Método de autentificación óptica utilizando funciones físicas inclonables

por el

Lic. Julio César Juárez Ramírez

Tesis sometida como requisito parcial para obtener el grado de

MAESTRÍA EN CIENCIAS EN LA ESPECIALIDAD DE ÓPTICA

en el

Instituto Nacional de Astrofísica, Óptica y Electrónica

Supervisada por:
Dr. Julio César Ramírez San Juan
INAOE

Junio 2016
Tonantzintla, Puebla

©INAOE 2016
El autor otorga al INAOE el permiso de reproducir y distribuir copias en su totalidad, o en partes, de esta tesis

Dedicatoria

Este trabajo esta dedicado a mis padres Navidad y Luis Rubén por su apoyo y motivación en todo momento y su guía, a mis hermanos; Miroslava, Alondra y Luis Eduardo, a mis abuelos Trinidad, Carmen y Placido, a mi familia en general.

A Bety por apoyarme siempre y estar a mi lado en las buenas y en las malas. Por el cariño y amor que me da y demuestra todos los días.

Quiero agradecer también a mi editora Nadia, a mis amigos Nayeli, Naharai, Angelo, Jorge, Isaac, a todos mis compañeros en INAOE.

Agradecimientos

A mis profesores Julio César Ramírez San Juan, Pepijn W. H. Pinkse, por guiarme en el proyecto, a todos mis compañeros en COPS, en especial Ravitej Uppu, Tristan Tentrup, Evangelos Marakis, Tom Wolterink por su apoyo, comentarios y discusiones.

Instituto Nacional de Astrofísica, Óptica y Electrónica

Coordinación de Óptica

"MÉTODO DE AUTENTIFICACIÓN ÓPTICA UTILIZANDO FUNCIONES FÍSICAS INCLONABLES"

Tesis Para Obtener el Título de:

MAESTRIA EN CIENCIAS CON ESPECIALIDAD EN ÓPTICA

PRESENTA:

Julio César Juárez Ramírez

jcgjuarezramirez@gmail.com

ASESOR:

Dr. Julio César Ramírez San Juan

jcram@inaoep.mx

Coordinación de Óptica
INAOE

Puebla Puebla - Julio 2016.

Índice general

1. Introducción **9**
1.1. Resumen 9
1.2. Autentificación 9
1.3. Auntentificación de seguridad cuántica 10
1.4. Objetivos 12
1.5. Distribución de capítulos 13

2. Conceptos básicos **15**
2.1. Desafío 15
2.1.1. Holograma de Lee 16
2.2. Esparcimiento de la luz 18
2.3. Esparcimiento múltiple 19
2.4. Matriz de esparcimiento 20
2.5. Función física inclonable (PUF) 22
2.5.1. La llave 22
2.6. Efecto memoria 23
2.7. Modelado de frente de onda 23
2.8. Modulación de amplitud binaria 24
2.9. Factor de mejora 25
2.9.1. Factor de mejora teórico 26

3. Arreglo óptico experimental **29**
3.1. Arreglo de caracterización y lectura clásica 29
3.1.1. Programas y velocidad 35

4. Análisis y discusion de resultados **37**
4.1. Estudio de estabilidad del arreglo óptico 37
4.2. Metodología 39
4.2.1. Creación de retos 39

4.2.2. Caracterización de las llaves 42
4.2.3. Lectura con luz clásica 44
4.2.4. Algoritmo de búsqueda 45
4.2.5. Prueba de estabilidad 51
4.3. Trabajo a futuro: Transición a estado cuántico 52

5. Sumario y conclusiones **55**

Referencias **57**

Capítulo 1

Introducción

Comenzaremos este capitulo con un breve resumen, motivación del trabajo y antecedentes del mismo. También se mencionan los objetivos y metas a realizar. Por último, se discute la distribución de los capítulos.

1.1. Resumen

En el presente trabajo se construyo un método de autentificación óptica. Utilizando funciones físicas inclonables, es decir, que no se pueden clonar. Para que el método funcione se requiere recolocar la llave con una precisión de micrómetros. Para esto se construyó un arreglo robusto de alta repetibilidad. Con el mismo fin se diseñó e implementa un algoritmo que busca la posición correcta de la llave. Una vez que se encuentra la mejor posición, el sistema se ajusta a sí mismo antes de leer la llave. El sistema construido es portátil, siendo de dimensiones de una caja de botas, un peso de 4,5kg. Además que se transportó en un aotomovil particular en una ocasión una distancia de 372km,[1] y en otra ocasión 278km[2] sin desalinearse. Con esto se demuestra que se puede construir un método de autentificación óptica de portátil, alta seguridad y fidelidad.

1.2. Autentificación

Cada vez que usamos un cajero automático, viajamos a otro país, revisamos que los billetes sean legítimos, encendemos el automóvil, accedemos a nuestra

[1] Distancia entre las ciudades de Enschede y Veldhoven en Los Países Bajos ida y vuelta.
[2] Distancia entre las ciudades de Enschede y Utrech en Los Países Bajos ida y vuelta

cuenta bancaria, seguro social, desbloqueamos nuestro teléfono celular; por mencionar algunos ejemplos, es necesario un proceso de autentificación. Ésta puede depender de una llave física, como en el caso de encender el coche con la llave de fabrica. Puede depender de poseer información de forma secreta, por ejemplo el patrón o número de identificación personal (NIP) que introducimos al desbloquear el teléfono celular. Puede depender de ambos, una llave física e información secreta, como al acceder a un cajero automático, es necesario introducir la tarjeta de crédito o débito y un código para permitir el acceso.

Cada método de autentificación es vulnerable a ataques y cada método puede ser superado por un atacante. Las llaves físicas pueden ser copiadas. Para burlar la autentificacion de un coche, basta ir al cerrajero y copiar la llave. Los métodos basados en poseer información secretamente, por ejemplo un banco, se rompen si el secreto (datos personales, contraseñas, etc.) es divulgado. Lo que compromete la seguridad.

En 2011, por ejemplo, se llevó acabo un gran fraude coordinado con tarjetas bancarias donde los atacantes lograron hacerse de 13 millones de dolares estadounidenses de una institución bancaria con sede en Florida [1]. Similarmente, a finales de 2012 otro ataque coordinado a nivel mundial atacó el Banco de Muscat en Medio Oriente robando 40 millones de dolares estadounidenses [2].

En 2012 una investigación por *Aite Group* reveló que en promedio el 27 % de la población ha sufrido fraude bancario. El estudio mostró que los países más afectados son Estados Unidos y México, donde más del 40 % de la población ha sufrido algún tipo de fraude bancario [3]. En Chile los fraudes con tarjetas bancarias crecieron un 94 % entre 2014 y 2015 [4].

Ejemplos de delitos como los anteriores muestran la urgencia de nuevos métodos de autentificación, debido a que los métodos de autentificación actuales pueden ser superados, lo que implica un riesgo en la seguridad de los usuarios.

1.3. Auntentificación de seguridad cuántica

Auntentificación de seguridad cuántica, QSA por sus siglas en inglés, es un método de autentificación creado en 2014 por A. Goorden y colaboradores [5]. Utiliza una llave física, pero explota la imposibilidad de copiar las

propiedades ópticas de un medio difuso, especialmente las propiedades de esparcimiento de materiales altamente esparcidores como una hoja de papel, pintura, tejido orgánico, sangre por mencionar algunos.

Además, QSA se basa en el hecho de que las propiedades de esparcimiento son únicas para cada muestra. Aún si se trata del mismo material (mismo espesor y forma macroscópica). Por lo que no es posible burlarlo copiando la llave macroscópicamente. Para copiar la llave es necesario copiarla a escalas nanométricas, partícula a partícula, con la misma posición, orientación, etc. Involucrando grados de libertad inmanejables, que lo hace virtualmente imposible de copiar [7], [8].

Sin embargo es posible emular la respuesta [9], por lo que en 2012 B. Skoric propuso la lectura cuántica en éste tipo de materiales [10]. Utilizando menos fotones que número de granos de speckle (nivel cuántico) tampoco es posible emular las propiedades ópticas del material con algún tipo de dispositivo óptico o electrónico. Debido a que aún si el atacante tiene acceso a todos los fotones enviados (toda la información disponible), la información no es suficiente para caracterizar todas las propiedades de la llave [9].

En el artículo original de QSA se utiliza una muestra de oxido de zinc (ZnO) [11] como llave. Con ayuda de un modulador espacial de luz (*SLM-desafío*) se crea un conjunto de frentes de onda diferentes a los que llamaremos *desafíos*. Los desafíos son almacenados en una base de datos. Se utiliza la técnica de *modelado de frente de onda* (WFS por sus siglas en inglés) [6] con un segundo modulador espacial de luz (*SLM-respuesta*) para invertir la respuesta combinada de la llave y cada uno de los desafíos en un punto enfocado en el plano imagen. El patrón generado para cada desafío usando WFS es almacenado en una base de datos destinada para cada llave.

En el momento de leer la llave, se selecciona un desafío de forma aleatoria del conjunto de desafíos con su correspondiente respuesta. Se le hace incidir a la llave pocas centenas de fotones. Si la llave es la correcta los fotones se enfocarán en un detector. El proceso se puede repetir con diferentes desafíos para cada llave por lectura incrementando la seguridad [5]

Este método no requiere mantener datos de forma secreta, ni en supuestos matemáticos no demostrados [5]. Además, es posible implementar este método con tecnología actual.

La intensión de este trabajo es diseñar y construir un arreglo demostrativo que sea más compacto y ligero. Además de reducir el tiempo de caracterización y lectura de las llaves. A diferencia del trabajo original de QSA [5], en este trabajo se logra la repetibilidad de lectura de llave, es decir, la capacidad de remover la llave de su posición y colocarla nuevamente sin perder la alineación del sistema. También se agrega la característica portátil del arreglo, lo cual nos permite transportarlo sin la necesidad de desmontar o volver a alinear el arreglo óptico. Finalmente, como meta a corto plazo, se desea comercializar la tecnología a instituciones con niveles de seguridad altos.

Las áreas de oportunidad para este trabajo son principalmente de seguridad, creando un método de autentificación seguro. Por lo que, puede ser utilizado en áreas de alta seguridad como departamento de seguridad nacional, bancos, hospitales, por mencionar algunos.

Pero además, los resultados de este trabajo pueden ser usados con fines biológicos, debido a que los tejidos biológicos son medios altamente esparcidores. Al enfocar un punto en reflexión o transmisión de un medio biológico se puede inferir que hay dentro del material biológico. Equivalentemente a que el medio sea transparente [6]. Nuestro trabajo permite enfocar un punto de la luz esparcida en reflexión por un medio esparcidor en 88,2s utilizando 1225 segmentos[3], velocidad limitada por la computadora que controla los moduladores espaciales de luz. Aumentando el poder de procesamiento de la computadora que controla los moduladores espaciales de luz, el tiempo que demora en enfocar depende de la velocidad de los moduladores espaciales de luz. El uso de dispositivos de micro-espejos (DMD, por sus siglas en inglés) permitiría enfocar en tejido biológico practicamente en tiempo real. Gracias al tiempo de respuesta de 44μs, por lo que el tiempo que tarda en enfocar se reduce a 0,1s.[4]

1.4. Objetivos

El objetivo de este proyecto es construir un arreglo óptico demostrativo de autentificación

- compacto
- ligero

[3] Ver sección 3.1.1

[4] Considerando una optimización de 1225 segmentos, $1225 \times 2 \times 44\mu\text{s} = 0{,}1\text{s}$

- robusto
- capaz de ser transportado fácilmente sin perder la alineación de los elementos ópticos
- lo más cerca posible a un escenario de vida real
- implementar un algoritmo de autoalineación para corregir errores en la posición de la llave
- capaz de remover y recolocar el medio esparcidor (llave) en la misma posición cada vez con una precisión de micrómetros
- reducir el tiempo de caracterización de cada llave

Proveer la prueba de funcionamiento, que permita a este sistema llevar a cabo la lectura con algunas centenas de fotones y que permita convertirlo en un arreglo demostrativo de autenticación de seguridad cuántica.

1.5. Distribución de capítulos

En el capítulo 2 se trata la teoría y conceptos básicos utilizados en este trabajo: hologramas digitales binarios, esparcimiento, efecto memoria y modelado de frente de onda.

Se muestra y discute el arreglo óptico experimental en el capítulo 3.

Dentro del capítulo 4 se presentan los resultados para diferentes experimentos realizados para probar el arreglo de autentificación.

Finalmente, en el capítulo 5 se presentan las conclusiones.

Capítulo 2

Conceptos básicos

Para realizar un método de autenticación de alta seguridad como el deseado, es necesario conocer algunos conceptos como los tratados en el siguiente capítulo. Como son los hologramas digitales binarios, el esparcimiento de la luz debido a un medio altamente esparcidor y funciones físicas inclonables (PUF). También se requiere conocer la técnica de modelado de frente de onda y su implementación empleando un modulador espacial de luz de amplitud binario.

2.1. Desafío

Al iluminar un medio altamente esparcidor al cual llamaremos *llave* con un frente de onda plano, la llave esparce la luz en forma de un patrón de speckle en reflexión y en transmisión. Debido a que la llave es una función física inclonable óptica [1], cada uno de estos patrones son únicos para cada llave, siendo como sus *huellas digitales*. Si se ilumina la llave con un frente de onda esférico, cada llave esparce de manera diferente formando nuevos patrones de reflexión y transmisión, equivalentemente a una segunda huella digital. De igual modo, si se ilumina con un frente de onda cónico, elíptico, con forma de corazón, etc. Es decir, es posible iluminar la llave con frentes de onda arbitrarios, diferentes entre sí, y cada uno forma un patrón único.

Se puede autenticar la llave con cada una de las huellas digitales o un subconjunto de éstas. Por lo que la seguridad del sistema aumenta mientras más huellas digitales tenga la llave.

[1] Ver sección 2.5

Por este motivo, estamos interesados en crear varios frente de onda que iluminen la llave (*desafío*). Para esto se debe tener control sobre la fase del frente de onda. En la sección 2.1.1 se muestra el método utilizado para conseguirlo.

2.1.1. Holograma de Lee

A diferencia de un modulador espacial de luz de cristal líquido, los DMDs no son capaces de modular la fase. Debido a que son arreglos de micro-espejos que solamente pueden ser colocados en dos posiciones. Por lo que, solamente modulan amplitud. La dificultad consiste en encontrar una función $h(x, y)$ tal que $h(x, y) \in \{0, 1\} \forall x, y \in R \subseteq \mathbb{R}$ produzca cualquier frente de onda deseado cambiando la distribución de unos y ceros. Afortunadamente, es posible crear hologramas binarios para controlar fase, por ejemplo, con hologramas de Lee [12] y hologramas de súper pixel [13]. En este trabajo de investación se utilizaron únicamente hologramas de Lee debido a su fácil implementación.

Wai-Hon Lee en 1974 propone dos métodos para crear hologramas binarios sintéticos (digitales) para reconstruir el frente de onda dado por la ecuación 2.1 [12]

$$w(x, y) = \exp\left[i\phi(x, y)\right]. \tag{2.1}$$

Una aproximación sugerida por Lee [12] es considerar la combinación de ondas $\exp\left[im\phi(x, y)\right]$ para reconstruir el frente $w(x, y)$, es decir

$$h(x, y) = \left| \sum_{m=0}^{N-1} \frac{1}{N} \exp\left[im\phi(x, y)\right] \right|^2, \tag{2.2}$$

agrupando términos se puede escribir

$$h(x, y) = \left(\frac{\operatorname{sen} N\phi(x, y)/2}{N \operatorname{sen} \phi(x, y)/2} \right)^2, \tag{2.3}$$

que para N grandes se cumple que

$$h(x, y) = \begin{cases} 1 & \phi(x, y) = 2\pi n \\ 0 & \text{otro caso} \end{cases}, \tag{2.4}$$

donde $n \in \mathbb{Z}$. La función $h(x, y)$ para N grandes cumple con los requisitos para ser un holograma binario. El holograma se construye evaluando la ecuación (2.4) para todos los puntos (x, y) en el plano holograma. Los puntos

que satisfacen (2.4) forman franjas angostas como las de un interferograma de múltiples haces.

El segundo método descrito por Lee [12] consiste en considerar un umbral $c = \cos\phi(x, y)$ que limite la función para generar el holograma. Por lo que se puede escribir la función holográfica como,

$$h(x, y) = \sum_{m=-\infty}^{\infty} \frac{\operatorname{sen}(m\pi q)}{m\pi} \exp\left[i\phi(x, y)\right], \tag{2.5}$$

donde $q \in [-1, 1]$ determina la anchura de las franjas. La función holográfica puede ser descrita como

$$h(x, y) = \begin{cases} 1 & \cos\phi(x, y) \geq \cos\pi q \\ 0 & \text{otro caso} \end{cases}. \tag{2.6}$$

Se puede reescribir la ecuación holográfica (2.6) como la desigualdad

$$-q/2 \leq \phi(x, y)/2\pi + n \leq q/2, \tag{2.7}$$

donde $n \in \mathbb{Z}$.

Los órdenes de difracción del holograma reconstruyen múltiples frentes de onda. Para evitar la superposición de los diferentes frentes de onda se puede introducir una inclinación en el frente de onda que automáticamente separara los órdenes de difracción, y de esta forma los frentes de onda reconstruidos sean separados. Tomando en cuenta la inclinación se puede escribir (2.7) como

$$-q/2 \leq \frac{x}{T} + \phi(x, y)/2\pi + n \leq q/2, \tag{2.8}$$

donde, si $\phi(x, y)$ es constante el holograma binario dado por (2.8) forma una rejilla de periodo T. La separación entre los órdenes está determinado por T.

La frecuencia espacial de un holograma generado por la ecuación (2.8) de acuerdo con Lee [12] es

$$\nu_x(x, y) = \frac{1}{T} + \frac{1}{2\pi}\frac{\partial\phi(x, y)}{\partial x}, \tag{2.9}$$

donde $1/T$ es la frecuencia portadora introducida por la inclinación del frente de onda y el segundo término es la frecuencia espacial del frente de onda

$w(x, y)$. Por lo que, el ancho de banda en dirección x del frente de onda $w(x, y)$ es

$$B_x = \frac{1}{\pi} \max_{x,y} \left| \frac{\partial \phi(x, y)}{\partial x} \right|, \tag{2.10}$$

similarmente, el ancho de banda en dirección y

$$B_y = \frac{1}{\pi} \max_{x,y} \left| \frac{\partial \phi(x, y)}{\partial y} \right|. \tag{2.11}$$

El orden -1 y $+1$ de difracción del holograma se encuentran separados del orden -2 y $+2$ respectivamente cuando

$$\frac{1}{T} \geq 1{,}5 B_x. \tag{2.12}$$

Considerando el periodo de muestreo $M \in \mathbb{Z}$. Multiplicando (2.8) por M y sustituyendo x por Tk_x/M e y por $2Tk_y$, calculando el módulo y aplicando algunas propiedades del módulo se tiene

$$\text{mód}\left[k_x + \frac{M\phi(Tk_x/M, 2Tk_y)}{2\pi} \leq \text{mód}\left[\frac{Mq}{2}\right]\right], \tag{2.13}$$

$$\text{mód}\left[k_x + \frac{M\phi(Tk_x/M, 2Tk_y)}{2\pi} \geq \text{mód}\left[M - \frac{Mq}{2}\right]\right], \tag{2.14}$$

por lo que, para crear el holograma, basta encontrar los puntos que satisfacen (2.13) ó (2.14). Para cada uno de esos puntos, se agrega un segmento de línea de largo $2T$ paralela al eje Y alrededor de ellos. Con este procedimiento, si el holograma tiene L franjas, el tiempo computacional requerido para crear el holograma es $M(L)^2/2$.

Para reconstruir el frente de onda se debe filtrar en el plano de Fourier del holograma el orden -1 ó $+1$ del patrón de difracción.

2.2. Esparcimiento de la luz

El color azul del cielo durante el día, rojizo durante el amanecer y el atardecer, el arcoíris, la aurora boreal y austral, el halo lunar y solar son fenómenos debidos al esparcimiento de la luz [14] (debido a las partículas en la atmósfera). El esparcimiento de la luz no sólo es responsable de estos fenomenos naturales, también los objetos visibles y algunos de sus colores son debido al esparcimiento de la luz sobre su superficie [14][15]. Éste trabajo se enfoca en

medios altamente esparcidores.

En general, cuando un campo electromagnético incide sobre la materia, éste excita a las partículas que lo conforman haciéndolas oscilar [16]. El campo eléctrico polariza las partículas formando dipolos. Cada dipolo oscilante radia una onda como resultado de la interacción. El conjunto de estas ondas interfieren unas con otras, siendo la posición y distribución de las partículas del medio las responsables de la respuesta macroscópica del material. Para medios transparentes, las partículas se encuentran distribuidas muy homogéneamente y las ondas radiadas por los dipolos del material interfieren de tal modo que sólo disminuye la velocidad de propagación del campo eléctrico en el medio. Éste fenómeno es conocido como refracción [17]. Para medios como leche, pintura, niebla, cristal esmerilado, tejido orgánico, etc., las partículas se encuentran distribuidas inhomogéneamente [17]. Por lo que las ondas radiadas por los dipolos dentro del material tienen fases no correlacionadas distribuidas aleatoriamente. A este tipo de medios se les llama medios *altarmente esparcidores*. Al hacer incidir un frente de onda de luz coherente sobre un medio altamente esparcidor como los mencionados previamente, se observa un patrón de moteado (speckle) como resultado de la interacción de la luz con la materia. El patrón de moteado depende de las propiedades físicas del medio esparcidor como son; geometría, estructura, índice de refracción, reflectancia, transmitancia. Así como también de la forma del frente de onda incidente, su coherencia, longitud de onda.

Los materiales esparcen la luz en diferentes medidas. El vidrio esmerilado de una lámpara, la hoja blanca de papel que usamos para leer y escribir, el pétalo de una flor, la pintura de la pared, el tejido orgánico constituyen ejemplos de materiales altamente esparcidores.

2.3. Esparcimiento múltiple

La trayectoria de la luz viajando dentro de un medio esparcidor cambia de dirección cada vez que se encuentra con una partícula. La distancia entre partículas depende del material, por lo que la distancia entre cambios de dirección también depende del material. A esta distancia se le conoce como *camino libre medio de esparcimiento* l_s [18]. Si la luz viaja en un medio de longitud L con $l_s < L$ ocurrirán múltiples esparcimientos. En caso de esparcimiento isotrópico, después de viajar una distancia l_s la dirección de la luz es aleatoria. En cambio, para esparcimiento anisotrópico la dirección de

la luz puede no ser aleatoria después de una distancia l_s. La distancia para la cual la dirección de la luz se mantiene conocida se conoce como *camino libre medio de transporte*, l_{tr}. La relación entre l_{tr} y l_s para medios anisotrópicos es [18]

$$l_{tr} = \frac{l_s}{1 - \langle \cos\theta \rangle}, \tag{2.15}$$

donde θ es el ángulo entre el haz incidente y el haz esparcido. Los paréntesis angulares representan el promedio sobre todos los ángulos θ. Para medios isotrópicos $\langle \cos\theta \rangle = 0$. Si el haz esparcido se encuentra en su totalidad en dirección recta entonces, $\langle \cos\theta \rangle = 1$ y la dirección del haz esparcida siempre es conocida [18]. En la figura 2.1 se muestra una representación esquemática de luz viajando en un medio esparcidor.

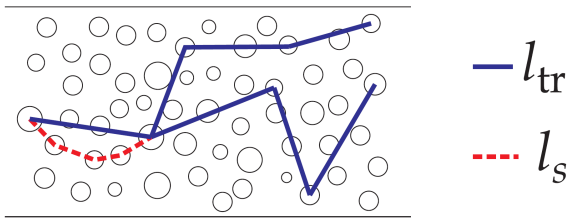

Figura 2.1: Camino libre medio de esparcimiento (l_s) y transporte (l_{tr}) para esparcimiento anisotrópico. Línea continua azul: Trayectoria de la luz esparcida debido a eventos de esparcimiento, cada evento se encuentra a la distancia l_{tr}. En este caso, se forman ángulos grandes. Línea punteada roja: Trayectoria de la luz esparcida debido a eventos de esparcimiento que se encuentran a la distancia l_s. Figura tomada de [19].

2.4. Matriz de esparcimiento

La relación entre el haz incidente y el esparcido por un medio esparcidor son bien descritos por la matriz de esparcimiento S [20]. En la figura 2.2 se muestra una representación esquemática para la matriz de esparcimiento y transmisión.

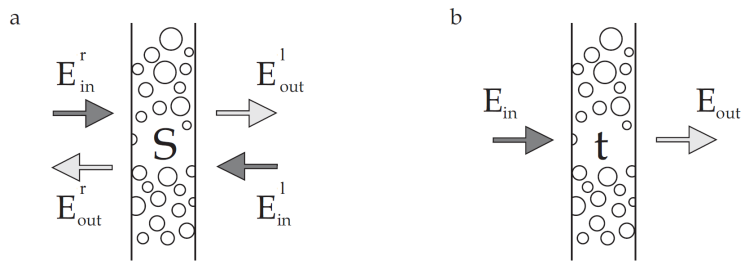

Figura 2.2: Representación esquemática de luz esparcida en un medio esparcidor en geometría de placa. a) El campo electromagnético incidente se acopla al campo electromagnético saliente debido al medio esparcidor. El acoplamiento puede ser descrito por la matriz de esparcimiento S. b) Considerando un experimento de transmisión, se hace incidir un campo únicamente por un lado, el campo detectado del otro lado es el campo transmitido. Para este caso, la matriz de transmisión caracteriza el acoplamiento. Figura tomada de [21].

Considerando un medio esparcidor con geometría de placa y etiquetando sus lados como derecho r e izquierdo l se tiene

$$\begin{pmatrix} E^l_{out} \\ E^r_{out} \end{pmatrix} = S \begin{pmatrix} E^l_{in} \\ E^r_{in} \end{pmatrix}, \tag{2.16}$$

donde E^l_{in}, E^r_{in} son los campos incidentes de izquierda y derecha respectivamente, E^l_{out}, E^r_{out} son los campos esparcidos de izquierda y derecha respectivamente. La matriz de esparcimiento S está formada por cuatro submatrices de reflexión y transmisión,

$$S = \begin{pmatrix} R^{ll} & T^{rl} \\ T^{lr} & R^{rr} \end{pmatrix}, \tag{2.17}$$

donde R^{ll}, R^{rr} representan las matrices de reflexión del lado izquierdo y derecho respectivamente. T^{rl} es la matriz de transmisión de derecha a izquierda y T^{lr} de izquierda a derecha. Por conservación de energía, la matriz S debe ser unitaria por lo que, T^{rl} y T^{lr} son transpuestos conjugados, es decir, $T^{lr} = T^{rl\dagger} = T$, por lo que, se puede escribir (2.17) como

$$S = \begin{pmatrix} R^{ll} & T^{\dagger} \\ T & R^{rr} \end{pmatrix}. \tag{2.18}$$

Las matrices R^{ll}, R^{rr}, T consisten de $N \times N$ números complejos. El campo incidente se escribe entonces como un vector de N coeficientes, es decir

$$E^r_{in} \equiv \left(E^r_{in,1}, E^r_{in,2}, ..., E^r_{in,N}\right), \tag{2.19}$$

$$E^l_{in} \equiv \left(E^l_{in,1}, E^l_{in,2}, ..., E^l_{in,N}\right). \tag{2.20}$$

La dimensión N de la matriz está limitado por el número de modos de luz acoplados a la muestra. Este número está dado por el número de puntos no superpuestos dentro del área de iluminación A, el tamaño de los puntos está dado por el límite de difracción. El número de modos se puede calcular [22] con la equación (2.21)

$$N \approx 2\pi A/\lambda^2. \tag{2.21}$$

2.5. Función física inclonable (PUF)

Una función física inclonable (PUF) son objetos físicos que no pueden ser copiados debido a que tienen un número de grados de libertad inmanejables [8]. Además de que poseen una respuesta diferente a estímulos que se pueden agrupar en un conjunto, como dominio de la función. Un medio altamente esparcidor es una función física inclonable (PUF). De ahora en adelante nos referiremos como *llave* a el medio altamente esparcidor utilizado.

2.5.1. La llave

Debido a que el patrón de speckle que genera cada muestra de un medio altamente esparcidor es diferente para cada frente de onda distinto con el cual es iluminado. Se puede considerar cada muestra como una función que transforma un frente de onda en un patrón de speckle.

Sí bien teóricamente la muestra de un medio altamente esparcidor no es imposible de copiar, reproducir las propiedades ópticas de la muestra, en particular las propiedades de esparcimiento es imposible de copiar debido al gran número de grados de libertad imposibles de manejar [7]. Para hacer una copia adecuada de la muestra se debe controlar la distribución, posición, orientación, etc. de cada partícula en la muestra.

Para alcanzar el propósito de este tema de investación, se requiere de un material que mantenga sus propiedades esparcidoras constantes a través del tiempo y un método para iluminar la llave siempre en la misma posición

y orientación. Debido a que en sistemas esparcidores la luz transmitida es sumamente sensible a cambios en la muestra [21]. En la sección 3.1 se discute más sobre el material de la llave. En la sección 4.2.4 y la sección 3.1 sobre cómo mantener la posición de la llave.

2.6. Efecto memoria

Feng, Kane, Lee y Stone (FKLS) en 1988 [23] reportaron su estudio sobre propiedades de correlación de ondas transmitidas a través de medios desordenados. En particular, una de las propiedades producto de la correlación de región pequeña es el llamado *efecto memoria*.

Posteriormente Freund, Rosenbluh y Feng demostraron experimentalmente la existencia del efecto memoria [24] en concordancia con los resultados presentados por FKLS [23].

El efecto memoria predice que al hacer incidir una onda con una pequeña inclinación θ a través de un medio esparcidor, el patrón de speckle en promedio, solamente se desplazará en el mismo ángulo θ [23].

La correlación que produce el efecto memoria decae de forma exponencial [23, 24]. Para un ángulo del orden de $\theta \approx \frac{\lambda}{2\pi L}$ la correlación es menor por un factor igual al número $e = 2{,}718$ [25], donde L es el espesor del medio esparcidor y λ la longitud de onda que ilumina el medio.

Una descripción matemática detallada sobre la correlación que produce el efecto memoria se encuentra en [23], así como la discusión sobre propagación de ondas en medios aleatorios de Rossum y Nieuwenhuizen [18], y el libro de Akkermans y Montambaux [26].

2.7. Modelado de frente de onda

Lo que al principio parece imposible, enfocar un frente de onda en un punto a través de un medio esparcidor se logró por primera vez en 2007 en el grupo *Complex photonics system* (COPS) en Los Países Bajos por I. M. Vellekoop y A. P. Mosk con la técnica conocida como *modelado de frente de onda* o *wavefront shaping* (WFS) [6].

Cuando se hace incidir un frente de onda plano a una lente, ésta enfoca la luz en un punto. En cambio, cuando se hace incidir un frente de onda plano en un medio esparcidor es esparcido formando un patrón de speckle en reflexión y en transmisión. Debido a que el medio esparcidor es diferente a una lente, es de esperarse que al hacer incidir el mismo frente de onda (onda plana) produzcan diferentes respuestas (punto enfocado y patrón de seckle respectivamente).

El patrón de speckle que a primera vista luce como un patrón caótico, resulta ser un fenómeno determinístico: es formado por la superposición de ondas producidas por el medio esparcidor al ser excitado por el frente de onda. Por lo que, se puede modelar y hacer incidir un frente de onda tal que el haz esparcido, ya sea en reflexión o transmisión, se enfoque en un punto. En la figura 2.3 se muestra una representación esquemática de WFS.

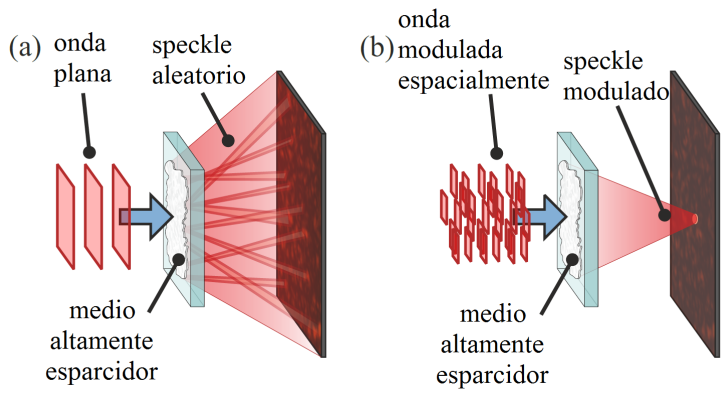

Figura 2.3: a) Un frente de onda plano incidente en un medio esparcidor por lo que un patrón de speckle es transmitido. b) El frente de onda incidente es modelado de tal modo que el haz se enfoca en un punto predefinido. Figura tomada de [6].

2.8. Modulación de amplitud binaria

Para invertir la respuesta conjunta del frente de onda desafío y de la llave, es posible reducir el tamaño y número de elementos del arreglo si en lugar de usar la técnica de *wavefront shapping*[6] se usa *Modulación de amplitud binaria* (BAM, por sus siglas en inglés) [19].

La técnica BAM consiste en bloquear selectivamente secciones del frente de onda que interfieren destructivamente en la región que se quiere optimizar. Es decir se bloquean las secciones de frente de onda tales que tengan una diferencia de fase $\Delta\phi > \pi$.

El principio de la técnica BAM es similar a la de WFS, salvo que en lugar de modelar la fase se modela la amplitud y únicamente de forma binaria.

Utilizando la matriz de reflexión R (o transmisión T), se puede describir el campo incidente y saliente. Los canales de esparcimiento son los modos espaciales o angulares de propagación del campo [20]. Los canales del campo incidente y saliente se relacionan con la matriz de reflexión [27].

$$E_m = \sum_{n=1}^{N} r_{mn} E_n, \tag{2.22}$$

donde E_m es campo eléctrico en el canal saliente $m - ésimo$, E_n el campo eléctrico en el canal incidente $n - ésimo$, r_{mn} los elementos de la matriz de reflexión. Haciendo uso de un modulador espacial de luz, se puede dividir el campo eléctrico que ilumina el medio esparcidor en un arreglo de segmentos cuadrados. Cada segmento corresponde a un rango específico de ángulos incidentes al medio esparcidor. Con cada segmento es posible de controlar un número de canales del campo incidente, lo que implica un control sobre los canales salientes. Mientras mayor sea el número de sementos en el SLM, mayor resolución se tiene, aumentando así el control de canales independientes.

Se puede implementar la técnica BAM utilizando un modulador de amplitud binario como un dispositivo de micro-espejos. Se crea un arreglo de segmentos de $n \times n$. Los segmentos cuya reflexión interfieren destructivamente en el área objetivo se colocan en posición-apagado. Similarmente, los segmentos que interfieren de forma constructiva se colocan en posición-encendido. El algoritmo para calcular el patrón BAM se muestra en algoritmo 1.

2.9. Factor de mejora

Una forma de cuantificar el contraste entre el grano de speckle optimizado y la intensidad de fondo es con el *factor de mejora* η. El factor de mejora η se define como:

$$\eta = \frac{I_{opt}}{\langle I_{ref} \rangle}, \tag{2.23}$$

Algoritmo 1 Cálculo de patrón BAM

Entrada: Región a optimizar R.
Salida: Patrón BAM que optimiza en la región deseada.

```
temp ← Arreglo de n × n segmentos vacíos
para cada segmento l del arreglo temp hacer
    Intensidades ← {0, 0}
    para cada posición pos del conjunto {apagado, encendido} hacer
        posición de segmento l ← pos
        Imagentemp ← obtener imagen
        Imagentemp ← extraer región R de Imagentemp
        Intensidades(pos) ← sumar todos los elementos de Imagentemp
    fin para
    si Intensidades(encendido) > Intensidades(apagado) entonces
        temp(l) ← encendido
    si no
        temp(l) ← apagado
    fin si
fin para
devolver temp
```

donde I_{opt} es la intensidad en la región de interés y $\langle I_{ref} \rangle$ es la intensidad promedio sin optimizar.

2.9.1. Factor de mejora teórico

La relación entre el número de segmentos N utilizados en el SLM y el factor de mejora máximo, η_{max}, que se puede alcanzar está dado por [19]

$$\langle \eta_{max} \rangle \approx 1 + \frac{1}{\pi}\left(\frac{N}{2} - 1\right). \tag{2.24}$$

En la figura 2.4 se grafica el factor de mejora teórico máximo (línea azul) y experimental (puntos rosas y morados) contra el número de segmentos utilizados en la optimización. El factor de mejora experimental se calculó utilizando la ecuación (2.24)

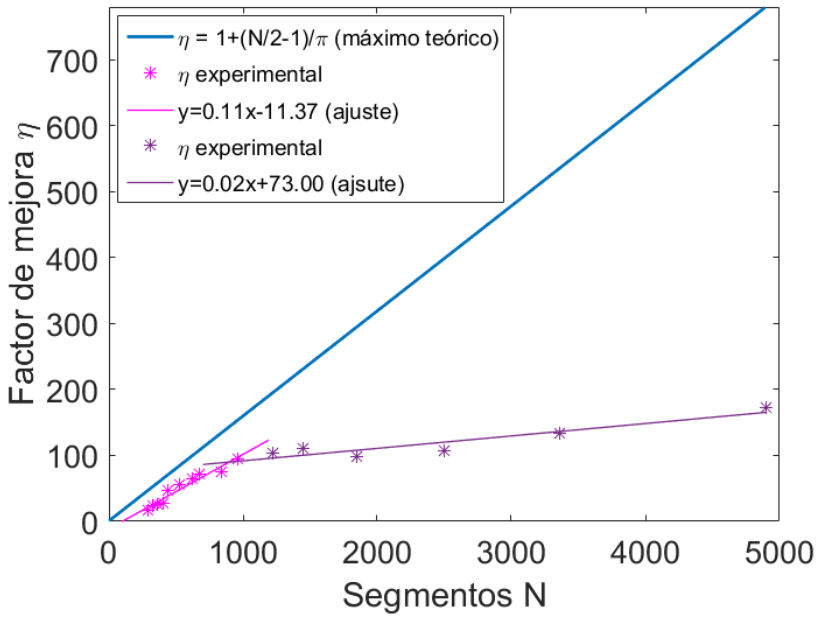

Figura 2.4: Gráfica de factor de mejora η teórico máximo y experimental. Representado en una línea azul el valor teórico. Los valores experimentales se grafican en dos colores, rosa ($N \leq 961$) y morado ($N > 961$). Se muestra un ajuste para cada conjunto de valores experimentales.

Los datos experimentales se encuentran por debajo del nivel teórico máximo (línea azul) debido a las limitantes experimentales, como son sensibilidad de la cámara, estabilidad del láser y el resto del arreglo, iluminación no deseada, etc. De la figura 2.4 se puede observa que el factor de mejor experimental muestra un efecto de saturación. Experimentalmente se determina que la saturación se da a partir de 1000 segmentos aproximadamente. Los valores experimentales son el promedio para 50 imágenes capturadas para el mismo patrón.

Capítulo 3

Arreglo óptico experimental

En el presente capítulo se discute sobre el arreglo óptico experimental utilizado, así como, los programas que controlan los dispositivos.

3.1. Arreglo de caracterización y lectura clásica

El arreglo óptico construido se muestra en la figura 3.1. Se utiliza un láser OBIS con longitud de onda de 641nm y 100mw de potencia. Un aislador óptico *ThorLabs* IOT-3D-633-VLP es colocado a la salida del láser para prevenir retroalimentación a la cavidad del láser. El haz es atenuado con un filtro de densidad media (no mostrado en figura 3.1) que reduce la potencia a 16mW. El haz láser es acoplado con un colimador (*ThorLabs* F810FC-635nm) en una fibra óptica monomodo, con una eficiencia de acoplamiento de 50 %. La salida de la fibra es colimada usando un colimador de fibra óptica de diámetro (d = 6mm) e incide en el DMD-Desafío (DMD-C). Los DMDs utilizados son dispositivos V-7000 *High-Speed* de *Texas Intruments*. Estos DMDs son capaces de desplegar 22727 cuadros por segundo, la distancia entre pixeles es de 13,7μm [28]. Los micro-espejos son capaces de estar en dos posiciones $\pm 12°$ [29]. Un retardador de media onda es utilizado para controlar el estado de polarización incidente sobre el DMD-C. En el DMD-C es desplegado el patrón-desafío. Usando hologramas de Lee (ver sección 2.1.1) en el DMD-C se controla la fase del frente de onda. Un patrón-desafío consiste en un arreglo de 20×20 segmentos. Cada segmento está formado por 20×20 micro-espejos y cada segmento es seleccionado para desplegar una fase escogida aleatoriamente del conjunto $\{0, 2\pi/3, 4\pi/3\}$ utilizando hologramas digitales. Lo que significa que el número de desafíos únicos es $3^{20\times 20} = 7 \times 10^{190}$. En la figura 3.2, se muestra un desafío típico. El patrón-

desafío ocupa solamente una porción (400×400)de la pantalla entera del DMD-C (1024×768).

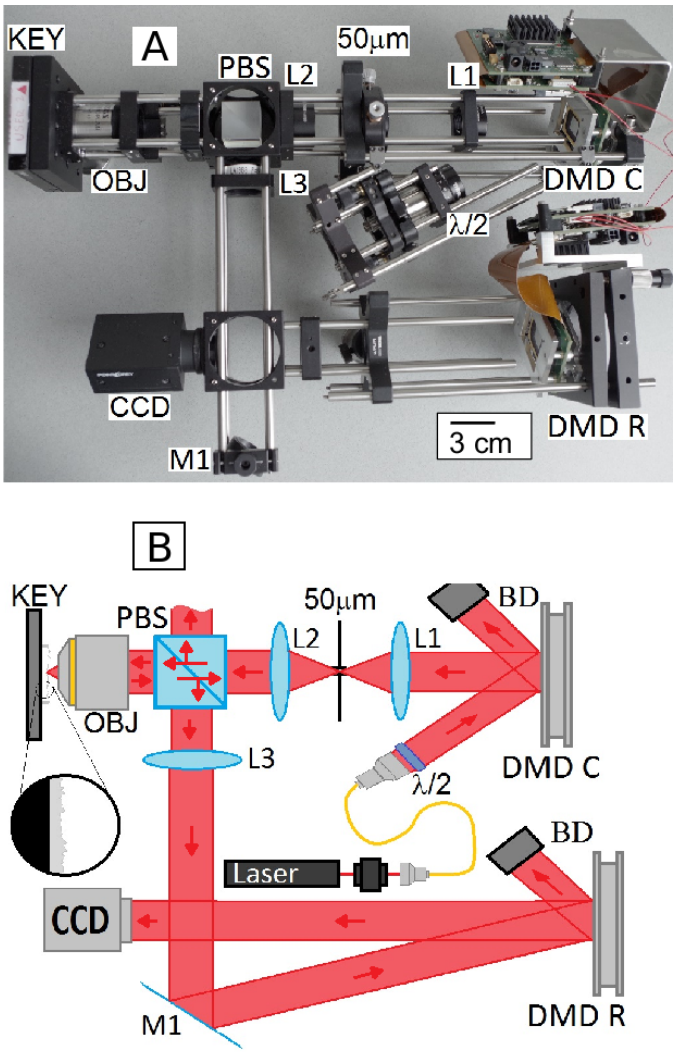

Figura 3.1: A) Fotografía del arreglo demostrativo de autenticación sin láser. B) Representación esquematica del arreglo demostrativo de autenticación.

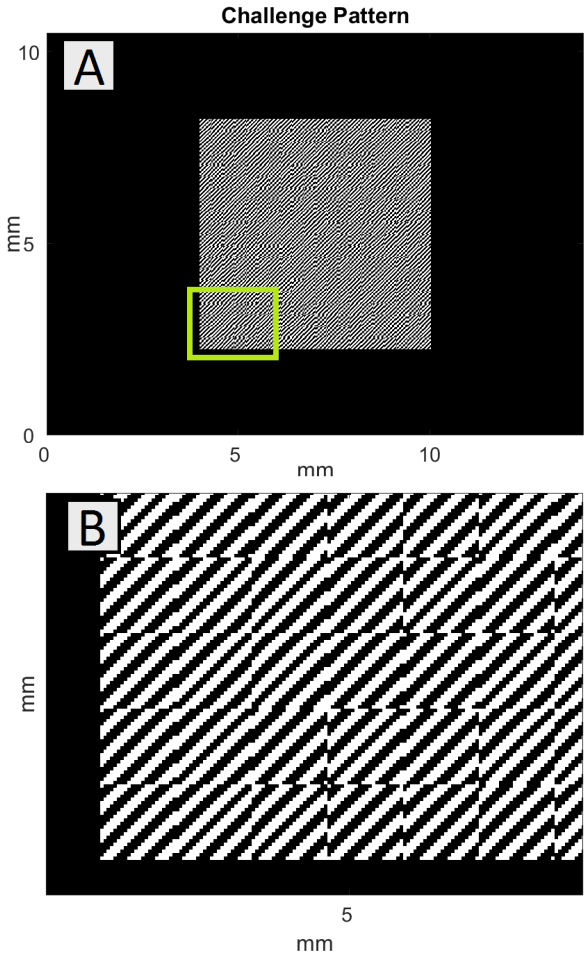

Figura 3.2: A) Desafío típico de 20×20 segmentos; hologramas de Lee con fase escogida aleatoriamente del conjunto $\{0, 2\pi/3, 4\pi/3\}$. Color negro representa micro-espejos en *posición-apagado*. Color blanco representa micro-espejos en *posición-encendido*. B) Acercamiento a la esquina inferior izquierda del patrón desafío.

Una lente plano convexa (L1) con distancia focal $f = 75$mm es usada para crear la imagen en el plano de Fourier de la luz reflejada por los micro-espejos del DMD-C en la posición-encendido. Un pinhole de 50μm en el plano de Fourier filtra el primer orden del patrón de difracción del holograma de Lee. La figura 3.3 muestra el patrón de difracción en el plano de Fourier.

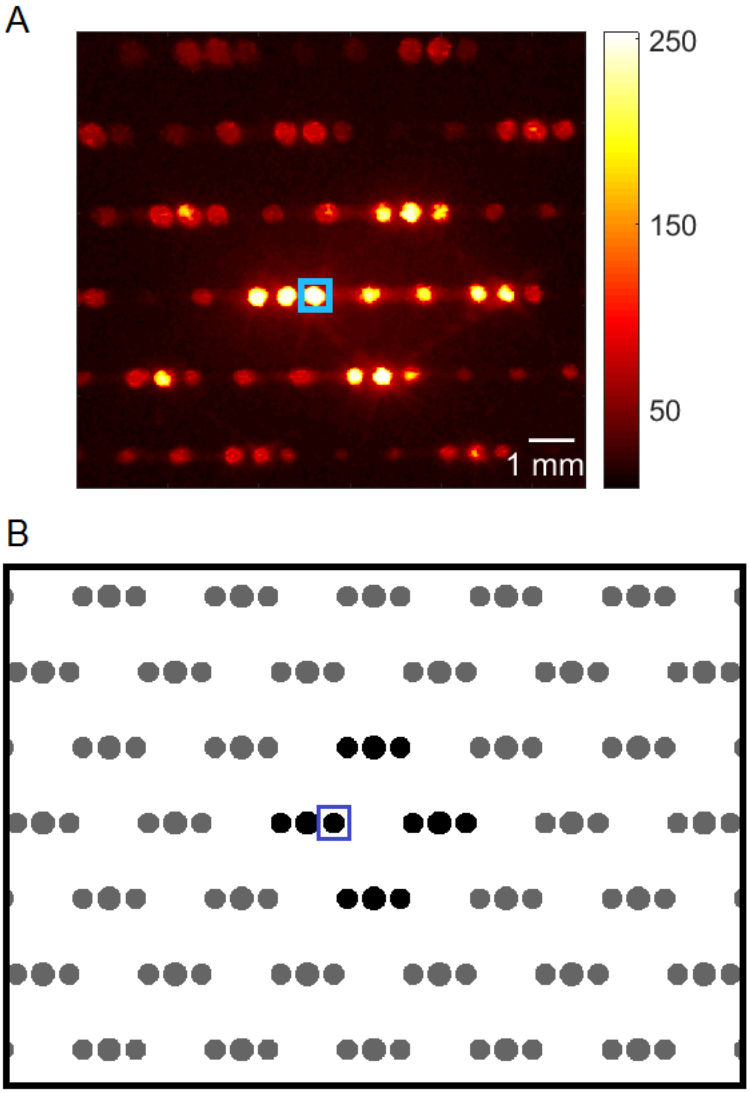

Figura 3.3: A) Fotografía del patrón de difracción del patrón-desafío en el plano de Fourier. La tripleta de puntos corresponde al patrón de difracción del holograma de Lee. Las réplicas de este patrón es debido al arreglo periódico de micro-espejos. El primer orden del holograma de Lee es marcado por un cuadro azul claro. B) Representación esquemática del patrón de difracción del holograma de Lee. El primer orden es marcado por el cuadro azul.

Una lente de 50mm de distancia focal (L2) es colocada a 50mm de distancia del pinhole. La luz pasa por un divisor de haz polarizado y luego a través de un objetivo Zeiss N Achroplan 63x/0,95, el cual, ilumina una placa de oxido de aluminio Al_2O_3 (la cual actúa como llave) de 1mm de espesor. Las llaves son sujetas a una base cinemática magnética (sujetador de llave) con una repetibilidad lateral de 30μm. Sin embargo los imanes originales fueron remplazados por otros más débiles, debido a que los imanes originales eran tan fuertes que el sujetador de llave golpeaba el arreglo cada vez que era colocado. Con los nuevos imanes, la repetibilidad lateral se redujo, teniendo una precisión promedio de 50,4μm y una desviación estándar de $\sigma = 14{,}7\mu$m. En la figura 3.4 se muestran las dos placas de oxido de aluminio colocadas sobre a los sujetadores de llave.

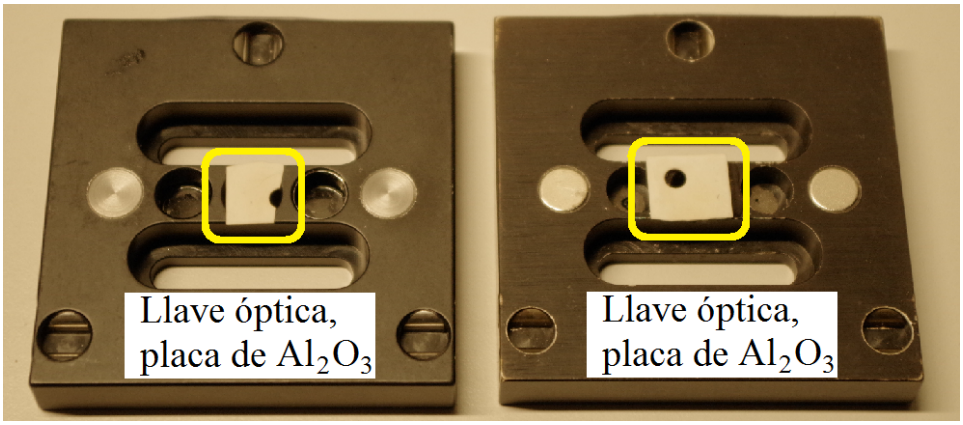

Figura 3.4: Dos llaves. Placas de oxido de aluminio (Al_2O_3) de 1mm de espesor sujetas a bases cinemáticas magnéticas. Los orificios en las placas son circunstanciales, ya que son fragmentos son fragmentos de placas más grandes con orificios en sus esquinas. Sin embargo, la luz no es enfocadas en estas regiones. Por lo tanto, estos orificios no afectan en absoluto el experimento.

La luz esparcida en reflexión es recolectada por el objetivo de 0,95 NA hacia el divisor de haz polarizado, el cual refleja hacia una lente de distancia focal de 100mm (L3). La lente L3 se colocó a 35mm del divisor de haz polarizado, formando la imagen de la superficie de la llave en el plano de DMD respuesta (DMD-R), el cual despliega el patrón-respuesta. Utilizando modulación de amplitud binaria (BAM) (ver sección 2.8) se enfoca la luz en un único grano de speckle en el plano de la cámara (*Point Grey grasshopper*

3-USB3-gs3-U3-41c6m). El patrón-respuesta es un arreglo de segmentos blancos y negros (micro-espejos en posición encendido y apagado). Se escoge la posición de cada segmento (encendido o apagado) dependiendo de cual de ellas tiene una contribución mayor a la intensidad del grano de speckle que se quiere incrementar. En la figura 3.5 se muestra un patrón-respuesta típico para un DMD de 1024×768 micro-espejos.

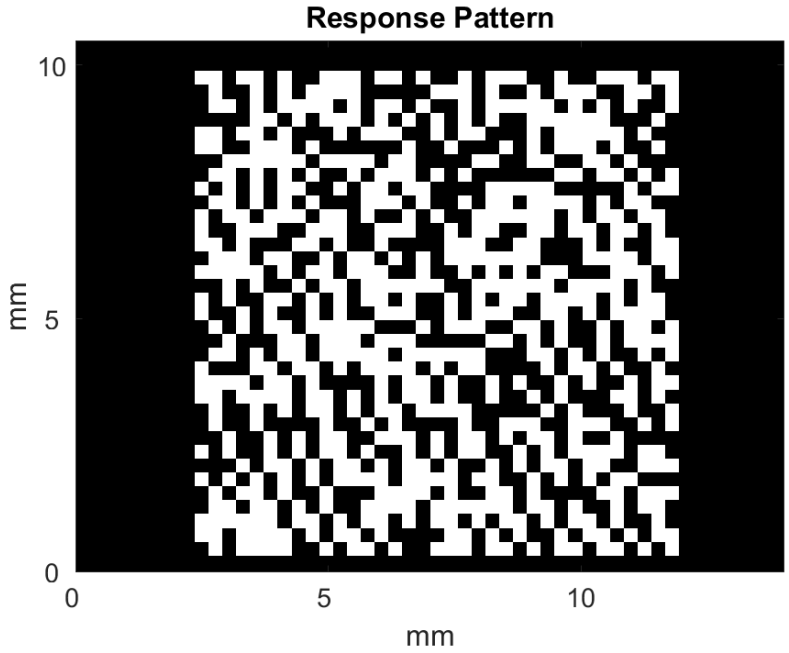

Figura 3.5: Patrón-respuesta típico de 35×35 segmentos. Color negro representa micro-espejos en la posición apagado. Color blanco representa micro-espejos en la posición encendido. El área total de la pantalla del DMD es representada.

La luz reflejada por los micro-espejos en la posición encendido va directamente a la cámara. El espejo (M1) entre L3 y DMD-R de la figura 3.1 es colocado para doblar el camino óptico reduciendo así el tamaño del arreglo óptico.

Para controlar los dispositivos se utilizó una computadora portátil *HP EliteBook* 840. Se diseñaron e implementaron dos programas principales escritos en *LabVIEW*. Uno de ellos para caracterizar las llaves. El otro para leer las llaves.

Para la estabilidad del sistema, el arreglo entero (excepto por el láser y el colimador) se encuentra dentro del sistema de jaula (*cage system*). El sistema de jaula permite conservar la alineación de los elementos, además de que elimina la necesidad de una mesa óptica. El tamaño del arreglo es de $40 \times 30 \times 22$cm (largo, ancho, alto) y un peso de 4,5kg.

3.1.1. Programas y velocidad

Los DMDs utilizados son capaces de procesar un cuadro cada 44μs. Sin embargo, la cámara puede procesar únicamente un cuadro cada 11ms. La computadora portátil (con el programa actual de caracterización) puede procesar un cuadro cada 36ms. Para el programa de lectura, la computadora puede procesar un cuadro cada 27ms. Con esta configuración, es la computadora portátil quien establece l limite de la velocidad del sistema. Por ejemplo, para una optimización de 1225 segmentos, demora $1225 \times 2 \times 0{,}035\text{s} = 88{,}2\text{s}$.

Los pares desafío-respuesta se guardan en archivos formato *png*. El espacio que requiere actualmente en disco duro es alrededor de 32kB por par desafío-respuesta, esto sin realizar ningún esfuerzo para reducir el tamaño de los archivos.

Capítulo 4

Análisis y discusion de resultados

Una vez que se tiene el arreglo óptico experimental y los programas descritos en el capítulo 3 se realizaron diferentes experimentos probando la estabilidad, repetibilidad, entre otros. En el siguiente capítulo se muestran resultados de estabilidad. También, se discute sobre la elaboración de desafíos, caracterización y lectura de la llave. Finalmente, se discute sobre el futuro del proyecto, los ajustes necesarios que se requieren para llevar el arreglo de autenticación implementado a un arreglo de autenticación cuántica (QSA) [5].

4.1. Estudio de estabilidad del arreglo óptico

Debido a que el patrón de speckle es muy sensible a la longitud de onda para obtener un grado de mejora elevado, es necesario usar un láser estable en frecuencia, sin desplazamientos y con un ancho frecuencial angosto. Además debido a que en la optimización BAM se busca la combinación de segmentos encendidos y apagados que maximice la intensidad en el área de interés. Las fluctuaciones en la intensidad del láser no son deseables. Por lo que un estudio sobre la estabilidad del láser se efectuó a diferentes potencias entre $1mW$ (potencia mínima) y 100mW (máxima potencia) analizando su espectro con un analizador de espectro. En la figura 4.1 se muestra el espectro del láser medido con el analizador de espectro.

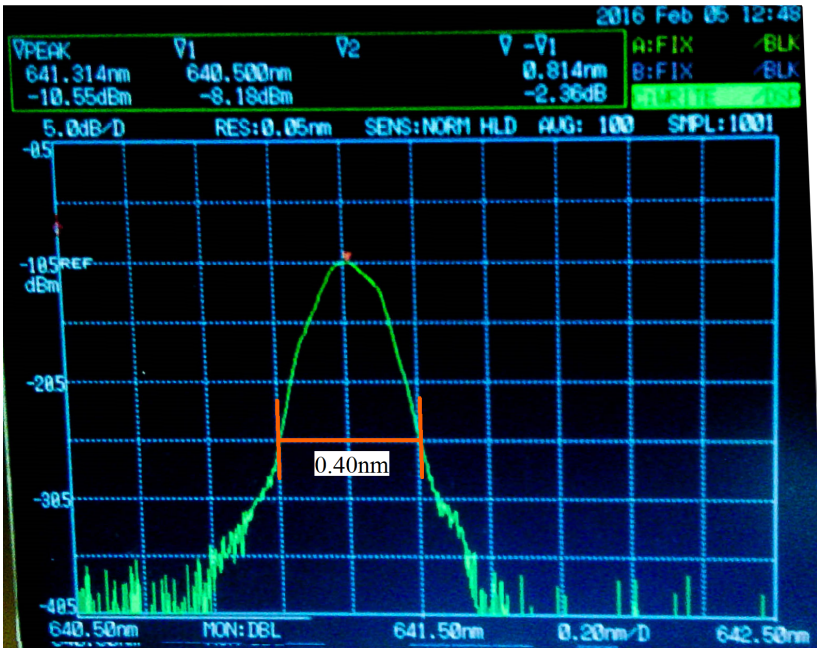

Figura 4.1: Espectro del láser a máxima potencia (100mW). Centrado en 641,3nm. La división en el eje Y es cada 5dBm, y en el eje X cada 0,2nm

Se puede observar de la figura 4.1 que la línea principal de emisión del láser tiene un ancho máximo a media altura de 0,4nm, centrado a 641,3nm. El estudio reveló que el láser se mantenía estable a máxima potencia (100mw) con un corrimiento de frecuencia menor a 8pm.

Para estudiar la estabilidad en intensidad se realizó una optimización BAM enfocando un punto en la cámara. Se capturó una fotografía cada 2 segundos durante 2 horas. En la figura 4.2 se muestra la intensidad en niveles de gris sumada en una región de 7×7 pixeles con el punto enfocado en el centro y el histograma de los datos. La intensidad promedio durante las dos horas es $I_{prom} = 3447{,}5$, con una desviación estándar de $\sigma = 200{,}6$ que es suficientemente estable para el propósito de este trabajo.

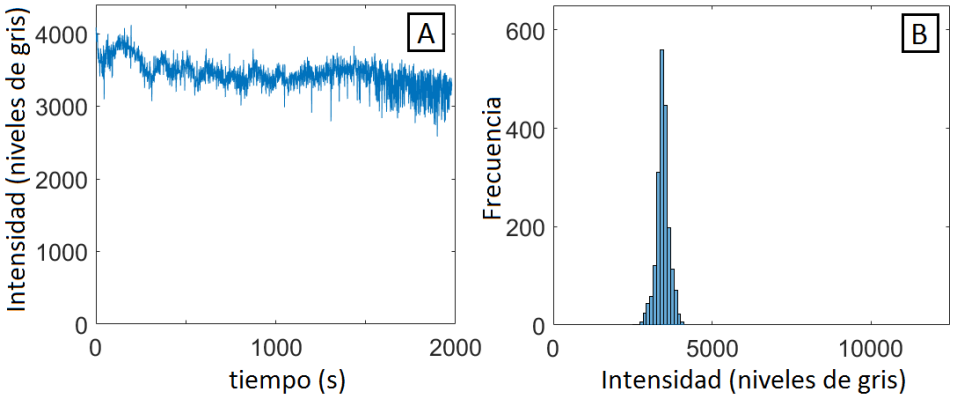

Figura 4.2: A) Intensidad en niveles de gris sumada en una región de 7×7 pixeles conteniendo en el centro al punto focal. El valor máximo que puede ser alcanzado en una regíon de 7×7 pixeles es $7 \times 7 \times 255 = 12495$. B) Histograma de la intensidad sumando el valor de cada pixel en una región de 7x7.

4.2. Metodología

Antes de distribuir las llaves a los usuarios es necesario tener una base de datos para las llaves. Caracterizar las llaves es entonces el primer punto en la agenda. Para esto se genera un conjunto de desafíos a invertir de la siguiente forma.

4.2.1. Creación de retos

Para crear una nueva base de datos de caracterización de llaves. La seguridad del sistema aumenta conforme se incrementa el número de pares desafío-respuesta por llave.

La caracterización de las llaves comienza con la creación de la base de datos de desafíos. Se fijan parámetros como el número de segmentos $N_{desafío}$ y tamaño de los segmentos S, así como el número de desafíos (n) que se desea crear. Para cada reto, se crea un arreglo de $N_{desafío}$ segmentos vacíos. En cada segmento, aleatoriamente se escoge una fase del conjunto $\{0, 2\pi/3, 4\pi/3\}$ y se fija en el segmento. Lo que implica que la cardinalidad del conjunto de desafíos es igual a la cardinalidad del conjunto fase elevado al número de segmentos $N_{desafío}$. Para los experimentos presentados se

utilizó $N_{desafío} = 20 \times 20 = 400$, por lo que, la cardinalidad del conjunto de desafíos es $3^{20\times20} = 7 \times 10^{190}$. La cardinalidad del conjunto de desafíos es el número máximo de desafíos que se pueden crear sin repetir alguno.

Retos no correlacionados

Se utilizó un método óptico para confirmar que los retos no están correlacionados entre sí, calculando la correlación del patrón de speckle de la llave en reflexión.

Con este método es posible crear 2000 desafíos. En la figura 4.3 se muestra el histograma del factor de correlación cruzada entre el primer desafío y el resto.

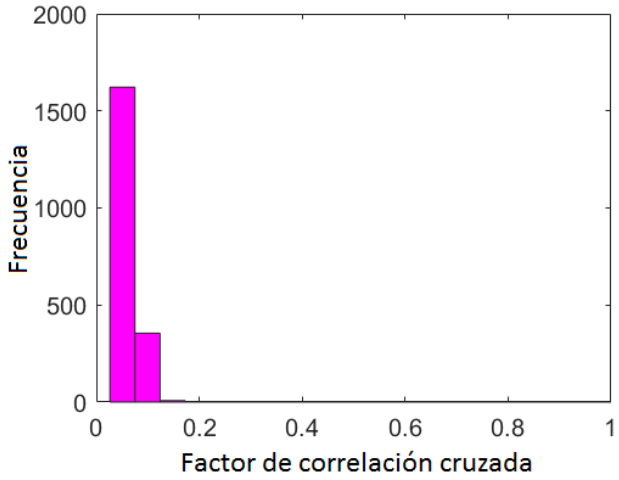

Figura 4.3: Histograma del factor de correlación cruzada entre la respuesta (patrón de speckle) de un desafío y la respuesta de los otros 1999 desafíos.

La figura muestra un factor de correlación cruzada promedio de 0,062 con una desviación estandar de $\sigma = 0{,}027$. Lo que muestra que el primer desafío es diferente a los otros 1999 desafíos.

En la figura 4.4 se muestran todos los factores de correlación cruzada en un arreglo de 40×40 segmentos. Donde el mapa de color representa la correlación cruzada entre los primeros 40 patrones de speckle generados por los primeros 40 desafíos. El segmento con coordenadas (l, k) representa el

factor de correlación cruzada entre la imagen l y la imagen k. Debido a que el factor de correlación cruzada de (l, k) es idénticamente igual al factor de correlación cruzada de (k, l). Para ahorrar tiempo de cómputo, los segmentos debajo de la diagonal no fueron calculados ya que son idénticamente igual a los segmentos sobre la diagonal. Además como el factor de correlación cruzada de (l, l) es igual a 1, los segmentos de la diagonal tampoco fueron calculados ya que no aportan información. Estos segmentos muestran un valor de cero por esta razón.

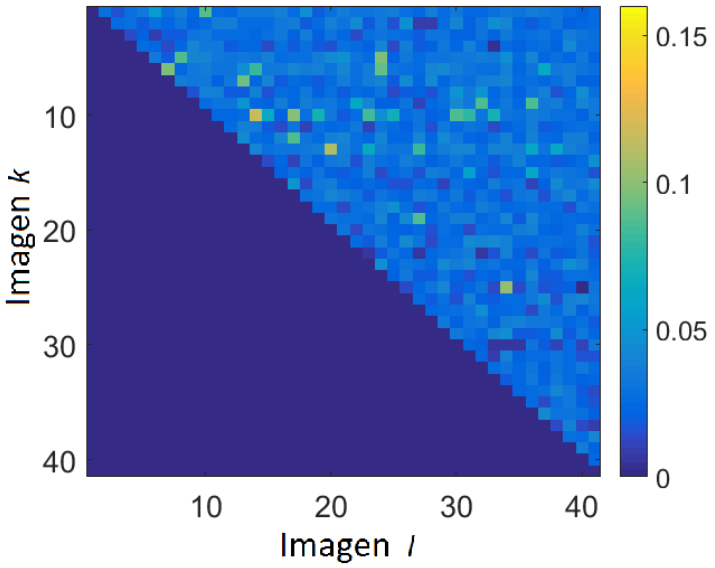

Figura 4.4: El mapa de color del segmento con coordenadas (l, k) representa el coeficiente de correlación cruzada entre las imágenes l y k. Cada imagen se tomó de un patrón de speckle resultado del desafío $l-ésimo$. El tiempo entre la captura de la foto l y $l+1$ es de 0,255 segundos. Los segmentos sobre la diagonal y debajo de ésta, no se calcularon por que no aportan información relevante o diferente a los segmentos que se encuentrán por encima de la diagonal.

En la figura 4.5 se muestra el histograma de correlación cruzada de los valores de la figura 4.4 considerando solamente los segmentos sobre la diagonal.

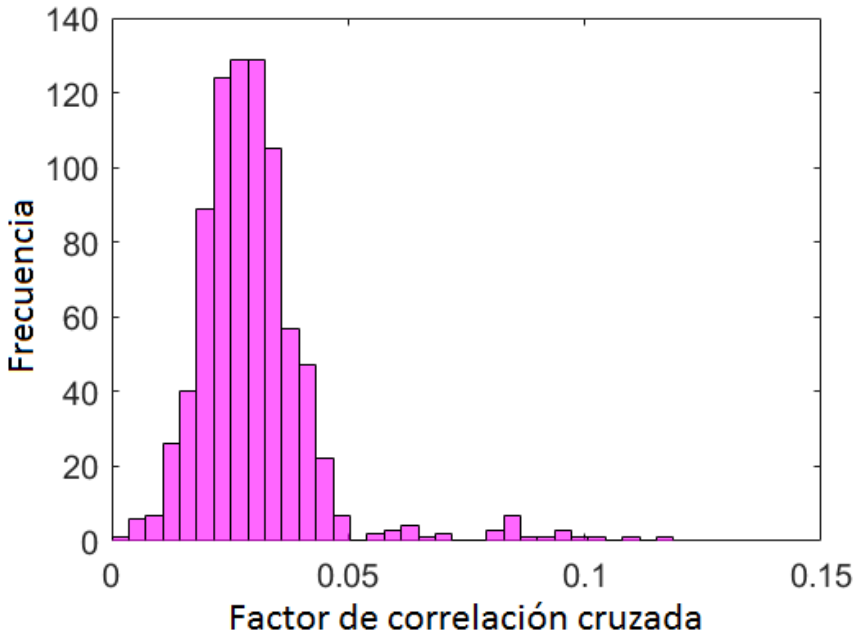

Figura 4.5: Histograma del factor de correlación cruzada de los valores de la figura 4.4, considerando solamente los segmentos sobre la diagonal.

El factor de correlación cruzada considerando solamente los segmentos sobre la diagonal es 0,03 con una desviación estandar de $\sigma = 0{,}013$. De la figura 4.3, 4.4 y 4.5 se concluyó que los desafíos creados por este método no están correlacionados entre sí.

4.2.2. Caracterización de las llaves

A cada llave se le hace incidir cada uno de los frente de onda generados por el DMD-C al desplegar un desafío. El haz de luz incide en la misma región para cada desafío. Cada desafío genera así diferentes respuestas en forma de patrón de speckle. El DMD-R invierte cada uno de los patrones de speckle generando un punto brillante en el plano de observación utilizando la técnica BAM. La caracterización de la llave finaliza al almacenar los patrones generados de la optimización en una base de datos. Éste proceso se repite para cada llave nueva.

En la figura 4.6 de la izquierda se muestra la sección central del patrón de

speckle que produce un desafío antes de ser optimizado. En la figura 4.6 de la derecha, se muestra la misma sección después de ser optimizado usando la técnica BAM. Similarmente en la figura 4.7 se muestran cortes transversales de la figura 4.6 en el pixel central del eje Y.

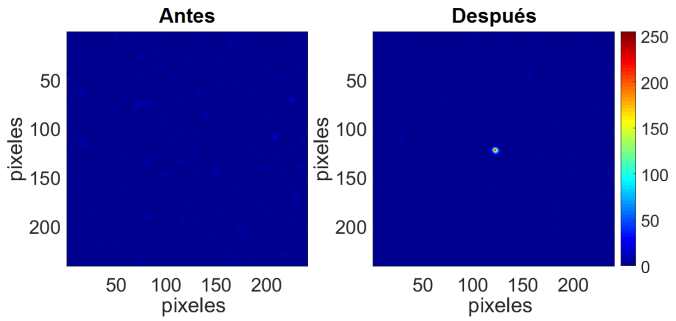

Figura 4.6: En la imagen izquierda se muestra la parte central del patrón de speckle que genera un desafío. En la imagen derecha se muestra la parte central del patrón de speckle después de la óptimización BAM. El tiempo de exposición para ambas fotos es 800μs.

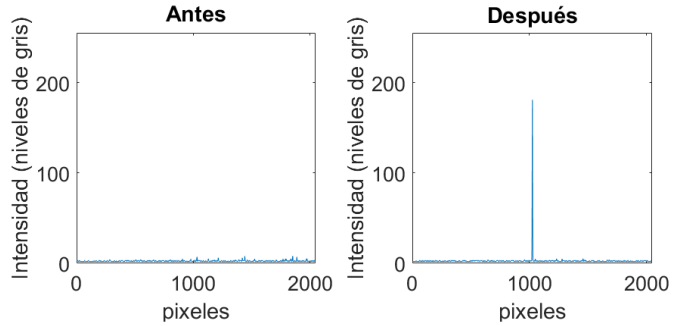

Figura 4.7: Perfil de las imagenes 4.6. En la gráfica izquierda se muestra el renglón central de la imagen del patrón de speckle que genera un desafío. En la gráfica derecha se muestra el renglón central del patrón de speckle después de la óptimización BAM. El tiempo de exposición para ambas fotos es 800μs.

Tanto en las figuras 4.6 como 4.7 se muestra que la intensidad del grano de speckle que se mejoró es considerablemente superior a la intensidad del resto de los granos de speckle. El factor de mejora promedio es de $\eta = 130$. El

factor de mejora más alto alcanzado en ésta implementación fue de $\eta = 268$. Esta mejora representa un récord de mejora para la técnica BAM en el grupo de *Complex Photonic Systems* (COPS) cuyo factor de mejora más alto era de $\eta = 19$ [19].

4.2.3. Lectura con luz clásica

El método de autentificanción consiste en tomar 50 pares de patrones *desafío-respuesta* de forma aleatoria de la base de datos para la llave actual. La selección aleatoria permite que sea posible repetir el mismo par *desafío-respuesta* mas de una vez. La secuencia de pares *desafío-respuesta* son desplegados en el DMD-C y DMD-R, respectivamente. Una forma de distinguir entre la llave correcta y la incorrecta consiste en utilizar el factor de mejora η del punto enfocado. Utilizando la definición de la sección 2.9:

$$\eta = \frac{I_{opt}}{\langle I_{ref} \rangle}, \tag{4.1}$$

donde I_{opt} es la intensidad en la región de interés y $\langle I_{ref} \rangle$ es el promedio de la intensidad reflejada para diferentes muestras.

Para medir I_{opt} se toma la intensidad promedio dentro de la región de interés. Para medir $\langle I_{ref} \rangle$ se toma el promedio de la intensidad dentro de la región de interés para 100 patrones de speckle diferentes. Las imágenes son normalizadas respecto al tiempo de exposición.

La llave se iluminada con cada uno de los 50 desafíos y el factor de mejora es calculado cada vez. El factor de mejora debe superar un umbral de autentificación al menos en el 75 % de los 50 pares *desafío-respuesta* para ser autentificado.

En la figura 4.8 se muestra el patrón de speckle que genera la llave correcta e incorrecta, respectivamente, en la lectura de autentificación.

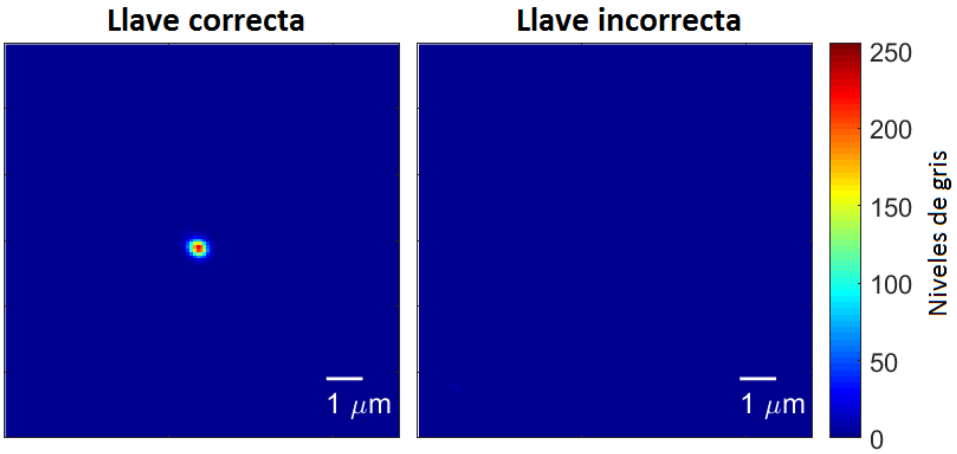

Figura 4.8: Patrón de speckle en el plano de la cámara con la llave correcta (izquierda) y la llave incorrecta (derecha) con la misma escala de color. La escala mostrada en la figura se encuentra en el plano objeto. El tamaño del pixel de la cámara es de 5,5μm.

De la figura 4.8 se notó que la diferencia entre la llave correcta y la llave incorrecta es claramente visible.

4.2.4. Algoritmo de búsqueda

El sujetador de llave debe colocar la llave siempre en la misma posición, con la misma orientación, etc., con precisión de micrómetros para que la luz dispersada en reflexión por la llave (patrón de speckle) sea el mismo en cada lectura y pueda ser invertido correctamente. Si bien el sujetador de llave es suficientemente preciso para colocar la llave en una posición muy cercana a la original, no siempre lo hace con una precisión suficiente para que el punto enfocado logre pasar la autentificación. Debido a que introduce pequeños desplazamiento en el eje x e y reduciendo el factor de mejora.

Podemos corregir la desalineación de la llave en el eje x e y sin introducir algún componente extra al arreglo experimental, usando únicamente los DMDs.

Para este propósito, se desarrolló el siguiente algoritmo que desplaza los patrones desafío y respuesta de la llave; En la figura 4.9 se muestra el diagrama de flujo del algoritmo.

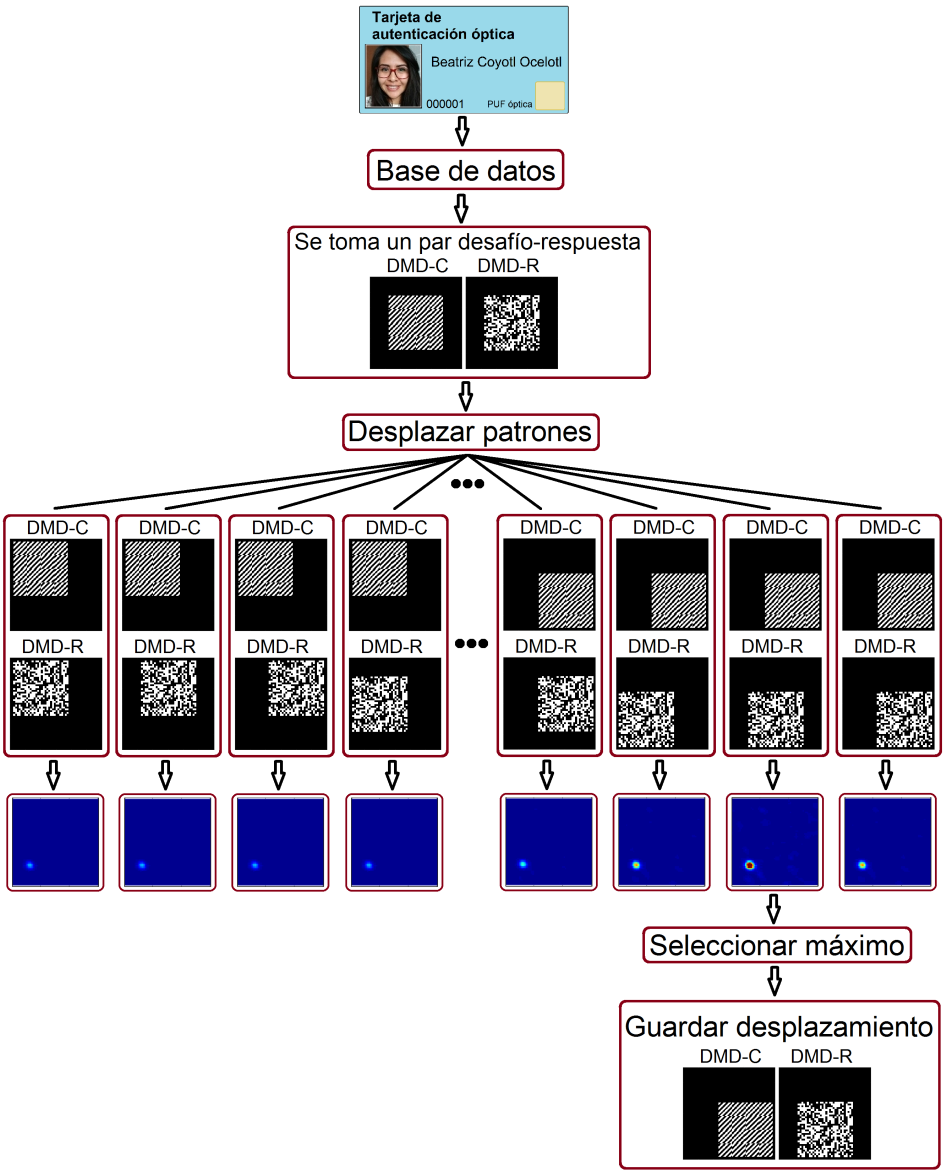

Figura 4.9: Diagrama de flujo del algoritmo de búsqueda.

Dada una tarjeta de identificación, se accede a su base de datos de pares desafío-respuesta. Aleatoriamente se escoge uno de los pares desafío-respuesta. Posteriormente, los patrones son desplazados en los DMDs. El patrón-desafío

en el DMD-C es desplazado 5 veces en la dirección x e y, respectivamente. Lo que significa, 25 posiciones diferentes en el DMD-C. La separación entre posiciones consecutivas en el DMD-C es 2 pixeles del DMD-C. Un desplazamiento en el patrón-desafío desplaza la posición que ilumina el haz en la llave (inclinación del haz de iluminación). Por lo que, el haz reflejado sufre una inclinación también. Debido a esto, el patrón-respuesta debe ser desplazado también. Similarmente al patrón-desafío es desplazado 5 veces en la dirección x e y respectivamente en pasos de 2 pixeles del DMD-R, para cada posición del patrón-desafío. En total, 625 posiciones diferentes son utilizadas para re-alinear la llave. Los desplazamientos del patrón-desafío son con la intención de iluminar el área correcta de la llave. Los desplazamientos del patrón-respuesta, tienen la intensión de alinear el haz reflejado con el patrón-respuesta.

Para cada combinación de posiciones de los patrones desafío y respuesta, dentro de una región cuadrada de 100×100 pixeles de CCD centrada en la posición original del punto enfocado, se busca el grano de speckle con el factor de mejora más alto. Después de todas las combinaciones, mantenemos la posición de patrones desafío y respuesta que producen el factor de mejora más alto.

Una vez que se conocen los desplazamientos necesarios en os patrones que maximizan el factor de mejora todos los pares desafío-respuesta utilizados para la lectura se desplazaran de la misma forma.

En la figura 4.10 se muestra un esquema del funcionamiento del algoritmo de búsqueda.

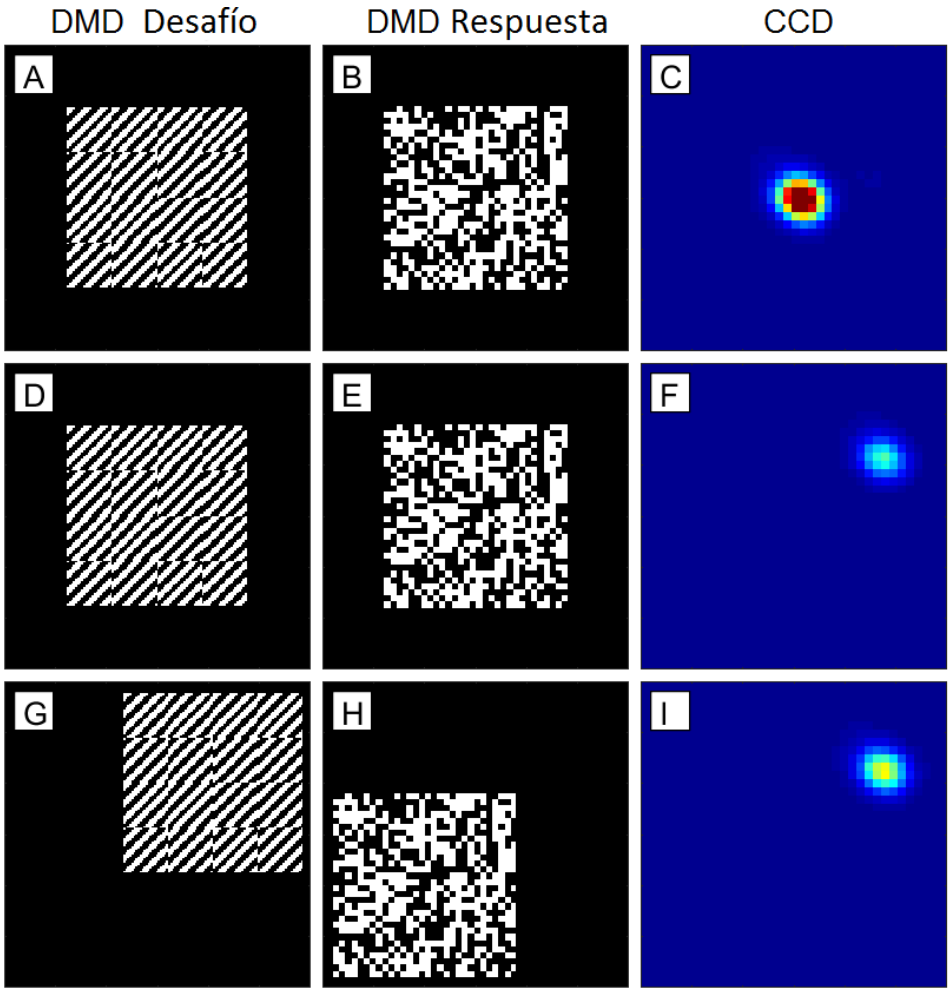

Figura 4.10: Representación esquemática del patrón-desafío en el DMD-C (figuras A, D, G), patrón-respuesta (figuras B, E, H) y de la región de lectura en la cámara (figuras C, F, I). Cuando los patrones en los DMD están centrados (A, B respectivamente) cuando la llave es correcta y esta en la posición original, se obtiene un punto con un alto factor de mejora (figura C). Sin embargo, cuando los patrones en los DMD están centrados (D, E respectivamente), la llave es correcta pero no se encuentra en la posición original, en la cámara (figura F) se observa un punto con un factor de mejora inferior al original. Después de corregir la posición de la llave con el algoritmo de búsqueda, los patrones son desplazados (G, H respectivamente), el factor de mejora en la región de lectura (figura I) se incrementa. Color negro simboliza micro-espejos en posición *apagado*. Color blanco simboliza micro-espejos en posición *encendido*.

En la primer fila de imágenes de la figura 4.10 se muestra en la imagen C la intensidad del punto enfocado cuando la llave esta en la posición correcta y los patrones están en sus posiciones originales (imágenes A y B).

La segunda fila de imágenes de la figura 4.10 muestra la intensidad del punto enfocado reducida y desplazada en la imagen F. Esto debido a que la llave no se encuentra en la posición adecuada y los patrones no han sido ajustados (imágenes D y E), manteniendo su posición original.

En la última fila de imágenes de la figura 4.10 se muestra la intensidad del punto enfocado en la imagen I después de ajustar los patrones a la posición que maximiza el factor de mejora (imágenes G y H). El punto enfocado en la imagen I muestra una mayor intensidad que en la imagen F gracias al ajuste.

Podemos notar del esquema en la figura 4.10 que si bien, la intensidad del punto enfocado después del algoritmo de búsqueda en I es mejor que la intensidad sin utilizar el algoritmo en F, pero siendo menor que en la intensidad original en C. Esto es debido a posibles desplazamientos en el eje z, así como a rotaciones de la llave. Y el algoritmo de búsqueda actualmente no considera este tipo de movimientos.

Prueba del algoritmo de búsqueda

Para probar el funcionamiento del algoritmo de búsqueda llevamos acabo el siguiente experimento; usando la base de datos para el usuario-uno, se lee la llave-uno (llave correcta) 52 veces sin y con el algoritmo de búsqueda. Se repite el experimento usando la base de datos del usuario-uno con la llave-dos (llave incorrecta). En la figura 4.11 se muestra el histograma del factor de mejora para la llave incorrecta después de haber aplicado el algoritmo de búsqueda (rosa) y la llave correcta sin aplicar el algoritmo (azul). El factor de mejora originalmente para el desafío utilizado fue de $\eta = 103$. De la figura 4.11 se observó que aún cuando no se usa el programa de búsqueda la llave correcta (histograma azul) presenta un factor de mejora significativamente superior a la llave incorrecta, inclusive alcanzando valores cercanos a $\eta = 55$. Esto debido al efecto memoria. Sin embargo, hay ocasiones que el factor de mejora sin utilizar el algoritmo de búsqueda es inferior a $\eta \leq 5$.

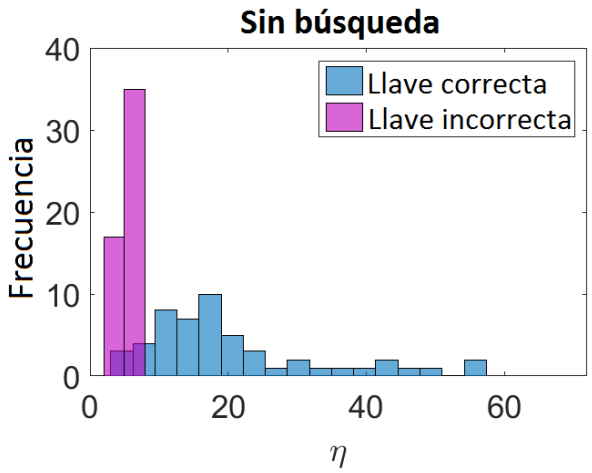

Figura 4.11: Histograma del factor de mejora para la llave incorrecta con el algoritmo de búsqueda (rosa) y la llave correcta sin utilizar el algoritmo de búsqueda (azul).

En la figura 4.12 se muestra el histograma del factor de mejora para la llave incorrecta (rosa) y para la llave correcta (naranja) después de haber aplicado el algoritmo de búsqueda.

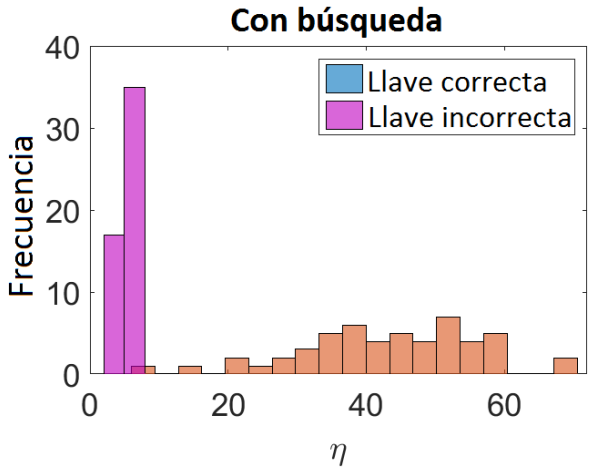

Figura 4.12: Histograma del factor de mejora para la llave incorrecta (rosa) y la llave correcta (naranja) con el algoritmo de búsqueda.

En la tabla 4.1 se muestra en factor de mejora promedio y la desviación estándar para la llave correcta e incorrecta.

Tabla 4.1: Factor de mejora promedio y desviación estándar de los histogramas de las figuras 4.11, 4.12.

	η_{pro}	σ
llave incorrecta después de búsqueda	5.5	1.0
llave correcta	20.5	12.7
llave correcta después de búsqueda	43.3	12.7

Para la llave incorrecta el valor esperado porcentual que se encuentra fuera del intervalo simetrico -4σ,4σ es 0,006334 %. Lo que significa que el valor esperado porcentual de que la llave incorrecta tenga un grano de speckle con un factor de mejora $\eta > 9{,}65$ es 0,003167 %. Por lo que, nos basta considerar un umbral de $\eta \geq 9{,}65$ para distinguir las llaves con una probabilidad de 0,003167 % falsos positivos.

4.2.5. Prueba de estabilidad

Con el objetivo de probar la estabilidad se realizó un experimento similar al descrito en la sección 4.2.1, tomando 40 fotografías cada 2 segundos de un punto enfocado en la cámara. Durante este proceso se mantienen todos los parámetros de la cámara y de iluminación. Se calculó el coeficiente de correlación cruzada entre la imagen l contra el resto de las imágenes, para toda $l \in 1, 2, ..., 40$. En la figura 4.13 se muestra un arreglo de 40x40 segmentos cuadrados. El mapa de color en el segmento (l, k) representa el factor de correlación cruzada entre la imagen l y la imagen k. Debido a que el coeficiente correlación cruzada de (l, k) es identico al de (k, l) y no aportan información nueva, estas correlaciones cruzadas no fueron calculadas. Además, la correlación cruzada de (l, l) es igual a 1 y tampoco aporta información a la estabilidad del sistema, los segmentos en la diagonal tampoco se calcularon.

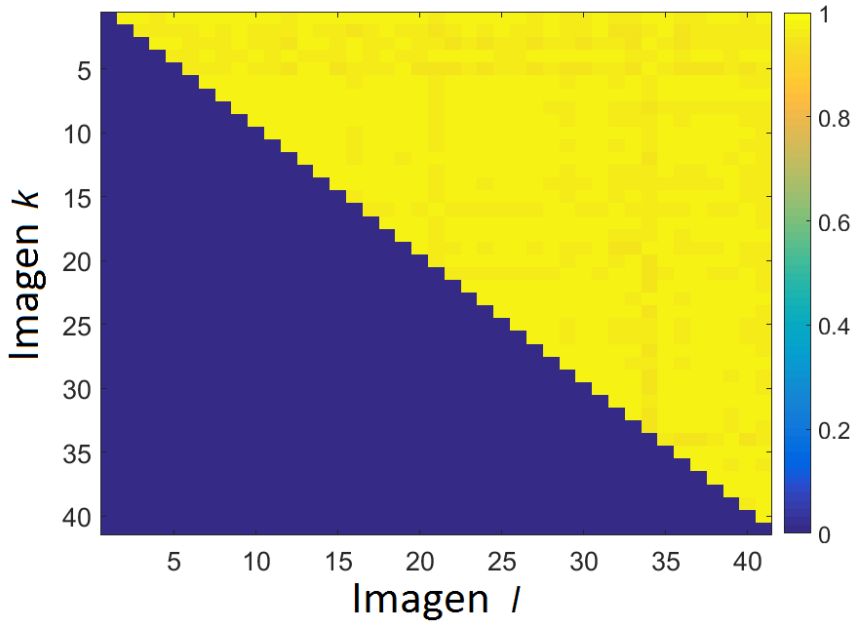

Figura 4.13: El mapa de color del segmento con coordenadas (l, k) representa el coeficiente de correlación cruzada entre las imágenes l y k. Cada imagen se tomó de un patrón de speckle focalizado en un punto tras una optimización BAM. El tiempo entre la captura de la foto l y $l + 1$ es de 4 segundos. Los segmentos sobre la diagonal y debajo de ésta, no se calcularon por que no aportan información relevante o diferente a los segmentos sobre la diagonal.

La figura 4.13 muestra una correlación cruzada alrededor de 1, demostrando que el arreglo es robusto y estable.

4.3. Trabajo a futuro: Transición a estado cuántico

Al usar funciones físicas inclonables, el método de autentificación resulta ser altamente seguro. Sin embargo, es posible incrementar el nivel de seguridad del método utilizando luz cuántica [5, 9, 10].

Para llevar a cabo la transición de autentificación con luz clásica a la autentificación con luz cuántica se requieren hacer pequeñas modificaciones al sistema y agregar algunos elementos. como son:

- Alternar la potencia del láser entre miliwatts y picowatts. Utilizando

miliwatts se puede hacer uso del algoritmo de búsqueda para mejorar la alineación. Una vez realineado el sistema, se decrementa la potencia del láser a picowatts.

- Agregar filtros para reducir la potencia. Una forma fácil de bajar la potencia del láser es hacerlo pasar por filtros capaces de reducir en gran medida la potencia del haz de luz. Por lo que, es necesario agregar filtros hasta que el número de fotones que alcanza la llave (y pueden ser leídos por un atacante) sea menor que el número de canales que posee la llave. Es decir, hasta que los fotones que alcanzan la llave son unas pocas centenas.

- Agregar un detector de fotones individuales. Se requiere un detector especial para detectar y contar fotones individualmente. Contando el número de fotones que alcanza el área de interés podremos distinguir entre la llave correcta e incorrecta [5].

- Agregar un contador de pulsos. Los detectores de fotones individuales mandan una señal de pulsos que debe ser traducida a una señal digital. Para esto, necesitamos el contador de pulsos.

Capítulo 5

Sumario y conclusiones

El método aleatorio utilizado para crear desafíos tiene grados de libertad suficientes para crear desafíos diferentes cada vez.

Con la elección de óxido de aluminio como medio esparcidor para la llave, ésta mantiene sus propiedades de esparcimiento invariantes ante cambios de temperaturas, presión y humedad. Además de que cuenta con una gran dureza previniendo cambios en la estructura microscópica.

En el primer prototipo para autentificación de seguridad cuántica no era posible remover y colocar la llave sin perder por completo la alineación 1.3. En este trabajo se logró autenticar la llave después de removerla en varias ocasiones. Ya que, el sujetador de la llave utilizado implementado es capaz de recolocar la llave con un rango lateral promedio de 50,5μm y una desviación estándar de $\sigma = 14{,}7\mu$m que es suficiente para visualizar el grano de speckle optimizado con una mejora promedio de $\eta = 20{,}5$ y desviación estándar de 12,7. Esto representa el 20 % de la mejora original.

Además se creó e implementó un algoritmo de búsqueda de la posición original de la llave que permite incrementar el factor de mejora sin agregar elementos al arreglo. El algoritmo de búsqueda incrementa el factor de mejora promedio a $\eta = 43{,}3$ con desviación estándar de 12,7 sin ni siquiera tocar la llave.

El primer arreglo para autentificación de seguridad cuántica no era posible transportarlo sin tener que desarmarlo por completo. Debido a la estructura de barras metálicas que une todos los elementos en el arreglo, éste es estable,

robusto y transportable. El arreglo viajo ida y vuelta en un auto particular en dos ocasiones: de la ciudad de Enshede a la ciudad de Veldhoven en Los Países Bajos, un total de 372km. En otra ocasión viajó de la ciudad de Enshede a la ciudad de Utrech en Los países Bajos un total de 278km. El arreglo no perdió la alineación durante los viajes.

El prototipo original para autentificación de seguridad cuántica requería una superficie aproximada de 2m^2. Con el trabajo realizado se logró optimizar el espacio y compactarlo a un volumen de $50 \times 30 \times 27\text{cm}^3$.

El arreglo fue probado en condiciones externas al laboratorio., y funcionó correctamente sin necesidad de controlar, temperatura, iluminación o vibraciones.

Por lo anterior, se puede concluir que nuestro método de autentificación óptica utilizando funciones físicas inclonables funciona satisfactoriamente bajo condiciones de la vida real.

Además que, el método es seguro debido a que las llaves son imposibles de copiar con la tecnología actual. Y serán imposibles de copiar por al menos varias décadas. Este hecho permite que este método pueda ser utilizado en instituciones de alta seguridad, como pueden ser, instituciones bancarias, laboratorios químicos, seguridad nacional, etc.

Referencias

[1] S. W. Inscoe,*Coordinated ATM heist nets thieves* 13M$ (Krebs on Security 2011)

[2] BBC Mundo,*Los secretos del cibercrimen organizado para robar tarjetas de crédito* (BBC 2014)

[3] S. W. Inscoe,*Global consumers react to rising fraud: beware back of wallet* (Aite Group LLC 2012)

[4] Felipe Díaz,*Fraudes con tarjetas bancarias casi se duplicaron en 2015* (La tercera, 2016)

[5] S. A. Goorden, M. Horstmann, A. P. Mosk, B. Skoric, and P. W. H. Pinkse *Quantum-secure authentication of a physical unclonable key* Optica 1, 421-424 (2014)

[6] I. M. Vellekoop, A. P. Mosk. *Focusing coherent light through opaque strongly scattering media.* Opt. Lett. 32, 2309-2311 (2007)

[7] R. Pappu, B. Recht, J. Taylor, N. Gershenfeld, *Physical one-way functions* Science 297, 2026-2030 (2002)

[8] J. D. R. Buchanan, R. P. Cowburn, A. V. Jausovec, D. Petit, P. Seem, G. Xiong, D. Atkinson, K. Fenton, D. A. Allwood, M. T. Bryan, *'fingerprinting'documents and packaging unique surface imperfection serve as easily identifiable feature in the fight against fraud.* Nature 436, 475 (2005)

[9] B. Skoric, A. P. Mosk, P. W. H. Pinkse. *Security of quantum-readout PUFs against quadrature-based challenge-estimation attacks* International Journal of Quantum Information 11, 1340041-1 (2013)

[10] B. Skoric. *Quantum readout of physical unclonable functions: Remorete authentication without trusted readers and authenticated quantum key exchange without initial shared secrets* International Journal of Quantum Information 10, 1250001-1 (2012)

[11] S. A. Goorden, M. Horstmann, A. P. Mosk, B. Skoric, and P. W. H. Pinkse *Quantum-secure authentication of a physical unclonable key: supplementary material* Optica 1, 421-424 (2014)

[12] Wai-Hon Lee. *Binary synthetic holograms.* Applied Optics 13, 1677-1682. (1974)

[13] S. A. Goorden, J. Bertolotti, A. P. Mosk . *Superpixel-based spatial amplitude and phase modulation using a digital micromirror device.* Opt. Express 22, 17999-18009 (2014)

[14] Milton Kerker. *The scattering of light and other electromagnetic radiation* (Academic Press, EUA-UK, 1969)

[15] L. I. Mandelstam. *Light scattering by inhomogeneous media* (1926)

[16] P. Sheng. *Introduction to wave scattering, localization and mesoscopic phenomena.* (Springer-Verlag Berlin Heidelberg, Alemania, 2006)

[17] Sebastianus Adrianus Goorden. *Reversible scattering of light exploited for quantum-secure authentication.* Tesis doctoral. (2015)

[18] W. van Rossum, M. Nieuwenhuizen *Multiple scattering of classical waves: microscopy, mesoscopy and diffusion.* Reviews of Modern Physics 71, 313-371 (1999)

[19] Duygu Akbulut. *Measurements of strong correlation in the transport of light through strongly scattering materials.* Tesis doctoral. (2013)

[20] C. W. J. Beenakker. *Random-matrix theory of quantum transport* Reviews of Modern Physics 69, 731 (1997)

[21] Eibert Gerjan van Putten. *Disorder-Enhanced imaging with spatially controlled light* Tesis doctoral. (2011)

[22] A. Mosk, A. Lagendijk, G. Lerosey, M. Fink. *Controlling waves in space and time for imaging and focusing in complex media.* Nature Photonics 6, 283-292 (2012)

[23] S. Feng, C. Kane, P. A. Lee, A. D. Stone. *Correlations and Fluctuations of Coherent Wave Transmission through Disordered Media.* Physical Review Letters 61, 834-837 (1988)

[24] I. Freund, M. Rosenbluh. *Memory Effects in Propagation of Optical Waves through Disordered Media.* Physical Review Letters 61, 2328-2331 (1988)

[25] I. M. Vellekoop, C. M. Aegerter *Scattered light fluorescence microscopy: imaging through turbid layers.* Optics letters 35, 1245-1247 (2010)

[26] E. Akkermans, G. Montambaux *Mesoscopic Physics of Electrons and Photons.* Cambridge (2011). ISBN:9780521349475

[27] J. W. Goodman, *Statistical optics.* Wiley (2000). ISBN:0-471-01502-4

[28] DLP. Texas Instruments *Hi-Speed V-Module. High-Performance subsystem for Texas Instruments DLP technology.* Disponible en *http://www.vialux.de/en/hi-speed-download.html*

[29] Texas Instruments *DLP7000 DLP 0.7XGA 2x LVDS Type A DMD.* (2015). Disponible en *http://www.ti.com/product/DLP7000*