

Sistemas ópticos compactos para la protección de información



John Alexis Jaramillo Osorio

Instituto de Física

Universidad de Antioquia

Medellín

2022

Sistemas ópticos compactos para la protección de información

Trabajo de grado para optar al título de Doctor en Física

Presentado por:

John Alexis Jaramillo Osorio

Dirigido por:

Dr. John Fredy Barrera Ramírez

Medellin

2022

“Hay hombres que luchan un día y son buenos. Hay otros que luchan un año y son mejores. Hay quienes luchan muchos años, y son muy buenos. Pero hay los que luchan toda la vida: esos son los imprescindibles.”

Bertolt Brecht

Agradecimientos

Agradezco de forma general a todas las personas que de una u otra manera han contribuido a la realización y culminación de este trabajo.

Al profesor John Fredy Barrera un agradecimiento especial por su paciencia y apoyo constante, por los conocimientos entregados tanto en lo académico como en lo personal, por los consejos, los tiempos de espera y por comprender muchas de las dificultades que se me presentaron. Gracias por la confianza depositada en mí desde el pregrado. A él le debo lo el estar hoy culminando este trabajo de investigación.

Quiero agradecer al profesor Alejandro Veléz, por el acompañamiento desde el primer momento en que tuve contacto con el grupo de investigación y el gran apoyo que me ha brindado, por el tiempo en el laboratorio y la buena energía en todo momento.

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

Un agradecimiento al programa Training and Research in Italian Laboratories (TRIL) del centro internacional Abdus Salam de física teórica y especialmente al profesor Humberto Cabrera, quién me acogió de excelentemente durante mi pasantía de investigación en su laboratorio.

Por último, pero no menos importante un agradecimiento inmenso a mi familia, a Dey y

a Sofi, por el apoyo incondicional y el amor que me brindan, la paciencia que me tuvieron en todos este tiempo de arduo trabajo. Gracias por compartir conmigo alegrías, frustraciones, tristezas y logros.

A todos muchísimas gracias.

Alexis Jaramillo Osorio

Noviembre 2022

Índice general

1. Introducción	1
1.1. Introducción general	1
1.2. Contenido por capítulos	7
Bibliografía	11
2. Sistemas ópticos de encriptación	17
2.1. Sistema óptico de encriptación basado en una arquitectura 4f	18
2.2. Sistema de encriptación JTC en el dominio de Fourier	23
2.3. Descripción del sistema de encriptación JTC en el dominio de Fourier	24
2.4. Registro y filtrado del dato encriptado	25
2.4.1. Registro del dato encriptado	25
2.4.2. Filtrado del dato encriptado	27
2.5. Registro y filtrado de la llave de encriptación	30
2.5.1. Registro del holograma de la TF de la llave	30
2.5.2. Filtrado de la llave de encriptación	32
2.6. Desencriptación	33
Bibliografía	36
3. Sistema de encriptación de Fourier fraccionario usando una lente electro- óptica de foco variable	39

3.1.	Sistema de encriptación FrJTC usando una lente electro-óptica de foco variable	42
3.2.	Proceso de encriptación	43
3.3.	Registro de la información de la llave	46
3.4.	Proceso de desencriptación en el sistema FrJTC	47
3.5.	Resultados	48
3.5.1.	Resultados numéricos	48
3.5.2.	Resultados experimentales	52
3.5.3.	Encriptación de múltiples datos	58
3.6.	Conclusiones	61
	Bibliografía	63
4.	Encriptación óptica usando modulación de fase a partir del efecto lente	
	térmica	70
4.1.	Modulación de la fase debido al efecto lente térmica	72
4.2.	Descripción del sistema JFSC	75
4.3.	Proceso de encriptación en el sistema JFSC usando ELT	76
4.4.	Registro del holograma de la llave	79
4.5.	Proceso de desencriptación	80
4.6.	Resultados experimentales	81
4.6.1.	Procesos de encriptación y recuperación	81
4.6.2.	Proceso de encubrimiento de información	85
4.6.3.	Resultados experimentales del proceso de encubrimiento	89
4.6.4.	Resistencia a ataques	91
4.7.	Conclusiones	94
	Bibliografía	97
5.	Sistema de encriptación con un solo brazo de iluminación	101
5.1.	Descripción del sistema con un solo brazo de iluminación	105
5.2.	Registro del dato encriptado	106

5.3.	Registro de la información de la llave	108
5.4.	Proceso de recuperación en el sistema en línea	110
5.5.	Resultados experimentales	112
5.5.1.	Tolerancia de los datos encriptados al ruido aleatorio y a la pérdida de información	115
5.5.2.	Recuperación libre de ruido	118
5.5.3.	Protocolo de multiplexado selectivo basado en mascarar binarias	122
5.5.4.	Teclado encriptado	129
5.5.5.	Recuperación experimental de un mensaje a partir del teclado óptico	132
5.6.	Conclusiones	136
	Bibliografía	138
6.	Holografía digital usando como sistema de proyección un dispositivo digital de microespejos	143
6.1.	Holografía digital en el dominio de Fourier y Fresnel usando un DDM	147
6.1.1.	Registro, filtrado y recuperación de un holograma de Fourier	147
6.1.2.	Registro, filtrado y recuperación de un holograma de Fresnel	150
6.2.	Resultados experimentales	152
6.2.1.	Registro holográfico con recuperación dinámica de datos	158
6.2.2.	Recuperación holográfica libre de ruido	162
6.3.	Conclusiones	163
	Bibliografía	165
7.	Prototipo de encriptación compacto y de bajo costo	171
7.1.	Sistema de codificación JFSC de bajo costo	173
7.1.1.	Resultados experimentales obtenidos en el sistema JFSC de bajo costo	174
7.2.	Prototipo de un sistema de encriptación compacto de bajo costo	175
7.2.1.	Resultados experimentales preliminares	176
7.3.	Conclusiones	178

Bibliografía	179
8. Conclusiones y perspectivas	181
A. Productos de investigación	186
A.1. Artículos internacionales publicados	187
A.2. Proceeding de un evento Iberoamericano	187
A.3. Trabajo presentado en un evento científico internacional	188
A.4. Trabajos presentados en eventos científicos nacionales	188

Capítulo 1

Introducción

1.1. Introducción general

Con el crecimiento continuo en la cantidad de información que se transmite a través de los medios disponibles actualmente, también se han incrementado la cantidad de ataques que buscan acceder a la información de forma fraudulenta. Debido a esto, personas, compañías y entidades que buscan proteger información valiosa se ven en la necesidad de buscar alternativas que permitan la manipulación segura de información confidencial. Como ejemplo, en 2021, el mercado global relacionado con los sistemas digitales de encriptación fue valorado en 10,9 mil millones de dolares y se espera que alcance los 22,1 mil millones de dolares para el 2026, con un porcentaje de crecimiento de 15,2% [1]. Los principales sectores de aplicación de este tipo de sistemas son el financiero y el bancario: enfocados en la protección de información y transacciones bancarias; el sector médico: donde se hace uso de algoritmos de seguridad para proteger información relacionada con pacientes con el propósito de ofrecer una mayor confidencialidad, integridad y autenticación [2]; en el sector de industria y comercio: se utilizan los protocolos de autenticación de productos y anti-falsificación (hologramas, etiqueta de seguridad, entre otros), a través de detección óptica e identificación de carac-

terísticas de seguridad [3]; en el área de bienes de lujo en tecnologías de autenticación de bienes de alto valor y anti-falsificación [4]; en el campo gubernamental para el incremento de los mecanismos de seguridad de los programas de gobierno en la nube (pasaportes, información privada de los ciudadanos, registradurías y notarías, aplicaciones, registros, imágenes de terrenos y/o propiedades, entre otros); y en la industria del entretenimiento para la adición de imágenes encriptadas en contenido audiovisual o imágenes, y la recuperación de la información con contenido sobre titulares de derechos. Adicionalmente, en el sector militar y fuerzas armadas del estado, y el comercio electrónico.

A pesar de los avances e implementaciones mencionadas anteriormente, los crecientes avances tecnológicos y computacionales han hecho posible que los algoritmos digitales usados para la protección de información puedan ser quebrantados, permitiendo el acceso de usuarios no autorizados a información sensible. Debido a esto, desde varias ramas de la ciencia se han venido adelantando investigaciones con el propósito de solventar este problema. Particularmente, en las últimas décadas, la manipulación de información a través de la luz se ha convertido en un área en constante crecimiento. Los avances científicos y tecnológicos en esa dirección han generado productos y subproductos que han permitido mejorar la calidad de vida de la sociedad actual; y se prevé que las investigaciones que se están llevando a cabo en este campo, contribuyan a la solución de problemas tecnológicos, sociales, económicos y ambientales que se puedan presentar a futuro [5, 6]. Específicamente, el área de la óptica encargada de la manipulación eficiente y segura de la información ha permitido desarrollar esquemas experimentales que han hecho posible la recepción, el almacenamiento y el envío de información de forma segura, convirtiéndose en una alternativa a los métodos de software y hardware que se usan comúnmente.

De acuerdo a lo antes mencionado, el área de la manipulación segura de información, ya sea a través de algoritmos o por medio de la luz, es un campo en constante evolución que busca dar solución a las problemáticas de seguridad que se presentan al momento del almacenamiento, envío y recepción de la información [7–11]. Tanto desde el sector seguridad, como desde sectores afines, aún se están buscando sistemas de protección que presenten un grado elevado de seguridad, de manera que sean confiables para los usuarios de los sistemas

públicos y privados que manipulan información sensible.

Con el propósito de contribuir a la solución de los problemas de seguridad y teniendo presente las capacidades y el gran desempeño que presentan los sistemas ópticos experimentales para la manipulación segura de la información, desde el campo de la óptica se han venido desarrollando investigaciones que tienen como finalidad el establecimiento de técnicas, protocolos y esquemas ópticos que permitan generar sistemas de seguridad confiables y que puedan ser implementados en aplicaciones de seguridad, inclusive se han reportado algunas patentes [12–15].

De forma general las técnicas empleadas para la protección de la información a través de la luz se les conoce como métodos ópticos de encriptación o de cifrado óptico, y los sistemas que tienen como propósito encriptar, ocultar o cifrar la información a partir de medios ópticos son conocidos como sistemas de encriptación o arquitecturas ópticas de encriptación. Por su parte, el proceso de recuperación de la información oculta es conocido como proceso de desencriptación o recuperación. En la última década, el estudio de los métodos de encriptación y en particular de las arquitecturas de encriptación ha venido tomando un papel preponderante, pues son considerados como una opción con gran potencial a los sistemas de protección que se usan actualmente. En los últimos 5 años, se han desarrollado avances que han permitido impulsar notoriamente esta área de investigación [8, 16–18].

Los desarrollos presentados a la fecha demuestran el gran potencial que tienen los sistemas ópticos de protección en aplicaciones de uso masivo, despertando aún más el interés por parte de la comunidad científica. Se debe tener en cuenta que la mayoría de los sistemas desarrollados son óptico-virtuales, es decir, simulaciones computacionales que buscan representar los arreglos experimentales. Aunque estos sistemas han sido útiles en la evaluación de algunos de los parámetros que intervienen en el proceso, han mostrado ser vulnerables [19, 20]. En contraste con lo anterior, los sistemas de encriptación implementados experimentalmente y que tienen como llave de seguridad un elemento físico y aleatorio han mostrado un alto grado de seguridad [16, 17, 21].

La gran confiabilidad de los sistemas experimentales de encriptación radica principalmente en el uso de un difusor (vidrio esmerilado, el cual es un elemento físico que introduce cambios de fase aleatorios a un haz incidente) como llave de seguridad, ya que a este tipo de elementos no se les pueden establecer parámetros como el tamaño de pixel o el número de pixeles, y no presentan un número definido y limitado de variaciones como los elementos de fase aleatorios usados en los sistemas óptico-virtuales, características que hacen que estos sistemas sean vulnerables a cierto tipo de ataques. Además, los grados de libertad que presentan los arreglos experimentales, como: la polarización de la luz, la longitud de onda de la luz usada, las pupilas, la amplitud y la fase del campo óptico, etc; pueden actuar como parámetros extra que refuerzan la seguridad que provee el sistema de encriptación. Por lo tanto, para acceder a la información cifrada ópticamente, es necesario conocer la información de la llave de seguridad y los parámetros extra involucrados al momento de realizar el proceso de ocultamiento óptico. Las características de la llave física en conjunto con los grados de libertad del procesador óptico experimental hacen que hasta ahora los sistemas experimentales de encriptación óptica garanticen un manejo seguro de datos, y que sean una alternativa válida a los sistemas que se usan actualmente [16, 17, 21].

Dentro de los sistemas ópticos de encriptación más implementados y estudiados se tiene el sistema de encriptación 4f [22]. Este sistema emplea una técnica de encriptación de doble máscara de fase aleatoria o DRPE (siglas en inglés de: double random phase encryption), debido a que usa la convolución de dos funciones aleatorias de fase para convertir el dato encriptado en un patrón de ruido blanco. En general, la implementación experimental de la arquitectura de codificación 4f requiere de un sistema interferométrico para el registro de la información que contiene el dato encriptado y la llave de seguridad [23–25]. Debido a lo anterior, es necesario utilizar una gran cantidad de elementos ópticos para llevar a cabo el proceso de encriptación y el proceso de registro de la llave, incrementando los requerimientos de alineación y estabilidad para garantizar el correcto desempeño del sistema. Con el propósito de desarrollar una arquitectura con menos exigencias experimentales que la arquitectura 4f, se propuso la arquitectura de encriptación óptica basada en el correlador transformada conjunta JTC (siglas en inglés de: joint transform correlator) [26, 27], arquitectura con menos elementos y con requerimientos de alineación y estabilidad menores a los exigidos por el

sistema 4f [28, 29].

El sistema JTC se ha estudiado y desarrollado en mayor medida debido a que es más propicio para implementaciones experimentales, y presenta mayor potencial para aplicaciones prácticas y un alto desempeño para el procesamiento seguro de información. A diferencia del sistema 4f, el sistema JTC presenta una arquitectura que es inherentemente holográfica, por lo cual no es necesario el uso de sistemas interferométricos fuera de eje (brazo de referencia) para el registro del dato encriptado.

A pesar de las grandes ventajas que presentan los sistemas de codificación basados en la técnica de DRPE, y específicamente el sistema de encriptación JTC, todavía existen algunas limitaciones que deben ser abordadas para que estos esquemas sean considerados como alternativa confiable y válida en esquemas de investigación básica y en un posible entorno aplicado. Uno de los principales desafíos que se debe abordar es el desarrollo de arquitecturas compactas, de bajo costo y eficientes para la manipulación segura de datos en ambientes experimentales y entornos prácticos, lo cual está directamente relacionado con las dimensiones y la complejidad de las configuraciones experimentales. En particular, el sistema JTC requiere de dos brazos de iluminación, un brazo permite obtener el dato encriptado, mientras que para llevar a cabo el registro de la llave de codificación se utilizan los dos brazos de iluminación, esto hace necesario el uso de múltiples elementos ópticos, lo que a su vez implica que su disposición experimental requiera de un espacio considerable.

Además de lo anterior, se deben superar los problemas relacionados con la degradación de los datos recuperados, buscando solventar esta dificultad, varios trabajos se han orientado hacia el desarrollo de técnicas enfocadas en la reducción del ruido y la degradación en los datos recuperados [30–34]. Estas técnicas han permitido mejorar la calidad de la información recuperada eliminando parcialmente la degradación generada principalmente por las máscaras de fase utilizadas en el proceso de codificación. Además de esto, buscando una recuperación libre de ruido, se introdujo el concepto de “contenedores de información” [35], con este método la información a encriptar es codificada previamente en un código QR (siglas en inglés de Quick Response), y luego el código QR con la información codificada es encriptado. Además

de los códigos QR, se han empleado otras representaciones como los contenedores diseñados para la seguridad óptica o CCOS (siglas en inglés de: customized containers for optical security) [36]. El uso de códigos QRs o CCOS permite llevar a cabo el proceso de encriptación con una recuperación libre de ruido.

Adicionalmente a los retos propios relacionados con la implementación experimental de los esquemas de codificación, se debe considerar que el registro holográfico de la información a partir de las configuraciones de cifrado óptico debe admitir la manipulación de grandes volúmenes de datos, lo cual hace costoso el manejo digital de dicha información limitando su rango de aplicación. Buscando sobrepasar esta dificultad, se han reportado varias investigaciones enfocadas en la compresión de datos holográficos a partir de medios ópticos, demostrando que los métodos ópticos son más eficientes que los digitales, cuando se trata de información holográfica [37]. Entre los métodos ópticos para la compresión de información holográfica se encuentran el escalado óptico [38, 39], el muestreo aleatorio [40, 41] y la implementación de algoritmos que posibilitan la compresión de información a partir de la manipulación de la fase de los datos holográficos [42, 43].

Otro aspecto importante que debe ser considerado para la implementación de sistemas de codificación ópticos está relacionado con la capacidad de procesar información en un ambiente multiusuario. Con este propósito se han estudiado ampliamente los métodos de multiplexado óptico, los cuales permiten almacenar una gran cantidad de información encriptada en un solo dato de campo óptico que se obtiene al variar alguno de los parámetros ópticos que intervienen durante el proceso de codificación [44–48]. Algunas técnicas de multiplexado se basan en la variación de la longitud de onda del haz de iluminación [44, 45], la modificación de la polarización de la luz [46], la rotación de la máscara de fase usada en el proceso de codificación [47], el desplazamiento lateral de la máscara aleatoria en un esquema JTC [48], entre otras. Por otro lado, algunos sistemas han incorporado técnicas de multiplexado basadas en la modificación del orden fraccionario en un sistema de codificación en el dominio de Fourier fraccionario [49]. Además de lo anterior, la implementación de técnicas de multiplexado ha posibilitado el procesamiento seguro de datos a color [50] y vídeos [51, 52].

Teniendo en cuenta los retos por superar y las ventajas experimentales del sistema JTC, en este trabajo se realiza un estudio teórico-experimental con el propósito de desarrollar una arquitectura de encriptación óptica experimental, basada en un sistema JTC, que posea un solo brazo de iluminación. Prescindir del brazo de referencia representa un reto, ya que debe generarse un protocolo que permita compensar su funcionalidad. En ese sentido, es muy importante el diseño del plano de entrada del sistema para que sea posible registrar el dato encriptado y la llave de seguridad usando únicamente una disposición experimental similar a la del sistema JTC convencional, sin la necesidad de incluir un brazo de referencia. Este nuevo sistema de encriptación debe permitir la implementación de técnicas ópticas no lineales para la reducción de ruido [31, 33, 34] y el uso de contenedores de información que permitan la manipulación de una gran cantidad de datos y una recuperación libre ruido [16, 35, 36]. Además, se debe garantizar que el sistema desarrollado permite la implementación de ambientes multi-usuarios a partir de técnicas de multiplexado [44–49], y procedimientos que permitan la reducción del volumen de la información procesada [53–56]. Lo anterior permitirá desarrollar un sistema compacto, de bajo costo, más flexible y mucho más conveniente para implementaciones encaminadas a la investigación básica, y además con mayor potencial para su aplicación en posibles futuras aplicaciones en el sector seguridad y afines.

1.2. Contenido por capítulos

En el segundo capítulo de este trabajo se presentan los esquemas ópticos de encriptación más usados que basan su funcionamiento en la técnica de DRPE (siglas en inglés de: doble random phase encoding), específicamente el sistema 4f y el sistema JTC (siglas en inglés de: joint transform correlator). El estudio de estas arquitecturas de encriptación es el punto de partida para las propuestas experimentales que se presentan en esta tesis. En particular, se hace una descripción detallada del proceso de encriptación y recuperación en el sistema JTC en el dominio óptico de Fourier, ya que este sistema presenta una arquitectura versátil que permite la implementación de protocolos para mejorar la seguridad y las capacidades en la manipulación segura de información, y su configuración experimental servirá de base

para el desarrollo de los esquemas implementados en este trabajo de investigación. Además, se presenta el proceso estándar de filtrado que se le aplica al dato encriptado y a la llave de seguridad, el cual es aplicado a la información obtenida en los sistemas de codificación implementados en este trabajo. Finalmente, se presentan algunos resultados experimentales que muestran las principales características de seguridad del sistema JTC en el dominio óptico de Fourier, estos resultados permiten establecer un punto de comparación entre los resultados ya reportados en múltiples trabajos y los resultados que se obtuvieron en este trabajo de investigación.

A partir del capítulo tres, se presentan las contribuciones originales que resultaron de este trabajo de investigación. En el tercer capítulo se realiza la descripción teórica y experimental de un sistema de encriptación en el dominio de Fourier fraccionario usando una lente electro-óptica de foco variable (LEFV). En este esquema el orden fraccionario de la transformada se modifica a partir de cambios en la longitud focal de la lente transformadora que se logran a través de variaciones en la corriente inducida sobre la LEFV. En los sistemas convencionales donde se usan lentes de foco fijo para modificar el orden fraccionario de la transformada, se requieren desplazadores mecánicos para cambiar la posición del plano de registro o cambiar la lente transformadora, aumentando los requerimientos de alineación y estabilidad en comparación con un sistema JTC de Fourier fraccionario en el cual se usa la LEFV. El sistema propuesto fue analizado computacional y experimentalmente, y los resultados obtenidos mostraron la viabilidad experimental de la propuesta. Cabe resaltar que para analizar el funcionamiento experimental del sistema propuesto, se realizó un proceso de calibración de la LEFV y posteriormente se llevó a cabo el proceso de encriptación. Después del análisis del funcionamiento básico del sistema, se realizó un estudio de la tolerancia a la desencriptación en función de la longitud focal inducida sobre la LEFV, estos resultados permitieron realizar un proceso de multiplexado basado en la modificación de la longitud focal de la LEFV. Los resultados experimentales demuestran que el sistema JTC en el dominio de Fourier fraccionario en combinación con el uso de una LEFV permiten establecer entornos multiusuario para la protección de información.

En el cuarto capítulo se presenta un sistema de encriptación óptica usando modulación

de fase a partir del efecto lente térmica dentro de un sistema JFSC (siglas en inglés de: joint free space cryptosystem). En este sistema el haz que ilumina el plano de entrada presenta una modificación de fase debido al efecto lente térmica (ELT). En este esquema se usa un láser de excitación que genera un gradiente de temperatura sobre una muestra, la cual posteriormente es iluminada por otro haz de prueba en el cual se observan los efectos de modulación de fase debido al ELT. Posteriormente, el haz de modulado por el ELT es usado para iluminar el plano de entrada del sistema JFSC. Para comprobar el funcionamiento básico del sistema se realiza el proceso de encriptación y recuperación de un dato. Además, debido a que la fase inducida por ELT cambia respecto a la posición de la muestra dentro del esquema óptico, se analiza la tolerancia a la desencriptación en función de la posición de la muestra. Finalmente, se presenta un protocolo de encubrimiento óptico, el cual permite reforzar la seguridad brindada por el sistema a partir del engaño y/o disuasión de los usuarios no autorizados que intenten acceder a la información sensible.

En el capítulo cinco se introduce una arquitectura de encriptación JFSC en línea. Este criptosistema no cuenta con un brazo de referencia para realizar el registro de la información de la llave, por lo tanto presenta una estructura más compacta y su implementación experimental requiere de menos elementos ópticos en comparación con los sistemas JTC convencionales. Con el objetivo de comprobar el funcionamiento básico del sistema se lleva a cabo el proceso de encriptación y recuperación de un dato. La robustez del sistema es analizada bajo la implementación de protocolos de encriptación que incluyen contenedores de información y procedimientos de multiplexado. Además, se presenta un protocolo de multiplexado selectivo basado en máscaras aleatorias binarias ortogonales que permite la implementación de un teclado óptico encriptado que posibilita la recuperación de mensajes encriptados de cualquier longitud. El sistema de encriptación desarrollado en este capítulo es compacto, tiene bajos requerimientos de alineación y estabilidad, posee menos elementos y su implementación ocupa menos espacio que los sistemas JTC convencionales.

Con el objetivo de desarrollar arquitecturas ópticas compactas y de bajo costo para el procesamiento seguro de información, en el capítulo seis se analiza un sistema holográfico que usa un dispositivo digital de microespejos (DDM) como sistema de proyección. El

desempeño del sistema es analizado a partir del registro holográfico de información en los dominios ópticos de Fourier y Fresnel. Además, se evalúa la robustez que presenta el esquema propuesto a partir del procesamiento holográfico de escenas dinámicas. El desempeño del sistema permite establecer que el DDM presenta múltiples ventajas para la proyección de imágenes binarias de amplitud, lo que evidencia que el DDM es una alternativa viable a los moduladores espaciales de luz (MEL) utilizados convencionalmente en los sistemas ópticos de encriptación. En general, hay múltiples aplicaciones donde el DDM puede sustituir el MEL como sistema de proyección, sin embargo los estudios realizados en este trabajo de investigación se centraron en el uso de DDM en sistemas holográficos, ya que este tipo de sistemas son la base del funcionamiento de los esquemas de codificación. El uso de DDM en los sistemas de codificación contribuiría al desarrollo de un dispositivo de codificación compacto, con bajos requerimientos de alineación y estabilidad, y de bajo costo.

En el capítulo siete se presenta una primera versión de un prototipo de encriptación de bajo costo basado en un sistema de codificación tipo JFSC lineal que usa un DDM como sistema de proyección, un láser de baja potencia como fuente de iluminación y una cámara web de bajo costo como medio de registro. Esta prototipo representa la primera versión de un sistema compacto y de bajo costo comparado con los sistemas disponibles actualmente. Este sistema debe ser estudiado con mayor detalle para lograr su optimización y su funcionamiento debe ser analizado en relación con todas las técnicas de procesamiento óptico presentadas en este trabajo.

El capítulo ocho contiene las conclusiones y perspectivas de este trabajo. Finalmente, se incluye un apéndice donde se presentan los productos de investigación asociados a esta tesis de Doctorado.

Bibliografía

- [1] GLOBAL ENCRYPTION SOFTWARE MARKET T. <https://bit.ly/3VmBidf> 2022.
- [2] J.B. LIMA, F. MADEIRO, F.J.R. SALES. **Signal Processing: image Communication Encryption of medical images based on the cosine number transform.** Sig. Process. Image. Commun. 2015;35:1–8.
- [3] S.K. KWOK, J.S. TING, A.H. TSANG, W.B. LEE, B.F. CHEUNG. **Design and development of a mobile EPC-RFID-based self-validation system (MESS) for product authentication.** Comput. Ind. 2010;61:624–35.
- [4] S.L. TING, A.H. TSANG. **A two-factor authentication system using radio frequency identification and watermarking technology.** Comput. Ind. 2013;64:268–79.
- [5] SCIENCE AND TECHNOLOGY IN SOCIETY (STS) FORUM KJ. <HTTP://WWW.STSFORUM.ORG/> 2017.
- [6] HORIZON 2020 UE. <HTTPS://EC.EUROPA.EU/PROGRAMMES/HORIZON2020/> 2019.
- [7] A. CARNICER, B.JAVIDI. **Optical security and authentication using nanoscale and thin-film structures.** Adv. Opt. Photonics. 2017;9:218–56.
- [8] B. JAVIDI, A. CARNICER, M. YAMAGUCHI, T. NOMURA, E. PÉREZ-CABRÉ, M.S. MILLÁN, ET AL. **Roadmap on optical security.** J. Opt. 2016;18:083001.

- [9] S.K. RAJPUT, O. MATOBA. **Optical voice encryption based on digital holography**. *Opt. Lett.* 2017;42:4619-22.
- [10] H. CHEN, Z. LIU, Q. CHEN, W. BLONDEL, P. VARIS. **Color image cryptosystem using Fresnel diffraction and phase modulation in an expanded fractional Fourier transform domain**. *Laser Phys.* 2018;28:055402.
- [11] K. LIM, K. YANG, L. HAILONG. **Holographic colour prints for enhanced optical security by combined phase and amplitude control**. *Nat. commun.* 2019;10:1–8.
- [12] G. GLUCKSTAD, F. RISO. **U.S. patent 6907124: “Optical encryption and decryption method and system”**, junio 14, 2005.
- [13] B. JAVIDI, E. TAJAHUERCE. **U.S. patent 7221760 B2: “Information security using digital holography”**, mayo 22, 2007.
- [14] B. JAVIDI, A. ESMAIL, G. ZHANG. **U.S. patent 7684098: “Optical Security system using Fourier plane encoding”**, marzo 23, 2010.
- [15] J.F. BARRERA-RAMÍREZ, A. MIRA-AGUDELO, R. TORROBA. **Patente de Invención: “Aparato óptico-físico y procedimientos para la encriptación y recuperación de información libre de ruido. Clasificación Internacional de Patentes (CIP): G06F-G06K, 2015.**
- [16] O. GRAYDON. **Cryptography Quick response codes**. *Nat. Photon.* 2013;7:343.
- [17] G. LI, W. YANG, H. WANG, G. SITU. **Image Transmission through Scattering Media Using Ptychographic Iterative Engine**. *Appl. Sci.* 2019;9:849.
- [18] R. TORROBA, J.F. BARRERA-RAMÍREZ. **Protección de datos usando un sistema experimental de encriptación de correlador de transformada conjunta**. *ACCEFYN.* 2015;39:55–60.
- [19] X. PENG, P. ZHANG, H. WEI, B. YU. **Known-plaintext attack on optical encryption based on double random phase keys**. *Opt. Lett.* 2006;31:1044-6.

- [20] J.F. BARRERA-RAMÍREZ, C. VARGAS, M. TEBALDI, R. TORROBA. **Chosen-plaintext attack on a joint transform correlator encrypting system.** *Opt. Commun.* 2010;283:3917–21.
- [21] D. PILE. **Optical encryption: The ghost holds a secret.** *Nat. Photon.* 2010;4:587.
- [22] P. REFREGIER, B. JAVIDI. **Optical image encryption based on input plane and Fourier plane random encoding.** *Opt. Lett.* 1995;20:767-97.
- [23] B. JAVIDI, T. NOMURA. **Securing information by use of digital holography.** *Opt. Lett.* 2000;25:28-30.
- [24] O. MATOBA, B. JAVIDI. **Encrypted optical storage with angular multiplexing.** *Appl. Opt.* 1999;38:7288-93.
- [25] J.F. BARRERA-RAMÍREZ, R. HENAO, M. TEBALDI R. TORROBA, N. BOLOGNINI. **Multiplexing encryption–decryption via lateral shifting of a random phase mask.** *Opt. Commun.* 2006;256:532-6.
- [26] T. NOMURA & B. JAVIDI. **Optical encryption using a joint transform correlator achitecture.** *Opt. Eng.* 2000;39:2031-6.
- [27] R. TORROBA, J.F. BARRERA-RAMÍREZ. **Protección de datos usando un sistema experimental de encriptación de correlador de transformada conjunta.** *Revista Acad. Colomb. Ci. Exact.* 2015;39:55–60.
- [28] E. RUEDA, J.F. BARRERA-RAMÍREZ, R. HENAO, R. TORROBA. **Optical encryption with a reference wave in a joint transform correlator architecture.** *Opt. Commun.* 2009;282:3243–9.
- [29] E. RUEDA, J.F. BARRERA-RAMÍREZ, R. HENAO, R. TORROBA. **Lateral shift multiplexing with a modified random mask in a joint transform correlator encrypting architecture.** *Opt. Eng.* 2009;48:27006.
- [30] J.F. BARRERA-RAMÍREZ, E. RUEDA, C. RIOS, M. TEBALDI, N. BOLOGNINI, R. TORROBA. **Experimental opto-digital synthesis of encrypted sub-samples of an image to improve its decoded quality.** *Opt. Commun.* 2011;284:4350-5.

- [31] J.M. VILARDY, M.S. MILLÁN, E. PÉREZ-CABRÉ. **Improved decryption quality and security of a joint transform correlator-based encryption system.** *J. Opt.* 2013;15:025401.
- [32] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Experimental optical encryption of grayscale information.** *Appl. Opt.* 2017;56:5883-9.
- [33] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Innovative speckle noise reduction procedure in optical encryption.** *J. Opt.* 2017;19:055704.
- [34] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Optimized random phase encryption.** *Opt. Lett.* 2018;43:3558-61.
- [35] J.F. BARRERA-RAMÍREZ, A. MIRA-AGUDELO, R. TORROBA. **Optical encryption and QR codes: secure and noise-free information retrieval.** *Opt. Express.* 2013;21:5373-8.
- [36] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Customized data container for improved performance in optical cryptosystems.** *J. Opt.* 2016;18:125702.
- [37] R. SHAHNAZ, J.F. WALKUP, T.F. KRILE. **Image compression in signal-dependent noise.** *Appl. Opt.* 1999;38:5560-7.
- [38] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, S. TREJOS, M. TEBALDI, R. TORROBA. **Optical field data compression by opto-digital means.** *J. Opt.* 2016;18:125701.
- [39] S. TREJOS, A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, M. TEBALDI, R. TORROBA. **Optical approach for the efficient data volume handling in experimentally encrypted data.** *J. Opt.* 2016;18:065702.
- [40] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Cross-talk free selective reconstruction of individual objects from multiplexed optical field data.** *Opt. Lasers Eng.* 2018;100:90-7.
- [41] S. TREJOS, A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, M. TEBALDI, R. TORROBA. **Compression of multiple 3D color scenes with experimental recording and reconstruction.** *Opt. Lasers Eng.* 2018;110:18-23.

- [42] A. VELEZ-ZEA, A. VILLAMIZAR-AMADO, M. TEBALDI, R. TORROBA. **Alternative representation for optimized phase compression in holographic data.** *OSA Contin.* 2019;2:572-81.
- [43] H. GU, G. JIN. **Phase-difference-based compression of phase-only holograms for holographic three-dimensional display.** *Opt. Express.* 2018;26:33592-603.
- [44] G. SITU, J. ZHANG. **Multiple-image encryption by wavelength multiplexing.** *Opt. Lett.* 2005;30:1306-8.
- [45] D. AMAYA, M. TEBALDI, R. TORROBA, N. BOLOGNINI. **Wavelength multiplexing encryption using joint transform correlator architecture.** *Appl. Opt.* 2009;48:2099-104.
- [46] J.F. BARRERA-RAMÍREZ, R. HENAO, M. TEBALDI, N. BOLOGNINI, R. TORROBA. **Multiplexing encrypted data by using polarized light.** *Opt. Commun.* 2006;260:109-12.
- [47] E. RUEDA, C. RIOS, J.F. BARRERA-RAMÍREZ, R. HENAO, R. TORROBA. **Experimental multiplexing approach via key code rotations under a joint transform correlator scheme.** *Opt. Commun.* 2011;284:2500-4.
- [48] E. RUEDA, J.F. BARRERA-RAMÍREZ, R. HENAO, R. TORROBA. **Lateral shift multiplexing with a modified random mask in a joint transform correlator encrypting architecture.** *Opt. Eng.* 2009;48:27006.
- [49] J.A. JARAMILLO-OSORIO, J.F. BARRERA-RAMÍREZ, A. VELEZ-ZEA, R. TORROBA. **Fractional optical cryptographic protocol for data containers in a noise-free multiuser environment.** *Opt. Lasers Eng.* 2018;102:119-25.
- [50] F. MOSSO, M. TEBALDI, J.F. BARRERA-RAMÍREZ, N. BOLOGNINI, R. TORROBA. **Pure optical dynamical color encryption.** *Opt. Express.* 2011;19:13779-86.
- [51] E. RUEDA, J.F. BARRERA-RAMÍREZ, R. HENAO, R. TORROBA. **Optical encryption with a reference wave in a joint transform correlator architecture.** *Opt. Commun.* 2009;282:3243-9.

- [52] N. SAINI, A. SINHA. **Video encryption using chaotic masks in joint transform correlator.** J. Opt. 2015;17:035701.
- [53] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Cross-talk free selective reconstruction of individual objects from multiplexed optical field data.** Opt. Lasers Eng. 2018;100:90-7.
- [54] S. TREJOS, A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, M. TEBALDI, R. TORROBA. **Compression of multiple 3D color scenes with experimental recording and reconstruction.** Opt. Lasers Eng. 2018;110:18-23.
- [55] A. VELEZ-ZEA, A. VILLAMIZAR-AMADO, M. TEBALDI, R. TORROBA. **Alternative representation for optimized phase compression in holographic data.** OSA Contin. 2019;2:572-81.
- [56] H. GU, G. JIN. **Phase-difference-based compression of phase-only holograms for holographic three-dimensional display.** Opt. Express. 2018;26:33592-603.

Capítulo 2

Sistemas ópticos de encriptación

Los sistemas de encriptación se encargan de transformar o modificar la información, convirtiéndola en un patrón ininteligible que impide que usuarios no autorizados puedan acceder a ella. El elemento clave encargado de modificar la información y darle seguridad al sistema se conoce como llave de seguridad, de modo que solo quienes conozcan la llave puedan acceder a la información original contenida en el dato codificado. Por otro lado, el procedimiento que permite acceder al dato recuperado se conoce como desencriptación.

Cuando el proceso de encriptación se lleva a cabo por medio de un sistema óptico, la información puede ser codificada utilizando llaves físicas o digitales. En particular, los esquemas de codificación óptica que emplean llaves físicas son los más seguros, ya que en estos se emplean como llaves de codificación difusores (experimentalmente vidrios rugosos) a los cuales no se les puede considerar como elementos que tienen un arreglo regular de píxeles con tamaño fijo que producen un cambio de fase bien definido. Adicionalmente, en los esquemas de codificación óptica es posible usar uno o varios de los grados de libertad del sistema óptico para generar llave(s) de seguridad adicional(es). En el caso de los sistemas que usan llave física, la combinación de ésta con los grados de libertad del sistema óptico permite incrementar la seguridad de los protocolos de codificación y ocultar información de

forma segura. El alto desempeño que han mostrado los sistemas de codificación óptica para el procesamiento seguro de información en conjunto con sus inherente capacidad de procesamiento en paralelo han demostrado su gran potencialidad, versatilidad y aplicabilidad en desarrollos experimentales, incluso se han generado algunas patentes [1–6].

En particular, la técnica de encriptación óptica que utiliza dos máscaras aleatorias de fase DRPE (siglas en inglés de: double random phase encoding) ha sido la técnica más implementada. Dentro de los sistemas más estudiados y desarrollados que emplean la técnica DRPE se encuentran el sistema 4f y el sistema JTC (siglas en inglés de: joint transform correlator). En esta sección se describe el sistema de encriptación 4f y, posteriormente, se presenta la descripción teórica y experimental del sistema de encriptación JTC.

2.1. Sistema óptico de encriptación basado en una arquitectura 4f

El sistema de encriptación 4f, desarrollado por P. Refregier *et. al* en 1995, emplea un esquema de DRPE en un arreglo 4f [7]. Para llevar a cabo el proceso de cifrado, en el plano de entrada del sistema, el dato a encriptar es multiplicado por una máscara aleatoria de fase (MAF). Posteriormente, una lente positiva realiza la transformada de Fourier (TF) del producto entre el objeto a encriptar y la MAF. Luego, la TF de este producto es multiplicado por otra MAF ubicada en el plano de Fourier de la lente, esta última MAF actúa como llave de seguridad. Seguidamente, una segunda lente realiza la TF de la función resultante de este último producto. Finalmente, en el plano de Fourier de la segunda lente se obtiene el dato encriptado (ver Fig. 2.1).

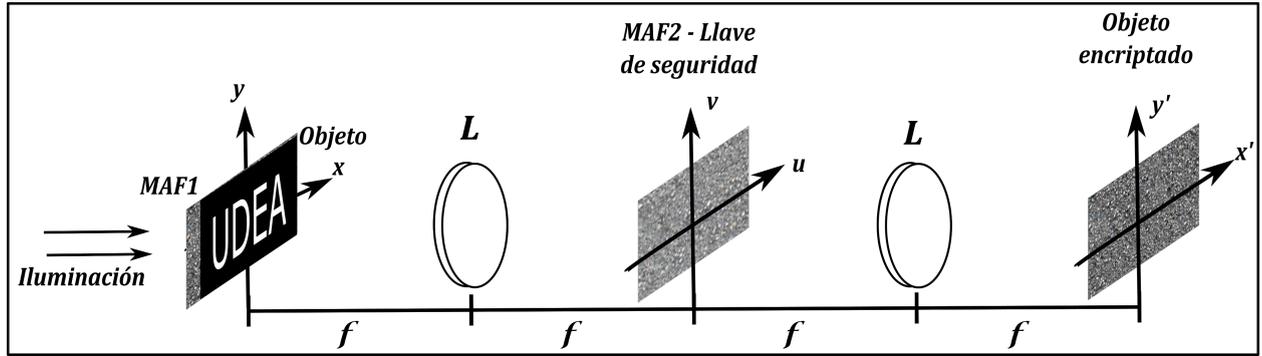


Figura 2.1: Esquema de un sistema de encriptación 4f. L: lente, f : longitud focal de las lentes, MAF: máscara aleatoria de fase.

De acuerdo con la configuración mostrada en la Fig.2.1, si consideramos que $f(x, y)$ es el objeto a encriptar y $m(x, y)$ es la MAF1, el plano de entrada del sistema es,

$$U_0(x, y) = f(x, y)m(x, y) \quad (2.1)$$

al iluminar el sistema con una onda plana, como se observa en la Fig. 2.1, la primera lente realiza la transformada de Fourier de la información presente en el plano de entrada (Ec. 2.1), esta distribución viene dada por,

$$U_1(u, v) = F(u, v) \otimes M(u, v) \quad (2.2)$$

$F(u, v)$ y $M(u, v)$ son las transformadas de Fourier de $f(x, y)$ y $m(x, y)$ respectivamente, y \otimes es el operador convolución. Después, en el plano de Fourier de la primera lente, la información es multiplicada por la MAF2 o llave de seguridad. Finalmente, la segunda lente realiza la transformada de Fourier de este último producto y en el plano de salida, ubicado a una distancia 4f del plano de entrada, se obtiene el dato encriptado,

$$e(x, y) = f(-x, -y)m(-x, -y) \otimes B(x, y) \quad (2.3)$$

donde $B(x, y)$ es la transformada de Fourier de la llave de seguridad. El objeto encriptado contiene información tanto de amplitud como de fase (Ec. 2.3), por lo cual para llevar a cabo el proceso de recuperación es necesario emplear algún método que permita registrar la información de amplitud y fase.

En la primera implementación experimental de este sistema, la información del dato encriptado se registró usando un sistema interferométrico fuera de eje y una película holográfica como medio de registro [8]. Esta implementación requiere de tres brazos de iluminación. En el primer brazo se ubica el sistema $4f$ con la información a encriptar Fig. 2.1, el segundo brazo contiene un haz de referencia utilizado para el registro holográfico del dato encriptado. Mientras que el tercer brazo es utilizado para llevar a cabo el proceso de recuperación. En este último brazo se ubica el dato encriptado en el plano de entrada de otro sistema $4f$, y en el plano de Fourier de la primera lente el complejo conjugado de la llave Fig. 2.2. Se debe mencionar que, generar el complejo conjugado de la llave de seguridad es un proceso técnicamente complicado, ya que en los esquemas experimentales la llaves más seguras son vidrios difusores [9].

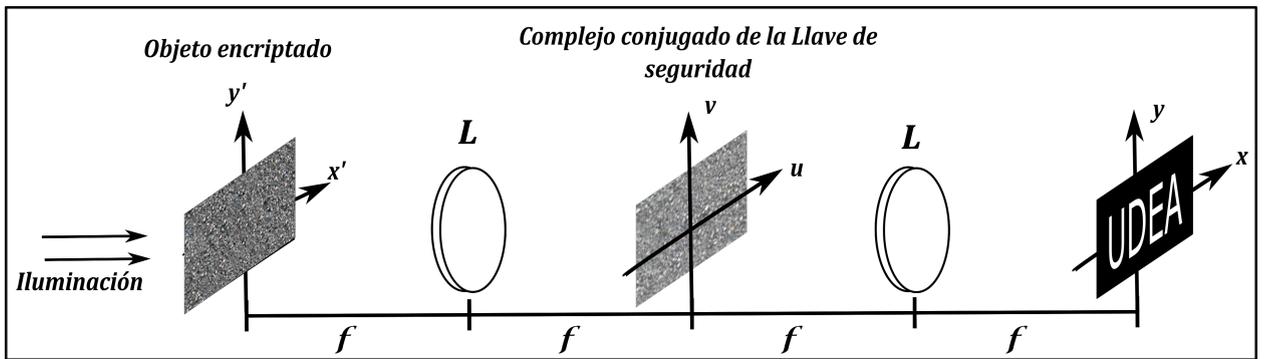


Figura 2.2: Esquema de recuperación en un sistema de encriptación $4f$ usando el complejo conjugado de la llave. L: lente, f : longitud focal de las lentes.

Una segunda implementación, cuya arquitectura está basada en un interferómetro de

Mach-Zehnder, permite llevar a cabo el proceso de encriptación usando holografía digital. En uno de los brazos de iluminación del interferómetro se ubica el sistema 4f con la información a encriptar (brazo objeto), mientras que el otro brazo del sistema contiene una onda de referencia [10]. El dato encriptado se obtiene a partir del holograma resultante de la interferencia entre la luz proveniente del brazo objeto y la onda de referencia. Para el registro de la llave, se debe desmontar el sistema 4f ubicado en el brazo objeto y registrar el holograma de la máscara utilizada como llave de encriptación. Para el correcto funcionamiento de este sistema se usa una MAF con una correlación de $10\mu m$ en el plano de entrada, y se utiliza una lente en lugar de una MAF como llave de seguridad. Estas restricciones se deben a la falta de ancho de banda del medio de registro empleado y las características del sistema óptico [10]. En este caso, el proceso de recuperación de la información se realiza de forma digital.

También es posible implementar la arquitectura de encriptación 4f usando cristales fotorrefractivos [11–18]. Aunque en este caso, la implementación también se realiza por medio de un interferómetro de Mach-Zehnder, se utiliza un cristal fotorrefractivo en lugar de una cámara digital para registrar la información. Sobre el cristal incide el patrón correspondiente a la interferencia entre la onda plana de referencia y el haz del dato encriptado, proveniente del sistema 4f. Esta distribución de intensidad genera un campo de cargas espaciales en el cristal debido a la redistribución de portadores. El campo espacial de cargas resultante produce una perturbación del índice refractivo, el cual replica y almacena la información encriptada. Por lo tanto, la información encriptada es registrada holográficamente como variaciones del índice de refracción dentro del cristal. Para llevar a cabo el proceso de recuperación, en lugar de introducir el complejo conjugado de la llave de seguridad (Fig. 2.2), se genera experimentalmente el complejo conjugado del objeto encriptado [11–18]. De esta forma, durante la desencriptación se compensan los cambios aleatorios que la llave de seguridad introdujo durante la encriptación para lograr la recuperación de la información original (Fig. 2.3).

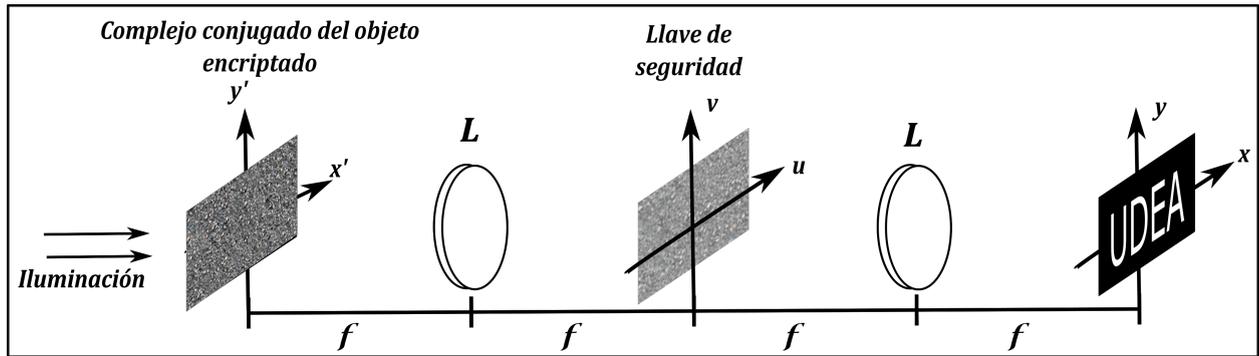


Figura 2.3: Esquema de recuperación en un sistema de encriptación $4f$ cuando el registro del dato encriptado se hace a partir de cristales fotorrefractivos. L: lente, f : longitud focal de las lentes

Esta implementación presenta algunas ventajas, entre ellas que la llave encriptación y la de recuperación son la misma, y que el proceso de encriptación y desencriptación son llevados a cabo en tiempo real. A pesar de estas ventajas, su implementación experimental tiene requerimientos de alineación y estabilidad elevados debido principalmente a la generación del complejo conjugado del objeto encriptado [11–18].

En general, la implementación experimental de la arquitectura de codificación $4f$ requiere de un sistema interferométrico para el registro de la información que contiene el dato encriptado y la llave de seguridad [10, 12, 17]. Por lo tanto, para garantizar el correcto desempeño del sistema $4f$, se hace necesario el uso de dos brazos de iluminación, uno que contiene el sistema de encriptación y el otro que brinda una onda de referencia. Por esta razón, no solo se tienen altas exigencias en alineación y estabilidad, sino que además se debe disponer de un área de trabajo que permita implementar el sistema interferométrico y todos los elementos ópticos asociados. Estos requerimientos pueden limitar su potencial aplicación en desarrollos de carácter investigativo y/o práctico [8, 10].

Con el propósito de desarrollar una arquitectura con menos exigencias experimentales que la arquitectura $4f$, se propuso la arquitectura de encriptación óptica basada en el correlador transformada conjunta JTC (siglas en inglés de: joint transform correlator) [19, 20], sistema mucho más compacto, versátil y con requerimientos de alineación y estabilidad menores a

los exigidos por el sistema 4f [21, 22].

El sistema JTC se ha estudiado y desarrollado en mayor medida pues es más propicio para usos experimentales y presenta mayor potencial para aplicaciones prácticas y un alto desempeño para el procesamiento seguro de información. Este sistema presenta una arquitectura que es inherentemente holográfica, por lo cual no es necesario el uso de sistemas interferométricos fuera de eje (brazo de referencia) para el registro del dato encriptado. Por otro lado, solo se necesita una lente transformadora para llevar a cabo el proceso de encriptación y en el proceso de recuperación no se requiere el complejo conjugado de la llave de seguridad.

2.2. Sistema de encriptación JTC en el dominio de Fourier

El correlador de transformada conjunta JTC, fue desarrollado por Weaver y Goodman con el objetivo de llevar a cabo ópticamente el proceso de convolución entre un par de funciones [23]. Posteriormente, Nomura y Javidi aprovecharon las ventajas experimentales presentes en esta arquitectura óptica y la emplearon para realizar el proceso de convolución entre el producto de un objeto multiplicado por una máscara aleatoria de fase (MAF) con otra MAF que actúa como llave de seguridad [19]. La convolución óptica entre este par de funciones produce un patrón aleatorio que contiene la información del dato encriptado. Este último dato a su vez contiene la información original, a la cual solo se podrá acceder si se conoce la información de la llave de seguridad.

El sistema JTC se caracteriza por tener una arquitectura compacta, con bajos requerimientos de alineación y estabilidad que posibilita una implementación experimental mucho más versátil en comparación con otros sistemas ópticos de encriptación. Además de esto, el dato encriptado se obtiene a partir de la intensidad de la transformada de Fourier conjunta

del objeto y la llave, información que pueden ser registrada con una cámara digital. Como se explicará en este capítulo, el registro digital permite la implementación de técnicas de procesamiento optico-digitales para la eliminación de información no relevante [24].

En este capítulo se presentará el modelo teórico y la implementación experimental que describen el funcionamiento del sistema de encriptación JTC. Las descripciones presentadas en este capítulo servirán de base para la explicación de las arquitecturas empleadas y desarrolladas como resultado de la investigación realizada en este trabajo.

2.3. Descripción del sistema de encriptación JTC en el dominio de Fourier

En el criptosistema JTC, la ventana objeto y la ventana llave se ubican en el plano de entrada del sistema con una separación determinada, ambas funciones se ponen en contacto con máscaras aleatorias de fase. La ventana objeto tiene la información del dato a encriptar y la ventana llave en contacto con el difusor genera la llave de seguridad. Una lente es ubicada entre el plano de entrada y el plano de salida, de tal modo que ambos planos queden ubicados en los puntos focales de dicha lente (Fig. 2.4). En este sistema, a diferencia del $4f$, solo se requiere de una lente transformadora para llevar a cabo el proceso de encriptación. Además, para el registro del dato encriptado no se requiere de un brazo de referencia, ya que la configuración del plano de entrada hace que el sistema sea inherentemente holográfico, debido a esto la implementación del sistema JTC requiere de menos elementos y presenta menores requerimientos de estabilidad y alineación comparada con el $4f$. Teniendo presente la configuración del sistema JTC, en el plano de salida se registra la intensidad de la transformada de Fourier conjunta o JPS (siglas en inglés de: joint power spectrum) de las funciones presentes en el plano de entrada [25]. El JPS contiene el dato encriptado y para su extracción se debe realizar un proceso de filtrado.

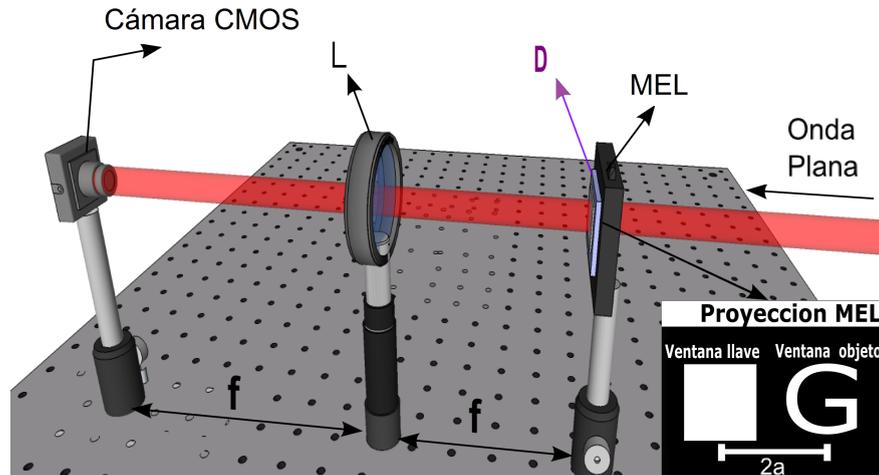


Figura 2.4: Esquema de un sistema de encriptación JTC. L: lente, f : longitud focal de la lente, D: difusor, MEL: modulador espacial de luz y $2a$: separación entre las ventanas objeto y llave.

2.4. Registro y filtrado del dato encriptado

2.4.1. Registro del dato encriptado

Para realizar el proceso de encriptación en el sistema JTC, se proyectan en un modulador espacial de luz (MEL) la ventana objeto, la cual contiene la información que se desea encriptar, y la ventana llave. Luego, el MEL se pone en contacto con un vidrio difusor que cubre la información proyectada para generar una máscara aleatoria de fase sobre la ventana objeto y la ventana llave (Fig. 2.4). El área del difusor en contacto con la ventana llave determina la información de la llave de encriptación $l(x, y)$.

Considerando $f(x, y) = o(x, y)r(x, y)$ con $o(x, y)$ el objeto a encriptar y $r(x, y)$ la máscara aleatoria correspondiente al área del difusor que está en contacto con el objeto, la función transmitancia en el plano de entrada del criptosistema JTC se puede escribir como,

$$u(x, y) = f(x, y) \otimes \delta(x - a, y) + l(x, y) \otimes \delta(x + a, y) \quad (2.4)$$

\otimes es el operador convolución y $\delta()$ es la función delta de Dirac. $x = a$ y $x = -a$ son las coordenadas de posicionamiento de la ventana objeto y la ventana llave en el plano de entrada, respectivamente. En el plano de salida se registra el JPS de la información presente en el plano de entrada (Ec. 2.4) [25], dada por

$$I_{JPS}(\nu, \omega) = |F(\nu, \omega)|^2 + |L(\nu, \omega)|^2 + F(\nu, \omega)L^*(\nu, \omega)e^{-4\pi i a \nu} + F^*(\nu, \omega)L(\nu, \omega)e^{4\pi i a \nu} \quad (2.5)$$

$F(\nu, \omega)$ y $L(\nu, \omega)$ son las transformadas de Fourier de $f(x, y)$ y $l(x, y)$ respectivamente, (ν, ω) son las coordenadas en el dominio de Fourier y $*$ representa el complejo conjugado.

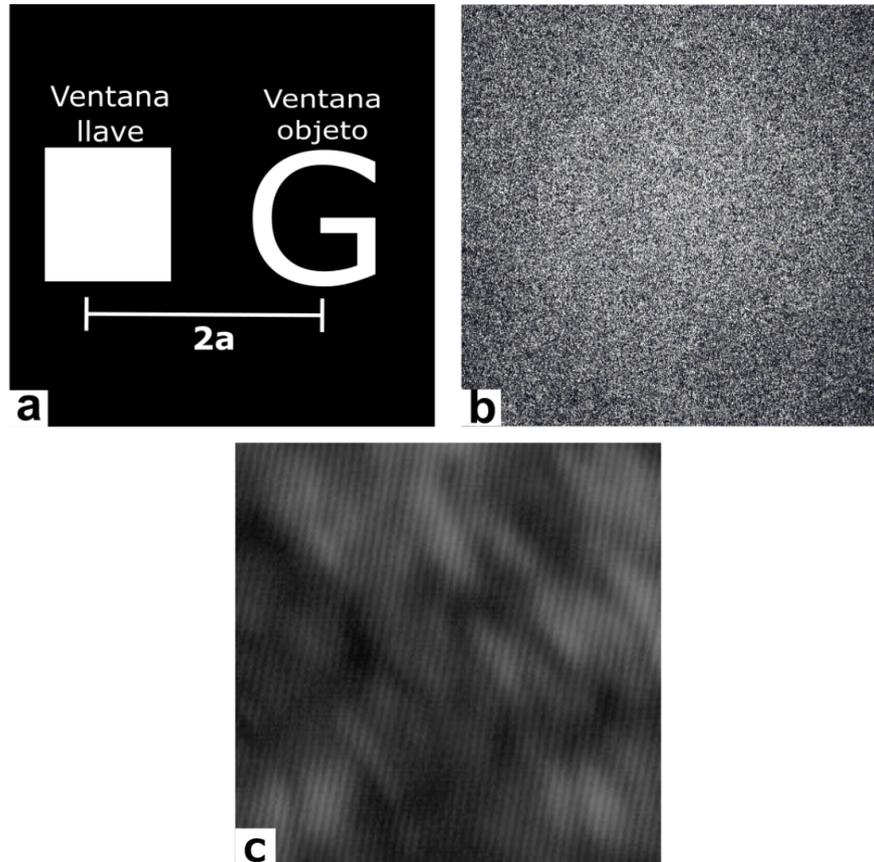


Figura 2.5: Plano de entrada y espectro conjunto de potencias. a) Intensidad del plano de entrada (proyección en el MEL), b) espectro conjunto de potencias (JPS) experimental de a) y c) ampliación de un sector de b)

2.4.2. Filtrado del dato encriptado

El JPS (Ec. 2.5) no sólo contienen la información relacionado con el dato encriptado, sino también información redundante, como las auto-correlaciones de las ventanas objeto y llave correspondientes al primer y segundo término en la Ec. 2.5 (Fig. 2.6(a)), y el complejo conjugado del dato encriptado correspondiente al cuarto término en la Ec. 2.5. Con el objetivo de obtener únicamente la información correspondiente al dato encriptado (tercer término en la Ec. 2.5), se realiza un proceso de filtrado que permite descartar la información redundante.

Para llevar a cabo este proceso de filtrado, se proyectan individualmente la ventana objeto

y la ventana llave. De esta manera se registra y almacena los términos $|F(\nu, \omega)|^2$ y $|L(\nu, \omega)|^2$ correspondientes a las autocorrelaciones del objeto y la llave respectivamente. Posteriormente, ambas distribuciones ($|F(\nu, \omega)|^2$ y $|L(\nu, \omega)|^2$) se restan del JPS (Ec. 2.5),

$$I'_{JPS}(\nu, \omega) = F(\nu, \omega)L^*(\nu, \omega)e^{-4\pi i a \nu} + F^*(\nu, \omega)L(\nu, \omega)e^{4\pi i a \nu} \quad (2.6)$$

Para finalizar el proceso de filtrado, se realiza una TF sobre la Ec. 2.6,

$$i(x, y) = f(x, y) \otimes l^*(x, y) \otimes \delta(x - 2a, y) + f^*(x, y) \otimes l(x, y) \otimes \delta(x + 2a, y) \quad (2.7)$$

debido a las funciones exponenciales presentes en la Ec. 2.6, después de realizar la TF se genera una separación espacial entre los términos, dada por las funciones delta; que se ven en la Ec. 2.7 y gráficamente en la Fig. 2.6b.

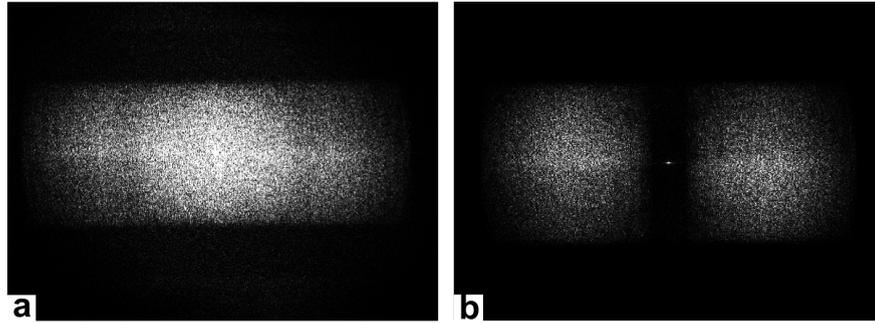


Figura 2.6: **Transformada de Fourier del espectro conjunto de potencias.** a) TF del JPS sin restar los términos de intensidad $|F(\nu, \omega)|^2$ y $|L(\nu, \omega)|^2$, y b) TF del JPS después de restar los términos de intensidad $|F(\nu, \omega)|^2$ y $|L(\nu, \omega)|^2$.

La separación entre los términos, en la Ec. 2.7, permite descartar el segundo término (Fig. 2.7a). Luego, seleccionando y reposicionando el primer término en las coordenadas (x', y') , se obtiene,

$$i'(x, y) = f(x, y) \otimes l^*(x, y) \otimes \delta(x - x', y - y') \quad (2.8)$$

finalmente realizando una transformada de Fourier inversa (TFI) a la Ec.2.8, se obtiene el dato encriptado (Fig. 2.7b).

$$E(\nu, \omega) = F(\nu, \omega)L^*(\nu, \omega)e^{2\pi i(x'\nu + y'\omega)} \quad (2.9)$$

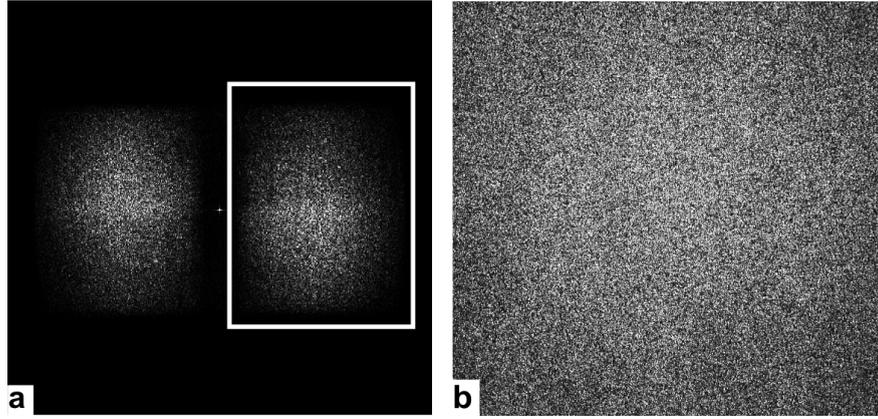


Figura 2.7: Proceso de filtrado y reposicionado. a) Selección del dato encriptado y b) dato encriptado y reposicionado.

Como se mostrará posteriormente en este trabajo, el reposicionamiento espacial del dato encriptado, en el último paso del proceso de filtrado, permite el desarrollo de métodos de multiplexado que facilitan el almacenamiento y desencriptado de múltiples datos evitando problemas de superposición en la recuperación.

Se debe tener en cuenta que este procedimiento de filtrado se utilizará para la obtención del dato encriptado en todos los sistemas empleados y desarrollados como producto de las investigaciones realizadas en esta tesis doctoral.

2.5. Registro y filtrado de la llave de encriptación

El dato encriptado (Ec. 2.9) contiene el producto entre la TF de la información del objeto multiplicado por una máscara aleatoria, y el complejo conjugado de la TF de la llave de seguridad. Debido a esto, si se realiza una TFI del dato encriptado (Ec. 2.9), buscando recuperar la información original que contiene el dato encriptado, se obtiene un patrón aleatorio debido a la convolución entre dos patrones aleatorios, y por ende la información permanece encriptada. De acuerdo con lo anterior, no se podrá acceder al dato recuperado sin la información de la llave de seguridad. Por consiguiente, para recuperar el objeto original es necesario multiplicar el dato encriptado ($E(\nu, \omega)$) por la información de la TF de la llave ($L(\nu, \omega)$) y después realizar una TFI.

2.5.1. Registro del holograma de la TF de la llave

Para obtener la información del campo óptico $L(\nu, \omega)$, se registra el patrón de interferencia entre una onda plana de referencia y la TF de la llave [21]. Para esto, se implementa experimentalmente el sistema interferométrico que se muestra en la Fig. 2.8.

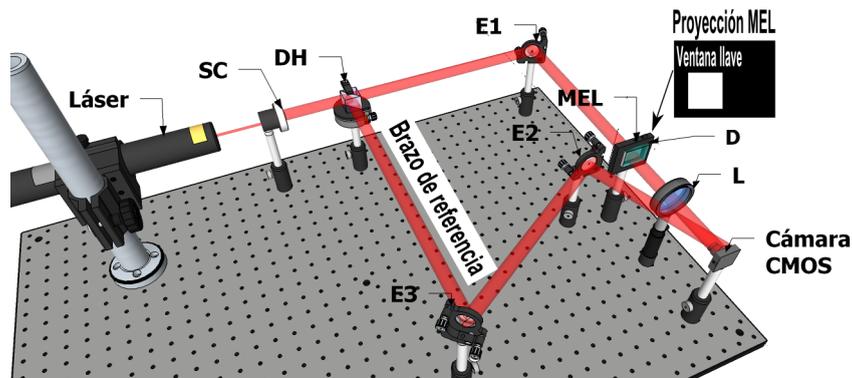


Figura 2.8: **Esquema experimental para el almacenamiento del holograma de la TF de la llave.** L: lente, D: difusor, SC: sistema de colimación, DH: divisor de haz, E: espejo, MEL: modulador espacial de luz y $2a$: separación entre las ventanas objeto y llave.

Este sistema holográfico (Fig. 2.8) cuenta con un sistema colimador (SC) que permite

generar una onda plana a partir de un haz láser. El SC está compuesto de un filtro espacial, el cual emplea un objetivo de microscopio y un pinhole (pupila pequeña) que permiten expandir y filtrar el haz emitido por la fuente láser. Después de generar la onda plana a partir del SC, ésta es dividida en dos haces de iluminación por medio de un divisor de haz (DH).

Uno de los brazos del sistema permite realizar la TF de la llave de seguridad, mientras que por el otro viaja una onda plana de referencia. Para hacer el registro holográfico de la llave, en el MEL se proyecta solo la ventana llave, que en contacto con un difusor genera la llave de seguridad. El espejo E2 (Fig. 2.8), permite combinar en el plano de la cámara la onda plana del brazo de referencia y la TF de la llave, de esta forma se registra el patrón de interferencia entre la TF de la llave y la onda plana.

Considerando $P(\nu, \omega) = e^{2\pi i \lambda (\alpha \nu + \beta \omega)}$ como la onda plana de amplitud unitaria proveniente del brazo de referencia y $L(\nu, \omega)$ como la transformada de Fourier de la ventana llave, la distribución de intensidad en el plano de la cámara viene dada por,

$$\begin{aligned}
 H(\nu, \omega) &= |P(\nu, \omega)|^2 + |L(\nu, \omega)|^2 + L^*(\nu, \omega) e^{2\pi i \lambda (\alpha \nu + \beta \omega)} \\
 &+ L(\nu, \omega) e^{-2\pi i \lambda (\alpha \nu + \beta \omega)}
 \end{aligned}
 \tag{2.10}$$

donde λ es la longitud de onda de la fuente de iluminación, y α y β son los ángulos de incidencia de la onda plana sobre la cámara [25, 26]. Estos ángulos se pueden modificar experimentalmente por medio de los espejos E2 y E3 del brazo de referencia.

2.5.2. Filtrado de la llave de encriptación

Como se observa en la Ec. 2.10, el holograma de la llave contiene información redundante que debe ser filtrada para poder llevar a cabo el proceso de recuperación. En este caso, la información redundante corresponde a los primeros tres términos presentes en la Ec. 2.10.

Realizando un proceso similar al que se llevó a cabo para la extracción del dato encriptado, es posible obtener la información de la llave presente en Ec. 2.10. En este caso, se registra y almacena $|P(\nu, \omega)|^2$ bloqueando el brazo objeto, mientras que para el registro y almacenamiento de $|L(\nu, \omega)|^2$ se bloquea el brazo de referencia. Posteriormente, estas dos distribuciones se restan a la Ec. 2.10,

$$H'(\nu, \omega) = L(\nu, \omega)e^{-2\pi i\lambda(\alpha\nu+\beta\omega)} + L^*(\nu, \omega)e^{2\pi i\lambda(\alpha\nu+\beta\omega)} \quad (2.11)$$

Ahora, realizando una TF de la Ec. 2.11 es posible obtener una separación espacial entre los términos (este proceso genera un resultado similar al mostrado en la Fig. 2.6b y Fig. 2.7). Dicha separación permite extraer el término que contiene la información de la llave. Finalmente, realizando un TFI sobre el término aislado, se obtiene la llave de encriptación posicionada en las coordenadas (x'', y'') , la cual corresponde al primer término de la Ec. 2.11,

$$K(\nu, \omega) = L(\nu, \omega)e^{2\pi i(x''\nu+y''\omega)} \quad (2.12)$$

2.6. Descriptación

Para llevar a cabo el proceso de descriptación, se debe multiplicar el dato encriptado (Ec. 2.9) por la información de la llave (Ec. 2.10). Por simplicidad, en este caso se realiza el reposicionado del dato encriptado y la llave en el origen de coordenadas. Por lo tanto, $x' = 0$ y $y' = 0$, y $x'' = 0$ y $y'' = 0$, obteniendo

$$E'(\nu, \omega) = F(\nu, \omega)L^*(\nu, \omega)L(\nu, \omega) \quad (2.13)$$

Ahora, considerando a $L(\nu, \omega)$ como una función de fase pura, se tiene que $L^*(\nu, \omega)L(\nu, \omega) \approx 1$ [11], y realizando un TFI de la Ec. 2.13, se obtiene el dato recuperado.

$$D(x, y) = f(x, y) = o(x, y)r(x, y) \quad (2.14)$$

El modulo cuadrado Ec. 2.14, permite obtener el dato recuperado (Fig. 2.9(d)). Se debe tener en cuenta que, experimentalmente el dato recuperado contiene ruido aleatorio de correlación debido a la auto-correlación de $l(x, y)$ [27], ya que experimentalmente la llave es una función tanto de amplitud como de fase. La degradación de la imagen debido al ruido puede ser reducida a partir de técnicas de reducción de ruido que serán tratadas más adelante en este trabajo.

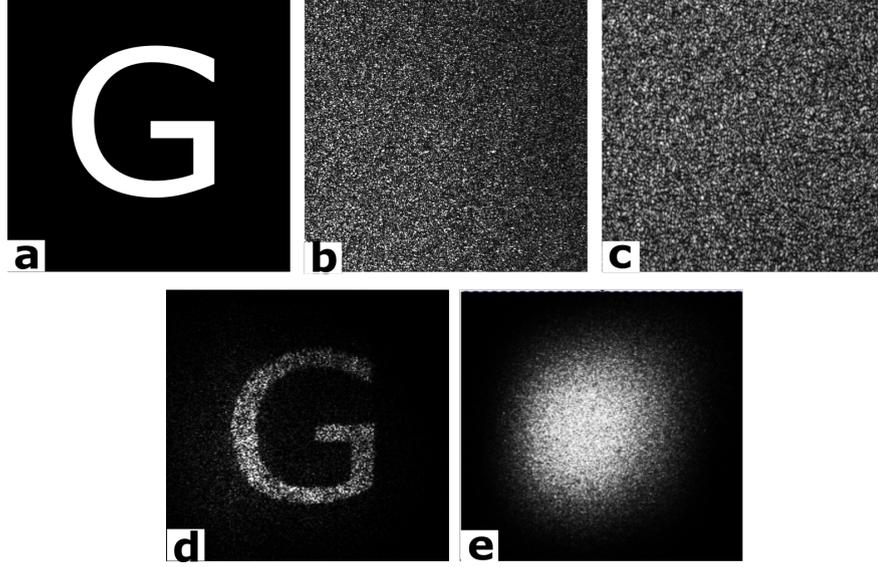


Figura 2.9: Resultados experimentales de la encriptación y la desencriptación. a) Dato original, b) dato encriptado, c) información de la TF de la llave de seguridad, d) dato desencriptado usando la llave correcta $L(\nu, \omega)$ y e) dato desencriptado usando una llave incorrecta $L_w(\nu, \omega)$.

Por otro lado, cuando se trata de recuperar la información encriptada empleando una llave incorrecta $L_w(\nu, \omega)$, el producto $L^*(\nu, \omega)L_w(\nu, \omega)$ será un patrón aleatorio y al realizar la TFI para recuperar la información se obtendría,

$$e_w(x, y) = f(x, y) \otimes l^*(x, y) \otimes l_w(x, y) \quad (2.15)$$

en la Ec. 2.15, la correlación entre las dos funciones aleatorias $l^*(x, y) \otimes l_w(x, y)$ imposibilita la recuperación de la información original (Fig. 2.9e), mantenido el objeto oculto y de esta forma corroborando la seguridad del sistema.

Para obtener los resultados experimentales mostrados en la Fig. 2.9, se empleó un láser de Helio-Neón con una potencia de 20 mW y una longitud de onda $\lambda = 632 \text{ nm}$. La longitud focal de la lente fue de $f = 200 \text{ mm}$. Para generar las máscaras aleatorias de fase en el plano de entrada se usó un vidrio esmerilado o difusor. La ventana objeto y llave fueron

proyectadas en un modulador espacial de luz HOLOEYE 2002 con un tamaño de pixel de $32 \mu m \times 32 \mu m$ y una resolución de 800×600 píxeles. Los tamaños de la ventana objeto y llave fueron de $9,6 mm \times 9,6 mm$ y $3,2 mm \times 3,2 mm$, respectivamente. La separación entre ambas ventanas en el plano de entrada fue de $2a = 4,8 mm$. Para el registro de la información se usó una cámara CMOS EO-10012M con una resolución de 3840×2748 píxeles y un tamaño de pixel de $1,67 \mu m \times 1,67 \mu m$.

Los procesos de registro y filtrado del dato encriptado, de la llave de encriptación y el procedimiento de recuperación, presentados en esta sección, serán implementados en los demás capítulos de este trabajo.

Bibliografía

- [1] B. JAVIDI. **Method and Apparatus for Encryption Using Partial Information.** (Febrero, 2003) U.S. Patent 6519340 B1.
- [2] G. GLUCKSTAD, F. RISO. **Optical encryption and decryption method and system.** (Junio 14, 2005) U.S. patent 6907124.
- [3] B. JAVIDI, E. TAJAHUERCE. **Information security using digital holography.** (Mayo 22, 2007) U.S. patent 7221760 B2.
- [4] B. JAVIDI, A. ESMAIL, G. ZHANG. **Optical Security system using Fourier plane encoding.** (Marzo 23, 2010) U.S. patent 7684098.
- [5] J.F. BARRERA-RAMÍREZ, A. MIRA-AGUDELO, R TORROBA. **Aparato óptico-físico y procedimientos para la encriptación y recuperación de información libre de ruido.** (Diciembre 18, 2015a) Patente de invención 14 98035.
- [6] W.C WANG, D. R. SCHIPF. **Fluid-optical encryption system and method thereof.**(Junio 13, 2019) US patent 0182407 A1.
- [7] P. REFREGIER, B. JAVIDI. **Optical image encryption based on input plane and Fourier plane random encoding.** Opt. Lett. 1995;20:767-97.
- [8] B. JAVIDI, G. ZHANG, J. LI. **Experimental demonstration of the random phase encoding technique for image encryption and security verification.** Opt. Eng. 1996;35:2506-12.

- [9] O. MATOBA, T. NOMURA, E. PEREZ-CABRE, M.S. MILLAN, B. JAVIDI **Optical techniques for information security**. Proceedings of the IEEE. 2009;97:1128-48.
- [10] B. JAVIDI, T. NOMURA. **Securing information by use of digital holography**. Opt. Lett. 2000;25:28-30.
- [11] G. UNNIKRISHNAN, J. JOSEPH, K. SINGH. **Optical encryption system that uses phase conjugation in a photorefractive crystal**. Appl. Opt. 1998; 37:8181-6.
- [12] O. MATOBA, B. JAVIDI. **Encrypted optical storage with angular multiplexing**. Appl. Opt. 1999; 38:7288-93.
- [13] G. UNNIKRISHNAN, J. JOSEPH, K. SINGH. **Optical encryption by double-random phase encoding in the fractional Fourier domain**. Opt. Lett. 2000;25:887-9.
- [14] N. NISHCHAL, J. JOSEPH, K. SINGH. **Fully phase encryption using fractional Fourier transform**. Opt. Eng. 2003;42:1583-8.
- [15] J.F. BARRERA-RAMÍREZ, R. HENAO, M. TEBALDI, R TORROBA, N. BOLOGNINI. **Multiplexing encrypted data by using polarized light**. Opt. Commun.2006;260:109-12.
- [16] J.F. BARRERA-RAMÍREZ, R. HENAO, M. TEBALDI, R TORROBA, N. BOLOGNINI. **Multiple image encryption using an aperture-modulated optical system**. Opt. Commun. 2006;261:29-33.
- [17] J.F. BARRERA-RAMÍREZ, R. HENAO, M. TEBALDI R. TORROBA, N. BOLOGNINI. **Multiplexing encryption–decryption via lateral shifting of a random phase mask**. Opt. Commun. 2006;256:532-6.
- [18] J.F. BARRERA-RAMÍREZ, R. HENAO, M. TEBALDI, R TORROBA, N. BOLOGNINI. **Code retrieval via undercover multiplexing**. Optik. 2008;119:139-42.
- [19] T. NOMURA & B. JAVIDI. **Optical encryption using a joint transform correlator achitecture**. Opt. Eng. 2000;39:2031-6.

- [20] R. TORROBA, J.F. BARRERA-RAMÍREZ. **Protección de datos usando un sistema experimental de encriptación de correlador de transformada conjunta.** Revista Acad. Colomb. Ci. Exact. 2015;39:55–60.
- [21] E. RUEDA, J.F. BARRERA-RAMÍREZ, R. HENAO, R. TORROBA. **Optical encryption with a reference wave in a joint transform correlator architecture.** Opt. Commun. 2009;282:3243–9.
- [22] E. RUEDA, J.F. BARRERA-RAMÍREZ, R. HENAO, R. TORROBA. **Lateral shift multiplexing with a modified random mask in a joint transform correlator encrypting architecture.** Opt. Eng. 2009;48:27006.
- [23] C.S. WEAVER & J.W. GOODMAN. **Technique for Optically Convolver Two Functions.** Appl. Opt. 1966;5:1248-9.
- [24] R. HENAO, E. RUEDA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Noise-free recovery of optodigital encrypted and multiplexed images.** Opt. Lett. 2010;35:333-5.
- [25] J. GOODMAN, **Intrduction to Fourier Optics.** MacGraw Hill. 1996; 2nd edition.
- [26] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, S. TREJOS, M. TEBALDI, R. TORROBA. **Optical field data compression by opto-digital means.** J. Opt. 2016;18:125701.
- [27] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA **Innovative speckle noise reduction procedure in optical encryption.** J. Opt. 2017;19:055704.

Capítulo 3

Sistema de encriptación de Fourier fraccionario usando una lente electro-óptica de foco variable

El desarrollo de protocolos ópticos alternativos de encriptación es un campo de investigación activo que busca la implementación de procesadores ópticos de seguridad que ofrezcan ventajas sobre los sistemas existentes. Para incrementar la seguridad de los sistemas de codificación, algunos protocolos han incluido la combinación de procesos óptico-digitales con técnicas de autenticación por huella dactilar [1]. También se han incorporado técnicas de estenografía, las cuales permiten proteger la información ocultándola dentro de una señal portadora señuelo que no tiene relación con la información original [2, 3]. Además de estas técnicas, se han realizado modificaciones sobre las arquitecturas de codificación óptica que han permitido aumentar la seguridad de los sistemas e incluso reducir la cantidad de elementos ópticos utilizados durante el proceso de encriptación. Específicamente, dentro de los sistemas de codificación de doble máscara de fase, comúnmente conocidos como DRPE (siglas en inglés de: doble random phase encoding), se tienen implementaciones que mejoraran la calidad de la información recuperada al ubicar la llave de encriptación en el brazo de

referencia [4]; otro sistema de encriptación alternativo hace uso de la transformada de Hartley en combinación con un interferómetro de Michelson para llevar a cabo el proceso de encriptación [5]. Asimismo, se han publicado avances en la codificación de información en escala de grises, datos a color y vídeos [6–10]; se han introducido técnicas de procesamiento que permiten la manipulación de múltiples datos [11–21], y se han reportado trabajos que han permitido el procesamiento de información proveniente de objetos 3D [21, 22]. Adicionalmente, la modificación de algunas arquitecturas de codificación óptica ha permitido llevar a cabo procesos de encriptación en diferentes dominios ópticos haciendo uso de transformadas de Fresnel [23–25], transformadas de Fourier fraccionaria [26–29], y otras transformaciones canónicas lineales [5, 32–34].

A pesar de la amplia gama de posibles esquemas de cifrado óptico que se han reportado, todavía existen limitaciones significativas para su adopción generalizada para la protección de información. En general, los métodos de cifrado óptico introducen ruido y degradación a los datos codificados, requiriendo la aplicación de protocolos de reducción de ruido [35, 36] o el uso de contenedores de información para lograr una recuperación libre de cualquier tipo de degradación [37–42]. Por otro lado, las implementaciones experimentales de estos esquemas tienen altas exigencias experimentales y a veces son poco flexibles; por ejemplo, en el sistema JTC en el dominio de Fourier es complicado cambiar del dominio óptico de encriptación de Fourier, al dominio de Fresnel o de Fourier fraccionario.

Una solución a esta última dificultad es el desarrollo de un sistema de encriptación basado en la transformada de Fourier fraccionaria, este esquema muestra una gran flexibilidad gracias a las diferentes configuraciones experimentales que se pueden obtener mediante la transformada fraccionaria [27–29]. El orden fraccionario de la transformada configura el dominio óptico en el cual se realiza el proceso de encriptación y al mismo tiempo puede ser tratado como un parámetro de seguridad [29]. Es de resaltar que el esquema de encriptación en el dominio de Fourier fraccionario mantiene una configuración similar al sistema JTC en el dominio óptico de Fourier, y por ende hereda todas sus características básicas de seguridad.

Teniendo presente las ventajas que presenta el sistema de encriptación de transforma-

da conjunta en el dominio de Fourier fraccionario o FrJTC(siglas en inglés de: fractional joint transform correlator); y con el objetivo de aportar al desarrollo de arquitecturas de codificación óptica con potencial aplicación en implementaciones de carácter investigativo y práctico, en este capítulo se desarrolla una arquitectura FrJTC que permite la modificación dinámica del orden fraccionario, y por lo tanto del dominio óptico de encriptación usando una lente electro-óptica de foco variable (LEFV). La modificación electrónica de la longitud focal de la lente permite operar el sistema de codificación en los dominios ópticos de Fourier, Fresnel y Fourier fraccionario. En este caso, a diferencia de los trabajos ya reportados [26, 27, 29], el cambio en el orden fraccionario de la transformada no requiere de desplazadores mecánicos, lo que reduce los requerimientos de alineación y estabilidad de la configuración. Otra ventaja que presenta el uso de la LEFV en esta implementación, radica en la posibilidad de cambiar la longitud focal de la LEFV, manteniendo una calidad óptica estable, con una rapidez significativa y un rendimiento constante en comparación con los esquemas convencionales [26, 27, 29].

Teniendo presente las ideas mencionadas, en este capítulo se presenta la implementación del sistema de encriptación FrJTC usando una LEFV, y se analiza su desempeño mediante simulaciones computacionales y su posterior implementación experimental. Los estudios llevados a cabo en este trabajo permiten establecer la tolerancia al cifrado-descifrado con diferentes longitudes focales de la LEFV. Además, se realiza un protocolo de multiplexado basado en la variación de la longitud focal de la LEFV. Estos resultados muestran la flexibilidad y la capacidad del sistema FrJTC para proteger información. Los procedimientos teóricos y resultados experimentales que se presentan a continuación fueron publicados en el marco de las investigaciones realizadas en este trabajo de doctorado [30].

3.1. Sistema de encriptación FrJTC usando una lente electro-óptica de foco variable

En el sistema FrJTC se proyectan en el plano de entrada las ventanas objeto y llave en contacto con un difusor, separadas una distancia $2b$, tal como se observa en la Fig. 3.1. Además, una LEFV se ubicada entre los planos de entrada y salida. En general, en este sistema los planos de entrada y salida no están ubicados en los puntos focales de la LEFV, cuando la posición de los planos de entrada y registro coinciden con los puntos focales de la LEFV, el sistema de encriptación FrJTC es equivalente al JTC en el dominio de Fourier.

De acuerdo con la configuración experimental del sistema de encriptación FrJTC, en el plano de salida se registra la intensidad de la transformada de Fourier fraccionaria conjunta de la información proyectada en el plano de entrada o JFrPD (siglas en inglés de: joint fractional power distribution). El JFrPD contiene el dato encriptado e información extra que debe ser filtrada para garantizar la seguridad de los datos encriptados [31]. Para llevar a cabo el proceso de recuperación, es necesario tener la información del dato encriptado, el orden fraccionario de la transformada y la información de la llave de encriptación. El dato encriptado se extrae del JFrPD, mientras que el orden fraccionario de la transformada dependerá de las distancias entre el plano de entrada y la LEFV, la distancia entre la LEFV y el plano de salida, y la longitud focal de la LEFV. Además, para obtener la información de la llave es necesario emplear un sistema interferométrico fuera de eje.

En las primeras implementaciones experimentales del sistema FrJTC, el orden fraccionario era modificado a partir de desplazamientos mecánicos de la lente, este proceso introduce problemas de alineación, estabilidad y reduce la rapidez con la que se puede modificar el orden fraccionario. Para solventar esta dificultad, en este trabajo se usa la LEFV con el fin de evitar la incorporación de desplazadores mecánicos para la modificación del orden fraccionario, con lo cual se reducen los efectos de inestabilidad y pérdida de alineación que sufren los sistemas FrJTC convencionales. Además, de contar con la calidad óptica estable, la rapidez significativa y el rendimiento constante de la LEFV. De manera general, una

LEFV es un dispositivo opto-electrónico controlado por una corriente eléctrica inducida que se compone de una cámara llena de un polímero translúcido en contacto con una membrana flexible. Esta membrana está rodeada por un electrodo anular que cambia su radio de acuerdo con la intensidad de la corriente inducida, este cambio introduce variaciones en la potencia óptica de la lente y por ende en la longitud focal [43]. A su vez, como se mencionó anteriormente, la modificación de la longitud focal de la lente genera un cambio en el orden fraccionario [27–29]. Las lentes electro-ópticas se han utilizado ampliamente en aplicaciones que van desde la tomografía de coherencia óptica [44], caracterización de elementos ópticos [45], hasta la medida de propiedades ópticas no lineales [46] y pulsos ultra cortos [47]. Incluso, aportes anteriores aprovecharon las propiedades de la LEFV para implementar una máscara de fase que podía modificarse dinámicamente [48].

A continuación se presenta la descripción teórica del sistema de encriptación FrJTC basado en una LEFV.

3.2. Proceso de encriptación

Para llevar a cabo el proceso de codificación óptica, se proyectan en un modulador espacial de luz (MEL) la ventana objeto, la cual contiene el dato a encriptar, y la ventana llave como se muestra en la Fig. 3.1. La ventana llave es un cuadrado blanco que limita el tamaño de la llave de encriptación. Un difusor (experimentalmente un vidrio esmerilado) se pone en contacto con el MEL cubriendo la información proyectada y generando una máscara aleatoria de fase sobre cada ventana. El área del difusor en contacto con la ventana llave genera la llave de encriptación.

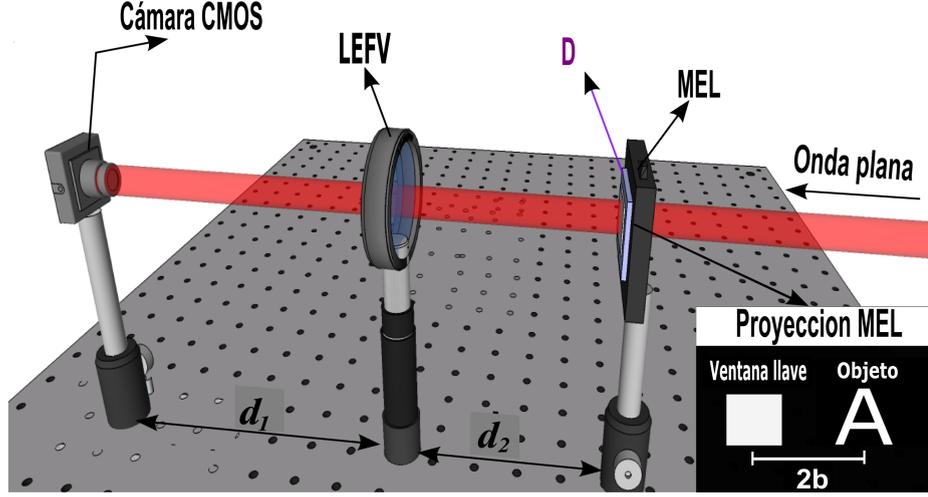


Figura 3.1: Esquema experimental de un sistema de encriptación JTC en el dominio de Fourier fraccional. D: difusor, d_1 : distancia plano de entrada-LEFV, d_2 : distancia plano de registro-LEFV, LEFV: lente electro-óptica de foco variable, MEL: modulador espacial de luz y $2b$: separación entre las ventanas objeto y llave.

De acuerdo con lo anterior, el plano de entrada del sistema de encriptación FrJTC viene dado por,

$$e(x, y) = \tau_{b, \alpha} \{c(x, y)\} + \tau_{-b, \alpha} \{l(x, y)\} \quad (3.1)$$

donde $c(x, y) = o(x, y)r(x, y)$, con $o(x, y)$ el objeto a encriptar, $r(x, y)$ una máscara aleatoria de fase (MAF), $l(x, y)$ es la MAF que representa la llave de encriptación, $2b$ es la separación entre las ventanas en el plano de entrada, τ es el operador de traslación fraccional que establece la posición de las ventanas objeto y llave en el plano de entrada, y α es el orden fraccional [29, 49, 50]. La combinación de la propagación en el espacio libre de la información entre el plano de entrada y la LEFV (d_1), la longitud focal de la LEFV (f) para una determinada corriente y la propagación en el espacio libre de la luz entre el plano de la LEFV y el plano de salida (d_2), determinan el orden fraccional α de la transformada fraccional en el plano de la cámara (ver Fig.3.1). En términos de las variables experimentales el orden fraccional viene dado por [29, 51, 52].

$$\alpha = \arccos \left(\frac{\sqrt{(d_1 - f)(d_2 - f)}}{f} \right) \quad (3.2)$$

Si $d_1 = d_2 = f$, entonces $\alpha = \pi/2$ y se tiene el caso particular del sistema de encriptación JTC en el dominio óptico de Fourier [29, 50]. Debido a que el orden fraccionario α depende de la variación de la longitud focal de la LEFV (Ec.3.2), solamente es necesario introducir variaciones de corriente eléctrica sobre la LEFV para conseguir una modificación en su longitud focal y de esta forma se estará realizando un cambio en el orden fraccionario de la transformada, esto garantiza que las condiciones de alineación y estabilidad del sistema no se vean afectadas. En particular, para obtener los resultados experimentales, se utilizó el modelo de LEFV EL-16-40-TC-VIS-20D (Optotune Switzerland AG, Switzerland) [53].

Para obtener el dato encriptado, en el plano de la cámara se registra el JFrPD de la entrada (Ec.3.1), que corresponde a la intensidad de la transformada fraccionaria conjunta de la información proyectada en el plano de entrada,

$$\begin{aligned} I_\alpha(\nu, \omega) &= |c_\alpha(\nu, \omega)|^2 + |l_\alpha(\nu, \omega)|^2 \\ &+ c_\alpha(\nu, \omega)l_\alpha^*(\nu, \omega)e^{4\pi i b \nu \csc(\alpha)} + c_\alpha^*(\nu, \omega)l_\alpha(\nu, \omega)e^{-4\pi i b \nu \csc(\alpha)} \end{aligned} \quad (3.3)$$

donde $c_\alpha(\nu, \omega)$ y $l_\alpha(\nu, \omega)$ son las transformadas de Fourier fraccionarias (TFFrs) de orden α de $c(x, y)$ y $l(x, y)$, respectivamente. $*$ representa el complejo conjugado y $\csc()$ es la función trigonométrica cosecante. Después de realizar el registro del JFrPD, se realiza el mismo procedimiento de filtrado presentado en la Sección 2.4.2, con lo que se obtiene el dato encriptado.

$$E_\alpha(\nu, \omega) = c_\alpha(\nu, \omega)l_\alpha^*(\nu, \omega) \exp[2\pi i b(\nu x' + \omega y') \csc(\alpha)] \quad (3.4)$$

Como se observa en la Ec. 3.4, el dato encriptado depende del orden fraccionario de la transformada. Por lo tanto, para llevar a cabo el proceso de recuperación, además de ser necesaria la información de la llave de seguridad, se requiere el mismo orden fraccionario usado en el proceso de encriptación.

3.3. Registro de la información de la llave

Para el registro experimental de la información de la llave de encriptación se implementa el sistema holográfico fuera de eje (Fig. 3.2) [29].

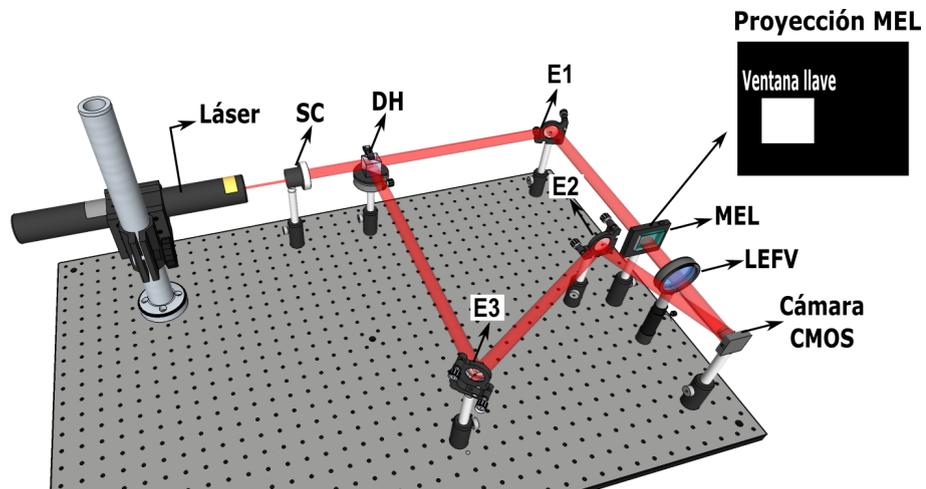


Figura 3.2: Esquema experimental para el registro de la información de la llave. D: difusor, SC: sistema de colimación, MEL: modulador espacial de luz, DH: divisor de haz, LEFV: lente electro-óptica de foco variable y E: espejo.

Este sistema cuenta con dos brazos de iluminación, en uno de ellos se ubica el sistema de encriptación FrJTC (Fig. 3.1) y en el otro una onda plana de referencia de amplitud unitaria, dada por,

$$P(\nu, \omega) = \exp[2\pi i \lambda (\nu \cos \alpha + \omega \cos \beta)] \quad (3.5)$$

λ es la longitud de onda de la luz incidente, $\cos\alpha$ y $\cos\beta$ son los cosenos directores de la onda en el plano de registro [54, 55]. En este caso, se proyecta en el MEL únicamente la ventana de la llave; por lo tanto, en el plano de la cámara se registra el holograma resultante de la interferencia entre la onda plana y la TFFr de la llave de seguridad.

$$\begin{aligned}
H_\alpha(\nu, \omega) &= |P(\nu, \omega)|^2 + |l_\alpha(\nu, \omega)|^2 + l_\alpha(\nu, \omega) \exp[-2\pi i \lambda (\nu \cos \alpha + \omega \cos \beta)] \\
&+ l_\alpha^*(\nu, \omega) \exp[2\pi i \lambda (\nu \cos \alpha + \omega \cos \beta)]
\end{aligned} \tag{3.6}$$

Después de realizar el registro holográfico, se realiza un proceso de filtrado similar al expuesto en la Sección 2.5.2, este proceso permite extraer la información de la llave, la cual es posicionada en las coordenadas (x', y') .

$$K_\alpha(\nu, \omega) = l_\alpha(\nu, \omega) \exp[2\pi i b (\nu x' + \omega y')] \tag{3.7}$$

3.4. Proceso de descryptación en el sistema FrJTC

Para recuperar la información original, un usuario autorizado debe multiplicar el dato encriptado (Ec. 3.4) por la información de la llave de encriptación (Ec. 3.7). Cuando ambos datos son reposicionados en el origen de coordenadas, su producto toma la forma,

$$D_\alpha(\nu, \omega) = c_\alpha(\nu, \omega) l_\alpha^*(\nu, \omega) l_\alpha(\nu, \omega) \tag{3.8}$$

si se considera $l_\alpha(\nu, \omega)$ como una función pura de fase, entonces $l_\alpha(\nu, \omega) l_\alpha^*(\nu, \omega) \approx 1$ [56].

Teniendo en cuenta esta aproximación y realizando un TFFr inversa de orden α sobre el campo representado por la Ec. 3.8, se obtiene el dato original multiplicado por la máscara aleatoria de fase $r(x, y)$.

$$d(x, y) = o(x, y)r(x, y) \quad (3.9)$$

El dato recuperado corresponde al módulo cuadrado de la Ec.3.9. Como se observa en el desarrollo teórico anterior, para lograr una correcta recuperación de la información, además del conocimiento del dato encriptado y la información de la llave, se debe conocer el orden fraccionario correcto. Por lo tanto, el orden fraccionario representa una llave extra de seguridad en el sistema de encriptación FrJTC [29].

3.5. Resultados

3.5.1. Resultados numéricos

Para analizar el funcionamiento del sistema FrJTC usando la LEFV se desarrolló un sistema óptico de codificación FrJTC digital, este sistema permite analizar digitalmente el comportamiento del criptosistema cuando se modifican sus parámetros, permitiendo optimizar y determinar su comportamiento para su posterior implementación experimental.

En esta simulación se empleó un plano de entrada con una resolución de 4000 pixeles x 4000 pixeles, cada pixel con un tamaño de $8 \mu m$ x $8 \mu m$ y una fuente de iluminación monocromática de longitud de onda de $532 nm$. La resolución de la ventana objeto y la ventana llave fue de 600 pixeles x 600 pixeles, con una separación entre ventanas de $2b = 800$ pixeles. Se implementó una MAF uniformemente distribuida con una resolución de 4000 pixeles x 4000 pixeles. Se usó una LEFV con una pupila circular de un diámetro de 2000

pixeles (16 mm), ubicada a una distancia de 12 cm del plano de entrada y a 24 cm del plano de registro.

Para verificar el correcto funcionamiento de la LEFV dentro del sistema óptico, se llevó a cabo el proceso de encriptación y recuperación para todo el rango de potencias ópticas de la LEFV, en este caso desde -6 D hasta 6 D . Posteriormente, la calidad del dato recuperado se comparó con el dato original a partir de la métrica del coeficiente de correlación (CC), definido así,

$$CC = \frac{\sum_x \sum_y (I_{xy} - \bar{I})(R_{xy} - \bar{R})}{\sqrt{\left(\sum_x \sum_y (I_{xy} - \bar{I})^2\right) \left(\sum_x \sum_y (R_{xy} - \bar{R})^2\right)}} \quad (3.10)$$

donde (x, y) son las coordenadas de los pixeles, I es el dato recuperado, R el objeto de entrada, \bar{I} y \bar{R} son los valores medios del objeto descryptado y el objeto de entrada, respectivamente.

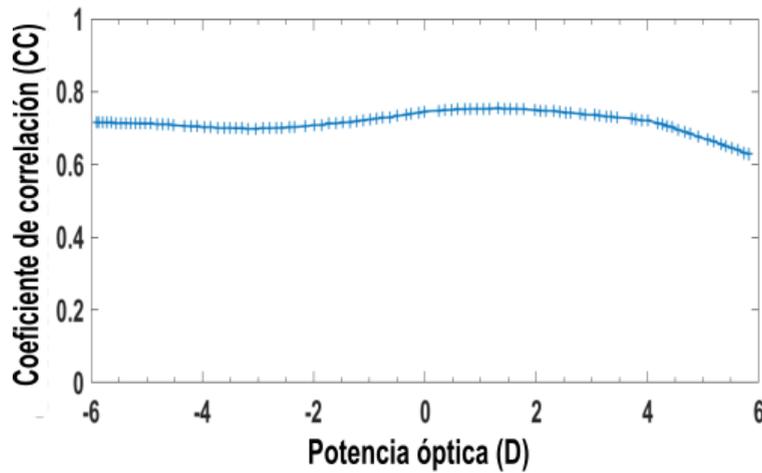


Figura 3.3: CC entre un objeto recuperado, después del proceso de encriptación y descryptación, y su correspondiente objeto original en función de la potencia óptica

En la Fig.3.3, se puede observar que la calidad del dato recuperado, después del proceso de encriptación y descryptación, no varía significativamente con los cambios en la potencia

óptica de la LEFV. Este comportamiento permite concluir que es posible llevar a cabo el proceso de encriptación y desencriptación para todo el rango de potencias ópticas de la LEFV sin perder la calidad en el dato recuperado.

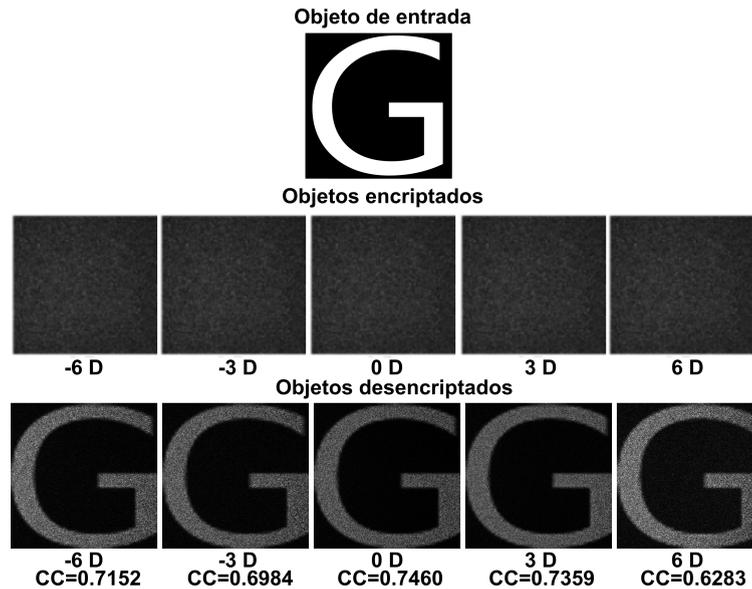


Figura 3.4: Encriptación numerica con su correspondiente recuperación para diferentes potencias ópticas de la LEFV

La Fig. 3.4 muestra la intensidad del dato encriptado, esta corresponde a un patrón aleatorio a partir del cual no se puede reconocer la información original. Por otro lado, después de llevar a cabo el proceso de desencriptación se obtiene el objeto recuperado, el cual exhibe la información original. Los resultados mostrados en Fig.3.4 demuestran que, aunque hay algunas fluctuaciones en el CC, la diferencia de calidad para los datos encriptados y recuperados con diferentes potencias ópticas es muy pequeña, confirmando que dentro del rango analizado es posible llevar a cabo de forma exitosa los procesos de encriptación y recuperación.

Además del estudio anterior, se analizó la tolerancia del proceso de desencriptación cuando la longitud focal empleada durante el proceso de encriptación difiere de la usada para registrar la llave de encriptación. Se debe destacar que, debido a que el orden fraccionario depende de la longitud focal de la LEFV, entre menor sea la tolerancia de recuperación mayor será la seguridad que brinda el orden fraccionario como parámetro extra de seguridad.

En la práctica, el cambio de fase introducido por la LEFV es inversamente proporcional a la longitud focal de la lente, y puede ser modelado por la función de fase de una lente,

$$L(x_1, y_1) = \exp \left[i \frac{\pi}{\lambda f} (x_1^2 + y_1^2) \right] \quad (3.11)$$

donde $f = 1/P$ es la longitud focal de la LEFV, P es la potencia óptica de la lente en dioptrías (D) y λ es la longitud de onda del haz de iluminación. De acuerdo con la ecuación Ec.3.11, cuando se tiene distancias focal cortas para la LEFV (potencias ópticas grandes) se induce grandes cambios en la fase de la lente. Por el contrario, cuando se tiene longitudes focal largas para la LEFV (potencias ópticas pequeñas) se inducen pequeños cambios en la fase de la lente. Con el objetivo de probar estas aseveraciones y comprender el funcionamiento de la LEFV dentro del sistema de codificación, se realizó el proceso de encriptación de un mismo objeto para distancias focales cortas y largas. Posteriormente, se realiza el proceso de desencriptación, para ambos casos utilizando la información de las llaves registradas para diferentes longitudes focales. Después, se calcula el CC entre el objeto recuperado con la información de la llave correcta y el recuperado con la información de las llave registradas para diferentes longitudes focales.

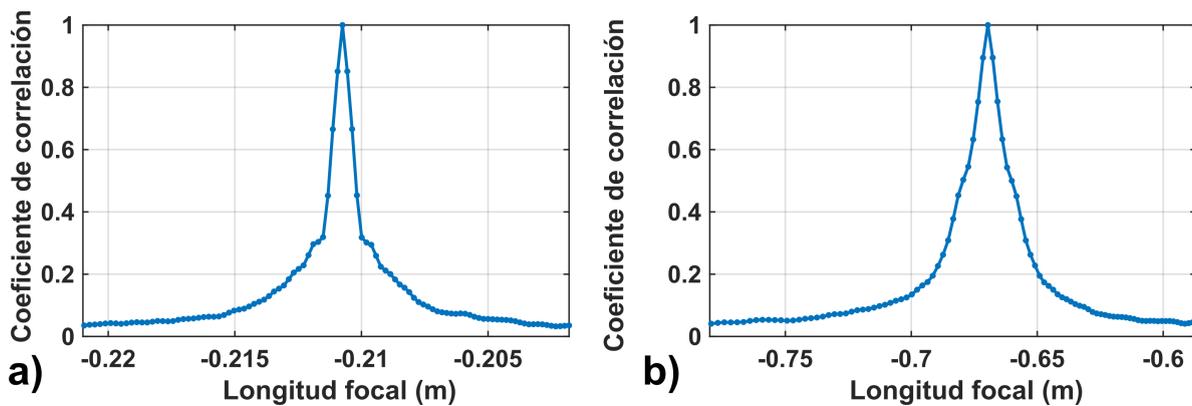


Figura 3.5: Coeficiente de correlación entre el objeto recuperado usando la llave correcta y el que se recupera cuando se usan llaves registradas con diferentes longitudes focales de la LEFV: a) objeto encriptado para una focal de $-0,211$ m ($-4,74$ D) y b) objeto encriptado para una focal de $-0,670$ m ($-1,49$ D)

Los resultados presentes en la Fig. 3.5 corroboran el comportamiento esperado. Se observa que, para el caso del objeto encriptado con una focal de la LEFV de $-0,211$ m, la tolerancia a la desencriptación es aproximadamente de $0,002$ m con respecto a la focal usada para el registro de la llave correcta de encriptación; mientras que, para el objeto encriptado con una focal de $-0,670$ m la tolerancia es cercana a los $0,070$ m. Estos resultados permiten establecer, además del rango de seguridad que puede presentar la longitud focal como parámetro extra de seguridad, el mínimo cambio en la longitud focal de la LEFV que asegura la obtención de dos llaves diferentes, garantizando que dos objetos, encriptados con la misma MAF y diferente distancia focal, no puedan ser recuperados con la misma llave. Este hecho es importante en los procesos de manipulación de múltiples datos.

Los resultados numéricos obtenidos permiten establecer los parámetros mínimos que posibilitan el desarrollo experimental del esquema y son parte fundamental para su implementación experimental. A continuación se presentan los resultados obtenidos a partir de la implementación experimental del esquema FrJTC usando una LEFV.

3.5.2. Resultados experimentales

Los resultados experimentales que se muestran a continuación fueron obtenidos con el sistema experimental mostrado en la Fig. 3.2. La fuente de iluminación utilizada fue un láser JDS UNIPHASE 1135 con una longitud de onda $\lambda = 632$ nm y una potencia de 20 mW. El medio de registro fue una cámara CMOS EO-10012M con un tamaño de pixel de $1,6$ μ m x $1,6$ μ m y una resolución de 3840 x 2848 pixeles. Como sistema de proyección se utilizó un MEI Holoeye 2002, con un tamaño de pixel de 32 μ m x 32 μ m, una resolución de 800 x 600 pixeles y un área de proyección de $25,6$ mm x $19,2$ mm. El tamaño de la ventana objeto fue de $9,6$ mm x $9,6$ mm, mientras que el tamaño de la ventana llave fue $3,2$ mm x $3,2$ mm, la separación entre ventanas fue $2b = 4,8$ mm. Se usó el modelo de LEFV EL-16-40-TC-VIS-20D con un rango de potencia óptica de -10 D hasta $+10$ D, una apertura de 16 mm y una respuesta de alrededor de 25 ms [53].

El correcto funcionamiento del sistema óptico está ligado a la correcta medición de la longitud focal inducida en la LEFV, debido a esto es necesario realizar una calibración de la lente LEFV. Estudios anteriores han demostrado que el comportamiento de la lente en función de la variación en la distancia focal presenta una respuesta tipo histéresis [57, 58], debido a esto, es posible tener más de una potencia óptica para el mismo valor de corriente inducida sobre la LEFV, dependiendo de la ruta de corriente creciente o decreciente que se siga. Para evitar este efecto de histéresis, el cual podría comprometer la seguridad del sistema, la LEFV es calibrada usando el método propuesto por Torres-Sepúlveda *et. al* [58]. Empleando este método, la LEFV es calibrada para un rango de potencias de $[-6, 6]$ D. El proceso de calibración fue llevado a cabo en un simulador visual [58, 59], el cual consta de un sensor Hartmann-Shack (SHS) que mide las aberraciones ópticas, en particular el desenfoque. En este caso, el método de calibración consiste en inducir una corriente eléctrica sobre la LEFV en pasos de 5 mA , desde 100 mA hasta -100 mA . Para cada cambio en la corriente las aberraciones son medidas por el SHS 6 veces, esto permite obtener una relación entre la corriente inducida y el coeficiente de Zernike (CZ) asociado al desenfoque. Después de obtener el CZ, se determina el inverso de la potencia óptica y, a partir de ésta, se determina la longitud focal inducida en la LEFV, que será usada para establecer el orden fraccionario α de la transformada (Ec.3.2).

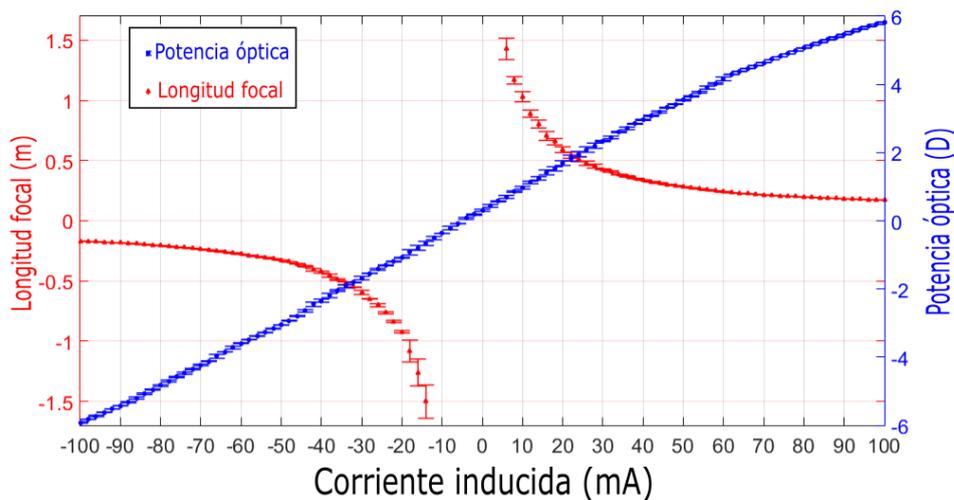


Figura 3.6: Curva de calibración de la LEFV

La curva de calibración de la LEFV (Fig.3.6), obtenida a partir del protocolo descrito en el párrafo anterior, evita el comportamiento tipo histéresis. En la Fig. 3.6 se observa que, bajo esta calibración la potencia óptica presenta un comportamiento lineal en el rango de $[-6, 6]$ D, mientras que la longitud focal presenta el comportamiento hiperbólico esperado para las lentes. Además, se puede notar que para una corriente de -5 mA se tiene un comportamiento asintótico, esto indica que cerca de este valor de corriente la longitud focal de la LEFV sufre cambios abruptos que deben ser tenidos en cuenta al momento de su implementación experimental.

Después de la calibración, las características de la LEFV se analizan experimentalmente dentro del esquema de encriptación. En primer lugar, usando el mismo difusor, se realiza el proceso de codificación y recuperación de un objeto para diferentes corrientes inducidas en un rango de operación de la LEFV de -60 mA a 60 mA, bajo las condiciones de calibración ya mencionadas, dentro de este rango de corriente la potencia óptica de la LEFV sigue una tendencia lineal. Posteriormente, la calidad del dato recuperado es comparada con el dato original a partir de la métrica del coeficiente de correlación (CC) Ec. (3.7).

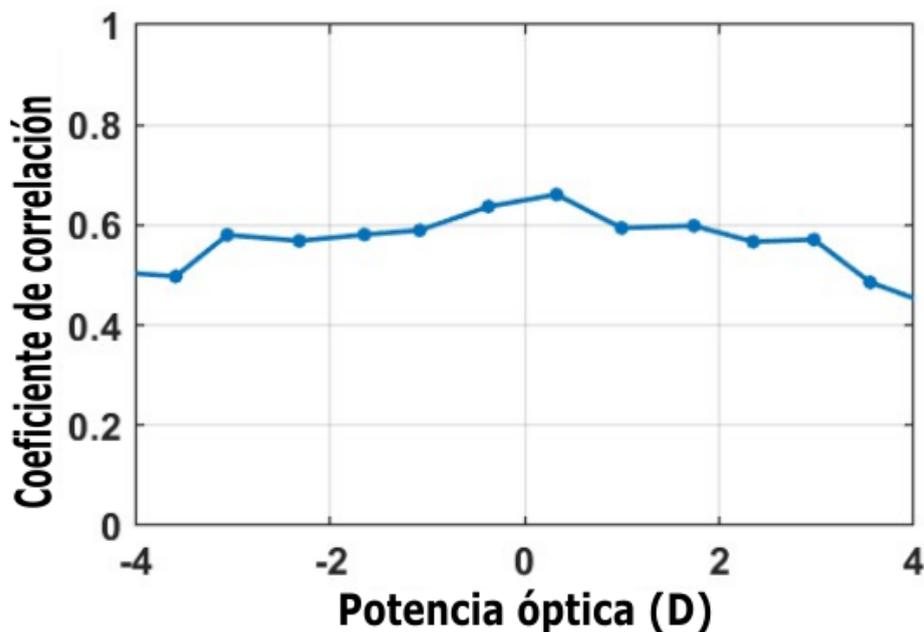


Figura 3.7: CC experimental entre un objeto recuperado, después de los procesos de encriptación y desencriptación, con su correspondiente objeto original en función de la potencia óptica

Como se observa en la Fig. 3.7, el CC no varía significativamente en el rango de potencias ópticas de operación de la LEFV, y por lo tanto, en este intervalo de operación la calidad del objeto recuperado permanece constante. Estos resultados experimentales validan y corroboran los resultados numéricos presentado en la sección anterior. Los resultados expuestos en la curva de correlación (Fig.3.7) se pueden visualizar en la Fig. 3.8.

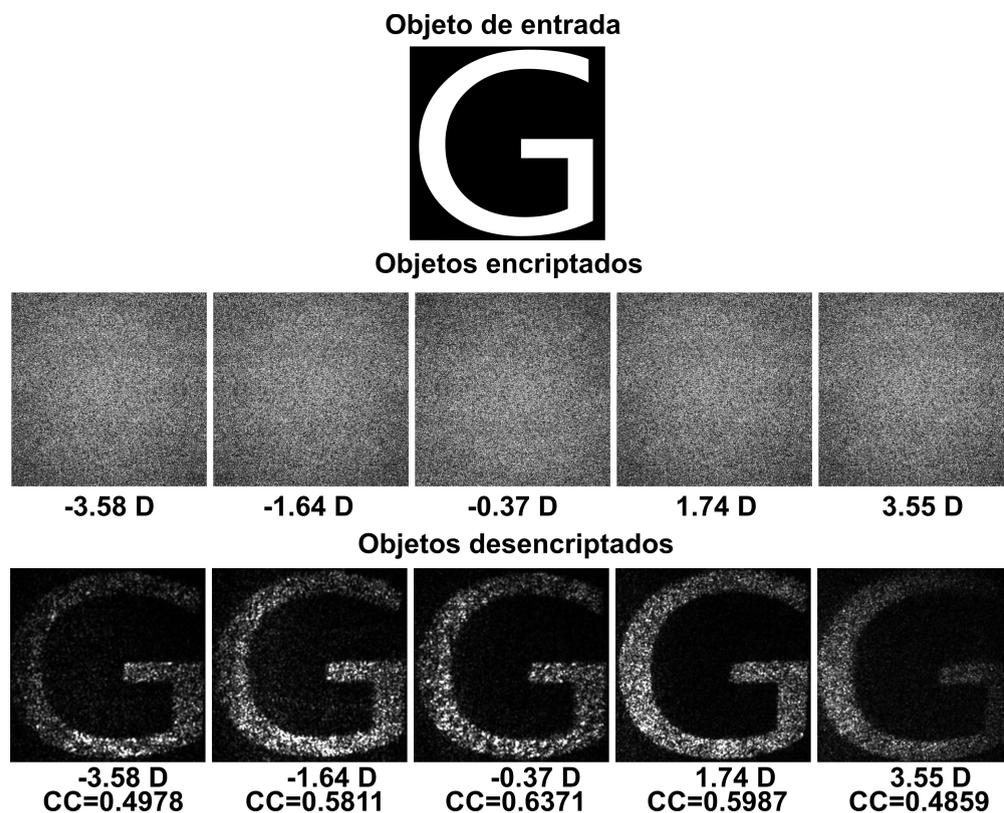


Figura 3.8: Encriptación experimental con su correspondiente recuperación para diferentes potencias ópticas de la LEFV

Se nota que, a pesar de la presencia de ruido inherente a los procesos de encriptación y recuperación experiemntal, la calidad de la imagen varía muy poco en todo el rango de operación (ver Fig. 3.8). Además, se observa que tanto el dato recuperado como el dato encriptado están en concordancia con los resultados obtenidos numéricamente (Sección 3.5.1).

Por otro lado, considerando la relación inversa entre la fase y la longitud focal de la LEFV, y con el propósito de corroborar los resultados numéricos expuestos en la sección anterior, se

realizó el proceso de encriptación de un dato para diferentes longitudes focales largas y cortas de la LEFV. Posteriormente, se llevó a cabo el proceso de recuperación con la información de las llaves registradas para diferentes focales de la LEFV y se calculó el coeficiente de correlación entre el dato recuperado con la información de la llave correcta, registrada en la misma longitud focal que el dato encriptado, y el dato recuperado con llaves registradas para diferentes longitudes focales de la LEFV. Esto permitió establecer la tolerancia a la descryptación con relación a la longitud focal de la LEFV.

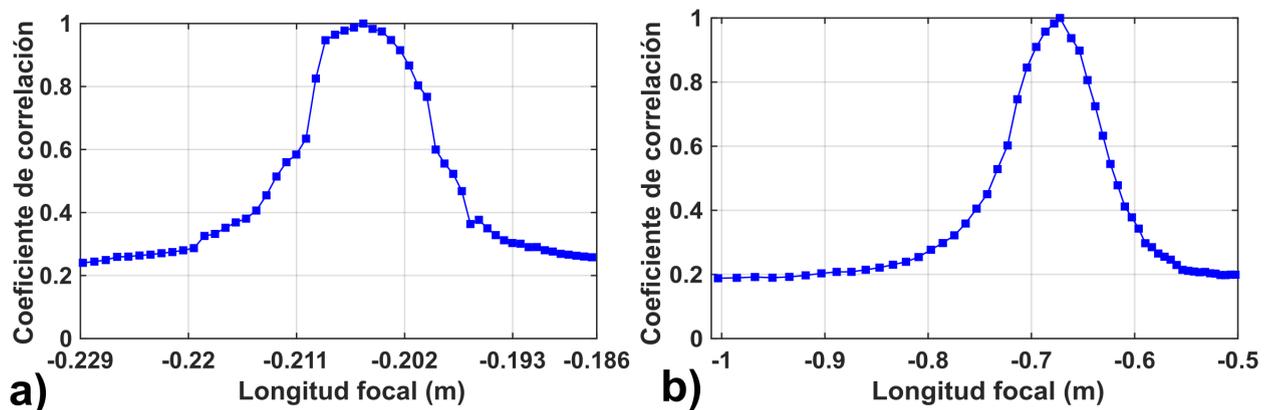


Figura 3.9: Coeficiente de correlación entre el objeto recuperado usando la llave correcta y el que se recupera cuando se usan llaves registradas con diferentes longitudes focales de la LEFV: a) objeto encriptado para una focal de $-0,205$ m ($-4,88$ D) y b) objeto encriptado para una focal de $-0,650$ m ($-1,54$ D)

Los resultados experimentales mostrados en la Fig. 3.9 son consistentes con los resultados numéricos presentes en la Fig. 3.5. Como se observa, cuando un objeto es encriptado usando una longitud focal para la LEFV de $-0,205$ m ($-4,88$ D) (Fig. 3.9(a)), la tolerancia a la descryptación es aproximadamente de $0,015$. Por otro lado, cuando se usa una longitud focal de $-0,650$ m ($1,54$ D), la tolerancia a la descryptación es cerca de $0,15$ m. Se puede concluir que la tolerancia es menor para longitudes focales cortas de la LEFV. Como se mencionó anteriormente, esta tolerancia representa el mínimo cambio que se debe hacer en la longitud focal para asegurar que después de encriptar un par de objetos con longitudes focales diferentes no sea posible recuperar uno de ellos con la llave del otro (ver Fig.3.10).

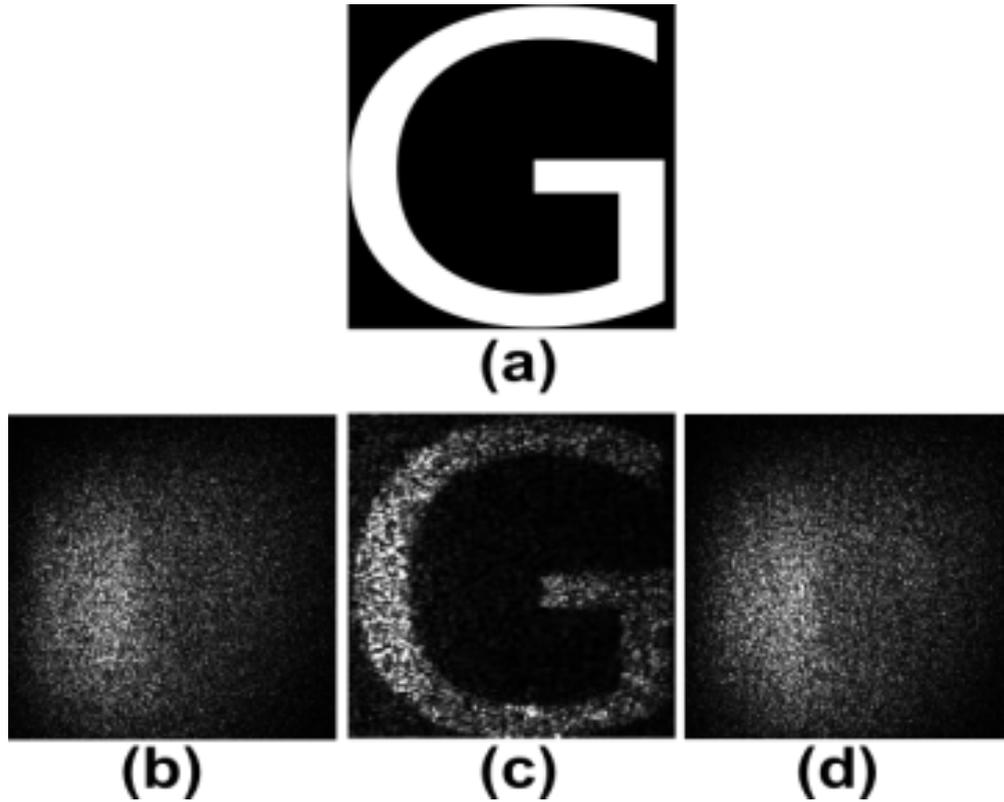


Figura 3.10: Descriptación de un dato usando la llave correcta y usando llaves registradas para diferentes longitudes focales de la LEFV: a) Objeto original a encriptar con una longitud focal de $-0,205$ m. Dato recuperado con llaves registradas usando una longitud focal de: b) $-0,229$ m c) $-0,205$ m y d) $-0,186$ m

En las Figs. 3.10(b) y (d) se observa que cuando el proceso de recuperación se hace con una llave registrada por encima del rango de tolerancias, para longitudes focales cortas, no es posible recuperar la información encriptada. Por otro lado, cuando el proceso de recuperación se lleva a cabo con la llave correcta la información es recuperada (ver fig.3.10(c)).

El análisis de la tolerancia a la descriptación permite establecer las condiciones experimentales para el desarrollo de protocolos de manipulación de múltiples datos, como el que se presenta a continuación.

3.5.3. Encriptación de múltiples datos

El desarrollo de protocolos que permitan el procesamiento seguro de múltiples datos requiere de la implementación de técnicas de multiplexado. Con estas técnicas se puede almacenar múltiples datos en un solo paquete, de manera que cuando se realice el proceso de recuperación sea posible acceder de manera individual a cada uno de los datos contenidos dentro del paquete. Dentro del campo de la manipulación segura a partir de medios ópticos, el proceso de multiplexado consiste en combinar múltiples datos encriptados en un solo dato de campo óptico de manera reversible [13–20], lo que permite que, al momento de la recuperación, se pueda acceder a cada uno de los datos de manera individual.

Los diversos parámetros que poseen los sistemas ópticos de encriptación han permitido el desarrollado diferentes métodos de multiplexados. Por ejemplo, la combinación de diferentes longitudes de onda [13, 14], variaciones en la polarización del haz de iluminación [15], la rotación de la máscara que genera la llave de encriptación [17], entre otros.

En este caso, se usará el cambio en la longitud focal de la LEFV como parámetro para llevar a cabo el proceso de multiplexado. En este trabajo, se realiza el proceso de multiplexado usando el rango de longitudes focales cortas, ya que como se observa en los resultados mostrados en las Figs.3.5 y 3.9, la tolerancia a la descriptación es menor. Es de resaltar que gracias a que en este rango se tienen tolerancias pequeñas, es posible multiplexar mayor cantidad de objetos, ya que los cambios necesarios en la longitud focal de la LEFV para generar diferentes llaves son pequeños, lo que conlleva a tener muchas mas llaves.

Para verificar el protocolo de manipulación de múltiples datos se encriptaron y multiplexaron los objetos **G**, **O** y **F**, siguiendo el procedimiento que se describe a continuación:

1. Cada objeto es encriptado usando una longitud focal diferente para la LEFV. De esta manera, el orden fraccionario es diferente para cada dato.
2. Se registra la llave de encriptación para las diferentes longitudes focales de la LEFV

usadas al momento de encriptar los datos.

3. Todos los datos encriptados con los diferentes ordenes fraccionarios, son multiplexados en un solo paquete.
4. Los usuarios autorizados solo pueden acceder a la información correspondiente a su llave y orden fraccionario.

En general, el multiplexado de N datos encriptados y reposicionados en las coordenadas (x_s, y_s) , viene dado por la siguiente expresión,

$$M(\nu, \omega) = \sum_{s=1}^N c_{\alpha_s}(\nu, \omega) l_{\alpha_s}^*(\nu, \omega) \exp[2\pi i b(\nu x_s + \omega y_s) \csc(\alpha_s)] \quad (3.12)$$

donde, $s = 1, 2, 3 \dots N$, $l_{\alpha_s}(\nu, \omega)$ representa la información de la llave que se debe poseer para poder recuperar el dato encriptado con el orden fraccionario α_j , el cual es modificado a partir del cambio de longitud focal de la LEFV. Por lo tanto, un usuario con la información de la llave s -ésima, podrá acceder únicamente a la información encriptada relacionada con el del dato s -ésimo, obteniendo

$$M_r(x, y) = S(x_s, y_s) + \sum_{s=1, s \neq k}^N R(x_k, y_k) \quad (3.13)$$

donde $S(x_s, y_s)$ es el dato recuperado y $R(x_k, y_k)$ es el ruido correspondiente los datos no desencriptados. Como consecuencia del proceso de filtrado y reposicionamiento, en la Ec. 3.13, el dato recuperado se posiciona en las coordenadas (x_s, y_s) , mientras que el ruido se ubica en las coordenadas (x_k, y_k) con $s \neq k$. Lo anterior garantiza que, después del proceso de desencriptación, el ruido de los datos no recuperados no se superponga con la información recuperada Fig.(3.11).

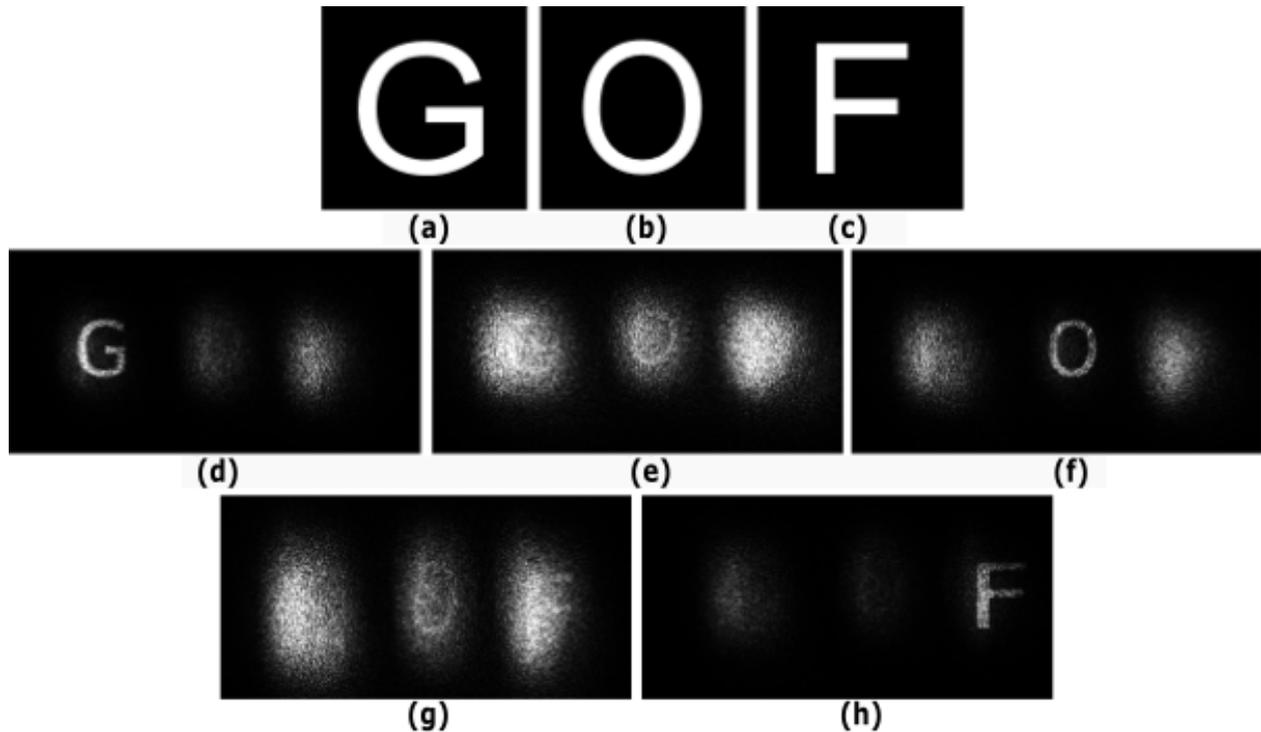


Figura 3.11: Protocolo de encriptación de múltiples datos: objetos de entrada a encriptar usando longitudes focales de la LEFV de (a) $-0,229$ m, (b) $-0,205$ m y (c) $-0,186$ m. Recuperación de los datos de usando llaves registradas para longitudes focales de la LEFV de (d) $-0,229$ m, (e) $-0,211$ m, (f) $-0,205$ m, (g) $-0,199$ m y (h) $-0,186$ m

Cuando el proceso de recuperación se realiza con llaves registradas por encima del rango de tolerancia, solo uno de los objetos es recuperado, mientras que los demás permanecen encriptados y aparecen en el plano de recuperación como ruido (Figs. 3.11(d),(f) y(h)). Por otro lado, cuando el proceso de recuperación se lleva a cabo con una llave registrada para una longitud focal de la LEFV entre las longitudes focales de la LEFV usadas para el registro de dos datos, es posible recuperar ambos objetos con degradación, tal como se observa en las Figs. 3.11(e) y (g). Este comportamiento es típico de este tipo de esquemas de encriptación y debe ser tenido en cuenta al momento de la implementación de protocolos de seguridad que involucren múltiples datos.

Es importante resaltar que para llevar a cabo el proceso de multiplexado, solo es necesario cambiar la corriente eléctrica inducida en la LEFV. Gracias a esto, se tiene una mayor rapidez en el registro de la información, y los requisitos de estabilidad y alineación para

el funcionamiento exitoso de este esquema de encriptación se reducen en comparación con otras configuraciones experimentales [29, 60, 61]. En consecuencia, la configuración de cifrado presentada en este trabajo puede considerarse como una alternativa con gran potencial para el desarrollo de sistemas de seguridad que puedan ser usados en aplicaciones de uso masivo.

3.6. Conclusiones

Los resultados numéricos y experimentales demuestran la viabilidad y la aplicabilidad de un sistema óptico de encriptación en el dominio de Fourier fraccionario utilizando un LEFV en lugar de una lente de foco fijo. El uso de la LEFV en la implementación experimental del sistema de encriptación FrJTC elimina la necesidad de un desplazador mecánico para modificar las distancias entre planos, y por ende el orden fraccionario de la transformada, reduciendo los requerimientos de estabilidad y alineación y mejorando la versatilidad del sistema. Asimismo, la rápida respuesta a los cambios de corriente que presenta la LEFV permite cambiar rápidamente la longitud focal de la LEFV, y por lo tanto el orden fraccionario, agilizando el proceso de registro del dato encriptado y de la información de la llave de seguridad.

Es importante tener presente que la LEFV debe estar correctamente caracterizada, debido al comportamiento tipo histéresis que presenta la potencia óptica y/o la fase de la LEFV con relación a la corriente que se induce sobre la LEFV para producir los cambios en la longitud focal. Este comportamiento tipo histéresis debe ser evitado, tal como se muestra en la calibración de la lente, ya que podría introducir algunas incertidumbres en el orden fraccionario alterando la seguridad que brinda este parámetro. Además, una calibración incorrecta de la LEFV podría afectar el rendimiento de el sistema en los procesos de multiplexación de datos.

Los resultados muestran que dentro de todo el rango de operación de la LEFV es posible llevar a cabo el proceso de cifrado y recuperación de manera exitosa. Además, la métrica

del coeficiente de correlación corrobora que dentro del rango de operación de la LEFV no se presentan cambios considerables en la calidad de los datos recuperados.

Adicionalmente, se demuestra la tolerancia a la descriptación usando llaves de encriptación registradas para diferentes longitudes focales de la LEFV. En particular, se corrobora que para longitudes focales cortas se tiene una menor tolerancia a la descriptación, lo que a su vez hace posible multiplexar una mayor cantidades de datos encriptados. Los resultados del análisis de tolerancia a la descriptación permiten la aplicación de un protocolo de cifrado multiusuario.

Esta primera demostración de un esquema DRPE fraccionario utilizando un LEFV podrá ser el punto de partida para la implementación de este tipo de esquemas en aplicaciones prácticas o experimentales enfocadas en la manipulación segura de información a través de medios ópticos. Cabe resaltar que este sistema de encriptación presenta una alta flexibilidad, ya que puede ser configurado para que incorpore transformadas de Fourier, Fourier fraccionario y Fresnel, característica que aumenta el rendimiento del sistema y que deben ser explotada en futuros trabajos

Todos los resultados presentados en este capítulo, como se observa en el apéndice del trabajo, fueron publicados en revista internacional como producto de la investigación llevada a cabo durante el doctorado [30].

Bibliografía

- [1] A. YAN, T.C. POON, Z. HU, J. ZHANG. **Optical image encryption using optical scanning and fingerprint keys.** J. Mod. Opt. 2016;63:38–43.
- [2] X. LIAO, Z. QIN, L. DING. **Data embedding in digital images using critical functions.** Signal Processing: Image. 2017;58:146-56.
- [3] X. LIAO, C. SHU. **Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels.** J. Vis. Commun. Image. Represent. 2015;28:21–7.
- [4] J.A. JARAMILLO-OSORIO, J.F. BARRERA-RAMÍREZ, S. MONTOYA, A. MIRAGUDELO, A. VELEZ-ZEA, R. TORROBA. **Improved decryption quality with a random reference beam cryptosystem.** Opt. Lasers Eng. 2019;112:119–27.
- [5] L. CHEN, D. ZHAO. **Optical image encryption with Hartley transforms.** Opt. Lett. 2006;31:3438–40.
- [6] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Experimental optical encryption of grayscale information.** Appl. Opt. 2019;56:5883–9.
- [7] M. TANHA, R. KHERADMAND, S. AHMADI-KANDJANI. **Gray-scale and color optical encryption based on computational ghost imaging.** Appl. Phys. Lett. 2012;101:101108.

- [8] F. MOSSO, J.F. BARRERA-RAMÍREZ, M. TEBALDI, N. BOLOGNINI, R. TORROBA. **All-optical encrypted movie.** *Opt. Express.* 2011;19:5706–12.
- [9] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Secure real-time generation and display of color holographic movies.** *Opt. Lasers Eng.* 2019;122:239–44.
- [10] H. CHENG, X. LI. **Partial encryption of compressed images and videos.** *IEEE Trans. Signal. Process.* 2000;48:2439–51.
- [11] A. ALFALOU, C. BROSSEAU, N. ABDALLAH, M. JRIDI. **Assessing the performance of a method of simultaneous compression and encryption of multiple images and its resistance against various attacks.** *Opt. Express.* 2013;21:8025–43.
- [12] D. AMAYA, M. TEBALDI, R. TORROBA, N. BOLOGNINI. **Digital color encryption using a multi-wavelength approach and a joint transform correlator.** *J. Opt. A Pure Appl. Opt.* 2008;10:104031.
- [13] G. SITU, J. ZHANG. **Multiple image encryption by wavelength multiplexing.** *Opt. Lett.* 2005;40:619-24.
- [14] D. AMAYA, M. TEBALDI, R. TORROBA, N. BOLOGNINI. **Wavelength multiplexing encryption using joint transform correlator architecture.** *Appl. Opt.* 2009;48:2099-04.
- [15] J.F. BARRERA-RAMÍREZ, R. HENAO, M. TEBALDI, N. BOLOGNINI, R. TORROBA. **Multiplexing encrypted data by using polarized light.** *Opt. Commun.* 2006;260:109-12.
- [16] J.F. BARRERA-RAMÍREZ, R. HENAO, M. TEBALDI, N. BOLOGNINI AND R. TORROBA. **Multiplexing encryption-decryption via lateral shifting of a random phase mask.** *Opt. Comm.* 2006;259:532-6.
- [17] E. RUEDA, C. RIOS, J.F. BARRERA-RAMÍREZ, R. HENAO, R. TORROBA. **Experimental multiplexing approach via code key rotations under a joint transform correlator scheme.** *Appl. Opt.* 2010;284:2500-4.

- [18] D. AMAYA, M. TEBALDI, R. TORROBA, N. BOLOGNINI. **Multichanneled encryption via a joint transform correlator architecture.** Appl. Opt. 2008;47:5903-7.
- [19] C. LIN, X. SHEN, R. TANG, ZOU X. **Multiple images encryption based on Fourier transform hologram.** Opt. Commun. 2012;285:1023-8.
- [20] Y. QIN, Q. GONG **Multiple image encryption in an interference based scheme by lateral shift multiplexing.** Opt. Commun. 2014;315:220-5.
- [21] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Multiplexing three-dimensional optically encrypted data.** Laser Sci. 2016;JW4A-45.
- [22] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Three-dimensional joint transform correlator cryptosystem.** Opt. Lett. 2016;41:599-602.
- [23] J.A. JARAMILLO-OSORIO, S. MONTOYA, J.F. BARRERA-RAMÍREZ, A. VELEZ-ZEA, R. TORROBA, A. MIRA-AGUDELO. **Experimental noise-free information recovery via reference beam encryption.** Act. Photonic Platforms X, SPIE 10721 2018;10721E.
- [24] X. SHI, D. ZHAO, Y. HUANG. **Double images hiding by using joint transform correlator architecture adopting two-step phase-shifting digital holography.** Opt. Commun. 2013;297:32-7.
- [25] G. SITU, J. ZHANG. **Double random-phase encoding in the Fresnel domain.** Opt. Lett. 2014;29:1584-6.
- [26] H.M. OZAKTAS, D. MENDLOVIC. **Fractional Fourier transforms and their optical implementation.** J. Opt. Soc. Am. A 1993;10:1875-81.
- [27] J.M. VILLARDY, Y. TORRES, M.S. MILLAN, E. PÉREZ-CABRÉ. **Nonlinear optical security system based on a joint transform correlator in the Fresnel domain.** App. Opt. 2014;53:1674-85.
- [28] S.K. RAJPUT, N.K. NISHCHAL. **Image encryption and authentication verification using fractional nonconventional joint transform correlator.** Opt. Lasers Eng. 2012;50:1474-83.

- [29] J.A. JARAMILLO, J.F. BARRERA-RAMÍREZ, A. VÉLEZ, R. TORROBA **Fractional optical cryptographic protocol for data containers in a noise-free multiuser environment.** *Opt. Lasers Eng.* 2018;102:119-25.
- [30] J.A. JARAMILLO-OSORIO, W. TORRES-SEPÚLVEDA, A. VELEZ-ZEA, A. MIRA-AGUDELO, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Focus-tunable experimental optical cryptosystem.** *Opt. Lasers Eng.* 2021;107689.
- [31] X. LIU, J. WU, W. HE, M. LIAO, C. ZHANG, X. PENG. **Vulnerability to ciphertext-only attack of optical encryption scheme based on double random phase encoding.** *Opt. Express.* 2015;23:18955-68.
- [32] Z.J. HUANG, S. CHENG, L.H. GONG, N.R. ZHOU. **Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform.** *Opt. Lasers Eng.* 2020;124:105821.
- [33] O. WATANABE, A. UCHIDA, T. FUKUHARA, H. KIYA. **An Encryption then compression system for JPEG 2000 standard.** *IEEE International Conference on Acoustics.* 2015;1226–30.
- [34] H. DI, K. ZHENG, X. ZHANG, E.Y. LAM, T. KIM, Y.S. KIM, T.C. POON, C. ZHOU. **Multiple-image encryption by compressive holography.** *Appl. Opt.* 2012;51:1000–9.
- [35] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Innovative speckle noise reduction procedure in optical encryption.** *J. Opt.* 2017;19:055704.
- [36] J.M. VILARDY, M.S. MILLÁN, E. PÉREZ-CABRÉ. **Improved decryption quality and security of a joint transform correlator-based encryption system.** *J. Opt.* 2013;15:025401.
- [37] J.F. BARRERA-RAMÍREZ, A. MIRA-AGUDELO, R. TORROBA. **Optical encryption and QR codes: Secure and noise-free information retrieval.** *Opt. Express.* 2013;21:5373–8.

- [38] J.F. BARRERA-RAMÍREZ, A. MIRA-AGUDELO, R. TORROBA. **Experimental QR code optical encryption: noise-free data recovering.** *Opt. Lett.* 2014;39:3074–7.
- [39] Y. QIN, H. WANG, Z. WANG, Q. GONG, WANG D. **Encryption of QR code and grayscale image in interference based scheme with high quality retrieval and silhouette problem removal.** *Opt. Lasers Eng.* 2016;84:62-73.
- [40] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Customized data container for improved performance in optical cryptosystems.** *J. Opt.* 2016;18:125702.
- [41] P.A. CHEREMKHIN, V.V. KRASNOV, V.G. RODIN, R.S. STARIKOV. **QR code optical encryption using spatially incoherent illumination.** *Laser Phys. Lett.* 2017;14:026202.
- [42] S. JIAO, W. ZOU, X. LI. **QR code based noise-free optical encryption and decryption of a gray scale image.** *Opt. Commun.* 2017;387:235-40.
- [43] M. BLUM, M. BÜELER, C. GRÄTZEL, M. ASCHWANDEN. **Compact optical design solutions using focus tunable lenses.** *Opt. Des. Eng. IV.* 2011;8167:81670W.
- [44] I. GRULKOWSKI, S. MANZANERA, L. CWIKLINSKI, F. SOBCZUK, K. KARNOWSKI, P. ARTAL. **Swept source optical coherence tomography and tunable lens technology for comprehensive imaging and biometry of the whole eye.** *Optica.* 2018;5:52–9.
- [45] Z. WANG, W. QU, F. YANG, A. TIAN, A. ASUNDI. **Absolute measurement of aspheric lens with electrically tunable lens in digital holography.** *Opt. Lasers Eng.* 2017;88:313-8.
- [46] E. RUEDA, J.H. SERNA, A. HAMAD, H. GARCIA. **Two-photon absorption coefficient determination using the differential F-scan technique.** *Opt. Laser Technol.* 2019;119:105584.
- [47] J. SERNA, A. HAMAD, E. RUEDA, H. GARCIA. **Autocorrelation measurement of an ultra-short optical pulse using an electrically focus-tunable lens.** *J. Opt.* 2015;17:105505.

- [48] D.R. SCHIPF, W.C. WANG. **Optical encryption using a liquid phase mask.** OSA Contin. 2018;1:1026–40.
- [49] R. TORRES, P. PELLAT-FINET, Y. TORRES. **Fractional convolution, fractional correlation and their translation invariance properties.** Signal Process. 2010;90:1976–84.
- [50] A. LOHMANN, D. MENDLOVIC. **Fractional joint transform correlator.** Appl. Opt. 1997;36:7402–7.
- [51] G. UNNIKRISHNAN, K.SINGH. **Double random fractional Fourier-domain encoding for optical security.** Opt. Eng. 2000;39:2853–9.
- [52] G. UNNIKRISHNAN, K.SINGH. **Optical encryption using quadratic phase systems.** Opt. Commun. 2001;193:51–7.
- [53] **Optotune. Electrically tunable large aperture lens EL-16-40-TC-VIS-20D.** 2016:1–9.
- [54] J.F. BARRERA-RAMÍREZ, S. TREJOS, M. TEBALDI, R. TORROBA. **Experimental protocol for packaging and encrypting multiple data.** J. Opt. 2013;15:055406.
- [55] J.W GOODMAN. **Introduction to Fourier Optics.** McGraw-Hill. 1996; 2nd edition.
- [56] G. UNNIKRISHNAN, J. JOSEPH, K. SINGH. **Optical encryption system that uses phase conjugation in a photo refractive crystal.** Appl. Opt. 1998;37:8181-6.
- [57] N. SUCHKOV, E.J. FERNÁNDEZ, P. ARTAL. **Wide-range adaptive optics visual simulator with a tunable lens.** J. Opt. Soc. Am. 2019;A36:722–30.
- [58] W. TORRES-SEPÚLVEDA, J. HENAO, J. MORALES-MARÍN, A. MIRA-AGUDELO, E. RUEDA. **Hysteresis characterization of an electrically focus-tunable lens.** Opt. Eng. 2020;59:044103.
- [59] W. TORRES-SEPÚLVEDA, A. MIRA-AGUDELO, J.F. BARRERA-RAMÍREZ, K. PETELCZYK, A. KOŁODZIEJCZYK. **Optimization of the light sword lens for presbyopia correction.** Transl. Vis. Sci. Technol. 2020;9:6.

- [60] D. LU, W. JIN. **Color image encryption based on joint fractional Fourier transform correlator.** Opt. Eng. 2011;50:068201.
- [61] Q.U. WANG, Q. GUO, L. LEI, J. ZHOU. **Optical image encryption based on joint fractional transform correlator architecture and digital holography.** Opt. Eng. 2013;52:048201.

Capítulo 4

Encriptación óptica usando modulación de fase a partir del efecto lente térmica

En la mayoría de los sistemas ópticos de encriptación tipo DRPE (siglas en inglés de: doble random phase encoding) que se han implementado de manera experimental, el haz que ilumina el plano de entrada corresponde a una onda plana, y para aumentar la versatilidad y la seguridad del sistema se introducen modificaciones entre el plano de entrada y el plano de salida. Aunque estas modificaciones han permitido aumentar la seguridad y capacidad de estos sistemas [1–4], otro tipo de modificación, menos explorada, es la inclusión de mecanismos que permitan modificar la iluminación sobre el plano de entrada. Se han reportado algunos trabajos en los cuales se ilumina el plano de entrada con un haz divergente [5] o con un frente de onda esférico convergente [6]. A pesar del prometedor concepto detrás de estas investigaciones, los cambios introducidos hasta ahora solo se limitan a modificaciones en la vergencia del haz de iluminación [5, 6], y en algunos casos su demostración solo se realiza a partir de simulaciones computacionales [6]. Los resultados presentes en estos trabajos permiten inferir que modificaciones más complejas sobre el haz de iluminación que incide sobre

el plano de entrada podrían incrementar la protección que brinda el sistema de codificación óptica.

En particular, una alternativa que permitiría la modulación de la fase de la onda que ilumina el plano de entrada es el efecto lente térmica (ELT), reportado por primera vez por Gordon *et al.* [7]. Inicialmente, los experimentos relacionados con el ELT se realizaban en las cavidades de los láseres. Después, utilizando un solo láser, los experimentos se llevaron a cabo por fuera de cavidades [8]. Posteriormente, se desarrollaron sistemas que utilizaban dos fuentes de iluminación láser, una de mayor potencia, conocida como láser de excitación (LE), que tiene como objetivo generar la lente térmica y otro de mucha menor potencia, conocido como láser de prueba (LP), en el cual se ven reflejados los efectos de la lente térmica. El proceso de interacción foto-térmica, base fundamental del funcionamiento del ELT, se puede modelar en cuatro etapas básicas [9]: a) absorción de la radiación óptica, en esta etapa una muestra recibe la radiación proveniente del LE; b) conversión de la energía óptica, proveniente del LE, en energía térmica; c) difusión del calor en la muestra para formar el gradiente de temperatura y d) la influencia del elemento termo-óptico, en este caso la lente térmica (LT), sobre el LP transmitido a través de la muestra. El ELT ha sido ampliamente utilizado en espectrometría para mediciones de absorción altamente sensibles [10, 11], medición de los espectros de absorción de etanol y agua [12], detección de bilirrubina libre en células endoteliales vasculares [13], identificación espectral, caracterización cuantitativa y formación de imágenes de proteínas celulares y orgánulos en células vivas [14], determinación de tóxicos como el Cr (VI) [15], y más recientemente en nano-análisis electroforético en línea [16]. Aunque hasta ahora no se ha utilizado el ELT en el área de la encriptación óptica de información, la modulación que genera el ELT sobre un LP permite modificar el haz que ilumina el plano de entrada de los sistemas de encriptación. Esta modificación depende de los parámetros experimentales involucrados en la generación de la LT, que en conjunto con los parámetros propios de los montajes de encriptación pueden ser usados para mejorar el desempeño de los sistema de codificación óptica.

Teniendo en cuenta lo anterior, en este capítulo se presenta un sistema de encriptación tipo JTC (siglas en ingles de: joint transform correlator) en el dominio óptico de Fresnel o

JFSC (siglas en ingles de: joint free space cryptosystem) [3, 17], donde el plano de entrada es iluminado por un frente de onda modificado por el ELT. En este caso se emplea el sistema JFSC, donde el proceso de encriptación se lleva a cabo sin la necesidad de una lente transformadora.

Con el objetivo de corroborar los efectos que introduce el ELT en el funcionamiento básico del sistema de codificación, se lleva a cabo el proceso de encriptación y recuperación de un objeto. Posteriormente, se analiza la tolerancia que presenta el esquema a la recuperación utilizando claves de encriptación registradas para diferentes modulaciones de ELT. Dichas modulaciones de fase son obtenidas llevando a cabo desplazamientos axiales de la muestra en el esquema experimental, lo que conlleva a que el LE se enfoque en puntos diferentes de la muestra y de esta manera se genere un cambio de fase diferente para cada posición de la muestra. Posteriormente, considerando los cambios de modulación de fase en la iluminación debido a desplazamientos de la muestra, se propone un procedimiento de encubrimiento para proteger información a partir de la encriptación de un dato señuelo. Finalmente, se analiza la resistencia del dato encriptado bajo el procedimiento de encubrimiento contra algunos de los ataques más comunes reportados en la literatura.

Los resultados teóricos y experimentales que se presentan a continuación fueron publicados en revista internacional como producto de investigación del trabajo de doctorado y demuestran la viabilidad, aplicabilidad y versatilidad del sistema propuesto [18].

4.1. Modulación de la fase debido al efecto lente térmica

La generación del efecto lente térmica (ELT) está basado en la excitación de una muestra con un láser de excitación (LE). Por otro lado, el fenómeno producido por el ELT es observado sobre un láser de prueba (LP) que ilumina la muestra excitada. En el esquema que se presenta

en la Fig.4.1, tanto el LP como el LE son colimados y enfocados en la muestra. Inicialmente, ambos haces son enfocados sobre la misma región de la muestra, debido a esto se logra la máxima modulación de fase sobre el LP. Los cambios de fase generados sobre el LP pueden ser modificados cambiando la posición de la lente L_2 , y por ende enfocando el LP en una región diferente respecto al LE.

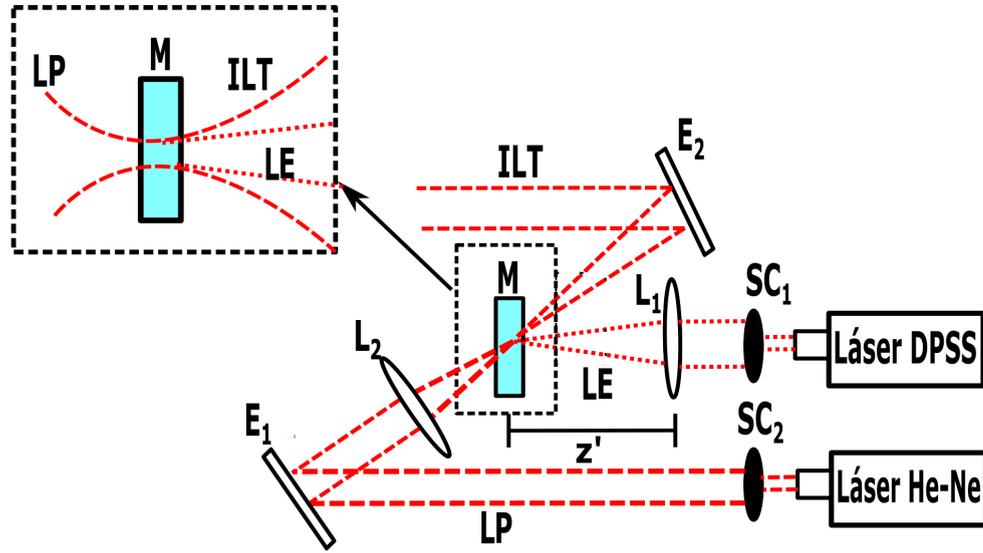


Figura 4.1: Generación del efecto lente térmica. M: muestra, SC: sistema de colimación, LP: láser de prueba, LE: láser de excitación, ILT: iluminación de lente térmica, L: lente, E: espejo y z' : distancia de propagación entre L_1 y M.

La modulación de fase introducida por el ELT sobre el LP depende de la posición de la muestra y el radio del LP, y en el estado estacionario vienen dada por [19],

$$h(r, z') = -\frac{\Phi_0}{2} \left[\log \left(\frac{2r^2}{\omega_e^2(z')} \right) + \Gamma \left(\frac{2r^2}{\omega_e^2(z')} \right) + \gamma \right] \quad (4.1)$$

donde,

$$\Phi_0 = \frac{P_e \alpha l (\partial n / \partial T)}{\kappa \lambda_p} \quad (4.2)$$

$$\omega_e(z') = \omega_{e,0} \sqrt{1 + (z' - a_e)^2 / z_e^2} \quad (4.3)$$

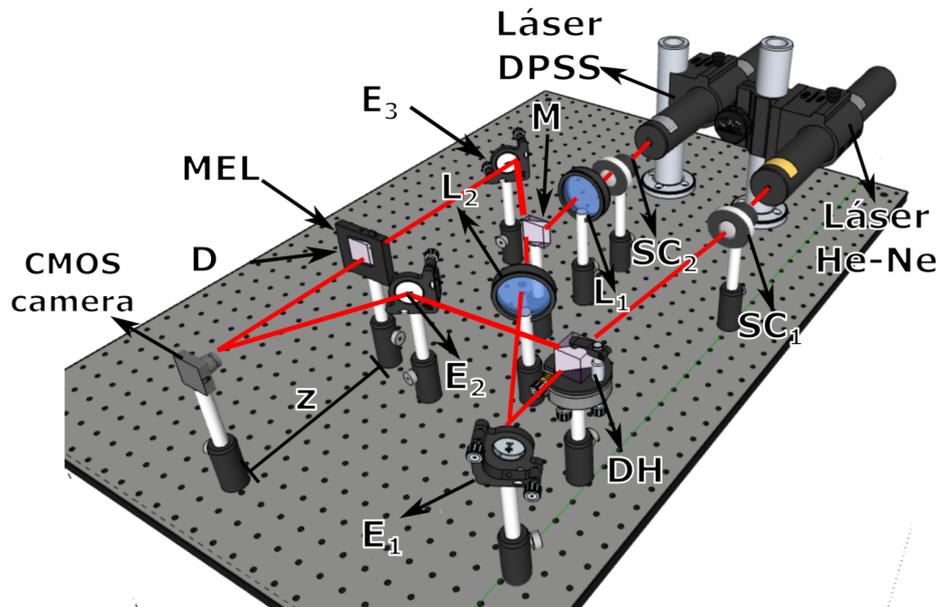
$$\omega_{e,0} = \sqrt{\frac{\lambda_e z_e}{\pi}} \quad (4.4)$$

P_e es la potencia del LE, z' es la distancia entre L_1 y la muestra, r es la coordenada longitudinal, a_e es el radio de la cintura del LE sobre la muestra, $\Gamma(r, z')$ es la función gamma, $\gamma = 0,577$ es la constante gamma de Euler, α es el coeficiente de absorción de la muestra, κ es la conductividad térmica de la muestra, l es el ancho de la muestra, λ_p y λ_e son las longitudes de onda de LP y LE, respectivamente. $\partial n / \partial T$ es el coeficiente de temperatura del índice de refracción de la muestra, z_e es la parámetro de Rayleigh para el LE y $\omega_{e,0}$ es la cintura del láser de excitación a una distancia z_e .

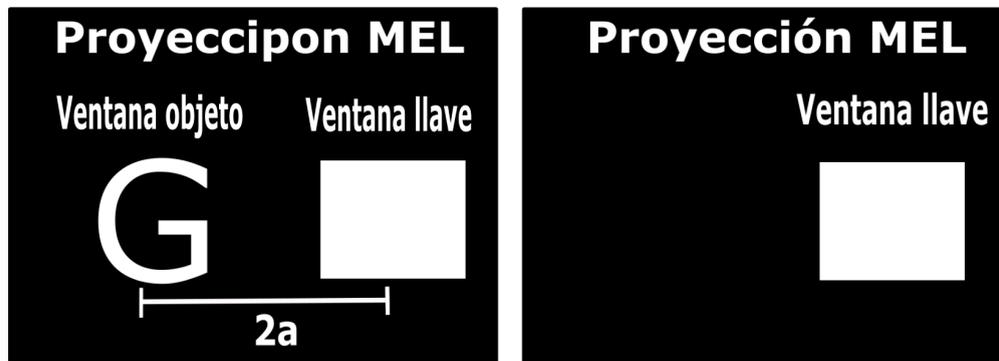
Teniendo en cuenta lo anterior, en este capítulo se presenta un sistema de encriptación en el dominio óptico de Fresnel, en el cual se ilumina el plano de entrada con la ILT que se obtiene a partir del sistema mostrado en la Fig. 4.1. Como se puede notar en la Ec. 4.1, la modulación de fase debido al ELT involucra parámetros como la potencia del LE, el radio del haz de excitación en la muestra y la posición de la muestra. Los desarrollos experimentales presentes a continuación se enfocarán en el estudio de la posición de la muestra como parámetro extra de seguridad.

4.3. Proceso de encriptación en el sistema JFSC usando ELT

En primer lugar, se implementa un sistema óptico que permita generar la iluminación modulada bajo el ELT (Fig.4.1). El haz modulada por el ELT es usado para iluminar el plano de entrada del sistema JFSC (Fig.4.2). El esquema experimental del sistema de encriptación en el dominio óptico de Fresnel usando modulación de luz a partir del ELT es mostrado en la Fig.4.3.



(a)



(b)

(c)

Figura 4.3: a) Esquema experimental del sistema de encriptación en el dominio óptico de Fresnel usando modulación de luz a partir del ELT. Proyección en el MEL para el registro de: (a) el dato encriptado y (c) la llave de encriptación. D: difusor, z : distancia entre el plano de entrada y el plano de salida, MEL: modulador espacial de luz, $2a$: separación entre las ventanas objeto y llave, SC: sistema de colimación, L: lente, E: espejo y DH: divisor de haz.

Para llevar a cabo el proceso de encriptación se proyecta en el plano de entrada las ventanas llave y objeto, separadas una distancia $2a$ (ver Fig.4.3)(b)). Durante este proceso, el haz de referencia que llega a la cámara CMOS desde el espejo E_2 es bloqueado. De acuerdo con la configuración experimental, la función transmitancia en el plano de entrada del sistema se puede escribir como,

$$u(x, y) = c(x, y) \otimes \delta(x - a, y) + l(x, y) \otimes \delta(x + a, y) \quad (4.5)$$

aquí $c(x, y) = h_1(x, y)o(x, y)r(x, y)$, donde $o(x, y)$ es el objeto a encriptar, $r(x, y)$ es la MAF en contacto con el objeto y $h_1(x, y)$ es la porción de la onda modulada por el ELT que incide sobre el objeto. Por otra parte $l(x, y) = h_2(x, y)m(x, y)$, representa la llave de encriptación o llave de seguridad, donde $m(x, y)$ es otra MAF generada por el área del difusor en contacto con la ventana llave y $h_2(x, y)$ es la porción de la onda modulada por el ELT que incide sobre la llave. $2a$ es la separación espacial entre las ventanas objeto y llave en el plano de entrada, \otimes es el operador convolución y δ es la función delta de Dirac.

En el plano de la cámara CMOS se registra el JFrPD, dado por [3],

$$\begin{aligned} I_{JFrPD}(\nu, \omega) &= |C_z(\nu, \omega)|^2 + |L_z(\nu, \omega)|^2 \\ &+ C_z(\nu, \omega)L_z^*(\nu, \omega)e^{-4i\pi a\nu} + C_z^*(\nu, \omega)L_z(\nu, \omega)e^{4i\pi a\nu} \end{aligned} \quad (4.6)$$

donde $C_z(\nu, \omega)$ y $L_z(\nu, \omega)$ son las transformadas de Fresnel de $c(x, y)$ y $l(x, y)$ para una distancia z , respectivamente. $\nu = \frac{x}{\lambda z}$ y $\omega = \frac{y}{\lambda z}$ son las coordenadas en el plano de Fresnel, y λ es la longitud de onda de la luz incidente. El tercer y cuarto término en la Ec.4.6 son el dato encriptado y su complejo conjugado respectivamente, mientras que el primer y segundo término corresponden al orden central, el cual debe ser filtrado para evitar ataques [20]. Llevando a cabo un proceso de filtrado igual al presentado en la Sección 2.4.2, se extrae el dato encriptado,

$$e_z(\nu, \omega) = C_z(\nu, \omega)L_z^*(\nu, \omega)e^{2\pi i(\nu x' + \omega y')} \quad (4.7)$$

(x', y') son las coordenadas de posicionamiento del dato encriptado. Se puede notar que en esta arquitectura de encriptación la función que representa el dato encriptada dependen de la distancia z , este hecho permite establecer que la distancia entre planos debe ser considerada al momento de realizar el proceso de recuperación [3]. Se debe destacar que, para llevar a cabo el proceso de desencriptación de manera exitosa, es necesario mantener la modulación de fase debido al ELT inalterada para el registro tanto del JFrPD como de la información de la llave.

4.4. Registro del holograma de la llave

El registro de la información de la llave de encriptación, requiere del mismo sistema mostrado en la Fig. 4.3, manteniendo la misma modulación de fase generada por ELT usada para el registro del JFrPD. En este caso, se proyecta únicamente la ventana llave en el MEL (Fig. 4.3 (c)), de este modo en el plano de la cámara se registra el patrón de interferencia entre la onda plana de referencia de amplitud unitaria y la intensidad de la transformada de Fresnel (TFr) del campo proveniente de la ventana llave. De esta manera, el holograma resultante viene dado por

$$H(\nu, \omega) = |1|^2 + |L_z(\nu, \omega)|^2 + L_z(\nu, \omega)e^{4\pi i a u} + L_z^*(\nu, \omega)e^{-4\pi i a u} \quad (4.8)$$

ahora, realizando un proceso de filtrado sobre la información presente en la Ec. 4.8, como el mostrado en la Sección 2.4.2, se obtiene la información de la llave de recuperación.

$$K(\nu, \omega) = L_z(\nu, \omega) \quad (4.9)$$

4.5. Proceso de desencriptación

Para realizar de manera exitosa el proceso de recuperación se debe multiplicar el dato encriptado (Ec. 4.7) por la información de la TFr de la llave (Ec. 4.9). Cuando ambos datos son reposicionados en el origen de coordenadas, su producto toma la forma,

$$E'(\nu, \omega) = C_z(\nu, \omega)L_z^*(\nu, \omega)L_z(\nu, \omega) \quad (4.10)$$

posteriormente, realizando una transformada de Fresnel inversa (TFrI) para una distancia z sobre la Ec. 4.10, se obtiene el dato recuperado,

$$d(x, y) = [h_1(x, y)o(x, y)r(x, y)] \otimes [\{h_2(x, y)m(x, y)\}^* \otimes \{h_2(x, y)m(x, y)\}] \quad (4.11)$$

El dato encriptado presenta un ruido multiplicativo debido a la modulación de fase causada por el ELT ($h_1(x, y)$) y un ruido convolutivo debido a la autocorrelación de $s(x, y) = h_2(x, y)m(x, y)$ que presenta un pico central y una nube de ruido de baja intensidad que recibe el nombre de ruido aleatorio de correlación o RCN (siglas en inglés de: random correlation noise) [21]. Debido a que $\{h_2(x, y)m(x, y)\}^* \otimes \{h_2(x, y)m(x, y)\} \approx 1$ [22], es posible reconocer el dato desencriptado, el cual corresponde a la distribución de intensidad del campo óptico representado por la Ec. 4.11.

4.6. Resultados experimentales

Los resultados experimentales que se exponen a continuación fueron obtenidos con el sistema mostrado en la Fig. 4.3. Como medio de registro se empleó una cámara CMOS EO-10012M, con una resolución de 3840 x 2748 pixeles y un tamaño de pixel de $1,67 \mu m$ x $1,67 \mu m$. El láser de prueba (LP) fue un láser He-Ne con una longitud de onda de $\lambda = 632 \text{ nm}$ y una potencia de 20 mW , el haz de excitación (LE) fue un láser DPSS con una longitud de onda $\lambda = 532 \text{ nm}$ y una potencia máxima de 100 mW . El tamaño de las ventanas objeto y llave fue de $3,2 \text{ mm}$ x $3,2 \text{ mm}$, con una separación entre ambas ventanas de $3,87 \text{ mm}$. El plano de entrada fue proyectado en un MEL Holoeye 2002 con tamaño de pixel de $32 \mu m$ x $32 \mu m$ y una resolución de 800 x 600 pixeles. La muestra utilizada fue una mezcla de etanol y azul de metilo, depositada en una celda de vidrio con un camino óptico de 2 mm . Se empleó una lente convexa (L_1) de longitud focal de 20 cm para enfocar el LE sobre la muestra. Por otro lado, el LP fue enfocando con un lente convexa (L_2) con una longitud focal de 15 cm .

4.6.1. Procesos de encriptación y recuperación

Con el propósito de analizar el desempeño básico del sistema JFSC basado en la modulación de fase a partir del ELT, se realizó el proceso de encriptación y desencriptación de un objeto. La Fig. 4.4 muestra el resultado experimental de este proceso.

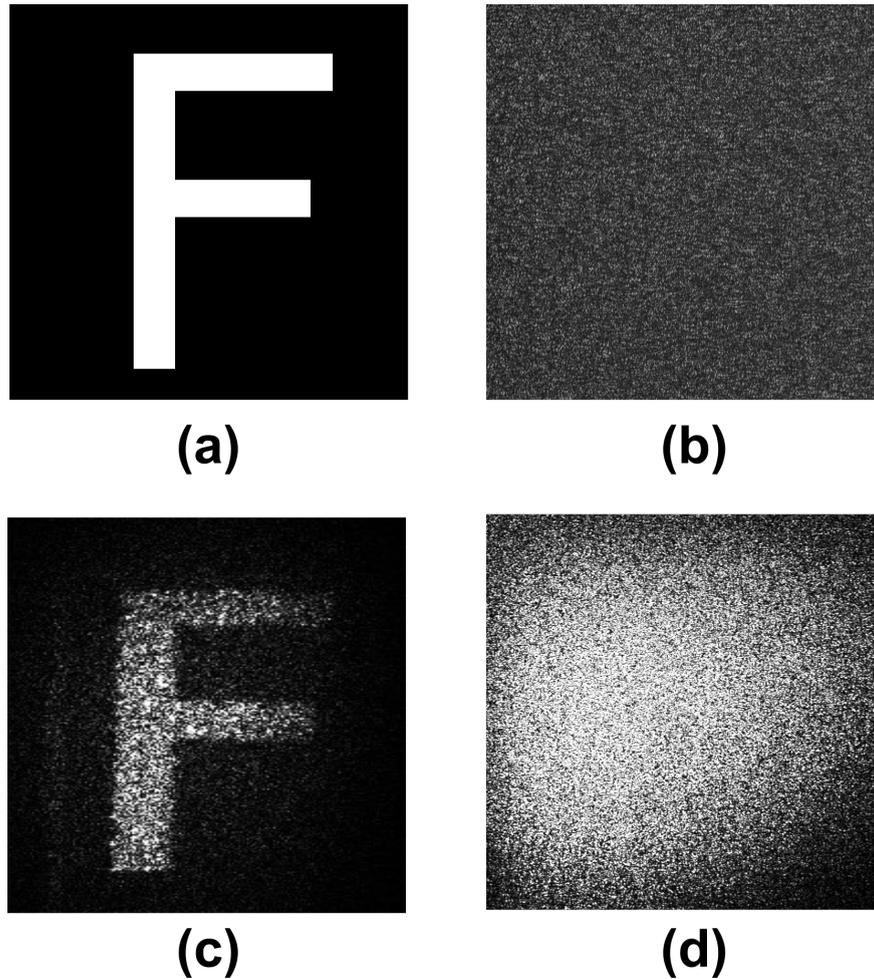


Figura 4.4: Resultado experimental del proceso de encriptación y recuperación de un objeto en el sistema JFSC con ELT, a) dato original (letra F), b) dato encriptado, c) objeto recuperado con la llave correcta y d) objeto recuperado con una llave incorrecta.

El objeto a encriptar (Fig. 4.4(a)) es proyectado en el MEL, por lo tanto en la cámara CMOS se registra el JFrPD, del cual se extrae el dato encriptado (Fig. 4.4(b)); después de llevar a cabo el proceso de recuperación, con la llave correcta, se obtiene el resultado que se muestra en la Fig. 4.4(c). El dato recuperado contiene ruido multiplicativo y el RCN, pero aún así es posible reconocer la información recuperada (Fig. 4.4(c)). Por otro lado, cuando el proceso de recuperación se lleva a cabo con una llave incorrecta, el resultado es un patrón de ruido como se puede apreciar en la Fig. 4.4(d). Los resultados presentados en la Fig. 4.4 demuestran la efectividad que posee el sistema de encriptación óptica en el dominio de Fresnel bajo la modulación de fase generada por ELT para la protección de datos.

Teniendo presente que la modulación de fase ($h(x, y)$) debido al ELT cambia con el desplazamiento axial de la muestra dentro del esquema experimental, se realizó un estudio con el propósito de establecer el mínimo desplazamiento de la muestra dentro del esquema para obtener una llave diferente, sin la necesidad de cambiar la máscara aleatoria de fase $m(x, y)$. En este caso, se llevó a cabo el proceso de encriptación de un dato con su respectiva llave para una posición determinada de la muestra; de esta forma se estableció la posición de referencia para la muestra. Posteriormente, se registraron llaves de recuperación para desplazamientos axiales de la muestra en un rango de -2 mm y 2 mm en pasos de $0,04 \text{ mm}$ alrededor del punto de referencia. Después del registro de las llaves, se realizó el proceso de recuperación del dato registrado en la posición de referencia con las llaves registradas para diferentes posiciones de la muestra. Para determinar la calidad en la recuperación, se empleó la métrica del coeficiente de correlación entre el dato recuperado en la posición de referencia con la llave correcta y el mismo dato pero recuperado con las llaves registradas en posiciones alrededor del punto de referencia (ver Fig. 4.5). Se debe destacar que para el registro de las llaves alrededor del punto de referencia las ventanas objeto y llave, la distancia entre planos z permanecieron fijas y solo se modificó la posición de la muestra en el esquema experimental de iluminación.

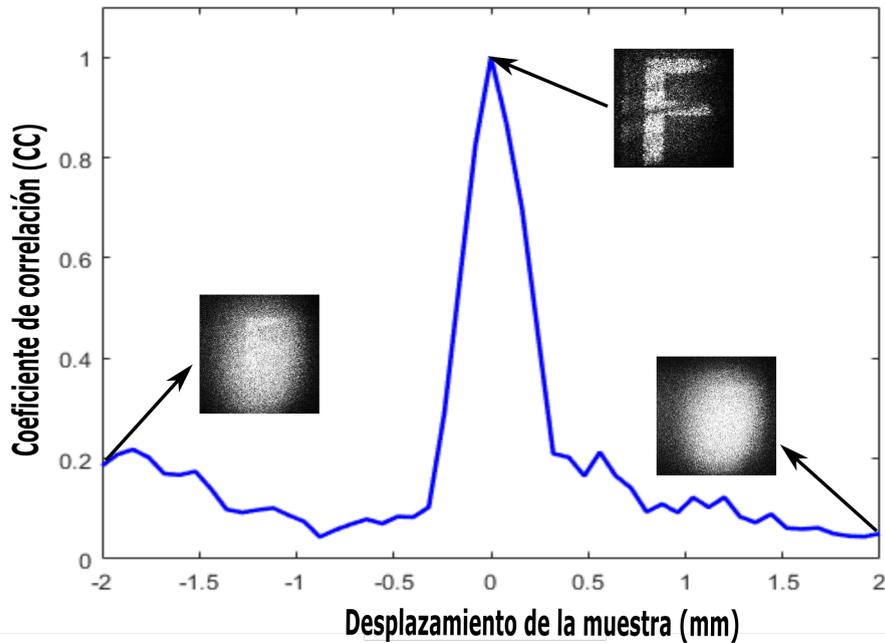


Figura 4.5: Coeficiente de correlación experimental (CC) entre el objeto descifrado con la muestra en el punto de referencia y el objeto recuperado con llaves de recuperación registradas para diferentes desplazamientos axiales de la muestra.

Como se observa en el resultado experimental de la Fig. 4.5, los datos recuperados presentan la mejor calidad cuando el objeto se recupera con la llave de recuperación registrada en la posición de referencia ($z' = 0 \text{ mm}$); por el contrario, cuando el proceso de recuperación es llevado a cabo con llaves registradas para un desplazamiento axial de la muestra superior a $\pm 0,25 \text{ mm}$ alrededor de la posición de referencia, la calidad de los datos recuperados disminuye sustancialmente. Estos resultados permiten establecer la tolerancia a la descifrado bajo diferentes condiciones de iluminación modulada por ELT, se debe resaltar que, cuando la muestra se aleja de la posición de referencia $z' = 0 \text{ mm}$, el punto de enfoque de la LP comienza a situarse fuera del radio del LE, lo que provoca un cambio en la modulación de fase inducida por el ETL en el haz de iluminación, esto a su vez provoca un cambio en la llave de recuperación registrada. Debido a esto, la información de la llave registrada en $z' = 2 \text{ mm}$ es diferente a la información de la llave registrada en la posición de referencia ($z' = 0 \text{ mm}$). Por lo tanto, al intentar recuperar un objeto encriptado con la muestra en la posición de referencia ($z' = 0 \text{ mm}$) utilizando una llave registrada para $z' = 2 \text{ mm}$, el proceso de

recuperación no tiene éxito y la información permanece encriptada.

4.6.2. Proceso de encubrimiento de información

Como se puede observar en los resultados mostrados en la Sección 4.6.1, es posible obtener dos llaves diferentes mediante desplazamientos axiales de la muestra; teniendo presente esta característica del sistema y con el fin de mejorar la seguridad sobre los datos procesados, se establece un protocolo de encubrimiento. En general, el objetivo de este procedimiento es engañar o disuadir a un atacante brindándole información sin valor (información señuelo) que él interpreta como información valiosa; mientras que la información relevante permanece encriptada. En este tipo de protocolos el atacante accede al multiplexado del dato valioso encriptado y del dato señuelo encriptado, y a la llave de recuperación del dato señuelo; con esta información el atacante obtiene la información del dato señuelo y cesa el ataque al interpretar que recuperó la información valiosa. Por otro lado, para acceder a la información valiosa, un usuario autorizado debe, además de tener el multiplexado de los datos encriptados y la llave correspondiente a la información valiosa, conocer el protocolo de encubrimiento y los parámetros extras usados en el proceso de encriptación que le permitan llevar a cabo el proceso de recuperación de forma exitosa.

En este caso, para llevar a cabo el procedimiento encubrimiento, se realiza el cifrado óptico de dos objetos $o_r(x, y)$ y $o_s(x, y)$ para dos posiciones diferentes de la muestra dentro del esquema experimental, en este caso 0 mm y 2 mm respectivamente. $o_r(x, y)$ representa la información valiosa (información relevante), mientras que $o_s(x, y)$ representa la información señuelo (información con la cual se desea engañar al atacante). De acuerdo con lo anterior, los datos encriptados asociados a $o_r(x, y)$ y $o_s(x, y)$ son $e_r(u, v) = G_{r,z}(u, v)L_{r,z}^*(u, v)$ y $e_s(u, v) = G_{s,z}(u, v)L_{s,z}^*(u, v)$, respectivamente. Para dar inicio al proceso de encubrimiento, se multiplica el dato encriptado $e_r(u, v)$ por el complejo conjugado de la fase de la llave de encriptación $b^*(u, v)$ usada para su encriptación, así se obtiene $e'_r(u, v) = e_r(u, v)b^*(u, v)$. Después de esto, se multiplexa $e'_r(u, v)$ con la información del dato señuelo encriptado ($e_s(u, v)$). De

esta forma el dato multiplexado viene dado por,

$$M(u, v) = e_r(u, v)b^*(u, v) + e_s(u, v) \quad (4.12)$$

después del proceso de multiplexado bajo el protocolo de encubrimiento se pueden presentar tres posibles casos para la recuperación de la información: (a) un usuario no autorizado realiza el proceso de recuperación con la llave asociada al dato señuelo, (b) un usuario no autorizado realiza el proceso de recuperación con la llave asociada a la información valiosa y (c) un usuario autorizado realiza el proceso de recuperación con la llave asociada a la información valiosa y con el conocimiento del protocolo encubrimiento. A continuación se detallan los tres casos.

Caso 1: un usuario no autorizado realiza el proceso de recuperación con la llave asociada al dato señuelo

Si un usuario con la llave asociada al dato señuelo $L_{s,z}(u, v)$ intenta acceder a la información realizando el proceso de recuperación; al multiplicar la Ec. 4.12 por la llave señuelo ($L_{s,z}(u, v)$) y posteriormente realizar una TFrI, obtendrá

$$\begin{aligned} C(x, y) &= \{h_{1r}(x, y)o_r(x, y)r_t(x, y)\} \otimes TFrI \{b^*(u, v)\} \\ &\otimes \{[h_{2r}(x, y)m(x, y)]^* \otimes [h_{2s}(x, y)m(x, y)]\} \\ &+ \{h_{1s}(x, y)o_s(x, y)r_s(x, y)\} \\ &\otimes \{[h_{2s}(x, y)m(x, y)]^* \otimes [h_{2s}(x, y)m(x, y)]\} \end{aligned} \quad (4.13)$$

debido a que $[h_{2s}(x, y)m(x, y)]^* \otimes [h_{2s}(x, y)m(x, y)] \approx 1$ [22], después del proceso de

recuperación el intruso accede a la información señuelo (segundo término en la Eq. 4.13), mientras que la información valiosa permanece oculta debido a la convolución entre la función $TFrI \{b^*(u, v)\}$ y la función aleatoria $\{[h_{2r}(x, y)m(x, y)]^* \otimes [h_{2s}(x, y)m(x, y)]\}$. Además, ya que el ruido generado por la información no recuperada se encuentra en la misma posición en la cual se obtienen el dato señuelo, no será posible identificar que existe una información extra asociada a la información relevante contenida en el paquete.

Caso 2: un usuario no autorizado realiza el proceso de recuperación con la llave asociada a la información valiosa

Si un usuario no autorizado con la información de la llave asociada a la información valiosa ($L_{r,z}(u, v)$) lleva a cabo el proceso de recuperación obtendrá,

$$\begin{aligned}
C(x, y) &= \{h_{1r}(x, y)o_r(x, y)r_t(x, y)\} \otimes TFrI \{b^*(u, v)\} \\
&\otimes \{[h_{2r}(x, y)m(x, y)]^* \otimes [h_{2r}(x, y)m(x, y)]\} \\
&+ \{h_{1s}(x, y)o_s(x, y)r_s(x, y)\} \\
&\otimes \{[h_{2s}(x, y)m(x, y)]^* \otimes [h_{2r}(x, y)m(x, y)]\}
\end{aligned} \tag{4.14}$$

En este caso, la presencia de la función $TFrI \{b^*(u, v)\}$ en el primer término y la convolución de $\{[h_{2s}(x, y)m(x, y)]^* \otimes [h_{2r}(x, y)m(x, y)]\}$ en el segundo, generan un patrón de ruido evitando que se recupera cualquiera de los datos dentro del paquete. De acuerdo con lo anterior, incluso con la información de la llave asociada a la información valiosa y el multiplexado no es posible acceder al dato con la información relevante. El resultado anterior podría disuadir a un atacante, llevándolo a concluir que la llave usada no es la correcta.

Caso 3: un usuario autorizado con la llave correcta y con el conocimiento del protocolo de encubrimiento recupera la información original

Para llevar a cabo el proceso de recuperación de forma exitosa, primero se debe extraer la función de fase $b(u, v)$ de la llave de encriptación asociada a la información valiosa $o_r(x, y)$. Posteriormente, se debe multiplicar el término $TFrI \{b^*(u, v)\}$ por $M(u, v)$,

$$M'(u, v) = e_r(u, v)b^*(u, v)b(u, v) + e_s(u, v)b(u, v) \quad (4.15)$$

Teniendo presente que $b^*(u, v)b(u, v) = 1$, debido a que es una función de fase pura,

$$M'(u, v) = e_r(u, v) + e_s(u, v)b(u, v) \quad (4.16)$$

Posteriormente, multiplicado por $L_{r,z}(u, v)$ y realizando el proceso de recuperación, se obtiene,

$$\begin{aligned} C(x, y) &= \{h_{1r}(x, y)o_r(x, y)r_t(x, y)\} \\ &\otimes \{[h_{2r}(x, y)m(x, y)]^* \otimes [h_{2r}(x, y)m(x, y)]\} \\ &+ \{h_{1s}(x, y)o_s(x, y)r_s(x, y)\} \otimes TFrI \{b(u, v)\} \\ &\otimes \{[h_{2s}(x, y)m(x, y)]^* \otimes [h_{2r}(x, y)m(x, y)]\} \end{aligned} \quad (4.17)$$

dado que $\{[h_{2r}(x, y)m(x, y)]^* \otimes [h_{2r}(x, y)m(x, y)]\} \approx 1$ [22], se puede establecer que el primer término de la Ec. 4.17 representa la información recuperada asociada al dato $o_r(x, y)$, el cual representa la información relevante. Por otro lado, debido a la convolución entre

$TFrI \{b(u, v)\}$ y la función aleatoria $\{[h_{2s}(x, y)m(x, y)]^* \otimes [h_{2r}(x, y)m(x, y)]\}$, la información asociada al dato señuelo $o_s(x, y)$ permanece encriptada. A pesar del ruido de la información no recuperada asociada al dato señuelo, es posible reconocer la información relevante en el plano de recuperación.

De acuerdo con los tres casos expuestos anteriormente, el protocolo de encubrimiento propuesto en este trabajo permite mejorar significativamente la seguridad en el proceso de transmisión de información. Además, es importante tener en cuenta que la cantidad de datos que se deben enviar para realizar el proceso de recuperación es la misma que se requiere para la recuperación de un solo dato. Como resultado, la eficiencia en el proceso de transmisión y recepción no se ve afectada al momento de la implementación de este proceso.

4.6.3. Resultados experimentales del proceso de encubrimiento

Para demostrar la efectividad del protocolo de encubrimiento, se realizó el proceso descrito anteriormente de manera experimental. En primer lugar se encriptaron dos objetos $o_r(x, y)$ y $o_s(x, y)$, para dos posiciones diferentes de la muestra 0 mm y 2 mm, respectivamente. La información valiosa ($o_r(x, y)$) corresponde al carácter **F** (Fig.4.6(a)), mientras que la información señuelo ($o_s(x, y)$) corresponde al carácter **O** (Fig.4.6(b)). Después del proceso de encriptación de los datos, el dato $e_r(x, y)$, correspondiente al dato encriptado asociado a $o_r(x, y)$, es multiplicado por la función de fase pura extraída del complejo conjugado de la llave de encriptación empleada durante su proceso de codificación. Finalmente, la información resultante del proceso anterior es multiplexada con el dato señuelo encriptado ($e_s(x, y)$).

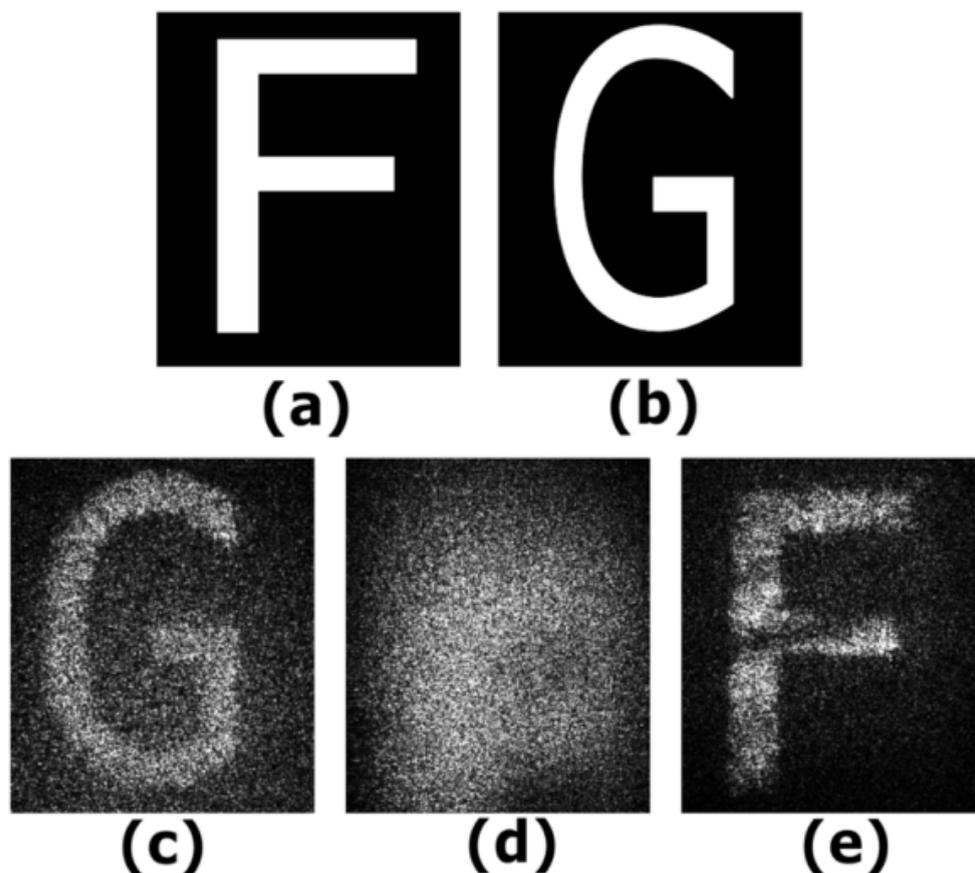


Figura 4.6: Recuperación después de implementar el protocolo de encubrimiento. (a) información valiosa, (b) dato de señuelo, procedimientos de descifrado utilizando: (c) la llave de recuperación asociada al dato señuelo, (d) la llave de recuperación asociada a la información valiosa, y (e) la llave de recuperación asociada a la información valiosa y aplicando correctamente el protocolo encubrimiento.

En la Fig. 4.6 se muestran los tres casos posibles de recuperación. Como se explicó anteriormente, cuando se lleva a cabo el proceso de recuperación con la llave de encriptación asociada al dato señuelo, se recupera la información mostrada en la Fig. 4.6(c). Por otro lado, cuando se realiza el proceso de recuperación usando la información de la llave de recuperación asociada a la dato relevante, la información recuperada corresponde a un patrón de ruido como se muestra en la Fig. 4.6(d). Finalmente, cuando el proceso de descifricación se realiza con la información de la llave de recuperación asociada a la información relevante y usando el protocolo de recuperación, como se describe en la Sección 4.6.2, se recupera la información valiosa (Fig. 4.6(e)). Los resultados expuestos en la Fig. 4.6 demuestran la viabilidad experimental del protocolo de encubrimiento propuesto en este trabajo.

4.6.4. Resistencia a ataques

En general, los sistemas de encriptación pueden estar sometidos a diferentes ataques, entre los ataques más comunes a los sistemas de encriptación de tipo DRPE se encuentra el KPA (siglas en inglés de: known-plaintext attack) [23–29]. En este tipo de ataques se asume que el intruso tiene acceso a uno o más textos planos (objetos) y sus respectivos textos cifrados (objetos encriptados). Por ejemplo, tomando el dato encriptado dado por la ecuación Ec. 4.7, posicionado en $(x' = 0, y' = 0)$

$$\begin{aligned} e_z(\nu, \omega) &= C_z(u, v)L_z^*(u, v) \\ &= [H_{1z}(u, v) \otimes O_z(u, v) \otimes R_z(u, v)]L_z^*(u, v) \end{aligned} \quad (4.18)$$

donde $H_{1z}(u, v)$, $O_z(u, v)$ y $R_z(u, v)$ son las transformadas de Fresnel de $h_{1z}(x, y)$, $o(x, y)$ y $r(x, y)$, respectivamente. Ahora, asumiendo que $L_z^*(u, v)$ es una función de fase pura, entonces la intensidad del dato encriptado Ec. 4.7, viene dada por

$$|e(u, v)|^2 = |TFrI \{h_1(x, y)o(x, y)r(x, y)\}|^2 \quad (4.19)$$

donde $TFrI$ significa transformada de Fresnel inversa. De acuerdo con la Ec. 4.19, si un atacante conoce la información asociada a $o(x, y)$, y dado que el texto plano es una distribución de amplitud, un intruso puede aplicar el algoritmo de Gerchberg-Saxton para recupera la fase correspondiente a la máscara aleatoria de fase $r(x, y)$. Después, con esta información, es posible estimar la llave de encriptación tras resolver la siguiente ecuación,

$$S_z(u, v) = \frac{e(u, v)}{TFrI \{h_1(x, y)o(x, y)r(x, y)\}} \quad (4.20)$$

para el caso de un dato sometido al protocolo de encubrimiento, cuando un atacante intenta acceder a la información cifrada después de llevar a cabo el proceso descrito en la Sección 4.6.2, de acuerdo con la Ec. 4.13, obtendrá

$$\begin{aligned}
M_z(u, v) &= [H_{1r,z}(u, v) \otimes O_{r,z}(u, v) \otimes R_{r,z}(u, v)]L_{r,z}^*(u, v) \otimes b^*(u, v) \\
&+ [H_{1d,z}(u, v) \otimes O_{d,z}(u, v) \otimes R_{d,z}(u, v)]L_{d,z}^*(u, v)
\end{aligned} \tag{4.21}$$

ahora para llevar a cabo el KPA se debe tomar la intensidad de la Ec. 4.21,

$$\begin{aligned}
|M_z(u, v)|^2 &= |[H_{1r,z}(u, v) \otimes O_{r,z}(u, v) \otimes R_{r,z}(u, v)]L_{r,z}^*(u, v) \otimes b^*(u, v)|^2 \\
&+ |[H_{1d,z}(u, v) \otimes O_{d,z}(u, v) \otimes R_{d,z}(u, v)]L_{d,z}^*(u, v)|^2 \\
&+ \{ [H_{1r,z}(u, v) \otimes O_{r,z}(u, v) \otimes R_{r,z}(u, v)]L_{r,z}^*(u, v) \otimes b^*(u, v) \}^* \\
&\times [H_{1d,z}(u, v) \otimes O_{d,z}(u, v) \otimes R_{d,z}(u, v)]L_{d,z}^*(u, v) \\
&+ \{ [H_{1r,z}(u, v) \otimes O_{r,z}(u, v) \otimes R_{r,z}(u, v)]L_{r,z}^*(u, v) \otimes b^*(u, v) \} \\
&\times [H_{1d,z}(u, v) \otimes O_{d,z}(u, v) \otimes R_{d,z}(u, v)]L_{d,z}^*(u, v)^*
\end{aligned} \tag{4.22}$$

en este caso, el primer término en la Ec. 4.22 es la intensidad de la FrT de la información valiosa, este término contiene la información relevante necesaria para llevar a cabo una recuperación exitosa de la llave de encriptación a partir del KPA. Sin embargo, debido a la multiplexación del dato asociado a la información valiosa y el dato señuelo durante el protocolo de encubrimiento, estos datos se solapan con los términos restantes presentes en la Ec. 4.22. Debido a esto, la información presente en la Ec. 4.22 garantiza que no se puede llevar a cabo un algoritmo de recuperación de fase con éxito, a menos que el atacante tenga acceso a información adicional como el dato señuelo, información que no debe estar disponible para

ningún usuario. Adicionalmente, el ELT introduce un grado extra de seguridad ya que la función $h(x, y)$ puede ser modificada a partir de los parámetros existentes dentro del sistema experimental.

Otro de los ataques más comunes es el ataque de texto plano escogido o CPA (siglas en inglés de: chosen plaintext attack) [23, 24]. En este caso, un intruso con acceso al criptosistema codifica una función delta de Dirac, el texto cifrado correspondiente a este objeto de entrada es la TFr del dato encriptado y está dado por,

$$e_{cpa}(x, y) = [h_1(x, y)\delta(x, y)r(x, y)] \otimes l^*(x, y) \quad (4.23)$$

la Ec. 4.23 contiene el complejo conjugado de la llave de encriptación, que corresponde al producto entre el complejo conjugado de la fase generada por el ELT y el complejo conjugado de la MAF utilizada para el procedimiento de cifrado ($l^*(x, y) = h_2^*(x, y)m^*(x, y)$). Ahora, cuando se lleva a cabo el procedimiento de encubrimiento, el texto cifrado resultante viene dado por,

$$\begin{aligned} e_{cpa}(x, y) &= [h_{1r}(x, y)\delta(x, y)r_r(x, y)] \otimes l^*(x, y) \\ &+ [h_{1s}(x, y)o_s(x, y)r_s(x, y)] \otimes s^*(x, y) \end{aligned} \quad (4.24)$$

si se garantiza que el dato señuelo se superpone con la llave de cifrado, es decir que $o_s(x, y)$ tiene una área mayor que $s(x, y)$, y que los términos presentes en la Ec. 4.24 no pueden ser separados, un intruso no podrá acceder a la información de la llave.

Finalmente, en los COAs (siglas en inglés de : ciphertext only attack) [28, 29], un intruso

busca acceder a la llave de encriptación tomando la amplitud recuperada en la Ec. 4.20 y llevando a cabo un algoritmo de levantamiento de fase sin tener conocimiento del texto plano encriptado. En este caso, debido a que el protocolo de encubrimiento implica la multiplexación del dato encriptado asociado a la información valiosa y el dato señuelo, la amplitud de la TFr asociada a la información valiosa no puede ser recuperada a partir del texto cifrado multiplexado (Ec. 4.17), debido a esto, no es posible realizar un COA convencional y obtener la fase de la llave de encriptación [30].

4.7. Conclusiones

En este trabajo se presenta la implementación de un sistema experimental de codificación óptica en el dominio de Fresnel, en el cual se utiliza como fuente de iluminación un haz modulado por el efecto lente térmica. Se pudo demostrar experimentalmente que la degradación debido al ruido multiplicativo y convolutivo que introduce el ELT sobre los datos recuperados no afecta notoriamente la calidad del dato recuperado. Además, después de realizar el proceso de encriptación y recuperación de un dato, se halló la tolerancia a la desencriptación en función del desplazamiento axial de la muestra dentro del sistema, de esta manera se demostró que estos desplazamientos introducen cambios en la fase del haz con el cual se ilumina el plano de entrada, lo que permite la generación, en este caso, de dos llaves de codificación diferentes.

Teniendo en cuenta el desempeño básico del sistema de codificación, se implementó un protocolo de encubrimiento, este procedimiento permite cifrar información valiosa junto con un dato señuelo con el propósito de incrementar la seguridad del sistema permitiendo disuadir y/o engañar atacantes. Con el protocolo de encubrimiento propuesto en este trabajo, un atacante que accede al multiplexado de los datos encriptados y a la llave asociada a la información relevante, no puede acceder a la información valiosa. Para poder acceder a la información valiosa un usuario debe poseer la información de la llave asociada a la información relevante y el multiplexado, y además conocer el protocolo de recuperación, este hecho hace

que el sistema tenga una mayor seguridad. Además de esto, se demuestra que la inclusión del protocolo encubrimiento incrementa la seguridad de los datos cifrados contra algunos de los ataques más comunes sobre sistemas tipo DRPE como lo son el KPA, CPA y COA. La descripción teórica y los resultados experimentales presentados en este capítulo demuestran que la modificación del haz de iluminación a través del ELT es una alternativa, diferente a las mencionadas en capítulos anteriores, para incrementar la seguridad de los sistemas de codificación óptica, y su implementación en criptosistemas tipo DRPE convencionales podría abrir una ruta para futuros desarrollos en el campo del procesamiento óptico de datos.

En investigaciones futuras se espera incluir técnicas de reducción de ruido que permitan solventar el problema asociado al ruido multiplicativo y convolutivo introducido por el ELT, esto podría conducir a una mejora considerable en la calidad de los datos recuperados. Además de esto, el uso de estos procedimientos de reducción de ruido podría permitir el procesamiento de datos de mayor complejidad, como información en escala de grises, imágenes estructuradas y/o contenedores de información. Por otro lado, para generar un esquema de encriptación más flexible es necesario explorar otros parámetros involucrados en la modulación por ELT, como lo son la potencia absorbida por el muestra, su conductividad térmica, el índice de refracción y el gradiente de temperatura que produce el cambio del índice de refracción de la muestra; además de las longitudes de onda del LP y el LE. Es importante señalar que los resultados experimentales mostrados en este trabajo, hasta donde se tienen conocimiento, representan la primera aplicación del ELT en sistemas de codificación óptica. Se debe tener en cuenta que los resultados experimentales expuestos en este trabajo son una primera prueba de concepto que busca aumentar la seguridad de los criptosistemas a partir del uso de luz estructurada para la iluminación del plano de entrada. El análisis del ELT es tratado desde un punto de vista fenomenológico y algunos efectos que este tipo de iluminación genera sobre los resultados experimentales son aún materia de estudio.

Aunque los resultados presentados en este capítulo permiten visualizar un mecanismo mediante el cual se contribuye a la seguridad del sistema, su implementación implica el uso de una cantidad considerable de elementos ópticos que conllevan a una configuración experimental que requiere un área de trabajo considerable y que presenta altos requerimientos

de alineación y estabilidad, y cuyo costo aumenta en comparación con los sistemas JTC convencionales. Debido a esto, se deben desarrollar sistemas que permitan incluir protocolos que ayuden a mejorar su seguridad, pero que presenten una arquitectura flexible y con exigencias experimentales y de implementación similares o menores a la que tienen los sistemas convencionales. Con este objetivo en mente, en el siguiente capítulo se presenta un sistema de codificación tipo JFSC de un solo brazo de iluminación. Este sistema presenta una arquitectura compacta, con menos elementos ópticos y con menos exigencias de estabilidad en comparación con los sistemas JTC convencionales, preservando sus ventajas experimentales y versatilidad.

Todos los resultados presentados en este capítulo, como se observa en la sección de anexos, fueron publicados en revista internacional como producto de la investigación realizada durante el doctorado [18]

Bibliografía

- [1] J.A. JARAMILLO, J.F. BARRERA-RAMÍREZ, A. VÉLEZ, R. TORROBA **Fractional optical cryptographic protocol for data containers in a noise-free multiuser environment** Opt. Lasers Eng. 2018;102:119-25
- [2] J.A. JARAMILLO-OSORIO, J.F. BARRERA-RAMÍREZ, S. MONTOYA, A. MIRAGUDELO, A. VELEZ-ZEA, R. TORROBA. **Improved decryption quality with a random reference beam cryptosystem.** Opt. Lasers Eng. 2019;112:119–27.
- [3] J.F. BARRERA-RAMÍREZ, J.A JARAMILLO-OSORIO, A. VELEZ-ZEA, R. TORROBA. **Experimental analysis of a joint free space cryptosystem.** Opt. Lasers Eng. 2016;83:126–30.
- [4] J.A. JARAMILLO-OSORIO, W. TORRES-SEPÚLVEDA, A. VELEZ-ZEA, A. MIRAGUDELO, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Focus-tunable experimental optical cryptosystem.** Opt. Lasers Eng. 2021;107689.
- [5] X. WANG, G. ZHOU, C. DAI, J. CHEN. **Optical image encryption with divergent illumination and asymmetric keys** IEEE Photonics J. 2017;9:1–8.
- [6] X.DING, X. DENG, K. SONG, G. CHEN. **Security improvement for asymmetric cryptosystem based on spherical wave illumination** Appl. Opt. 2013;52:467–73.
- [7] J.P. GORDON, R.C.C LEITE, R.S. MOORE, S.P.S PORTO, J.R. WHINNERY. **Long-transient effects in lasers with inserted liquid samples.** J. Appl. Phys. 1965;36:3–8.

- [8] K.E. RIECKHOFF. **Self-induced divergence of CW laser beams in liquids-A new nonlinear effect in the propagation of light.** Appl. Phys. Lett. 1966;9:87-8.
- [9] M.A. PROSKURNIN, M. Y. KONONETS. **Modern analytical thermo-optical spectroscopy.** Russ. Chem. Rev. 2004;73:1143-72.
- [10] R.D. SNOOK, R.D. LOWE. **Thermal lens spectrometry.** Analyst. 1995;120:2051-68.
- [11] R.D. LOWE, R.D. SNOOK. **Photobleaching of Methylene Blue in continuous wave thermal lens spectrometry.** Analyst. 1993;118:613-6.
- [12] H. CABRERA, J. AKBAR, D. KORTE, F. ASHRAF, E.E. RAMÍREZ-MIQUET, E. MARÍN, J. NIEMELA. **Absorption spectra of ethanol and water using a photo-thermal lens spectrophotometer.** Appl. Spectrosc. 2018;72:1069-73.
- [13] L. ŽIBERNA, M. MARTELANC, M. FRANKO, S. PASSAMONTI. **Bilirubin is an endogenous antioxidant in human vascular endothelial cells.** Sci. Rep. 2016;6:1-6.
- [14] D. ZHANG, C. LI, C. ZHANG, M.N. SLIPCHENKO, G. EAKINS, J.X. CHENG. **Depth-resolved mid-infrared photothermal imaging of living cells and organisms with submicrometer spatial resolution.** Sci. Adv. 2016;2:e1600521.
- [15] M. FRANKO, M. LIU, A. BOŠKIN, A. DELNERI, M.A. PROSKURNIN. **Fast screening techniques for neurotoxic substances and other toxicants and pollutants based on thermal lensing and microfluidic chips.** Anal. Sci. 2016;32:23-30.
- [16] B.A.N. ASBAGHI, A. ALSADIG, H. CABRERA. **Online electrophoretic nanoanalysis using miniaturized gel electrophoresis and thermal lens microscopy detection.** J. Chromatogr. 2021;A1657:462596.
- [17] J.M. VILARDY, M.S. MILLÁN & E. PÉREZ-CABRÉ. **Non linear optical security system based on a joint transform correlator in the Fresnel domain.** Appl. Opt. 2014;53:1674-82.
- [18] J.A. JARAMILLO-OSORIO, A. VELEZ-ZEA, H. CABRERA, J. NIEMELA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Optical encryption using phase modulation generated by thermal lens effect.** J. Opt. 2022;24:025702.

- [19] A. MARCANO, C. LOPER, N. MELIKECHI. **Pump-probe mode-mismatched thermal lens Z scan.** J. Opt. Soc. Am. B. 2002;19:119–24.
- [20] X. LIU, J. WU, W. HE, M. LIAO, C. ZHANG, X. PENG. **Vulnerability to ciphertext-only attack of optical encryption scheme based on double random phase encoding.** Opt. Express. 2015;23:18955–68.
- [21] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Innovative speckle noise reduction procedure in optical encryption.** J. Opt. 2017;19:055704.
- [22] G. UNNIKRISHNAN, J. JOSEPH & K. SINGH. **Optical encryption system that uses phase conjugation in a photo refractive crystal.** Appl. Opt. 1998;37:8181-6.
- [23] A. CARNICER, M. MONTES-USATEGUI, S. ARCOS, I. JUVELLS. **Vulnerability to chosen-ciphertext attacks of optical encryption schemes based on double random phase keys.** Opt. Lett. 2005;30:1644–6.
- [24] K. FALAGGIS, A.H. RAMÍREZ-ANDRADE, J.G GAXIOLA-LUNA, C.G. OJEDA, R. PORRAS-AGUILAR. **Optical encryption with protection against Dirac delta and plain signal attacks.** Opt. Lett. 2016;41:4787–90.
- [25] Y. FRAUEL, A. CASTRO, T.J. NAUGHTON, B. JAVIDI. **Resistance of the double random phase encryption against various attacks.** Opt. Express. 2007;15:10253–65.
- [26] J.F. BARRERA-RAMÍREZ, C. VARGAS, M. TEBALDI, R. TORROBA, N. BOLOGNINI. **Known-plaintext attack on a joint transform correlator encrypting system.** Opt. Lett. 2010;35:3553–5.
- [27] H. TASHIMA, M. TAKEDA, H. SUZUKI, T. OBI, M. YAMAGUCHI, N. OHYAMA. **Known plaintext attack on double random phase encoding using fingerprint as key and a method for avoiding the attack.** Opt. Express. 2010;18:13772–81.
- [28] C. GUO, I. MUNIRAJ, J.T. SHERIDAN. **Phase-retrieval-based attacks on linear-canonical-transform-based DRPE systems.** Appl. Opt. 2016;55:4720–8.

- [29] M. LIAO, W. HE, D. LU, X. PENG. **Ciphertext-only attack on optical cryptosystem with spatially incoherent illumination: from the view of imaging through scattering medium.** Sci. Rep. 2017;7:1–9.
- [30] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Cryptographic salting for security enhancement of double random phase encryption schemes.** J. Opt. 2017;19:105703.

Capítulo 5

Sistema de encriptación con un solo brazo de iluminación

Las descripciones teóricas y experimentales realizadas en los capítulos anteriores permite concluir que los sistemas de encriptación tipo JTC (siglās en inglés de: joint transform correlator) presentan una arquitectura versátil que permite la inclusión de procedimientos para aumentar la seguridad brindada por el sistema. A pesar de esto, todavía existen algunas limitaciones que deben ser abordadas para que estos esquemas sean considerados una alternativa confiable y válida en esquemas prácticos.

Uno de los desafíos más importantes en el desarrollo de sistemas ópticos de encriptación basados en la configuración de doble máscara de fase aleatoria DRPE (siglas en inglés de: doble random phase encoding) está relacionado con el tamaño y la complejidad de las configuraciones necesarias para su implementación experimental. En particular, los sistemas JTC requieren de dos brazos de iluminación, un brazo permite obtener el dato encriptado, mientras que para llevar a cabo el registro de la llave de codificación se utilizan los dos brazos de iluminación, hecho que hace necesario el uso de una gran cantidad de elementos ópticos, lo que a su vez implica que su disposición experimental requiere de un espacio considera-

ble. Además, para aumentar la seguridad del sistema se deben desarrollar mecanismos que permitan generar llaves adicionales de seguridad, pero sin incrementar significativamente el volumen ocupado por la arquitectura de codificación y la cantidad de elementos, como el montaje implementado en el capítulo anterior, ya que esto se traduce en mayores exigencias en la alineación y la estabilidad, lo que también implica un aumento en el costo de la implementación limitando su desarrollo en implementaciones enfocadas en investigación básica y aplicada.

Un segundo reto que se debe superar está relacionado con la degradación de los datos recuperados; para solventar esta dificultad, varios trabajos se han enfocado en el desarrollo de métodos que permitan reducir el ruido y la degradación en los datos recuperados [2–6]. Una de las técnicas de reducción de ruido que permiten mejorar la calidad de los datos recuperados se basa en un procedimiento no lineal [3]; en esta propuesta, el dato encriptado es dividido por la intensidad de la llave de codificación. Debido a las ventajas presentes en esta técnica, esta técnica fue usada en combinación con otro método no lineal, en el cual además de dividir el dato cifrado por la intensidad de la llave, se divide el dato recuperado por la intensidad de la máscara de fase que se encuentra en contacto con el dato a codificar [4], la combinación de estas dos técnicas genera una mayor reducción del ruido en la información recuperada. Un enfoque diferente, pero que busca solventar los problemas de degradación de la información recuperada, es la técnica PST (siglas en inglés de: pixel separation technique) [5], la cual consiste en reorganizar los píxeles del objeto de entrada introduciendo una separación espacial entre cada uno de ellos. Este método aprovecha la relación entre el ruido debido a la correlación de la llave y la geometría de la entrada, reduciendo así la degradación sobre el objeto recuperado. Además de lo anterior, se ha propuesto el uso de fases aleatorias optimizadas, lo que da como resultado una mejora considerable en la calidad del dato recuperado [6].

Por otro lado, un enfoque diferente para solventar los efectos del ruido y la degradación presente en los datos recuperados es el uso de “contenedores de información”, este método propuesto por Barrera *et al.* [7], consiste en codificar la información a encriptar en un código QR (siglas en inglés de: Quick Response), y luego proceder a encriptar este código utilizando

un sistema de encriptación basado en la técnica de DRPE. Aunque el código descriptado presenta el ruido inherente a los procesos de encriptación y descriptación, los datos originales contenidos dentro del QR pueden ser recuperados sin ruido a partir de la lectura del código descriptado. Posteriormente, el concepto de contenedor de información basado en códigos QR para la reducción de ruido fue demostrado experimentalmente utilizando un criptosistema JTC [8]. La aplicación experimental de los contenedores de información inspiró otras investigaciones; entre ellas se implementaron códigos QR con procedimientos en los cuales se divide por secciones del mismo tamaño el objeto de entrada antes de llevar a cabo el proceso de codificación óptica, esta técnica permite procesar códigos QR de alta complejidad [9]. Los códigos QR también han sido utilizados en sistemas de codificación basados en iluminación incoherente [10], en criptosistemas no lineales de fase truncada con recuperación libre de ruido en el dominio de óptico de Fresnel [11], en el cifrado de imágenes binarias en una arquitectura JTC [7], y en técnicas de validación [8]; por mencionar algunos ejemplos.

Un desarrollo interesante basado en el concepto de contenedores de información fue la implementación de un contenedor diseñado para la seguridad óptica o CCOS (siglas en inglés de: customized containers for optical security) [12]. El CCOS básico es un arreglo binario cuadrado de 3 x 3 celdas. El arreglo está rodeado de un borde blanco que delimita el código y la información se codifica y se lee de izquierda a derecha y de arriba a abajo utilizando la codificación estándar ASCII para caracteres de 8 bits. En este tipo de códigos se puede modificar el tamaño de los bloques y la separación entre cada uno de ellos, lo que permite mejorar el rendimiento para una determinada configuración óptica, además el diseño del CCOS le permite almacenar una gran cantidad de información en un área pequeña y presenta una mayor resistencia al ruido que los códigos QR. El CCOS ha dado lugar a investigaciones novedosas, siendo aplicado en un sistema óptico de codificación combinado con operaciones tipo XOR [13], en algoritmos de recuperación de fase [14], y en protocolos de imágenes fantasma [15].

Un tercer desafío que afrontan los sistemas ópticos de codificación está relacionado con las vulnerabilidades que se han venido descubriendo [16]. Con el propósito de solventar

esta dificultad, se han venido desarrollando métodos y protocolos que permitan aumentar la protección de los sistemas ópticos frente a diferentes tipos de ataques [17–20]. Dentro de estos estudios, se ha demostrado que algunas de las propuestas de reducción de ruido también permiten mejorar la seguridad del sistema. Por ejemplo, las modificaciones no lineales [3, 4], no solo contribuyen con la reducción del ruido en los datos recuperados, sino que también aumentan la seguridad contra los ataques de tipo CPA (siglas en inglés de: chosen plaintext attack) y COA (siglas en inglés de: chipertext-only attack). Otras modificaciones, como el uso de funciones tipo “salteado” sobre los datos cifrados [21] y la codificación de solo fase [22, 23], evitan ataques de tipo KCA (siglas en inglés de: known chipertext attack).

Finalmente, un cuarto desafío está relacionado con los grandes volúmenes de datos producidos por las configuraciones de cifrado óptico. Un primer enfoque para abordar este problema fue aplicar algoritmos de compresión de imágenes digitales como el formato de compresión con pérdida del JPEG (siglas en inglés de: joint photography expert group) [24]. La aplicación de este método de compresión ha mostrado un rendimiento limitado cuando es usado para datos que contienen ruido aleatorio, haciéndolo inadecuado para la compresión de datos holográficos [25]. En este sentido, otros trabajos han demostrado que la compresión de datos holográficos a partir de métodos ópticos, en lugar de los algoritmos convencionales, presenta mejores resultados. Entre los métodos ópticos para la compresión de información holográfica se encuentran el escalado óptico [26, 27], el muestreo aleatorio [28, 29] y la implementación de algoritmos que posibilitan la compresión de información a partir de la manipulación de la fase de los datos holográficos [30, 31].

Teniendo presente los retos que deben ser tenidos en cuenta para mejorar el desempeño de los sistemas de codificación óptica, en este capítulo se presenta un criptosistema óptico de un solo brazo de iluminación en el dominio óptico de Fresnel o JFSC de un solo brazo de iluminación. En este sistema el registro del dato encriptado y de la información de la llave de recuperación son llevados a cabo sin la necesidad de un brazo de referencia fuera de eje. Por lo tanto, en comparación con los sistemas JTC convencionales, esta configuración requiere menos elementos ópticos, con lo cual se logra reducir el tamaño y la complejidad del esquema experimental. Además, buscando mejorar la calidad de los datos recuperados, se incluyen

procedimientos no lineales de reducción de ruido y la implementación de códigos CCOS, lo que da como resultado una recuperación sin ruido después del proceso de descryptación. Por otro lado, se aplican protocolos de codificación y compresión para reducir el volumen de la información almacenada. Los resultados demuestran que el CCOS es resistente a la pérdida de información, lo que significa que es posible aplicar niveles de compresión con pérdida sobre los datos cifrados y aún así obtener una recuperación con una calidad aceptable. Por último se implementa un protocolo de multiplexado a partir del uso de máscaras binarias, este tipo de procedimientos permite la manipulación de múltiples datos con una recuperación selectiva de la información, la viabilidad experimental de este tipo de procedimientos permite además incluir protocolos de encriptación de mensajes de cualquier tamaño, esta aplicación se lleva a cabo a partir de la introducción de un teclado óptico cifrado.

Los resultados teóricos y experimentales presentados en este capítulo son productos originales del trabajo de investigación doctoral [32, 33], y en combinación con los estudios que se presentarán en el capítulo siguiente apuntan al desarrollo de una arquitectura de codificación con una estructura compacto y de bajo costo para el procesamiento de información.

5.1. Descripción del sistema con un solo brazo de iluminación

El sistema de encriptación JFSC (sigla en inglés de: joint free space cryptosystem) de un solo brazo de iluminación no requiere de un brazo de referencia para el registro de la información de la llave seguridad (Fig.5.1). En este sistema, solo una parte del modulador espacial de luz (MEL) se pone en contacto con un difusor. Para el registro del dato encriptado, en el área del MEL que se encuentra en contacto con el difusor se proyectan las ventanas objeto y llave separadas una distancia $2b$, por lo cual, en el plano de salida del sistema se registra el espectro conjunto de potencias de Fresnel o JFPD (siglas en inglés de: joint Fresnel power distribution) que corresponde a la intensidad de la interferencia entre las

transformadas de Fresnel del objeto en contacto con un difusor y la llave de encriptación, del cual se extrae el dato encriptado. Por otro lado, el área del MEL que no se encuentra en contacto con el difusor es usada para realizar el registro de la información de la llave de seguridad, en este caso se proyectan la ventana llave en el área del MEL en contacto con el difusor y la ventana de la onda plana en el área que no se encuentra en contacto con el difusor. Por lo tanto, en el plano de salida se registra el holograma resultante de la interferencia entre las intensidades de las TFr (transformada de Fresnel) de las ventanas llave y onda plana. Se debe destacar que este sistema hereda todas las características de seguridad del sistema JFSC convencional, por lo cual la distancia entre el plano de entrada y el plano de registro es un parámetro que debe ser considerado para el proceso de recuperación.

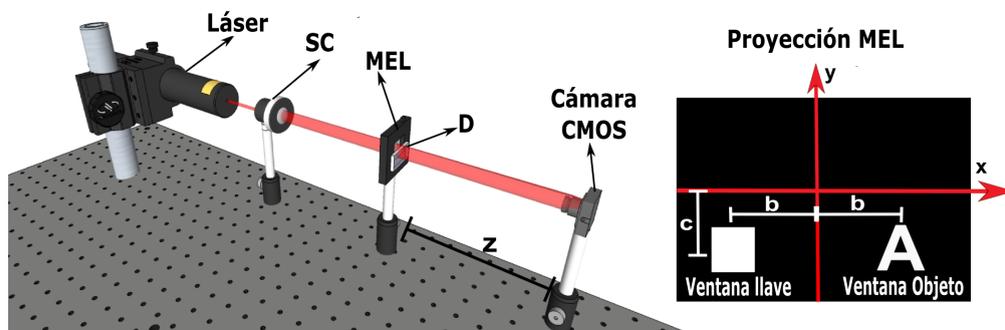


Figura 5.1: Sistema de encriptación JFSC de un solo brazo de iluminación. SC: sistema de colimación, z : distancia entre los planos de entrada y registro, D: difusor, MEL: modulador espacial de luz, $2b$: separación entre las ventanas objeto y llave.

5.2. Registro del dato encriptado

Para realizar el registro del dato encriptado, se proyectan las ventanas objeto y llave en el área del MEL que se encuentra en contacto con un difusor, de esta manera el difusor genera una MAF sobre cada ventana (Fig. 5.1). De acuerdo con lo anterior, el área del difusor en contacto con la ventana de la llave determina la llave de encriptación. El plano de entrada del sistema viene dado por,

$$e(x, y) = c(x, y) \otimes \delta(x - b) + l(x, y) \otimes \delta(x + b) \quad (5.1)$$

donde $c(x, y) = o(x, y)r(x, y)$ con $o(x, y)$ el objeto a encriptar y $r(x, y)$ una MAF generada por el área del difusor en contacto con la ventana objeto; $l(x, y)$ es la llave de encriptación y $2b$ es la separación entre las ventanas objeto y llave en el plano de entrada. Siguiendo el procedimiento expuesto en el capítulo anterior (ver Sección 4.3), el dato encriptado es,

$$E(\nu, \omega) = C_z(\nu, \omega)L_z^*(\nu, \omega)e^{2\pi i(\nu x' + \omega y')} \quad (5.2)$$

aquí $C_z(\nu, \omega)$ y $L_z(\nu, \omega)$ son las transformadas de Fresnel de $c(x, y)$ y $l(x, y)$ para una distancia z respectivamente y (x', y') son las coordenadas en el plano de recuperación. Si se intenta recuperar el objeto a partir de la Ec. 5.2 realizando una transformada de Fresnel inversa (TFrI), se obtiene,

$$e(x, y) = o(x, y)r(x, y) \otimes l^*(x, y) \quad (5.3)$$

debido a que $r(x, y)$ y $k(x, y)$ son funciones de fase aleatorias, su convolución en la Ec.5.3 dará como resultado otra función aleatoria, por lo tanto, el objeto $o(x, y)$ permanecerá encriptado. Por esta razón, para lograr la recuperación de la información se requiere de la información de la llave de seguridad ($L_z(\nu, \omega)$). Se debe destacar que en los sistemas experimentales, aunque las llaves de seguridad por su naturaleza aleatoria y física (difusores) son las principales responsables de la seguridad, también generan ruido sobre la información recuperada, por lo tanto incluso cuando el proceso de recuperación se lleva a cabo con la información de la llave correcta, el proceso de cifrado óptico puede introducir ruido en la recuperación. Para reducir este ruido, hay varios procedimientos propuestos; uno de estos métodos consiste en dividir el dato encriptado (Ec. 5.2) por la intensidad de la llave $|L_z(\nu, \omega)|^2$

[3]. Después de realizar esta operación y repositonar el dato cifrado en las coordenadas $(x' = 0, y' = 0)$, el dato encriptado adquiere la forma,

$$E(\nu, \omega) = \frac{C_z(\nu, \omega)L_z^*(\nu, \omega)}{|L_z(\nu, \omega)|^2} \quad (5.4)$$

posteriormente, de manera experimental y a partir de la métrica del coeficiente de correlación (CC), se mostrará como este procedimiento permite reducir el ruido de speckle y mejorar la calidad del dato recuperado.

5.3. Registro de la información de la llave

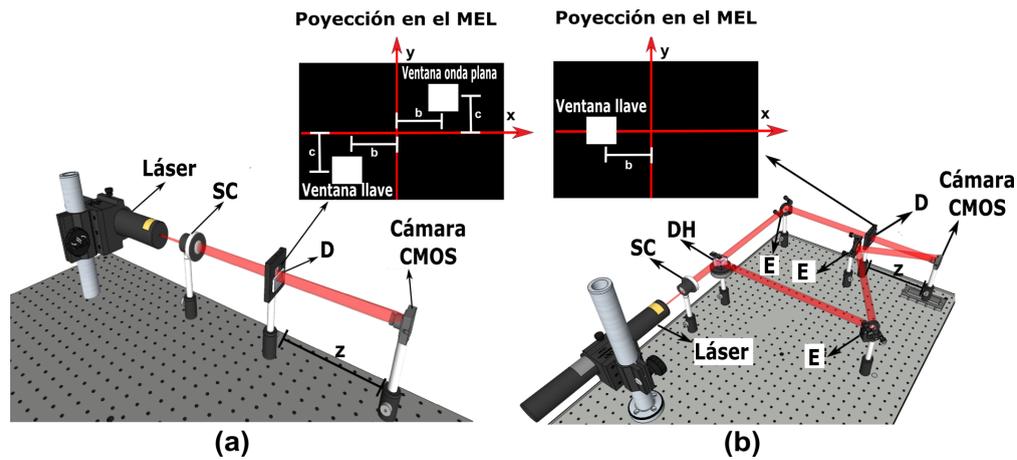


Figura 5.2: Configuración experimental utilizada para registrar la información de la llave de recuperación en un: (a) sistema JFSC con un solo brazo de iluminación y (b) sistema JFSC convencional. CS: sistema de colimación, MEL: modulador de luz espacial, DH: divisor de haz, D: difusor, z : distancia entre el MEL y la cámara CMOS.

De acuerdo con la Ec. 5.4, se requiere la información de la llave de cifrado para poder realizar el proceso de recuperación. En general, para el registro experimental de la llave de seguridad se implementa un sistema holográfico fuera de eje [34]. La Fig. 5.2(b), muestra el esquema experimental de un sistema JFSC convencional usado para el registro de la

información de la llave de recuperación, este esquema cuenta con un brazo fuera de eje que permite realizar el registro holográfico [35]. Por otro lado, en la Fig. 5.2(a) se presenta el esquema experimental para el registro de la información de la llave en el sistema JFSC de un solo brazo de iluminación. En el JFSC convencional la información de la llave se obtiene de la interferencia entre la transformada de Fresnel de la llave y la onda plana proveniente del brazo de referencia fuera de eje, este brazo de referencia se usa solo para el registro de la información de la llave y debe ser bloqueado durante el proceso de encriptación. Por otro lado, en el esquema JFSC con un solo brazo de iluminación, en lugar de incluir un brazo de referencia separado para registrar la información de la llave de encriptación, se proyecta una ventana vacía en el área del MEL que no está en contacto con el difusor. Esta ventana proporciona la onda plana de referencia (Fig. 5.2(a)). De acuerdo con esto, para llevar a cabo el registro del dato encriptado y de la información de la llave de seguridad, se utiliza la misma configuración experimental, y solo se varía la proyección en el MEL (Fig. 5.1 y Fig. 5.2(a)). En consecuencia, el sistema JFSC de un brazo de iluminación presenta una arquitectura más compacta que el sistema JFSC convencional, ya que solo requiere de una fuente de luz colimada, un MEL y un medio de registro. Esto disminuye las posibles fuentes de aberraciones, los requisitos de estabilidad y alineación del esquema, además de simplificar la manipulación del sistema de codificación, y como beneficio adicional reduce el costo total de su implementación experimental.

De acuerdo con lo anterior, para llevar a cabo el proceso de registro de la información de la llave, se proyecta el plano de entrada mostrado en la Fig. 5.2(a)). Por lo tanto, en el plano de registro se obtiene el holograma resultante entre la transformada de Fresnel de la onda plana proveniente de la ventana de la onda plana y de la transformada de Fresnel de la ventana llave en contacto con el difusor. Siguiendo el mismo procedimiento de registro y filtrado presentado en la Sección 2.5.2, se obtiene la información de la llave,

$$K(\nu, \omega) = L_z(\nu, \omega) \quad (5.5)$$

se puede notar, que tanto el dato encriptado (Ec. 5.2) como la información de la llave (Ec. 5.5), tienen la misma forma que en el sistema JFSC convencional [35].

5.4. Proceso de recuperación en el sistema en línea

Para obtener el dato recuperado se debe primero multiplicar el dato encriptado (Ec. 5.4) por la información de la llave (Ec. 5.5). Por simplicidad, en este caso se realiza el reposicionado del dato encriptado y la llave en el origen de coordenadas. Por lo tanto $x' = 0$ y $y' = 0$, obteniendo

$$E'(\nu, \omega) = \frac{C_z(\nu, \omega)L_z^*(\nu, \omega)L_z(\nu, \omega)}{|L_z(\nu, \omega)|^2} \quad (5.6)$$

ahora, realizando un TFr inversa para la distancia z usada en el proceso de encriptación, se obtiene.

$$d(x, y) = o(x, y)r(x, y) \quad (5.7)$$

El dato recuperado corresponde a la distribución de intensidad del campo óptico representado por la Ec. 5.7. Se puede notar que el proceso de recuperación es igual al que se lleva a cabo cuando los datos son registrados en el sistema JFSC convencional, por lo tanto se puede concluir que el sistema JFSC de un solo brazo de iluminación o JFSC en línea, además de requerir menos elementos ópticos para su desarrollo, no introduce procesos extra que puedan incrementar los requerimientos experimentales.

Se debe destacar que dentro de los sistemas de encriptación tipo DRPE (siglas del inglés: doble random phase encoding), existe otra fuente de ruido que debe ser tomada en cuenta

durante la implementación experimental. En la práctica se debe considerar que la intensidad de la información de la llave de encriptación ($|L_z(\nu, \omega)|^2$) se registra experimentalmente en un momento diferente al JFPD (siglas en inglés de: joint fresnel power distribution), y que los difusores no son máscaras aleatorias de fase pura ya que presentan cambios de amplitud aleatorios. Esto significa que hay una ligera diferencia entre el numerador y el denominador de la Ec. 5.6 y, por lo tanto, el término asociado a la llave de encriptación no se pueden cancelar con exactitud. Con el objetivo de minimizar los efectos generado por el difusor se implementa otra técnica no lineal de reducción de ruido, esta técnica consiste en obtener la información de la máscara aleatoria de fase que está en contacto con el objeto y luego dividir el dato encriptado por su intensidad. Inicialmente se lleva a cabo el proceso de encriptación, luego se proyecta una ventana que tiene el mismo tamaño y posición del objeto que se encriptó, de esta forma se obtiene un dato encriptado que corresponde a la máscara de referencia encriptada [4]. Posteriormente, se lleva a cabo el proceso de recuperación y se divide el objeto desencriptado por la máscara de referencia desencriptada. De esta forma, la intensidad del dato recuperado después de incluir esta reducción de ruido, toma la siguiente forma,

$$|d(x, y)|^2 = \frac{|o(x, y)r(x, y)|^2}{|r(x, y)|^2} \quad (5.8)$$

Este método reduce la degradación introducida en la recuperación por la máscara aleatoria que se encuentra en contacto con la ventana objeto, lo que conlleva a una reducción significativa del ruido sobre el dato recuperado [4]. El dato recuperado después del proceso mencionado viene dado por,

$$d(x, y) = o(x, y) + N(x, y) \quad (5.9)$$

donde $N(x, y)$ representa el ruido residual causado por factores experimentales.

5.5. Resultados experimentales

Los resultados experimentales que presentados a continuación fueron obtenidos con el sistema experimental mostrado en la Fig. 5.1. Como medio de registro se empleó una cámara CMOS EO-10012M con una resolución de 3840 x 2748 pixeles y un tamaño de pixel de $1,67 \mu m \times 1,67 \mu m$. El tamaño de las ventanas objeto, llave y onda plana fue de 250 x 250 pixeles, 150 x 150 pixeles y 100 x 100, respectivamente. La separación $2b$ entre las ventanas objeto y llave fue de 300 pixeles, mientras que la separación c entre las ventanas y el centro del MEL fue de 100 pixeles. El plano de entrada fue proyectado en un MEL Holoeye 2002 con tamaño de pixel de $32 \mu m \times 32 \mu m$, una resolución de 800 x 600 pixeles y un área de proyección de $25,6 mm \times 19,2 mm$. Como fuente de iluminación se utilizó un láser JDS UNIPHASE 1135 He-Ne con una longitud de onda $\lambda = 632 nm$ y una potencia de $20 mW$.

Para analizar el desempeño básico del sistema JFSC en línea, realizó el proceso de encriptación y recuperación de tres objetos, tal como se observa en la Fig. 5.3.



Figura 5.3: Resultados experimentales del proceso de encriptación y recuperación usando el sistema JFSC en línea y aplicando técnicas de reducción de ruido.

Los resultados presentes en la Fig. 5.3 demuestra que el sistema JFSC en línea es capaz de procesar información de forma segura, corroborando así el funcionamiento básico del sistema. Cabe destacar que para obtener los resultados presentados en la Fig. 5.3, se dividió el dato encriptado por la intensidad de la llave ($|F(\nu, \omega)|^2$) y posteriormente el dato recuperado fue dividido por la máscara de referencia desencriptada, estas técnicas reducen la degradación y el ruido del objeto desencriptado [3, 4]. Después de verificar el desempeño básico del sistema, se debe corroborar el rendimiento de la arquitectura de encriptación JFSC en línea en comparación con el sistema JFSC convencional (Fig. 5.2(b)) [35]. En este caso, se lleva a cabo el proceso de encriptación y recuperación de los mismos objetos de entrada bajo las mismas condiciones experimentales, tanto en el sistema JFSC convencional como en el

sistema JFSC en línea, y posteriormente se calcula el coeficiente de correlación (CC) entre el objeto de entrada y los objetos recuperados.

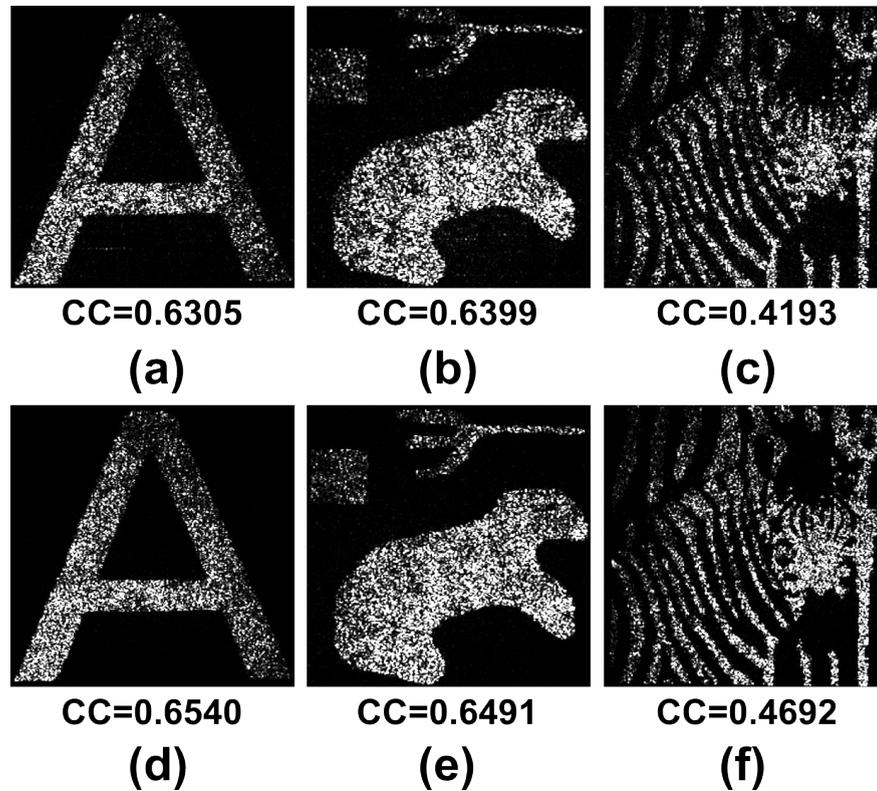


Figura 5.4: (a),(b), (c) resultados de la recuperación utilizando el sistema JFSC en línea; (d),(e) y (f) resultados de la desencriptación con el sistema JFSC convencional.

En la Fig. 5.4 se muestran los diferentes valores obtenidos para el CC para tres objetos recuperados, después de ser encriptados usando el JFSC en línea (Fig. 5.4(a), Fig. 5.4(b) y Fig. 5.4(c)) y usando el sistema JFSC convencional (Fig. 5.4(c), Fig. 5.4(d) y Fig. 5.4(e)). Se puede observar que los valores para el CC obtenido después de procesar la información en el sistema JFSC en línea son muy cercanos a los valores para el CC obtenidos después de llevar a cabo el proceso de encriptación y recuperación en el sistema JFSC convencional. Lo anterior permite concluir que, bajo condiciones similares, la calidad de los datos recuperados después del proceso de encriptación y recuperación en el sistema JFSC en línea no se ve afectada notoriamente en comparación con los datos recuperados a partir del sistema JFSC convencional. Además de esto, el sistema JFSC en línea tiene la ventaja, sobre el sistema convencional, de ser menos complejo y más compacto. Los resultados expuestos en la Fig. 5.4

demuestran el potencial y el rendimiento de la configuración JFSC en línea en comparación con el JFSC convencional.

5.5.1. Tolerancia de los datos encriptados al ruido aleatorio y a la pérdida de información

Con el propósito de establecer el funcionamiento del sistema JFSC en línea cuando se producen pérdidas de información en los procesos de transmisión y almacenamiento, se realiza un análisis de desempeño del sistema que permita establecer los niveles de tolerancia al ruido aleatorio y a la pérdida de información que admiten los datos procesados en el sistema. En principio se analizará la calidad del dato recuperado en función del ruido aleatorio, para esto se agrega ruido aleatorio de amplitud creciente (RAAC) a los datos codificados, de esta forma el dato encriptado toma la siguiente forma,

$$E_{RAAC}(\nu, \omega) = e_z(\nu, \omega) + A_n \exp[2\pi i \phi(\nu, \omega)] \quad (5.10)$$

donde A_n es la amplitud de la función de ruido aleatorio y $\phi(\nu, \omega)$ es una función aleatoria. A_n varía en un rango de -20 dB a 20 dB respecto a la amplitud del dato encriptado. Por lo tanto, cuando $A_n = 0$, no se agrega ruido al dato cifrado. Después de agregar el RRAC al dato encriptado, se realiza el proceso de recuperación y se calcula el CC entre los datos recuperados con ruido y el dato recuperado sin ruido. Este proceso se realiza para datos encriptados con los sistemas JFSC en línea y JFSC convencional, los resultados son presentados en la Fig. 5.5.

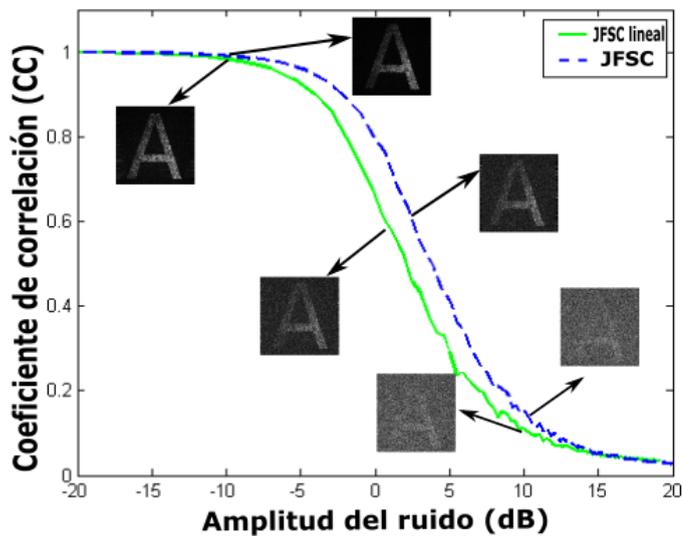


Figura 5.5: Coeficiente de correlación en función de la amplitud del ruido entre objetos recuperados a partir de datos encriptados con adición de ruido aleatorio y un dato recuperado sin ruido añadido.

En la Fig. 5.5 se puede observar que tanto para el sistema JFSC lineal como para el JFSC convencional el CC presenta un comportamiento muy similar respecto a la amplitud del ruido en decibeles agregado al dato encriptado, demostrando una resistencia considerable al ruido aleatorio. En ambos casos, el coeficiente de correlación, y por ende la calidad del dato recuperado, varía levemente cuando la amplitud del ruido aleatorio se encuentra entre -20 dB y -10 dB, indicando que el ruido asociado a este rango no introduce una degradación considerable sobre los datos descifrados. Por otro lado, cuando la amplitud del ruido es superior a -10 dB, los valores de CC disminuyen, y la degradación de la calidad de la imagen recuperada aumenta rápidamente. Los resultados presentados en la Fig. 5.5 demuestran que el sistema JFSC en línea tiene la misma tolerancia que el sistema JFSC convencional para soportar los problemas que se presentan al momento de usar canales de transmisión y almacenamiento que agregan ruido a los datos encriptados.

Además de la tolerancia al ruido aleatorio, también se analizó la resistencia que presentan los datos cifrados frente a la pérdida aleatoria de información. Para llevar a cabo este análisis, se cambiaron aleatoriamente por cero un porcentaje creciente de píxeles del dato encriptado,

este procedimiento simula una pérdida de información que puede ser asociada al proceso de almacenamiento y/o transmisión de información. Con el propósito de comparar el desempeño del sistema JFSC lineal con el sistema JFSC convencional, el proceso fue llevado a cabo para datos cifrados en ambos esquemas de codificación. Posteriormente, se realizó el proceso de recuperación de los datos encriptados con pérdida y se midió la calidad de los datos recuperados respecto al dato recuperado sin pérdida a través de la métrica del coeficiente de correlación.

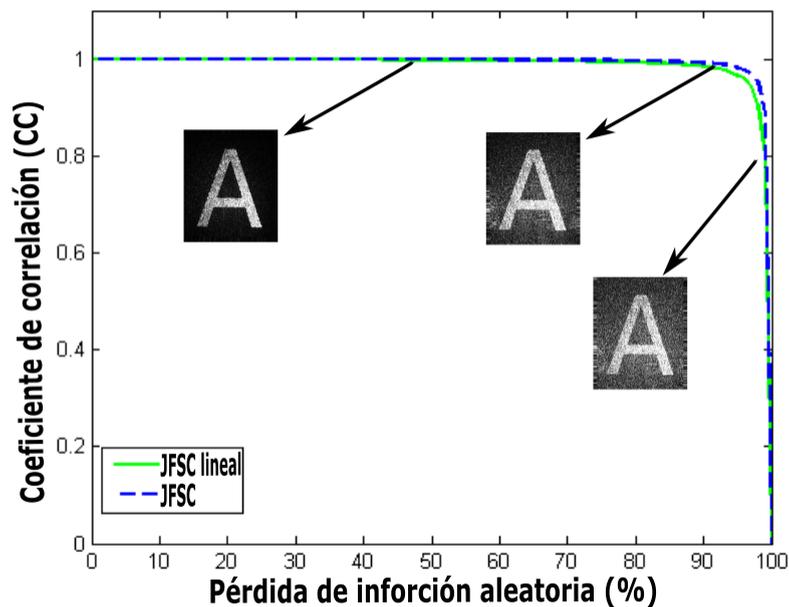


Figura 5.6: Coeficiente de correlación en función del porcentaje de pérdida aleatoria de información en los datos encriptados para objetos descifrados a partir de datos cifrados con y sin pérdida aleatoria.

En la Fig. 5.6 se muestra el comportamiento del coeficiente de correlación en función del porcentaje de pérdida aleatoria de información en los datos para los sistemas JFSC en línea y JFSC convencional. Las imágenes insertadas en la figura muestran los resultados de la reconstrucción de un dato, después de ser procesado en el sistema JFSC en línea, cuando se tiene una pérdida aleatoria de información en el dato encriptado del 50 %, 90 % y 97 %. A partir de estos resultados, se observa que la degradación debida a la pérdida de información aleatoria en un rango de 0 % a 90 % es pequeña para ambos criptosistemas. Por otro lado, cuando la pérdida de información aleatoria supera el 90 %, la calidad de la imagen recu-

perado disminuye rápidamente. Los resultados experimentales demuestran la alta tolerancia a la pérdida de información aleatoria, este comportamiento se puede explicar debido a la redundancia que presentan los datos registrados de manera holográfica. Los resultados presentes en la Fig. 5.6 permiten comprobar que el desempeño del sistema de codificación óptico JFSC en línea es similar al JFSC convencional, por lo cual se podría considerar como una alternativa interesante con que, no solo se reducen los requisitos experimentales y el costo de la implementación experimental en comparación con las arquitecturas JTC ya mostradas en este trabajo, sino que también permite un alto rendimiento para el procesamiento de datos.

5.5.2. Recuperación libre de ruido

A pesar de las técnicas de reducción de ruido aplicadas para recuperar la información original, se puede observar que el objeto descifrado aún presenta degradación (Fig. 5.4), este ruido se debe principalmente al uso de claves de seguridad aleatorias y físicas (difusores) en el proceso de encriptación óptica. Para lograr una recuperación libre de ruido y degradación se propuso e implementó un protocolo de encriptación que usa contenedores de información, como los códigos QR. En particular, en este caso se utilizarán contenedores diseñados para la seguridad óptica o CCOS (siglas en inglés de: customized containers for optical security) [12]. El CCOS básico es un arreglo binario cuadrado de 3 x 3 celdas, en el cual cada celda contiene un bloque de tamaño X, con una separación Y entre los bloques. El arreglo está rodeado por un borde blanco que delimita el código. Para llevar a cabo la lectura del código se calcula la intensidad promedio de cada celda de izquierda a derecha y de arriba a abajo, y luego es comparada con un valor límite que se establece de acuerdo con el sistema óptico. Si la celda tiene una intensidad promedio por encima del valor límite se le asigna un valor de 1, de lo contrario se le asigna un valor de 0. La codificación dentro del CCOS se hace a partir de una representación en código ASCII, por lo tanto un código representa un carácter de 8 bits. La versatilidad de los CCOS permiten organizar varios códigos básicos (que contienen un solo carácter) en un patrón cuadrado de mayor tamaño para codificar mensajes extensos. Con el objetivo de llevar a cabo una recuperación libre de

ruido, la información a proteger se codifica en un CCOS y luego este código es encriptado en el sistema JFSC en línea. Aunque después de la recuperación el CCOS desencriptado presenta el ruido inherente debido al proceso de codificación óptica, la información original contenida en el CCOS recuperado puede ser leída brindando la información original libre de ruido y degradación.

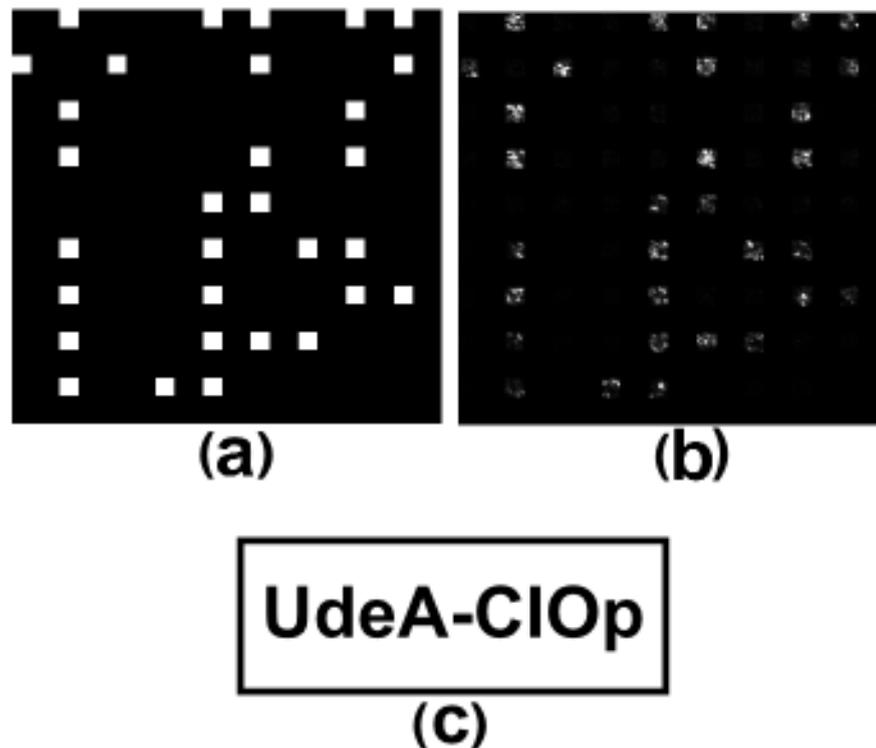


Figura 5.7: Recuperación de información libre de ruido y degradación para un conjunto de CCOS que conforman el mensaje “UdeA-CIOp”. (a) CCOS original para “UdeA-CIOp”, (b) CCOS descifrado, y (c) lectura del código recuperado.

En la Fig. 5.7(a) se observa el CCOS original cuya información codificada corresponde a la frase “UdeA-CIOp”. Por otro lado, en la Fig. 5.7(b) se muestra el CCOS después del proceso de encriptación y recuperación; este código (Fig. 5.7(b)) puede ser leído, lo que permite acceder a la información contenida libre de ruido y degradación, como se observa en la Fig. 5.7(c). Los resultados experimentales mostrados en la Fig. 5.7 demuestran que la tolerancia al ruido que presenta el código asegura que después de la lectura de este, se obtenga el mensaje original contenido dentro del CCOS sin ruido o degradación.

Con el objetivo de analizar el desempeño de los CCOS para la protección y manipulación segura de información, y teniendo presente que la información codificada presenta una alta tolerancia a la pérdida debido a la redundancia que presentan los datos cifrados, tal como se demostró con los resultados presentes en la Fig. 5.6, se realizó un análisis de pérdida de información por oclusión. En este proceso se simula una pupila que bloquea gradualmente una porción de la información encriptada. Un porcentaje de oclusión del 0% implica que se tiene disponible toda la información del dato encriptado, sin ninguna pérdida. Como se puede observar en la Fig. 5.8, a pesar de la pérdida de información debido a la oclusión, se obtienen lecturas exitosas del CCOS para porcentajes de oclusión de hasta el 97%. Los resultados anteriores demuestran que el uso de CCOS en conjunto con la redundancia que tienen los datos registrados holográficamente, permiten llevar a cabo el proceso de recuperación libre de ruido y degradación, incluso con una alta pérdida de información en el dato encriptado.

Cabe destacar que en los resultados experimentales mostrados hasta el momento, el CCOS encriptado tiene una resolución de 3840 x 2748 pixeles (correspondiente a la resolución de la cámara CMOS), dando como resultado un volumen para el CCOS encriptado de 10,36 MB. Sin embargo, de acuerdo a los resultados mostrados en la Fig. 5.8, es posible lograr un recuperación exitosa para un CCOS cifrado y almacenado con un volumen de 310 KB, correspondiente a una oclusión del 97%. De acuerdo con lo anterior, se puede establecer que la combinación de la tolerancia al ruido de la lectura del CCOS junto con un procedimiento de oclusión permite reducir significativamente el volumen de los datos ópticos obtenidos después del proceso de codificación óptica, generando como resultado una reducción en los recursos necesarios para la transmisión y almacenamiento de datos, lo que demuestra la capacidad del sistema JFCS en línea para el procesamiento seguro y eficiente de información.

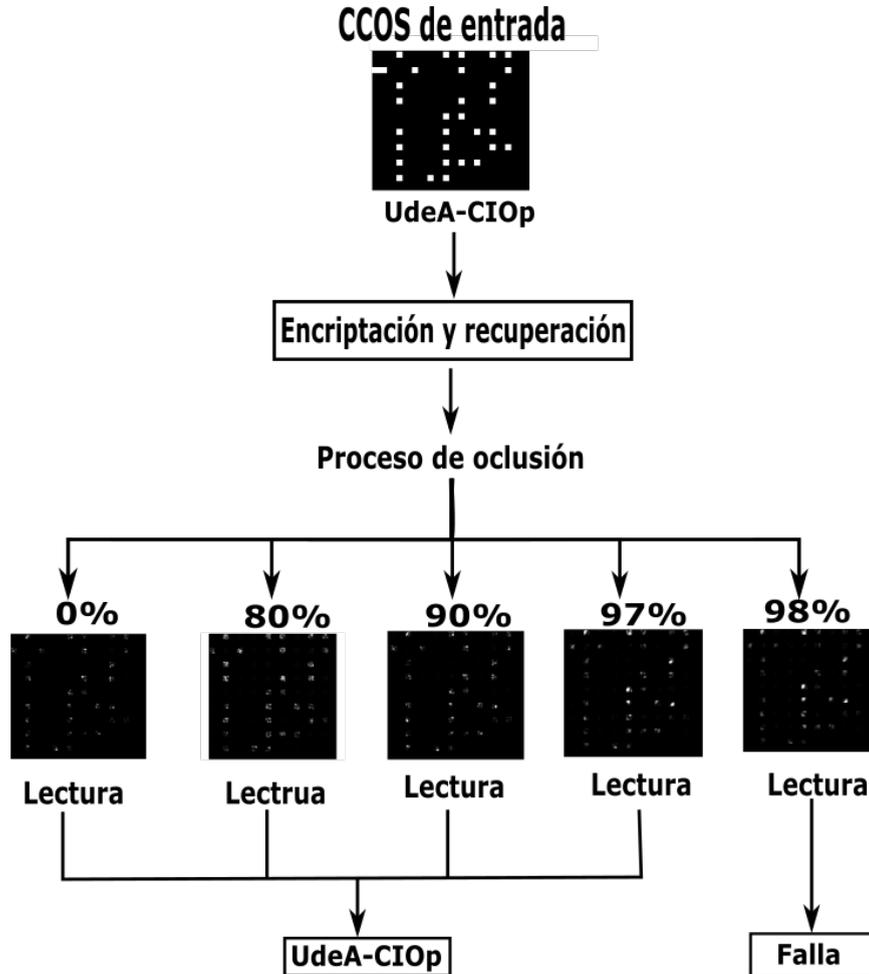


Figura 5.8: Tolerancia de un CCOS encriptado a la reducción de volumen debido al proceso de oclusión.

Además de lo anterior, se debe mencionar que las técnicas de reducción de ruido incluidas en el protocolo de seguridad, no solo conducen a una mejora en la calidad de los datos recuperados, sino también a un aumento en la seguridad del sistema [3], ya que la división de los datos cifrados por la intensidad de la llave de cifrado ayuda a proteger la información contenida en los datos encriptados contra ataques del tipo CPA (siglas en inglés de: chosen plaintext attack) [4]. Asimismo, debido al uso de máscaras aleatorias físicas en lugar de máscaras de solo fase y al proceso de dividir el objeto descifrado por una máscara de referencia previamente descifrada, posibilita que el sistema JFSC en línea sea resistente a los ataques comunes tales como el COA (siglas en inglés de: ciphertext-only attack).

5.5.3. Protocolo de multiplexado selectivo basado en máscaras binarias

Con el objetivo de seguir analizando el desempeño y versatilidad del sistema JFSC de un solo brazo de iluminación, se introduce un protocolo de multiplexado basado en máscaras binarias aleatorias (MBA). En este protocolo se realiza un proceso de muestreo de cada dato encriptado usando máscaras binarias aleatorias ortogonales (MBAOs), posteriormente todos los datos cifrados y muestreados son multiplexados. El uso de MBAOs en este protocolo permite recuperar de manera individual cada dato dentro del multiplexado sin la presencia del ruido asociado a los datos no recuperados, de esta manera se mejora la capacidad de procesamiento del sistema óptico y se incrementa la seguridad de la información codificada ya que ningún usuario tiene la posibilidad de estimar cuantos datos encriptados contiene el multiplexado.

Antes de presentar el protocolo de multiplexado selectivo, se analiza la resistencia que presenta un dato cifrado al muestreo aleatorio con un máscara binaria aleatoria (MBA). Primero se realiza el proceso de encriptación de un objeto, siguiendo el procedimiento descrito en la Sección 5.2. Luego, el dato encriptado se muestrea con un MBA con un porcentaje determinado de píxeles blancos (ver Fig. 5.9). Posteriormente, se lleva a cabo el proceso de recuperación del dato encriptado y muestreado. Como se puede observar, el objeto es recuperado a pesar de la pérdida de información que sufre la información encriptada debido al muestreo. Aunque la calidad del objeto recuperado disminuye a medida que disminuye el porcentaje de píxeles blancos (aumenta el número de píxeles negros en la MBA), se encuentra que para tasas de muestreo muy bajas (porcentajes bajos de píxeles blancos), la información recuperada sigue siendo reconocible. Este comportamiento se debe principalmente a la redundancia inherente que tienen los datos registrados holográficamente. La viabilidad experimental demostrada a partir de los resultados de la Fig. 5.9 son la base para la implementación del protocolo de multiplexado selectivo.

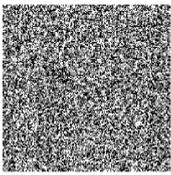
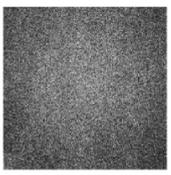
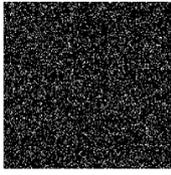
		Dato encriptado	Llave de encriptación
			
Dato original	Dato recuperado	Dato encriptado y muestreado	
		MBA 25.00%	MBA 1.92%
			
		Dato recuperado	
			

Figura 5.9: Recuperación de datos encriptados y muestreados con máscaras binarias aleatorias.

Después de corroborar la tolerancia que presentan los datos encriptados al proceso de muestreo con MBA, se introduce el protocolo de multiplexado selectivo. Este protocolo de empaquetamiento de datos con recuperación selectiva consiste en muestrear cada objeto encriptado con MBAOs, y luego de esto multiplexar los objetos encriptados y muestreados. Este protocolo puede ser resumido en los siguientes pasos:

1. Siguiendo el procedimiento expuesto en la Sección 5.2, se lleva a cabo el proceso de encriptación de los datos a multiplexar.
2. Se genera un conjunto de máscaras binarias aleatorias ortogonales (MBAOs). Se debe tener en cuenta que la cantidad de máscaras dentro del conjunto de MBAOs es igual a la cantidad de datos encriptados.

3. Cada objeto encriptado es muestreado con una MBAO diferente.
4. Todos los datos encriptados y muestreados se multiplexan.

Si un solo dato encriptado viene dado por la Ec. 5.6 y $m(\nu, \omega)$ representa una MBA dentro del conjunto de MBAOs, entonces en el origen de coordenadas ($x' = 0$ y $y' = 0$) el multiplexado será,

$$M(\nu, \omega) = \sum_{i=1}^N E_i(\nu, \omega) \times m_i(\nu, \omega) = \sum_{i=1}^N (C_z(\nu, \omega) L_z^*(\nu, \omega))_i \times m_i(\nu, \omega) \quad (5.11)$$

donde N es el número de datos multiplexados, $i = 1, 2, 3, \dots, j, \dots, N$, $E_i(\nu, \omega)$ representa el i -ésimo dato encriptado, y $m_i(\nu, \omega)$ representa la máscara i -ésima del conjunto de MBAOs. En general, los objetos se pueden encriptar utilizando diferentes llaves, sin embargo en este caso se empleará la misma llave ($L_z(\nu, \omega)$) en el proceso de encriptación de cada dato. Por lo tanto, la expresión para el dato multiplexado puede reescribirse de la siguiente forma,

$$M(\nu, \omega) = \sum_{i=1}^N (C_z(\nu, \omega))_i \times L_z^*(\nu, \omega) \times m_i(\nu, \omega) \quad (5.12)$$

Una vez es obtenido el multiplexado con los datos encriptados, se lleva a cabo el procedimiento de recuperación selectiva de cada dato original de manera individual. El primer paso para recuperar el objeto j -ésimo encriptado y muestreado $E_j(\nu, \omega)$ es multiplicar los datos multiplexados (Ec. 5.12) por la j -ésima MBAOs $m_j(\nu, \omega)$,

$$D_j(\nu, \omega) = \sum_{i=1}^N [(C_z(\nu, \omega))_i \times L_z^*(\nu, \omega) \times m_i(\nu, \omega)] \times m_j(\nu, \omega) \quad (5.13)$$

ahora, debido a que las máscaras utilizadas en el proceso de muestreo son ortogonales, se tiene que,

$$m_i(\nu, \omega)m_j(\nu, \omega) = \begin{cases} 0 & \text{si } i \neq j \\ m_j(\nu, \omega) & \text{si } i = j \end{cases} \quad (5.14)$$

aplicando, sobre la Ec. 5.13, la condición de ortogonalidad presente en la Ec. 5.14,

$$D_j(\nu, \omega) = (C_z(\nu, \omega))_j \times L_z^*(\nu, \omega) \times m_j(\nu, \omega) = e_j(\nu, \omega) \times m_j(\nu, \omega) \quad (5.15)$$

Como se puede observar en la Ec. 5.15, las MBAOs permiten seleccionar solo un dato encriptado y muestreado de los datos multiplexados. Por lo tanto, un usuario que posee una MBAO solo puede acceder al dato encriptado asociado a esa máscara. En consecuencia, el muestreo de los datos encriptados con una MBAO, antes del proceso de multiplexado, permite establecer un proceso de encriptación de múltiples datos con una recuperación selectiva.

Llevando a cabo el proceso de recuperación del dato original $o_j(x, y)$, el dato encriptado seleccionado (Ec. 5.15) es multiplicado por la información de la llave de recuperación $L_z(\nu, \omega)$. Después, al aplicar una TFr inversa, se obtiene,

$$d_j(x, y) = c_j(x, y) = o_j(x, y)r_j(x, y) \quad (5.16)$$

aquí $r_j(x, y)$ es la MAF en contacto con el dato j –esimo durante el proceso de encriptación. Como se observa en la Fig. 5.9, la alta redundancia de los datos registrados holográficamente permite una recuperación exitosa y de buena calidad a pesar de la pérdida aleatoria que produce el muestreo con las MBAOs. Además, es de resaltar que los demás datos dentro del multiplexado, asociados a las otras MABOs, no aparecen en el plano de re-

cuperación, por lo tanto el ruido asociado a esta información no recuperada no se superpone con la información recuperada asociada al dato seleccionado.

Con el propósito de realizar una primera prueba del protocolo propuesto, se encriptan y se muestrean con MBAOs cuatro objetos de entrada correspondientes a las letras “A”, “B”, “C” y “D” (ver Fig. 5.10). Posteriormente, los cuatro objetos encriptados y muestreados se multiplexan, de esta manera para llevar a cabo el proceso de recuperación de un dato individual es necesario multiplicar el multiplexado por la MBAO correspondiente al dato al cual se desea acceder. Luego de esto, se realiza el proceso de descryptación con la llave de seguridad. Para esta implementación, se utilizó un conjunto de cuatro MBAOs con un 25 % de píxeles blancos cada una. El procedimiento de codificación y recuperación se muestra en el diagrama de flujo de la Fig. 5.10 y como puede verse, cuando se aplica el procedimiento de recuperación sin multiplicar previamente el multiplexado por una de las MBAO, se obtienen en el plano de recuperación los objetos simultáneamente y superpuestos, imposibilitando su adecuada identificación. Por otro lado, cuando se multiplica el multiplexado por una de las MBAO utilizada en el muestreo y se realiza el proceso de recuperación, se descrypta únicamente el objeto correspondiente a esa MBAO.

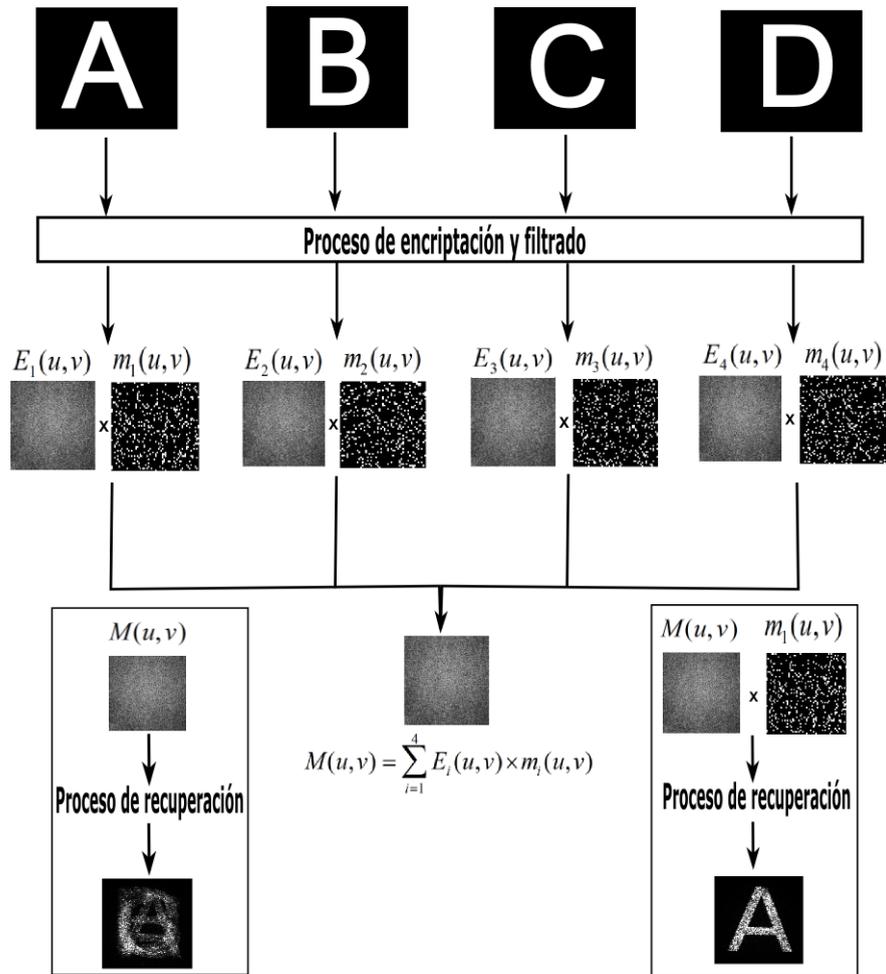


Figura 5.10: Proceso de cifrado-recuperación usando el protocolo de multiplexado selectivo.

Los resultados mostrados en la Fig. 5.4 muestran que para lograr un recuperación exitosa se requiere la información del MBAO, por lo cual, se puede considerar las MBAOs utilizadas en el proceso de encriptación como un parámetro de seguridad adicional que refuerza el protocolo de encriptación. Para demostrar aún más la solidez de esta propuesta, se realiza un proceso de oclusión, igual al expuesto en la sección anterior, sobre los datos multiplexados. Este proceso permite simular la tolerancia a la pérdida que podrían ocasionar los procesos de transmisión y almacenamiento sobre los datos multiplexados, y que reducirían la calidad de la información recuperada. Para este análisis, se mide la degradación en la calidad del objeto recuperado en función del área ocluida. Posteriormente, la calidad de los datos recuperados se mide utilizando la métrica del coeficiente de correlación (CC), para lo cual se calcula el CC entre el objeto recuperado obtenido antes y después de ocluir el paquete multiplexado.

Los resultados se muestran en la Fig. 5.11.

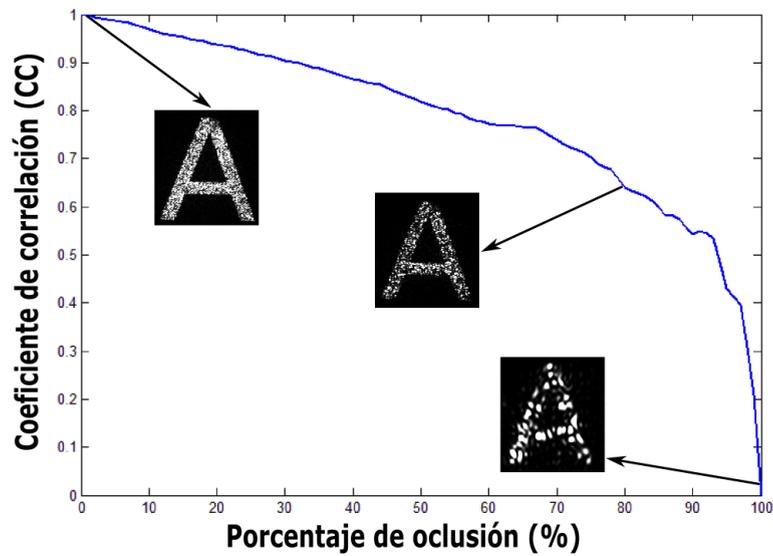


Figura 5.11: Coeficiente de correlación entre el objeto recuperado obtenido antes y después de ocluir el multiplexado.

Los resultados experimentales mostrados en la Fig. 5.11 demuestran que tras el proceso de oclusión y la pérdida por muestreo con máscaras binarias, los datos multiplexados aún mantienen un alto grado de redundancia, lo que permite la recuperación de los datos con una calidad aceptable. Se puede observar que cuando el procedimiento de oclusión está por encima del 50% hay una pequeña degradación, aún así la calidad de la información recuperada puede ser comparada con la recuperación de un dato que no está sometido al procedimiento de oclusión. Por otro lado, cuando la oclusión está por encima del 97%, la reducción en la calidad de los datos recuperados se vuelve muy notoria.

Ahora, para continuar probando la robustez del criptosistema JFSC de un solo brazo de iluminación bajo el protocolo de multiplexado selectivo, se adiciona a los datos multiplexados ruido aleatorio aditivo, igual al que se le adiciona a un solo dato encriptado en la Ec. 5.10. Luego, se realiza el procedimiento de recuperación de la información desde el dato multiplexado con ruido añadido y se calcula el coeficiente de correlación (CC) entre estos resultados y los obtenidos a partir de los datos multiplexados originales sin ruido añadido.

Como se puede ver en la Fig. 5.12, a pesar de la inclusión de los MBAOs y el ruido aleatorio aditivo, el comportamiento del CC corrobora el desempeño del protocolo selectivo. Se nota que el CC cae lentamente cuando la amplitud del ruido aleatorio oscila entre -20 dB y 0 dB, esto indica que existe una degradación menor sobre los datos descritos. Por otro lado, cuando la amplitud del ruido aleatorio aditivo es superior a los 5 dB, los valores de CC disminuyen significativamente y la degradación de la imagen aumenta rápidamente. Este comportamiento es similar al que se presenta para un solo dato sometido a las mismas adición de ruido (ver 5.12)). Estos resultados corroboran la solidez del esquema experimental y su capacidad para hacer frente a las pérdidas debidas a la transmisión o el almacenamiento.

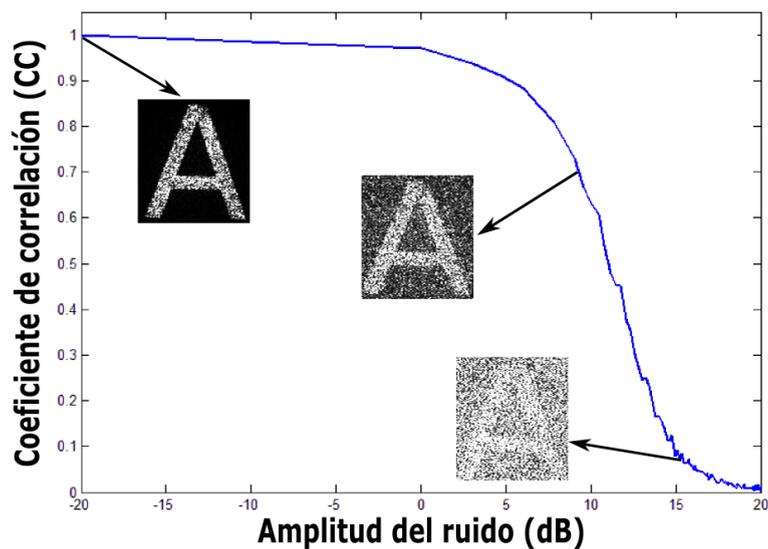


Figura 5.12: Coeficiente de correlación en función de la amplitud del ruido para un objeto recuperado a partir de datos multiplexados con y sin ruido aleatorio.

5.5.4. Teclado encriptado

Una aplicación que se puede establecer a partir del protocolo de protección de datos múltiples con recuperación selectiva, es la implementación experimental de un teclado óptico que permita proteger mensajes de cualquier longitud. En este caso, se encriptan las letras minúsculas y mayúsculas del alfabeto, lo que representa 52 caracteres. Cada letra es encriptada y muestreada por una máscara binaria aleatoria ortogonal. Posteriormente, los 52 datos

cifrados y muestreados son multiplexados lo que permite obtener el teclado óptico cifrado. En este caso, debido a la cantidad de datos cifrados y muestreados, las MBAOs tienen solo un 1,92% de píxeles blancos. Para emplear correctamente el teclado óptico encriptado, un usuario autorizado debe tener el multiplexado con los datos encriptados junto con el conjunto completo de MBAOs asociado a los caracteres que conforman la información relevante que se desea recuperar. Luego, para garantizar que cada carácter del mensaje aparezca en la posición deseada en el plano de recuperación, cada dato codificado seleccionado se multiplica por una función de fase constante que contiene la información correspondiente a las coordenadas finales del objeto asociado a esa MBAO [9]. De acuerdo con lo anterior, el j -ésimo dato cifrado seleccionado y multiplicado por la función de fase de posicionamiento será,

$$E_j(\nu, \omega) = (C_z(\nu, \omega))_j \times L_z^*(\nu, \omega) \times m_j(\nu, \omega) \times p_j(\nu, \omega) \quad (5.17)$$

donde $p_j(\nu, \omega)$ representa la función de fase utilizada para posicionar el j -ésimo dato desencriptado en el plano de recuperación. Después de llevar a cabo la multiplicación del dato seleccionado por la función de fase, se realiza el procedimiento de desencriptación con máscaras descrito en la Sección 5.5.3. Como se observa en la Fig. 5.13, el posicionamiento correcto de cada dato desencriptado permite una lectura exitosa y rápida de la información, por lo tanto un usuario autorizado, con la información asociada al teclado óptico encriptado y la clave de encriptación, podrá acceder al mensaje correcto usando secuencialmente el conjunto correcto de MBAOs y llevando a cabo el proceso de desencriptación con la información de la llave de recuperación. Debido a que la longitud del mensaje depende de la cantidad de MBAOs usadas en el proceso de muestreo y en este caso se usó el alfabeto completo, este método de encriptación y recuperación permite proteger mensajes de cualquier longitud. Se debe destacar que cuando el proceso de recuperación se realiza utilizando únicamente el conjunto de MBAOs, sin la función de fase de posicionamiento, todos los caracteres se recuperan en la misma posición, esto genera una superposición de todos los datos en el plano de recuperación impidiendo la lectura del mensaje (ver Fig 5.13). Por otro lado, cuando el proceso de recuperación se realiza utilizando las MBAOs y el protocolo de posicionamiento,

se accede a la mensaje codificado (Fig. 5.13). Con el objetivo de mostrar como se realizaría la recuperación de un mensaje en tiempo real, en el vídeo 1 (<https://bit.ly/3DG8G8E>) se presenta la recuperación dinámica del mensaje completo mostrado en la Fig. 5.13. Dado que cada letra se recupera en su orden respectivo, es posible leer el mensaje completo en el plano de salida. Además, se debe destacar que la combinación entre del multiplexado con MBAOs y el posicionamiento mediante la función de fase de posicionamiento hace que sea muy complicado para un intruso inferir cuántos y qué caracteres contienen el paquete de datos, incluso si el intruso tiene la información de multiplexado, la llave de cifrado y las MBAOs, la cantidad de posibilidades para posicionar aleatoriamente las letras hace difícil que este pueda acceder a la información codificada. Por lo tanto, entre mayor sea la longitud del mensaje enviado, más complicado le será a un atacante acceder a la información codificada.

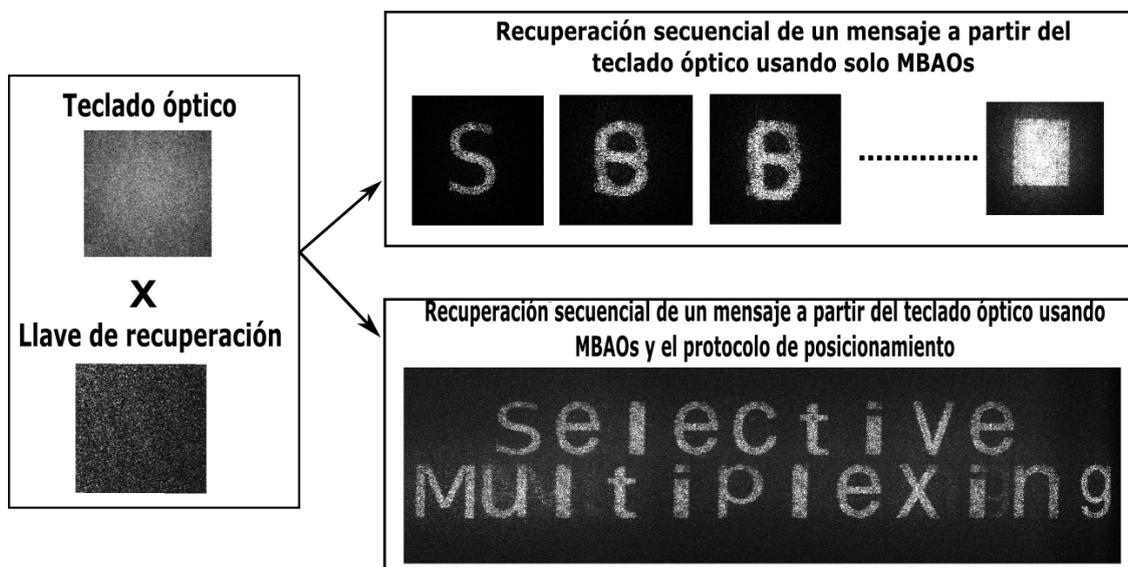


Figura 5.13: Recuperación de un mensaje a partir del teclado óptico encriptado usando MBAOs con y sin protocolo de posicionamiento.

5.5.5. Recuperación experimental de un mensaje a partir del teclado óptico

Para corroborar la versatilidad del protocolo de recuperación selectiva, se implementó una configuración que permitió la recuperación experimental del mensaje usando el protocolo descrito. En este caso, se utilizó un modulador espacial de luz (MEL) PLUTO-2-VIS-016 con un tamaño de pixel de $8 \mu m \times 8 \mu m$ y una resolución de 1920×1080 pixeles. Para la iluminación del plano de proyección se usó un láser LaserGlow LCS-0532-TOC-00050-05 con una longitud de onda de 532 nm y una potencia de $59,9 \text{ mW}$. El medio de registro fue una cámara CMOS con un tamaño de pixel de $1,6 \mu m \times 1,6 \mu m$ y una resolución de 3840×2848 pixeles.

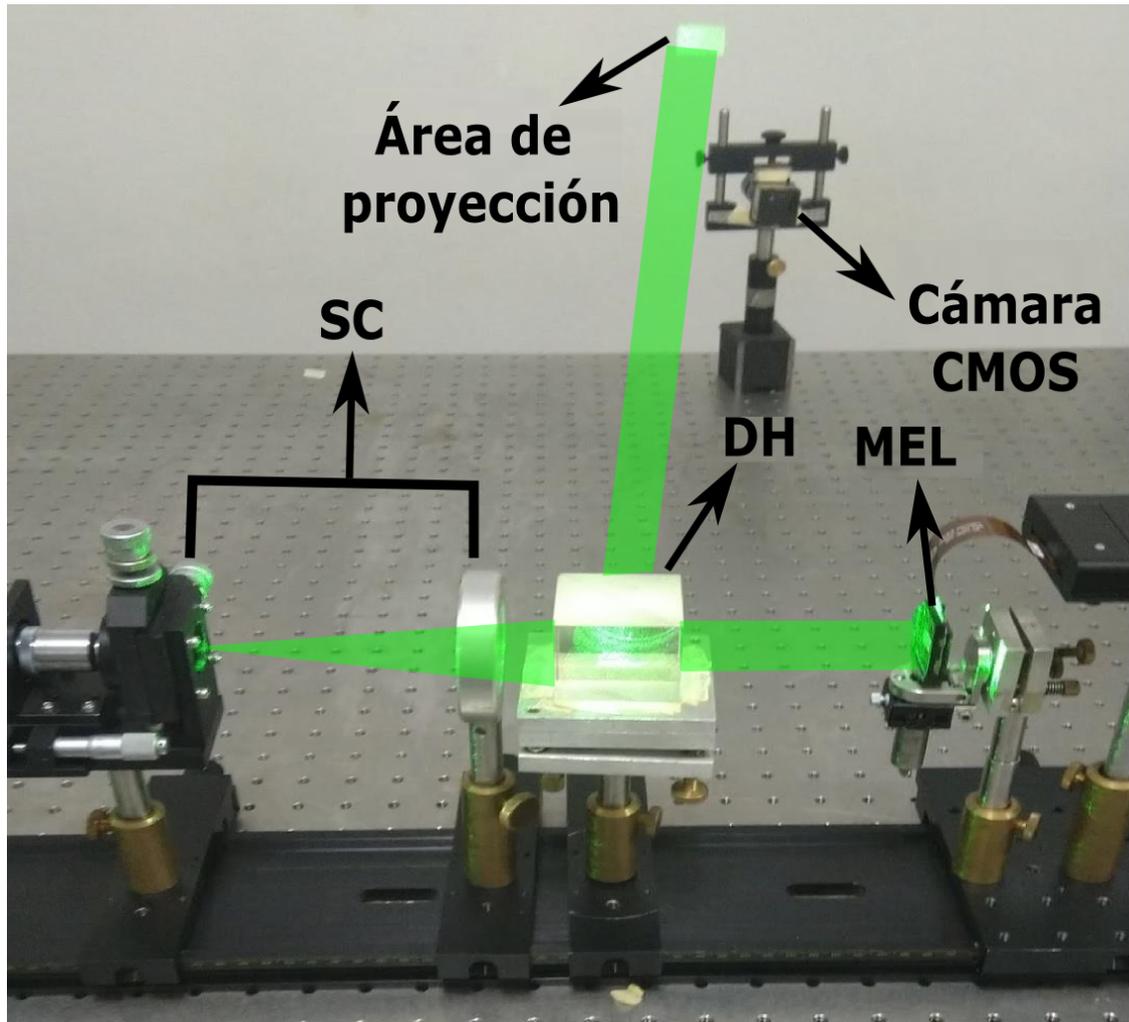


Figura 5.14: Esquema experimental para la recuperación de mensajes a partir del teclado óptico. SC: sistema de colimación, DH: divisor de haz, MEL: modulador espacial de luz.

Para llevar a cabo la recuperación experimental, primero se multiplican los datos multiplexados por la llave de seguridad y luego estos datos son multiplicados por cada una de las MBAOs asociadas al mensaje que se desea transmitir. Al resultado anterior se le extrae la fase; esta es multiplicada por una función de fase de posicionamiento y una fase fija correspondiente a la de una lente, esto último posibilita la reconstrucción sin necesidad de lentes físicas, permite controlar la posición del plano de reconstrucción y evita la luz no difractada procedente del MEL que reduciría la calidad de la información recuperada. Posteriormente, esta información es proyectada en el MEL e iluminada por una onda plana (ver Fig. 5.14) y la recuperación óptica es registrada usando una cámara CMOS como se muestra en la Fig.

5.14. Este procedimiento se repite para cada dato del paquete multiplexado perteneciente al mensaje enviado, la función de fase de posicionamiento garantiza que cada letra se situó de forma correcta en el plano de recuperación y de esta forma se puede recuperar un mensaje completo. Finalmente, cada dato recuperado se combina de manera secuencial para generar la recuperación dinámica mostrada en el vídeo 2 (<https://bit.ly/3SL1Lzk>). El mensaje final será la combinación de todos los caracteres recuperados y posicionados correctamente, como se observa en la Fig. 5.15 (último fotograma del vídeo 2).

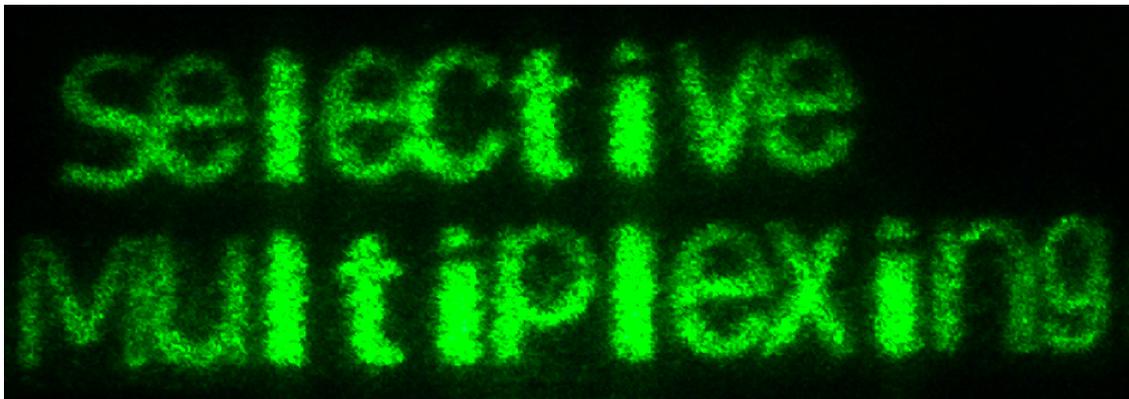


Figura 5.15: Recuperación experimental de un mensaje desde un teclado óptico encriptado utilizando MBAO y un protocolo de posicionamiento.

Los resultados experimentales que se muestran en la Fig. 5.15 demuestran que a pesar de la pérdida debida al muestreo, es posible una recuperación experimental satisfactoria. El protocolo de recuperación selectiva propuesto e implementado se realiza de forma opto-digital sin la necesidad de piezas móviles en las configuraciones experimentales. Se debe tener en cuenta que, en algunas técnicas de multiplexación, el plano de reconstrucción contiene los datos recuperados y el ruido debido a la información no descriptada, este ruido puede afectar la información relevante al generar degradación en la información recuperada, además de que permite reconocer la cantidad de datos encriptados [36]. Por el contrario, en el protocolo de multiplexado selectivo, gracias al proceso de muestreo el plano de recuperación solo contiene los datos recuperados asociados a las MBAOs utilizadas, por lo cual ningún usuario podrá determinar si hay más datos cifrados. Por otro lado, cuando el proceso de recuperación se lleva a cabo solo con la información del paquete multiplexado y la llave de cifrado $L_z(\nu, \omega)$, se obtendrán todos los datos recuperados superpuestos, lo que impedirá acceder a la infor-

mación correcta, esta característica aumenta la seguridad del procedimiento ya que ningún usuario podrá acceder a los mensajes cifrados solo con la información de los datos multiplexados y la información de la llave. Lo anterior permite concluir que las MBAOs actúan como llaves de seguridad adicionales pues permiten seleccionar la información requerida dentro del teclado óptico.

Por otro lado, otra mejora de seguridad que introduce este protocolo se puede notar al reescribir los datos encriptados muestreados y multiplexados (Ec. 5.12) como,

$$M(\nu, \omega) = E_j(\nu, \omega)m_j(\nu, \omega) + \sum_{i \neq j}^N E_i(\nu, \omega)m_i(\nu, \omega) \quad (5.18)$$

donde $E_j(\nu, \omega)$ es el término que contiene los datos cifrados relevantes para el usuario autorizado j -ésimo y el segundo término $\sum_{i \neq j}^N E_i(\nu, \omega)m_i(\nu, \omega)$ son los demás datos cifrados muestreados pertenecientes al multiplexado. De acuerdo con la Ec. 5.18, al realizar el proceso de recuperación con la llave correcta, pero sin las MBAOs correspondientes a un mensaje codificado, debido a la presencia del segundo término en la Ec. 5.18, se obtendrá la superposición de todos los caracteres descifrados en el plano de recuperación, dificultando la recuperación de un dato del paquete multiplexado. Esta característica podría mejorar la seguridad general del sistema y tiene el potencial de hacer que el esquema sea resistente a los ataques tipo delta de Dirac [18] o ataques en los que el intruso tiene acceso a uno o más textos planos y sus respectivos textos cifrados [37, 38], este comportamiento es similar al descrito en el capítulo anterior. En este sentido, cada dato muestreado encriptado podría comportarse como datos criptográficos que sirven para muestrear a los demás datos, haciendo las veces de una función tipo “salteado” [21], lo que conduce a una mejora de la seguridad del general procedimiento.

5.6. Conclusiones

En este capítulo se demuestra la viabilidad experimental del sistema de encriptación óptica JFSC con un solo brazo de iluminación. La implementación experimental de este sistema permite una reducción en la cantidad de elementos utilizados en comparación con el criptosistema JFSC convencional, manteniendo las mismas características de seguridad y versatilidad. La configuración experimental ofrecida por el JFSC de un solo brazo de iluminación ofrece importantes ventajas tangibles, como una estructura compacta, con bajos requisitos de alineación y estabilidad, y menor cantidad de equipo en comparación con otros criptosistemas que requieren un brazo de referencia para registrar la llave de recuperación. Además, el esquema JFSC con un solo brazo de iluminación permite incluir un protocolo basado en CCOS que posibilita la recuperación de la información libre de ruido y degradación. Todas estas ventajas hacen de este esquema una opción para aplicaciones prácticas, como por ejemplo, configuraciones de cifrado óptico portátiles. Por otro lado, se demuestra que la resistencia a la oclusión del CCOS encriptado permite una reducción significativa en el volumen ocupado por la información encriptada, lo que hace que este enfoque sea atractivo para aplicaciones donde se deben manejar grandes cantidades de datos de manera segura. Además, las técnicas de reducción de ruido incluidas en el proceso de encriptación y recuperación conducen a un aumento de la seguridad del esquema.

Por otro lado, se demostró la viabilidad experimental que posee este sistema para admitir un protocolo de recuperación selectiva a partir de un muestreo del dato encriptado con máscaras binarias aleatorias ortogonales (MBAOs). En este sentido, se demostró que gracias a la alta redundancia que presentan los datos registrados holográficamente es posible muestrear objetos con MBAOs de 1,92 % de píxeles blancos, multiplexarlos y recuperar la información. Además, este protocolo de multiplexado selectivo con MBAOs asegura la recuperación de los datos seleccionados, evitando el solapamiento de la información descifrada con los demás datos contenidos en el paquete multiplexado. Por otro lado, la recuperación individual que se logra mediante el uso de MBAOs elimina la posibilidad de reconocer la cantidad de datos encriptados contenidos en el paquete multiplexado, lo que lleva a un aumento en la segu-

ridad del sistema en comparación con algunas técnicas de multiplexación convencionales. Las ventajas experimentales del protocolo de multiplexado selectivo permite el desarrollo de un teclado óptico codificado, en el que cada letra se selecciona con una máscara dentro del conjunto de MBAO utilizadas para muestrear cada dato encriptado. En este caso, para reconstruir correctamente un mensaje, se debe tener la información del multiplexado, la información de la llave de recuperación, el conjunto de MBAOs, y aplicar correctamente el procedimiento de reposicionamiento y recuperación para acceder a la información original de manera exitosa. Además, se implementó un sistema experimental para llevar a cabo una recuperación experimental. Este esquema permite la reconstrucción experimental de cada letra de manera individualmente, y después de llevar a cabo el procedimiento de posicionamiento de las letras recuperadas, se pueden leer mensajes de cualquier longitud. A parte de las ventajas en cuanto el procesamiento propio de información, las características del multiplexado selectivo pueden conducir a una mayor resistencia tanto a los ataques tipo delta de Dirac como a los ataques en los que el intruso tiene acceso a uno o más textos planos (objetos a encriptar) y sus respectivos textos cifrados (objeto encriptado), sin embargo esta característica debe ser sujeto de estudio y corroboración en futuras investigaciones. Cabe resaltar que el protocolo basado en MBAOs puede ser extendido a otros esquemas de codificación óptica, incluidos los sistemas de que procesan información 3D (tres dimensiones) u objetos cuya reconstrucción se de en diferentes planos.

La implementación experimental del sistema JFSC de un solo brazo de iluminación, en conjunto con los protocolos de reducción de ruido y el multiplexado, en combinación con sistemas de proyección como los dispositivos digitales de microespejos podría llevar al desarrollo de un sistema de codificación de alta aplicabilidad, con un alto desempeño para el procesamiento de información y de bajo costo, convirtiéndose en una atractiva alternativa a los sistemas de codificación ya existentes.

Todos los resultados presentados en este capítulo, como se observa en la sección de anexos, fueron presentados en un evento científico a nivel internacional [39] y publicados en revista internacional como producto de la investigación llevada a cabo durante el doctorado [32, 33]

Bibliografía

- [1] J.A. JARAMILLO-OSORIO, A. VELEZ-ZEA, H. CABRERA, J. NIEMELA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Optical encryption using phase modulation generated by thermal lens effect.** J. Opt. 2022;24:025702.
- [2] J.F. BARRERA-RAMÍREZ, E. RUEDA, C. RIOS, M. TEBALDI, N. BOLOGNINI, R. TORROBA. **Experimental opto-digital synthesis of encrypted sub-samples of an image to improve its decoded quality.** Opt. Commun. 2011;284:4350-5.
- [3] J.M. VILARDY, M.S. MILLÁN, E. PÉREZ-CABRÉ. **Improved decryption quality and security of a joint transform correlator-based encryption system.** J. Opt. 2013;15:025401.
- [4] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Experimental optical encryption of grayscale information.** Appl. Opt. 2017;56:5883-9.
- [5] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Innovative speckle noise reduction procedure in optical encryption.** J. Opt. 2017;19:055704.
- [6] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Optimized random phase encryption.** Opt. Lett. 2018;43:3558-61.
- [7] J.F. BARRERA-RAMÍREZ, A. MIRA-AGUDELO, R. TORROBA. **Optical encryption and QR codes: secure and noise-free information retrieval.** Opt. Express. 2013;21:5373-8.

- [8] J.F. BARRERA-RAMÍREZ, A. MIRA-AGUDELO, R. TORROBA. **Experimental QR code optical encryption: noise-free data recovering.** *Opt. Lett.* 2014;39:3074-7.
- [9] J.F. BARRERA-RAMÍREZ, A. VELEZ-ZEA, R. TORROBA. **Experimental scrambling and noise reduction applied to the optical encryption of QR codes.** *Opt. Express.* 2014;22:20268-77.
- [10] P.A. CHEREMKHIN, V.V. KRASNOV, V.G. RODIN, R.S. STARIKOV. **QR code optical encryption using spatially incoherent illumination.** *Laser Phys. Lett.* 2017;14:026202.
- [11] J. WANG, L. SONG, X. LIANG, Y. LIU, P. LIU. **Secure and noise-free nonlinear optical cryptosystem based on phase-truncated Fresnel diffraction and QR code.** *Opt. Quantum Electron.* 2016;48:1-11.
- [12] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Customized data container for improved performance in optical cryptosystems.** *J. Opt.* 2016;18:125702.
- [13] Y. QIN, Y. ZHANG. **Information encryption in ghost imaging with customized data container and XOR operation.** *IEEE Photonics J.* 2017;9:1-8.
- [14] Y. QIN, Z. WANG, H. WANG, Q. GONG, N. ZHOU. **Robust information encryption diffractive-imaging-based scheme with special phase retrieval algorithm for a customized data container.** *Opt. Lasers Eng.* 2018;105:118-24.
- [15] S. LIANSHENG, D. CONG, X. MINJIE, T. AILING, A. ANAND. **Information encryption based on the customized data container under the framework of computational ghost imaging.** *Opt. Express.* 2019;27:16493-506.
- [16] C. LI, Y. ZHANG, E.Y. XIE. **When an attacker meets a cipher-image in 2018: A year in review.** *J. Inf. Secur. Appl.* 2019;48:102361.
- [17] C. ZHANG, M. LIAO, W. HE, X. PENG. **Ciphertext-only attack on a joint transform correlator encryption system.** *Opt. Express.* 2013;21:28523-30.

- [18] A. CARNICER, M. MONTES-USATEGUI, S. ARCOS, I. JUVELLS. **Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys.** Opt. Lett. 2005;30:1644-6.
- [19] M. LIAO, W. HE, D. LU, X. PENG **Ciphertext-only attack on optical cryptosystem with spatially incoherent illumination: from the view of imaging through scattering medium.** Sci. Rep. 2017;7:1-9.
- [20] Y. FRAUEL, A. CASTRO, T.J. NAUGHTON, B. JAVIDI. **Resistance of the double random phase encryption against various attacks.** Opt. Express. 2007;15:10253-65.
- [21] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Cryptographic salting for security enhancement of double random phase encryption schemes.** J. Opt. 2017;19:105703.
- [22] K. FALAGGIS, A.H.R. ANDRADE, J.G.G. LUNA, C.G. OJEDA, R. PORRAS-AGUILAR. **Optical encryption with protection against Dirac delta and plain signal attacks.** Opt. Lett. 2016;41:4787-90.
- [23] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Secure real-time generation and display of color holographic movies.** Opt Lasers Eng. 2019;122:239-44.
- [24] G.K. WALLACE. **The JPEG still picture compression standard.** Commun. ACM. 1991;34:30-44.
- [25] R. SHAHNAZ, J.F. WALKUP, T.F. KRILE. **Image compression in signal-dependent noise.** Appl. Opt. 1999;38:5560-7.
- [26] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, S. TREJOS, M. TEBALDI, R. TORROBA. **Optical field data compression by opto-digital means.** J. Opt. 2016;18:125701.
- [27] S. TREJOS, A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, M. TEBALDI, R. TORROBA. **Optical approach for the efficient data volume handling in experimentally encrypted data.** J. Opt. 2016;18:065702.

- [28] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Cross-talk free selective reconstruction of individual objects from multiplexed optical field data.** *Opt. Lasers Eng.* 2018;100:90-7.
- [29] S. TREJOS, A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, M. TEBALDI, R. TORROBA. **Compression of multiple 3D color scenes with experimental recording and reconstruction.** *Opt. Lasers Eng.* 2018;110:18-23.
- [30] A. VELEZ-ZEA, A. VILLAMIZAR-AMADO, M. TEBALDI, R. TORROBA. **Alternative representation for optimized phase compression in holographic data.** *OSA Contin.* 2019;2:572-81.
- [31] H. GU, G. JIN. **Phase-difference-based compression of phase-only holograms for holographic three-dimensional display.** *Opt. Express* 2018;26:33592-603.
- [32] J.A. JARAMILLO-OSORIO, J.F. BARRERA-RAMÍREZ, A. MIRA-AGUDELO, A. VELEZ-ZEA, R. TORROBA. **High performance compact optical cryptosystem without reference arm.** *J. Opt.* 2020;22:035702.
- [33] J.A. JARAMILLO-OSORIO, J.F. BARRERA-RAMÍREZ, A. MIRA-AGUDELO, A. VELEZ-ZEA, R. TORROBA. **Secure selective recovery protocol for multiple optically encrypted data.** *Opt Lasers Eng.* 2021;137:106383.
- [34] E.RUEDA, J.F. BARRERA-RAMÍREZ, R. HENAO, R. TORROBA. **Optical encryption with a reference wave in a joint transform correlator architecture.** *Opt. Commun.* 2009;282:3243-9.
- [35] J.F. BARRERA-RAMÍREZ, J.A. JARAMILLO-OSORIO, A. VELEZ-ZEA A, R. TORROBA. **Experimental analysis of a joint free space cryptosystem.** *Opt. Lasers Eng.* 2016;83:126-30.
- [36] J.A. JARAMILLO-OSORIO, J.F. BARRERA-RAMÍREZ, A. VELEZ-ZEA, R. TORROBA R. **Fractional optical cryptographic protocol for data containers in a noise-free multiuser environment** *Opt. Laser. Eng.* 2018;119:25.

- [37] X. PENG, P. ZHANG, H. WEI, B. YU. **Known-plaintext attack on optical encryption based on double random phase keys.** *Opt. Lett.* 2006;31:1044–6.
- [38] J.F. BARRERA-RAMÍREZ, C. VARGAS, M. TEBALDI, R. TORROBA, N. BOLOGNINI. **Known-plaintext attack on a joint transform correlator encrypting system.** *Opt. Lett.* 2010;35:3553–5.
- [39] J.A. JARAMILLO-OSORIO, J.F. BARRERA-RAMÍREZ, A. MIRA-AGÚDELO, A. VÉLEZ, R. TORROBA. **Sistema de encriptación de un solo brazo en el dominio de Fresnel.** X Reunión Iberoamericana de Óptica y XIII Reunión Iberoamericana de Óptica, Láseres y Aplicaciones (RIAO/OPTILAS). Cancún, Mexico. 2019. (enlace: <https://bit.ly/3VbhbyK>).

Capítulo 6

Holografía digital usando como sistema de proyección un dispositivo digital de microespejos

La holografía digital es una técnica importante en el campo de la óptica que posibilita aplicaciones relevantes y de alto impacto como la microscopía holográfica [1], la metrología [2], la seguridad óptica [3, 4], entre otras. En particular, la holografía digital permite el registro digital de un campo óptico para su posterior procesamiento a partir de técnicas computacionales [5–8], de esta manera dicho campo puede ser comprimido, transmitido, encriptado, analizado y reconstruido sin la necesidad de un esquema óptico físico.

En general, dependiendo de la aplicación que se desee realizar, hay diversas configuraciones experimentales que permiten ejecutar la técnica de la holografía digital, las cuales se clasifican según el tipo de configuración experimental, el tipo de holograma que se registra de acuerdo al objeto de entrada, el dominio óptico o tipo de transformada que se realiza entre la entrada y el plano de registro [9]. En particular, las configuraciones utilizadas para registrar los hologramas digitales son de particular interés, en estas se proyecta la informa-

ción a procesar en el plano de entrada del sistema, generalmente por medio de un modulador espacial de luz (MEL) de cristal líquido u otra pantalla direccionable digitalmente [10, 11]. Con lo anterior se logra la conversión de los datos de entrada en un holograma digital, el cual puede ser posteriormente procesado opto-digitalmente. Aunque la conversión de un dato de entrada en un holograma pueda lograrse por medio de algoritmos de holografía generados por computadora, el uso de un esquema experimental de holografía digital aprovecha todos los grados de libertad de la luz como la polarización [12], el momento orbital angular [13], la coherencia [14], los cuales son difíciles de tener en cuenta dentro de algoritmos computacionales y que experimentalmente pueden ser usados para mejorar los procesos de manipulación de la información. Las ventajas que poseen los sistemas experimentales utilizados para el registro holográfico de información, hacen de estos la piedra angular de muchas configuraciones de cifrado óptico y métodos de procesamiento óptico de información.

Generalmente, los esquemas holográficos usan un MEL como dispositivo para la proyección de los datos, estos dispositivos pueden modular la fase y la amplitud del campo óptico y han sido utilizado como pantallas holográficas [15], dispositivos para la corrección de aberraciones [16], trampas ópticas [17], entre otros. A pesar de su alta demanda dentro de los esquemas ópticos, estos elementos tiene un costo elevado, ofrecen una resolución limitada y generalmente presentan frecuencias de actualización de pantalla bajas, lo que conduce a limitaciones en muchos aplicaciones experimentales. Buscando solventar estas limitantes, se han empezado a estudiar otros dispositivos para la proyección de información, recientemente los dispositivos digital de microespejos (DDM) han venido convirtiéndose en una interesante alternativa a los MEL de cristal líquido. Los DDM permiten la modulación de amplitud a partir de la luz que se refleja en la matriz de microespejos que lo conforman. Además, cada microespejo dentro de la matriz puede inclinarse individualmente lo que permite la proyección de entradas binarias de amplitud. Por otro lado, los costos de fabricación de los DDM son bajos y tiene frecuencias de actualización significativamente más altas que los MEL de cristal líquido [18], razones por las cuales los DDM han reemplazado a los MEL en aplicaciones comerciales como proyectores de vídeo, y en investigaciones recientes se ha demostrado su utilidad para una amplia gama de técnicas, como en el procesamiento de imágenes coherentes en sistemas sin lentes [19], compresión y detección de campos ópticos [20], detección

remota [21], detección de frentes de onda [22], polarimetría [23] y generación de vórtice ópticos [24, 25], por mencionar algunas. También, se han utilizado DDMs en la modulaciones conjuntas de amplitud y fase, la cual ha sido probada mediante hologramas generados por computador [26].

Como se mencionó anteriormente, en el caso de la holografía digital, una vez que se obtiene el registro del campo óptico asociado al holograma, existe una amplia gama de técnicas de procesamiento opto-digital que pueden ser implementadas y que facilitan la manipulación de la información registrada. Generalmente, estas técnicas han sido aplicadas a hologramas digitales obtenidos a partir de configuraciones que utilizan un MEL como dispositivo de entrada. Con el objetivo de solventar algunas de las desventajas que genera el uso de MEL y desarrollar nuevas técnicas que permitan la manipulación holográfica de la información, se quiere probar la eficacia y viabilidad de las técnicas y/o procesos holográficas ya implementadas dentro de un configuración que utilice DDMs en lugar de MEL.

Para analizar la efectividad y versatilidad del DDM como sistema de proyección, se emplea dentro de un sistema holográfico fuera de eje en los dominios de Fresnel y Fourier. Particularmente, debido a las limitaciones en el rango dinámico de la cámara CMOS usada en el registro del holograma, es necesario usar máscaras de fase aleatorias para garantizar el registro adecuado de los hologramas de Fourier. Aunque las máscaras permiten el registro de la información, también introducen ruido y degradación en el dato recuperado. Para solventar esta desventaja se usan técnicas no lineales de reducción de ruido, las cuales ayudan a disminuir los efectos de la máscara aleatoria de fase sobre el dato recuperado reduciendo el ruido y la degradación en la información reconstruida [27, 28].

Además de lo anterior, se demuestra que los hologramas registrados en ambos dominios con la configuración basada en el DDM conserva las características básicas de los hologramas digitales registrados en sistemas convencionales que emplean MELs. Adicionalmente, se analiza el desempeño del sistema propuesto a partir de la implementación de técnicas de multiplexado que permitan la manipulación de múltiples datos. En el multiplexado se combinan múltiples datos de campos óptico en uno solo dato, lo que facilita el almacenamiento,

la transmisión y la manipulación de datos holográficos sin incrementar los requerimientos experimentales y/o computacionales. Dentro de las aplicaciones del multiplexado, se encuentra el multiplexado de datos ópticamente codificados, que permite un manejo rápido y seguro de la información, mejorando el desempeño de los sistemas de codificación óptica y posibilita la implementación de entornos multiusuario [29–31]. Por otra parte, en holografía y compresión de datos, la multiplexación permite: la reconstrucción en un solo paso de múltiples datos de campo óptico [32, 33], el desarrollo de pantallas holográficas a color [15], la compresión de escenas en color [34], entre otras aplicaciones. En general hay varios métodos de multiplexado óptico, entre estos se destacan el multiplexado angular [35], el multiplexado por desplazamiento de máscara [36] y el multiplexado por rotación de la polarización del haz [12].

Con el propósito de analizar el desempeño del sistema holográfico usando el DDM para el procesamiento de múltiples datos, se emplea una técnica de multiplexado espacial para la reconstrucción de un vídeo holográfico, esta técnica consiste en proyectar y registrar los fotogramas del vídeo individualmente y luego obtener un paquete que contiene todo el vídeo en un solo dato de campo óptico. Este procedimiento ya se ha realizado a partir de modulación theta [4, 37], multiplexado espacial [38] y muestreo con máscaras binarias [39, 40], pero en todas estas configuraciones se usan MELs en lugar de DDMs como dispositivos para la proyección de la información de entrada.

Finalmente, se usa el concepto de contenedor de información a partir del uso de códigos QR (quick response), para obtener una recuperación libre de ruido y degradación [41, 42]. El uso de QRs como contenedores de información ya ha sido verificado e implementado dentro de arquitecturas de encriptación 4f [41] y JTC (siglas en inglés de: joint transform correlator) [42, 45]. El uso de códigos QR genera una ventaja extra dentro de la configuración experimental, ya que estos posibilitan la recuperación holográfica de datos cuya complejidad o longitud son difíciles de procesar de manera directa en el sistema óptico.

Los resultados teóricos y experimentales presentados en este capítulo son productos originales del trabajo de investigación doctoral [46]. La experiencia y herramientas adquiridas con el uso de los DDMs en holografía digital serán la base para el desarrollo de una ar-

arquitectura de codificación óptica con un esquema compacto, de bajo costo que posibilite la generación de nuevas aplicaciones en el campo de la óptica basadas en la implementación de estas tecnologías.

6.1. Holografía digital en el dominio de Fourier y Fresnel usando un DDM

6.1.1. Registro, filtrado y recuperación de un holograma de Fourier

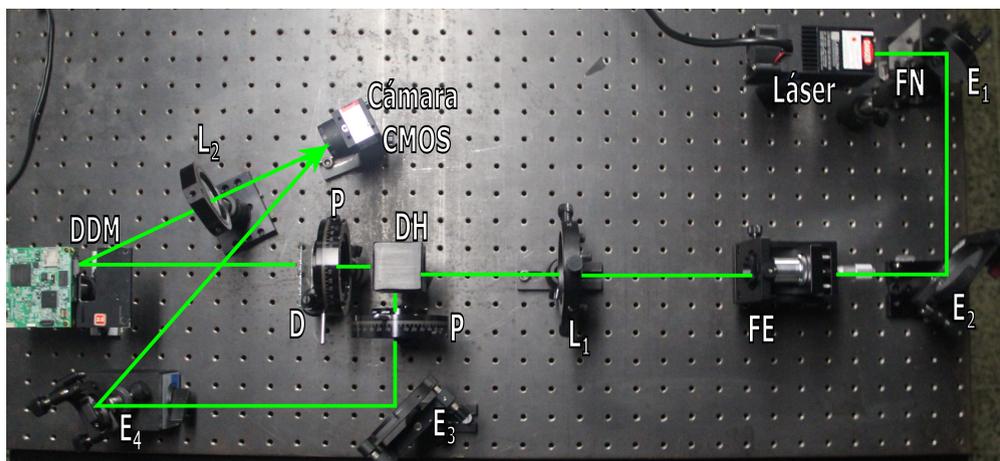


Figura 6.1: Configuración experimental para el registro holográfico en el dominio de Fourier. FN: filtro de neutro, E: espejos, FE: filtro espacial, L: lente, DH: divisor de haz, P: polarizador, D: difusor y DDM: dispositivo digital de microespejos.

En este sistema, la cámara CMOS y el DDM se encuentran en los planos focales de la lente convergente L_2 (Fig. 6.1). En el plano de entrada del sistema, generado por el DDM, se proyecta el objeto $o(x, y)$, el cual se multiplica por una función de fase $r(x, y)$ resultante del paso de la luz a través de un difusor (vidrio esmerilado) y su posterior propagación hasta el DDM. De acuerdo con esto $f(x, y)$ viene dado por,

$$f(x, y) = o(x, y)r(x, y) \quad (6.1)$$

de acuerdo con lo anterior, en la cámara CMOS se registra el holograma resultante entre la interferencia de la onda plana proveniente del espejo E_4 y la transformada de Fourier (TF) de $f(x, y)$, el cual viene dado por,

$$H(\nu, \omega) = |F(\nu, \omega)|^2 + |W(\nu, \omega)|^2 + F(\nu, \omega)W^*(\nu, \omega) + F^*(\nu, \omega)W(\nu, \omega) \quad (6.2)$$

donde $*$ representa el complejo conjugado, $F(\nu, \omega)$ TF de $f(x, y)$ y $W(\nu, \omega) = \exp\left[-\frac{2\pi i}{\lambda}(\nu\alpha + \omega\beta)\right]$ es la onda plana de referencia de amplitud unitaria proveniente del espejo E_4 . α y β son los ángulos de inclinación de la onda plana sobre la cámara CMOS y λ es la longitud de onda de la fuente de iluminación [47].

El holograma resultante (Ec. 6.2) contiene información no relevante e información redundante que debe ser filtrada. El tercer y cuarto término en la Ec. 6.2 son el holograma del objeto y su complejo conjugado respectivamente, mientras que el primer y segundo término corresponden al orden central. Con el objetivo de extraer la información relevante, que esta contenida en el tercer término de la Ec. 6.2, se realiza un proceso de filtrado [48]. En primer lugar, se bloquea el brazo de referencia y se registra la intensidad de la TF de $f(x, y)$, es decir $|F(\nu, \omega)|^2$. Después, se bloquea el brazo objeto, en el cual se encuentra el DDM, y se registra la intensidad de la onda plana ($|W(\nu, \omega)|^2$). Estos dos términos se le restan al holograma, obteniéndose,

$$H'(\nu, \omega) = F(\nu, \omega)W^*(\nu, \omega) + F^*(\nu, \omega)W(\nu, \omega) \quad (6.3)$$

posteriormente, para finalizar el proceso de filtrado se realiza una TF sobre la Ec. 6.3,

$$n(x, y) = f(x, y) \otimes \delta(x - \lambda\alpha, y - \lambda\beta) + f^*(x, y) \otimes \delta(x + \lambda\alpha, y + \lambda\beta) \quad (6.4)$$

donde \otimes es el operador de convolución y δ es la función delta de Dirac. El primer término de la Ec. 6.4 correspondiente al objeto y el segundo correspondiente al complejo conjugado del objeto. Estos datos se encuentran separados espacialmente, lo cual permite seleccionar el primer término y descartar el segundo. Luego, realizando una transformada de Fourier inversa (TFI) sobre el dato seleccionado se obtiene el dato holográfico de Fourier filtrado, el cual puede ser reposicionado en las coordenadas $x' = 0$ y $y' = 0$.

$$H_f(\nu, \omega) = F(\nu, \omega) \quad (6.5)$$

Este mismo proceso será usado para el filtrado de datos holográficos en el dominio de Fresnel.

Ahora, para llevara cabo el proceso de reconstrucción del holograma, se debe realiza una TFI sobre el dato holográfico de Fourier filtrado (Ec. 6.5). Es importante tener en cuenta que la reconstrucción del objeto presenta degradación y ruido debido al uso del difusor en el plano de entrada, por los cual se implementan técnicas no lineales para la reducción de ruido sobre los datos holográficos [27], y sobre el dato recuperado [28]. En la Fig. 6.2, se puede notar que cuando se realiza el proceso de recuperación directa, sin aplicación de técnicas de reducción de ruido, el dato recuperado presenta mayor degradación debido al ruido de speckle (Fig. 6.2 (a)) en comparación con el dato recuperado cuando se aplican las técnicas de reducción de ruido (Fig. 6.2 (b)).

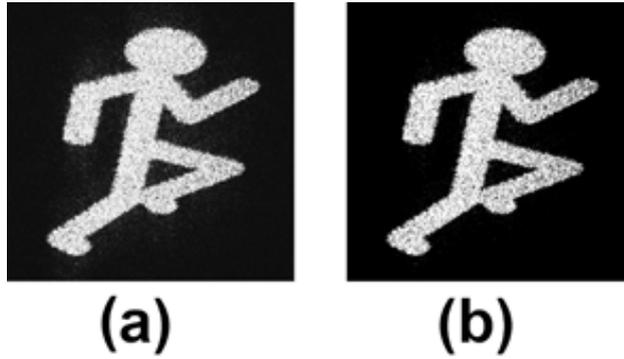


Figura 6.2: Objeto reconstruido: (a) sin la implementación de técnicas de reducción de ruido y (b) después de la aplicación de técnicas no lineales de reducción de ruido.

6.1.2. Registro, filtrado y recuperación de un holograma de Fresnel

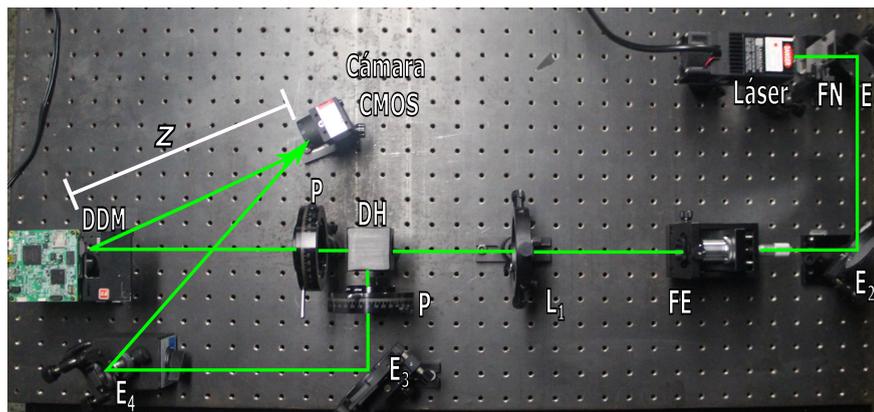


Figura 6.3: Configuración experimental para el registro holográfico en el dominio de Fresnel. FN: filtro de neutro, z : distancia entre el plano de entrada y la cámara, E: espejos, FE: filtro espacial, DH: divisor de haz, P: polarizadores, D: difusor y DDM: dispositivo digital de microespejos.

Para llevar a cabo el registro holográfico en el dominio de Fresnel se emplea la configuración experimental que se muestra en la Fig. 6.3. En este caso, los objetos de entrada no se multiplican por un difusor, y no se ubica una lente transformadora entre el plano del DDM y la cámara CMOS.

Si $s(x, y)$ es la función que se proyecta en el DDM, entonces la intensidad del holograma resultante entre la información reflejada por el DDM, la cual contienen la información de $s(x, y)$, y el haz proveniente del espejo E_4 ubicado en el brazo de referencia, viene dada por [49],

$$H_z(\nu, \omega) = |S_z(\nu, \omega)|^2 + |W_z(\nu, \omega)|^2 + S_z(\nu, \omega)W_z^*(\nu, \omega) + S_z^*(\nu, \omega)W_z(\nu, \omega) \quad (6.6)$$

donde z es la distancia entre el DDM y el cámara CMOS, $S_z(u, v)$ es la transformada de Fresnel (TFr) de $s(x, y)$ y $W_z(\nu, \omega) = \exp\left[-\frac{2\pi iz}{\lambda}(\nu \cos \alpha + \omega \cos \beta)\right]$ es la onda de referencia en el plano de la cámara. α y β son los ángulos de inclinación del haz de referencia en el plano de registro. Aplicando el mismo procedimiento de filtrado y reposicionamiento realizado en la sección anterior, se extrae la información holográfica relevante $S_z(\nu, \omega)$ de la Ec. 6.6. En este caso, para realizar el proceso de recuperación del objeto original, se debe realizar la transformada inversa de Fresnel (TFrI) para una distancia z del dato filtrado,

$$s(x, y) = TFrI_z[S_z(\nu, \omega)] \quad (6.7)$$

En la Fig.6.4(b), se puede observar el dato reconstruido a partir del holograma de Fresnel del objeto de entrada mostrado en la Fig.6.4(a). Se puede notar que la calidad del dato recuperado es comparable con el objeto original. Por otro lado, como no se usa un difusor en el proceso de registro holográfico, se puede apreciar que el dato reconstruido no contiene ruido de speckle.

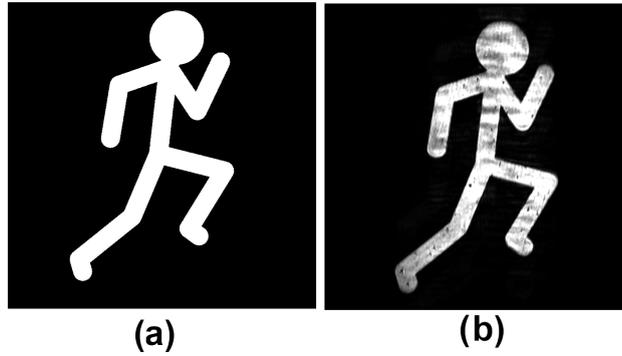


Figura 6.4: Reconstrucción de un holograma en el dominio de Fresnel (a) objeto original y (b) objeto reconstruido.

6.2. Resultados experimentales

Para implementar las configuraciones experimentales para el registro holográfico en los dominios ópticos de Fourier y Fresnel mostrados en la sección anterior, se usó como fuente de iluminación un láser de estado sólido Nd:YAG con una longitud de onda de 532 nm y una potencia de $124,4 \text{ mW}$. En el sistema de Fourier se usó una lente (L_2) de longitud focal de 10 cm . Todos los hologramas se registraron con una cámara CMOS EO-10012M con un tamaño de pixel de $1,67 \times 1,67 \mu\text{m}$ y una resolución de 3840×2748 pixeles. Para la proyección de los objetos se usó un DDM con un tamaño de pixel de $7,637 \times 7,637 \mu\text{m}$ y una resolución de $684 \times 608 \mu\text{m}$ pixeles. Para el sistema holográfico en el dominio de Fresnel las distancias z entre el DDM y la cámara CMOS usadas fueron de $9,50 \text{ cm}$ y $9,85 \text{ cm}$.

Con el objetivo de analizar el desempeño del sistema holográfico en los dominios de Fourier y Fresnel, se realizó el proceso de registro holográfico y la recuperación de un objeto de entrada, los resultados experimentales son mostrados en la Fig. 6.5.

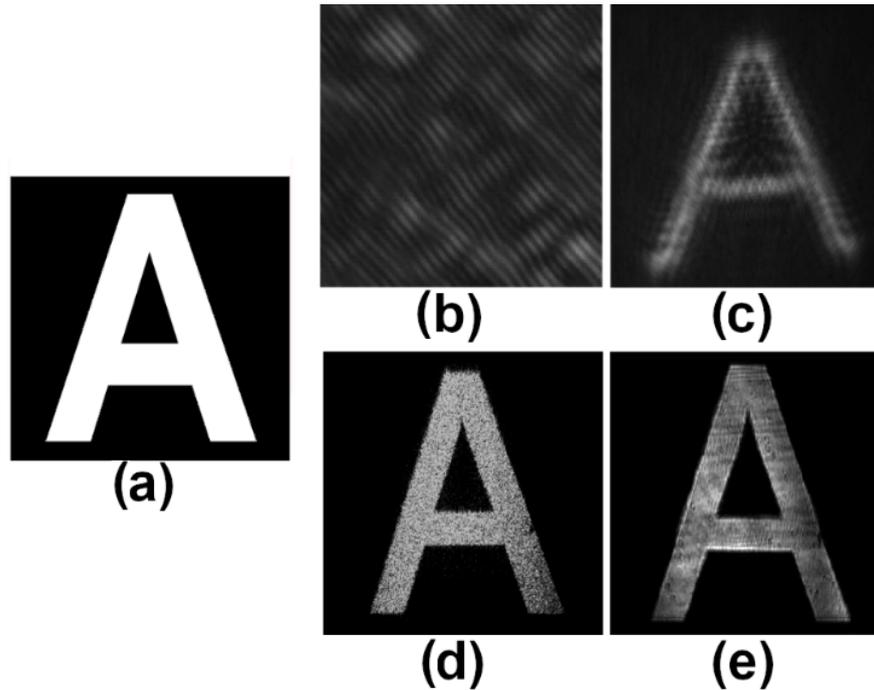


Figura 6.5: Resultados experimentales del proceso de registro holográfico y recuperación para un objeto usando como sistema de proyección un DDM. (a) objeto de entrada, (b) y (c) hologramas registrados en los dominios de Fourier y Fresnel respectivamente, (d) y (e) datos recuperados a partir de (b) y (c) respectivamente.

Las Figs. 6.5(b) y (c), corresponden a la distribución de intensidad registrada por la cámara CMOS de los hologramas de Fourier y Fresnel del objeto de entrada (Fig. 6.5(a)), respectivamente. Al realizar el proceso de reconstrucción, se puede observar que la calidad del dato recuperado en ambos dominios ópticos, Fourier (Fig. 6.5(d)) y Fresnel (Fig. 6.5(e)), presentan una calidad similar, estos resultados demuestran el funcionamiento básico del sistema en ambos dominios ópticos, y muestran la versatilidad del DDM como elemento para la proyección de imágenes binarias de amplitud. Como resultado de lo anterior, se puede establecer que los DDMs son un sistema de proyección que puede ser considerado como una alternativa viable para reemplazar los moduladores espaciales de luz cuando se requiera la proyección de objetos binarios de amplitud.

Con el objetivo de analizar el desempeño del DDM dentro del sistema, se realizó el registro holográfico de objetos de entrada de mayor complejidad. Los resultados son presentados en la Fig. 6.6.

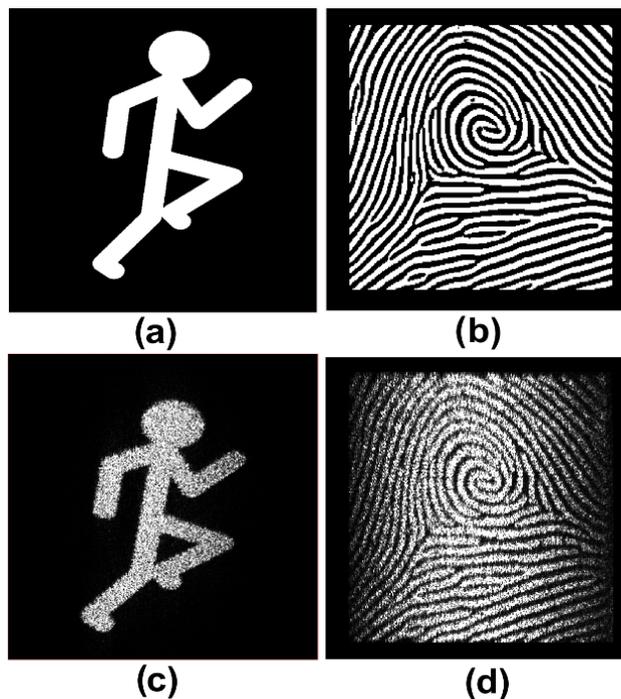


Figura 6.6: Recuperación experimental para diferentes objetos de entrada procesado holográficamente en el dominio de Fourier: (a) y (b) objetos de entrada, (c) y (d) datos recuperados.

Aunque las imágenes recuperadas (Figs. 6.6(c) y (d)) contienen ruido de speckle que no puede ser suprimido completamente a partir de la aplicación de técnicas no lineales de reducción de ruido, la calidad de la reconstrucción no se ve afectada significativamente. En particular, los detalles de la huella dactilar recuperada son distinguibles y comparables con el dato original (Figs. 6.6(b) y (d)).

Por otro lado, para analizar la calidad de la recuperación se realiza el proceso de registro holográfico y filtrado para tres objetos de entrada. Posteriormente, se realiza la recuperación de cada uno de ellos en diferentes planos de reconstrucción alrededor del plano de Fourier. Finalmente, se utiliza la métrica del coeficiente de correlación (CC) para medir la calidad de los datos recuperados en los diferentes planos respecto al dato recuperado en el plano de Fourier. El CC para los tres objetos es mostrado en la Fig. 6.7. Los resultados presentados en la Fig. 6.7 muestran que el valor del CC disminuye rápidamente cuando se realiza el proceso de reconstrucción en un plano diferente al de Fourier, este comportamiento es típico de los

datos registrados en esquemas holográficos en este dominio óptico.

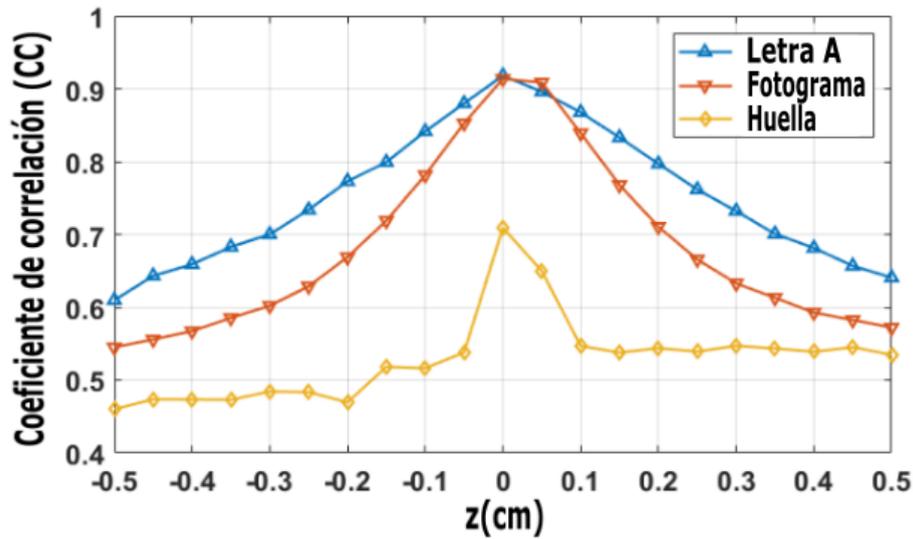


Figura 6.7: Coeficiente de correlación entre los tres objetos originales y sus respectivos objetos recuperados alrededor del plano de Fourier.

Después de analizar el desempeño del sistema holográfico en el dominio de Fourier, se procede a probar la robustez del sistema en el dominio de Fresnel. Como en este caso no se usa un difusor para llevar a cabo el registro holográfico, los datos recuperados (Figs. 6.8(c) y (d)) no presentan ruido de speckle y en relación con los datos originales (Figs. 6.8(a) y (b)) muestran una buena calidad.

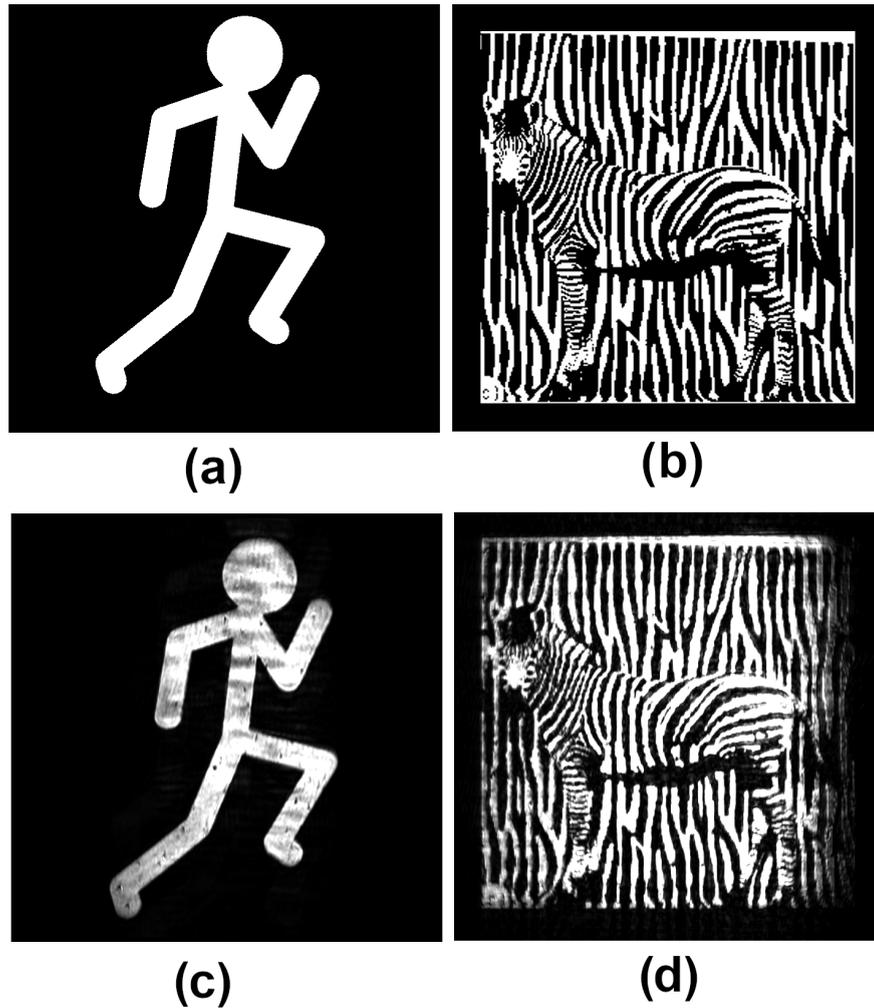


Figura 6.8: Recuperación experimental para diferentes objetos de entrada procesado holográficamente en el dominio de Fresnel: (a) y (b) objetos de entrada, (c) y (d) datos recuperados.

Ahora, para analizar la calidad de la recuperación en relación con el plano de reconstrucción en el dominio óptico de Fresnel, se realiza el proceso de registro holográfico y filtrado para dos objetos de entrada. Posteriormente, se realiza la recuperación de cada uno de los datos para diferentes planos alrededor del plano de recuperación, y se utiliza la métrica del coeficiente de correlación (CC) para medir la calidad de los datos recuperados en los diferentes planos respecto al dato recuperado en el plano óptico de recuperación. El CC para los dos objetos es presentado en la Fig. 6.9.

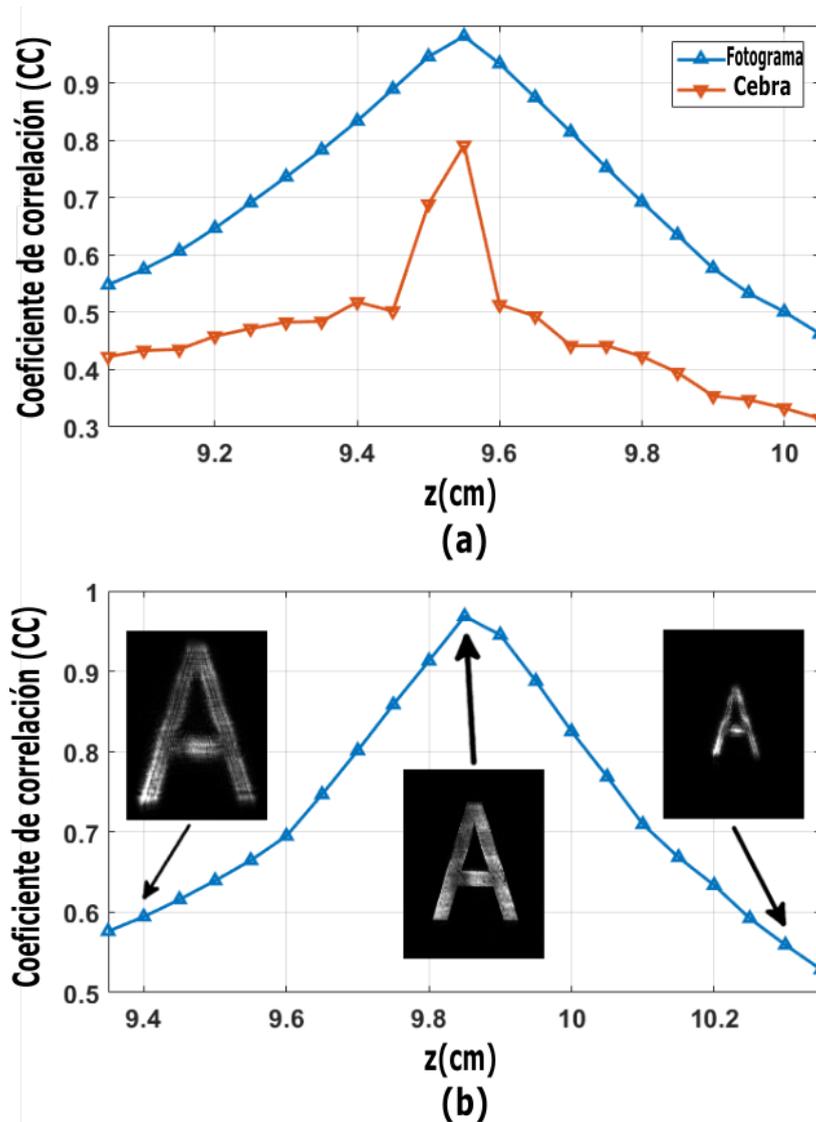


Figura 6.9: a) Coeficiente de correlación entre los datos originales y recuperados después de hacer el proceso de recuperación de diferentes objetos en diferentes planos de reconstrucción. (b) Coeficiente de correlación para un objeto.

En la Fig. 6.9 se puede ver que la calidad del objeto disminuye cuando el plano de reconstrucción es diferente del plano de registro, este comportamiento es típico de los hologramas de Fresnel. Como es de esperar, se observa que el coeficiente de correlación alcanza su máximo cuando el proceso de recuperación se lleva a cabo para un distancia igual a la usada en el proceso de registro.

Los resultados mostrados en esta sección permiten verificar el desempeño del sistema

holográfico en los dominios de Fresnel y Fourier, demostrando que el DDM es una alternativa interesante para la proyección de imágenes de amplitud binarias y que podría sustituir dentro de esquemas holográficos y de encriptación a los moduladores espaciales de luz, disminuyendo los costos de las implementaciones experimentales. Con el fin de explorar la potencialidad del sistema, en la siguiente sección se implementará un protocolo que permite el procesamiento holográfico de escenas dinámicas.

6.2.1. Registro holográfico con recuperación dinámica de datos

El registro holográfico de vídeos es una aplicación donde los DDMs tienen ventajas particulares sobre los moduladores espaciales de luz (MEL), ya que la velocidad a la que la configuración holográfica con un DDM puede registrar diferentes hologramas sólo está limitada por la velocidad de la cámara digital. Esto se debe a que el DDM tiene una tasa de actualización de pantalla más rápida (velocidades hasta 22 kHz) que los cristales líquido de silicio utilizados en los MEL, cuya velocidad de actualización de pantalla es generalmente de 60 Hz, especialmente cuando se trata de entradas binarias. Por otro lado, el registro holográfico de escenas dinámicas presenta desafíos relacionados con la capacidad de almacenamiento efectivo de grandes volúmenes de información, para solucionar esta situación se implementan un protocolo de multiplexación que permite registrar y almacenar eficientemente vídeos holográficos. Para llevar a acabo el procedimiento de multiplexado, inicialmente se registra holográficamente y se filtra, de acuerdo con el procedimiento presentado en la Sección 6.1.1, cada fotograma del vídeo. Posteriormente, para evitar la superposición de los datos holográficos en el plano de recuperación, cada holograma es multiplicado por una función de fase de posicionamiento [4], dada por

$$G_p(\nu, \omega) = \exp^{2\pi i(\nu x_p + \omega y_p)} \quad (6.8)$$

donde ν y ω son las coordenadas en el dominio de Fourier o de Fresnel. x_p y y_p son las

coordenadas en el plano de reconstrucción para el dato holográfico p -ésimo. De esta forma, después de multiplicar cada holograma por la función de fase de reposicionamiento, estos pueden ser multiplexados en un solo dato de campo óptico. En el dominio de Fourier el multiplexado de esta información está dado por,

$$M_F(\nu, \omega) = \sum_{p=1}^l [F(\nu, \omega)]_p \exp^{2\pi i(\nu x_p + \omega y_p)} \quad (6.9)$$

y en el dominio de Fresnel por,

$$M_{Fr}(\nu, \omega) = \sum_{p=1}^l [S_z(\nu, \omega)]_p \exp^{2\pi i(\nu x_p + \omega y_p)} \quad (6.10)$$

aquí, l es el número total de hologramas multiplexados, $p = 1, 2, 3, \dots, l$. $[F(\nu, \omega)]_p$ y $[S_z(\nu, \omega)]_p$ corresponden al holograma filtrado del p -ésimo fotograma en los dominios de Fourier y Fresnel, respectivamente. Todos los fotogramas del multiplexado pueden ser reconstruidos simultáneamente a partir de una TIF o TIFr, dependiendo del dominio utilizado durante el proceso de registro holográfico. En particular, el proceso de multiplexado de holográfico en el dominio de Fourier se puede ver en la Fig. 6.10.

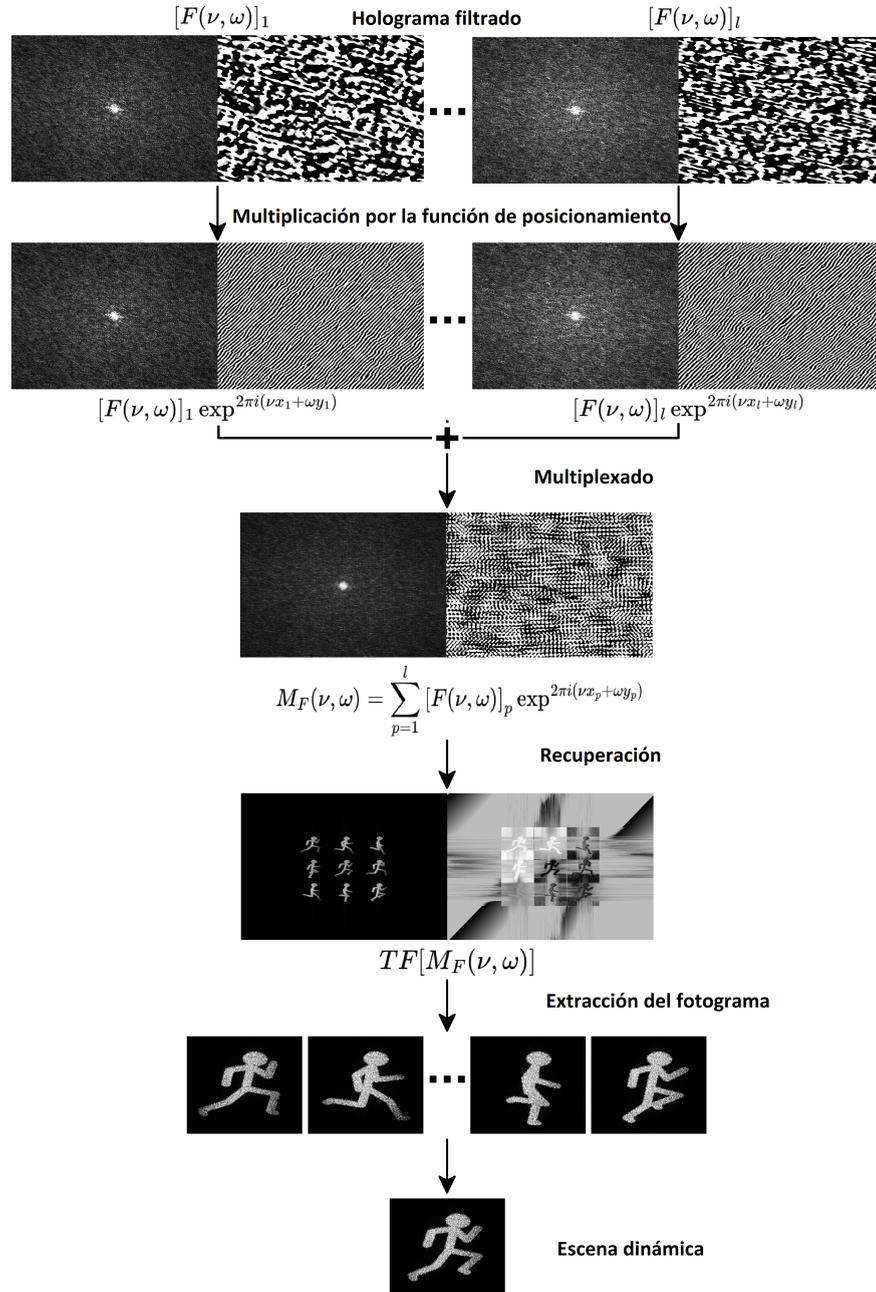


Figura 6.10: Video holográfico. Los hologramas filtrados y multiplicados por la función de posicionamiento se suman para generar el vídeo holográfico.

Cabe resaltar que en los resultados mostrados en la Fig. 6.10 se han aplicado las técnicas no lineales de reducción de ruido sobre cada dato holográfico [28]. Para recuperar los fotogramas originales, al multiplexado se le aplica la transformada inversa correspondiente al dominio óptico usado para el registro del holograma de cada fotograma.

Como se puede observar en la Fig. 6.11, la función de posicionamiento hace que los fotogramas recuperados no se superpongan en el plano de recuperación. Por lo tanto, al recortar y sincronizar los fotogramas recuperados se genera el vídeo recuperado, el vídeo (<https://bit.ly/3DKKy4V>) es la recuperación del video holográfico de Fourier y el vídeo 2 (<https://bit.ly/3Wi95Wa>) correspondientes a los hologramas de Fresnel. Se debe destacar que el protocolo de multiplexado permite combinar todos los hologramas filtrados y multiplicados por la función de posicionamiento en un solo dato de campo óptico, reduciendo el volumen de la información que se debe procesar y permitiendo la reconstrucción de todos los fotogramas al aplicar solo una transformada (Fourier o Fresnel) sobre el multiplexado.

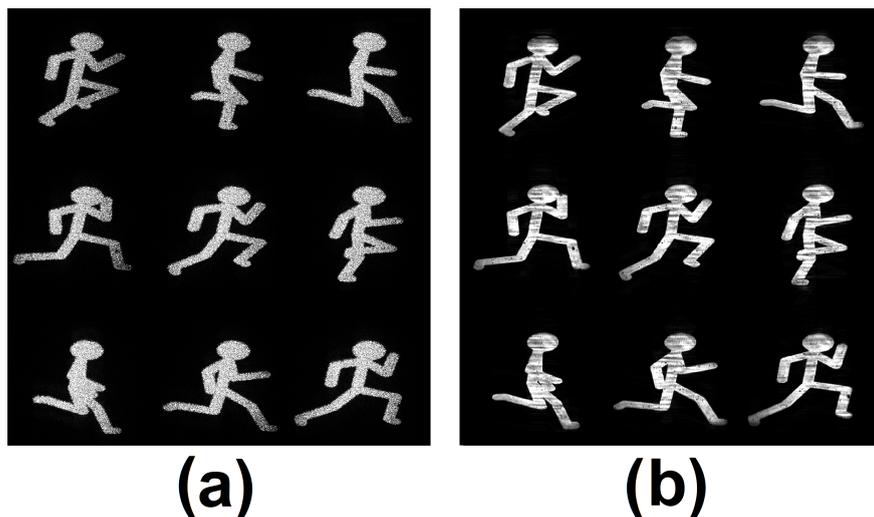


Figura 6.11: Recuperación de los fotogramas procesados en los dominios de (a) Fourier y (b) Fresnel.

Para obtener el video recuperado a partir el multiplexado, se utilizó una CPU Intel Core i7-8550U a 1,80 GHz 1,99 GHz la cual permite realizar las transformadas de Fourier y Fresnel en 0,4 s y 1,3 s, respectivamente. Por su parte, el procedimiento de recorte tuvo una duración de alrededor 0,003 s por fotograma. Esto es 21,07 fotogramas por segundo para el vídeo holográfico en el dominio de Fourier y 6,78 fotogramas por segundo para el vídeo holográfico en el dominio de Fresnel.

Los resultados presentados en esta sección demuestran la capacidad que tiene el sistema experimental para el registro holográfico de vídeos a partir de técnicas de multiplexación

en los dominios de Fourier y Fresnel. Además, se demuestra que el DDM presenta un buen rendimiento para aplicaciones holográficas, convirtiéndose en una alternativa interesante para la proyección de información binaria de amplitud.

6.2.2. Recuperación holográfica libre de ruido

Teniendo en cuenta la eficiencia que presentan los contenedores de información para posibilitar una recuperación libre de ruido, se realiza un procedimiento de recuperación holográfica de datos basada en códigos QR (siglas en inglés de: quick response) como contenedores de información, para obtener una reconstrucción libre de ruido y degradación en los dominios de Fourier y Fresnel [42]. Para esto, en lugar de proyectar directamente la información a procesar en el DDM, se proyecta el código QR que tiene codificada la información a procesar. Para recuperar ópticamente el código QR se emplea el procedimiento de recuperación en el dominio que fue registrado el holograma. Después del proceso de recuperación, se realiza la lectura del código QR reconstruido.

Los códigos QR recuperados y su respectiva lectura se muestra en la Fig. 6.12. Una de las características fundamentales que presentan los códigos QR es su corrección integrada de errores, la cual permite limitar parte de la capacidad de almacenamiento a cambio de una mayor resistencia a la degradación. Gracias a esto, la información puede ser correctamente escaneada y leída a pesar de daños y/o contaminación localizada que pueda afectar el código.

Dato original	Dato recuperado	Lectura
		<p data-bbox="975 367 1222 405">Fourier Holography</p>
		<p data-bbox="975 658 1222 696">Fresnel Holography</p>

Figura 6.12: Recuperación libre de ruido. De izquierda a derecha: códigos QR de entrada proyectados por el DDM, códigos QR recuperados y su respectiva lectura.

Los resultados presentados en la Fig. 6.12 muestran que el sistema experimental propuesto en este capítulo permite, en los dominios de Fourier y Fresnel, el registro holográfico de códigos QR y su posterior lectura para obtener una recuperación libre de ruido y degradación.

6.3. Conclusiones

En este capítulo se demuestra experimentalmente el alto rendimiento del DDM como sistema de proyección en aplicaciones holográficas en los dominios óptico de Fourier y Fresnel, convirtiéndolo en una interesante y eficaz alternativa a los moduladores espaciales de luz. A diferencia de los MELs que funcionan por reflexión, en el DDM la luz reflejada de los píxeles activos, correspondiente al objeto proyectado, no viaja en la misma dirección que la luz reflejada por los píxeles que no contienen información, eliminando la posibilidad de superposición entre estos dos haces de luz. Además, los microespejos del DDM permiten una modulación de contraste más alta que la mayoría de los MEL de transmisión, por lo que

se puede concluir que el DDM es particularmente adecuado para la proyección de objetos binarios.

Se muestra que el DDM en conjunto con técnicas de multiplexado permite el procesamiento holográfico de escenas estáticas y dinámicas dos dimensionales. Además, la inclusión de técnicas no lineales de reducción de ruido minimizan la degradación en los datos reconstruidos. En particular, en el dominio de Fourier, donde las máscaras aleatorias de fase garantizan el adecuado registro del holograma, las técnicas de reducción de ruido permiten obtener una recuperación de alta calidad. Por otro lado, se implementó un esquema de registro holográfico de información con recuperación libre de ruido usando códigos QR como contenedores de información.

Aunque hay muchas aplicaciones donde el MEL puede ser reemplazado por un DDM, en el contexto de este trabajo de investigación la implementación se centró en los sistemas holográficos ya que en el siguiente capítulo se usará como dispositivo de proyección en un sistema de encriptación tipo JTC. La inclusión efectiva del DDM en este sistema contribuiría al desarrollo de un dispositivo compacto, con bajos requerimientos de alineación y estabilidad, y de bajo costo.

Todos los resultados presentados en este capítulo, como se observa en la sección de anexos, fueron publicados en revista internacional como producto de la investigación realizada durante el doctorado [46] y presentados en un evento científico a nivel nacional [50, 51].

Bibliografía

- [1] G. ZHANG, T. GUAN, Z. SHEN, X. WANG, T. HU, D. WANG, N. XIE. **Fast phase retrieval in off-axis digital holographic microscopy through deep learning.** *Opt. Express.* 2018;26:19388-405.
- [2] V. JAEDICKE, S. GOEBEL, N. KOUKOURAKIS, N.C. GERHARDT, H. WELP, M.R. HOFMANN. **Multiwavelength phase unwrapping and aberration correction using depth filtered digital holography.** *Opt. Lett.* 2014;39:4160-3.
- [3] W. CHEN. **Multiple-wavelength double random phase encoding with CCD-plane sparse-phase multiplexing for optical information verification.** *Appl. Opt.* 2015;54:10711-6.
- [4] F. MOSSO, J.F BARRERA-RAMÍREZ, M. TEBALDI, N. BOLOGNINI, R. TORROBA. **All-optical encrypted movie.** *Opt. Express.* 2011;19:5706-12.
- [5] U. SCHNARS. **Direct phase determination in hologram interferometry with use of digitally recorded holograms.** *JOSA A.* 1994;11:2011-5.
- [6] W. OSTEN, A. FARIDIAN, P. GAO, K. KÖRNER, D. NAIK, G. PEDRINI, M. WILKE. **Recent advances in digital holography.** *Appl. Opt.* 2014;53:G44-63.
- [7] J.W. GOODMAN, R.W. LAWRENCE. **Digital image formation from electronically detected holograms.** *Appl. Phys. Lett.* 1967;11:77-9.
- [8] T.S HUANG. **Digital holography.** *Proceedings of the IEEE.* 1971;59:1335-46.

- [9] G. NEHMETALLAH, P.P. BANERJEE. **Applications of digital and analog holography in three-dimensional imaging.** *Adv. Opt. Photon.* 2012;4:472-553.
- [10] M. SUTKOWSKI, M. KUJAWIŃSKA. **Application of liquid crystal (LC) devices for optoelectronic reconstruction of digitally stored holograms.** *Opt. Lasers Eng.* 2000;33:191-201.
- [11] C. KOHLER, X. SCHWAB, W. OSTEN. **Optimally tuned spatial light modulators for digital holography.** *Appl. Opt.* 2006;45:960-7.
- [12] J.F. BARRERA-RAMÍREZ, R. HENAO, M. TEBALDI, R. TORROBA, N. BOLOGNINI. **Multiplexing encrypted data by using polarized light.** *Opt. Commun.* 2006;260:109-12.
- [13] 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.* 2007;46:4680-5.
- [14] T. KOZACKI, M. CHLIPALA. **Color holographic display with white light LED source and single phase only SLM.** *Opt. Express.* 2016;24:2189-99.
- [15] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Secure real-time generation and display of color holographic movies.** *Opt. Lasers Eng.* 2019;122:239-44.
- [16] A. MIRA-AGUDELO, W. TORRES-SEPÚLVEDA, J.F. BARRERA-RAMÍREZ, R. HENAO, N. BLOCKI, K. PETELCZYC, A. KOŁODZIEJCZYK. **Compensation of presbyopia with the light sword lens.** *Invest. Ophthalmol. Vis. Sci.* 2016;57:6870-7.
- [17] H. KIM, M. KIM, W. LEE, J. AHN. **Gerchberg-Saxton algorithm for fast and efficient atom rearrangement in optical tweezer traps.** *Opt. Express.* 2019;27:2184-96.
- [18] I.N. KOMPANETS, A.L.V. ANDREEV. **Microdisplays in spatial light modulators.** *Quantum Electron.* 2017;47:294.

- [19] G. VDOVIN, H. GONG, O. SOLOVIEV, P. POZZI, M. VERHAEGEN. **Lensless coherent imaging by sampling of the optical field with digital micromirror device.** *J. Opt.* 2015;17:122001.
- [20] A. SUN, Z. DING-FU, Y. SHENG, H. YOU-JUN, Z. PENG, Y. JIAN-MING. **Optical scanning holography based on compressive sensing using a digital micromirror device.** *Opt. Commun.* 2017;385:19-24.
- [21] X. ZHANG, J. XIE, C. LI, R. XU, Y. ZHANG, S. LIU, J. WANG. **MEMS-based super-resolution remote sensing system using compressive sensing.** *Opt. Commun.* 2018;426:410-7.
- [22] B. VOHNSEN, A.C. MARTINS, S. QAYSI, N. SHARMIN. **Hartmann–Shack wavefront sensing without a lenslet array using a digital micromirror device.** *Appl. Opt.* 2018;57:E199-204.
- [23] A. MANTHALKAR, I. NAPE, N.T. BORDBAR, C. ROSALES-GUZMÁN, S. BHATTACHARYA, A. FORBES, A. DUDLEY. **All-digital Stokes polarimetry with a digital micromirror device.** *Opt. Lett.* 2020;45:2319-22.
- [24] X. HU, Q. ZHAO, P. YU, X. LI, Z. WANG, Y. LI, L. GONG. **Dynamic shaping of orbital-angular-momentum beams for information encoding.** *Opt. Express.* 2018;26:1796-808.
- [25] L. GONG, Y. REN, W. LIU, M. WANG, M. ZHONG, Z. WANG, Y. LI. **Generation of cylindrically polarized vector vortex beams with digital micromirror device.** *J. Appl. Phys.* 2014;116:183105.
- [26] L. LIU, Y. GAO, X. LIU. **High-precision joint amplitude and phase control of spatial light using a digital micromirror device.** *Opt. Commun.* 2018;424:70-9.
- [27] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Innovative speckle noise reduction procedure in optical encryption.** *J. Opt.* 2017;19:055704.
- [28] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Experimental optical encryption of grayscale information.** *Appl. Opt.* 2017;56:5883-9.

- [29] S. TREJOS, J.F. BARRERA-RAMÍREZ, M. TEBALDI, R. TORROBA. **Experimental opto-digital processing of multiple data via modulation, packaging and encryption.** *J. Opt.* 2014;16:055402.
- [30] J.A. JARAMILLO-OSORIO, J.F. BARRERA-RAMÍREZ, A. VELEZ-ZEA, R. TORROBA. **Fractional optical cryptographic protocol for data containers in a noise-free multiuser environment.** *Opt. Lasers Eng.* 2018;102:119-25.
- [31] R. HENAO, E. RUEDA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Noise-free recovery of optodigital encrypted and multiplexed images.** *Opt. letters.* 2010;35:333-5.
- [32] J.F. BARRERA-RAMÍREZ, R. TORROBA. **One step multiplexing optical encryption.** *Opt. Commun.* 2010;283:1268-72.
- [33] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **One-step reconstruction of assembled 3D holographic scenes.** *Opt. Laser Technol.* 2015;75:146-50.
- [34] S. TREJOS, J.F. BARRERA-RAMÍREZ, A. VELEZ-ZEA, M. TEBALDI, R. TORROBA. **Compression of multiple 3D color scenes with experimental recording and reconstruction.** *Opt. Lasers Eng.* 2018;110:18-23.
- [35] O. MATOBA, B. JAVIDI. **Encrypted optical storage with angular multiplexing.** *Appl. Opt.* 1999;38:7288-93.
- [36] J.F. BARRERA-RAMÍREZ, R. HENAO, M. TEBALDI, R. TORROBA, N. BOLOGNINI. **Multiplexing encryption–decryption via lateral shifting of a random phase mask.** *Opt. Commun.* 2006;259:532-6.
- [37] F. MOSSO, M. TEBALDI, J.F. BARRERA-RAMÍREZ, N. BOLOGNINI, R. TORROBA. **Pure optical dynamical color encryption.** *Opt. Express.* 2011;19:13779-86.
- [38] J.F. BARRERA-RAMÍREZ, M. TEBALDI, C. RÍOS, E. RUEDA, N. BOLOGNINI, R. TORROBA. **Experimental multiplexing of encrypted movies using a JTC architecture.** *Opt. Express.* 2012;20:3388-93.

- [39] S. TREJOS, M. GÓMEZ, A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Compression of 3D dynamic holographic scenes in the Fresnel domain.** Appl. Opt. 2020;59:230-8.
- [40] M. GÓMEZ-VALENCIA, S. TREJOS, A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Experimental holographic movie compression using optical scaling and sampling.** J. Opt. 2020;22:035703.
- [41] J.F. BARRERA-RAMÍREZ, A. MIRA-AGUDELO, R. TORROBA. **Optical encryption and QR codes: secure and noise-free information retrieval.** Opt. Express. 2013;21:5373-8.
- [42] J.F. BARRERA-RAMÍREZ, A. MIRA-AGUDELO, R. TORROBA. **Experimental QR code optical encryption: noise-free data recovering.** Opt. Lett. 2014;39:3074-7.
- [43] ISO, B. (2006). IEC 16022: INFORMATION TECHNOLOGY-AUTOMATIC IDENTIFICATION AND DATA CAPTURE TECHNIQUES-DATA MATRIX BAR CODE SYMBOLOGY SPECIFICATION. BS ISO/IEC, 16022.
- [44] K.C. LIAO, W.H. LEE. **A novel user authentication scheme based on QR-code.** J. Netw. 2010;5:937.
- [45] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Experimental scrambling and noise reduction applied to the optical encryption of QR codes.** Opt. Express. 2014;22:20268–77.
- [46] J.A. JARAMILLO-OSORIO, S. BUSTAMANTE, B. MUÑOZ, A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Experimental Fresnel and Fourier digital holography using a digital micro-mirror device.** J. Opt. 2021;23:035701.
- [47] S. TREJOS, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Optimized and secure technique for multiplexing QR code images of single characters: application to noiseless messages retrieval.** J. Opt. 2015;17:085702.
- [48] E. CUCHE, P. MARQUET, C. DEPEURSINGE. **Spatial filtering for zero-order and twin-image elimination in digital off-axis holography.** Appl. Opt. 2000;39:4070-5.

- [49] J.F BARRERA-RAMÍREZ, J.A. JARAMILLO-OSORIO, A. VELEZ-ZEA, R. TORROBA R. **Experimental analysis of a joint free space cryptosystem.** Opt. Lasers Eng. 2016;83:126-30.
- [50] S. BUSTAMANTE, B. MUÑOZ, J.A. JARAMILLO-OSORIO, A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Holografía digital de Fresnel usando un dispositivo digital de microespejos y estudio de la influencia de la distancia de propagación en la recuperación.** XVI Encuentro Nacional de Óptica y VI Conferencia Andina y del Caribe en Óptica y sus Aplicaciones. Universidad de Córdoba - Colombia, noviembre 2019.
- [51] B. MUÑOZ, S. BUSTAMANTE, J.A. JARAMILLO-OSORIO, A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Video holográfico de Fourier usando un dispositivo digital de microespejo.** XVI Encuentro Nacional de Óptica y VI Conferencia Andina y del Caribe en Óptica y sus Aplicaciones. Universidad de Córdoba - Colombia, noviembre 2019.

Capítulo 7

Prototipo de encriptación compacto y de bajo costo

Los avances mostrados en los capítulos anteriores demuestran que es posible implementar sistemas de encriptación compactos y que se pueden usar nuevos dispositivos para aumentar la versatilidad de los sistemas convencionales. Con base en estos desarrollos, como resultado inédito de esta tesis se implementó una primera versión de un prototipo de encriptación compacto y de bajo costo.

En general, los sistemas de codificación tiene tres elementos fundamentales que garantizan su correcto funcionamiento, estos son: la fuente iluminación, generalmente un láser de alta coherencia y con una potencia considerable, una cámara de alta resolución utilizada para el registro de la información y un modulador espacial de luz usado para la proyección de la información que se desea cifrar. Aunque se debe tener en cuenta que los esquemas experimentales poseen otros elementos ópticos, estos tres elementos son los encargados de elevar los costos de la disposición experimental. Por lo tanto, para el desarrollo de una primera versión de un prototipo de codificación, además de usar un arquitectura compacta se deben incluir elementos que permitan una reducción en los costos de la implementación.

Para el desarrollo de este prototipo se utiliza un dispositivo digital de microespejos (DDM) como sistema de proyección, en lugar de un modulador espacial de luz (MEL). La implementación del DDM permite sustituir el elemento más costoso de la implementación experimental. Además, en comparación con los MELs, los DDMs presentan frecuencias de actualización de pantalla superiores y tienen una mejor respuesta para la proyección de imágenes binarias de amplitud. Por otro lado, a diferencia de los MELs que funcionan por reflexión, en el DDM la luz reflejada de los píxeles activos, correspondiente al objeto proyectado, no viaja en la misma dirección que la luz reflejada por los píxeles que no contienen información, eliminando la posibilidad de superposición entre estos haces de luz, y permitiendo el adecuado registro de la información relevante.

Además del sistema de proyección, otros elementos que incrementan los costos de la implementación experimental son la cámara utilizada para el registro de la información y la fuente de iluminación. En el prototipo se emplea una cámara web comercial y un diodo láser de baja potencia, el uso de estos elementos permite que el valor del prototipo sea mucho menor al costo de una implementación convencional. Además, el uso de un diodo láser de baja potencia, en lugar de una fuente láser convencional, permite reducir los requerimientos energéticos necesarios para el funcionamiento del sistema.

A continuación se muestran el esquema experimental de la primera versión del prototipo y algunos resultados preliminares. Se debe destacar que, al ser esta una primera versión de un prototipo de codificación, los resultados que se presentan deben ser optimizados. Además, se debe evaluar la mejoras que puedan introducir los procedimientos de reducción de ruido [1–5], el desempeño de los protocolos para la recuperación libre de ruido basado en contenedores de información [6, 7], entre otras técnicas utilizadas en este trabajo..

7.1. Sistema de codificación JFSC de bajo costo

Con el objetivo de estudiar el desempeño del DDM, en conjunto con una cámara de bajo costo y el diodo láser, se realizó una primera implementación de un sistema de codificación de bajo costo basada en un sistema JFSC (siglas en inglés de: joint free space cryptosystem) convencional [8, 9]. En este sistema, el proceso de encriptación se realiza en el dominio óptico de Fresnel, por lo cual no requiere de una lente transformadora, evitando los problemas de aberración que este elemento puede inducir. Además, en esta arquitectura la distancia entre el plano de entrada y el plano de registro es un parámetro extra de seguridad. El esquema experimental del prototipo de bajo costo puede verse en la Fig.7.1.

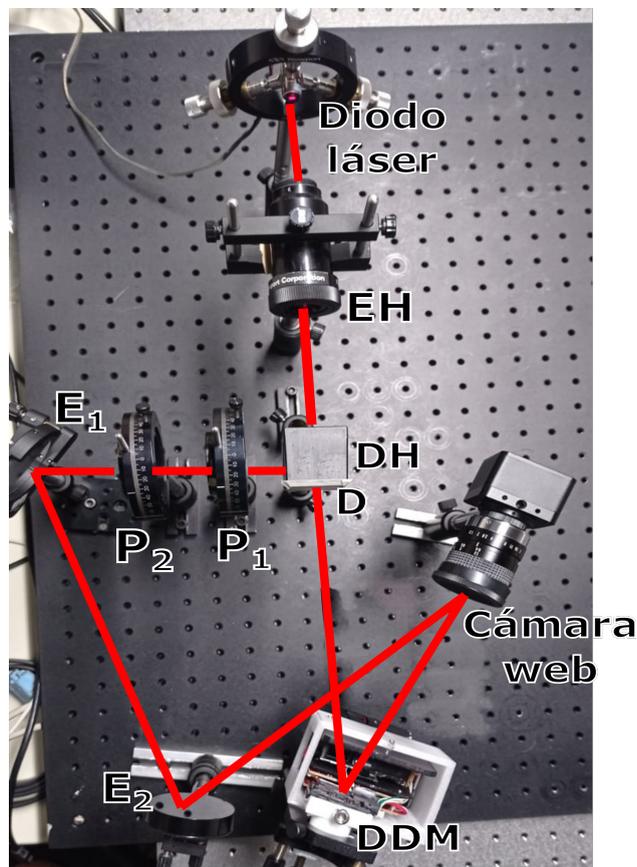


Figura 7.1: Sistema de encriptación de bajo costo basado en una arquitectura JFSC. E: espejo, P: polarizador, D: difusor, EH: expansor de haz, DH: divisor de haz y DDM: dispositivo digital de microespejos.

Este sistema de codificación mantiene todas las características experimentales del sistema

JFSC convencional. Por lo tanto, el registro del dato encriptado y de la información de la llave se realizan siguiendo los procedimientos expuestos en el Capítulo 5 de este trabajo.

7.1.1. Resultados experimentales obtenidos en el sistema JFSC de bajo costo

Los resultados experimentales que se exponen a continuación fueron obtenidos con el sistema experimental mostrado en la Fig. 7.1. Como fuente de iluminación se utilizó un diodo láser con una potencia de 5 mW y una longitud de onda de 650 nm . El medio de registro fue una MOKOSE Cámara USB 4K con una resolución de 3840×2160 pixeles y un tamaño de pixel de $12\ \mu\text{m}$. Como sistema de proyección se utilizó un DDM con un tamaño de pixel de $7,637 \times 7,637\ \mu\text{m}$ y una resolución de $684 \times 608\ \mu\text{m}$ pixeles.

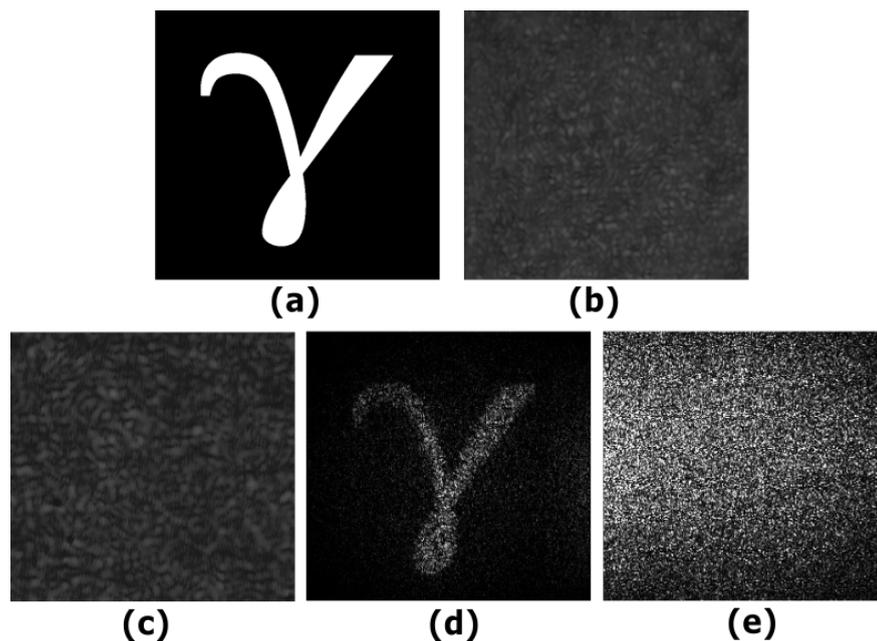


Figura 7.2: Encriptación y recuperación experimental en el prototipo de encriptación de bajo costo. (a) Dato original, (b) dato encriptado, (c) holograma de la llave, (d) recuperación con la llave correcta y (e) recuperación con llave incorrecta.

Para analizar las desempeño básico del sistema, se realizó el proceso de encriptación y recuperación de un dato (Fig. 7.2). Los resultados experimentales demuestran que cuando un

usuario no autorizado desea acceder a la información encriptada (Fig. 7.2b) usando una llave incorrecta, la información permanece oculta (Fig. 7.2e). Por otro lado, cuando un usuario autorizado realiza el proceso de recuperación con la llave de encriptación (Fig. 7.2c), éste puede recuperar el dato que estaba encriptado (Fig. 7.2d). Los resultados experimentales mostrados en la Fig. 7.2 demuestran la capacidad que tiene el sistema de encriptación de bajo costo para proteger información.

Se puede notar que, a pesar del uso de elementos bajo costo (cámara, diodo láser y DDM), la calidad del dato recuperado es comparable con la que presentan los sistemas de codificación convencional. Por último, se debe resaltar que los resultados presentados no han sido sometidos a ningún procedimiento extra para reducir el ruido.

7.2. Prototipo de un sistema de encriptación compacto de bajo costo

Después de corroborar el funcionamiento del DDM, el diodo láser y la cámara Web comercial dentro del esquema JFSC convencional, se presenta la primera versión del prototipo de codificación basada en un sistema JFSC en línea [10, 11]. Como se demostró en el Capítulo 5, este sistema hereda todas las características de versatilidad, rendimiento, estabilidad y seguridad del sistema JFSC convencional. En el esquema que se muestra en la Fig.7.3 se presenta el esquema del prototipo de codificación de bajo costo.

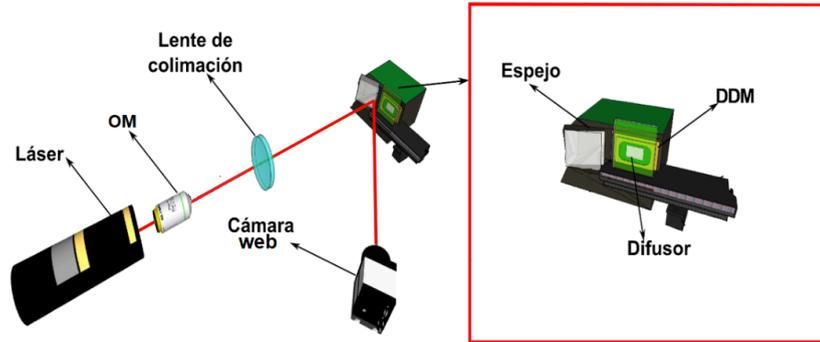


Figura 7.3: (a) Prototipo de encriptación compacto de bajo costo DDM: dispositivo digital de microespejos y OM: objetivo de microscopio. Proyección en el DDM para: (b) el registro del dato encriptado y (c) el registro de la información de la llave de encriptación.

Como se puede observar en la Fig.7.3(a), el prototipo de codificación de bajo costo que se presenta en este trabajo solo tiene un brazo de iluminación. En este sistema, para el registro del dato encriptado se proyecta en el DDM el plano de entrada mostrado en la Fig.7.3(b), que corresponde al plano de entrada del sistema JFSC convencional (ver Sección 5.2) [11]. Por otro lado, para el registro de la información de la llave se proyecta en el DDM la ventana llave (Fig. 7.3(c)), en este caso la luz que incide por fuera del área activa del DDM es usada como onda de referencia el reflejarse en un espejo adyacente que la direcciona hacia la cámara, donde se registra el holograma resultante de la interferencia de los haces provenientes del espejo y el DDM. A partir de este holograma se extrae la información de la llave de seguridad. Para realizar el proceso de recuperación de la información se sigue el mismo procedimiento mostrado en la Sección 5.4.

7.2.1. Resultados experimentales preliminares

Los resultados que se muestran en la Fig. 7.4 fueron obtenidos a partir del esquema experimental mostrado en la Fig. 7.3, para esto se usaron las mismas condiciones experimentales usadas para la obtención de los resultados presentados en la Sección 7.1.1. En este caso, se realizó una primera prueba del funcionamiento básico del prototipo utilizando contenedores de información [6, 7], específicamente CCOS (siglas en ingles de: customized containers for

optical security) [7].

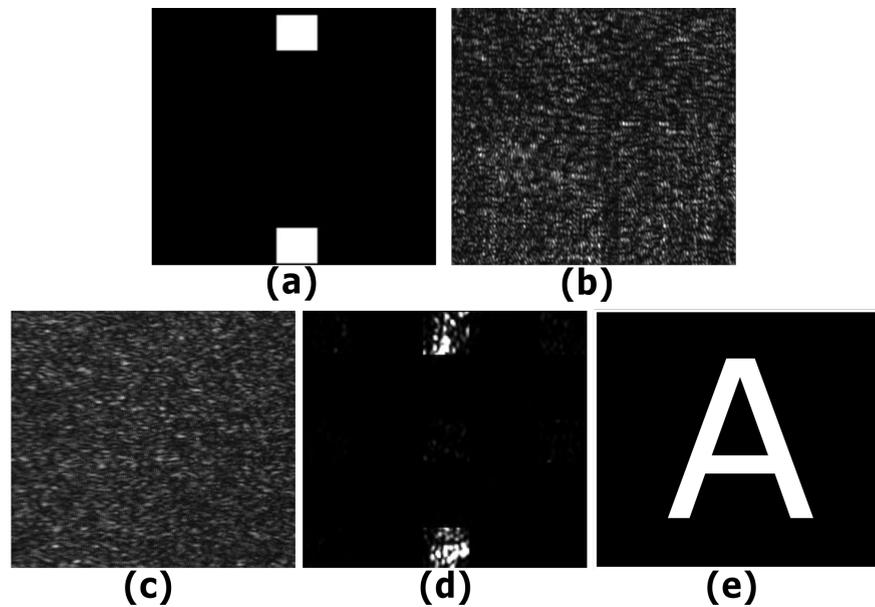


Figura 7.4: Recuperación libre de ruido basada en contenedores de información CCOS. (a) Código CCOS original, (b) código encriptado, (c) holograma de la llave, (d) código recuperado y (e) lectura del código recuperado.

En la Fig. 7.4(a), se presenta el CCOS original con la información correspondiente a la letra A. Después del proceso de desencriptación, utilizando la información de la llave correcta (Fig. 7.4(b)) y el dato encriptado (Fig. 7.4(c)), se obtiene el código recuperado mostrado en la Fig. 7.4(d). Posteriormente, el código recuperado (Fig. 7.4(d)) puede ser leído para obtener la información original libre de ruido y degradación (Fig. 7.4(e)). Los resultados mostrados en la Fig. 7.4 demuestran la viabilidad experimental del prototipo de codificación compacto de bajo costo. Estos resultados preliminares permiten establecer que la implementación de elementos comerciales de bajo costo dentro de arquitecturas de codificación posibilitan el diseño de un sistema con alto potencial para su utilización en investigación básica y para futuras aplicaciones prácticas.

7.3. Conclusiones

En primer lugar se muestra experimentalmente que el uso de DDMs, cámaras web comerciales y diodos láser, dentro de un esquema JFSC convencional permite la implementación de un sistema de codificación JFSC de bajo costo. Como se evidencia en los resultados preliminares, la calidad de la información recuperada es comparable con la calidad de los datos reconstruidos en los sistemas JTC convencionales.

Los resultados obtenidos con la implementación experimental del sistema JFSC de bajo costo permitieron el desarrollo de una primera versión de un prototipo de encriptación basado en un sistema de codificación JFSC lineal. Este sistema no requiere de un brazo de iluminación fuera de eje para el registro de la información de la llave, reduciendo la cantidad de elementos ópticos necesarios, el volumen requerido por el esquema experimental, y los requerimientos de estabilidad y alineación para su adecuado funcionamiento. La reducción en la cantidad de los elementos ópticos requeridos, disminuye los problemas de aberración que estos introducen dentro del procesamiento. Además de esto, con el uso de un DDM, una cámara comercial de bajo costo y un diodo láser, se reducen los costos de la implementación. Finalmente, el uso del diodo láser en lugar de las fuentes láser convencionalmente usadas en los esquemas ópticos de encriptación, reduce el consumo de energía necesaria para llevar a cabo el proceso de codificación óptica. Estas características convierten a este prototipo en una alternativa válida para el procesamiento seguro de la información con un potencial importante para futuras aplicaciones.

El sistema que se presenta en este capítulo representa una primera versión de un prototipo de codificación óptica, corresponde a un desarrollo inédito, evidenciando un factor de innovación generado a partir del trabajo de investigación realizado en esta tesis de doctorado.

Bibliografía

- [1] J.F. BARRERA-RAMÍREZ, E. RUEDA, C. RIOS, M. TEBALDI, N. BOLOGNINI, R. TORROBA. **Experimental opto-digital synthesis of encrypted sub-samples of an image to improve its decoded quality.** *Opt. Commun.* 2011;284:4350-5.
- [2] J.M. VILARDY, M.S. MILLÁN, E. PÉREZ-CABRÉ. **Improved decryption quality and security of a joint transform correlator-based encryption system.** *J. Opt.* 2012;15:025401.
- [3] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Experimental optical encryption of grayscale information.** *Appl. Opt.* 2017;56:5883-9.
- [4] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Innovative speckle noise reduction procedure in optical encryption.** *J. Opt.* 2017;19:055704.
- [5] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Optimized random phase encryption.** *Opt. Lett.* 2018;43:3558-61.
- [6] J.F. BARRERA-RAMÍREZ, A. MIRA-AGUDELO, R. TORROBA. **Optical encryption and QR codes: secure and noise-free information retrieval.** *Opt. Express.* 2013;21:5373-8.
- [7] A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Customized data container for improved performance in optical cryptosystems.** *J. Opt.* 2016;18:125702.

- [8] J.M. VILARDY, M.S. MILLÁN, E. PÉREZ-CABRÉ. **Nonlinear optical security system based on a joint transform correlator in the Fresnel domain.** Appl. Opt. 2014;53:1674–82.
- [9] J.F. BARRERA-RAMÍREZ, J.A. JARAMILLO-OSORIO, A. VELEZ-ZEA, R. TORROBA. **Experimental analysis of a joint free space cryptosystem.** Opt. Laser Eng. 2016;83:126–30.
- [10] J.A. JARAMILLO-OSORIO, J.F. BARRERA-RAMÍREZ, A. MIRA-AGUDELO, A. VELEZ-ZEA, R. TORROBA. **High performance compact optical cryptosystem without reference arm.** J. Opt. 2020;22:035702.
- [11] J.A. JARAMILLO-OSORIO, J.F. BARRERA-RAMÍREZ, A. MIRA-AGUDELO, A. VELEZ-ZEA, R. TORROBA. **Secure selective recovery protocol for multiple optically encrypted data.** Opt. Lasers Eng. 2021;137:106383.

Capítulo 8

Conclusiones y perspectivas

Este trabajo de investigación tuvo como objetivo principal el desarrollo teórico-experimental de un sistema óptico de encriptación compacto y de bajo costo para la protección de información. Para llevar a cabo este objetivo, se tomó como base los sistemas de codificación óptica basados en la técnica DRPE (siglas en inglés de: doble random phase encoding), específicamente el sistema de encriptación JTC (siglas en inglés de: joint transform correlator), ya que su configuración experimental, además de admitir diferentes técnicas ópticas para el procesamiento de datos, presenta una estructura versátil que permite la implementación de protocolos para mejorar la seguridad y las capacidades en la manipulación segura de información.

Los resultados obtenidos muestran que el uso de una lente electro-óptica de foco variable (LEFV) en un sistema JTC en el dominio óptico de Fourier fraccionario permite reducir los requerimientos de alineación y estabilidad necesarias para llevar a cabo el proceso de encriptación en este dominio. Se demostró que la inclusión de la LEFV, en lugar de una lente de foco fijo dentro del sistema JTC de Fourier fraccionario no afecta notoriamente la calidad de la información recuperada en comparación con los sistemas JTC convencionales. El uso de este tipo de dispositivos opto-electrónicos posibilitó el desarrollo de protocolos multiusuarios

basados en la modificación de la longitud focal de la LEFV sin la necesidad de elementos mecánicos adicionales, generando un arquitectura más estable y con bajos requerimientos de alineación en comparación con el sistema JTC de Fourier fraccionario convencional. El análisis realizado permitió concluir que la aplicación de nuevas tecnologías dentro de los sistemas de codificación convencionales permite el desarrollo de esquemas más robustos y de alto rendimiento, manteniendo las características básicas de los sistemas ya existentes. Los resultados obtenidos son, hasta donde se tiene conocimiento, la primera demostración de un esquema DRPE de Fourier fraccional en el que se utiliza un LEFV y podrían ser el punto de partida para la implementación de este tipo de esquemas en aplicaciones prácticas o experimentales enfocadas en la manipulación segura de información a través de medios ópticos. Por último, se debe mencionar que este sistema de encriptación presenta una alta flexibilidad, ya que es posible configurar el sistema para que incorpore transformadas de Fourier, Fourier fraccionario y Fresnel, característica que aumenta el rango de aplicabilidad del sistema.

Por otro lado, buscando mejorar la seguridad que brindan los esquemas ópticos de codificación, se realizó una modificación en el haz utilizado para iluminar el plano de entrada de un sistema JFSC (siglas en inglés de: joint free space cryptosystem). En este caso, la fase del haz que ilumina el plano de entrada fue modulada a partir del efecto lente térmica (ELT). Los resultados experimentales mostraron que la modificación de fase que produce el ELT sobre el haz con que se ilumina el plano de entrada permite obtener diferentes llaves de seguridad. Este hecho permitió establecer un protocolo de encubrimiento óptico cuyo objetivo es disuadir y/o engañar a un atacante que desea acceder a la información que está encriptada. Aunque los resultados obtenidos a partir del sistema JFSC con iluminación modulado por el ELT permiten visualizar un mecanismo mediante el cual se contribuye a la seguridad del sistema, su implementación implica el uso de una gran cantidad de elementos ópticos que conllevan a una configuración experimental que requiere un área de trabajo considerable y que presenta altos requerimientos de alineación y estabilidad, y cuyo costo aumenta en comparación con los sistemas JTC convencionales. Estas características deben ser consideradas al momento de usar el ELT en otras arquitecturas y/o en aplicaciones prácticas dentro del campo de la codificación óptica.

Buscando reducir la cantidad de elementos, el volumen, y los requerimientos de alienación y estabilidad de los sistemas de codificación óptico JTC, se presentó un sistema JFSC con un solo brazo de iluminación. A diferencia de los sistemas JTC convencionales, la configuración experimental del sistema JFSC con un solo brazo de iluminación no requiere de un brazo de referencia para el registro de la llave de recuperación, lo cual hace que este esquema presente una estructura mucho más compacta en comparación con las arquitecturas presentadas anteriormente. Los resultados experimentales mostraron la viabilidad experimental del sistema en línea y que la calidad de la información recuperada es comparable con la calidad de los datos recuperados en los sistemas convencionales. Se demostró que el esquema JFSC con un solo brazo de iluminación permite incluir un protocolo basado en contenedores de información que posibilita la recuperación de la información libre de ruido y degradación. Por otro lado, con el objetivo de probar el desempeño del sistema, se incluyeron técnicas basadas en máscaras binarias aleatorias ortogonales, que además de permitir una reducción del volumen de la información procesada, posibilitaron la inclusión de un protocolo de multiplexado selectivo. Por su parte, el multiplexado selectivo permitió el desarrollo de un teclado óptico con el cual se pueden recuperar mensajes de cualquier longitud. Además, se demostró que el multiplexado selectivo pueden conducir a una mayor resistencia a algunos de los ataques más comunes a los que son sometidos los sistemas de codificación. La implementación experimental del sistema JFSC de un solo brazo de iluminación apunta directamente al objetivo principal de este trabajo, ya que tiene una arquitectura de codificación compacta, con bajos requerimientos de alienación y estabilidad, que podría llevar al desarrollo de nuevos esquemas de codificación, convirtiéndose en un gran aporte para el campo de la encriptación óptica.

Con el objetivo de reducir los costos del sistema encriptación, se implementa un sistema holográfico que usa un dispositivo digital de microespejos (DDM) en lugar de un modular espacial de luz (MEL) como sistema de proyección. El funcionamiento del sistema holográfico es analizado en los dominios ópticos de Fourier y Fresnel. En primer lugar se muestra que el sistema propuesto permite el registro y la reconstrucción de datos holográficos con una calidad comparable con la de los sistemas holográficos que usan un MEL. Además, se corrobora que el DDM en conjunto con técnicas de multiplexado permite el procesamiento holográfico de escenas estáticas y dinámicas dos dimensionales. Por otro lado, la inclusión

de técnicas no lineales de reducción de ruido permitieron minimizar la degradación en los hologramas reconstruidos. Lo anterior, sumado al hecho de que los DDMs presentan un costo considerablemente menor que los MELs, permite concluir que los DDMs presentan un buen rendimiento como elementos de proyección en sistemas holográficos.

Finalmente, con base en los resultados expuestos en los capítulos anteriores, en el Capítulo 7 se desarrolló una primera versión de un prototipo de codificación óptico compacto y de bajo costo basado en una arquitectura tipo JFSC lineal. En el prototipo desarrollado tiene un DDM como sistema de proyección, un diodo láser de baja potencia y bajo costo como fuente de iluminación y una cámara web comercial como medio de registro. El uso de estos dispositivos en combinación con la disposición experimental del esquema de codificación JFSC en línea, permite el desarrollo de un esquema que ocupa un volumen reducido, con bajos requerimientos de estabilidad y alineación, y con una estructura de bajo costo que preserva las características de seguridad que presentan los esquemas tradicionales. Esta primera versión del prototipo, además de tener grandes beneficios para aplicaciones en ciencia básica, puede ser una alternativa interesante como sistema de codificación en entornos prácticos.

Teniendo presente el potencial de la primera versión del prototipo de codificación compacto y de bajo costo desarrollado, las perspectivas de este trabajo están enmarcadas en la optimización y el mejoramiento de su desempeño. En particular, futuros trabajos estarán enfocados en los siguientes aspectos:

1. Establecer los requerimientos necesarios para suprimir el espejo encargado de generar el haz de referencia. La eliminación de este elemento reducirá los requerimientos de estabilidad del esquema y evitará las imperfecciones que pueda introducir el espejo en la onda de referencia.
2. Determinar el tamaño óptimo que deben tener las ventanas llave y objeto en el plano de entrada proyectado en el DDM para garantizar el correcto registro de la información encriptada correspondiente a objetos estructurados. Y por lo tanto, brindar una recuperación apropiada.

3. Establecer las características mínimas que deben tener una cámara web para garantizar el correcto registro de la información encriptada correspondiente a objetos estructurados, de manera que sea posible garantizar una desencriptación con una buena calidad.
4. Implementar técnicas de reducción de ruido que permitan mejorar la calidad del dato recuperado, además optimizar el sistema para garantizar el correcto funcionamiento bajo protocolos basados en contenedores de información.
5. Buscar las condiciones que se deben garantizar para el correcto funcionamiento de protocolos multiusuario con recuperación libre de ruido.
6. Establecer un protocolo de encriptación que permita el procesamiento de objetos en escala de grises.

Los resultados originales de este trabajo de investigación contribuyen al campo de la encriptación óptica pues generan alternativas y soluciones a algunas de las dificultades y limitaciones que presentan los sistemas ópticos de codificación. Las arquitecturas, técnicas y procedimientos expuestos deben ser optimizados y analizados de acuerdo con el sistema que se desee desarrollar. En particular, los resultados expuestos en los últimos tres capítulos permitieron el desarrollo de una primera versión de un dispositivo de protección de datos basado en la manipulación de la luz con una estructura compacta y de bajo costo. La implementación experimental de este esquema permite reducir las altas exigencias experimentales que tienen los sistemas de codificación convencionales, y aunque se deben realizar investigaciones adicionales, se muestra como una alternativa válida a los sistemas convencionales de encriptación óptica con gran potencial para su adopción en aplicaciones prácticas.

Apéndice A

Productos de investigación

Las investigaciones desarrolladas en el marco de este trabajo de investigación generaron 11 productos académicos y de investigación. Los productos incluyen un prototipo inédito de un sistema de encriptación compacto y de bajo costo presentado en la sección 7.2, evidenciando la componente de innovación de la investigación.

Como resultado de la investigación, también se publicaron 5 artículos científicos en revistas internacionales de reconocido prestigio que presentan 16 citas hasta noviembre de 2022 (ver Google Scholar: <https://bit.ly/3Ewe3H1>), lo que demuestra el impacto e interés de la comunidad científica por estas contribuciones. Además, algunos resultados de la investigación aparecen publicados en un proceedings de un evento científico iberoamericano.

En lo que respecta a la divulgación y apropiación social de conocimiento, se presentó 1 trabajo en un evento científico internacional y 3 trabajos en eventos nacionales. Estos productos garantizan el rigor científico, la generación de nuevo conocimiento, la novedad, originalidad, visibilidad e impacto del trabajo de investigación.

A.1. Artículos internacionales publicados

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

- J.A. JARAMILLO-OSORIO, W. TORRES-SEPÚLVEDA, A. VELEZ-ZEA, A. MIRA-AGUDELO, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Focus-tunable experimental optical cryptosystem** Opt. Laser Techno. 2022;148:107689. (enlace: <https://bit.ly/3XkPjtS>).
- J.A. JARAMILLO-OSORIO, A. VELEZ-ZEA, H. CABRERA, J. NIEMELA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Optical encryption using phase modulation generated by thermal lens effect**. J. Opt. 2022;24:025702. (enlace: <https://bit.ly/3ggYm9L>).
- J.A. JARAMILLO-OSORIO, J.F. BARRERA-RAMÍREZ, A. MIRA-AGUDELO, A. VELEZ-ZEA, R. TORROBA. **High performance compact optical cryptosystem without reference arm**. J. Opt. 2020;22:035702. (enlace: <https://bit.ly/3tTsekA>).
- J.A. JARAMILLO-OSORIO, J.F. BARRERA-RAMÍREZ, A. MIRA-AGUDELO, A. VELEZ-ZEA, R. TORROBA. **Secure selective recovery protocol for multiple optically encrypted data**. Opt Lasers Eng. 2021;137:106383. (enlace: <https://bit.ly/3XkbMab>).
- J.A. JARAMILLO-OSORIO, S. BUSTAMANTE, B. MUÑOZ, A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Experimental Fresnel and Fourier digital holography using a digital micro-mirror device**. J. Opt. 2021;23:035701. (enlace: <https://bit.ly/3XpiD2g>).

A.2. Proceeding de un evento Iberoamericano

- J.A. JARAMILLO-OSORIO, J.F. BARRERA-RAMÍREZ, A. MIRA-AGUDELO, A. VÉLEZ, R. TORROBA. **Sistema de encriptación de un solo brazo en el dominio de Fresnel**. X Reunión Iberoamericana de Óptica y XIII Reunión Iberoamericana de

Óptica, Láseres y Aplicaciones (RIAO/OPTILAS). Cancún, Mexico. 2019. (enlace: <https://bit.ly/3UtmCrM>).

A.3. Trabajo presentado en un evento científico internacional

Algunos de los resultado parciales y finales del trabajo de investigación fueron presentados en un evento científico internacional:

- J.A. JARAMILLO-OSORIO, J.F. BARRERA-RAMÍREZ, A. MIRA-AGÚDELO, A. VÉLEZ, R. TORROBA. **Sistema de encriptación de un solo brazo en el dominio de Fresnel.** X Reunión Iberoamericana de Óptica y XIII Reunión Iberoamericana de Óptica, Láseres y Aplicaciones (RIAO/OPTILAS). Cancún, Mexico. 2019. (enlace: <https://bit.ly/3VbhbyK>).

A.4. Trabajos presentados en eventos científicos nacionales

Algunos de los resultados parciales del trabajo de investigación fueron presentados en dos eventos científicos nacionales:

- S. BUSTAMANTE, B. MUÑOZ, J.A. JARAMILLO-OSORIO, A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Holografía digital de Fresnel usando un dispositivo digital de microespejos y estudio de la influencia de la distancia**

- de propagación en la recuperación.** XVI Encuentro Nacional de Óptica y VI Conferencia Andina y del Caribe en Óptica y sus Aplicaciones. Universidad de Córdoba - Colombia, noviembre 2019. (enlace: <https://bit.ly/3ACmQWy>).
- B. MUÑOZ, S. BUSTAMANTE, J.A. JARAMILLO-OSORIO, A. VELEZ-ZEA, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Video holográfico de Fourier usando un dispositivo digital de microespejo.** XVI Encuentro Nacional de Óptica y VI Conferencia Andina y del Caribe en Óptica y sus Aplicaciones. Universidad de Córdoba - Colombia, noviembre 2019. (enlace: <https://bit.ly/3VC6jKz>).
 - J.A. JARAMILLO-OSORIO, W. TORRES-SEPULVEDA, A. VELEZ-ZEA, A. MIRAGÚDELO, J.F. BARRERA-RAMÍREZ, R. TORROBA. **Encriptación óptica en el dominio óptico de Fourier fraccionario usando una lente de foco variable.** XVII Encuentro Nacional de Óptica y VII Conferencia Andina y del Caribe en Óptica y sus Aplicaciones. Universidad Pontificia Bolivariana Medellín - Colombia, noviembre 2021. (enlace: <https://bit.ly/3GAIzSJ>).