Clave óptica privada mediante un código QR cifrado

Alejandro PADRÓN-GODÍNEZ
Instrumentación Científica e Industrial - ICAT, Universidad Nacional Autónoma de México
Ciudad Universitaria, Coyoacán 04510/CDMX, México

Rafael PRIETO-MELÉNDEZ
Instrumentación Científica e Industrial - ICAT, Universidad Nacional Autónoma de México
Ciudad Universitaria, Coyoacán 04510/CDMX, México

Carlos G. TREVIÑO-PALACIOS
Coordinación de óptica, Instituto Nacional de Astrofísica, Óptica y Electrónica
Santa María Tonantzintla, San Andrés 72840/Puebla, México

RESUMEN

La importancia de un diseño y construcción de una clave óptica privada encriptada mediante un código de pronta respuesta, es el aumento en el nivel de seguridad, minimizando la posibilidad de clonaciones e impedir suplantaciones de identidad. Es decir, fenómenos de física óptica junto con la composición de mecanismos de seguridad con técnicas de criptografía y esteganografía, traen consigo evadir agujeros de seguridad en el diseño de nuevos dispositivos. El sistema desarrollado consiste en el grabado de un holograma, el patrón de difracción como marca de agua, sobre un bloque de vidrio BK7 de 1.44 [cm^3]. Para esto se usa una fuente de luz láser controlada computacionalmente e inducida, a través de una rejilla generada por la imagen de la matriz de puntos del código de pronta respuesta con información cifrada. En este trabajo presentamos un dispositivo óptico con servicios y mecanismos de seguridad implementados, según la arquitectura del estándar ISO 7498-2. El mecanismo implementado es un cifrado de información confidencial por bloques mediante el algoritmo criptográfico AES-128 anunciado como FIPS PUB 197 por la NIST. 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.

Palabras Claves: Esteganografía, Criptografía, Óptica, Hologramas, Difracción, Códigos QR, Marcas de Agua Digitales.

1. INTRODUCCIÓN

Muchos sistemas digitales de seguridad en la actualidad ya son cada vez más comunes y de uso cotidiano, lo cual es una buena práctica. Las implementaciones de estos sistemas en medios portátiles como identificaciones personales, chips dentro de tarjetas de crédito, generadores de claves, telefonía celular, computadoras, por mencionar algunos, se encuentran disponibles para el usuario en general. En la actualidad los sistemas con Servicios de Seguridad (SS) vienen siendo implementados en dispositivos móviles y en su mayoría estos son transparentes para el usuario, están ocultos dentro de los protocolos de comunicación. Casi todos los SS se logran mediante la implantación de mecanismos de seguridad, ya sean en hardware o software, en sistemas portátiles que permiten la autenticidad, la confidencialidad, integridad, el no repudio de una manera convincente, excepto el servicio de la disponibilidad y control de acceso. Algunos sistemas de protección como marcas de agua imperceptibles, firmas a obscuras, certificados digitales son empleadas como candados en documentos valiosos, un ejemplo son los pagos de aranceles por medio de transacciones o cheques bancarios para verificar su integridad y su autenticidad. Aunque la seguridad por obscuridad no es la forma de obtener sistemas o medios seguros [1]. La combinación de mecanismos de seguridad mediante algoritmos criptográficos y procedimientos de esteganografía traen consigo aumentar el nivel de seguridad en la manufactura de nuevos equipos portables seguros. Las Tecnologías de la Información y Comunicaciones (TIC) contemporáneas a base de lectores biométricos sólo hacen un reconocimiento de un vector característico de las propiedades biológicas intrínsecas de los usuarios (iris, voz, huella digital, etc.). Los accesos quedan restringidos en estos casos a que el sistema de seguridad tenga disponibilidad o funcione bien, además de tomar en cuenta la autonomía energética, la capacidad y manejo de datos de almacenamiento. Con el desarrollo de las TIC se propone una nueva la construcción de una clave privada con SS mediante el fenómeno de propagación de luz y rejillas semitransparentes que pueden afectar el movimiento de fotones de un modo específico. Usando los fenómenos clásicos involucrados también en los interferómetros, como el principio de Huygens-Fresnel, [2]. Como sabemos los "Quick Response Codes" (QRC por sus siglas en inglés) fueron desarrollados por una organización japonesa para competir con sus sucesores, los códigos de barras. Una ventaja de la creación de los QRC es que fueran leídos por dispositivos portátiles electrónicos para el manejo y almacenamiento masivo de datos, como en el caso de un levantamiento de inventarios. A nuestro grupo de trabajo nos interesan los QRC fundamentalmente por dos razones, para guardar información confidencial cifrada en ellos y la construcción de la matriz de puntos correspondiente [3]. En este trabajo presentamos una mezcla entre un fenómeno físico de la propagación de luz y la implementación de mecanismos de seguridad para el diseño de una clave privada, dispositivo ID óptico, que contenga información confidencial dentro de un QRC. La información dentro del QRC está cifrada mediante el algoritmo "Advanced Encryption Standart" (AES) de 128 bits, [4,5]. Con la matriz de puntos del QRC generamos una rejilla de difracción que produce patrones de difracción y sus correspondientes patrones logarítmicos, es decir el logaritmo en base dos del patrón de difracción. La matriz de puntos a su vez genera una rejilla que al incidir sobre ella luz monocromática producirá el fenómeno de difracción, luego mediante el fenómeno de propagación se tendría su correspondiente patrón

de difracción. El patrón de difracción formado por la superposición de ondas tiene información de los QRC cifrados mediante AES-128. El fenómeno de propagación sobre una abertura (rejilla de difracción como obstrucción) es una aproximación matemática a obtener la transformada rápida de Fourier, así podemos obtener los patrones de difracción y producir imágenes (hologramas) en dos dimensiones. Estas rejillas producirán las imágenes que se grabarán o quemarán para generar la clave óptica privada, un dispositivo óptico único a su correspondiente QRC cifrado, mediante el daño óptico sobre un vidrio BK7. Cabe señalar que la herramienta para realizar el daño óptico permite hacer el grabado tanto en amplitud como en fase, lo que se traduce como el área y la profundidad del vidrio a grabar para el holograma de la clave óptica privada. En la figura (1) mostramos un esquema general para la construcción del dispositivo mediante las herramientas involucradas para ello.

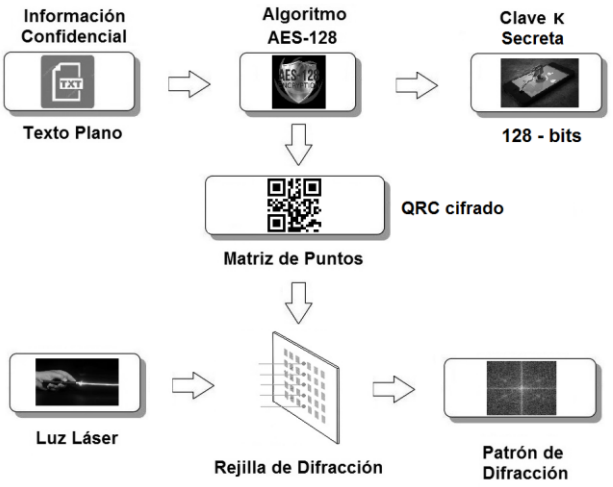

Figura 1. Desarrollo del dispositivo para la clave óptica privada.

Una vez grabados los QRC se iniciara el proceso de recuperación, primero mediante la lectura del patrón de difracción u holograma en el dispositivo óptico. Aplicando la transformada inversa de Fourier se puede obtener el QRC con la informacion cifrada, esto también puede realizarse si se calcula cuatro veces la transformada rápida de Fourier. Luego con un lector de QRC se obtiene el texto cifrado con AES, quien sea el poseedor de la clave secreta K de 128-bits podrá descifrar y obtener el texto plano.

2. SERVICIOS DE SEGURIDAD

La ISO 7498-2 hace la descripción de los SS y sus mecanismos relacionados, esta norma es 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 SS 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 TIC es una técnica que se utiliza para implementar un servicio. Los mecanismos de seguridad proporcionan varios servicios básicos de seguridad o combinaciones de ellos – los SS especifican "cuáles" controles son requeridos y los mecanismos de superposición de ondas tiene información de los QRC cifrados 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).

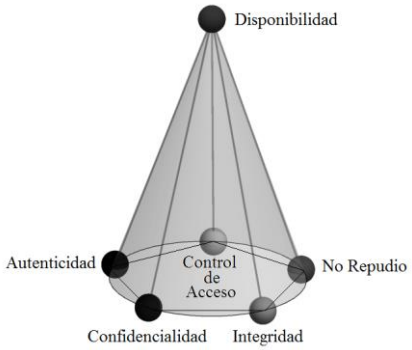

Figura 2. Aristas de una pirámide como SS.

3. ALGORITMO DE CIFRADO AES-128

En esta sección presentamos en forma reducida cómo funciona el mecanismo de seguridad o algoritmo de criptográfico estándar que usaremos para el cifrado de la información que se va a introducir en los QRC para la creación de la clave óptica privada. Así para entender cómo trabaja el algoritmo AES será necesario mencionar algunos antecedentes en el campo de la Aritmética de Números Finitos y Matemáticas Discretas. Antecedentes que habrá que recordar o revisar consultando bibliografía específica en los temas de representaciones de números en diferentes bases (binaria, decimal, hexadecimal y polinomial), sus operaciones básicas en cada base (suma, resta, multiplicación y división) [4,7]. Estrictamente hablando, AES no es precisamente Rijndael (aunque en la práctica se los llama de manera indistinta) ya que Rijndael permite un mayor rango de tamaño de bloques y longitud de claves; AES tiene un tamaño de bloque fijo de 128 bits y tamaños de llave de 128, 192 o 256 bits, mientras que Rijndael puede ser especificado por una clave que sea múltiplo de 32 bits, con un mínimo de 128 bits y un máximo de 256 bits. AES opera en una matriz de 4×4 bytes, llamada “state” (algunas versiones de Rijndael con un tamaño de bloque mayor tienen columnas adicionales en el state). La estructura del algoritmo Rijndael está formada por un conjunto de “rondas”, entendiendo por rondas un conjunto de iteraciones de 4 funciones matemáticas diferentes e invertibles. Luego el algoritmo representa el state como una matriz rectangular de bytes, que posee 4 renglones y N_b columnas. Siendo el número de columnas N_b en función del tamaño del bloque y se puede calcular de acuerdo a la Ec. (1).

$$N_b = \textit{tamaño del bloque utilizado en bits} \;/\; 32 \qquad (1)$$

La clave del sistema se representa con una estructura análoga a la del state, es decir, se representa mediante una matriz rectangular de bytes de 4 renglones y Nk columnas. Siendo el

número de columnas Nk en función del tamaño de la clave, como se muestra en la Ec. (2).

$$N_k = tamaño\ de\ la\ clave\ en\ bits\ /32 \quad (2)$$

Las cuatro transformaciones que aplica el algoritmo a la matriz state por ronda son: i) función "ByteSub" (sustitución con propiedades óptimas de no linealidad), ii) función "ShiftRow" (permiten confusión de la información a lo largo de las diferentes rondas, iii) función "MixColumn" (permiten transposición de la información a lo largo de las diferentes rondas) y iv) función "AddRoudKey" (permite aplicar a la matriz state una operación "xor" or-exclusiva con la subclave correspondiente a cada ronda). Sustitución y transposición juntas son operaciones producto clásicas en criptografía que causan confusión y difusión respectivamente. Los autores definen que para tamaños de bloques y claves de 128 y 256 bits (con incrementos de 32 bits) el número de rondas Nr es determinado por la expresión de la Ec. (3).

$$N_r = \max(N_k, N_b) + 6 \quad (3)$$

En la figura (3) se muestra el proceso de cifrado.

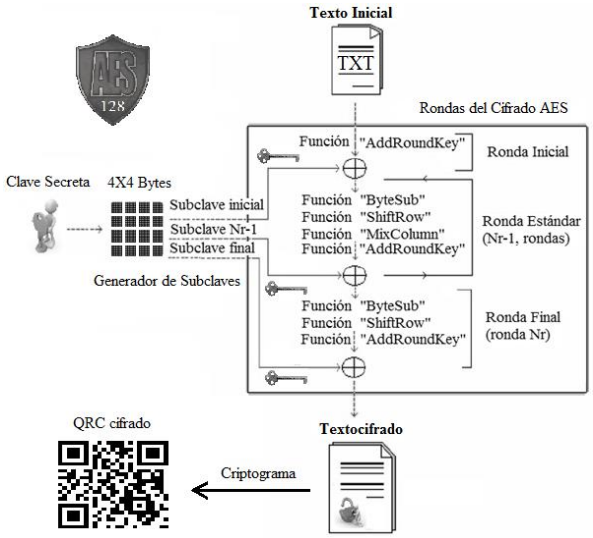

Figura 3. Algoritmo de cifrado AES-128 por rondas.

El criptograma de la información confidencial se usa para crear el QRC cifrado. Increíblemente que parezca para el descifrado del criptograma se aplican las funciones en forma inversa, se usa una tabla inversa para la función de sustitución y la clave de cifrado.

4. CÓDIGOS DE PRONTA RESPUESTA (QRC)

En esta sección describiremos las características propias de los códigos de pronta respuesta o bien QRC y las capacidades de almacenamiento así como la construcción de la matriz de puntos. Particularmente en los QRC (Model 2) se tiene un valor de 58 en el número de simbología, conjunto alfanumérico de bytes dados por el conjunto de caracteres Kanji, [8]. 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 dada 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 los QRC.

Formato	Capacidad datos	Caracteres
Numérico	7089 caracteres	0-9
Alfanumérico	4296	0-9, A-Z (mayúsculas) espacio $ % ‘ + - , . / :
Binarios	2953 bytes	Codificación por defecto: ISO 8859-1 (QRC 2005)
Kanji	1817 caracteres	Desplazamiento 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 AES-128 bits si lo usamos con algún modo de cifrado por bloque para convertirlo en un cifrado por flujo como el "Electronic Code Book" (ECB) o un "Cipher Feed-Back" (CFB). De igual importancia son las dimensiones del símbolo del QRC con los cuales desarrollamos las rejillas de difracción.

5. DIFRACCIÓN DE ONDAS

El fenómeno que se describe cuando ocurre una desviación de la propagación en línea recta de la radiación electromagnética, 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. 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". Lo cual se puede entender que estuviéramos hablando de dos fenómenos, difracción e interferencia, lo cierto es que no hay ninguna distinción física [2]. 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 de la Ec. 4.

$$\tilde{E} = \frac{\mathcal{E}_A e^{i(\omega t - \kappa R)}}{R} \iint_{Rendija} e^{i\kappa(X_x + Y_y)/R} dS. \quad (4)$$

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

$$\Psi(f_x, f_y, z) = \frac{e^{ikz}}{i\lambda z} \iint_A \Psi_A(x,y) e^{-i\,2\pi(f_x x + f_y y)}\, dx.dy \qquad (5)$$

donde $\psi_A(x, y)$ es la abertura y (f_x, 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 Ec. (5) se puede obtener a partir de la integral de superficie de Fresnel-Kirchhoff usada para la difracción sobre aberturas con simetría rectangular [9,10], figura (4). Cuando la integral se define sobre el intervalo [-∞, ∞] 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 logarítmico se calcula el logaritmo en base 2 de la Transformada rápida de Fourier resultante.

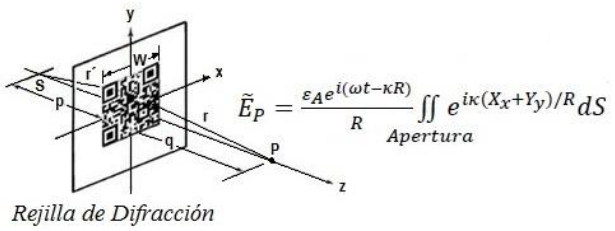

Figura 4. Sistema de la propagación sobre las rejillas para la obtención de los patrones de difracción.

6. SELLOS O MARCAS DE AGUA

Los sellos o las Marcas de Agua (MA) no son 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 esquema impreso sobre una pieza de papel durante una producción y para la identificación del *copyright*, figura (5). El esquema 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 del 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. [3]

Figura 5. Marca de agua sobre: a) papel, 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 (6) 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.

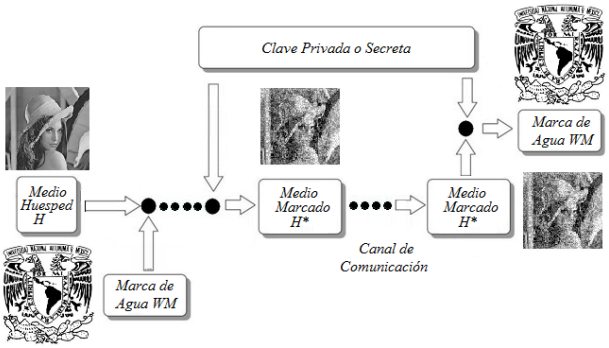

Figura 6. Esquema de inserción para Marcas de Agua Digitales.

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. [11-18]

6.1 Condiciones para las Marcas de Agua

Las condiciones para una inserción de marcas de agua son tres:
I. Capacidad: Es la cantidad máxima de información que puede ser ocultada en un medio.

II. 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.
III. 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 [19,20].

7. METODOLOGÍA DE GRABADO Y LECTURA

Con base en el diagrama de la figura (1), la metodología consiste en cifrar el texto claro (información clasificada) con una clave privada de 128-bits, mediante AES, después generar los QRC de la información cifrada. Luego para la obtención de los patrones de difracción, realizaremos el cálculo de la Transformada Rápida de Fourier (FFT, por sus siglas en ingles) en dos dimensiones del modelo analítico de la apertura de la rejilla. Esto como una aproximación matemática del modelo de difracción en óptica para calcular los patrones en campo lejano, a partir de una fuente de luz monocromática [10]. Se define un sistema de coordenadas en un arreglo “X” y “Y” colocando adecuadamente el origen. La propagación de radiación electromagnética a través de la rejilla es lo que determinará el patrón de difracción generado. Estos patrones se forman en la zona de Fresnel y que deben cumplir las condiciones de difracción mediante la superposición de las ondas en un corte plano perpendicular a la dirección de propagación. Para desplegar la intensidad de la luz en campo lejano se calcula el cuadrado del campo y se visualiza el patrón de difracción.
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, se producirá el daño óptico sobre un bloque de vidrio BK7 de 1.2 [cm] de altura por 1.2 [cm] de ancho y por 1 [cm] de profundidad usando un láser de Nd:YAG que opera con pulsos con perfil de intensidad gaussiano de 35 [ps], un ancho de 5 [mm] y con una energía de 35 [mJ], figura (7).

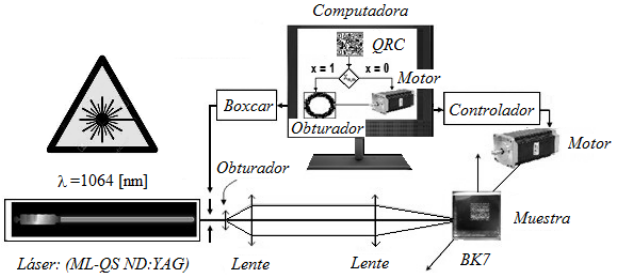

Figura 7. Sistema de daño óptico computarizado.

Este sistema será una entidad repositoria acreditada conocida también como autoridad certificadora donde se encuentran todas las claves ópticas públicas conocidas, figura (8). Para la lectura del dispositivo óptico (placa de vidrio) se implementó un sistema automatizado que permite leer el código cifrado.

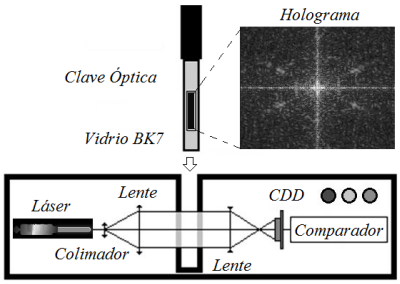

Figura 8. Sistema de lectura de la clave óptica.

Este sistema sólo reconocerá la clave óptica privada, es decir, saber quién es el poseedor del dispositivo o quien la porta, pero no puede conocer la información confidencial cifrada dentro del mismo y a su vez la autenticidad [8,13]. El sistema tiene la opción de comprobación de la información confidencial mediante su clave privada usada para cifrar la información con el algoritmo criptográfico AES. De igual forma tiene un señalamiento de comprobación de la clave privada y de la vigencia del dispositivo óptico. El dispositivo diseñado actuará como una clave óptica privada que cumple con SS mediante la lectura del grabado de la placa de vidrio del patrón generado por los QRC cifrados que es único. Esto puede semejar a un NIP o a un token que es utilizado para el control de acceso en comercio electrónico. Los resultados obtenidos son los medios portadores, patrones de difracción (imágenes bidimensionales) en el dispositivo óptico con la información clasificada oculta de la matriz de puntos de los QRC cifrados que es una clave óptica de seguridad. Si algún atacante quisiera recuperar la información debe de realizar el procedimiento inverso, es decir escanear el patrón de difracción, obtener los QRC cifrados, extraer la información del QRC cifrada, aplicar el algoritmo inverso de cifrado y recuperar el texto claro. Los pasos anteriores tienen cada uno de ellos un grado de dificultad, lo que nos va proporcionando niveles de seguridad implementados en nuestro sistema. Pero la seguridad no se implementa ocultando información (Esteganografía), sino implementando el cifrado de la información, esto es el uso de algoritmos criptográficos. Nuestro grupo académico ha trabajado sobre el preprocesamiento de información para introducirla y ocultarla en un medio portador digital de forma imperceptible [14,15].

8. CRIPTOGRAFÍA DE CLAVE PÚBLICA

Este tipo de criptografía comienza a ser ampliamente usado y conocido a través de su aplicación en los sistemas de correo electrónico seguro “Pretty Good Privacy” (PGP), "Privacy Enhanced Mail" (PEM) y "Distinguish Encoding Rules" (DER) bajo el estándar X.509 permitiendo cifrar e incluir una firma digital adjunta al documento o e-mail enviado y también en los navegadores WEB. Como hemos mencionado cada usuario tendrá dos claves una privada y otra pública, inversas entre si dentro de un sistema, además usan funciones unidireccionales con trampa (FUT). Estas FUT son funciones matemáticas de un solo sentido y que nos permiten usar la función en sentido directo o de cálculo fácil para cifrar y descifrar (usuarios legítimos) y fuerza el sentido inverso o de cálculo difícil para aquellos impostores, hackers, etc. Que lo que desean es atacar o criptoanalizar el criptograma.

8.1 El acuerdo de claves Diffie & Hellman

El inicio de los sistemas de clave pública se debe al estudio hecho por Whitfield Diffie y Martin Hellman (1976), [29,30]. Debido al protocolo de Intercambio de claves de Diffie y Hellman. Alice y Bob seleccionan un grupo multiplicativo (con inverso) p y un generador α de dicho primo, ambos valores públicos.

• Alice genera un número aleatorio a y envía a Bob $\alpha^a \bmod p$.
• Bob genera un número aleatorio b y envía a Alice $\alpha^b \bmod p$.
• Bob calcula $(\alpha^a)^b \bmod p = \alpha^{ab} \bmod p$ y luego destruye b.
• Alice calcula $(\alpha^b)^a \bmod p = \alpha^{ba} \bmod p$ y luego destruye a.
• El secreto compartido por Alice y Bob es el valor $\alpha^{ab} \bmod p$.

9. DISEÑO DE PROTOCOLOS CON SEGURIDAD

Por definición un protocolo es una serie de pasos, que implica a dos o más partes, diseñadas para cumplir una tarea. Se trata de una definición importante. "Una serie de pasos" significa que el protocolo sigue una secuencia de estos de principio a fin. Cada paso debe ser ejecutado a su vez y no puede tomarse antes de que termine el paso anterior. "Con dos o más partes" se entiende que al menos dos personas son necesarias para completar el protocolo. Una sola persona puede realizar una serie de pasos para realizar una tarea (como hornear un pastel), pero esto no se trata de un protocolo. (Alguien debe comer la torta y comunicarlo para que sea un protocolo). Por último, "diseñado para cumplir una tarea" significa que el protocolo debe lograr algo. Los protocolos tienen otras características como: la mayoría de los involucrados en el protocolo deben conocerlo y todos los pasos a seguir por adelantado. Todos los involucrados deben estar de acuerdo en seguirlo. El protocolo debe ser inequívoco; cada paso debe ser bien definido y no debe haber ninguna posibilidad de un malentendido. El protocolo debe ser completado; debe haber una acción determinada para cada situación posible.

El interés de los Protocolos en la vida cotidiana, hay protocolos informales para casi todo: pedir mercancías por teléfono, jugar al póker, votar en una elección. Nadie piensa mucho acerca de ellos, han evolucionado con el tiempo y digamos todo el mundo sabe cómo usarlos, funcionan razonablemente bien. En estos días, la interacción más humana ocurre por redes informáticas en lugar de cara a cara. Las computadoras necesitan protocolos formales para hacer las mismas cosas que la gente hace sin pensar. Casi todos los protocolos cara a cara se llevan a cabo en presencia del pueblo por ejemplo las votaciones, para garantizar la equidad y la seguridad.

9.1 Autoimplementación de Protocolos

Este tipo de protocolos se diseñan de tal manera que hacen virtualmente imposible el engaño. Dado que no requieren ni árbitro ni juez y garantizan que si cualquier participante engaña, el engaño es descubierto de inmediato por el otro u otros participantes.

Características Típicas:

• Detección de la conexión física sobre la que se realiza la conexión (cableada o sin cables)
• Pasos necesarios para comenzar a comunicarse (“Hand-shaking”, saludo de manos)
• Negociación de las características de la conexión.
• Cómo se inicia y cómo termina un mensaje.
• Formato de los mensajes.
• Qué hacer con los mensajes erróneos o corruptos (corrección de errores)
• Cómo detectar la pérdida inesperada de la conexión, y qué hacer en ese caso.
• Terminación de la sesión de conexión.
• Estrategias para asegurar la seguridad (autenticación, cifrado).

La última propiedad del protocolo de comunicación es la que implementaremos en este trabajo mediante servicios de seguridad y con la comprobación de las secuencias pseudoaleatorias utilizando los postulados de Golomb [5].

9.2 Protocolo con base en criptografía de clave pública

En esta subsección construiremos el escenario para establecer la comunicación y qué tipo de servicio de seguridad se implementará en el diseño del protocolo. Para esto veamos primero unos simples desarrollos para entender la notación a utilizar [15]. Partimos de un sistema de comunicación entre Alice y Bob como comúnmente se muestra en la Figura (9), donde también hay un guardián del canal de comunicación.

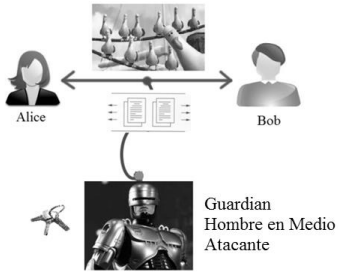

Figura 9. Diagrama de comunicación entre dos partes y un atacante del mensaje enviado.

Veamos las consideraciones para generar el protocolo:
- Alice tiene el documento que desea transmitir.
- Se usará el algoritmo RSA para firmar y verificar (criptografía asimétrica).
- Todas las claves K están certificadas.
- Todas las partes tienen sus propias parejas de claves (púbica y privada).
- AC: Asociación Certificadora, es confiable además verifica todas las firmas.

Objetivo.- A, B y C deben firmar el documento m y AC debe verificar todas y cada una de las firmas. Para este estudio se emplearán tanto técnicas de criptografía simétrica como pública, en particular los algoritmos son el AES de 128-bits y RSA de 1024 respectivamente. Para empezar nuestro protocolo del escenario citado veamos como empleamos los algoritmos de cifrado:

1. *A: genera K_s*
2. *A:* $E_{K_s}^{AES}(m) = C_1$
3. *A:* $E_{RSA_{K_B}}^{pub}(E_{RSA_{K_A}}^{priv}(K_s)) = C_2$ donde $E_{RSA_{K_A}}^{priv}(K_s)$ es la firma
4. *A → B: C_1, C_2*
5. *B:* $E_{K_B}^{priv}(C_2) = Firma$
6. *B:* $D_{K_A}^{pub}(E_{K_A}^{priv}(K_s)) = K_s$
7. $D_{K_s}^{AES}(C_2) = m$

Ahora vamos a implementar la Confidencialidad y Autenticación mutua:

1. *A:* $E_{K_{ab}}(m) = C_1$
2. *A → B: C_1*

3. *B:* $D_{K_{ab}}(C_1) = m$
4. *B:* $E_{K_{ab}}(m') = C_2$
5. *B →A: C2*
6. *A:* $D_{K_{ab}}(C_2) = m'$
7. *A: m'=m, compara*

Si le sumamos Integridad al protocolo anterior se obtiene:

1. *A:* $E_{K_{ab}}(m) = C_1$
2. *A:* $E^{CBC}_{K_{ab}}(m) = C^{A}_{MAC-64}$
3. *A →B:* (C_1, C^{A}_{MAC-64})
4. *B:* $D_{K_{ab}}(C_1) = m'$
5. *B:* $E^{CBC}_{K_{ab}}(m) = C^{B}_{MAC-64}$
6. *B:* $C^{B}_{MAC-64} = C^{A}_{MAC-64}$ *compara*
7. *B →A(* C^{B}_{MAC-64} *, m')*
8. *A:* $E^{CBC}_{K_{ab}}(m') = C^{A}_{MAC-64}$
9. *A:* $C^{A}_{MAC-64} = C^{A}_{MAC-64}$' *compara,*

donde *MAC*: *Message Autentication Code* y *m'*: el mensaje a comparar. Así se puede hacer la lectura de la clave óptica bajo un esquema de criptografía pública o de clave asimétrica.

10. RESULTADOS

Sistema de grabado

Realizando varios experimentos se logró obtener un umbral para la potencia que necesitamos en el láser para el daño óptico en vidrios BK7 de 1.44 [cm^3] (n_r=1.506 y transmitancia 0.999), con una longitud de onda λ=1064 [nm] del láser Nd:YAG la potencia es de 7.1 ± 0.3 [mW]. El daño óptico dentro del BK7 se hace penetrando en un plano interno paralelo a la superficie de incidencia aunque el daño puede hacerse tomando en cuenta la fase lo cual produciría un holograma tridimensional de la clave óptica privada. La profundidad del daño varía desde unas micras hasta 2 [mm], esto se debe al tiempo de exposición directamente relacionado con el obturador. Para las alteraciones locales sobre la estructura del material óptico se tienen varias características como: una uniformidad de densidad del BK7 que es no controlable pero sería deseable, tiene una estabilidad de emisión también no controlable pero sería deseable, se tiene una repetición de pulsos y enfoque controlable no deseable y deseable respectivamente. El movimiento de la muestra es deseable que fuera completamente automatizado, sin embargo se tiene movimiento sobre las abscisas mediante un motor a pasos de 10 [μm] y en las ordenadas manualmente mediante un tornillo micrométrico. Los resultados que se muestran a continuación son parámetros propios del sistema de daño óptico y de los diámetros producidos debido a los daños de acuerdo a la energía de incidencia. Primero con una Frecuencia de Repetición de Pulsos (FRP) de 5 [Hz] y un diámetro del obturador de 5[mm] se tiene:

Distancia focal [mm]	Energía [mJ]	Diámetro del daño [mm]
25.4	0.3	0.06
25.4	0.3	0.12
25.4	0.4	0.12
100	0.25	0.18

Luego para una FRP de ω=10 [Hz], λ=1064 [nm], con un diámetro del obturador de D=20 [mm] y una distancia focal de f=25.4 [mm] se puede obtener el radio del disco de Airy para calcular el tamaño del haz enfocado mediante la expresión:

$$d \approx 2.44 \frac{f\lambda}{D} \tag{6}$$

$d_{teórico}$=3.29 [μm] y d_{medio}=50 [μm],

esto nos da el tamaño del ancho haz gaussiano con que se hace el daño óptico sobre el BK7. El grabado de las rejillas se hace con periodos de 70, 80 y 100 [μm], figura (10). Para producir una imagen 2D de buena calidad son necesarios cerca de 100,000 puntos en un área de 7 x 7 [mm]. Si la distancia entre dos puntos adyacentes del grabado de pistas en el plano XY, perpendicular al haz láser, es más pequeña que d, un desplome (fractura interna) puede ocurrir.

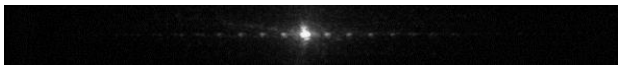

Figura 10. Patrón de difracción producido por 11 líneas grabadas con separación de 100 [μm], con 7 órdenes de difracción.

Patrones de Difracción generados por los QRC

Como resultados mostraremos los QRC con cifrado y sin cifrado para observar la diferencia en su matriz de puntos generada. Para este caso usaremos una clave privada formada por 16-Bytes de 128-bits binaria, que forman una palabra de 16 caracteres para el algoritmo de cifrado AES-128. La clave privada empleada fue 0123456789ABCDEF, 16-caracteres con un total de 128-bits. La figura (11a) muestra un ejemplo de los QRC con texto plano y la (11b) es su respectivo QRC cifrado, donde se pueden apreciar las diferencias entre ambos arreglos de puntos.

Figura 11. QRC con a) texto plano: CISCI20_CISCI20_ b) texto cifrado: ÍÂÙhM3feÅ,ÏM6®^þ.

Dos casos particulares se presentan en las figuras (12) y (13), son ejemplos de la metodología empleada para la obtención de los Patrones de Difracción (PD) y sus Patrones Logarítmicos (PL), que son los logaritmos en base 2 de los patrones de difracción.

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

*A_1= rect((X-delta)/b).*rect((Y-delta)/b)*
*-rect((X-delta)/a).*rect((Y-delta)/a);*
*A_2=rect((X-delta)/b).*rect((Y-delta)/b)*
*-rect((X-delta)/a).*rect((Y-delta)/a);*
*A_3=rect((X+delta)/b).*rect((Y-delta)/b)*
*-rect((X+delta)/a).*rect((Y-delta)/a);*
*A_4=rect((X-delta)/d).*rect((Y-delta)/d)*
*+rect((X+delta)/d).*rect((Y+delta)/d)*
*+rect((X+delta)/d).*rect((Y-delta)/d);*

$$A_5=rect((X)/(4*dc)).*rect((Y-dc)/(dc)) +rect((X+5)/(2*dc)).*rect((Y+b)/(dc)) +rect((X)/(4*dc)).*rect((Y+80)/(dc)) +rect((X+16)/(0.65*dc)).*rect((Y+32)/(9.2*dc)). \quad (7)$$

Y así la abertura está dada por $A = A_1+A_2+A_3+A_4+A_5$; con la función *rect(X, Y)* en el intervalo de [-1/2,1/2] y con constantes a=70; b=40; d=20; dc=10; delta=340. En la imagen de la figura (12a), se muestra el modelo matemático de la apertura de la rejilla con los tres cuadrados de referencia de los QRC y la letra "E" al centro, la figura (12b) se calcula a partir de la Ec. (5) la transformada rápida de Fourier. La figura (12c) es una ventana del PD y la figura (12d) es el Log_2 del PD, [14-17].

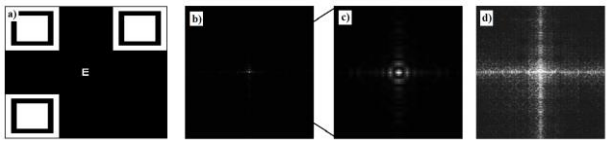

Figura 12. a) Código QR con la letra E, b) patrón de difracción, c) ventana del patrón de difracción y d) logaritmo del patrón de difracción.

La figura (13a) tiene también los tres cuadrados de referencia y un logotipo al centro, calculamos la FFT obteniendo su PD y PL respectivamente, figuras (13b) y (13d).

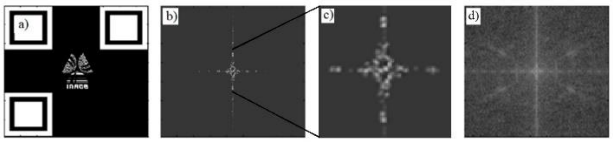

Figura 13. a) Código QR con logotipo del INAOE, b) patrón de difracción, c) ventana del patrón de difracción y d) logaritmo del patrón de difracción.

A continuación presentamos los datos con los mensajes, claves y mensajes cifrados usados en el algoritmo AES-128, para la construcción de los QRC. Los caracteres de la Tabla (2) están dados en el ASCII latín donde algunos caracteres no tienen símbolo o no son imprimibles. Las imágenes de los QRC cifrados, su patrón de difracción y su correspondiente patrón logarítmico se presentan en las figuras (14), (15), (16) y (17), en todos estos casos usamos la misma clave de cifrado AES-128, K=0123456789ABCDEF en arreglos de 4X4 bytes.

Tabla 2. Mensaje, claves y cifrados con AES-128.

Mensaje	Clave	Cifrado
CISCI20_CISCI20_	0123456789ABCDEF	ÍÂÜhM3feÄ,ÏM6®^þ
INAOEPUEINAOEPUE	0123456789ABCDEF	Ô→×↔È)R´ä⊥→1º_-¸
AABBCCDDEEFFGGHH	0123456789ABCDEF	«ü␣ÎÔ8ü[→?s|nu§
0123456789ABCDEF	0123456789ABCDEF	·→]ýØºÖ→þB→Ä! →

Luego como casos de estudio utilizaremos cuatro matrices de puntos con información cifrada como rejillas para obtener los PD, un acercamiento del mismo PD y sus correspondientes PL, donde pueden observarse mejor el patrón de puntos.

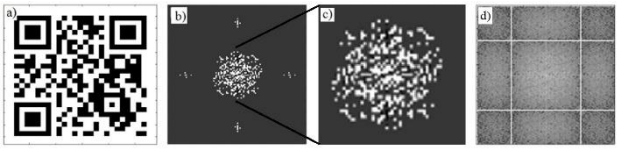

Figura 14. a) QRC cifrado del texto plano: CISCI20_CISCI20_, b) patrón de difracción, c) ventana del patrón de difracción y d) logaritmo del patrón de difracción.

Los PD son tenues como en el caso de la inserción de una marca de agua poco perceptible, sin embargo en el PL es más perceptible, [11,18]. Aunque son más perceptibles las marcadas de las referencias de los QRC. 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 rápida de Fourier que se utiliza para hacer la aproximación de la propagación de la luz incidente sobre las aberturas. Algo que pudimos 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.

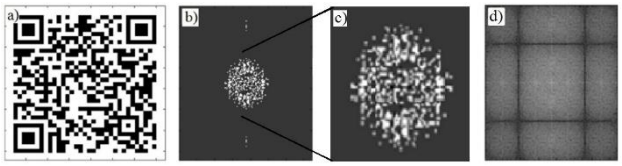

Figura 15. a) QRC cifrado del texto plano: INAOEPUEINAOEPUE, b) patrón de difracción c) ventana del patrón de difracción y d) logaritmo del patrón de difracción.

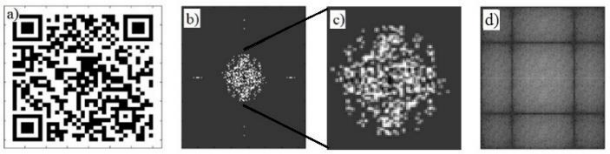

Figura 16. a) QRC cifrado del texto plano: AABBCCDDEEFF, b) patrón de difracción c) ventana del patrón de difracción y d) logaritmo del patrón de difracción.

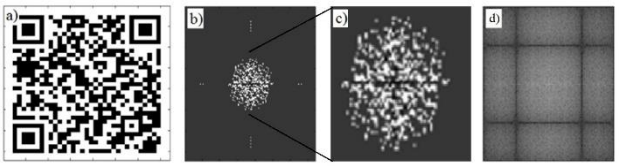

Figura 17. a) QRC cifrado del texto plano: 0123456789ABCDEF, b) patrón de difracción c) ventana del patrón de difracción y d) logaritmo del patrón de difracción.

Pruebas de factibilidad

Lo que a continuación mostramos es como quedaría la clave privada usando la técnica de grabado mostrada en la referencia [11,18], 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 QRC y ocultados como MA en los patrones de difracción. La figura (18 y 19) es una muestra de la factibilidad del dispositivo.

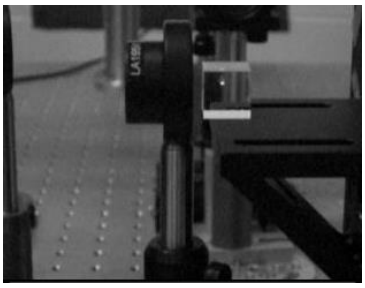

Figura 18. Grabado punto por punto sobre el BK7 con separación de 70 [μm].

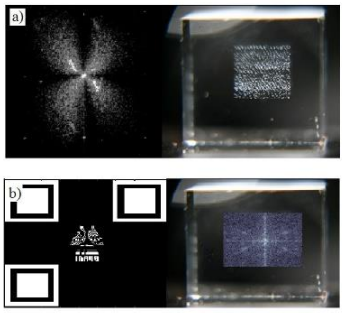

Figura 19. a) Hologramas creados y grabados dentro de un BK7. b) Un QRC con logotipo y su grabado.

Lectura y Recuperación del Mensaje

Mostremos ahora el proceso de recuperación a parir de la marca de agua u holograma para obtener el QRC según la figura (20).

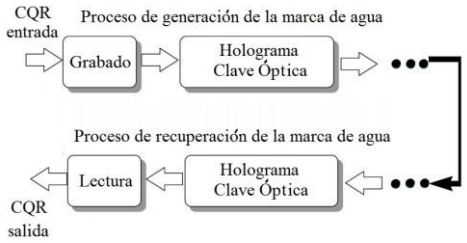

Figura 20. Diagrama para el proceso de recuperación del CQR.

Entonces para la recuperación de los QRC será necesario calcular la transformada rápida inversa de Fourier de las claves ópticas leídas con el sistema de la figura (8), obteniendo los QRC que cualquiera pudiera leer con una aplicación adecuada. Sin embargo la información de los QRC está cifrada con AES-128 mediante una clave privada que sólo el poseedor de ella podrá leer esa información, descifrando los criptogramas obtenidos. Para descifrar los criptogramas se usa la clave privada 0123456789ABCDEF en todos los casos mediante el descifrado de AES-128 que se usó y se obtiene los mensajes: CISCI20_CISCI20_, INAOEPUEINAOEPUE, AABBCCDDEEFFGGHH y 0123456789ABCDEF. En las lecturas, los cifrados de los QRC de la figura (21) corresponden en el código ASCII (latino) a los caracteres mostrados, que es la información cifrada de los textos en planos.

Figura 21. Códigos QR a partir de los patrones de radiación.

La lectura de clave óptica debe cumplir con el esquema de criptografía asimétrica y seguir el siguiente protocolo, Alice (usuario), Bob (sistema de lectura):

a) Alice cifra su información confidencial (mensaje: M), mediante AES-128 $E_{AES}[K_A^{priv}(M)]$, genera su código QR y lo envía a Bob.

b) Bob recibe el código QR genera la rejilla de difracción, la graba sobre el vidrio BK7 usando su clave privada $E_{sis}[K_B^{priv}(E_{AES}(K_A^{priv}(M))]]=K_A^{opt}$.

c) Bob genera una clave secreta de Alice que nunca conoce $K_A^{sec}(M)$ como identificador y envía la clave óptica K_A^{opt} a Alice.

Para control de acceso se tiene:

d) Alice porta su clave óptica K_A^{opt} de identificación y la muestra al sistema de lectura que tiene Bob.

e) Bob con su sistema de lectura, lee la clave óptica de Alice $E_{sis}^{-1}[K_A^{opt}]$ identifica a Alice con $K_A^{sec}(M)$ dándole luz verde de acceso.

En este protocolo nunca se pone en claro la información confidencial de Alice. Para verificar la clave privada de Alice, Alice debería encontrar el patrón de radiación con la antitransformada de Fourier para obtener el código QR con la clave privada de Bob. Una vez obtenido el código QR cualquiera lo puede leer pero la información está cifrada, sólo Alice puede verla haciendo el descifrado AES de la misma con $E_{AES}^{-1}[K_A^{priv}(M)]$ obteniendo M. Lo cual semeja al algoritmo del mensaje en la caja que nadie puede ver sólo Alice.

Ahora introduzcamos algunos resultados demostrativos para una discusión breve sobre seguridad en patrones de difracción y en sistemas de holografía digital. Primero presentaremos una rejilla de difracción de una hipocicloide, figura (22).

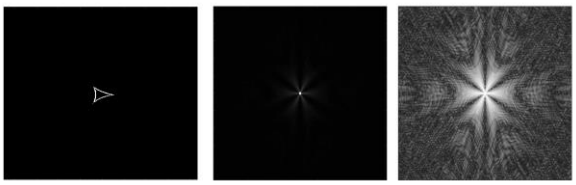

Figura 22. La rejilla de difracción de una hipocicloide, su patrón de difracción y su patrón logarítmico.

Calcularemos cuatro veces la transformada de Fourier rápida discreta de la rejilla de difracción producida por la hipocicloide, recuperando la rejilla inicial, ver la figura (22).

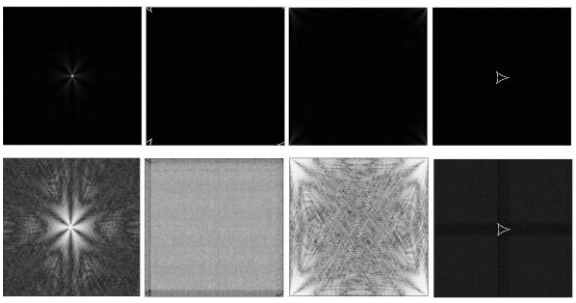

Figura 23. Cuatro veces la Transformada de Fourier rápida discreta de una hipocicloide, fila de arriba; patrón de difracción logarítmico, fila de abajo.

Después para hacer más evidente lo que deseamos discutir en la sección siguiente, haremos lo mismo con un QRC, recuperando la rejilla inicial, es decir el QRC con el texto plano.

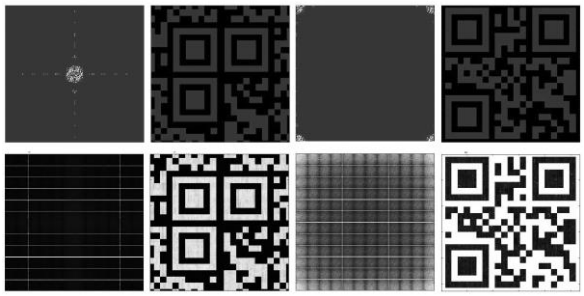

Figura 24. Cuatro veces la Transformada de Fourier rápida discreta de un QRC cifrado del texto plano INAOEPUEINAOEPUE, fila de arriba. La transformada cuatro veces del patrón de difracción logarítmico, fila de abajo.

En las dos figuras (23 y 24) anteriores, se muestran la recuperación de la rejilla con la que se obtuvieron los patrones de difracción. En el caso de la figura (24), con cualquier aplicación lectora de QRC se puede descubrir el mensaje oculto en un patrón de difracción, lo cual no es seguro.

11. DISCUSIÓN

Lo que hemos mostrado en este trabajo es como usando varias técnicas y fenómenos físicos se puede aumentar el nivel de seguridad en los dispositivos de identificación usados como control de acceso, confidencialidad de datos, integridad, no repudio y autenticidad. Sin embargo para la sociedad y a veces para la comunidad científica, el ocultar información clasificada por un procedimiento como rotación, redimensionamiento, transformación en el campo de la frecuencia por mencionar algunos; con eso ya tienen un sistema criptográfico [21-25]. Como en el caso de la obtención del patrón de difracción mediante QRC no cifrados, este es un procedimiento puramente esteganográfico (ocultar información en otro medio), ya que después de aplicar varias veces el procedimiento de transformación o la transformación inversa obtenemos los mensajes en claro. Al usar un QRC cifrado mediante el estándar AES-128, tenemos un sistema con mecanismos y servicios de seguridad; lo que hacen al producto un dispositivo óptico seguro. Una comprobación se muestra en la figura (25), donde cualquier aplicación lectora de QRC puede ver el contenido.

Figura 25. Lectura de un QRC con cifrado mediante una aplicación en el celular. El texto plano se escribió para saber de dónde provino el criptograma.

Aunque la información que logré obtener el lector QRC, será información cifrada y es indescifrable para cualquiera que no tenga la clave secreta del proceso de cifrado mediante el AES-128. En seguridad de la información donde todo sistema con servicios de seguridad implementados sigue normas y estándares, se dice que es un sistema criptográfico si se emplean mecanismos de seguridad. Y los mecanismos de seguridad son implementados mediante algoritmos criptográficos estándares y protocolos de comunicación seguros.

Por otro lado hay varios sistemas de generación de claves donde el requerimiento es obtener secuencias de números binarios en forma pseudoaleatoria. Además de cumplir una serie de pruebas estadísticas, de la norma SP 800-22, para considerar esos resultados como sistemas generadores de claves en aplicaciones criptográficas. Los fenómenos físicos de la naturaleza pueden ser completamente aleatorios como el clima, el ruido, el entrelazamiento de fotones, interferencias por mencionar algunos y con ellos generar secuencias binarias aleatorias. En general estos sistemas pueden ser empleados para generadores de claves, sin embargo nuevamente no son seguros, sino se tiene un buen diseño de protocolos de comunicación que logré la distribución segura de claves. Un problema principal de la seguridad de la información es la distribución y administración de las claves usadas en sistemas criptográficos. Estas discusiones nos llevan a la creación de sistemas de seguridad ocupando estos aspectos, distribución de claves y generación de claves mediante protocolos seguros que en trabajos posteriores se desarrollarán y realizaremos sus conexiones con tecnologías como el "Blockchain", los "Bitcoin", criptomonedas y el internet de las cosas, [26-28].

12. CONCLUSIONES

La intención de producir un objeto manejable con estas características es para generar un dispositivo con una clave óptica privada con SS implementados portable, casi como una huella digital sin depender de generadores de secuencias dinámicas pseudoaleatorias [14-17]. La seguridad que presentamos es: cualquiera puede leer la información formada en la matriz de puntos del QRC pero no cualquiera la puede descifrar, aun sabiendo que hay información oculta en el patrón de difracción o estego-objetos cifrados que muestran los resultados. El dispositivo creado como un medio portador de la información clasificada, contiene mecanismos de seguridad, hablando de los SS pueden emplearse ya sea como control de acceso por convicción, además de que tiene confidencialidad, autenticidad, no repudio e integridad [6]. El grabado o daño óptico puede mejorarse en forma automatizada incrementando la precisión en la posición de cada disparo del láser cerca de lo óptimo, en la cual se pueda reproducir fielmente cada pixel de la rejilla de difracción. Se obtuvo el menor daño posible con la mínima energía a las frecuencias de repetición de pulsos 5 y 10 [Hz], esto nos ayuda a la disminución del tamaño del daño al cambiar la lente con distancia focal más corta. En los resultados reportados [12], se determinó el umbral de daño para el vidrio BK7 aproximadamente de 91[GW/cm2] (energía de 0.25 [mJ], en un área de 7.85 x 10-5 [cm2]). Es importante recordar que el patrón de difracción prácticamente desaparece conforme la distancia entre las líneas disminuye y la cantidad de luz dispersada aumenta. Otro dato importante reportado es que el tamaño mínimo del daño que es de 50 ± 10 [μm]. En el vidrio se genera una birrefringencia inducida debida a los impactos del láser sobre el material. Hay una fuerte componente de

dispersión espacial en el registro del holograma. La lectura de las claves ópticas privadas se realiza bajo el esquema de criptografía asimétrica usando dos claves una privada para AES-128 (cifrado y descifrado) y otra la clave pública para el sistema de la figura (6) y un identificador del usuario [15]. El sistema de lectura consiste en usar los parámetros adecuados para reproducir el patrón de difracción del holograma grabado en el vidrio BK7, los cuales son distancia focal, longitud de onda del láser, periodo de la rejilla.

13. AGRADECIMIENTOS

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).

14. REFERENCIAS

[1] E. Daltabuit, L. Hernández, G. Mallén, J. Vázquez, "La seguridad de la Información", **Ed. Limusa**, 2007.

[2] E. Hecht, "Óptica". 3a. edición. **Ed. Addison Wesley Iberoamericana**, Madrid 2000.

[3] Códigos QR. **Wikipedia.** Available at: https://es.wikipedia.org/wiki /C%C3%B3digo_QR , (Accessed on: Aug 23, 2017).

[4] Computer Security Standard. **FIPS-197**, Specification for the Advanced Encryption Standard (AES). (2001).

[5] A.J. Meneses, P.C. Van Oorschot, S.A. Vanstone, "Handbook of Applied Cryptography", **Ed. CRC**, 2000.

[6] INTERNATIONAL STANDARD, **ISO 7498-2**, Information processing – Open Systems Interconnection – Basic Reference Model. Security Architecture. First edition 1989-02-15.

[7] A. Padrón Godínez, "Implantación del algoritmo de cifrado AES en FPGA para protección de datos". **Tesis**, Maestría en Ingeniería en Seguridad y Tecnologías de la información, ESIME-Culhuacán, IPN, México, 2013.

[8] INTERNATIONAL STANDARD, **ISO / IEC 18004**, Information technology — Automatic identification and data capture techniques — Bar code symbology — QR Code., First edition 2000-06-15.

[9] F.L. Pedrotti, L.S. Pedrotti, "Introduction to Optics", **Ed. Prentice-Hall Int. Inc.**, USA, 1993.

[10] Matlab Manual. **The MathWorks**, Inc. 1994-2018.

[11] F.Y. Shih, "Digital Watermarking and Steganography", **Ed. CRC Press**, USA, 2008.

[12] C.G. Treviño-Palacios, A. Olivares-Pérez, O.J. Zapata-Nava, , "Optical damage as a computer generated hologram recording mechanism," **Journal of Applied Research and Technology**. Vol. 13 (2015) 591595. http://dx.doi.org/10.1016/j.jart.2015.10.015.

[13] A. Padrón-Godínez, R. Prieto Meléndez, C.G. Treviño-Palacios, "Authentication of QR codes used as watermarks in diffraction patterns". **Conference:** Mexican Optics and Photonics Meeting. Tonantzintla, Puebla - México, 2017. DOI: 10.13140/RG.2.2.17959.29608.

[14] A. Padrón-Godínez, R. Prieto Meléndez, C. G. Treviño-Palacios, "Códigos QR cifrados como Marcas de Agua en Patrones de Difracción". **Memorias:** SOMI XXXII, Congreso de Instrumentación, Acapulco, Guerrero-México, 2017.

[15] A. Padrón-Godínez, R. Prieto Meléndez, C. G. Treviño-Palacios, "Lectura de clave óptica bajo el esquema de criptografía asimétrica". **Memorias:** SOMI XXXIV, Congreso de Instrumentación, Morelia, Michoacán-México, 2019.

[16] N. Castro-Acuña, M. A. Leguizamón-Páez, A. L. Mora-Lancheros, "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, España, https://doi.org/10.18273/revuin.v18n4-2019015, 2019.

[17] A. Padrón-Godínez, R. Prieto Meléndez, C. G. Treviño-Palacios, "Confidencialidad de datos mediante el grabado de códigos QR cifrados: ID-óptico", **I+D Tecnológico**, 16 (2), 15, 2020. DOI https://doi.org/10.33412/idt.v16.2.2832.

[18] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, T. Kalker, "Digital Watermarking and Steganography", **Ed. Morgan Kaufmann**. pp. 624, 2007. https://doi.org/10.1016/B978-0-12-372585-1.X5001-3.

[19] Y. In-Kwon, J. K. Hyoung, "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.

[20] A.J.M. Houtsma, T.D. Rossing, "Auditory Demonstrations". Institute of Perception Research, 1987. **Folleto del CD** "Auditory Demonstrations", Philips 1126-061.

[21] O.J.M. Vilardy, C. Jimenez, C.O. Torres Moreno, "Optical Image Encryption System Using Several Tilted Planes". **Photonics,** 6(4):116. November 2019. DOI: 10.3390/photonics6040116.

[22] W. Chen, Javidi, B., X. Chen, "Advances in optical security systems". **Advances in Optics and Photonics** 6(2). June 2014. DOI: 10.1364/AOP.6.000120.

[23] W. Chen, X. Chen, "Arbitrarily modulated beam for phase-only optical encryption". **Journal of optics**, 16(10):105402. September 2014. DOI: 10.1088/2040-8978/16/10/105402.

[24] W. Chen, G. Situ, X. Chen, "High-flexibility optical encryption via aperture movement". **Optics Express**, 21(21):24680-91. October 2013. DOI: 10.1364/OE.21.024680.

[25] Q. Gao, Y. Wang, T. Li, Y. Shi, "Optical encryption of unlimited-size images based on ptychographic scanning digital holography". **Applied Optics**, 53(21). July 2014. DOI: 10.1364/AO.53.004700.

[26] K. Murugeswari, B. Balamurugan, G. Ganesan, "Blockchain and Bitcoin Security". **Cryptocurrencies and Blockchain Technology Applications**. May 2020. DOI: 10.1002/9781119621201.ch8.

[27] N. Sfetcu, "Blockchain Philosophy - Bitcoin". March 2019. DOI:10.13140/RG.2.2.28007.80803.

[28] S., Mohsienuddin Mohammad, "Blockchain and Bitcoin Security in IT Automation". **SSRN Electronic Journal**, 68(3):103-110. March 2020. DOI: 10.14445/22312803/IJCTT-V68I3P121

[29] W. Diffie and M. Hellman, "New Directions in Cryptography". **IEEE Information Theory Workshop**, Lenox, MA, EUA. (1975).

[30] L. Hoffmann, W. Diffie, M. Hellman. "Finding New Directions in Cryptography". **Communications of the ACM**, 59(6):112-111. May (2016). DOI: 10.1145/2911977