

**IMPLEMENTACIÓN DE UN PROCESADOR  
ÓPTICO-VIRTUAL DE ENCRIPCIÓN DE  
TRANSFORMADA CONJUNTA PARA LA GENERACIÓN  
DE CRIPTOGRAMAS CAMUFLADOS**

**MARÍA ALEJANDRA GUERRERO VANEGAS**



**DEPARTAMENTO DE FÍSICA Y GEOLOGÍA  
FACULTAD DE CIENCIAS BÁSICAS  
UNIVERSIDAD DE PAMPLONA  
PAMPLONA, COLOMBIA**

**2018**

**IMPLEMENTACIÓN DE UN PROCESADOR  
ÓPTICO-VIRTUAL DE ENCRIPCIÓN DE  
TRANSFORMADA CONJUNTA PARA LA GENERACIÓN  
DE CRIPTOGRAMAS CAMUFLADOS**

**MARÍA ALEJANDRA GUERRERO VANEGAS**

Trabajo de grado presentado como requisito para optar al título de Físico

**Director**

**JORGE ENRIQUE RUEDA PARADA**

**Doctor en Ciencias Naturales - Física**



**GRUPO DE ÓPTICA MODERNA  
DEPARTAMENTO DE FÍSICA Y GEOLOGÍA  
FACULTAD DE CIENCIAS BÁSICAS  
UNIVERSIDAD DE PAMPLONA  
PAMPLONA, COLOMBIA**

**2018**

*“El científico no estudia la naturaleza por la utilidad que le pueda reportar; la estudia por el gozo que le proporciona, y este gozo se debe a la belleza que hay en ella... La belleza intelectual se basta a sí misma, y es por ella, más que quizá por el bien futuro de la humanidad, por lo que el científico consagra su vida a un trabajo largo y difícil”*

**Henri Poincaré**

# **Agradecimientos**

*A mi director Dr. Jorge Enrique Rueda Parada, por su apoyo, dedicación y confianza que permitieron la realización de este trabajo, y que han representado un gran aporte a mi formación académica y personal.*

*Al Mg. Dudbil Pabon, por proporcionarme los códigos y orientación en el proceso de caracterización del modulador de cristal líquido.*

*A mis profesores, por sus valiosas enseñanzas.*

*A mis compañeros y amigos por su constante apoyo, particularmente a Johan, Yesid, Lorena, Andrea, Pedro y Carlos.*

*A mis padrinos, Vicente Polentino y Myriam Ramirez, por que su apoyo fue fundamental para alcanzar esta meta.*

*A mis padres, mis hermanos y mi familia por su amor, paciencia, comprensión y especialmente por siempre creer en mi.*

*A todos los que directa o indirectamente contribuyeron a alcanzar esta meta.*

# **IMPLEMENTACIÓN DE UN PROCESADOR ÓPTICO-VIRTUAL DE ENCRIPCIÓN DE TRANSFORMADA CONJUNTA PARA LA GENERACIÓN DE CRIPTOGRAMAS CAMUFLADOS**

**María Alejandra Guerrero Vanegas**

*Estudiante de Física*

**Jorge Enrique Rueda Parada**

*Doctor en Ciencias Naturales - Física*

*Director del trabajo*

---

---

## **Resumen**

Se implementó un procesador óptico-virtual de encriptación usando una arquitectura de transformada conjunta. Presentamos una técnica óptica de encriptación que camufla el criptograma de ruido blanco, usando doble llave amplitud. Ubicamos en el plano objeto una llave de solo amplitud y en el plano de referencia una llave amplitud compleja. Validamos el método mediante simulaciones computacionales, usando imágenes binarias y RGB. El criptograma es de amplitud real y de aspecto único para cada imagen encriptada. Romper el criptograma requiere, adicionalmente a su detección, que se conozcan las dos llaves. Además, se presenta el diseño del sistema de cifrado-descifrado de transformada conjunta óptico-digital y los resultados del proceso de caracterización de un modulador espacial de luz de cristal líquido LCR-2500, realizado como parte del diseño del sistema de encriptación.

**Palabras clave:** Encriptación óptica, óptica de Fourier, transformada conjunta, armónicos circulares.

# Contenido

---

---

<b>1. INTRODUCCIÓN</b>	<b>1</b>
<b>2. FUNDAMENTOS DE ENCRIPCIÓN ÓPTICA</b>	<b>7</b>
2.1. Fundamentos de la Transformada de Fourier Óptica . . . . .	7
2.2. Procesador de Encriptación de Transformada Conjunta . . . . .	16
2.2.1. Proceso de cifrado . . . . .	18
2.2.2. Proceso de descifrado . . . . .	20
2.2.3. Encriptación usando doble máscara de fase aleatoria (DRPE)	28
<b>3. IMPLEMENTACIÓN DE UN PROCESADOR ÓPTICO-VIRTUAL DE ENCRIPCIÓN USANDO LLAVES DE AMPLITUD PERIÓDICA Y FASE EN ARMÓNICOS CIRCULARES</b>	<b>30</b>
3.1. Encriptación usando llaves en armónicos circulares . . . . .	30
3.1.1. Descomposición en Componentes Armónicas Circulares . .	31
3.1.2. Llaves de fase en CHC . . . . .	32
3.1.3. Encriptación usando una llave en armónicos circulares . . .	36
3.2. Encriptación usando una llave de amplitud periódica y fase en armónicos circulares . . . . .	38
<b>4. DISEÑO DE UN SISTEMA DE ENCRIPCIÓN DE TRANSFOR- MADA CONJUNTA ÓPTICO-DIGITAL</b>	<b>47</b>
4.1. Sistema de Encriptación de Transformada Conjunta Óptico-Digital	47

---

4.2. Caracterización de un Modulador de Cristal Líquido de Fase Nemática . . . . .	50
4.2.1. Polarización . . . . .	53
4.2.2. Proceso de Caracterización . . . . .	58
<b>5. CONCLUSIONES Y PERSPECTIVAS</b>	<b>72</b>
<b>REFERENCIAS BIBLIOGRÁFICAS</b>	<b>74</b>
<b>ANEXOS</b>	<b>80</b>
<b>A. MANUAL DE USUARIO PROCESADOR ÓPTICO VIRTUAL DE ENCRIPCIÓN JTCRYPTO.GOM</b>	<b>81</b>
A.1. Descripción de la ventana de encriptación: . . . . .	82
A.2. Descripción de la ventana de desencriptación: . . . . .	85
<b>B. MANUAL DE USUARIO SLM.GOM</b>	<b>88</b>
B.1. Descripción del panel Predecir Fase-Intensidad: . . . . .	89
<b>C. CARACTERIZACIÓN MODULADOR LCR 2500: GRAFICAS DE INTENSIDAD</b>	<b>91</b>

## Lista de Tablas

---

4.1. Características del TN-LCD Holoeye LC-R 2500 . . . . .	50
4.2. Fase introducida por el modulador . . . . .	67

## Lista de Figuras

---

---

2.1. Geometría de la difracción . . . . .	10
2.2. Aproximaciones de la teoría escalar de la difracción . . . . .	11
2.3. Difracción de Fraunhofer usando una lente. $f$ es la longitud focal de la lente convergente $L$ , $t(x, y)$ es la transmitancia del objeto difractor, $E(x_o, y_o)$ es el campo difractado. . . . .	13
2.4. Esquema de un procesador de encriptación de transformada conjunta. $f$ es la longitud focal de las lentes $L$ . El arreglo es iluminado con un frente de onda plano y coherente con longitud de onda $\lambda$ . . . . .	17
2.5. Diagrama del proceso de cifrado. $\mathcal{F}$ representa la transformada de Fourier; $\oplus$ representa el operador suma de las transformadas de $h(x, y) + k_f(x, y)$ . . . . .	18
2.6. Plano de entrada procesador de encriptación de transformada conjunta. $W_x$ representa el ancho del plano de entrada en el eje $x$ y $L_x$ es el ancho de la imagen a cifrar y de la llave de cifrado. . . . .	18
2.7. Ejemplo de un criptograma $I(f_x, f_y)$ . . . . .	19
2.8. Diagrama del proceso de descifrado. $\mathcal{F}$ representa la transformada de Fourier; $\otimes$ representa el operador multiplicación aritmética . . . . .	20
2.9. Diagrama del proceso de filtrado . . . . .	20
2.10. Proceso de de filtrado pasa-banda aplicado al criptograma . . . . .	22
2.11. Características de la llave de encriptación . . . . .	23
2.12. Resultado de la imagen descifrada. . . . .	24
2.13. Resultados del proceso de encriptación-descifrado. . . . .	25
2.14. Resultado de la encriptación usando una llave de fase aleatoria. . . . .	27

2.15. Resultados de la encriptación usando DRPE. . . . .	28
2.16. Resultados de la encriptación usando DRPE . . . . .	29
3.1. Descomposición en armónicos circulares (Orden $m = 1$ ) . . . . .	32
3.2. Fase e histogramas de las llaves $K(x, y)$ y $K_{CHC}(r, \theta)$ . . . . .	33
3.3. Fase e histogramas de las llaves $K_{CHC}(r, \theta)$ con distintos órdenes de descomposición . . . . .	34
3.4. Fase e histogramas de las llaves $K_{CHC}(r, \theta)$ con órdenes de des- composición fraccional . . . . .	35
3.5. Resultados de la encriptación usando llaves en CHC . . . . .	36
3.6. Resultados de la encriptación usando llaves en CHC . . . . .	37
3.7. Diagrama del método de encriptación . $\mathcal{F}$ representa la transfor- mada de Fourier, $\otimes$ representa multiplicación aritmética . . . . .	38
3.8. Resultados de la encriptación con llaves de amplitud periódica y fase en armónicos circulares . . . . .	42
3.9. Resultados de la encriptación con llaves de amplitud periódica y fase en armónicos circulares . . . . .	43
3.10. Resultados de la encriptación con llaves de amplitud periódica y fase en armónicos circulares . . . . .	44
3.11. Resultados de la encriptación con llaves de amplitud periódica y fase en armónicos circulares . . . . .	45
3.12. Resultados de la encriptación con llaves de amplitud periódica y fase en armónicos circulares . . . . .	46
4.1. Esquema experimental Sistema de Encriptación JT Óptico-Digital. SLM representa el modulador de cristal líquido, $R\lambda/2$ representa un retardador de media onda, BS: cubos divisores, M: Espejo, P.L: Polarizador Lineal, L: Lente positiva con focal f. . . . .	48
4.2. Esquema de la orientación del director del cristal líquido en un TN-LCD (a) Voltaje Nulo (b) Voltaje intermedio (c) Voltaje máximo	51
4.3. Diagrama del proceso de caracterización del modulador espacial de cristal líquido . . . . .	58

4.4. Arreglo Experimental Polarimetro de Mueller-Stokes. P.L: Polarizador lineal, $R\lambda/4$ : Retardador de cuarto de onda. SLM: Modulador LC-R 2500. El arreglo es iluminado por un frente de onda plano con longitud de onda $\lambda = 532nm$ . . . . .	61
4.5. Coeficientes de la matriz de Mueller del SLM para $\lambda = 532nm$ . .	62
4.6. Intensidad predicha por las matrices de Mueller vs Intensidad experimental . . . . .	63
4.7. Arreglo experimental para la determinación de la modulación en fase. L1 : Lente focal +25 cm. E: Espejo. $C_1, C_2, C_3$ : Cubos divisores. P.L: Polarizador Lineal. $R_{\lambda/2}$ : Retardador de media onda. SLM: Modulador LC-R 2500. $L_2$ : Lente focal +20 cm. La fuente de iluminación es un láser de estado sólido con longitud de onda $\lambda = 532nm$ . . . . .	64
4.8. Interferogramas: Zona de referencia nivel de gris 0; Zona de variable nivel de gris 40 . . . . .	66
4.9. Curvas de fase para modulación en sólo fase . . . . .	67
4.10. Matriz de Jones del SLM para $\lambda = 532nm$ . . . . .	69
4.11. Curvas de fase para distintas configuraciones de polarización. $\delta$ es la fase medida por interferometría, $\delta_{MJ}$ es la fase derivada de la matriz de Jones y $\beta = \delta - \delta_{MJ}$ es la fase asociada a la birrefringencia de la pantalla. . . . .	70
4.12. Fase $\beta$ . . . . .	71
A.1. Ventana menú JTCRYPTO.GOM . . . . .	82
A.2. Ventana Encriptar JTCRYPTO.GOM . . . . .	82
A.3. Ventana Encriptar; proceso cargar imagen . . . . .	83
A.4. Ventana Encriptar; proceso generar llave de fase . . . . .	83
A.5. Ventana Encriptar; proceso generar llave de amplitud . . . . .	84
A.6. Ventana Encriptar; proceso Encriptar . . . . .	84
A.7. Ventana desencriptar . . . . .	85
A.8. Ventana desencriptar; proceso cargar criptograma . . . . .	85

A.9. Ventana desencriptar; proceso generar llave de fase . . . . .	86
A.10. Ventana desencriptar; proceso generar llave de amplitud . . . . .	86
A.11. Ventana desencriptar; proceso desencriptar . . . . .	87
A.12. Ventana desencriptar; proceso guardar . . . . .	87
B.1. Ventana interface SLM.GOM . . . . .	88
B.2. Ventana interfaz SLM.GOM; panel Predecir Fase-Intensidad . . . . .	89
B.3. Ventana interfaz SLM.GOM; panel Buscar Modulación Fase-Intensidad . . . . .	90
C.1. Sistema de medida de intensidades-Polarimetro de Mueller. PL: Polarizador lineal; $R_{\lambda/4}$ : Retardador de cuarto de onda; E.O: Eje Óptico; E.R: Eje Rápido. La flecha verde representa la dirección de propagación del haz. . . . .	91
C.2. Ángulo Lámina Generadora= $0^\circ$ . . . . .	92
C.3. Ángulo Lámina Generadora= $52^\circ$ . . . . .	93
C.4. Ángulo Lámina Generadora= $103^\circ$ . . . . .	94
C.5. Ángulo Lámina Generadora= $155^\circ$ . . . . .	95
C.6. Ángulo Lámina Generadora= $206^\circ$ . . . . .	96
C.7. Ángulo Lámina Generadora= $258^\circ$ . . . . .	97
C.8. Ángulo Lámina Generadora= $310^\circ$ . . . . .	98

# Capítulo 1

## INTRODUCCIÓN

---

El término criptografía hace referencia a la disciplina encargada de diseñar y construir métodos de encriptación, donde la información cifrada denominada criptograma, solo pueda hacerse legible para aquellos que poseen la clave de descifrado [1,2].

Haciendo una reseña histórica, la necesidad de mantener comunicaciones privadas y de transmitir información de forma segura ha motivado el desarrollo de la criptografía desde los inicios de la humanidad [3]. Los primeros referentes históricos se encuentran en Egipto, China, Mesopotamia y la India donde la escritura por si misma era considerada un lenguaje secreto. Más adelante, en el siglo V a.c, aparecen en Grecia y Roma los primeros sistemas criptográficos, basados en los principios de sustitución y transposición. La sustitución consiste en cambiar la letra del texto original por otras que se encuentran ubicadas en un determinado número de espacios del alfabeto, usando este principio se creó en Roma el cifrario del Cesar que consistía en un algoritmo de sustitución monoalfabético; la transposición consiste en reorganizar el mensaje de tal forma que sea ilegible, ejemplo de ello es la escitela espartana. La escitela y el cifrario del Cesar son los dos referentes más importantes de la criptografía en la antigüedad. Durante la edad media los árabes desarrollaron métodos de criptoanálisis para descifrar mensajes. La criptografía resurge en Europa con el renacimiento, en esta época

es de destacar a León Alberti considerado uno de los padres de la criptografía, quien desarrolló el primer sistema de cifrado polialfabético conocido como disco de Alberti.

A partir del siglo XVIII se desarrollan distintos métodos criptográficos y la criptografía se hace de uso extensivo en Europa. El desarrollo del telégrafo, que permitió la transmisión de mensajes a lugares remotos, y la aparición del código morse, que si bien no es un método criptográfico sirve como alfabeto alternativo, hacen de la criptografía un campo de interés popular [3]. En los periodos de la primera y segunda guerra mundial los sistemas criptográficos tuvieron grandes avances alcanzando altos niveles de sofisticación. Como ejemplo de la automatización de la criptografía se encuentran, las máquinas “Enigma” ideada por los alemanes para cifrar sus mensajes, la máquina “Colossus” ideada por los ingleses para descifrar las claves de “Enigma”, y la máquina “MarkII (SIGABA)” desarrollada por los Estados Unidos.

La criptografía científica o moderna se desarrolla a partir de 1949 cuando Shanon la cimienta sobre bases matemáticas, de ello surgen los criptosistemas de llave privada: Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES); después de 1977 surgen los sistemas criptográficos de llave pública: Algoritmo de Rivest, Shamir y Adleman (RSA), Digital Signature Algorithm(DSA) y criptografía de curva elíptica, que utilizan una llave pública para cifrar y una privada para descifrar.

Con la llegada de la era digital y las nuevas tecnologías, la seguridad se ha convertido en un elemento fundamental de las comunicaciones planteando nuevos retos para los procesos de encriptación, que además de garantizar la confidencialidad del mensaje deben garantizar su autenticación, privacidad, autenticidad e integridad, sumado a la gran cantidad de información a procesar. Aunque ha habido grandes avances en los sistemas de encriptación estos no son 100% seguros dejando campo a nuevas investigaciones sobre sistemas de encriptación clásicos

---

y cuánticos. Recientemente la criptografía cuántica ha tenido grandes avances, y resulta ser un campo con grandes potencialidades en la transmisión totalmente segura de la información, en este sentido se han desarrollado algoritmos para la encriptación de imágenes basados en principios cuánticos [4, 5], con el propósito de mejorar la seguridad que proporcionan los métodos clásicos de encriptación de imágenes.

Dentro de la criptografía clásica, los procesadores ópticos de encriptación resultan de interés en el campo de la seguridad informática por ofrecer robustez y gran seguridad en el cifrado de información donde se aprovechan las ventajas del procesamiento óptico en cuanto a su alta capacidad y velocidad de procesamiento en paralelo, sumado a los múltiples grados de libertad a la hora de cifrar, que los hace herramientas eficientes [3]. Tomando como base tales ventajas de la óptica, se han realizado diferentes estudios, con el objetivo de obtener procesadores de encriptación ópticos que otorguen gran robustez y seguridad en el cifrado.

La primera propuesta de encriptación óptica la hace Francon en 1975 donde sugiere encriptar usando los cambios aleatorios de fase producidos por un difusor. En 1995 Refregier y Javidi [6] proponen los sistemas de procesamiento óptico como herramientas de encriptación segura. En 1996 Javidi implementó experimentalmente la encriptación de imágenes basado en una arquitectura  $4f$  utilizando un método de doble máscara de fase o DRPE (Double Random Phase Encoding) [7] que permite codificar la información como ruido blanco. En el 2000 Javidi et Al. [8] proponen la implementación de un procesador de encriptación usando DRPE y una arquitectura de correlación de transformada conjunta, encontrando la ventaja de eliminar la necesidad del complejo conjugado de la llave en la desencriptación.

A partir de estos aportes se han implementado diferentes procesadores de encriptación sobre la base de la arquitectura de los correladores ópticos Vander Lugt (VLC: Vander Lugt Correlator) y de transformada conjunta (JTC: Joint

---

Transform Correlator). Se han desarrollado trabajos donde se utilizan distintos métodos de encriptación, se ha hecho encriptación en amplitud y totalmente en fase [9, 10]; se han utilizado distintas transformadas [11–14]. Como alternativas a las máscaras convencionales se ha propuesto el uso de máscaras determinísticas de fase [15], máscaras fractales [16] y máscaras de fase en armónicos circulares [17]; se ha encriptado en términos de la longitud de onda, de la polarización de la luz, entre otros, aprovechando los grados de libertad que ofrecen los sistemas ópticos [13, 15, 17–24]. Además se han realizado trabajos acerca de su robustez, vulnerabilidad y limitaciones [10, 25–27]. En la actualidad, las investigaciones se han centrado en las técnicas de multiplexado implementado inicialmente por M. Islam [19]. Esta técnica consiste en la combinación de una cantidad de información en un mismo medio de registro, con la finalidad de aprovechar los canales de transmisión [19, 28, 29].

La encriptación usando un JTC ha sido extendida al dominio de Fresnel y Fraccional [12], se han implementado distintos procesadores de encriptación sobre la base de esta arquitectura, por ejemplo, se ha hecho uso de máscaras fractales [16], llaves usando mapas caóticos [23], encriptación de videos [30], entre otros [18, 19, 25, 28, 31, 32]; Se han realizado trabajos sobre el diseño óptimo de llaves de encriptación en un JTC y su implementación experimental [33–35], trabajos referentes a multiplexado [29] y criptoanálisis [26].

En los diferentes trabajos reportados, la información cifrada o criptograma, tiene una apariencia ligada a las máscaras y llaves de cifrado que se implementan en el procesador. De esta forma, en un procesador de encriptación convencional donde el cifrado se realiza a partir de máscaras de ruido blanco es de esperar que la información sea encriptada bajo este mismo aspecto. Un cambio en los parámetros de encriptación permitiría la modificación del criptograma, de forma tal que si se diseñasen máscaras y llaves que puedan ser modificadas según ciertos parámetros, es posible controlar el aspecto de los criptogramas. Transformar el aspecto del criptograma se hace interesante al proporcionar un valor adicional

---

de seguridad, que permite ocultar o borrar la idea de presencia de información cifrada, al camuflarla en imágenes con una apariencia determinística.

En vista de lo anterior nos planteamos como objetivo implementar un procesador de encriptación óptico-virtual, usando llaves en armónicos circulares y máscaras de estructura periódica, de tal forma que el resultado fuera la generación de criptogramas camuflados como una imagen determinística y diferente para cada criptograma, centrándonos en el uso de una arquitectura de transformada conjunta en la encriptación, y un procesador 4f para la desencriptación de la información.

Este trabajo se enmarca dentro de un tema de investigación que se ha venido trabajando en el Grupo Óptica Moderna de la Universidad de Pamplona, donde se han realizado distintos trabajos referentes a la criptografía óptica [2, 11, 17, 36, 37]; dentro de ellos está la implementación de un procesador virtual de encriptación usando una arquitectura VLC que permite camuflar el criptograma en una imagen de aspecto determinístico y único para cada imagen cifrada [2], la transformación del criptograma en ese trabajo se basa en el uso de máscaras de amplitud periódica y llaves en armónicos circulares, y fue el principal referente para la realización de la investigación.

Para una clara presentación de los resultados este informe se estructuró como sigue, en el capítulo 2 se presentan los aspectos físico-matemáticos de la transformada de Fourier, su relación con el fenómeno de la difracción, y la modelación del procesador óptico de encriptación de transformada conjunta, que constituyen los conceptos básicos sobre los que se fundamenta este trabajo. En el capítulo 3 se detalla el método de encriptación desarrollado para la transformación del criptograma; el método consiste en utilizar llaves con fase en armónicos circulares y amplitud periódica. En el capítulo 4 se presenta un esquema del diseño de un arreglo de encriptación óptica de transformada conjunta, que queda como perspectiva de implementación en trabajos futuros. En este sentido, teniendo en cuenta que el Grupo Óptica Moderna cuenta uno de los dispositivos fundamen-

tales para sintetizar llaves de encriptación (modulador espacial de cristal líquido LCR-2500), se implementó un método de caracterización de este modulador de luz, por cuanto en la eventual implementación óptica de las llaves de encriptación se hace necesario conocer la respuesta de modulación en fase e intensidad de este dispositivo. Se presentan los resultados de la caracterización.

Producto de los resultados obtenidos se desarrollaron dos interfaces gráficas, los aspectos técnicos de su funcionamiento se detallan en los anexos. La primera interfaz denominada JTCrypto.GOM, corresponde una herramienta de encriptación con el método desarrollado que permite encriptar imágenes bitmap en un formato novedoso. La otra interfaz denominada SLM.GOM permite predecir el comportamiento en fase e intensidad que tendrá el modulador para diferentes configuraciones polarimétricas.

# Capítulo 2

## FUNDAMENTOS DE ENCRIPCIÓN ÓPTICA

---

Los procesadores ópticos de encriptación se basan en arquitecturas de correlación para procesamiento óptico tipo Vander Lugh [38] y de transformada conjunta [39] que permiten el cifrado de información mediante operaciones de convolución y correlación. Estos procesadores se fundamentan en la propiedad de correlación de la transformada de Fourier y en la posibilidad de implementar arreglos ópticos que permiten calcular dicha transformada.

### 2.1 FUNDAMENTOS DE LA TRANSFORMADA DE FOURIER ÓPTICA

La transformada de Fourier llamada así por Joseph Fourier, fue desarrollada a partir de las series de Fourier y es una herramienta de gran utilidad en el análisis de funciones periódicas y no periódicas [40]. La transformada de Fourier convierte una función del dominio espacial o temporal al dominio de las frecuencias y viceversa, siempre que la función sea continua y de cuadrado integrable.

La transformada de Fourier  $G(u, v)$  de una función  $g(x, y)$  se define como:

$$G(u, v) = \int \int_{-\infty}^{\infty} g(x, y) e^{-i2\pi(ux+vy)} dx dy \quad (2.1)$$

Donde  $(u, v)$  son las coordenadas de frecuencias espaciales relativas a las coordenadas  $(x, y)$ . De forma abreviada la transformada se denota como  $\mathcal{F}\{g(x, y)\}$ .

La transformada inversa  $\mathcal{F}^{-1}\{G(u, v)\}$ , se define como:

$$g(x, y) = \int \int_{-\infty}^{\infty} G(u, v) e^{i2\pi(ux+vy)} du dv \quad (2.2)$$

Es conocido que la transformada de Fourier está ligada al fenómeno de difracción de la luz. Este fenómeno da cuenta de la propagación de las ondas electromagnéticas al pasar por obstáculos de dimensiones comparables con su longitud de onda.

Haciendo una breve reseña histórica [40], Francesco Grimaldi expone por primera vez el fenómeno de difracción acuñando el nombre de “diffractio” [41]. J Sommerfeld definió la difracción como “toda desviación de los rayos luminosos de su trayectoria rectilínea que no se puede explicar ni por refracción ni por reflexión”. Huygens (1678) propone la teoría ondulatoria y expresa que si cada punto del frente de onda es considerado como un nuevo frente de onda esférico “secundario” se podría determinar la superficie de la onda en cualquier instante posterior mediante la construcción de la envolvente de las ondas secundarias. Fresnel (1818) se apoya en el principio de Huygens y en la interferencia de Young para dar las bases matemáticas a la difracción. Kirchhoff (1882) formula el problema de la difracción basándolo en un teorema integral que expresa la solución de la ecuación de onda homogénea como un problema de valores de frontera de la luz sobre la superficie del obstáculo. Poincaré y Sommerfeld corrigen esta formulación demostrando que las ecuaciones de Kirchhoff eran falsas y que el principio de Huygens-Fresnel era válido solo en primera aproximación. Sommerfeld elimina

la ecuación de Kirchhoff correspondiente a las condiciones de Frontera y hace uso de las funciones de Green; esto conduce a lo que se conoce como teoría de difracción de Rayleigh-Sommerfeld.

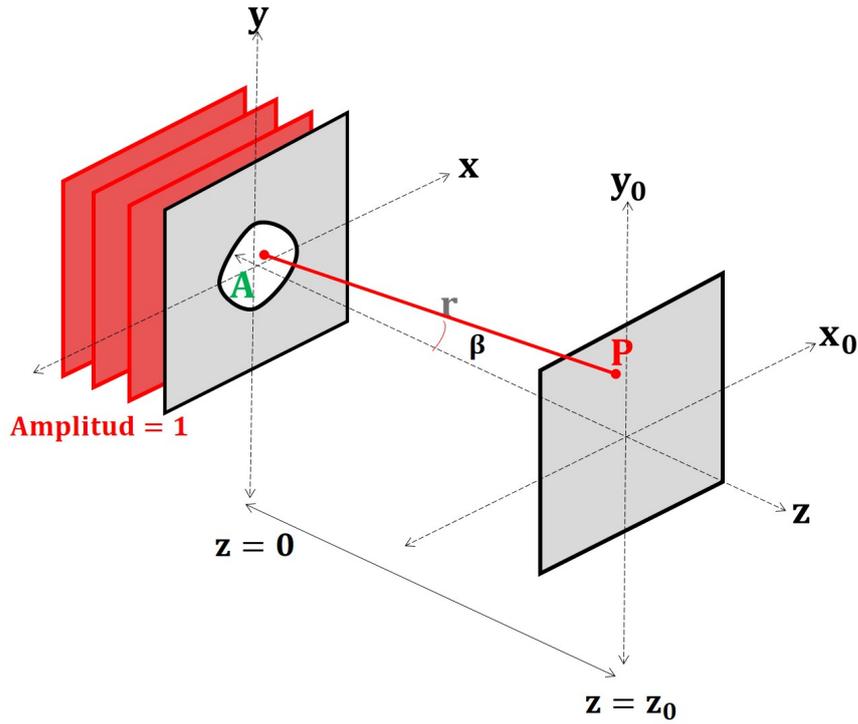
La teoría escalar de la difracción permite tratar el comportamiento de la propagación de la luz de forma simplificada al no considerar el carácter vectorial de las ondas electromagnéticas; esta simplificación es válida cuando la fuente se encuentra muy alejada de la pantalla y el obstáculo tiene dimensiones mayores que la longitud de onda, bajo esas condiciones los efectos de la polarización son despreciables y el campo puede tratarse como una variable que verifica la ecuación de onda escalar:

$$\nabla^2 E(x, y, z, t) = \frac{1}{v^2} \frac{\partial^2}{\partial t^2} E(x, y, z, t) \quad (2.3)$$

De esta forma, la onda difractada en un punto P (Figura 2.1) puede expresarse haciendo uso de la ecuación de Rayleigh-Sommerfeld, como sigue:

$$E(x_o, y_o, z_o) = \frac{1}{i\lambda} \int_A t(x, y) \frac{\exp(ikr)}{r} \cos(\beta) dx dy \quad (2.4)$$

La anterior expresión se explica como una suma ponderada de ondas esféricas que parten de la abertura A con función de transmitancia  $t(x, y)$  y que llegan a un punto P con coordenadas  $(x_o, y_o, z_o)$ ; la integración se realiza sobre el área de la abertura A y la distancia al punto P es  $r = \sqrt{(x - x_o)^2 + (y - y_o)^2 + z_o^2}$ . En la ecuación 2.4,  $k$  es el número de onda,  $\cos(\beta)$  se refiere al factor de oblicuidad y  $\lambda$  es la longitud de onda.

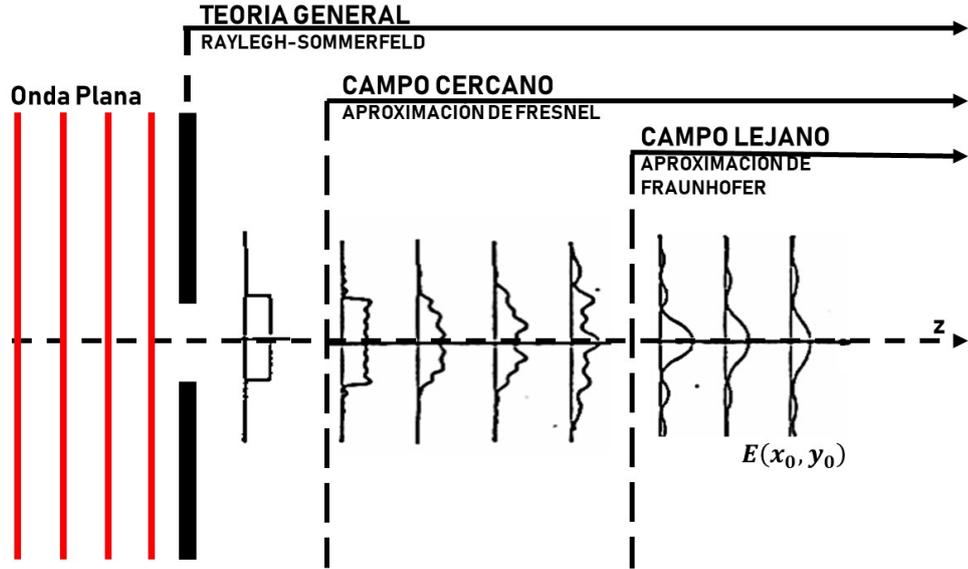


**Figura 2.1:** Geometría de la difracción

La ecuación (2.4) se suele simplificar mediante aproximaciones más sencillas. Estas aproximaciones permiten hacer simplificaciones de la integral de difracción para valores de  $z_0$  mucho mayores que las dimensiones transversales del objeto. Esto es posible partiendo de que  $r$  puede expresarse como  $r = z_0 \sqrt{1 + \left(\frac{x-x_0}{z_0}\right)^2 + \left(\frac{y-y_0}{z_0}\right)^2}$ , que puede ser aproximado a partir de una serie de Taylor, de la siguiente forma:

$$kr = kz_0 + \frac{k}{2z_0}(x_0^2 + y_0^2) - \frac{k}{z_0}(x_0x + y_0y) + \frac{k}{2z_0}(x^2 + y^2) - \frac{k}{8z_0^3}[(x - x_0)^2 + (y - y_0)^2]^2 + \dots \quad (2.5)$$

Se denomina aproximación de Fresnel si se toman los cuatro primeros términos de la expansión, es una aproximación de Fraunhofer si tomamos los tres primeros términos. La Figura 2.2 es un esquema conceptual que describe las zonas de propagación del campo difractado.



**Figura 2.2:** Aproximaciones de la teoría escalar de la difracción

En la aproximación de Fresnel o de campo cercano las ondas que salen de la abertura  $A$  no son esféricas, son ondas de perfil paraboloides, así la onda difractada se expresa como:

$$E(x_o, y_o, z_o) = \frac{1}{i\lambda z} \int_A t(x, y) \exp \left[ ik \left( z_o + \frac{(x - x_o)^2 + (y - y_o)^2}{2z_o} \right) \right] dx dy \quad (2.6)$$

Donde  $E(x_o, y_o)$  es el campo observado sobre el plano  $(x_o, y_o)$  ubicado a una distancia  $z_o$  del objeto difractor de transmitancia  $t(x, y)$ . Al realizarse la integración sobre la abertura  $A$ , la ecuación anterior puede ser generalizada a todo el espacio, tomando la función  $t(x, y) = 0$  por fuera de abertura, así:

$$E(x_o, y_o, z_o) = \frac{\exp(ikz_o)}{i\lambda z_o} \exp \left( \frac{ik}{2z_o} (x_o^2 + y_o^2) \right) \int \int_{-\infty}^{\infty} t(x, y) \exp \left[ \frac{ik}{2z_o} (x^2 + y^2) \right] \exp \left[ \frac{-ik}{z_o} (x_o x + y_o y) \right] dx dy \quad (2.7)$$

Si consideramos un plano de observación tal que  $z_o$  sea mucho mayor que las dimensiones del objeto difractor, entonces,  $e^{\frac{ik}{2z_o}(x^2+y^2)} \approx 1$ , y si realizamos el cambio de variable  $u = \frac{x_o}{\lambda z_o}$ ,  $v = \frac{y_o}{\lambda z_o}$ , donde  $u$ ,  $v$  son las frecuencias espaciales en el plano  $(x_o, y_o)$ ; estas consideraciones nos conducen a la aproximación de Fraunhofer, por lo que la integral de difracción toma la forma:

$$E(u, v, z_o) = \frac{\exp(ikz_o)}{i\lambda z_o} \exp(i\pi(u^2 + v^2)) \int \int_{-\infty}^{\infty} t(x, y) \exp(-i2\pi(ux + vy)) dx dy \quad (2.8)$$

Como se observa en la ecuación (2.8), la aproximación refiere a que las ondas elementales en el plano A son ondas planas. Esta ecuación contiene en la integral la transformada de Fourier del objeto difractor  $t(x, y)$ . La difracción de Fraunhofer produce una transformada de Fourier no exacta del objeto difractor; el espectro del campo de difracción de Fraunhofer será equivalente al de una transformada de Fourier salvo por la constante  $\frac{1}{(\lambda z_o)^2}$ :

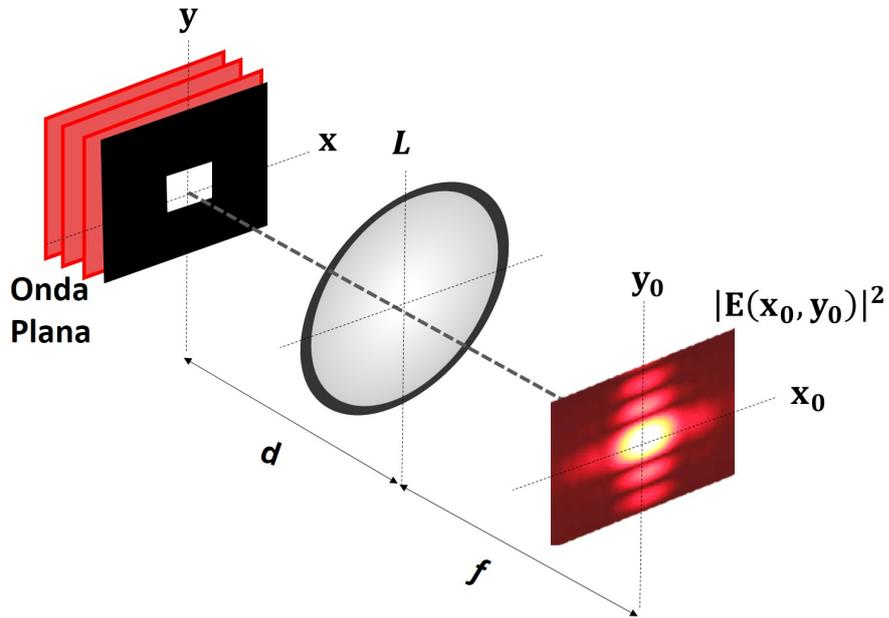
$$I(u, v, z) = \frac{1}{(\lambda z_o)^2} \left| \int \int_{-\infty}^{\infty} t(x, y) \exp(-i2\pi(ux + vy)) dx dy \right|^2 \quad (2.9)$$

Adicionalmente, haciendo uso de una lente convergente es posible implementar arreglos ópticos que permitan obtener transformadas de Fourier en el plano focal de la lente. Esto se puede explicar partiendo de que la transmitancia de una lente introduce en el frente de onda un factor de fase  $\exp\left(\frac{-ik}{2f}(x^2 + y^2)\right)$ , siendo  $f$  la longitud focal de la lente.

Si ubicamos el plano difractor con transmitancia  $t(x, y)$  en el plano anterior a la lente, al atravesarla obtenemos el campo  $t'(x, y) = t(x, y) \exp\left(\frac{-ik}{2f}(x^2 + y^2)\right)$ , al introducir  $t'(x, y)$  en la ecuación (2.7), el factor de fase cuadrático que se presenta en la integral es compensado por la transmitancia de la lente, por lo que el campo

de Fraunhofer se visualizará en el plano de observación ubicado en la focal de la lente ( $z_o = f$ ). Si el plano difractor se encuentra a una distancia  $d$  de la lente (figura 2.3), el campo en el plano  $(x_o, y_o)$  se puede expresar como sigue:

$$E(x_o, y_o, f) = \frac{\exp(ikf)}{i\lambda f} \exp\left[\frac{ik}{2d}\left(1 - \frac{d}{f}\right)(x_o^2 + y_o^2)\right] \int \int_{-\infty}^{\infty} t(x, y) \exp\left[\frac{-i2\pi}{\lambda f}(x_o x + y_o y)\right] dx dy \quad (2.10)$$



**Figura 2.3:** Difracción de Fraunhofer usando una lente.  $f$  es la longitud focal de la lente convergente  $L$ ,  $t(x, y)$  es la transmitancia del objeto difractor,  $E(x_o, y_o)$  es el campo difractado.

En el caso particular en que  $d = f$ , tenemos un arreglo óptico correspondiente a un procesador  $2f$ , donde el objeto difractor y el plano de observación se encuentran a la distancia focal de la lente, este arreglo permite calcular una transformada de Fourier escalada:

$$E(x_o, y_o, f) = \frac{\exp(ikf)}{i\lambda f} \int \int_{-\infty}^{\infty} t(x, y) \exp\left[\frac{-i2\pi}{\lambda f}(x_o x + y_o y)\right] dx dy \quad (2.11)$$

El proceso de encriptación óptica se fundamenta en la transformada de Fourier, que permite el cifrado-descifrado de imágenes mediante operaciones de convolución y correlación con funciones de fase con valores aleatorios, denominados llaves de encriptación. En la descripción físicomatemática realizada anteriormente, se mostró que es posible obtener transformadas de Fourier a partir de arreglos ópticos. Esta propiedad es la base de los procesadores ópticos, que consisten en combinaciones de arreglos 2f.

El procesador óptico de encriptación implementado en este trabajo se basa en un correlador de transformada conjunta en la etapa de cifrado, por lo que su arquitectura corresponde a un procesador 2f que transforma simultáneamente dos escenas (la imagen a cifrar y la llave de encriptación), el espectro conjunto de potencias dará como resultado una imagen cifrada denominada criptograma. El proceso de descifrado corresponde a un procesador 4f que permite la recuperación de la imagen.

Teniendo en cuenta que el objetivo de este trabajo es la implementación de simulaciones computacionales de criptosistemas ópticos de transformada conjunta, es necesario establecer la transformada de Fraunhofer discreta, en cuyo caso se requiere reescribir la transformada de Fourier discreta, esto es:

$$G(u, v) = \frac{1}{NM} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} g(x, y) \exp \left[ -2\pi \left( u \frac{x}{M} + v \frac{y}{N} \right) \right] \quad (2.12)$$

Donde  $u = 0, \dots, (M - 1)$  ;  $v = 0, \dots, (N - 1)$ , siendo  $N \times M$  el tamaño de la imagen  $g(x, y)$ .

En la modelación computacional realizada trabajamos con el algoritmo de la transformada rápida de Fourier discreta (FFT) desarrollado por MathWorks. La transformada rápida fue adaptada para simular la propagación del campo óptico.

La expresión de la difracción de Fraunhofer puede ser reconocida como una transformada de Fourier escalada con el cambio de variable:  $u \rightarrow x_o/\lambda z_o$ ,  $v \rightarrow y_o/\lambda z_o$ , ya que la transformada discreta no incluye los intervalos de muestreo  $\Delta x$ ,  $\Delta y$ , es necesario agregarlos para obtener la escala apropiada del problema físico [42]. Si consideramos la expresión para la difracción del campo en un arreglo 2f (ecuación 2.11), la propagación discretizada será:

$$\begin{aligned} G(u, v) &= \frac{\exp(ikf)}{i\lambda f} \frac{1}{NM} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} g(x, y) e^{-2\pi i(u \frac{x}{M} + v \frac{y}{N})} \Delta x \Delta y \quad (2.13) \\ &= \frac{\exp(ikf)}{i\lambda f} \mathbf{FFT} \{g(x, y)\} \Delta x \Delta y \end{aligned}$$

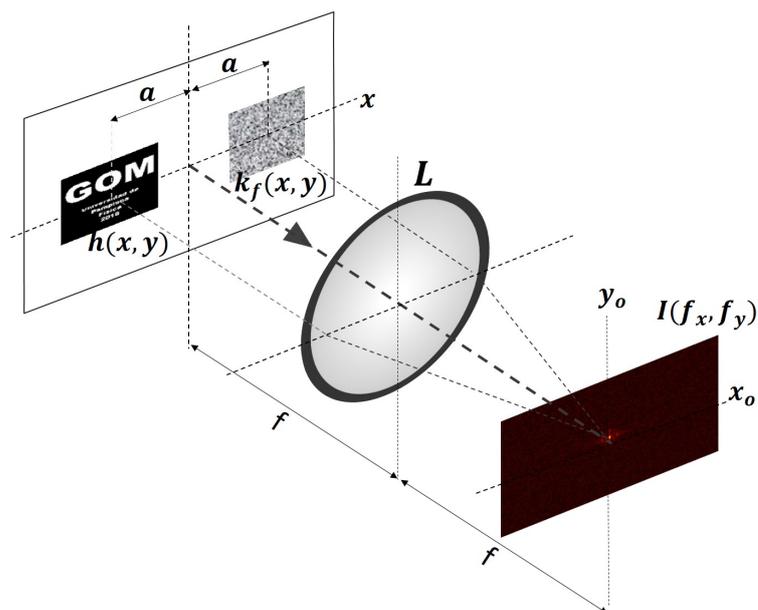
Los resultados presentados en este trabajo se obtuvieron usando la modelación de la propagación del campo en un procesador óptico, el algoritmo implementado requiere los parámetros del plano fuente, la longitud de onda con que se ilumina el arreglo y la focal de la lente utilizada.

---

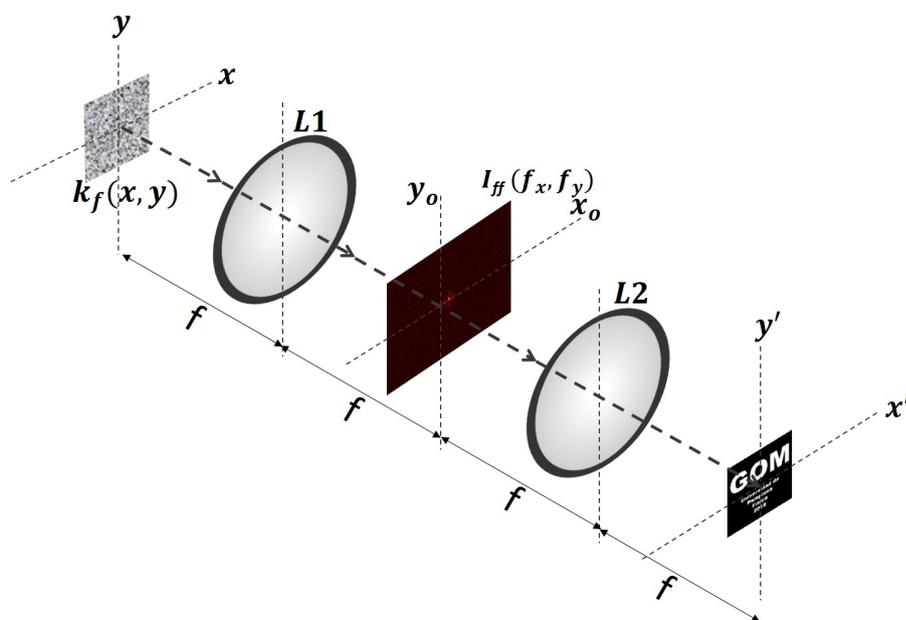
## 2.2 PROCESADOR DE ENCRIPCIÓN DE TRANSFORMADA CONJUNTA

El correlador de transformada conjunta (JTC: Joint Transform Correlator) es un arreglo óptico que permite correlacionar o convolucionar dos funciones 2D [39], su característica principal es que el filtro y la función a ser filtrada se encuentran simultáneamente en el plano de entrada por lo que en el plano de Fourier se obtienen sus transformadas de forma conjunta; la correlación entre las escenas se obtendrá difractando el espectro de potencias de la transformada conjunta, este sistema tiene la ventaja de ser inherentemente holográfico por lo que no requerirá una onda de referencia para registrar la información de fase. Este método ha sido usado extensivamente en el reconocimiento de patrones [43,44] y también es objeto de estudio en la encriptación de imágenes [8].

El proceso de encriptación usando una arquitectura de transformada conjunta registra simultáneamente la transformada de Fourier de la llave de encriptación y la imagen a cifrar, la información cifrada corresponderá al espectro de potencias de esta transformada. El descifrado se realiza haciendo uso de un procesador 4f, con la ventaja respecto a otros métodos de encriptación, de no requerir la conjugación en fase de la llave de encriptación para la recuperación de la imagen. El procesador de encriptación de transformada conjunta se describe en dos etapas, el proceso de cifrado y el proceso de descifrado (Figura 2.4), la descripción físico-matemática del procesador se presenta a continuación.



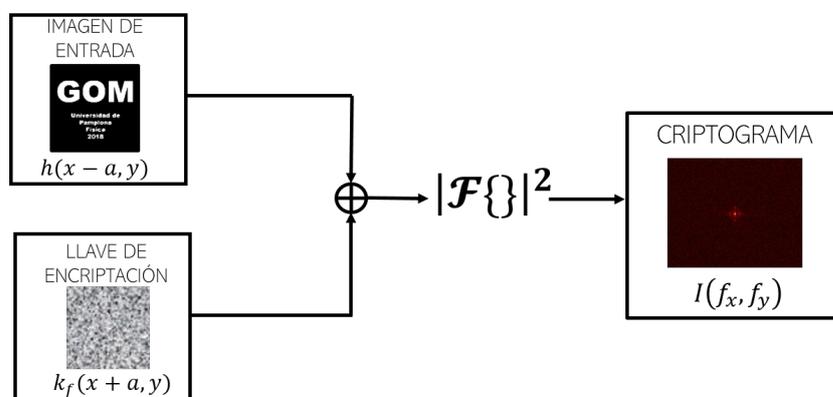
(a) Procesador de cifrado



(b) Procesador de descifrado

**Figura 2.4:** Esquema de un procesador de encriptación de transformada conjunta.  $f$  es la longitud focal de las lentes  $L$ . El arreglo es iluminado con un frente de onda plano y coherente con longitud de onda  $\lambda$ .

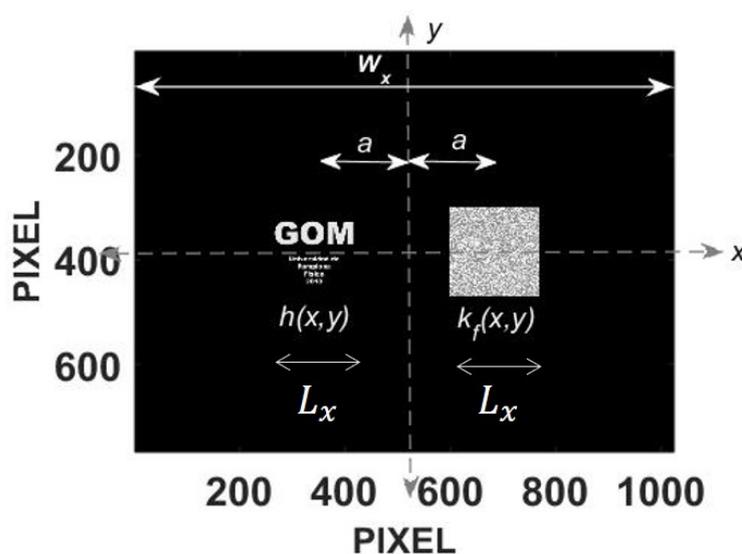
## 2.2.1 PROCESO DE CIFRADO



**Figura 2.5:** Diagrama del proceso de cifrado.  $\mathcal{F}$  representa la transformada de Fourier;  $\oplus$  representa el operador suma de las transformadas de  $h(x, y) + k_f(x, y)$

Como se indicó, el proceso de cifrado requiere una arquitectura  $2f$  (Figura. 2.4(a) y figura. 2.5) en la cual la imagen a cifrar  $h(x, y)$  y la llave  $k_f(x, y)$  se encuentran en el mismo plano separadas una distancia  $a$  del centro en el eje  $x$ :

$$f(x, y) = h(x + a, y) + k_f(x - a, y) \quad (2.14)$$



**Figura 2.6:** Plano de entrada procesador de encriptación de transformada conjunta.  $W_x$  representa el ancho del plano de entrada en el eje  $x$  y  $L_x$  es el ancho de la imagen a cifrar y de la llave de cifrado.

Mediante la transformada de Fourier producida por la lente L obtenemos la imagen cifrada en el plano  $(x_o, y_o)$ . Esta transformada corresponde a la superposición de las transformadas de Fourier de la imagen a cifrar y la llave de cifrado, esto es:

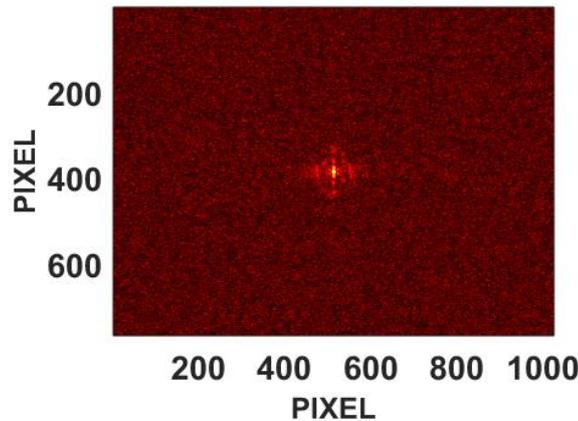
$$F(f_x, f_y) = \frac{1}{\lambda f} [H(f_x, f_y) \exp(i2\pi a f_x) + K_f(f_x, f_y) \exp(-i2\pi a f_x)] \quad (2.15)$$

$$\text{Con } f_x = \frac{x_o}{\lambda f} \text{ y } f_y = \frac{y_o}{\lambda f}$$

Donde  $H(f_x, f_y)$  corresponde a la transformada de Fourier de la imagen  $h(x, y)$  y  $K_f(f_x, f_y)$  a la transformada de Fourier de la llave  $k_f(x, y)$ ,  $\lambda$  a la longitud de onda del frente de onda que ilumina el arreglo,  $f$  es la focal de la lente L, y  $f_x$  y  $f_y$  son coordenadas de frecuencias espaciales.

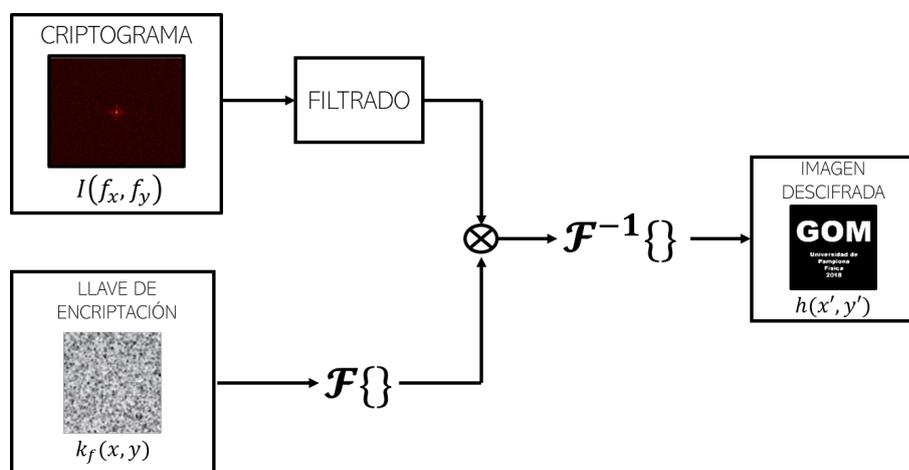
La imagen cifrada  $I(f_x, f_y) = |F(f_x, f_y)|^2$ , en adelante denominada criptograma, corresponderá al espectro de potencias de la transformada conjunta, esto es:

$$I(f_x, f_y) = \frac{1}{(\lambda f)^2} \left[ |H(f_x, f_y)|^2 + |K_f(f_x, f_y)|^2 + H(f_x, f_y) K_f^*(f_x, f_y) \exp(i4\pi a f_x) + H^*(f_x, f_y) K_f(f_x, f_y) \exp(-i4\pi a f_x) \right] \quad (2.16)$$



**Figura 2.7:** Ejemplo de un criptograma  $I(f_x, f_y)$

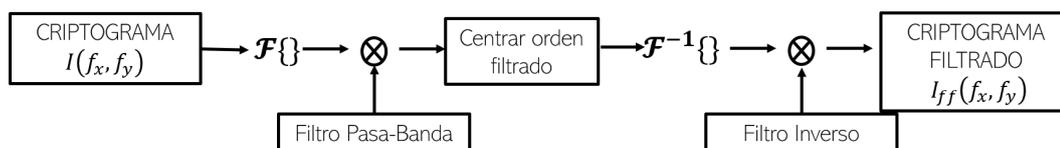
## 2.2.2 PROCESO DE DESCIFRADO



**Figura 2.8:** Diagrama del proceso de descifrado.  $\mathcal{F}$  representa la transformada de Fourier;  $\otimes$  representa el operador multiplicación aritmética

### 2.2.2.1 Proceso de filtrado

El criptograma fue modificado usando dos procesos de filtrado descritos en la figura 2.9, los dos procesos se realizaron con el objetivo de mejorar la relación señal-ruido en la imagen descifrada.



**Figura 2.9:** Diagrama del proceso de filtrado

De la ecuación (2.16) es fácil ver que el criptograma contiene términos no necesarios para descifrar la imagen, en cambio estos términos pueden ocasionar una reducción en la relación señal ruido en la imagen descifrada. Mediante un filtro pasa banda aplicado a la transformada de Fourier del criptograma es posible seleccionar la información necesaria para el descifrado y mejorar su calidad. Esta transformada tiene la siguiente forma:

$$\begin{aligned} \mathcal{F}\{I(f_x, f_y)\} = \frac{1}{\lambda f} & \left[ h(x', y') \odot h(x', y') + k_f(x', y') \odot k_f(x', y') \right. \\ & \left. + h(x' + 2a, y') \odot k_f(x' + 2a, y') + k(x' - 2a, y') \odot h_f(x' - 2a, y') \right] \end{aligned} \quad (2.17)$$

El operador  $\odot$  denota correlación. Considerando  $W_x$  como el ancho del plano en dirección x, y  $L_x$  como el ancho de la imagen a encriptar y de la llave, las dimensiones de los términos de la ecuación 2.17, permiten obtener un criterio para realizar el filtrado pasa-banda de manera óptima, así:

$$\frac{W_x - 2L_x}{4} \geq a, f_p > \frac{L_x}{\lambda f} \quad (2.18)$$

Siendo  $f_p = \frac{a}{\lambda f}$  la frecuencia portadora de la transformada conjunta.

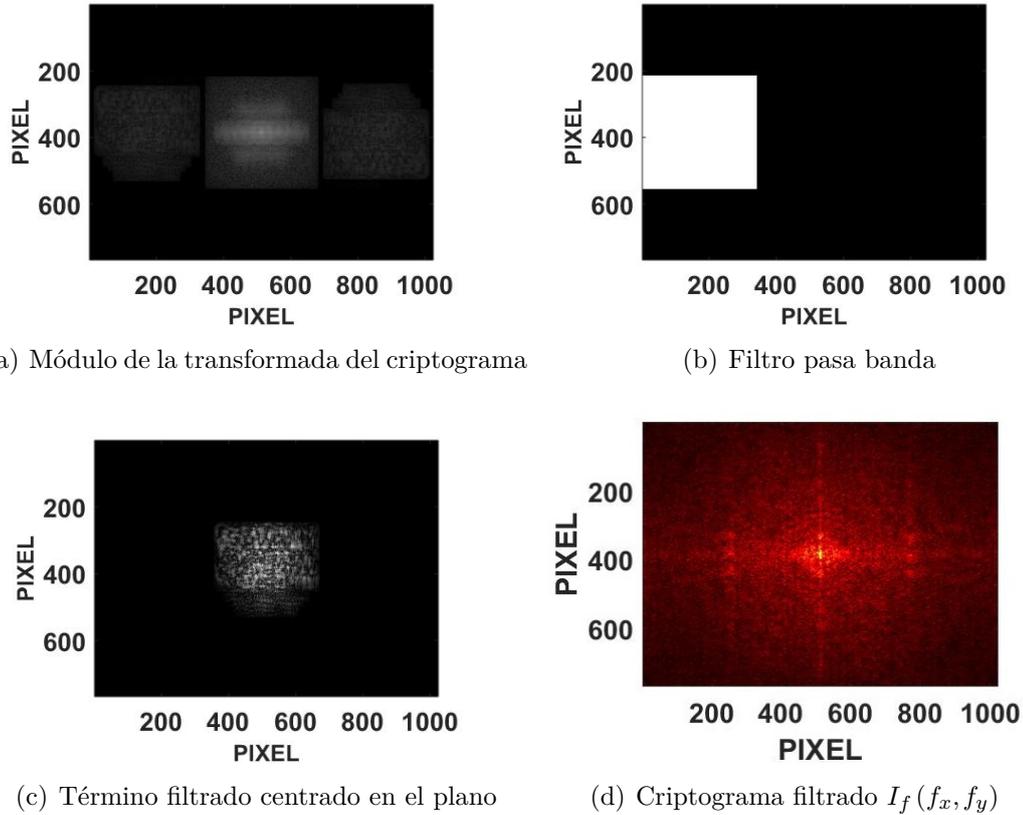
Es importante resaltar que el procesador de transformada conjunta impone restricciones en el tamaño del plano de entrada y de las escenas allí ubicadas, estos deben cumplir las condiciones anteriormente descritas (Ecuación 2.18), pues de lo contrario se presentará superposición de los términos al descifrar o al filtrar. Aplicamos a la ecuación 2.17 el siguiente filtro pasa-banda, con el propósito de eliminar el primer, segundo y cuarto término:

$$Rect(x' + 2a, y') = \begin{cases} 1 & \text{si } -2a - L_x \leq x' \leq -2a + L_x \\ & -L_y \leq y' \leq L_y \\ 0 & \text{Fuera} \end{cases} \quad (2.19)$$

El resultado de aplicar el filtro se traslada al origen de coordenadas y se hace una transformada de Fourier, de tal forma que el criptograma posterior al primer filtrado toma la siguiente forma:

$$I_f(f_x, f_y) = \frac{1}{(\lambda f)^2} \left[ H(f_x, f_y) K_f^*(f_x, f_y) \right] \quad (2.20)$$

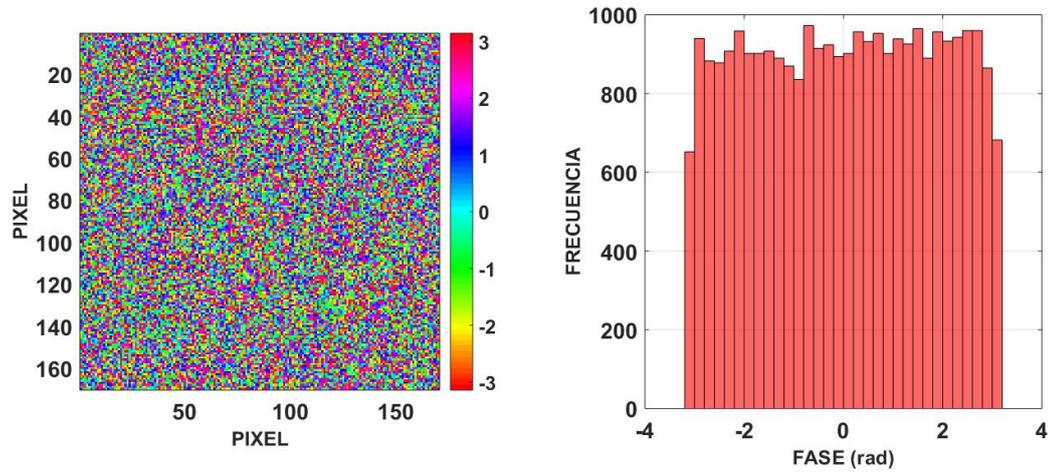
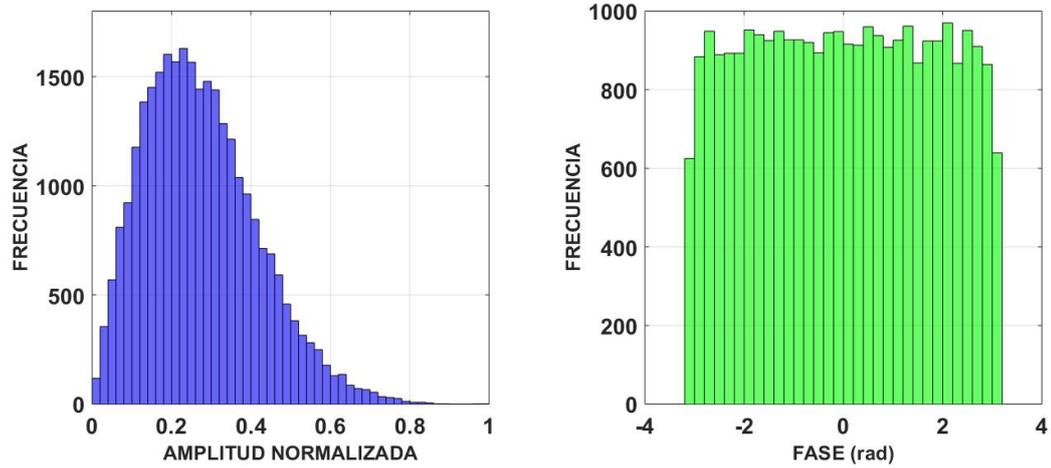
La figura 2.10 es un resultado, ejemplo, del proceso de filtrado pasa banda aplicado al criptograma:



**Figura 2.10:** Proceso de de filtrado pasa-banda aplicado al criptograma

Por otro lado, en un procesador de encriptación de transformada conjunta, la llave  $\mathcal{F}\{k_f(x, y)\} = K_f(f_x, f_y)$  debe ser de solo fase, así se garantiza que al ser iguales la llave de cifrado y la llave de descifrado, entonces  $K_f(f_x, f_y)K_f^*(f_x, f_y) = 1$ , eliminando toda la información correspondiente a ella de la imagen descifrada.

En este trabajo las llaves de encriptación son de la forma  $k_f(x, y) = \exp(i\phi(x, y))$ , donde la fase  $\phi(x, y)$  corresponde a valores aleatorios uniformemente distribuidos entre  $[-\pi, \pi]$  (Figura 2.11 (a) y (b)). Al realizar la transformada de la llave, la fase de esta también será una distribución de valores aleatorios entre  $[-\pi, \pi]$  como se observa en la figura (Figura 2.11 (d)), pero no corresponderá a una función de sólo fase, por lo que se obtiene el producto  $K_f(f_x, f_y)K_f^*(f_x, f_y) = |K(f_x, f_y)|^2$ , que representará ruido superpuesto a la imagen descifrada.

(a) Distribución de fase de la llave de  $k_f(x, y)$ (b) Histograma de la fase de  $k_f(x, y)$ (c) Histograma del modulo de  $K_f(f_x, f_y)$ (d) Histograma de la fase de  $K_f(f_x, f_y)$ **Figura 2.11:** Características de la llave de encriptación

Para solucionar este problema de ruido, con la amplitud de la transformada de la llave (Figura 2.11 (c)), se construyó un filtro inverso  $\frac{1}{|K_f(f_x, f_y)|^2}$  que se aplica al criptograma para eliminar toda la información correspondiente a la llave.

Una vez filtrado, el criptograma es:

$$I_{ff}(f_x, f_y) = \frac{1}{(\lambda f)^2} \frac{H(f_x, f_y)}{K_f(f_x, f_y)} \quad (2.21)$$

Finalmente, la imagen descifrada se obtiene mediante un procesado 4f como se muestra en la figura 2.4(b).

En el plano de entrada del 4f tenemos la llave de cifrado  $k_f(x, y)$ , y debido a la transformada realizada por la lente L1, en el plano espectral  $(x_o, y_o)$  obtendremos:

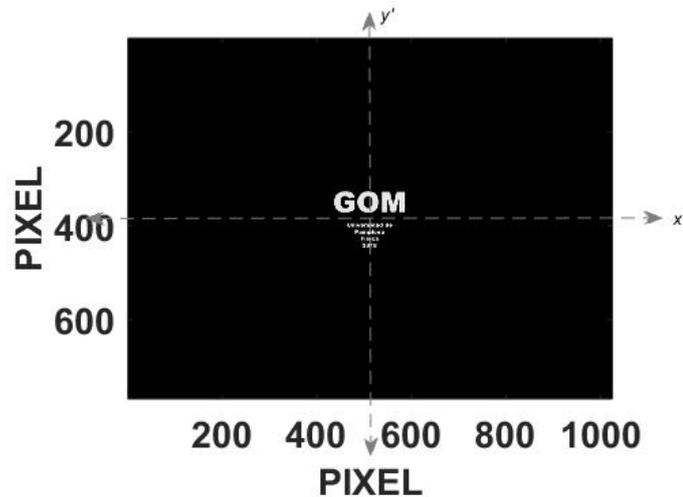
$$\mathcal{F}\{k_f(x, y)\} = \frac{1}{(\lambda f)} [K_f(f_x, f_y)] \quad (2.22)$$

El criptograma  $I_{ff}(f_x, f_y)$  está ubicado en el plano  $(x_o, y_o)$ , por lo cual tendremos el producto:

$$I_{ff}(f_x, f_y) K_f(f_x, f_y) = \frac{1}{(\lambda f)^3} [H(f_x, f_y)] \quad (2.23)$$

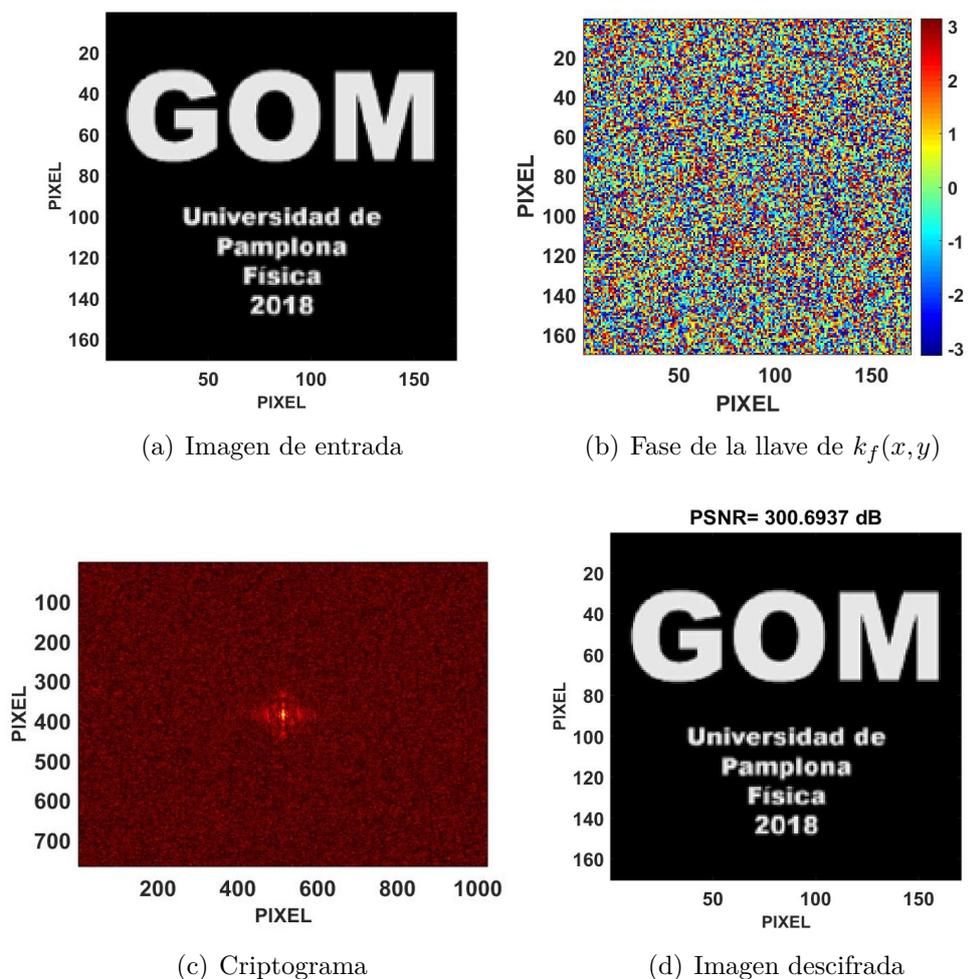
De esta forma, mediante la transformada de Fourier producida por la lente L2 observamos la imagen descifrada centrada en el plano  $(x', y')$ , así:

$$\begin{aligned} D(x', y') &= \mathcal{F}^{-1}\{I_{ff}(f_x, f_y) K_f(f_x, f_y)\} \\ &\approx h(x', y') \end{aligned} \quad (2.24)$$



**Figura 2.12:** Resultado de la imagen descifrada.

Desarrollamos una herramienta que simula el procesador óptico de encriptación, las simulaciones realizadas fueron ajustadas a las posibles condiciones con que se implementaría experimentalmente el procesador óptico. La herramienta permite la encriptación de imágenes BITMAP (binarias, de intensidad y RGB) de  $170 \times 170$  píxeles; el plano de entrada tiene un tamaño de  $1024 \times 768$  píxeles; el tamaño de pixel es de  $19 \mu m$ , por lo que las dimensiones del plano de entrada son  $19.6 \text{ mm} \times 14.6 \text{ mm}$ , estos parámetros corresponden a las características del modulador LCR 2500 con el que se implementaría experimentalmente este procesador. La figura 2.13 es un ejemplo de los resultados obtenidos usando el método de encriptación descrito anteriormente, para una imagen de entrada binaria.



**Figura 2.13:** Resultados del proceso de encriptación-desencriptación.

### 2.2.2.2 Análisis de la calidad de la imagen descifrada:

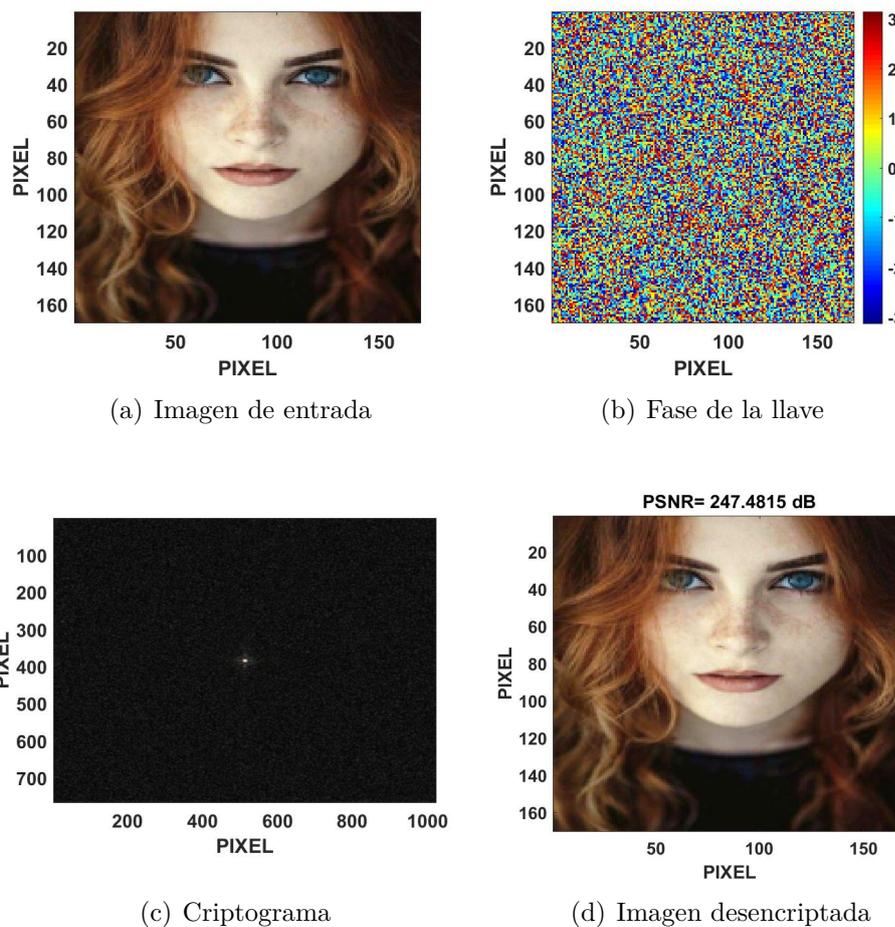
La calidad de la imagen descifrada se midió mediante el cálculo de la relación señal-ruido PSNR (Peak Signal Noise Ratio), dada por la expresión:

$$PSNR = 10 \text{Log}_{10} \left( \frac{[\max\{h(x,y)\}]^2}{MSE} \right) \quad (2.25)$$

$$MSE = \frac{1}{MN} \sum \sum [h(x,y) - h_d(x,y)]^2, \quad (2.26)$$

Donde MSE (Mean Square Error) es el error cuadrático medio,  $\max\{g(x,y)\}$  es el valor máximo en la imagen a cifrar,  $h_d(x,y)$  es la imagen descifrada, N es número de filas y M el de columnas de  $h_d(x,y)$ .

El valor del PSNR aumenta a medida que la semejanza entre la imagen descifrada y la imagen original aumenta, pudimos establecer que por debajo de 15 dB el ruido genera cambios significativos en la imagen y por debajo de 10 dB no es posible identificarla. Para el resultado de la Figura 2.13, la imagen descifrada tiene una relación PSNR=300.6937 dB, lo que representa una gran similitud con la imagen de entrada, siendo el ruido imperceptible al observador.

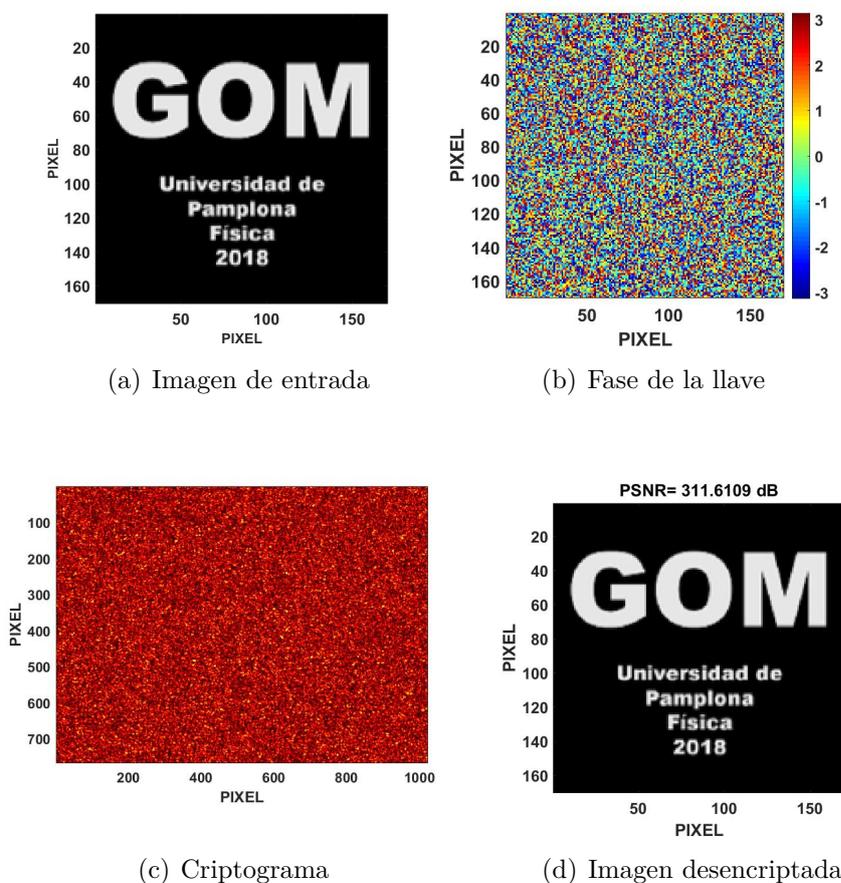


**Figura 2.14:** Resultado de la encriptación usando una llave de fase aleatoria.

Probamos la encriptación usando más imágenes complejas y en formato RGB, un resultado de esto se presenta en la Figura 2.14. El comportamiento para este caso es similar al observado anteriormente, el valor del PSNR es indicador de un buen descifrado. Los distintos resultados obtenidos para el cifrado usando una sola llave arrojaron resultados similares obteniendo criptogramas con un aspecto que guarda gran similitud al espectro de la imagen de entrada, razón para considerar otras alternativas a la encriptación que proporcionen resultados con mayor nivel de seguridad. En el siguiente aparte se describe la encriptación con doble máscara de fase aleatoria que corresponde a una alternativa más segura y fiable en el cifrado de imágenes.

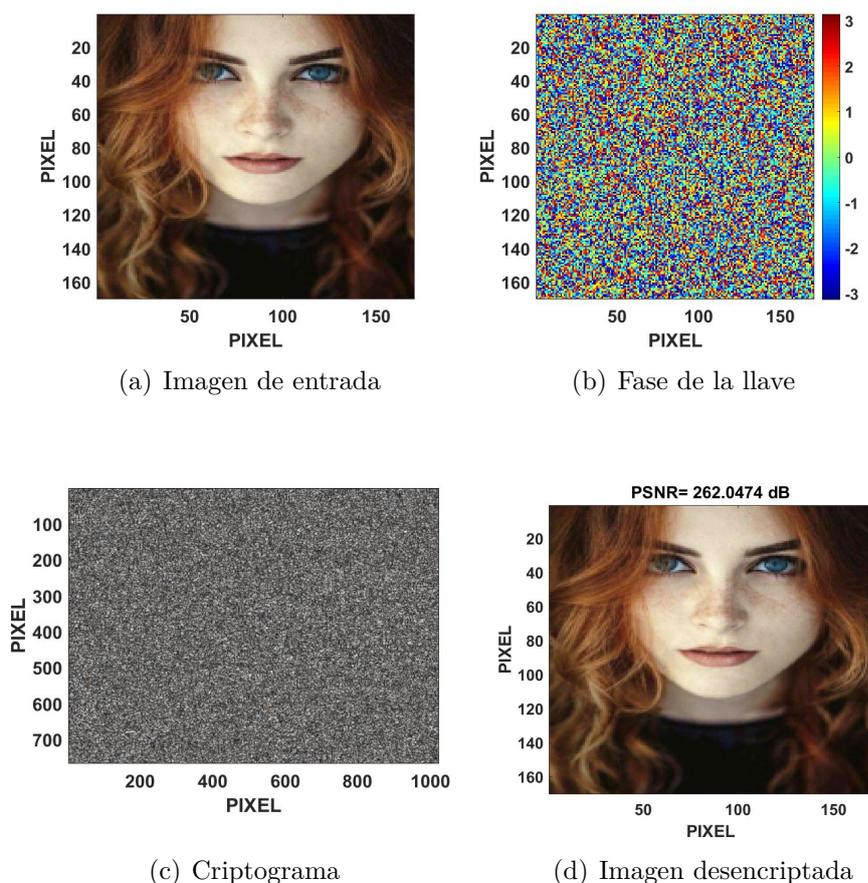
### 2.2.3 ENCRIPCIÓN USANDO DOBLE MÁSCARA DE FASE ALEATORIA (DRPE)

La encriptación usando doble máscara de fase aleatoria es la técnica de uso generalizado en la encriptación de imágenes por el alto nivel de seguridad que otorga en el cifrado. El proceso de encriptación usando doble máscara de fase aleatoria (DRPE) es similar a lo descrito en la sección anterior, con la diferencia de que la imagen a cifrar es multiplicada en el plano de entrada por una máscara de fase  $Mf = \exp(i\alpha(x,y))$ , donde  $\alpha(x,y)$  es una distribución de valores aleatorios entre  $[-\pi, \pi]$ . Al momento de descifrar, en el plano de salida obtenemos la imagen multiplicada por la máscara, que al ser de solo fase se elimina tomando el valor absoluto de la información descifrada. Las máscaras y llaves de encriptación utilizadas presentan distribuciones de fase como las presentadas en la figura 2.11.



**Figura 2.15:** Resultados de la encriptación usando DRPE.

La figura 2.15 es un ejemplo de los resultados obtenidos usando este método; el valor del PSNR obtenido para este caso es de 311 dB indicador de una imagen recuperada con una buena calidad, mejorando los resultados obtenidos usando una sola llave. Por otra parte, cifrar la información como ruido que oculta por completo la imagen o su espectro, aumenta el nivel de seguridad considerablemente en comparación a la encriptación usando solo una llave de fase.



**Figura 2.16:** Resultados de la encriptación usando DRPE

La figura 2.16 representa otro resultado usando DRPE. El valor del PSNR es de 262 dB indicador de un buen descifrado. Los distintos resultados obtenidos usando DRPE dan muestra de que todos los criptogramas conservan la misma apariencia de ruido sin cambios aparentes entre una y otra imagen cifrada, este método proporciona un buen nivel de seguridad y una calidad óptima en el descifrado de las imágenes. Sin embargo, el criptograma sigue teniendo la forma convencional de los criptogramas clásicos.

# Capítulo 3

## IMPLEMENTACIÓN DE UN PROCESADOR ÓPTICO-VIRTUAL DE ENCRIPCIÓN USANDO LLAVES DE AMPLITUD PERIÓDICA Y FASE EN ARMÓNICOS CIRCULARES

---

---

Esta parte del trabajo se enfocó hacia la implementación de un método de encriptación que permitiera la transformación del formato del criptograma, para ello abordamos la encriptación usando llaves con una componente de amplitud periódica y fase en componentes armónicas circulares. En este capítulo se presenta la descripción del método implementado y los resultados obtenidos.

### 3.1 ENCRIPCIÓN USANDO LLAVES EN ARMÓNICOS CIRCULARES

La descomposición en componentes armónicas circulares (CHC: Circular Harmonics Components) ha sido utilizada en la reconstrucción de imágenes y en el reconocimiento de patrones [45], con el fin de solucionar la varianza a la rotación que se presenta en los productos de correlación y convolución. En la encriptación óptica la descomposición en armónicos circulares se realiza sobre una distribución de fase aleatoria en coordenadas cartesianas, la fase de esta descomposición es usada como llave de cifrado [17].

### 3.1.1 DESCOMPOSICIÓN EN COMPONENTES ARMÓNICAS CIRCULARES

Las componentes armónicas circulares reposan en el hecho de que una función expresada en coordenadas polares es periódica en la variable  $\theta$ , con periodo  $2\pi$ , como consecuencia es posible expresar una función  $f(x, y)$  en CHC mediante una serie de Fourier [40], como sigue:

$$f_{CHC}(r, \theta) = \sum_{m=-\infty}^m f_m(r) e^{im\theta} \quad (3.1)$$

donde los coeficientes de Fourier  $f_m$ , están dados por la expresión:

$$f_m = \frac{1}{2\pi} \int_0^{2\pi} f(r, \theta) e^{-im\theta} d\theta \quad (3.2)$$

En la ecuación (3.2),  $r$  es la componente radial,  $\theta$  es la componente angular de la función  $f$  en coordenadas polares y  $m$  es el orden de la descomposición en armónicos circulares.

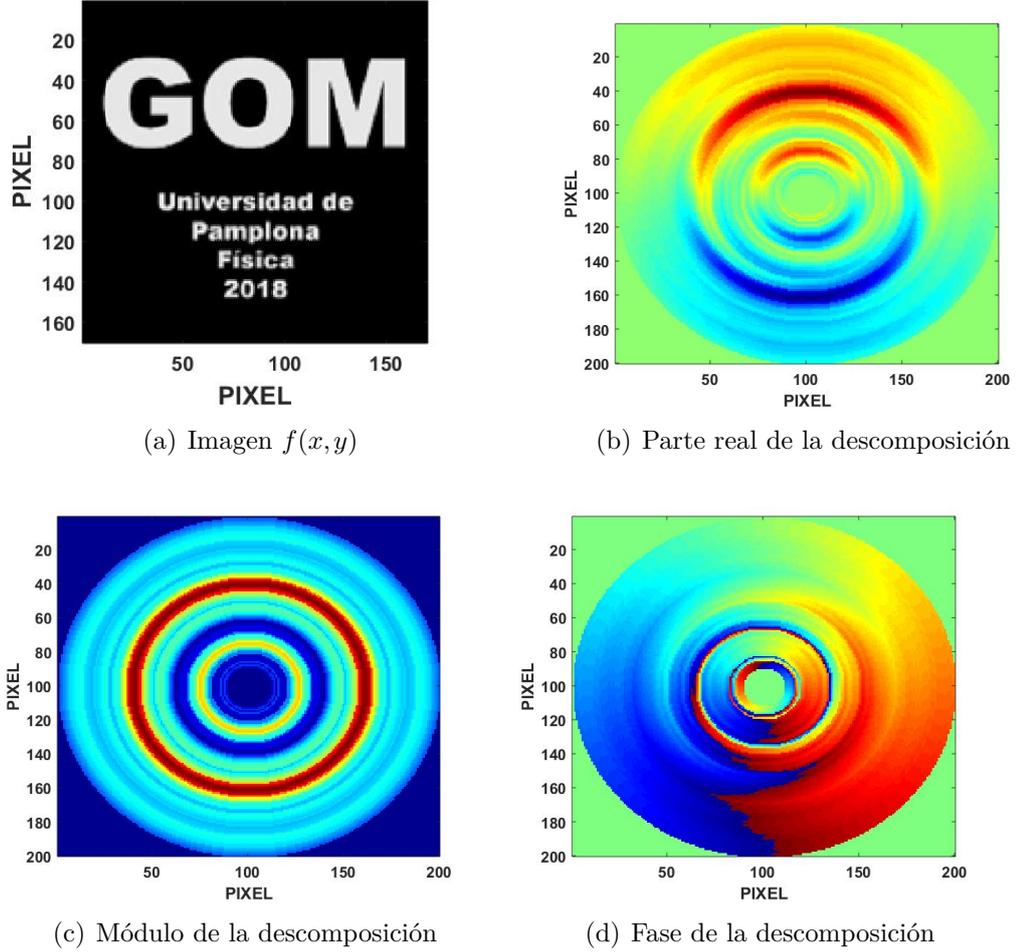
El algoritmo utilizado fue adaptado de uno utilizado para el diseño de filtros en el reconocimiento de patrones, propuesto por los autores de la referencia [45]. Una explicación más detallada del funcionamiento del algoritmo utilizado puede encontrarse en la referencia [2].

El cálculo de la descomposición en CHC, parte de transformar la imagen  $f(x, y)$  a coordenadas polares  $f(r, \theta)$ ; una vez expresada la imagen en coordenadas polares, se calculan los coeficientes  $f_m(r)$  en forma discreta, descritos por la expresión:

$$f_m(r) = \frac{1}{n} \sum_{k=1}^n f\left(\frac{2\pi k}{n}\right) \exp\left(-im \frac{2\pi k}{n}\right) \quad (3.3)$$

donde  $n$  es el número de muestras entre  $[0, 2\pi]$ . Con los coeficientes  $f_m(r)$  se puede obtener la matriz final  $f_{CHC}$ .

Los resultados de la figura 3.1 corresponden a la parte real, la fase y la amplitud de la descomposición aplicando el algoritmo de descomposición en CHC.



**Figura 3.1:** Descomposición en armónicos circulares (Orden  $m = 1$ )

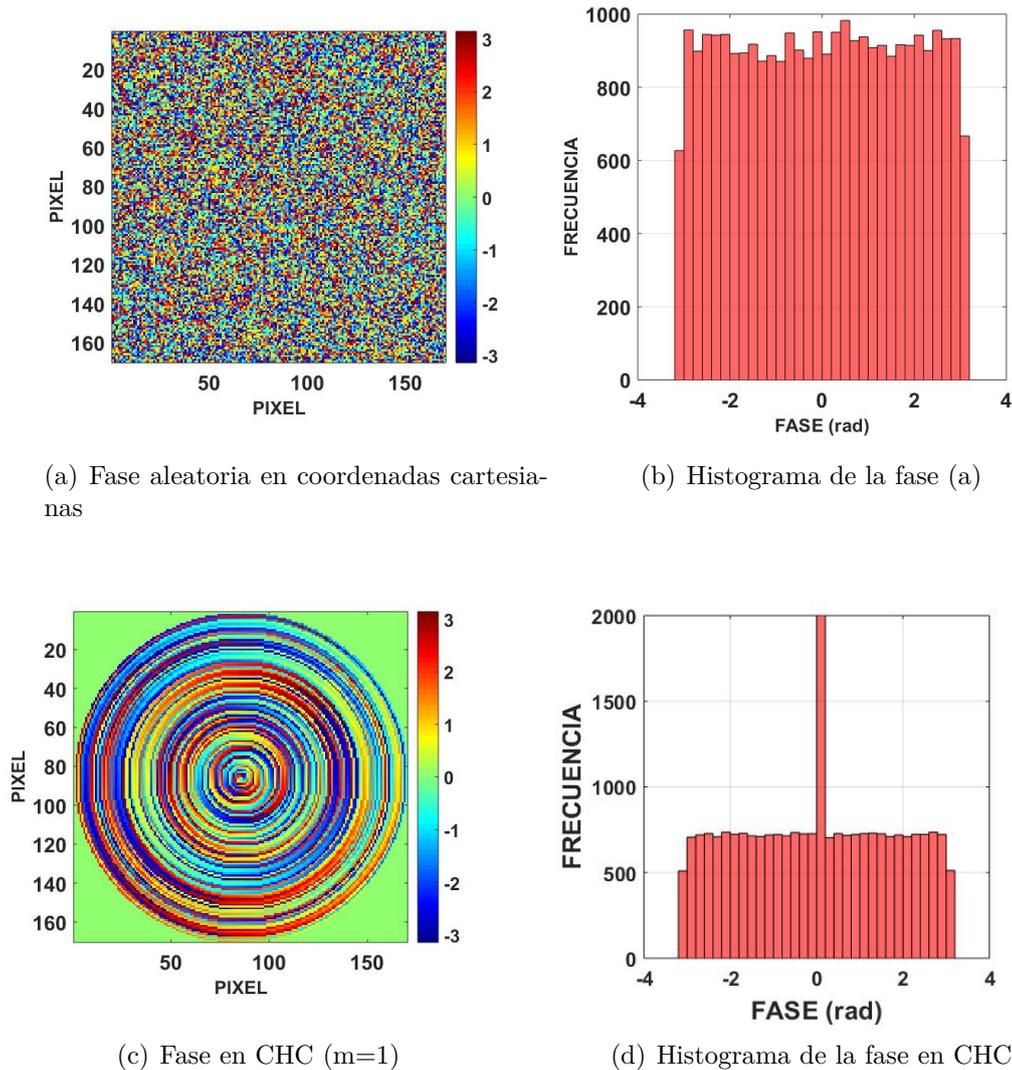
### 3.1.2 LLAVES DE FASE EN CHC

La generación de las llaves de encriptación inicia con la descomposición en componentes armónicas circulares de una distribución de fase aleatoria  $\phi(x,y)$  definida en coordenadas cartesianas, aplicando las ecuaciones (3.1) y (3.2). Como resultado de la descomposición se obtiene una expresión compleja que puede reescribirse de la siguiente forma:

$$\phi_{CHC}(r,\theta) = |\phi_{CHC}(r,\theta)| e^{i\psi(r,\theta)} \quad (3.4)$$

Donde  $\psi(r, \theta)$  es la fase en armónicos circulares. La nueva llave de encriptación se obtendrá dividiendo la ecuación (3.4) en su módulo, así:

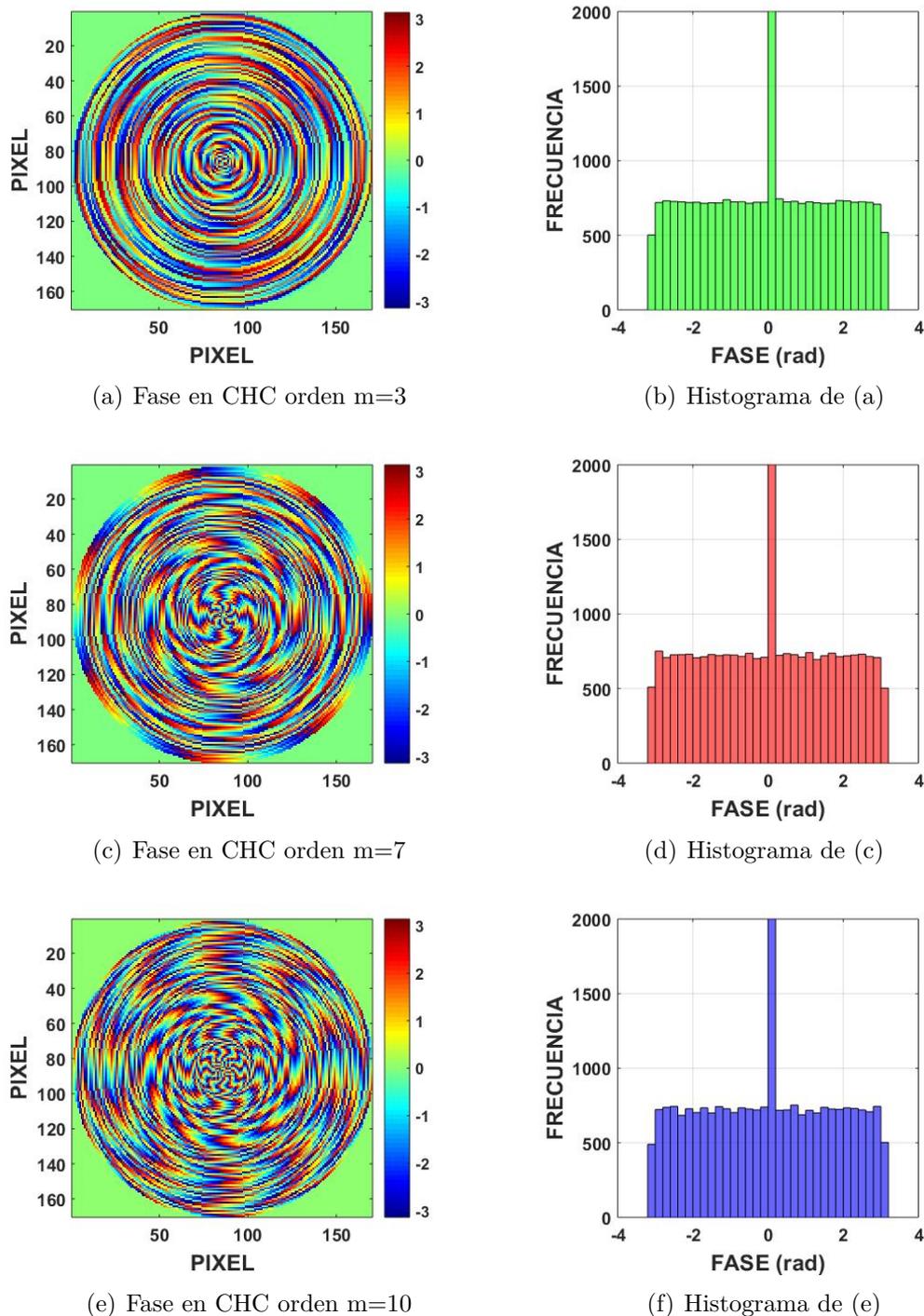
$$K_{CHC}(r, \theta) = e^{i\psi(r, \theta)} \quad (3.5)$$



**Figura 3.2:** Fase e histogramas de las llaves  $K(x, y)$  y  $K_{CHC}(r, \theta)$

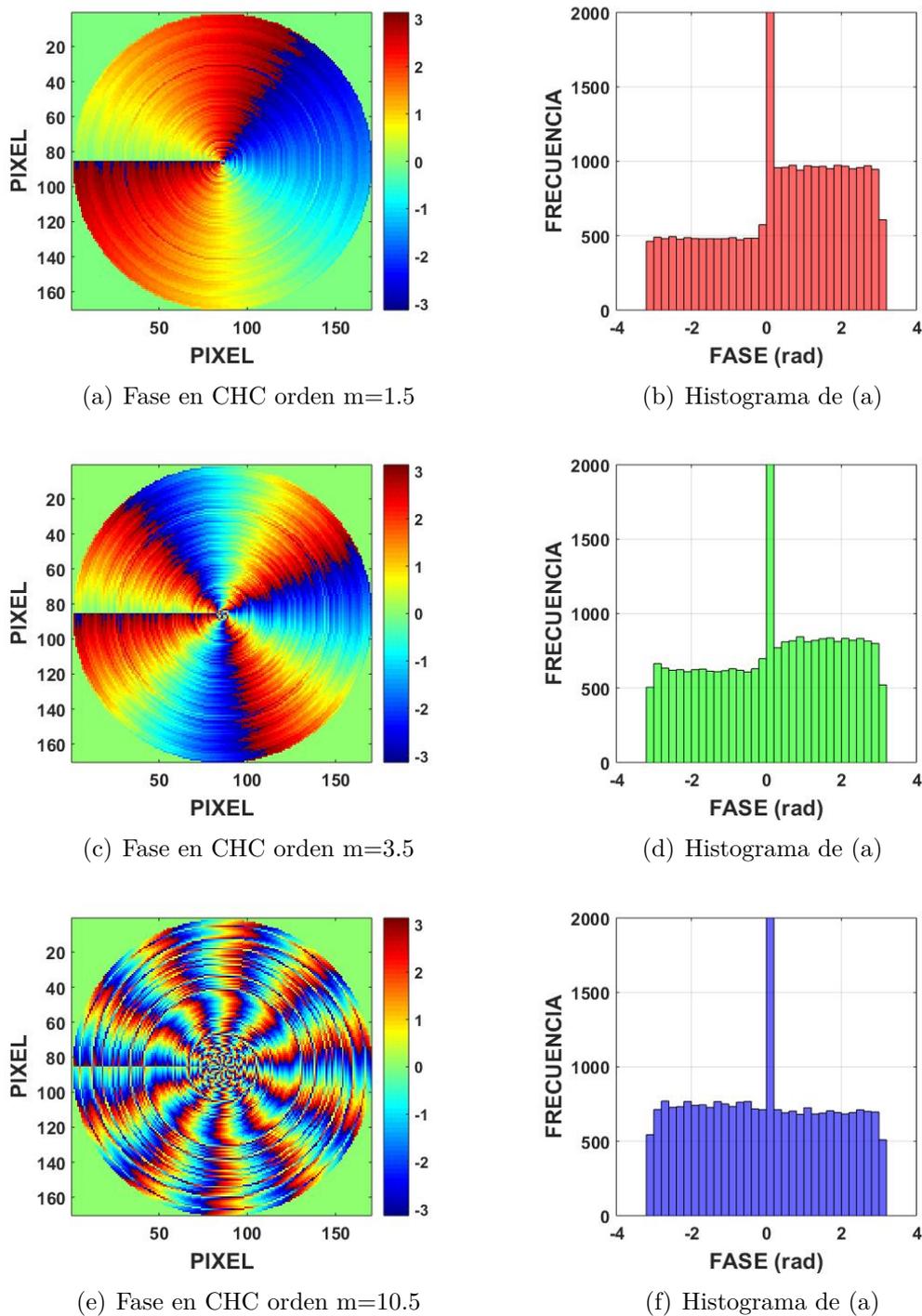
Los resultados de la figura 3.2 son distribuciones de fase aleatoria en coordenadas cartesianas y su respectiva fase calculada en armónicos circulares. Ambos histogramas presentan una distribución de fase cuasi-uniformes, indicador de que las dos distribuciones de fase permiten encriptar con un buen nivel de seguridad.

Se calcularon llaves en CHC usando diferentes órdenes de descomposición armónica, las figuras 3.3 muestran que para otros órdenes enteros de descomposición las llaves también presentan distribuciones de fase cuasi-uniformes.



**Figura 3.3:** Fase e histogramas de las llaves  $K_{CHC}(r, \theta)$  con distintos órdenes de descomposición

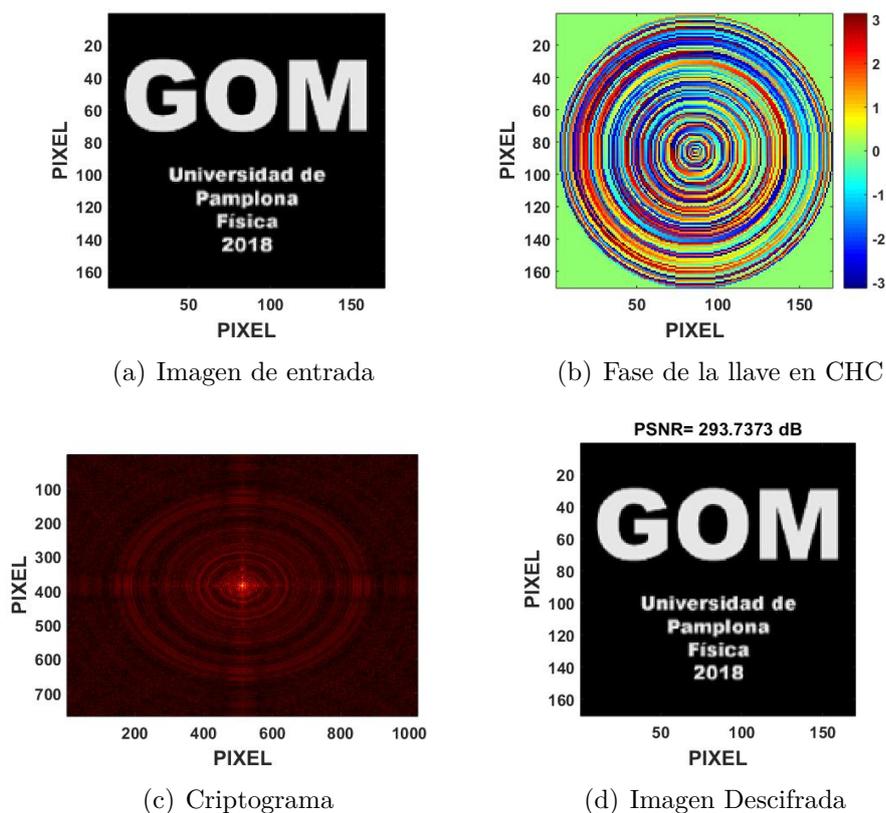
También consideramos los órdenes fraccionales, en este caso algunas de las llaves presentan distribuciones no uniformes, lo que en principio sería indicador de no proporcionar un buen nivel de cifrado.



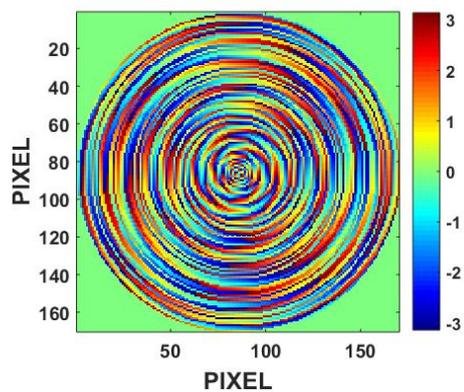
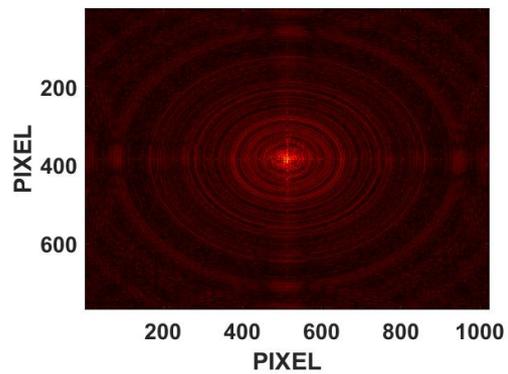
**Figura 3.4:** Fase e histogramas de las llaves  $K_{CHC}(r, \theta)$  con órdenes de descomposición fraccional

### 3.1.3 ENCRIPCIÓN USANDO UNA LLAVE EN ARMÓNICOS CIRCULARES

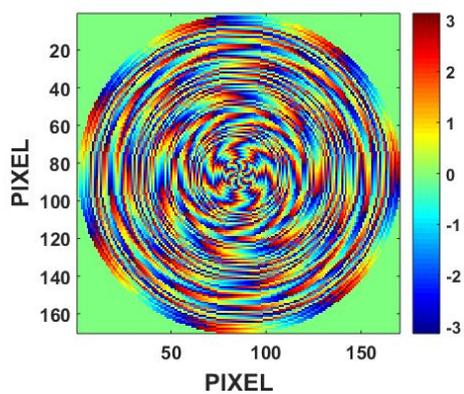
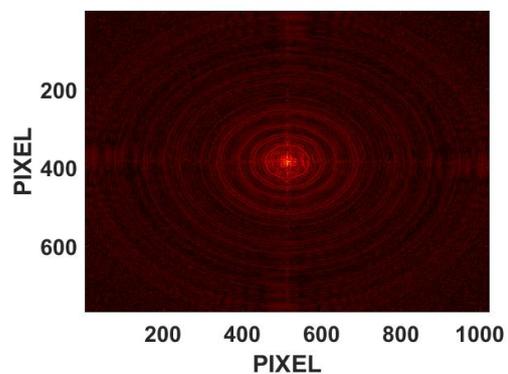
Las llaves en armónicos circulares proporcionan una alternativa a las llaves de encriptación convencionales, con la ventaja de que la función de fase a descomponer y el orden de la descomposición constituyen parámetros de seguridad en la encriptación. El proceso de encriptación con llaves en armónicos circulares corresponde a lo descrito en el capítulo anterior, en las figuras 3.5 y 3.6 se presentan los resultados de su implementación. El uso de llaves en armónicos circulares cambia el aspecto de los criptogramas, los cuales toman una apariencia simétrica, a diferencia de las llaves de ruido blanco, sin embargo los criptogramas obtenidos no presentan diferencias significativas en su apariencia ante cambios del orden de la descomposición o de la imagen a cifrar.



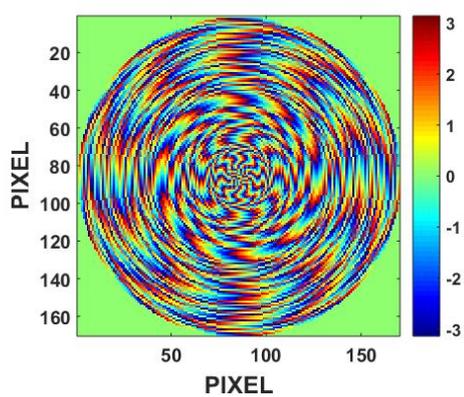
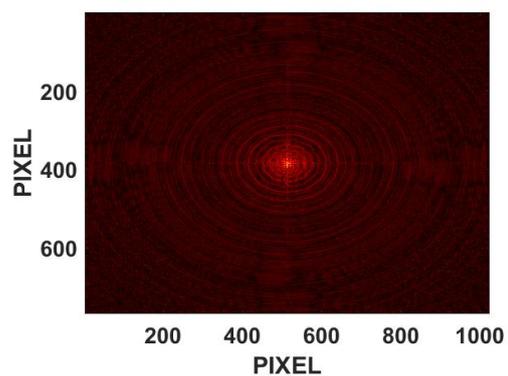
**Figura 3.5:** Resultados de la encriptación usando llaves en CHC

(a) Fase de la llave en CHC  $m=3$ 

(b) Criptograma

(c) Fase de la llave en CHC  $m=7$ 

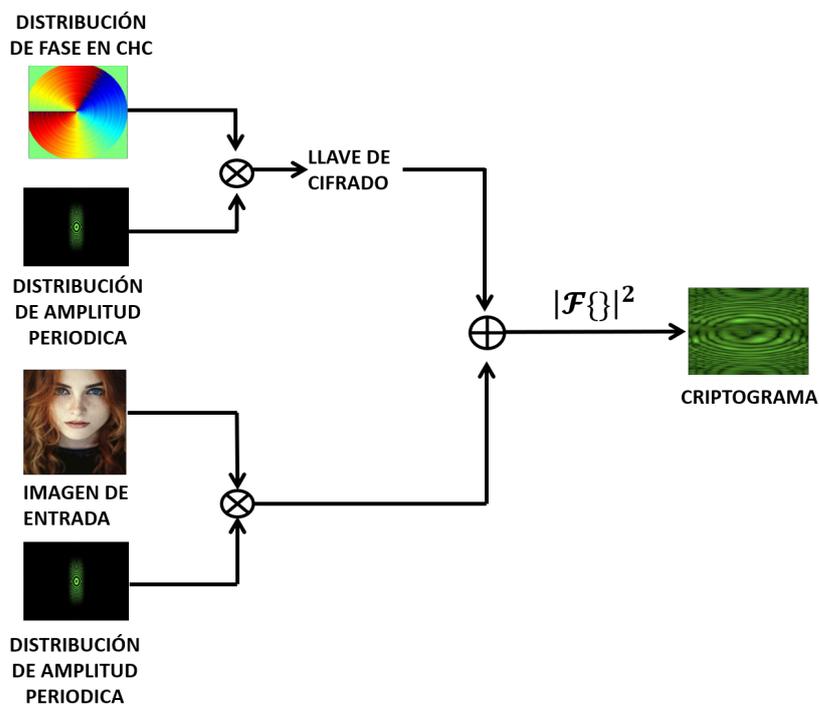
(d) Criptograma

(e) Fase de la llave en CHC  $m=10$ 

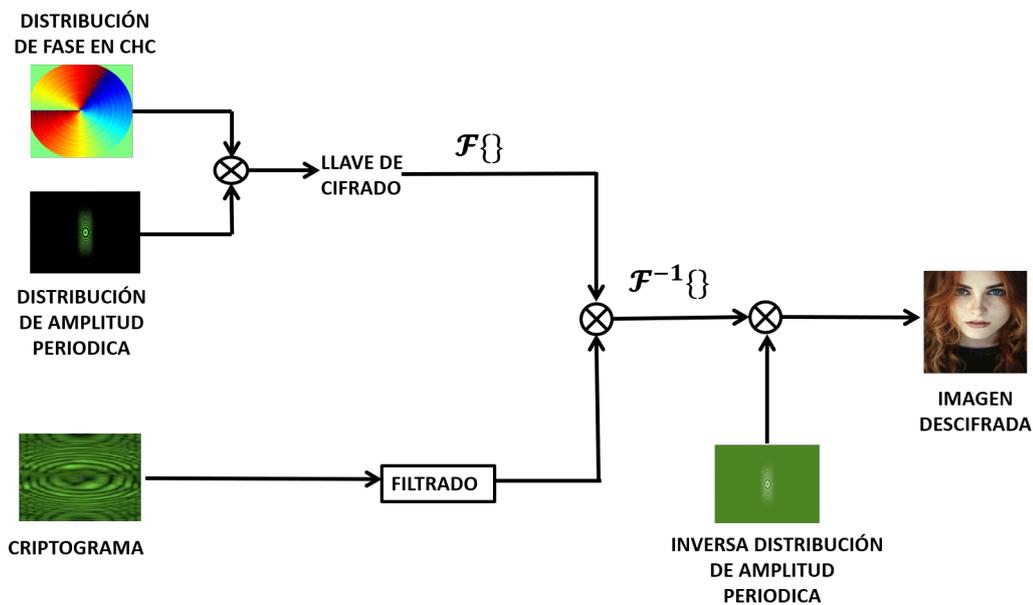
(f) Criptograma

**Figura 3.6:** Resultados de la encriptación usando llaves en CHC

### 3.2 ENCRIPCIÓN USANDO UNA LLAVE DE AMPLITUD PERIÓDICA Y FASE EN ARMÓNICOS CIRCULARES



(a) Diagrama proceso de cifrado



(b) Diagrama proceso de descifrado

**Figura 3.7:** Diagrama del método de encriptación.  $\mathcal{F}$  representa la transformada de Fourier,  $\otimes$  representa multiplicación aritmética

El método implementado usa llaves con una componente de fase en componentes armónicas circulares y una distribución de amplitud periódica de la forma  $\kappa_m(ax^p, by^q)$ , la distribución de amplitud periódica también es usada como máscara que multiplica la imagen de entrada. El diagrama de flujo del método se presenta en la figura 3.7.

La descripción físico-matemática corresponde a un procedimiento análogo a lo descrito en el capítulo anterior, razón por la que no se detalla a totalidad el proceso, sin embargo es necesario redefinir la transmitancia del plano de entrada:

$$f(x, y) = h(x + a, y) \kappa_m(x + a, y) + \kappa(x - a, y) \quad (3.6)$$

siendo,

$$\kappa(x - a, y) = \kappa_m(x - a, y) \kappa_{ch}(x - a, y) \quad (3.7)$$

$\kappa_m(x, y)$  es el término de amplitud, de distribución periódica, y  $\kappa_{ch}(x, y)$  es el término de fase, cuyos valores se obtienen descomponiendo en armónicos circulares una distribución de ruido blanco.

Por lo tanto el criptograma  $I(f_x, f_y) = |F(f_x, f_y)|^2$ , toma la forma:

$$\begin{aligned} I(f_x, f_y) &= \frac{1}{(\lambda f)^2} \left[ |G(f_x, f_y)|^2 + |K(f_x, f_y)|^2 \right. \\ &\quad + G^*(f_x, f_y) K(f_x, f_y) \exp(-i4\pi a f_x) \\ &\quad \left. + G(f_x, f_y) K^*(f_x, f_y) \exp(i4\pi a f_x) \right] \end{aligned} \quad (3.8)$$

Con,

$$f_x = \frac{x_0}{\lambda f}, \quad f_y = \frac{y_0}{\lambda f} \quad (3.9)$$

$$K(f_x, f_y) = K_m(f_x, f_y) * K_{ch}(f_x, f_y) \quad (3.10)$$

$$G(f_x, f_y) = H(f_x, f_y) * K_m(f_x, f_y) \quad (3.11)$$

El operador  $*$  denota convolución. Los procesos de filtrado aplicados corresponden a lo ya descrito, el proceso de descifrado requiere la totalidad de la amplitud compleja de la llave, así en el plano de salida  $(x', y')$ , se obtiene la convolución entre la llave y la transformada del criptograma filtrado  $I_{ff}(f_x, f_y)$ .

$$\begin{aligned} D(x', y') &= \mathcal{F}^{-1} \{ I_{ff}(f_x, f_y) K(f_x, f_y) \} \\ &\approx h(x', y') \kappa_m(x', y') \end{aligned} \quad (3.12)$$

Este resultado se debe dividir entre la máscara  $\kappa_m$ , solo así, finalmente se obtiene la imagen descriptada.

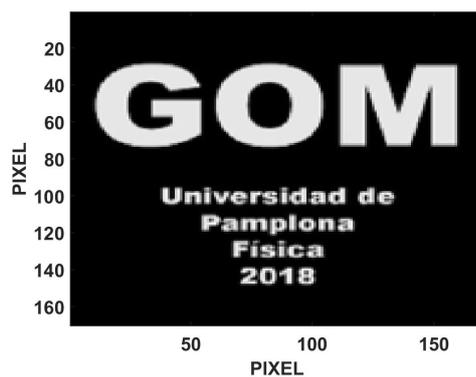
El sistema óptico de encriptación implementado cuenta con 4 parámetros de ajuste en la amplitud y 2 parámetros de ajuste en la fase (la función a descomponer y el orden de la descomposición). Para la generación de la fase de la llave se usaron tanto órdenes fraccionales como enteros, encontrado que en los dos casos es posible cifrar la información con un buen nivel de seguridad. La combinación de los términos de fase y amplitud permiten que el aspecto de los criptogramas pueda ser modificado haciendo una elección adecuada de los parámetros de la llave. En los resultados presentados se muestran las distribuciones de amplitud y fase utilizadas en la encriptación de las imágenes.

Los resultados de la figura 3.8 y 3.9, corresponden a la encriptación de la misma imagen con diferentes parámetros de la llave. Los cambios en las componentes de fase y amplitud generan criptogramas totalmente distintos, como se observa en los resultados. La calidad de las imágenes recuperadas es óptima si se conoce la distribución de amplitud con exactitud, esto se midió mediante la relación señal ruido PSNR, obteniendo resultados para el PSNR mayores a 150 dB. Aunque en principio es fácil ver que los criptogramas no dan idea de la imagen que fue

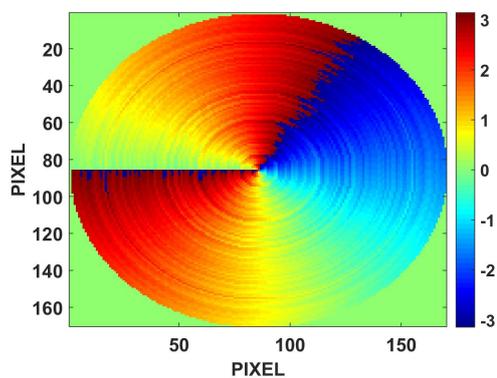
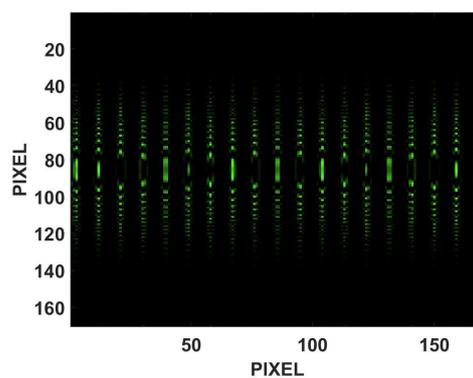
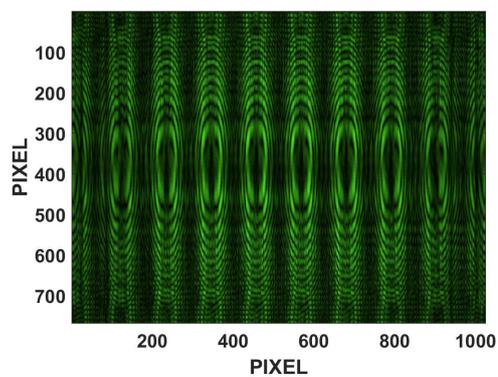
cifrada, las distintas verificaciones realizadas, por ejemplo, usando la transformada inversa o el descifrado sin la totalidad de la llave, dejaron ver que es difícil vulnerar la encriptación. El aspecto de los criptogramas generados está relacionado con las convoluciones que se presentan en la encriptación, estas convoluciones hacen imposible recuperar la imagen si no se conoce la llave de cifrado. Además, el método permite camuflar la información cifrada en un formato de imagen determinística, diferente para cada imagen de entrada, siendo este un parámetro de seguridad adicional de carácter subjetivo, este formato no da idea de la llave o de la imagen cifrada.

El descifrado de la imagen requiere conocer todos los parámetros de la llave por lo que el sistema implementado representa una alternativa bastante segura en el cifrado de imágenes. La técnica implementada no es tolerante a variaciones en los parámetros de cifrado por lo que es imposible recuperar la información ante ruido o pérdida de valores de la llave.

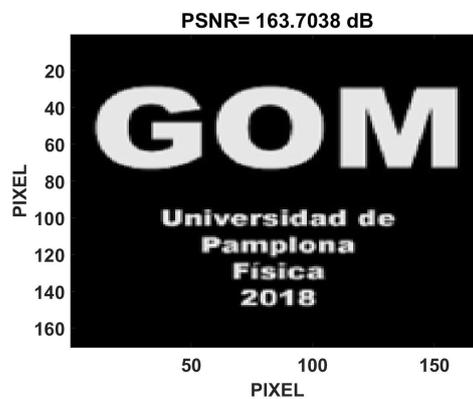
Las figuras 3.10, 3.11, 3.12, son otros resultados del método usando imágenes más complejas, para este caso los criptogramas también presentan cambios significativos en su aspecto determinados por el cambio de los parámetros de cifrado. En el caso de la imagen descifrada el PSNR proporciona valores alrededor de 150 dB indicador de un buen descifrado. Los distintos resultados dan muestra de varianza a los parámetros de cifrado pero pocos cambios entre uno y otro criptograma ante el cambio de imágenes a cifrar.



(a) Imagen a cifrar

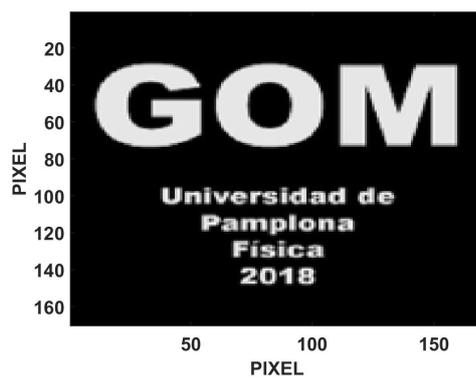
(b) Fase de la llave  $\kappa_{CH}$   $m=1.5$ (c) Máscara  $a=7$ ,  $b=1$ ,  $p=2$ ,  $q=2$ 

(d) Criptograma

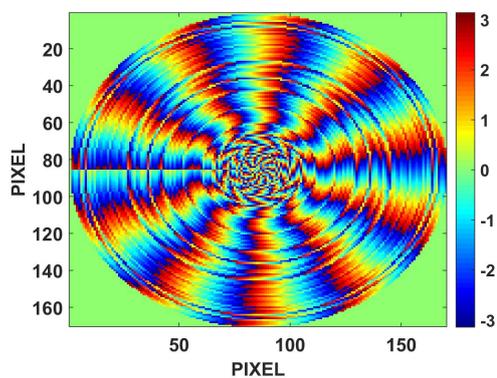
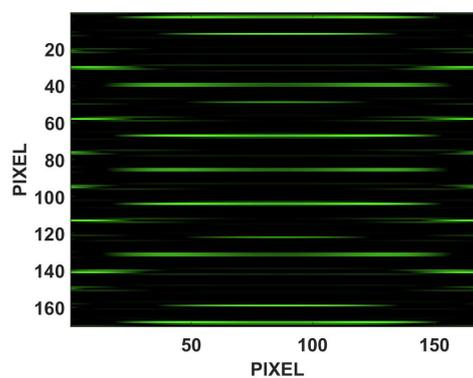
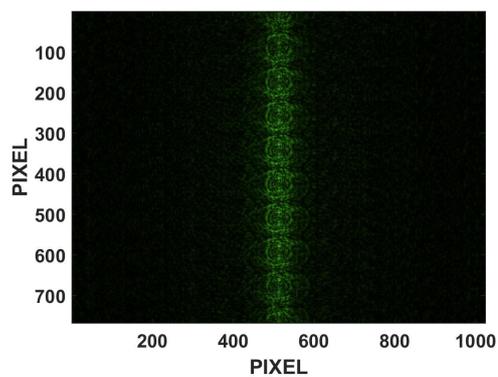


(e) Imagen descifrada

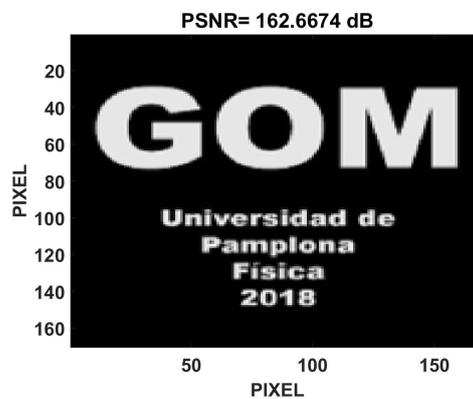
**Figura 3.8:** Resultados de la encriptación con llaves de amplitud periódica y fase en armónicos circulares



(a) Imagen a cifrar

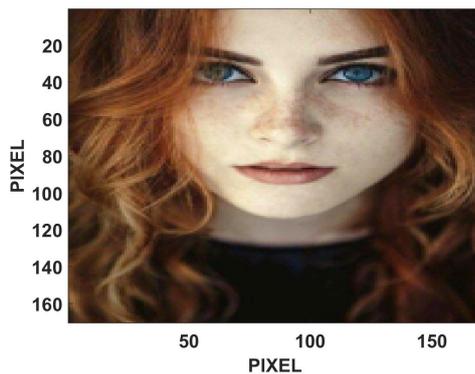
(b) Fase de la llave  $\kappa_{CH}$   $m=10.5$ (c) Máscara  $a=0.1$ ,  $b=7$ ,  $p=2$ ,  $q=2$ 

(d) Criptograma

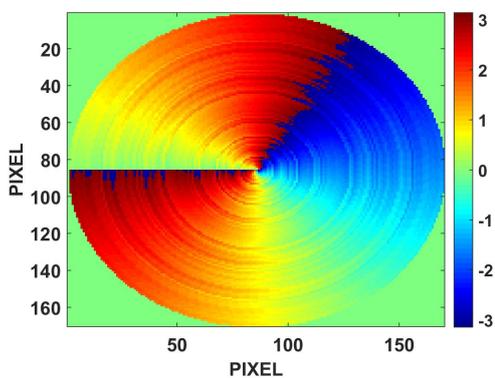
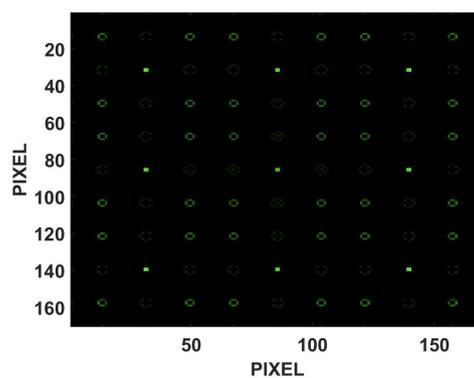
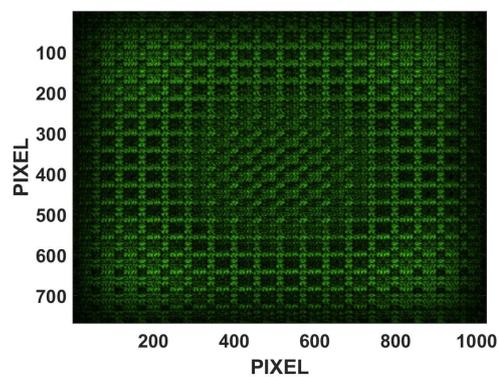


(e) Imagen descifrada

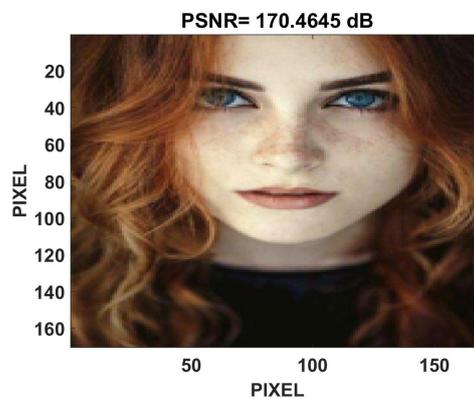
**Figura 3.9:** Resultados de la encriptación con llaves de amplitud periódica y fase en armónicos circulares



(a) Imagen a cifrar

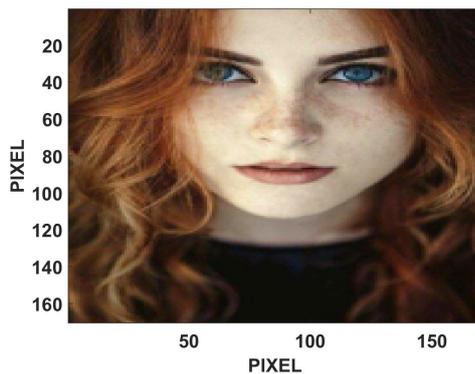
(b) Fase de la llave  $\kappa_{CH}$   $m=1.5$ (c) Máscara  $a=5$ ,  $b=5$ ,  $p=2$ ,  $q=2$ 

(d) Criptograma

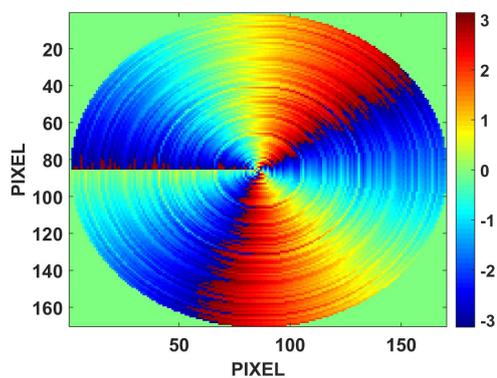
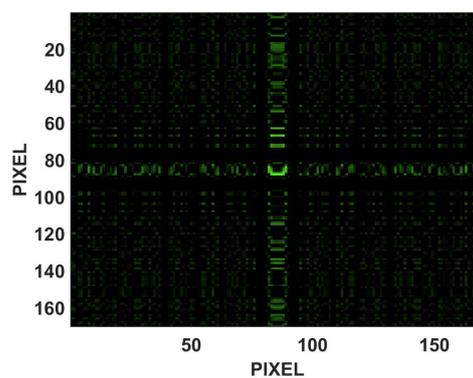
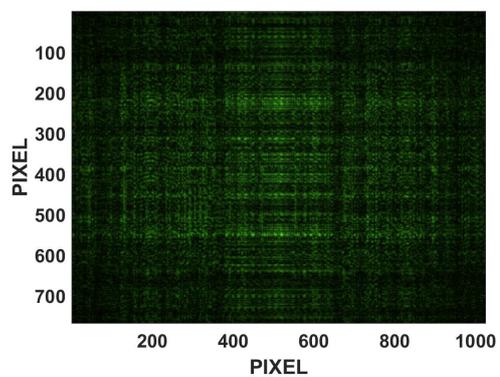


(e) Imagen descifrada

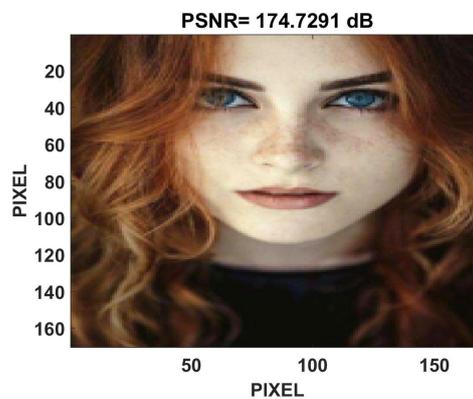
**Figura 3.10:** Resultados de la encriptación con llaves de amplitud periódica y fase en armónicos circulares



(a) Imagen a cifrar

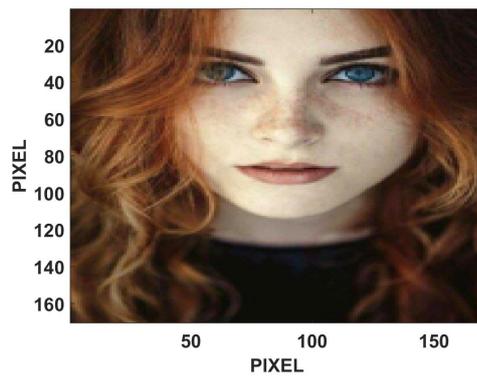
(b) Fase de la llave  $\kappa_{CH}$   $m=2.5$ (c) Máscara  $a=7$ ,  $b=7$ ,  $p=4$ ,  $q=2$ 

(d) Criptograma

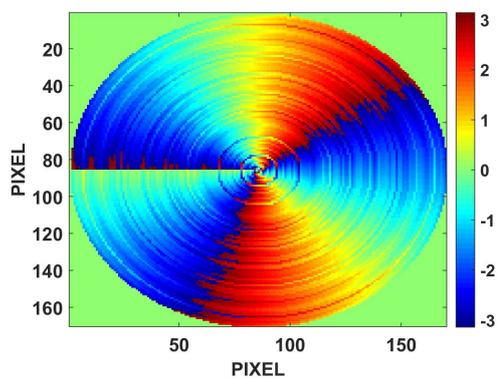
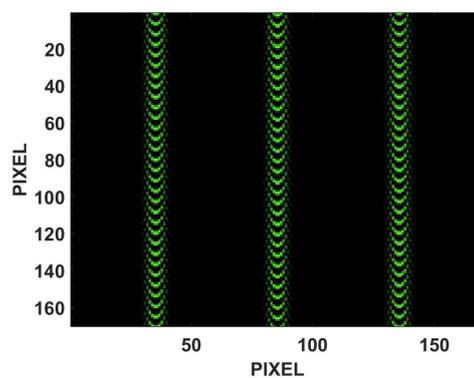
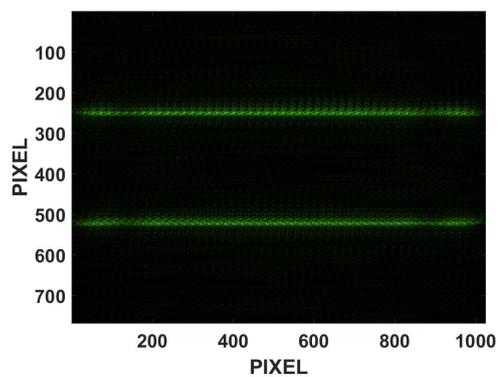


(e) Imagen descifrada

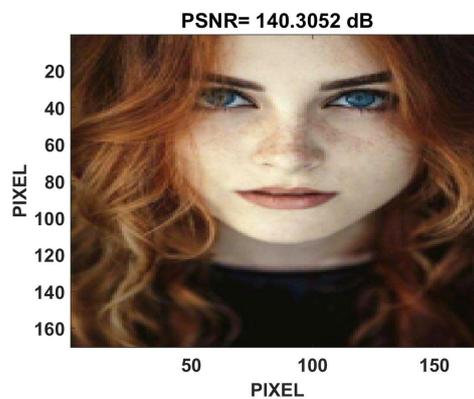
**Figura 3.11:** Resultados de la encriptación con llaves de amplitud periódica y fase en armónicos circulares



(a) Imagen a cifrar

(b) Fase de la llave  $\kappa_{CH}$   $m=2.5$ (c) Máscara  $a=3$ ,  $b=5$ ,  $p=2$ ,  $q=1$ 

(d) Criptograma



(e) Imagen descifrada

**Figura 3.12:** Resultados de la encriptación con llaves de amplitud periódica y fase en armónicos circulares

# Capítulo 4

## DISEÑO DE UN SISTEMA DE ENCRIPCIÓN DE TRANSFORMADA CONJUNTA ÓPTICO-DIGITAL

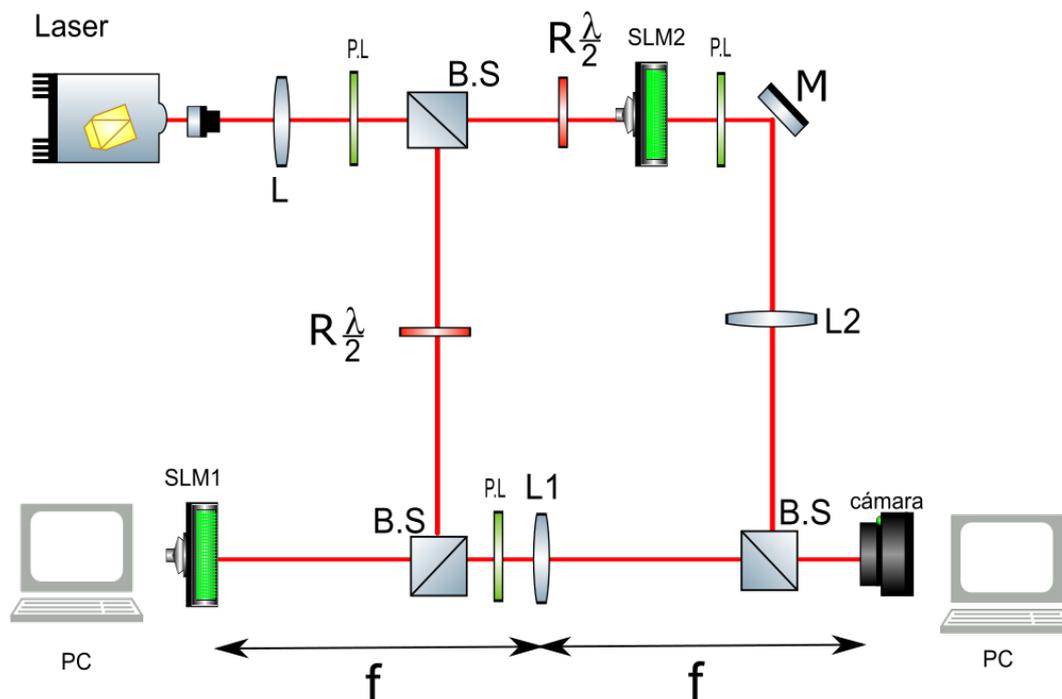
---

---

### 4.1 SISTEMA DE ENCRIPCIÓN DE TRANSFORMADA CONJUNTA ÓPTICO-DIGITAL

Los resultados obtenidos en la implementación del procesador óptico-virtual motivaron la implementación experimental del sistema de cifrado-descifrado. Para ello proponemos el diseño de un procesador de encriptación óptico-digital haciendo uso de moduladores espaciales de cristal líquido. Las limitaciones de tiempo no permitieron abarcar la totalidad de la implementación experimental, que está más allá de los objetivos propuestos, sin embargo, se dejan planteadas la bases que permitan implementar el sistema de encriptación en un trabajo futuro.

Proponemos un sistema óptico-digital para la encriptación de imágenes; los sistemas híbridos resultan herramientas versátiles al aprovechar las ventajas del procesamiento óptico y los canales de transmisión digitales [3]. El sistema propuesto se compone de dos etapas, la etapa de cifrado se realiza experimentalmente haciendo uso de moduladores espaciales de cristal líquido en una arquitectura de transformada conjunta.



**Figura 4.1:** Esquema experimental Sistema de Encriptación JT Óptico-Digital. SLM representa el modulador de cristal líquido,  $R\lambda/2$  representa un retardador de media onda, BS: cubos divisores, M: Espejo, P.L: Polarizador Lineal, L: Lente positiva con focal  $f$ .

Un posible esquema experimental se muestra en la figura 4.1. En el esquema el modulador de cristal líquido SLM1 es un modulador que funciona por reflexión, en este se sintetiza la llave de encriptación. El modulador SLM2 corresponde a un modulador de cristal líquido que funciona por transferencia, en este se sintetiza la imagen multiplicada por la máscara de cifrado. El sistema de polarizadores lineales y retardadores de media onda permite orientar la polarización para elegir la modulación en fase o intensidad requerida. La fuente de iluminación del sistema corresponderá a un frente de onda plano, con la longitud de onda para la que fue caracterizada la respuesta del modulador SLM1. El esquema experimental corresponde a un interferómetro tipo Mach-Zehnder, en cada brazo se construye un arreglo  $2f$  entre el respectivo modulador y la cámara. El patrón de interferencia entre las transformadas producidas por las lentes L1 y L2 se registra en la cámara y corresponderá al criptograma. El esquema sugerido tiene la ventaja de permitir el ajuste del ángulo de incidencia entre los dos haces, lo que posibilita el control de la modulación de la transformada conjunta.

Una vez registrado el criptograma la siguiente etapa corresponde al descifrado, esto incluye el proceso de filtrado. El descifrado se realizará digitalmente, para ello es necesario simular la propagación del campo óptico en el arreglo experimental que permita ajustar correctamente la escala del problema físico, al realizar el proceso de forma digital. El criptograma procesado digitalmente se multiplica por la transformada de la llave de cifrado y se realiza su transformada inversa; a la salida debemos recupera la imagen de entrada, siguiendo la misma lógica de la descripción físico-matemática realizada en los capítulos anteriores. Las simulaciones realizadas en este trabajo fueron ajustadas a las condiciones experimentales bajo las que se propone implementar el sistema de encriptación, esto es, simulamos las condiciones de propagación del campo óptico para generar el algoritmo de encriptación y sintetizamos las máscaras de cifrado con los parámetros que corresponden a las dimensiones del modulador de cristal líquido.

De otra parte, la implementación experimental de un procesador de encriptación y las distintas aplicaciones de la modulación de información [46–48], requieren poder controlar la amplitud y la fase de los frentes de onda, por lo cual resulta especialmente útil representar de forma precisa la acción de estos dispositivos sobre los frentes de onda; lo anterior motivó la realización de una caracterización de la respuesta en intensidad y fase de un modulador de cristal líquido LCR 2500 con el que actualmente contamos al interior del Grupo Óptica Moderna. El uso de un modulador de cristal líquido se justifica en cuanto a su fácil manejo, el control electrónico que permite la conexión digital-óptica, la alta resolución, alta eficiencia óptica y bajo consumo energético. De esta forma las pantallas de cristal líquido resultan un dispositivo clave para la construcción de interfaces óptico-digitales, donde la información digital se transfiere eléctricamente a cada celda, el valor se codifica localmente en términos de birrefringencia y la lectura de la información se hace ya sea por luz que atraviese el modulador o que se refleje en él, según su modo de operación.

## 4.2 CARACTERIZACIÓN DE UN MODULADOR DE CRISTAL LÍQUIDO DE FASE NEMÁTICA

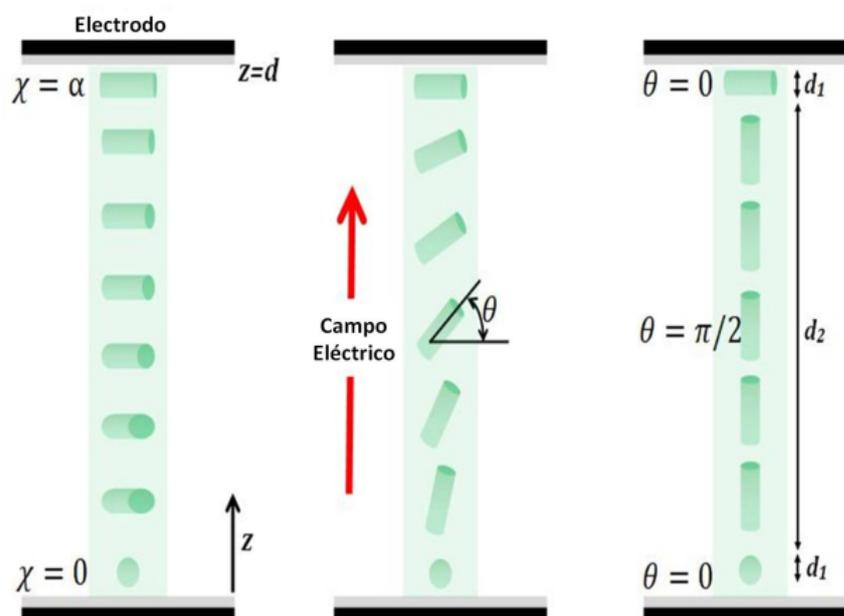
Los moduladores espaciales de luz (SLM: Spatial Light Modulator) son dispositivos que permiten cambiar las propiedades físicas de un frente de onda que incide en ellos, como la intensidad, la fase o el estado de polarización, en función de un parámetro controlado externamente [49]. Dependiendo del fenómeno físico involucrado en la modulación existen distintos tipos de SLM [50], podemos encontrar los moduladores de cristal líquido, los magneto-ópticos, los de espejos-deformables, los de pozos cuánticos, los electro-ópticos y los acusto-ópticos.

El modulador empleado para este trabajo es una pantalla de cristal líquido LCR 2500 fabricada por Holoeye, algunas de las especificaciones técnicas del modulador están contenidas en la tabla 4.1. El modulador es de la familia de las pantallas de cristal líquido nemáticas, con un twist de  $45^\circ$ , que funciona por reflexión y permite modular en intensidad, y en fase desde 0 a  $2\pi$ . Este equipo contiene una caja de comando electrónico que permite interfazar la pantalla con el computador, vía puerto DVI. El modulador es controlado desde el computador mediante software hecho en Matlab.

Descripción	
Dimensiones del área activa	19.6 mm $\times$ 14.6 mm
Proporción de la pantalla	4(H):3(V)
Resolución de la pantalla	1024(H) $\times$ 768(V) pixeles
Tamaño del pixel	19 $\mu$ m $\times$ 19 $\mu$ m
Configuración de los pixeles	Ortogonal
Niveles de gris	256 (8 bit)
Eficiencia óptica	> 75%
Tipo de cristal líquido	Nemático rotado $45^\circ$
Frecuencia de refresco	75 Hz
Iluminación	> 2 W/cm <sup>2</sup>

**Tabla 4.1:** Características del TN-LCD Holoeye LC-R 2500

Los cristales líquidos son sustancias que presentan una fase intermedia entre los estados sólido y líquido, lo que les confiere una combinación única de propiedades eléctricas y ópticas. Aunque se conocen desde hace más de un siglo, su uso es relativamente reciente en especial en el campo de la optoelectrónica, siendo pioneros los trabajos de Williams y Heilmair [51–53]. En los setenta Helfrich y Schadt hablan del efecto electro-óptico en los cristales líquidos de tipo nemático [54]. Este efecto consiste en un giro en las moléculas mediante la acción de un campo eléctrico aplicado, es decir se trata de una actividad óptica inducida en el material que permite rotar el plano de polarización [55]. El cristal líquido actúa como un material uniaxial anisótropo, de modo que se modifican las propiedades de fase y polarización de la luz incidente en función del campo aplicado. Las moléculas de los cristales líquidos nemáticos se caracterizan por ser de forma alargada y estar orientadas a un eje de simetría conocido como eje director. El eje director de las celdas de cristal líquido se orienta mediante la aplicación de un campo eléctrico, las moléculas se alinean en dirección del campo y se presenta birrefringencia que varía con el voltaje aplicado.



**Figura 4.2:** Esquema de la orientación del director del cristal líquido en un TN-LCD (a) Voltaje Nulo (b) Voltaje intermedio (c) Voltaje máximo

---

Una pantalla de cristal líquido se compone de una capa de cristal líquido nemático y un par de electrodos transparentes de trióxido de indio (ITO) evaporados sobre las caras de la celda que encierra el cristal. Los electrodos permiten aplicar potenciales eléctricos a través del cristal líquido, que ocasiona que las moléculas se alineen en dirección al campo. El eje director del cristal líquido se sitúa paralelo a la superficie del sustrato que lo limita y describe un giro en forma de hélice hasta la salida. Normalmente el ángulo de giro que describe el eje director del cristal (ángulo de twist) dentro de la celda es de  $90^\circ$ . Sin embargo, existen moduladores sin rotación del director (Que permite modulación en solo fase) y moduladores con rotación superior a  $90^\circ$ .

Cuando se crea una diferencia de potencial entre las dos capas de ITO, el campo eléctrico provoca una inclinación  $\theta$  del director del cristal líquido sobre dicha dirección (Figura 4.2). Cuando el campo eléctrico es suficiente todas las moléculas del cristal quedan orientadas en la misma dirección excepto aquellas de la superficie pues se encuentran fijas. Este ángulo  $\theta$  es el mismo para todas las moléculas y es el responsable de generar la diferencia de camino óptico, por la tanto se relaciona con la modulación en fase. De esta forma, para obtener modulación en solo fase es necesario orientar la polarización de la luz incidente paralela al eje director del modulador, así la luz que incida solo tendrá cambios de camino óptico como consecuencia del voltaje aplicado, esto se traducirá en retardos de fase proporcionales al nivel de gris aplicado.

Para la modulación en intensidad es necesario una configuración polarizador-analizador, la pantalla se utiliza entre polarizadores cruzados, esto se explica porque en ausencia de campo eléctrico la luz emergente del polarizador sigue la dirección del giro del cristal líquido y al llegar al segundo polarizador la intensidad es máxima, a medida que se aplica un potencial eléctrico en la caras del cristal la moléculas se alinean en dirección del campo eléctrico, bajo estas condiciones el eje de polarización de la luz que pasa por la pantalla ya no tendrá la misma dirección que el polarizador a la salida, como resultado habrá un cambio en la

transmitancia del sistema óptico. Una modulación en solo intensidad se obtiene cuando la polarización incidente es perpendicular al eje director del modulador, de esta forma la modulación en fase es nula.

Cuando las configuraciones de polarización son adecuadamente seleccionadas podemos controlar la modulación del frente de onda. Usualmente la modulación en intensidad y fase es evaluada haciendo uso de las matrices de Jones; como alternativa, las matrices de Mueller son una herramienta bastante precisa y elegante para evaluar la modulación en intensidad. La combinación Mueller-Jones provee una caracterización completa de una pantalla de cristal líquido. El método empleado en este trabajo no requiere hacer consideraciones del modelo microscópico para el cristal líquido y permite obtener la matriz de Mueller y la matriz de Jones, con las cuales es posible predecir la respuesta en fase e intensidad para distintas orientaciones de polarización [56–58]

### 4.2.1 POLARIZACIÓN

La polarización define la dirección de oscilación del campo eléctrico de la luz. Considerando una onda plana monocromática propagándose en la dirección  $z$ :

$$\vec{E}(\vec{r}, t) = \vec{E}_0 e^{i(kz - \omega t)} \quad (4.1)$$

El vector de amplitud  $\vec{E}_0$  es en general complejo y en él se representa el estado de polarización de la luz. De acuerdo con los valores que tomen las componentes del campo óptico y la relación de fase entre ellas, la luz puede presentar estados de polarización lineal, circular o elíptico. El estado de polarización y los cambios de polarización producidos por un dispositivo pueden ser representados a partir de vectores y matrices. Existen dos sistemas algebraicos para abordar la polarización óptica, las matrices de Jones y las matrices de Mueller [59–61]. En lo siguiente se describen los dos formalismos.

### 4.2.1.1 Vectores y matrices de Jones

El formalismo de Jones es una consecuencia natural de la descripción matemática en amplitud y fase de la luz. Este trata a los estados de polarización como vectores de dos componentes y a los elementos ópticos polarizantes como matrices de  $2 \times 2$ . Los vectores de Jones son complejos y describen la amplitud y la fase de la luz, las matrices de Jones también son complejas y describen la acción de los elementos ópticos sobre la amplitud y fase del haz incidente. De esta forma, un vector de Jones describe la polarización de la luz en términos de sus componentes, como sigue:

$$\vec{J} = \begin{pmatrix} E_x e^{i\phi_x} \\ E_y e^{i\phi_y} \end{pmatrix} \quad (4.2)$$

Donde  $E_x$  y  $E_y$  son las amplitudes de las componentes del campo.

Los cambios en el estado de polarización pueden describirse a partir de matrices  $2 \times 2$  que relacionan la polarización de la luz que incide sobre un dispositivo óptico polarizante y la luz que emerge de él, así:

$$\begin{pmatrix} E_x \\ E_y \end{pmatrix} = \begin{pmatrix} J_{00} & J_{01} \\ J_{10} & J_{11} \end{pmatrix} \begin{pmatrix} E_{x0} \\ E_{y0} \end{pmatrix} \quad (4.3)$$

Su desventaja está en considerar únicamente luz que se encuentra totalmente polarizada, despreciando la capacidad de diatenuación y despolarización.

### 4.2.1.2 Vectores de Stokes y Matrices de Mueller

Los parámetros de Stokes corresponden a una descripción completa del estado de polarización de la luz a partir de ciertas consideraciones sobre las mediciones de intensidad, de esta forma es posible representar el estado de polarización de la luz en términos de 4 elementos determinados a partir de parámetros observables.

Los parámetros de Stokes permiten describir la luz totalmente polarizada, parcialmente polarizada o no polarizada.

Un vector de Stokes se representa como:

$$\vec{S} = \begin{pmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{pmatrix} \quad (4.4)$$

El primer parámetro expresa la intensidad total del campo óptico incidente. Los otros tres parámetros describen el estado de polarización de la luz, específicamente,  $S_1$  representa la tendencia del haz a encontrarse en polarización lineal vertical u horizontal,  $S_2$  la tendencia a estar a  $45^\circ$  y  $S_3$  la tendencia a estar polarizada elípticamente. En términos de las componentes del campo, los elementos del vector de Stokes pueden escribirse como sigue:

$$S_0 = E_x^2 + E_y^2 \quad (4.5)$$

$$S_1 = E_x^2 - E_y^2 \quad (4.6)$$

$$S_2 = 2E_x E_y \cos\delta \quad (4.7)$$

$$S_3 = 2E_x E_y \sin\delta \quad (4.8)$$

Donde la siguiente igualdad se cumple en el caso de luz totalmente polarizada:

$$S_0^2 \geq S_1^2 + S_2^2 + S_3^2 \quad (4.9)$$

Los parámetros serán entonces proporcionales a la irradiancia y por lo tanto pueden ser determinados a partir de mediciones de intensidad.

Siguiendo el formalismo de Stokes, la matriz asociada a un elemento óptico es una matriz  $4 \times 4$  de coeficientes reales denominada matriz de Mueller. Las matrices de Mueller relacionan el vector de Stokes a la entrada con el vector de Stokes a la salida. Esta representación permite estudiar la interacción de la luz con elementos polarizantes y adicionalmente proporciona información de la diatenuación y del grado de polarización de la luz. Las matrices se componen de 16 elementos (Matrices  $4 \times 4$ ), donde todos los valores son reales al estar relacionada con la intensidad, así:

$$\vec{S}_{salida} = \begin{pmatrix} m_{00} & m_{01} & m_{02} & m_{03} \\ m_{10} & m_{11} & m_{12} & m_{13} \\ m_{20} & m_{21} & m_{22} & m_{23} \\ m_{30} & m_{31} & m_{32} & m_{33} \end{pmatrix} \vec{S}_{entrada} \quad (4.10)$$

La transmitancia del dispositivo óptico se define como la razón entre el parámetro  $S_0$  a la entrada y  $S_0$  a la salida, así:

$$T = \frac{m_{00}S_0 + m_{01}S_1 + m_{02}S_2 + m_{03}S_3}{S_0} \quad (4.11)$$

La diatenuación queda definida por los coeficientes de la primera fila de la matriz de Mueller, como sigue:

$$D = \frac{\sqrt{m_{01}^2 + m_{02}^2 + m_{03}^2}}{m_{00}} \quad (4.12)$$

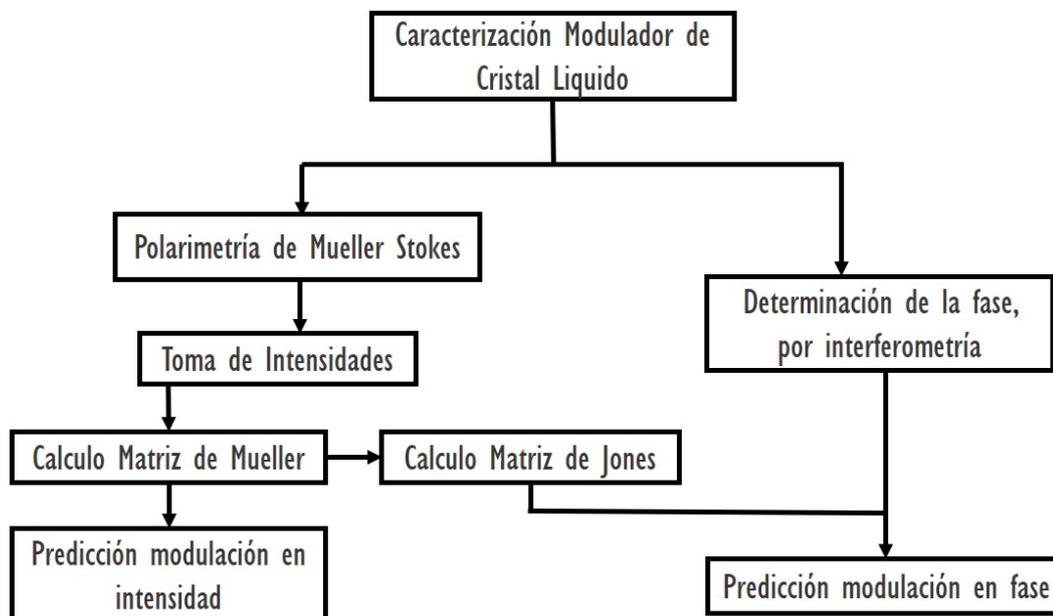
La diatenuación  $\mathbf{D}$ , nos da información de la relación entre las transmitancias máxima y mínima de dicho elemento, y toma valores entre 0 y 1. A medida que  $D$  se aproxima a 1 el elemento se va asemejando a un polarizador lineal, debido a que la diferencia entre la transmitancia máxima y mínima es muy grande. En cambio, a medida que  $D$  se aproxima a cero tenemos que el sistema actúa como un filtro neutro, por lo que la absorción sufrida por componentes ortogonales es muy similar, siendo la misma en  $D = 0$ .

---

El grado de polarización de la luz se puede expresar como la razón entre la cantidad de luz polarizada y el total de la luz. La polarizancia se define como la polarización resultante luego de incidir en un elemento óptico un haz no polarizado, en este caso, el vector de Stokes que caracteriza el estado de polarización a la salida del elemento óptico quedará totalmente descrito por la primera columna de la matriz de Mueller. Si entre los coeficientes  $m_{10}$ ,  $m_{20}$ ,  $m_{30}$ , hay alguno o más de uno diferente de cero, la matriz de Mueller transformará el estado de luz totalmente despolarizado en un estado de luz polarizada o parcialmente polarizada. Cuando la polarizancia es cercana a 0, el elemento no ejerce efectos polarizantes sobre el haz. Cuando se acerca a 1, el elemento es un dispositivo completamente polarizador. Este factor se determina como:

$$P = \frac{\sqrt{m_{10}^2 + m_{20}^2 + m_{30}^2}}{m_{00}} \quad (4.13)$$

#### 4.2.2 PROCESO DE CARACTERIZACIÓN



**Figura 4.3:** Diagrama del proceso de caracterización del modulador espacial de cristal líquido

#### Modulación en intensidad: Polarimetría de Mueller-Stokes

Denominamos polarímetro de Mueller al dispositivo que permite medir los 16 elementos de la matriz de Mueller de una muestra. La construcción de un polarímetro requiere contar con un sistema generador de estados de polarización y un sistema analizador de estados de polarización; de la relación entre el vector de polarización de la luz incidente en la muestra y la polarización después de la muestra, podemos obtener ecuaciones que nos permitan caracterizar la matriz de Mueller del dispositivo. La caracterización de una muestra requiere medir un mínimo de 16 intensidades, tomadas para distintas configuraciones del sistema generador-analizador, que permitan obtener todos los elementos de la matriz de Mueller. Una descripción más detallada puede encontrarse en las referencias [56, 62]

Para generar los estados de polarización que inciden en el elemento óptico, se requiere de un sistema generador, formado por un polarizador lineal y una lámina

retardadora de cuarto de onda. Debido a que en nuestro sistema el polarizador se mantiene fijo a  $0^\circ$  de la vertical del laboratorio, a la salida de la lámina retardadora la polarización del haz estará descrita por el vector:

$$\vec{S} = \begin{pmatrix} 1 \\ \cos^2(2\theta) \\ \frac{1}{2}\text{sen}(4\theta) \\ \text{sen}(2\theta) \end{pmatrix} \quad (4.14)$$

Donde  $\theta$  es el ángulo formado por el eje óptico de la lámina respecto al del polarizador en el sistema generador.

Por otro lado, el sistema analizador está compuesto por una lámina retardadora de cuarto de onda y por un polarizador lineal. A partir de la intensidad que emerge del sistema podemos reconstruir el vector de Stokes del haz incidente. Esto se realiza midiendo la intensidad saliente rotando la lámina retardadora del sistema analizador  $M$  veces a un paso  $\theta_r$ . De este modo, el vector de Stokes antes del sistema analizador puede escribirse de la forma:

$$\begin{pmatrix} S_0^r \\ S_1^r \\ S_2^r \\ S_3^r \end{pmatrix} = \frac{1}{M} \begin{pmatrix} \left( 2 \sum_{r=1}^M I\left(\frac{\pi}{2}, \theta_r\right) - 4 \sum_{r=1}^M I\left(\frac{\pi}{2}, \theta_r\right) \cos(4\theta_r) \right) \\ 8 \sum_{r=1}^M I\left(\frac{\pi}{2}, \theta_r\right) \cos(4\theta_r) \\ 8 \sum_{r=1}^M I\left(\frac{\pi}{2}, \theta_r\right) \text{sen}(2\theta_r) \\ -4 \sum_{r=1}^M I\left(\frac{\pi}{2}, \theta_r\right) \text{sen}(2\theta_r) \end{pmatrix} \quad (4.15)$$

Donde  $M$  es la cantidad de medidas realizadas,  $\pi/2$  representa el desfase introducido por la lámina retardadora de cuarto de onda y  $\theta_r$  es el ángulo de rotación de dicha lámina.

Ahora, ya que el estado de polarización de la luz que incide en la muestra a caracterizar es conocido (Ecuación (4.14)) y que es posible caracterizar la polari-

zación de la luz emergente de esta muestra (Ecuación (4.15)), entonces podemos relacionar los vectores de Stokes del sistema generador y del sistema analizador, de tal forma que la matriz de Mueller de un elemento óptico polarizante puede escribirse de la siguiente manera:

$$M = \frac{1}{N} \begin{pmatrix} \sum_{r=1}^N S_0^r - 2 \sum_{r=1}^N S_0^r \cos(4\theta) & 4 \sum_{r=1}^N S_0^r \cos(4\theta) & 4 \sum_{r=1}^N S_0^r \sin(4\theta) & 2 \sum_{r=1}^N S_0^r \sin(2\theta) \\ \sum_{r=1}^N S_1^r - 2 \sum_{r=1}^N S_1^r \cos(4\theta) & 4 \sum_{r=1}^N S_1^r \cos(4\theta) & 4 \sum_{r=1}^N S_1^r \sin(4\theta) & 2 \sum_{r=1}^N S_1^r \sin(2\theta) \\ \sum_{r=1}^N S_2^r - 2 \sum_{r=1}^N S_2^r \cos(4\theta) & 4 \sum_{r=1}^N S_2^r \cos(4\theta) & 4 \sum_{r=1}^N S_2^r \sin(4\theta) & 2 \sum_{r=1}^N S_2^r \sin(2\theta) \\ \sum_{r=1}^N S_3^r - 2 \sum_{r=1}^N S_3^r \cos(4\theta) & 4 \sum_{r=1}^N S_3^r \cos(4\theta) & 4 \sum_{r=1}^N S_3^r \sin(4\theta) & 2 \sum_{r=1}^N S_3^r \sin(2\theta) \end{pmatrix} \quad (4.16)$$

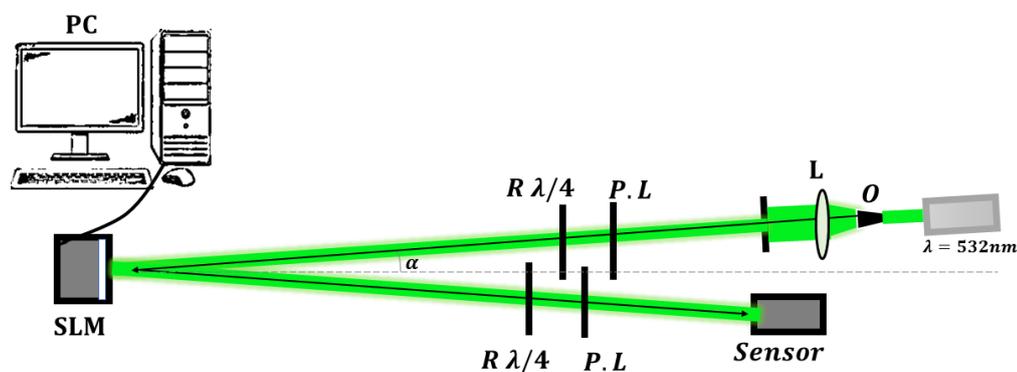
Usando la ecuación (4.16) es posible caracterizar un dispositivo óptico polarizante a partir del registro de intensidades para diferentes polarizaciones incidentes, que se generan variando N veces, un ángulo  $\theta$  la lámina retardadora del sistema generador y se caracterizan reconstruyendo el vector de Stokes a la salida.

En ese orden, se usó un arreglo polarimétrico que permitió la determinación de la matriz de Mueller del modulador en función del nivel de gris. El montaje consta de un sistema generador de estados de polarización y de un sistema detector de estados de polarización (Figura 4.4). Los dos sistemas se componen de una lámina retardadora de cuarto de onda y de un polarizador lineal. Los polarizadores están dispuestos sobre monturas rotativas de 1° de precisión y los retardadores están dispuestos sobre monturas rotativas de 2° de precisión. El eje óptico de los dispositivos está alineado con el eje vertical del laboratorio.

El sistema permite generar distintos estados de polarización, rotando la lámina retardadora. Para este caso se generaron 7 estados de polarización rotando la lámina a un paso de 52°. El haz incide con un ángulo  $\alpha = 4$  (Figura 4.4) sobre la pantalla de cristal líquido, que es controlada desde el computador con un soft-

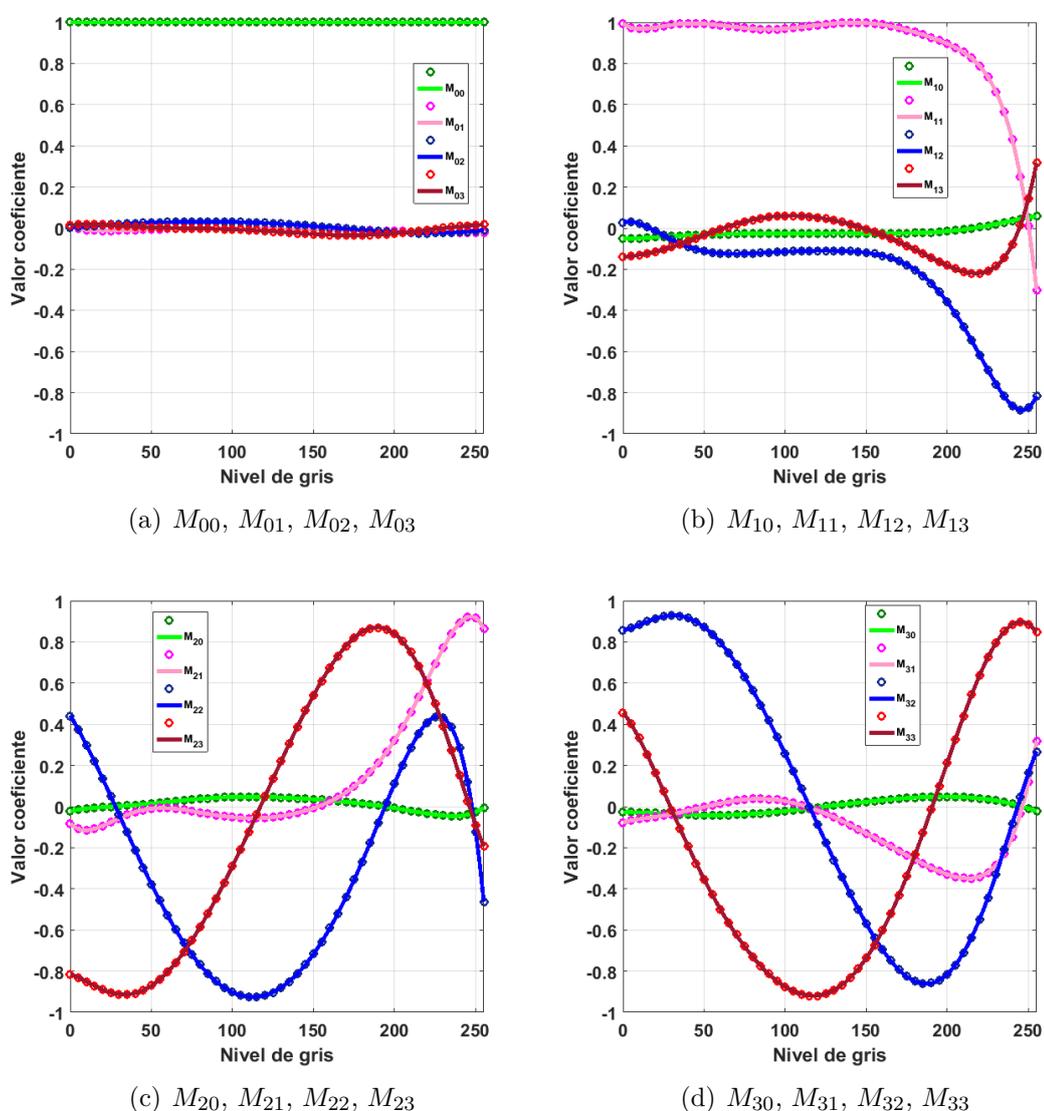
ware realizado en MatLab, donde se determina el nivel de gris a proyectar. Para cada estado de polarización generado, la luz reflejada en el modulador pasa por el sistema analizador de estados de polarización, donde se tomaron 7 medidas rotando la lámina retardadora a un paso de  $52^\circ$ . La intensidad es medida en un detector LaserPowerMeter modelo FieldMate.

Las intensidades permiten la reconstrucción del vector de Stokes saliente de la pantalla y al ser conocido el estado de la polarización a la entrada, es posible obtener el comportamiento del modulador para ese nivel de gris, descrito por su correspondiente matriz de Mueller. El proceso requirió tomar 49 intensidades por cada nivel de gris, se tomaron datos para 52 niveles de gris (de 0 a 255 cada 5 niveles). Las intensidades se tomaron 3 veces con el propósito de hacer una estadística y reducir el error producido por las fallas de precisión en la rotación de la lámina y la precisión del sensor. Las gráficas de los datos experimentales se presentan en el Anexo C. A partir de las intensidades medidas se determinan los 16 coeficientes de Mueller para cada nivel de gris.



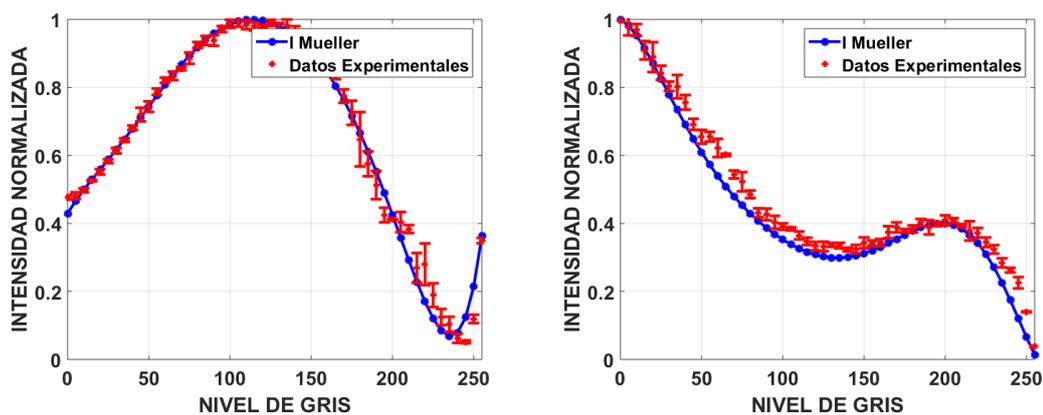
**Figura 4.4:** Arreglo Experimental Polarímetro de Mueller-Stokes. P.L: Polarizador lineal,  $R\lambda/4$  : Retardador de cuarto de onda. SLM: Modulador LC-R 2500. El arreglo es iluminado por un frente de onda plano con longitud de onda  $\lambda = 532nm$

En la figura 4.5 se gráfica el valor de los coeficientes de la matriz de Mueller en función del nivel de gris, normalizados al coeficiente  $M_{00}$ . Los valores de los coeficientes de la matriz fueron ajustados a una función polinómica para corregir las desviaciones producidas por errores en la toma de intensidades y en el cálculo de los coeficientes. En la matriz encontrada los valores de la primera fila y primera columna se encuentran con valores próximos a cero, lo cual representa que los efectos de diatenuación y polarizancia no son significativos. Los demás coeficientes de la matriz describen el comportamiento del modulador de cristal líquido.

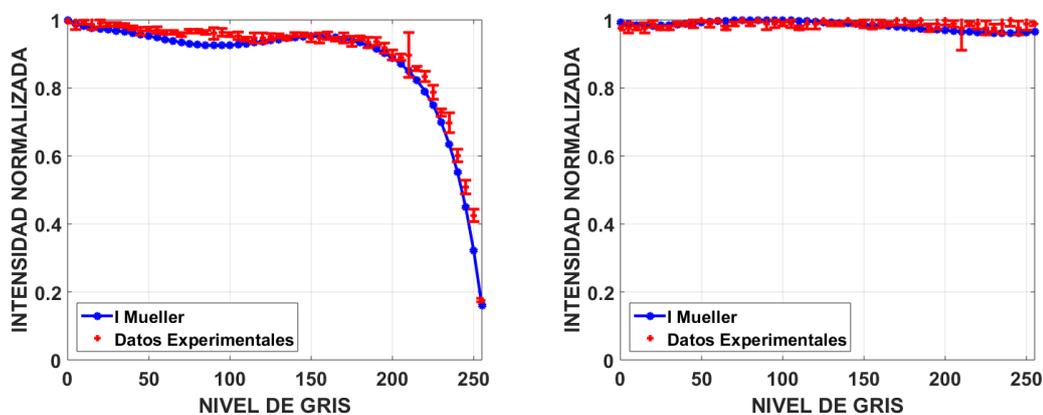


**Figura 4.5:** Coeficientes de la matriz de Mueller del SLM para  $\lambda = 532nm$

Una vez caracterizada la matriz de Mueller del modulador, y utilizando las expresiones teóricas para las matrices de Mueller de polarizadores y láminas retardadoras, se puede predecir la intensidad de salida como función del nivel de gris para una dada configuración del polarímetro. Haciendo el producto de matrices se evaluó la capacidad predictiva de las simulaciones comparando con experimentos de medición de intensidad, los resultados se presentan en la figura 4.6.



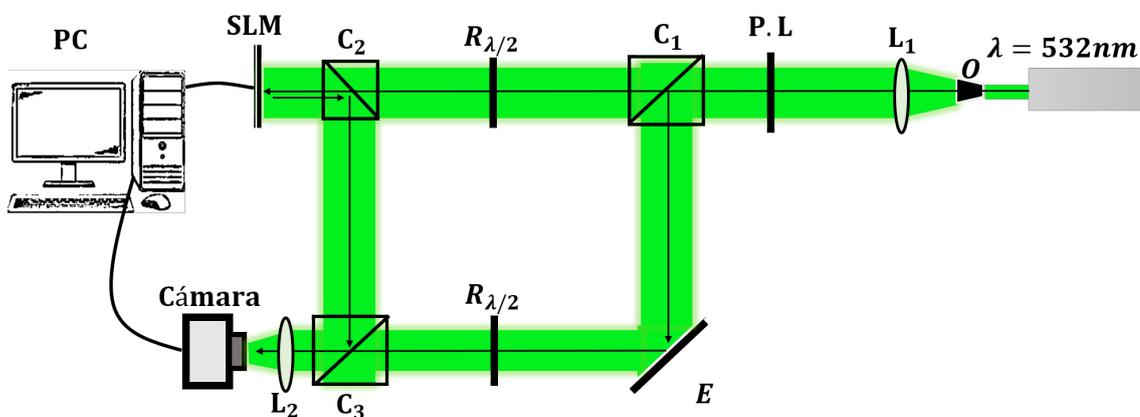
(a) Configuración: Polarizador lineal a  $124^\circ$  +SLM + Polarizador lineal a  $58^\circ$  (b) Configuración: Polarizador lineal a  $130^\circ$  + lámina  $\lambda/4$  a  $140^\circ$  +SLM + lámina  $\lambda/4$  a  $101^\circ$  + Polarizador lineal a  $100^\circ$



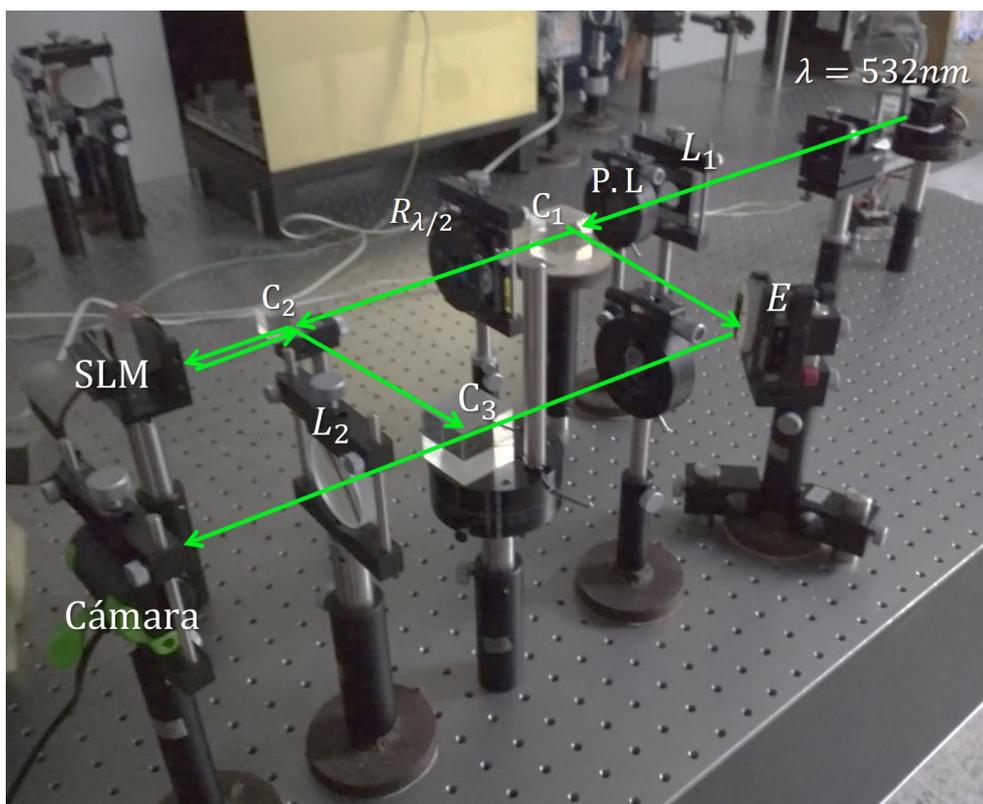
(c) Configuración: Polarizador lineal a  $0^\circ$  + lámina  $\lambda/4$  (d) Configuración: Polarizador lineal a  $10^\circ$  +SLM a  $284^\circ$  +SLM + Polarizador lineal a  $0^\circ$

**Figura 4.6:** Intensidad predicha por las matrices de Mueller vs Intensidad experimental

### 4.2.2.1 Modulación en fase



(a) Esquema del interferómetro tipo Mach-Zehnder



(b) Fotografía del Arreglo Experimental

**Figura 4.7:** Arreglo experimental para la determinación de la modulación en fase.  $L_1$  : Lente focal +25 cm.  $E$ : Espejo.  $C_1, C_2, C_3$  : Cubos divisores. P.L: Polarizador Lineal.  $R_{\lambda/2}$ : Retardador de media onda. SLM: Modulador LC-R 2500.  $L_2$ : Lente focal +20 cm. La fuente de iluminación es un láser de estado sólido con longitud de onda  $\lambda = 532nm$

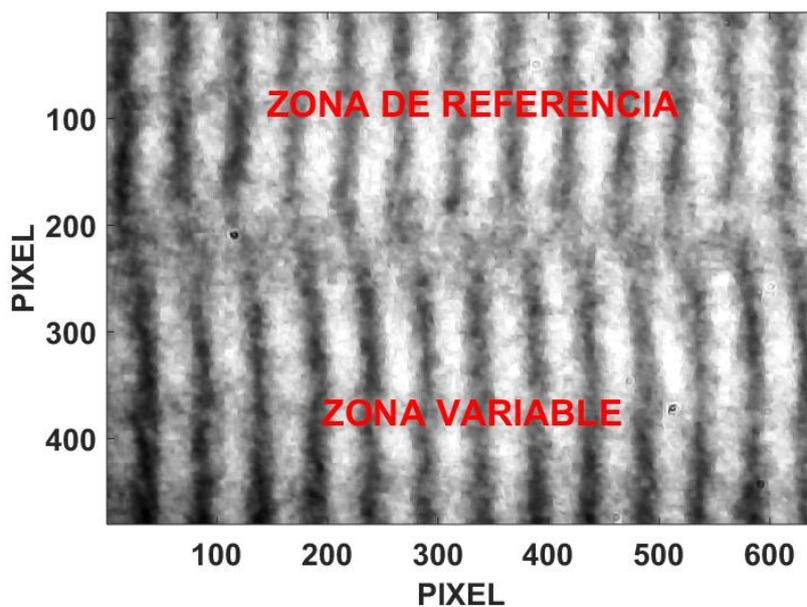
---

Las matrices de Mueller únicamente son sensibles a la intensidad del campo, por lo que no nos permiten predecir la modulación en fase. Para este trabajo, realizamos una caracterización de la modulación en sólo fase para la pantalla de cristal líquido; paralelo a esto se dedujo una matriz de Jones equivalente para la pantalla, a partir de la matriz de Mueller calculada. Conociendo la curva de fase asociada a la pantalla es posible completar la matriz de transferencia de Jones, lo que nos permitirá predecir la modulación en fase para distintas configuraciones polarimétricas.

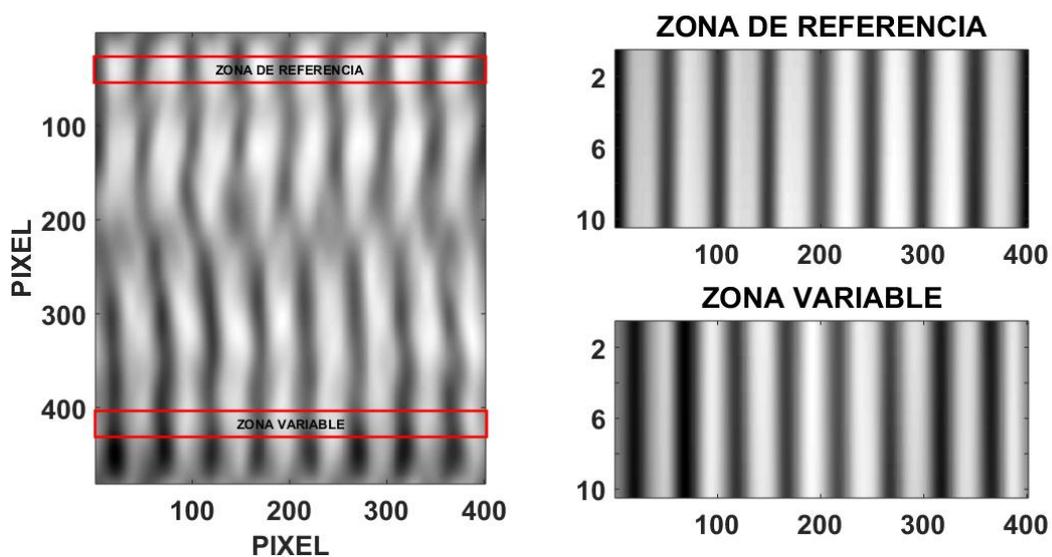
La modulación en fase se determinó utilizando un interferómetro Mach-Zehnder. El esquema experimental se presenta en la figura 4.7. En el esquema el modulador se ubica en uno de los brazos del interferómetro, la incidencia del haz es normal a la pantalla de cristal líquido [63]. La pantalla del modulador se divide en dos, la mitad se configura en el nivel de gris 0, que se tomó como referencia para medir el desfase de las franjas y en la otra mitad se varia progresivamente el nivel de gris; a medida que se cambia el nivel de gris en la zona variable se observa un corrimiento rígido de las franjas como consecuencia de la fase introducida por el modulador.

Dividir la pantalla de esta forma nos permite reducir el error ocasionado por vibraciones mecánicas. El interferómetro es iluminado con luz polarizada linealmente, el retardador de media onda está ubicado sobre una montura rotativa de precisión  $2^\circ$ , este permite rotar el plano de polarización de la luz que incide en el modulador. La polarización se orientó paralela al eje director del modulador, bajo esta condición se debe producir la máxima modulación en fase y la mínima modulación en intensidad. En el haz de referencia la polarización se orientó de forma tal que las franjas tuvieran un buen contraste. Utilizamos una cámara CMOS modelo STARTEC webcam, en la que registramos la interferencia entre el haz que pasa por la pantalla y el haz de referencia.

El patrón de franjas de interferencia fue restaurado digitalmente usando un procesamiento basado en la transformada de Fourier (Figura 4.8). A partir de las franjas procesadas se determinó la máxima modulación en fase introducida por el modulador en función del nivel de gris, los resultados obtenidos se presentan en la figura 4.12 y en la tabla 4.2.



(a) Interferograma

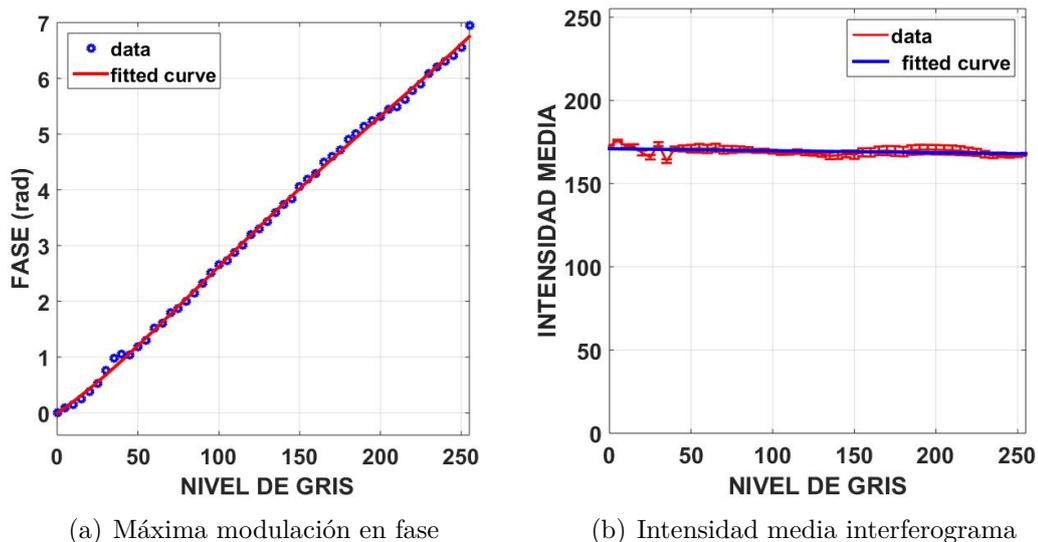


(b) Interferograma procesado

(c) Interferograma procesado

**Figura 4.8:** Interferogramas: Zona de referencia nivel de gris 0; Zona de variable nivel de gris 40

La dificultad para medir la modulación en sólo fase se encuentra en garantizar paralelas la orientación de la polarización de la luz y eje director del modulador. Una forma de encontrar esta orientación consiste dividir la pantalla del modulador en dos, una se configura con el máximo nivel de gris (255) y la otra con el nivel de gris 0; el ángulo para el cual el corrimiento entre las franjas es máximo, corresponde la orientación del eje director, en una orientación de la luz paralela a ello obtendremos modulación en solo fase, es decir máxima modulación en fase y modulación mínima de intensidad [64]. Se determinó que el eje director se encuentra a  $-6^\circ$  de la vertical del laboratorio.



**Figura 4.9:** Curvas de fase para modulación en sólo fase

$\lambda$ (nm)	Fase $\pi$ (Nivel de Gris)	Fase $2\pi$ (Nivel de Gris)	Fase Máxima (rad)
532	115	240	6.94

**Tabla 4.2:** Fase introducida por el modulador

Por otro lado, considerando que las contribuciones de polarizancia y diatenuación de la pantalla son despreciables, es posible aplicar descomposición polar a la matriz de Mueller y encontrar la matriz de Jones equivalente, a falta de un factor de fase que debe determinarse por interferometría. De esta forma, y sin considerar el modelo microscópico, la matriz de jones para una pantalla de cristal líquido puede ser expresada como sigue [56].

$$J_{SLM} = \exp(i\beta) \begin{pmatrix} A & B \\ -B & A^* \end{pmatrix} \quad (4.17)$$

Los valores  $A = r_{00} \exp(i\theta_{00})$  y  $B = r_{01} \exp(i\theta_{01})$  se obtienen en términos de los elementos  $m_{ij}$  de la matriz de Mueller, como sigue [61]:

$$r_{00} = [(m_{00} + m_{01} + m_{10} + m_{11})]^{1/2} \quad (4.18)$$

$$r_{01} = [(m_{00} - m_{01} + m_{10} - m_{11})]^{1/2} \quad (4.19)$$

$$r_{10} = [(m_{00} + m_{01} - m_{10} - m_{11})]^{1/2} \quad (4.20)$$

$$r_{00} = [(m_{00} - m_{01} - m_{10} + m_{11})]^{1/2} \quad (4.21)$$

$$\cos(\theta_{00} - \theta_{01}) = \frac{(m_{02} + m_{12})}{[(m_{00} + m_{10})^2 - (m_{01} + m_{11})^2]^{1/2}} \quad (4.22)$$

$$\sin(\theta_{00} - \theta_{01}) = \frac{(m_{03} + m_{13})}{[(m_{00} + m_{10})^2 - (m_{01} + m_{11})^2]^{1/2}} \quad (4.23)$$

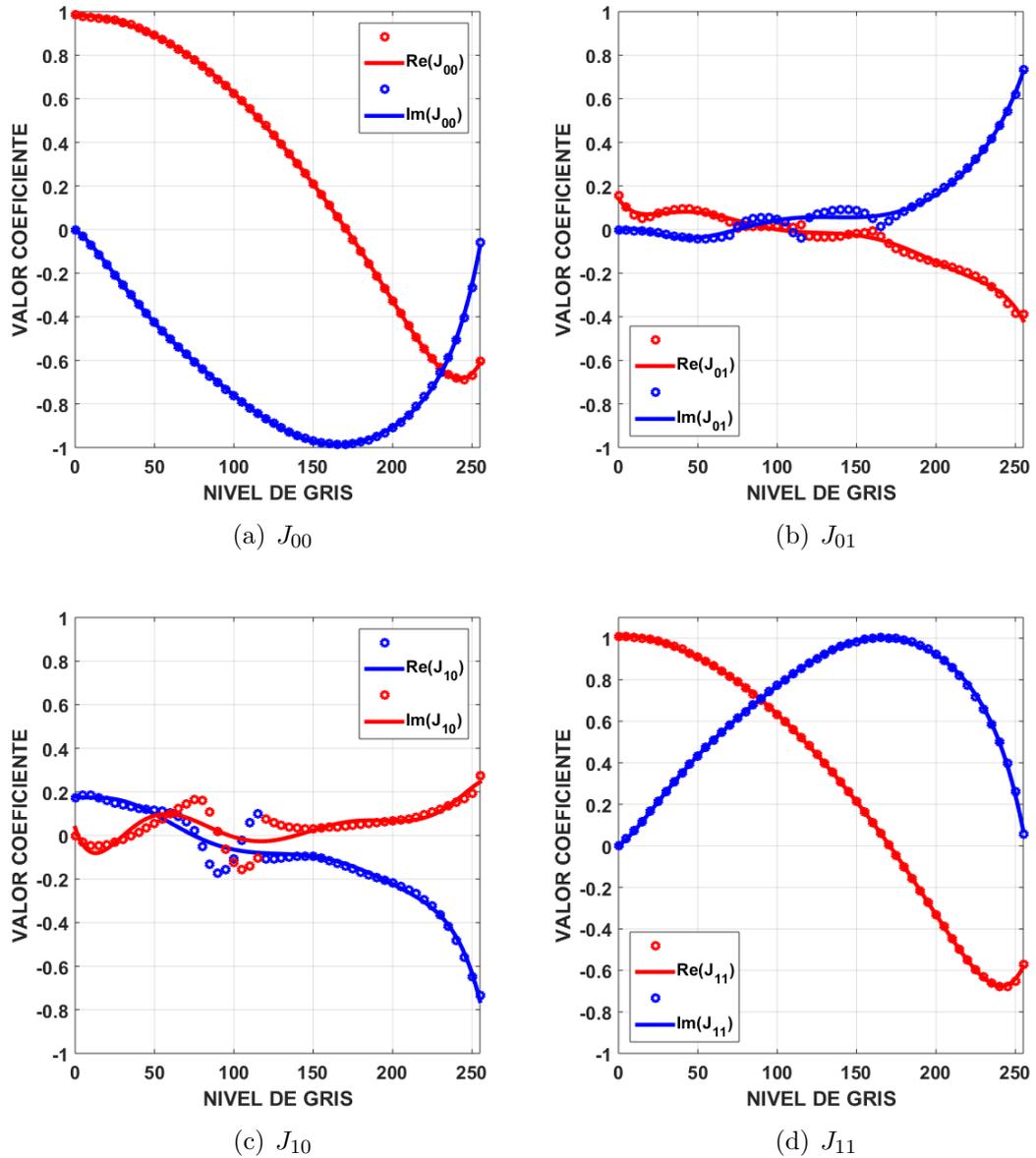
$$\cos(\theta_{10} - \theta_{00}) = \frac{(m_{20} + m_{21})}{[(m_{00} + m_{01})^2 - (m_{10} + m_{11})^2]^{1/2}} \quad (4.24)$$

$$\sin(\theta_{10} - \theta_{00}) = \frac{(m_{30} + m_{31})}{[(m_{00} + m_{01})^2 - (m_{10} + m_{11})^2]^{1/2}} \quad (4.25)$$

$$\cos(\theta_{00} - \theta_{11}) = \frac{(m_{22} + m_{33})}{[(m_{00} + m_{11})^2 - (m_{10} + m_{01})^2]^{1/2}} \quad (4.26)$$

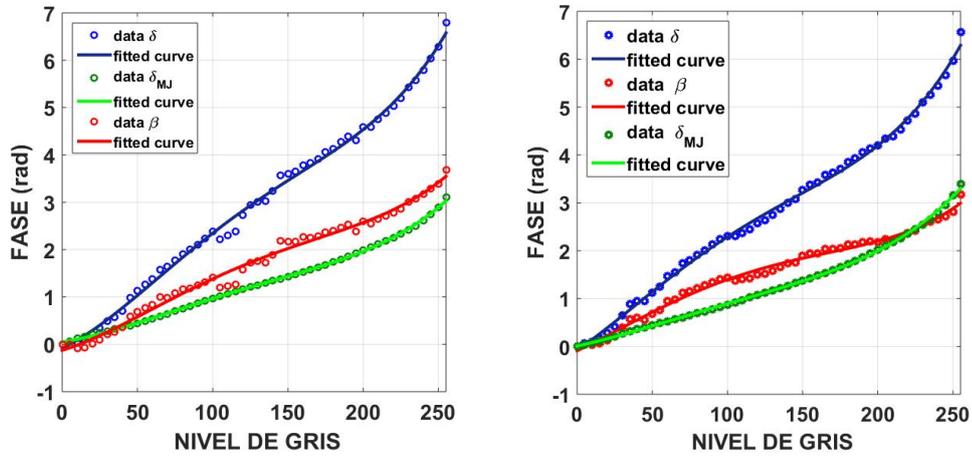
$$\sin(\theta_{11} - \theta_{00}) = \frac{(m_{32} + m_{23})}{[(m_{00} + m_{11})^2 - (m_{12} + m_{01})^2]^{1/2}} \quad (4.27)$$

Aplicamos descomposición polar a las matrices de Mueller del aparte anterior, y obtuvimos la matriz de Jones en función del nivel de gris para el modulador.



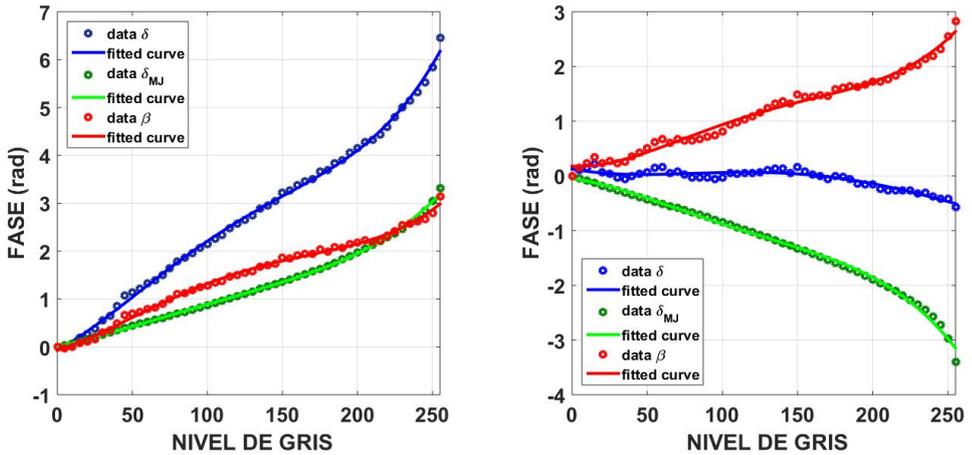
**Figura 4.10:** Matriz de Jones del SLM para  $\lambda = 532nm$

En la ecuación (4.17), el factor  $\beta$  corresponde a la fase que introduce la pantalla como consecuencia de su birrefringencia. Conociendo la matriz de Jones determinada aplicando descomposición polar a las matrices de Mueller y conociendo la curva de fase introducida por el modulador, podemos relacionar la fase derivada de la matriz de Jones y relacionarla con la fase medida, para obtener la fase  $\beta$ . Esta curva es única para el modulador por lo que la curva determinada en modulación en sólo fase y las distintas mediciones de fase para otras configuraciones nos deben conducir a la misma respuesta.



(a) Configuración: Polarización lineal orientada a  $0^\circ$

(b) Configuración: Polarización lineal orientada a  $12^\circ$

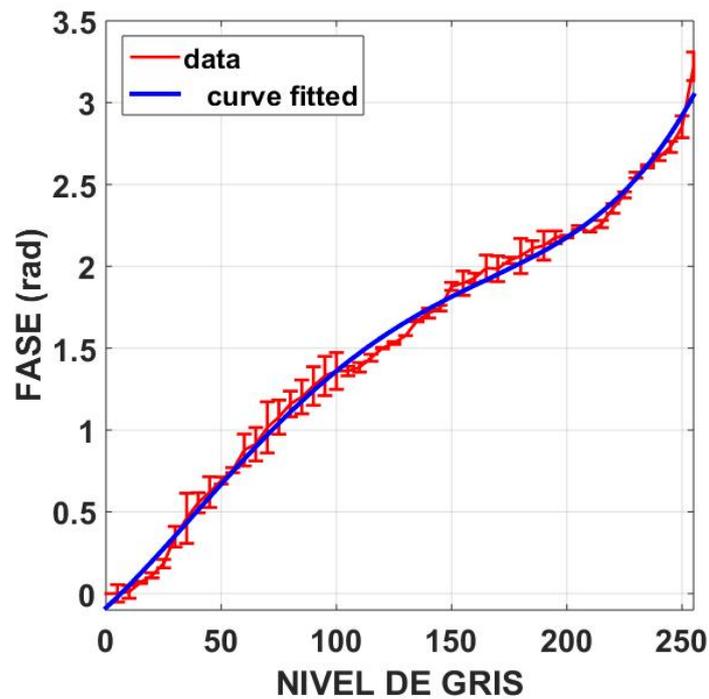


(c) Configuración: Polarización lineal orientada a  $6^\circ$

(d) Configuración: Polarización lineal orientada a  $90^\circ$

**Figura 4.11:** Curvas de fase para distintas configuraciones de polarización.  $\delta$  es la fase medida por interferometría,  $\delta_{MJ}$  es la fase derivada de la matriz de Jones y  $\beta = \delta - \delta_{MJ}$  es la fase asociada a la birrefringencia de la pantalla.

Se realizaron distintas medidas con el objetivo de calibrar la fase con precisión. De esta forma la curva de fase asociada a la birrefringencia de la pantalla será:



**Figura 4.12:** Fase  $\beta$

Una vez obtenidas las matrices características del modulador (Mueller y Jones) podemos predecir el comportamiento en fase e intensidad que tendrá el modulador para diferentes configuraciones de polarizadores y retardadores. Usando estos resultados se implementó una interfaz gráfica como apoyo a la caracterización del modulador. Con la interfaz gráfica diseñada es posible predecir las curvas teóricas para distintas configuraciones de polarizadores, el código requiere los parámetros del arreglo óptico (Polarizadores, retardadores con su correspondiente orientación y/o desfase). Los detalles de funcionamiento se presentan en el anexo B.

# Capítulo 5

## CONCLUSIONES Y PERSPECTIVAS

---

---

Se implementó un procesador óptico-virtual de encriptación de transformada conjunta, en este sentido se simuló el procesador óptico usando encriptación con una sola llave de fase aleatoria, y con doble máscara de fase aleatoria. Presentamos una técnica de encriptación para la generación de criptogramas camuflados como imágenes determinísticas [65,66], la técnica desarrollada se basa en el uso de llaves con amplitud periódica y fase en componentes armónicas circulares. En los métodos de encriptación de imágenes ya conocidos, no existe diferencia aparente entre los criptogramas de cada imagen, generalmente son ruido blanco o conservan elementos de similitud. Camuflar el criptograma en formatos diferentes podría ser un elemento distractor para su detección por usuarios no autorizados, así agregamos un elemento adicional de seguridad cualitativo. Los distintos resultados para la encriptación de imágenes complejas e imágenes binarias fueron presentados, verificando que los criptogramas generados son variantes ante los parámetros de cifrado. El método implementado resulta una técnica con un buen nivel de seguridad al requerir la totalidad de la amplitud compleja de la llave de encriptación para el descifrado de la imagen, lo anterior constituye 6 parámetros de seguridad: 4 para la generación de la amplitud de la llave y 2 en la generación de la fase de llave, además del camuflaje de los criptogramas que constituye un parámetro de seguridad subjetivo.

---

Tomando como base los resultados obtenidos en la implementación virtual del procesador, se diseñó el procesador óptico-digital pensando en una futura implementación experimental del sistema de cifrado-descifrado, se presentó el diseño de un esquema experimental del procesador de encriptación haciendo uso de moduladores espaciales de luz para la síntesis de las llaves de encriptación en un esquema interferométrico tipo Mach-Zehnder. Como parte del diseño se realizó la caracterización de la respuesta en intensidad y fase para un modulador espacial de cristal líquido LCR 2500. El proceso de caracterización del modulador constó de dos partes; realizando polarimetría de Mueller-Stokes obtuvimos la matriz de Mueller para la pantalla de cristal líquido, con la cual podemos predecir la curva de intensidad en función del nivel de gris para la pantalla de cristal líquido; por otro lado se realizó la determinación de la curva de fase del modulador usando interferometría, mediante este resultado y aplicando descomposición polar a la matriz de Mueller, encontramos la matriz de Jones para la pantalla de cristal líquido, con esto podemos predecir la respuesta en fase en función del nivel de gris. Es necesario señalar que la caracterización realizada es aplicable únicamente para la longitud de onda de 532 nm, con incidencia cuasi-normal al modulador de cristal líquido.

Queda como perspectiva del trabajo la implementación experimental del sistema óptico-digital de encriptación. También se hace interesante realizar un trabajo referente a criptoanálisis del método propuesto que permita establecer los límites de su funcionamiento, así como validar su seguridad.

## REFERENCIAS BIBLIOGRÁFICAS

---

- [1] A. J. Meneses, P. C. van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. 2001.
- [2] C. A. Pinzon, “Procesadores ópticos virtuales de encriptación usando llaves en armonicos circulares,” 2016.
- [3] E. A. Rueda, *Encriptación y desencriptación dinámica de información por medios óptico-digitales*. PhD thesis, Universidad de Antioquia, 2009.
- [4] S. Behnia, P. Ayubi, and W. Soltanpoor, “Image encryption based on quantum chaotic map and fsm transforms,” in *15th International Telecommunications Network Strategy and Planning Symposium (NETWORKS)*, IEEE, 2012.
- [5] T. HuaJiamin, C. PeiWenquan, and Z. Zhou, “Quantum image encryption algorithm based on image correlation decomposition,” *International Journal of Theoretical Physics*, vol. 54, p. 526–537, 2015.
- [6] P. Refregier and B. Javidi, “Optical image encryption based on input plane and fourier plane random encoding,” *Optics letters*, vol. 20, no. 7, pp. 767–769, 1995.
- [7] B. Javidi, G. Zhang, and J. Li, “Experimental demonstration of the random phase encoding technique for image encryption and security verification,” *Optical Engineering*, vol. 35, no. 9, 1996.

- 
- [8] T. Nomura and B. Javidi, "Optical encryption using a joint transform correlator architecture," *Optical Engineering*, vol. 39, no. 8, 2000.
- [9] N. Towghi, B. Javidi, , and Z. Luo, "Fully phase encrypted image processor," *Optical Society of America*, 1999.
- [10] B. Javidi, N. Towgh, N. Maghzi, and S. C. Verrall, "Error-reduction techniques and error analysis for fully phase and amplitude based encryption," *Applied Optics*, 2000.
- [11] J. Rueda and A. L. Romero, "Optical cryptography using fresnel diffraction and phase conjugation," *Dyna*, no. 181, pp. 25–30, 2013.
- [12] J. M. Vilardy, M. S. Millan, and E. Pérez-Cabré, "Joint transform correlator-based encryption system using the fresnel transform and nonlinear filtering," *Proceedings of Spie*, 2013.
- [13] N. Singh and A. Sinha, "Optical image encryption using improper hartley transforms and chaos," *Optik*, p. 918–925, 2010.
- [14] J. Wu, L. Zhang, and N. Zhou, "Image encryption based on the multiple-order discrete fractional cosine transform," *Optics Communications*, p. 1720–1725, 2010.
- [15] W. Zamrani, E. Ahouzi, A. Lizana, J. Campos, and M. J. Yzuel, "Optical image encryption technique based on deterministic phase masks," *Optical Engineering*, vol. 55, 2016.
- [16] M. Tebaldi, "Optical-data storage-readout technique based on fractal encrypting masks," *Optics Letters*, vol. 34, no. 3, 2009.
- [17] J. E. Rueda, "Encryption using circular harmonic key," *Dyna*, vol. 82, no. 190, pp. 70–73, 2015.
- [18] O. Matoba and B. Javidi, "Encrypted optical storage with angular multiplexing," *Applied optics*, vol. 38, no. 35, 1999.

- [19] M. N. Islam, “Optical security system employing quadrature multiplexing,” *Optical Engineering*, 2008.
- [20] O. M. Enrique Tajahuerce, S. C. Verrall, and B. Javidi, “Optoelectronic information encryption with phase-shifting interferometry,” *Applied Optics*, vol. 39, no. 14, 2000.
- [21] E. Ahouzi, W. Zamrani, N. Azami, A. Lizana, and J. C. M. J. Yzuel, “Optical triple random-phase encryption,” *Optical Engineering*, vol. 56(11), 2017.
- [22] Q. Wang, Q. Guo, and J. Zhou, “Multiple-image encryption using polarized light encoding and the optical interference principle in the fresnel-transform domain,” *Applied Optics*, 2013.
- [23] H. Zhao, Z. Zhong, W. Fang, H. Xie, Y. Zhang, and M. Shan, “Double-image encryption using chaotic maps and nonlinear non-dc joint fractional fourier transform correlator,” *Optical Engineering*, 2016.
- [24] S. Liu, C. Guo, and J. T. Sheridan, “A review of optical image encryption techniques,” *Optics and Laser Technology*, 2014.
- [25] O. Matoba and B. Javidi, “Secure three-dimensional data transmission and display,” *Applied optics*, vol. 43, no. 11, 2004.
- [26] W. Qin, X. Peng, and X. Meng, “Cryptanalysis of optical encryption schemes based on joint transform correlator architecture,” *Optical Engineering*, vol. 50(2), 2011.
- [27] A. Akhavan, A. Samsudin, and A. Akhshani, “Cryptanalysis of an image encryption algorithm based on dna encoding,” *Optics and Laser Technology*, vol. 95, pp. 94–99, 2017.
- [28] M. M. Islam, M. A. Karim, and M. S. Alam, “Optical cryptographic system employing multiple reference-based joint transform correlation technique,” *Optical Engineering*, vol. 50, 2011.

- [29] J. F. Barrera, M. Tebaldi, D. Amaya, W. D. Furlan, J. A. Monsoriu, N. Bolognini, and R. Torroba, “Multiplexing of encrypted data using fractal masks,” *Optics Letters*, vol. 37, no. 14, 2012.
- [30] J. F. Barrera, “Experimental multiplexing of encrypted movies using a jtc architecture,” *Optics Express*, vol. 20, no. 4, 2012.
- [31] J. F. Barrera, E. Rueda, C. Ríos, M. Tebladi, N. Bolognini, and R. Torroba, “Subsampling technique to enhance the decoded output of jtc encrypting system,” in *Proceedings of Spie*, vol. 8011.
- [32] D. Lu and W. Jim, “Color image encryption based on joint fractional fourier transform correlator,” *Optical Engineering*, vol. 50(6), 2011.
- [33] L.-C. Lin and C.-J. Cheng, “Optimal key mask design for optical encryption based on joint transform correlator architecture,” *Optics Communications*, vol. 258, p. 144–154, 2006.
- [34] C.-L. Chen and L.-C. Lin, “Design and implementation of an optical joint transform encryption system using complex-encoded key mask,” *Optical Engineering*, 2008.
- [35] X. Song, J. Zhao, C. W. Wencheng Yuan, and S. Li, “Necessity analyses of phase masks in joint fractional fourier transform correlator,” *Optics Communications*, 2006.
- [36] A. L. Romero, “Criptografía de imágenes utilizando la transformada de fourier,” 2006.
- [37] A. L. Romero, “Síntesis de llaves Ópticas de encriptación utilizando moduladores espaciales de luz,” Master’s thesis, Universidad de Pamplona, 2010.
- [38] V. Lugt, “Signal detection by complex spatial filtering,” *IEEE transactions on Information*, vol. 10, p. 139, 1964.
- [39] C. S. W. and J. W. Goodman, “A technique for optically convolving two functions,” *Applied Optics*, vol. 5, pp. 1248–1249, 1966.

- [40] J. W. Goodman, *Introduction to Fourier Optics*. The McGraw-Hill, 1996.
- [41] F. M. Grimaldi, “Físico mathesis de lumine, coloribus, et iride, aliisque annexis libri duo,” pp. 1–11, 1665.
- [42] D. Voelz, *Computational Fourier Optics: A MATLAB Tutorial*. Society of Photo-Optical Instrumentación Engineers (SPIE), 2011.
- [43] S. Jutamulia, “Joint transform correlators and their applications,” in *Conference proceedings of spie*, pp. 233–243, 1992.
- [44] M. S. Alam and M. A. Karim, “Fringe-adjusted joint transform correlation,” *Applied Optics*, vol. 32, no. 23, 1993.
- [45] O. Gualdrón and H. Arsenault, “Phase derived circular harmonic filter,” *Optics Communications*, vol. 104, pp. 32–34, 1993.
- [46] W. Osten, C. Kohler, and J. Liesener, “Evaluation and application of spatial light modulators for optical metrology,” *Óptica pura y aplicada*, 2005.
- [47] R. Tudela, E. Martín-Badosa, I. Labastida, and S. Vallmitjana, “Full complex fresnel holograms displayed on liquid crystal devices,” *Journal of Optics A: Pure and Applied Optics*, 2003.
- [48] H.-K. Liu, J. A. Davis, and R. A. Lilly, “Optical-data-processing properties of a liquid-crystal television spatial light modulator,” *Optics Letters*, 1985.
- [49] I.-C. Khoo, *Liquid Crystals*. John Wiley Sons, 2007.
- [50] U. Efron, ed., *Spatial light modulator technology: material, devices and application*. 1995.
- [51] E. Lueder, *Liquid Crystal Displays: Addressing Schemes and Electro-Optical Effects*. John Wiley Sons, 2001.
- [52] S. T. Wu and D. K. Yang, *Reflective Liquid Crystal Displays*. John Wiley Sons, 2001.

- [53] X. Wang, H. T. Dai, K. Y. Liu, and J. H. Liu, "Characteristics of lcos phase-only spatial light modulator and its applications," *Optics Communications*, pp. 269276,, 2004.
- [54] A. Langner, H. Gruber, S. Kruger, G. Wernicke, and S. Osten, "Nematic lcos spatial light modulators-performance in diffractive optics," in *Proceedings of SPIE*, pp. 627–631, 2004.
- [55] V. D. Bosch, *Optimización del funcionamiento de un modulador espacial de luz de cristal líquido mediante el modelo retardador-rotor*. PhD thesis, Universidad de Valencia, 2008.
- [56] I. Moreno, A. Lizana, J. Campos, A. Márquez, C. Iemmi, and M. J. Yzuel, "Combined mueller and jones matrix method for the evaluation of the complex modulation in a liquid-crystal-on-silicon display," *Optics Letters*, 2008.
- [57] A. Marquez, C. Iemmi, I. Moreno, J. J. Davis, and M. Yzuel, "Quantitative predictions of the modulation behavior of twisted nematic liquid crystal displays based on a simple physical model," *Optical Engineering*, 2001.
- [58] D. S. Sabatke, M. R. Descour, E. Dereniak, W. Sweatt, S. Kemme, and G. Phipps, "Optimization of retardance for a complete stokes polarimeter," *Optics Letters*, 2000.
- [59] M. Born and E. Wolf, *Principles of optics*. Cambridge, 1999.
- [60] K. K. Sharma, *Optics: Principles and Applications*. ELSELVIER, 2006.
- [61] D. Goldstein, *Polarized Light*. Marcel Dekker, 2003.
- [62] A. Lizana, "Procedimiento de caracterización y optimización de la respuesta en intensidad de una pantalla lcos." Trabajo de Investigación de Tercer Ciclo, 2008.
- [63] A. Lizana, N. Martín, M. Estapé, E. Fernández, I. Moreno, A. Márquez, C. Iemmi, J. Campos, and M. Yzuel, "Influence of the incident angle in the performance of liquid crystal on silicon displays.," *Opt Express*, 2009.

- 
- [64] J. E. Rueda, A. L. Romero, and L. A. Guerra, “Characterization of reflective tn-lcd, tuned in phase-only modulation and to six wavelengths,” *Photonics Letters Of Poland*, vol. 2, pp. 174–176, 2010.
- [65] A. Guerrero and J. E. Rueda, “Cryptogram optical camouflage technique using amplitude keys.” manuscrito en trámite de publicación, *Optik*, 2018.
- [66] A. Guerrero and J. E. Rueda, “Transformación del criptograma clásico en una imagen abstracta,” in *Memorias XV Encuentro Nacional de Óptica y VI Conferencia Andina y del Caribe en Óptica y Sus Aplicaciones*, 2017.

# Anexo A

## MANUAL DE USUARIO PROCESADOR ÓPTICO VIRTUAL DE ENCRIPCIÓN JTCRYPTO.GOM

---

JTCRYPTO.GOM es un procesador óptico virtual de encriptación de transformada conjunta que permite generar criptogramas camuflados como una imagen determinística. Las imágenes de entrada son BITMAP de cualquier tipo: Binaria, de intensidad, indexada o RGB, y de cualquier formato que soporte MATLAB (bmp, jpg, tif, etc). Esta herramienta se desarrolló utilizando el entorno visual interfaz de usuario GUI MATLAB. La arquitectura es simétrica, es decir de clave privada (se encripta y desencripta con la misma llave). El diseño de la interfaz gráfica consta de tres partes: menú principal , ventana de Encriptación y ventana de Desencriptación.

En el menú principal los botones Encriptar y Desencriptar enlazan las ventanas de encriptación y desencriptación.



Figura A.1: Ventana menú JTCRYPTO.GOM

### A.1 DESCRIPCIÓN DE LA VENTANA DE ENCRIPCIÓN:

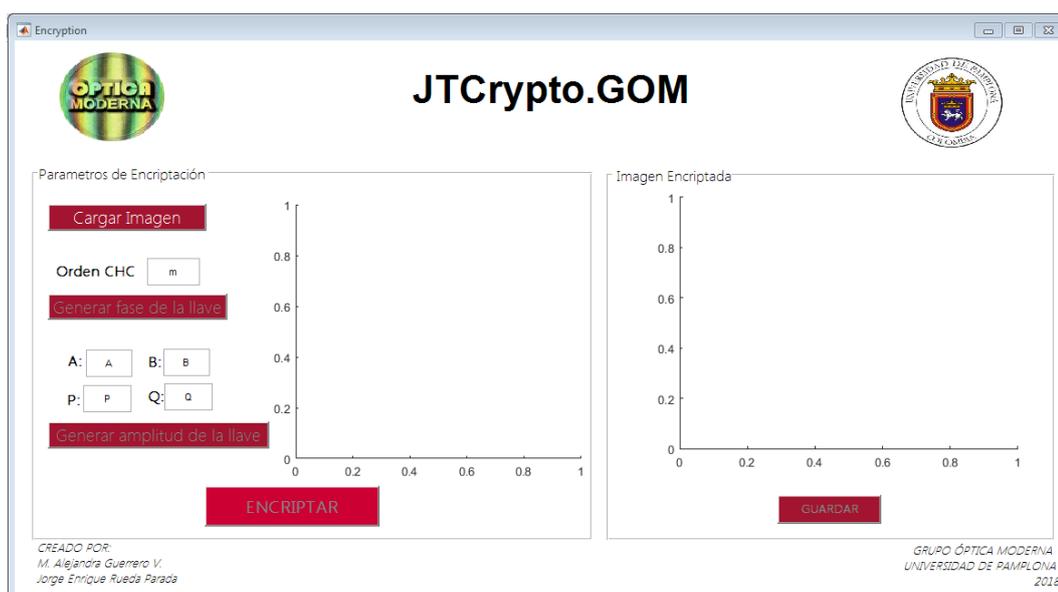
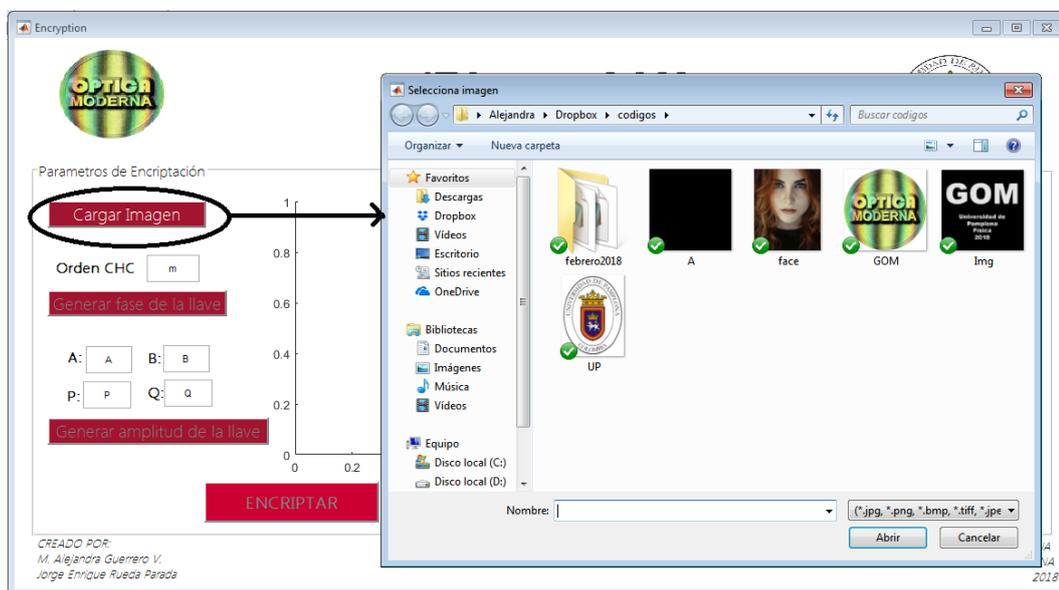


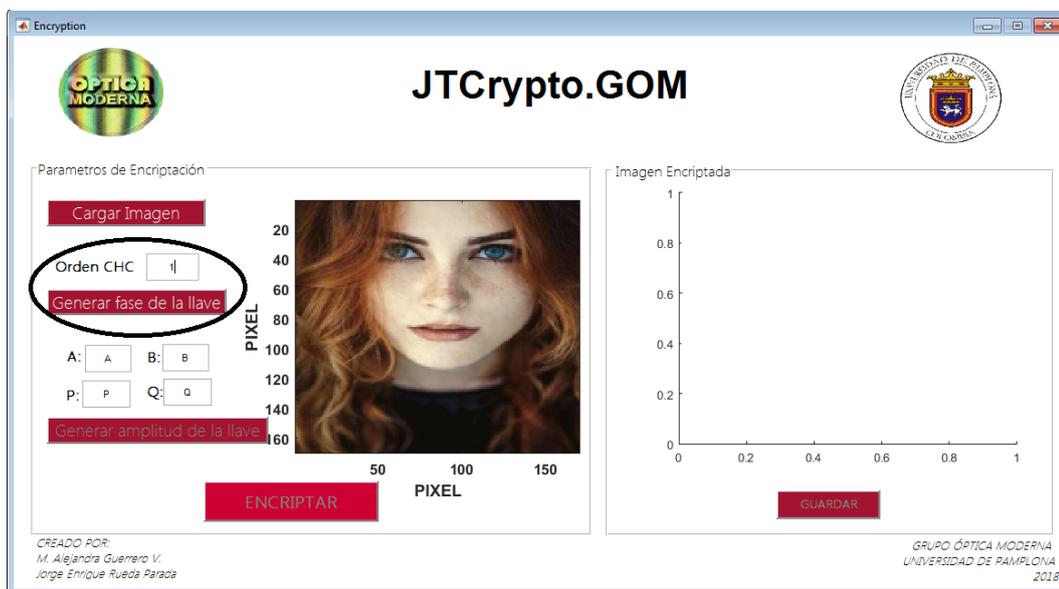
Figura A.2: Ventana Encriptar JTCRYPTO.GOM

1. Botón Cargar Imagen: Permite llamar y visualizar la imagen que se desea encriptar.



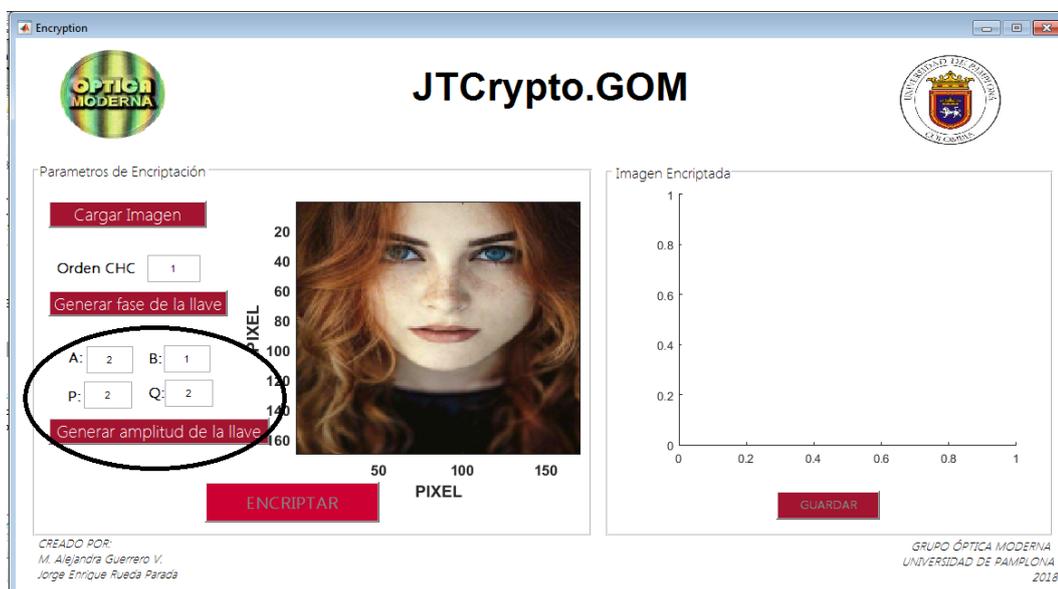
**Figura A.3:** Ventana Encriptar; proceso cargar imagen

2. Botón Generar fase de la llave: Genera la fase de la llave en componentes armónicas circulares con el orden de la descomposición ingresado por teclado;



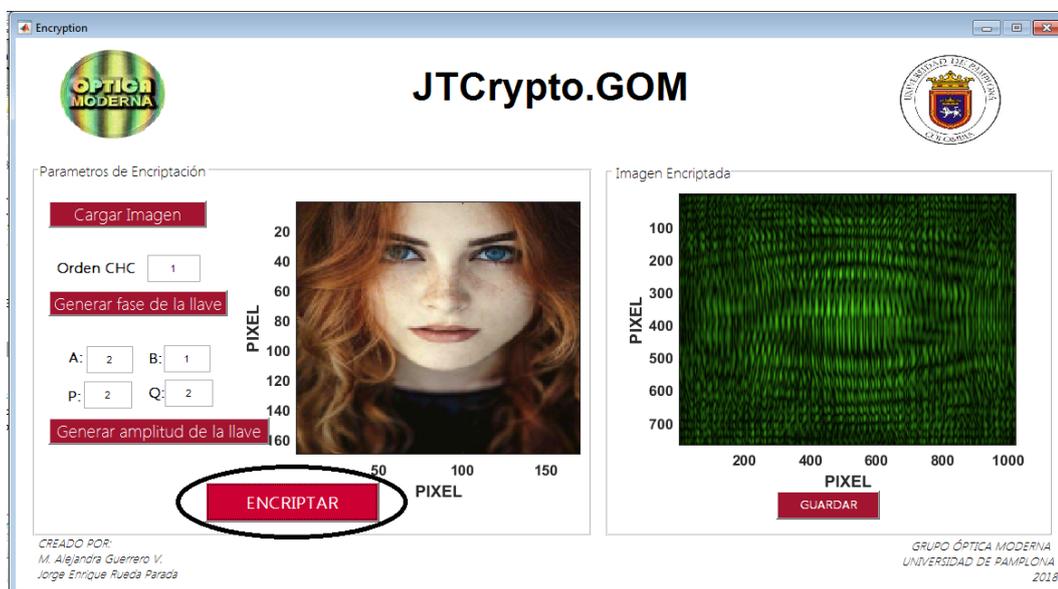
**Figura A.4:** Ventana Encriptar; proceso generar llave de fase

3. Botón generar amplitud de la llave: Genera una distribución de amplitud periódica teniendo en cuenta los parámetros ingresados;



**Figura A.5:** Ventana Encriptar; proceso generar llave de amplitud

4. El botón Encriptar permite encriptar la imagen y visualizarla.

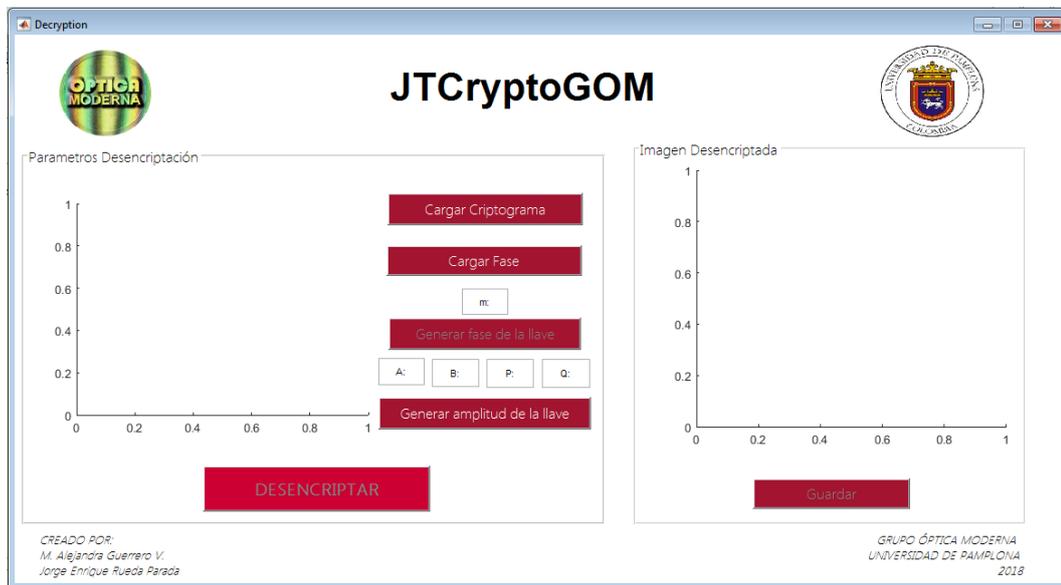


**Figura A.6:** Ventana Encriptar; proceso Encriptar

5. El botón Guardar permite guardar la imagen encriptada en formato \*.mat, la fase de la llave como un archivo \*.mat. y almacena los parámetros de la máscara en un archivo \*.txt.

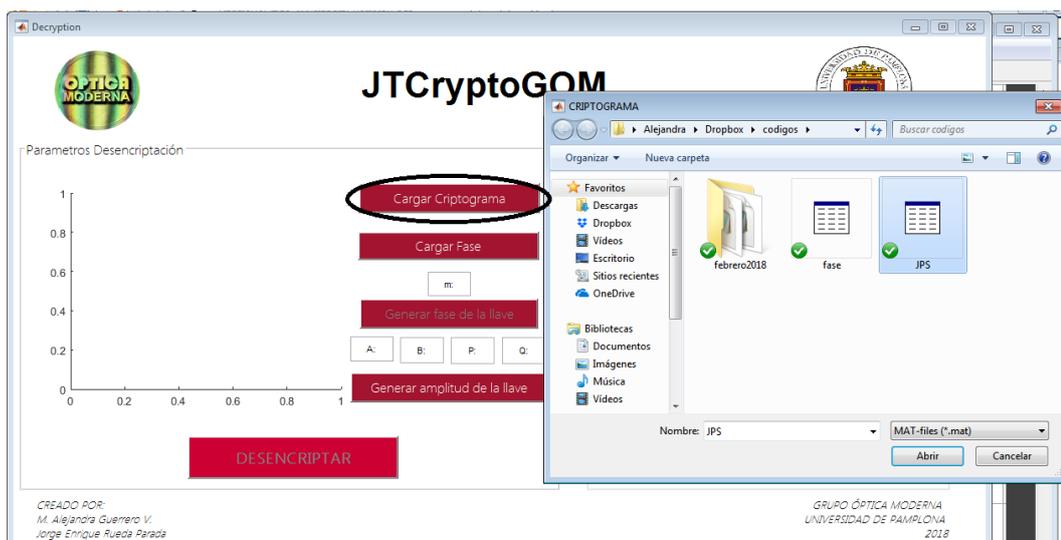
## A.2 DESCRIPCIÓN DE LA VENTANA DE DESENCRIPTACIÓN:

El segundo botón del menú (Figura A.1) nos lleva a una segunda ventana, donde se realizará el proceso de descryptación de la información.



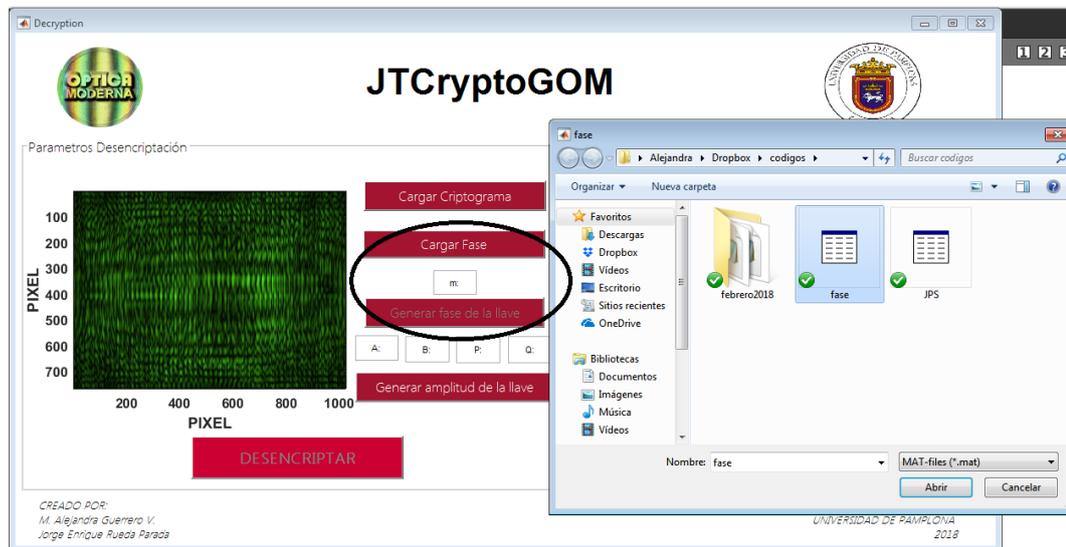
**Figura A.7:** Ventana descryptar

1. Botón Cargar Criptograma: permite llamar el archivo de la imagen encriptada (JPS.mat) y visualizarla.



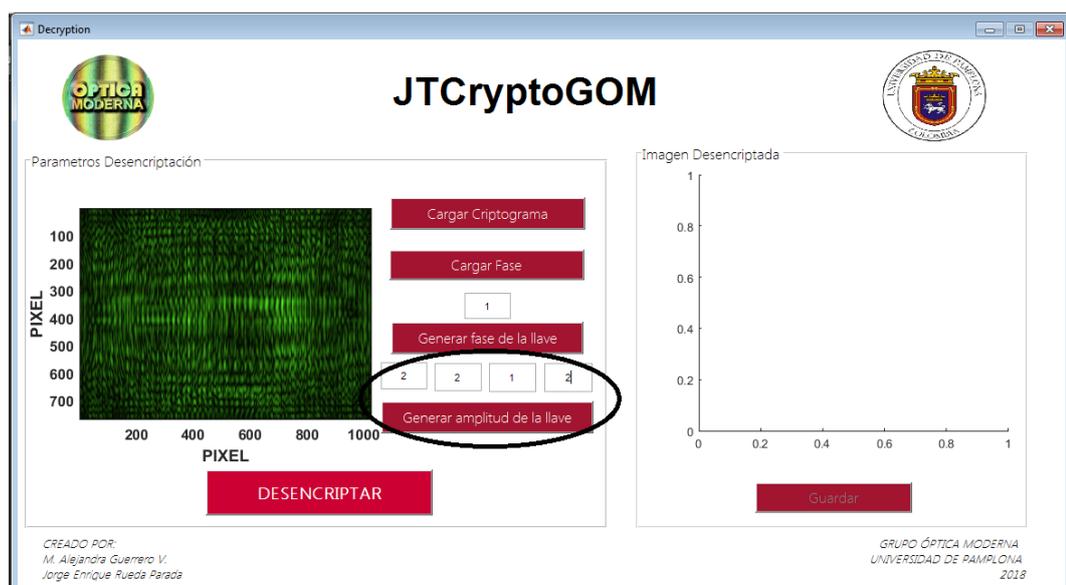
**Figura A.8:** Ventana descryptar; proceso cargar criptograma

2. Botón Cargar Fase: permite cargar el archivo \*.mat de la fase de la llave.
3. Botón Generar fase de la llave: Genera la descomposición en armónicos circulares usando los valores de fase cargados y el orden de la descomposición ingresado por el usuario, este debe corresponder al mismo valor usado en la encriptación.



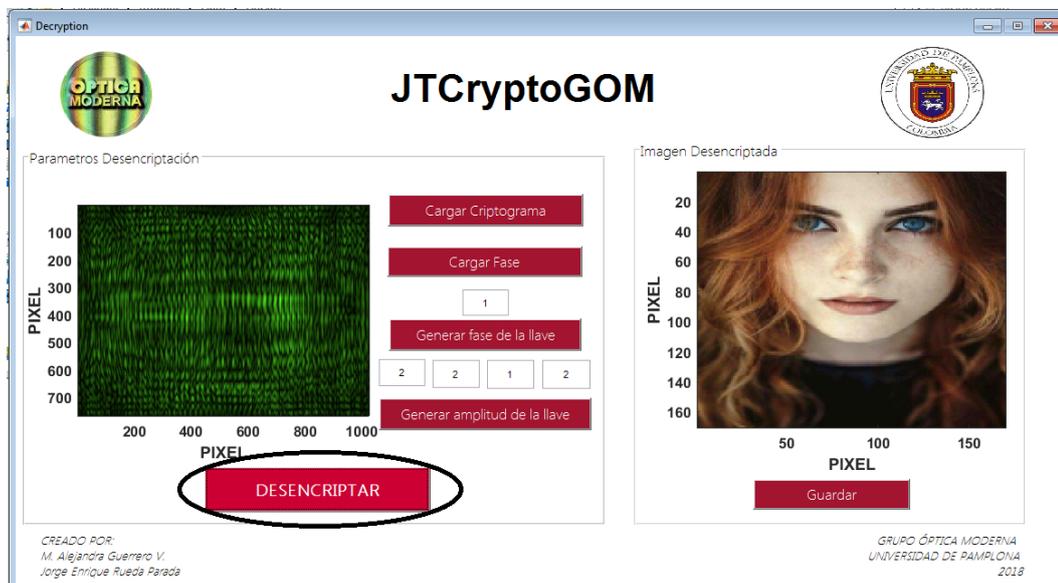
**Figura A.9:** Ventana desenscriptar; proceso generar llave de fase

4. Panel Generar amplitud de la llave: Permite generar la distribución de amplitud periódica ingresando los mismos parámetros usados en el proceso de encriptación.



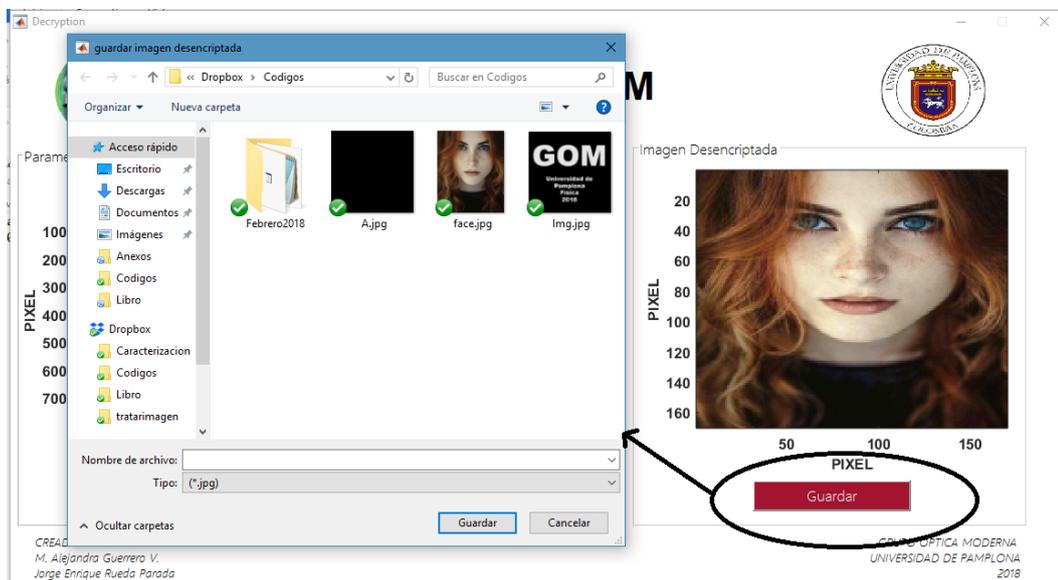
**Figura A.10:** Ventana desenscriptar; proceso generar llave de amplitud

5. Botón Desencriptar: permite desencriptar la imagen encriptada y visualizarla.



**Figura A.11:** Ventana desencriptar; proceso desencriptar

6. Botón Guardar Desencriptada: permite guardar la imagen desencriptada en cualquier formato de imagen.

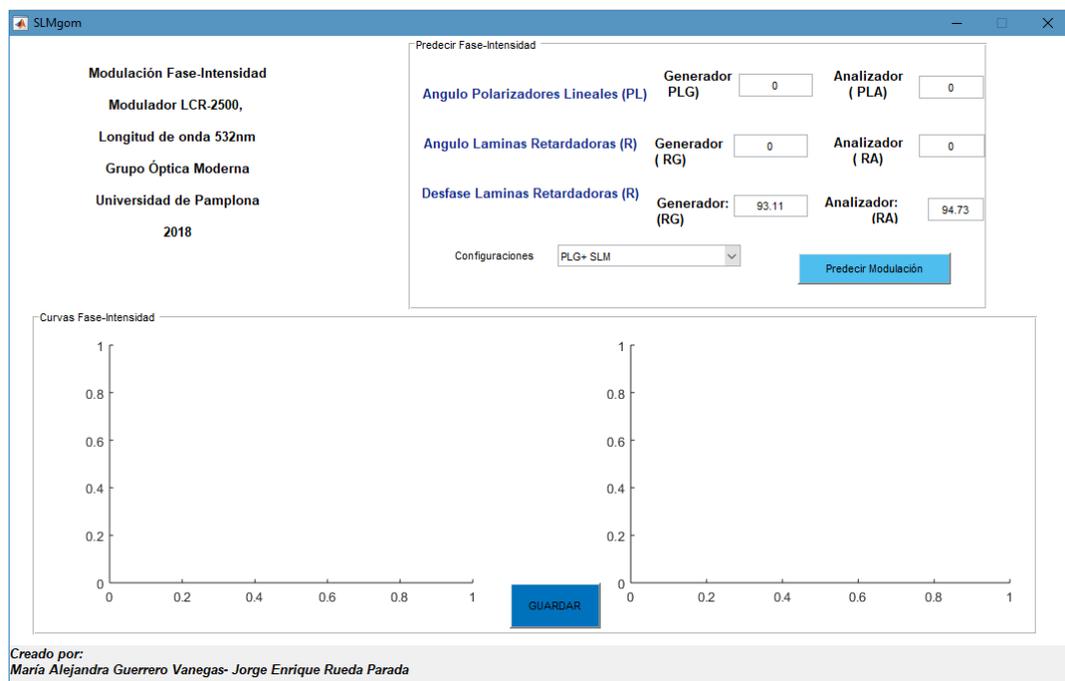


**Figura A.12:** Ventana desencriptar; proceso guardar

# Anexo B

## MANUAL DE USUARIO SLM.GOM

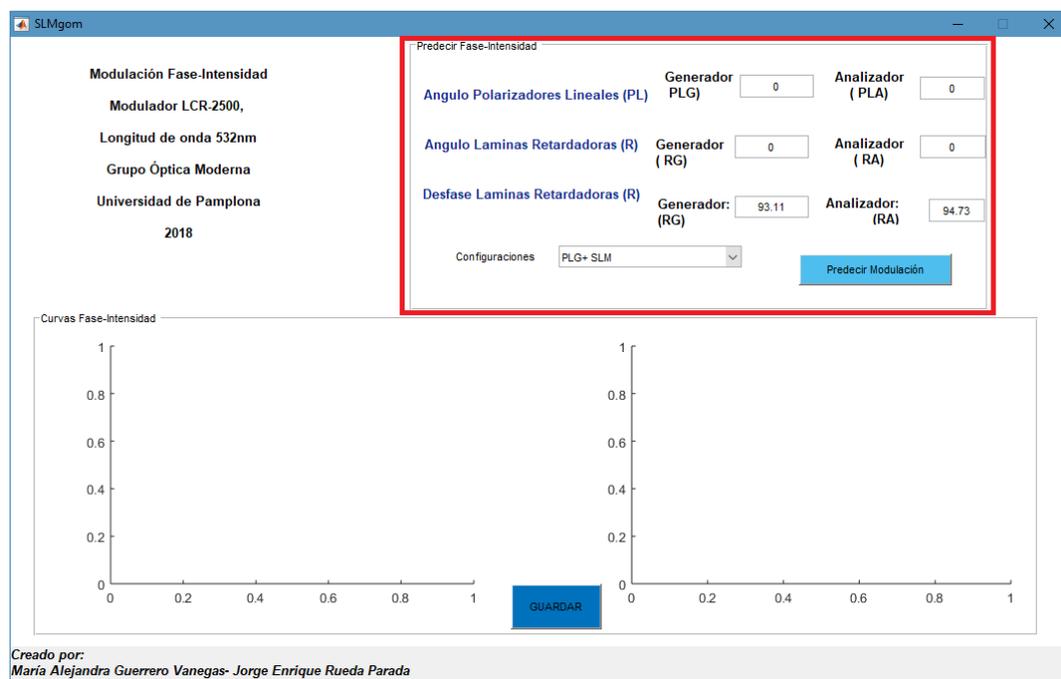
SLM.GOM es una interfaz gráfica desarrollada como producto del proceso de caracterización del modulador de cristal líquido LCR-2500. La interfaz permite predecir la respuesta en fase e intensidad que tendrá la pantalla de cristal líquido de acuerdo a la configuración de elementos polarizantes escogidos.



**Figura B.1:** Ventana interface SLM.GOM

La interfaz gráfica consta de 3 paneles: Predecir Fase-Intensidad, Buscar Modulación Fase-Intensidad, Curvas Fase-Intensidad.

## B.1 DESCRIPCIÓN DEL PANEL PREDECIR FASE-INTENSIDAD:

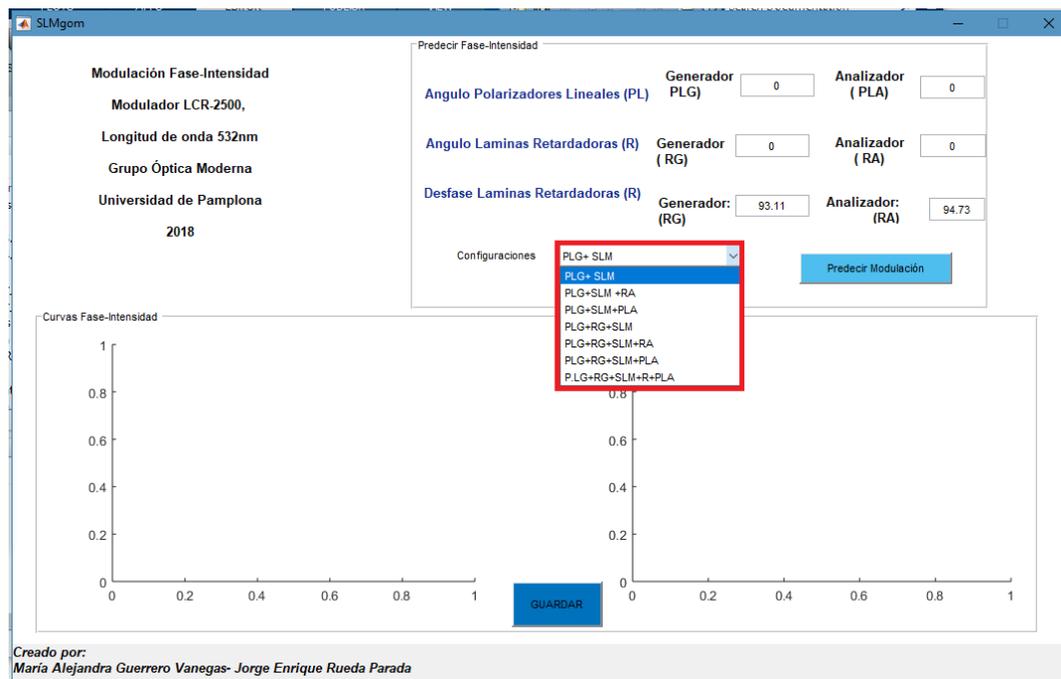


**Figura B.2:** Ventana interfaz SLM.GOM; panel Predecir Fase-Intensidad

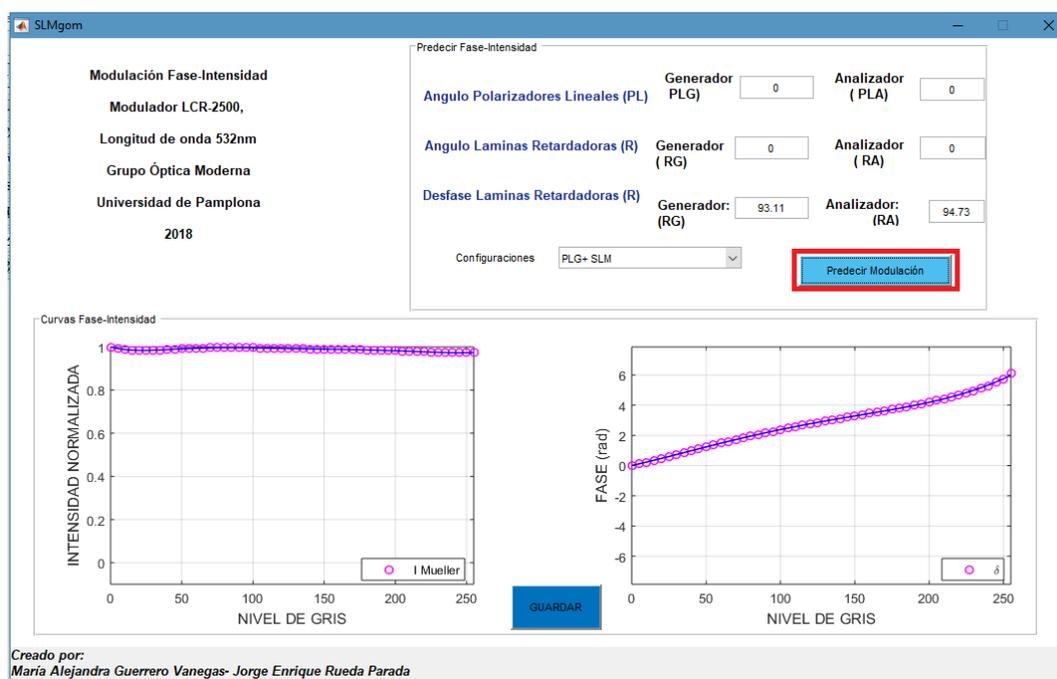
El panel Predecir Fase-Intensidad permite elegir la configuración de elementos polarizantes usados en el arreglo óptico e introducir sus características, orientación del eje óptico y desfase introducido por las Láminas retardadoras. El software permite seleccionar una configuración entre 7 combinaciones posibles.

En la interfaz PL significa polarizador lineal, R Lámina retardadora y SLM representa el modulador de cristal líquido. Los sigla de cada elemento va acompañado de una G (Generador) o una A (Analizador), según sea su ubicación en el arreglo óptico.

El botón "Predecir Modulación" genera las curvas de Fase en función del nivel de gris y de intensidad en función del nivel de gris, para la configuración seleccionada. Las gráficas se visualizaran en el panel curvas fase-intensidad.



(a) Proceso seleccionar configuración



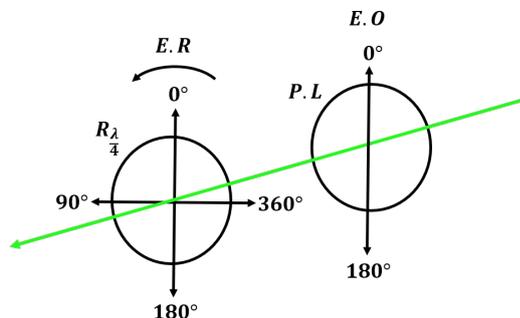
(b) Proceso predecir modulación

**Figura B.3:** Ventana interfaz SLM.GOM; panel Buscar Modulación Fase-Intensidad

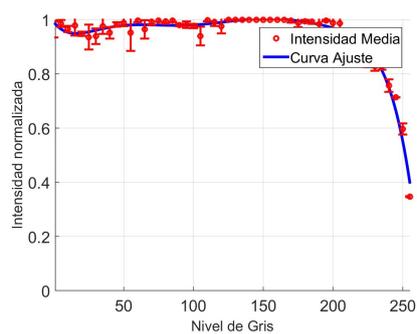
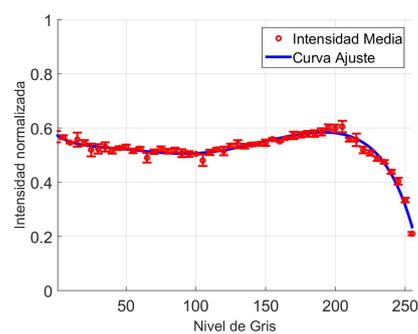
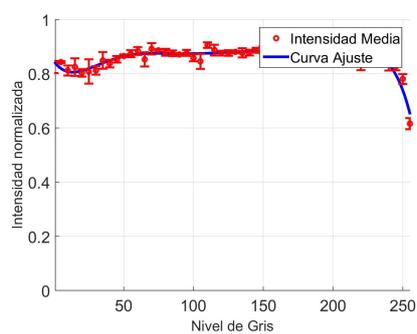
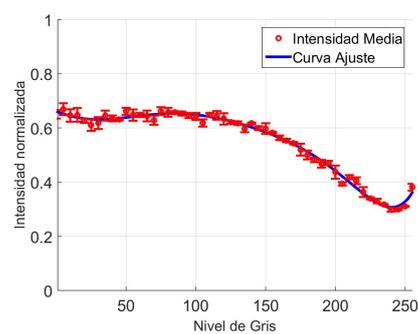
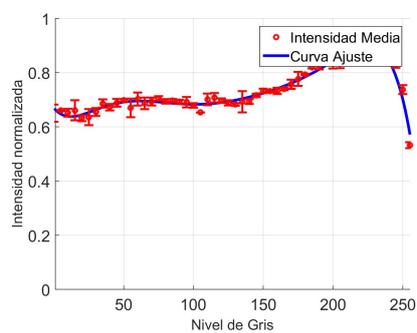
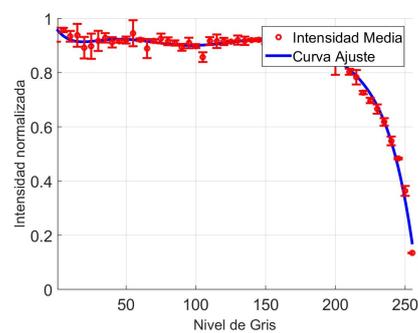
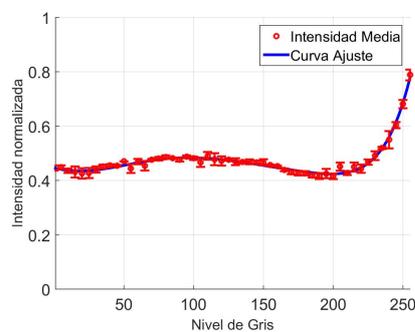
# Anexo C

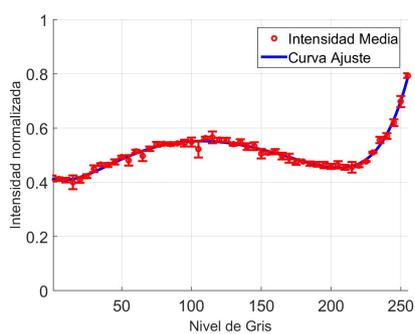
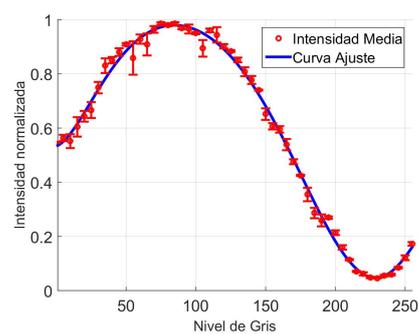
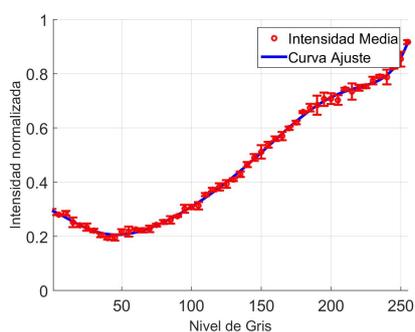
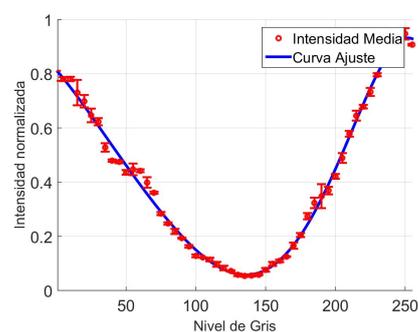
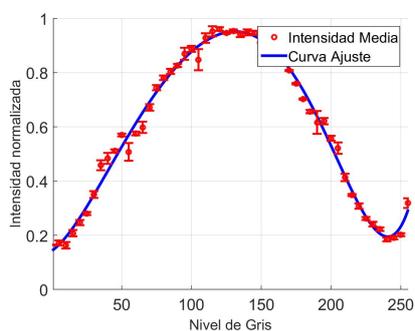
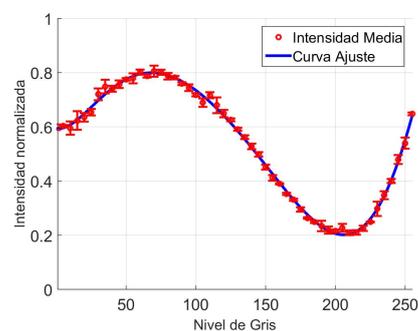
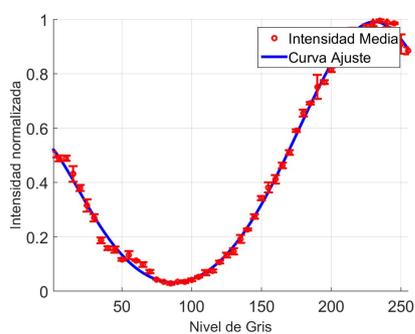
## CARACTERIZACIÓN MODULADOR LCR 2500: GRAFICAS DE INTENSIDAD

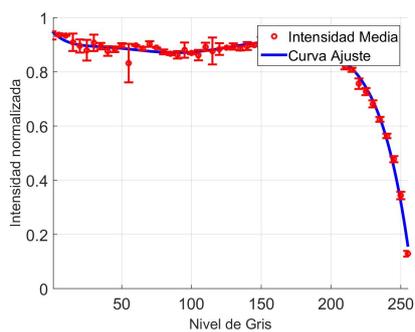
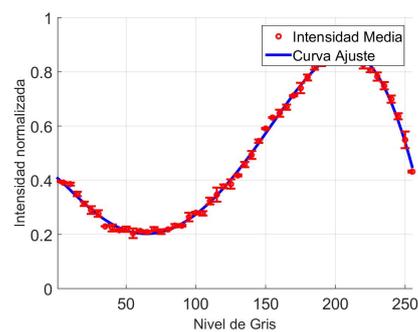
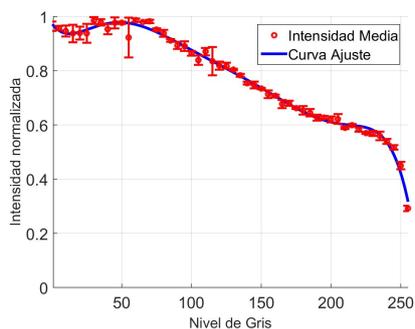
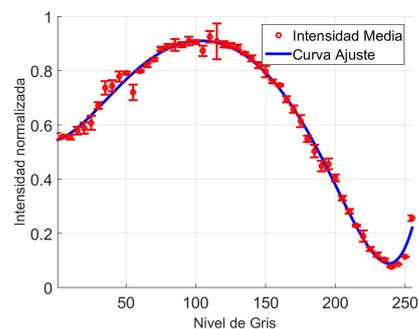
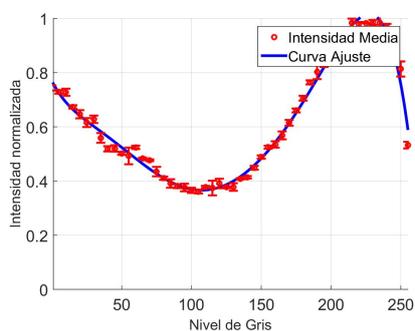
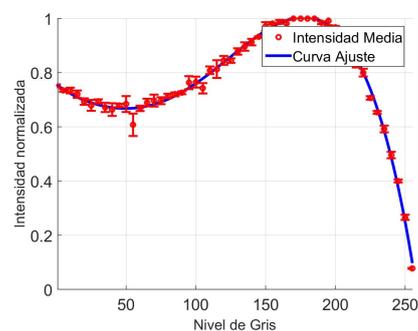
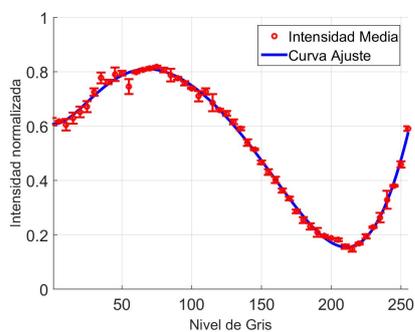
Las gráficas presentadas corresponden a la intensidad en función del nivel de gris, tomada para cada rotación de la Lámina retardadora del sistema analizador en el proceso de caracterización de la pantalla de cristal líquido LCR 2500. Se tomaron 7 medidas de intensidad en función del nivel de gris para cada estado de polarización generado. Los estados de polarización se generaron rotando una Lámina retardadora cuarto de onda del sistema generador a un paso de  $52^\circ$ , generándose 7 estados diferentes. El eje óptico de todos los dispositivos fue alineado al eje vertical, la convención de rotación fue girar los dispositivos en el sentido contrario a las manecillas del reloj, como se muestra en la gráfica. La intensidad fue medida en un sensor de potencia, Laser Power Meter, midiendo intensidades del orden de los microwatts, las intensidades en las gráficas presentadas fueron normalizadas.

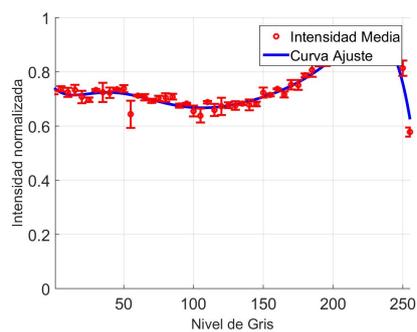
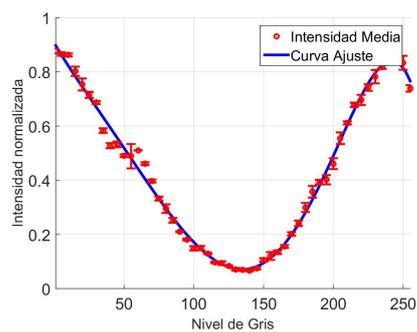
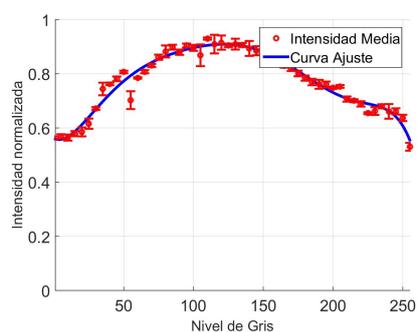
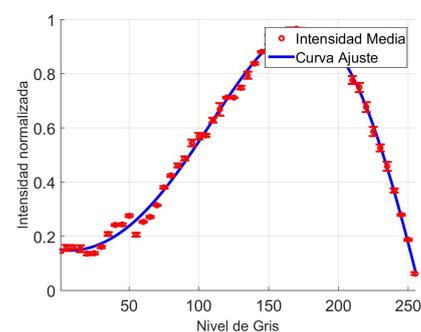
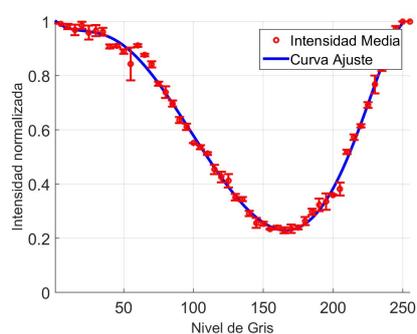
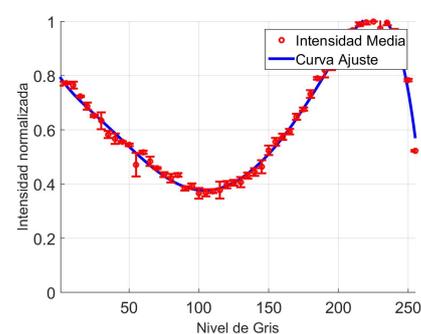
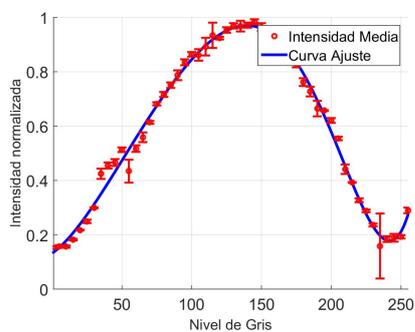


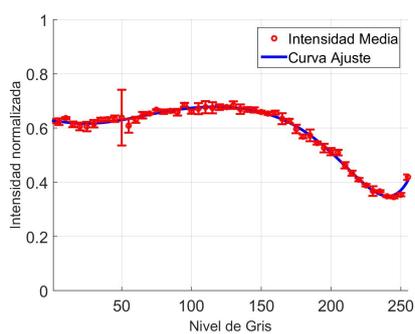
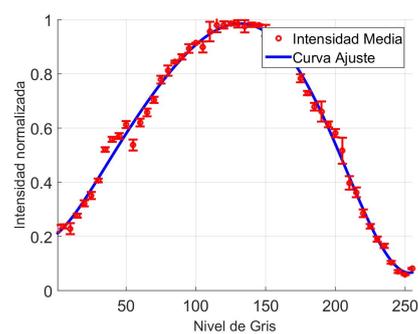
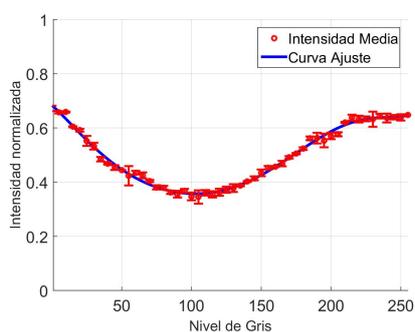
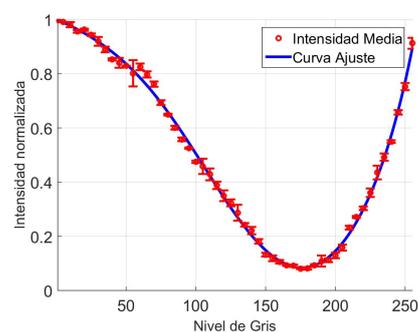
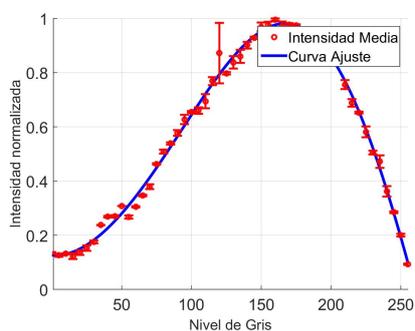
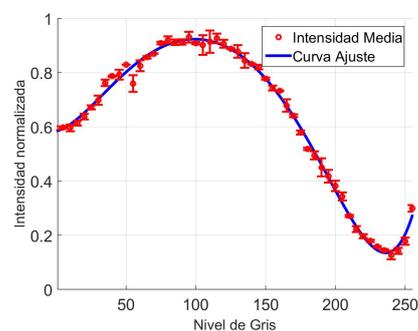
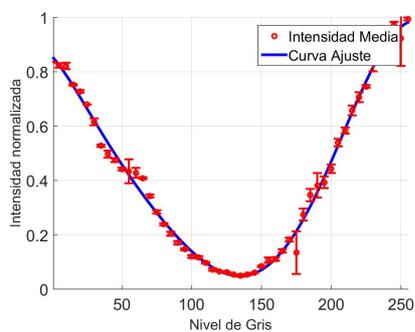
**Figura C.1:** Sistema de medida de intensidades-Polarimetro de Mueller.  $PL$ : Polarizador lineal;  $R_{\lambda/4}$ : Retardador de cuarto de onda;  $E.O$ : Eje Óptico;  $E.R$ : Eje Rápido. La flecha verde representa la dirección de propagación del haz.

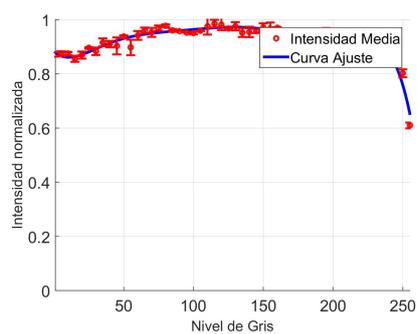
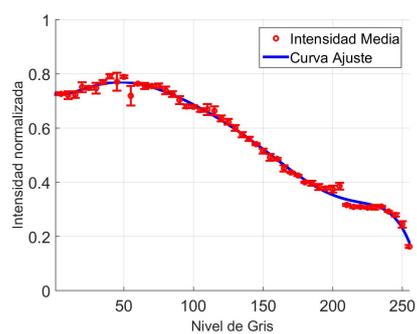
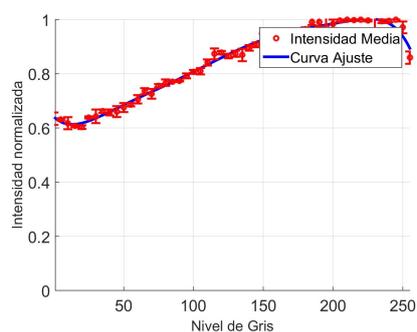
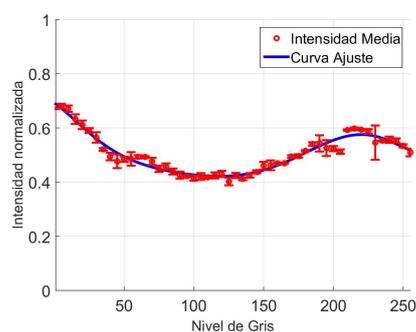
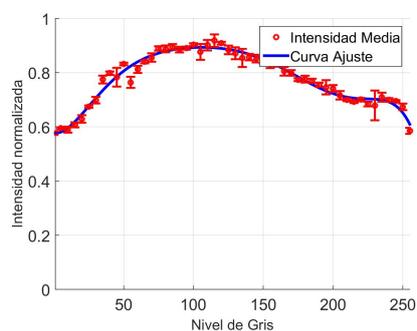
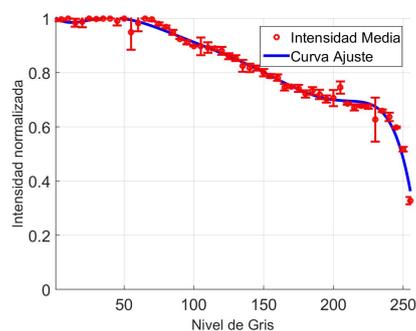
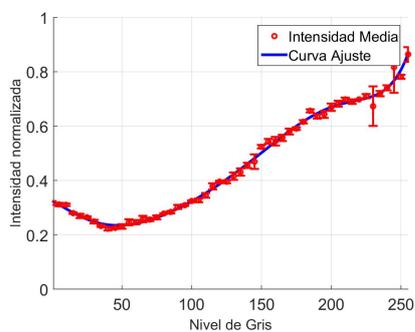
(a) Lámina Analizadora  $\theta_r = 0^\circ$ (b) Lámina Analizadora  $\theta_r = 52^\circ$ (c) Lámina Analizadora  $\theta_r = 103^\circ$ (d) Lámina Analizadora  $\theta_r = 155^\circ$ (e) Lámina Analizadora  $\theta_r = 206^\circ$ (f) Lámina Analizadora  $\theta_r = 258^\circ$ (g) Lámina Analizadora  $\theta_r = 310^\circ$ **Figura C.2:** Ángulo Lámina Generadora= $0^\circ$

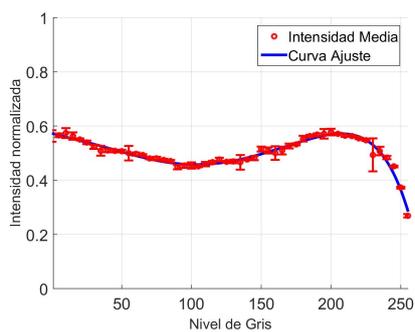
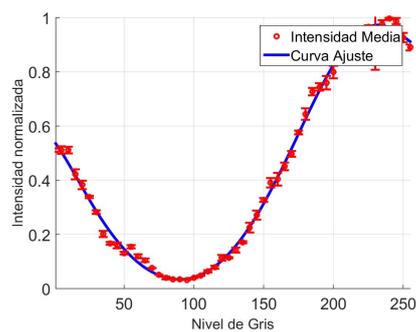
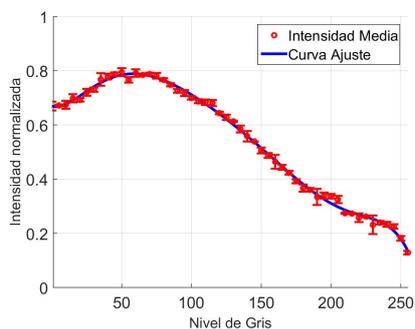
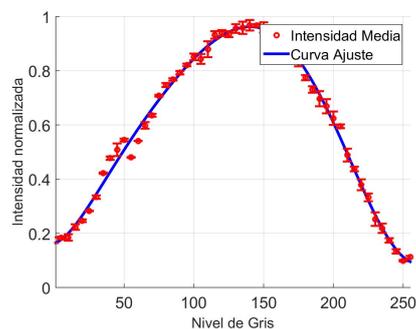
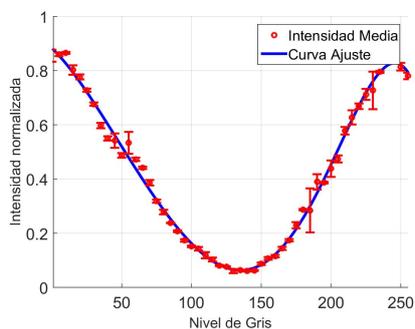
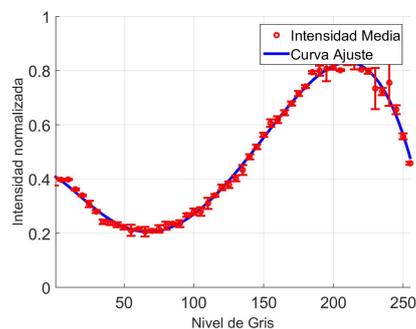
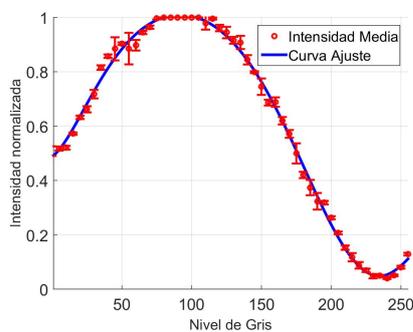
(a) Lámina Analizadora  $\theta_r = 0^\circ$ (b) Lámina Analizadora  $\theta_r = 52^\circ$ (c) Lámina Analizadora  $\theta_r = 103^\circ$ (d) Lámina Analizadora  $\theta_r = 155^\circ$ (e) Lámina Analizadora  $\theta_r = 206^\circ$ (f) Lámina Analizadora  $\theta_r = 258^\circ$ (g) Lámina Analizadora  $\theta_r = 310^\circ$ **Figura C.3:** Ángulo Lámina Generadora= $52^\circ$

(a) Lámina Analizadora  $\theta_r = 0^\circ$ (b) Lámina Analizadora  $\theta_r = 52^\circ$ (c) Lámina Analizadora  $\theta_r = 103^\circ$ (d) Lámina Analizadora  $\theta_r = 155^\circ$ (e) Lámina Analizadora  $\theta_r = 206^\circ$ (f) Lámina Analizadora  $\theta_r = 258^\circ$ (g) Lámina Analizadora  $\theta_r = 310^\circ$ **Figura C.4:** Ángulo Lámina Generadora= $103^\circ$

(a) Lámina Analizadora  $\theta_r = 0^\circ$ (b) Lámina Analizadora  $\theta_r = 52^\circ$ (c) Lámina Analizadora  $\theta_r = 103^\circ$ (d) Lámina Analizadora  $\theta_r = 155^\circ$ (e) Lámina Analizadora  $\theta_r = 206^\circ$ (f) Lámina Analizadora  $\theta_r = 258^\circ$ (g) Lámina Analizadora  $\theta_r = 310^\circ$ **Figura C.5:** Ángulo Lámina Generadora= $155^\circ$

(a) Lámina Analizadora  $\theta_r = 0^\circ$ (b) Lámina Analizadora  $\theta_r = 52^\circ$ (c) Lámina Analizadora  $\theta_r = 103^\circ$ (d) Lámina Analizadora  $\theta_r = 155^\circ$ (e) Lámina Analizadora  $\theta_r = 206^\circ$ (f) Lámina Analizadora  $\theta_r = 258^\circ$ (g) Lámina Analizadora  $\theta_r = 310^\circ$ **Figura C.6:** Ángulo Lámina Generadora= $206^\circ$

(a) Lámina Analizadora  $\theta_r = 0^\circ$ (b) Lámina Analizadora  $\theta_r = 52^\circ$ (c) Lámina Analizadora  $\theta_r = 103^\circ$ (d) Lámina Analizadora  $\theta_r = 155^\circ$ (e) Lámina Analizadora  $\theta_r = 206^\circ$ (f) Lámina Analizadora  $\theta_r = 258^\circ$ (g) Lámina Analizadora  $\theta_r = 310^\circ$ **Figura C.7:** Ángulo Lámina Generadora= $258^\circ$

(a) Lámina Analizadora  $\theta_r = 0^\circ$ (b) Lámina Analizadora  $\theta_r = 52^\circ$ (c) Lámina Analizadora  $\theta_r = 103^\circ$ (d) Lámina Analizadora  $\theta_r = 155^\circ$ (e) Lámina Analizadora  $\theta_r = 206^\circ$ (f) Lámina Analizadora  $\theta_r = 258^\circ$ (g) Lámina Analizadora  $\theta_r = 310^\circ$ **Figura C.8:** Ángulo Lámina Generadora= $310^\circ$