ID óptico mediante QR-cifrados, patrones de difracción y marcas de agua

1st Alejandro Padrón-Godínez
Inst. y Medición, ICAT - Coord. Óptica
UNAM - INAOE
CDMX - Tonantzintla, Puebla - México
apadron@inaoep.mx

2nd Rafael Prieto Meléndez
Instrumentación y Medición, ICAT
UNAM
CDMX, México
rafael.prieto@ccadet.unam.mx

3rd Carlos Gerardo Treviño-Palacios
Coord. Óptica
INAOE
Tonantzintla, Puebla - México
carlost@inaoep.mx

***Resumen*—Las nuevas tecnologías han traído una diversidad de sistemas de seguridad implementadas tanto en software como en hardware portátiles para su uso como identificadores personales, algunos pocos ejemplos son tarjetas grabadas o con chips integrados, biométricos como lectores de huellas o iris. En este trabajo presentamos una mezcla entre implantación de mecanismos de seguridad y fenómenos físicos de propagación para el diseño de un dispositivo ID óptico que contenga información confidencial dentro de un código QR. La información dentro del código QR de pronta lectura esta cifrada mediante el algoritmo "Triple Data Encryption Standart"(FIPS46-3) de 8 bytes. La matriz de puntos del código QR genera una rejilla de difracción que produce patrones de difracción y sus correspondientes patrones entrelazados. Los patrones de difracción son insertados como marcas de agua mediante el proceso de daño óptico.**

***Palabras Clave*—criptografía, códigos-QR, difracción, marcas de agua**

I. Introducción

El diseño y construcción de sistemas seguridad de reconocimiento para control de acceso en la actualidad ya son más comunes y de uso diario, éstos son implementaciones en medios portátiles como identificadores personales, chips dentro de tarjetas de crédito, telefonía celular, computadoras, productos o activos para almacenamiento como las RFid, por mencionar algunos. Sin embargo, algunos dispositivos no tienen integrados los servicios y mecanismos de seguridad que permiten ingresar a un sistema o a lugares altamente confidenciales en forma segura. Lo recomendable es usar llaves públicas y privadas con generadores de secuencias pseudoaleatorias para que por medio de criptografía asimétrica ingresen de forma segura [1]. La mayor parte de los servicios de seguridad se logran mediante la implantación de algoritmos de cifrado, ya sea en hardware o software [2]. Algunos mecanismos como las marcas de agua son empleadas como candados en documentos valiosos, un ejemplo son los billetes de dinero para verificar su integridad y su autenticidad. Aunque la seguridad por obscuridad no es la forma de obtener dispositivos o medios seguros. La combinación de mecanismos de seguridad mediante Criptografía y Esteganografía trae consigo un aumento en el nivel de seguridad en el diseño de nuevos dispositivos portátiles de control de acceso [3]. La ventaja de la creación de los códigos QR de pronta lectura, es que fueran leídos por dispositivos portátiles electrónicos de almacenamiento para el manejo masivo de información como en el caso de levantamiento de un inventario [4]. Los QR fueron inventados por una empresa japonesa como sucesores de los códigos de barras, a nosotros nos interesan por dos razones, para guardar información confidencial cifrada en ellos y la generación de la matriz de puntos. La matriz de puntos a su vez genera una rejilla que al incidir sobre ella luz producirá el fenómeno de difracción, luego mediante el fenómeno de superposición de ondas electromagnéticas se tendrá su correspondiente patrón de difracción [5]. El patrón de difracción formado por la superposición tiene información de los códigos QR cifrados mediante el algoritmo 3DES [6]. En óptica física sabemos que el fenómeno de propagación sobre una apertura (rejilla de difraccón) es semejante a obtener la transformada de Fourier para obtener los patrones de difracción podemos producir imágenes en dos dimensiones de los patrones que serán nuestras marcas de agua [6]. Estas marcas de agua se insertarán o quemarán para hacer los dispositivos ID ópticos únicos a su correspondiente código QR cifrado, mediante el daño óptico sobre un cristal [7]. El esquema del procedimiento empleado se muestra en la Fig.(1). Para verificar la información se debe realizar el procedimiento inverso, escanear las marcas de agua producidas por los códigos QR, descifrar con el algoritmo 3DES para visualizar el texto plano. Debemos tener presente que las marcas de agua pueden ser perceptibles o imperceptibles dependiendo cuanta información se quiera ocultar en el patrón de difracción o el medio portador. En otros trabajos sobre marcas de agua imperceptibles en imágenes y en

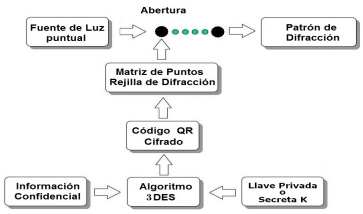

Fig. 1. Esquema para la generación del patrón de difracción generado por la abertura del código QR cifrado.

audio [8], [9], el procedimiento es procesar información para introducirla y ocultarla en un medio portador digital mediante algoritmos de inserción de forma imperceptible [10]. El patrón de difracción generado mediante la transformada de Fourier en dos dimensiones de la rejilla, es producido por la abertura y la propagación de radiación electromagnética a través de ella. Esto es lo que determina el procedimiento para ocultar la información y el fenómeno debe cumplir con las condiciones de interferencia mediante la superposición de ondas en un corte plano perpendicular a la dirección de propagación.

II. Servicios de Seguridad

Los servicios de seguridad (SS) que se manejan para el intercambio de información mediante un protocolo de comunicación son: confidencialidad, autenticidad, integridad, no repudio, control de acceso y disponibilidad [11]. No es posible implementarlos todos pero si se pueden implementar algunos gracias a los mecanismos de seguridad que han sido desarrollados hasta ahora. Estos pueden recordarse fácilmente en el triángulo de oro de la Fig. (2), (aunque en realidad se convierte en el tetraedro de oro). La Disponibilidad como SS está fuera del alcance de los mecanismos de seguridad, lo cual puede ser discutido en análisis subsecuentes de dichos mecanismos. El control de acceso dependerá del sistema de seguridad que se implemente [12].

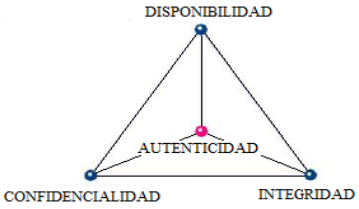

Fig. 2. Tetraedro de los servicios de seguridad.

III. Difracción

La radiación electromagnética representada en forma de luz se ha usado para explicar el fenómeno de interferencia en óptica, de acuerdo a que dos o más ondas coherentes individuales de luz, procedentes de una fuente única y separada por división de amplitud o frente de onda, se juntan para interferir. Particularmente, el mismo fenómeno está implicado en la difracción de la luz. La difracción es cualquier desviación de la óptica geométrica que resulta de la oclusión de un frente de onda de luz. Así una pantalla semitransparente con un orificio representa dicha oclusión y en una pantalla situada más allá del orificio, el círculo de la luz puede mostrar complejos efectos de borde. Este tipo de oclusión es común en muchos instrumentos ópticos que utilizan la parte de un frente de onda que pasa a través de una lente redonda. Una oclusión poligonal irregular muestra la estructura detallada en su propia sombra lo cual es inesperado sobre la base de la óptica geométrica. Efectos de difracción son una consecuencia del carácter de onda de la luz. Además si el obstáculo no es semitransparente, es decir, si éste causa transiciones locales en la fase o la amplitud del frente de onda de la luz transmitida, se observarán estos efectos. Ciertas imperfecciones en una lente producen patrones de difracción no esperados al transmitir luz láser. Debido a que se desvanecen los bordes de las imágenes ópticas por difracción, el fenómeno se limita a la precisión de la posición de los elementos del sistema como en el caso de los interferómetros. Si la fuente de luz tanto como la pantalla de observación están efectivamente lo suficientemente lejos de la abertura de difracción los frentes de ondas que llegan a la abertura y a la pantalla de observación pueden considerarse planos, se dice entonces que tenemos difracción de Fraunhofer o campo lejano; cuando éste no es el caso y la curvatura del frente de onda debe tomarse en cuenta para el cálculo del campo, tenemos difracción de Fresnel, o de campo cercano [13]. Para generar los patrones de difracción hacemos incidir luz láser sobre la matriz de puntos de los códigos QR cifrados en campo lejano [14]. Los patrones de difracción producidos son las marcas de agua generadas bajo el esquema que se mostró en la Fig.(1).

IV. Marcas de Agua

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 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 [8]. Entre los aspectos generales de las MA están la imperceptibilidad, seguridad, capacidad y robustez que son entre muchos aspectos necesarios para el diseño de las MA, el medio con MA debe ser indistinguible del medio original sin alterar, Fig.(3). Un sistema MA ideal debe insertar

Fig. 3. Marcas de agua sobre a) billetes, b) imagénes y c) videos.

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) [9]. 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 que sea imperceptible e irremovible, si una MA grande puede ser introducida dentro de un medio huésped, el proceso debería ser empleado para muchas otras aplicaciones [10].

V. METODOLOGÍA

El primer paso es cifrar la información confidencial o texto plano, pueden ser datos personales, con el algoritmo 3DES. Un segundo paso es generar el código QR correspondiente con esta información cifrada. En el tercer paso la matriz de puntos creada en el código QR es una imagen digital en blanco y negro en mapa de bits de 256 colores de 400x400 pixeles, hay que convertirla en una imagen de mapa de bits monocromática para que podamos usarla como rejilla de difracción. Para generar una rejilla de difracción o abertura usaremos dos técnicas, una es a través del modelo matemático de la abertura, la otra es a través directamente de la imagen del código QR cifrado y simular la propagación sobre ellas. Realizaremos varios casos, en el primero generamos la abertura de la letra "A" con los tres cuadros de referencia del código QR. Entonces con la siguiente expresión:

$$\begin{aligned} Ap_x &= rect((X)/(4*\delta)) * rect((Y-10)/(\delta)) + \\ &\quad rect((X)/(4*\delta)) * rect((Y+10)/(\delta)) \\ Ap_y &= rect((X-15)/\delta) * rect((Y+10)/(4*\delta)) + \\ &\quad rect((X+15)/(\delta)) * rect((Y+10)/(4*\delta)), \end{aligned} \quad (1)$$

y sumando estas expresiones $Ap = Ap_x + Ap_y$ se tiene la letra "A". Con la función rect(X, Y) en el intervalo de [-1/2,1/2] y con constantes $\delta = 10$; la forma de esta abertura se muestra en la Fig.(4), después se mostrará como código QR, Fig.(7). Una vez que tenemos los modelos matemáticos o

Fig. 4. Representación del modelo matemático de una abertura tipo "A".

bien las imágenes de las aberturas definidas, podemos propagar la radiación electromagnética a través de ellas emitiendo luz desde una fuente puntual y colocando abertura y pantalla de observación en difracción de Fraunhofer o campo lejano. Para esto usamos la función de onda en dos dimensiones mediante la siguiente ecuación para la propagación del campo y encontrar la irradiancia emitida:

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

donde $\psi_A(x,y)$ es la abertura y f_x y f_y están relacionadas con las frecuencias espaciales, λ 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 [13], Fig.(5). Cuando la integral se define sobre el intervalo $[-\infty, \infty]$ se convierte en la transformada de Fourier de la abertura, $\mathcal{F}(\psi_A(x,y))$. 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.

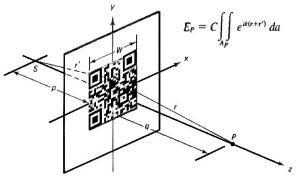

Fig. 5. Sistema de difracción de las aberturas para las Marcas de Agua.

VI. RESULTADOS

Al inicio de esta sección mostramos los códigos QR con cifrado y sin cifrado para observar la diferencia entre sus matrices de puntos, Fig.(6). Usaremos la clave privada "Santiago" 8-Bytes o 64-bits, que forman una palabra de 8 caracteres para el algoritmo de cifrado 3DES. Luego utilizaremos cuatro

Fig. 6. Cdigos QR con a) texto plano y b) texto cifrado para las aberturas.

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. Ahora se muestran figuras del código QR cifrado, patrón de difracción alias marca de agua y su patrón entrelazado de los cuatro casos de estudio en este trabajo, Fig.(7, 8, 9, y 10). Los patrones de difracción son tenues, que

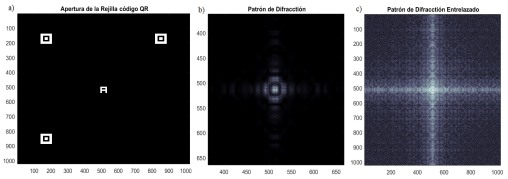

Fig. 7. a) Código QR con la letra A, b) patrón de radiación y c) patrón de radiación entrelazado.

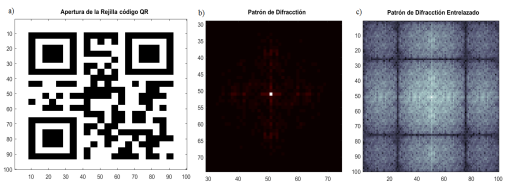

Fig. 8. a) Código QR cifrado del texto plano: 2018RCI4, b) patrón de radiación y c) su correspondiente patrón de radiación entrelazado.

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

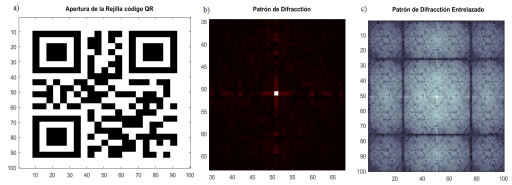

Fig. 9. a) Código QR cifrado del texto plano: ABCDEFGH, b) patrón de radiación y c) su correspondiente patrón de radiación entrelazado.

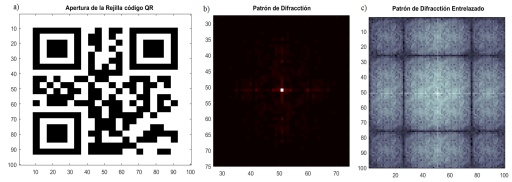

Fig. 10. a) Código QR cifrado del texto plano: INAOEPUE, b) patrón de radiación y c) su correspondiente patrón de radiación entrelazado.

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 de lo que pudimos percatarnos con los lectores de códigos QR 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 que nosotros deseamos asegurar mediante el cifrado en los códigos QR y ocultados como MA en los patrones de difracción. La Fig. (11) es una muestra de la factibilidad del dispositivo.

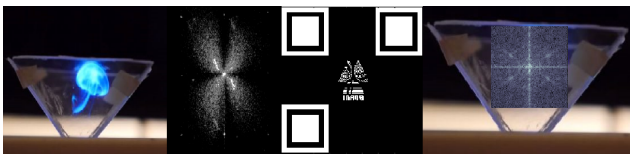

Fig. 11. Hologramas creados y grabados dentro de un cristal (las dos imágenes de la izquierda). Un código QR con logotipo y su grabado (las dos imágenes de la derecha).

VII. Conclusiones

La intención de producir un dispositivo con información confidencial cifrada es para generar un dispositivo ID óptico como una clave privada de control de acceso portable casi como una huella digital sin depender de generadores de secuencias dinámicas pseudoaleatorias. El dispositivo de lectura o reconocimiento tiene que realizar el proceso inverso para captar el texto en claro procedente de la información oculta y cifrada, y conocer la clave secreta que se uso en el algoritmo 3DES. 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 sin la clave privada aún sabiendo que hay información oculta en el patrón de difracción entrelazado o estego-objetos cifrados que mostramos en los resultados. El dispositivo creado como un medio portador de la información clasificada cifrada, contiene mecanismos de seguridad (algoritmo criptográfico 3DES), y hablando de los SS pueden emplearse como control de acceso, autenticidad, no repudio e integridad, [6]. Las características y pruebas de los grabados las dejamos para un trabajo futuro, ya que dependemos de una buena calibración y alineación de la óptica involucrada y de la potencia del láser que emplearemos para el daño óptico. Así como las dimensiones, longitudes de onda y del material para el medio portador.

Agradecimientos

Este trabajo ha sido financiado por la Dirección General de Personal Académico de la Universidad Nacional Autónoma de México bajo el Programa de Apoyos para la Superación del Personal Académico a través de la beca doctoral.

Referencias

[1] QR codes. Available at: “https://es.wikipedia.org/wiki/Código-QR,” Aug,23,2017.
[2] Daltabuit E., Hernández L., Mallén G., Vázquez J., “La seguridad de la Informacin,” Ed. Limusa, 2007.
[3] Meneses A. J., Van Oorschot P. C., Vanstone S. A., “Hanbok of Applied Cryptography”, CRC, 2000.
[4] FIPS Publication 46-3, (1999). Data Encryption Standard (DES).
[5] INTERNATIONAL STANDARD, ISO/IEC 18004, “Information technology - Automatic identification and data capture techniques - Bar code symbology QR Code,” First edition 2000-06-15.
[6] INTERNATIONAL STANDARD, ISO 7498-2, “Information processing - Open Systems Interconnection - Basic Reference Model. Security Architecture,” First edition 1989-02-15.
[7] Padrón Godínez A., Azuara Pérez L., Prieto Meléndez R., Herrera Becerra A. A., “Robustez de Marcas de Agua ante ataques,” XXIV Congreso de Instrumentación, Mérida, Yucatán, México, 2009, 6 páginas.
[8] Padrón Godínez A., González Lee M., Prieto Meléndez R., Herrera Becerra A. A., “Marcas de Agua Imperceptibles en Audio Digital,” SOMI XXIII Congreso de Instrumentación, Sociedad Mexicana de Instrumentación, Xalapa, México, octubre de 2008, 7 páginas.
[9] Padrón Godínez A., González Lee M., Prieto Meléndez R., Herrera Becerra A. A., “Ocultamiento de Datos en Imagénes Digitales Mediante BPCS”. SOMI XXIII Congreso de Instrumentación, Sociedad Mexicana de Instrumentación, Xalapa, México, octubre de 2008, 6 páginas.
[10] Shih F. Y., “Digital Watermarking and Steganography,” CRC Press, USA, 2008.
[11] 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):237242, Digital Object Identifier 10.1109/ITCC.2001.918798.
[12] Houtsma, A. J. M., Rossing T. D., “Auditory Demonstrations,” Institute of Perception Research, 1987. Folleto del CD “Auditory Demonstrations,” Philips 1126-061.
[13] Pedrotti F. L. and Pedrotti L. S. “Introduction to Optics”, Ed. Prentice-Hall Int. Inc., USA, 1993.
[14] 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) 591595
[15] Treviño-Palacios C. G., Olivares-Pérez A., Zapata-Nava O.J., “Security system with optical key Access,” Proc. of SPIE Vol. 6422 642218-1, 2007.