

**Procesamiento de múltiples datos y compresión de
información por medio de técnicas ópticas análogo-digitales**



TESIS PARA OPTAR AL TÍTULO DE DOCTOR EN FÍSICA

Sorayda Trejos Gonzalez

Universidad de Antioquia

Facultad de Ciencias Exactas y Naturales

Instituto de Física

2017

**Procesamiento de múltiples datos y compresión de
información por medio de técnicas ópticas análogo-digitales**

TESIS PARA OPTAR AL TÍTULO DE DOCTOR EN FÍSICA
PRESENTADA POR:

Sorayda Trejos Gonzalez

DIRECTOR:

Dr. John Fredy Barrera Ramírez

CODIRECTOR:

Dr. Roberto Torroba

Universidad de Antioquia

Facultad de Ciencias Exactas y Naturales

Instituto de Física

2017

Agradecimientos

Agradezco a varias personas ya que de una u otra forma aportaron a la realización y culminación de este trabajo de investigación.

Quiero empezar agradeciendo al Dr. John Fredy Barrera por su valiosa ayuda y siempre sabio consejo tanto académico como personal durante el tiempo de desarrollo de este trabajo, por los conocimientos y experiencias entregadas como director de esta tesis de doctorado.

Al Dr. Roberto Torroba del CIOp (Centro de investigaciones ópticas, La Plata-Argentina), por su constante acompañamiento tanto a la distancia como personalmente. Fue de gran apoyo como co-director, que de igual manera que mi tutor dirigió y contribuyó con su sabia experiencia en los resultados obtenidos en este trabajo.

A la Dr. Myrian Tebaldi, y a mi colega Alejandro Veléz estudiante de doctorado, también pertenecientes al CIOp, por su acompañamiento y constante apoyo tanto académico como personal. Su compañía durante mi trabajo de investigación y pasantía doctoral en el CIOp, fue valiosa para los resultados de este trabajo, como los gratos y divertidos momentos en las largas horas de trabajo.

A los integrantes del Grupo de Óptica y Fotónica de la Universidad de Antioquia, por compartir sus conocimientos, y hacer amenas las largas horas de trabajo en el laboratorio.

En especial, gracias a mi madre y mis familiares por su paciencia, apoyo incondicional y motivación que siempre me han brindado. Por compartir las alegrías, experiencias y logros obtenidos durante mi trabajo.

A todos infinitos agradecimientos.

Sorayda Trejos Gonzalez

Junio 2017

1. Introducción	1
1.1. Contenido por capítulos	5
2. Sistemas análogo-digitales para el procesamiento de información	11
2.1. Sistemas ópticos de encriptación	13
2.1.1. Arquitectura 2f	14
2.1.2. Esquema óptico de encriptación de doble máscara de fase con la arquitectura 2f	16
2.1.3. Arquitectura JTC	17
2.1.4. Esquema óptico de encriptación de doble máscara de fase con una arquitectura JTC	19
2.2. Registro holográfico de la información procesada por sistemas ópticos	21
2.2.1. Holografía digital	21
2.3. Encriptación de doble máscara de fase con un sistema análogo-digital 2f	23
2.4. Encriptación de doble máscara de fase con un sistema análogo-digital JTC	26
2.5. Multiplexado de la información procesada por sistemas de encriptación análogo-digitales	29
2.5.1. Multiplexado para información procesada en un sistema de encriptación 2f	30
2.5.2. Multiplexado para información procesada en un sistema de encriptación JTC	30

3. Protocolo análogo-digital para el manejo seguro de mensajes con recuperación libre de ruido	36
3.1. ¿Qué es un código QR?	38
3.2. Descripción del proceso de encriptación de un código QR	39
3.3. Procesamiento de los múltiples códigos QR y encriptación	41
3.4. Proceso de recuperación	42
3.5. Resultados experimentales	43
3.6. Proceso de binarización	43
4. Reducción de volumen de datos encriptados ópticamente	49
4.1. Reducción del volumen por medio de la técnica de cuantización	51
4.1.1. Procesamiento de múltiples datos y encriptación	51
4.1.2. Cuantización y recuperación	51
4.1.3. Resultados experimentales	52
4.2. Reducción de volumen por medio de la técnica de escalado óptico	55
4.2.1. Procesamiento de un dato	56
4.2.2. Escalado óptico	56
4.2.3. Procesamiento de múltiples datos encriptados	57
4.2.4. Proceso de recuperación	59
4.2.5. Resultados experimentales	59
4.3. Reducción del volumen combinando las técnicas de cuantización y escalado óptico	63
4.3.1. Escalado digital	63
4.3.2. Resultados experimentales	63
5. Reducción de volumen en hologramas de objetos tridimensionales	73
5.1. Compresión de hologramas por medio de escalado óptico	75
5.1.1. Registro holográfico y dato de campo óptico	76
5.1.2. Resultados experimentales y desempeño de las técnicas de compresión	77
5.2. Compresión de hologramas a color por medio de máscaras binarias aleatorias	81
5.2.1. Registro y procesamiento de hologramas de objetos 3D a color	82
5.2.2. Técnica de compresión por medio de máscaras binarias aleatorias	84
5.2.3. Resultados experimentales y desempeño de las técnicas de compresión	86
6. Conclusiones y perspectivas	96
A. Lista de publicaciones, trabajos en eventos y reconocimientos	101

ÍNDICE DE FIGURAS

2.1. Arquitectura $2f$ para generar la transformada de Fourier de un objeto. O plano objeto, S plano de salida (el cual corresponde al plano de Fourier) y f es la distancia focal de la lente L	14
2.2. Arquitectura JTC . (a): Plano de entrada O , lente L de distancia focal f y K el plano del JPS ; (b) el plano con el JPS es ahora el plano de entrada y S el plano de salida.	18
2.3. Sistema de encriptación JTC : O plano de entrada, K plano de encriptación (plano de Fourier donde se obtiene el JPS) y L lente con distancia focal f	19
2.4. Sistema de desencriptación: O plano de entrada con la llave de seguridad, K plano que contiene la información encriptada que es multiplicada con la TF de la llave y D plano de desencriptación.	20
2.5. Sistema que registra hologramas de Fourier en configuración fuera de eje. E espejo, DH divisor de haz, MEL modulador espacial de luz donde se proyecta el objeto y L lente de longitud focal f	22
2.6. Esquema interferométrico de Fourier fuera de eje (DH: divisor de haz, E: espejo, MEL: modulador espacial de luz, L: lente de longitud focal f).	24
2.7. Distribución de intensidad asociada a la ecuación (2.29).	25
2.8. Esquema del criptosistema JTC de Fourier fuera de eje (DH: divisor de haz, MEL: modulador espacial de luz, E: espejo y L lente de longitud focal f).	27
2.9. Distribución de intensidad asociada a la ecuación (2.37).	27
3.1. Plano de entrada que representa la proyección de una porción de un código QR en el MEL de un sistema de encriptación $2f$ (ver Figura 2.6).	39

3.2.	Procesamiento, multiplexado y encriptación de 144 porciones de códigos QR.	40
3.3.	(a) Esquema para desencriptar, recuperar y mostrar el paquete de códigos QR. (b) Imagen ampliada de la recuperación en (a).	42
3.4.	(a) Panel con todos los códigos QR recuperados, (b) un QR del panel correspondiente al cuadrado blanco en (a), (c) sección magnificada del QR en (b), (d) valor promedio de cada bloque en (b) (entre 0 y 255) y (e) QR recuperado ya binarizado. 44	
3.5.	Panel con (a) los códigos QR procesados y binarizados y (b) los códigos QR originales, y (c) comparación de la misma región cuadrada del código QR en (a) y (b).	44
3.6.	(a) Mensaje recuperado con el protocolo propuesto (https://goo.gl/JqfMlw), y (b) mensaje recuperado con el procedimiento clásico.	45
4.1.	Recuperación de los 100 objetos para distintos valores de cuantización.	54
4.2.	Sistema óptico virtual usado para escalar ópticamente el dato de campo óptico: d_1 distancia objeto, L lente convergente, d_2 distancia imagen, M magnificación.	57
4.3.	Paquete $N_l(\mu, \nu)$ que contiene los datos de campo óptico de 16 objetos encriptados sobre un arreglo matricial.	58
4.4.	Recuperación: (a) sin el proceso de escalado sobre el multiplexado y (b) con escalado óptico de $M=0.5$ sobre el multiplexado.	60
4.5.	NMSE entre los datos recuperados desde el arreglo de la Figura 4.4 (a) antes y después de magnificación.	61
4.6.	Dependencia de ΔV con el número de objetos procesados para cinco valores de M	62
4.7.	Porcentaje en la reducción del volumen en función de la magnificación.	62
4.8.	Objetos recuperados a distintos valores de cuantización, escalado óptico y escalado digital.	64
4.9.	Estadística speckle para el método de escalado óptico.	66
4.10.	Estadística speckle para el método de escalado digital.	67
4.11.	Comparación para dos valores de reducción de volumen con ambos métodos de escalado.	68
4.12.	Coefficiente de correlación en términos de la magnificación para diferentes valores de cuantización.	69
5.1.	Montaje de holografía digital de Fourier fuera de eje (SC: sistema de colimación, DH: divisor de haz, E: espejo, L: lente de longitud focal f).	76

5.2.	(a) Holograma, b) intensidad del dato de campo óptico y c) intensidad del objeto reconstruido a partir del dato de campo óptico de (b).	77
5.3.	Coefficiente de correlación entre el objeto reconstruido desde el dato de campo óptico sin comprimir y el campo de dato óptico comprimido por ambos métodos de compresión, escalado óptico y JPEG en términos de la diferencia de volumen.	79
5.4.	Diferencia de volumen en amplitud y fase para los datos comprimidos en términos de: (a) magnificación y (b) el factor de calidad.	80
5.5.	Esquema holográfico de Fourier fuera de eje para registrar un objeto 3D en los tres canales RGB. (SC: sistema de colimación, DH: divisor de haz, E: espejos y L: lente de longitud focal f).	82
5.6.	Diagrama de flujo donde se ilustra el proceso de compresión propuesto por medio de máscaras binarias complementarias y la recuperación del objeto a color. <i>Re</i> corresponde a la parte real del campo e <i>Im</i> corresponde a la parte imaginaria del campo.	85
5.7.	Esquema de recuperación experimental. SC: sistema de colimación, MEL: modulador espacial de luz y L: lente de longitud focal f.	87
5.8.	Panel de los cinco objetos recuperados por el sistema óptico virtual con información de (a) amplitud y fase de los campos ópticos, (b) fase de los campos ópticos y (c) fase de los campos ópticos muestreados con máscaras binarias.	88
5.9.	Panel de los cinco objetos recuperados por el sistema óptico experimental de la Figura 5.7. Con información de (a) fase de los campos ópticos y (c) fase de los campos ópticos muestreados con máscaras binarias.	89
A.1.	El artículo <i>Optical field data compression by opto-digital means</i> en la exclusiva sección IOPselect.	124
A.2.	El artículo <i>Optical field data compression by opto-digital means</i> en la sección exclusiva “Highlights 2016”	124
A.3.	El artículo <i>Optical field data compression by opto-digital means</i> como el artículo de la semana en la revista <i>Journal of Optics</i>	125
A.4.	El artículo <i>Optimized and secure technique for multiplexing QR code images of single characters: application to noiseless messages retrieval</i> , en la sección <i>Lab talk: Optical cryptography</i> en la revista <i>Journal of Optics</i>	125
A.5.	Reconocimiento al trabajo <i>Secure opto-digital protocol to handle messages using the multiplexing of processed QR codes</i> , con presentación modalidad póster.	126
A.6.	Reconocimiento al trabajo <i>Reducción del volumen de información holográfica</i> , con presentación modalidad oral.	127

CAPÍTULO 1

INTRODUCCIÓN

Gracias a los avances tecnológicos de las últimas décadas es posible procesar y transmitir grandes cantidades de datos en forma de archivos de texto, imágenes, videos y música. Esta posibilidad ha conducido a un aumento considerable en el flujo de información necesario para suplir las necesidades de una sociedad que evoluciona constantemente. A la par, la capacidad de almacenamiento de datos ha crecido y se prevé que seguirá aumentando, considerándose un tema de investigación en constante desarrollo. El crecimiento en el flujo de información no solo ha motivado el desarrollo de medios con gran capacidad de almacenamiento, sino que además ha promovido el surgimiento de técnicas encaminadas a un manejo eficiente de la información. Estas técnicas se emplean ampliamente en muchas y diversas aplicaciones que dependen del procesamiento, almacenamiento y transmisión de información. El gran desarrollo de las telecomunicaciones y el notable avance de la Internet de los últimos años, junto con la proyección del crecimiento en la cantidad de información que debe ser almacenada y transmitida, han evidenciado la necesidad de optimizar las técnicas que actualmente se emplean para el manejo seguro y eficiente de los datos, y generar nuevas técnicas que permitan abordar este reto desde otra perspectiva [1]. Por esta razón, las técnicas que permiten un manejo eficiente de la información han presentado una gran evolución y están jugando un papel protagónico en el área del procesamiento de información.

Frente a estos requerimientos, las tecnologías ópticas se posicionan como candidatas importantes para el procesamiento de datos debido a que procesan información a velocidades superiores a las manejadas en los dispositivos electrónicos, además por la inherente capacidad de

procesar en paralelo de la luz, siendo esta una característica de gran importancia para aplicaciones en tiempo real. Adicionalmente se pueden aprovechar los distintos grados de libertad de los sistemas ópticos, como la longitud de onda, la polarización, la amplitud y la fase, entre otros, para procesar información. Estos grados de libertad han sido empleados para manejar múltiples datos que han sido manipulados por sistemas ópticos y posteriormente registrados digitalmente, principalmente en procesos encaminados a la protección de información [2]. Los mecanismos que permiten el procesamiento óptico de la información han presentado un gran desarrollo y han jugado un papel protagónico en los últimos años, y a su vez han creado la necesidad de desarrollar nuevas técnicas que permitan manipular la información generada por los sistemas ópticos. En particular, se ha prestado gran interés al manejo de múltiples datos donde se está realizando un esfuerzo intensivo para que la información se manipule de forma segura, rápida y eficiente.

Los procesadores o sistemas ópticos se fundamentan principalmente en algunas de las arquitecturas ópticas básicas, entre ellas las más empleadas son las arquitecturas $2f$, $4f$, y JTC (por las siglas en inglés: joint transform correlator) [3]. Estas arquitecturas ópticas han sido usadas ampliamente para el procesamiento óptico de información, en particular con base en ellas se han desarrollado sistemas ópticos que permiten encriptar y validar información, líneas de investigación que han presentado un gran desarrollo en los últimos años [4–14]. Asimismo, las técnicas de procesamiento óptico se han usado para implementar técnicas de multiplexado, las cuales permiten manipular múltiples datos. El multiplexado es un procedimiento o técnica que permite combinar una gran cantidad de datos procesados por un sistema óptico en un solo dato, lo cual es de gran utilidad en el momento de almacenar o transmitir la información. Además, cualquiera de los procesadores ópticos conformados por alguna de las arquitecturas básicas se puede llegar a combinar con técnicas de procesamiento digital; la unificación entre el alto rendimiento del procesamiento de información con sistemas ópticos y la flexibilidad computacional resulta en una combinación útil para el procesamiento de múltiples datos. Los sistemas experimentales que se componen de esta combinación, se les denomina sistemas híbridos o análogo-digitales.

Por consiguiente, todos los datos procesados por un sistema análogo pueden ser multiplexados para formar un único dato, lo que es ampliamente usado en procesos de encriptación de múltiples datos permitiendo así reforzar la seguridad del proceso [15–17]. En un principio, cuando se deseaba recuperar uno de los datos contenidos en el multiplexado, se presentaba superposición entre el dato recuperado y los patrones generados por los otros datos que estaban contenidos en el multiplexado; para evitar esta superposición se presentaron técnicas que permitieron recuperar cada uno de los datos que estaban multiplexados sin la influencia de los otros [18–22].

Además, debido a que los sistemas ópticos poseen un límite de resolución natural que depende de las dimensiones físicas y las características de los elementos que lo componen, no era posible encriptar y recuperar apropiadamente objetos con frecuencias espaciales que excedieran este límite. Esta limitación se sobrepasó al procesar el objeto en secciones, donde cada sección se proyectó en el sistema con el mismo tamaño del objeto original y luego se encriptó. Después se empleó el multiplexado para combinar las secciones encriptadas, de manera que a partir de la información multiplexada se puede recuperar apropiadamente el objeto original [23].

Es importante tener presente que un sistema análogo-digital es viable para proteger información en aplicaciones prácticas y masivas, cuando es seguro y permite manipular múltiples datos; adicionalmente, hay que tener en cuenta que el usuario final exige que la información a la que tiene acceso este completamente libre de ruido. Este ruido, no solo depende del límite de resolución, o de la cantidad de datos en un paquete multiplexado; además, hay otras causas de ruido como la suciedad (polvo) y las fluctuaciones del índice de refracción a las que está expuesto un procesador óptico experimental, por mencionar dos de ellas. Hasta ese momento, el ruido de superposición y el efecto del límite de resolución del sistema lograron ser evitados con varias propuestas que ya han sido reportadas en la literatura, como se indicó anteriormente [23]. Pero el ruido que presentaban los datos recuperados y que está asociado al procesamiento óptico con máscaras aleatorias, no había sido eliminado por completo.

Con estos antecedentes, en el 2013 se presentó una solución al ruido generado sobre los datos recuperados [24]. Dicha solución consiste en convertir la información original en un código de respuesta rápida QR (por las siglas en inglés: Quick Response code) [24]. Los códigos QR codifican la información que se desea proteger en forma de un patrón binario bidimensional, cuya lectura es resistente al ruido y a las distorsiones [25], permitiendo así recuperar la información contenida en ellos sin pérdida de fidelidad. El código QR que almacena la información original es encriptado y luego desencriptado. Aunque el dato recuperado contendrá el ruido debido al procesamiento óptico, gracias a la resistencia de la lectura de los códigos QR, el dato original es recuperado completamente libre de ruido o degradación. Por lo tanto, la inclusión de los códigos QR en la encriptación óptica permite la eliminación del ruido generado por el procesamiento óptico.

En paralelo a todos los avances en el área de encriptación óptica que permitieron evitar el ruido y solapamiento generado sobre los datos recuperados, se implementaron técnicas de multiplexado que permitieron aumentar la seguridad del proceso, y encriptar múltiples datos y vi-

deos [19]. La principal ventaja del multiplexado es almacenar en un solo dato toda la información involucrada, de esta forma un video encriptado ópticamente está contenido en un solo dato [19]. En este contexto el multiplexado trae consigo la ventaja de manipular, transmitir y recibir un solo dato en lugar de un conjunto de ellos. Por otro lado, hoy en día las técnicas empleadas para reducir el volumen de la información se conocen como técnicas de compresión. Estas técnicas son digitales y son ampliamente utilizadas a nivel mundial en todas las áreas del conocimiento y en todos los ámbitos. En particular, los métodos de compresión digital han sido empleados para reducir el volumen de datos generados en el procesamiento de información por medio de sistemas ópticos [26–29]. Estos métodos se basan en el análisis de los parámetros estadísticos de imágenes y las características de percepción visual del ojo humano. También se centran en la eliminación de información redundante o en suprimir armónicos innecesarios de la representación espectral. Sin embargo, en el caso de los hologramas digitales, estos métodos son mucho menos aplicables [30]. Hasta el momento de iniciar este trabajo de investigación no se habían presentado mecanismos que permitieran una manipulación eficiente de la información por medio de la combinación de técnicas de multiplexado con mecanismos que permitieran la reducción del volumen que ocupan los datos.

De acuerdo a lo antes mencionado, es evidente que el estudio, desarrollo y optimización de mecanismos para el manejo seguro y eficiente de datos basados en procesadores ópticos experimentales, es de gran importancia para la comunidad científica debido a sus grandes implicaciones académicas y tecnológicas [25,31]. Dichos mecanismos deben incluir métodos que permitan el manejo eficiente de información por medio de técnicas de multiplexado y la reducción de volumen de la información, en el caso de la encriptación óptica se debe garantizar que la información sea recuperada libre de ruido, todo ello contribuiría a generar sistemas seguros, prácticos y versátiles para el manejo eficiente de la información por medios análogo-digitales.

Este trabajo plantea sus objetivos en el contexto anterior. Como objetivo general, se quiere proponer e implementar sistemas ópticos análogo-digitales que permitan el manejo seguro y eficiente de información. Estos sistemas serán compactos, buscarán una reducción de volumen en la cantidad de información transmitida y/o almacenada, y permitirán que la información sea recuperada sin ruido en los sistemas ópticos de encriptación. Los aspectos antes mencionados, se evidencian en los siguientes capítulos de este trabajo.

1.1. Contenido por capítulos

Este trabajo consta de seis capítulos cuyos lineamientos generales se describen a continuación.

El capítulo 1 contiene la introducción, mientras que en el capítulo 2 se presenta la teoría básica para el entendimiento de los sistemas ópticos para el procesamiento de información. Inicialmente se estudian los sistemas basados en las arquitecturas básicas $2f$ y JTC , y como son implementados para encriptar información. Luego, se describe un montaje de holografía de Fourier fuera de eje y su utilización para llevar a cabo la implementación experimental de los sistemas de encriptación. Posteriormente, se muestra que mediante una técnica de multiplexado es posible adicionar múltiples datos encriptados para formar un solo paquete de información. Además se discuten las técnicas que se han empleado para evitar la superposición de los datos en el plano de recuperación. Este capítulo tiene como objetivo describir los principales conceptos acerca de los sistemas análogo-digitales, y los conceptos expuestos ayudarán a comprender adecuadamente el desarrollo de este trabajo de investigación en los siguientes capítulos.

En el capítulo 3 se presenta un protocolo para el manejo de mensajes de forma segura y eficiente con una recuperación libre de ruido. Este protocolo se implementa usando un sistema de encriptación $2f$ para procesar ópticamente cada dato y la información procesada es registrada por medio de un esquema de holografía de Fourier fuera de eje. Luego, los códigos QR son procesados ópticamente y posteriormente filtrados, posicionados y multiplexados para obtener un solo paquete que contiene toda la información. Este paquete se multiplica por una máscara aleatoria de fase para brindarle seguridad a la información, obteniéndose de esta forma un paquete de datos encriptado. Los usuarios autorizados reciben el paquete encriptado y el complejo conjugado de la máscara aleatoria para obtener un arreglo de códigos QR desencriptados. Además, cada usuario recibe la secuencia de lectura de códigos que le permite revelar el mensaje que le corresponde sin ningún tipo de degradación.

En especial, los datos encriptados representan una gran cantidad de información que posteriormente debe ser almacenada, enviada y/o procesada. Por consiguiente, el capítulo 4 tiene como finalidad abordar la reducción de volumen de la información contenida en los datos de campo óptico, los cuales se obtienen después de aplicar un proceso de filtrado sobre los hologramas registrados. En primer lugar se aplica la técnica digital de cuantización, y luego se propone e implementa una técnica óptico-virtual novedosa para reducir el volumen de los datos de campo óptico multiplexados y encriptados. Luego, se combinan estas técnicas y se evalúa la reducción

de volumen que producen. Este capítulo contiene tres secciones donde se describen las técnicas, su implementación y sus respectivos resultados. El contenido por secciones es el siguiente:

1. En la primera sección se implementa una técnica de cuantización sobre el paquete encriptado de datos de campo óptico. Los datos de campo óptico son obtenidos después de filtrar los hologramas de datos procesados por un sistema de encriptación experimental $2f$ y registrados por una técnica de holografía de Fourier fuera de eje. Aunque la cuantización es una técnica digital, es necesario evaluar su desempeño cuando se aplica sobre los datos obtenidos por los sistemas ópticos descritos en este trabajo.
2. En la segunda sección se describe la propuesta e implementación de una técnica óptico-digital para la reducción del volumen de datos que se define como *escalado óptico*. Esta técnica se aplica sobre los datos de campo óptico que se obtienen después de filtrar los hologramas generados por un sistema de encriptación experimental JTC y registrados por medio de una técnica de holografía digital fuera de eje. Además, se evalúa la eficiencia de la técnica.
3. En la tercera sección, se evalúa la reducción de volumen que resulta de la acción combinada de las técnicas de cuantización digital y escalado óptico. Además se compara la reducción de volumen que se produce cuando se aplican las técnicas de escalado óptico y digital. En este caso, las técnicas de reducción se aplican sobre multiplexado de los datos de campo óptico que fueron obtenidos como se describe en la sección 2.

En el capítulo anterior se aplican algunas técnicas de reducción de volumen sobre información holográfica, la cual fue obtenida mediante el procesamiento de datos bidimensionales con los sistemas de encriptación $2f$ y JTC . Debido a que las técnicas holográficas permiten registrar la información proveniente de objetos bidimensionales (2D) y tridimensionales (3D) [32], en el capítulo 5 se aplican técnicas de reducción de volumen a la información holográfica proveniente de objetos 3D. Este capítulo se divide en dos secciones:

1. En la primera sección se compara el desempeño entre dos métodos de compresión de información, el escalado óptico y el formato de compresión digital JPEG (por las siglas en inglés de: Joint Photographic Experts Group). Ambos métodos son aplicados sobre el dato de campo óptico obtenido a partir del holograma Fourier fuera de eje de un objeto 3D. Para ambos métodos de compresión, se analiza la calidad del objeto 3D recuperado en función de la reducción de volumen del dato de campo óptico por medio del coeficiente de correlación. Al final de esta sección, se lleva a cabo el análisis del comportamiento de la información de amplitud y de fase contenida en los datos de campo óptico comprimida usando ambos métodos.

-
2. En la segunda sección se presenta una nueva técnica de compresión de datos de campo óptico provenientes de hologramas de objetos tridimensionales a color. Se utiliza un esquema experimental de holografía de Fourier fuera de eje que permite registrar por separado tres hologramas del objeto 3D en los canales cromáticos RGB. Luego, se extraen los datos de campo óptico contenidos en cada holograma y se retiene su información de fase, posteriormente la información de fase es muestreada al multiplicarla con una máscara binaria aleatoria. Finalmente, la información muestreada es multiplexada para formar un único paquete. A partir del paquete se puede reconstruir el campo del objeto 3D a color, reconstrucción que se lleva a cabo por medio de un sistema óptico-virtual y usando un montaje experimental.

Finalmente, en el capítulo seis se presentan las conclusiones generales y perspectivas de este trabajo.

- [1] E. Setyaningsih, R. Wardoyo. *Review of Image Compression and Encryption Techniques*. International Journal of Advanced Computer Science and Applications (IJACSA), 8:080212, 2017.
- [2] B. Javidi, A.Carnicer, M. Yamaguchi, T. Nomura, E. Pérez-Cabré, M.S. Millán, N.K. Nishchal, R. Torroba, J.F Barrera, W. He, X. Peng, A. Stern, Y. Rivenson, A. Alfalou, C. Brosseau, C. Guo, J.T. Sheridan, G. Situ, M.Naruse, T. Matsumoto, I. Juvells, E. Tajahuerce, J. Lancis, W. Chen, X. Chen, P.W. Pinkse, A.P. Mosk, A. Markman. *Roadmap on optical security*. J. Opt., 18:083001, 2016.
- [3] J.W. Goodman. *Introduction to Fourier Optics*. McGraw-Hill, 2nd edition, 1996.
- [4] B. Javidi, J.L. Horner. *Optical pattern recognition for validation and security verification*. Opt. Eng., 33:1752–1756, 1994.
- [5] P. Refregier, B. Javidi. *Optical image encryption based on input plane Fourier plane random encoding*. Opt. Lett., 20:767–769, 1995.
- [6] B. Javidi, G. Zhang, J. Li. *Experimental demonstration of the random phase encoding technique for image encryption and security verification*. Opt. Eng., 35:2506–2512, 1996.
- [7] B. Javidi, A. Sergent . *Fully phase encoded key and biometrics for security verification*. Opt. Eng., 36:935–942, 1997.
- [8] G. Unnikrishnan, J. Joseph, K. Singh. *Optical Encryption System That Uses Phase Conjugation in a Photorefractive Crystal*. Appl. Opt., 37:8181–8186, 1998.

-
- [9] O. Matoba, B. Javidi. *Encrypted optical memory system using three-dimensional keys in the Fresnel domain*. *Opt. Lett.*, 24:762–764, 1999.
- [10] O. Matoba, B. Javidi. *Encrypted optical storage with angular multiplexing*. *Appl. Opt.*, 38:7288–7293, 1999.
- [11] B. Javidi (Editor). *Optical and Digital Techniques for Information Security*. Springer, New York, 2005.
- [12] J.F. Barrera, R. Henao, M. Tebaldi, R. Torroba, N. Bolognini. *Multiplexing encryption–decryption via lateral shifting of a random phase mask*. *Opt. Commun.*, 259:532–536, 2006.
- [13] J.F. Barrera, M. Tebaldi, R. Torroba, N. Bolognini. *Multiplexing encryption technique by combining random amplitude and phase masks*. *Optik*, 120:351–355, 2009.
- [14] J.F. Barrera, R. Henao, M. Tebaldi, R. Torroba, N. Bolognini. *Digital encryption with undercover multiplexing by scaling the encoding mask*. *Optik - International Journal for Light and Electron Optics*, 120:342–346, 2009.
- [15] G. Situ, J. Zhang. *Multiple-image encryption by wavelength multiplexing*. *Opt. Lett.*, 30:1306–1308, 2005.
- [16] D. Amaya, M. Tebaldi, R. Torroba, N. Bolognini. *Multichanneled puzzle-like encryption*. *Opt. Commun.*, 281:3434–3439, 2008.
- [17] E. Rueda, J.F. Barrera, R. Henao, R. Torroba. *Lateral shift multiplexing with a modified random mask in a joint transform correlator encrypting architecture*. *Opt. Eng.*, 48:027006, 2009.
- [18] J.F. Barrera, R. Henao, M. Tebaldi, R. Torroba, N. Bolognini. *Multiplexing encrypted data by using polarized light*. *Opt. Commun.*, 260:109–112, 2006.
- [19] F. Mosso, J.F. Barrera, M. Tebaldi, N. Bolognini, R. Torroba. *All-optical encrypted movie*. *Opt. Exp.*, 19:5706–5712, 2011.
- [20] J.F. Barrera, M. Tebaldi, C. Ríos, E. Rueda, N. Bolognini, R. Torroba. *Experimental multiplexing of encrypted movies using a JTC architecture*. *Opt. Exp.*, 20:3388–3393, 2012.
- [21] J.F. Barrera, S. Trejos, M. Tebaldi, R. Torroba. *Experimental protocol for packaging and encrypting multiple data*. *J. Opt.*, 15:055406, 2013.

-
- [22] S. Trejos, J.F. Barrera, M. Tebaldi, R. Torroba. *Experimental opto-digital processing of multiple data via modulation, packaging and encryption*. J. Opt., 16:055402, 2014.
- [23] J.F. Barrera, E. Rueda, C. Ríos, M. Tebaldi, N. Bolognini, R. Torroba. *Experimental opto-digital synthesis of encrypted sub-samples of an image to improve its decoded quality*. Opt. Commun., 284:4350 – 4355, 2011.
- [24] J.F. Barrera, A. Mira, R. Torroba. *Optical encryption and QR codes: Secure and noise-free information retrieval*. Opt. Exp., 21:5373–5378, 2013.
- [25] O. Graydon. *Cryptography: Quick response codes*. Nature Photonics, 7:343, 2013.
- [26] T. Nomura, A. Okazaki, M. Kameda, Y. Morimoto, B. Javidi. *Image reconstruction from compressed encrypted digital hologram*. Opt. Eng., 44:1–7, 2005.
- [27] S.T. Sateesh, R. Sakthivei, K. Nirosha, H.M Kittur. *An optimized architecture to perform image compression and encryption simultaneously using modified DCT algorithm*. In *International Conference on Signal Processing, Communication, Computing and Networking Technologies*, pages 442–447, 2011.
- [28] D. Blinder, T. Bruylantsa, E. Stijns, H. Ottevaere, P. Schelkens . *Wavelet coding of off-axis holographic images*. page 88561L. SPIE, 2013.
- [29] T. Bruylantsr, D. Blinder, H. Ottevaere, A. Munteanu, P. Schelkens . *Microscopic off-axis holographic image compression with JPEG 2000*. page 91380F. SPIE, 2014.
- [30] E.A. Kurbatova, P.A. Cheremkhin, N.N. Evtikhiev, V.V. Krasnov, S.N. Starikov. *Methods of Compression of Digital Holograms*. Physics Procedia, 73:328 – 332, 2015.
- [31] *Information security through light: Protecting information with optical processors*. sección Labtalk, J. Opt., 2013.
- [32] A. Velez, J.F Barrera, R. Torroba. *One-step reconstruction of digitally assembled 3D extended holographic scenes*. Opt. Laser Technol., 75:146–150, 2015.

CAPÍTULO 2

SISTEMAS ANÁLOGO-DIGITALES PARA EL PROCESAMIENTO DE INFORMACIÓN

Algunos de los procedimientos empleados para manipular información estuvieron enmarcados exclusivamente en el dominio digital, no obstante, en los últimos años se han llevado a cabo múltiples investigaciones que han demostrado que los procesadores ópticos tienen una gran potencialidad para aplicaciones prácticas [1]. Hasta ahora, se han desarrollado técnicas de procesamiento de información con sistemas completamente ópticos, otros con sistemas análogo-digitales donde se utiliza un sistema óptico experimental en conjunto con un sistema óptico virtual, y algunos con sistemas ópticos virtuales. Dentro de todas las posibles técnicas, aquellas que involucran elementos ópticos y técnicas digitales son las más prometedoras para el desarrollo de nuevos métodos para el manejo de información [2–4].

Muchos de los sistemas ópticos utilizados para manipular datos se fundamentan principalmente en algunas de las arquitecturas ópticas básicas, entre ellas las más usadas son las arquitecturas $2f$ y JTC . En una arquitectura $2f$, el campo se propaga una distancia f desde el plano de entrada hasta incidir sobre una lente convergente de longitud focal f , luego este campo se propaga dentro de la lente (la traslación del campo dentro de la lente es despreciable) y sale sobre su cara opuesta, el campo saliente de la lente se propaga una distancia f hasta el plano de salida. Puede demostrarse que bajo ciertas condiciones la distribución del campo en el plano de salida es proporcional a la transformada de Fourier del plano de entrada, lo que muestra la capacidad que posee una lente convergente para realizar un análisis espectral de la función de entrada de un sistema físico [5], y convierte a la lente en una herramienta eficaz para el procesamiento de

información.

Por otro lado, Weaver y Goodman mostraron que la operación correlación puede realizarse ópticamente por medio de un correlador de transformada conjunta o *JTC* [6]. El correlador de transformada conjunta permite, como su nombre lo indica, realizar la operación correlación entre dos objetos, lo cual se lleva a cabo cuando los objetos a correlacionar se ubican en el plano de entrada del sistema $2f$, y luego se procesa la intensidad registrada en el plano de salida. Una de las aplicaciones más importantes del *JTC* es la validación de información por medios ópticos [7], la cual se basa en la comparación de información por medio de la operación correlación. Como aplicación práctica se puede pensar en un sistema de seguridad basado en la comparación de los elementos almacenados en una base de datos que permiten un acceso determinado, y el dato que contiene un usuario. Si el elemento de seguridad que posee el usuario no coincide con uno de los elementos almacenados, entonces el sistema no permitirá el acceso. Otra aplicación en el campo de la seguridad en la información es la encriptación óptica de datos, donde el primer sistema de encriptación basado en la arquitectura óptica *JTC* fue presentado por Nomura y Javidi [8], donde el plano de entrada contiene la información a encriptar y la llave de seguridad.

Además de su utilización en sistemas de seguridad, las arquitecturas ópticas básicas junto con las técnicas de multiplexado son la base de procedimientos que buscan la manipulación de múltiples datos, donde varias investigaciones realizadas en las últimas décadas han demostrado su efectividad y gran potencialidad para aplicaciones prácticas [3, 9–14]. El desarrollo de las investigaciones en esta línea de trabajo mostró que al manipular múltiples datos se pueden presentar problemas de superposición y ruido en el momento de la recuperación de cada dato, en consecuencia se buscaron alternativas para sobrepassar estos inconvenientes. Recientemente se desarrollaron dos técnicas para el manejo de múltiple datos que permiten evitar la superposición de los datos recuperados, donde ambas propuestas emplean un sistema análogo-digital [15, 16]. En este sistema cada uno de los datos es procesado usando un sistema óptico basado en la arquitectura $2f$, luego el dato es procesado y almacenado holográficamente para ser manipulado digitalmente. Esto permite que todos los datos sean recuperados en el mismo plano, al mismo tiempo y sin que se presente superposición.

En este contexto, el objetivo de este capítulo es dar a conocer los conceptos fundamentales asociados a los sistemas ópticos de encriptación haciendo énfasis en aquellos sistemas basados en las arquitecturas $2f$ y *JTC*. Primero se describe cada una de las arquitecturas ópticas y cómo se utilizan para encriptar información por medio de dos máscaras aleatorias de fase, donde la

máscaras usadas en los montajes experimentales son materiales transparentes y rugosos conocidos en la literatura como difusores [17]. Posteriormente, se presenta una técnica de holografía digital para registrar la información procesada por dichos sistemas de encriptación, y la implementación de técnicas de multiplexado para el manejo de múltiples datos encriptados.

2.1. Sistemas ópticos de encriptación

Desde que ha existido el hombre, siempre se ha tenido la necesidad de comunicarse, pero en muchas ocasiones es necesario que la comunicación sea confidencial. Desde las primeras civilizaciones se desarrollaron técnicas para ocultar y enviar mensajes, por ejemplo durante las guerras para evitar que se supiera información confidencial en caso de caer en manos enemigas, ésta se ocultaba o cifraba antes de ser enviada. Esta manera de ocultar la información se denominó como *criptografía*. El término de *encriptación* en el contexto de ocultamiento óptico de datos fue propuesto por O. Kafri y E. Keren en 1987 [18], utilizando la idea de codificar información usando distribuciones aleatorias, idea que fue previamente propuesta por M. Francon en 1975 [19].

La encriptación, es un proceso que se encarga de *transformar* o *modificar* la información, convirtiéndola en un patrón a partir del cual no se puede reconocer la información. Lo que ayuda a modificar la información y darle seguridad, se conoce como *llave de seguridad*, de modo que solo quienes conozcan la llave puedan acceder a la información. El proceso de acceder a la información por medio de la llave se conoce como *desencriptación*. Este tipo de procesos rodea nuestra vida cotidiana, ya que se encuentra presente en el envío de información por correos, cifrar u ocultar carpetas o archivos en la computadora, en las claves bancarias, en general en cualquier proceso que involucre información que se deba proteger de terceros.

Cuando el proceso de la encriptación se lleva a cabo por medio de un sistema óptico, la información se encripta utilizando una llave física, y la variación de uno o varios de los grados de libertad del sistema óptico genera llave(s) de seguridad adicional(es), lo que lleva consigo varias ventajas como: confidencialidad, privacidad y protección. En este capítulo se describe la técnica de encriptación óptica que utiliza dos máscaras aleatorias de fase *DRPE* (por las siglas en inglés: Double Random Phase Encoding). De esta forma, los primeros conceptos que se abordan en esta sección están relacionados con el funcionamiento básico de un sistema óptico $2f$ y su utilización para encriptar información. Después, se describe el funcionamiento básico de un sistema óptico *JTC* y su implementación para encriptar información.

2.1.1. Arquitectura 2f

Se tiene una transparencia con amplitud de transmitancia $t_A(x_0, y_0)$ en la entrada del sistema ilustrado en la Figura 2.1. Si la entrada es iluminada por una onda plana monocromática que incide normalmente con amplitud A , el campo emergente del plano de entrada O será [5]:

$$U_0(x_0, y_0) = At_A(x_0, y_0). \quad (2.1)$$

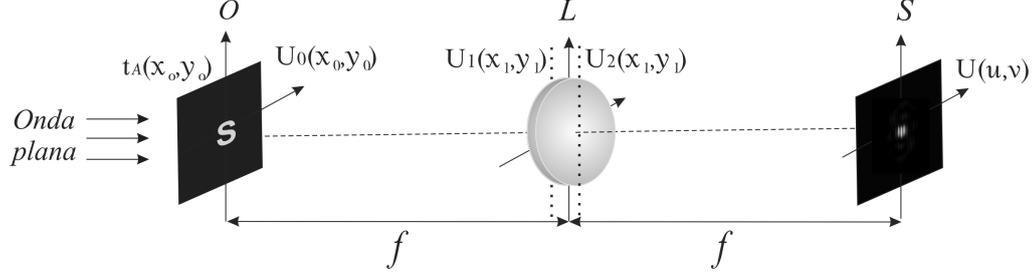


Figura 2.1: Arquitectura $2f$ para generar la transformada de Fourier de un objeto. O plano objeto, S plano de salida (el cual corresponde al plano de Fourier) y f es la distancia focal de la lente L .

El campo $U_0(x_0, y_0)$ se propaga una distancia f hasta incidir sobre la lente, el campo que está exactamente antes de la lente $U_1(x_1, y_1)$ usando la aproximación se Fresnel se expresa como [5]:

$$\begin{aligned} U_1(x_1, y_1) &= \frac{e^{ikf}}{i\lambda f} \iint_{-\infty}^{+\infty} U_0(x_0, y_0) e^{i\frac{k}{2f}[(x_1-x_0)^2+(y_1-y_0)^2]} dx_0 dy_0 \\ &= \frac{e^{ikf}}{i\lambda f} e^{i\frac{k}{2f}(x_1^2+y_1^2)} \iint_{-\infty}^{+\infty} U_0(x_0, y_0) e^{i\frac{k}{2f}(x_0^2+y_0^2)} e^{-i\frac{k}{f}(x_1x_0+y_1y_0)} dx_0 dy_0, \end{aligned} \quad (2.2)$$

donde $e^{i\frac{k}{2f}(x_1^2+y_1^2)}$ es el término de Fresnel debido a la propagación de $U_0(x_0, y_0)$ por una distancia f . Después el campo $U_1(x_1, y_1)$ atraviesa la lente, la cual se considera delgada y convergente, por lo tanto, el campo $U_2(x_1, y_1)$ exactamente después de la lente viene dado por:

$$U_2(x_1, y_1) = U_1(x_1, y_1) e^{-i\frac{k}{2f}(x_1^2+y_1^2)} \quad (2.3)$$

donde la lente bajo aproximación paraxial introduce un factor de fase multiplicativo de la forma $e^{-i\frac{k}{2f}(x_1^2+y_1^2)}$. Nótese que las coordenadas antes y después de la lente son iguales, debido a que en una “lente delgada” cuando un rayo entra por un punto con coordenadas (x_1, y_1) sobre una cara, sale aproximadamente en la misma coordenada sobre la cara opuesta, i.e, existe una traslación despreciable del rayo dentro de la lente. Reemplazando (2.2) en (2.3) se obtiene:

$$U_2(x_1, y_1) = \frac{e^{ikf}}{i\lambda f} \iint_{-\infty}^{+\infty} U_0(x_0, y_0) e^{i\frac{k}{2f}(x_0^2+y_0^2)} e^{-i\frac{k}{f}(x_1x_0+y_1y_0)} dx_0 dy_0. \quad (2.4)$$

Para encontrar la distribución del campo $U(u, v)$ después de la propagación del campo $U_2(x_1, y_1)$ por una distancia f hasta el plano S , se aplica de nuevo la aproximación de Fresnel [5]:

$$U(u, v) = \frac{e^{ikf}}{i\lambda f} \iint_{-\infty}^{+\infty} U_2(x_1, y_1) e^{i\frac{k}{2f}(u^2+v^2)} e^{i\frac{k}{2f}(x_1^2+y_1^2)} e^{-i\frac{k}{f}(ux_1+vy_1)} dx_1 dy_1, \quad (2.5)$$

Finalmente, al reemplazar (2.4) en (2.5) se tiene que el campo en el plano de salida es:

$$U(u, v) = \frac{e^{2ikf}}{(i\lambda f)^2} e^{i\frac{k}{2f}(u^2+v^2)} \times$$

$$\iint_{-\infty}^{+\infty} \left[\iint_{-\infty}^{+\infty} U_0(x_0, y_0) e^{i\frac{k}{2f}(x_0^2+y_0^2)} e^{-i\frac{k}{f}(x_1x_0+y_1y_0)} dx_0 dy_0 \right]$$

$$e^{i\frac{k}{2f}(x_1^2+y_1^2)} e^{-i\frac{k}{f}(ux_1+vy_1)} dx_1 dy_1. \quad (2.6)$$

La ecuación (2.6) puede simplificarse teniendo en cuenta que [5]:

- El término $e^{i\frac{k}{2f}(x_1^2+y_1^2)}$ se puede reescribir como: $e^{i\frac{k}{2}\left(\frac{1}{z_1} + \frac{1}{z_2} - \frac{1}{f}\right)(x_1^2+y_1^2)}$ con $z_1=z_2=f$, y de la ley de lentes de óptica geométrica debe cumplirse:

$$\frac{1}{z_1} + \frac{1}{z_2} - \frac{1}{f} = 0$$

por lo tanto el término $e^{i\frac{k}{2f}(x_1^2+y_1^2)}$ es igual a la unidad.

- El término $e^{i\frac{k}{2f}(x_0^2+y_0^2)}$ puede ser ignorado, por que la distribución de fase a través del plano focal no es la misma que la distribución de fase a través del espectro de la entrada, la diferencia entre las dos distribuciones es una curvatura de fase [5], la cual es despreciable.

Teniendo en cuenta las aproximaciones anteriores, la ecuación (2.6) se transforma en:

$$U(u, v) = \frac{e^{2ikf}}{(i\lambda f)^2} e^{i\frac{k}{2f}(u^2+v^2)} \times$$

$$\iint_{-\infty}^{+\infty} \left[\iint_{-\infty}^{+\infty} U_0(x_0, y_0) e^{-i\frac{k}{f}(x_1x_0+y_1y_0)} dx_0 dy_0 \right]$$

$$e^{-i\frac{k}{f}(ux_1+vy_1)} dx_1 dy_1. \quad (2.7)$$

Resolviendo la integral correspondiente a las coordenadas (x_1, y_1) , se obtiene:

$$U(u, v) = \frac{e^{2ikf}}{(i\lambda f)^2} e^{i\frac{k}{2f}(u^2+v^2)} \iint_{-\infty}^{+\infty} U_0(x_0, y_0) e^{-i\frac{k}{f}(ux_0+vy_0)} dx_0 dy_0 \quad (2.8)$$

El término de fase cuadrático puede ser ignorado pues no contribuye a la distribución de intensidad en el plano de salida.

Teniendo en cuenta lo anterior, la ecuación (2.8) se convierte en:

$$U(u, v) = \frac{e^{2ikf}}{(i\lambda f)^2} \iint_{-\infty}^{+\infty} U_0(x_0, y_0) e^{-i\frac{k}{f}(ux_0+vy_0)} dx_0 dy_0 \quad (2.9)$$

Por simplicidad en las expresiones, el término $\frac{e^{2ikf}}{(i\lambda f)^2}$ se hace igual a la unidad, teniendo en cuenta que esta expresión contiene parámetros que son constantes. Finalmente, la ecuación (2.9) puede expresarse de forma simplificada como:

$$U(u, v) = \iint_{-\infty}^{+\infty} U_0(x_0, y_0) e^{-i\frac{k}{f}(ux_0+vy_0)} dx_0 dy_0 \quad (2.10)$$

La ecuación (2.10) es la distribución de campo en el plano de salida del sistema $2f$, y corresponde a la transformada de Fourier del plano de entrada ilustrado en la Figura 2.1. Lo anterior muestra la capacidad que posee una lente para realizar un análisis espectral de la función de entrada del sistema físico, lo cual hace que ella se convierta en una herramienta eficaz para el procesamiento óptico de información.

2.1.2. Esquema óptico de encriptación de doble máscara de fase con la arquitectura $2f$

Una máscara aleatoria de fase $n(x_0, y_0)$ dada por $\exp[2\pi i B(x_0, y_0)]$ ($B(x_0, y_0)$ es una función aleatoria distribuida uniformemente entre los valores $[0, 1]$), se pone en contacto con el plano de entrada O de la arquitectura $2f$ mostrado en la Figura 2.1. De esta manera el plano de entrada del sistema de encriptación $2f$ viene descrito por:

$$U_0(x_0, y_0) = i(x_0, y_0)n(x_0, y_0), \quad (2.11)$$

donde $i(x_0, y_0)$ es el objeto a encriptar. En el plano de salida del sistema $2f$ (Figura 2.1), se obtiene la transformada de Fourier de la entrada (ecuación (2.11)).

$$U_1(\mu, \nu) = [I(\mu, \nu) \otimes N(\mu, \nu)], \quad (2.12)$$

con $I(\mu, \nu)$ como la TF del objeto de entrada $i(x_0, y_0)$ y $N(\mu, \nu)$ la TF de la máscara aleatoria $n(x_0, y_0)$. El proceso de encriptación del objeto $i(x_0, y_0)$ finaliza cuando el campo $U_1(\mu, \nu)$ se multiplica con una máscara aleatoria de fase $M(\mu, \nu)$ que actúa como llave de seguridad, es decir, que el dato encriptado en el sistema $2f$ es:

$$U_2(\mu, \nu) = [I(\mu, \nu) \otimes N(\mu, \nu)] M(\mu, \nu) \quad (2.13)$$

El proceso de descryptación permite recuperar el objeto a partir del dato encriptado, en la primera etapa del proceso se multiplica el dato encriptado por el complejo conjugado de la llave de seguridad:

$$U(\mu, \nu) = U_2(\mu, \nu)M^*(\mu, \nu) \quad (2.14)$$

Luego se genera una transformada de Fourier inversa (TFI):

$$u(x, y) = i(x, y)n(x, y) \quad (2.15)$$

Esta última expresión representa el objeto descryptado $i(x, y)$ superpuesto a la máscara aleatoria $n(x, y)$. Más adelante, se muestra la implementación experimental de este sistema de encriptación empleando una técnica de holografía digital para registrar y procesar el dato encriptado y la llave.

2.1.3. Arquitectura JTC

La representación esquemática de la arquitectura *JTC* se muestra en la Figura 2.2. Esta arquitectura permite realizar la operación correlación entre dos funciones, la cual se lleva a cabo por medio de un sistema óptico donde los dos objetos a correlacionar se ubican en el plano de entrada [5].

El plano de entrada O viene representado matemáticamente por:

$$U_0(x_0, y_0) = f(x_0, y_0) \otimes \delta(x_0 - d, y_0) + h(x_0, y_0) \otimes \delta(x_0 - (-d), y_0), \quad (2.16)$$

donde \otimes es la operación convolución, $f(x_0, y_0)$ y $h(x_0, y_0)$ corresponden a dos funciones a correlacionar ubicadas en las posiciones d y $-d$ respectivamente, cuya ubicación esta representada por la función delta de Dirac δ ; por lo tanto estas dos funciones se encuentran separadas una distancia $2d$ en el plano O como se ilustra en la Figura 2.2(a).

El espectro conjunto de potencias *JPS* (por las siglas en inglés: Joint Power Spectrum) en el plano K , es la intensidad de la transformada de Fourier de la entrada ($|TF_{u,v}\{U_0(x_0, y_0)\}|^2$). El *JPS* puede ser registrado usando un medio sensible a la intensidad como una cámara CCD o CMOS, los cristales fotorefractivos, películas holográficas, etc.

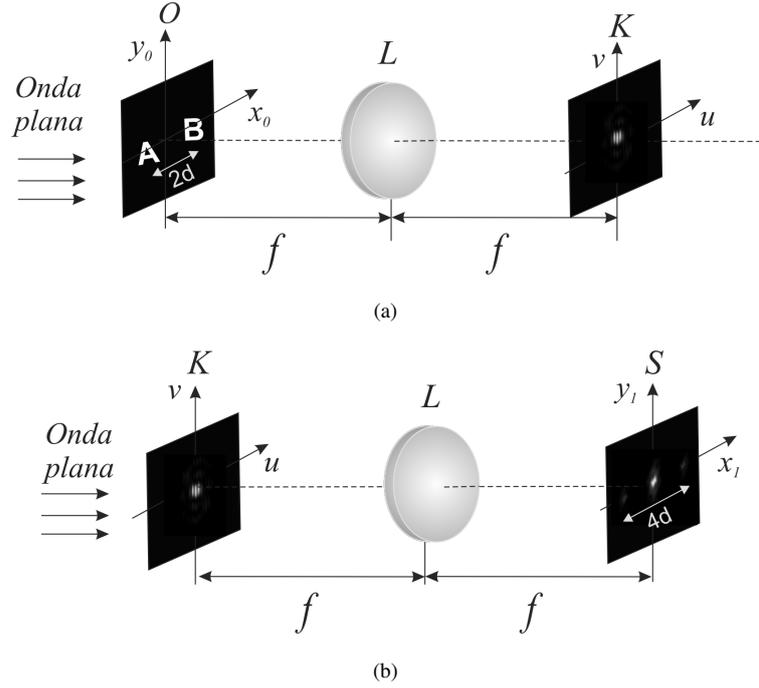


Figura 2.2: Arquitectura *JTC*. (a): Plano de entrada *O*, lente *L* de distancia focal *f* y *K* el plano del *JPS*; (b) el plano con el *JPS* es ahora el plano de entrada y *S* el plano de salida.

El *JPS* se representa matemáticamente como [20]:

$$I_{JPS} = |F(u, v)|^2 + |H(u, v)|^2 + F(u, v)H^*(u, v)e^{-i2\pi(d-(-d))u} + F^*(u, v)H(u, v)e^{-i2\pi((-d)-d)u}, \quad (2.17)$$

con $F(u, v)$ y $H(u, v)$ como las transformadas de Fourier de $f(x_0, y_0)$ y $h(x_0, y_0)$ respectivamente.

La correlación de las funciones del plano de entrada se genera cuando el *JPS* es iluminado con una onda plana monocromática como se muestra en la Figura 2.2(b). Por lo tanto en el plano *S* se obtiene:

$$U_S(x_1, y_1) = e^{-i\pi/2}f(-x_1, -y_1) \otimes f^*(x_1, y_1) + e^{-i\pi/2}h(-x_1, -y_1) \otimes h^*(x_1, y_1) + e^{-i\pi/2}f(-x_1, -y_1) \otimes h^*(x_1, y_1) \otimes \delta(x_1 - (-2d), y_1) + e^{-i\pi/2}f^*(x_1, y_1) \otimes h(-x_1, -y_1) \otimes \delta(x_1 - 2d, y_1), \quad (2.18)$$

donde los dos primeros términos corresponden a las auto-correlaciones de las funciones de entrada y los dos últimos términos a correlaciones entre las dos funciones. Los dos últimos términos de

la ecuación (2.18) se encuentran separados una distancia $4d$, como se muestra en la Figura 2.2(b).

Esta arquitectura óptica de correlación es de gran utilidad no solo en procesos de validación de información, sino también en procesos de encriptación, reconocimiento de objetos, restauración de imágenes, entre otros [21]. A continuación se describe como esta arquitectura es la base de un sistema óptico de encriptación.

2.1.4. Esquema óptico de encriptación de doble máscara de fase con una arquitectura JTC

El funcionamiento de este esquema para el proceso de encriptación, se basa en poner en contacto el plano de entrada (Figura 2.2 (a)) con una máscara aleatoria de fase $n(x_0, y_0)$. Las dos funciones que se ubican en el plano de entrada son el objeto que se quiere encriptar y la ventana de la llave representada por el cuadrado en la Figura 2.3. Con esta configuración, el plano de entrada O de este sistema de encriptación viene descrito por (Figura 2.3):

$$U_0(x_0, y_0) = f(x_0, y_0) \otimes \delta(x_0 - (-a), y_0) + m(x_0, y_0) \otimes \delta(x_0 - a, y_0), \quad (2.19)$$

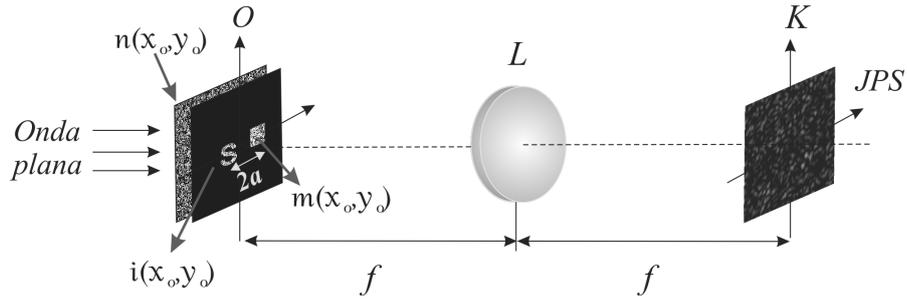


Figura 2.3: Sistema de encriptación JTC : O plano de entrada, K plano de encriptación (plano de Fourier donde se obtiene el JPS) y L lente con distancia focal f .

con $f(x_0, y_0) = i(x_0, y_0)n(x_0, y_0)$, donde $i(x_0, y_0)$ es la información a encriptar, $m(x_0, y_0)$ es una máscara aleatoria de fase que actúa como la llave de seguridad, y se forma con el área del difusor $n(x_0, y_0)$ que está limitada por la ventana de la llave. El objeto y la llave se encuentran separados una distancia $2a$ en el plano O (Figura 2.3). En el plano K se obtiene el JPS que corresponde a la intensidad de la transformada de Fourier del plano de entrada, y se describe como:

$$I_{JPS}(\mu, \nu) = |F(\mu, \nu)|^2 + |M(\mu, \nu)|^2 + F(\mu, \nu)M^*(\mu, \nu)e^{i4\pi a\mu} + F^*(\mu, \nu)M(\mu, \nu)e^{-i4\pi a\mu}, \quad (2.20)$$

donde $*$ representa el complejo conjugado, y $F(\mu, \nu)$ y $M(\mu, \nu)$ son las transformadas de Fourier de $f(x_0, y_0)$ y $m(x_0, y_0)$ respectivamente. El *JPS* contiene información redundante, donde uno de los términos es suficiente para obtener la información necesaria [20]. Por lo tanto, se procede a filtrar la ecuación (2.20).

En el plano de entrada, se bloquea la ventana llave y se registra el intensidad de la TF correspondiente al objeto $|F(\mu, \nu)|^2$, luego, se bloquea solo el objeto y se registra la intensidad de la TF de la llave $|M(\mu, \nu)|^2$. Las intensidades $|F(\mu, \nu)|^2$ y $|M(\mu, \nu)|^2$ se restan del *JPS* (ecuación (2.20)). Luego, como el tercer y cuarto término corresponden a la información encriptada, donde uno de ellos es el complejo conjugado del otro, se retiene el tercer término, que corresponde al objeto encriptado:

$$E(\mu, \nu) = F(\mu, \nu)M^*(\mu, \nu)e^{i4\pi a\mu} \quad (2.21)$$

Para el proceso de descryptación se utiliza un sistema $4f$ como se ilustra en la Figura 2.4, que cuenta con dos lentes convergentes cada una de igual distancia focal f . En el plano de entrada se ubica la llave de seguridad $m(x_0, y_0)$, la primera lente realiza la TF de la llave que se multiplica con la información encriptada en el plano K . Este plano se representa como:

$$S(\mu, \nu) = E(\mu, \nu)M(\mu, \nu)e^{-i2\pi a\mu} \quad (2.22)$$

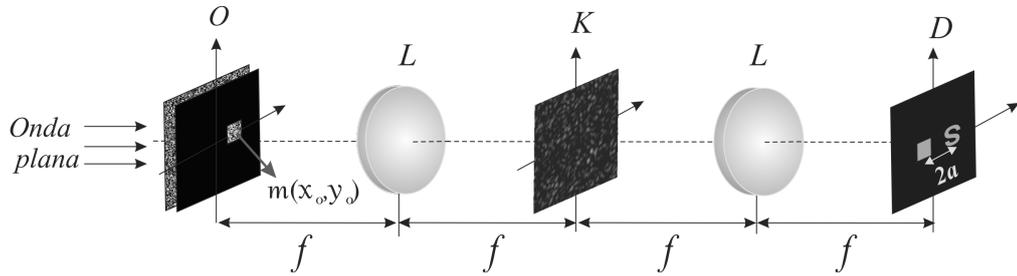


Figura 2.4: Sistema de descryptación: O plano de entrada con la llave de seguridad, K plano que contiene la información encriptada que es multiplicada con la TF de la llave y D plano de descryptación.

Finalmente se realiza una segunda transformada de Fourier con la segunda lente L , y en el plano de descryptación D se obtiene:

$$D(x', y') = f(-x', -y') \otimes \delta(x' - a, y') \quad (2.23)$$

Este término corresponde a la información del producto entre el objeto original $i(-x', -y')$ y una máscara de fase aleatoria. Este producto se encuentra ubicado en la posición $(a, 0)$ en el plano de recuperación D , como se muestra en la Figura (2.4).

Se debe destacar, que ambas arquitecturas, la $2f$ y JTC , han sido exploradas en los últimos años, y debido al alto rendimiento que exhiben estas arquitecturas para el procesamiento óptico de información, se han combinado con sistemas digitales para procesar eficientemente múltiples datos [3,9–16]. Por ello, la siguiente sección de este capítulo estará enfocada en la descripción de un sistema de holografía digital que permitirá registrar la información proveniente de los sistemas ópticos para su posterior procesamiento. Aunque existen varios esquemas de holografía digital, se describirá en particular el funcionamiento del sistema de holografía digital de Fourier fuera de eje empleado durante este trabajo de investigación.

2.2. Registro holográfico de la información procesada por sistemas ópticos

En este trabajo se usa la técnica de *holografía digital de Fourier fuera de eje* para almacenar la información procesada por los sistemas ópticos anteriormente mencionados. Inicialmente se describe el registro de información bidimensional $2D$ que es procesada por los sistemas de encriptación $DRPE$ en $2f$ y JTC . Más adelante, la técnica de holografía de Fourier fuera de eje se utiliza para registrar información de objetos tridimensionales $3D$ difusos. A continuación, se da una breve descripción de holografía digital y se incluye su descripción matemática.

2.2.1. Holografía digital

La *holografía* permite el registro de la amplitud y la fase de un campo óptico. Esta técnica se basa en el registro de la intensidad del campo que resulta de la interferencia entre una onda transmitida o reflejada por un objeto ($2D$ o $3D$) y una onda de referencia. Esta intensidad conocida como *holograma*, en general se compone de franjas de interferencia que normalmente no son visibles al ojo humano debido a su alta frecuencia, y es almacenado en un medio de registro que puede ser una película fotográfica, un cristal fotorefractivo o una cámara digital (CCD o CMOS).

Los hologramas pueden registrarse en dos tipos de configuración, sobre eje o fuera de eje [22]. En la configuración sobre eje la onda de referencia y la onda reflejada por el objeto inciden sobre el medio de registro por el mismo eje, lo que genera que el objeto reconstruido se superponga con una imagen real distorsionada y la luz de la onda de reconstrucción. Más adelante, dicho sistema fue modificado, de manera que la onda de referencia incidiera sobre el medio de registro en un eje distinto al de la onda proveniente del objeto como se muestra en la Figura 2.5.

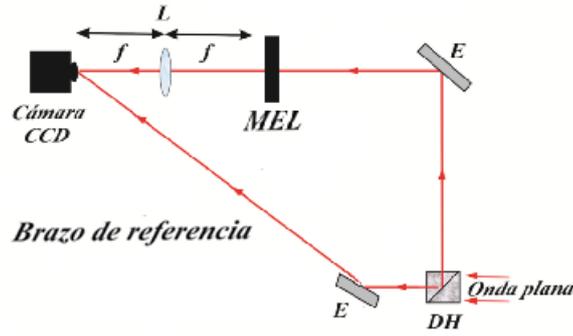


Figura 2.5: Sistema que registra hologramas de Fourier en configuración fuera de eje. *E* espejo, *DH* divisor de haz, *MEL* modulador espacial de luz donde se proyecta el objeto y *L* lente de longitud focal *f*.

A su vez, los hologramas se pueden clasificar en cinco clases [22]: Holograma de Fresnel, holograma de Fraunhofer, holograma de Fourier, holograma de imagen y holograma de Fourier sin lente. En particular, cuando se desea registrar un holograma de Fourier se captura la interferencia entre una onda de referencia y una onda que contiene la transformada de Fourier de la luz reflejada o transmitida por el objeto. En el esquema experimental de la Figura 2.5, el objeto proyectado en un modulador espacial de luz (MEL) y la cámara CCD están en los planos conjugados de una lente convergente *L* de longitud focal *f*.

Sin importar la configuración del registro o la clase de holograma, el principio generalmente es el mismo, una onda de referencia y una onda reflejada o transmitida por un objeto interfieren sobre un medio que registra la intensidad de dicha interferencia. Para representar matemáticamente el proceso de registro holográfico, se representará el campo óptico complejo de la onda objeto que incide sobre la cámara como [22]:

$$O(v, \omega) = a_O(v, \omega)e^{-j\phi_O(v, \omega)} \quad (2.24)$$

donde $a_O(v, \omega)$ representa la amplitud y $\phi_O(v, \omega)$ la fase de la onda objeto. De igual manera se representa el campo de la onda de referencia sobre el mismo plano:

$$R(v, \omega) = a_R(v, \omega)e^{-j\phi_R(v, \omega)} \quad (2.25)$$

donde $a_R(v, \omega)$ representa la amplitud y $\phi_R(v, \omega)$ la fase. Luego, la intensidad de la interferencia de ambos campos en el plano de registro se define como:

$$H(v, \omega) = I(v, \omega) = |O(v, \omega) + R(v, \omega)|^2 = |O(v, \omega)|^2 + |R(v, \omega)|^2 + O(v, \omega)R^*(v, \omega) + O^*(v, \omega)R(v, \omega) \quad (2.26)$$

La anterior ecuación representa el holograma que es registrado y almacenado, para luego ser procesado óptica o digitalmente.

En este trabajo de investigación se utilizará un sistema de holografía digital de Fourier fuera de eje, donde los hologramas se registran con una cámara digital en el plano focal de una lente que hace parte de un sistema óptico, y donde la lente genera la transformada de Fourier del campo proveniente del objeto.

De este modo, las siguientes secciones comprenden la combinación de los sistemas ópticos con el esquema de holografía de Fourier fuera de eje, generando así los sistemas de encriptación para procesar y registrar digitalmente los datos utilizados en este trabajo de investigación.

2.3. Encriptación de doble máscara de fase con un sistema análogo-digital 2f

El objeto a encriptar $o_l(x_0, y_0)$ es proyectado en un modulador espacial de luz que esta en contacto con un vidrio esmerilado o difusor $r(x_0, y_0)$, de esta manera el plano de entrada se representa como (Figura 2.6):

$$d_l(x_0, y_0) = [o_l(x_0, y_0)r(x_0, y_0)] \otimes \delta(x_0 - (-a), y_0), \quad (2.27)$$

donde δ es la función delta de Dirac, \otimes representa la operación convolución y $|a|$ es la distancia entre el objeto y el eje óptico en el plano de entrada, la cual se puede variar en la proyección del MEL.

De esta forma, el holograma registrado por la CCD se representa como:

$$H_l(u, v) = |D_l(u, v)|^2 + |P(u, v)|^2 + D_l(u, v)P^*(u, v)e^{2\pi i(\alpha\lambda fu, \beta\lambda fv)} + D_l^*(u, v)P(u, v)e^{-2\pi i(\alpha\lambda fu, \beta\lambda fv)} \quad (2.28)$$

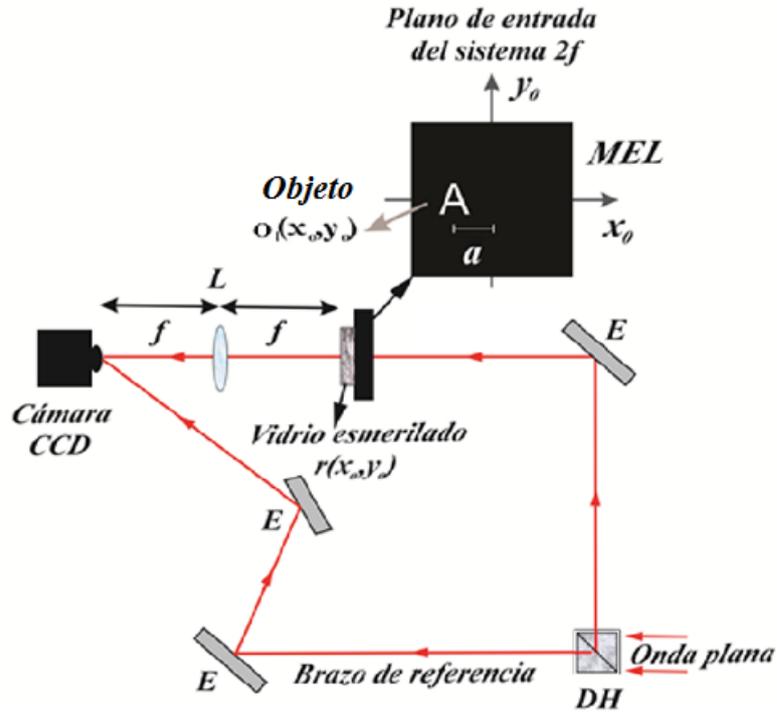


Figura 2.6: Esquema interferométrico de Fourier fuera de eje (DH: divisor de haz, E: espejo, MEL: modulador espacial de luz, L: lente de longitud focal f).

donde $D_l(u, v)$ es la TF de $d_l(x_0, y_0)$, λ la longitud de onda, $*$ es el complejo conjugado, $P(u, v) = e^{2\pi i(\alpha\lambda f u + \beta\lambda f v)}$ representa la onda plana de referencia en las coordenadas frecuenciales $u = x_0/\lambda f$ y $v = y_0/\lambda f$ donde $\alpha = \cos\theta/\lambda$ y $\beta = \cos\varphi/\lambda$ son los cosenos directores [5]. Estos ángulos directores se pueden modificar experimentalmente por medio de los espejos E del brazo de referencia (Figura 2.6).

Si se aplica una operación TF sobre la intensidad representada por la ecuación (2.28), se obtiene la distribución de intensidad que se muestra en la Figura 2.9 y se representa como:

$$\begin{aligned}
 TF\{H_l(u, v)\} = & d_l(x', y') \otimes d_l^*(x', y') + p(x', y') \otimes p^*(x', y') + \\
 & d_l(x', y') \otimes \delta(x' + \alpha\lambda f, y' + \beta\lambda f) \otimes \delta(x' - a, y') + \\
 & d_l^*(x', y') \otimes \delta(x' - \alpha\lambda f, y' - \beta\lambda f) \otimes \delta(x' + a, y')
 \end{aligned} \tag{2.29}$$

donde 1+2 son los órdenes centrales correspondientes a los dos primeros términos de la ecuación (2.29), mientras los órdenes 3 y 4 son los dos últimos términos de (2.29) respectivamente. Para poder eliminar la información redundante se debe filtrar el holograma del objeto procesado, y obtener un solo término, como se ilustra en la Figura 2.7.

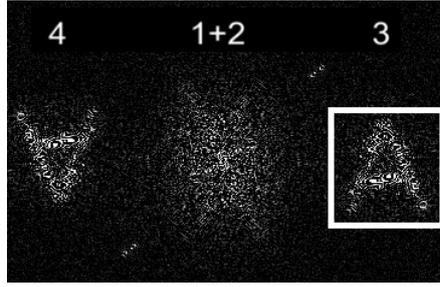


Figura 2.7: Distribución de intensidad asociada a la ecuación (2.29).

Para realizar el filtrado del holograma, primero se debe bloquear el brazo de referencia y se registra la intensidad de la TF de $d_l(x_0, y_0)$ ($|D_l(u, v)|^2$), luego se obstruye el brazo objeto y se registra la intensidad de la onda de referencia $|P(u, v)|^2$. Estos términos son restados de la ecuación (2.28), obteniendo así:

$$Q_l(u, v) = D_l(u, v)P^*(u, v)e^{2\pi i(\alpha\lambda fu, \beta\lambda fv)} + D_l^*(u, v)P(u, v)e^{-2\pi i(\alpha\lambda fu, \beta\lambda fv)} \quad (2.30)$$

Ahora se procede a filtrar uno de los términos de la ecuación anterior, para lograrlo se realiza la transformada de Fourier de (2.30), y de esta forma se obtienen dos términos separados espacialmente como se observa en la ecuación (2.31), y se representan en la Figura 2.9 como las distribuciones 3 y 4.

$$TF\{Q_l(u, v)\} = d_l(x', y') \otimes \delta(x' + \alpha\lambda f, y' + \beta\lambda f) \otimes \delta(x' - a, y') + d_l^*(x', y') \otimes \delta(x' - \alpha\lambda f, y' - \beta\lambda f) \otimes \delta(x' + a, y') \quad (2.31)$$

donde la separación entre los dos términos de la ecuación (2.31) es proporcional a $|a|$, el cual es un parámetro que se controla durante la proyección del objeto de entrada en el MEL. Este valor es cuidadosamente escogido para prevenir cualquier solapamiento entre los términos de la ecuación (2.31). Ahora, se filtra solo el tercer término, resultando:

$$n_l(x', y') = d_l(x', y') \otimes \delta(x' + \alpha\lambda f, y' + \beta\lambda f) \otimes \delta(x' - a, y'), \quad (2.32)$$

y se aplica una operación TF sobre $n_l(x', y')$, produciendo:

$$N_l(u, v) = D_l(u, v)e^{2\pi i(\alpha\lambda fu + \beta\lambda fv)}e^{-2\pi iau} \quad (2.33)$$

El término representado por la ecuación (2.33), se define como *dato de campo óptico*. Este término contiene la información a partir de la cual se puede recuperar la información de interés. Luego, el dato de campo óptico se multiplica por la máscara aleatoria $R_1(u, v)$, resultando de esta manera el dato encriptado $E_l(u, v)$.

$$E_l(u, v) = [D_l(u, v)e^{2\pi i(\alpha\lambda fu + \beta\lambda fv)}e^{-2\pi iau}]R_1(u, v) \quad (2.34)$$

La etapa de descryptación consta de multiplicar (2.34) por el conjugado de la llave de encriptación $R_1^*(u, v)$, y una posterior TFI, permite recuperar la información del objeto dada por la ecuación (2.35).

$$u_l(x, y) = d_l(x, y) \otimes \delta(x + a + \lambda f \alpha, y + \lambda f \beta) \quad (2.35)$$

De la ecuación (2.35) se observa la dependencia de la posición del objeto recuperado con los ángulos directores de la onda de referencia α y β , y la distancia entre el objeto y el eje óptico en el plano de entrada $|a|$. Estos parámetros se pueden manipular experimentalmente con el fin de evitar la superposición espacial de los cuatro órdenes que se obtienen (ecuación (2.29) y la Figura 2.9), y poder realizar un filtrado del término de interés. Usando como base lo descrito en esta sección, a continuación se describe el procesamiento de encriptación de un objeto por medio de un sistema análogo-digital *JTC*.

2.4. Encriptación de doble máscara de fase con un sistema análogo-digital JTC

En el sistema de encriptación basado en la arquitectura *JTC*, el plano de entrada está constituido por el objeto que se va a encriptar $o_l(x_o, y_o)$ y la ventana de la llave, el cual se pone en contacto con un difusor $r(x_o, y_o)$ (Figura 2.8). El objeto y la ventana llave son proyectados en un modulador espacial de luz, y la llave de seguridad $r_2(x_o, y_o)$ es la región del difusor limitada por la ventana de la llave.

Para encriptar el objeto con el sistema experimental mostrado en la Figura 2.8 se llevan a cabo los siguientes pasos. Primero se bloquea el brazo de referencia, de esta forma la lente genera la TF del plano de entrada sobre la CCD, registrando el *JPS* que se expresa como:

$$\begin{aligned} JPS(\mu, \nu) = & |C_l(\mu, \nu)|^2 + |R_2(\mu, \nu)|^2 \\ & + C_l(\mu, \nu)R_2^*(\mu, \nu)e^{4\pi i b \mu} + C_l^*(\mu, \nu)R_2(\mu, \nu)e^{-4\pi i b \mu} \end{aligned} \quad (2.36)$$

donde $2b$ es la distancia de separación de la ventana llave y el objeto, $C_l(\mu, \nu)$ es la TF de $o_l(x_o, y_o)r(x_o, y_o)$, y $R_2(\mu, \nu)$ es la TF de la llave de encriptación $r_2(x_o, y_o)$.

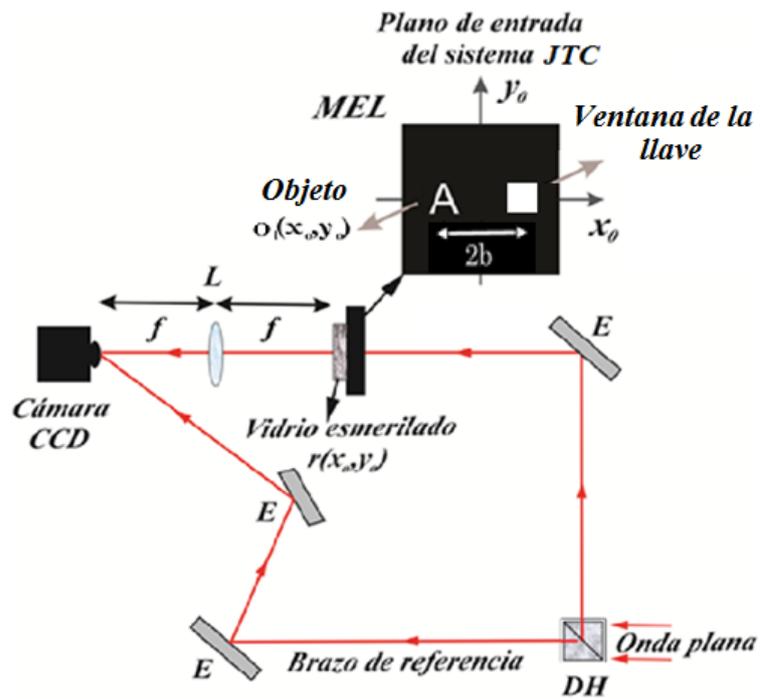


Figura 2.8: Esquema del criptosistema JTC de Fourier fuera de eje (DH: divisor de haz, MEL: modulador espacial de luz, E: espejo y L lente de longitud focal f.)

De igual forma que en el sistema de encriptación $2f$, si se lleva a cabo un operación TF sobre la intensidad registrada, en este caso el JPS (2.36), se obtiene cuatro términos de intensidad (ver Figura 2.9):

$$TF\{JPS(\mu, \nu)\} = c_1(x, y) \otimes c_1^*(x, y) + r_2(x, y) \otimes r_2^*(x, y) + c_1(x, y) \otimes r_2^*(x, y) \otimes \delta(x + 2b, y) + c_1^*(x, y) \otimes r_2(x, y) \otimes \delta(x - 2b, y), \quad (2.37)$$

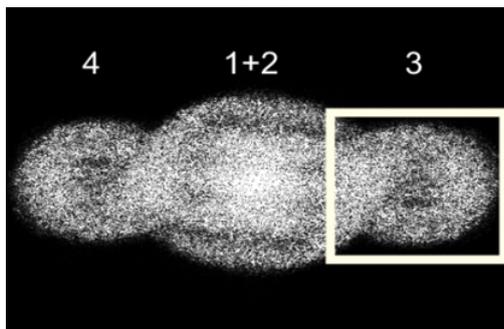


Figura 2.9: Distribución de intensidad asociada a la ecuación (2.37).

Para retener el dato encriptado contenido en el *JPS*, se bloquea el brazo de referencia y en el plano de entrada se obstruye la llave, de esta manera se registra la intensidad de la TF de $o_l(x_o, y_o)r(x_o, y_o) (|C_l(\mu, \nu)|^2)$. Luego se obstruye brazo del sistema *JTC* y se registra la intensidad de la TF de la llave $|R_2(\mu, \nu)|^2$. Posteriormente, estas intensidades se restan de la ecuación (2.36), resultando en:

$$u_l(x, y) = c_l(x, y) \otimes r_2^*(x, y) \otimes \delta(x + 2b, y) + c_l^*(x, y) \otimes r_2(x, y) \otimes \delta(x - 2b, y), \quad (2.38)$$

Luego, se descarta el segundo término y se retiene el primero, obteniéndose:

$$u_l(x, y) = c_l(x, y) \otimes r_2^*(x, y) \otimes \delta(x + 2b, y), \quad (2.39)$$

y una posterior TF, permite obtener el dato encriptado:

$$E_l(\mu, \nu) = C_l(\mu, \nu)R_2^*(\mu, \nu)e^{4\pi ib\mu} \quad (2.40)$$

La ecuación (2.40) representa el dato de campo óptico que es obtenido después del proceso de filtrado de cada *JPS*. Este término contiene la información a partir de la cual se puede recuperar la información de interés.

Para recuperar la información original a partir del dato encriptado, se procede a registrar la información de la llave de la seguridad. Primero, se desbloquea el brazo de referencia y se bloquea el brazo del sistema *JTC*, para registrar la intensidad de la onda plana de referencia dada por $|P(\mu, \nu)|^2$. Luego, los dos brazos del interferómetro se mantienen desbloqueados mientras que en el plano de entrada se obstruye el objeto $o_l(x_0, y_0)$ para registrar el holograma de la llave $H_{ll}(\mu, \nu)$, dado por:

$$H_{ll}(\mu, \nu) = |P(\mu, \nu)|^2 + |R_2(\mu, \nu)|^2 + P(\mu, \nu)R_2^*(\mu, \nu)e^{2\pi i(\alpha\lambda f\mu + \beta\lambda f\nu)} + P^*(\mu, \nu)R_2(\mu, \nu)e^{-2\pi i(\alpha\lambda f\mu + \beta\lambda f\nu)} \quad (2.41)$$

Luego, se resta de la ecuación (2.41) la intensidad de la llave y la intensidad de la onda de referencia, después de aplicar una TF se obtiene:

$$h(x, y) = p(x, y) \otimes r_2^*(x, y) \otimes \delta(x + \alpha\lambda f, y + \beta\lambda f) + p^*(x, y) \otimes r_2(x, y) \otimes \delta(x - \alpha\lambda f, y - \beta\lambda f) \quad (2.42)$$

Descartando el primer término y centrando el término restante se genera:

$$h'(x, y) = r_2(x, y) \quad (2.43)$$

Finalmente se aplica una operación TF sobre la última expresión para obtener la llave de descifrado $R_2(\mu, \nu)$. A continuación para descifrar la información, se procede a multiplicar el dato encriptado (2.40) con $R_2(\mu, \nu)$ y se realiza una posterior TF, obteniéndose:

$$D(x, y) = [o_l(x, y)r(x, y)] \otimes [r_2^*(x, y) \otimes r_2(x, y)] \otimes \delta(x + 2b, y) \quad (2.44)$$

Aplicando la aproximación $r_2^*(x, y) \otimes r_2(x, y) \approx \delta(x, y)$ [23], finalmente se obtiene:

$$D(x, y) = [o_l(x, y)r(x, y)] \otimes \delta(x + 2b, y) \quad (2.45)$$

Esta ecuación representa el producto entre el objeto original y una máscara de fase aleatoria, producto ubicado en las coordenadas $(x + 2b, y)$. Si un usuario no autorizado intenta recuperar el objeto empleando una llave $r_3(x, y)$ distinta a la llave de encriptación, el término $r_2^*(x, y) \otimes r_3(x, y)$ no se puede aproximar a una $\delta(x, y)$, por lo tanto la información no se logra recuperar, lo que se obtiene es un patrón aleatorio ya que la información permanece encriptada [20]. En la ecuación (2.44) se observa la dependencia de la posición en la que se recupera el objeto con el parámetro b , el cual se puede manipular a la hora de proyectar el objeto y la ventana llave en el MEL.

Teniendo en cuenta las ventajas que ofrecen los sistemas análogo-digitales para encriptar un objeto, se pueden desarrollar técnicas basadas en estos sistemas para procesar múltiples datos. De esta manera, la combinación de los sistemas análogo-digitales descritos con las técnicas de multiplexado, permite un manejo seguro y eficiente de múltiples datos. A continuación se describe la técnica de multiplexado.

2.5. Multiplexado de la información procesada por sistemas de encriptación análogo-digitales

Las técnicas de multiplexado permiten adicionar N datos en uno solo, conocido usualmente como el multiplexado o paquete; el multiplexado de datos ha sido utilizado con el fin de dar una mayor seguridad a los datos encriptados, los cuales pueden ser recuperados al usar las llaves adecuadas [3,9–11,13–17]. En esta sección se describe el proceso de multiplexado y recuperación de múltiples datos por medio de los sistemas de encriptación $2f$ y JTC .

2.5.1. Multiplexado para información procesada en un sistema de encriptación $2f$

En la sección 2.3 se describió como se encripta y recupera un solo objeto. Si se tienen N objetos procesados por el mismo esquema y encriptados con una misma llave $R_1(u, v)$, se obtiene el paquete de datos encriptados esta dado por:

$$M_l(u, v) = \sum_{l=1}^N E_l(u, v) = \sum_{l=1}^N [D_l(u, v) e^{2\pi i(\alpha\lambda f u + \beta\lambda f v)} e^{-2\pi i a u}] R_1(u, v) \quad (2.46)$$

donde $E_l(u, v)$ representa el dato de campo óptico del l -ésimo dato encriptado (ecuación (2.34)). Para recuperar los objetos encriptados, el paquete se multiplica por el complejo conjugado de la llave de seguridad y se aplica una TF, obteniéndose:

$$m_l(x, y) = \sum_{l=1}^N u_l(x, y) = \sum_{l=1}^N [d_l(x, y) \otimes \delta(x + a + \alpha\lambda f, y + \beta\lambda f)] \quad (2.47)$$

donde $d_l(x, y) = o_l(x_o, y_o) r(x_o, y_o)$. De acuerdo a la ecuación anterior, todos los datos se recuperan en las mismas coordenadas, es decir, que en el plano de recuperación se superponen todos los datos. Otro esquema de multiplexado consiste en procesar todos los datos con el mismo sistema $2f$, pero encriptar cada uno de ellos con una llave distinta. Si bajo este esquema se desea recuperar el l -ésimo dato a partir del multiplexado de datos encriptados, en el plano de recuperación se genera un campo de la forma:

$$m_l(x, y) = \sum_{l=1}^N u_l(x, y) = d_l(x, y) \otimes \delta(x + a + \alpha\lambda f, y + \beta\lambda f) \quad (2.48)$$

$$+ \sum_{m=1, m \neq l}^N d_m(x, y) \otimes \delta(x + a + \alpha\lambda f, y + \beta\lambda f) \otimes [r_{1m}^*(x, y) \otimes r_{1l}(x, y)]$$

El primer término de la ecuación representa el l -ésimo dato recuperado, mientras que el segundo término muestra que los demás datos permanecen encriptados debido a que las llaves de encriptación son diferentes y por lo tanto el término $r_{1m}^*(x, y) \otimes r_{1l}(x, y)$ no puede aproximarse a una función $\delta(x, y)$. En este caso, el ruido generado por el segundo término se superpone con el dato recuperado. A continuación, se ilustran los dos esquemas de multiplexado para el caso de datos encriptados en un sistema JTC .

2.5.2. Multiplexado para información procesada en un sistema de encriptación JTC

De igual manera se realiza la representación matemática del multiplexado para N objetos procesados por un sistema de encriptación JTC (sección 2.4). Cuando se encriptan todos los

objetos con una misma llave y se multiplexan, el paquete de datos encriptados adquiere la forma:

$$M_l(\mu, \nu) = \sum_{l=1}^N E_l(\mu, \nu) = \sum_{l=1}^N [C_l(\mu, \nu) R_2^*(\mu, \nu) e^{4\pi i b \mu}] \quad (2.49)$$

y su respectiva recuperación se representa como (ecuación (2.45)):

$$m_l(x, y) = \sum_{l=1}^N D_l(x, y) = \sum_{l=1}^N [o_l(x, y) r(x, y)] \otimes \delta(x + 2b, y) \quad (2.50)$$

En este caso, aunque todos los objetos se desencriptan simultáneamente, se superponen en el plano de recuperación. En el segundo esquema los datos se encriptan con llaves distintas, por lo tanto la recuperación se representa como:

$$\begin{aligned} m_l(x, y) &= \sum_{l=1}^N D_l(x, y) = [o_l(x, y) r(x, y)] \otimes \delta(x, y) \otimes \delta(x + 2b, y) \\ &+ \sum_{m=1, m \neq l}^N [o_m(x, y) r(x, y)] \otimes [r_{2m}^*(x, y) \otimes r_{2l}(x, y)] \otimes \delta(x + 2b, y) \end{aligned} \quad (2.51)$$

Acá se identifican dos términos, el primero es la l -ésima imagen desencriptada correctamente, y el segundo término es la contribución de ruido debido al producto convolutivo entre $[o_m(x, y) r(x, y)]$ con dos llaves distintas $[r_{2m}^*(x, y) \otimes r_{2l}(x, y)]$.

En conclusión, durante el proceso de recuperación de datos que han sido multiplexados, se llegan a presentar dos situaciones que generan ruido sobre la información recuperada:

1. Cuando todos los objetos son encriptados con la misma llave de seguridad y luego son multiplexados, se genera la superposición de todos los objetos en el plano de recuperación.
2. Cuando cada objeto se encripta con una llave de seguridad diferente, a la hora de recuperar uno de los objetos con su respectiva llave, éste se superpone con los demás objetos que permanecen encriptados.

En ambos casos, en el proceso de recuperación se presenta un deterioro parcial o total de la información, a su vez, siguiendo el procedimiento descrito no hay manera de recuperar todas los datos al mismo tiempo sin que se presente solapamiento. En consecuencia, recientemente se lograron desarrollar técnicas que permiten recuperar todos los objetos multiplexados al mismo tiempo y en el mismo plano, evitando el problema de ruido debido a la superposición [15, 16].

En la primera propuesta [15], cada dato fue procesado ópticamente y registrado holográficamente, seguido de un proceso de filtrado y de *posicionamiento* que permitió asignarle una coordenada particular en el plano de recuperación a cada dato. Además todos los datos ya procesados,

filtrados y posicionados se multiplexaron para obtener un solo paquete. Por último con el fin de proteger el paquete, éste se multiplicó por una llave. El proceso de recuperación consistió en multiplicar el paquete encriptado y el conjugado de la llave, para luego aplicar una transformada de Fourier usando un sistema óptico virtual $2f$. Este procedimiento permitió recuperar todos los datos procesados sin que se presentara ningún tipo de superposición. La segunda propuesta [16], usó la técnica de *modulación theta* para ubicar cada dato de campo óptico en una posición particular [24]. En este caso, la posición de cada dato en el plano de recuperación depende de la frecuencia y la orientación de la red moduladora. Luego los datos modulados se multiplexan para generar un paquete, el cual es encriptado. En esta técnica, todos los datos también son recuperados sin presentar ningún tipo de superposición. Es importante resaltar que ambas técnicas tienen la capacidad de ubicar el dato de campo óptico en cierta posición específica, sin necesidad de alterar la configuración del montaje experimental o adicionar elementos, permitiendo desencriptar múltiples datos en un mismo plano sin que se presente superposición.

Este capítulo abarca toda la información necesaria concerniente al procesamiento de información por medio de sistemas análogo-digitales para el manejo seguro de la información. De esta forma, sirve como herramienta fundamental para el entendimiento de lo que se presentará en cada uno de los siguientes capítulos.

Hasta acá, se ha mencionado como recuperar información sin solapamiento y con menos ruido gracias a la implementación de la técnica de posicionamiento o modulación junto con el multiplexado, pero es de interés poder recuperar la información completamente libre de ruido. Por lo tanto en el siguiente capítulo se presenta una nueva propuesta que permite recuperar múltiple información sin ningún ruido. Allí se utilizará un sistema de encriptación $2f$ con registro de Fourier fuera de eje, para el manejo de mensajes de manera segura y eficiente con ayuda del multiplexado por posicionamiento y de los códigos QR como contenedores de información.

- [1] M.S. Millán, E. Pérez-Cabré. *Optical data encryption Optical and Digital Image Processing: Fundamentals and Applications*. ed G. Cristóbal, P Schelkens and H Thienpont, 2011.
- [2] E. Rueda, J.F. Barrera, R. Henao, R. Torroba. *Optical encryption with a reference wave in a joint transform correlator architecture*. *Opt. Commun.*, 282:3243 – 3249, 2009.
- [3] E. Rueda, J.F. Barrera, R. Henao, R. Torroba. *Lateral shift multiplexing with a modified random mask in a joint transform correlator encrypting architecture*. *Opt. Eng.*, 48:027006, 2009.
- [4] E. Rueda, C. Rios, J.F. Barrera, R.Henao, R. Torroba. *Experimental multiplexing approach via code key rotations under a joint transform correlator scheme*. *Opt. Commun.*, 284:2500 – 2504, 2011.
- [5] J.W Goodman. *Introduction to Fourier Optics*. McGraw-Hill, 2nd edition, 1996.
- [6] C. S. Weaver, J. W. Goodman. *A Technique for Optically Convolving Two Functions*. *Appl. Opt.*, 5:1248–1249, 1966.
- [7] Y. Morimoto B. Javidi T. Nomura, S. Mikan. *Secure optical data storage with random phase key codes by use of a configuration of a joint transform correlator*. *Appl. Opt.*, 42:1508–1514, 2003.
- [8] T. Nomura, B. Javidi. *Optical encryption using a joint transform correlator architecture*. *Opt. Eng.*, 39:2031–2035, 2000.

-
- [9] G.i Situ, J. Zhang. *Multiple-image encryption by wavelength multiplexing*. Opt. Lett., 30:1306–1308, 2005.
- [10] J.F. Barrera, R. Henao, M. Tebaldi, R. Torroba, N. Bolognini. *Multiplexing encrypted data by using polarized light*. Opt. Commun., 260:109–112, 2006.
- [11] D. Amaya, M. Tebaldi, R. Torroba, N. Bolognini. *Multichanneled puzzle-like encryption*. Opt. Commun., 281:3434–3439, 2008.
- [12] D. Amaya, M. Tebaldi, R. Torroba, N. Bolognini. *Digital color encryption using a multi-wavelength source and a joint transform correlator*. In *6th Ibero-American Conference on Optics (RIO) 9th Latin-American Meeting on Optics, Lasers and Applications (OPTILAS)*, volume 992, pages 1083–1087, 2008.
- [13] F. Mosso, J.F. Barrera, M. Tebaldi, N. Bolognini, R. Torroba. *All-optical encrypted movie*. Opt. Exp., 19:5706–5712, 2011.
- [14] J.F. Barrera, M. Tebaldi, C. Ríos, E. Rueda, N. Bolognini, R. Torroba. *Experimental multiplexing of encrypted movies using a JTC architecture*. Opt. Exp., 20:3388–3393, 2012.
- [15] J. F. Barrera, S. Trejos, M. Tebaldi, R. Torroba. *Experimental protocol for packaging and encrypting multiple data*. J. Opt., 15:055406, 2013.
- [16] S. Trejos, J.F. Barrera, M. Tebaldi, R. Torroba. *Experimental opto-digital processing of multiple data via modulation, packaging and encryption*. J. Opt., 16:055402, 2014.
- [17] K. Singh G. Unnikrishnan, J. Joseph. *Optical encryption system that uses phase conjugation in a photorefractive crystal*. Appl. Opt., 37:8181–8186, 1998.
- [18] O. Kafri, E. Keren. *Encryption of pictures and shapes by random grids*. Opt. Lett., 12:377–379, 1987.
- [19] M. Françon. *Information processing using speckle patterns*. Laser Speckle and Related Phenomena. Springer-Verlag, New York, 1975.
- [20] Edgar Alberto Rueda Muñoz. *Encriptación y Desencriptación Dinámica de Información por Medios Ópticos-Digitales*. Universidad de Antioquia, 2009.
- [21] M.S. Millán. *Advanced optical correlation and digital methods for pattern matching -50th anniversary of Vander Lugt matched filter*. J. Opt., 14, 2012.
- [22] P.P. Banerjee G. Nehmetallah. *Applications of digital and analog holography in three-dimensional imaging*. Adv. Opt. Photon., 4:472–553, 2012.

-
- [23] J. Villardi, M. Millan, E. Perez-Cabre. *Improved decryption quality and security of a joint transform correlator based encryption system*. *J. Opt.*, 15:025401, 2013.
- [24] J. D. Armitage, A. W. Lohmann. *Theta Modulation in Optics*. *Appl. Opt.*, 4:399–405, 1965.

CAPÍTULO 3

PROTOCOLO ANÁLOGO-DIGITAL PARA EL MANEJO SEGURO DE MENSAJES CON RECUPERACIÓN LIBRE DE RUIDO

Como se mencionó en el capítulo anterior, cuando se aplican técnicas de multiplexado sobre datos procesados por sistemas ópticos, se presenta superposición de información en el plano de recuperación. Es decir, cuando se lleva a cabo el procedimiento que permite recuperar uno de los datos contenidos en el multiplexado, en el plano de recuperación se obtiene el dato correspondiente, pero superpuesto con la información que generan de los datos que no fueron recuperados. En este caso, la información no recuperada representa ruido sobre el dato de interés. Adicional a la superposición, se debe considerar el ruido que presentan los datos recuperados debido al procesamiento óptico de la información. Esto implica que un procesamiento eficiente de múltiples datos debe incluir mecanismos que eviten la superposición y elimine o reduzca significativamente el ruido generado por el procesamiento óptico. En este capítulo se mostrará que la superposición puede evitarse mediante una técnica de posicionamiento [1] y que la información se puede recuperar sin ruido incluyendo una etapa codificación de la información.

En particular, cuando la información se procesa por medio de sistemas que usan elementos físicos aleatorios, el ruido generado sobre la información recuperada debida al procesamiento óptico proviene principalmente de estos elementos. Este ruido representó un obstáculo significativo en el área de la encriptación óptica de información [1–10]. Para superar esta limitación, se propuso emplear códigos de respuesta rápida QR como contenedores de la información [11].

Esta propuesta fue demostrada por medio de un sistema de encriptación $4f$, donde primero se codificó la información en un código QR y luego este código fue encriptado. Al final, pese a que el código es recuperado con el ruido usual debido al procesamiento óptico, él puede ser leído por dispositivos que actualmente son de uso masivo y están ampliamente disponibles, como los teléfonos inteligentes o las tabletas [12], esto gracias a que los códigos QR son tolerantes a pérdidas, desalineación y degradación.

La posterior demostración experimental del uso de códigos QR para eliminar el ruido en la información recobrada, se llevó a cabo con un sistema de encriptación *JTC* [13]. Debido a que el sistema experimental tiene un límite de resolución, no se puede procesar todo el código QR en un mismo paso, por lo tanto el código se dividió en varias secciones y luego cada sección fue procesada por el sistema óptico. Además, mediante la selección adecuada de las coordenadas de posicionamiento de cada partición procesada, fue posible producir un multiplexado de las secciones encriptadas, que al ser sometido a un procedimiento correcto de desencriptación condujo a la recuperación del código QR que contiene la información. En general, el número de divisiones para la reconstrucción satisfactoria de un objeto depende de su contenido de frecuencias espaciales. Finalmente, para hacer más simple y rápido el proceso de lectura o de decodificación, se llevó a cabo un proceso digital de binarización para obtener el código QR recuperado solo en blanco y negro, y así asegurar la lectura con cualquier dispositivo o programa de decodificación. Mediante la técnica descrita anteriormente se pueden encriptar objetos cuyas frecuencias espaciales superan el límite del sistema, dividiendo el objeto original en secciones cuyos detalles pueden ser resueltos satisfactoriamente. Si bien este método permitió superar el límite de resolución del sistema, no es útil si se desea procesar ópticamente un mensaje extenso, porque es necesario procesar una cantidad de datos proporcional a la longitud del mismo, lo cual puede resultar impráctico. Para ello se propuso e implementó experimentalmente un método novedoso, en el cual, procesando una cantidad limitada de datos fue posible enviar mensajes encriptados de longitud arbitraria por medio de dos llaves que garantizaron la seguridad del mensaje [14].

La técnica consistió en proyectar por separado, en la ventana objeto del sistema de encriptación *JTC*, cada uno de los símbolos que componen un teclado, utilizando la misma llave de seguridad para la encriptación de cada símbolo. Los símbolos encriptados, fueron multiplexados para generar un teclado encriptado, el cual requiere la llave de seguridad para ser recuperado. Las posiciones de los símbolos en el plano de recuperación son asignadas después del proceso de encriptación. Una vez recuperado el teclado con la llave de seguridad, se procede a la recuperación del mensaje empleando una segunda llave, la cual es una secuencia de coordenadas

denominada llave coordinada. De esta manera, una vez el usuario autorizado accede al teclado descriptado, puede recuperar mensajes de cualquier longitud recibiendo solo la llave coordinada correspondiente a cada mensaje. Lo anterior demuestra que se pueden manipular apropiadamente múltiples datos que han sido procesados por un sistema análogo-digital de encriptación de arquitectura *JTC*, y además que es posible obtener una recuperación libre de ruido mediante el uso de códigos QR.

Por consiguiente, en este capítulo se presenta un nuevo protocolo que combina las ventajas que ofrecen los códigos QR y un sistema óptico $2f$ de encriptación para recuperar múltiples datos completamente libre de ruido y generar un protocolo donde se pueden transmitir y recibir múltiples mensajes de forma segura y eficiente. A continuación se da una breve descripción de los códigos QR y su procesamiento en un sistema de encriptación $2f$. Seguidamente, se describe el procesamiento de los códigos encriptados y su recuperación simultánea. Al final, se describe el proceso de binarización aplicado sobre los QR recuperados y se ilustra una aplicación que permite el intercambio seguro de mensajes en un ambiente multiusuario. Es importante tener en cuenta que los resultados presentados en este capítulo representan uno de los aportes originales de este trabajo de investigación y fueron publicados en una revista internacional [15].

3.1. ¿Qué es un código QR?

Un código QR (por las siglas en inglés: Quick Response code) es un código bidimensional compuesto de bloques en blanco y negro sobre una cuadrícula cuadrada. Estos códigos tienen una característica particular, poseen tres cuadrados que se encuentran en las esquinas que permiten que los dispositivos lectores de estos códigos los detecten rápidamente. La información codificada en estos códigos puede estar compuesta por algunos tipos estandarizados de datos como numéricos, alfanuméricos y byte / binario, o por medio de extensiones compatibles [16, 17]. Específicamente, los códigos QR han dirigido gran atención debido a su resistencia al ruido, entre otras características, haciéndolos muy apropiados para servir como contenedores de información [11].

Los códigos QR pueden emplearse como contenedores de la información en protocolos de protección de datos cuando se procesan en sistemas análogo-digitales de encriptación. En esta aplicación, el código QR descriptado contendrá el ruido intrínseco que genera el procesamiento óptico, pero puede ser leído, recuperándose de esta forma la información codificada en el QR sin ruido. De esta manera, los códigos QR ofrecen una solución práctica, representando una alter-

nativa válida para resolver el problema de ruido debido al procesamiento óptico, y haciendo más atractivo el uso de técnicas de encriptación óptica pues los códigos QR pueden ser escaneados por teléfonos inteligentes o tabletas con usando programas ampliamente disponibles [12, 18].

3.2. Descripción del proceso de encriptación de un código QR

Como el procesamiento óptico de un código QR no es posible en un solo paso, debido al límite de resolución de los sistemas ópticos [19], el código es dividido en nueve porciones de igual tamaño, donde cada porción es ubicada en el plano de entrada de un sistema $2f$ como se muestra en la Figura 3.1.

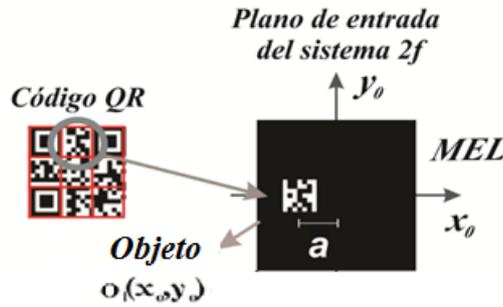


Figura 3.1: Plano de entrada que representa la proyección de una porción de un código QR en el MEL de un sistema de encriptación $2f$ (ver Figura 2.6).

La porción del código proyectada en el MEL (Figura 3.1) del sistema experimental de encriptación $2f$ (Figura 2.6), es procesada ópticamente, registrada y filtrada como se describe en la sección 2.3. De este modo, se obtiene el término filtrado de la porción del QR (ver ecuación (2.32)):

$$s_l(x', y') = d_l(x', y') \otimes \delta(x' + \alpha\lambda f, y' + \beta\lambda f) \otimes \delta(x' - a, y'), \quad (3.1)$$

con $d_l(x_o, y_o) = o_l(x_o, y_o)r(x_o, y_o)$, donde $o_l(x_o, y_o)$ es la porción a procesar ubicada en $-a$ en el plano de entrada, el cual está en contacto con un difusor $r(x_o, y_o)$. Ahora, la ecuación (3.1) que corresponde al término de la porción del QR procesado y filtrado, es *posicionado* en una coordenada deseada (x_l, y_l) . Esto es posible por que las dos funciones delta de Dirac se compactan en una sola función delta, asignando así una ubicación con coordenadas específicas. Así, la ecuación (3.1) se reescribe como:

$$f_l(x', y') = d_l(x', y') \otimes \delta(x' - x_l, y' - y_l), \quad (3.2)$$

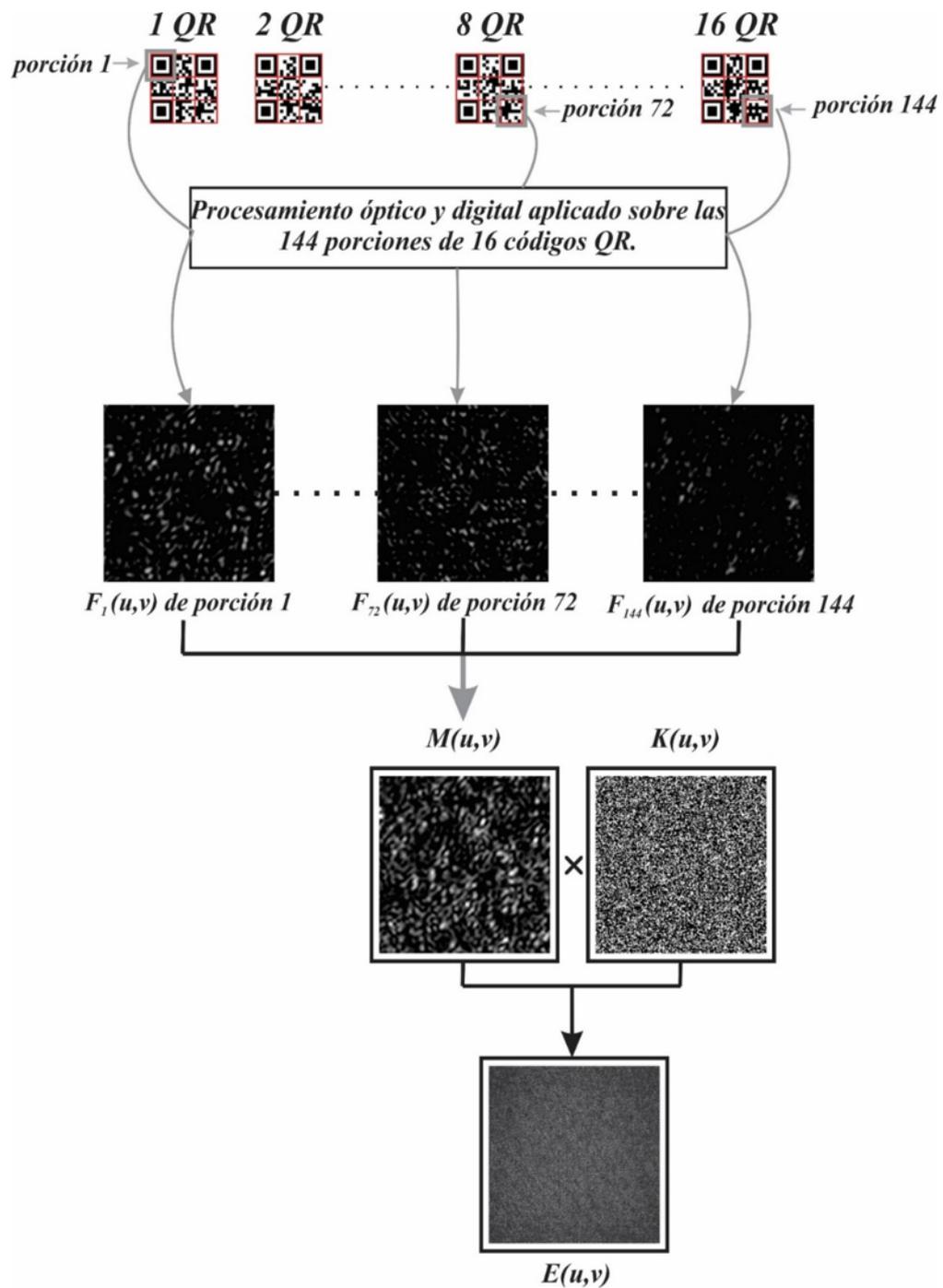


Figura 3.2: Procesamiento, multiplexado y encriptación de 144 porciones de códigos QR.

Posteriormente se aplica una TFI sobre (3.2) para completar el proceso de filtrado y posicio-

namiento [1]:

$$F_l(\mu, \nu) = D_l(\mu, \nu)e^{2\pi i(x_l\mu + y_l\nu)} \quad (3.3)$$

La última ecuación representa el proceso análogo-digital de la porción del código QR para obtener el respectivo dato de campo óptico. Siguiendo el mismo proceso descrito, se procesan las demás porciones del código para obtener los respectivos datos de campo óptico $F_l(\mu, \nu)$ (ver Figura 3.2). Las coordenadas de posicionamiento (x_l, y_l) son cuidadosamente escogidas y permiten localizar las porciones de los códigos QR recuperadas en el plano de salida. El proceso de posicionamiento es una herramienta de gran utilidad ya que se desea procesar múltiples códigos QR, y por lo tanto múltiples secciones de códigos QR, de manera que no se superpongan en el plano de recuperación.

3.3. Procesamiento de los múltiples códigos QR y encriptación

En este trabajo, se procesaron 16 códigos QR, donde cada uno se dividió en 9 porciones, por lo tanto se procesaron individualmente por separado 144 porciones (ver Figura 3.2). Los campos ópticos $F_l(\mu, \nu)$ correspondientes a cada porción procesada son obtenidos como se describe en la sección anterior. Finalmente los 144 campos ópticos se multiplexan y se obtiene un solo paquete de información $M(\mu, \nu)$ que se expresa como:

$$M(\mu, \nu) = \sum_{l=1}^{144} F_l(\mu, \nu) = \sum_{l=1}^{144} D_l(\mu, \nu)e^{2\pi i(x_l\mu + y_l\nu)} \quad (3.4)$$

El proceso de multiplexado, permite enviar toda la información en un solo paquete en lugar de enviar por separado cada uno de los datos procesados. Logrando así, una manipulación más compacta y eficiente de los múltiples datos. Durante el proceso, las coordenadas (x_l, y_l) son distintas para cada porción, para asegurar un correcto reensamblaje al recuperar todas las porciones y recuperar el código QR. El posicionamiento y el multiplexado descrito es una herramienta práctica en el manejo de múltiples datos sin necesidad de alterar la configuración del montaje experimental o de introducir otros elementos, como se evidencia en la ecuación (3.2).

Como paso final, se protege el paquete usando una máscara aleatoria de fase digital $K(\mu, \nu)$ (ver Figura 3.2), obteniéndose el paquete encriptado:

$$E(\mu, \nu) = M(\mu, \nu)K(\mu, \nu) \quad (3.5)$$

Este resultado y el complejo conjugado de la llave $K^*(\mu, \nu)$ se le envían por separado a los usuarios autorizados para que puedan recuperar la información. Todos recibirán el mismo

paquete encriptado y la llave, pero cada uno recibirá un llave de secuencia distinta dependiendo del mensaje que se le quiere entregar, como se mostrará más adelante.

3.4. Proceso de recuperación

Ahora, el usuario final aplica una multiplicación entre el paquete encriptado $E(\mu, \nu)$ y el conjugado de la llave $K^*(\mu, \nu)$, seguido de un operación TF (Figura 3.3 (a)), logrando recuperar todos los códigos en las posiciones determinadas. La recuperación de todos los códigos QR procesados es representada como:

$$m(x, y) = TF \{E(\mu, \nu)K^*(\mu, \nu)\} = \sum_{l=1}^{144} [o_l(x, y)r(x, y)] \otimes \delta(x - x_l, y - y_l) \quad (3.6)$$

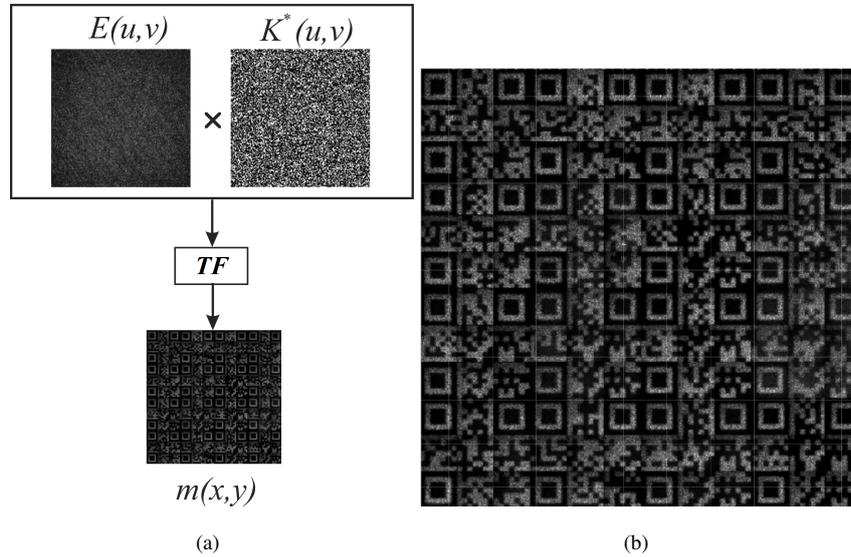


Figura 3.3: (a) Esquema para descriptar, recuperar y mostrar el paquete de códigos QR. (b) Imagen ampliada de la recuperación en (a).

Los códigos QR se recuperan en un solo paso, en el mismo plano, y simultáneamente (Figura 3.3 (b)). Se observa que los códigos QR se recuperan con el ruido asociado al procesamiento óptico con máscaras aleatorias de fase, por esta razón, se adiciona un proceso de binarización sobre los QRs recuperados para que puedan leídos con más facilidad y rapidez por cualquier dispositivo decodificador de códigos.

3.5. Resultados experimentales

Cada porción de los códigos QR fue procesada por el montaje experimental descrito en la Figura 2.6 del capítulo anterior, donde el plano de entrada está dado por la Figura 3.1. Se utiliza un láser de estado sólido que funciona a una longitud de onda de 632 nm . Se coloca un vidrio esmerilado en contacto con el modulador MEL, que proporciona la máscara aleatoria de fase. El área de la porción del QR proyectado en el MEL es de $6,4\text{ mm} \times 6,4\text{ mm}$. El MEL es un Holoeye LC2002, cuyo ancho de píxel es de $32\text{ }\mu\text{m}$. La distancia $|a|$ entre el objeto y el eje óptico en el plano de entrada es de $5,6\text{ mm}$.

El modulador se coloca a una distancia f de una lente positiva L de longitud focal $f = 200\text{ mm}$ y la cámara CCD se coloca de modo que la distancia entre la lente y el sensor sea igual a f . La resolución de la cámara es $3840\text{ píxeles} \times 2748\text{ píxeles}$ y el tamaño del píxel es $1,67\text{ }\mu\text{m} \times 1,67\text{ }\mu\text{m}$. Cada porción de un código QR es procesado por este montaje análogo, y luego es filtrado y posicionado digitalmente para obtener el campo óptico respectivamente (ver Figura 3.2).

Para la realización experimental, se manejaron 144 porciones (16 códigos QR), donde cada porción se procesó de acuerdo con la descripción de las secciones 3.2 y 3.3. Después de los pasos experimentales y digitales, se obtienen los códigos QR procesados listos para ser multiplexados y encriptados con la máscara de encriptación como se describió anteriormente. Es importante remarcar que la multiplexación contiene la información de todos los códigos QR procesados. Para recuperar los códigos QR, es necesario multiplicar el paquete encriptado con el complejo conjugado de la llave y luego realizar una operación TF (ver Figura 3.3 (a)). Seguidamente, se procede a realizar un proceso adicional de binarización sobre el panel de los códigos recuperados.

3.6. Proceso de binarización

Se incluye un proceso de binarización para obtener un QR en solo bloques de píxeles blancos y negros (ver Figura 3.4). Se divide cada código QR desencriptado en bloques, donde cada bloque contiene varios píxeles del código (Figura 3.4 (c)). Se promedia el valor de cada píxel en niveles de grises (Figura 3.4 (d)), y se determina un valor umbral de tal manera que los valores de gris por encima del umbral se convierten en blanco, y los valores de gris debajo del valor umbral se convierten en negro, generando así un código en solo bloques de blanco y negro o binarizado como se muestra en la Figura 3.4(e).

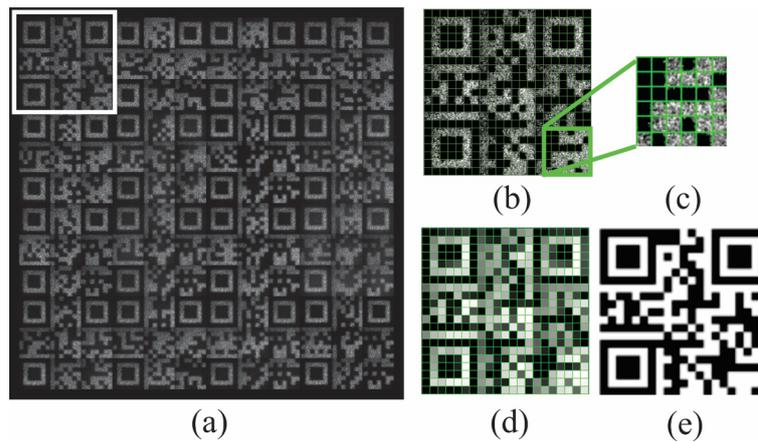


Figura 3.4: (a) Panel con todos los códigos QR recuperados, (b) un QR del panel correspondiente al cuadrado blanco en (a), (c) sección magnificada del QR en (b), (d) valor promedio de cada bloque en (b) (entre 0 y 255) y (e) QR recuperado ya binarizado.

Se espera que hayan algunas diferencias entre los códigos QR procesados y binarizados (Figura 3.5 (a)), y los QR originales antes de ser procesados (Figura 3.5 (b)), debido a los cambios sufridos por el QR durante la aplicación del proceso descrito en este capítulo. Para poder hacer evidente estas diferencias, se hace una comparación de la misma región del código original y del código recuperado binarizado. La Figura 3.5 (c) muestra claramente diferencias entre los códigos QR procesados y originales, a pesar de estas diferencias, la lectura de los códigos QR es exitosa debido a la tolerancia al ruido que exhibe la decodificación de los códigos QR.

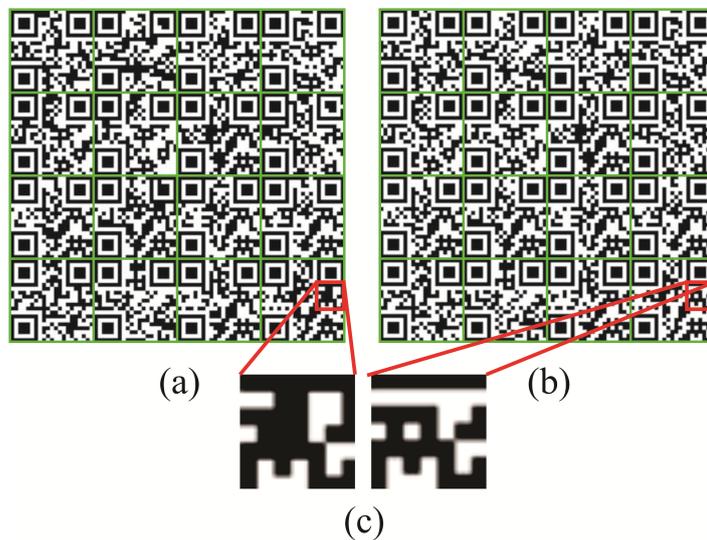


Figura 3.5: Panel con (a) los códigos QR procesados y binarizados y (b) los códigos QR originales, y (c) comparación de la misma región cuadrada del código QR en (a) y (b).

Finalmente, el mensaje oculto libre de ruido se puede recuperar mediante una secuencia sobre el panel de códigos QR binarizados (Figura 3.6 (a)). Por ejemplo la frase *PACKAGING AND CODING* se reconstruye sin rastros de ruido ni de degradación (<https://goo.gl/JqfMlw>), lo que implica que múltiples usuarios autorizados tienen acceso al mismo panel y al conjugado de la llave, pero a cada uno se le envía una llave de secuencia distinta y dependiendo de la secuencia obtendrá un mensaje diferente.

Por otro lado, comparando este nuevo protocolo con resultados obtenidos en los procedimientos de encriptación y manejo de múltiples datos estándar [1–10], se observa que los resultados finales en el mensaje recuperado presenta ruido de speckle y degradación el cual es generado por el procesamiento análogo-digital como se muestra en la Figura 3.6(b). Por lo tanto, se logra evidenciar la potencialidad del protocolo propuesto en este capítulo.



(a)



(b)

Figura 3.6: (a) Mensaje recuperado con el protocolo propuesto (<https://goo.gl/JqfMlw>), y (b) mensaje recuperado con el procedimiento clásico.

Lo anteriormente descrito y analizado en este capítulo, permite mostrar un nuevo protocolo multiusuario para el manejo seguro y eficiente de múltiple información, la cual fue encriptada por medio de un sistema $2f$ junto a una técnica holográfica de Fourier fuera de eje. Combinando dichos procesos análogos y digitales con la codificación de los códigos QR, se logró una recuperación de la información completamente libre de ruido. Cabe destacar que dichos resultados

fueron publicados en una revista internacional (ver Apéndice A).

Es necesario tener claro, que tanto las técnicas tradicionales, como la propuesta en este capítulo para procesar múltiples datos, requieren de una alta capacidad de almacenamiento y una mayor velocidad de transmisión, generando grandes volúmenes de información. Con dicho problema, surge la necesidad de generar propuestas que permitan manipular múltiples datos holográficos que ocupen menos volumen. Por eso, los próximos capítulos se enfocan en analizar y desarrollar nuevas técnicas que logren comprimir la información que se procesa en sistemas análogo-digitales.

- [1] J. F. Barrera, S. Trejos, M. Tebaldi, R. Torroba. *Experimental protocol for packaging and encrypting multiple data*. J. Opt., 15:055406, 2013.
- [2] B. Javidi, J.L. Horner. *Optical pattern recognition for validation and security verification*. Opt. Eng., 33:1752–1756, 1994.
- [3] P. Refregier, B. Javidi. *Optical image encryption based on input plane Fourier plane random encoding*. Opt. Lett., 20:767–769, 1995.
- [4] O. Matoba, B. Javidi. *Encrypted optical memory system using three-dimensional keys in the Fresnel domain*. Opt. Lett., 24:762–764, 1999.
- [5] T. Nomura, B. Javidi. *Optical encryption using a joint transform correlator architecture*. Opt. Eng., 39:2031–2035, 2000.
- [6] J.F. Barrera, E. Rueda, C. Ríos, M. Tebaldi, N. Bolognini, R. Torroba. *Experimental opto-digital synthesis of encrypted sub-samples of an image to improve its decoded quality*. Opt. Commun., 284:4350 – 4355, 2011.
- [7] J.F. Barrera, A. Vélez, R. Torroba. *Experimental multiplexing protocol to encrypt messages of any length*. J. Opt., 15:055404, 2013.
- [8] J.M. Vilarly, M.S. Millán, E. Pérez-Cabré. *Improved decryption quality and security of a joint transform correlator-based encryption system*. J. Opt., 15:025401, 2013.
- [9] S. Trejos, J.F. Barrera, M. Tebaldi, R. Torroba. *Experimental opto-digital processing of multiple data via modulation, packaging and encryption*. J. Opt., 16:055402, 2014.

-
- [10] W. Chen, B. Javidi, X. Chen. *Advances in optical security systems*. Adv. Opt. Photon., 6:120–155, 2014.
- [11] J.F. Barrera, A. Mira, R. Torroba. *Optical encryption and QR codes: Secure and noise-free information retrieval*. Opt. Exp., 21:5373–5378, 2013.
- [12] O. Graydon. *Cryptography: Quick response codes*. Nature Photonics, 7:343, 2013.
- [13] J.F. Barrera, A. Agudelo, R. Torroba. *Experimental QR code optical encryption: noise-free data recovering*. Opt. Lett., 39:3074–3077, 2014.
- [14] J.F. Barrera, A. Vélez, R. Torroba. *Experimental multiplexing protocol to encrypt messages of any length*. J. Opt., 15:055404, 2013.
- [15] S. Trejos, J.F. Barrera, R. Torroba. *Optimized and secure technique for multiplexing QR code images of single characters: application to noiseless messages retrieval*. J. Opt., 17:085702, 2015.
- [16] ISO, IEC 18004: 2006. *Information technology - Automatic identification and data capture techniques - QR Code 2005 bar code symbology specification*. International Organization for Standardization, Geneva, Switzerland, 2006.
- [17] K.C. Liao, W.H. Lee. *A novel user authentication scheme based on QR-Code*. J. Netw., 5:937–941, 2010.
- [18] E. Ohbuchi, H. Hanaizumi, L.A. Hock. *Barcode Readers Using the Camera Device in Mobile Phones*. In *Proceedings of the 2004 International Conference on Cyberworlds, CW '04*, pages 260–265, 2004.
- [19] J.W. Goodman. *Introduction to Fourier Optics*. McGraw-Hill, 2nd edition, 1996.

CAPÍTULO 4

REDUCCIÓN DE VOLUMEN DE DATOS ENCRIPTADOS ÓPTICAMENTE

La encriptación ha jugado un papel importante en el procesamiento óptico de información en los últimos años [1–3]. En el contexto de la encriptación óptica se pueden distinguir la etapa de encriptación, manipulación, envío, recepción, y finalmente la desencriptación de la información. En particular, cuando se manipulan de forma segura muchos datos, no sólo debe evitarse una eventual superposición durante la recuperación, sino que también es importante el manejo eficiente de la información para facilitar su almacenamiento, envío y recepción [4, 5]. En los procesos de protección de datos que usan sistemas ópticos de encriptación se debe manipular información holográfica. Cuando se procesan múltiples datos, la información holográfica que contiene los datos encriptados representa una cantidad significativa de datos que pueden ser combinados para conformar una única unidad o paquete de información [5].

El manejo eficiente de datos holográficos ya ha sido abordado mediante varias técnicas de compresión digital [6, 7]. En particular, se presentó una propuesta basada en varias técnicas digitales de compresión estándar y métodos digitales con pérdidas, como la cuantización, el remuestreo o disminución de tamaño del holograma, y la transformada discreta de Fourier, en vez de la transformada discreta coseno, dentro del algoritmo de compresión digital JPEG (por las siglas en inglés de: Joint Photography Expert Group) [6]. Los resultados muestran que la cuantización es una técnica muy efectiva para comprimir interferogramas digitales, mientras que el remuestreo digital no ha mostrado un buen rendimiento pues conduce a un submuestreo de las microfranjas holográficas. Desde otro punto de vista, algunos investigadores propusieron algunas alternativas

para el manejo eficiente de los datos obtenidos en sistemas ópticos. Por ejemplo, usar solo la fase del campo óptico permite reducir los requisitos de almacenamiento a la mitad, con una pérdida mínima de potencia óptica durante la reconstrucción [8]. El procesamiento en el dominio de Fourier representa otra táctica mediante el filtrado de los términos no relevantes contenidos en el holograma [9]. Aunque el filtrado es ampliamente usado en el procesamiento de hologramas para eliminar información redundante, no se ha abordado desde el punto de vista de la reducción del volumen de la información holográfica. Con este antecedente, de ahora en adelante se analizará el proceso de filtrado como un mecanismo, que no solo permite suprimir información no relevante, sino que además posibilita la reducción del volumen de la información generada en sistemas ópticos.

En este capítulo, primero se aborda una de las técnicas de compresión estándar, la cuantización, con el fin de reducir el volumen de los múltiples datos generados por medio de un sistema de encriptación $2f$, y registrados por un esquema holográfico de Fourier fuera de eje. En este caso, la cuantización no se aplica sobre el holograma registrado, sino que se aplica sobre el dato de campo óptico que se obtiene después de un procesado de filtrado. Con el proceso de filtrado, además de eliminar los términos no relevantes, se eliminan las microfranjas holográficas. En la primera sección, se describe el proceso de cuantización o variación de la profundidad de bits para obtener una reducción en el volumen de los datos experimentales.

Como la cuantización es una técnica de compresión digital, surgió la idea de crear una técnica con un nuevo enfoque, para reducir el volumen de los datos holográficos obtenidos en los montajes de encriptación. Si los datos que se tienen provienen de sistemas ópticos, ¿por qué no generar un método óptico de compresión que me permita reducir el volumen de los datos?. Para dar respuesta a esa pregunta, en la segunda sección de este capítulo se propone la técnica de escalado óptico para reducir el volumen de los datos. Entre las diferentes arquitecturas ópticas de encriptación, se elige la arquitectura de correlador de transformada de conjunta JTC para mostrar la eficiencia del método de compresión propuesto. Es importante tener presente que los resultados presentados en esta sección representan otro de los aportes originales de este trabajo de investigación y fueron publicados en una revista internacional [10].

El método óptico de compresión puede complementarse con técnicas de compresión digital para aumentar la eficiencia del proceso. Por lo tanto, en la tercera sección, se utilizan los datos obtenidos por el sistema de encriptación JTC , y se combinan los procesos de cuantización y escalado óptico. Esta combinación se compara con la técnica de escalado digital (ED) y cuanti-

zación [6].

4.1. Reducción del volumen por medio de la técnica de cuantización

La cuantización consiste en reducir la profundidad de bits de un dato, de esta forma se tiene un dato con una escala menor de bits y por lo tanto una reducción en su volumen. En esta sección, se presenta la reducción de volumen que resulta cuando la profundidad de los datos de campo óptico multiplexados se varía entre 8 bits y 2 bits de cuantización.

4.1.1. Procesamiento de múltiples datos y encriptación

En el montaje experimental de encriptación $2f$ se procesaron individualmente 100 objetos que corresponden a varias letras del alfabeto, números y símbolos del teclado latino. Cada carácter es ubicado individualmente en el plano de entrada del sistema de encriptación $2f$ ilustrado en el capítulo 2 Figura 2.6. Cada letra, número y símbolo es procesado de igual forma en que se procesó cada porción de un código QR (ver Figura 3.2), lo cual se describió en detalle en la sección 3.2. Por lo tanto, después de procesar cada carácter del teclado latino se obtiene el respectivo dato de campo óptico $F_l(\mu, \nu)$, que se representa (ecuación (3.3)):

$$F_l(\mu, \nu) = D_l(\mu, \nu)e^{2\pi i(x_l\mu + y_l\nu)} \quad (4.1)$$

Luego cada dato de campo óptico $F_l(\mu, \nu)$, se multiplexa con los demás campos óptico obtenidos, para generar un solo paquete de información $M(\mu, \nu)$:

$$M(\mu, \nu) = \sum_{l=1}^{100} F_l(\mu, \nu) = \sum_{l=1}^{100} D_l(\mu, \nu)e^{2\pi i(x_l\mu + y_l\nu)} \quad (4.2)$$

Seguidamente, se encripta el paquete $M(\mu, \nu)$ con la llave $K(\mu, \nu)$ para dar seguridad a los múltiples datos procesados, obteniéndose:

$$E(\mu, \nu) = M(\mu, \nu)K(\mu, \nu) \quad (4.3)$$

El paquete encriptado $E(\mu, \nu)$ es el dato que será comprimido usando la técnica de cuantización.

4.1.2. Cuantización y recuperación

El paquete encriptado $E(\mu, \nu)$ de la ecuación (4.3) posee 8 bits de profundidad, cuyo valor está asociado al registro con la cámara CCD. Luego se reduce la profundidad de bits a valores de

6 bits, 4 bits y finalmente a 2 bits de forma digital, de esta manera se obtiene el paquete $E(\mu, \nu)$ cuantizado.

Finalmente, el proceso de recuperación consiste en multiplicar el paquete encriptado $E(\mu, \nu)$ cuantizado y el conjugado de la llave $K^*(\mu, \nu)$, y una posterior transformada de Fourier (ver Figura 3.3), permite recuperar todos los objetos procesados y cuantizados sin que haya ningún tipo de superposición, como se mostrará a continuación.

4.1.3. Resultados experimentales

En el sistema análogo-digital de encriptación $2f$ (Figura 2.6), los 100 objetos fueron individualmente procesados y registrados usando una cámara CCD PULNIX TM6703 con 640 píxeles \times 480 píxeles de resolución, 8 bits de profundidad y un ancho de píxel de $9\mu m$. En este caso el volumen de datos se define como $X_c * Y_c * B_c$, donde X_c , y Y_c son la resolución horizontal y vertical respectivamente, y B_c la profundidad de bits del dispositivo de adquisición. De esta manera, cada holograma posee un volumen $V_H = 640 * 480 * 1Byte$ donde 1 Byte (B) = 8 bits, resultando en un volumen $V_H = 0,29MB$ por holograma ($MB=Megabytes$). Por lo tanto se tendrá un volumen inicial $V_I = 29MB$ de datos a procesar.

La primera etapa en la reducción de volumen consiste en aplicar el proceso de filtrado sobre cada holograma, proceso que consiste en retener solo uno de los términos de la distribución de intensidad que se presenta en la Figura 2.9 del capítulo 2. El área de filtrado, demarcada por el rectángulo de bordes blancos en la Figura 2.9 definirá el volumen del dato filtrado. En este caso la ventana tiene un tamaño de 100 píxeles \times 100 píxeles, y aplicando una TF sobre la ventana de filtrado, se obtiene el dato de campo óptico dado por la ecuación (2.33) generando un volumen $V = 2 * 100 * 100 * 1B = 0,019MB$ donde el factor de 2 se debe a la contribución de la amplitud y la fase producto del procesamiento del holograma. Ahora, estos 100 datos de campo óptico son multiplexados y ocupan un volumen total de $V_F = 1,9MB$, por lo tanto, el proceso de filtrado produce una reducción del volumen del 93,4% sobre el volumen inicial. La manera en que se multiplexaron todos los datos de campo óptico, no permite una recuperación de todos los objetos sin que haya superposición, como se demostró en la sección 2.5.1.

Por eso se aplicó sobre los datos filtrados, la técnica de posicionamiento para ubicarlos sobre una matriz de mayor tamaño como se describió en la sección 4.1.1. La cantidad de objetos procesados y el tamaño de la ventana de filtrado, son los que definen el tamaño de la matriz de posicionamiento. En este caso la ventana tiene un tamaño de 100 píxeles \times 100 píxeles, la cual se

posiciona sobre una matriz de tamaño de 1000 píxeles \times 1000 píxeles, y luego de una operación TF se obtiene el dato de campo óptico $F_l(\mu, \nu)$ (ecuación 4.1). El posterior multiplexado de los 100 campos ópticos y su encriptación, origina un paquete encriptado $E(\mu, \nu)$ con un volumen total de $V_{E(\mu, \nu)} = 2 * 1000 * 1000 * 1B = 1,9MB$.

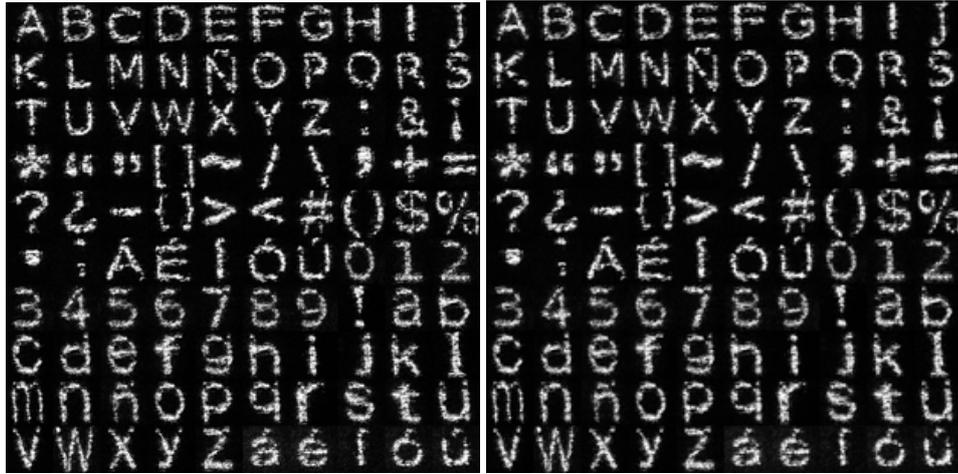
Como se puede notar, el volumen obtenido después del proceso de filtrado, y el volumen después del proceso de multiplexado y encriptación, son iguales, lo que implica que los procesos de multiplexado por posicionamiento y encriptación aplicados, no generan una reducción en el volumen. La ventaja de este proceso de multiplexado radica en que permite enviar toda la información en un solo paquete, en lugar de enviar por separado cada uno de los datos de campo óptico, además se pueden recuperar simultáneamente todos los objetos sin ninguna superposición. Por lo tanto, se puede afirmar que el multiplexado es un mecanismo mediante el cual múltiples datos se manipulan compacta y eficientemente.

Una vez obtenido el multiplexado encriptado, se aplica la técnica de cuantización sobre $E(\mu, \nu)$. El volumen que ocupa el paquete encriptado cuantizado se calcula como:

$$V = 2 * X_o * Y_o * S \quad (4.4)$$

donde $X_o = Y_o = 1000$ para valores de cuantización S de $1 B$ (8 bits), $0.75 B$ (6 bits), $0.5 B$ (4 bits) y $0.25 B$ (2 bits). De esta forma se obtuvo para un valor de cuantización de 6 bits un volumen $V_{E(u, v)}^{6bits} = 1,43MB$, a 4 bits un volumen $V_{E(u, v)}^{4bits} = 0,95MB$, y para 2 bits un volumen $V_{E(u, v)}^{2bits} = 0,47MB$. En la Figura 4.1 se muestra la recuperación para los distintos valores de cuantización.

Al observar los resultados de la Figura 4.1 (b) no se aprecia un deterioro sustancial sobre los objetos recuperados en comparación con la recuperación original (Figura 4.1 (a)), mientras que en las recuperaciones presentadas en las Figuras 4.1 (c) y (d) se evidencia una degradación de la recuperación. Como era de esperarse, a mayor reducción de volumen debida a la disminución en el número de bits, menor será la calidad de los objetos recuperados. Aunque la recuperación mostrada en la Figura 4.1 (c) no tiene la misma calidad que la recuperación original a 8 bits (Figura 4.1 (a)), en la Figura 4.1 (c) se pueden reconocer todos los objetos recuperados, por lo tanto se tendrá en cuenta el valor de volumen asociado a 4 bits de cuantización para analizar la eficiencia del método.



(a) 8 bits, $V_{E(u,v)}^{8bits} = 1,9MB$

(b) 6 bits, $V_{E(u,v)}^{6bits} = 1,43MB$



(c) 4 bits, $V_{E(u,v)}^{4bits} = 0,95MB$

(d) 2 bits, $V_{E(u,v)}^{2bits} = 0,47MB$

Figura 4.1: Recuperación de los 100 objetos para distintos valores de cuantización.

Para cuantificar la eficiencia de esta técnica de cuantización sobre los datos holográficos procesados, primero se cuantifica la reducción del volumen debido al proceso de filtrado. Para ello se define el *factor de reducción* como:

$$FR = V_I/V_F \quad (4.5)$$

Por consiguiente, el factor de reducción para 8 bits sobre los hologramas es de $FR = 29MB/1,9MB = 15$. Es de aclarar, que esta reducción de volumen esta asociada solo al pro-

ceso de filtrado. Este factor de reducción obtenido con 8 bits se puede aumentar con diferentes valores de profundidad de bits, como se indica en los datos recuperados. En el caso de una profundidad de 4 bits el factor de reducción es de $FR = 29MB/0,95MB = 30$ con respecto al volumen inicial. De esta manera el factor de reducción se logró duplicar cuantizando a 4 bits.

Ahora, se determina el factor de reducción a partir del proceso de filtrado, con el fin de cuantificar la compresión debido solo al proceso de cuantización a 4 bits. De esta forma, el factor de reducción es de $FR = V_F/V_{E(u,v)}^{4bits} = 1,9MB/0,95MB = 2$. Esto indica que el proceso de filtrado es el que más contribuye a la reducción de volumen, ya que su factor de reducción es de 15, mientras que la cuantización tiene un factor de reducción igual a 2. Los valores porcentuales de compresión asociados a cada proceso vienen dados por:

$$V_I = 29MB \Rightarrow 100\%$$

$$V_F = V_{E(u,v)}^{8bits} = 1,9MB \Rightarrow 6,6\% \text{ (una reducción de volumen del } 93,4\%)$$

$$V_{E(u,v)}^{4bits} = 0,95MB \Rightarrow 3,3\% \text{ (una reducción de volumen del } 96,7\%)$$

donde se evidencia que el proceso de cuantización a 4 bits solo aporta un 3,3% a la reducción de volumen.

En la siguiente sección se propone e implementa otra técnica de compresión. Esta técnica permite la reducción del volumen de datos de campo óptico de objetos procesados por un sistema de encriptación *JTC* y registrados holográficamente.

4.2. Reducción de volumen por medio de la técnica de escalado óptico

En esta sección se presenta una nueva propuesta para la reducción de volumen de datos holográficos. Esta propuesta posee un enfoque óptico, y se aplicará sobre los datos de campo óptico obtenidos por medio de un sistema de encriptación *JTC* y registrados por medio de un esquema de holografía de Fourier fuera de eje.

4.2.1. Procesamiento de un dato

En el montaje de encriptación *JTC* descrito por la Figura 2.8 del capítulo 2, se procesaron individualmente 16 objetos que corresponden a varios caracteres del teclado. Cada objeto $o_l(x_o, y_o)$ es ubicado en el plano de entrada junto a la llave de encriptación $r_2(x_o, y_o)$ separados una distancia $2b$, donde la CCD registra el respectivo *JPS*. Luego el *JPS* registrado y filtrado, como se describe en la sección 2.4, se representa como:

$$u_l(x, y) = c_l(x, y) \otimes r_2^*(x, y) \otimes \delta(x + 2b, y) \quad (4.6)$$

donde $c_l(x_o, y_o) = o_l(x_o, y_o)r(x_o, y_o)$ y $o_l(x_o, y_o)$ es el carácter. Ahora, el término de la ecuación (4.6) es *posicionado* en una coordenada escogida (x_l, y_l) . De esta forma (4.6) se reescribe como:

$$e_l(x, y) = c_l(x, y) \otimes r_2^*(x, y) \otimes \delta(x - x_l, y - y_l) \quad (4.7)$$

y aplicando una TF sobre (4.7), se obtiene el dato de campo óptico encriptado en las nuevas coordenadas de posicionamiento (x_l, y_l) :

$$E_l(\mu, \nu) = C_l(\mu, \nu)R_2^*(\mu, \nu)e^{2\pi i(x_l\mu + y_l\nu)} \quad (4.8)$$

A continuación, se definen nuevos parámetros que permiten cuantificar la eficiencia del método de reducción del volumen que se propone y que se aplicará sobre el dato de campo óptico $E_l(\mu, \nu)$ para ilustrar el concepto.

4.2.2. Escalado óptico

Primero se define el factor de eficiencia E como la relación entre el volumen de datos inicial y final después de los diferentes procedimientos aplicados sobre los datos. El factor de eficiencia E_f obtenido con el proceso de filtrado para un *JPS* viene dado por:

$$E_f = \frac{V_{JPS}}{V_{ft}} = \frac{X_c * Y_c * B_c}{2 * X_o * Y_o * B_c}, \quad (4.9)$$

donde V_{JPS} es el volumen del *JPS* registrado por la CCD, y V_{ft} es el volumen resultante del *JPS* filtrado. Como el tamaño de filtrado es menor que el tamaño del *JPS* se asegura la relación $V_{ft} < V_{JPS}$. Así, siempre el factor de eficiencia E_f será mayor que 1.

Para incrementar la eficiencia en la reducción del volumen, se introduce el nuevo proceso de *escalado óptico*, que es aplicado sobre el dato de campo óptico. Este proceso consta de un sistema óptico virtual que utiliza una lente convergente para escalar o magnificar el dato filtrado (ver Figura 4.2). El parámetro de compresión de este sistema se define como la *magnificación* M con valores entre $0 < M < 1$, cuando $M = 1$ no hay reducción de volumen.

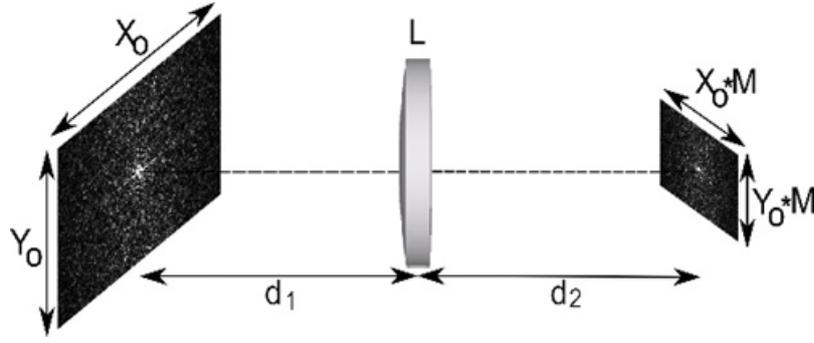


Figura 4.2: Sistema óptico virtual usado para escalar ópticamente el dato de campo óptico: d_1 distancia objeto, L lente convergente, d_2 distancia imagen, M magnificación.

A continuación se define, el factor de eficiencia del proceso de escado óptico E_M como:

$$E_M = \frac{V_{ft}}{V_M} = \frac{2 * X_o * Y_o * B_c}{2 * X_o * Y_o * B_c * M^2} = \frac{1}{M^2} \quad (4.10)$$

donde V_M es el volumen después del proceso de escalado óptico y M es la magnificación del sistema óptico virtual. Una demagnificación ($M < 1$) es obligatoria para lograr una eficiencia $E_M > 1$ (ver ecuación (4.10)).

Después de realizar el filtrado y el escalado óptico, se consigue un factor de eficiencia E de:

$$E = \frac{V_{JPS}}{V_M} = \frac{X_c * Y_c * B_c}{2 * X_o * Y_o * B_c * M^2} \quad (4.11)$$

De acuerdo a las ecuaciones (4.9), (4.10) y (4.11) el factor de eficiencia es igual al producto de los factores de eficiencia del filtrado y el escalado $E = E_f E_M$.

4.2.3. Procesamiento de múltiples datos encriptados

De igual forma en que se procesó un objeto en el sistema descrito en la sección 4.2.1, se obtienen los demás datos de campo óptico, representados por la función $E_l(\mu, \nu)$, donde cada uno está posicionado en una coordenada distinta formando un único paquete como se ilustra en la Figura 4.3.

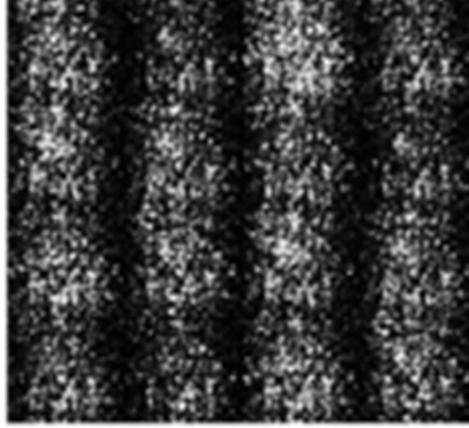


Figura 4.3: Paquete $N_l(\mu, \nu)$ que contiene los datos de campo óptico de 16 objetos encriptados sobre un arreglo matricial.

Este paquete multiplexado se representa como:

$$N_l(\mu, \nu) = \sum_{l=1}^N E_l(\mu, \nu) = \sum_{l=1}^N [C_l(\mu, \nu) R_2^*(\mu, \nu) e^{2\pi i(x_l \mu + y_l \nu)}] \quad (4.12)$$

Ahora, el proceso de reducción de volumen descrito, se generaliza para el caso de N objetos y se aplica sobre el paquete (4.12). De esta manera, el factor de eficiencia para los N datos se representa como:

$$E_N = \frac{N * V_{JPS}}{V_{NM}} = \frac{N * X_c * Y_c * B_c}{2 * N * X_o * Y_o * B_c * M^2} \quad (4.13)$$

donde V_{NM} es el volumen de los N datos filtrados y multiplexados que han sido escalados. De las ecuaciones (4.11) y (4.13) se puede concluir que el factor de eficiencia del filtrado y el escalado no depende del número de objetos cifrados, es decir, $E_N = E$.

El parámetro que cuantifica la eficiencia de la propuesta en términos del volumen de los datos, es la diferencia de volumen entre el volumen inicial y el volumen final dado por:

$$\Delta V = N * (V_{JPS} - V_M) \quad (4.14)$$

Utilizando la ecuación (4.11) se puede obtener:

$$\Delta V = N * V_{JPS} \left(1 - \frac{1}{E}\right) \quad (4.15)$$

Como se esperaba, ΔV depende del número de objetos encriptados y del factor de eficiencia logrado con los procesos de filtrado y escalado. Como $E_f > 1$ y $E_M > 1$ se consigue un factor de eficiencia $E > 1$, asegurando una reducción de volumen de datos.

4.2.4. Proceso de recuperación

El multiplexado de datos de campo óptico que se muestra en la Figura 4.3, permitirá la recuperación de todos los objetos sin ninguna superposición entre ellos. De esta manera se obtiene un solo paquete sobre el cual se aplicará el escalado óptico.

Teniendo en cuenta que fueron encriptados con la misma llave de seguridad $r_2(x_o, y_o)$, se procede a recuperar la información con la llave de descryptación $R_2(\mu, \nu)$. Una multiplicación entre el paquete (4.12) con la llave $R_2(\mu, \nu)$, y una posterior TF, permiten descryptar todos los datos en el mismo plano y sin superposición:

$$n_l(x, y) = \sum_{l=1}^N [c_l(x, y) \otimes \delta(x - x_l, y - y_l)] \quad (4.16)$$

De la ecuación anterior, es evidente que la posición (x_l, y_l) de cada carácter descryptado en el plano de recuperación es impuesta durante el proceso posicionamiento.

4.2.5. Resultados experimentales

Se encriptaron 16 objetos, donde el *JPS* correspondiente a cada objeto es individualmente almacenado usando el montaje experimental de encriptación de la Figura 2.8. Cada *JPS* fue registrado usando una cámara CCD PULNIX TM6703 con 640 píxeles \times 480 píxeles de resolución, 8 bits de profundidad y ancho de píxel de $9\mu m$. Por lo tanto, cada *JPS* tiene un volumen $V_{JPS} = 300KB = 0,2929MB$, y como se tienen 16 objetos el volumen inicial será $V_I = 4,69MB$.

El tamaño de cada dato de campo óptico esta asociado al tamaño de la ventana de filtrado que se ilustra en la Figura 2.9 del capítulo 2. En este caso, la ventana tiene un tamaño de 177 píxeles \times 198 píxeles, y una TF sobre el filtrado genera el dato de campo óptico con un volumen de $68,45KB$, donde cada dato de campo óptico esta representado por la ecuación (2.40). Lo anterior implica que los 16 datos de campo óptico tienen un volumen $V_F = 1,07MB$, generando una reducción de volumen del 77,18 %.

El paso siguiente es aplicar la técnica de multiplexado por posicionamiento como se describió en la sección 4.2.3. Como se mencionó anteriormente, la cantidad de objetos procesados y el tamaño de la ventana de filtrado, son los que determinan el tamaño de la ventana de posicionamiento. De esta forma, se tiene para los 16 datos de campo óptico de tamaño 177 píxeles \times 198 píxeles cada uno, generando un arreglo matricial de 708 píxeles \times 792 píxeles y por lo tanto un

volumen $V_{N_i(\mu,\nu)} = 1,07MB$. Como se mostró en la sección 4.1.3, el multiplexado no genera ningún cambio en el volumen de los datos, las ventajas del multiplexado son un manejo más eficiente de los múltiples datos con una recuperación sin superposición.

Ahora, sobre el multiplexado de los datos de campo óptico (Figura 4.3), se aplica el escalado óptico para reducir su volumen. En la Figura 4.4 (a) se muestra la recuperación para los casos en que no se ha escalado ópticamente y en la Figura 4.4 (b) cuando se hizo el escalado óptico con valor de magnificación $M = 0,5$, respectivamente. Con este valor de magnificación se obtiene un volumen $V_{N_i(\mu,\nu)}^{M=0,5} = 0,27MB$. El proceso completo tiene un factor de eficiencia $E = E_f E_M = 17,53$ (ecuaciones (4.9) y (4.10)) y una diferencia de volumen $\Delta V = 4,42MB$ (ecuación (4.15)). Esto significa que se alcanza una reducción de volumen del 94,24%, donde por proceso de filtrado aporta un 77,18%, mientras que el escalado óptico permite una reducción del 17,06%.



Figura 4.4: Recuperación: (a) sin el proceso de escalado sobre el multiplexado y (b) con escalado óptico de $M=0.5$ sobre el multiplexado.

Los resultados muestran que el proceso de escalado óptico aporta un mayor porcentaje de reducción en el volumen, con respecto al 3,3% reportado por la técnica de cuantización. Se debe tener en cuenta que la técnica de cuantización fue aplicada sobre el paquete de datos encriptados en un sistema de $2f$, y que se tuvo en cuenta una mayor cantidad de objetos. Más adelante se aplican las técnicas de cuantización y escalado óptico sobre los datos de campos óptico generados en un sistema de encriptación *JTC*.

Con el fin de medir el error causado por el procedimiento de escalado, se calcula el error

cuadrático medio normalizado NMSE (por las siglas en inglés: normalized mean square error) entre los datos recuperados para diferentes valores de M y los datos recuperados sin magnificación.

$$NMSE = \frac{\sum_{p,q}^{N,M} |m(p,q) - m_r(p,q)|^2}{\sum_{p,q}^{N,M} |m(p,q) - m_w(p,q)|^2} \quad (4.17)$$

donde $m(p,q)$ es la recuperación de la información magnificada, $m_r(p,q)$ la referencia que corresponde a la recuperación de la información sin magnificar, (p,q) son las coordenadas de los píxeles, N y M es el número de píxeles horizontales y verticales de los datos recuperados, y $m_w(p,q)$ es el caso con mínima magnificación.

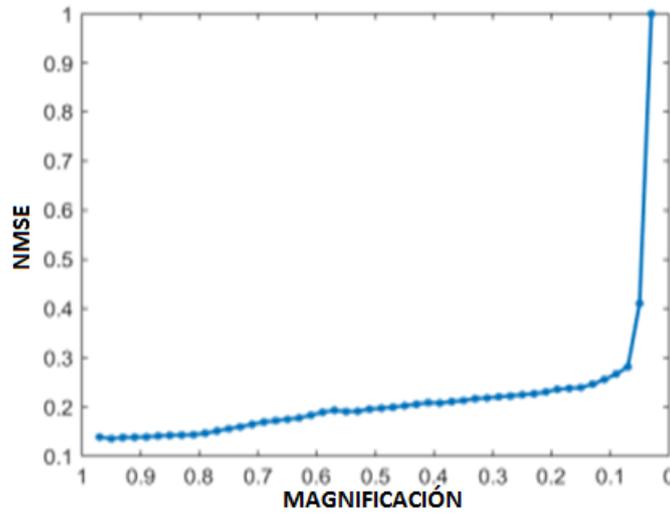


Figura 4.5: NMSE entre los datos recuperados desde el arreglo de la Figura 4.4 (a) antes y después de magnificación.

Existe una conexión evidente entre la magnificación de los campos ópticos multiplexados (Figura 4.4 y ecuación (4.12)) y la calidad de la imagen recuperada, como se deduce claramente del gráfico de la Figura 4.5. Este comportamiento se puede explicar por la pérdida gradual de las frecuencias espaciales del plano de entrada en el procedimiento de escalado óptico a medida que disminuye el valor de magnificación. En ese sentido, la degradación de la calidad de la reconstrucción dependerá del contenido específico de frecuencias del multiplexado.

En la Figura 4.6, se observa que la pendiente ΔV (ecuación (4.15)) como función del número de objetos N , depende del valor de magnificación M (donde E es inversamente proporcional a M^2 como se muestra en la ecuación (4.11)). En este caso, los objetos empleados para generar la curva de número de objetos tiene las mismas propiedades que las mostrados en la Figura 4.4.

La línea correspondiente a $M = 1$ muestra la diferencia de volumen cuando se considera sólo el proceso de filtrado. Es evidente que la reducción en el volumen aumenta a medida que se incrementa el número de objetos involucrados y disminuye la magnificación.

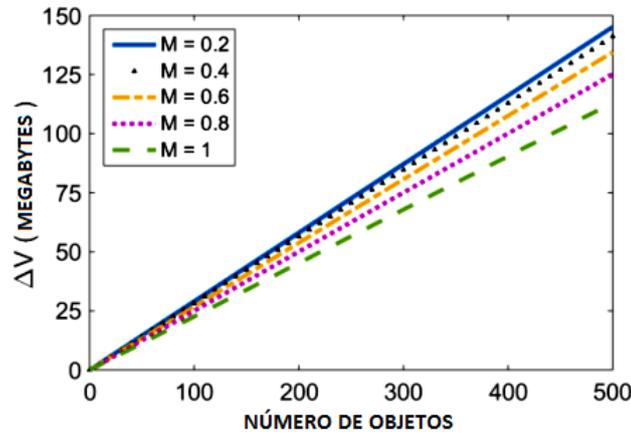


Figura 4.6: Dependencia de ΔV con el número de objetos procesados para cinco valores de M .

De la Figura 4.7, se evidencia que el procedimiento de filtrado establece una línea de base inicial de 77,18 % al porcentaje de reducción de volumen. La magnificación añade una reducción adicional del 17,06 % sobre este valor base. La reducción mostrada en esta gráfica es una indicación de la potencialidad del proceso de escalado óptico.

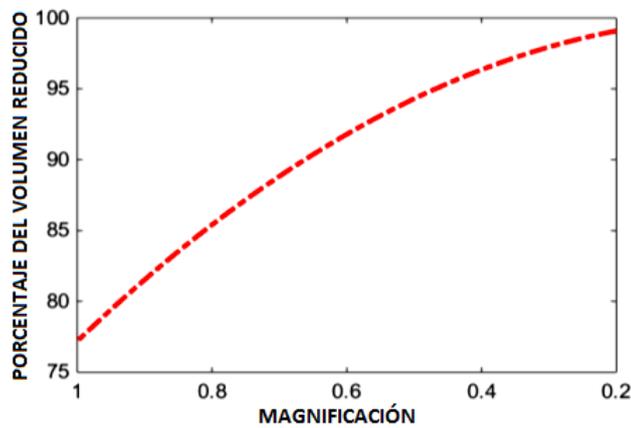


Figura 4.7: Porcentaje en la reducción del volumen en función de la magnificación.

Es de resaltar, que los resultados obtenidos en esta sección con la nueva propuesta de compresión por medio de un sistema óptico-virtual, fueron publicados en un revista internacional

(ver Apéndice A).

4.3. Reducción del volumen combinando las técnicas de cuantización y escalado óptico

En las secciones anteriores se mostró el efecto de reducción de volumen que se alcanza cuando se aplican las técnicas de cuantización y escalado óptico sobre los datos de campo óptico multiplexados, en ese caso se usaron datos provenientes de sistemas de encriptación $2f$ y JTC en cada caso respectivamente. En esta sección se analiza cualitativa, y cuantitativamente a través del coeficiente de correlación, la calidad de la información descriptada en términos de la reducción del volumen para diferentes valores de cuantización y escalado óptico empleando datos procesado en un sistema de encriptación JTC . Estos resultados se comparan con los resultados obtenidos cuando se aplica un procedimiento de escalado digital (ED) sobre el multiplexado cuantizado.

4.3.1. Escalado digital

La técnica de escalado digital o remuestreo consiste en disminuir el tamaño del holograma digital, para lo cual generalmente se emplean tres estrategias de interpolación antes de la reconstrucción [6]. En este trabajo se implementa una técnica de escalado digital que consiste en la reducción de tamaño de la imagen, donde la reducción se realiza de forma equivalente al proceso de escalado óptico, es decir, que consiste en simplemente escalar la imagen de forma digital. En este trabajo, la reducción digital se aplica sobre el multiplexado de datos de campo óptico y no sobre el holograma como se hace habitualmente. De esta manera, la técnica de escalado digital (ED) implementada se cuantificará con el parámetro ED que varía de la siguiente forma $0 < ED < 1$, donde $ED = 1$ representa el caso del paquete con tamaño original o inicial, y valores menores a 1 representa el paquete escalado.

4.3.2. Resultados experimentales

Se registraron 16 objetos con el sistema de encriptación JTC y se procesaron para obtener los datos de campo óptico posicionados sobre un arreglo matricial, como se describió en la sección 4.2 (ver Figura 4.3). Inicialmente, sobre el paquete se aplica la reducción de volumen disminuyendo la profundidad de bits de 8 bits a 4 bits. Luego, sobre el paquete cuantizado se realiza una reducción de volumen por medio del escalado óptico, disminuyendo el valor de magnificación.

En las Figuras 4.8 (a), (b) y (c) se muestra la recuperación con una profundidad de 8 bits para valores de M igual 0,5, 0,4 y 0,1. En particular con un valor de $M = 0,5$, se logró un volumen final $V_{N_i(\mu,\nu)}^{M=0,5} = 0,27MB$. En las Figuras 4.8 (d), (e) y (f) se muestra las recuperaciones a 4 bits para los mismos valores de M . Se puede observar que la recuperación mostrada en la Figura 4.8(e) es comparable con la recuperación obtenida en (a); para comprobar dicha afirmación, más adelante se analiza la calidad de las recuperaciones por medio del coeficiente de correlación para distintos valores de cuantización a distintos valores de magnificación.

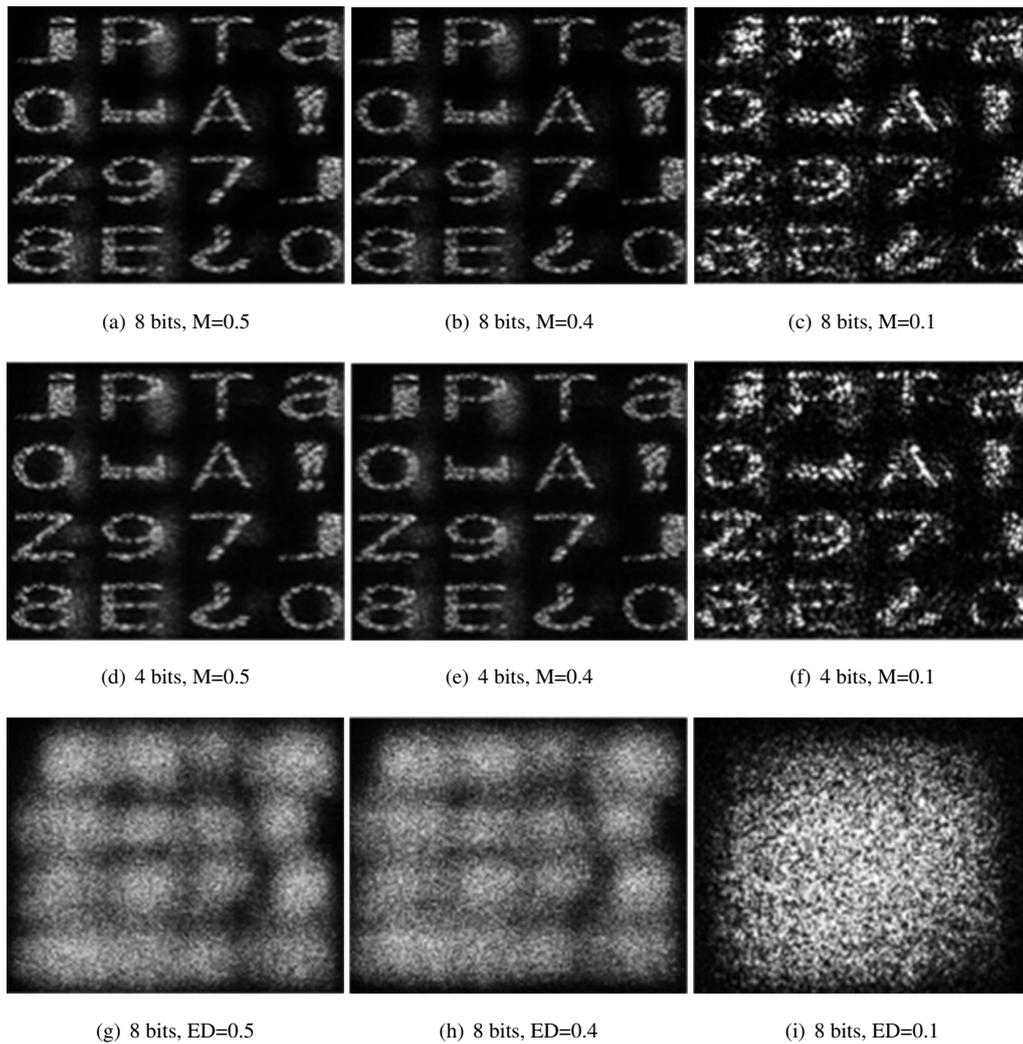


Figura 4.8: Objetos recuperados a distintos valores de cuantización, escalado óptico y escalado digital.

Adicionalmente el paquete cuantizado a 8 bits es escalado digitalmente, para valores de ED de 0,5, 0,4 y 0,1. En la Figuras 4.8 (g), (h) e (i) se muestra la respectiva recuperación. Se puede observar que cuando se aplica el proceso de escalado digital no se pueden recuperar exitosamente los datos, lo que permite concluir que el escalado digital no es una técnica válida de reducción de volumen cuando se trata de un multiplexado de datos de campo óptico. A continuación se realiza un breve análisis de estadística speckle [11], para determinar el efecto que tienen los procesos de escalado sobre la información.

Se procede a analizar el comportamiento de ambos procesos de escalado a 8 bits, para ello se observa el comportamiento de la estadística speckle después de escalar el paquete de datos de campo óptico encriptado $N_I(\mu, \nu)$. Primero se determina la distribución de intensidad (estadística de speckle de primer orden) para cada valor de escalado óptico y escalado digital, y posteriormente se determina la función de autocorrelación para los mismos valores de escalado (estadística de speckle de segundo orden).

En la Figura 4.9 (a) se presenta la distribución de intensidad del paquete, mientras que en las figuras 4.9 (b) y (c) se observan las curvas de distribución de intensidad para los valores de M igual a 0,5 y 0,1 respectivamente. Estas curvas reflejan el comportamiento de la función exponencial negativa que es característico en las fluctuaciones de intensidad de un patrón de speckle. Pero, la estadística de primer orden es insuficiente para describir otras propiedades de un patrón de intensidad de speckle [11], por lo tanto se determina la función de autocorrelación para la intensidad dada por:

$$R_I(\Delta x, 0) = \langle I \rangle^2 \left(1 + \text{sinc}^2 \frac{L\Delta x}{\lambda z} \right) \quad (4.18)$$

función importante en la estadística de segundo orden. Una deformación del speckle se traduce en una disminución del valor máximo de la autocorrelación para la intensidad. En la Figura 4.9 (d) se ilustra las funciones de autocorrelación asociadas a cada uno de los valores de escalado óptico. Se observa que el ancho medio de las curvas azul ($M = 1$) y roja ($M = 0,5$) son bastante parecidas, lo que implica que el proceso de escalado óptico no afecta en gran proporción las propiedades del speckle. De esta manera se puede afirmar que en el proceso de escalado óptico, el speckle varía a medida que aumenta la reducción de volumen, pero las posiciones relativas de los speckles no cambia. Es decir, la estadística de speckle se mantiene, esto permite que la información contenida en el multiplexado se conserve y los datos se puedan recuperar (ver Figuras 4.8 (b) y (c)).

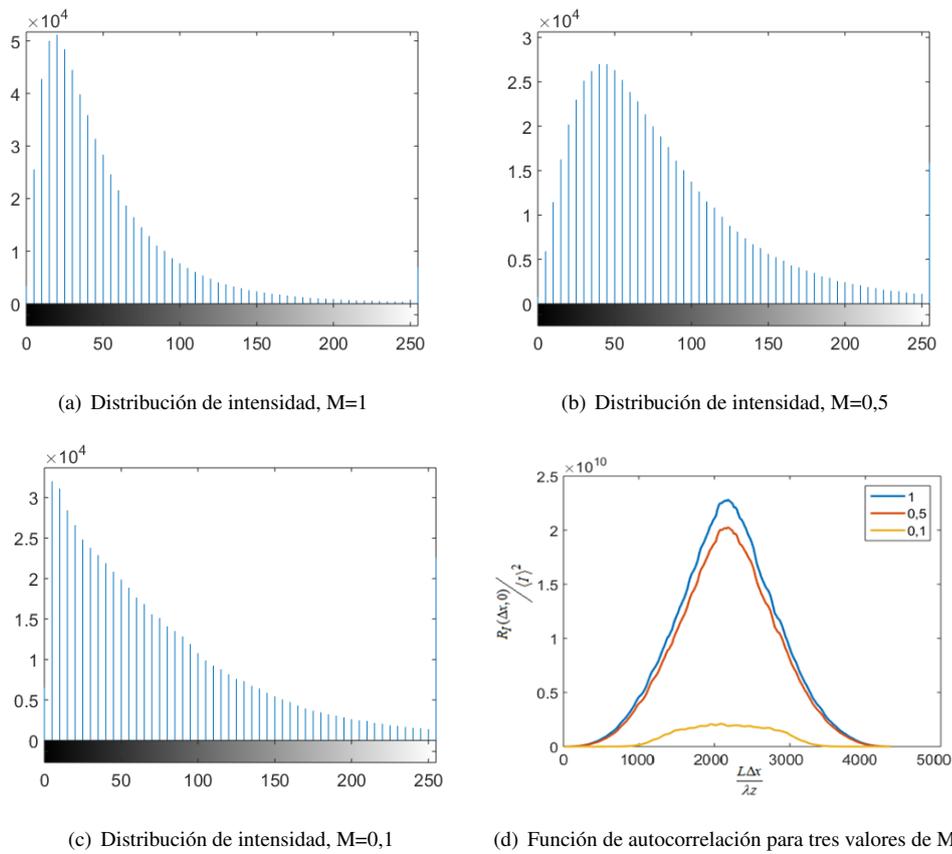


Figura 4.9: Estadística speckle para el método de escalado óptico.

De igual forma se analiza la intensidad del campo con la estadística de primer y segundo orden cuando el paquete $N_I(\mu, \nu)$ es escalado digitalmente. Las Figuras 4.10(a), (b) y (c) muestran que el escalado digital hace que la distribución de intensidad disminuya significativamente. Por su parte, las funciones de autocorrelación presentadas en la Figura 4.10(d), muestran que la forma de la curva cambia drásticamente y sus valores disminuyen significativamente para un $ED = 0,5$; y para el caso de $ED = 0,1$ desaparece la curva de autocorrelación característica de un patrón de intensidad de speckle. Este comportamiento muestra que el escalado digital afecta la estructura del speckle contenido en el paquete, generando que la información contenida en multiplexado se vaya degradando a medida que aumenta la reducción de volumen debida al escalado digital (ver Figura 4.8 (g), (h) e (i)). Estos resultados permiten concluir que la propuesta de escalado óptico tienen un mejor desempeño que el escalado digital para valores equivalentes de M y ED .

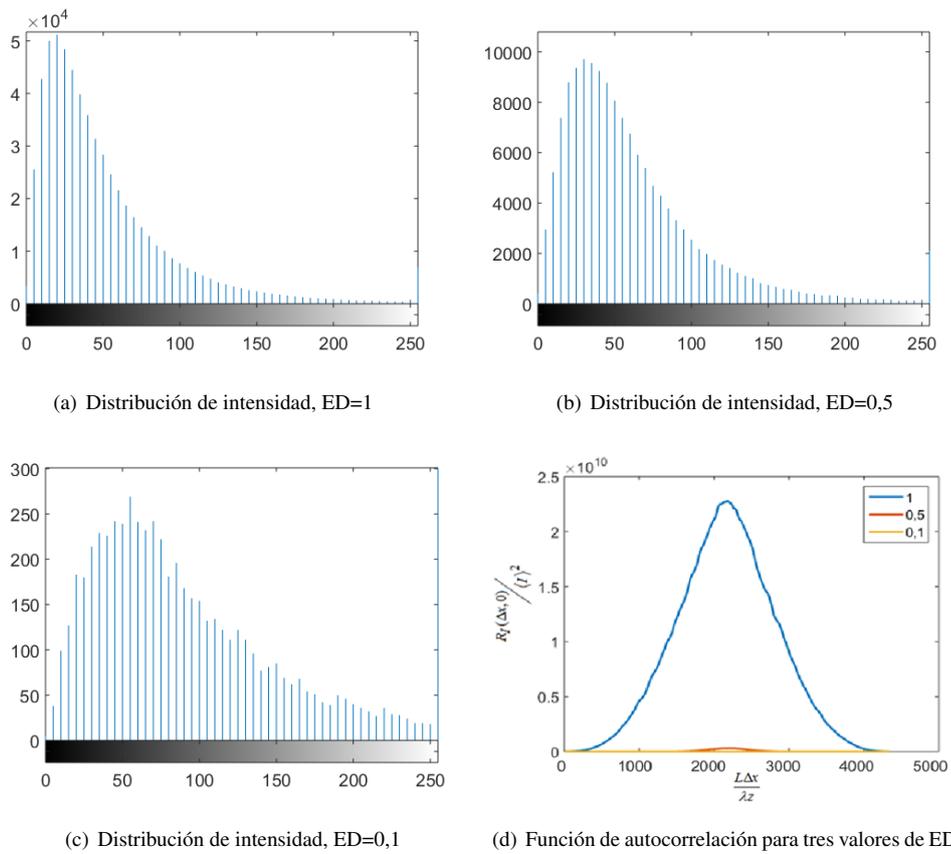
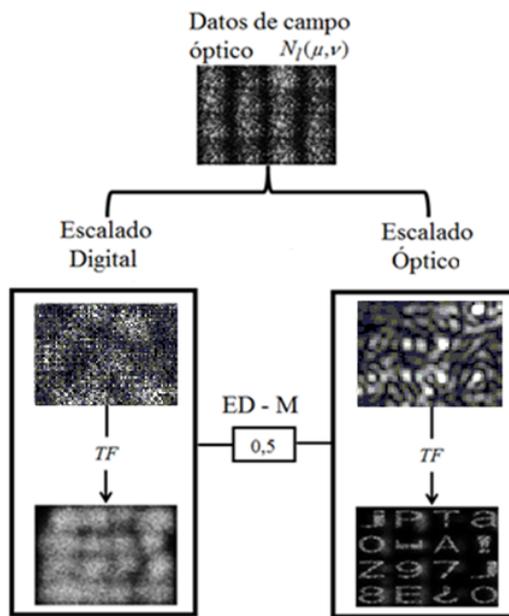
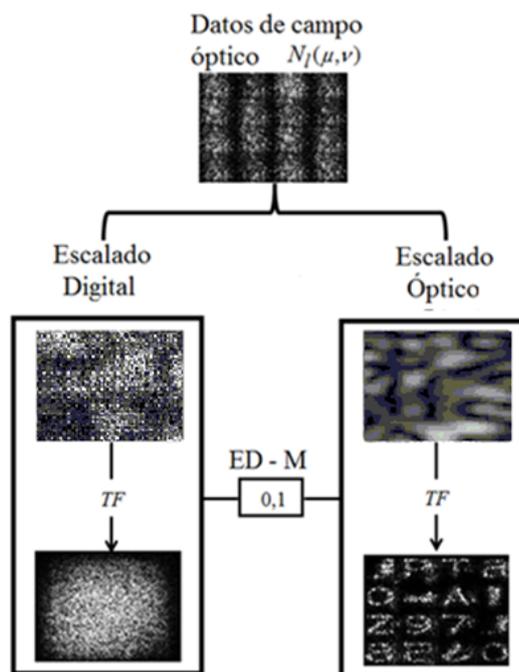


Figura 4.10: Estadística speckle para el método de escalado digital.

En la Figuras 4.11 (a) y (b) se muestra una comparación de como se ve afectada la reconstrucción cuando el DCO es escalado digitalmente y ópticamente con valor de (a) 0.5 y (b) 0.1. El escalado digital lo que hace sobre el DCO, es realizar una interpolación de 4×4 píxeles, es decir interpola los 16 píxeles cercanos, deformando de esta manera el speckle que contiene la información necesaria para su recuperación.



(a) 0.5



(b) 0.1

Figura 4.11: Comparación para dos valores de reducción de volumen con ambos métodos de escalado.

Ahora, para determinar la calidad de la información recuperada cuando el DCO es escalado ópticamente, se analiza cuantitativamente el desempeño del escalado óptico para distintos valores de cuantización por medio del coeficiente de correlación CC , el cual se define como [12]:

$$CC = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{\sum_m \sum_n (A_{mn} - \bar{A})^2 (B_{mn} - \bar{B})^2}} \quad (4.19)$$

donde m y n son las coordenadas de píxel, A es la intensidad de los objetos reconstruidos sin escalamiento, B la intensidad de los objetos reconstruidos cuando se combinan el escalado óptico y la cuantización, y \bar{A} , \bar{B} son los valores medios de A y B respectivamente.

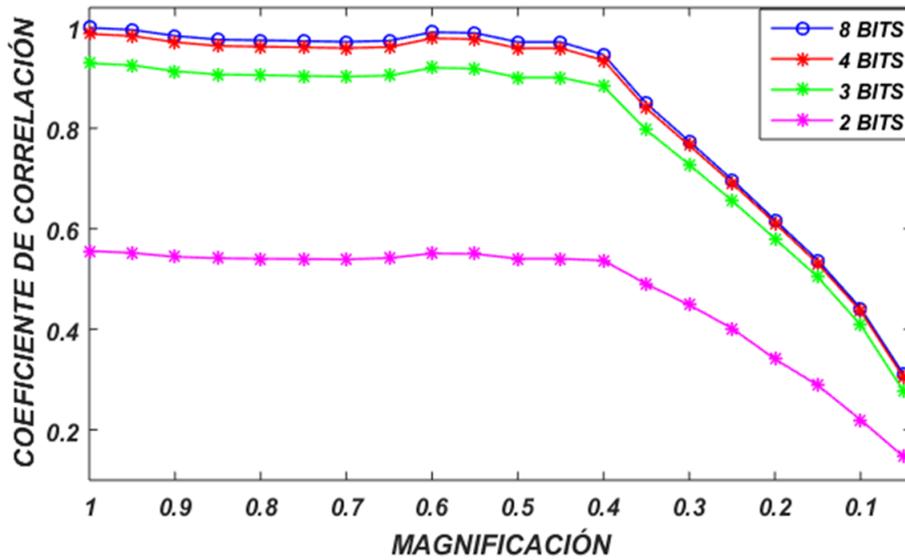


Figura 4.12: Coeficiente de correlación en términos de la magnificación para diferentes valores de cuantización.

En la figura 4.12 se observa que para valores de 8 y 4 bits con valores de magnificación hasta $M = 0,4$, se tiene una recuperación comparable al caso $M = 1$, como se puede inferir de las recuperaciones presentadas en la Figura 4.4 y las Figuras 4.8 (b) y (e); mientras que para valores inferiores a $M = 0,4$ la recuperación se degrada a medida que disminuye la magnificación. Por otro lado, cuando los valores de cuantización son menores a 4 bits, se presenta degradación para todos los valores de magnificación (ver figura 4.8(c)), degradación que se hace más pronunciada a medida que disminuye el valor de la cuantización y para valores de la magnificación inferiores a 0.4.

Finalmente, se calculará la reducción de volumen resultante de aplicar los procesos de filtrado, el escalado óptico y la cuantización. El volumen asociado al escalado óptico para N objetos

está definido como:

$$V_{NM} = 2 * N * X_o * Y_o * B_o * M^2 \quad (4.20)$$

Para valores de $B_o = 4bits = (0,5bytes)$ y $M = 0,4$ se obtiene un volumen $V_{N_t(\mu,\nu)}^{M=0,4(4bits)} = 0,085MB$, resultando una reducción del volumen del 98,18%, debido a la acción combinada del filtrado, el escalado óptico y la cuantización. De esta manera, el porcentaje de reducción asociado al filtrado es de 77,18%, y el 21% restante, se debe a la combinación de escalado óptico con un 17,1% y cuantización con un 3,9% aproximadamente. Estos resultados muestran que la técnica de escalado óptico puede combinarse efectivamente con técnicas digitales de compresión para alcanzar una mayor reducción del volumen.

Lo descrito y analizado en este capítulo, permite mostrar la potencialidad del nuevo método de reducción de volumen, el cual se denominó *escalado óptico*. Los resultados evidencian que la técnicas digitales como la cuantización y el escalado digital son menos eficientes para comprimir la información contenida dentro de los datos de campo óptico, los cuales fueron obtenidos a partir de hologramas que fueron procesados en los sistemas de encriptación $2f$ y JTC y registrados por medio de la técnica de Fourier fuera de eje. A pesar de que la cuantización y el escalado digital se aplican sobre datos que no poseen franjas interferenciales, pues el proceso de filtrado eliminó dichas franjas, los resultados muestran que la técnica de escalado óptico presenta un mejor desempeño que estas técnicas digitales. Además, al analizar la estadística de speckle de primer y segundo orden del paquete de datos campo óptico comprimido usando las técnicas de escalado óptico y digital, se demuestra que la nueva propuesta de escalado óptico afecta en menor proporción la información contenida en los datos de campo óptico, en comparación con la técnica de escalado digital. De acuerdo a lo anterior, se concluye que la técnica de escalado óptico no es solo un mecanismo viable para la compresión de datos de campo óptico, sino que además presenta un desempeño superior a las técnicas digitales de cuantización y escalado. Se debe destacar que algunos resultados de esta sección hacen parte de los resultados originales de esta tesis y fueron publicados en una revista internacional (ver Apéndice A).

- [1] E. Tajahuerce, O. Matoba, S.C. Verrall, B. Javidi. *Optoelectronic information encryption with phase-shifting interferometry*. *Appl. Opt.*, 39:2313–2320, 2000.
- [2] O. Matoba, T. Nomura, E. Pérez-Cabré, M.S. Millan, B. Javidi. *Optical techniques for information security*. volume 97, pages 1128–1148. *Proceedings of the IEEE*, 2009.
- [3] J. F. Barrera, A. Mira-Agudelo, R. Torroba. *Experimental QR code optical encryption: noise-free data recovering*. *Opt. Lett.*, 39:3074–3077, 2014.
- [4] J. F. Barrera, M. Tebald, C. Ríos, E. Rueda, N. Bolognini, R. Torroba. *Experimental multiplexing of encrypted movies using a JTC architecture*. *Opt. Exp.*, 20:3388–3393, 2012.
- [5] S. Trejos, J. F. Barrera, R. Torroba. *Optimized and secure technique for multiplexing QR code images of single characters: application to noiseless messages retrieval*. *J. Opt.*, 17:085702, 2015.
- [6] T.J. Naughton, Y. Frauel, B. Javidi, E. Tajahuerce. *Compression of digital holograms for three-dimensional object reconstruction and recognition*. *Appl. Opt.*, 41:4124–4132, 2002.
- [7] E. Darakis, J. J. Soraghan. *Reconstruction domain compression of phase-shifting digital holograms*. *Appl. Opt.*, 46:351–356, 2007.
- [8] O. Matoba, T.J. Naughton, Y. Frauel, N. Bertaux, B. Javidi. *Real-time three-dimensional object reconstruction by use of a phase-encoded digital hologram*. *Appl. Opt.*, 41:6187–6192, 2002.
- [9] E. Cucho, P. Marquet, C. Depeursinge. *Spatial filtering for zero-order and twin-image elimination in digital off-axis holography*. *Appl. Opt.*, 39:4070–4075, 2000.

-
- [10] S. Trejos, J.F. Barrera, A. Velez, M. Tebaldi, R. Torroba. *Optical approach for the efficient data volume handling in experimentally encrypted data*. *J. Opt.*, 18:065702, 2016.
- [11] J.C Dainty, A.E Ennos, M. Francon, J.W Goodman, T.S McKenchie, G. Parry.
- [12] J.W Goodman. *Statistical Optics*. New York: Wiley, 2nd edition, 2000.

CAPÍTULO 5

REDUCCIÓN DE VOLUMEN EN HOLOGRAMAS DE OBJETOS TRIDIMENSIONALES

La holografía digital es una técnica que permite el procesamiento computacional de la información generada en sistemas ópticos. Esta técnica ha permitido el desarrollo de métodos ópto-digitales sofisticados que aprovechan las propiedades de los sistemas ópticos y la flexibilidad que brinda el procesamiento digital. Entre áreas que han aprovechado las ventajas de la holografía digital se encuentran la metrología, la microscopía, el procesamiento de imágenes médicas y la seguridad óptica [1–10], por nombrar algunas. Específicamente, aplicando técnicas de holografía digital se puede procesar la información generada en el procesamiento óptico de información proveniente de objetos bidimensionales y tridimensionales [11, 12], proporcionando un alto grado de flexibilidad en la manipulación de la información [13–15]. En particular, la técnicas de holografía digital permiten la reconstrucción de escenas con profundidad [16].

Mediante las técnicas de holografía digital se registra un patrón de intensidad que contiene la información de amplitud y fase de un campo óptico, lo que implica el registro de un patrón franjas de interferencia [17]; o de múltiples patrones obtenidos por medio de desplazamientos de fase [18]. Como resultado, se almacena digitalmente un gran volumen de datos que posteriormente deben ser procesados. Se han propuesto varias técnicas para disminuir los desafíos impuestos por este volumen de datos, las cuales se centran principalmente en técnicas de cuantización [18–20], filtrado [21], y algoritmos de compresión de datos sin pérdida y compresión con pérdida [22, 23].

Se ha aplicado métodos de compresión digital estándar, como el JPEG (por las siglas en inglés de: Joint Photography Expert Group), sobre información holográfica [24–27]. Este grupo de métodos se basa en el análisis de parámetros estadísticos de imágenes y las características de percepción visual del ojo humano. También se centran en la eliminación de información redundante o en suprimir armónicos innecesarios de la representación espectral. En particular, el formato de compresión con pérdida de JPEG [28], funciona subdividiendo la imagen de entrada en bloques de 8×8 píxeles. A continuación se aplica una transformada coseno discreta DCT (por las siglas en inglés de: Discrete Cosine Transform) a cada bloque, y se realiza una cuantificación de los componentes de la transformación resultante. Esta cuantificación es la etapa del protocolo JPEG que conduce a pérdidas. Los datos se comprimen aún más mediante la aplicación de la codificación de Huffman sin pérdidas [29]. La pérdida y el grado de compresión que puede conseguir el formato JPEG puede controlarse mediante un parámetro definido como factor de calidad (FC) que toma valores entre 1 y 100.

Sin embargo, en el caso de los hologramas digitales, estos métodos son mucho menos aplicables por cuatro factores [30]: En primer lugar, la calidad de la imagen reconstruida a partir del holograma es más importante que la percepción visual del holograma comprimido. En segundo lugar, los algoritmos de compresión digitales son más aplicables para imágenes con cambios graduales de brillo, pero los hologramas digitales son imágenes interferenciales, y en general, no hay cambios graduales de brillo en los hologramas. En tercer lugar, por lo general el holograma de un objeto tiene una gran cantidad de detalles. Como resultado, no tener en cuenta varios componentes espectrales del holograma conduce a una pérdida de calidad significativa de la imagen reconstruida, situación que no sucede en el caso de compresión de fotografías estándar. En cuarto lugar, las imágenes habituales como una fotografía, surgen del registrar la amplitud de una onda, y en los hologramas no sólo se registra la amplitud, sino también la fase de una onda. De acuerdo a lo anterior, es de interés generar métodos que permitan reducir el volumen de información holográfica reteniendo la mayor cantidad de frecuencias espectrales que permitan una mejor calidad en la recuperación, y que además eviten el problema de pérdida de contraste de las franjas interferométricas.

Teniendo como referencia lo antes mencionado, este capítulo se enfoca en la compresión de hologramas de objetos tridimensionales (3D), donde la información del objeto es registrada por medio de la técnica de holografía de Fourier fuera de eje. En la primera sección de este capítulo, se describe la aplicación de la técnica de escalado óptico y el formato de compresión JPEG sobre el dato de campo óptico obtenido a partir de un holograma. Posteriormente se evalúa el rendi-

miento de ambos métodos de compresión aplicados sobre el mismo campo óptico. Finalmente, se analiza el comportamiento de la información de amplitud y fase contenida en el campo óptico, cuando se aplican a ambos métodos de compresión.

Mientras que en la segunda sección, se presenta una nueva técnica para comprimir información de hologramas de objetos 3D a color, donde parte de la reducción de volumen se lleva a cabo insertando máscaras binarias aleatorias. El procedimiento consiste en registrar tres hologramas por cada objeto, cada uno correspondiente a una longitud de onda de los canales de registro RGB en un sistema experimental. Luego, se extraen los campos ópticos de los hologramas de Fourier fuera de eje, y de ellos se retiene la información de fase. Posteriormente estos campos son muestreados con la multiplicación de cada uno con una máscara binaria aleatoria; este proceso es realizado usando diferentes máscaras binarias para la información de fase de cada uno de los campos ópticos involucrados. En seguida, estos campos muestreados son multiplexados generando un único paquete. Para recuperar la información del objeto tridimensional a color a partir del paquete comprimido, se multiplica el paquete por una de las máscaras binarias para seleccionar la información de fase de uno de los campos ópticos, y después de un proceso de reconstrucción con la operación TF se recupera uno de los canales de color del objeto 3D; este procedimiento se repite para los dos canales restantes. La imagen final en color se obtiene mediante la transformación de los valores tricromáticos RGB en el espacio de color [31]. Finalmente, se compara y evalúa el rendimiento de la técnica propuesta con la técnica de compresión digital JPEG. Es importante resaltar que en este caso se la reconstrucción se lleva cabo usando un sistema óptico-virtual y un montaje experimental.

A continuación se describen los pormenores del registro, procesamiento y compresión de los hologramas de objetos a color tridimensionales.

5.1. Compresión de hologramas por medio de escalado óptico

El concepto de compresión por medio de escalado óptico se introdujo en la sección 4.2.2 del capítulo anterior. Esta técnica se basa en un sistema óptico virtual que usa una lente positiva para magnificar el dato de campo óptico (ver Figura 4.2), donde el parámetro de compresión es la magnificación M . En seguida se describe como se obtiene el respectivo dato de campo óptico para aplicar posteriormente el escalado óptico.

5.1.1. Registro holográfico y dato de campo óptico

Se registra la información de un objeto difuso 3D por medio de un esquema de holografía digital de Fourier fuera de eje como se ilustra en la Figura 5.1 (ver sección 2.2.1).

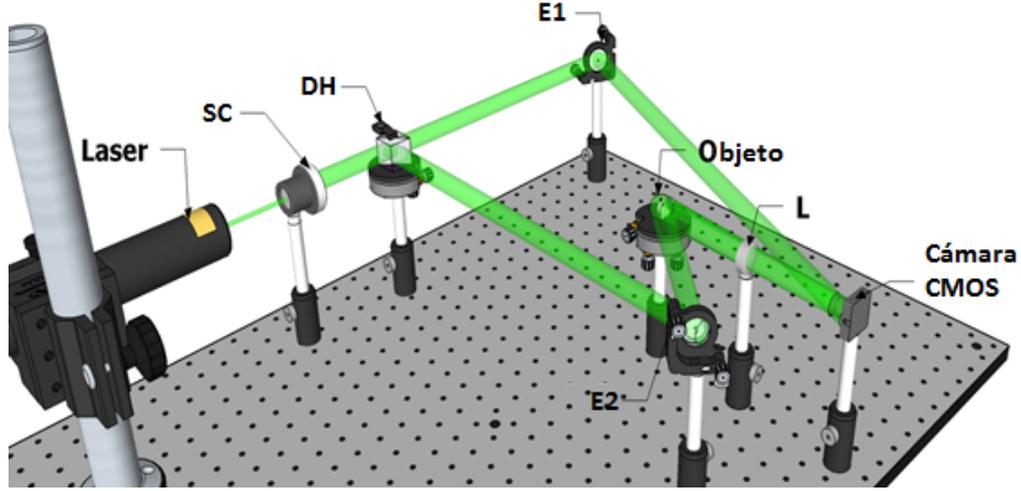


Figura 5.1: Montaje de holografía digital de Fourier fuera de eje (SC: sistema de colimación, DH: divisor de haz, E: espejo, L: lente de longitud focal f).

En el plano de la cámara CMOS, se registra la interferencia entre la onda plana de referencia y la transformada de Fourier de la luz reflejada por el objeto. Esta interferencia (ver Figura 5.2 (a)) viene dada por la ecuación (2.26):

$$H(\mu, \nu) = |O(\mu, \nu)|^2 + |R(\mu, \nu)|^2 + O(\mu, \nu)R^*(\mu, \nu) + O^*(\mu, \nu)R(\mu, \nu) \quad (5.1)$$

donde $O(\mu, \nu)$ es la TF del campo reflejado del objeto tridimensional y $R(\mu, \nu)$ es la onda plana de referencia descrita por [32]:

$$R(\mu, \nu) = e^{2\pi i f(\mu \cos \theta + \nu \cos \varphi)} \quad (5.2)$$

donde los ángulos θ y φ determinan la inclinación de la onda de referencia, y f es la longitud focal de la lente. Ahora se realiza una operación TF sobre el holograma registrado, obteniéndose:

$$h(x, y) = o(x, y) \otimes o^*(x, y) + r(x, y) \otimes r^*(x, y) + o(x, y) \otimes \delta(x + f \cos \alpha, y + f \cos \beta) + o^*(x, y) \otimes \delta(x - f \cos \alpha, y - f \cos \beta) \quad (5.3)$$

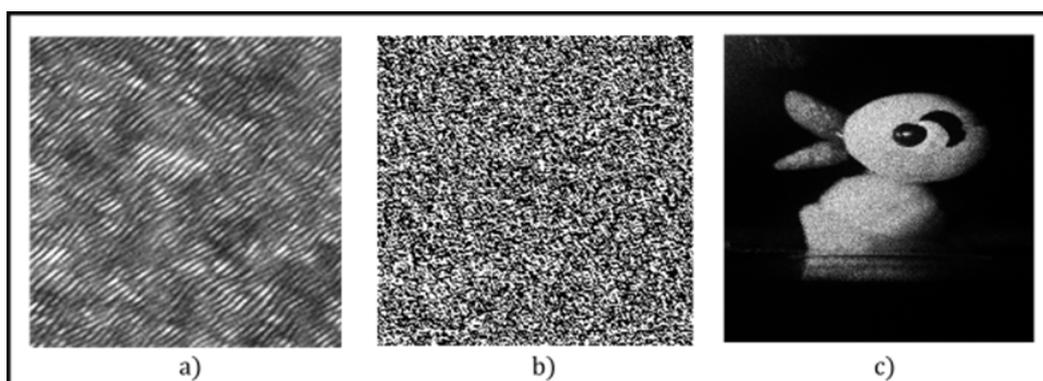


Figura 5.2: (a) Holograma, b) intensidad del dato de campo óptico y c) intensidad del objeto reconstruido a partir del dato de campo óptico de (b).

En la ecuación (5.3), $o(x, y)$ y $r(x, y)$ representan la TF de $O(\mu, \nu)$ y $R(\mu, \nu)$ respectivamente. Los dos primeros términos son las autocorrelaciones de las transformadas de Fourier de la onda objeto y onda plana correspondientes al orden central respectivamente. Los dos últimos términos son las TFs del campo objeto y su complejo conjugado, espacialmente separados debido a la convolución con la función delta de Dirac, resultante de la TF sobre la onda plana (ecuación (5.2)). Aprovechando esta separación espacial, se selecciona el orden correspondiente a la TF del tercer término de la ecuación (5.3), y de esta forma los términos restantes son excluidos. Después de aplicar la transformada de Fourier inversa sobre este término filtrado, se obtiene finalmente el dato del campo óptico $O(\mu, \nu)$ (ver Figura 5.2 (b)). Una posterior TF sobre este dato de campo óptico permitirá reconstruir el objeto $o(x, y)$ (Figura 5.2 (c)). El objeto mostrado en la Figura 5.2 (c) será la referencia con la que se medirá la calidad de los objetos reconstruidos a partir del dato de campo óptico comprimido con las diferentes técnicas.

5.1.2. Resultados experimentales y desempeño de las técnicas de compresión

Aunque el filtrado reduce significativamente la cantidad de datos a almacenar, en el siguiente análisis se emplea el dato de campo óptico como entrada para ser procesado por ambos métodos de compresión. Los hologramas son registrados utilizando el montaje de la Figura 5.1 por medio de una cámara CMOS EO-10012M, con $3480 \text{ píxeles} \times 2748 \text{ píxeles}$ de resolución y un tamaño de píxel de $1,67 \mu\text{m} \times 1,67 \mu\text{m}$. El objeto tiene dimensiones máximas de $18 \text{ mm} \times 24 \text{ mm} \times 16 \text{ mm}$, y la longitud focal de la lente es de 200 mm . Se emplea un láser de estado sólido bombeado por diodo Laserglow Technologies que emite en una longitud de onda de 532 nm y una potencia de salida de 50 mW . El ángulo entre el objeto y el haz de referencia es de aproximadamente 5° ,

y el tamaño de píxel de la cámara utilizada permite un ángulo máximo de $9,13^\circ$, garantizando así que se pueda resolver la frecuencia más alta del patrón de interferencia.

Se obtiene el dato de campo óptico del holograma registrado como se describió en la sección 5.1.1 (ver Figura 5.2 (b)), y se comprime con el método de escalado óptico para valores de M entre 0 y 1. Por otro lado, para fines de comparación, el mismo campo óptico se comprime utilizando compresión JPEG con un FC entre 1 y 100. Luego, se procede a evaluar la diferencia de volumen, definida como:

$$\Delta V = V_R - V_C \quad (5.4)$$

donde V_R es el volumen del dato de campo óptico sin comprimir, y V_C es el dato de campo óptico comprimido, ambos se expresan en unidades de *Kilobytes KB*.

Para este caso particular, el tamaño del dato de campo óptico es de $940 \text{ píxeles} \times 940 \text{ píxeles}$ con una profundidad de 8 bits, resultando en un volumen $V_R = 1726KB$. El volumen del dato de campo óptico comprimido es el número de bytes del archivo en la memoria de un ordenador después de aplicar las técnicas de compresión de escalado óptico y JPEG. Como se está tratando con métodos de compresión con pérdida, también se debe comparar la calidad de los objetos reconstruidos. Esto se logra reconstruyendo digitalmente los objetos a partir de los campos ópticos comprimidos y no comprimidos, y luego se calcula el coeficiente de correlación (ver ecuación (4.19) cuando se emplean ambas técnicas de compresión).

En la Figura 5.3 cada marcador de la curva JPEG representa una disminución del FC en pasos de 5, comenzando en un valor de 100 para el cual la diferencia de volumen $\Delta V = 0$. Cada punto de la curva de escalado óptico corresponde a una disminución de 0,05 del valor de M , comenzando en un valor de 1 para el cual $\Delta V = 0$. La compresión JPEG consigue la mayor disminución de volumen dentro del intervalo de FC entre 100 y 45, pero una reducción adicional del FC degrada severamente la calidad del objeto reconstruido y contribuye muy poco al incremento en la diferencia de volumen ΔV . Por otro lado, el escalado óptico permite una menor pérdida de calidad que la compresión JPEG a altos valores de compresión, como se muestra en la Figura 5.3 en $\Delta V \geq 1380KB$ (ver la línea punteada negra vertical insertada en el gráfico).

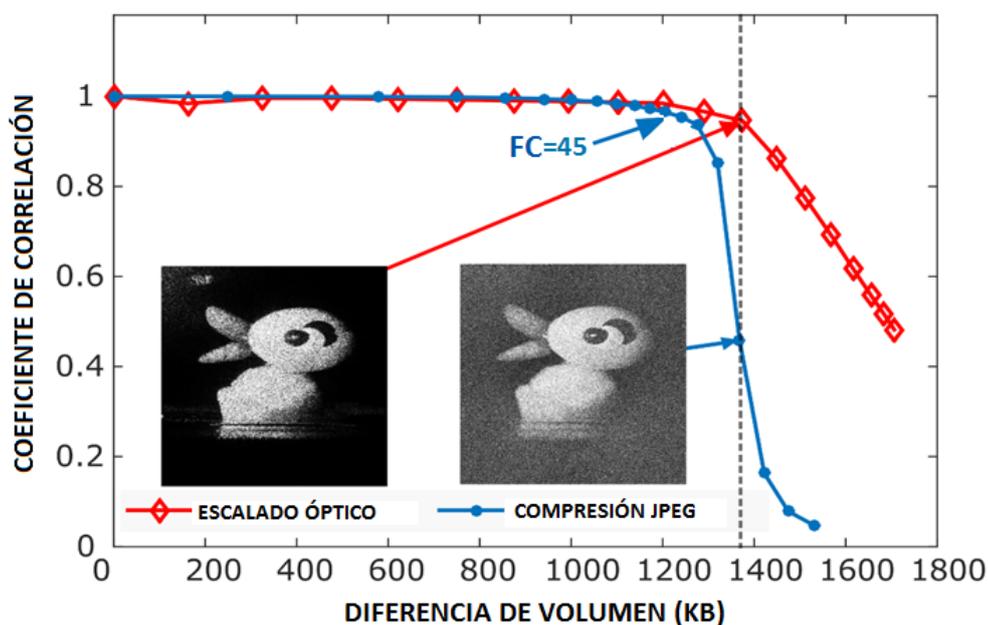
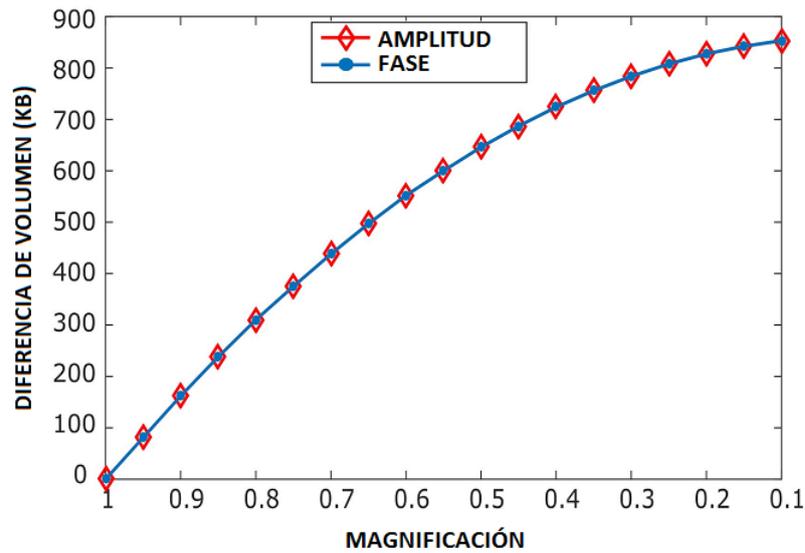


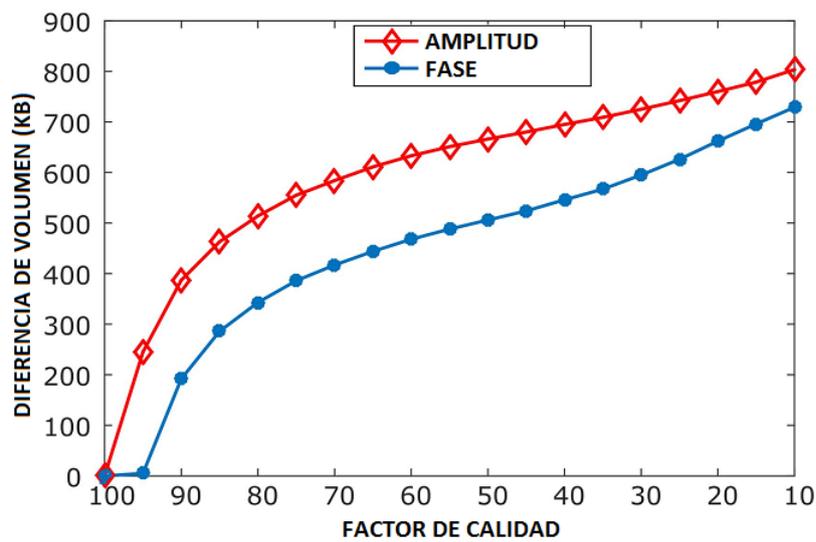
Figura 5.3: Coeficiente de correlación entre el objeto reconstruido desde el dato de campo óptico sin comprimir y el campo de dato óptico comprimido por ambos métodos de compresión, escalado óptico y JPEG en términos de la diferencia de volumen.

Se demostró que el formato de compresión JPEG muestra una disminución en su rendimiento cuando la distribución de los datos es aleatoria [33]. Cuando se tienen objetos difusos, la información de fase del dato de campo óptico tiene una distribución más aleatoria que la información de amplitud. En consecuencia, el comportamiento del formato de compresión debe ser diferente en ambos casos. Para verificar esto, se procede a evaluar el comportamiento de la información de fase y de amplitud por separado, cuando se aplican los dos métodos de compresión. Con el fin de realizar este análisis, se mide la diferencia de volumen en la fase y en la amplitud de los datos de campo óptico comprimidos en términos de los parámetros de magnificación y factor de calidad.

La Figura 5.4 confirma que hay una diferencia en el rendimiento para ambos métodos. La compresión por escalado óptico (Figura 5.4(a)) muestra el mismo comportamiento para la información de fase y amplitud. Mientras que la compresión JPEG (Figura 5.4 (b)) muestra un rendimiento significativamente menor cuando se aplica la compresión a la información de fase.



(a) Escalado óptico



(b) Compresión JPEG

Figura 5.4: Diferencia de volumen en amplitud y fase para los datos comprimidos en términos de: (a) magnificación y (b) el factor de calidad.

Si bien estos resultados parecen mostrar que el escalamiento óptico es más adecuado para la compresión de la información de fase de los datos de campo óptico, vale la pena señalar que la pérdida causada por ambos métodos es cualitativamente diferente. En el caso de escalado óptico, el objeto reconstruido muestra una pérdida de frecuencias altas, mientras que en el caso

de la compresión JPEG muestra un aumento del ruido (<https://goo.gl/HVkdDeD>). En este sentido, el escalado óptico muestra un comportamiento más predecible para los datos de campo óptico.

5.2. Compresión de hologramas a color por medio de máscaras binarias aleatorias

La iluminación con múltiples longitudes de onda es empleada ampliamente en los sistemas de formación de imágenes porque proporciona información a diferentes escalas de color. Las imágenes formadas con múltiples longitudes de onda se han utilizado, por ejemplo, en estudios sobre pinturas de arte [34, 35], para arqueología y la preservación del arte [36], en microbiología para estudios de la piel [37–40], en el análisis de células vivas [41, 42], y muchas otras aplicaciones en las ciencias de la vida [43–46]. Otro campo de investigación que ha aprovechado la ventaja de imágenes a color es el procesamiento óptico de información. En particular, en años recientes se han propuesto e implementado algunos esquemas de encriptación de imágenes a color [47–49]. En general, estas técnicas consisten en registrar y procesar por separado cada uno de sus canales de color, realizar el proceso de encriptación, en enviar la información y recuperar las imágenes a color realizando el proceso de desencriptación y la composición con los canales procesados.

Para registrar información de un objeto a color, este se ilumina con luz correspondiente a los tres canales de color RGB. Los canales tricromáticos RGB se representan como: longitud de onda roja R (*red*), longitud de onda verde G (*green*) y longitud de onda azul B (*blue*) respectivamente. Los hologramas se registran por medio de una técnica de holografía digital para cada longitud de onda por separado usando una cámara digital (CCD o CMOS). Durante la reconstrucción de hologramas de objetos a color, el uso de las distintas longitudes de onda genera tres tipos de acromatización o aberración cromática [50]: aberración cromática de magnificación, aberración cromática lateral y aberración cromática axial. Cuando la reconstrucción de estos hologramas se hace de forma numérica, la acromatización puede superarse mediante el algoritmo de zero-padding, es decir, se ajusta la distancia reconstruida por medio de un sistema óptico virtual [51, 52]. Si la reconstrucción se realiza en un sistema óptico experimental, la acromatización se puede superar mediante el ajuste o corrección de parámetros ópticos asociados al sistema experimental [50, 53, 54]. A continuación, se describe el registro de la información de objetos 3D a color, por medio de un montaje de holografía de Fourier fuera de eje.

5.2.1. Registro y procesamiento de hologramas de objetos 3D a color

La Figura 5.5 muestra el sistema holográfico de Fourier fuera de eje empleado para registrar los hologramas digitales de objetos tridimensionales a color.

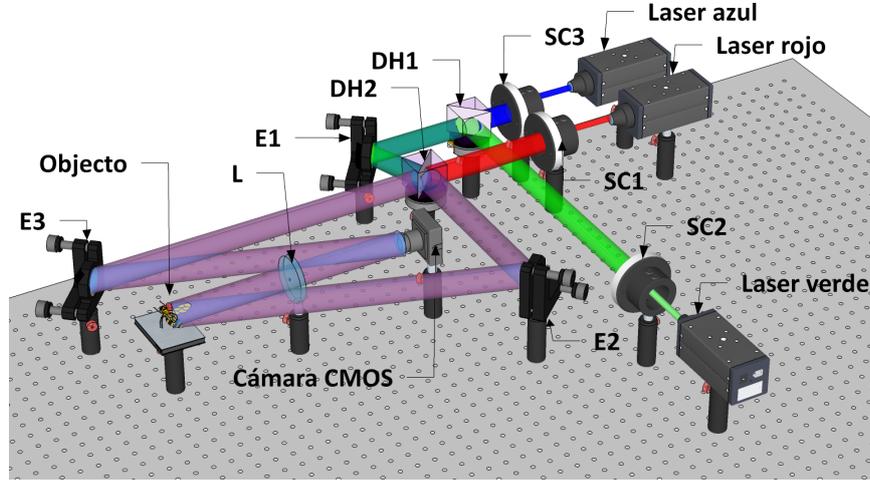


Figura 5.5: Esquema holográfico de Fourier fuera de eje para registrar un objeto 3D en los tres canales RGB. (SC: sistema de colimación, DH: divisor de haz, E: espejos y L: lente de longitud focal f).

Se utilizaron tres fuentes láser, donde cada haz R,G y B colimado pasa a través del divisor de haz DH2, generando un haz que se divide en dos brazos, el brazo objeto y el brazo de referencia. Los haces reflejados por los espejos E2 y E3 son el haz objeto y haz de referencia respectivamente. El haz de referencia interfiere en el plano de la cámara CMOS con el haz que contiene la transformada de Fourier de la luz reflejada por el objeto 3D, esta interferencia se registra por separado para cada canal RGB y se representa como:

$$I(\mu, \nu) = \sum_{\lambda_i=1}^3 H_{\lambda_i}(\mu, \nu) = \sum_{\lambda_i=1}^3 [|O_{\lambda_i}(\mu, \nu)|^2 + |R_{\lambda_i}(\mu, \nu)|^2 + O_{\lambda_i}(\mu, \nu)R_{\lambda_i}^*(\mu, \nu) + O_{\lambda_i}^*(\mu, \nu)R_{\lambda_i}(\mu, \nu)] \quad (5.5)$$

donde λ_i es la longitud de onda de cada fuente láser ($\lambda_1=R$, $\lambda_2=G$ y $\lambda_3=B$), $O_{\lambda_i}(\mu, \nu)$ es la TF del campo objeto para cada canal y $R_{\lambda_i}(\mu, \nu)$ es la onda plana de referencia descrita por [32]:

$$R_{\lambda_i}(\mu, \nu) = e^{2\pi i f(\mu_{\lambda_i} \cos \alpha + \nu_{\lambda_i} \cos \beta)} \quad (5.6)$$

Los ángulos α y β en (5.6) determinan la inclinación de la onda de referencia, f es la longitud focal de la lente, y $\mu_{\lambda_i} = x/\lambda_i f$ y $\nu_{\lambda_i} = y/\lambda_i f$ son las coordenadas en el plano de la cámara

CMOS [32].

Después de registrar los tres hologramas por separado, se procede a filtrar y extraer los datos de campo óptico correspondientes a cada longitud de onda. Vale la pena aclarar que estos datos de campo óptico se obtienen de manera idéntica al obtenido por medio del proceso descrito en la sección 5.1.1 (ver Figura 5.2(b)). Estos tres campos ópticos contienen toda la información necesaria para la reconstrucción del objeto tridimensional a color. Para ajustar el tamaño de píxel reconstruido en los tres canales, y evitar la acromatización, se utiliza el método de zero-padding [51] sobre los datos de campos ópticos. Este método utiliza un mayor número de píxeles en el proceso de reconstrucción rellenando con ceros, de tal manera que el holograma registrado a la mayor longitud de onda $\lambda_R > \lambda_G$, se reconstruye con un número de píxeles igual a: $N_R = N_G(\lambda_R/\lambda_G)$, donde N_G es el número de píxeles en el holograma registrado a la longitud de onda más corta λ_G , para obtener el mismo ancho del píxel reconstruido a una distancia d . Mediante el multiplexado de estos tres campos, se forma un solo paquete $P(\mu, \nu)$ que se representa como:

$$P(\mu, \nu) = \sum_{\lambda_i=1}^3 O_{\lambda_i}(\mu, \nu) \quad (5.7)$$

el cual ocupa un volumen V_P .

La importancia de la información fase en el procesamiento de imágenes se mostró por primera vez en 1981 [55], donde se presentaron varios enfoques para justificar la importancia relativa de los argumentos estadísticos de fase, junto con una serie de argumentos informales que sugieren razones para la importancia de la fase. Trabajos previos sobre reconstrucción de imágenes, han demostrado que la información de fase contenida en un holograma digital es suficiente para la reconstrucción de un objeto difuso [56,57], lo que permite reducir los requisitos de almacenamiento a la mitad con una pérdida mínima de potencia óptica durante la reconstrucción [56]. Por lo tanto el volumen que ocupa la información de fase del campo óptico se representa como: $V_{phase} = V_P/2$. Además, si se realiza reconstrucción de forma experimental utilizando un modulador espacial de luz el cual modula solo en fase pura, entonces solo se requerirá de la información de fase del holograma. Teniendo presente estos aspectos, se retiene entonces solo la información de fase de cada campo óptico $Im(O_{\lambda_i}(\mu, \nu))$. De esta forma, en este trabajo se utilizó la información de fase de los datos de campo óptico para demostrar la validez de una propuesta nueva de compresión, que se describe a continuación.

5.2.2. Técnica de compresión por medio de máscaras binarias aleatorias

Con el objetivo de comprimir la información contenida en la fase de los datos de campo óptico, primero se multiplica la información de fase del campo óptico con una máscara binaria aleatoria, muestreando la información del campo. Al tener múltiples campos ópticos, uno por cada longitud de onda, se requiere crear varias máscaras binarias aleatorias distintas entre sí, de esta manera cada máscara no va a muestrear el mismo píxel a la hora de multiplexar los campos muestreados, es decir, las máscaras deben ser ortogonales entre sí [58]. En este caso particular, para cada objeto 3D se obtienen tres campos ópticos con información de fase, de manera que se requieren tres máscaras binarias distintas para muestrear estos campos antes de ser multiplexados. El número de campos que se multiplexan en un único paquete determina el porcentaje de píxeles blancos que se necesitan para que las máscaras binarias aleatorias sean ortogonales [58]. La ortogonalidad de estas máscaras las hace complementarias y permite la separabilidad de la información dentro del paquete multiplexado. De esta manera, se muestrea cada uno de los tres campos con una máscara binaria distinta con porcentajes de píxeles blancos del 33,3%. Ahora se multiplexa en un solo paquete $PB(\mu, \nu)$ la información de fase de los tres campos ópticos $Im(O_{\lambda_i}(\mu, \nu))$, que fueron muestreados con las máscaras binarias $B_{\lambda_i}(\mu, \nu)$, obteniéndose:

$$PB(\mu, \nu) = \sum_{\lambda_i=1}^3 Im(O_{\lambda_i}(\mu, \nu)) B_{\lambda_i}(\mu, \nu) \quad (5.8)$$

donde este paquete ocupa un volumen V_{PB} . El proceso descrito hasta ahora, se ilustra en el diagrama de flujo de la Figura 5.6.

Por efecto de la multiplicación por las máscaras binarias, el paquete $PB(\mu, \nu)$ ocupa menos volumen que el paquete $P(\mu, \nu)$, siendo más eficiente su almacenamiento y/o transmisión, además contiene la información necesaria para recuperar la información del objeto 3D a color. Cada máscara binaria muestrea un píxel distinto sobre la información de fase del campo óptico respectivo, de esta manera, se puede elegir del paquete $PB(\mu, \nu)$ el l -ésimo dato de campo óptico con solo multiplicar este paquete por la máscara binaria $B_{\lambda_l}(\mu, \nu)$. Este proceso de demultiplexación, es equivalente al proceso de descompresión de información. Una posterior operación TF sobre el l -ésimo dato descomprimido, permite reconstruir la l -ésima componente del objeto 3D asociado a la información de fase del campo óptico muestreado con la máscara binaria $B_{\lambda_l}(\mu, \nu)$ (ver Figura 5.6).

$$R_{\lambda_l}(x, y) = Im(o_{\lambda_l}(x, y)) \otimes b_{\lambda_l}(x, y) \quad (5.9)$$

La ecuación (5.9) corresponde al objeto 3D reconstruido para una sola longitud de onda,

convolucionado con la TF de la máscara binaria aleatoria.

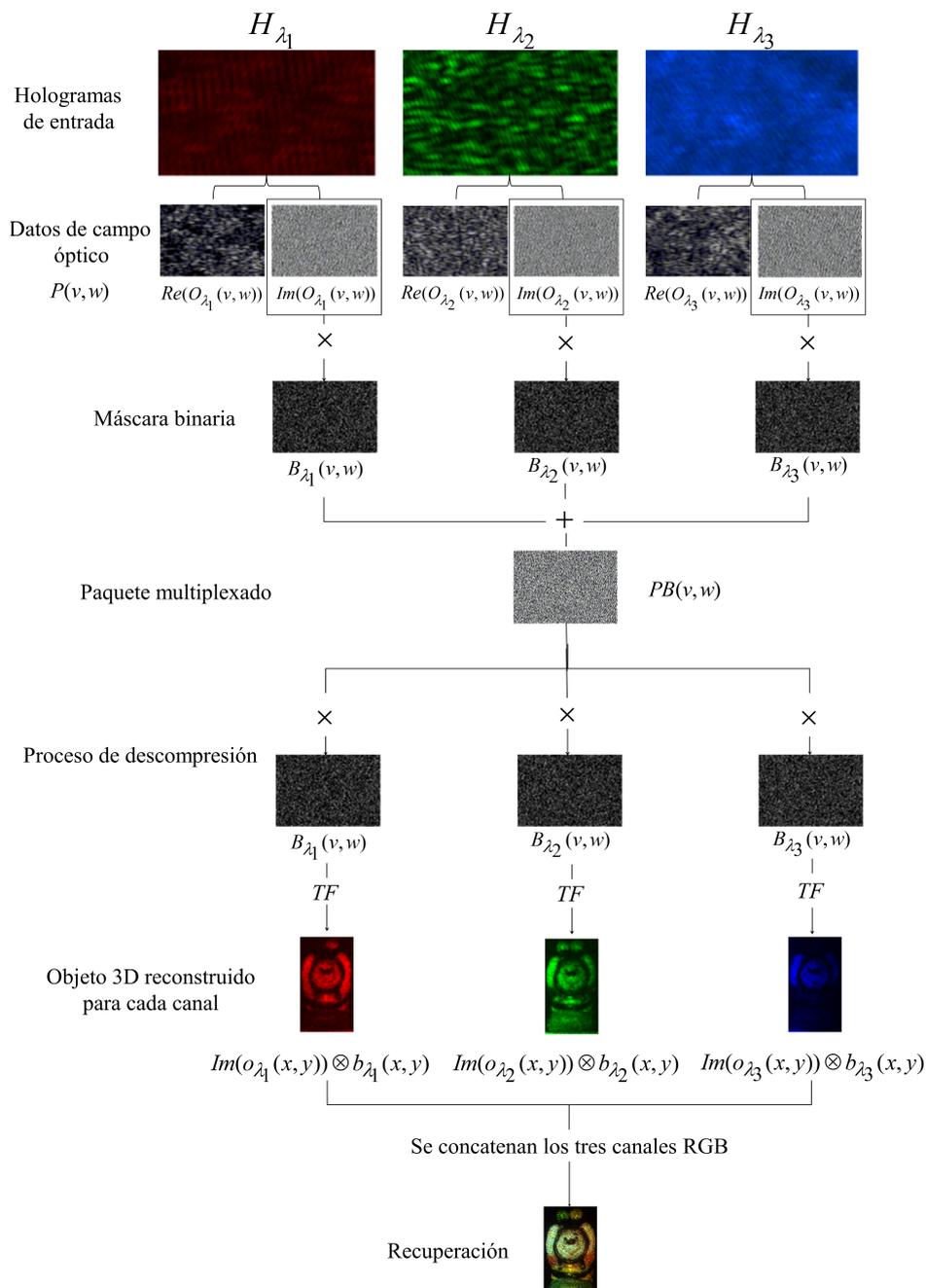


Figura 5.6: Diagrama de flujo donde se ilustra el proceso de compresión propuesto por medio de máscaras binarias complementarias y la recuperación del objeto a color. Re corresponde a la parte real del campo e Im corresponde a la parte imaginaria del campo.

Esta recuperación tendrá un ruido aleatorio de fondo y un pico agudo con una intensidad máxima igual a la intensidad media de $B_{\lambda_i}(\mu, \nu)$. El uso de una máscara aleatoria tiene como ventaja que su TF presenta un pico agudo [32], mientras que la TF de una máscara binaria con distribución no aleatoria puede generar órdenes centrales extendidos, lo que resulta en una reconstrucción borrosa y con pérdidas de frecuencias específicas. Finalmente, cada imagen que compone la secuencia RGB es un arreglo matricial de $M \times N \times 3$ píxeles de color. Cada píxel tiene componentes correspondientes al rojo, verde y azul, por lo tanto, la imagen a color se obtiene mediante la transformación de los valores tricromáticos RGB en el espacio de colores [31]. Por lo tanto, al concatenar las tres imágenes recuperadas, se puede reconstruir el campo del objeto 3D a color (ver Figura 5.6).

5.2.3. Resultados experimentales y desempeño de las técnicas de compresión

Se procesaron cinco objetos, donde cada uno fue registrado, procesado y comprimido (ver la descripción en las secciones 5.2.1 y 5.2.2) con la técnica propuesta, y posteriormente reconstruidos por separado. En la configuración experimental de la Figura 5.5 se utilizó una cámara CMOS EO-10012C, con 3840 píxeles \times 2748 píxeles de resolución, un tamaño de píxel de $1,67\mu m \times 1,67\mu m$ y 8 bits de profundidad. Los láseres utilizados fueron: Laser He-Ne con una longitud de onda de $632nm$ y una potencia de salida de $70mW$ para el rojo, un láser DPSS de Laserglow Technologies con una longitud de onda de $532nm$ y una potencia de $50mW$ para el verde, y un DPSS con una longitud de onda de $472nm$ con una potencia de $150mW$ para el azul. Los objetos 3D tienen dimensiones máximas de aproximadamente $28mm \times 15mm \times 14mm$ y la longitud focal de la lente es de $500mm$.

Para la recuperación óptica experimental (ver Figura 5.7), se emplea un láser DPSS de Laserglow Technologies que opera a una longitud de onda de $532nm$. Un modulador de reflexión de fase HOLOEYE PLUTO-VIS-006-HR, con resolución full HD de 1920 píxeles \times 1080 píxeles y un ancho de píxel de $8\mu m$ con un área activa diagonal de $0,7''$. Este modulador espacial de luz se calibró en la longitud de onda del verde, y la polarización del haz incidente para la modulación de fase pura está a lo largo del eje de visualización más largo. La lente tiene una longitud focal de $260mm$ y una cámara EO-10012C CMOS con una resolución de 3840 píxeles \times 2748 píxeles registra la imagen reconstruida.

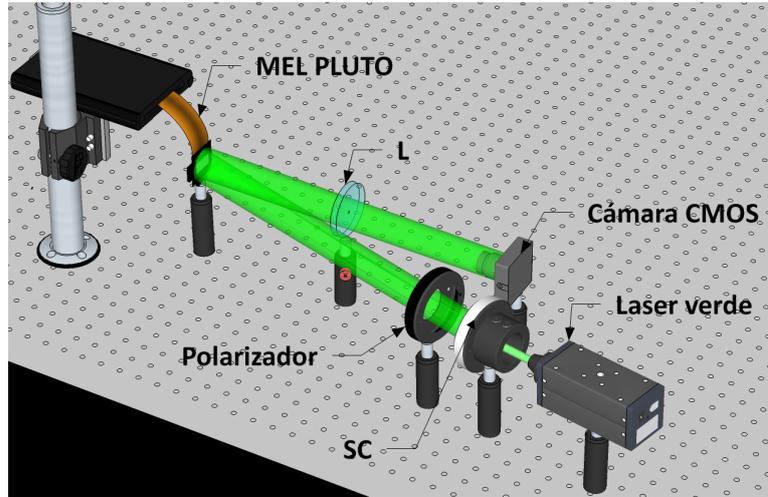


Figura 5.7: Esquema de recuperación experimental. SC: sistema de colimación, MEL: modulador espacial de luz y L: lente de longitud focal f .

En particular, se analiza el volumen para el caso de un objeto registrado con los parámetros experimentales ya definidos. Cada holograma tiene una resolución de $3840 \text{ píxeles} \times 2748 \text{ píxeles}$, resultando con un volumen de $3840 \times 2748 \times 1B = 10,06MB$ cada uno. Generando un volumen total de los tres registros por objeto de $V_H = 30,18MB$. Luego, cada uno de los datos de campo óptico, tiene un tamaño de $1920 \text{ píxeles} \times 1080 \text{ píxeles}$ los cuales deben tener el tamaño de resolución para ser proyectados adecuadamente en el modulador, por lo tanto, cada campo óptico con información de amplitud y fase posee un volumen de $V_{CO} = 2 \times 1920 \times 1080 \times 1B = 3,95MB$, donde el factor de 2 es por la información de amplitud y fase. Posteriormente, multiplexando estos campos se obtiene un paquete (ecuación (5.7)) con un volumen $V_P = 11,85MB$. Teniendo en cuenta que el volumen se divide por igual en amplitud y fase, el paquete que contiene la información de fase de los datos de campo óptico de los objetos tiene un volumen $V_{fase} = 5,925MB$.

Después de aplicar el método de compresión propuesto (sección 5.2.2), se obtiene un paquete (ecuación (5.8)) con un volumen $V_{PB} = 1,98MB$. Con respecto al volumen inicial $V_H = 30,18MB$, la reducción del volumen total fue del $93,44\%$, donde por proceso de filtrado y retención de la fase aportan una reducción de volumen del $80,36\%$, mientras que el proceso de máscaras binarias aporta un $13,08\%$. Esta reducción en el volumen se debe a la multiplicación de la fase de los datos de campo de óptico con las máscaras binarias que poseen una porcentaje de píxeles negros (con valor cero), que en este caso es del $66,66\%$. Este paquete es almacenado y/o enviado para su posterior descompresión, tal y como se muestra en la Figura 5.6.

Cada uno de los datos del campo óptico descomprimidos se proyecta por separado en el modulador. El haz que incide sobre la pantalla del modulador se refleja con un ángulo menor a 5° (de acuerdo a las especificaciones del modulador) y es procesado por la lente L (ver Figura 5.7). En la cámara se registra la TF del haz reflejado por el MEL en niveles de gris entre 0 y 255, que es la respectiva componente recuperada. Posteriormente, se concatenan o se enlazan los valores de las componentes recuperadas para finalmente reconstruir el objeto a color [31].

En la Figura 5.8 se muestra la recuperación óptico virtual del esquema que se muestra en la Figura 5.7 cuando se procesan cinco objetos a color. Cada objeto fue registrado, procesado, comprimido por medio de las máscaras binarias, multiplexado y recuperado con el proceso descrito en este capítulo. En la Figura 5.8 (a) se muestra la recuperación cuando se tienen los datos de campo óptico con la información de amplitud y de fase, mientras en la Figura 5.8 (b) se muestra la recuperación cuando solo se tiene la información de fase de los datos de campo óptico. Y en la Figura 5.8 (c) se muestra la recuperación cuando se tienen los datos de campo óptico de fase que fueron muestreados con las máscaras binarias complementarias. Comparando las tres recuperaciones puede observar una degradación que aumenta a medida que se aplica el método de compresión. Esta degradación esta asociada con la información que se descarta cuando se toma la información de fase, y posteriormente al efecto de las máscaras binarias.

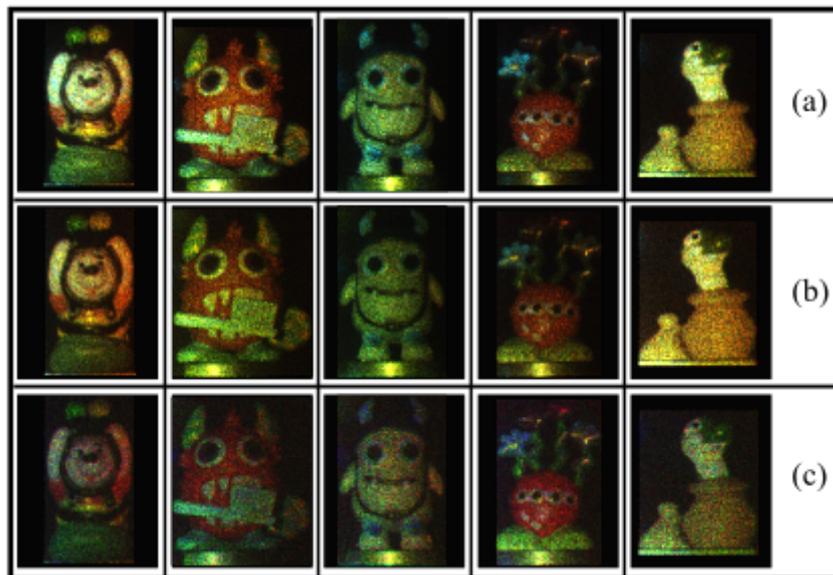


Figura 5.8: Panel de los cinco objetos recuperados por el sistema óptico virtual con información de (a) amplitud y fase de los campos ópticos, (b) fase de los campos ópticos y (c) fase de los campos ópticos muestreados con máscaras binarias.

Adicionalmente, en la Figura 5.9 se presenta la respectiva recuperación experimental realizada usando el montaje de la Figura 5.7. Comparando las Figuras 5.9 (a) y (b) se observa que en la Figura 5.9 (a) se presenta una degradación de la recuperación que esta asociado a la información que se descarta cuando se muestra la información de fase de los datos de campo óptico con las máscaras binarias. En la Figura 5.9 (b) se evidencia más el ruido asociado al uso de las máscaras binarias complementarias. A pesar de las diferencias entre la recuperación con un sistema óptico virtual y un sistema experimental, las recuperaciones de las Figuras 5.8 (b) y (c) y las Figuras 5.9 (a) y (b) son comparables.

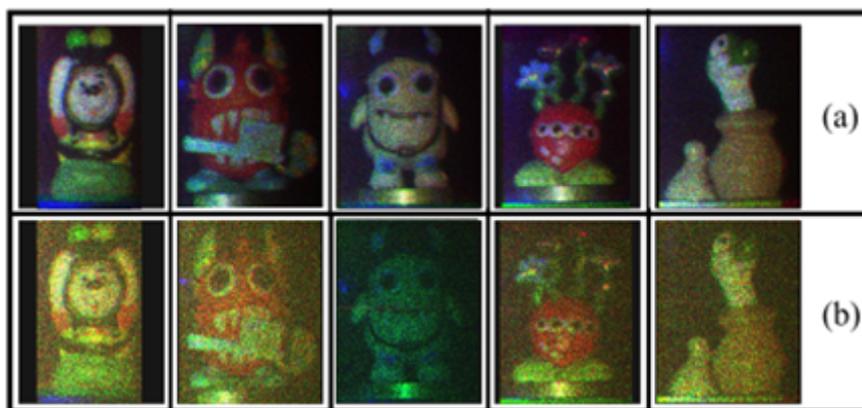


Figura 5.9: Panel de los cinco objetos recuperados por el sistema óptico experimental de la Figura 5.7. Con información de (a) fase de los campos ópticos y (c) fase de los campos ópticos muestreados con máscaras binarias.

En este caso, comparando el volumen final $V_{PB} = 1,98MB$ con respecto al volumen inicial $V_H = 30,18MB$ la reducción del volumen total fue del 93,44 %, donde los datos de campo óptico con información solo de fase contribuye a una reducción del volumen del 80,36 %. Por consiguiente el método de máscaras binarias aportó una reducción en el volumen de 13,08 %.

Vale la pena aclarar, que el proceso de compresión descrito en esta sección fue implementado sobre cada uno de los objetos por separado, y que su reconstrucción requiere de tres campos ópticos con información de fase asociados a cada canal de color RGB. Este método puede extenderse al multiplexado de datos de campo óptico de múltiples objetos 3D a color. En ese caso, para cada objeto se tendrán tres campos ópticos. Por lo tanto, al aumentar la cantidad de campos ópticos a multiplexar se incrementa el número de máscaras binarias aleatorias y complementarias, lo que implica una reducción en la cantidad de píxeles blancos (con valor 1) que contienen las máscaras.

En la primera sección de este capítulo, fue comparada la reducción de volumen que brindan

la técnica de escalado óptico y la técnica digital de compresión JPEG, cuando se aplican sobre datos de campo óptico provenientes de información holográfica de un objeto 3D. Además, usando el coeficiente de correlación se hizo un análisis del efecto que tienen estas técnicas de compresión sobre la información recuperada. Los resultados evidencian que la técnica de escalado óptico presenta un mejor rendimiento que la técnica de compresión digital JPEG para los datos de campo óptico. Además, se muestra que la técnica de escalado óptico presenta un comportamiento similar cuando comprime la información de fase y de amplitud del campo óptico, mientras que la técnica digital JPEG presenta un desempeño significativamente menor cuando se aplica sobre la información de fase. Se debe destacar que los resultados presentados en esta sección hacen parte de los resultados originales de esta tesis y fueron publicados en una revista internacional (Ver el Apéndice A).

En la segunda sección se propuso e implementó una técnica de compresión que se aplicó sobre hologramas de objetos 3D a color. Esta técnica posee dos etapas, la primera consiste en tomar solo la información de fase de los datos de campo óptico, y en la segunda se muestrea la información de fase por medio de máscaras aleatorias binarias y complementarias. Como la técnica se aplica sobre la información holográfica asociada a los canales RGB del objeto a color, se incluye una técnica de multiplexado para generar un paquete de datos comprimidos a partir del cual se puede recuperar el campo del objeto 3D a color. Los resultados de la recuperación obtenidos por medio de un sistema óptico virtual y un montaje experimental son comparables, donde el proceso de reducción de volumen conduce a una degradación de la imagen que está asociada a la información que se descarta en cada etapa de la técnica. Aplicando esta técnica se alcanzó una reducción de volumen del 93,44 % con una recuperación aceptable, donde el proceso de máscaras binarias complementarias contribuyó con el 13,08 %, lo que demuestra la gran efectividad y potencialidad de este método de compresión. Estos resultados hacen parte de los resultados originales de este trabajo de investigación.

- [1] W. Osten, A. Faridian, P. Gao, K. Körner, D. Naik, G. Pedrini, A.K. Singh, M. Takeda, M. Wilke. *Recent advances in digital holography (Invited)*. Appl. Opt., 53:G44–G63, 2014.
- [2] V. Jaedicke, S. Goebel, N. Koukourakis, N.C Gerhardt, H. Welp, M.R Hofmann. *Multi-wavelength phase unwrapping and aberration correction using depth filtered digital holography*. Opt. Lett., 39:4160–4163, 2014.
- [3] D. Merrill, R. An, J. Turek, D.D Nolte. *Digital holography of intracellular dynamics to probe tissue physiology*. Appl. Opt., 54:A89–A97, 2015.
- [4] B. Javidi, A.Carnicer, M. Yamaguchi, T. Nomura, E. Pérez-Cabré, M.S. Millán, N.K. Nishchal, R. Torroba, J.F Barrera, W. He, X. Peng, A. Stern, Y. Rivenson, A. Alfalou, C. Brosseau, C. Guo, J.T. Sheridan, G. Situ, M.Naruse, T. Matsumoto, I. Juvells, E. Tajahuerce, J. Lancis, W. Chen, X. Chen, P.W. Pinkse, A.P. Mosk, A. Markman. *Roadmap on optical security*. Journal of Optics, 18:083001, 2016.
- [5] X. Shen, C. Lin, D. Kong. *Fresnel–transform holographic encryption based on angular multiplexing and random–amplitude mask*. Opt. Eng., 51:068201, 2012.
- [6] F. Mosso, M.Tebaldi, J.F. Barrera, N. Bolognini, R. Torroba. *Pure optical dynamical color encryption*. Opt. Exp., 19:13779–13786, 2011.
- [7] J.F. Barrera, R. Henao, M. Tebaldi, R. Torroba, N. Bolognini. *Multiplexing encrypted data by using polarized light*. Opt. Commun., 260:109–112, 2006.
- [8] J. Lin, X.C Yuan, S.H Tao, R.E Burge. *Multiplexing free-space optical signals using superimposed collinear orbital angular momentum states*. Appl. Opt., 46:4680–4685, 2007.

-
- [9] S. Trejos, J.F. Barrera, M. Tebaldi, R. Torroba. *Experimental opto-digital processing of multiple data via modulation, packaging and encryption*. J. Opt., 16:055402, 2014.
- [10] W. Chen, X. Chen. *Digital holography-secured scheme using only binary phase or amplitude as ciphertext*. Appl. Opt., 55:6740–6746, 2016.
- [11] V. Micó, C. Ferreira, J. Garcia. *Lensless object scanning holography for two-dimensional mirror-like and diffuse reflective objects*. Appl. Opt., 52:6390–6400, 2013.
- [12] G. Nehmetallah, P.P Banerjee. *Applications of digital and analog holography in three-dimensional imaging*. Adv. Opt. Photon., 4:472–553, 2012.
- [13] F. Mosso, J.F. Barrera, M. Tebaldi, N. Bolognini, R. Torroba. *All-optical encrypted movie*. Opt. Exp., 19:5706–5712, 2011.
- [14] C. Lin, X. Shen, B. Li. *Four-dimensional key design in amplitude, phase, polarization and distance for optical encryption based on polarization digital holography and QR code*. Opt. Exp., 22:20727–20739, 2014.
- [15] W. Chen. *Multiple-wavelength double random phase encoding with CCD-plane sparse-phase multiplexing for optical information verification*. Appl. Opt., 54:10711–10716, 2015.
- [16] A. Velez, J.F. Barrera, R. Torroba. *One-step reconstruction of assembled 3D holographic scenes*. Opt. Laser Technol., 75:146–150, 2015.
- [17] U. Schnars, W.P.O Jüptner. *Digital recording and numerical reconstruction of holograms*. Meas. Sci. Technol., 13:R85–R101, 2002.
- [18] E. Darakis, J.J Soraghan. *Reconstruction domain compression of phase-shifting digital holograms*. Appl. Opt., 46:351–356, 2007.
- [19] G.A Mills, I. Yamaguchi. *Effects of quantization in phase-shifting digital holography*. Appl. Opt., 44:1216–1225, 2005.
- [20] O. Matoba, T.J Naughton, Y. Frauel, N. Bertaux, B. Javidi. *Real-time three-dimensional object reconstruction by use of a phase-encoded digital hologram*. Appl. Opt., 41:6187–6192, 2002.
- [21] E. Cuhe, P. Marquet, C. Depeursinge. *Spatial filtering for zero-order and twin-image elimination in digital off-axis holography*. Appl. Opt., 39:4070–4075, 2000.
- [22] T.J Naughton, Y. Fraue, B. Javidi, E. Tajahuerce. *Compression of digital holograms for three-dimensional object reconstruction and recognition*. Appl. Opt., 41:4124–4132, 2002.

-
- [23] A. Alfalou, C. Brosseau. *Implementing compression and encryption of phase- shifting digital holograms for three-dimensional object reconstruction*. *Opt. Commun.*, 307:67–72, 2013.
- [24] T. Nomura, A. Okazaki, M. Kameda, Y. Morimoto, B. Javidi. *Image reconstruction from compressed encrypted digital hologram*. *Opt. Eng.*, 44:1–7, 2005.
- [25] S.T. Sateesh, R. Sakthivei, K. Nirosha, H.M Kittur. *An optimized architecture to perform image compression and encryption simultaneously using modified DCT algorithm*. In *International Conference on Signal Processing, Communication, Computing and Networking Technologies*, pages 442–447, 2011.
- [26] D. Blinder, T. Bruylantsa, E. Stijns, H. Ottevaere, P. Schelkens . *Wavelet coding of off-axis holographic images*. page 88561L. SPIE, 2013.
- [27] T. Bruylantsr,D. Blinder, H. Ottevaere, A. Munteanu, P. Schelkens . *Microscopic off-axis holographic image compression with JPEG 2000*. page 91380F. SPIE, 2014.
- [28] G.K Wallace. *The JPEG still picture compression standard*. In *IEEE Trans. Consum. Electron.*, volume 38, page xviii–xxxiv, 1992.
- [29] D.A Huffman. *A method for the construction of minimum-redundancy codes*. *Proc. IRE*, 40:1098–1101, 1952.
- [30] E.A. Kurbatova, P.A. Cheremkhin, N.N. Evtikhiev, V.V. Krasnov, S.N. Starikov. *Methods of Compression of Digital Holograms*. *Physics Procedia*, 73:328 – 332, 2015.
- [31] R.W.G. Hunt. *Measuring Color*. Fountain Press, England, 4th ed. edition, 1998.
- [32] J.W Goodman. *Introduction to Fourier Optics*. McGraw-Hill, 2nd ed. edition, 1996.
- [33] R. Shahnaz, J.F. Walkup, T.F Krile. *Image compression in signal-dependent noise*. *Appl. Opt.*, 38:5560–5567, 1999.
- [34] S. Baronti, A. Casini, F. Lotti, S. Porcinai . *Multispectral imaging system for the mapping of pigments in works of art by use of principalcomponent analysis*. *Appl. Opt.*, 37:1299–1309, 1998.
- [35] A. Pelagotti, A. D. Mastio, A. D. Rosa, A. Piva . *Multispectral imaging of paintings*. *IEEE Signal Process. Mag.*, 25:27–36, 2008.
- [36] H. Liang . *Advances in multispectral and hyperspectral imaging for archaeology and art conservation*. *Appl. Phys. A* , 106:309–323, 2012.

-
- [37] A.N. Yaroslavsky, J. Barbosa, V. Neel, C. DiMarzio, R. R. Anderson . *Combining multispectral polarized light imaging and confocal microscopy for localization of nonmelanoma skin cancer*. J. Biomed. Opt., 10:014011, 2005.
- [38] A. Bekina, I. Diebele, U. Rubins, J. Zaharans, A. Derjabo, J. Spigulis . *Multispectral assessment of skin malformations using a modified video-microscope*. Latv. J. Phys. Tech. Sci. , 49:4–8, 2012.
- [39] I. Kuzmina, I. Diebele, D. Jakovels, J. Spigulis, L. Valeine, J. Kapostinsh, A. Berzina. *Towards noncontact skin melanoma selection by multispectral imaging analysis*. J. Biomed. Opt., 16:060502, 2011.
- [40] M. Lee, O. Yaglidere, A. Ozcan. *Field-portable reflection and transmission microscopy based on lensless holography*. Biomed. Opt. Express, 2:2721–2730, 2011.
- [41] Y. Hiraoka, T. Shimi, T. Haraguchi. *Multispectral imaging fluorescence microscopy for living cells*. Cell Struct. Funct., 27:367–374, 2002.
- [42] J. Haseloff. *GFP variants for multispectral imaging of living cells*. Methods Cell Biol., 58:139–151, 1998.
- [43] R. M. Levenson, J. R. Mansfield. *Multispectral imaging in biology and medicine: slices of life*. Cytom. A , 69:748–758, 2006.
- [44] D. Roblyer, R. Richards-Kortum, K. Sokolov, A. K. El-Naggar, M. D. Williams, C. Kura-chi, A. M. Gillenwater. *Multispectral optical imaging device for in vivo detection of oral neoplasia*. J. Biomed. Opt., 13:024019, 2008.
- [45] M. A. Roula, J. Diamond, A. Bouridane, P. Miller, A. Amira. *A multispectral computer vision system for automatic grading of prostatic neoplasia*. in Proceedings of IEEE International Symposium on Biomedical Imaging (IEEE, 2002), page 193–196, 2002.
- [46] Hu, Q. Wu, S. Liu, L. Wei, X. Chen, Z. Yan, J. Yu, L. Zeng, Y. Ding. *Study of rice pollen grains by multispectral imaging microscopy*. Microsc. Res. Tech., 68:335–346, 2005.
- [47] L Chen, D. Zhao. *Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms*. Opt. Exp., 14:8552–8560, 2006.
- [48] L Chen, D. Zhao. *Color information processing (coding and synthesis) with fractional Fourier transforms and digital holography*. Opt. Exp., 15:16080–16089, 2007.
- [49] M. Joshi, Chandrashakher, K. Singh. *Color image encryption and decryption using fractional Fourier transform*. Opt. Commun., 279:35–42, 2007.

-
- [50] J. Wang, H.D. Zheng, Y.J. Yu. *Achromatization in Optical Reconstruction of Computer Generated Color Holograms*. J. Display Technol., 12:390–396, 2016.
- [51] P. Ferraro, S. De Nicola, G. Coppola, A. Finizio, D. Alfieri, G. Pierattini. *Controlling image size as a function of distance and wavelength in Fresnel-transform reconstruction of digital holograms*. Opt. Lett., 29:854–856, 2004.
- [52] J. L. Zhao, H. Z. Jiang, J. L. Di. *Recording and reconstruction of a color holographic image by using digital lensless Fourier transform holography*. Opt. Exp., 16:2514–2519, 2008.
- [53] K. Sato. “*Record and display of color 3-D images by electronic holography*. In *Adaptive Optics: Analysis and Methods/Computational Optical Sensing and Imaging/Information Photonics/Signal Recovery and Synthesis Topical Meetings*, volume DWA2 of OSA Tech. Dig. Proc., page 1–3, 2007.
- [54] M. Morimoto, K. Fujii, K. Sato, A. Sugita. *Reconstruction of color images of high quality by a holographic display*, 2006.
- [55] A.V. Oppenheim, J.S. Lim. *The importance of phase in signals*. Proceedings of the IEEE, 69:529–541, 1981.
- [56] O. Matoba, T.J. Naughton, Y. Frauel, N. Bertaux, B. Javidi. *Real-time three-dimensional object reconstruction by use of a phase-encoded digital hologram*. Appl. Opt., 41:6187–6192, 2002.
- [57] I. Yamaguchi, Ka. Yamamoto, G.A. Mills, M. Yokota. *Image reconstruction only by phase data in phase-shifting digital holography*. Appl. Opt., 45:975–983, 2006.
- [58] J.A. Davis, D.M. Cottrell. *Random mask encoding of multiplexed phase-only and binary phase-only filters*. Opt. Lett., 19:496–498, 1994.

CAPÍTULO 6

CONCLUSIONES Y PERSPECTIVAS

Este trabajo de investigación se orientó al estudio e implementación de técnicas ópticas análogo-digitales para el procesamiento de múltiples datos y compresión de información. Las técnicas se aplicaron sobre información holográfica de datos que fueron procesados por sistemas ópticos, y registrados por una técnica de holografía de Fourier fuera de eje. Como primera etapa del proceso, se aplicó una técnica de filtrado sobre cada holograma, con el fin de eliminar la información redundante, y obtener lo que se denominó dato de campo óptico, que es la información a partir de la cual se puede recuperar la información de interés.

Inicialmente se manipularon múltiples hologramas de datos bidimensionales (2D) procesados por medio de los sistemas de encriptación $2f$ y JTC . Con el fin de manipular eficientemente la información encriptada, se aplicó un proceso de multiplexado por posicionamiento a los datos de campo óptico obtenidos a partir de estos hologramas. El multiplexado por posicionamiento permite que los datos de campo óptico estén contenidos en un solo paquete de información (o un solo dato), lo que permite un manejo eficiente de la información pues facilita su almacenamiento, envío y recepción. Además, todos los objetos se recuperan en el mismo plano, al mismo tiempo y sin superposición usando un sistema de recuperación compacto. Una ventaja adicional del proceso, es que la manipulación de los múltiples datos se puede llevar a cabo sin necesidad de alterar la configuración del montaje experimental o de introducir elementos adicionales. Lo anterior implica que la técnica de multiplexado por posicionamiento es una herramienta válida para la manipulación eficiente de múltiples datos.

Por otro lado, cuando se manipulan datos encriptados se deben incluir mecanismos que eli-

minen o reduzcan significativamente el ruido generado por el procesamiento óptico. Teniendo en cuenta lo anterior, en la primera parte del trabajo de investigación se propuso e implementó por primera vez un protocolo multiusuario para manipular mensajes de forma segura, eficiente y con recuperación libre de ruido. El protocolo consiste en codificar en códigos QR la información que se desea proteger, los códigos son encriptados por medio de un sistema de encriptación $2f$ y a sus hologramas se les aplica los procesos de filtrado y multiplexado por posicionamiento. Como aplicación particular, se encriptaron los códigos QR de varios caracteres del alfabeto, de manera que al realizar el procedimiento de desencriptación se obtiene el panel de códigos QR. Finalmente, una llave de secuencia brinda la información sobre el orden en que se deben leer los códigos para generar un mensaje particular sin ningún tipo de ruido o degradación. De esta forma, aunque muchos usuarios autorizados puedan acceder al panel de códigos QR desencriptados, cada uno debe poseer la llave de secuencia para recuperar el mensaje que le corresponde. Por lo tanto, el sistema de encriptación permite un manejo seguro de la información, mientras que el proceso de filtrado y multiplexado permite un manejo eficiente de los datos. La recuperación libre de ruido se debe a la codificación de la información que se desea proteger en códigos QR, ya que aunque los códigos QR desencriptados poseen el ruido generado por el procesamiento óptico-digital de la información, su lectura es tolerante al ruido y permite decodificar la información que contiene el código.

El procesamiento y registro de múltiples datos encriptados, y en general de múltiples hologramas, deriva en una gran cantidad de información que se debe procesar, almacenar y/o transmitir. Por esto, la segunda parte del trabajo de investigación se centró en analizar la reducción de volumen, que conlleva el proceso de filtrado y la aplicación de técnicas de reducción de volumen, también llamadas técnicas de compresión, a los datos de campo óptico provenientes de sistemas de encriptación $2f$ y JTC . Inicialmente se aplicó la técnica de compresión digital de cuantización, con el fin de reducir el volumen variando la profundidad de bits sobre el paquete de datos de campo óptico que fueron obtenidos a partir de datos encriptados por un sistema de encriptación $2f$. Los resultados muestran que combinando procesos de filtrado y cuantización, se logra una reducción de volumen del 96,7%, donde el filtrado aporta un 93,4% de la reducción y el proceso de cuantización a 4 bits contribuye con una reducción del 3,3%.

Debido a que se está tratando con información obtenida por sistemas ópticos, surgió la idea de generar mecanismos ópticos para la reducción del volumen de los datos que se manipulan con técnicas ópticas análogo-digitales. En esta dirección, se planteó e implementó una nueva técnica de reducción de volumen que se denominó escalado óptico. En esta técnica se usa un

sistema óptico virtual que usa una lente convergente para magnificar (o escalar) los datos de campo óptico. Los resultados demuestran que el escalado óptico tiene un desempeño superior a las técnicas digitales de cuantización y el escalado digital. El desempeño en la reducción de volumen se determinó por medio del factor de reducción, el factor de eficiencia, el error cuadrático medio normalizado y el coeficiente de correlación. Además, por medio de la estadística speckle de primer y segundo orden, se evidenció que la técnica de escalado óptico permite preservar la información que contiene el multiplexado de datos de campo óptico, lo que muestra la potencialidad que tiene la técnica para reducción de volumen de múltiples datos obtenidos en los sistemas de encriptación análogo-digitales.

Al evidenciarse un mejor desempeño por parte del escalado óptico para comprimir múltiple información encriptada y registrada holográficamente, se decidió aplicar el escalado óptico sobre los datos de campos ópticos obtenidos a partir de hologramas de objetos tridimensionales (3D), dando lugar a la tercera parte de este trabajo de investigación. Primero, se implementó el escalado óptico sobre el dato de campo óptico de un holograma registrado por medio de un sistema de holografía de Fourier fuera de eje. Como el escalado óptico es un método de compresión por pérdida, se comparó con un formato de compresión digital por pérdida como el JPEG, ambos aplicados sobre el mismo dato de campo óptico. Al analizar el comportamiento y desempeño de ambas técnicas por medio del coeficiente de correlación y la diferencia de volumen, se logró mostrar que la fase lleva una cantidad significativa de la información holográfica. Además, se verificó que el procedimiento de escalado óptico presenta un mejor rendimiento que la compresión JPEG cuando se aplica sobre distribuciones aleatorias.

Posteriormente, se planteó y aplicó una técnica novedosa de compresión sobre la información de fase de los datos de campo óptico obtenidos de hologramas de objetos 3D a color. Para cada objeto se registran tres hologramas, uno por para canal de color RGB, y luego se obtienen los respectivos datos de campo óptico y se retiene su información de fase. La técnica que se propone aprovecha la redundancia de la información holográfica que se procesa, para muestrear la información de fase de los datos de campo óptico por medio de máscaras binarias aleatorias y complementarias. Luego, la información de fase muestreada es multiplexada para formar un único paquete de información. A partir del paquete y cada una de las máscaras, se puede seleccionar la información de fase de cada uno de los datos de campo óptico para reconstruir la información de cada uno de los canales RGB por separado. Finalmente, concatenando la información de los canales se puede recuperar el objeto 3D a color. El procesamiento de los hologramas condujo a una compresión del 93,44 %, donde el filtrado y la retención de la información de fase con-

tribuyeron con el 80,36 %, y la compresión con máscaras binarias aportó el 13,08 %. En este caso no es necesario aplicar la técnica de multiplexado por posicionamiento, ya que las máscaras complementarias tienen una propiedad de selectividad que permite obtener de la información de cada uno de los datos de campo óptico muestreados a partir del paquete. Los resultados muestran que la técnica de muestreo por máscaras complementarias es una alternativa válida y con gran potencial para la reducción del volumen de información holográfica.

Los métodos de compresión que propusieron e implementaron en este trabajo de investigación demuestran un mejor rendimiento que algunas técnicas digitales. El escalado óptico aportó un 17,06 % de reducción de volumen y la compresión por máscaras un 13,08 %. Demostrando que los métodos de reducción de volumen desarrollados en este trabajo son una gran alternativa para comprimir información holográfica. Se debe tener en cuenta que el proceso de filtrado que se aplicó a todos los hologramas procesados en este trabajo contribuye a una reducción de volumen entre el 60,73 % y el 93,4 % de la compresión total.

A partir de este trabajo de investigación surgen algunas preguntas y temas de trabajo que serán el motivo de las futuras investigaciones que se describen a continuación:

1. Investigar el rango de aplicabilidad de las propuestas de compresión presentadas en este trabajo. Por ejemplo, aplicar estos métodos en los campos de investigación donde se realicen registros holográficos.
2. Evidenciar el gran potencial de las técnicas propuestas aplicándolas en procesos donde se manipule un volumen significativo de información, ya que en esos casos se puede alcanzar un ahorro relevante. Por ejemplo, cuando se manipula una gran cantidad de datos holográficos que contienen escenas dinámicas (vídeos).
3. Aunque las técnicas de multiplexado empleadas en este trabajo permiten un manejo eficiente de la información, no contribuyen a la reducción de volumen. Por lo tanto, es necesario explorar otras técnicas de multiplexado, buscando que ellas aporten a la reducción en el volumen de datos que se están manipulando.
4. Aplicar las técnicas propuestas en este trabajo sobre los hologramas, y no sobre los datos de campo óptico. Por ejemplo, con el objeto de determinar si el escalado óptico es más eficiente que los métodos de compresión digitales cuando se aplica a hologramas con franjas interferométricas.
5. Ya que la información puede ser recuperada usando la información de fase de los datos de campo óptico, se deben implementar métodos análogos-digitales que conduzcan a un

aumento en el porcentaje de la reducción de la información de fase. Buscando a su vez, que se pueda manejar una cantidad significativa de objetos donde la pérdida de información por el proceso de compresión no comprometa el reconocimiento de los datos recuperados.

6. Realizar una comparación entre el método de compresión con máscaras complementarias y un método de compresión digital como el JPEG. Donde el desempeño en la reducción de volumen de ambos métodos se determine sobre recuperaciones obtenidas por medio de sistemas ópticos virtuales y experimentales.
7. Explorar nuevos procedimientos que permitan recuperar la información libre de ruido y degradación, y su efecto sobre la reducción de volumen.

Al final de esta tesis se incluye un apéndice donde se enumeran las publicaciones realizadas en el marco de este trabajo de investigación, así como las conferencias y presentaciones en eventos nacionales e internacionales. Además, se incluye la información relacionada con los reconocimientos y premios obtenidos por medio de las investigaciones realizadas en el desarrollo de este trabajo de investigación.

APÉNDICE A

LISTA DE PUBLICACIONES, TRABAJOS EN EVENTOS Y RECONOCIMIENTOS

Algunas de las contribuciones originales de este trabajo de grado fueron la base para las siguientes publicaciones:

1. *Optimized and secure technique for multiplexing QR code images of single characters: application to noiseless messages retrieval.* Sorayda Trejos, John Fredy Barrera, Roberto Torroba, *Journal Of Optics*, publicado el 31 de julio de 2015, doi:10.1088/2040-8978/17/8/085702.
2. *Optical approach for the efficient data volume handling in experimentally encrypted data.* Sorayda Trejos, John Fredy Barrera, Alejandro Velez, Myrian Tebaldi, Roberto Torroba, *Journal Of Optics*, publicado el 5 de abril de 2016, doi:10.1088/2040-8978/18/6/065702.
3. *Optical field data compression by optodigital means.* Alejandro Velez, John Fredy Barrera, Sorayda Trejos, Myrian Tebaldi, Roberto Torroba, *Journal Of Optics*, publicado el 1 de noviembre de 2016, doi:10.1088/2040-8978/18/12/125701.
4. *Compression of multiple 3D color scenes with experimental recording and reconstruction.* Sorayda Trejos, John Fredy Barrera, Alejandro Velez, Myrian Tebaldi, Roberto Torroba, *En referato en la revista Optics Letters*.

También, en el desarrollo de este trabajo de investigación se presentaron los siguientes trabajos en congresos internacionales y nacionales:

1. *Secure opto-digital protocol to handle messages using the multiplexing of processed QR codes. Presentación modalidad póster.* Sorayda Trejos, John Fredy Barrera y Roberto To-

rroba. *Libro de resúmenes: VI International Conference on Speckle Metrology, Hotel Camino Real en Guanajuato-México, agosto 24 al 26 del 2015.*

2. *Reducción del volumen de información holográfica. Presentación modalidad oral.* Sorayda Trejos, John Fredy Barrera, Roberto Torroba, Alejandro Velez y Myrian Tebaldi. *Libro de resúmenes: XIV Encuentro Nacional De Óptica (XIV ENO) Y V Conferencia Andina Y Del Caribe En Óptica Y Sus Aplicaciones (V CANCOA), Universidad del Valle en Cali-Colombia, noviembre 16 al 20 del 2015.*
3. *Protocolo ópto-digital para el manejo seguro de mensajes con recuperación libre de ruido. Presentación modalidad póster.* Sorayda Trejos, John Fredy Barrera y Roberto Torroba. *Libro de resúmenes: XIV Encuentro Nacional De Óptica (XIV ENO) Y V Conferencia Andina Y Del Caribe En Óptica Y Sus Aplicaciones (V CANCOA), Universidad del Valle en Cali-Colombia, noviembre 16 al 20 del 2015.*
4. *Reducción del volumen de datos holográficos mediante escalado óptico. Presentación modalidad póster.* Sorayda Trejos, John Fredy Barrera, Roberto Torroba, Alejandro Velez y Myrian Tebaldi. *Libro de resúmenes: IX Reunión Iberoamericana de Óptica y XII Reunión Iberoamericana de Óptica, Láseres y Aplicaciones (RIAO/OPTILAS 2016), Pucon-Chile, noviembre 21 al 25 del 2016.*

Además, se recibieron los siguientes reconocimientos:

1. El artículo *Optical field data compression by opto-digital means* fue seleccionado para ser incluido en la exclusiva sección *IOPselect* de la plataforma científica *IOPscience*. Enlace <http://iopscience.iop.org/collection/10/1;jsessionid=84892A23A8DDA65F88387F21BDF64340.c3.iopscience.cld.iop.org>.

Posteriormente fue elegido como uno de los artículos del año *Highlights of 2016* de la revista *Journal of Optics*. Enlace <http://iopscience.iop.org/journal/2040-8986/page/Highlights-of-2016>.

Además, días después de su publicación en noviembre de 2016, fue elegido artículo de la semana (*Paper of the week*) de la revista *Journal of Optics*.

2. El artículo *Optimized and secure technique for multiplexing QR code images of single characters: application to noiseless messages retrieval*, fue seleccionado para ser incluido

en la sección *Lab talk: Optical cryptography* en la revista *Journal of Optics*. en agosto de 2015.

Enlace <http://iopscience.iop.org/journal/2040-8986/labtalk/article/63208>.

3. El trabajo *Secure opto-digital protocol to handle messages using the multiplexing of processed QR codes*. Sorayda Trejos, John Fredy Barrera y Roberto Torroba. Obtuvo el segundo puesto en la categoría póster en el evento *VI International Conference on Speckle Metrology, Hotel Camino Real en Guanajuato-México, agosto 24 al 26 del 2015*.
4. El trabajo *Reducción del volumen de información holográfica*. Sorayda Trejos, John Fredy Barrera, Roberto Torroba, Alejandro Velez y Myrian Tebaldi. Obtuvo el tercer puesto en la categoría presentación oral en el evento *XIV Encuentro Nacional De Óptica (XIV ENO) Y V Conferencia Andina Y Del Caribe En Óptica Y Sus Aplicaciones (V CANCOA), Universidad del Valle en Cali-Colombia, noviembre 16 al 20 del 2015*.

Optimized and secure technique for multiplexing QR code images of single characters: application to noiseless messages retrieval

Sorayda Trejos¹, John Fredy Barrera¹ and Roberto Torroba²

¹Grupo de Óptica y Fotónica, Instituto de Física, Facultad de Ciencias Exactas y Naturales, Universidad de Antioquia UdeA, Calle 70 No. 52-21, Medellín, Colombia

²Centro de Investigaciones Óptica (CONICET La Plata-CIC) and UID OPTIMO, Facultad de Ingeniería, Universidad Nacional de La Plata, PO Box 3, C.P 1897, La Plata, Argentina

E-mail: sorayda.trejos@udea.edu.co

Received 13 February 2015, revised 10 June 2015

Accepted for publication 11 June 2015

Published 31 July 2015



CrossMark

Abstract

We present for the first time an optical encrypting–decrypting protocol for recovering messages without speckle noise. This is a digital holographic technique using a $2f$ scheme to process QR codes entries. In the procedure, letters used to compose eventual messages are individually converted into a QR code, and then each QR code is divided into portions. Through a holographic technique, we store each processed portion. After filtering and repositioning, we add all processed data to create a single pack, thus simplifying the handling and recovery of multiple QR code images, representing the first multiplexing procedure applied to processed QR codes. All QR codes are recovered in a single step and in the same plane, showing neither cross-talk nor noise problems as in other methods. Experiments have been conducted using an interferometric configuration and comparisons between unprocessed and recovered QR codes have been performed, showing differences between them due to the involved processing. Recovered QR codes can be successfully scanned, thanks to their noise tolerance. Finally, the appropriate sequence in the scanning of the recovered QR codes brings a noiseless retrieved message. Additionally, to procure maximum security, the multiplexed pack could be multiplied by a digital diffuser as to encrypt it. The encrypted pack is easily decoded by multiplying the multiplexing with the complex conjugate of the diffuser. As it is a digital operation, no noise is added. Therefore, this technique is threefold robust, involving multiplexing, encryption, and the need of a sequence to retrieve the outcome.

 Online supplementary data available from stacks.iop.org/JOPT/17/085702/mmedia

Keywords: QR codes, optical packaging, image processing, digital holography, multiplexing

1. Introduction

In recent years, optical encryption has shown remarkable development [1–56]. Since the first report on the double random phase encoding (DRPE) technique [1, 2], further remarkable progress was published, including a generalization to 3D keys [3]. Later, an optical DRPE method using a joint transform correlator architecture was proposed and

successfully implemented [4]. In this encrypting architecture, the conjugate of the encrypted key is not required to recover the original information. Overviews show some important advances that illustrate the evolution of the subject [5, 6]. Among new highly developed areas, we can mention QR code optical encryption [7–18], video optical encryption [19–24], structured masks [25–27], asymmetric security systems [28–33], cryptosystems analysis [34–42], and multiplexing

techniques [43–56], to name a few. Specifically, QR codes have driven great attention due to their resistance to noise, among other characteristics, making them highly appropriate to serve as ‘information containers’. Optical encryption and QR coding have been successfully merged to protect information [7, 8]. For security purposes, the information to be protected is encoded into a QR code, and, instead of the original information, this QR code is in turn encrypted. As expected in optical encrypting techniques, the rightly decrypted QR code contains noise. Scanning the noisy decrypted code renders the original data to the final user; he/she receives the pertinent information without the noise arising in the traditional optical encrypting techniques. QR codes offered a practical solution to the noise present over decrypted images, thus releasing a valid actual alternative to solve the problem, besides making more attractive the use of optical encrypting techniques, as QR codes can be scanned by smartphones or tablets with the appropriate program [8, 11, 12].

The insertion of a QR code as an ‘information container’ in optical encryption was introduced for the first time by Barrera *et al* [7]. In this pioneer contribution, the information to be encrypted is transformed into a QR code, and then the QR code is encrypted with a DRPE technique in a $4f$ architecture. The decrypted QR code contains noise due to the optical processing with an optical encrypting arrangement that includes random phase masks. Finally, the decrypted QR code is scanned using a smartphone, rendering the original information free of any kind of noise. This contribution merges QR coding and optical encryption to demonstrate a secure and a noise-free management of information employing widely used technological tools [8].

Nevertheless, to fully profit from the QR code characteristics outside the encryption procedures, we need to further improve the reading capabilities under more severe conditions. Therefore, some ‘cleaning’ methods were developed to get a better reading from polluted QR codes for existing market apps (Android, Apple, etc) available to the common user [9, 10]. The experimental demonstration of the QR optical encryption was performed using a joint transform correlator *JTC* encrypting architecture [9]. As the implementation is not possible in a single step due to the limit of resolution of the optical system, a multiplexing procedure to encrypt QR codes is added. Once the QR code is rightly decrypted and scanned, the original information is recovered free from noise and using the most basic, fast, and free available software [9]. This contribution represents the first experimental demonstration of the QR code optical encryption. Afterward, two techniques to reinforce the QR code optical encryption were presented [10]. First, the inclusion of an experimental scrambling technique in the encrypting protocol adds more protection to the security proposal. Additionally, a nonlinear normalization technique is applied to reduce the noise over the recovered QR codes, besides increasing the security against attacks [51, 52]. The combination of these improvements favored specially the QR codes use as ‘containers’ of the original data.

This novel application revitalized traditional optical encrypting methods; further, it represents an advance in presenting a practical tool, which can be massively used, and solving the drastic issue of the ever-present noise altering the outcome. Motivated by this new approach, several applications came forward, such as multidimensional keys [13], phase retrieval [14, 15], and incoherent superposition [16], to name a few. Also, the QR coding was even adapted for validation purposes [17, 18].

Regardless the input to a given optical system, we always face the problem of image resolution. Besides determining if we are using coherent light sources, we have the intrusion of the speckle phenomenon and both produce corresponding image deterioration. A practical partial solution to this problem is found in the contribution of Barrera *et al* [53]. It is an experimental protocol to visualize images that otherwise would have been barely recognizable due to the above-mentioned issues. This protocol is based on an optical image synthesis with digital holography using enlarged sub-samples of an entire image together with a multiplexing technique. As a result, they get smaller speckle patterns on the final assembled image and a spatial frequency enhancement with respect to the input image obtained with the conventional procedures. This enhancement allows us to implement a protocol to process, in a secure manner, messages of any length employing a *JTC* encrypting processor [54]. The correct retrieving of the message requires the individual encryption of several characters, a multiplexing procedure to obtain an encrypted keyboard, and a selection-position key that gives the right sequence. The experimental results show the feasibility of the proposal, representing an actual application of the optical encrypting protocols. Although optical encryption has achieved huge popularity due to its great range of possible applications, some protocols, procedures, and even the optical encrypting processors must be improved to represent an actual tool with a real potential for commercial purposes. In order to further reduce the optical architecture normally involved in optical processing, in particular in the above-mentioned technique, an optical packaging and encrypting (SOPE) procedure [55] is employed. Although intended for encryption purposes, its use can be extended to other practical image-handling approaches. An interferometric architecture with a simple $2f$ optical processor in one arm and a corresponding reference beam in the other allows recording several processed data; then, after digital processing, the data are filtered, repositioned, and multiplexed. During recovery, all processed information is displayed in the same plane employing a friendly retrieving procedure. This procedure allows the packaging of multiple entries in a single unit without introducing image superposition or cross-talk. This protocol can also be performed using a theta modulation procedure over each part of processed data before multiplexing, assuring the recovering of all data without superposition [56].

The constant improvement of optical components and the advances in optical processing has made the achievement of a new style of optical information handling possible, by using digital holographic techniques together with the packaging of

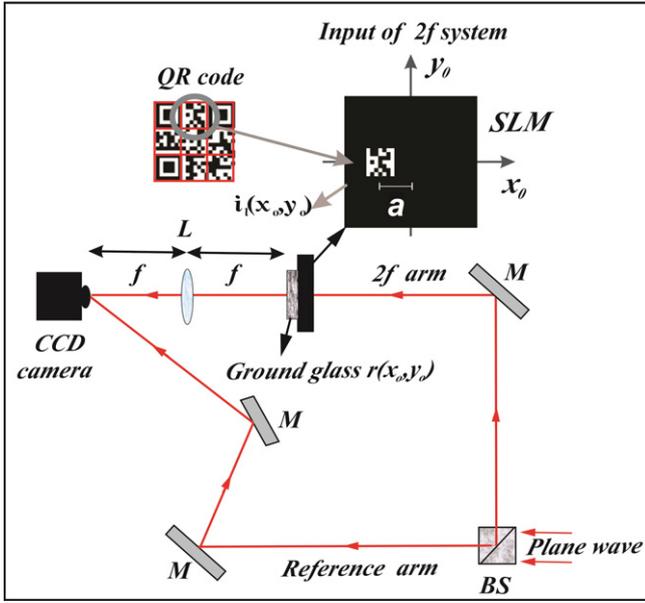


Figure 1. Interferometric setup to register the holograms of the processed QR code sections (BS: beam splitter, M: mirror, SLM: spatial light modulator, L: Lens of focal length f).

multi-images and its final encryption. This type of optical information handling is used and implemented in this paper in an actual application with great potential, namely a panel made with QR codes for each letter. In the present approach, each letter is transformed into a QR code and then, to avoid any optical resolution problem, we subdivide the QR codes into portions. Afterward, portions are displayed in a spatial light modulator (SLM) covered by a diffuser. A hologram is obtained and digitally stored for each portion. Posteriori filtering, repositioning, and adding operations compose the multiplexing. This procedure represents the first reported multiplexing of encrypted QR codes. To offer another strengthening step, we digitally multiply the pack by a random phase mask, thus making a simple encrypting mechanism. The pack and decryption random mask are sent once to the user, while the sequence ordering the codes can be changed according to the delivered message. Once the QR codes are recovered, then by the most basic, fast, and free available software on the Internet, the message is obtained without the noise associated with optodigital processing. This technique represents end-user benefits whenever there is an efficient combination of the optical security methods and the digital procedures.

2. Basic processing for every QR code

This section describes and illustrates the process performed for a single QR code. As the optical processing of a QR code is not possible in a single step, due to the limit of resolution of the optical system [9, 53], the code is divided into nine equal-size portions, where each one is located in the entrance plane of a $2f$ setup. For the experimental realization, each QR code section is attached to a random phase mask. An

interferometric setup allows us to record the hologram of the optically processed data, as depicted in figure 1. The input plane of the $2f$ optical processor is described by

$$q_l(x_0, y_0) = [i_l(x_0, y_0)r(x_0, y_0)] \otimes \delta(x_0 - (-a), y_0) \quad (1)$$

where $i_l(x_0, y_0)$ is the QR section projected in a SLM, the ground glass placed behind the SLM is represented by the random phase mask $r(x_0, y_0)$, \otimes means convolution, $\delta()$ is the Dirac delta function, and $|a|$ is the distance between the QR section and the optical axis in the input plane. We illuminate this input with a monochromatic plane wave, and we get at the output plane the processed QR code section:

$$Q_l(u, v) = FT \left\{ [i_l(x_0, y_0)r(x_0, y_0)] \otimes \delta(x_0 - (-a), y_0) \right\} \quad (2)$$

The expression $FT \{ \}$ denotes the Fourier transform (FT) operation. At this step, we can deduce from equation (2) that the object spectrum will be spread in a wider area in the output plane.

Then, the optically processed QR code section is holographically recorded using the interferometrical arrangement of figure 1. The interferogram registered in the CCD camera is mathematically represented by

$$I_l(u, v) = |Q_l(u, v)|^2 + |P(u, v)|^2 + Q_l^*(u, v)P(u, v) \exp(-2\pi i \alpha u) + Q_l(u, v)P^*(u, v) \exp(2\pi i \alpha u) \quad (3)$$

where $*$ means complex conjugate, $P(u, v) = \exp[2\pi i(\alpha u f + \beta v f)]$ represents the reference plane wave written in frequency coordinates $u = x_0/\lambda f$ and $v = y_0/\lambda f$ where $\alpha = \cos \theta/\lambda$ and $\beta = \cos \phi/\lambda$, and $\cos \phi$ are the directional cosines, and λ is the wavelength. Then, we filtered the terms of no interest in equation (3). For this purpose, we register separately the terms $|P(u, v)|^2$ and $|Q_l(u, v)|^2$ by blocking the $2f$ arm and the reference arm, respectively. The procedure up to this point is experimentally developed, and from now on, we perform digital operations. Subtracting these last two terms from equation (3) we obtain

$$S_l(u, v) = Q_l^*(u, v)P(u, v) \exp(-2\pi i \alpha u) + Q_l(u, v)P^*(u, v) \exp(2\pi i \alpha u) \quad (4)$$

From equation (4), we want to only retain one term. Then, we proceed to perform the FT of equation (4) to get two spatially separated terms:

$$t_l(x', y') = q_l^*(x', y') \otimes \delta(x' + \alpha \lambda f, y' + \beta \lambda f) \otimes \delta(x' + a, y') + q_l(x', y') \otimes \delta(x' - \alpha \lambda f, y' - \beta \lambda f) \otimes \delta(x' - a, y') \quad (5)$$

The separation between the terms in equation (5) is proportional to $|a|$, which is controlled during the projection of the QR code section on the SLM. The value of $|a|$ is carefully selected to prevent any kind of superposition between these two terms.

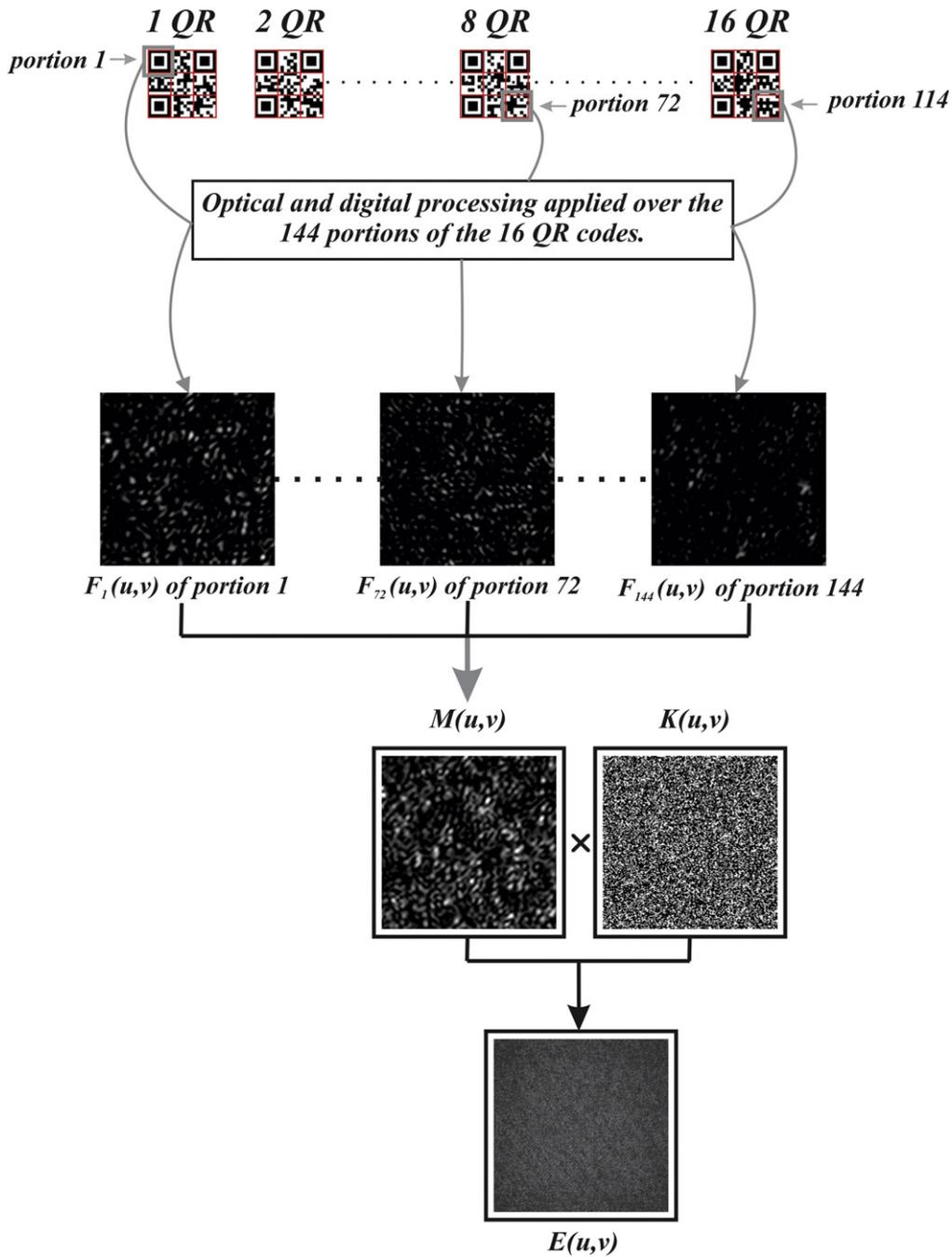


Figure 2. Processing, multiplexing, and encrypting of 144 QR codes portions.

Then, the first term of equation (5) is removed by filtering and the remaining term is repositioned around a desired coordinate (x_l, y_l) , then we apply an inverse FT to complete the filtering process [55]:

$$F_l(u, v) = Q_l(u, v) \exp[2\pi i(x_l u + y_l v)] \quad (6)$$

This last equation represents the optodigital processed QR portion (see figure 2). The positioning at coordinates (x_l, y_l) allow us to locate the recovered data in any desired position in the output plane, as we want to process multiple QR codes and recover them without superposition.

3. Multiple data processing and encryption

In this case, 16 QR codes are processed. As each QR code is divided in nine portions, 144 QR portions are processed individually by the optical system, filtered, and positioned digitally, as discussed in section (2), getting so for every single portion its respective function $F_l(u, v)$.

The multiplexing is a practical tool to manage multiple data without altering the optical setup or introducing other elements, becoming a practical solution for processing QR codes. Therefore, once all data is optodigital processed, a multiplexing operation is applied to generate

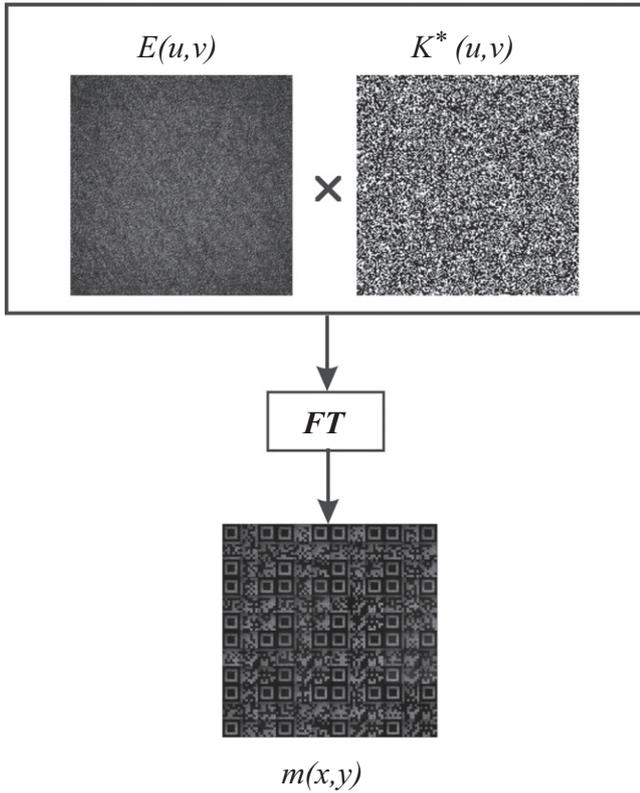


Figure 3. Scheme for decrypting, recovering, and displaying the package of QR codes.

a single information unit $M(u, v)$. As we process 144 sections (equation (6)), the optical package is expressed as:

$$M(u, v) = \sum_{l=1}^{144} F_l(u, v) = \sum_{l=1}^{144} Q_l(u, v) \exp[2\pi i(x_l u + y_l v)] \quad (7)$$

Multiplexing allows the easily handling of the sent information, as instead of separately sending each processed data, we send a single package containing all processed data. During processing of each portion, the coordinates (x_l, y_l) are carefully chosen to assure a correct reassembly when retrieving all portions. As a final step, we protect the package using one random digital phase mask $K(u, v)$ (see figure 2), which acts as the encrypting key. Accordingly, by a digital multiplication of $M(u, v)$ and $K(u, v)$, we get the encrypted package:

$$E(u, v) = M(u, v)K(u, v) \quad (8)$$

This result and the complex conjugate of the key $K^*(u, v)$ are sent separately to users in remote locations. The end user performs a multiplication between the encrypted data and the complex conjugate of the key, and with a subsequent FT operation, the hidden codes are recovered in the imposed positions. The recovering of all processed QR codes is

represented as:

$$m(x, y) = \sum_{l=1}^{144} q_l(x, y)k(x, y) \otimes \delta(x - x_l, y - y_l) \quad (9)$$

The QR codes are displayed in one step, in the same plane, and at the same time. As $K(u, v)$ is a random phase mask, it vanishes when we record the intensity of $m(x, y)$ to get the intensity of the recovered portions $|q_l(x, y)|^2$. Note that our experimental technique does not imply setup alterations. We want to emphasize that the new scheme is neither a $4f$ nor a JTC architecture, although it uses two phase masks to protect the information. In this contribution, we use a $2f$ architecture (only one lens), where the masks are placed at the input plane and at the Fourier plane of the lens. Meanwhile, the $4f$ system consists of two lenses of focal length f , therefore the distance between input and output planes is $4f$ [1]. The first encoding mask is positioned at the input plane and the remaining mask at the first Fourier plane (at a distance f from the first lens). Regarding the JTC encrypting architecture, it uses one lens in order to encrypt the information, but the object and the two encrypting masks are placed at the input plane [4].

Contrasting other methods, where all data are first encrypted and then multiplexed [24, 32, 46, 50], in our proposal we start by processing multiple data, then multiplex and finally encrypt them in a single step by a multiplication with the second key.

4. Experimental results

In the experimental arrangement, we use a solid-state laser operating at a wavelength of 632 nm. A diffusing glass is placed in contact in the SLM to provide the random phase mask. The size of the projected object into the SLM is 6.4×6.4 mm. The SLM is a Holoeye LC2002, whose pixel size is $32 \mu\text{m}$. The distance $|a|$ between the object and the optical axis in the input plane is 5.6 mm.

The SLM is placed at a distance f of a positive lens L of focal length $f=200$ mm and the CCD camera is placed so that the distance between the lens and the sensor is equal to f (see figure 1). The camera size is 3840×2748 pixels and the pixel size is $1.67 \times 1.67 \mu\text{m}$.

For the experimental realization, 144 portions were handled (16 QR codes), where each portion was optodigitally processed according to the description of section (2) and (3). After the experimental and digital steps, we obtain the processed QR codes ready to be encrypted with the encoding mask as described previously. It is important to remark that the multiplexing contains the information of all managed QR codes. In order to recover the original QR codes, it is necessary to cancel the effect of the encrypting key and perform a FT operation (see figure 3). From the last operation, we get the QR codes, which are not free of speckle. From a practical point of view in a security system, one of its main requirements is that the recovering process should be friendly

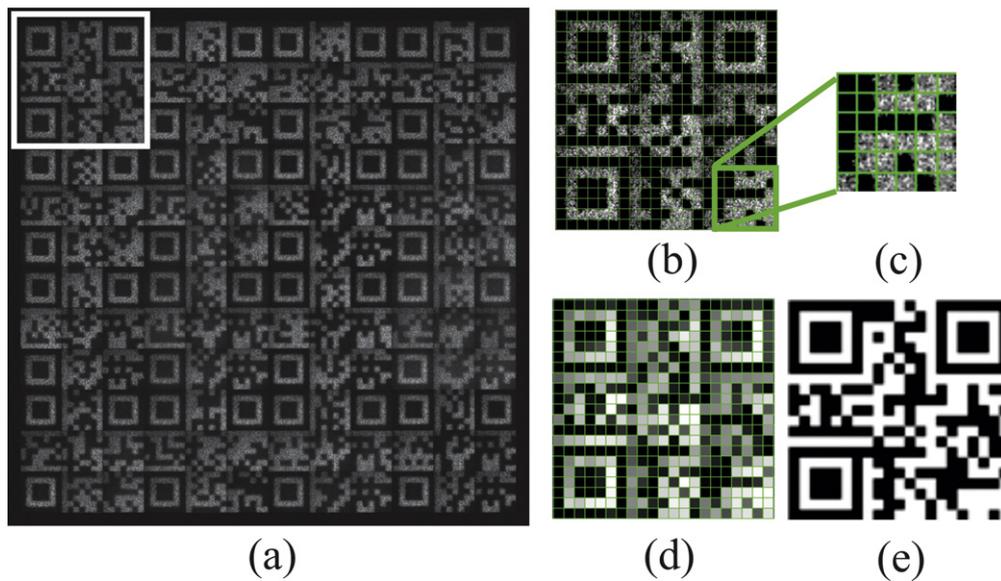


Figure 4. (a) Panel containing all recovered QR codes after using the appropriate recovering procedure, (b) one QR code of the panel corresponding to the white square in (a), (c) magnified inset box of a section of (b), (d) average value of each block in (c) (between 0 and 255), and (e) decrypted QR code after the process of binarization.

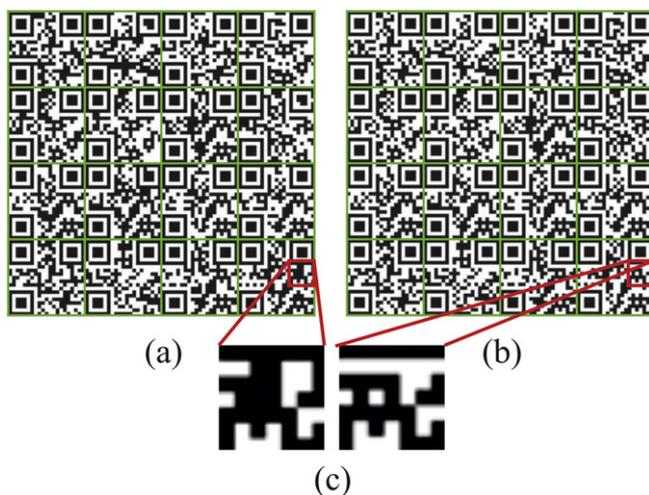


Figure 5. Panel with (a) the processed and binarized QR codes and (b) the original QR codes, and (c) the zooming of one portion of a QR code in (a) and the zooming of its corresponding section in (b).

to the final user. Although the processing of the QR codes involves several optical and digital operations, the retrieving of the QR codes implies only two operations to display all QR codes on the same plane, at the same time, without any kind of overlap, and using informatics tools freely available for everybody.

According to the described proposal, a panel containing several QR codes is displayed after performing the correct retrieving protocol. As each code contains the information of a single character, the final step is scanning the panel using the appropriate sequence to reveal the hidden message. The scanning process can be performed using a QR scanning program from a smartphone, a computer, or a tablet [7, 8, 10–12]. Other option is employing the most basic, fast, and free

available software on the Internet. This software works only for binary QR codes. An original QR code consists of black and white blocks arranged in a square grid, while decrypted QR codes are not binary (figure 4(b)). We want to take advantage of this software to make the scanning process simpler and faster. Therefore, we proceed to binarize individually each QR code contained in the panel. For doing so, first we divide each decrypted QR code in blocks, where each block contains several pixels of the code. A threshold value is chosen such that gray values above the threshold become white, while for gray values lower than the threshold become black, thus generating a QR code binarized as shown in the figure 4(e).

Figure 5(a) presents the binarized panel with the retrieved QR codes, while figure 5(b) shows a panel containing the original QR codes. From a simple visual comparison between figures 5(a) and (b), it is not easy to deduce the differences between the original and the processed and binarized QR codes. We expect some differences between the original and binarized QR codes due to the changes suffered by the QR codes during the application of the protocol. In order to make evident these differences, we zoomed in on one section of a binarized QR code and the corresponding sections taken from its original version. Figure 5(c) clearly shows dissimilarities among the processed and original QR codes. Despite these differences, the processed QR codes using our proposed technique can be successfully scanned.

If we now add a predetermined sequence over the final QR panel (figure 5(a)), we are able to recover a noiseless hiding message, as shown in figure 6(a) (see media 1). The phrase ‘PACKAGING AND CODING’ is reconstructed without traces of degradation. In the standard procedures [1–6, 51–56], we observe that the final outcomes are recovered with a speckle noise generated by the optodigital processing

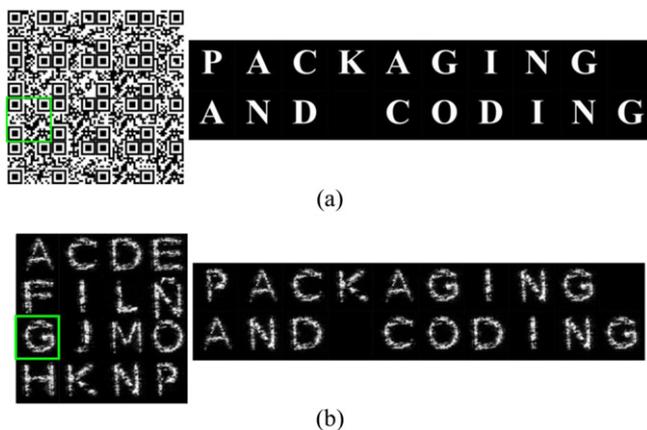


Figure 6. (a) Recovered message with the proposed protocol (media 1) and (b) message retrieved with the classical procedure.

(see figure 6(b)). This noise is because each character is directly processed by the optical system, while in our proposal, each character is first converted into a QR code and then the QR code is processed instead. Processing noise affects the recovered multiplexing of the processed QR codes, but when binarizing and reading each code, the finally decoded message is noise-free (see figure 6(a)).

The important advance represented by the new implementation is evident from figure 6 and media 1. The new security protocol allows recovering secret messages with no noise, while in classical optical security protocols, the retrieved message contains the noise arising from the processing. Also, once we get the panel with the recovered QR codes, we only need a new scanning sequence to reveal a new message, thus saving resources.

Although 16 QR codes are used to illustrate the procedure (figure 4(a)), the scheme is not altered if the number of QR codes changes. Our protocol can be extended for the general case where the authorized user can recover a panel containing a complete keyboard whose keys are contained in the QR codes. Using this panel and recovery sequence, it is possible to obtain a message of any length and any content. In the general case, the maximum number of multiplexed QR codes corresponds to the amount of letters, symbols, and numbers that a keyboard may contain.

Under the proposed protocol, the user gets in one occasion the multiplexed and encrypted information and the corresponding decode key. After performing the correct recovering procedure, the retrieved panel of QR codes allows us to recover the protected message using the reading sequence (see media 1). In the general case, where the panel contains a complete keyboard constituted by the corresponding QR codes of its characters, different messages with a variety of content and extent are recovered when applying the reading sequences over the panel. It is important to remark that once the panel is obtained, to recover any new message, it is only necessary to access its corresponding reading sequence. Note that the spatial location of the QR codes in the panel should not necessarily follow that of a regular QWERTY keyboard.

5. Conclusions

In the present contribution, we proposed and implemented for the first time an optodigital protocol to securely manage messages, besides assuring their recovery was free of any kind of noise or degradation. We employ a simple $2f$ system and an interferometrical arrangement for the optical processing. A QR coding of the original information elements (letters) along with a filtering, positioning, multiplexing, and encryption completed the process to obtain an encrypted package with the QR processed codes. The multiplexing procedure not only represents the first multiplexing of optodigital processed QR codes, but also allows us to include in a single unit of information all processed QR codes, thus simplifying the handling and recovery of multiple QR codes. The proposed protocol is friendly to the final user because the recovery stage includes only two operations to bring the display of all QR codes in the same plane, at the same time, and without any kind of overlap. Then, by binarizing the recovered QR codes and acceding to the right scanning sequence, it is possible to recover the clean message. The protocol involves informatics tools available for free. Once the user gets the recovered and binarized panel of the QR codes, the retrieving of new messages only requires the knowledge of the scanning sequence. This protocol can be implemented for a multi-user environment. In this case, all authorized users receive the encrypted package and the encrypting mask by separate channels, and then each user gets the corresponding sequence in order to recover a particular message.

Acknowledgments

This research was performed under grants from Estrategia de Sostenibilidad 2014–2015 and Comité para el Desarrollo de la Investigación -CODI- (Universidad de Antioquia-Colombia), COLCIENCIAS (Colombia), MINCYT-COLCIENCIAS CO/13/05, CONICET nos. 0863/09 and 0549/12 (Argentina), and Facultad de Ingeniería, Universidad Nacional de La Plata no. 11/I168 (Argentina). J F Barrera Ramírez acknowledges the support from The International Centre for Theoretical Physics ICTP Associateship Scheme and The World Academy of Sciences TWAS.

References

- [1] Refregier P and Javidi B 1995 Optical image encryption based on input plane fourier plane random encoding *Opt. Lett.* **20** 767–9
- [2] Javidi B and Horner J L 1994 Optical pattern recognition for validation and security verification *Opt. Eng.* **33** 1752–6
- [3] Matoba O and Javidi B 1999 Encrypted optical memory system using three-dimensional keys in the Fresnel domain *Opt. Lett.* **24** 762–4
- [4] Nomura T and Javidi B 2000 Optical encryption using a joint transform correlator architecture *Opt. Eng.* **39** 2031–5

- [5] Matoba O, Nomura T, Perez-Cabre E, Millá M S and Javidi B 2009 Optical techniques for information security *Proc. IEEE* **97** 1128–48
- [6] Chen W, Javidi B and Chen X 2014 Advances in optical security systems *Adv. Opt. Photon* **6** 120–55
- [7] Barrera J F, Mira A and Torroba R 2013 Optical encryption and QR codes: secure and noise-free information retrieval *Opt. Express* **21** 5373–8
- [8] Graydon O 2013 Quick response codes *Nat. Photonics* **7** 343
- [9] Barrera J F, Mira A and Torroba R 2014 Experimental QR code optical encryption: noise-free data recovering *Opt. Lett.* **39** 3074–7
- [10] Barrera J F, Vélez A and Torroba R 2014 Experimental scrambling and noise reduction applied to the optical encryption of QR codes *Opt. Express* **22** 20268–77
- [11] Ohbuchi E, Hanaizumi H and Hock L A 2004 Barcode readers using the camera device in mobile phones in *Proc. of IEEE 2004 Int. Conf. Cyberworlds (IEEE, 2004)* pp 260–5
- [12] Liao K C and Lee W H 2010 A novel user authentication scheme based on QR-Code *J. Netw* **5** 937–41
- [13] Lin C, Shen X and Li B 2014 Four-dimensional key design in amplitude, phase, polarization and distance for optical encryption based on polarization digital holography and QR code *Opt. Express* **22** 20727–39
- [14] Wang Z, Zhang S, Liu H and Qin Y 2014 Single-intensity-recording optical encryption technique based on phase retrieval algorithm and QR code *Commun.* **332** 36–41
- [15] Fan D, Meng X, Wang Y, Yang X, Peng X, He W, Dong G and Chen H 2013 Optical identity authentication scheme based on elliptic curve digital signature algorithm and phase retrieval algorithm *Appl. Opt.* **52** 5645–52
- [16] Qin Y and Gong Q 2014 Optical information encryption based on incoherent superposition with the help of the QR code *Opt. Commun.* **310** 69–74
- [17] Markman A, Javidi B and Tehramipour M 2014 Photon-counting security tagging and verification using optically encoded QR codes *IEEE Photon. J.* **6** 6800609
- [18] Carnicer A, Hassanfiroozi A, Latorre-Carmona P, Huang Y P and Javidi B 2015 Security authentication using phase-encoded nanoparticle structures and polarized light *Opt. Lett.* **40** 135–8
- [19] Mosso F, Barrera J F, Tebaldi M, Bolognini N and Torroba R 2011 All-optical encrypted movie *Opt. Express* **19** 5706–12
- [20] Mosso F, Tebaldi M, Barrera J F, Bolognini N and Torroba R 2011 Pure optical dynamical color encryption *Opt. Express* **19** 13779–86
- [21] Barrera J F, Tebaldi M, Ríos C, Rueda E, Bolognini N and Torroba R 2012 Experimental multiplexing of encrypted movies using a JTC architecture *Opt. Express* **20** 3388–93
- [22] Zhong Z, Yu Zhang, Shan M, Wang Y, Zhang Y and Xie H 2014 Optical movie encryption based on a discrete multiple-parameter fractional Fourier transform *J. Opt.* **16** 125404
- [23] Aldossari M, Alfalou A and Brosseau C 2014 Simultaneous compression and encryption of closely resembling images: application to video sequences and polarimetric images *Opt. Express* **22** 22349–68
- [24] Saini N and Sinha A 2015 Video encryption using chaotic masks in joint transform correlator *J. Opt.* **17** 035701
- [25] Barrera J F, Tebaldi M, Amaya D, Furlan W D, Monsoriu J, Bolognini N and Torroba R 2012 Multiplexing of encrypted data using fractal masks *Opt. Lett.* **37** 2895–97
- [26] Abuturab M R 2012 Color image security system using double random-structured phase encoding in gyrator transform domain *Appl. Opt.* **51** 3006–16
- [27] Singh H, Yadav A K, Vashisth S and Singh K 2015 Double phase-image encryption using gyrator transforms, and structured phase mask in the frequency plane *Opt. Laser Eng.* **67** 145–56
- [28] Chen W and Chen X 2011 Optical asymmetric cryptography using a three-dimensional space-based model *J. Opt.* **13** 075404
- [29] Rajput S K and Nishchal N K 2012 Asymmetric color cryptosystem using polarization selective diffractive optical element and structured phase mask *Appl. Opt.* **51** 5377–86
- [30] Wenqi H, Meng X and Peng X 2013 Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang-Gu algorithm: comment *Opt. Lett.* **38** 4044
- [31] Mehra I and Nishchal N K 2014 Asymmetric cryptosystem for securing multiple images using two beam interference phenomenon *Opt. Laser Technol.* **60** 1–7
- [32] Liu W, Xie Z, Liu Z, Zhang Y and Liu S 2015 Multiple-image encryption based on optical asymmetric key cryptosystem *Opt. Commun.* **335** 205–11
- [33] Sui L, Duan K, Liang J and Hei X 2014 Asymmetric double-image encryption based on cascaded discrete fractional random transform and logistic maps *Opt. Express* **22** 10605–21
- [34] Barrera J F, Vargas C, Tebaldi M, Torroba R and Bolognini N 2010 Known-plaintext attack on a joint transform correlator encrypting system *Opt. Lett.* **35** 3553–5
- [35] Barrera J F, Vargas C, Tebaldi M and Torroba R 2010 Chosen-plaintext attack on a joint transform correlator encrypting system *Opt. Commun.* **283** 3917–21
- [36] Qin W, Peng X and Meng X 2011 Cryptanalysis of optical encryption schemes based on joint transform correlator architecture *Opt. Eng.* **50** 028201
- [37] Wang X and Zhao D 2012 Double images encryption method with resistance against the specific attack based on an asymmetric algorithm *Opt. Express* **20** 11994–2003
- [38] Kumar P, Joseph J and Singh K 2012 Known-plaintext attack-free double random phase-amplitude optical encryption: vulnerability to impulse function attack *J. Opt.* **14** 045401
- [39] Wang X and Zhao D 2012 A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms *Opt. Commun.* **285** 1078–81
- [40] Liao M, He W, Peng X, Liu X and Meng X 2013 Cryptanalysis of optical encryption with a reference wave in a joint transform correlator architecture *Opt. Laser Technol.* **45** 763–7
- [41] Rajput S K and Nishchal N K 2013 Known-plaintext attack-based optical cryptosystem using phase-truncated Fresnel transform *Appl. Opt.* **52** 871–8
- [42] Zhang C, Liao M, He W and Peng X 2013 Ciphertext-only attack on a joint transform correlator encryption system *Opt. Express* **21** 28523–30
- [43] Wang X and Zhao D 2011 Multiple-image encryption based on nonlinear amplitude-truncation and phase-truncation in Fourier domain *Opt. Commun.* **284** 148–52
- [44] Liu Z, Zhanga Y, Zhao H, Ahmad M A and Liu S 2011 Optical multi-image encryption based on frequency shift *Optik* **122** 1010–3
- [45] Lin C, Shen X, Tang R and Zou X 2012 Multiple images encryption based on Fourier transform hologram *Opt. Commun.* **285** 1023–8
- [46] Shen X, Lin C and Kong D 2012 Fresnel-transform holographic encryption based on angular multiplexing and random-amplitude mask *Opt. Eng.* **51** 068201
- [47] Yin S and Tao S 2013 Compression and storage of multiple images with modulating blazed gratings *J. Opt.* **15** 075406
- [48] Zhao H, Liu J, Jia J, Zhu N, Xie J and Wang Y 2013 Multiple-image encryption based on position multiplexing of Fresnel phase *Opt. Commun.* **286** 85–90
- [49] Alfalou A, Brosseau C, Abdallah N and Jridi M 2013 Assessing the performance of a method of simultaneous compression and encryption of multiple images and its resistance against various attacks *Opt. Express* **21** 8025–43

- [50] Wang Y, Quan C and Tay C J 2014 Nonlinear multiple-image encryption based on mixture retrieval algorithm in Fresnel domain *Opt. Commun.* **330** 91–8
- [51] Vilarity J M, Millán M S and Perez-Cabre E 2013 Improved decryption quality and security of a joint transform correlator-based encryption system *J. Opt.* **15** 025401
- [52] Vilarity J M, Millán M S and Perez-Cabre E 2014 Nonlinear optical security system based on a joint transform correlator in the Fresnel domain *Appl. Opt.* **53** 1674–82
- [53] Barrera J F, Rueda E, Rios C, Tebaldi M, Bolognini N and Torroba R 2011 Experimental opto- digital synthesis of encrypted sub-samples of an image to improve its decoded quality *Opt. Commun.* **284** 4350–5
- [54] Barrera J F, Vélez A and Torroba R 2013 Experimental multiplexing protocol to encrypt messages of any length *J. Opt.* **15** 055404
- [55] Barrera J F, Trejos S, Tebaldi M and Torroba R 2013 Experimental protocol for packaging and encrypting multiple data *J. Opt.* **15** 055406
- [56] Trejos S, Barrera J F, Tebaldi M and Torroba R 2014 Experimental optodigital processing of multiple data via modulation, packaging and encryption *J. Opt.* **16** 055402

Optical approach for the efficient data volume handling in experimentally encrypted data

Sorayda Trejos¹, John Fredy Barrera¹, Alejandro Velez²,
Myrian Tebaldi^{2,3} and Roberto Torroba^{2,3}

¹Grupo de Óptica y Fotónica, Instituto de Física, Facultad de Ciencias Exactas y Naturales, Universidad de Antioquia UdeA, Calle 70 No. 52-21, Medellín, Colombia

²Centro de Investigaciones Ópticas (CONICET La Plata-CIC—UNLP) PO Box 3, C.P 1897, La Plata, Argentina

³UIDET OPTIMO, Facultad de Ingeniería, Universidad Nacional de La Plata, La Plata, Argentina

E-mail: sorayda.trejos@udea.edu.co

Received 21 December 2015, revised 19 February 2016

Accepted for publication 7 March 2016

Published 5 April 2016



CrossMark

Abstract

Experimental optical procedures generate a tremendous amount of data, which must be then processed for any practical application. We present a new optical approach in terms of the data volume for the efficient handling of multiple data obtained from an experimental cryptosystem. In order to achieve this goal, we use the combination of optical filtering and optical scaling of the experimentally registered data. The intention is to reduce by optical means the amount of data to be managed. We define a so called ‘efficiency factor’ to describe the effectiveness of the approach. We find that volume reduction depends on this factor and the number of objects to be processed. We achieved substantial data volume reductions up to 94.24%. We introduce the basic concepts as well as experimental results that support both the feasibility and the applicability of our approach.

Keywords: data processing by optical means, pattern recognition, optical security and encryption

(Some figures may appear in colour only in the online journal)

1. Introduction

Experimental optical encryption has played a significant role in many optics scenarios in recent years. Different optical architectures were presented in the technical literature [1–3]. In practice we can distinguish an encryption step, handling, sending and reception steps, and finally the decryption by the end user. In particular, when many input objects are used, not only an eventual superposition has to be avoided, but efficient handling to convey the information is also important [4, 5]. Precisely, this handling defines the way the encrypted data is organized so as to manage several inputs to conform a single unit to be sent. The optimal handling of holographic data was approached using digital compression techniques [6, 7]. In particular, we found in [6] a proposal based on four digital industry-standard compression techniques and digital lossy

methods like resampling, quantization and discrete Fourier transformation. The results show that digital resampling is not an effective technique for digital interferograms. This is due to the fact that resampling results in an undersampling on the holographic microfringes. These digital compression techniques are digitally based.

Researchers proposed exploring many options to solve this problem. For instance, using the optical field phase only allows the storing requirements to be reduced by half with a minimal optical power loss during reconstruction [8]. Processing in the Fourier domain represents another tactic by filtering non-relevant terms contained in the hologram [9]. Recent examples deal with multiplexing and reconstruction in one step of 3D scenes [10].

The purpose of this contribution is to present an implementation of optical procedures to reduce the data volume

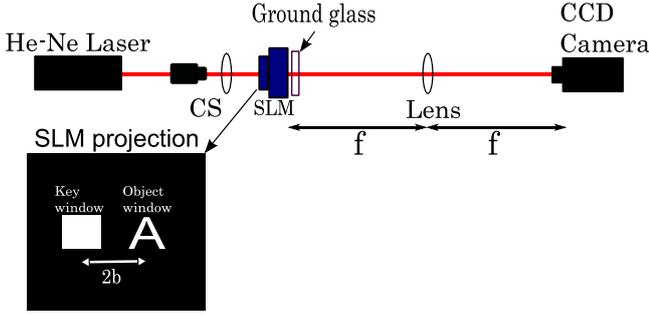


Figure 1. Scheme of the JTC cryptosystem. (CS: collimation system, SLM: spatial light modulator, f : lens focal length).

handling in experimental data obtained by optical means. Certainly, this approach can be complemented with digital compression techniques to further reduce the data. We employed experimental interferometric data and a virtual optical system to perform data volume reduction and reconstruction of the original information.

Among the different optical architectures, we select the joint transform correlator (JTC), which gives rise to the interferometric output we require as explained in the following. Any other interferometrical opto-digital cryptosystem will also equally serve.

2. Methodology for volume reduction

The proposal is based on the processing of the joint power spectrum (JPS) captured by using a CCD camera in the JTC cryptosystem, as show in figure 1.

In the JTC encrypting system the input plane contains the information of the object to be encrypted $o(x_0, y_0)$ attached to a random-phase mask $r_1(x_0, y_0)$, and another random-phase mask $r_2(x_0, y_0)$ that acts as the encrypting key. In our experimental implementation, the object and the window that limits the area of the encryption key are projected in a spatial light modulator (SLM), and the random-phase masks are generated by a ground glass. Therefore, the input plane is obtained when the SLM and the ground glass are placed in contact.

According to the scheme depicted in figure 1 a lens performs the Fourier transform (FT) of the input on the CCD camera. The result is the recording of the JPS of this input [11],

$$\begin{aligned} \text{JPS}(u, v) = & |C(u, v)|^2 + |R_2(u, v)|^2 \\ & + C^*(u, v)R_2(u, v)\exp(-4\pi i b u) \\ & + C(u, v)R_2^*(u, v)\exp(4\pi i b u) \end{aligned} \quad (1)$$

where $2b$ is the separation between the object and the key, $*$ means complex conjugate; $C(u, v)$ is the FT of $o(x_0, y_0)r_1(x_0, y_0)$, and $R_2(u, v)$ is the FT of the encoding key $r_2(x_0, y_0)$. Equation (1) arises from the interference between the light from both windows at the SLM plane.

In general, we take as data volume the amount of data in a file or database. In our case, the data volume of the JPS is $X_c * Y_c * B_c$, where X_c and Y_c are the horizontal and vertical

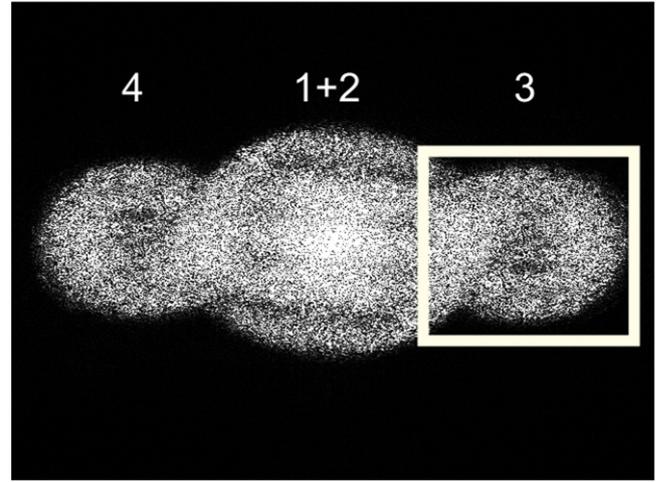


Figure 2. Intensity of the FT of equations (1); 1 + 2 central order corresponding to the FT of the object and key intensity, 3 and 4 are the FT of the third and fourth terms respectively.

resolutions respectively, and B_c the bit depth of the acquisition device. As we require a minimum volume for efficient handling, we focus our attention in retaining the third term of the JPS which contains the encrypted object information.

We perform the FT of the intensity represented by equation (1), obtaining the corresponding intensity distribution shown in figure 2, thanks to the interference fringes. We see a dc term corresponding to the FT of the key and object intensities and two orders, corresponding to the FT of the third and fourth term.

As shown in figure 2, we can select the third term which is smaller in size than the original JPS, and contains the information required to perform an adequate recovery of the original object [12]. In general, the size of the FT of the desired term is related to the physical dimensions of the object and the camera technical specifications. In this case, the filter window size is 177×198 . It is worth mentioning that increasing the filter widow size does not affect the quality of the final output and further reduction may cause both intensity and information loss. According to the previous definition, the data volume of the filtered object is $2 * X_o * Y_o * B_c$ where factor 2 is because the FT of the JPS contains both phase and amplitude information.

We define the 'efficiency factor' (E) as the ratio between the initial and final data volume after the different procedures applied over the data. As our technique encompasses two steps, each step will contribute to the final efficiency factor. Therefore in the following we analyze each contribution separately. The efficiency factor E_f achieved with filtering is given by

$$E_f = \frac{V_{\text{jps}}}{V_{\text{ft}}} = \frac{X_c * Y_c * B_c}{2 * X_o * Y_o * B_c} \quad (2)$$

where V_{jps} is the volume of the JPS registered by the CCD camera, and V_{ft} is the volume of the data after filtering. The filtered region in our JTC cryptosystem is equal to or less than one third of the total JPS region, thus guaranteeing that $V_{\text{ft}} < V_{\text{jps}}$. In this way the efficiency factor due to filtering is

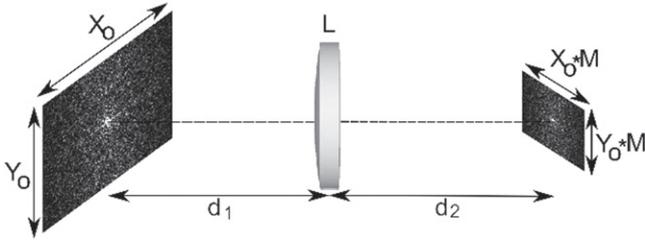


Figure 3. Virtual optical system used for scaling the filtered data: d_1 object distance, L convergent lens, d_2 image distance, X_0 filtered object width, Y_0 filtered object height, M magnification.

always greater than 1, meaning that we can reduce the data volume to be processed later simply with the filtering process.

In order to further increase the efficiency in data handling, we introduce an optical scaling procedure, to be applied over the filtered data. This procedure employs a virtual optical setup composed of a convergent lens used to scale the filtered data (see figure 3). Therefore, the efficiency factor for optical scaling E_M is given by

$$E_M = \frac{V_{ft}}{V_M} = \frac{2 * X_o * Y_o * B_c}{2 * X_o * Y_o * B_c * M^2} = \frac{1}{M^2} \quad (3)$$

where V_M is the volume of the data after scaling and M is the magnification of the virtual optical setup. It is important to take into account that the filtered data no longer contain the interferometrical fringes. A demagnification ($M < 1$) is mandatory in order to achieve $E_M > 1$ (equation (3)).

Therefore, an optical scaling over the filtered data does not involve the undersampling on the holographic microfringes present in digital resampling. Then, after performing both filtering and optical scaling, we achieve an efficiency factor of

$$E = \frac{V_{jps}}{V_M} = \frac{X_c * Y_c * B_c}{2 * X_o * Y_o * B_c * M^2}. \quad (4)$$

According to equations (2), (3) and (4), we can see that the efficiency factor of our proposal is the product of the efficiency factors of the filtering and optical scaling procedures $E = E_f E_M$.

This efficiency factor holds for a single encrypted object; however, we are interested in handling large amounts of encrypted objects. In order to take advantage of the inherent parallelism of optics, we can place all filtered data in a square matrix arrangement [12]. Then by performing the optical scaling over this arrangement, we process simultaneously all objects, instead of applying the procedure separately to each filtered data. In the following analysis, we assume that all objects share the same size and are registered in the same experimental setup; however, the procedure can be extended to the handling of data with different sizes from different setups.

The efficiency factor for N encrypted objects after filtering and scaling becomes

$$E_N = \frac{N * V_{jps}}{V_{NM}} = \frac{N * X_c * Y_c * B_c}{2 * N * X_o * Y_o * B_c * M^2} \quad (5)$$

defining V_{NM} as the data volume of N filtered objects after scaling. We can conclude, from equations (4) and (5), that the efficiency factor of the filtering and scaling does not depend on the number of encrypted objects $E_N = E$.

The parameter to quantify the efficiency of our proposal in terms of the data volume is the difference between the initial and the final volume,

$$\Delta V = N * (V_{jps} - V_M). \quad (6)$$

Using equation (4) we explicitly obtain

$$\Delta V = N * V_{jps} \left(1 - \frac{1}{E} \right). \quad (7)$$

As we expected, ΔV depends on the number of encrypted objects and the efficiency factor achieved with filtering and scaling processes. As $E_f > 1$ and $E_M > 1$ we achieve an efficiency factor $E > 1$, assuring a data volume reduction. We look for a data volume reduction as a result of our efficient procedure; therefore, we present an example to quantify the reduction achieved in an actual experimental case.

3. Results

In the next experimental example, we use 16 input objects, where the JPS corresponding to each object is individually recorded using the scheme of figure 1. The JPS of each encrypted object is recorded using a PULNIX TM6703 CCD camera with 640×480 pixels and a pixel pitch of $9 \mu\text{m}$. Consequently, each recorded JPS has a volume of 300.00 kB. For our 16 objects we have an initial data volume of 4.69 MB.

Afterwards, each JPS is filtered and, as discussed above, each filtered data is arranged within a square matrix as shown in figure 4(a). The input for the scaling process is the arrangement of filtered data (figure 4(a)). The area of the matrix arrangement will be equal to the area of the filtered JPS of each object multiplied by the number of objects to be multiplexed. In this example the filtered area is 177×198 pixels, with a data volume of 68.45 kB and the matrix arrangement has an area of 708×792 pixels, with a data volume of 1.07 MB. In figure 4(b) we show the outcome after data recovery [12]. Therefore, the initial data volume is 4.69 MB, and after filtering we achieve a volume of 1.07 MB. Finally, this arrangement is optically scaled using the setup of figure 3, and after recovery we obtain the result shown in figure 4(c).

When using a magnification of 0.5, we achieve a final data volume of 0.27 MB. The entire process has an efficiency factor of 17.53, and the final volume difference ΔV is

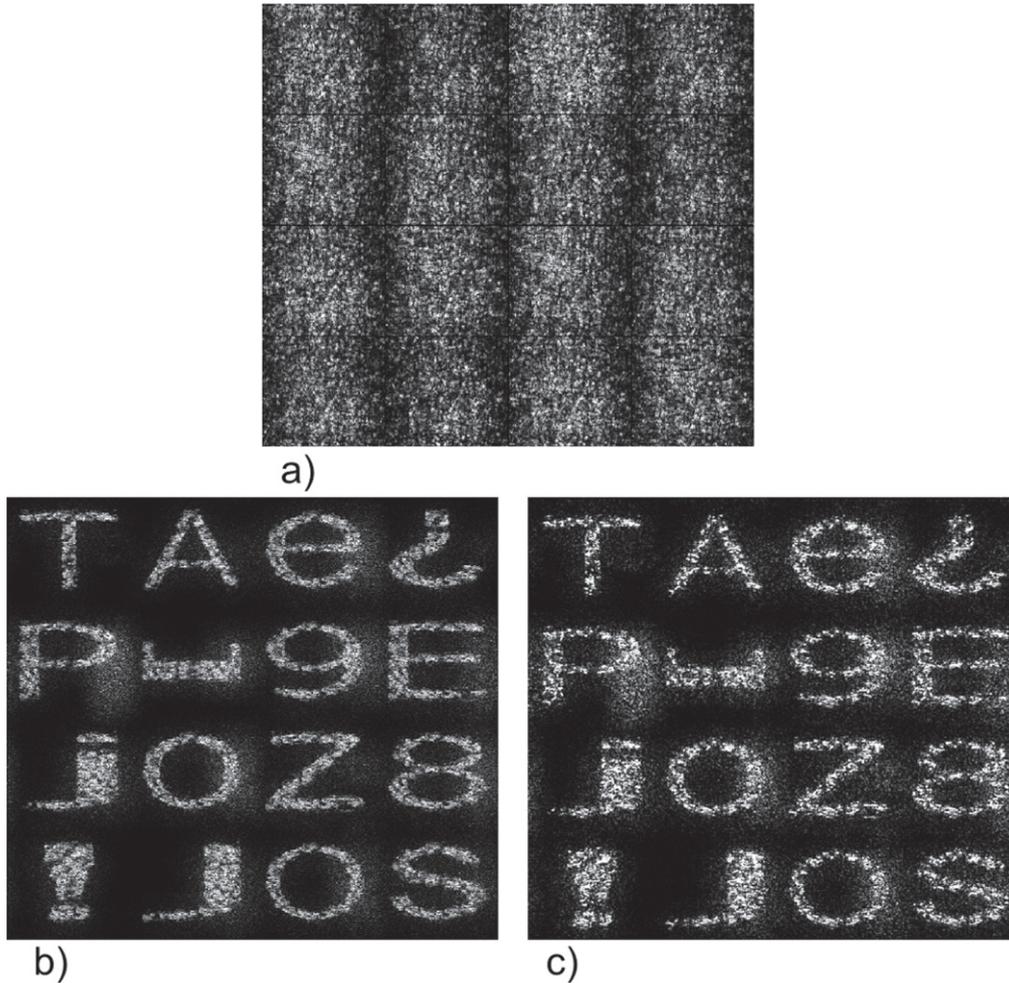


Figure 4. (a) Arrangement of 16 filtered objects in a square matrix, recovered objects from (a): (b) without optical scaling and (c) with scaling ($M = 0.5$).

4.42 MB. This means a percentage volume reduction of 94.24%.

In order to measure the error caused by the magnification procedure, we calculate the normalized mean square error (NMSE) between the data recovered from different magnifications of the matrix arrangement of figure 4(a) and the data recovered without magnification. If the recovery from the magnified matrix is $m(p, q)$ and the reference recovered from the non-magnified is $m_r(p, q)$, the NMSE is given by

$$NMSE = \frac{\sum_{p,q}^{N,M} |m(p, q) - m_r(p, q)|^2}{\sum_{p,q}^{N,M} |m(p, q) - m_w(p, q)|^2} \quad (8)$$

where (p, q) are the pixels coordinates, N and M are the number of horizontal and vertical pixels of the recovered data, and $m_w(p, q)$ is the case with minimal magnification.

As can be seen in figure 5, the error increases as the magnification decreases. Besides, there is an evident connection between image magnification and image quality as straightforwardly noted from the graphic of figure 5. This behavior can be explained by the gradual loss of spatial frequencies of the input in the optical scaling procedure as the magnification decreases. Depending on the specific frequency content of the particular input, we can expect the degradation

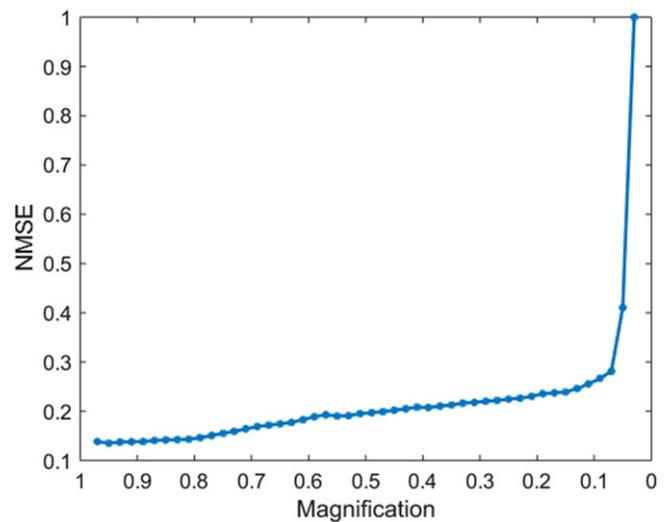


Figure 5. NMSE between the recovered data from the arrangement of figure 4(a) before and after magnification.

of quality to happen on a lower or higher magnification. In this sense there is not a general minimal achievable magnification, because it will strongly depend on the input and the parameters involved in the whole procedure.

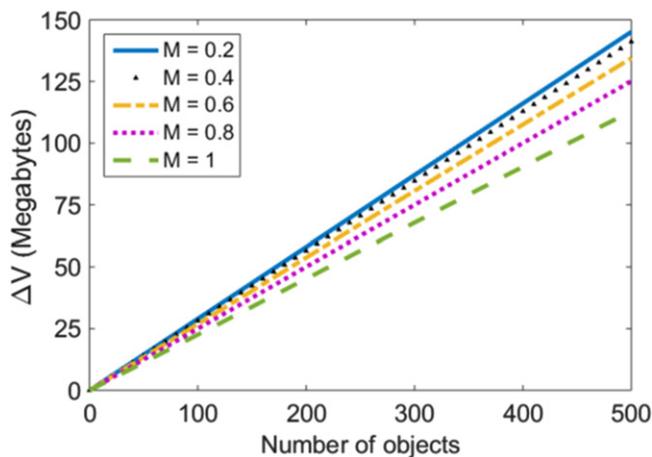


Figure 6. Dependence of ΔV on the number of objects for five M values.

We observe in figure 6 that the slope of ΔV as a function of the object number depends on the magnification. In this case, each object has the same properties as those shown in figure 4. The line corresponding to $M = 1$ shows the difference of volume when considering only the filtering process. Also, we see that the slope rate change diminishes as magnification reduces. Note that the volume reduction increases as the number of objects increases and the magnification reduces.

From figure 7, we stress that the filtering procedure sets a starting baseline of 77.18% to the volume reduction percentage. Magnification adds a further reduction from this baseline. The reduction shown in this plot is an indication of the potentials of filtering and optical scaling.

4. Conclusions

With this new optical approach, we present a strategy that improves the handling of a large volume of data. The combination of optical filtering and optical scaling steps allows formalizing the experimental technique. In order to measure the effectiveness of our method, we define the efficiency factor in terms of the parameters involved in each step. The resulting efficiency of the entire process is the product of the efficiency associated to each step. The final volume difference is a figure of merit that shows the final achievement. We would also like to emphasize that, in our demonstrations, we use experimental information and that the image reconstruction was solely based on previously known decoding techniques.

Any input can be processed as long as the experimental setup allows a proper encoding-decoding. Experimental results highlight the great potential of the method in impressively reducing the amount of data volume to be stored and transmitted. Although we introduced the experimental technique with a JTC encrypting architecture, any other optical encoding scheme can be successfully adapted to these ideas.

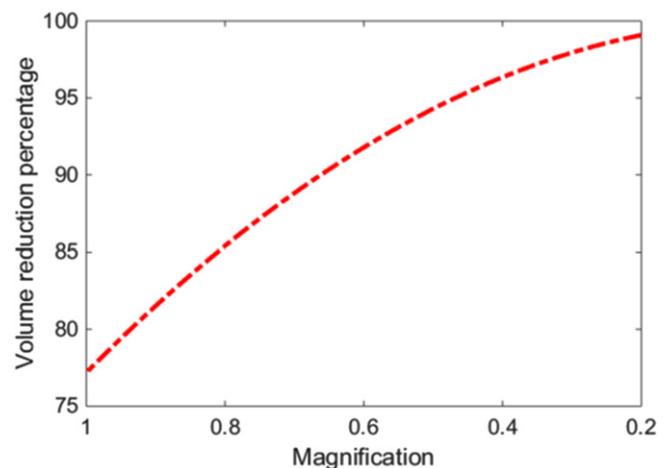


Figure 7. Percentage of volume reduction as a function of the magnification.

Handling optically encrypted images with data volume reduction techniques involving simple procedures, like the ones presented here, opens avenues for saving space in information conveying actions. This ability to form a single encrypted information unit with reduced space in managing multiplexed data opens new possibilities related to image techniques. The results obtained with a virtual optical system mean that it should be possible to implement the proposed optical protocol in an experimental optical setup, with all the advantages associated with optical processors.

This procedure can be extended to the handling of 2D and 3D multiple data in optical information processing. Even these concepts can be extended to the digital domain. Finally, we can mention that our optical techniques can be accompanied by digital techniques presented in the literature to improve data volume reduction. In this contribution, we only intend to introduce the concept, thus deferring the logical optimizations of the whole procedure to future contributions.

Acknowledgments

This research was performed under grants from Estrategia de Sostenibilidad 2014–2015 and Comité para el Desarrollo de la Investigación -CODI- (Universidad de Antioquia-Colombia), COLCIENCIAS (Colombia), MINCYT-COLCIENCIAS CO/13/05, CONICET No. 0549/12 (Argentina), and Facultad de Ingeniería, Universidad Nacional de La Plata No. 11/1168 (Argentina). John Fredy Barrera Ramírez acknowledges the support from The International Centre for Theoretical Physics (ICTP) Associateship Scheme.

References

- [1] Matoba O, Nomura T, Pérez-Cabré E, Millán M S and Javidi B 2009 Optical techniques for information security *Proc. IEEE* **97** 1128

- [2] Tajahuerce E, Matoba O, Verrall S C and Javidi B 2010 Optoelectronic information encryption with phase-shifting interferometry *Appl. Opt.* **39** 2313
- [3] Barrera J F, Mira-Agudelo A and Torroba R 2014 Experimental QR code optical encryption: noise-free data recovering *Opt. Lett.* **39** 3074
- [4] Barrera J F, Tebaldi M, Ríos C, Rueda E, Bolognini N and Torroba R 2012 Experimental multiplexing of encrypted movies using a JTC architecture *Opt. Express* **20** 3388
- [5] Trejos S, Barrera J F and Torroba R 2015 Optimized and secure technique for multiplexing QR code images of single characters: application to noiseless messages retrieval *J. Opt.* **17** 085702
- [6] Naughton T J, Frauel Y, Javidi B and Tajahuerce E 2002 Compression of digital holograms for three-dimensional object reconstruction and recognition *Appl. Opt.* **41** 4124
- [7] Darakis E and Soraghan J J 2007 Reconstruction domain compression of phase-shifting digital holograms *Appl. Opt.* **46** 351
- [8] Matoba O, Naughton T J, Frauel Y, Bertaux N and Bahram J 2002 Real-time three-dimensional object reconstruction by use of a phase-encoded digital hologram *Appl. Opt.* **41** 6187
- [9] Cucho E, Marquet P and Depeursinge C 2000 Spatial filtering for zero-order and twin-image elimination in digital off-axis holography *Appl. Opt.* **39** 4070
- [10] Velez A, Barrera J F and Torroba R 2015 One-step reconstruction of digitally assembled 3D extended holographic scenes *Opt. Laser Technol.* **75** 146
- [11] Nomura T and Javidi B 2000 Optical encryption using a joint transform correlator architecture *Opt. Eng.* **39** 2031
- [12] Barrera J F, Velez A and Torroba R 2013 Experimental multiplexing protocol to encrypt messages of any length *J. Opt.* **15** 055404

Optical field data compression by opto-digital means

Alejandro Velez¹, John Fredy Barrera², Sorayda Trejos²,
Myrian Tebaldi^{1,3} and Roberto Torroba^{1,3}

¹Centro de Investigaciones Ópticas (CONICET La Plata-CIC-UNLP) PO Box 3, C.P. 1897, La Plata, Argentina

²Grupo de Óptica y Fotónica, Instituto de Física, Facultad de Ciencias Exactas y Naturales, Universidad de Antioquia UdeA, Calle 70 No. 52-21, Medellín, Colombia

³UIDET OPTIMO, Facultad de Ingeniería, Universidad Nacional de La Plata, La Plata, Argentina

E-mail: alejandrov@ciop.unlp.edu.ar

Received 23 August 2016, revised 4 October 2016

Accepted for publication 6 October 2016

Published 1 November 2016



CrossMark

Abstract

Compression of optical field data is of interest due to the many applications where this kind of information processing is necessary. In particular, holographic recording has significant requirements in a high volume of both phase and amplitude data. We analyze and present a comparison between the performances of two lossy compression methods applied over optical field data: the optical scaling compression technique based on a virtual optical system that performs a scaling of the optical field data, and the JPEG format. In particular, we study the compression of optical fields data extracted from off-axis digital holograms. Our results show that optical scaling is better suited for the compression of the highly random phase information found in the optical field data of 3D diffuse objects. Data loss and volume reduction for each method are measured and compared.

 Online supplementary data available from stacks.iop.org/JOPT/18/125701/mmedia

Keywords: compression, holography, data processing by optical means

(Some figures may appear in colour only in the online journal)

1. Introduction

Digital holography is a powerful technique that allows optical processing by computational means. This technique has given rise to the development of sophisticated opto-digital methods that profit from both the properties of optical systems and the flexibility of digital data processing algorithms. Among the applications of digital holography, we find metrology, microscopy, medical imaging, and optical security [1–10], to name a few. Specifically, digital holography allows for recording information from 2D and 3D objects [11, 12], providing additional degrees of freedom for optical processing [13–15], and consequently making possible the reconstruction of scenes with depth [16].

Digital holography requires the record of an intensity pattern containing either phase and amplitude information, implying the recording of interference fringes [17] or multiple

phase-shifted images [18]. As a result, a large volume of data needs to be processed and stored digitally. Techniques to reduce the challenges imposed by this volume of data have been proposed, dealing mainly with quantization techniques [18–20], filtering [21], and both lossless and lossy data compression algorithms [22, 23].

One of the most used image compression algorithm is the Joint Photography Expert Group (JPEG) lossy compression format [24]. JPEG format works by subdividing the input image into 8×8 pixel blocks. A discrete cosine transform (DCT) is then applied to each block, and a quantization of the components of the resulting transform is performed. This quantization is the lossy part of JPEG format. The data is further compressed by application of the lossless Huffman coding [25]. The loss and degree of compression achievable by JPEG format can be controlled by a user defined quality factor (QF) that can take values between 1 and 100. This

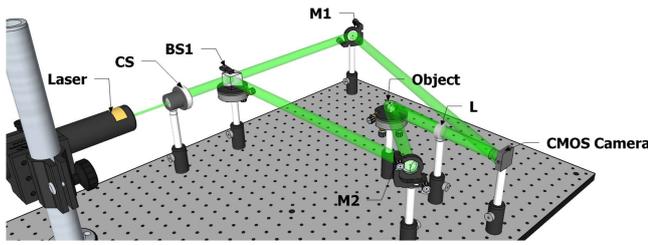


Figure 1. Scheme of the off-axis Fourier holographic setup. (CS: collimation system, BS: beam splitter, M: mirror, L: lens).

factor determines the coarseness of the quantization steps of the DCT.

JPEG compression has been applied to digital holograms [26], but it has been shown to have decreased compression performance with inputs exhibiting random noise [27]. A first approach would be a reduction by filtering the noise from the input. However, in data extracted from a hologram of a diffuse object, the near random oscillations of the phase carry information required for an adequate reconstruction. In this sense, noise cannot be removed, since it contains the information we must compress.

A different compression approach, whose performance is not dependent on the input, might be better suited to deal with the optical field data. In this sense, we have a technique based on using a virtual optical system to perform a scaling of the optical field data [28]. The proposal presented in [28] is based on the processing of the joint power spectrum (JPS) captured by using a CCD camera in a JTC cryptosystem. As usual, the input plane of the encryption system contains the information of the object to be encrypted attached to a random-phase mask and another random-phase mask that acts as the encrypting key. The JPS, which contains the encrypted object information, is captured by a CCD camera. The FT of the captured JPS allows obtaining a filtered region less than the total JPS region. In order to increase the volume reduction, an optical scaling operation is implemented. The scaling technique uses an optical operation, namely, image formation with magnification less than one by means of a positive lens. It should be mentioned that the main cause of loss of the optical scaling is precisely the finite size of the scaling lens. This size sets a limit to the high frequency of the compressed object. The input placed in the object plane of the lens is the optical field data, obtained after filtering the relevant information from the hologram. Operating directly over the optical field data instead over the hologram, ensures that the scaling does not result in the subsampling of holographic microfringes. After filtering and scaling, a compression of up to 94% over an input hologram is reported.

A way to confirm our assumptions is to evaluate the performance of the mentioned optical scaling procedure in comparison with the well-known JPEG compression format. We will show that the performance of optical scaling and JPEG compression are noticeably different when applied over both the phase and amplitude information of optical field data. In particular, this difference in terms of achievable compression will be noted when considering the reconstruction quality and efficiency of both methods. The quality is

assessed by measuring the correlation coefficient (CC) between the reconstructed objects from compressed and uncompressed data [29]. The compression efficiency is the volume difference expressed in kilobytes (KB). We employ these metrics for both JPEG compression and optical scaling when applied to actual optical field data.

2. Hologram registering and optical field data extraction

In order to evaluate our technique, we register the information of a diffuse 3D object by means of the off-axis Fourier digital holographic setup shown in figure 1.

In the CMOS camera plane, we register the interference between a reference plane wave and the Fourier transform (FT) of the light reflected by the input object, given by (see figure 2(a))

$$H(v, w) = |O(v, w)|^2 + |P(v, w)|^2 + O(v, w)P^*(v, w) + O^*(v, w)P(v, w), \quad (1)$$

where $O(v, w)$ is the FT of the object field, $P(v, w)$ is the tilted reference plane wave and * means complex conjugate. In the experimental setup, the reference wave is described as

$$P(v, w) = \exp(-i2\pi f(v \cos \alpha + w \cos \beta)), \quad (2)$$

where the angles α and β determine the tilt of the reference wave, and f is the focal length. We now perform the FT of the registered hologram,

$$h(x, y) = o(x, y) \otimes o^*(x, y) + p(x, y) \otimes p^*(x, y) + o(x, y) \otimes \delta(x - f \cos \alpha, y - f \cos \beta) + o^*(x, y) \otimes \delta(x + f \cos \alpha, y + f \cos \beta). \quad (3)$$

In equation (3), $o(x, y)$ and $p(x, y)$ represent the FT of $O(v, w)$ and $P(v, w)$ respectively.

The first two terms are the autocorrelations of the FT of the object and reference beams corresponding to the central order. The last two terms are the FT of the object field and its complex conjugate, spatially separated due to the convolution with the Dirac delta function resulting from the FT of the plane wave given by equation (2). Taking advantage of this spatial separation, we select the order corresponding to the FT of the third term of equation (3), filtering the remaining terms. After applying the inverse Fourier transform over this filtered term, we finally obtain the optical field data $O(v, w)$ (see figure 2(b)). A FT over this optical field data will reconstruct the object data $o(x, y)$. The object shown in figure 2(c) will be the reference against which we will measure the quality of the reconstructed objects from the compressed optical field data.

3. Quality and compression performance

Although filtering significantly reduces the amount of data to be stored, in the subsequent analysis we use the optical

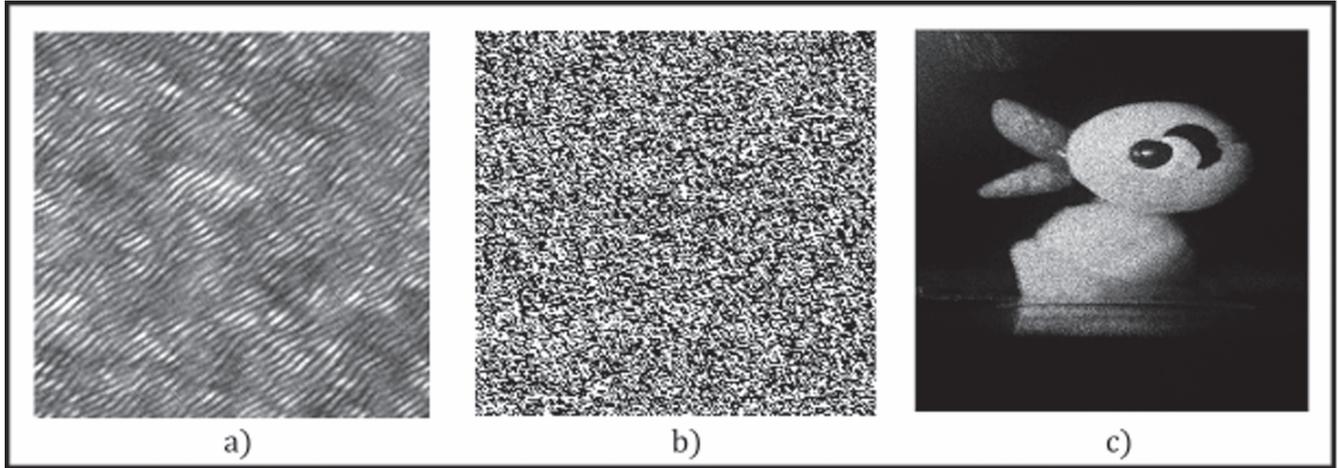


Figure 2. (a) Hologram, (b) intensity of the optical field data and (c) intensity of the object reconstructed from the optical field data.

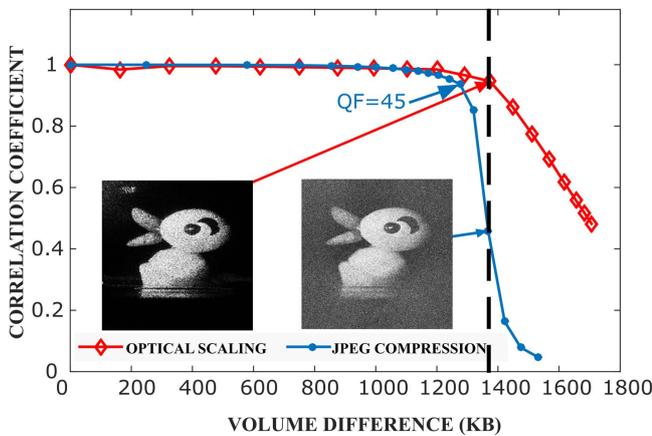


Figure 3. Correlation coefficient between the object reconstructed from the uncompressed and compressed field data for optical scaling and JPEG compression in terms of the achieved volume difference.

field data as the input to be processed by both compression methods. The experimental data to be compressed are recorded by using CMOS EO-10012M camera, with a pixel size of $1.67 \mu\text{m} \times 1.67 \mu\text{m}$ and $3480 \text{ pixel} \times 2748 \text{ pixel}$ resolution. The object has maximum dimensions of $18 \text{ mm} \times 24 \text{ mm} \times 16 \text{ mm}$. The focal length of the lens was 200 mm. A Laserglow Technologies diode pumped solid state laser operating at a wavelength of 532 nm and an output power of 50 mW is employed. The angle between the object and reference beam was approximately 5° , and the pixel size of the camera used allows for a maximum angle of 9.13° , thus ensuring that we can resolve the highest frequency of the interference pattern. This optical field data will be processed with the scaling compression method for values of magnification between 0 and 1 [28]. On the other hand, for comparison purposes, the same data is compressed using JPEG compression with QF between 1 and 100. Then, we proceed to evaluate the volume difference, defined as

$$\Delta V = V_R - V_C, \quad (4)$$

where V_R is the volume of the uncompressed optical field data and V_C is the volume of the compressed optical field data,

both volumes expressed in KB. In our experimental case, the original optical field data area is 940×940 pixels and depth of 8 bits resulting a data volume of $V_R = 1726 \text{ KB}$. The volume of the compressed optical field data is the number of bytes of the file in a computer memory after applied optical scaling and JPEG compression techniques.

Since we are dealing with lossy compression, we must also compare the quality of the reconstructed objects. We achieve this by digitally reconstructing the objects from the compressed and uncompressed optical fields and then evaluating their quality by using the CC defined as

$$CC = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{(\sum_m \sum_n (A_{mn} - \bar{A})^2)(\sum_m \sum_n (B_{mn} - \bar{B})^2)}}, \quad (5)$$

where m, n are the pixel coordinates, A the object intensity reconstructed from the uncompressed optical field, B the object intensity reconstructed from the compressed field data and \bar{A}, \bar{B} are the mean values of A and B , respectively.

In figure 3, each marker of the JPEG curve represents a decrease of the QF in steps of 5, starting at 100. This value corresponds to $\Delta V = 0$. Each point of the optical scaling curve corresponds to a decrease of 0.05 of the magnification value stating at 1 when $\Delta V = 0$. The JPEG compression achieves the largest volume decrease within the QF range between 100 and 45, and further reduction of the QF severely degrades the reconstructed object quality for a small increase in the volume difference (see media 1). On the other hand, optical scaling allows for a lesser loss of quality than JPEG compression at high compression ratios, as shown in the figure 3 at $\Delta V \geq 1380 \text{ KB}$ (see dotted line and inset figures).

In [27], it was demonstrated that the JPEG compression format shows decreased performance when the distribution of data is random. In diffuse objects, phase information has more random distribution in comparison with the amplitude information. In consequence, the behavior of the compression format should be different in both cases. To verify this, we proceed to evaluate the phase and amplitude information independently for each method. In order to perform the evaluation, we measure the volume difference of the phase and

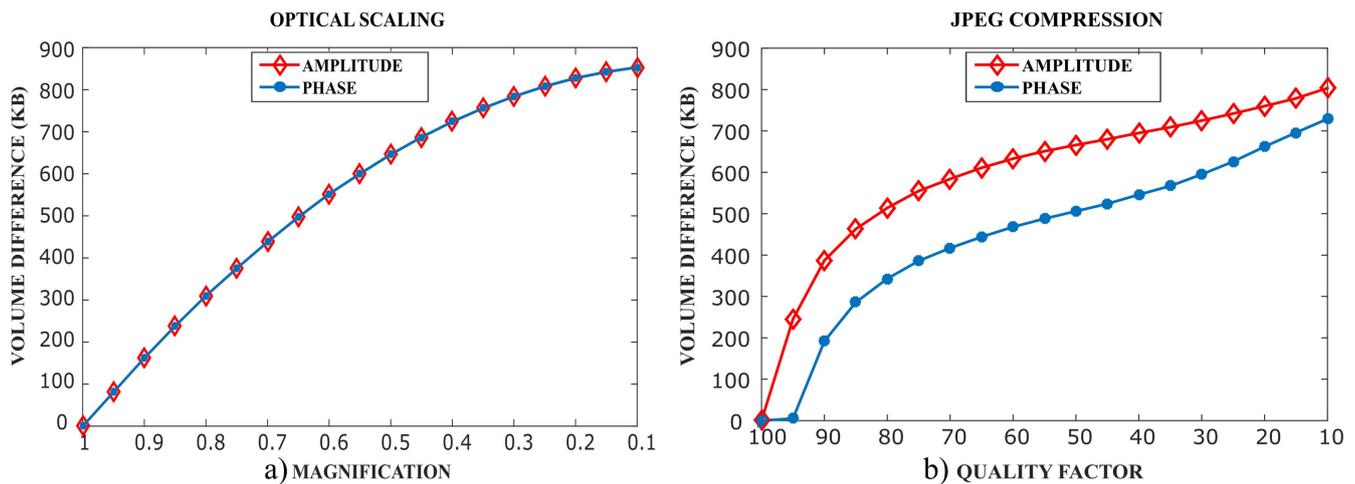


Figure 4. Volume difference of the phase and amplitude of the compressed data in terms of: (a) the magnification and (b) the QF.

the amplitude of the compressed optical field data in terms of the magnification and the QF parameters.

Figure 4 confirms that there is a difference in the performance of both methods. Optical scaling compression (figure 4(a)) shows the same behavior for both phase and amplitude information. On the other hand, JPEG compression (figure 4(b)) shows a significantly lower performance when applied to phase information. While these results seem to show that optical scaling is better suited to the compression of phase information of the optical field data, it is worth noting that the loss caused by both methods is qualitatively different. In the case of optical scaling the reconstructed object shows loss of high frequencies, while in the case of the JPEG compression it shows an increase in noise. In this sense, while optical scaling shows a more predictable behavior for optical field data, there may be cases where the loss of high frequency fringes is not desirable.

4. Conclusions

Since phase carries a significant amount of the holographic information, it is necessary to achieve the maximum possible compression with the minimum loss. Methods used for general image compression like JPEG or other spatial or spectral quantization compression methods were not developed for random distributions. In this work we verified that the optical scaling procedure is an adequate alternative with better performance in comparison with JPEG compression for random data distributions. We believe that efficient compression of optical field data requires taking into account the properties of phase information, therefore other optical methods should be further explored.

Acknowledgments

This research was performed under grants from Estrategia de Sostenibilidad 2014–2015 and Comité para el Desarrollo de

la Investigación -CODI- (Universidad de Antioquia-Colombia), MINCyT-COLCIENCIAS CO/13/05, CONICET Nos. 0849/16 and 0549/12 (Argentina), and Facultad de Ingeniería, Universidad Nacional de La Plata No. 11/I215 (Argentina). John Fredy Barrera Ramírez acknowledges the support from the International Centre for Theoretical Physics ICTP Associateship Scheme.

References

- [1] Osten W, Faridian A, Gao P, Körner K, Naik D, Pedrini G, Singh A K, Takeda M and Wilke M 2014 Recent advances in digital holography (Invited) *Appl. Opt.* **53** G44–63
- [2] Jaedicke V, Goebel S, Koukourakis N, Gerhardt N C, Welp H and Hofmann M R 2014 Multiwavelength phase unwrapping and aberration correction using depth filtered digital holography *Opt. Lett.* **39** 4160–3
- [3] Merrill D, An R, Turek J and Nolte D D 2015 Digital holography of intracellular dynamics to probe tissue physiology *Appl. Opt.* **54** A89–97
- [4] Javidi B et al 2016 Roadmap on optical security *J. Opt.* **18** 083001
- [5] Shen X, Lin C and Kong D 2012 Fresnel–transform holographic encryption based on angular multiplexing and random–amplitude mask *Opt. Eng.* **51** 068201
- [6] Mosso F, Tebaldi M, Barrera J F, Bolognini N and Torroba R 2011 Pure optical dynamical color encryption *Opt. Express* **19** 13779–86
- [7] Barrera J F, Henao R, Tebaldi M, Torroba R and Bolognini N 2006 Multiplexing encrypted data by using polarized light *Opt. Commun.* **260** 109–12
- [8] Lin J, Yuan X C, Tao S H and Burge R E 2007 Multiplexing free-space optical signals using superimposed collinear orbital angular momentum states *Appl. Opt.* **46** 4680–5
- [9] Trejos S, Barrera J F, Tebaldi M and Torroba R 2014 Experimental optodigital processing of multiple data via modulation, packaging and encryption *J. Opt.* **16** 055402
- [10] Chen W and Chen X 2016 Digital holography-secured scheme using only binary phase or amplitude as ciphertext *Appl. Opt.* **55** 6740–6
- [11] Micó V, Ferreira C and Garcia J 2013 Lensless object scanning holography for two-dimensional mirror-like and diffuse reflective objects *Appl. Opt.* **52** 6390–400

- [12] Nehmetallah G and Banerjee P P 2012 Applications of digital and analog holography in three-dimensional imaging *Adv. Opt. Photon.* **4** 472–553
- [13] Mosso F, Barrera J F, Tebaldi M, Bolognini N and Torroba R 2011 All-optical encrypted movie *Opt. Express* **19** 5706–12
- [14] Lin C, Shen X and Li B 2014 Four-dimensional key design in amplitude, phase, polarization and distance for optical encryption based on polarization digital holography and QR code *Opt. Express* **22** 20727–39
- [15] Chen W 2015 Multiple-wavelength double random phase encoding with CCD-plane sparse-phase multiplexing for optical information verification *Appl. Opt.* **54** 10711–6
- [16] Velez A, Barrera J F and Torroba R 2015 One-step reconstruction of assembled 3D holographic scenes *Opt. Laser Technol.* **75** 146–50
- [17] Schnars U and Jüptner W P O 2002 Digital recording and numerical reconstruction of holograms *Meas. Sci. Technol.* **13** R85–101
- [18] Darakis E and Soraghan J J 2007 Reconstruction domain compression of phase-shifting digital holograms *Appl. Opt.* **46** 351–6
- [19] Mills G A and Yamaguchi I 2005 Effects of quantization in phase-shifting digital holography *Appl. Opt.* **44** 1216–25
- [20] Matoba O, Naughton T J, Frauel Y, Bertaux N and Javidi B 2002 Real-time three-dimensional object reconstruction by use of a phase-encoded digital hologram *Appl. Opt.* **41** 6187–92
- [21] CuChe E, Marquet P and Depeursinge C 2000 Spatial filtering for zero-order and twin-image elimination in digital off-axis holography *Appl. Opt.* **39** 4070–5
- [22] Naughton T J, Frauel Y, Javidi B and Tajahuerce E 2002 Compression of digital holograms for three-dimensional object reconstruction and recognition *Appl. Opt.* **41** 4124–32
- [23] Alfalou A and Brosseau C 2013 Implementing compression and encryption of phase-shifting digital holograms for three-dimensional object reconstruction *Opt. Commun.* **307** 67–72
- [24] Wallace G K 1992 The JPEG still picture compression standard *IEEE Trans. Consum. Electron.* **38** xviii–xxxiv
- [25] Huffman D A 1952 A method for the construction of minimum-redundancy codes *Proc. IRE* **40** 1098–101
- [26] Darakis E and Soraghan J J 2006 Compression of interference patterns with application to phase-shifting digital holography *Appl. Opt.* **45** 2437–43
- [27] Shahnaz R, Walkup J F and Krile T F 1999 Image compression in signal-dependent noise *Appl. Opt.* **38** 5560–7
- [28] Trejos S, Barrera J F, Velez A, Tebaldi M and Torroba R 2016 Optical approach for the efficient data volume handling in experimentally encrypted data *J. Opt.* **18** 065702
- [29] Goodman J W 2000 *Statistical Optics* (New York: Wiley) p 17

PAPER • IOPSELECT

Optical field data compression by opto-digital means

Alejandro Velez¹, John Fredy Barrera², Sorayda Trejos², Myrian Tebaldi^{1,3} and Roberto Torroba^{1,3}

Published 1 November 2016 • © 2016 IOP Publishing Ltd
Journal of Optics, Volume 18, Number 12



1383 Total downloads

Turn on MathJax

Share this article



Get permission to re-use this article

Figura A.1: El artículo *Optical field data compression by opto-digital means* en la exclusiva sección IOPselect.

Journal of Optics

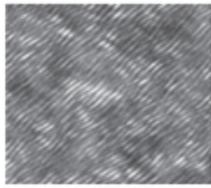
This is to certify that the article

Optical field data compression by opto-digital means
by **Alejandro Velez, John Fredy Barrera, Sorayda Trejos,
Myrian Tebaldi and Roberto Torroba**

has been selected by the editors of *Journal of Optics* for inclusion in the exclusive
'Highlights of 2016' collection. Articles are chosen on the basis
of referee endorsement, novelty, scientific impact and broadness of appeal.

Figura A.2: El artículo *Optical field data compression by opto-digital means* en la sección exclusiva "Highlights 2016".

Editorial & news



**Paper of the Week –
Optical field data
compression by opto-
digital means**
Alejandro Velez *et al*

verify that the optical scaling procedure is an adequate alternative with better performance in comparison with JPEG compression for random data distributions.

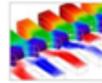
LabTalk

Most recent

Most read



**Practicable optical hiding
method of a 3D object**
Oct 25, 2016



**Self-sustained coherent
phonon generation in
optomechanical cavities**
Oct 18, 2016

Figura A.3: El artículo *Optical field data compression by opto-digital means* como el artículo de la semana en la revista Journal of Optics.

IOPscience Journals Books Login Search all IOPscience content Search Article lookup

Journal of Optics

Optical cryptography

Data safeguarding with the power of light.



00:03 00:05

Cryptography is of increasing importance in our technological age using broadcast, network communications, Internet, e-mail, cell phones, etc., all of which may transmit sensitive information related to finances, politics, business and private confidential matters. Cryptography relates to transmitting information with access restricted only to the intended recipient even if the message is

Related links

Optimized and secure technique for multiplexing QR code images of single characters: application to noiseless messages retrieval
Optics and Photonics Group at Universidad de Antioquia

Most recent Most read

- Practicable optical hiding method of a 3D object
Oct 25, 2016
- Self-sustained coherent phonon generation in optomechanical cavities
Oct 18, 2016
- An asymmetric two-photon quantum

Figura A.4: El artículo *Optimized and secure technique for multiplexing QR code images of single characters: application to noiseless messages retrieval*, en la sección *Lab talk: Optical cryptography* en la revista Journal of Optics.

SPIE.

2015 CERTIFICATE
OF EXCELLENCE

Sorayda Trejo González

For Second Place Student Presentation
secure optodigital protocol to handle messages using the multiplexing of
processed QR codes

SIXTH INTERNATIONAL CONFERENCE ON SPECKLE METROLOGY

MEXICO
AUGUST, 25 2015

Toyohiko Yatagai
Prof. Toyohiko, SPIE 2015 President

Sorayda Trejos G

Figura A.5: Reconocimiento al trabajo *Secure opto-digital protocol to handle messages using the multiplexing of processed QR codes*, con presentación modalidad póster.

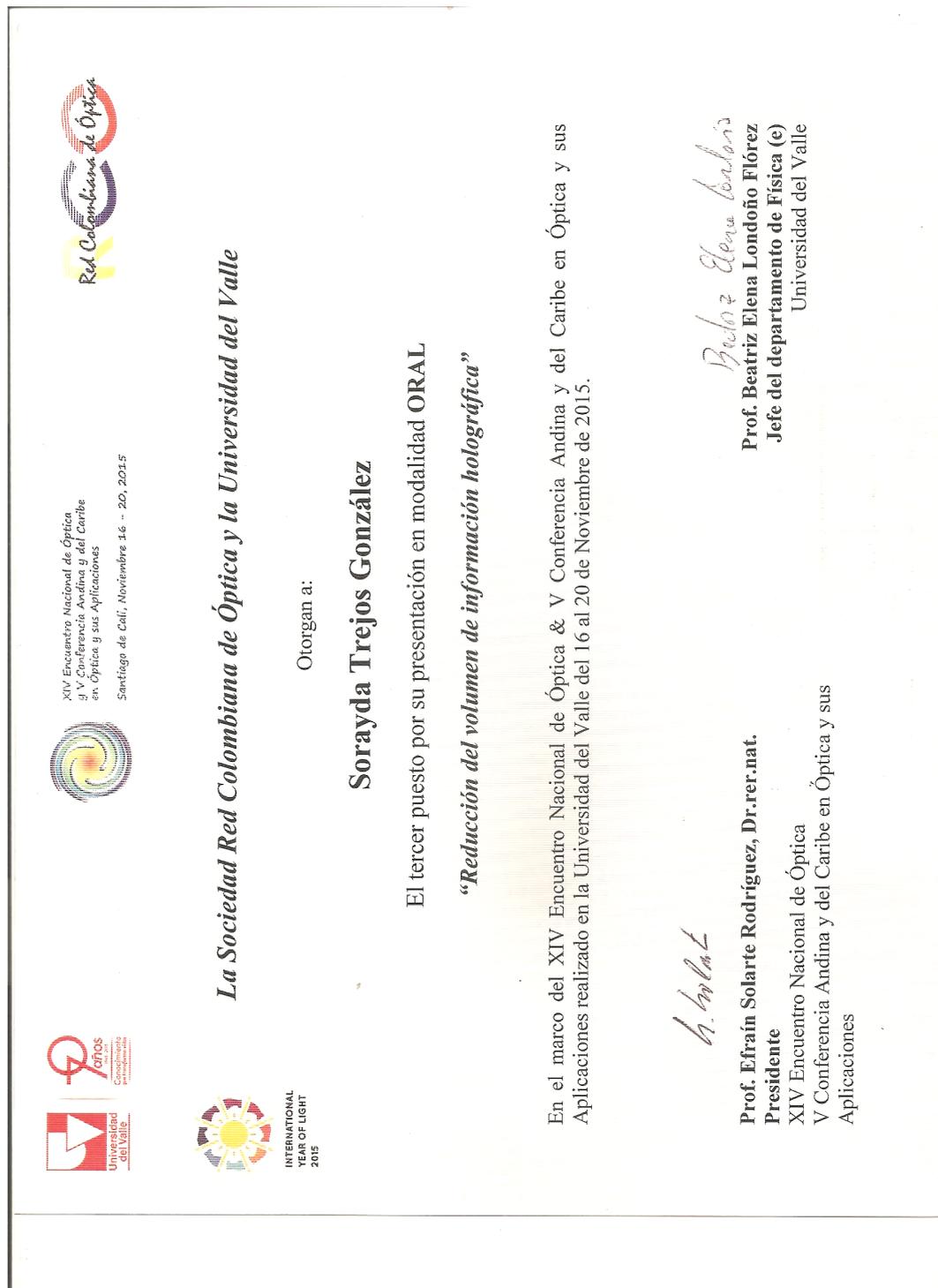


Figura A.6: Reconocimiento al trabajo *Reducción del volumen de información holográfica*, con presentación modalidad oral.