# Confidencialidad de datos mediante el grabado de códigos QR cifrados: ID-Óptico

**Alejandro Padrón Godínez**[(a), (b)1,2], **Rafael Prieto Meléndez**[1], **Carlos G. Treviño-Palacios**[2]

[1] Instituto de Ciencias Aplicadas y Tecnología, Universidad Nacional Autónoma de México, CDMX-México

[2] Instituto Nacional de Astrofísica, Óptica y Electrónica, Tonantzintla, Puebla-México

alejandro.padron@icat.unam.mx, rafael.prieto@icat.unam.mx, carlost@inaoep.mx

**DOI** 10.33412/pri.v11.1.2534

**Resumen:** *La combinación de mecanismos de seguridad mediante Criptografía y Esteganografía trae consigo aumentar el nivel de seguridad en el diseño de nuevos dispositivos. En este trabajo implementamos una mezcla de sistemas de seguridad para la confidencialidad de datos, en el diseño de una marca de agua que contenga un código QR cifrado mediante el algoritmo "Data Encryption Standard" de 8 bytes. Además de la generación de una rejilla dada por una matriz de puntos del propio código QR que produce un patrón de difracción y su correspondiente patrón entrelazado. Se presentan los resultados de las marcas de agua o patrones de difracción en imágenes digitales. Éstas también podrán ser observadas cuando se graban en placas de vidrio portables, mediante un proceso de daño óptico automatizado. Así tenemos identificadores ópticos de control de acceso con confidencialidad de datos. La aportación de este artículo es la integración de varias disciplinas de las ciencias e ingenierías para el desarrollo tecnológico de aplicaciones de uso diario en sistemas de seguridad.*

**Palabras clave:** *códigos QR, criptografía, difracción, hologramas, marcas de agua, servicios y mecanismos de seguridad*

**Title**: Confidentiality data by engraving encrypted QR codes: Optical-ID

**Abstract:**

*The combination of security mechanisms through Cryptography and Steganography leads a level increase of security in the design of new devices. In this work we implement a mix of security systems for data confidentiality, in the design of a watermark that contains an encrypted QR code using the 8-byte Data Encryption Standard algorithm. In addition to the generation of a grating given by matrix points of QR code itself that produces a diffraction pattern and its corresponding enhanced pattern. The results of watermarks or diffraction patterns are presented in digital images. These can also be observed when recording on portable glass plates, through an automated optical damage process. Thus, we have optical identifiers of access control with data confidentiality. The contribution of this article is the integration of several disciplines of science and engineering for the technological development of applications for daily use in security systems.*

**Keywords**: *QR codes, cryptography, diffractions, hologram, watermark, security services and mechanism.*

Tipo de artículo: original.
Fecha de recepción: 18 de septiembre de 2019
Fecha de aprobación: 21 de enero de 2020.

## 1. Introducción

Los códigos QR fueron creados para ser leídos por dispositivos electrónicos móviles de almacenamiento con una rápida respuesta y son usados para etiquetar o inventariar objetos de producción masiva, etiquetas de presentación y muchas otras aplicaciones. Los códigos QR fueron inventados por una empresa japonesa como sucesores de los códigos de barras, pero el interés de este trabajo es manejar la información dentro del módulo de matriz de puntos con la cual son generados, de acuerdo con la ISO/IEC 18004 [1]. La información dentro de los QR se empleará en particular para diseñar una rejilla que tomará el rol de abertura que producirá el fenómeno de difracción, cada rejilla QR tendrá su correspondiente patrón de difracción, este procedimiento es semejante cuando se realiza las marcas de agua sobre un documento digital o se quiere preservar derechos de autor en una imagen o fotografía. La marca de agua que tiene información de los códigos QR cifrados mediante el algoritmo "Data Encryption Standard" [2], puede ser perceptible o imperceptible dependiendo cuanta información se quiera ocultar en el patrón de difracción o el medio portador. Nuestro grupo académico de modelado y simulación ha trabajado sobre marcas de agua imperceptibles en audio [3], donde el procedimiento es procesar información para introducirla y ocultarla en un medio portador digital de forma imperceptible [4], [5]. La generación del patrón de difracción mediante la transformada de Fourier en dos dimensiones de la rejilla, es decir de la abertura y la propagación de radiación electromagnética a través de ella es quien determina el procedimiento para ocultar la información. Los patrones generados se forman en la zona de Fresnel donde la abertura que causa la difracción son los códigos QR cifrados y ciertamente se deben cumplir las condiciones de

interferencia mediante la superposición de las ondas en un corte plano perpendicular a la dirección de propagación. El esquema de inserción se muestra en la figura 1.

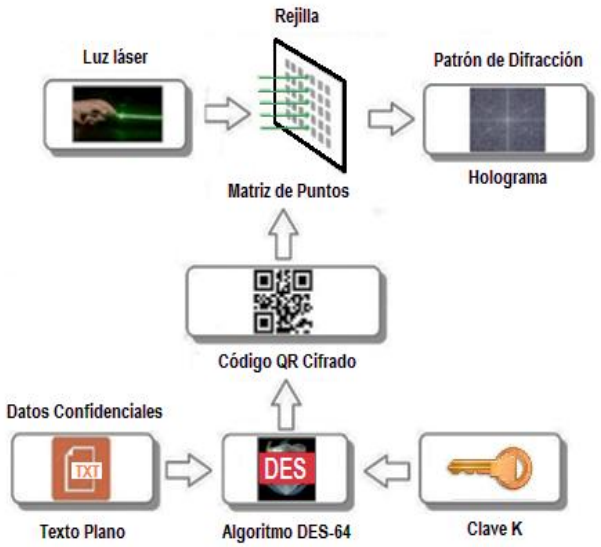


Figura 1. Esquema de inserción de la marca de agua para la generación de un patrón de difracción.

Los resultados obtenidos son los medios portadores, patrones de difracción (imágenes bidimensionales) con la información clasificada oculta de la matriz de puntos de los códigos QR cifrados, que pueden ser almacenados, compartidos sin sospecha de que tienen información valiosa, como claves o llaves privadas. Para recuperar la información se debe realizar el procedimiento inverso y escanear los códigos QR con el algoritmo de descifrado empleado para visualizar el texto plano.

## 2. Servicios y mecanismos de seguridad

Una descripción de los servicios de seguridad y sus mecanismos relacionados se encuentran en la ISO 7498-2, acerca de la arquitectura de seguridad que deben tener los sistemas. En ella se habla acerca del proceso de la información en sistemas, como deben interconectarse y como deben implementarse. En esta ISO se mencionan los seis servicios de seguridad que son: la confidencialidad, la autenticidad, la integridad o verificación de la integridad, la disponibilidad, el no repudio y el control de acceso [6]. En general un mecanismo de seguridad en el ramo de las tecnologías de la información es una técnica que se utiliza para implementar un servicio. Los mecanismos de seguridad proporcionan varios servicios básicos de seguridad o combinaciones de los seis servicios – los servicios de seguridad especifican "cuáles" controles son requeridos y los mecanismos de seguridad especifican "con qué" deben ser implementados. No es posible con un sólo mecanismo implementar todos los servicios, a pesar de esto, la mayoría de ellos pueden emplear algoritmos de criptografía basados en el cifrado de la información con uso de claves privadas. Muchos ingenieros en tecnologías de la información y seguridad de la información tanto como los criptógrafos y criptoanalistas para recordar los SS usan ahora una pirámide a diferencia de un triángulo o tetraedro, donde cada arista representa uno de ellos. La disponibilidad es la arista superior ya que sigue teniendo alto grado de dificultad implementarla, ver figura 2.

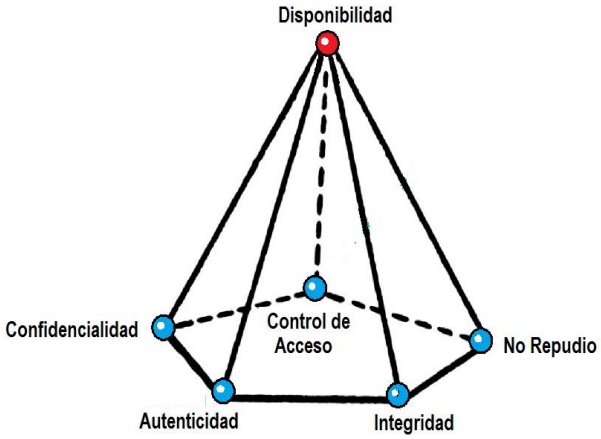


Figura 2. Aristas de una pirámide como servicios de seguridad.

## 3. Códigos de pronta lectura QR

En esta sección describiremos las características propias de los QRC (Quick-Read Code, por sus siglas en inglés o bien CQR) y las capacidades de almacenamiento, así como la construcción de la matriz de puntos. Particularmente en los QRC (Modelo 2) se tiene un valor de 58 en el número de simbología, conjunto alfanumérico de bytes dados por el conjunto de caracteres Kanji [7]. Se tiene una tasa de impresión de 1:1 y una tasa de formato de 1B:1S. La revisión de dígitos es automática dada por la simbología y un control de impresión C=QRC. El estándar de los QRC está dado por la AIM International ITS/97-001 y ISO/IEC 18004:2000. Este tipo de codificación se desarrolló para soportar formatos industriales y una gran cantidad de datos que podemos observar en la tabla 1.

Tabla 1. Capacidad de datos soportada en QRC.

| Formato | Pacidad de datos | Caracteres |
|---|---|---|
| Numérico | 089 caracteres | 0-9 |
| Alfanumérico | 4296 | A-Z (mayúsculas) espacio $ %+ - , . /: |
| Binarios | 2953 bytes | Codificación defecto: ISO 8859-1(2005) |
| Kanji/Kana | 817 caracteres | esplazamiento JIS X 0208 |

Además, una capacidad máxima de 2953 bytes de datos binarios usando una matriz de 177X177 puntos. Un ejemplo de la versión 22 (104X104 puntos) puede codificar aproximadamente 1 [KB] de datos usando un bajo nivel de corrección de errores. El tamaño del símbolo es cerca de 37X37 [mm] cuando se usa un tamaño de los puntos de 0.35 [mm]. Es importante tomar en cuenta estas especificaciones ya que esto limita la cantidad de información cifrada por el algoritmo DES-64 bits si lo usamos con algún modo de cifrado por bloque para convertirlo en un cifrado por flujo como el ECB (Electronic Code Book) o un CFB (Cipher Feedback). De igual importancia son las dimensiones del símbolo del QRC con los cuales desarrollamos las rejillas de difracción.

## 4. Algoritmo de cifrado DES

"Data Encryption Standard" (DES) es un cifrador de por bloques tipo Feistel se convirtió en estándar durante casi treinta años, usado en aplicaciones bancarias y se seguirá usando durante algún tiempo, sabemos que AES-256 es el estándar mundial ahora, pero para nuestra aplicación DES es bastante sólido como prueba de concepto. Tiene una clave de 64-bits quitando algunos bits menos significativos una clave real de 56-bits y se revuelve durante 16 vueltas o rondas [2]. Cifra mensajes de 64-bits suficientes para la información que vamos a usar en los códigos QR de pronta lectura. DES es de fácil comprensión y usa cajas S (de compresión) de sustitución al igual que varios algoritmos más modernos como el actual AES. El algoritmo emplea matrices de permutación inicial y final y en la creación de las claves por ronda se usan desplazamientos, así como matrices de expansión, un esquema lo podemos ver en la figura 3.

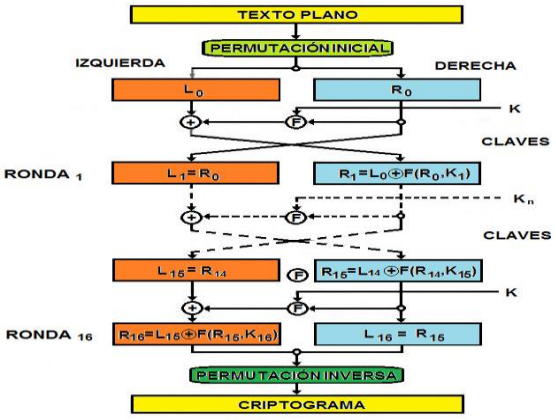


Figura 3. Cálculo de cifrado en el algoritmo DES.

Cuando DES empezó a ser vulnerable debido a ataques por desarrolladores de algoritmos como los laboratorios RSA y al crecimiento del desarrollo tecnológico en prueba de millones de claves por segundo que van desde 96 días hasta 2.5 días en romper la clave de cifrado (una inversión). Entonces DES dejo de ser el estándar, así este se usó desde 1976 hasta 1997 que la NIST lo descertifico como estándar. Sin embargo, se siguió utilizando hasta que en 2006 se implementó al algoritmo AES como estándar mundial. Algunas características que cumplía DES son: el nivel de seguridad de DES computacional era bastante alto, la seguridad del sistema que usaba este cifrado no debía verse comprometido por la publicación y divulgación del algoritmo. Estaba disponible a todos los usuarios y podía usarse en varias aplicaciones como en el caso de este trabajo, la implementación en hardware o software sigue siendo de bajo costo y era usado también como validación y debería ser exportable.

## 5. Marcas de Agua

Las Marcas de Agua (MA) no es un fenómeno nuevo, por muchos años las MA sobre papel han sido empleadas visiblemente para indicar un publicista en particular y desalentar la falsificación de divisas. Una MA es un diseño impreso sobre una pieza de papel durante una producción y para la identificación del copyright, figura 4. El diseño puede ser un patrón, un logotipo o alguna otra imagen. En la era moderna como muchos datos e información están almacenados y comunicados en forma digital, prueban autenticidad y juegan claramente un importante rol. Como un resultado, la MA digital es un proceso a través de la cual información arbitraria es codificada dentro de una imagen o una pista de audio de tal forma que sea imperceptible al sistema visual humano o al oído humano. Las MA digitales han sido propuestas como una herramienta apropiada para identificar la fuente, el creador, propietario, distribuidor o consumidor autorizado de un documento, obra musical o imagen. También pueden ser empleadas para detectar un documento, melodía o imagen que ha sido ilegalmente distribuida o modificada. Otra tecnología, es el cifrado que es un proceso de obscurecer (manchar) información para hacerla ilegible a observadores sin conocer las claves específicas. Esta tecnología se refiere algunas veces a una mezcla de datos. Las MA cuando son complementadas por cifrado, pueden servir para un vasto número de propósitos incluyendo la protección del copyright, monitoreo de transmisiones y autenticación de datos [8].

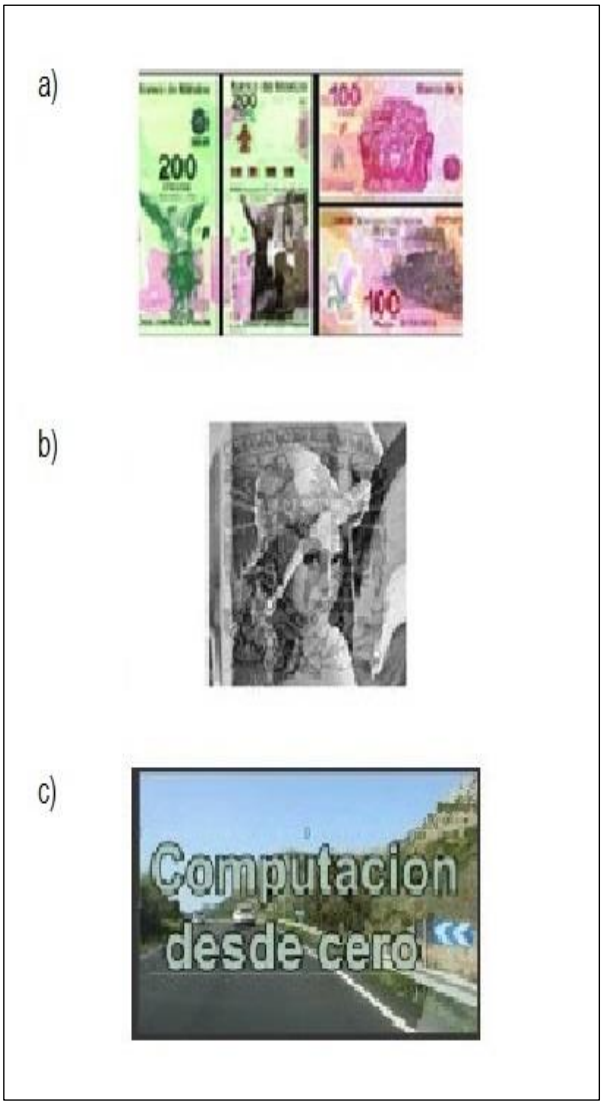


Figura 4. Marca de agua sobre: a) papel moneda, b) una imagen y c) en un video.

En el mundo digital, una MA es un patrón de bits insertados dentro de un medio digital que puede identificar al creador o a usuarios autorizados. La MA digital a diferencia del sello tradicional visible, la MA es diseñada para que sea invisible a la vista. Los bits insertados dentro de un audio digital o imagen son esparcidos por todo el documento (archivo) para evitar su identificación o modificación. Por lo que, la MA digital debe ser robusta y debe prevalecer a detecciones, compresiones y otras operaciones que pueden ser aplicadas al documento.

En la figura 5 se describe un sistema general de MA digital, en donde un mensaje W se inserta como MA dentro de un medio, el cual está definido como un anfitrión o huésped medio H, el resultado es el medio con MA H*. En el proceso de inserción, una llave secreta K, está dada por un generador aleatorio de números involucra algunas veces para generar una MA más segura. El documento con MA H* es entonces transmitido a través del canal de comunicación, la MA puede ser detectada o extraída después.

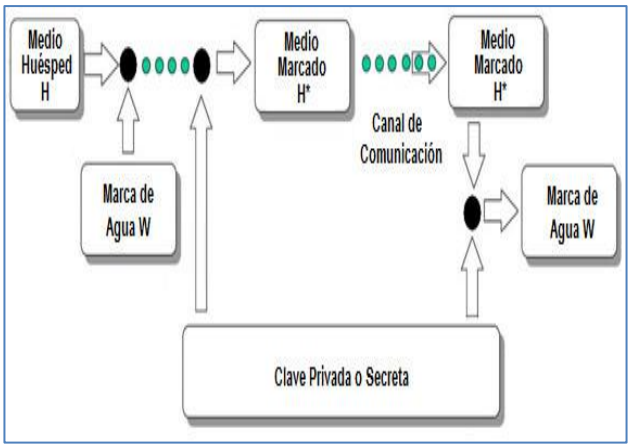


Figura 5. Sistema general para Marcas de Agua Digitales.

Imperceptibilidad, seguridad, capacidad y robustez son entre muchos aspectos para el diseño de MA, el medio con MA debe ser indistinguible del medio original sin alterar. Un sistema MA ideal debe insertar una gran cantidad de información perfectamente segura, pero sin degradación visible en el medio huésped. La MA debe ser robusta ante ataques de variaciones intencionales (recorte, redimensionamiento o compresión) y no intencionales (ruido). Muchas investigaciones se han enfocado sobre seguridad y robustez, pero raramente sobre la capacidad de las MA. La cantidad de datos que un algoritmo puede introducir en un medio tiene implicaciones para como las MA pueden ser aplicadas. En efecto, ambas seguridad y robustez son importantes debido a que la MA insertada se espera imperceptible e irremovible, si una MA grande puede ser introducida dentro de un medio huésped, el proceso debería ser empleado para muchas otras aplicaciones [9].

### 5.1 Requerimientos de las marcas de agua

Los requerimientos básicos de una aplicación de marcas de agua son tres:

a.- Capacidad: Es la cantidad máxima de información que puede ser ocultada en un medio.

b.- Robustez: Es la capacidad que tiene un algoritmo de marcas de agua para poder extraer el mensaje incrustado del medio marcado después de que éste último haya sido atacado.

c.- Impacto perceptual: Un algoritmo de marcas de agua es verdaderamente imperceptible si no se puede distinguir a simple vista las diferencias entre el medio marcado y el medio original. Aunque esta capacidad es en origen subjetiva, existen métricas para evaluarla. Como ejemplo se tiene a la relación señal a ruido (PSNR), el error cuadrático medio (EMS), la correlación, el error absoluto máximo (MAE), etc. Nótese que para poder evaluar esta capacidad es necesario comparar al medio marcado con el

medio original. Como normalmente se distribuye el medio marcado sin el medio portador es suficiente que las modificaciones en el medio marcado pasen desapercibidas para que el algoritmo de marcas de agua utilizado sea considerado como imperceptible [10].

## 6. Difracción

Cuando ocurre una desviación de la propagación en línea recta de la luz mediante un medio semitransparente se le denomina difracción. Este fenómeno físico es una propiedad del movimiento ondulatorio que se llevan a cabo donde cualquier fracción de un frente de onda está siendo obstruida. Si la propagación se ve alterada en la amplitud o en la fase de una región del frente de onda lo que ocurrirá es una difracción. Como mencionamos en la introducción si un tren de onda se propaga más allá de la obstrucción interfieren por la superposición de ondas lo que produce una distribución de densidad de energía llamada patrón de difracción [11]. Recordando al principio de Huygens-Fresnel establece que "cada espacio sin desviación de un frente de onda produce un tren de ondas esféricos secundarios, con la misma frecuencia que la onda original y da como resultado una superposición de los trenes de onda". Pareciera que estuviéramos hablando de dos fenómenos el de difracción e interferencia, lo cierto es que no hay ninguna distinción física. Pero se vuelve más tradicional el hablar de interferencia cuando se analizan sólo un poco de ondas y de difracción cuando se trata de analizar un gran número de ondas. En el caso en que producimos una obstrucción mediante un modelo matemático, consideramos el estudio de la difracción a través de la suma de varias aberturas rectangulares. Para esto una onda plana monocromática que se propaga en la dirección perpendicular a la rejilla de difracción semitransparente. En el análisis queremos encontrar la distribución de densidad de flujo correspondiente en el espacio, es decir, en cualquier punto P alejado. Análogamente al principio de Huygens-Fresnel, una superficie diferencial *dS* en la rejilla puede observarse como si se incidiera sobre ella varias fuentes puntuales secundarias coherentes. La perturbación total que llega al punto *P* alejado es de la forma:

$$\tilde{E}_P = \frac{\varepsilon_A e^{i(\omega t-\kappa R)}}{R}\iint_{Apertura} e^{i\kappa(X_x+Y_y)/R}dS. \qquad (1)$$

Luego usando el análisis de Fourier para la difracción emplearemos una integración bajo la propagación en la rejilla de acuerdo con

$$\Psi(f_x, f_y, z) = \frac{e^{ikz}}{i\lambda z}\iint_A \Psi_A(x,y)e^{-i2\pi(f_x x+f_y y)}\,dx.dy\,, \qquad (2)$$

donde $\psi_A(x, y)$ es la abertura y $f_x$ y $f_y$ están relacionadas con las frecuencias espaciales, $\lambda$ la longitud de onda, k el vector de onda, z la dirección de la propagación. La ecuación (2) se puede obtener a partir de la integral de superficie de Fresnel-Kirchhoff usada para la difracción sobre aberturas con simetría rectangular [12], figura 6. Cuando la integral se define sobre el intervalo $[-\infty,\infty]$ se convierte en la transformada de Fourier de la abertura, $\Im(\psi_A(x, y))$. El resultado de la solución de la integral de propagación es el patrón de difracción generado sobre la pantalla de observación y para el patrón entrelazado se calcula el logaritmo en base 2 de la Transformada de Fourier resultante.

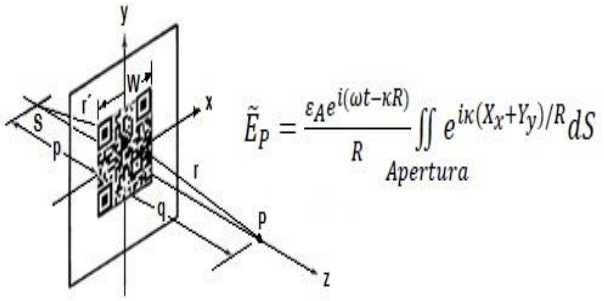


Figura 6. Sistema de la propagación sobre las rejillas para la obtención de los patrones de difracción.

## 7. Procedimiento

Para generar o crear una abertura como rejilla de difracción para este trabajo usaremos dos técnicas, una es a través del modelo matemático de la abertura y hacer su propagación sobre ella, la otra es a través directamente del código QR cifrado. En esta última técnica el código QR generado después de haber insertado la información cifrada con el algoritmo DES, que es una imagen digital en blanco y negro en mapa de bits de 256 colores, hay que convertirla en una imagen de mapa de bits monocromática, o sea blanco y negro para que podamos usarla como rejilla de difracción a través de su matriz de puntos.

En física óptica al calcular la transformada de Fourier digital sobre la apertura o rejilla producirá el patrón de radiación, en nuestro caso la rejilla será el QR con la información cifrada.

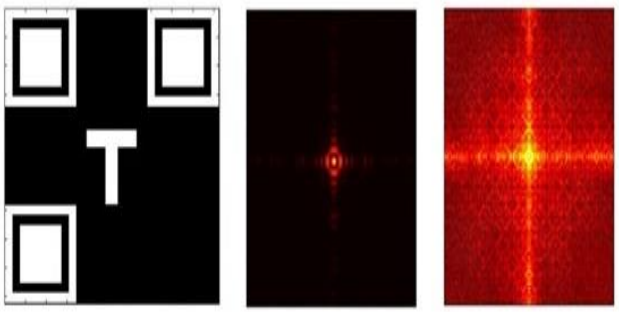

Figura 7. Rejilla de abertura – Marca de Agua – Patrón entrelazado de la letra T.

Para el primer caso generamos la abertura de la letra "T" con los tres cuadros de referencia del código QR de acuerdo con el siguiente modelo:

$$
\begin{aligned}
A1 &= rect\left(\left(X-delta\right)/b\right).*rect\left(\left(Y-delta\right)/b\right)\\
&\quad -rect\left(\left(X-delta\right)/a\right).*rect\left(\left(Y-delta\right)/a\right)\\
&\quad +rect\left(\left(X+delta\right)/b\right).*rect\left(\left(Y+delta\right)/b\right)\\
&\quad -rect\left(\left(X+delta\right)/a\right).*rect\left(\left(Y+delta\right)/a\right)\\
&\quad +rect\left(\left(X+delta\right)/b\right).*rect\left(\left(Y-delta\right)/b\right)\\
&\quad -rect\left(\left(X+delta\right)/a\right).*rect\left(\left(Y-delta\right)/a\right);\\
A2 &= rect\left(\frac{X-delta}{d}\right).*rect\left(\frac{Y-delta}{d}\right);\\
A3 &= rect\left(\left(X+delta\right)/d\right).*rect\left(\left(Y+delta\right)/d\right);\\
A4 &= rect\left(\left(X+delta\right)/d\right).*rect\left(\left(Y-delta\right)/d\right);\\
A5 &= rect\left(\left(X\right)/\left(4*dc\right)\right).*rect\left(\left(Y-60\right)/\left(dc\right)\right)\\
&\quad +rect\left(X/dc\right).*rect\left(\left(Y+50\right)/\left(4*dc\right)\right);
\end{aligned}
\tag{3}
$$

La abertura está dada por: A = A1 + A2 + A3 + A4 + A5 con la función Rect(X, Y) en el intervalo de [-1/2,1/2] y con constantes a=270; b=340; d=200; dc=60; delta=340, la forma de esta abertura se muestra en la figura 7.

Ahora mostraremos algunos ejemplos en la figura 8 de patrones de radiación sobre los cuales se propaga luz sobre unas rejillas [13].

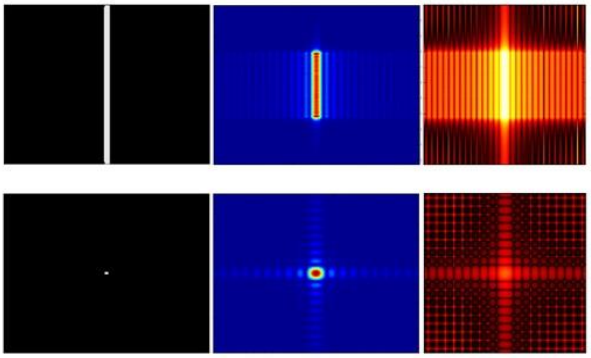

Figura 8. Dos ejemplos de patrones de radiación, rejilla-patrón-entrelazado.

La capacidad de información que se puede almacenar en un código QR según la norma AIM International ITS/97 y ISO/IEC 18004:200 para datos binarios es de 2953 bytes, lo cual está sobrado para una rejilla de 148 X 148 pixeles de daño óptico sobre los vidrios de la información cifrada, figura 9.


Figure 9. Códigos QR con a) texto plano: INAOE y b) su texto cifrado mediante DES.

## 8. Procedimiento de grabado y lectura de los Id-ópticos

Con los códigos QR cifrados se tienen los datos binarios que convertimos a pixeles en blanco y negro para producir mediante un sistema de control de grabado computarizado, el daño óptico sobre una placa de vidrio BK7 usando un láser de Nd: YAG que opera con pulsos con perfil de intensidad gaussiano de 35 [ps] y con una energía de 35 [mJ], figura 10.

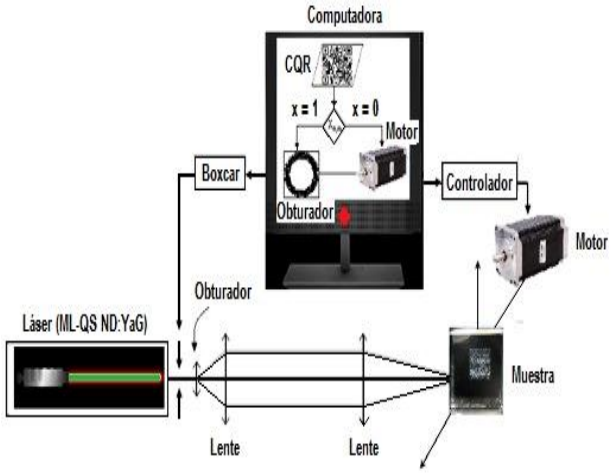


Figura 10. Sistema de daño óptico computarizado.

Para la lectura del dispositivo óptico (dije o placa) se implementó un sistema automatizado que permite leer el código cifrado. Este sistema jugará el rol de una entidad repositoria acreditada conocida también como autoridad certificadora donde se encuentran todas las claves ópticas públicas conocidas, figura 11. Este sistema sólo reconocerá la ID-óptica, es decir, saber quién es el poseedor del dispositivo o quien la porta, pero no puede conocer la información confidencial cifrada dentro del mismo [14].

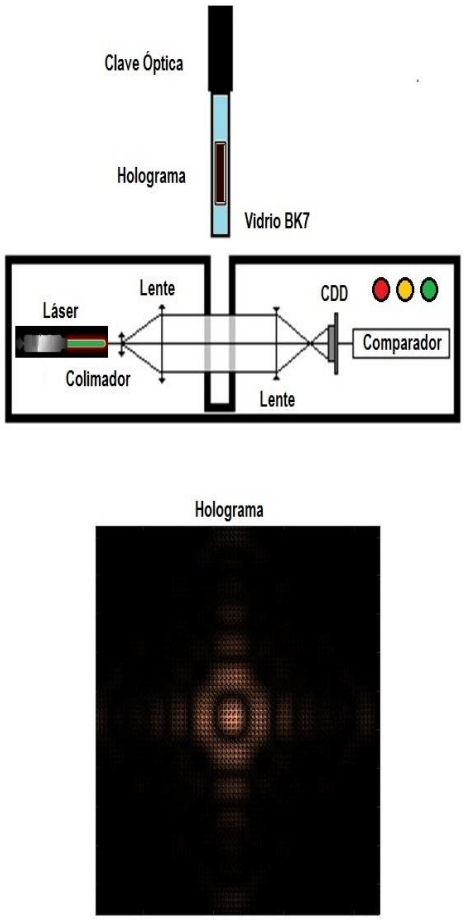


Figura 11. Sistema de lectura de la clave óptica.

El sistema tiene la opción de comprobación de la información confidencial mediante su clave privada usada para cifrar la información con el algoritmo criptográfico DES. De igual forma tiene un señalamiento de comprobación de vigencia del dispositivo id-óptico.

## 9. Resultados

Usamos una clave de 64-bits para el algoritmo de cifrado DES, la cual usamos como clave secreta o privada de quien desea manejar un mensaje (información confidencial). La palabra "Santiago" de 8-caracteres se usó en los tres casos presentamos a continuación.

Utilizamos tres matrices de puntos con información cifrada como rejillas de difracción que juegan el rol de abertura para obtener los patrones de difracción y sus correspondientes patrones entrelazados. Se muestran figuras del código QR cifrado, patrón de difracción alias marca de agua y su patrón entrelazado de los tres casos de estudio en este trabajo, figuras 12, 13 y 14.

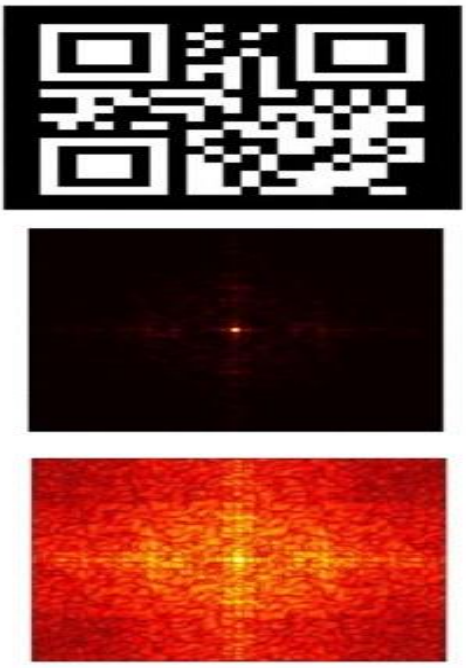

Figure 12. Rejilla de Abertura del QRC – Marca de Agua o Patrón de Difracción – Patrón entrelazado del texto-cifrado: INAOE.

Siguiendo el procedimiento se obtienen los patrones de difracción, puede notarse la diferencia en los QRC, con detalle puede notarse la diferencia en las marcas de agua y se pueden apreciar las diferencias en los patrones entrelazados.

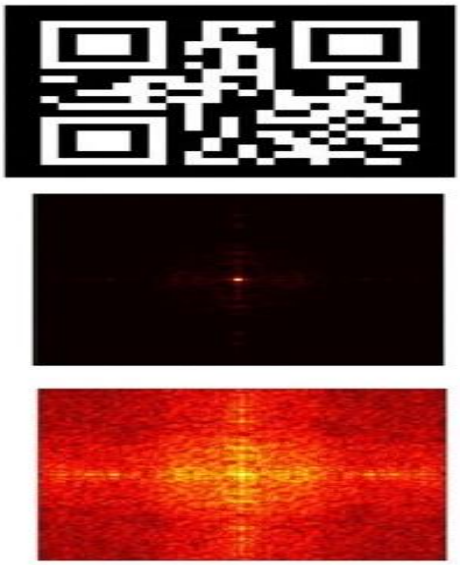

Figure 13. Rejilla de Abertura del QRC – Marca de Agua o Patrón de Difracción – Patrón entrelazado del texto-cifrado: ABCDEFGH.

La semejanza en los patrones de difracción se debe a los cuadros de referencia que se usan en los QRC que hay en las dos esquinas superiores y otro en la esquina inferior izquierda.

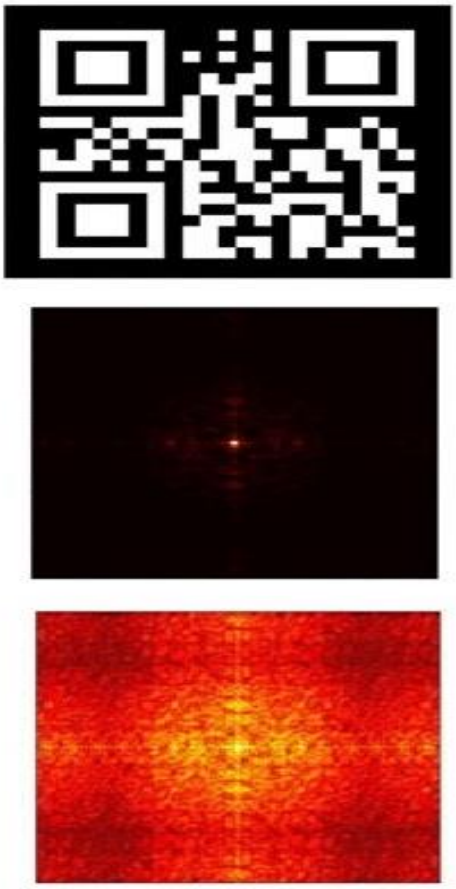

Figure 14. Rejilla de Abertura del QRC – Marca de Agua o Patrón de Difracción – Patrón entrelazado del texto-cifrado: Alejandro.

Los patrones de difracción son tenues que es lo que muestra la inserción de una marca de agua poco perceptible, sin embargo, en el patrón de difracción entrelazado es más perceptible. Aunque sólo es eso una mancha donde a simple vista no puede detectarse nada. La mayor parte de la información en los patrones de difracción se muestra en los centros de las imágenes, debido al método de la transformada discreta de Fourier que se utiliza para hacer la propagación de la luz incidente sobre las aberturas. Algo que logramos percatarnos con los lectores de QRC, es que no importa si la matriz de puntos es el negativo o el positivo, ellos siempre leen la misma información. Lo que a continuación mostramos es como quedaría el dispositivo ID óptico usando la técnica de grabado mostrada en la referencia [15], para el grabado de las marcas de agua y que efectivamente se pueda grabar un holograma dentro de un cristal. Este holograma contiene la información confidencial que nosotros deseamos asegurar mediante el cifrado en los QRC y ocultados como MA en los patrones de difracción. La figura 15 es una muestra de la factibilidad del dispositivo.

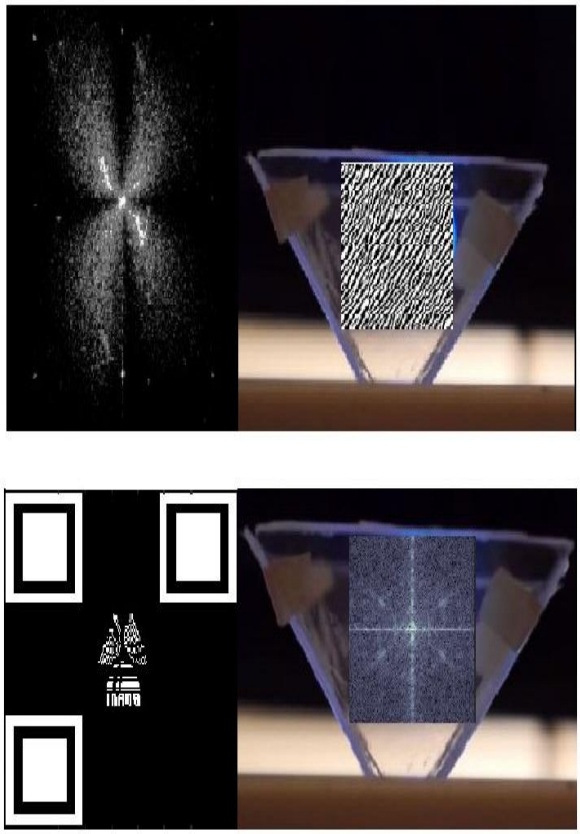

Figura 15. Hologramas creados y grabados dentro de un cristal (las dos imágenes de la izquierda). Un código QR con logotipo y su grabado (las dos imágenes de la derecha).

## Conclusión

La confidencialidad de los datos queda grabada en el medio portátil de forma segura, al implementar tanto técnicas criptográficas como esteganográficas. El procedimiento que hemos seguido para la inserción de la marca de agua, si sólo fuera obtener el patrón difracción de la rejilla creada por la matriz de puntos del código QR, se estaría creando una imagen deformada de la información dentro del código QR (texto-plano), como se hizo en [15] cuando se generó un holograma. Lo cual en seguridad se clasifica como “seguridad por obscuridad” que en realidad es parte de los métodos de la Esteganografía, ocultar información dentro de un medio portador y que no es seguridad. La seguridad que presentamos es: cualquiera puede leer la información formada en la matriz de puntos del código QR, pero

no cualquiera la puede descifrar aun sabiendo que hay información oculta en el patrón de difracción entrelazado o estego-objetos cifrados que muestran los resultados.

Con el medio portador de la información clasificada, como en [14] desarrollamos un sistema óptico con mecanismos de seguridad implementados, hablando de los SS pueden emplearse ya sea como control de acceso [16], autenticidad, no repudio e integridad. También estamos conscientes de que el algoritmo de cifrado DES está en desuso, sin embargo, en este trabajo se quiere ejemplificar el incremento de seguridad usando Estaganografía y Criptografía, por lo que después se usará en algoritmo "*Advanced Encryption Standart*" dado por la FIPS PUB 197 de 2005 para Criptografía simétrica de 256-bits.

Para recuperar la información se debe realizar el procedimiento inverso y escanear los códigos QR con el algoritmo de cifrado empleado para visualizar el texto plano. Como trabajo futuro sobre este campo de la seguridad de la información es optimizar la implementación del software para generar el código cifrado dentro del módulo de la matriz de puntos para generar los códigos QR. También analizaremos la funcionalidad de grabar o quemar los códigos QR cifrados o los patrones de difracción generados por estos mismos. Lo anterior debido a las características propias del sistema de grabación como son dimensiones, longitudes de onda de la radiación electromagnética empleada, potencia y medio portador.

Las aplicaciones que se han desarrollado están en el sentido de usar el dispositivo óptico como control de acceso, además que se desarrolló un protocolo mediante criptografía asimétrica para su lectura [17].

## Agradecimiento

Este trabajo ha sido patrocinado por la Dirección General de Asuntos del Personal Académico (DGAPA) de la Universidad Nacional Autónoma de México bajo el "Programa de Apoyos para la Superación del Personal Académico (PASPA)" a través de una beca de doctorado, (2015-2018).

## Referencias

[1] (2017), QR codes [Online]. Disponible en: https://es.wikipedia.org/
[2] FIPS Publication 46-3, (1999). Data Encryption Standard (DES).
[3] Padrón Godínez A., González Lee M., et al. "Marcas de Agua Imperceptibles en Audio Digital". SOMI XXIII Congreso de Instrumentación, Sociedad Mexicana de Instrumentación, Xalapa, México, octubre de 2008, 7 páginas.
[4] Padrón Godínez A., Azuara Pérez L., et al. "Robustez de Marcas de Agua ante ataques". XXIV Congreso de Instrumentación, Mérida, Yucatán, México, 2009, 6 páginas.
[5] Padrón Godínez A., González Lee M., et al. "Ocultamiento de Datos en Imágenes Digitales Mediante BPCS". SOMI XXIII Congreso de Instrumentación, Sociedad Mexicana de Instrumentación, Xalapa, México, octubre de 2008, 6 páginas.
[6] INTERNTIONAL STANDARD, ISO 7498-2, Information processing – Open Systems Interconnection – Basic Reference Model. Security Architecture. First edition 1989-02-15.
[7] INTERNAIONAL STANDARD, ISO/IEC 18004, Information technology — Automatic identification and data capture techniques — Bar code symbology — QR Code., First edition 2000-06-15.
[8] Shih F. Y., "Digital Watermarking and Steganography", CRC Press, USA, 2008.
[9] In-Kwon Yeo, Hyoung Joong Kim. "Modified Patchwork Algorithm: a novel audio watermarking scheme". Information Technology Coding and Computing, 2001. Proceedings. International Conference on Volume, Issue, Apr 2001 Page(s):237–242, Digital Object Identifier 10.1109/ITCC.2001.918798.
[10] Houtsma, A.J.M., Rossing T. D., "Auditory Demonstrations". Institute of Perception Research, 1987. Folleto del CD "Auditory Demonstrations", Philips 1126-061.
[11] Pedrotti F. L. and Pedrotti L. S. "Introduction to Optics", Ed. Prentice-Hall Int. Inc., USA, 1993.
[12] Steck D. A., "Classical and Modern Optics", Oregon University, 2006.
[13] Hecht E., "Óptica". 3a. edición. Ed. Addison Wesley Iberoamericana, Madrid 2000.
[14] Treviño-Palacios C. G., Olivares-Pérez A., Zapata-Nava O.J., "Security system with optical key Access", 2007. Proc. of SPIE Vol. 6422 642218-1.
[15] Treviño-Palacios C. G., Olivares-Pérez A., Zapata-Nava O.J., "Optical damage as a computer generated hologram recording mechanism", Journal of Applied Research and Technology 13 (2015) 591–595.
[16] Padrón-Godínez A., Prieto Meléndez R., Treviño-Palacios C. G., "Dispositivo óptico de seguridad usado como clave cifrada de control de acceso", SOMI XXXIII Congreso de Instrumentación, Oct-2018.
[17] Padrón-Godínez A., Prieto Meléndez R., Treviño-Palacios C. G., "Lectura de clave óptica bajo el esquema de criptografía asimétrica", SOMI XXXIV Congreso de Instrumentación, Oct-2019.