tabla 4, en las cuales para la versión 1 incrustada en versión 13, se aplicó un nivel de corrección de error bajo (ECC L). En la versión 10 incrustada en la versión 38, se usó un nivel de corrección de error alto (ECC H). El efecto en la estego imagen, en ambos casos, no afectó la decodificación del texto con el teléfono inteligente.

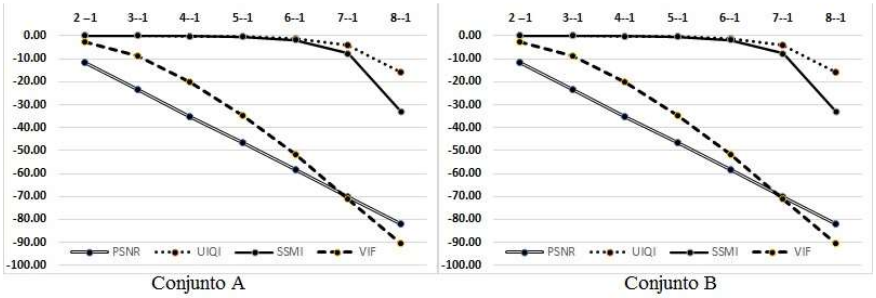

Fig. 5. Tasa porcentual relativa al LSB para el conjunto A de imágenes y B.

Al final se utiliza la llave del algoritmo LSB para recuperar la imagen oculta, recuperándose correctamente. Para conocer el grado de similitud, calidad de imagen y fidelidad visual entre la imagen de portada y la estego imagen se utilizaron las métricas propuestas en la primera sección programadas en el lenguaje Python con la librería "Sewar" que permite el cálculo PSNR, SSIM, UQUI y VIF [18].

Las imágenes que se tomaron como portada fueron las de un código QR versión 13 y la imagen oculta fue la versión 10, descritas en la Tabla 4, el proceso esteganográfico que se realizó en ellas fue desde LSB (1er. bit) hasta MSB (8vo. bit) formándose dos conjuntos de imágenes A: imágenes de un código QR versión 1 incrustada en código QR versión 13 y ECC L, y B: imágenes QR versión 1 incrustada en imagen de un código QR versión 13 y ECC H. Los cálculos de los índices para cada conjunto de imágenes se resumen en la Tabla 5.

Al aplicar el algoritmo esteganográfico desde el LSB hasta el MSB, la imagen de portada sufre varios cambios como se observa en la Fig. 4. Este comportamiento fue similar para el conjunto de imágenes A y B descritos en la Tabla 5, del 2do bit al 4to bit se empezó a mostrar degradación en la imagen en tonos visibles en gris que son perceptibles al aplicar una ampliación del 50%, y detectable en los valores de las métricas VIF y PSNR que se muestran en la Tabla 5, donde se presentan los índices de calidad entre la imagen estego y la imagen cubierta.

Notar que la tendencia a descender su valor, deduciendo que la fidelidad de la imagen se empieza a deteriorar, pero las métricas SSMI y UIQUI no muestran cambios significativos y se mantienen estables a pesar de mostrar un decremento en la calidad de la imagen cubierta como se muestra en la Fig. 4.

La aplicación del algoritmo en el 5to bit al 8vo bit (MSB), es donde se muestran cambios más significativos en la imagen estego como se observan en la Fig. 4b y 4c. Se notan marcas de la imagen oculta. Al usar el 8vo bit, la imagen estego presenta decoloración importante. Los índices VIF y PSNR son malos y la degradación de la imagen es notable. Las métricas UIQUI y SSMI muestran cambios relevantes por el uso del 7mo bit u 8vo bit, demostrando que los cambios deterioran considerablemente la capacidad de similitud y calidad de imagen.

En la Fig. 5, se muestra la tasa de cambio relativo para el conjunto A y B de imágenes estego descritas en la Tabla 5, muestran que a medida que se va cambiando el bit en la imagen cubierta, la imagen estego va perdiendo sus características de Fidelidad Visual, Similitud y Calidad de Imagen.

El cambio más significativo se observa en las métricas VIF y PSNR, mientras que en las métricas SSIM y UIQI el índice de cambio es visible a partir del 6to bit. Es notable que el comportamiento de los índices SSIM y UIQI, se asocia más a la pérdida de calidad en la imagen estego. Este resultado se interpreta como que en este tipo de imágenes podría incrustarse más de una imagen de código QR, al observar que podrían usarse además del bit LSB ya que la percepción en la imagen estego ocurre hasta el 6to bit.

Esto podría incrementar la capacidad de carga de la imagen cubierta. También se observa que la propiedad ECC de los códigos QR de cada conjunto a pesar de ser diferente no interfiere directamente en los índices de la métrica ya que el valor es similar para ambos conjuntos.

3. Conclusiones

El proceso esteganográfico llevado a cabo en las imágenes de portada con código QR, fue posible al usar los parámetros calculados e indicados en la Tabla 4. Al aplicar el algoritmo LSB en la imagen de cubierta y producir la imagen estego, pasó completamente desapercibida y por los cálculos obtenidos de las métricas de calidad de imagen, se nota que el cambio poco perceptible.

Los cambios importantes en la imagen estego se mostraron al usar el algoritmo esteganográfico en el 5to bit 5 al 8vo bit, donde el parámetro de imperceptibilidad se reduce, haciendo que el proceso esteganográfico sea detectable. La lectura de la imagen estego, la cual contiene información del código QR, fue posible en una distancia de 10 veces la dimensión física del código QR. Al conocer las proporciones que debe contener una imagen con código QR para poder ocultarla dentro de otra, permite que pueda pasar desapercibida e indicar que podría usarse más de un bit y así aumentar la cantidad de información que podría contener la imagen de portada.

Al observar la Fig. 5, fue interesante notar que los índices SSIM y UIQI mostraron como la calidad de la imagen estego no es afectada en una escala importante al usar los bits del 1 (LSB) a 6to bit de la imagen estego. Al ser el algoritmo LSB reversible el proceso de la recuperación del código QR oculto se logró satisfactoriamente en todos los casos. Al recuperar el QR podría usarse como como una marca de agua y aplicarse para autentificar códigos QR. Como trabajo futuro se buscará probar la robustez de las imágenes estego con código QR y así, conocer la resistencia ante ataques de estegoanálisis.

Agradecimientos. Al CONACYT por el apoyo a la Maestría en Ciencias de la Computación de la Universidad Autónoma del Estado de México.

Referencias

1. Yahya, A.: Steganography techniques for digital images. Palapye.Springer (2019)
2. Caballero, H., Muños, V., Ramos, M., Romero, M.: Steganography method through fractal dimension and lsb algorithm: A new perspective on RGB images. Tecnología Educativa Revista CONAIC, vol. 6, no. 1, pp. 25–30 (2019)

3. Centurión, A., Soria, A., Moreno, E.: Un algoritmo esteganográfico vinculado a los cuadrados mágicos. REDEL, Revista Granmense de Desarrollo Local, vol. 3, no. 4, pp. 225–238 (2019)
4. Denso Wave Incorpored.QRCode®. Essentials (2021) https://www.qrcode.com/en/about/version.html. [Último acceso: 1 abril 2021]
5. Muñoz, A.: Privacidad y ocultacion de informacion digital Esteganografía. Protegiendo y atacando redes informáticas, RA-Ma, pp. 35–38 (2017)
6. Mahdi, M., Mohd, M. S., Abass, F., Sabah, M., Salman, H.: Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats. International Journal of Engineering & Technology, vol. 7, no. 4, pp. 3505–3514 (2018)
7. Mahdi, M., Mohd, M., Abass, F., Sabah, M., Al-Wan, A., Amir, N.: An extensive analysis and conduct comparative based on statistical attach of LSB substitution and LSB matching. International Journal of Engineering & Technology, vol. 7, no. 4, pp. 4008–4023 (2018)
8. Jawad, I., Premaratne, P., Vial, P. J., Halloran, B.: Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research. Neurocomputing, vol. 335, pp. 299–326 (2019)
9. Muhammad, K., Ahmad, J., Jan, Z., Sajjad, M., Rehman, N. U.: CISSKA-LSB: Color image steganography using stego key-directed adaptive LSB substitution method. Multimed Tools and Applications, vol. 76, no. 6, pp. 8597–8626 (2017)
10. Pramanik, S., Singh, R., Ghosh, R.: Application of bi-orthogonal wavelet transform and genetic algorithm in image steganography. Multimedia Tools and Applications, pp. 1–20 (2020)
11. Guzmán, Y., Pérez, E., Centurión, A.: Un algoritmo esteganográfico adaptativo para lograr mayor indetectabilidad. Lecturas Matemáticas, vol. 41, no. 2, pp.149–164 (2020)
12. Castro-Acuña, N., Leguizamón-Páez, M., Mora-Lancheros, A.: Análisis de métodos y técnicas existentes para minimizar agujeros de seguridad al usar códigos QR. Revista UIS Ingenierías, vol. 18, no. 4, pp. 157–172 (2019)
13. Padrón, A., Prieto, R., Treviño, C.: Clave óptica privada mediante un código QR cifrado. Sistemas, Cibernética e Informática, vol. 17, no. 2, pp. 5–15 (2020)
14. Remya, P.: A review on stegnography in QR codes. International Research Journal of Engineering and Technology (IRJET), vol. 5, no. 5, pp. 4294–4296 (2018)
15. Alajmi, M., Elashry, I., El-Sayed, H., Faragallah, O.: Steganography of encrypted messages inside. IEEE Access, vol. 8, pp. 27861–27873 (2020)
16. Luque, J.: Códigos QR. Manual formativo de ACTA, vol. 63, pp. 9–28 (2012)
17. Loop, L.: The python package index (PyPI), pure python QR code generator. (2021) Available: https://pypi.org/project/qrcode/. [Último acceso: 12 abril 2021]
18. Khalel, A.: The python package index (PyPI). Project Sewar, (2021) Available: https://pypi.org/project/sewar/. [Último acceso: 7 abril 2021]