

Universidad Nacional de la Plata

Facultad de Ciencias Exactas

Departamento de Física



**Optimización de técnicas ópticas de
seguridad. Procesos dinámicos de
encriptación**

TESIS DOCTORAL
Edward Fabián Mosso Solano
Junio de 2012

Universidad Nacional de la Plata

Facultad de Ciencias Exactas

Departamento de Física



Tesis para optar al grado de Doctor

Presentada por:

Edward Fabián Mosso Solano

Director: Dr. Néstor Bolognini
Codirector: Dra. Myrian Tebaldi

Junio de 2012

Ami hija Valery

Agradecimientos

Realmente es complicado mencionar todas aquellas personas que en mayor o menor medida ayudaron a materializar esta Tesis. Me disculpo por las posibles omisiones y nombraré a quienes han influido positivamente en esta etapa de mi vida.

Mi más sincero agradecimiento al Dr. Néstor Bolognini y a la Dra. Myrian Tebaldi por su ardua labor al dirigir este trabajo. Su orientación, apoyo, opinión objetiva, confianza y respaldo incondicional han sido fundamentales para culminarlo. Absorbí una ínfima parte de su vasto conocimiento lo que ayudo a mi crecimiento personal y profesional. Siempre estaré muy agradecido.

Al Dr. Jorge Tocho y al Dr. Marcelo Trivi, Autoridades del Centro de Investigaciones Ópticas (CIOP), les agradezco la oportunidad de realizar este trabajo en la Institución.

Le agradezco de forma especial al Dr. Roberto Torroba que siempre tuvo la mejor disposición para aclararme conceptos, discutir y desarrollar ideas. De igual forma, sus enseñanzas y pensamientos ayudaron a mi crecimiento profesional y personal.

Un agradecimiento a los viejos y nuevos integrantes de la línea de investigación Alberto, Gustavo, Dafne, Luisa, Daniel, todos ellos dispuestos a colaborar con sus conocimientos. Agradezco en especial a la vieja guardia, Gustavo, Dafne y Alberto quienes muy amablemente me resolvieron cualquier inquietud del momento o colaboraron con alguna labor en particular. De igual forma agradezco a todos los buenos momentos compartidos.

Agradezco a todo el personal del Centro de Investigaciones Ópticas (CIOp). Investigadores, (especialmente quienes desarrollan su labor en el entrepiso), Profesionales, Becarios, Técnicos y Administrativos. Su cordialidad y ayuda siempre facilitaron mi labor dentro de la institución.

Al Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET) por otorgarme una Beca Doctoral Tipo I y Tipo II con Países Latinoamericanos.

Un agradecimiento personal a Jesica, Ángela, Lorena, Cristian y Fredy por los momentos compartidos, sus buenos consejos y la motivación que siempre me inyectaron durante estos años.

A Antonia y Pocho (QPD) que me acogieron y me trataron como un miembro más de su Familia, mis sinceros agradecimientos.

A mi Familia en general que siempre ha estado pendiente de mi bienestar (Ti@s, Prim@s y demás Familiares), muchas gracias.

Jamás terminaré de agradecerle a mi madre Fabiola y mis hermanos, Alexander y Julián. Su apoyo incondicional me ha brindado el respaldo necesario para seguir adelante en todos los aspectos de mi vida. He adquirido de ellos sus buenos valores y no tienen responsabilidad sobre mis muchos defectos. Este es un logro más que se lo debo íntegramente a ellos.

A Alied, le agradezco su comprensión y apoyo diario. Su presencia en mi vida ha sido fundamental para alcanzar esta meta que es para el bien común y de nuestra hija. También le doy gracias a sus padres y hermanos por el apoyo cotidiano.

Al igual que el resto de mi ser, estas últimas líneas son de mi hija Valery. Desde su primer instante de vida fue mi principal motivación para salir avante. Su sonrisa a la distancia no me dejó desfallecer en algunos momentos de soledad. A ella le dedico especialmente este trabajo.

A todos, muchas gracias.

La Plata, Junio de 2012

Contenidos

| | | |
|----------|---|-----------|
| 1 | Introducción general..... | 1 |
| 1.1 | Motivaciones y objetivos..... | 1 |
| 1.2 | Esquema general..... | 8 |
| 1.3 | Bibliografía..... | 10 |
| 2 | Técnicas ópticas de encriptación..... | 13 |
| 2.1 | Introducción..... | 13 |
| 2.2 | Sistema de encriptación de doble máscara de fase en configuración $4f$ | 14 |
| 2.3 | Sistema de encriptación con registro en memorias holográficas..... | 17 |
| 2.4 | Otras arquitecturas de encriptación óptica..... | 21 |
| 2.4.1 | Sistema de encriptación de doble máscara de fase basado en un correlador de transformada conjunta JTC | 21 |
| 2.4.2 | Sistema de encriptación de doble máscara de fase en el dominio de Fresnel..... | 25 |
| 2.5 | Sistemas ópticos-digitales en la encriptación..... | 27 |
| 2.6 | Bibliografía..... | 30 |
| 3 | Sistemas ópticos virtuales en el procesamiento de información..... | 37 |
| 3.1 | Introducción..... | 37 |
| 3.2 | Representación discreta del proceso de propagación en el espacio libre.... | 40 |
| 3.2.1 | Espectro angular de ondas planas..... | 41 |
| 3.2.2 | Aproximaciones del principio de Huygens-Fresnel..... | 43 |
| 3.2.2.1 | Aproximación de Fresnel..... | 43 |
| 3.2.2.2 | Aproximación de Fraunhofer..... | 45 |
| 3.2.3 | Implementación del espectro angular de ondas planas usando la transformada rápida de Fourier (FFT)..... | 46 |
| 3.2.4 | Implementación de la integral de Fresnel usando la transformada rápida de Fourier (FFT)..... | 50 |
| 3.3 | Implementación de elementos ópticos virtuales..... | 52 |
| 3.3.1 | Lente óptica virtual..... | 53 |

| | | |
|----------|---|------------|
| 3.3.2 | Pupilas ópticas..... | 54 |
| 3.3.3 | Red de amplitud sinusoidal..... | 56 |
| 3.3.4 | Difusores virtuales..... | 56 |
| 3.4 | Sistemas ópticos virtuales y su aplicación en sistemas de difracción e interferencia..... | 58 |
| 3.4.1 | Propagación en el espacio libre..... | 60 |
| 3.4.2 | Transformada óptica de Fourier..... | 62 |
| 3.4.3 | Sistema formador de imágenes..... | 64 |
| 3.4.4 | Difracción de una red de amplitud sinusoidal..... | 66 |
| 3.4.5 | Distribuciones de <i>speckle</i> | 68 |
| 3.4.6 | Distribuciones de <i>speckle</i> moduladas..... | 70 |
| 3.5 | Implementación de un sistema de encriptación en configuración $4f$ en SOV..... | 74 |
| 3.6 | Bibliografía..... | 76 |
| 4 | Multiplexado de información encriptada en un medios de registro planos. | 81 |
| 4.1 | Introducción..... | 81 |
| 4.2 | Multiplexado de información..... | 85 |
| 4.2.1 | Multiplexado de imágenes encriptadas en un sistema $4f$ | 85 |
| 4.3 | Solapamiento de información recuperada..... | 89 |
| 4.3.1 | Solapamiento de información recuperada correctamente..... | 90 |
| 4.3.2 | Solapamiento de información recuperada incorrectamente..... | 93 |
| 4.4 | Deterioro de la información recuperada a partir de un multiplexado de imágenes encriptadas..... | 97 |
| 4.5 | Técnica de modulación theta..... | 107 |
| 4.5.1 | Composición de color..... | 111 |
| 4.5.2 | Multiplexado de información..... | 116 |
| 4.6 | Bibliografía..... | 118 |
| 5 | Técnica de encriptación de eventos dinámicos..... | 123 |
| 5.1 | Introducción..... | 123 |
| 5.2 | Sistema de encriptación de eventos dinámicos en arquitectura $4f$ | 125 |
| 5.2.1 | Etapas de Encriptación..... | 125 |
| 5.2.2 | Etapas de modulación..... | 127 |
| 5.2.3 | Etapas de Multiplexado..... | 128 |
| 5.2.4 | Etapas de sincronización y filtrado secuencial..... | 129 |
| 5.2.5 | Etapas de desencriptación..... | 132 |
| 5.3 | Consideraciones generales de implementación..... | 134 |
| 5.3.1 | Extensión finita de las lentes en un SOV..... | 134 |
| 5.3.2 | Escalamiento del objeto para su modulación..... | 136 |

| | | |
|----------|--|------------|
| 5.3.3 | Optimización de las redes de modulación..... | 139 |
| 5.5 | Comentarios sobre la seguridad del sistema..... | 142 |
| 5.4 | Bibliografía..... | 144 |
| 6 | Técnica de encriptación de eventos dinámicos: Aplicaciones..... | 145 |
| 6.1 | Introducción..... | 145 |
| 6.2 | Encriptación de escenas dinámicas monocromáticas..... | 146 |
| 6.2.1 | Descripción general..... | 147 |
| 6.2.2 | Descripción del método..... | 148 |
| 6.2.3 | Discusión de resultados..... | 154 |
| 6.3 | Encriptación de escenas dinámicas policromáticas..... | 163 |
| 6.3.1 | Descripción general..... | 164 |
| 6.3.2 | Descripción del método..... | 162 |
| 6.3.3 | Discusión de resultados..... | 170 |
| 6.4 | Aplicación de la técnica de encriptación de eventos dinámicos a un proceso multiusuario..... | 181 |
| 6.4.1 | Descripción general..... | 182 |
| 6.4.2 | Descripción del método..... | 183 |
| 6.4.3 | Discusión de resultados..... | 186 |
| 6.5 | Bibliografía..... | 190 |
| 7 | Generación de llaves de seguridad para técnicas de codificación óptica..... | 193 |
| 7.1 | Introducción..... | 193 |
| 7.2 | Transformaciones geométricas en coordenadas homogéneas..... | 197 |
| 7.3 | Representación matricial de transformaciones afines..... | 200 |
| 7.3.1 | Transformación de traslación..... | 200 |
| 7.3.2 | Transformación de reflexión..... | 202 |
| 7.3.3 | Transformación de rotación..... | 202 |
| 7.3.4 | Transformación de contracción o escalamiento..... | 203 |
| 7.3.5 | Transformación de <i>shearing</i> | 204 |
| 7.4 | Generación de imágenes pseudoaleatorias..... | 205 |
| 7.4.1 | Sensibilidad de las imágenes $I_{at}^{(N)}$ ante la pérdida de información de pixeles de la imagen fuente..... | 211 |
| 7.4.2 | Sensibilidad de las imágenes $I_{at}^{(N)}$ al usar una imagen fuente restaurada..... | 215 |
| 7.4.3 | Sensibilidad de las imágenes $I_{at}^{(N)}$ al usar una imagen fuente con ruido speckle..... | 217 |
| 7.4.4 | Sensibilidad de las imágenes $I_{at}^{(N)}$ al usar una imagen fuente transmitida en formato comprimido..... | 219 |

| | | |
|----------|--|------------|
| 7.5 | Aleatoriedad de las imágenes generadas en el PGI_{at} | 222 |
| 7.6 | Encriptación de información usando llaves de seguridad generadas a partir de imágenes $I_{at}^{(N)}$ | 226 |
| 7.7 | Reducción del tamaño las llaves de seguridad transmitidas en un canal de información clásico..... | 231 |
| 7.8 | Bibliografía..... | 237 |
| 8 | Conclusiones y perspectivas | 241 |
| | Apéndice A:Conceptos básicos de holografía digital..... | 249 |
| A.1 | Introducción..... | 249 |
| A.2 | Registro y reconstrucción de un holograma digital..... | 250 |
| A.3 | Bibliografía..... | 255 |
| | Apéndice B: Métricas para el análisis de resultados..... | 257 |
| B.1 | Introducción..... | 257 |
| B.2 | Estimadores estadísticos..... | 258 |
| B.3 | Consideraciones de las métricas aplicadas en los análisis de resultados... | 261 |
| | B.3.1 Promediado radial y angular de intensidades..... | 262 |
| | B.3.2 Correlación cruzada y autocorrelación..... | 263 |
| B.4 | Bibliografía..... | 264 |
| | Apéndice C: Imágenes recuperadas..... | 265 |
| C.1 | Introducción..... | 265 |
| C.2 | Imágenes descriptadas la secuencia monocromática..... | 266 |
| C.3 | Imágenes descriptadas de secuencias policromáticas..... | 268 |
| C.4 | Imágenes descriptadas de un proceso multiusuario..... | 276 |
| | Lista de Publicaciones..... | 279 |

Capítulo 1

Introducción general

1.1 Motivaciones y objetivos

La confidencialidad es una parte integral en las diferentes facetas de cada persona donde las experiencias más cotidianas conllevan muchas veces a exposiciones de información que es de carácter individual. En este sentido, las personas manipulan elementos del común como documentos de identificación, número de seguro social, números de cuentas bancarias, entre otra información que es de uso propio y que sirve para desenvolverse en la sociedad. En este aspecto, la seguridad de la información permite mantener la privacidad del atributo al que hace referencia cada uno de estos elementos personales mientras se emplean como unidades de identificación o uso particular en la vida cotidiana.

En otro contexto, en el campo de la información tecnológica y en las ciencias de las comunicaciones, la seguridad de información se volvió un factor imprescindible tanto para el emisor cuanto para el receptor en un proceso de comunicación. En este sentido, se trata de salvaguardar, transmitir y recuperar datos asegurando un proceso de protección que evita la falsificación y previene la intrusión de personas no autorizadas. Esta línea puede comprender temas muy amplios de la informática como la criptografía, control de acceso, protocolos, software [1.1], etc., temas que se deben dominar para implementar aplicaciones reales de manejo de datos. En esta área los sistemas criptográficos están muy bien establecidos y en un estado muy avanzado de aplicación.

Actualmente, la tendencia global es la miniaturización de los dispositivos así como un incremento de la capacidad de almacenamiento y de procesamiento. Estos elementos apuntan a mejorar las velocidades de transmisión de grandes volúmenes de datos en internet. Frente a estos requerimientos, las tecnologías ópticas se posicionan como principales candidatas para procesar importantes volúmenes de información a velocidades superiores a las manejadas electrónicamente. En términos de seguridad, a estos datos se los debe proteger para mantener su confidencialidad en los procesos de transmisión. Por lo tanto, es de gran interés generar técnicas ópticas optimizadas que cumplan con esta función.

Las comunicaciones digitales y el procesamiento óptico de datos han tenido una estrecha relación. El desarrollo de la ciencia de las comunicaciones y su descripción en la teoría de sistemas y tratamiento de señales establecieron sistemas eficaces para la transmisión de datos. Por otra parte, el rápido desarrollo del láser y del semiconductor permitió acoplar dispositivos ópticos y opto-electrónicos para implementar arquitecturas en el área de las telecomunicaciones ópticas y el procesamiento óptico de información.

Referente a lo anterior, el trabajo realizado por Marechal y Croce [1.2] fue quizás la primera contribución clara de la analogía entre un instrumento óptico formador de imágenes y un sistema de red de comunicaciones. Se dedujo que sus representaciones matemáticas eran las mismas y que los dos dispositivos bajo ciertas condiciones pueden considerarse como sistemas lineales invariantes [1.3]. De esta manera, se estableció que ambos mecanismos servían como medios para llevar, transferir o transformar información en el dominio del espacio o en el dominio del tiempo.

En el campo de la óptica, el esquema introducido por Marechal y Croce hacia principios de los años cincuenta [1.2], conocido hoy como el sistema $4f$ [1.4], [1.5], es la arquitectura más directa para realizar procesamiento óptico de información. Este arreglo experimental de simple descripción matemática es el arreglo básico más usado para realizar procesados ópticos coherentes referentes a las experiencias de filtrado espacial, reconocimiento de patrones, correlación óptica, etc. Estas aplicaciones se basan en

variaciones de los elementos involucrados en cualquiera de los tres planos principales del sistema $4f$: plano de entrada, de frecuencias y de salida.

El mayor atractivo que presentan los sistemas ópticos sobre los sistemas electrónicos es el gran volumen de información compleja (amplitud y fase) que pueden procesar en paralelo y transmitir a velocidades muy grandes. Además, el uso de materiales fotosensibles de alta resolución permite que dicha información pueda ser almacenada en materiales de registro de pequeñas dimensiones. Usufructuando estas características, por varias décadas los investigadores han dedicado sus mayores esfuerzos en implementar arquitecturas de procesamiento óptico de información teniendo presente los aspectos fundamentales en la protección de los datos.

Se han desarrollado técnicas de seguridad óptica que permiten realizar procesos de codificación o encriptación, verificación y autenticación de datos. De la misma manera, se han realizado avances en arquitecturas que permiten emplear patrones biométricos como técnica de seguridad. Del mismo modo, se han implementado múltiples variantes de los esquemas básicos de codificación permitiendo generar llaves de seguridad que tienen como variables dependientes la amplitud, fase, polarización, longitud de onda, posición espacial y parámetros frecuenciales, dando altos niveles de seguridad por los grados de libertad involucrados.

El éxito de estas técnicas ópticas de seguridad radica en la transformación de los datos en una distribución de ruido blanco estacionario. Una distribución aleatoria es muy difícil de duplicar y su propagación o transformada de Fourier dan como resultado una distribución de *speckle* [1.6]. Estas distribuciones luminosas tienen la propiedad de ser portadores aleatorios de información. El primer registro donde se plantea la idea de codificar información mediante la modulación por un difusor aleatorio fue realizado por Françon [1.7].

Ya que un difusor matemáticamente puede ser expresado como $|t(x, y)|e^{i\varphi(x, y)}$, donde $t(x, y)$ es una función de transmisión y $\varphi(x, y)$ es una función aleatoria de valores de fase distribuidos uniformemente en el rango $-\pi$ y π , el difusor puede ser de amplitud o fase. Estos elementos pueden ser empleados para el desarrollo de técnicas ópticas de

seguridad como llaves de codificación. La ventaja principal de las máscaras de fase sobre las máscaras de amplitud es que bajo iluminación convencional no pueden ser registradas por detectores que son sensibles en intensidad, adicionando un nivel de seguridad cuando se adosan a un objeto de amplitud.

Uno de los primeros trabajos que usufructuó este hecho fue realizado por Javidi y Horner en 1994 [1.8]. En esta experiencia, una máscara de fase es adosada a un objeto de amplitud que representa un elemento de identificación personal. Este elemento es sometido a verificación usando un correlador óptico de transformada conjunta (JTC) [1.9]. Cualquier intento de remover la máscara de fase destruye el patrón correcto de identificación dando como resultado una verificación incorrecta.

Un año más tarde, Refregier y Javidi presentan el trabajo pionero en el área de la encriptación óptica [1.10]. El sistema propuesto, emplea una codificación de fase aleatoria en el plano del objeto y en el plano de Fourier (llave de seguridad) de un procesador óptico en configuración $4f$. Esta arquitectura de encriptación de doble máscara de fase mostró como la codificación convierte la información de entrada en una señal de ruido blanco estacionario. La información original únicamente es recuperada haciendo uso del conjugado en fase de la llave de seguridad.

Posteriormente, se presentaron los resultados ópticos experimentales de esta técnica aplicada a la encriptación de imágenes [1.11]. Aquí se evaluó el rendimiento del sistema óptico como herramienta de seguridad y se analizó el comportamiento del mismo ante la presencia de diferentes tipos de ruido y distorsiones de la llave de encriptación. Estos resultados posicionaron a la arquitectura de codificación óptica como un sistema robusto y confiable para resguardar datos.

Sucesivamente, se emplearon memorias ópticas holográficas como medios de registro en el sistema de codificación $4f$ [1.12]. En esta propuesta, para objetos de fase se mostró que si las dos máscaras de encriptación son estadísticamente independientes las imágenes codificadas se registran como ruido blanco estacionario en la memoria holográfica. Esta característica no permite recuperar la información sin el conocimiento de las máscaras de fase correctas.

Hasta este momento, la técnica introducida por Refregier y Javidi para codificar información, necesitaba del complejo conjugado de la llave de seguridad para recuperar los datos originales. Fue hasta que se emplearon cristales fotorrefractivos como medio de registro que se logró generar la fase conjugada de la imagen codificada [1.13]. Esto permitió realizar los procesos de encriptación/desencriptación en tiempo real.

A pesar de este avance, las técnicas de encriptación óptica no tenían una vinculación definida con los sistemas digitales de comunicación. Esto se concretó con el desarrollo del elemento más importante que impulsó el procesado óptico coherente. El desarrollo de dispositivos de cristales líquidos programables bidimensionales LCLV (liquid crystal light valve) [1.14] ha remplazado actualmente a la placa holográfica en los correladores ópticos, redes de interconexiones ópticas y en otras aplicaciones, permitiendo que estas arquitecturas operen a tiempo real. Los progresos tecnológicos permitieron implementar moduladores espaciales de luz SLM (spatial light modulator) [1.15] y otros dispositivos de modulación [1.16]. En los SLM, los píxeles actúan independientemente modulando la amplitud y la fase de la luz. La modulación de los píxeles es controlada electrónicamente convirtiendo la información digital en un medio para manipular características presentes en el dominio de la óptica.

De esta manera, las interfaces optoelectrónicas dan viabilidad a los sistemas de procesamiento óptico a tiempo real, entre ellos, los sistemas ópticos de codificación. Así, las técnicas de encriptación óptica dejan de ser sistemas puramente analógicos y se convierten en sistemas híbridos o sistemas opto-digitales que aprovechan las ventajas que ofrece cada una de estas líneas de desarrollo.

Con estos avances, se realiza la primera encriptación empleando holografía digital [1.17]. En esta propuesta, tanto la imagen encriptada cuanto la llave de seguridad se registran en forma de hologramas digitales [1.18]. Para recuperar la información original, la etapa de decodificación es implementada haciendo uso del holograma digital de la llave de seguridad y cálculos numéricos para realizar el proceso de decodificación. En esta línea, la vinculación entre los sistemas opto-electrónicos y digitales se realizó usando un SLM en

los dispositivos de seguridad óptica [1.19] y un OA-SLM (Optically Addressed Spatial Light Modulator) [1.20].

Actualmente, la combinación de las técnicas de encriptación óptica, moduladores espaciales de luz, cámaras CCD, técnicas de holografía digital, junto a desarrollos de software/hardware, permiten que las técnicas ópticas de seguridad continúen desarrollándose como sistemas híbridos. Su implementación mediante sistemas opto-digitales brinda la posibilidad de transmitir por un canal de comunicación la llave de seguridad y la información codificada que ha sido almacenada holográficamente en un medio de registro plano (CCD). El usuario tiene la posibilidad de recuperar la información digitalmente ó en forma analógica.

Por otro lado, los cálculos numéricos no sólo han contribuido para que los sistemas de encriptación óptica hayan tenido un avance significativo desde su primera propuesta. Las herramientas digitales se han usado para evaluar su desempeño y robustez desde el punto de vista del criptoanálisis [1.21]. Estos estudios determinan qué sistema se comporta adecuadamente ante posibles situaciones de intrusión. Es de enfatizar, que estos análisis no serían posibles sin el uso de herramientas computacionales, ya que para evaluar el buen comportamiento de un sistema de encriptación, el sistema analógico de codificación debe ser modelado matemáticamente constituyendo un prototipo virtual [1.22]. De esta forma, la “experimentación” sobre este sistema permite apreciar la seguridad y confiabilidad del sistema real [1.23].

Consecuentemente, el desarrollo en el área de la encriptación óptica muestra la viabilidad de sistemas que operan con interfaces entre el procesamiento óptico y el procesamiento digital. También, ha mostrado que las tecnologías digitales son herramientas fundamentales para probar y generar configuraciones ópticas optimizadas para procesar información de manera segura. Al implementar estas arquitecturas en sistemas ópticos virtuales, se pueden definir rendimientos óptimos del sistema analógico a partir del análisis de su modelo. Esto conduce al diseño de arquitecturas de encriptación más eficientes. Además, se reducen costos de implementación de pruebas experimentales y se reducen tiempos de ejecución. Por otro lado, al considerar aplicaciones de los sistemas

de codificación óptica en comunicaciones digitales, el comportamiento del sistema total (canal de información clásico o canal de comunicación [1.24]) puede ser evaluado directamente. Las reconstrucciones de la información se realizan de manera digital y se pueden realizar post-procesados de información. La limitación de los sistemas ópticos virtuales es el tiempo de cálculo de los algoritmos que definen cada elemento óptico. Sin embargo, este tiempo de cálculo es menor al de la experimentación de prueba y error.

Los aspectos mencionados han motivado a enmarcar esta Tesis en el ámbito de la óptica virtual. Como objetivo general, se busca optimizar los procesos involucrados en la transmisión de datos codificados en un canal de información clásico. Esto se refiere al proceso de encriptación aplicado a la información enviada, al proceso de desencriptación aplicado a la información codificada recibida y al proceso de transmisión de datos codificados por un canal de comunicación. Para cumplir esta tarea, el desarrollo de sistemas ópticos virtuales de encriptación permitirá “experimentar” y generar variaciones optimizadas de las técnicas conocidas de seguridad óptica. Esto conduce a la implementación digital de sistemas ópticos analógicos y asegurar su buen funcionamiento ejecutando los procesos concernientes a la validación de los modelos matemáticos computacionales [1.25]. Esto último implica verificar los resultados arrojados por el sistema óptico virtual comparando con resultados de algunas experiencias analógicas conocidas. Se espera de manera general que los resultados obtenidos aporten significativamente al área de la encriptación óptica perfeccionando la operatividad de los procesos ópticos aplicados en la protección de los datos.

Algunos de los objetivos específicos propuestos son los siguientes. Buscar alternativas que solucionen la problemática de la técnica convencional de multiplexado en medios de registros planos. Convencionalmente, el uso de esta técnica presenta el problema de la degradación en la información recuperada. Esto hace que los procesos de transmisión de grandes cantidades de información sean ineficientes. Por lo tanto, es de gran relevancia presentar una solución. Si bien en la literatura se han reportado varios trabajos de esta técnica, no existe un estudio sistemático del mismo. Esencialmente se busca desarrollar una técnica que permita manejar un mayor volumen de datos encriptados de

forma óptima. Este aspecto es relevante para el manejo de múltiple información en un canal de información clásico.

Por otro lado, contrario a realizar una variante de los parámetros ópticos para generar funciones que definan nuevas llaves de seguridad en un sistema de encriptación (como se hace regularmente), se propone generar un proceso alternativo que permita optimizar el proceso de transmisión en el canal de comunicación. Esto permitirá definir un protocolo diferente al usado en las transmisiones convencionales de información codificada. Esto requiere que se modifique la transmisión de la pareja, “imagen encriptada-llave de seguridad”. Encontrar un nuevo método para recuperar la información original que no implique el uso de esta pareja, definirá un grado mayor de seguridad en los sistemas convencionales de encriptación ante posibles intrusiones. Con estos planteamientos, se pretende completar la optimización en la operatividad de los procesos involucrados en un canal de información clásico o en un proceso de comunicación.

1.2 Esquema general

Esta Tesis consta de siete capítulos cuyos lineamientos generales se describen a continuación.

En el Capítulo 2 se presentan las arquitecturas básicas de encriptación óptica. Se describe en detalle el sistema de codificación de doble máscara de fase en configuración $4f$. Se explica la arquitectura de encriptación usando cristales fotorefractivos como medio de registro y se describen brevemente otras dos arquitecturas de seguridad óptica, el sistema de doble máscara de fase en configuración JTC y un sistema de encriptación que está regido por parámetros en el dominio de Fresnel. En la parte final del capítulo se introduce de forma general el concepto de óptica virtual y su aplicación en sistemas de codificación.

En la parte inicial del Capítulo 3 se retoma el concepto de óptica virtual. Seguido de esto, se describen los fundamentos teóricos para implementar elementos ópticos virtuales tales como lentes, difusores, pupilas, etc. Posteriormente, se implementan los tratamientos discretos de la propagación en el espacio libre usando el espectro angular de las ondas planas y la integral de Fresnel. Estas implementaciones constituyen los elementos ópticos

virtuales. Por lo tanto, se debe demostrar el buen funcionamiento del arreglo de varios de estos elementos en la conformación de un sistema óptico virtual (SOV). Consecuentemente, se implementan en estos SOV experiencias de procesamiento óptico de información de diferente complejidad y se cotejan los resultados con los valores teóricos esperados de las experiencias analógicas conocidas. Finalmente, se describe la implementación de una arquitectura de encriptación óptica en configuración $4f$ en un SOV.

En el Capítulo 4 se introducen los conceptos básicos, ventajas y deficiencias del multiplexado de imágenes encriptadas en un sistema de codificación $4f$. Seguidamente, se analiza el deterioro de las imágenes recuperadas a partir de un multiplexado de imágenes encriptadas registradas en un medio de registro plano. Se examinan los dos tipos de solapamiento de información que representan una deficiencia en esta técnica al manejar grandes volúmenes de información. Finalmente, se introduce la técnica de modulación theta como otra forma de realizar multiplexado de información. Se muestra su funcionamiento realizando dos aplicaciones en sistemas ópticos virtuales, la composición de color y multiplexado de datos.

En el Capítulo 5 se plantea una nueva arquitectura que es una opción para solucionar la problemática de la degradación de imágenes recuperadas presente en la técnica de multiplexado. Esta es la técnica de encriptación de eventos dinámicos, la cual hace uso de un sistema de codificación en configuración $4f$, de la modulación theta aplicada sobre la información codificada y del multiplexado. La combinación adecuada de estos tres procesos produce varias etapas adicionales en el proceso de encriptación y en el proceso de desencriptación. Se describen estas etapas y se realizan consideraciones para su implementación. Finalmente se comentan aspectos de la seguridad del sistema.

En el Capítulo 6 se presentan tres aplicaciones de la técnica de encriptación de eventos dinámicos. Por primera vez, se introduce el concepto de una película encriptada mediante métodos ópticos. De esta manera, se presenta la aplicación de encriptación de escenas dinámicas monocromáticas, escenas policromáticas de diferente extensión y múltiples escenas para la aplicación en procesos multiusuario. Estas experiencias muestran como este sistema de codificación funciona adecuadamente en el manejo múltiple de datos.

La recuperación de la información en estas aplicaciones optimizan los procesos en un canal de información clásico. Con la arquitectura propuesta se puede procesar, codificar, transmitir y decodificar mayor cantidad de información en comparación a las técnicas actuales de encriptación.

Finalmente, en el Capítulo 7 se presenta una nueva estrategia para generar llaves de seguridad a partir de transformaciones lineales aplicadas sobre una imagen fuente. Se muestran las transformaciones de traslación, reflexión, rotación, contracción o escalamiento y *shearing* que al unir las en un proceso iterativo forman un proceso para generar imágenes con características pseudo-aleatorias. Se presentan análisis originales de la sensibilidad de estas llaves de seguridad. Se discute la aleatoriedad de las imágenes generadas y se muestra la aplicación de estas imágenes como llaves de encriptación en un SOV de doble máscara de fase en configuración *4f*. Finalmente se comprueba cómo el proceso de generación de estas llaves de seguridad permite cambiar el protocolo de transmisión en un proceso de comunicación convencional.

1.3 Bibliografía

- [1.1] M. Stamp, Information security. Principles and practice. John Wiley y Sons, Inc., Hoboken, New Jersey (2006), pp. 1-7.
- [1.2] A. Marechal, P. Croce, “Un filtre de fréquences spatiales pour l'amélioration du contraste des images optiques”, C. R. Acad. Sci. Paris, 237, 607-609, (1953).
- [1.3] H. Stark, “Theory and measurement of the optical Fourier transform”, pp. 1-40, en H. Stark, Applications of optical Fourier transforms, Academic Press, New York (1982).
- [1.4] P. Almeida, G. Indebetouw, “Pattern recognition via complex spatial filtering”, pp. 46-48 en H. Stark, Applications of optical Fourier transforms, Academic Press, New York (1982).
- [1.5] J. W. Goodman, Introduction to Fourier Optics, McGraw-Hill, 2nd ed. (1996), pp. 232-236.

- [1.6] J. C. Dainty, *Laser speckle and related phenomena*. Springer-Verlag Berlin Heidelberg New York (1975).
- [1.7] M. Françon, “Information processing using *speckle* patterns”, pp. 183-185, en C. Dainty, *Láser speckle and related phenomena*, Springer-Verlag Berlin Heidelberg New York (1975).
- [1.8] B. Javidi, J. L. Horner, “Optical pattern recognition for validation and security verification,” *Opt. Eng.*, 33, 1752–756, (1994).
- [1.9] J. W. Goodman, *Introduction to Fourier Optics*, McGraw-Hill, 2nd ed. (1996), pp. 243-246.
- [1.10] P. Refregier, B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” *Opt. Lett.*, 20, 767–769, (1995).
- [1.11] B. Javidi, G. Zhang, J. Li, “Experimental demonstration of the random phase encoding technique for image encryption and security verification,” *Opt. Eng.* 35, 2506 (1996).
- [1.12] B. Javidi, G. Zhang, J. Li, “Encrypted optical memory using double-random phase encoding,” *Appl. Opt.* 36, 1054-1058, (1997).
- [1.13] G. Unnikrishnan, J. Joseph, K. Singh, “Optical encryption system that uses phase conjugation in a photorefractive crystal,” *Appl. Opt.* 37, 8181-8186 (1998).
- [1.14] J. Grinberg, A. Jacobson, W. Bleha, L. Miller, L. Fraas, D. Boswell, y G. Myer. “A new real-time non-coherent to coherent light image converter: the hybrid field effect liquid crystal light valve,” *Opt. Eng.*, 14(3): 217-25 (1975).
- [1.15] P. Birch, R. Young, C. Chatwin, “Spatial Light Modulators (SLMs)”, pp. 179-200 en G. Cristóbal, P. Schelkens, H. Thienpont. *Optical and digital image processing fundamentals and applications*, WILEY-VCH Verlag GmbH y Co. KGaA, Boschstr. 12, 69469 Weinheim, Germany (2011).

- [1.16] J. W. Goodman, Introduction to Fourier Optics. McGraw-Hill, 2nd ed. (1996). pp. 184-209.
- [1.17] B. Javidi, T. Nomura, "Securing information by use of digital holography," Opt. Lett. 25, 28-30, (2000).
- [1.18] T. C. Poon, Digital holography and three-dimensional display. Principles and Applications, Springer Science+Business Media Inc. (2006). pp. 53-57.
- [1.19] O. Matoba, B. Javidi, "Optical retrieval of encrypted digital holograms for secure real-time display," Opt. Lett. 27, 321-323 (2002).
- [1.20] P. Birch, R. Young, C. Chatwin, "Spatial Light Modulators (SLMs)", pp. 190-191 en G. Cristóbal, P. Schelkens, H. Thienpont en Optical and digital image processing fundamentals and applications. WILEY-VCH Verlag GmbH y Co. KGaA, Boschstr. 12, 69469 Weinheim, Germany (2011).
- [1.21] M. Stamp, Information security. Principles and practice. John Wiley y Sons, Inc., Hoboken, New Jersey (2006). pp. 9-31.
- [1.22] P. Fritzson, Introducción al modelado y simulación de sistemas técnicos y físicos. Wiley-IEEE Press (2003) p. 20.
- [1.23] A. J. Menezes, P. C. Van Oorschot, y S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, (1997). pp. 1-6.
- [1.24] D. E. Robling, Cryptography and data security, ADDISON-WESLEY, (1982). pp. 3-7.
- [1.25] R. C. Bu, Simulación, un enfoque practico. Editorial LIMUSA S.A. (2003). pp. 11-18.

Capítulo 2

Técnicas ópticas de encriptación

2.1 Introducción

Los sistemas de encriptación óptica desarrollados en las últimas dos décadas tienen como objetivo principal dar protección a los datos de cualquier índole que sean relevantes para una persona o entidad en particular. De ahora en adelante, se referirá como información a cualquier clase de datos transmisibles por medio de un canal de comunicación, tales como señales, imágenes, textos, códigos, etc., los cuales son relevantes para quien de ahora en adelante se referirá como el usuario final.

Para introducir los SOV como herramientas de estudio en el área de la encriptación óptica, inicialmente se hace una revisión de las técnicas de seguridad más representativas que han permitido el avance en esta disciplina. Se enfatiza en el sistema de codificación de doble máscara de fase en configuración $4f$ y las aplicaciones presentadas en esta Tesis son realizadas en este sistema. Por otro lado, se señalan algunas contribuciones relevantes mostrando el estado actual de esta línea de investigación.

Este capítulo inicia con la Sección 2.2 describiendo el sistema de encriptación de doble máscara de fase en configuración $4f$, posteriormente en la Sección 2.3 se describe la arquitectura de encriptación que emplea cristales fotorrefractivos como medio de registro. En la Sección 2.4 se describen brevemente otras dos arquitecturas de codificación, el sistema de doble máscara de fase basado en configuración JTC y la arquitectura de

codificación de doble máscara de fase en el dominio de Fresnel. Por último, en la Sección 2.5 se introduce el concepto de óptica virtual que se desarrollará en el Capítulo 3.

2.2 Sistema de encriptación de doble máscara de fase en configuración $4f$

El trabajo realizado por Refrégier y Javidi [2.1] abrió el camino para el desarrollo de múltiples propuestas en el área de la seguridad óptica. Esta contribución fue la idea primigenia de lo que hoy son los sistemas ópticos de encriptación, sus variantes implementadas en sistemas opto-digitales y los sistemas ópticos virtuales de encriptación. En su primera propuesta, mostraron simulaciones numéricas y los conceptos matemáticos necesarios para desarrollar la idea de codificar una imagen, sugiriendo que la experiencia podría ser implementada tanto ópticamente cuanto electrónicamente.

Básicamente, estos autores plantearon que para codificar una imagen de entrada, la información de amplitud y de fase que contiene su espectro debían ser modificadas, ya que a partir de cualquiera de estas dos cantidades es posible obtener información de la imagen original por medio de una transformada inversa de Fourier. Con este propósito, se adicionaron dos máscaras de fase aleatorias al procesador óptico $4f$, una adosada al objeto de entrada y otra ubicada en el plano de Fourier. De esta manera, en el plano de salida se obtiene una imagen de ruido blanco estacionario. La etapa de encriptación de esta propuesta está esquematizada en la Figura 2.1.

En el plano de entrada el objeto $O(x, y)$ es multiplicado por una máscara de fase $m_0(x, y)$ que matemáticamente puede ser expresada como $m_0 = \exp[i\varphi_0(x, y)]$, donde $\varphi_0(x, y)$ es una distribución aleatoria de fase con valores uniformemente distribuidos en el rango $-\pi$ a π . A la transmitancia de entrada se le realiza inicialmente una transformada de Fourier usando la lente L_1 de distancia focal f . En el plano de Fourier, el espectro resultante es multiplicado por una segunda máscara de fase $m_1(x_f, y_f)$, expresada como $m_1 = \exp[i\varphi_1(x_f, y_f)]$. Finalmente, a este producto se le realiza una última transformada de Fourier usando la lente L_2 de distancia focal f , obteniendo en el plano de salida el objeto encriptado $E(x_0, y_0)$.

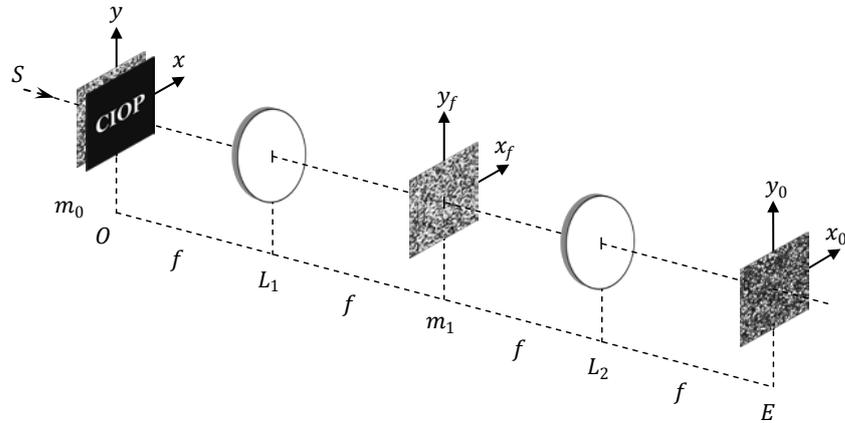


Figura 2.1: Sistema óptico de encriptación de doble máscara de fase. Etapa de encriptación. S es la fuente de iluminación del sistema, L_1 y L_2 son lentes de distancia focal f , O es el objeto de entrada, m_0 es la primera máscara de fase, m_1 es la llave de seguridad y E es la imagen encriptada.

La imagen codificada es una cantidad compleja de amplitud y fase que puede ser representada matemáticamente como:

$$E(x_0, y_0) = \{O(-x, -y) \exp[i\varphi_0(-x, -y)]\} \otimes h(x_0, y_0) \quad (2.1)$$

donde \otimes denota la operación de convolución, los signos negativos indican la inversión de coordenadas, $h(x_0, y_0) = \mathcal{F}\{\exp[i\varphi_1(x_f, y_f)]\}$ es la respuesta impulso de la llave de seguridad $m_1(x_f, y_f)$ y \mathcal{F} es la transformada de Fourier.

Para recuperar la información se realiza la etapa de desencriptación mostrada en la Figura 2.2. Esta consiste de un procesador $4f$. Inicialmente, la imagen encriptada $E(x_0, y_0)$ es iluminada con una onda plana S . El espectro generado por la lente L_1 es multiplicado en el plano de Fourier por el complejo conjugado de la llave de seguridad $m_1(x_f, y_f)$ que esta de forma invertida. Finalmente una segunda lente L_2 realiza la transformada de Fourier de este producto para encontrar la imagen original en el plano de salida del sistema de desencriptación.

Matemáticamente, el campo complejo de la imagen decodificada puede ser expresado como:

$$O_R(x, y) = \mathcal{F}\{\mathcal{F}[E(x_0, y_0)] \exp[-i\varphi_1(-x_f, -y_f)]\} \quad (2.2)$$

Note que a la llave de seguridad $m_1(x_f, y_f)$ en la Ecuación (2.2) se le ha aplicado la operación de conjugación de fase y que está de manera invertida denotándola en función de coordenadas negativas. Usando el teorema de convolución y sustituyendo la Ecuación (2.1) en la Ecuación (2.2), el campo complejo de la imagen recuperada puede ser escrito como:

$$O_R(x, y) = \mathcal{F}\{\mathcal{F}[O(-x, -y)m_0(-x, -y)]m_1(-x_f, -y_f)m_1^*(-x_f, -y_f)\} \quad (2.3)$$

Se puede observar como la llave de seguridad $m_1^*(-x_f, -y_f)$ realiza la compensación de las fases introducidas en la etapa de codificación. Por otro lado, se puede notar que al usar una llave de seguridad incorrecta, no se realiza una compensación adecuada, como resultado se obtendrá la convolución entre el objeto recuperado y un producto de fases aleatorias, en otras palabras, la imagen permanecerá encriptada.

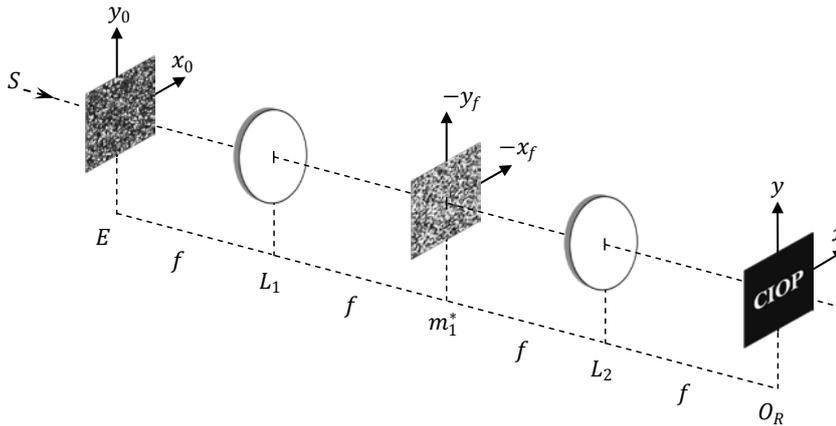


Figura 2.2: Sistema óptico de encriptación de doble máscara de fase. Etapa de desencriptación. S es la fuente de iluminación del sistema, L_1 y L_2 son lentes de distancia focal f , E es la imagen encriptada, m_1^* es la fase conjugada de la llave de seguridad que se encuentra invertida y O_R es el campo complejo recuperado.

Ahora, si se emplea la llave de seguridad correcta, la amplitud compleja del objeto recuperado estará dada por:

$$O_R(x, y) = O(x, y) \exp[i\varphi_0(x, y)] \quad (2.4)$$

Ya que se registra en un detector de intensidad, la distribución recuperada puede ser escrita como:

$$O_R O_R^* = |O(x, y)|^2 \quad (2.5)$$

La primera comprobación experimental de esta técnica [2.2] se realizó empleando una placa holográfica como medio de registro. La información codificada es almacenada por medio de un haz de referencia produciendo un registro holográfico de la imagen encriptada.

Se puede observar que esta propuesta inicial y su implementación experimental traen complicaciones en la etapa de decodificación. No es práctico tener que invertir la llave de seguridad y tener que realizarle el complejo conjugado. De esta manera se restringe su aplicabilidad mostrándola sin versatilidad para aplicaciones en tiempo real.

En este sentido, en la siguiente sección se muestra la implementación del sistema de codificación en configuración 4f usando materiales fotorrefractivos como medio de registro [2.3]. La inclusión de estos materiales permitió realizar aplicaciones en tiempo real de las etapas de codificación/decodificación y mostró la técnica de encriptación óptica con un mayor grado de versatilidad presentándose como una potencial aplicación para asegurar grandes volúmenes de información.

2.3 Sistema de encriptación con registro en memorias holográficas

Algunos cristales electro-ópticos al ser iluminados con un haz de luz no uniforme liberan electrones que migran por difusión o por el efecto fotovoltaico a través de la red cristalina [2.4], [2.5]. Estos electrones son atrapados nuevamente en las regiones del cristal que no han sido iluminadas produciendo una distribución de carga espacial que modula el índice de refracción a través del efecto electro-óptico. Como resultado, se forma un holograma de volumen. Estos cristales fotorrefractivos tienen una gran sensibilidad, una alta capacidad de multiplexado, son materiales reversibles en su uso y no necesitan de un proceso químico para acceder a la información registrada. Estas características los hacen adecuados para el procesamiento óptico de información.

Algunas de las aplicaciones más importantes de estos materiales se han realizado en técnicas de interferometría a tiempo real [2.6], reducción de *speckle* por integración de

imágenes [2.7], amplificación óptica [2.8], holografía dinámica [2.9],[2.10] y la generación continua de un frente de onda de fase conjugada [2.11], [2.12].

Las técnicas de encriptación óptica también se han beneficiado de estos materiales al incluirlos en las arquitecturas ópticas de encriptación/desencriptación. Aprovechando sus inherentes características, los cristales fotorrefractivos han sido empleados para generar el frente de onda conjugado de la imagen encriptada en un proceso de decodificación. Otra importante aplicación es el uso como memorias holográficas para registrar múltiples imágenes codificadas [2.13]. Para recuperar cualquiera de los datos registrados en el medio fotorrefractivo, se emplea la llave de seguridad asignada al dato encriptado mientras la información restante se mantiene codificada.

En la Figura 2.3 están esquematizadas las etapas de encriptación/desencriptación usando un cristal fotorrefractivo. Una onda plana representada por la fuente S ilumina la entrada de un procesador $4f$ realizando el proceso de codificación descrito en párrafos anteriores. Ahora, el campo complejo R , el cual contiene la información de la imagen encriptada, interfiere con una onda de referencia s sobre el material fotorrefractivo, modulando la información encriptada. A la salida del cristal se genera el haz conjugado s^* , este se refleja en el espejo M_2 y se produce una onda contrapropagante al haz de referencia. Al interactuar nuevamente en el cristal fotorrefractivo forma la conjugación de fase del campo complejo de la imagen encriptada, generándose R^* .

El campo contrapropagante recuerda las distorsiones introducidas en la fase de la onda luminosa al propagarse por el sistema óptico. Al volver el haz conjugado por el mismo camino y al interactuar con los mismos elementos dispersores compensará los cambios de fase del campo incidente. Así, las aberraciones en el sistema óptico son corregidas y las diferencias de fase debido al proceso de encriptación son compensadas si se usa la llave de seguridad correcta.

El proceso de decodificación en la Figura 2.3 es análogo a iluminar con el haz de referencia la fase conjugada de la imagen codificada, tal como se muestra en la imagen de la Figura 2.4. Esta configuración se considera cuando se trabaja en SOV o en

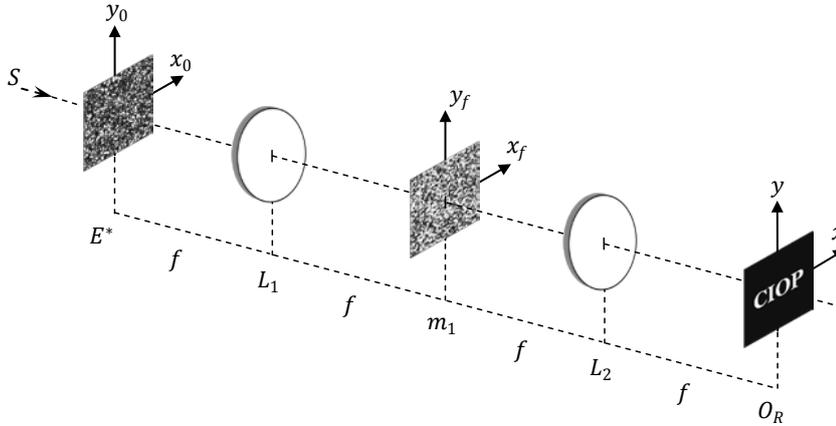


Figura 2.4: Etapa de descriptación iluminando la imagen encriptada de fase conjugada. El sistema está compuesto de dos lentes L_1 y L_2 de distancia focal f . E^* es la imagen codificada de fase conjugada, S es la fuente de iluminación, m_1 es la llave de encriptación y O es el campo complejo del objeto recuperado.

Sustituyendo en la Ecuación (2.6) el complejo conjugado de la Ecuación (2.1), el campo complejo recuperado puede ser escrito como:

$$O_R(x, y) = O^*(x, y) \exp[-i\varphi_0(x, y)] \quad (2.7)$$

Ya que el medio de registro es un detector de intensidad, la distribución recuperada está dada por:

$$O_R O_R^* = |O(x_0, y_0)|^2 \quad (2.8)$$

De esta manera, un objeto en el plano de entrada puede ser codificado en forma de ruido blanco estacionario y el usuario autorizado puede recuperar la información empleando únicamente la llave de seguridad $m_1(x_f, y_f)$ en la etapa de decodificación.

La aplicación en tiempo real de un sistema de encriptación con cristales fotorrefractivos es de interés debido a que son elementos reversibles en su uso. Por otro lado, se tiene un rápido tiempo de acceso a la información codificada en el orden de los sub-milisegundos permitiendo una lectura de manera casi instantánea y en paralelo. Además, gracias a la relación biunívoca que existe entre el haz de lectura y la información almacenada mediante la condición de Bragg [2.14], es posible una reconstrucción selectiva de la información codificada sin solapamiento de los diferentes registros. Finalmente, la información que ha sido almacenada en este medio puede ser usada como una base de

datos debido a la alta densidad del material, logrando realizar aplicaciones de verificación o reconocimiento de patrones.

A pesar de estas grandes ventajas, las técnicas de encriptación óptica fueron encaminadas a que la información codificada y las llaves de seguridad pudieran ser enviadas al usuario final por canales de transmisión abiertos o privados para su uso en internet. En este sentido, se ha explorado la inclusión de otras tecnologías como moduladores espaciales de luz (SLM) [2.15] y otras técnicas de registro, como la holografía digital [2.16]. Estas técnicas permiten darle al usuario final facilidades para acceder digitalmente a la información codificada ópticamente.

2.4 Otras arquitecturas de encriptación óptica

Además del sistema de codificación de doble máscara de fase en configuración $4f$, se han desarrollado arquitecturas basadas en otras configuraciones de procesamiento óptico de información. Todas estas arquitecturas de codificación y sus variantes tratan de implementar aplicaciones eficientes para el manejo seguro de datos.

2.4.1 Sistema de encriptación de doble máscara de fase basado en un correlador de transformada conjunta

Se deben mencionar algunas contribuciones que han permitido el avance de la encriptación óptica realizando la protección de la información en otras configuraciones diferentes a la arquitectura de codificación $4f$. Una de estas técnicas es el sistema de encriptación de doble máscara de fase llamado JTC [2.17] basado en un correlador de transformada conjunta [2.18].

Paralelo a los avances realizados con el sistema de codificación $4f$, se han realizado estudios centrados en analizar la eficiencia de las propuestas relacionadas con esta técnica de seguridad, evaluando su resistencia ante ataques abordados desde el criptoanálisis [2.19]-[2.22].

Principalmente, a partir de estos estudios se estableció que la técnica de seguridad en configuración $4f$ presentaba gran sensibilidad ante defectos de alineación del sistema óptico, ya que al tener que registrar valores complejos se requiere un haz de referencia para implementar un registro holográfico. Como alternativa se desarrolló una técnica de codificación de doble máscara de fase basada en la configuración de un correlador de transformada conjunta (*JTC*).

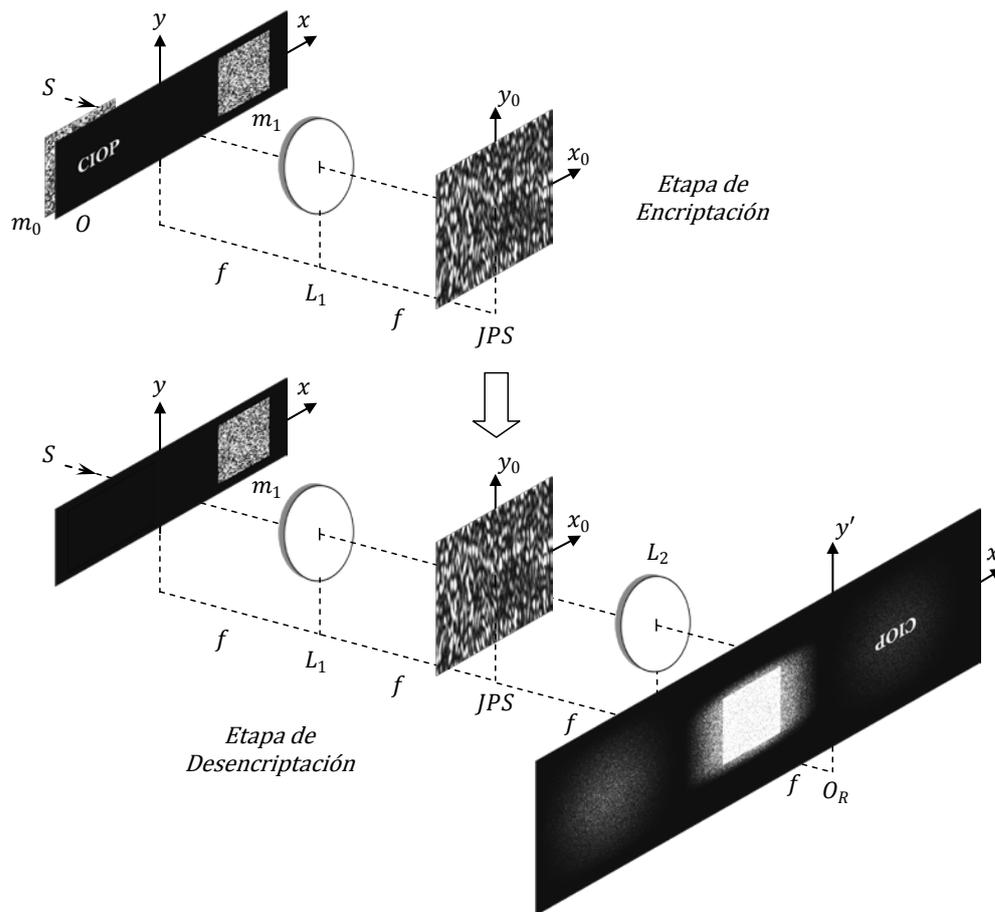


Figura 2.5: Etapa de encriptación y etapa de desencriptación de un sistema de doble máscara de fase basado en una arquitectura *JTC*. La etapa de encriptación consiste de una lente L_1 de distancia focal f . O es el objeto de entrada, m_0 es la máscara de fase adosada al objeto y m_1 es la llave de seguridad. *JPS* es el espectro conjunto de potencia encriptado y es registrado digitalmente en intensidad. La etapa de desencriptación consiste de un procesador $4f$. L_1 y L_2 son lentes de distancia focal f . En el plano de entrada se encuentra la llave de seguridad m_1 . En el plano de salida se obtiene el objeto correctamente decodificado en la posición $(x' = a, y' = 0)$.

La etapa de codificación y la etapa de decodificación de esta técnica están esquematizadas en la Figura 2.5. En el proceso de encriptación se emplea una lente L_1 que produce la transformada de Fourier del plano de entrada donde se ubica el objeto a

encriptar y la llave de codificación. El objeto se encuentra adosado a una máscara de fase aleatoria y el conjunto que está desplazado respecto al origen en la posición $x = -a$ puede expresarse como $O(x, y)m_0(x, y) \otimes \delta(x + a, y)$. Del mismo modo, la llave de seguridad es expresada como $m_1(x, y) \otimes \delta(x - a, y)$. Es decir, el objeto y la llave de encriptación están separados una distancia $2a$ respecto sus centros. La imagen encriptada es el espectro del plano de entrada que es registrado en un detector de intensidad y es llamado espectro conjunto de potencia encriptado descrito por las siglas *JPS*.

Para recuperar la información, se emplea un procesador óptico $4f$ ubicando en el plano de entrada la llave de seguridad m_1 en la misma posición que en el registro. En el plano de Fourier de la primera lente L_1 se encuentra el *JPS* el cual es iluminado con la transformada de Fourier de la llave de seguridad. Al campo complejo resultante se le realiza una última transformada de Fourier usando la lente L_2 para encontrar en el plano de salida el objeto correctamente decodificado. Ya que la imagen de salida puede estar superpuesta con el orden central, se debe garantizar la separación adecuada entre la imagen de entrada y la llave de seguridad [2.23] para que en la etapa de desencriptación la difracción del *JPS* permita visualizar correctamente la imagen decodificada.

Es de notar que el resultado de la etapa de desencriptación consiste de cuatro términos donde únicamente uno revela la información correctamente decodificada. Esto es, considerando que matemáticamente en el plano de entrada se tiene:

$$T(x, y) = O(x, y)m_0(x, y) \otimes \delta(x + a, y) + m_1(x, y) \otimes \delta(x - a, y) \quad (2.9)$$

donde \otimes representa la operación de convolución y $\delta(\cdot)$ denota la distribución de delta de Dirac, los cuatro términos en el plano de Fourier de la lente L_1 en la etapa de decodificación pueden ser expresados como:

$$\begin{aligned} O_R(x', y') = & [O(-x', -y')m_0(-x', -y')] \otimes [O^*(x', y')m_0^*(x', y')] \otimes m_1(-x', -y') \\ & \otimes \delta(x' + a, y') + m_1(-x', -y') \otimes \delta(x' + a, y') \\ & + [O(-x', -y')m_0(-x', -y')] \otimes \delta(x' - a, y') + [O^*(x', y')m_0^*(x', y')] \\ & \otimes m_1(-x', -y') \otimes m_1(-x', -y') \otimes \delta(x' + 3a, y') \end{aligned} \quad (2.10)$$

En la Ecuación (2.10), la intensidad del tercer término produce la información del objeto original en la posición $(x' = a, y' = 0)$, por otro lado, el primer, segundo y cuarto término representan ruido en la etapa de recuperación, el primer y segundo término están solapados en la posición $(x' = -a, y' = 0)$, mientras que el cuarto término está ubicado en la posición $(x' = -3a, y' = 0)$.

Es importante destacar la diferencia en las etapas de recuperación de los sistemas de encriptación en arquitectura $4f$ y en arquitectura JTC . En la arquitectura JTC , en el plano de entrada en el proceso de desencriptación se ubica la llave de seguridad mientras que en el plano de Fourier de la primera lente la imagen encriptada. Por otro lado, en la arquitectura $4f$, en el plano de entrada en el proceso de desencriptación se posiciona el objeto encriptado mientras que en el plano de Fourier de la primer lente la llave de seguridad. Por último, para recuperar adecuadamente la información, por las características holográficas de la arquitectura JTC , no es necesario hacer uso de un haz de referencia ni tampoco realizar la operación del complejo conjugado a la llave de seguridad o en su defecto, la operación de complejo conjugado a la información encriptada.

Aunque la arquitectura de codificación de doble máscara de fase en configuración JTC aporta ciertas ventajas de implementación, se debe tener presente que las técnicas de holografía y holografía digital están muy bien establecidas. Ellas han permitido realizar importantes aplicaciones en metrología, espectroscopia, telecomunicaciones, entre otras, posicionándolas como técnicas eficaces para procesar y almacenar grandes flujos de información. Desde que J. Goodman y R.W. Lawrence desarrollaron la holografía digital [2.24], se han implementado técnicas que manejan adecuadamente el campo complejo del frente de onda, recuperando la fase por medios digitales en fracciones de segundo. De esta manera, se han realizado experiencias en microscopía holográfica digital [2.25] en holografía digital a color en aplicaciones biológicas [2.26], [2.27] y en holografía digital empleando corrimientos de fase [2.28].

En este sentido, estas aplicaciones que utilizan la holografía digital contribuyen a no dejar de lado al sistema de codificación de doble máscara de fase en configuración $4f$, sino que por el contrario, estimulan a analizar más a fondo sus posibles variantes y a

proponer nuevas estrategias de encriptación ópticas que tienen como soporte a esta técnica (ver Apéndice A).

2.4.2 Sistema de encriptación de doble máscara de fase en el dominio de Fresnel

Algunos autores han introducido variantes al sistema de codificación $4f$ definiendo nuevos parámetros de seguridad del sistema de encriptación. Un buen ejemplo se encuentra en [2.29], [2.30], donde las llaves de seguridad se encuentran ubicadas en el dominio de Fresnel. La implementación experimental de esta técnica se realizó registrando tres imágenes diferentes en un cristal fotorrefractivo usando un multiplexado angular [2.31]. Las posiciones de las máscaras de fase en el sistema óptico pueden ser consideradas como llaves adicionales que el usuario debe tener para poder recuperar adecuadamente la información original. De esta manera se hace más seguro el proceso de desencriptación.

El montaje básico de un sistema de codificación en el dominio de Fresnel se muestra en la Figura 2.6. La etapa de encriptación consiste en iluminar con una onda plana S al objeto de entrada $O(x, y)$. El campo difractado se propaga en la región de Fresnel hasta encontrar la primera llave de codificación $m_0(x', y')$, ubicada a una distancia d_1 del plano del objeto. Consecutivamente continúa hasta la lente L_1 de distancia focal f pasando a través de ella hasta encontrar la segunda máscara de fase $m_1(x'', y'')$ ubicada a una distancia d_2 de su plano focal posterior propagándose luego el campo complejo resultante hasta dicho plano. Finalmente la lente L_2 de distancia focal f , realiza una transformada de Fourier para obtener la imagen encriptada $E(x_0, y_0)$.

Para realizar el proceso de decodificación y recuperar nuevamente la información original, es necesario usar el complejo conjugado de la información encriptada y ubicar en las posiciones correctas las llaves de decodificación $m_0(x', y')$ y $m_1(x'', y'')$ con el fin de compensar los cambios de fase originados por el sistema óptico de encriptación.

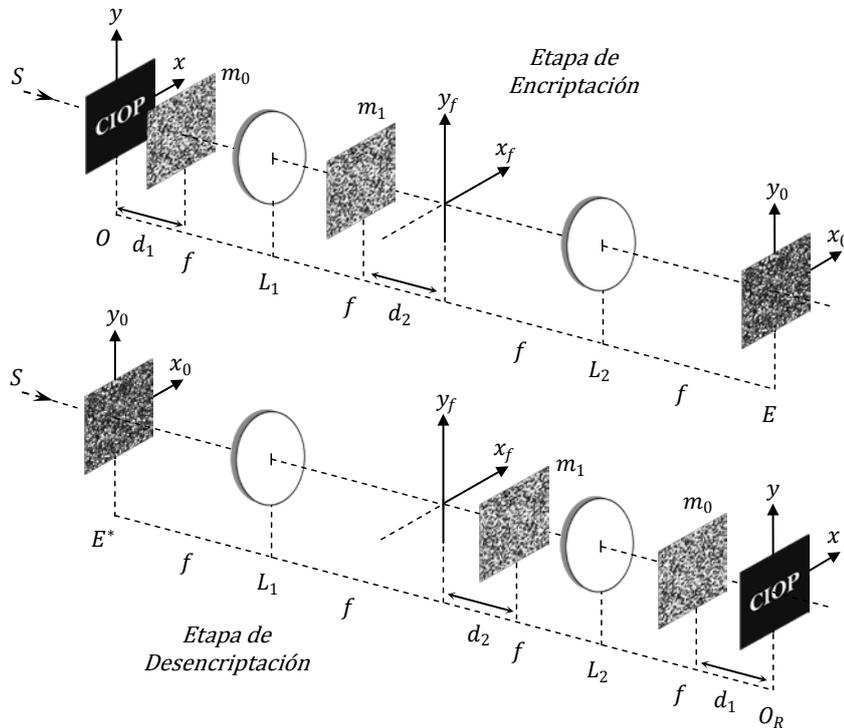


Figura 2.6: Etapa de encriptación y etapa de desencriptación de un sistema de doble máscara de fase en el dominio de Fresnel. S es la onda plana de iluminación, O es el objeto a codificar, d_1 es la distancia medida desde el objeto a la primera máscara de fase m_0 y d_2 es la distancia entre la segunda máscara de fase m_1 y el plano de Fourier de la lente L_1 , E es la imagen encriptada, O_R es el objeto recuperado.

Para recuperar la información, se ilumina con una onda plana el complejo conjugado de la imagen encriptada $E(x_0, y_0)$ y se le realiza una primera transformada de Fourier mediante la lente L_1 de distancia focal f . Posteriormente, el espectro se propaga en el dominio de Fresnel una distancia d_2 hasta encontrar la máscara de fase $m_1(x'', y'')$. El campo resultante continúa propagándose hasta la lente L_2 para luego llegar a la máscara de fase $m_0(x', y')$ ubicada a una distancia d_1 del plano de salida. Finalmente se propaga hasta el plano de salida donde se recupera la imagen correctamente desencriptada.

El valor agregado de esta técnica radica en controlar los parámetros de ubicación de las máscaras de fase que conforman la llave de seguridad. Si se colocan las máscaras en planos incorrectos, la compensación de la fase no será realizada de manera adecuada y la información permanecerá codificada.

Dentro de esta línea de sistemas alternativos de codificación de doble máscara de fase, se encuentra el que emplea únicamente parámetros de propagación ubicando las

máscaras de codificación en diferentes planos del dominio de Fresnel sin usar lentes en el sistema óptico de encriptación [2.32]. Otras contribuciones relacionadas con el uso de distancias de posicionamiento de las máscaras de fase junto con la dependencia de la longitud de onda en el dominio de Fresnel son presentadas en [2.33]-[2.35], mientras que en el dominio fraccional de Fourier en [2.36]-[2.39]. Principalmente, el cambio de la ubicación de las dos máscaras de fase en el plano de Fourier, en planos fraccionales de Fourier o en planos de Fresnel hace que se cambien los anchos de banda de las frecuencias espaciales de la información encriptada dependiendo de la configuración utilizada. De esta manera, las variaciones de posición de cada llave de codificación actúan como variables que definen parámetros de seguridad que son relevantes a la hora de recuperar la información original.

2.5 Sistemas ópticos-digitales en la encriptación

Como se ha discutido en la referencia [2.40], la inherente naturaleza bidimensional de un sistema óptico permite aceptar grandes bloques de datos para ser procesados en paralelo, ofreciendo ventajas únicas sobre los procesadores electrónicos. En un procesador óptico, todos los puntos de una imagen son procesados a la vez y no punto a punto como en un sistema electrónico. Esto ofrece una velocidad de procesamiento casi instantánea. Además, ya que la transformada de Fourier se puede implementar de forma simple en un sólo bloque por medio de una lente, se pueden diseñar sistemas que realicen operaciones complejas de correlación, convolución, diferenciación, filtrado, etc.

Por otro lado, los sistemas basados en la óptica de Fourier son inherentemente analógicos teniendo dificultades para alcanzar altos grados de exactitud y precisión como cualquier sistema analógico eléctrico o mecánico. Un sistema óptico analógico puro por sí mismo no puede tomar decisiones como lo hace un sistema electrónico, por ejemplo, realizar una comparación de varios conjuntos de elementos con una determinada base de datos y arrojar una estadística en un tiempo estimado. Este tipo de operaciones no pueden ser realizadas por sistemas ópticos puros sin la ayuda de interfaces electrónicas. Consecuentemente, un sistema óptico no se puede programar en un sentido convencional y a manera comparativa, se asemeja al hardware en un computador. Por otro lado, al querer

aplicar el procesado óptico a otros datos de entrada que sean diferentes a imágenes, se deben emplear moduladores espaciales de luz para convertir las señales eléctricas a señales ópticas. Finalmente para el procesado óptico se requiere luz con un alto grado de coherencia.

En vista de lo anterior, las debilidades de un sistema óptico pasan a ser las fortalezas de algunos sistemas electrónicos-digitales. Por ejemplo, la precisión, exactitud, control, flexibilidad de programación, etc. Por estos motivos, es razonable la idea de aprovechar de forma optimizada las ventajas que ofrecen cada una de estos sistemas.

Aun se puede afirmar que los métodos ópticos son los más rápidos para realizar operaciones bidimensionales, sin embargo, el progreso incesante del formato digital los ha desplazado en muchas aplicaciones de interés. En la actualidad es muy poco frecuente encontrar sistemas puramente analógicos sin la influencia de sistemas electrónicos. La mayoría de sistemas de procesado de señales dependen de tecnologías ópticas y tecnologías digitales. Esto brinda el beneficio adicional de obtener precisión, exactitud y programación en las tareas específicas a desarrollar. Usualmente las imágenes constituyen la información a ser procesadas y la mayoría de las veces han interactuado con un sistema óptico previo a su manipulación digital.

Por lo tanto, la idea de combinar tecnologías electrónicas o digitales con sistemas ópticos es una forma de usufructuar las características del paralelismo y rápido procesado de información que brindan las arquitecturas ópticas. Del mismo modo, permite aprovechar las ventajas de los sistemas electrónicos-digitales programables para realizar actividades complejas, por ejemplo, tareas más eficientes de análisis de resultados que arrojen datos para la retroalimentación de variables que sirven en la optimización del sistema óptico.

En este sentido, el campo de la encriptación óptica ha obtenido ventaja de las interfaces analógicas-digitales. Las arquitecturas de codificación pasaron a ser sistemas híbridos o sistemas opto-digitales. En la literatura se han propuesto variantes en la forma de registro en los sistemas de codificación las cuales van encaminadas a que las técnicas de seguridad óptica puedan ser utilizadas en canales clásicos de información.

Posteriormente al uso de materiales fotorrefractivos, las técnicas de registro mediante holografía digital vincularon las arquitecturas de encriptación y el procesamiento digital de datos. Como se mencionó, esto se mostró en la primera implementación del sistema de codificación $4f$ empleando holografía digital [2.41] y el empleo de moduladores SLM [2.42]. Los procesos de recuperación se lograron realizar electrónicamente después de transmitir la información encriptada por canales de comunicación digital. Esto facilitó el desarrollo de varias propuestas de encriptación basadas en la implementación sobre sistemas híbridos haciendo uso de tecnologías optoelectrónicas y técnicas opto-digitales [2.43].

En otro aspecto, los tratamientos digitales permitieron desarrollar estudios para identificar vulnerabilidades de los sistemas de codificación ante ataques basados en fundamentos del criptoanálisis [2.44]-[2.50]. De esta manera, se planteó una nueva estrategia de investigación basada en la implementación de sistemas opto-digitales y sistemas ópticos virtuales. Estos últimos han permitido proponer nuevas arquitecturas de codificación. Su metodología de implementación presenta la ventaja de poder realizar análisis complejos por medio de herramientas computacionales (hardware y software) [2.51]-[2.56]. Las experiencias analógicas para replicar estos estudios conllevarían tiempos excesivos. En este sentido, en relación al criptoanálisis la “experimentación” mediante los sistemas ópticos virtuales facilita la búsqueda de arquitecturas optimizadas resistentes a ataques convencionales. Esto permite economizar tiempo y recursos frente a la misma búsqueda en el laboratorio, brindando un proceso de selección eficiente de los parámetros ópticos involucrados en las configuraciones analógicas.

En esta línea se debe enfatizar que los sistemas ópticos virtuales son conceptos de la física óptica que tienen una teoría bien establecida sobre la cual se soportan. Los algoritmos computacionales que definen cada elemento virtual son implementados de manera robusta dependiendo de la aplicación específica a desarrollar. La idea fundamental de esta estrategia de trabajo, es que el sistema óptico virtual brinde cabalmente información del comportamiento analógico real ante cambios de los parámetros ópticos. De esta manera se evalúa su funcionamiento bajo condiciones específicas y permite recolectar datos significativos para la adecuada implementación experimental.

En el capítulo siguiente se introducen los sistemas ópticos virtuales aplicados de manera general al procesamiento óptico de información. En capítulos posteriores se aplicarán a experiencias específicas de encriptación óptica.

2.6 Bibliografía

- [2.1] P. Refregier, B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” *Opt. Lett.*, 20, 767–769, (1995).
- [2.2] B. Javidi, G. Zhang, J. Li, “Experimental demonstration of the random phase encoding technique for image encryption and security verification,” *Opt. Eng.* 35, 2506 (1996).
- [2.3] G. Unnikrishnan, J. Joseph, K. Singh, “Optical encryption system that uses phase conjugation in a photorefractive crystal,” *Appl. Opt.* 37, 8181-8186 (1998).
- [2.4] J. Frejlich, *Photorefractive materials: Fundamental Concepts, Holographic Recording and Materials Characterization*. A John Wiley y Sons, Inc. (2007). pp. 5-18.
- [2.5] P. Hariharan, *Optical Holography. Principles, techniques and applications*. Cambridge University Press (1996). pp. 119-122.
- [2.6] J. Liou, C. Lee, K. Wu, “Photorefractive crystal-based holographic interferometry system for full-field wave propagation metrology,” *Opt. Express* 15, 5460-5472 (2007).
- [2.7] J. P. Huignard, J. P. Herriau, L. Pichon, A. Marrakchi, “*Speckle*-free imaging in four-wave mixing experiments with $\text{Bi}_{12}\text{SiO}_{20}$ crystals,” *Opt. Lett.* 5, 436-437 (1980).
- [2.8] A. V. Khomenko, A. García-Weidner, A. A. Kamshilin, “Amplification of optical signals in $\text{Bi}_{12}\text{TiO}_{20}$ crystal by photorefractive surface waves,” *Opt. Lett.* 21, 1014-1016 (1996).

- [2.9] N. A. Vainos, S. L. Clapham, R. W. Eason, "Multiplexed permanent and real time holographic recording in photorefractive BSO," *Appl. Opt.* 28, 4381-4385 (1989).
- [2.10] P. Hariharan, *Optical Holography. Principles, techniques and applications.* Cambridge University Press (1996). pp. 201-204.
- [2.11] A. Yariv, P. Yeh, "Phase conjugate optics and real-time holography". *IEEE Journal of Quantum Electronics*, 14 (9) (1978). pp. 650-660.
- [2.12] J. P. Huignard, J. P. Herriau, P. Aubourg, E. Spitz, "Phase-conjugate wavefront generation via real-time holography in $\text{Bi}_{12}\text{SiO}_{20}$ crystals," *Opt. Lett.* 4, 21-23 (1979).
- [2.13] G. Unnikrishnan, J. Joseph, K. Singh, "Optical Encryption System That Uses Phase Conjugation in a Photorefractive Crystal," *Appl. Opt.* 37, 8181-8186 (1998).
- [2.14] M. Born, E. Wolf, *Principles of optics: electromagnetic theory of propagation, interference and diffraction of light.* Cambridge: Cambridge University Press, (1999). pp. 706-708.
- [2.15] P. Birch, R. Young, C. Chatwin, "Spatial Light Modulators (SLMs)". pp. 190-191 en G. Cristóbal, P. Schelkens, H. Thienpont. *Optical and digital image processing fundamentals and applications.* WILEY-VCH Verlag GmbH y Co. KGaA, Boschstr. 12, 69469 Weinheim, Germany (2011).
- [2.16] T. C. Poon, *Digital holography and three-dimensional display. Principles and Applications,* Springer Science+Business Media Inc. (2006). pp. 53-57.
- [2.17] T. Nomura, B. Javidi, "Optical encryption using a joint transform correlator architecture", *Opt. Eng.* 39, 2031 (2000).
- [2.18] J. W. Goodman, *Introduction to Fourier Optics.* McGraw-Hill, 2nd ed. (1996). pp. 243-246.
- [2.19] B. Javidi, A. Sergent, G. Zhang, L. Guibert, "Fault tolerance properties of a double phase encoding encryption technique," *Opt. Eng.* 36, pp. 992-998, (1997).

- [2.20] B. Wang, C. Sun, W. Su, A. E. T. Chiou, "Shift-Tolerance Property of an Optical Double-Random Phase-Encoding Encryption System," *Appl. Opt.* 39, 4788-4793 (2000).
- [2.21] Y. Frauel, A. Castro, T. Naughton, B. Javidi, "Resistance of the double random phase encryption against various attacks," *Opt. Express* 15, 10253-10265 (2007).
- [2.22] W. Liu, G. Yang, H. Xie, "A hybrid heuristic algorithm to improve known-plaintext attack on Fourier plane encryption," *Opt. Express* 17, 13928-13938 (2009).
- [2.23] J. W. Goodman, *Introduction to Fourier Optics*. McGraw-Hill, 2nd ed. (1996). p. 242.
- [2.24] J. W. Goodman, R. W. Lawrence, "Digital image formation from electronically detected holograms", *Appl. Phys. Lett.* 11, 77 (1967).
- [2.25] J. Di, J. Zhao, H. Jiang, P. Zhang, Q. Fan, W. Sun, "High resolution digital holographic microscopy with a wide field of view based on a synthetic aperture technique and use of linear CCD scanning," *Appl. Opt.* 47, 5654-5659 (2008).
- [2.26] C. J. Mann, M. K. Kim, "Phase-Imaging Digital Holographic Movies of Animal Cells," in *Conference on Láseres and Electro-Optics/Quantum Electronics and Láser Science and Photonic Applications Systems Technologies, Technical Digest (CD)* (Optical Society of America, 2005), paper CWH1.
- [2.27] C. J. Mann, A. Khmaladze, M. K. Kim, "Phase Contrast Movies of Cell Migration by Multi-Wavelength Digital Holography," in *Conference on Láseres and Electro-Optics/Quantum Electronics and Láser Science Conference and Photonic Applications Systems Technologies, Technical Digest (CD)* (Optical Society of America, 2006), paper CTuG5.
- [2.28] I. Yamaguchi, "Phase-Shifting Digital Holography," *Optics y Photonics News* 19(7), 48-53 (2008).

- [2.29] O. Matoba, T. Nomura, E. Perez, M.S. Millan, B. Javidi, Optical techniques for information security. Proc. IEEE J., 97, 1128–1148. (2009).
- [2.30] M. S. Millan, E. Pérez, Optical Data Encryption. pp. 751-753 en G. Cristóbal, P. Schelkens, H. Thienpont. Optical and digital image processing fundamentals and applications. WILEY-VCH Verlag GmbH y Co. KGaA, Boschstr. 12, 69469 Weinheim, Germany (2011).
- [2.31] O. Matoba, B. Javidi, “Encrypted optical memory system using three-dimensional keys in the Fresnel domain,” Opt. Lett. 24, 762-764 (1999).
- [2.32] G. Situ, J. Zhang, “Double random-phase encoding in the Fresnel domain,” Opt. Lett. 29, 1584-1586 (2004).
- [2.33] L. Chen, D. Zhao, “Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms,” Opt. Express 14, 8552–8560 (2006).
- [2.34] A. Nelleri, J. Joseph, K. Singh, “Digital Fresnel field encryption for three-dimensional information security”, Opt. Eng. 46, 045801 (Apr 27, 2007).
- [2.35] W. Chen, X. Chen, C. J. R. Sheppard, “Optical color-image encryption and synthesis using coherent diffractive imaging in the Fresnel domain,” Opt. Express 20, 3853-3865 (2012).
- [2.36] G. Unnikrishnan, J. Joseph, K. Singh, “Optical encryption by double-random phase encoding in the fractional Fourier domain,” Opt. Lett. 25, 887-889 (2000).
- [2.37] G. Unnikrishnan, Kehar Singh, “Double random fractional Fourier-domain encoding for optical security”, Opt. Eng. 39, 2853 (2000).
- [2.38] R. Tao, Y. Xin, Y. Wang, “Double image encryption based on random phase encoding in the fractional Fourier domain,” Opt. Express 15, 16067-16079 (2007).
- [2.39] R. Tao, J. Lang, Y. Wang, “Optical image encryption based on the multiple-parameter fractional Fourier transform,” Opt. Lett. 33, 581-583 (2008).

- [2.40] J. Leger, S. Lee, Processing using Hybrid Systems, pp.131-134, en H. Stark Applications of Optical Fourier Transforms Signal, Academic Press, New York (1982).
- [2.41] B. Javidi, T. Nomura, "Securing information by use of digital holography," *Opt. Lett.* 25, 28-30, (2000).
- [2.42] O. Matoba, B. Javidi, "Optical retrieval of encrypted digital holograms for secure real-time display," *Opt. Lett.* 27, 321-323 (2002).
- [2.43] T. Nomura, Hybrid optical encryption of a 3D object by use of a digital holographic technique, pp. 85-95 en B. Javidi, Advanced sciences and technologies for security applications, Springer Science+Business Media, Inc.(2006).
- [2.44] A. J. Menezes, P. C. Van Oorschot, y S. A. Vanstone. Handbook of Applied Cryptography, CRC Press, (1997). pp. 41-44.
- [2.45] X. Peng, P. Zhang, H. Wei, B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," *Opt. Lett.* 31, 1044-1046 (2006).
- [2.46] X. Peng, H. Wei, P. Zhang, "Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain," *Opt. Lett.* 31, 3261-3263 (2006).
- [2.47] G. Situ, U. Gopinathan, D. Monaghan, J. Sheridan, "Cryptanalysis of optical security systems with significant output images," *Appl. Opt.* 46, 5257-5262 (2007).
- [2.48] X. Cheng, L. Cai, Y. Wang, X. Meng, H. Zhang, X. Xu, X. Shen, G. Dong, "Security enhancement of double-random phase encryption by amplitude modulation," *Opt. Lett.* 33, 1575-1577 (2008).
- [2.49] X. Yong-Liang, Z. Xin, Y. Sheng, L. Qiang, L. Yang-Cong, "Multiple-image optical encryption: an improved encoding approach," *Appl. Opt.* 48, 2686-2692 (2009).
- [2.50] Y. Chen, J. Chen, "Cryptosystem for plaintext messages utilizing optical properties of gratings," *Appl. Opt.* 49, 2041-2046 (2010).

- [2.51] X. Peng, Z. Cui, T. Tan, “Information encryption with virtual-optics imaging system,” *Opt. Commun.* 212, 235-245 (2002).
- [2.52] X. Peng, L. Yu, L. Cai, “Double-lock for image encryption with virtual optical wavelength,” *Opt. Express* 10, 41-45 (2002).
- [2.53] H. Kim, D. Kim, Y. Lee, “Encryption of digital hologram of 3-D object by virtual optics,” *Opt. Express* 12, 4912-4921 (2004).
- [2.54] H. Suzuki, H. Tashima, M. Yamaguchi, T. Obi, M. Yachida, N. Ohyama, “File Encryption Software Using Fingerprint Keys Based on Double Random Encoding,” in *Frontiers in Optics, OSA Technical Digest Series* (Optical Society of America, 2005), paper JWA50.
- [2.55] X. Wang, D. Zhao, F. Jing, X. Wei, “Information synthesis (complex amplitude addition and subtraction) and encryption with digital holography and virtual optics,” *Opt. Express* 14, 1476-1486 (2006).
- [2.56] B. Chen, H. Wang, “Optically-induced-potential-based image encryption,” *Opt. Express* 19, 22619-22627 (2011).

Capítulo 3

Sistemas ópticos virtuales en el procesamiento de información

3.1 Introducción

En la parte final del capítulo anterior se abordó el concepto de sistema óptico virtual (SOV). Para entender en más detalle el significado de este concepto se deben emplear los fundamentos básicos de sistema, modelado y simulación [3.1]-[3.3]. Un sistema virtual debe comportarse según los fundamentos matemáticos que describen al sistema analógico implementado y se debe tener la certeza que la información obtenida de la “experimentación” sean datos de confianza. No es suficiente generar las funciones matemáticas en un lenguaje de programación y realizar su cálculo numérico. Dentro de la implementación es necesario analizar minuciosamente el comportamiento y los resultados del sistema virtual para afirmar que representa adecuadamente al sistema real bajo estudio.

El sistema analógico modelado es un conjunto de elementos cuyas propiedades se desean conocer más a fondo. La finalidad es desarrollar experiencias optimizadas o comprender más la naturaleza de los fenómenos involucrados. Por lo tanto, la selección y definición de lo que constituye el sistema virtual debe estar guiado por el uso que se va a hacer de él.

En un experimento virtual no es posible tener en cuenta todas las variables analógicas que se pueden presentar. Muchas veces los métodos experimentales suelen estar bajo la influencia de entradas inaccesibles, llamadas entradas de perturbación. Por ejemplo,

al trabajar con una fuente altamente coherente, se producirá el efecto inherente del *speckle* el cual es muy difícil de minimizar, otro ejemplo podrían ser las vibraciones en una mesa holográfica las cuales no se pueden controlar, etc. De la misma manera, gran parte de las salidas que son útiles del sistema no son accesibles por medidas directas. Éstas suelen denominarse estados internos del sistema. En este sentido, el experimentador debe restringirse a seleccionar los detalles más significativos sin descartar variables que conduzcan a la pérdida de generalidad de la experiencia analógica.

Alguna razones para adquirir esta estrategia de trabajo usando sistemas virtuales están asociadas muchas veces con problemas prácticos en la realización de un experimento real [3.2]. Para dar un ejemplo, el experimento podría ser demasiado costoso, demasiado peligroso o el sistema sobre el que se desea experimentar podría aún no existir. Otras razones están asociadas al hecho que el conocimiento ganado sugiere mejoras para el sistema analógico. De la misma manera, los sistemas virtuales pueden ser usados para reforzar o verificar soluciones analíticas, además permite experimentar con nuevos diseños antes de la implementación experimental y hace posible que los sistemas puedan ser empleados por personas no calificadas, entre otras [3.3].

Inicialmente, para construir un sistema virtual, se debe plantear el concepto de modelo. Este puede considerarse como un sistema abreviado que refleja las propiedades más relevantes del sistema real. Si se implementa un modelo lo suficientemente realista del sistema analógico se lo podrá emplear para investigar y responder preguntas sobre su comportamiento. Esto implica que se le puede aplicar un “experimento” sin realizar experimentos sobre el sistema mismo.

Los sistemas representados mediante modelos matemáticos en un lenguaje de programación se denominan a menudo prototipos virtuales [3.2]. El proceso de construir, optimizar e investigar sobre tales modelos se le puede llamar “experimentación virtual”. Algunas veces, el término “modelado físico” también es empleado dentro este contexto.

El marco de esta Tesis está desarrollado sobre el concepto de sistemas ópticos virtuales y su aplicación específica será al estudio de sistemas ópticos de encriptación. Estudiar un sistema óptico bajo el concepto de SOV significa que todos los elementos

analógicos de la arquitectura son implementados digitalmente adoptando las bases teóricas de los conceptos involucrados en el procesamiento óptico de información. Bajo esta visión, los procesos de propagación, procesos de difracción u otros procesos relevantes serán implementados estrictamente en el marco de la óptica virtual. Se restringe la aplicación a sistemas ópticos que cumplen los requerimientos para los cuales la teoría escalar de la difracción tiene validez.

Para implementar en un SOV una arquitectura de encriptación, en primera medida se deben entender las descripciones matemáticas del fenómeno de propagación en el espacio libre y su correspondiente discretización. En segunda instancia se deben conocer las representaciones discretas de los elementos ópticos involucrados en las arquitecturas de codificación como lentes, pupilas, difusores, etc. para realizar su implementación digital. Por último se debe asegurar el buen funcionamiento de la articulación de estas componentes realizando experimentos virtuales de algunas experiencias conocidas de procesamiento óptico de información comparando los resultados obtenidos con lo reportado en la teoría.

Consecuentemente, en este capítulo se describen los conceptos necesarios para implementar elementos ópticos virtuales que permitan modelar y analizar sistemas ópticos analógicos de diferente complejidad. En la Sección 3.2, se presentan los fundamentos básicos de difracción y la discretización de la propagación de ondas planas en el espacio libre. El primer tratamiento discreto de este fenómeno es implementado sobre el espectro angular de ondas planas. El segundo tratamiento discreto es realizado sobre las aproximaciones de Fresnel y Fraunhofer del principio de Huygens-Fresnel. En la Sección 3.3 se enuncian las expresiones básicas para implementar digitalmente lentes, pupilas ópticas, redes de amplitud sinusoidales y difusores ópticos. En la Sección 3.4 se muestra la concordancia entre los resultados de la teoría y los obtenidos mediante las arquitecturas de procesamiento óptico implementadas en SOV. Las experiencias van desde la simple propagación en el espacio libre de un campo complejo, un sistema formador de imágenes, arquitecturas para formar *speckle* objetivo y subjetivo, etc., hasta la reconstrucción de un holograma digital. Por último, en la Sección 3.5 se describe el proceso para implementar digitalmente el sistema de codificación de doble máscara de fase en configuración $4f$.

3.2 Representación discreta del proceso de propagación en el espacio libre

En la década del 80 del siglo XIX, Kirchhoff realizó el desarrollo matemático con el cual demostró que las hipótesis propuestas en la formulación del principio de Huygens-Fresnel [3.4] son resultados que surgen naturalmente de las ecuaciones de Maxwell que describen el comportamiento ondulatorio de la luz [3.5], [3.6]. Para realizar esta demostración, Kirchhoff planteó dos condiciones de contorno para resolver satisfactoriamente el problema de difracción de una abertura en una pantalla opaca plana infinita. Sin embargo, se comprobó que las condiciones de contorno de Kirchhoff eran incompatibles. Tiempo después Sommerfeld modificaría las condiciones de Kirchhoff para evitar dicha incompatibilidad [3.7], [3.8] y dar las bases sólidas para el desarrollo de la teoría escalar de la difracción.

Los planteamientos matemáticos realizados por Rayleigh-Sommerfeld explican con mucha precisión una gran cantidad de fenómenos ópticos, sin embargo esta teoría no funciona de manera general en todos los casos. Esto es debido a que se asume un tratamiento escalar de la luz, es decir, se manipula una sola componente del campo electromagnético, desacoplando el campo eléctrico y el campo magnético para tratarlos independientemente y por igual. No obstante, la teoría escalar de la difracción presenta resultados muy precisos si se cumplen las siguientes condiciones: 1) el tamaño del objeto que difracta es grande en comparación con la longitud de onda de la luz y 2) el plano de observación del campo difractado no se encuentra demasiado cerca de la abertura, aproximadamente a una distancia mayor a cuatro veces la longitud de onda de la luz. De esta manera, esta teoría y sus aproximaciones permiten realizar un análisis preciso de los sistemas ópticos que cumplen con estas condiciones como, por ejemplo, en los sistemas de formación de imágenes, reconocimiento de patrones, tratamiento óptico de señales, encriptación óptica de información, entre otros.

Sin duda, las experiencias mencionadas tienen como fenómeno principal a la propagación del campo complejo de un frente de onda. Por esta razón, a continuación se

presentan los conceptos necesarios para realizar su implementación como un elemento óptico virtual.

3.2.1 Espectro angular de ondas planas

La amplitud compleja de cualquier perturbación óptica monocromática propagándose en el vacío o en un medio dieléctrico homogéneo obedece a la ecuación de Helmholtz:

$$(\nabla^2 + k^2)U(\vec{r}) = 0 \quad (3.1)$$

donde ∇^2 es el operador Laplaciano, k es el número de onda igual a $2\pi/\lambda$, λ es la longitud de onda y $U(\vec{r})$ es una amplitud compleja, función de la posición \vec{r} , y es igual a $E(\vec{r})e^{j\Theta(\vec{r})}$, donde $E(\vec{r})$ y $\Theta(\vec{r})$ son la amplitud y la fase del fasor, respectivamente.

Un primer modo de resolver el problema de difracción es dar solución a esta ecuación haciendo uso de la noción del espectro angular de las ondas planas [3.10], [3.11], [3.12]. Este método frecuencial presenta la propagación del campo complejo de una onda plana como un sistema lineal en el sentido de la teoría de las señales.

Para abordar este tratamiento se considera el campo complejo de una onda $U(x, y, z)$ propagándose en la dirección z . La representación del campo de la onda a la distancia $z = 0$, en términos de su transformada de Fourier, está dada por:

$$U(x, y, 0) = \iint_{-\infty}^{\infty} A(f_x, f_y, 0) e^{j2\pi(f_x x + f_y y)} df_x df_y \quad (3.2)$$

donde

$$A(f_x, f_y, 0) = \iint_{-\infty}^{\infty} U(x, y, 0) e^{-j2\pi(f_x x + f_y y)} dx dy \quad (3.3)$$

La expresión $A(f_x, f_y, 0)$ es llamado el espectro angular de $U(x, y, 0)$ y la cantidad $A(f_x, f_y, 0)e^{j2\pi(f_x x + f_y y)}$ en la Ecuación (3.2) es una onda plana en el plano $z = 0$, con frecuencias espaciales f_x y f_y . Las frecuencias espaciales están definidas en términos de las

componentes del vector de onda \vec{k} , dadas por $k_i = \alpha_i 2\pi/\lambda$. Esta onda plana se propaga según los cosenos directores α_i , donde $i = x, y, z$, los cuales están definidos como $\alpha_x = \lambda f_x$, $\alpha_y = \lambda f_y$ y $\alpha_z = (1 - \lambda^2 f_x^2 - \lambda^2 f_y^2)^{1/2}$ y la relación de sus cuadrados está dada por $\alpha_x^2 + \alpha_y^2 + \alpha_z^2 = 1$.

Ahora, el campo de la onda a una distancia z en términos de su espectro angular esta dado por:

$$U(x, y, z) = \iint_{-\infty}^{\infty} A(f_x, f_y, z) e^{j2\pi(f_x x + f_y y)} df_x df_y \quad (3.4)$$

Sustituyendo la Ecuación (3.4) en la Ecuación (3.1) lleva a la ecuación:

$$\iint_{-\infty}^{\infty} \left\{ \frac{d^2}{dz^2} A(f_x, f_y, z) + [k^2 + 4\pi^2(f_x^2 + f_y^2)] A(f_x, f_y, z) \right\} e^{j2\pi(f_x x + f_y y)} df_x df_y = 0 \quad (3.5)$$

que tiene como solución:

$$A(f_x, f_y, z) = A(f_x, f_y, 0) e^{jz \sqrt{k^2 - 4\pi^2(f_x^2 + f_y^2)}} \quad (3.6)$$

De esta manera, si el campo de entrada $U(x, y, 0)$ es conocido, su espectro angular $A(f_x, f_y, 0)$ puede ser calculado y posteriormente el campo $U(x, y, z)$ difractado a la distancia z puede ser determinado usando la Ecuación (3.6) y la Ecuación (3.4).

Ahora, los límites de integración pueden ser acotados a una región circular:

$$4\pi^2(f_x^2 + f_y^2) \leq k^2 \quad (3.7)$$

siempre y cuando z sea mucho mayor que la longitud de onda de tal manera que las ondas evanescentes no sean tenidas en cuenta. Esto implica tener una frecuencia de corte de módulo $f_c = 1/\lambda$ indicando que dentro de la teoría escalar de la difracción, la onda electromagnética difractada no puede llevar información correspondiente a detalles menores que λ .

Bajo estas condiciones se muestra que la propagación en un medio homogéneo es equivalente a un filtro lineal espacial en dos dimensiones con una función de transferencia que está dada por:

$$H(f_x, f_y) = \begin{cases} e^{jz\sqrt{k^2 - 4\pi^2(f_x^2 + f_y^2)}} & 4\pi^2(f_x^2 + f_y^2)k^2 \\ 0 & \text{en otro caso} \end{cases} \quad (3.8)$$

De esta manera, la propagación de una onda en la dirección z en el campo cercano y en el campo lejano es correctamente descrita por la propagación del espectro angular.

Si $\mathcal{F}[\]$ y $\mathcal{F}^{-1}[\]$ denotan la transformada de Fourier y la transformada inversa de Fourier, respectivamente, el campo complejo de la onda en el plano z puede ser escrito como:

$$U(x, y, z) = \mathcal{F}^{-1} \left[\mathcal{F}[U(x, y, 0)] e^{jkz\sqrt{1 - \alpha_x^2 - \alpha_y^2}} \right] \quad (3.9)$$

La Ecuación (3.9) representa la amplitud compleja de una onda plana viajando en la dirección especificada por los cosenos directores. En este caso, el efecto de la propagación es modificar las fases relativas de las ondas según la cantidad $\exp(jkz\sqrt{1 - \alpha_x^2 - \alpha_y^2})$ sin cambiar sus amplitudes.

3.2.2 Aproximaciones del principio de Huygens-Fresnel

Un segundo método para calcular la difracción del campo complejo de una onda se obtiene al realizar algunas aproximaciones sobre el principio de Huygens-Fresnel. La aproximación de Fresnel y la aproximación de Fraunhofer son expresiones matemáticas menos complejas que permiten calcular los patrones de difracción más fácilmente y de manera muy precisa [3.13]-[3.15].

3.2.2.1 Aproximación de Fresnel

La aproximación de Fresnel consiste en tomar los tres primeros términos de la expansión en series de Taylor de la distancia r medida entre un punto en el plano del objeto y un punto en el plano de observación para aproximar ondas esféricas por superficies

cuadráticas en la Ecuación (3.10) que representa al campo complejo del objeto a la distancia z :

$$U(x_0, y_0, z) = \frac{1}{j\lambda} \iint_{-\infty}^{\infty} U(x, y, 0) \frac{z}{r^2} e^{jkr} dx dy \quad (3.10)$$

donde $U(x, y, 0)$ es el campo de entrada, $U(x_0, y_0, z)$ es el campo de salida, k es el número de onda igual a $2\pi/\lambda$, λ es la longitud de onda y r es la longitud del vector desde el punto $(x, y, 0)$ al punto (x_0, y_0, z) .

Tomando los tres primeros términos del desarrollo en series de r se tiene que:

$$r = [z^2 + (x_0 - x)^2 + (y_0 - y)^2]^{1/2} \cong z \left(1 + \frac{g}{2}\right) \quad (3.11)$$

donde, $g = (x_0 - x)^2 + (y_0 - y)^2/z^2$. El cuarto término y los que le siguen se pueden despreciar ya que son mucho menores que la longitud de onda λ .

El error introducido por despreciar los términos de orden superior y al aproximar $r \cong z$ en el denominador en la Ecuación (3.10) es considerablemente pequeño. Por otro lado, pequeños cambios en el argumento de la exponencial hace que la función varíe rápidamente produciendo cambios significativos. Por lo tanto, se reemplaza la Ecuación (3.11) en la función exponencial. De esta manera, la Ecuación (3.10) puede ser reescrita como:

$$U(x_0, y_0, z) = \frac{e^{jkz}}{j\lambda z} \iint_{-\infty}^{\infty} U(x, y, 0) \exp\left\{j \frac{k}{2z} [(x_0 - x)^2 + (y_0 - y)^2]\right\} dx dy \quad (3.12)$$

El siguiente término en la expansión de series de Taylor estima la magnitud del error máximo en la fase dado por:

$$E_{max} \leq \frac{1}{8} z g^2 k \quad (3.13)$$

Esta relación establece que la aproximación de Fresnel no es lo suficientemente buena en problemas donde E_{max} sea más grande que 1 radián. Para una abertura de 1 cm, una región de observación de 1 cm, una longitud de onda de 500 nm, se obtendrán mediciones precisas en el plano de observación ubicado a una distancia $z \gg 25$ cm. Sin embargo, esta condición en la parte experimental puede ser flexible y no tan restrictiva como su valor teórico. Una explicación para este hecho puede ser dada en términos del método de fases estacionarias [3.16]-[3.19].

Separando las variables que representan las coordenadas de los planos de entrada y salida en la Ecuación (3.12) se tiene que el campo de salida puede ser expresado usando una integral de Fourier de la siguiente manera:

$$U(x_0, y_0, z) = \frac{e^{jkz}}{j\lambda z} e^{jk \frac{(x_0^2 + y_0^2)}{2z}} \iint_{-\infty}^{\infty} U(x, y, 0) e^{jk \frac{(x^2 + y^2)}{2z}} e^{-j2\pi(f_x x + f_y y)} dx dy \quad (3.14)$$

donde las frecuencias espaciales f_x y f_y están definidas por:

$$f_x = \frac{x_0}{\lambda z} \quad y \quad f_y = \frac{y_0}{\lambda z} \quad (3.15)$$

Se referencia a la Ecuación (3.12) y la Ecuación (3.14) como la integral de difracción de Fresnel.

3.2.2.2 Aproximación de Fraunhofer

Esta aproximación describe el frente de onda a una distancia lejana del plano del objeto (campo lejano). La condición sobre la distancia de propagación $z \gg k(x^2 + y^2)/2$ permite aproximar en la Ecuación (3.14) el factor de fase $\exp[jk(x^2 + y^2)/2z]$ a la unidad. Por lo tanto, el campo complejo difractado puede ser encontrado directamente usando una transformada de Fourier de la distribución en el plano de entrada como:

$$U(x_0, y_0, z) = \frac{e^{jkz}}{j\lambda z} e^{jk \frac{(x_0^2 + y_0^2)}{2z}} \iint U(x, y, 0) e^{-j2\pi(f_x x + f_y y)} dx dy \quad (3.16)$$

donde f_x y f_y son frecuencias espaciales que están dadas por las expresiones de la Ecuación (3.15). Bajo esta aproximación la intensidad es proporcional al cuadrado del módulo de la cantidad $U(x_0, y_0, z)$ eliminándose los factores de fase cuadráticos y coincidiendo con el cuadrado del módulo de la transformada de Fourier del objeto difractado.

Se debe notar que si se emplea un elemento óptico que compense el factor de fase cuadrático antes de la difracción del objeto no es necesario usar esta aproximación. Este es el caso de una lente convergente (ver Sección 3.3.1). Este elemento óptico (según la posición en que se encuentre respecto al objeto) actúa como un filtro que elimina o compensa el factor de fase cuadrático que acompaña al objeto de entrada en la Ecuación (3.14).

Para implementar un elemento óptico virtual es necesario realizar una descripción, de cada uno de los fenómenos que se quiere modelar, en forma discreta.

3.2.3 Implementación del espectro angular de ondas planas usando la transformada rápida de Fourier (*FFT*)

Al hacer referencia a la Figura 3.1, el espectro angular de las ondas planas que relaciona el campo $U(x, y, z)$ con el campo $U(x, y, 0)$ puede ser implementado usando la transformada rápida de Fourier discretizando y truncando las variables del espacio y de las frecuencias de la siguiente manera [3.20]:

$$\begin{aligned} x &= n_x \Delta x \\ y &= n_y \Delta y \\ f_x &= m_x \Delta f_x \\ f_y &= m_y \Delta f_y \end{aligned} \quad (3.17)$$

donde, Δx , Δy , Δf_x y Δf_y son los intervalos de muestreo en el plano del objeto y en el plano de las frecuencias, respectivamente, n_x , n_y , m_x y m_y son números enteros que están en el rango $[0, M-1]$ siendo M el número total de elementos discretos del campo difractado en el plano de frecuencias.

De esta manera, un objeto $U(x, y, 0)$ en el plano de entrada será representado como $U(n_x \Delta x, n_y \Delta y, 0)$. Del mismo modo, su espectro angular $A(f_x, f_y, 0)$ en el plano de frecuencias será representado como $A(m_x \Delta f_x, m_y \Delta f_y, 0)$. Para evitar confusión, se emplea la notación reducida $U(n_x, n_y, 0)$ para el objeto en el plano de entrada y $A(m_x, m_y, 0)$ para su espectro en frecuencias.

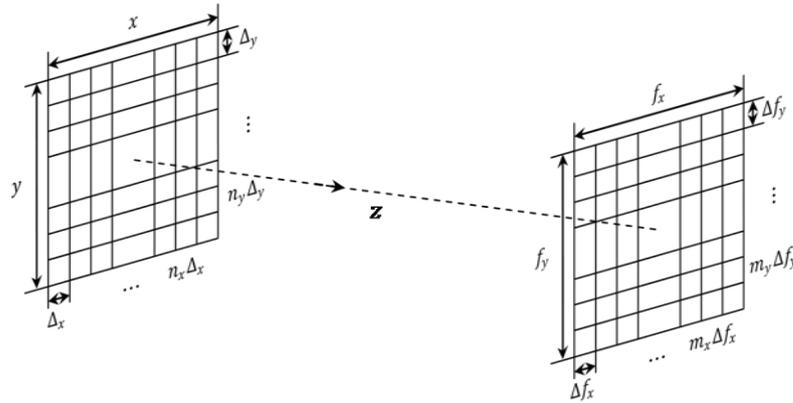


Figura 3.1: Representación discreta de las variables en el plano objeto y en el plano de frecuencias.

Por lo tanto, de forma discreta, el espectro angular del objeto de entrada puede ser expresado como:

$$A(m_x, m_y, 0) = \Delta x \Delta y \sum_{n_x} \sum_{n_y} U(n_x, n_y, 0) e^{-j2\pi(\Delta f_x \Delta x n_x m_x + \Delta f_y \Delta y n_y m_y)} \quad (3.18)$$

así, el campo de la onda a la distancia z está dado por:

$$U(n_x, n_y, z) = \Delta f_x \Delta f_y \sum_{m_x} \sum_{m_y} A(m_x, m_y, 0) e^{jz \sqrt{k^2 - 4\pi^2(\Delta f_x^2 m_x^2 + \Delta f_y^2 m_y^2)}} \times e^{j2\pi(\Delta f_x \Delta x n_x m_x + \Delta f_y \Delta y n_y m_y)} \quad (3.19)$$

Escogiendo una región rectangular en el dominio de Fourier tal que se cumplan las relaciones:

$$\begin{aligned} |k_x| &= 2\pi|f_x| \leq k \\ |k_y| &= 2\pi|f_y| \leq k \end{aligned} \quad (3.20)$$

se pueden expresar las frecuencias máximas de corte como $|f_{x_{max}}| = |f_{y_{max}}| = 1/\lambda$.

A menudo las frecuencias máximas $f_{x_{max}}$ y $f_{y_{max}}$ son conocidas. Teniendo en cuenta el número total de elementos discretos $M = M_x = M_y$, que contienen al campo difractado, escogiendo los muestreos de frecuencias $\Delta f = \Delta f_x = \Delta f_y$ y remplazando en las relaciones:

$$M_x = \frac{f_{x_{max}}}{\Delta f_x} \quad y \quad M_y = \frac{f_{y_{max}}}{\Delta f_y} \quad (3.21)$$

se encuentra que:

$$M = \frac{1}{\Delta f \lambda} \quad (3.22)$$

Ahora, si $\rho = \Delta x = \Delta y$ y $\Delta f = \Delta f_x = \Delta f_y$, para poder aplicar correctamente la **FFT** dentro del rango aceptable de las aproximaciones, se debe cumplir que:

$$\rho \Delta f = \frac{1}{N} \quad (3.23)$$

donde N es el tamaño de la matriz de frecuencias que contiene la transformada de Fourier. Con esta condición, las ecuaciones (3.18) y (3.19) pueden ser expresadas en términos de la transformada discreta de Fourier como:

$$A(m_x, m_y, 0) = \rho^2 \sum_{n_x=0}^{N-1} \sum_{n_y=0}^{N-1} U(n_x, n_y, 0) e^{-j \frac{2\pi}{N} (n_x m_x + n_y m_y)} \quad (3.24)$$

$$U(n_x, n_y, z) = (\Delta f)^2 \sum_{m_x=0}^{N-1} \sum_{m_y=0}^{N-1} A(m_x, m_y, z) e^{j \frac{2\pi}{N} (n_x m_x + n_y m_y)} \quad (3.25)$$

donde

$$A(m_x, m_y, z) = A(m_x, m_y, 0) e^{jz \sqrt{k^2 - 4\pi^2 (\Delta f_x^2 m_x^2 + \Delta f_y^2 m_y^2)}} \quad (3.26)$$

Las Ecuaciones (3.24) y (3.25) tienen un comportamiento regular con N al usar la **FFT** para calcular las transformadas discretas de Fourier [3.21], [3.22]. El uso de la **FFT** provoca un efecto de *aliasing* o llamado también efecto Nyquist, atribuido a que se realiza una convolución circular en vez de una convolución lineal dando lugar a una superposición de replicas periódicas del espectro del objeto difractado [3.23].

Para reducir este efecto el campo de entrada puede ser colocado en una matriz de ceros más grande (*zero padded*). Comúnmente para evitar errores en la medida se toma una matriz que tiene el doble de tamaño del campo discreto de entrada. Es aconsejable escoger un número que sea potencia de dos para que se ejecute más rápidamente el algoritmo de la **FFT**.

Por último, la Ecuación (3.25) tiene la forma de una transformada inversa discreta de Fourier excepto por un factor de normalización. Como $(\rho\Delta f)^2 = 1/N^2$, pueden omitirse estos factores en los cálculos y al final de las operaciones, la Ecuación (3.25) debe ser multiplicado por el factor $1/N^2$.

Resumiendo, el elemento virtual que realiza la propagación del espectro angular puede ser implementado de la siguiente manera:

1. Realizar la representación discreta del campo complejo de entrada definiendo un tamaño de muestreo espacial y un tamaño de muestreo en frecuencia.
2. Calcular el espectro angular del campo complejo de entrada usando la **FFT** según la Ecuación (3.24).
3. Calcular el espectro angular del campo complejo a una distancia de propagación z según la Ecuación (3.26).
4. Calcular el campo complejo a la distancia de propagación z usando la **FFT** según la Ecuación (3.25).

De esta forma se implementa digitalmente el fenómeno de propagación usando dos **FFT**. Este elemento virtual tiene la ventaja que puede describir la propagación en todas las regiones del espacio. Por otro lado, debido a que en todos los planos de propagación se

conserva el mismo valor de muestreo, presenta la desventaja de consumir altos recursos computacionales para su aplicación donde intervienen distancias de propagación muy grandes.

3.2.4 Implementación de la integral de Fresnel usando la transformada rápida de Fourier (FFT)

De la misma manera que la discretización del espectro angular, la integral de difracción de Fresnel puede ser evaluada y discretizada usando la transformada rápida de Fourier [3.24]. Haciendo referencia a la Figura 3.2, las variables discretizadas y truncadas en el plano del objeto y en el plano de observación de la onda difractada están dadas por:

$$\begin{aligned} x &= n_x \Delta_x \\ y &= n_y \Delta_y \\ x_0 &= m_x \Delta_{0x} \\ y_0 &= m_y \Delta_{0y} \end{aligned} \quad (3.27)$$

donde Δ_x y Δ_y , son los intervalos de muestreo en el plano del objeto, Δ_{0x} y Δ_{0y} son los intervalos de muestreo en el plano de observación y n_x , n_y , m_x y m_y son números enteros que están en el rango $[0, M-1]$ siendo M el número total de elementos discretos.

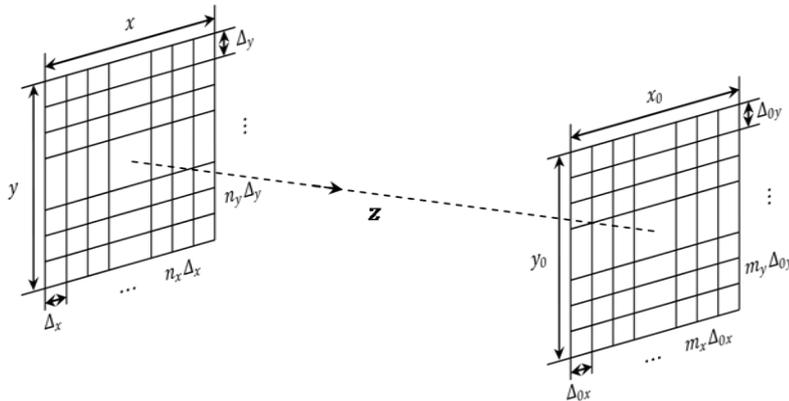


Figura 3.2: Representación discreta de las variables en el plano objeto y el plano de difracción.

Al sustituir las relaciones de la Ecuación (3.27) en la Ecuación (3.15) se encuentra que las frecuencias espaciales son expresadas como:

$$f_x = \frac{m_x \Delta_{0x}}{\lambda z} \quad y \quad f_y = \frac{m_y \Delta_{0y}}{\lambda z} \quad (3.28)$$

Ahora, al reemplazarlas en la Ecuación (3.14) y al realizar una analogía con los pesos complejos de la transformada discreta de Fourier:

$$\exp \left[-j2\pi \left(\frac{n_x m_x}{M_x} + \frac{n_y m_y}{M_y} \right) \right] \quad (3.29)$$

se deben cumplir las relaciones:

$$\Delta_{0x} \Delta_x = \frac{\lambda z}{M_x} \quad y \quad \Delta_{0y} \Delta_y = \frac{\lambda z}{M_y} \quad (3.30)$$

De esta forma, el campo difractado a una distancia z es representado por la ecuación:

$$U(m_x, m_y, z) = \beta \Delta_x \Delta_y \sum_{n_x=0}^{M_x-1} \sum_{n_y=0}^{M_y-1} U(n_x, n_y, 0) e^{jk \frac{(n_x^2 \Delta_x^2 + n_y^2 \Delta_y^2)}{2z}} e^{-j2\pi \left(\frac{n_x m_x}{M_x} + \frac{n_y m_y}{M_y} \right)} \quad (3.31)$$

donde β es el factor:

$$\beta = \frac{e^{jkz}}{j\lambda z} e^{jk \frac{(m_x^2 \Delta_{0x}^2 + m_y^2 \Delta_{0y}^2)}{2z}} \quad (3.32)$$

Es de mencionar que las condiciones de la Ecuación (3.30) hacen que se cumpla el teorema del muestreo de Nyquist-Shannon. Estas condiciones deben ser siempre respetadas al discretizar y usar transformadas rápidas de Fourier.

De forma directa, la aproximación de Fraunhofer establece que la distancia de propagación es más grande que el factor cuadrático en la exponencial que acompaña al objeto difractado. Esto es, en la Ecuación (3.14), $z \gg k(x^2 + y^2)/2$, aproximación que hace que el factor de fase cuadrático $\exp[jk(x^2 + y^2)/2z]$ dentro de la integral sea igual a la unidad. De la misma manera, en el proceso de discretización y asumiendo que se

trabajan con matrices cuadradas, $M_x = M_y = N$, en la Ecuación (3.31), la difracción en el campo lejano que representa el campo difractado a una distancia z queda expresada como:

$$U(m_x, m_y, z) = \Delta_x \Delta_y \frac{e^{jkz}}{j\lambda z} e^{jk \frac{(m_x^2 \Delta_{0x}^2 + m_y^2 \Delta_{0y}^2)}{2z}} \sum_{n_x=0}^{N-1} \sum_{n_y=0}^{N-1} U(n_x, n_y, 0) e^{-j \frac{2\pi}{N} (n_x m_x + n_y m_y)} \quad (3.33)$$

Resumiendo, el elemento virtual que realiza la propagación usando la integral de Fresnel puede ser implementado de la siguiente manera:

1. Realizar una discretización del campo complejo de entrada definiendo un tamaño de muestreo espacial.
2. Encontrar el factor β dado por la Ecuación (3.32).
3. Calcular el campo complejo a la distancia de propagación z usando la *FFT* según la Ecuación (3.31).

De esta forma se implementa digitalmente el fenómeno de propagación usando una *FFT*. Este elemento virtual tiene la ventaja que no requiere altos recursos computacionales para trabajar a distancias grandes de propagación. El tamaño de muestreo en los planos de propagación es variable y no necesita relleno de ceros para su ejecución, por lo tanto funciona eficientemente a estas distancias. Sin embargo, tiene restricciones para trabajar en el campo cercano (discusión que no se abordará en este documento ver [3.16]-[3.19]). Ya que los experimentos que se realizan en esta Tesis incumben distancias de propagación del orden de las distancias focales ($f > 5$ cm) se puede usar este elemento virtual sin restricciones.

3.3 Implementación de elementos ópticos virtuales

En la sección anterior se implementó el fenómeno de propagación en el espacio libre como un elemento virtual. Ahora, se implementan algunos componentes ópticos que se emplearán en esta Tesis para construir las arquitecturas analógicas de encriptación en SOV.

3.3.1 Lente óptica

El elemento más importante en un procesador óptico formador de imágenes es la lente. Este componente óptico puede ser estudiado desde la teoría de trazado de rayos y en forma general con la formulación de la óptica ondulatoria.

Como se mostró, bajo la aproximación de Fraunhofer la transformada de Fourier del objeto es formada cuando la distancia de observación del patrón difractado es lo suficientemente grande. Esto produce que el factor cuadrático dentro de la integral de la Ecuación (3.14) se aproxime a la unidad.

Ahora, si se emplea un elemento óptico que compense este factor de fase cuadrático antes de la difracción, se puede formar la transformada de Fourier del objeto a una distancia menor y no necesariamente en el campo lejano. En otras palabras, no se requiere usar la aproximación de Fraunhofer. Este es el caso de una lente convergente la cual actúa como un filtro lineal que elimina o compensa este factor de fase. El objeto también puede ser colocado en el plano focal anterior de la lente formando en el plano focal posterior la transformada de Fourier escalada. Esta magnificación es proporcional a la longitud de onda y a la distancia focal [3.25], [3.26].

En base a lo anterior, se puede decir que la lente es un elemento óptico que realiza una transformación de fase en el campo complejo que incide sobre ella. Idealmente, la transformación de fase de una lente perfecta (infinita y sin aberraciones) puede ser escrita como:

$$t(x, y) = e^{jk\Lambda_0} e^{-j\frac{k}{2f}(x^2+y^2)}, \quad (3.34)$$

donde Λ_0 es el espesor máximo de la lente, $k = 2\pi/\lambda$ es el número de onda, f es la distancia focal de la lente y x e y son las coordenadas del plano de la lente. La extensión finita de la abertura de la lente puede ser tomada en cuenta definiendo una función pupila (ver Sección 3.3.2) $P(x, y)$ definida por:

$$P(x, y) = \begin{cases} 1 & \text{dentro de la apertura de la lente.} \\ 0 & \text{en otro caso.} \end{cases} \quad (3.35)$$

La deducción de la Ecuación (3.34) y la convención de signos empleada, implican adoptar un signo para la distancia focal f . Así, se pueden expresar lentes de diferente tipo: lentes doble convexas, plano convexas y menisco positivas las cuales tienen una focal f positiva. En este caso se representa una onda esférica convergiendo hacia un punto ubicado atrás de la lente. Por otro lado, la distancia focal f también permite expresar lentes doble cóncavas, plano cóncavas y menisco negativas con una focal f negativa. En este caso se representa una onda esférica divergiendo hacia un punto ubicado al frente de la lente.

Una lente puede ser modelada como un elemento virtual discretizando las variables espaciales de la siguiente manera:

$$\begin{aligned} x &= m_x \Delta_x \\ y &= m_y \Delta_y \end{aligned} \quad (3.36)$$

donde, Δ_x , Δ_y son los intervalos de muestreo en el plano de la lente y donde m_x y m_y son números enteros que están en el rango $[0, N-1]$, donde N representa la longitud de elementos que tiene el vector en el *eje* x o en el *eje* y en el plano de la lente. Remplazando las variables discretas y asumiendo lentes delgadas realizando la aproximación $e^{jk\Lambda_0} \approx 1$ en la Ecuación (3.34) se obtiene la expresión:

$$L(m_x, m_y) = e^{-j\frac{k}{2f}(m_x^2\Delta_x^2 + m_y^2\Delta_y^2)} \quad (3.37)$$

De esta forma, el elemento óptico virtual $L(m_x, m_y)$ representa una lente óptica.

3.3.2 Pupilas ópticas

Las aberturas que limitan la cantidad de rayos o que limitan el campo complejo de una onda emergente en un punto determinado son llamadas pupilas ópticas. En un sistema óptico la pupila del sistema juega un papel fotométrico limitando la cantidad de iluminación que pasa por un determinado punto obstruyendo y recortando un campo emergente. En una arquitectura óptica es necesario tener en cuenta las curvaturas, posición y dimensión de la pupila ya que influyen sobre las aberraciones del sistema. Además producen el importante efecto de limitar la resolución del sistema óptico [3.27].

Generalmente para un sistema que está compuesto de varias lentes la pupila de salida del sistema es la imagen de la pupila de entrada a través de la totalidad del sistema.

La función pupila es una función matemática que describe el comportamiento general de la pupila que físicamente, de la manera más simple, es una transmitancia que tiene valores iguales a la unidad en una abertura y de transmitancia cero fuera de ella. Su forma está definida por una función bidimensional $f(x, y)$. De esta forma, la función pupila $P(x, y)$ puede ser expresada como:

$$P(x, y) = \begin{cases} 1 & \text{dentro de la abertura } f(x, y) \\ 0 & \text{en otro caso} \end{cases} \quad (3.38)$$

Por ejemplo, una abertura circular está definida por la función:

$$f(x, y) = \begin{cases} 0 & |\sqrt{x^2 + y^2}| > w \\ 1 & |\sqrt{x^2 + y^2}| \leq w \end{cases} \quad (3.39)$$

que generalmente es representada por una transmitancia de amplitud como:

$$t_A(q) = \text{circ}\left(\frac{q}{w}\right) \quad (3.40)$$

donde q es la coordenada radial en el plano de la abertura y w es su radio.

Otro ejemplo es una abertura rectangular de lados w_x y w_y la cual está definida por la función:

$$f(x, y) = \begin{cases} 1 & w_x \leq x \leq w_x \\ 0 & -w_x > x > w_x \\ 1 & w_y \leq y \leq w_y \\ 0 & -w_y > y > w_y \end{cases} \quad (3.41)$$

que generalmente es representada por una transmitancia de amplitud como:

$$t_A(x, y) = \text{rect}\left(\frac{x}{2w_x}\right) \text{rect}\left(\frac{y}{2w_y}\right) \quad (3.42)$$

Aquí, es conveniente mencionar que para las expresiones anteriores y para las expresiones de las secciones siguientes se entenderá que las variables en el espacio coordinado están discretizadas según la Ecuación (3.36) y que cada elemento es implementado digitalmente en arreglos matriciales para formar un elemento óptico virtual. De esta forma, por medio de la Ecuación (3.39) y la Ecuación (3.41), se implementa como un elemento virtual una pupila circular o una pupila rectangular, respectivamente.

3.3.3 Red de amplitud sinusoidal

En la práctica, un objeto difractivo puede ser más complejo que aberturas en una pantalla opaca finita con transmitancia unitaria en la abertura y transmitancia cero fuera de ella. En una abertura se puede introducir una atenuación espacial como, por ejemplo, una transparencia fotográfica absorbente que tenga valores reales de transmitancia $t_A(x, y)$ entre cero y la unidad. Del mismo modo, se pueden introducir patrones espaciales de corrimiento de fase por medio de placas transparentes de diferente grosor.

Un ejemplo de estos elementos difractantes es una red de amplitud sinusoidal delgada definida por la función de transmitancia:

$$t_A(x, y) = \left[\frac{1}{2} + \frac{m}{2} \cos(2\pi\nu_0 x) \right] \text{rect}\left(\frac{x}{2w}\right) \text{rect}\left(\frac{y}{2w}\right) \quad (3.43)$$

En este caso, la red es limitada por una abertura cuadrada de ancho $2w$. El parámetro m representa el cambio de amplitud entre picos y ν_0 es la frecuencia espacial de la red.

La implementación de este tipo de elementos ópticos se realiza de la misma manera que los elementos ópticos anteriores, las variables espaciales se discretizan según la Ecuación (3.36) y se implementan digitalmente en arreglos matriciales para formar un elemento virtual.

3.3.4 Difusores aleatorios

Un difusor aleatorio puede ser considerado como un conjunto de elementos dispersores de diferente forma y tamaño que introducen cambios de fases aleatorios en la luz incidente. Para implementar estos elementos virtualmente, se considera que la función que describe el

difusor es una función aleatoria que puede tomar valores entre el rango $[0,1]$ los cuales son convertidos a valores de fase pura por medio de una asignación dependiendo del número de bits con que se esté trabajando (cuantización). Por ejemplo, si se está trabajando con 8 bits, el difusor puede ser representado por un elemento que tiene una distribución de fase aleatoria uniformemente distribuida en el rango de $-\pi$ a π con 256 valores discretos de fase.

Ya que los difusores son implementados con una función de generación de números aleatorios, las dos características básicas de estos elementos son la pseudo-aleatoriedad y la impredecibilidad. La aleatoriedad pura es muy difícil de alcanzar, no obstante, siempre se trabajan con aproximaciones muy buenas de un conjunto de números aleatorios con secuencias largas donde no existe una manera para predecir el siguiente número de la secuencia. Existen varias maneras para generar secuencias de esta clase, los algoritmos computacionales regularmente usan generadores congruenciales cuadráticos, métodos aditivos, métodos mixtos, métodos mezcla, entre otros [3.28], [3.29].

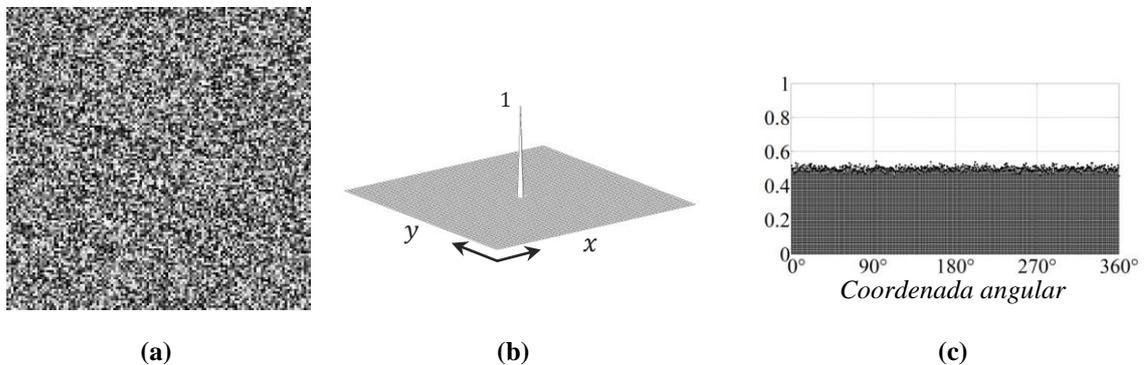


Figura 3.3: Difusor óptico en un SOV. (a) Fase del difusor, (b) Autocorrelacion de las fases y (c) Promedio angular de valores de fase.

Las propiedades de pseudo-aleatoriedad de los difusores empleados se pueden verificar por medio de la función de autocorrelación y un promediado angular de intensidades (ver Sección B.3.1). Matemáticamente un difusor R puede ser expresado como:

$$R = |t(x,y)|e^{i\varphi(x,y)} \quad (3.44)$$

donde $t(x,y)$ es la función de transmisión y $\varphi(x,y)$ es una función aleatoria de fase que tiene valores entre $-\pi$ a π distribuidos uniformemente en el plano. Nótese que la función

de transmisión $t(x, y)$ define si el difusor es de amplitud, $t(x, y) \neq 1$, o únicamente de fase pura, $t(x, y) = 1$.

La Figura 3.3 (a) muestra la fase de un difusor. En la Figura 3.3 (b) se muestra su autocorrelación donde se observa claramente un pico el cual ha sido normalizado a la unidad. Debido a las características del difusor, la operación de autocorrelación evidencia un pico angosto y agudo el cual predice que existe la mayor similitud en las posiciones de las fases sólo cuando coinciden las dos distribuciones. En caso contrario, se obtendrá una superficie de ruido y no se observara ningún pico pronunciado.

La Figura 3.3 (c) muestra el resultado del promediado angular de las fases normalizadas. Se puede notar como el promedio tiende a $1/2$ a lo largo de todas los pixeles que tienen la misma coordenada angular. Esto indica que las fases están uniformemente distribuidas en todo el plano del difusor. La misma media se obtiene al hacer promediados en diferentes direcciones.

Por lo tanto, el resultado de la autocorrelación muestra que las fases son estadísticamente independientes y el resultado del promediado angular muestra que las fases están distribuidas uniformemente sobre todo el plano.

De la misma manera que en las secciones anteriores, se aplica el argumento para implementar este componente óptico como un elemento virtuales. Esto es, las variables espaciales de la Ecuación (3.44) son truncadas y discretizadas según la Ecuación (3.36).

A continuación se exponen algunos resultados obtenidos de diferentes arquitecturas de procesamiento óptico implementadas en SOV. Cada arquitectura fue realizada con la articulación de los elementos vistos en esta sección.

3.4 Sistemas ópticos virtuales y su aplicación en sistemas de difracción e interferencia

Se ha presentado un conjunto de elementos ópticos con su representación matemática y su correspondiente discretización con el fin de modelar elementos ópticos virtuales que permitan implementar y analizar sistemas ópticos analógicos. Los sistemas implementados

pueden ser empleados como herramientas para experimentar con variantes de arquitecturas ópticas de diferente complejidad. El análisis del comportamiento de estos sistemas ante la variación de parámetros ópticos brinda la posibilidad de encontrar configuraciones que tengan grados eficientes de operatividad. De esta forma se optimizan tiempos de ejecución y se investiga eficientemente soluciones experimentales que pueden llegar a tener análisis matemáticos complejos.

A continuación se presentan un conjunto de experiencias ópticas que tienen como objetivo corroborar y afianzar el uso de los elementos ópticos virtuales y la combinación de los mismos. Se muestran resultados ya conocidos que tienen un soporte teórico ya establecido. Los resultados arrojados por los SOV deben estar acordes a lo encontrado en la literatura. Esto es usado como método de calibración y caracterización.

Inicialmente se considera un proceso de propagación libre usando el propagador virtual basado en la discretización de la integral de Fresnel. Posteriormente, se realiza un SOV que encuentra la transformada óptica de Fourier haciendo uso de una lente convergente. En este caso se realizan los procesos de propagación-lente-propagación. Seguido a esto, se implementa una variante cambiando la ubicación del objeto de entrada a una distancia Z_0 y cambiando la ubicación del plano de observación de la imagen a una distancia Z_C , así se produce un sistema virtual formador de imágenes. Seguida a esta experiencia, se realiza la difracción de una red de amplitud sinusoidal. Posteriormente, se aumenta el nivel de complejidad al introducir un difusor virtual en el plano del objeto en el sistema de propagación libre. Esto formará una distribución de *speckle*. Consecutivamente, en el sistema formador de imágenes se introducirá un difusor en el plano del objeto y una pupila de múltiples aberturas en el plano de la lente para formar una distribución de *speckle* modulada. Finalmente, la verificación de los SOV termina con la reconstrucción de un holograma digital usando los dos elementos virtuales de propagación (espectro angular e integral de Fresnel). Este apartado es mostrado en el Apéndice A.

A los valores de los resultados obtenidos de las siguientes experiencias se les ha aplicado la operación de redondeo. Los valores del muestreo del plano de salida son definidos por la Ecuación (3.23) y la Ecuación (3.30) según el algoritmo usado para el

elemento virtual de propagación. Estos valores definen la precisión en el plano de observación. Por ejemplo, si el tamaño de muestreo de entrada es de $10\ \mu\text{m}$, la longitud de onda de $632.8\ \text{nm}$, se realiza una observación a una distancia de $150\ \text{mm}$ y si la matriz que contiene la distribución de salida es de tamaño 4096×4096 , el tamaño del pixel de salida es de $2.3\ \mu\text{m}$ y resulta en la precisión del sistema.

3.4.1 Propagación en el espacio libre

Estrictamente hablando, la propagación es la base fundamental del diseño y funcionamiento de los SOV. Su aplicación se encuentra implícita en todos los sistemas implementados. Se debe hacer énfasis que se trabaja en el campo lejano únicamente. Consecuentemente se puede aplicar cualquier elemento virtual de propagación. Por este motivo es importante evaluar el comportamiento de los SOV a estas distancias de propagación.

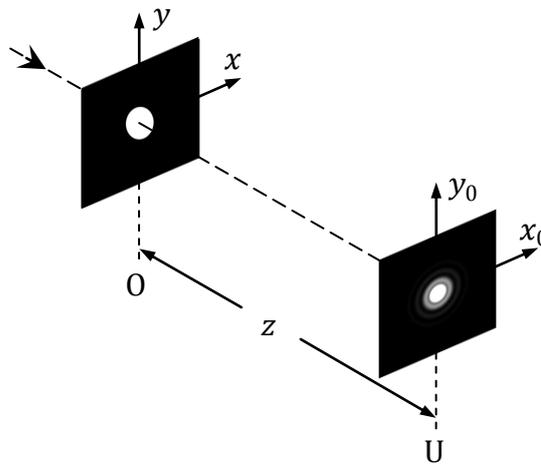


Figura 3.4: Propagación en el espacio libre de una apertura circular. O es el plano del objeto, U es el plano del campo complejo propagado y z es la distancia de propagación medida desde el plano objeto.

Como primer ejemplo se ha tomado la distribución de difracción de una pupila que tiene una abertura circular. Haciendo referencia a la Figura 3.4, la pupila es representada matemáticamente por la Ecuación (3.40). Su patrón de difracción en la región de Fraunhofer tiene forma de círculos concéntricos. El primer mínimo forma el disco de Airy cuyo radio está dado por [3.30]:

$$q = 1.22 \frac{\lambda z}{2w} \quad (3.45)$$

donde λ es la longitud de onda, z es la distancia de propagación y w es el radio de la abertura circular. La amplitud compleja de la distribución en la región de Fraunhofer puede ser expresada como:

$$U(r) = e^{jkz} e^{j\frac{kr^2}{2z}} \frac{\pi w^2}{j\lambda z} \left[2 \frac{J_1(kwr/z)}{kwr/z} \right] \quad (3.46)$$

donde r es la coordenada radial en el plano de observación. La intensidad en la región de Fraunhofer está determinada por el producto de la Ecuación (3.46) por su conjugado.

La experiencia óptica virtual consiste en iluminar con una longitud de onda de 632.8 nm una abertura circular de diámetro 300 μm y observar el patrón de difracción a una distancia de 80 mm. El sistema realiza la propagación en el espacio libre del frente de onda proveniente del objeto de entrada.

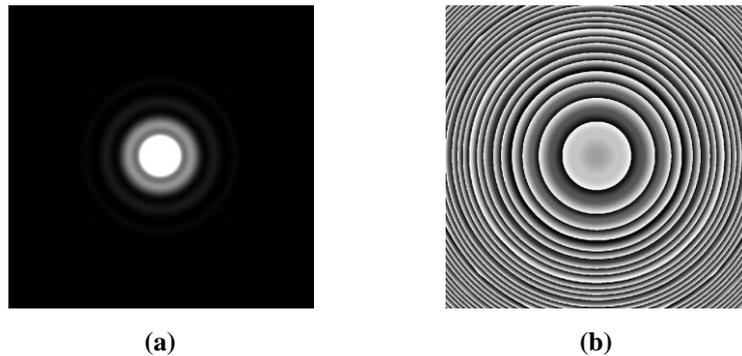


Figura 3.5: Propagación en el espacio libre de una abertura usando un sistema óptico virtual. (a) intensidad y (b) fase del patrón obtenido.

En la Figura 3.5 se muestra la intensidad y la fase, respectivamente, del patrón difractado por la abertura circular. Con estos parámetros ópticos el valor teórico del diámetro del disco de Airy determinado por la Ecuación (3.45) es de 411.7 μm y el obtenido al medir el diámetro del disco de Airy en el patrón obtenido por el SOV es de aproximadamente 410.3 μm . Esto corrobora que bajo la teoría escalar de difracción, el fenómeno de difracción es bien descrito si se implementa la experiencia en un SOV.

Ahora bien, la propagación en el espacio libre de un campo de entrada hasta formar su transformada de Fourier no es de gran utilidad experimentalmente debido a que se forma en la región de Fraunhofer o a distancias de propagación z muy grandes

produciendo un espectro ensanchado que esta escalado con la cantidad λz . Como se ha mencionado, la transformada de Fourier puede ser observada a distancias menores si el objeto de entrada es iluminado por una onda esférica que converge hacia el observador o si una lente positiva es apropiadamente situada entre el observador y el objeto.

3.4.2 Transformada óptica de Fourier

Un caso particular del uso de una lente positiva para procesar información es colocándola entre el observador y el objeto de entrada a una separación igual a su distancia focal. Este sistema realiza la transformada óptica de Fourier y es implementado en un SOV de la siguiente manera: el frente de onda de entrada se propaga, según la Ecuación (3.31), una distancia igual a la distancia focal de la lente, el campo complejo resultante interactúa con la lente óptica virtual representada por la Ecuación (3.37). Finalmente, haciendo uso nuevamente del proceso discretizado de la Ecuación (3.31), el frente de onda emergente de la lente se vuelve a propagar una distancia igual a la distancia focal. Cuando el objeto de entrada es ubicado en el plano frontal de la lente, la curvatura de fase desaparece dejando la relación exacta de la transformada de Fourier formada en el plano focal posterior de la lente [3.31].

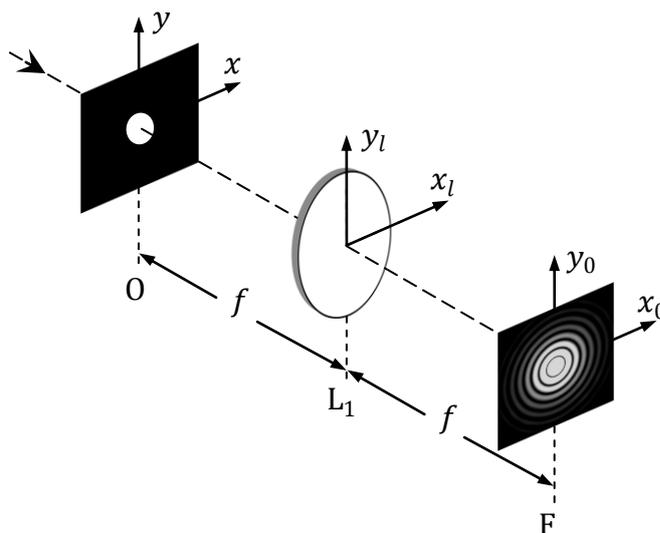


Figura 3.5: Transformada de Fourier de una apertura circular realizada por una lente. O es el plano del objeto, L_1 es el plano de la lente, F es el plano del plano de Fourier y f es la distancia focal de la lente.

En la Figura 3.5 se muestra la representación de una abertura circular de diámetro $300\ \mu\text{m}$ que es iluminada con una longitud de onda de $632.8\ \text{nm}$ y que es colocada en el plano focal frontal de una lente que tiene una distancia focal de $150\ \text{mm}$.

En el plano posterior de la lente se encuentra la transformada de Fourier de la abertura circular la cual sirve para evaluar el comportamiento del sistema óptico virtual. La Figura 3.6 (a) muestra la intensidad y la Figura 3.6 (b) la fase de la transformada de Fourier de la abertura circular. Se puede observar que este SOV reproduce muy bien esta experiencia de difracción cuya teoría predice que el valor del primer mínimo que define el radio del disco de Airy está dado por la Ecuación (3.45). El valor teórico encontrado para el diámetro del disco de Airy usando los parámetros ópticos antes mencionados es de $772\ \mu\text{m}$, mientras que el valor obtenido en el SOV es aproximadamente de $770\ \mu\text{m}$.

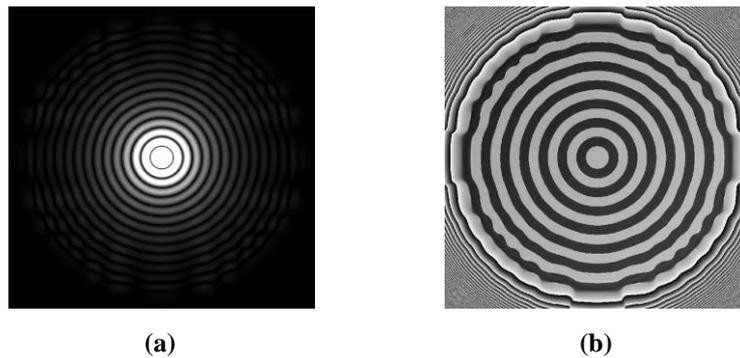


Figura 3.6: Transformada de Fourier realizada por un sistema óptico virtual. (a) intensidad y (b) fase del patrón obtenido.

De esta experiencia se puede observar como los círculos concéntricos del patrón de la fase y del patrón de intensidad empiezan a perder levemente su forma circular. Este efecto es atribuido a la discretización en los bordes de la abertura que tienden a una línea escalonada y no a una línea continua, por lo tanto, los bordes de la pupila producen este efecto que se ve reflejado en la amplitud y en la fase de la transformada de Fourier.

Este sencillo ejemplo sirve para caracterizar las lentes ópticas virtuales y los elementos virtuales que realizan la propagación en el espacio libre.

3.4.3 Sistema formador de imágenes

Teniendo presente la sección anterior, si el objeto es colocado a una distancia mayor que la distancia focal, se obtendrá un sistema formador de imágenes, la imagen ideal producida por un sistema óptico limitado por la difracción y libre de aberraciones, es una versión escalada e invertida de la imagen original. El efecto que produce la difracción en la imagen observada es la pérdida de detalles finos del objeto debido a la convolución de la imagen ideal con el patrón de difracción de Fraunhofer de la pupila de la lente. Esto resulta en la pérdida de fidelidad de la imagen original [3.31].

Según la óptica geométrica, y haciendo referencia a la Figura 3.6, la imagen se formará siguiendo la relación:

$$\frac{1}{f} = \frac{1}{Z_C} + \frac{1}{Z_0} \quad (3.47)$$

donde f es la distancia focal de la lente, Z_0 es la distancia medida desde la lente al plano del objeto y Z_C es la distancia medida desde la lente al plano de observación de la imagen.

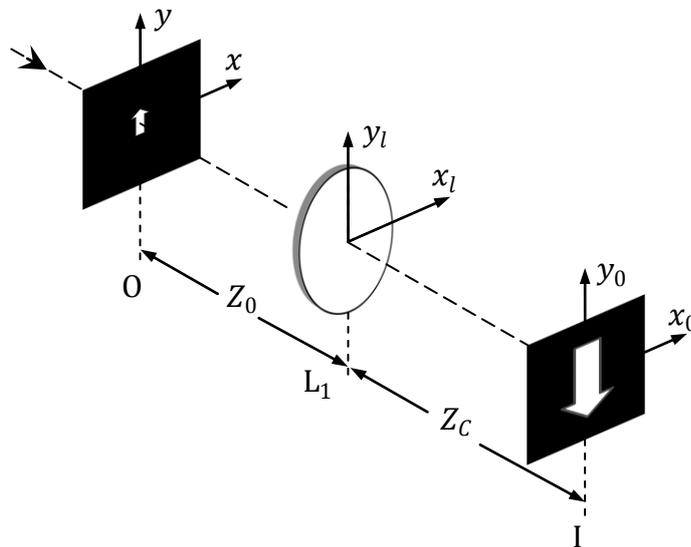


Figura 3.6: Esquema de un sistema formador de imágenes implementado en un SOV. O es el plano del objeto, L_1 es el plano de la lente, I es el plano de la imagen, f es la distancia focal de la lente Z_0 es la distancia medida desde la lente al plano del objeto y Z_C es la distancia medida desde la lente al plano de observación de la imagen.

Para implementar esta configuración como un SOV, el objeto de entrada es ubicado a una distancia de 300 mm de la lente y es iluminado con una longitud de onda de 632.8 nm. La implementación de este sistema implica emplear la Ecuación (3.31) para propagar una distancia Z_0 , posteriormente el campo resultante interacciona con la lente óptica virtual representada por la Ecuación (3.37) y finalmente se hace uso de la Ecuación (3.31) propagando una distancia Z_C .

La lente tiene una distancia focal de 150 mm, por lo tanto, la fórmula gaussiana para las lentes indica que la imagen del objeto se formará a una distancia de 300 mm medida desde el plano de la lente. Para esta configuración la imagen será real, invertida y del mismo tamaño.

La Figura 3.7 (a) muestra el objeto de entrada y las Figuras 3.7 (b)-(d) muestran las imágenes observadas a tres distancias diferentes medidas desde el plano de la lente. Estas distancias son 250 mm, 350 mm y 300 mm, respectivamente. La magnificación del sistema está dada por $M = -Z_C/Z_0$, donde el signo negativo significa que la imagen es invertida. La Figura 3.7 (b) es la distribución de intensidad observada a una distancia de 250 mm, es decir, 50 mm menos del punto de formación de la imagen. Se nota como la distribución observada es de menor tamaño que la imagen original. Por lo contrario, la Figura 3.7 (c) es el frente de onda observado a una distancia de 350 mm, es decir 50 mm más allá del punto de formación de la imagen. Aquí se puede notar como esta distribución es de mayor tamaño que la imagen original representando una mayor propagación o un desenfoque abrupto.

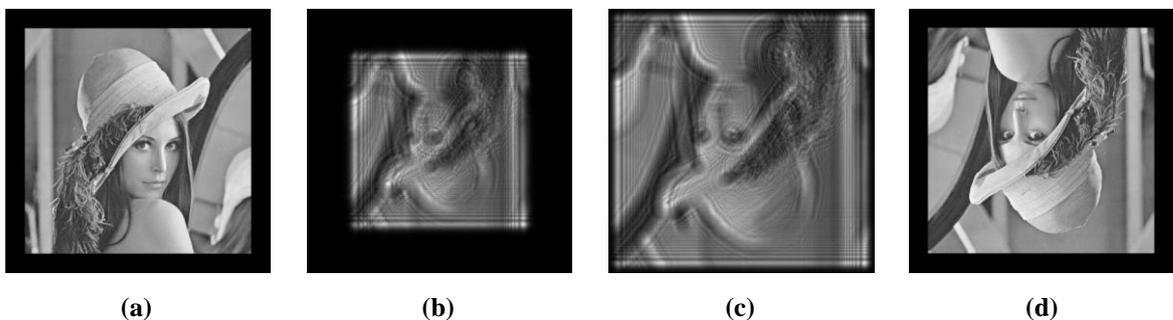


Figura 3.7: Sistema formador de imágenes usando un sistema óptico virtual. (a) Imagen original, imagen observada a una distancia de (b) 250 mm, (c) 350 mm y (d) 300 mm medida desde el plano de la lente.

Nótese como la Ecuación (3.47) no ha sido introducida explícitamente en las Ecuación (3.31) o Ecuación (3.37). No obstante, los resultados obtenidos con los SOV, que trabajan con la teoría escalar de la difracción, están acordes al tratamiento geométrico de las lentes (como debe ser) [3.31]. Esto muestra que los sistemas ópticos virtuales implementados son apropiados para estudiar procesos referentes a sistemas formadores de imágenes y otras arquitecturas experimentales que involucren lentes y procesos de propagación.

3.4.4 Difracción de una red de amplitud sinusoidal

En esta sección se implementa un SOV que realiza la difracción de una red delgada de amplitud. Su transmitancia está definida por la Ecuación (3.43):

$$t_A(\xi, \eta) = \left[\frac{1}{2} + \frac{1}{2} \cos(2\pi\nu_0\xi) \right] \text{rect}\left(\frac{\xi}{2w}\right) \text{rect}\left(\frac{\eta}{2w}\right) \quad (3.48)$$

donde ν_0 es la frecuencia espacial de la red. Se asume que está limitada por una abertura cuadrada de ancho $2w$ y que el cambio de amplitud entre picos consecutivos es la unidad, $m = 1$.

Al realizar los siguientes cálculos: la transformada de Fourier de la función periódica expresada en corchetes, la transformada de Fourier de la función rectángulo, al emplear el teorema de convolución y teniendo en cuenta la condición $\nu_0 \gg 1/w$, la distribución de intensidad del campo difractado en la región de Fraunhofer puede ser escrita como:

$$I(x, y) \approx \left[\frac{A}{j2\lambda z} \right]^2 \text{sinc}^2\left(\frac{2wy}{\lambda z}\right) \left\{ \text{sinc}^2\left(\frac{2wx}{\lambda z}\right) + \frac{1}{4} \text{sinc}^2\left[\frac{2w}{\lambda z}(x + \nu_0\lambda z)\right] + \frac{1}{4} \text{sinc}^2\left[\frac{2w}{\lambda z}(x - \nu_0\lambda z)\right] \right\}. \quad (3.49)$$

donde A es el área que limita la red. Esta función es observada en la Figura 3.14 donde se muestra el orden cero y dos órdenes difractados. El pico está normalizado a la unidad.

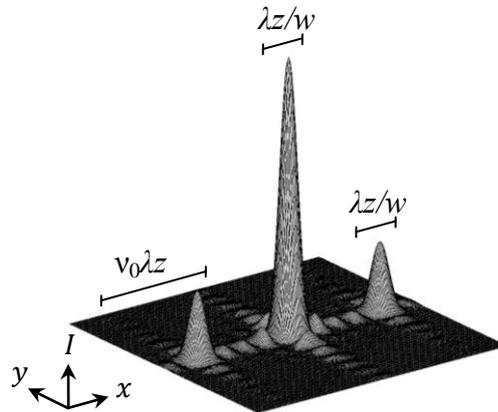


Figura 3.14: Intensidad normalizada de la difracción de Fraunhofer de una red delgada sinusoidal descrita por la Ecuación (3.43).

En la Figura 3.14 se puede observar que la mayor parte de la energía es enviada al orden cero. También se puede observar que parte de la energía va a los dos órdenes de difracción, por otro lado se debe mencionar que otra parte de la energía es absorbida por la red [3.32].

La separación espacial del primer orden de difracción desde el orden central está dada por la relación $\nu_0\lambda z$, mientras que el ancho de los lóbulos difractados está dado por $\lambda z/w$. Estas relaciones deben ser verificadas al implementar esta experiencia en un SOV.

En la experiencia virtual, se ha usado una red delgada sinusoidal de tamaño 1.3 mm con un *pitch* de aproximadamente de 260 μm . Esta red es iluminada con una longitud de onda $\lambda = 632.8 \text{ nm}$ y el plano de observación esta a una distancia de 150 mm. Los resultados de esta experiencia son mostrados en la Figura 3.15.

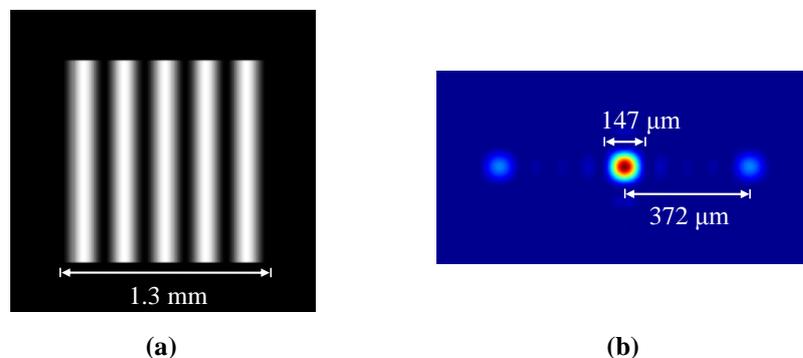


Figura 3.15: Difracción de una red de amplitud delgada sinusoidal. (a) Red de amplitud limitada por una función rectángulo, (b) difracción de la red sinusoidal a una distancia de 150mm.

Con los valores de los parámetros ópticos antes mencionados y aplicando las relaciones para la separación entre el orden central y el primer orden difractado se encuentra que el valor teórico es de aproximadamente $370.1 \mu\text{m}$, mientras que el ancho de los lóbulos del orden central y difractado tienen un valor teórico de $148.3 \mu\text{m}$. El valor encontrados en la experiencia óptica virtual para la separación entre el orden central y el primer orden difractado es de $372 \mu\text{m}$. El valor encontrado para el ancho de los lóbulos del orden central y los órdenes difractados es de $147 \mu\text{m}$. Estos valores concuerdan con gran precisión con los valores teóricos, mostrando un buen comportamiento de esta experiencia implementada en un SOV.

3.4.5 Distribuciones de *speckle*

Cuando una superficie rugosa (rugosidad comparable con la longitud de onda de la radiación incidente) es iluminada por una fuente coherente se forma una distribución aleatoria en el espacio de aspecto granular. Esta granularidad óptica o *speckle*, está relacionado con un fenómeno de interferencia aleatoria cuya descripción requiere de un análisis puramente estadístico [3.33]. El *speckle* puede ser colectado en el plano de observación después de una propagación libre (*speckle* objetivo) o en el plano de observación luego de propagarse a través de una lente (*speckle* subjetivo). Estas distribuciones derivan de la superposición de ondas generadas por la superficie en todas las direcciones interfiriendo constructiva o destructivamente conformando así la distribución de *speckle*.

La dimensión promedio de un grano de *speckle*, δt puede ser calculada evaluando las dimensiones de la región de coherencia [3.34] o por la función de autocorrelación de la intensidad en el plano de observación. Estos valores pueden ser calculados para la geometría de propagación libre o para la geometría de formación de imágenes [3.35]. En los dos casos, la dimensión promedio del grano de *speckle* es definido por el semiancho del lóbulo central de la correspondiente función de autocorrelación.

Se encuentra que la dimensión transversal promedio de un grano de *speckle* δt está dada aproximadamente por:

$$\delta t \cong 1.22 \frac{\lambda z}{q} \quad (3.50)$$

donde λ es la longitud de onda del haz de iluminación, z es la distancia entre la superficie y el plano de observación y q es el diámetro de la superficie iluminada. La distribución de *speckle* observada esta magnificada en un factor de escala λz y será constante si las fases relativas que difracta el objeto o el medio de propagación no cambian con el tiempo. En caso contrario, se llamará *speckle* dinámico [3.36]. En la Ecuación (3.50), cuando se usa una lente para coleccionar la distribución de *speckle*, el diámetro q es remplazado por el diámetro de la abertura circular de la pupila de la lente siempre y cuando sea de menor tamaño que el área de iluminación. En caso contrario q seguirá siendo el diámetro del área iluminada.

Un ejemplo de un patrón de *speckle* subjetivo modulado se muestra en la siguiente sección, por ahora se genera un *speckle* objetivo usando un SOV. Teniendo en cuenta la Figura 3.8, en el plano de entrada del sistema de propagación libre de la Sección 3.4.1 se coloca un difusor que tiene las características descritas en la Sección 3.3.4. Adosado al difusor se encuentra una pupila con una abertura circular, Ecuación (3.40), que limita el área de iluminación.

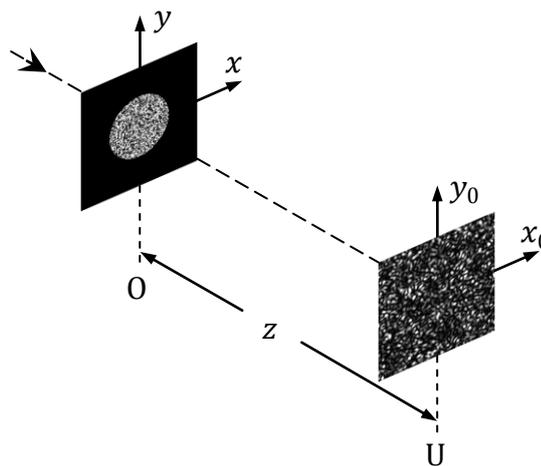


Figura 3.8: Formación de una distribución de *speckle* objetivo. O es el plano del objeto donde se encuentra el difusor, U es el plano de observación y z es la distancia de propagación.

Teniendo en cuenta lo anterior, se ilumina un área circular del difusor de 5.1 mm de diámetro con una longitud de onda de 632.8 nm. El frente de onda difractado se observa a

una distancia de propagación de 300 mm. Una versión magnificada de la distribución de *speckle* es mostrada en la Figura 3.9 (a). La Figura 3.9 (b) muestra el lóbulo central del resultado de la autocorrelación de la intensidad del *speckle*. Esta función define el tamaño promedio del grano de *speckle*.

El resultado de los cálculos teóricos predice que la dimensión transversal del grano de *speckle* en esta configuración empleando los parámetros ópticos antes mencionados es de aproximadamente $\delta t \approx 45.2 \mu\text{m}$. Al medir el ancho del lóbulo central obtenido en la autocorrelación de la distribución de intensidad de *speckle* es $\delta t \approx 46.3 \mu\text{m}$.

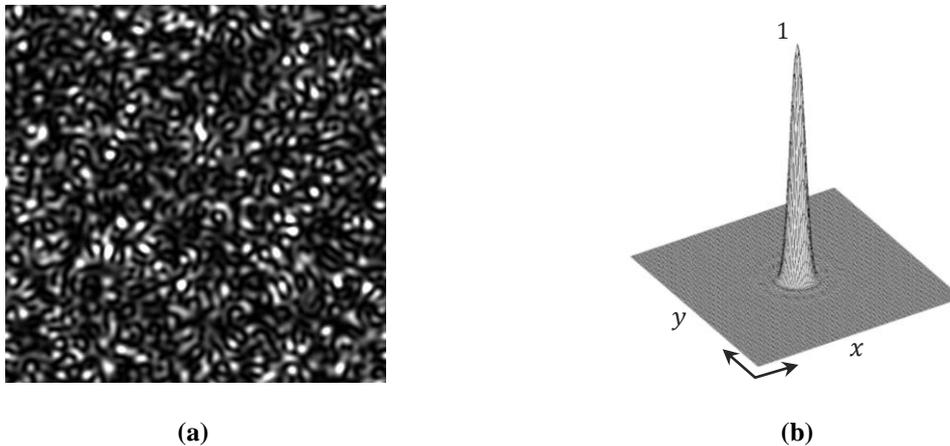


Figura 3.9: Distribución de *speckle* objetivo obtenida usando un SOV. (a) versión aumentada de la distribución de *speckle*. (b) lóbulo central de la función de autocorrelación que determina la dimensión transversal promedio del grano de *speckle*.

Es notable el acuerdo que tienen los resultados con las predicciones teóricas para los tamaños promedio de los granos de *speckle* tratándose de un proceso estocástico el cual es reproducido muy bien por el SOV implementado.

3.4.6 Distribuciones de *speckle* moduladas

El uso de las distribuciones de *speckle* como portadores aleatorios de información ha permitido que se desarrollen aplicaciones en el área de metrología óptica, filtrado espacial, transmisión de datos, entre otras. Al colocar en contacto el objeto con un difusor, la información del objeto es modulada distribuyéndose de forma aleatoria en todo el plano de observación produciendo un amplio espectro de frecuencias espaciales. Una descripción

detallada de las aplicaciones de las distribuciones de *speckle* como herramienta para procesar información puede ser encontrada en [3.37].

Una parte importante de estas aplicaciones surge cuando el *speckle* exhibe una modulación interna de la cual se puede extraer información metrológica. Cuando se emplea una pupila de doble o múltiples aberturas en cualquiera de los dos planos, en el plano del objeto en un sistema de propagación libre o en el plano de la lente en un sistema formador de imágenes, la distribución de *speckle* en el plano de observación se encuentra modulada por franjas de Young. Este sistema puede ser implementado en un SOV. La Figura 3.10 muestra la arquitectura para reproducir esta modulación interna en los granos de *speckle* debido a la presencia de una pupila con múltiples aberturas en el plano de la lente. En esta experiencia se evalúa únicamente el tamaño promedio del grano de *speckle* con el fin de mostrar el comportamiento del sistema óptico virtual. Para un análisis más detallado de esta arquitectura se puede acudir a la referencia [3.38].

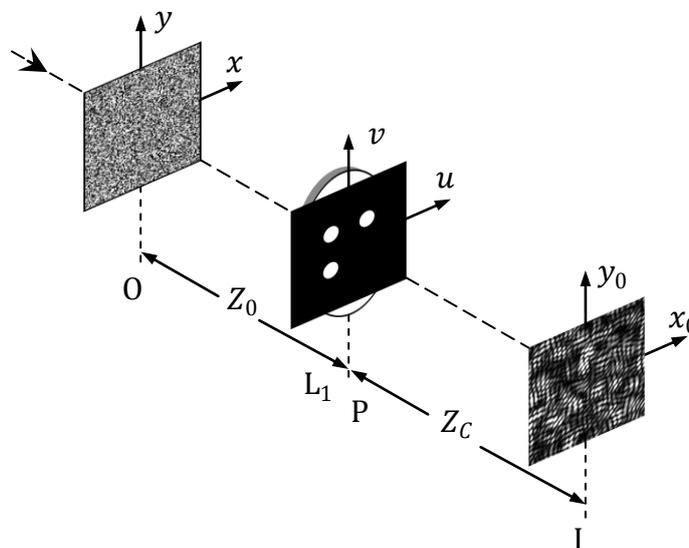


Figura 3.10: Arquitectura para reproducir un *speckle* modulado. O es el plano del objeto, L_1 es la lente de distancia focal f , I es el plano de observación, P es la pupila, Z_0 es la distancia medida desde la lente al plano del objeto y Z_c es la distancia medida desde la lente al plano de observación de la imagen.

La experiencia virtual consiste en iluminar con una longitud de onda de 632.8 nm un difusor de fase ubicado a 300 mm de una lente de 200 mm de distancia focal. En el plano de la lente se encuentra la pupila de la Figura 3.11 y el plano de observación se ubica a una distancia de 600 mm.

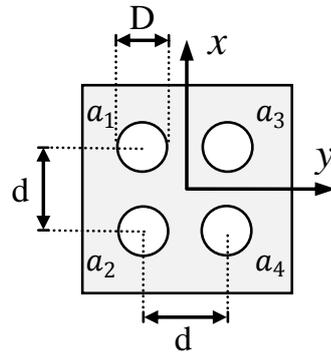


Figura 3.11: Representación esquemática de una pupila con cuatro aberturas de diámetro D localizadas sobre los vértices de un cuadrado de lado d .

La pupila en el plano de la lente está formada por varias aberturas de diámetro $D=2.37$ mm con sus centros localizados sobre los vértices de un cuadrado de lado $d=4.7$ mm. El tamaño del grano de *speckle* producido por cada una de las aberturas estará determinado por la Ecuación (3.42). El resultado de los cálculos teóricos predice que la dimensión transversal del grano de *speckle* en esta configuración empleando los parámetros ópticos antes mencionados es $\delta t \approx 195$ μm . Al medir el ancho del lóbulo central de la autocorrelación de la intensidad de las distribuciones resultantes al iluminar una apertura de la pupila es $\delta t \approx 201$ μm .

De esta experiencia, también podemos observar la modulación introducida por las franjas de Young sobre los granos de *speckle*. Al usar diferentes configuraciones para la pupila ubicada en el plano de la lente se obtienen las imágenes de la Figura 3.12 y las imágenes de la Figura 3.13. Cada una de estas distribuciones tiene dimensiones de $\sim 3 \times 3$ mm^2 .

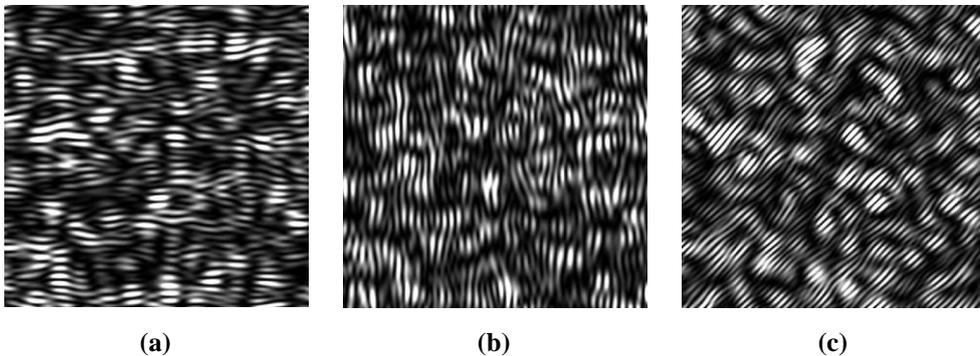


Figura 3.12: *Speckle* modulado. Cada imagen es obtenida usando la arquitectura de la Figura 3.10 empleando los pares de aberturas: (a) a_1 y a_2 , (b) a_1 y a_3 y (c) a_1 y a_4 .

En la Figura 3.12 (a) se muestran los resultados al dejar transmitir la luz por los pares de aberturas a_1 y a_j , donde $j = 2,3,4$, respectivamente. Por otro lado, las imágenes de la Figura 3.13 muestran las distribuciones de *speckle* moduladas cuando se usan dos, tres y cuatro aberturas en la pupila, respectivamente.

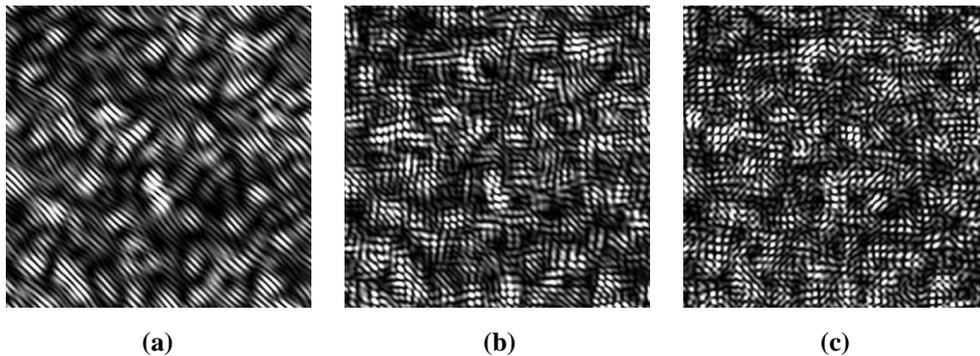


Figura 3.13: *Speckle* modulado. Cada imagen es obtenida usando la arquitectura de la Figura 3.10. En cada caso se deja transmitir luz de las aberturas (a) a_2 y a_3 , (b) a_1 , a_2 y a_3 y (c) a_1 , a_2 , a_3 y a_4 .

Se puede observar que a medida que se va aumentando el número de aberturas en la pupila, el *speckle* modulado presenta microestructuras que tienen relación con su geometría [3.39]. Un tratamiento más detallado de estas estructuras de *speckle* que tienen un alto grado de modulación puede ser encontrado en [3.40].

Finalmente, la última aplicación para asegurar el buen funcionamiento de los SOV, es presentada en el Apéndice A. Esta aplicación consiste en la reconstrucción de un holograma digital usando los elementos que describen la propagación de un frente de onda en el espacio libre.

De estas experiencias virtuales, se puede concluir que los resultados obtenidos de un SOV están acordes con lo establecido en la teoría de cada experiencia analógica. Por lo tanto, se puede afirmar que los elementos ópticos virtuales y su articulación funcionan correctamente y puede ser empleados como herramientas para evaluar sistemas ópticos que se encuentren dentro del rango de validez de la teoría escalar de la difracción.

3.5 Implementación de un sistema de encriptación en configuración $4f$ en SOV

En las secciones anteriores se ha mostrado el desempeño eficiente al articular elementos ópticos virtuales para describir arquitecturas de procesamiento de información. Estas experiencias reafirman a los SOV como una herramienta apropiada para realizar estudios de arquitecturas de diferente complejidad. Algunos casos particulares son las técnicas de encriptación óptica descritas en el Capítulo 2.

Ya que las aplicaciones de los siguientes capítulos están basadas en el sistema de codificación de doble máscara de fase en configuración $4f$, se detalla su implementación en un sistema óptico virtual. Haciendo referencia a la Figura 3.14, un sistema de encriptación en configuración $4f$ consiste de dos lentes iguales separadas una distancia $2f$. El objeto de entrada es adosado a un primer difusor m_0 . La lente L_1 realiza una primera transformada de Fourier y el espectro resultante interactúa con la llave de seguridad m_1 que se encuentra en el plano de frecuencias. Finalmente la lente L_2 realiza una última transformada de Fourier para obtener el objeto encriptado E .

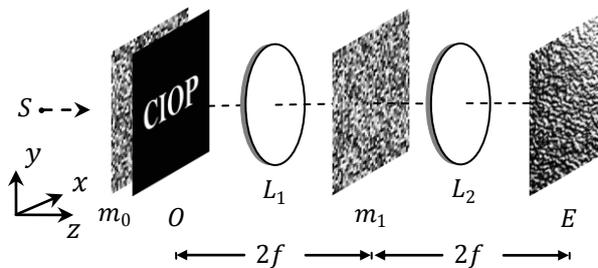


Figura 3.14: Sistema de encriptación en configuración $4f$. Etapa de encriptación. S es la fuente de iluminación, m_0 es la primera máscara de fase, m_1 es la llave de seguridad, L_1 y L_2 son lentes de distancia focal f , O es el objeto de entrada y E es la imagen encriptada.

Esta configuración es implementada satisfactoriamente en un sistema óptico virtual realizando el siguiente procedimiento:

1. El objeto de entrada se multiplica por un difusor de fase m_0 descrito por la Ecuación (3.44) para obtener la transmitancia compleja de entrada.
2. Se aplica la Ecuación (3.31) para propagar la transmitancia de entrada una distancia igual a la distancia focal de la lente L_1 .

3. El frente de onda resultante del ítem (2) interacciona con una lente óptica virtual representada por la Ecuación (3.34).
4. Se realizar nuevamente el proceso del ítem (2) siendo el resultado del ítem (3) el campo de entrada.
5. El frente de onda resultante del ítem (4) es multiplicado por la llave de seguridad m_1 descrita por la Ecuación (3.44). Esta vez se emplea otra función aleatoria de fase $\varphi(x, y)$ para generar la llave de seguridad.
6. Se aplican nuevamente los procesos descritos en los ítems (2), (3) y (4) para obtener la información encriptada en el plano focal de la lente L_2 .

Para decodificar la información, se emplea la arquitectura de la Figura 3.15. Este es un sistema $4f$ compuesto de dos lentes de igual distancia focal separadas $2f$. Esta vez, en el plano de entrada se coloca el complejo conjugado de la imagen encriptada. De la misma forma que el proceso de codificación, la lente L_1 realiza una primera transformada de Fourier y el espectro resultante interactúa con la llave de seguridad m_1 que se encuentra en el plano de frecuencias. Finalmente la lente L_2 realiza una última transformada de Fourier para obtener el objeto original.

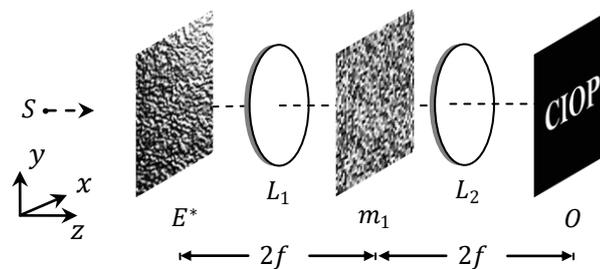


Figura 3.15: Sistema de encriptación en configuración $4f$. Etapa de desencriptación. S es la fuente de iluminación, L_1 y L_2 son lentes de distancia focal f , E^* es la fase conjugada de la imagen encriptada y O es el objeto recuperado.

De la misma forma que para la etapa de codificación, esta proceso es implementado en un SOV siguiendo el siguiente procedimiento:

1. Se realiza la conjugación de fase de la imagen encriptada para definir la transmitancia compleja de entrada.
2. Se aplica la Ecuación (3.31) para propagar la transmitancia de entrada una distancia igual a la distancia focal de la lente L_1 .

3. El frente de onda resultante del ítem (2) interacciona con una lente óptica virtual representada por la Ecuación (3.34).
4. Se realizar nuevamente el proceso del ítem (2) siendo el resultado del ítem (3) el campo de entrada.
5. El frente de onda resultante del ítem (4) es multiplicado por la llave de seguridad m_1 descrita por la Ecuación (3.44).
6. Se aplican nuevamente los procesos descritos en los ítems (2), (3) y (4) para obtener la información encriptada en el plano focal de la lente L_2 .

De esta forma concluye la implementación en SOV de la etapa de encriptación y la etapa de desencriptación de un sistema de codificación en configuración $4f$.

Evidentemente, el uso de estos elementos virtuales brinda una ventaja sustancial para estudiar sistemas ópticos complejos. Se puede experimentar una y otra vez variando los parámetros ópticos del sistema. Esto conducirá a explorar arquitecturas con grados eficientes de operatividad lo cual conlleva a un ahorro de tiempo en pruebas de ensayo y error en el laboratorio. Por otro lado, la comprensión acabada del comportamiento del sistema analógico permitirá conocer sus virtudes y alcances, dando pie para explorar nuevas arquitecturas ópticas. En el caso particular de las técnicas de encriptación óptica, el uso de los sistemas ópticos virtuales será determinante para encontrar una configuración que aventaje a las técnicas convencionales de codificación. De este modo, esta herramienta será fundamental para optimizar los procesos concernientes a la codificación y decodificación de datos en un canal clásico de información.

3.6 Bibliografía

- [3.1] R. C. Bu, Simulación, un enfoque practico. Editorial LIMUSA S.A. (2003). pp. 11-18.
- [3.2] P. Fritzson, Introducción al modelado y simulación de sistemas técnicos y físicos. Wiley-IEEE Press. (2003). pp. 15-26.
- [3.3] J. Banks, J. Carson, B. Nelson, D. Nicol, Discrete-event system simulation. Prentice Hall. (2004). pp. 3-20.

- [3.4] G. S. Landsberg, *Óptica* tomo I. Editorial MIR Moscú. (1983). pp. 156-181.
- [3.5] J. W. Goodman, *Introduction to Fourier Optics*. McGraw-Hill, 2nd ed. (1996). pp. 32-61.
- [3.6] J. Cowley, *Diffraction physics*. 3rd. rev. ed. North-Holland Personal Library. (1995). pp. 5-14.
- [3.7] J. W. Goodman, *Introduction to Fourier Optics*. McGraw-Hill, 2nd ed. (1996). p. 46.
- [3.8] M. Born, E. Wolf, *Principles of optics: electromagnetic theory of propagation, interference and diffraction of light*. Cambridge: Cambridge University Press, (1999). p. 413.
- [3.9] E. Hecht, *Optics*, Addison Wesley (2003). p. 104.
- [3.10] J. W. Goodman, *Introduction to Fourier Optics*. McGraw-Hill, 2nd ed. (1996). p. 55.
- [3.11] O. Ersoy, *Diffraction, Fourier Optics and Imaging*. Wiley-Interscience, A. John Wiley & Sons, INC., Publications. New Jersey (2007). p. 44.
- [3.12] P. Pellat-Finet, *Lecciones de óptica de Fourier*. Universidad Industrial de Santander (2004). p. 13.
- [3.13] J. W. Goodman, *Introduction to Fourier Optics*. McGraw-Hill, 2nd ed. (1996). pp. 63-75.
- [3.14] O. Ersoy, *Diffraction, Fourier Optics and Imaging*. Wiley-Interscience, A. John Wiley & Sons, INC., Publications. New Jersey (2007). p. 63.
- [3.15] P. Pellat-Finet, *Lecciones de óptica de Fourier*. Universidad Industrial de Santander (2004). p. 28.
- [3.16] J. W. Goodman, *Introduction to Fourier Optics*. McGraw-Hill, 2nd ed. (1996). p. 69.

- [3.17] W. H. Southwell, "Validity of the Fresnel approximation in the near field," *J. Opt. Soc. Am.* 71, 7-14 (1981).
- [3.18] A. M. Steane, H. N. Rutt, "Diffraction calculations in the near field and the validity of the Fresnel approximation," *J. Opt. Soc. Am. A* 6, 1809-1814 (1989).
- [3.19] S. Mezouari, A. R. Harvey, "Validity of Fresnel and Fraunhofer approximations in scalar diffraction," *J. Opt. A: Pure Appl. Opt.* 5 S86 (2003).
- [3.20] O. Ersoy, *Diffraction, Fourier Optics and Imaging*. Wiley-Interscience, A. John Wiley & Sons, INC., Publications. New Jersey (2007). p.47.
- [3.21] J. W. Cooley, J. W. Tukey, "An algorithm for the machine calculation of complex Fourier series", *Math. Computat.*, 19, 197-301, (1965).
- [3.22] E. Chu, A. George, *Inside the FFT Black Box: Serial and Parallel Fast Fourier Transform Algorithms*. CRC Press LLC, (2000).
- [3.23] G. Blanchet, M. Charbit, *Digital signal and image processing using MATLAB*. Wiley-ISTE (2006).
- [3.24] O. Ersoy, *Diffraction, Fourier Optics and Imaging*. Wiley-Interscience, A. John Wiley & Sons, INC., Publications. New Jersey (2007). p. 72.
- [3.25] J. W. Goodman, *Introduction to Fourier Optics*. McGraw-Hill, 2nd ed. (1996). p. 103.
- [3.26] O. Ersoy, *Diffraction, Fourier Optics and Imaging*. Wiley-Interscience, A. John Wiley & Sons, INC., Publications. New Jersey (2007). p. 134.
- [3.27] A. Maréchal, *Imagerie géométrique, aberrations*, Masson Paris (1967).
- [3.28] James E. Gentle *Random Number Generation and Monte Carlo Methods* Springer Verlag, (1998). p. 5.
- [3.29] R. C. Bu, *Simulación, un enfoque práctico*. LIMUSA Noriega, (2002). p.19.

- [3.30] J. W. Goodman, Introduction to Fourier Optics. McGraw-Hill, 2nd ed. (1996). p. 77.
- [3.31] J. W. Goodman, Introduction to Fourier Optics. McGraw-Hill, 2nd ed. (1996). pp. 101-114.
- [3.32] J. W. Goodman, Introduction to Fourier Optics. McGraw-Hill, 2nd ed. (1996). p. 81.
- [3.33] J. C. Dainty, Laser *speckle* and related phenomena. Springer-Verlag Berlin Heidelberg New York (1975). p. 1.
- [3.34] G. S. Landsberg, Óptica, Mir, Moscú (1983) Tomo1, p. 112.
- [3.35] J. W. Goodman, “Statistical properties of laser *speckle* patterns” p. 35-42 en J. C. Dainty, Laser *speckle* and related phenomena. Springer-Verlag Berlin Heidelberg New York (1975).
- [3.36] H. Rabal, R. Braga Jr., Dynamic laser *speckle* and applications. CRC Press (2009).
- [3.37] M. Françon, “Information processing using *speckle* patterns”. pp. 171-201, en .C. Dainty. Laser *speckle* and related phenomena. Springer-Verlag Berlin Heidelberg New York (1975).
- [3.38] L. Angel, “Estudio de distribuciones de *speckles* modulados y aplicaciones”, Tesis Doctoral, Universidad Nacional de La Plata, Facultad de Ciencias Exactas, Departamento de Física. Marzo de 2000. pp. 41-78.
- [3.39] E. Mosso, M. Tebaldi, A. Lencina, N. Bolognini, “Cluster *speckle* structures through multiple apertures forming a closed curve,” Optics Communications, Volume 283, Issue 7, 1 April (2010), 1285-1290.
- [3.40] J. P. Staforelli, J. M. Brito, E. Vera, P. Solano, A. Lencina, “A clustered *speckle* approach to optical trapping,” Optics Communications, Volume 283, Issue 23, 1 December (2010), 4722-4726.

Capítulo 4

Multiplexado de información encriptada en medios de registro planos

4.1 Introducción

En el Capítulo 3 se presentó el concepto de sistemas ópticos virtuales. En el marco de la validación de modelos se implementaron eficientemente arquitecturas ópticas de experiencias conocidas. Se comprobó que el modelado de arquitecturas ópticas en SOV es una herramienta valiosa para estudiar sistemas ópticos de diferente complejidad. En este sentido, las arquitecturas de encriptación presentadas en el Capítulo 2 pueden ser implementadas usando los elementos virtuales desarrollados. Particularmente se implementó en un SOV la arquitectura de codificación de doble máscara de fase en configuración $4f$.

La eficiencia y robustez del sistema $4f$ han sido ampliamente estudiadas [4.1]-[4.8]. Sin embargo, se ha encontrado que bajo ciertas condiciones presenta debilidades ante diversos tipos de ataques que tienen como fundamentos el criptoanálisis [4.9]. Una de estas intrusiones consiste en tener acceso al sistema de codificación manipulándolo para descifrar la llave de encriptación. El intruso aplica una señal delta de Dirac en la entrada del sistema y el resultado en el plano de Fourier es el espectro de la función delta multiplicado por la llave de encriptación. Tras una nueva transformada de Fourier, en el plano de salida se obtiene el espectro de la llave de codificación. De esta manera, se compromete la seguridad del sistema por medio de una transformada inversa de Fourier.

Un proceso iterativo es usado para reconstruir la llave de seguridad y poder decodificar otra información resguardada con la misma llave y el mismo sistema de encriptación. En otros ataques la intrusión se realiza empleando un conjunto de imágenes especialmente cifradas con el sistema de encriptación. Con estas imágenes es posible obtener las máscaras aleatorias empleadas en el plano de entrada y en el plano de Fourier del sistema *4f*.

En general, los diferentes tipos de ataques a este sistema se centran en obtener la llave de seguridad ubicada en el plano de Fourier. Comúnmente se asume un conocimiento a priori de la arquitectura de codificación. Algunos de estos procedimientos son efectivos y otros son poco prácticos en su implementación ya que el número de pruebas de ensayo y error aumenta a medida que la llave de seguridad está compuesta de un número mayor de elementos dispersores. Es decir, estos ataques evidencian debilidades únicamente cuando el sistema de encriptación es muy simple, por ejemplo, cuando se emplea una única llave de seguridad para codificar diferente información.

Consecuentemente, una manera de reforzar la seguridad del sistema es usar llaves de encriptación de gran tamaño que tengan un número grande de elementos dispersores y emplear una única llave para cada información que se va a encriptar. Otra forma de aumentar la seguridad es realizar variantes sobre la arquitectura óptica de encriptación. De esta manera se definen nuevas funciones para las llaves de codificación. Por ejemplo, se pueden generar llaves de seguridad relacionadas con parámetros del sistema, como longitud de onda, polarización, distancias de propagación en el domino de Fresnel o en planos fraccionales de Fourier, etc.

Otro modo de reforzar la seguridad de los sistemas de encriptación es emplear el concepto de multiplexado de información codificada. Por medio de esta técnica se pierde la relación biunívoca entre la imagen y su versión encriptada haciendo ineficientes los ataques del criptoanálisis. El multiplexado de información codificada presenta gran relevancia al aumentar la cantidad de datos transmitidos de manera segura, genera diferentes canales de información y múltiples niveles de acceso para procesos multiusuarios. El multiplexado de información es una técnica que se maneja ampliamente

en el área de procesamiento de señales, en comunicaciones ópticas y que ha sido adoptada en las técnicas ópticas de seguridad.

Es de mencionar que el registro múltiple de hologramas en medios de volumen ha sido ampliamente estudiado evaluando eficiencias de difracción y selectividad angular [4,10]-[4.12]. En estos análisis, se destacan las ventajas que tiene un medio de registro en volumen como los cristales fotorrefractivos. Por ejemplo, estos materiales presentan un buen comportamiento en la reconstrucción de hologramas a partir de un multiplexado realizado con diferentes longitudes de onda [4.13]. También permiten que los mínimos cambios en el ángulo del haz de registro/lectura, guarden/reconstruyan eficientemente diferentes hologramas [4.14]. Aprovechando esta característica de selectividad angular, se han presentado montajes experimentales que permiten multiplexar información codificada en estos medios de volumen [4.15], [4.16].

Sin embargo, existen escasas referencias donde se aborda la problemática referente al multiplexado de información codificada en medios de registro planos (cámara CCD), específicamente, en el sistema de codificación de doble máscara de fase en configuración $4f$. De hecho, no existe referencia alguna de una técnica que permita suplir dichas deficiencias.

Se puede considerar que uno de los dispositivos opto-electrónicos que permite realizar la interfaz con el área digital es la cámara CCD. Este dispositivo digitaliza la información procesada analógicamente por medios ópticos para que los datos sean procesados y transmitidos en formato digital. Particularmente, uno de estos procesos es el multiplexado de información encriptada. Consecuentemente, es importante realizar un estudio de sus bondades y problemáticas ya que influyen directamente en las etapas involucradas en un canal de información clásico o una red de comunicación convencional.

Estos últimos están compuestos básicamente por un emisor, un receptor y un canal de transmisión. Si en la etapa del emisor se aplica un proceso de encriptación óptica, la información encriptada debe ser digitalizada y enviada por un canal de transmisión como cualquier archivo común. La información que recibe el receptor está codificada y necesita de un proceso de recuperación o etapa de decodificación. Lo más habitual es que los datos

enviados sean desplegados en una computadora en forma de un archivo multimedia, texto, imagen, sonido o video, por lo tanto, es justificable que la etapa de reconstrucción sea un proceso digital usando sistemas ópticos virtuales o tecnologías basadas en software/hardware. En este sentido, es importante tener un estudio acabado del comportamiento del multiplexado de información codificada en medios de registro planos. Este interviene en la protección que realiza el emisor, influye en el proceso de transmisión de datos y finalmente se ve reflejado en la eficiencia al recuperar la información, proceso realizado por el receptor.

En este capítulo se desarrollan algunos aspectos de la técnica de multiplexado de información encriptada. La visión de abordar esta técnica radica en la potencial optimización de un canal de información clásico, esto se refiere a los procesos de transmisión y recepción de datos encriptados. Inicialmente, se presenta un estudio de la técnica de multiplexado de imágenes codificadas en un sistema de encriptación en configuración *4f*. Cada imagen encriptada es registrada en un medio de registro plano, particularmente se hará énfasis en los inconvenientes que presenta esta técnica al usar medios que no son de volumen. Por otro lado, es conocido que multiplexar señales en electrónica (transmitir más de un mensaje al mismo tiempo en un canal digital) y el almacenamiento por multiplexado en óptica (guardar más de una imagen en un mismo medio de registro), requieren que las señales o imágenes puedan ser moduladas apropiadamente [4.17]. En este sentido, al final de este capítulo se introduce la técnica de modulación theta como estrategia para modular las señales ópticas codificadas.

De esta forma, el presente capítulo se divide en seis secciones. En la Sección 4.2 se introducen los conceptos básicos, ventajas y deficiencias del multiplexado de imágenes encriptadas en el sistema de codificación *4f*. En la Sección 4.3 se estudian los dos tipos de solapamiento de información que se pueden encontrar en la etapa de desencriptación a partir de un multiplexado lineal. En la Sección 4.4 se realiza un estudio del deterioro de la información recuperada a partir del multiplexado lineal. Finalmente, en la Sección 4.5 se introduce la técnica de modulación theta que se usa como estrategia de modulación de información codificada. El introducir esta técnica permitirá suplir las deficiencias expuestas en las primeras secciones de este capítulo.

4.2 Multiplexado de información

Desde que las técnicas ópticas aparecieron como herramientas prácticas para guardar de manera segura información se han realizado importantes avances en la optimización de diferentes diseños y arquitecturas que brindan la posibilidad de manejar grandes volúmenes de datos.

Una aplicación importante en el área de la encriptación óptica es la técnica de multiplexado. Esta técnica tiene como principio básico el almacenamiento múltiple de información encriptada en un único medio de registro. La técnica de multiplexado proporciona la opción de guardar y transmitir múltiple información a diferentes usuarios y la posibilidad de manejar niveles de acceso. Al mismo tiempo, incrementa el grado de seguridad de los sistemas convencionales de encriptación ya que se verifica que esta técnica mejora la robustez y vuelve inmune a los sistemas convencionales ante ataques de texto cifrado y de texto plano [4.9].

La gran diversificación de los esquemas experimentales tiene su origen en que los sistemas ópticos de codificación son sensibles al cambio de parámetros ópticos, como la polarización, la longitud de onda, el posicionamiento de la llave de seguridad, etc., permitiendo implementar diferentes estrategias de multiplexado. Entre las contribuciones que emplean esta técnica, se encuentran: multiplexado usando la longitud de onda [4.18], multiplexado por traslaciones de la llave de seguridad [4.19], multiplexado modificando el estado de polarización de la luz [4.20], multiplexado usando múltiples aperturas que cambian entre exposición [4.21].

A continuación se restringe la aplicación de la técnica de multiplexado de información encriptada a un sistema óptico de codificación en configuración $4f$.

4.2.1 Multiplexado de imágenes encriptadas en un sistema $4f$

El sistema de encriptación en configuración $4f$ es implementado en un SOV según los lineamientos de la Sección 3.5. De forma general, el multiplexado $M(x_0, y_0)$ de dos o

más datos encriptados en un sistema óptico de encriptación puede ser representado de la forma:

$$M(x_0, y_0) = \sum_{m=1}^N E_m(x_0, y_0) \quad (4.1)$$

donde N es el número total de imágenes encriptadas $E_m(x_0, y_0)$. En particular, el multiplexado de información de imágenes encriptadas en una arquitectura $4f$ se realiza sumando las imágenes codificadas obtenidas en el sistema descrito en la Sección 2.2.

Haciendo referencia al esquema de la Figura 4.1, inicialmente en el plano de entrada de un procesador $4f$ es ubicado un objeto $O_1(x, y)$ multiplicado por una primera máscara de fase $e^{i\varphi_0(x, y)}$. La primera lente de distancia focal f produce la transformada de Fourier de la transmitancia del plano de entrada que posteriormente es multiplicada por la llave de encriptación $e^{i\varphi_1(u, v)}$. La segunda lente de distancia focal f concluye el proceso de encriptación realizando una última transformada de Fourier obteniéndose así en el plano de salida el primer objeto codificado. Realizando este proceso para m objetos de entrada, se obtienen m objetos encriptados.

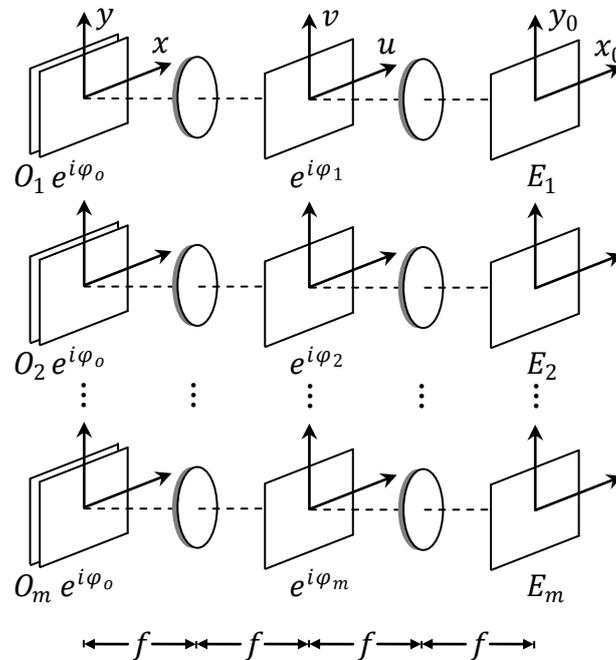


Figura 4.1: Encriptación de m objetos usando el sistema de doble máscara de fase en configuración $4f$. El sistema consiste de dos lentes de distancia focal f , O_m representa el objeto a encriptar, $e^{i\varphi_0}$ es la primera máscara de fase, $e^{i\varphi_m}$ es la llave de seguridad con la cual se codifica O_m y E_m es el objeto encriptado.

Se debe notar que cada objeto de entrada es multiplicado por una primera máscara de fase $e^{i\varphi_o(x,y)}$ que es idéntica en todos los casos, a diferencia de la segunda máscara de fase $e^{i\varphi_m(u,v)}$ que es diferente para codificar cada objeto.

Matemáticamente, para un sistema convencional de encriptación en arquitectura $4f$ la amplitud compleja de cada imagen encriptada $E_m(x_0, y_0)$ puede ser escrita como:

$$E_m(x_0, y_0) = \mathcal{F}\{\mathcal{F}[O_m(x, y)e^{i\varphi_o(x,y)}]e^{i\varphi_m(u,v)}\} \quad (4.2)$$

donde $O_m(x, y)$ es la imagen de entrada, $e^{i\varphi_o(x,y)}$ es la primera máscara de fase, $e^{i\varphi_m(u,v)}$ es la segunda máscara de fase o la llave de codificación, y \mathcal{F} representa la transformada de Fourier.

El multiplexado de información encriptada se obtiene realizando la suma de cada una de las imágenes encriptadas de la Ecuación (4.2). De esta manera, el multiplexado en un sistema convencional $4f$ puede ser escrito como:

$$M_{4f}(x_0, y_0) = \sum_{m=1}^N \mathcal{F}\{\mathcal{F}[O_m(x, y)e^{i\varphi_o(x,y)}]e^{i\varphi_m(u,v)}\} \quad (4.3)$$

De la misma forma, si se quisiera extender esta técnica a otra arquitectura de encriptación, por ejemplo, para el sistema de encriptación de doble máscara de fase en configuración JTC , el término $E_m(x_0, y_0)$ de la Ecuación (4.1) debe ser escrito como:

$$E_m(x_0, y_0) = \mathcal{F}[T_m(x, y)]\{\mathcal{F}[T_m(x, y)]\}^* = JPS_m(x_0, y_0) \quad (4.4)$$

donde $JPS_m(x_0, y_0)$ es el espectro conjunto de potencia definido en la Sección 2.4.1, $T_m(x, y)$ es el plano de entrada dado por la Ecuación (2.9) y el signo $*$ representa la operación de conjugación de fase. De esta manera, el multiplexado en un sistema de codificación en configuración JTC puede ser expresado como:

$$M_{JTC}(x_0, y_0) = \sum_{m=1}^N JPS_m(x_0, y_0) \quad (4.5)$$

Por lo tanto, la técnica de multiplexado es aplicable de forma general a cualquier sistema de encriptación óptica. En cada caso, la imagen encriptada estará definida según la arquitectura específica de codificación.

Haciendo énfasis en el sistema de encriptación de doble máscara de fase en configuración $4f$, a partir del multiplexado $M_{4f}(x_0, y_0)$ dado por la Ecuación (4.3), se puede recuperar correctamente cualquier información multiplexada empleando la llave de encriptación adecuada.

El proceso de recuperación en esta arquitectura está esquematizado en la Figura 4.2. Para recuperar el objeto k a partir de un multiplexado, inicialmente en la entrada de un procesador $4f$ se ubica el complejo conjugado de la cantidad $M_{4f}(x, y)$. Una primera lente realiza la transformada de Fourier de la entrada y el espectro resultante es multiplicado por la llave de codificación $e^{i\varphi_k(u,v)}$. Finalmente, una segunda lente realiza una nueva transformada de Fourier para obtener el objeto desencriptado.

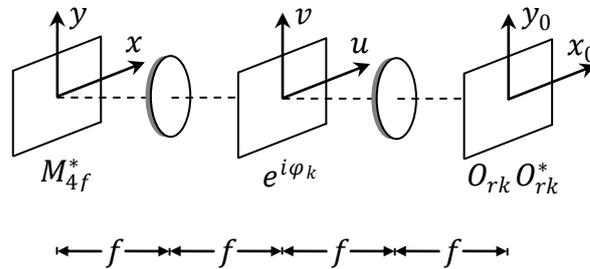


Figura 4.2: Etapa de desencriptación del objeto k a partir de un multiplexado de imágenes encriptadas con el sistema de doble máscara de fase en configuración $4f$.

La amplitud compleja del objeto k recuperado puede ser escrita como:

$$O_{rk}(x_0, y_0) = \mathcal{F}\{\mathcal{F}[M_{4f}^*(x, y)]e^{i\varphi_k(u,v)}\} \quad (4.6)$$

Remplazando el multiplexado de la Ecuación (4.3), después de un cambio de coordenadas y realizando las transformadas de Fourier, se tiene:

$$O_{rk}(x_0, y_0) = O_k^*(x, y)e^{-i\varphi_o(x,y)} + \left\{ \sum_{\substack{m=1 \\ m \neq k}}^N [O_m(x, y)e^{i\varphi_o(x,y)}]^* \otimes \mathcal{F}[e^{-i\varphi_{mk}(u,v)}] \right\} \quad (4.7)$$

donde $e^{-i\varphi_{mk}(u,v)} = e^{-i[\varphi_m(u,v) - \varphi_k(u,v)]}$. Ya que es un sistema sin magnificación, las coordenadas del objeto recuperado (x_0, y_0) y las coordenadas del objeto de entrada (x, y) son las mismas.

Se puede observar que la amplitud compleja del objeto recuperado $O_{r_k}(x_0, y_0)$ tiene información del objeto descrito correctamente $O_k^*(x, y)$ más un término adicional de superposición de imágenes representado por la sumatoria en la Ecuación (4.7). Este término produce superposición de información y es uno de los principales impedimentos para multiplexar grandes volúmenes de imágenes codificadas.

Particularmente, se pueden presentar dos casos de solapamiento de información. 1) la superposición de la información de interés con información correctamente descrita. 2) la superposición de información de interés con información incorrectamente descrita.

En la siguiente sección se presenta un análisis de cada uno de estos dos casos en términos de la energía total de los objetos encriptados. La importancia de este enfoque radica en que el contenido energético de cada información procesada influye directamente en la cantidad de ruido de una imagen recuperada. Esto implica que el aplicar la técnica convencional de multiplexado se imponen condiciones y restricciones sobre la información que se quiere transmitir. Evidentemente este hecho es un problema que se debe considerar ya que las características de la información transmitida no deberían ser un elemento de exclusión para aplicar una técnica de seguridad. En los capítulos siguientes se presenta una solución para evitar este fenómeno.

4.3 Solapamiento de información recuperada

La mayoría de los sistemas ópticos de encriptación que son variantes de la configuración 4f basan su efectividad principalmente en el uso de dos máscaras de fase aleatorias. Teniendo en cuenta que el elemento más importante de esta configuración de codificación es la llave de encriptación, se analiza la aplicación de la técnica de multiplexado para dos casos particulares. 1) la llave de seguridad $e^{i\varphi_m(u,v)}$ es la misma para encriptar cada objeto de entrada, esto implica la existencia de superposición de imágenes descifradas

correctamente. 2) la llave de seguridad $e^{i\varphi_m(u,v)}$ es diferente para encriptar cada objeto de entrada, esto implica la existencia de superposición de imágenes descriptadas incorrectamente.

4.3.1 Solapamiento de información recuperada correctamente

Si en el proceso de encriptación se emplea una única llave de seguridad, es decir $e^{i\varphi_m(u,v)} = e^{i\varphi_1(u,v)}$, el multiplexado en un sistema convencional $4f$ puede ser expresado como:

$$M_{4f}(x_0, y_0) = \sum_{m=1}^N \mathcal{F}\{\mathcal{F}[O_m(x, y)e^{i\varphi_o(x,y)}]e^{i\varphi_1(u,v)}\} \quad (4.8)$$

donde $O_m(x, y)$ es la imagen de entrada, $e^{i\varphi_o(x,y)}$ es la primera máscara de fase y $e^{i\varphi_1(u,v)}$ es la llave de seguridad del sistema de encriptación $4f$. Nótese que cada imagen encriptada ha sido codificada con la máscara de fase $e^{i\varphi_1(u,v)}$.

Haciendo referencia a la Figura 4.2 para el proceso de decodificación, en el plano de entrada del sistema $4f$ se ubica la fase conjugada del multiplexado dado por la Ecuación (4.8). De esta forma, la amplitud compleja del objeto recuperado $O_{r_m}(x_0, y_0)$ puede ser escrita como:

$$O_{r_m}(x_0, y_0) = \mathcal{F}\{\mathcal{F}[M_{4f}^*(x, y)]e^{i\varphi_1(u,v)}\} \quad (4.9)$$

Sustituyendo la Ecuación (4.8) y realizando las transformadas de Fourier en la Ecuación (4.9) se tiene:

$$O_{r_m}(x_0, y_0) = \mathcal{F}\left\{\sum_{m=1}^N \left\{\mathcal{F}[O_m(x, y)e^{i\varphi_o(x,y)}]\right\}^* e^{-i\varphi_1(u,v)} e^{i\varphi_1(u,v)}\right\} \quad (4.10)$$

$$O_{r_m}(x_0, y_0) = \sum_{m=1}^N [O_m(x, y)e^{i\varphi_o(x,y)}]^*$$

Desarrollando la sumatoria, el campo complejo puede ser escrito como:

$$O_{r_m}(x_0, y_0) = O_1^*(x, y)e^{-i\varphi_o(x, y)} + \dots + O_m^*(x, y)e^{-i\varphi_o(x, y)} + \dots + O_N^*(x, y)e^{-i\varphi_o(x, y)} \quad (4.11)$$

La Ecuación (4.11) tiene la contribución de todas las amplitudes complejas de los objetos $O_k^*(x, y)$, con $k = 1, 2, \dots, N$, multiplicadas por un factor de fase $e^{-i\varphi_o(x, y)}$. De esta manera, la intensidad del objeto recuperado, $O_{r_m}(x_0, y_0)O_{r_m}^*(x_0, y_0)$ puede ser escrita como:

$$O_{r_m}(x_0, y_0)O_{r_m}^*(x_0, y_0) = \sum_{j=1}^N O_j(x, y)O_j^*(x, y) + 2Re \left[\sum_{k=1}^{N-1} \sum_{l=k+1}^N O_k(x, y)O_l^*(x, y) \right] \quad (4.12)$$

donde N es el número de imágenes encriptadas multiplexadas.

En el lado derecho de la igualdad en la Ecuación (4.12) se puede identificar la contribución de dos términos. El primer término representado por la primera sumatoria tiene todos los valores positivos y es la contribución de las intensidades de los objetos correctamente recuperados. El segundo término es la parte real de los productos cruzados de los términos $O_k O_l^*$. Se puede comprobar que la sumatoria sobre estos últimos siempre va a ser menor que la suma sobre los términos $O_j O_j^*$, resultando valores positivos ya que son valores de intensidad. A continuación se describe un ejemplo para este primer caso.

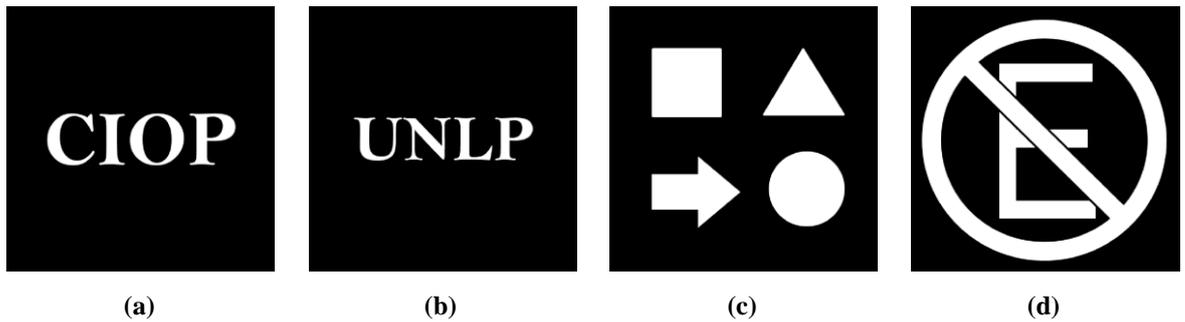


Figura 4.3: Imágenes binarias a encriptar en un sistema de codificación $4f$.

Usando un SOV de encriptación $4f$, cada una de las imágenes de la Figura 4.3 es codificada con la misma llave de seguridad $e^{i\varphi_1(u, v)}$, se asume que el registro se realiza en un medio plano (CCD) y que el multiplexado se hace digitalmente. La expresión para el multiplexado está dada por la Ecuación (4.8) con $N = 4$. Al recuperar la información a

partir de este multiplexado y al usar la única llave de encriptación, la información decodificada estará dada por la Ecuación (4.12).

Si esta experiencia se implementa experimentalmente, el registro de cada imagen codificada debería hacerse aplicando la técnica de holografía digital (ver Apéndice A). Ya que se está trabajando con sistemas ópticos virtuales, se asume el caso ideal donde se registra el campo complejo en la salida del sistema $4f$ para luego realizar el multiplexado computacionalmente. En sistemas ópticos virtuales la imagen obtenida de la etapa de encriptación tiene amplitud y fase directamente, por lo tanto, se asume una recuperación ideal del campo complejo de la imagen encriptada a partir de un registro holográfico.

En la Figura 4.4 se muestran los dos términos de la Ecuación (4.12) y la imagen recuperada a partir del multiplexado usando la única llave de seguridad $e^{i\varphi_1(u,v)}$.

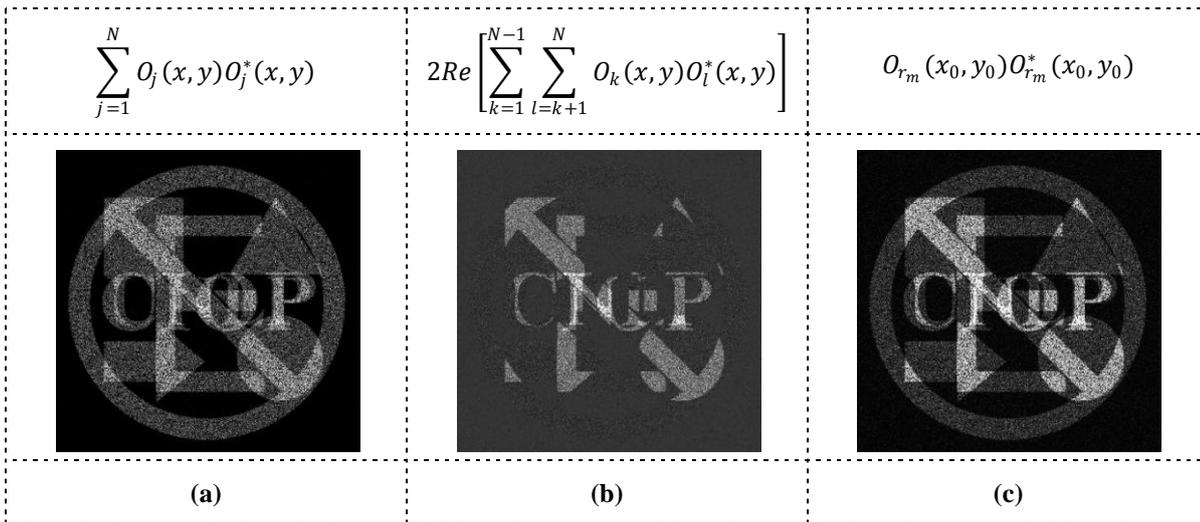


Figura 4.4: Solapamiento de información recuperada a partir de un multiplexado de cuatro imágenes encriptadas usando una única llave de seguridad. Las imágenes (a) y (b) son los términos del lado derecho de la igualdad de la Ecuación (4.12) y (c) es la imagen recuperada con solapamiento de información.

Se puede observar en la Figura 4.4 (c), como la adición del segundo término en la Ecuación (4.12) realza ciertos sectores en la imagen recuperada. La imagen desencriptada a partir de un multiplexado usando una única llave de seguridad, no sólo está compuesta por la contribución de las imágenes correctamente decodificadas, Figura 4.4 (a), sino que existe el término adicional mostrado en la Figura 4.4 (b).

El solapamiento de información correctamente decodificada a partir de un multiplexado de imágenes encriptadas y registradas en un medio de registro plano es un problema que impide que se manejen grandes volúmenes de información sin que exista deterioro en la información recuperada. Nótese que esta forma convencional de realizar el multiplexado no permite usar una única llave de seguridad para decodificar múltiples objetos. El solapamiento de información es evidente produciendo un deterioro indeseado en cualquier imagen de interés.

De la Ecuación (4.10) se puede observar que la compensación de fases es realizada correctamente por la llave única de seguridad. Sin embargo, toda la información decodificada se encuentra superpuesta en un mismo plano. La idea más directa para solucionar este inconveniente es usar diferentes llaves de seguridad para codificar cada imagen. Esto conduce al segundo caso de solapamiento de información que se presenta en la siguiente sección.

4.3.2 Solapamiento de información recuperada incorrectamente

Si en el proceso de encriptación en un sistema $4f$ se emplea una llave de seguridad diferente, $e^{i\varphi_m(u,v)}$, para codificar cada objeto $O_m(x,y)$, siendo $m = 1, 2, \dots, N$, la imagen recuperada con una de las llaves de seguridad a partir de un multiplexado estará degradada en calidad. Esto es debido a la superposición de información en forma de ruido presente en la etapa de recuperación. Para este caso, el multiplexado de información encriptada puede ser expresado como:

$$M_{4f}(x_0, y_0) = \sum_{m=1}^N \mathcal{F}\{\mathcal{F}[O_m(x, y)e^{i\varphi_o(x,y)}]e^{i\varphi_m(u,v)}\} \quad (4.13)$$

donde $e^{i\varphi_o(x,y)}$ es la primera máscara de fase y $e^{i\varphi_m(u,v)}$ es la llave de seguridad con la cual se codifica el objeto $O_m(x, y)$. Nótese que la variable m varía en el objeto y en la llave de seguridad.

En la etapa de desencriptación, el campo complejo recuperado $O_{r_k}(x_0, y_0)$ a partir del multiplexado de la Ecuación (4.13) puede ser expresado como:

$$O_{r_k}(x_0, y_0) = \mathcal{F}\{\mathcal{F}[M_{4f}^*(x, y)]e^{i\varphi_k(u, v)}\} \quad (4.14)$$

Remplazando la Ecuación (4.13) y calculando las transformadas de Fourier en la Ecuación (4.14), se obtiene:

$$O_{r_k}(x_0, y_0) = \mathcal{F}\left\{\sum_{m=1}^N \left\{\mathcal{F}[O_m(x, y)e^{i\varphi_o(x, y)}]\right\}^* e^{-i\varphi_{mk}(u, v)}\right\} \quad (4.15)$$

donde $e^{-i\varphi_{mk}(u, v)} = e^{-i[\varphi_m(u, v) - \varphi_k(u, v)]}$.

Ahora, realizando las transformadas de Fourier y extrayendo de la sumatoria el k -ésimo término (imagen decodificada correctamente con la llave de seguridad $e^{i\varphi_k(u, v)}$) se tiene:

$$O_{r_k}(x_0, y_0) = O_k^*(x, y)e^{-i\varphi_o(x, y)} + \left\{\sum_{\substack{m=1 \\ m \neq k}}^N [O_m(x, y)e^{i\varphi_o(x, y)}]^* \otimes \mathcal{F}[e^{-i\varphi_{mk}(u, v)}]\right\} \quad (4.16)$$

La amplitud compleja recuperada $O_{r_k}(x_0, y_0)$ contiene el campo complejo del k -ésimo objeto $O_k^*(x, y)$ multiplicado por el factor de fase $e^{-i\varphi_o(x, y)}$ más el término de la sumatoria que representa objetos que aún siguen encriptados. Debido a que las máscaras de fase son estadísticamente independientes entre sí, la fase $e^{-i\varphi_{mk}(u, v)}$ en la Ecuación (4.16) hace que los objetos $O_m(x, y)$ permanezcan codificados y se adicionen al objeto recuperado como distribuciones de ruido blanco estacionario.

La intensidad $O_{r_k}(x_0, y_0)O_{r_k}^*(x_0, y_0)$ puede ser escrita como:

$$\begin{aligned} O_{r_k}(x_0, y_0)O_{r_k}^*(x_0, y_0) &= O_k^*(x, y)O_k(x, y) + O_k^*(x, y)e^{-i\varphi_o(x, y)}r_k^*(x_0, y_0) \\ &\quad + O_k(x, y)e^{i\varphi_o(x, y)}r_k(x_0, y_0) + r_k^*(x_0, y_0)r_k(x_0, y_0) \end{aligned} \quad (4.17)$$

donde

$$r_k(x_0, y_0) = \sum_{\substack{m=1 \\ m \neq k}}^N [O_m(x, y)e^{i\varphi_o(x, y)}]^* \otimes \mathcal{F}[e^{-i\varphi_{mk}(u, v)}] \quad (4.18)$$

con $e^{-i\varphi_{mk}(u, v)} = e^{-i[\varphi_m(u, v) - \varphi_k(u, v)]}$.

En la Ecuación (4.17) se pueden identificar cuatro términos. El término $O_k^*(x, y)O_k(x, y)$ es la intensidad de la k -ésima imagen recuperada, mientras que la suma del segundo y tercer término $O_k^*(x, y)e^{-i\varphi_o(x, y)}r_k^*(x_0, y_0) + O_k(x, y)e^{i\varphi_o(x, y)}r_k(x_0, y_0)$ es la contribución del producto del objeto original y el ruido r_k . Esta suma se puede simplificar a $2Re[O_k^*(x, y)e^{-i\varphi_o(x, y)}r_k^*(x_0, y_0)]$. Por último está el término de “ruido puro” que es la suma de las imágenes que han sido descryptadas incorrectamente al usar la llave $e^{i\varphi_k(u, v)}$. El ruido puro $r_k^*(x_0, y_0)r_k(x_0, y_0)$ adicionado a la k -ésima imagen recuperada de un multiplexado puede ser expresado como:

$$\begin{aligned} r_k^*(x_0, y_0)r_k(x_0, y_0) &= \sum_{\substack{m=1 \\ m \neq k}}^N \{[O_m(x_0, y_0)e^{i\varphi_o(x_0, y_0)}]^* \otimes \mathcal{F}[e^{-i\varphi_{mk}(u, v)}]\} \\ &\quad \times \sum_{\substack{m=1 \\ m \neq k}}^N \{[O_m(x_0, y_0)e^{i\varphi_o(x_0, y_0)}]^* \otimes \mathcal{F}[e^{-i\varphi_{mk}(u, v)}]\}^* \end{aligned} \quad (4.19)$$

Obsérvese que en la Ecuación (4.18), cuando se encripta una única imagen, no existen términos para $r_k(x_0, y_0)$, es decir, no existe ruido debido a un multiplexado. Empiezan a aparecer términos de ruido dados por la Ecuación (4.18) o Ecuación (4.19) cuando se multiplexan como mínimo dos imágenes. Nótese también que los términos en las sumatorias de estas ecuaciones aumentan a medida que se aumentan los objetos multiplexados, consecuentemente, al multiplexar un mayor número de objetos representará un grado mayor de ruido produciendo un deterioro en la calidad de la imagen decodificada correctamente.

Esto se puede observar nuevamente con un ejemplo en un SOV de encriptación 4f. Esta vez se han multiplexado cinco objetos con diferentes llaves de seguridad $e^{i\varphi_m(u, v)}$,

con $m = 1, 2, \dots, 5$. El objeto $O_k(x, y)$ se recupera con su llave de seguridad $e^{i\varphi_k(u, v)}$ a partir del multiplexado. El resultado es la Ecuación (4.17) evaluada para $N = 5$. En la Figura 4.5 se muestran las imágenes de los términos de la Ecuación (4.17). La intensidad del objeto recuperado $O_{r_k}(x_0, y_0)O_{r_k}^*(x_0, y_0)$ tiene la contribución de la imagen correctamente decodificada, Figura 4.5 (a), a la cual se le adiciona las otras dos imágenes, Figura 4.5 (b) y Figura 4.5 (c), que contribuyen únicamente en el deterioro de la imagen. Estos dos últimos términos adicionan ruido de fondo gobernado por la imagen de la Figura 4.5 (c) que representa el término de ruido puro o ruido de multiplexado de imágenes incorrectamente descriptadas.

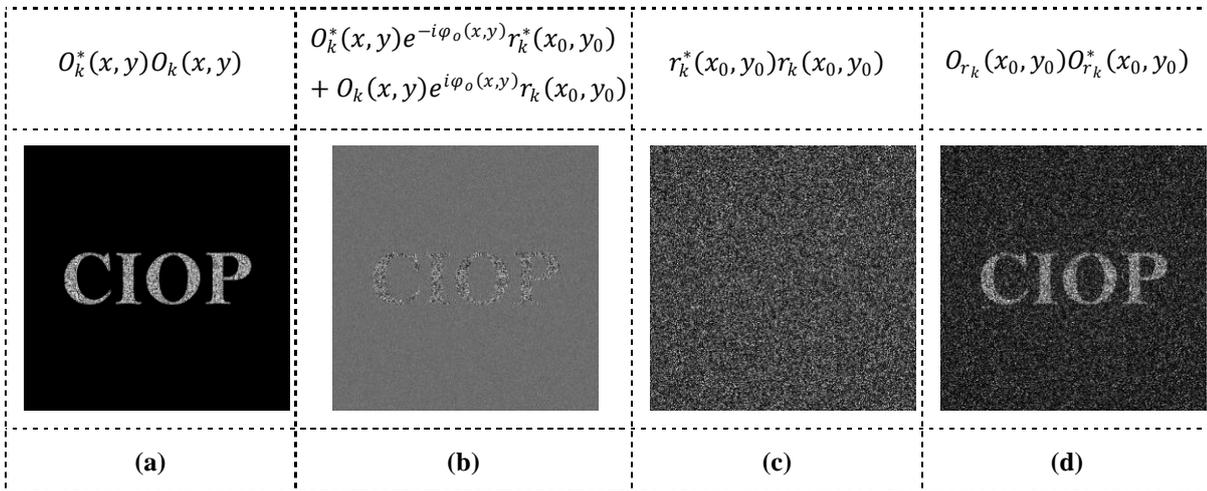


Figura 4.5: Términos que componen la imagen recuperada a partir de un multiplexado de cinco imágenes encriptadas. Las imágenes (a), (b) y (c) son los términos de la derecha de la Ecuación (4.17) y (d) es la imagen recuperada con superposición de ruido.

De estos análisis también se comprueba que el deterioro en la imagen tiene una dependencia directa con la cantidad de energía que tienen los objetos encriptados en el multiplexado. En el proceso de descriptación se tiene que el término de ruido puro $r_k^*(x_0, y_0)r_k(x_0, y_0)$ tiene valores energéticos altos o bajos que se adicionan a la imagen recuperada según la relación que exista entre la energía de la imagen original descriptada y la suma total de energías del resto de imágenes multiplexadas. Esto quiere decir que si esta última cantidad es mayor que la energía de la imagen original recuperada, el ruido de multiplexado se destacará cada vez en la etapa de decodificación. En caso contrario, la imagen recuperada no tendrá un alto grado de deterioro.

4.4 Deterioro de la información recuperada a partir de un multiplexado de imágenes encriptadas

Para corroborar las afirmaciones con que se finalizó la sección anterior, se realiza una serie de pruebas en el SOV esquematizado en la Figura 4.6. Este usa el sistema de codificación $4f$ para encriptar múltiples objetos (ver Sección 3.5), cada uno de ellos con una llave de seguridad diferente. Después de obtener todas las imágenes codificadas se aplica el proceso de multiplexado en forma digital.

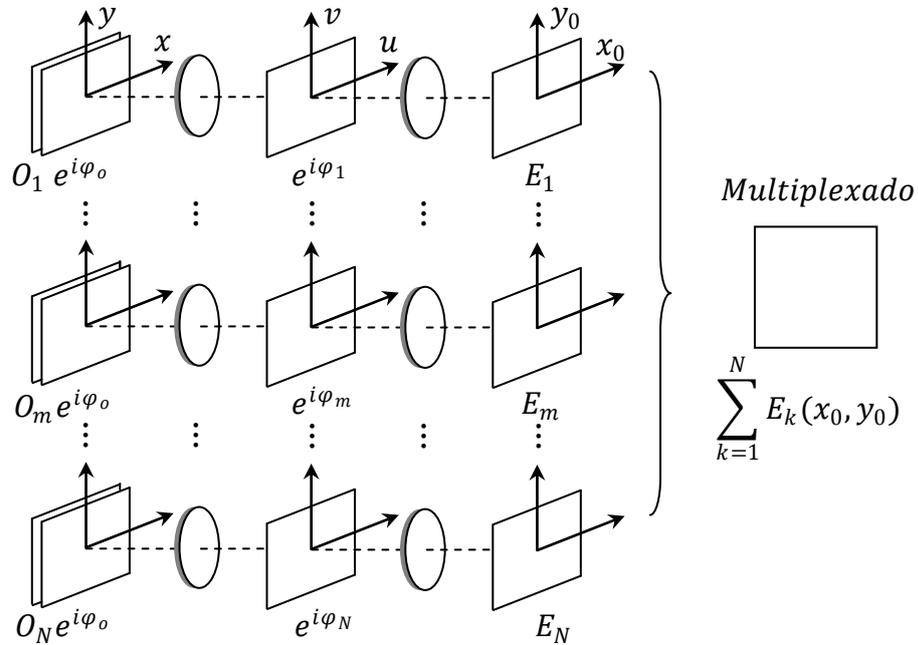


Figura 4.6: Esquema de sistema óptico virtual para multiplexar 300 objetos. El sistema consiste de dos lentes de distancia focal f , O_k representa los objetos a encriptar, donde $k = 1, 2 \dots, 300$, $e^{i\phi_o}$ es la primera máscara de fase, $e^{i\phi_k}$ es la llave de seguridad con la cual se codifica cada objeto y E_k es el objeto encriptado. Al final del proceso de encriptación se realiza el multiplexado de imágenes encriptadas.

Todos los objetos son imágenes de 256 niveles de gris, tienen tamaño 512×512 y se supone un detector de intensidad de 8 bits para tener en cuenta la saturación en el registro. El primer objeto es la palabra “CIOP” y las 299 imágenes restantes son planos constantes, es decir, todos los píxeles de la imagen tienen un único valor de niveles de gris n_g (ver Figura 4.7). La característica en común de estas 299 imágenes es que tienen la misma energía total. Para cada caso la energía de las 299 imágenes es $512 \times 512 \times n_g$.

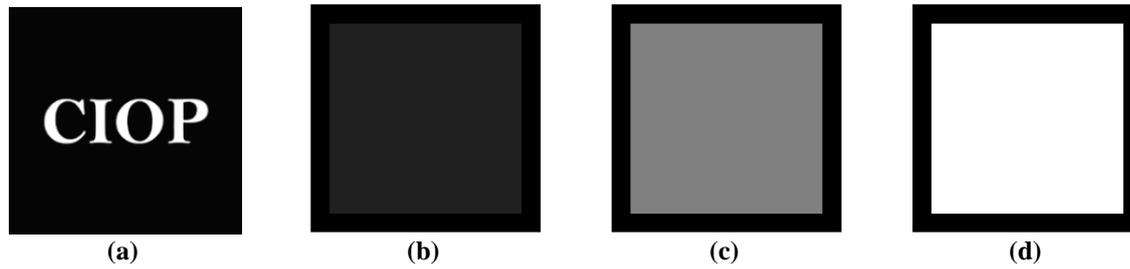


Figura 4.7: Objetos a encriptar y multiplexar. (a) Imagen de la palabra “CIOP”, (b) imagen de niveles de gris $n_g=32$, (c) imagen de nivel de gris $n_g=128$ y (d) imagen de nivel de gris de $n_g=255$.

La prueba consiste en el siguiente procedimiento. Tomando como referencia la Figura 4.6, inicialmente se realiza un multiplexado de dos imágenes encriptadas con dos llaves de seguridad diferentes. Posteriormente, se recupera con la llave de seguridad correcta la primera imagen (palabra “CIOP”) a partir de este multiplexado. Finalmente, se evalúa la semejanza de la imagen recuperada con una imagen de referencia aplicando la métrica de la raíz cuadrada del error cuadrático medio (RMSE) (ver Apéndice B). Luego se realiza el mismo procedimiento multiplexando tres imágenes encriptadas con tres llaves de seguridad diferentes y luego recuperando la primera imagen con la llave de seguridad correcta. Este procedimiento se realiza aumentando de a una imagen encriptada en el multiplexado, así, hasta multiplexar 300 objetos. Es decir, que se obtienen 299 multiplexados diferentes.

El procedimiento anterior se realiza para tres casos diferentes. 1) multiplexando la palabra “CIOP” y las imágenes de planos constantes de $n_g=32$ (Figura 4.7 (b)). 2) multiplexando la palabra “CIOP” y las imágenes de planos constantes de $n_g=128$ (Figura 4.7 (c)). 3) multiplexando la palabra “CIOP” y las imágenes de planos constantes de $n_g=255$ (Figura 4.7 (d)). En los tres casos se usa el mismo conjunto de llaves de seguridad, de esta manera se asegura un análisis del ruido en función de la energía total de las imágenes multiplexadas.

Los resultados de estos análisis son mostrados en la Figura 4.8. En las curvas de *RMSE* se puede observar la dependencia de la calidad de la imagen recuperada en términos del número de imágenes multiplexadas. Es de notar que el primer valor de las curvas es cero debido a que la imagen de referencia es la imagen recuperada de un sistema de

encriptación $4f$, es decir, se codifica y se recupera la palabra “CIOP” y se toma como imagen de referencia.

Las tres curvas tienen el mismo comportamiento y saturan a un valor diferente dependiendo directamente de la energía total de las imágenes multiplexadas la cual es determinada por el nivel de gris n_g correspondiente a cada caso. El color de cada curva de error $RMSE$, negro, azul y fucsia indican los valores de niveles de gris $n_g=255$, $n_g=128$ y $n_g=32$, respectivamente de las 299 imágenes encriptadas y multiplexadas junto a la palabra “CIOP”.

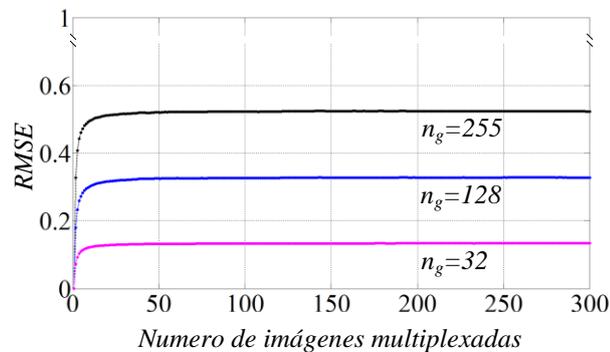


Figura 4.8: Comportamiento del $RMSE$ que muestra la dependencia con el número de imágenes encriptadas multiplexadas y la intensidad total de los objetos multiplexados, donde n_g es el número de nivel de gris del plano constante que representa cada imagen multiplexada diferente a la palabra “CIOP”.

Otra información relevante es referente a la intensidad del $RMSE$. Nótese que para un mismo número de imágenes encriptadas y multiplexadas, los valores de $RMSE$ indican un deterioro en calidad dependiente de n_g . Según las curvas, es de esperarse que al usar imágenes de mayor energía (n_g grande) se obtenga una imagen recuperada con un grado mayor de deterioro. Por el contrario, al emplear imágenes con menor energía (n_g pequeño), el ruido no sobresaldrá sobre la imagen recuperada. Por otro lado, ya que las curvas saturan a un valor constante, indica que se afecta el contraste de las imágenes recuperadas (dependiente también de la energía de entrada). El valor de saturación en las curvas $RMSE$ indica si la imagen deteriorada es de alto o bajo contraste.

Este comportamiento es verificado en la Figura 4.9. Aquí se pueden observar los resultados de las imágenes recuperadas de la palabra “CIOP” a partir de tres multiplexados. Cada uno de estos es de cinco imágenes encriptadas de tamaño 512×512 . De las cinco

imágenes encriptadas, cuatro imágenes tienen todos sus píxeles constantes. Para el primer multiplexado, cuatro imágenes son de valor $n_g=32$. Para el segundo multiplexado, cuatro imágenes son de valor $n_g=128$ y para el tercer multiplexado, cuatro imágenes son de valor $n_g=255$. La imagen de la Figura 4.9 (a) es recuperada del primer multiplexado (imágenes $n_g=32$). La imagen de la Figura 4.9 (b) es recuperada del segundo multiplexado (imágenes $n_g=128$). La imagen de la Figura 4.9 (c) es la imagen recuperada del tercer multiplexado (imágenes $n_g=256$).

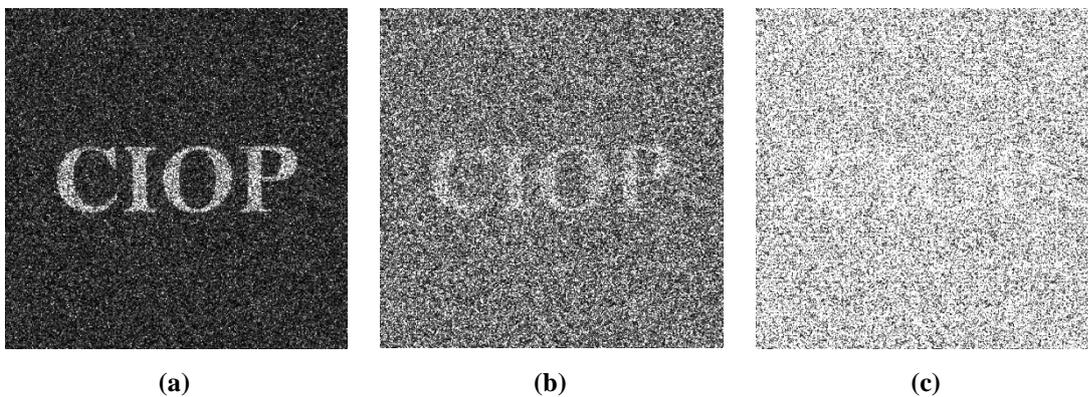


Figura 4.9: Imágenes descriptadas de un multiplexado de cinco imágenes las cuales cuatro tienen todos sus píxeles constantes de valor **a)** $n_g=32$, **b)** $n_g=128$ y **c)** $n_g=255$.

Se puede observar que el ruido en la Figura 4.9 (a) presenta menor contraste y un grado menor de deterioro en su calidad en comparación a la Figura 4.9 (b) y la Figura 4.9 (c). La saturación en estas imágenes se debe entender como que cada punto blanco brillante ha llegado a un valor máximo de 255. Debido a que la recuperación se realiza digitalmente, las imágenes recuperadas pueden ser sometidas a un proceso de recuperación donde no se incluya la saturación, de esta forma resultará la imagen con ruido *speckle* superpuesto. También se debe aclarar que estos resultados han tenido en cuenta un proceso de discretización y cuantización a 8 bits en el registro de la CCD. Esto quiere decir que la amplitud compleja de cada imagen encriptada tiene únicamente 256 valores discretos.

Al retomar el ejemplo, se observa que a medida que se aumentan las intensidades de las imágenes de entrada, las imágenes recuperadas presentan un ruido más denso en el proceso de descriptación. Este es uno de los motivos por el cual al multiplexar imágenes en niveles de gris de altos contenidos frecuenciales (las cuales suman generalmente una

contribución energética grande) produce mayor pérdida en la calidad de la imagen recuperada en comparación a cuando se realiza un multiplexado de imágenes binarias sencillas (códigos, letras, etc).

En el ejemplo anterior se usaron imágenes constantes en el proceso de multiplexado. La intensidad del ruido en la imagen recuperada (sea nivel de gris o binaria) depende directamente de la intensidad total multiplexada. Esto demuestra que el multiplexado impone algún tipo de restricción relacionada con la cantidad de información que se está codificando.

Ahora lo que se estudia es si la energía promedio de la suma de todas las imágenes de entrada produce el mismo comportamiento para el ruido en la etapa de recuperación, independientemente si la energía total tiene contribuciones de imágenes que aportan poco o bastante a este promedio energético total.

Con este fin, se realiza un nuevo experimento virtual, el procedimiento es el mismo descrito para el ejemplo anterior. Esta vez, las 299 imágenes multiplexadas con la palabra “CIOP” son las que se muestran en la Figura 4.10. La Figura 4.10 (a) es la imagen de la palabra “CIOP”, la Figura 4.10 (b) es una permutación de los píxeles de la palabra “CIOP” y la Figura 4.10 (c) es una imagen degradada de niveles de gris que tiene la misma energía total que la palabra “CIOP”. Estas tres imágenes tienen en común su energía total.

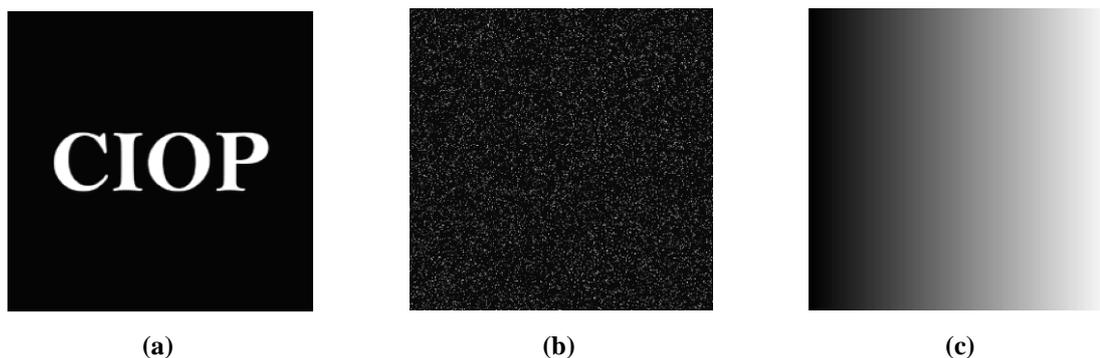


Figura 4.10: Imágenes a encriptar empleadas para realizar los multiplexados de la Figura 4.11

El primer multiplexado se realiza con 300 imágenes codificadas de la palabra “CIOP”, cada imagen se encripta con una llave de seguridad diferente $e^{-i\varphi_k(u,v)}$. El

segundo multiplexado se realiza con una imagen encriptada de la palabra “CIOP” y 299 imágenes encriptadas que son permutaciones de los píxeles de la imagen mostrada en la Figura 4.10 (b), nuevamente cada imagen se encripta con una llave de seguridad diferente $e^{-i\varphi_k(u,v)}$. Finalmente, el tercer multiplexado se realiza con una imagen encriptada de la palabra “CIOP” y 299 imágenes encriptadas que son permutaciones de los píxeles de la imagen mostrada en la Figura 4.10 (c), nuevamente cada imagen se encripta con una llave de seguridad diferente $e^{-i\varphi_k(u,v)}$.

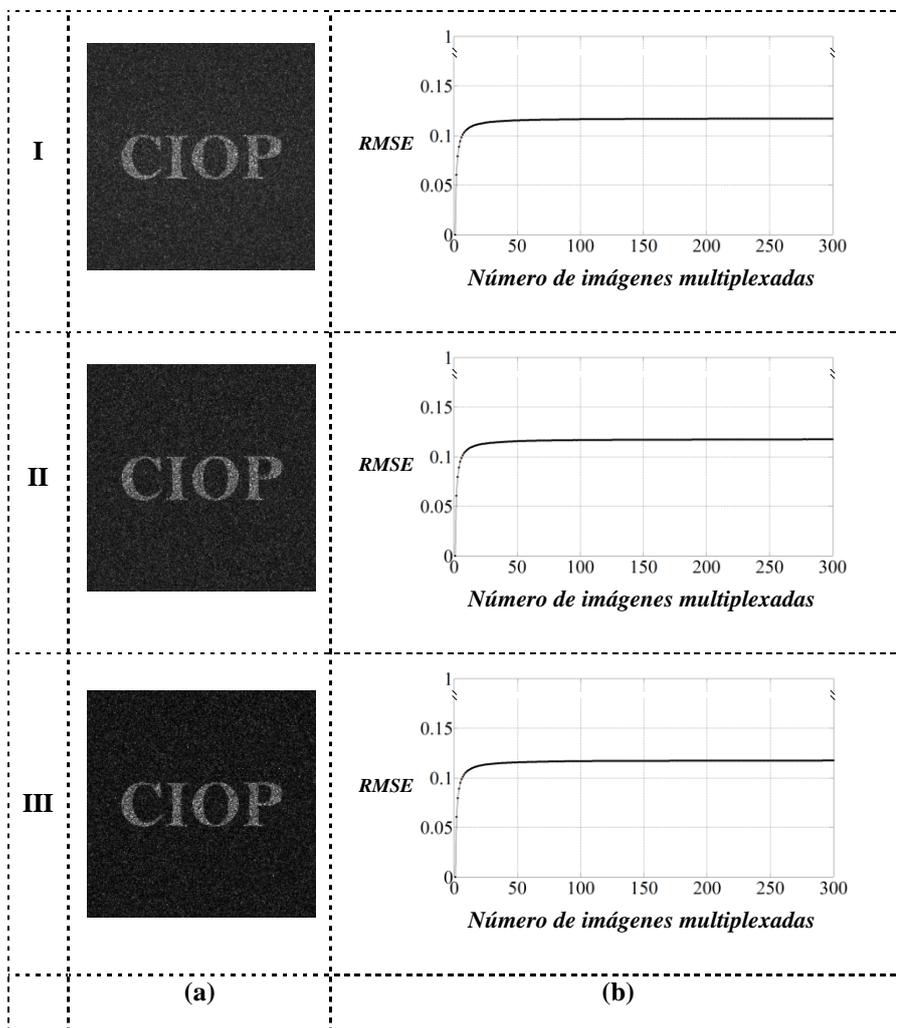


Figura 4.11: Imágenes recuperadas de un multiplexado de diez imágenes encriptadas y curvas de error *RMSE* de una imagen recuperada a partir de multiplexados de 2 a 300 imágenes encriptadas.

Los resultados son mostrados en la Figura 4.11. Las curvas de error *RMSE* de la Figura 4.11 (b) son calculadas entre la imagen de referencia (palabra “CIOP” recuperada sin multiplexar la información) y la imagen observada recuperada de un multiplexado de 2

a 300 imágenes encriptadas. Se puede observar que las curvas I, II y III tienen el mismo comportamiento y saturan a un mismo valor.

Ahora, las imágenes de la Figura 4.11 (a), son recuperadas de un multiplexado de diez objetos encriptados. Se puede observar cómo se presenta un ruido del mismo orden superpuesto sobre cada imagen decodificada. Por otro lado, obsérvese como al comparar estas imágenes recuperadas con la imagen de la Figura 4.9 (b) o Figura 4.9 (c), presentan menos ruido a pesar que las imágenes de la Figura 4.11 (a) han sido recuperadas de un multiplexado de diez imágenes, a diferencia de las imágenes de la Figura 4.9 que han sido recuperadas de un multiplexado de cinco imágenes. La presencia de más densidad de ruido es debido a que las intensidades totales de las imágenes encriptadas y multiplexadas involucradas en los resultados de la Figura 4.9 son mayores que las intensidades totales de las imágenes encriptadas y multiplexadas involucradas en los resultados de la Figura 4.11.

Nótese también de esta comparación que la curva fucsia en la Figura 4.8 tiene aproximadamente el mismo valor de saturación que las curvas de la Figura 4.11 (b). Comparando la calidad de cada imagen, la cota de saturación se ve reflejada en el contraste de las imágenes recuperadas: a mayor valor de cota más contraste. Regularmente, estos valores son normalizados para una mejor visualización de la información recuperada.

Para el ejemplo anterior se usaron imágenes que en promedio tienen la energía total de la palabra “CIOP”. Independientemente que sean binarias o en niveles de gris, el comportamiento de las curvas *RMSE* es el mismo y la única relación en común es esta energía total. Nótese también que es independiente de las frecuencias espaciales que pueda producir el objeto de entrada ya que no se tiene en cuenta un objeto en particular para las pruebas.

En este sentido, se realiza un último testeo con imágenes de niveles de gris. El procedimiento es el mismo descrito para los dos ejemplos anteriores. Inicialmente, se realiza un primer multiplexado donde la primera imagen encriptada es la palabra “CIOP” y las imágenes restantes son imágenes encriptadas que tienen diferentes distribuciones de niveles de gris con diferentes histogramas (imágenes cotidianas). El segundo multiplexado

se realiza con la palabra “CIOP” encriptada y las imágenes restantes son permutaciones aleatorias de los píxeles de cada imagen usada en el primer multiplexado, de esta manera se conserva la misma energía total. Y por último se realiza un tercer multiplexado donde la primera imagen encriptada es la palabra “CIOP” y las imágenes restantes son imágenes de niveles de gris uniformemente distribuidas en el rango de 0 a 255 y que tienen la misma energía total promedio del primer y segundo multiplexado. Los resultados de esta experiencia virtual, se pueden observar en la Figura 4.12.

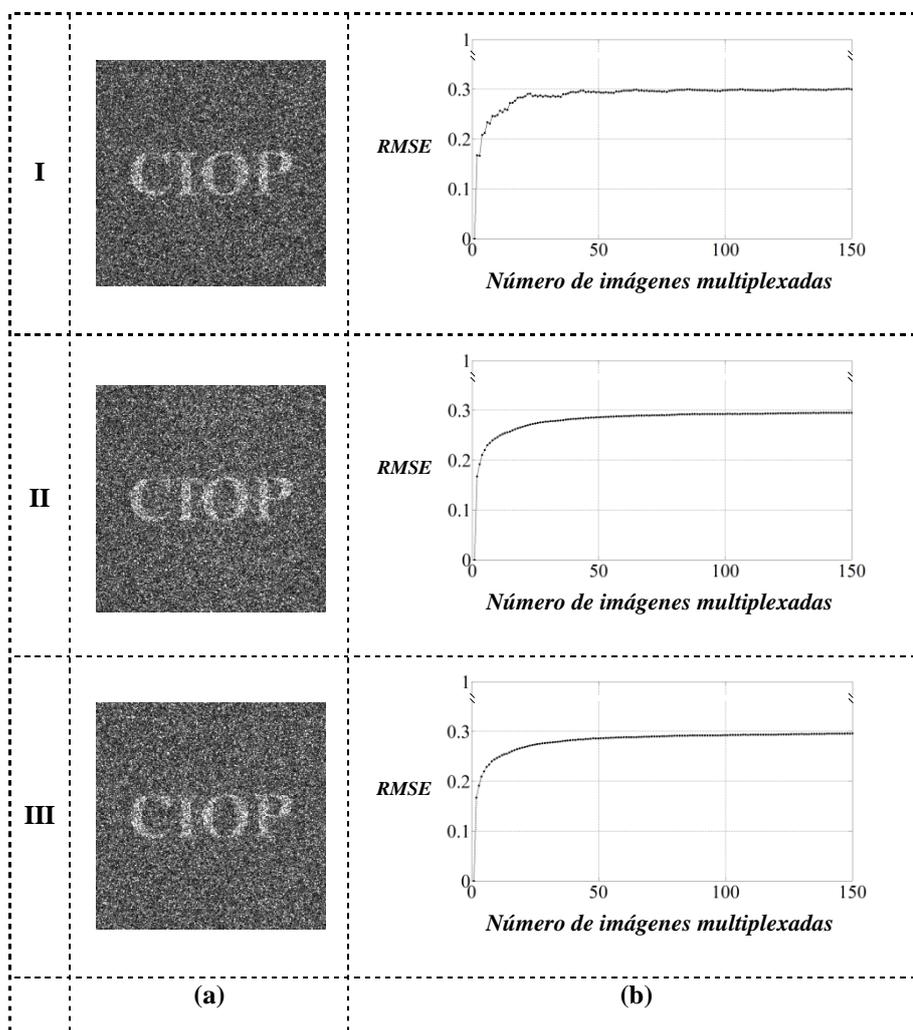


Figura 4.12: Imágenes recuperadas de un multiplexado de cinco imágenes encriptadas y curvas de error *RMSE* de una imagen recuperada a partir de multiplexados de 2 a 300 imágenes encriptadas.

Las imágenes de la Figura 4.12 (a) son recuperadas de un multiplexado de cinco imágenes encriptadas. Al compararlas con las imágenes de la Figura 4.11 (a), presentan mayor degradación pese a que han sido recuperadas de un multiplexado de cinco imágenes

encriptadas, a diferencia de las imágenes de la Figura 4.11 (a) que han sido recuperadas de un multiplexado de diez imágenes encriptadas. Nuevamente esto se puede relacionar con el único parámetro de variación, el promedio total de la energía multiplexada.

Las curvas de error *RMSE* de la Figura 4.12 (b), tienen el mismo comportamiento y saturan a un mismo valor independientemente de las imágenes usadas. Esto comprueba irrefutablemente que la relevancia del ruido en un multiplexado depende directamente de las energías de las imágenes multiplexadas. Los tres ejemplos mostrados soportan esta hipótesis.

Estos análisis son de gran importancia ya que explican el comportamiento de la calidad de las imágenes recuperadas respecto a la energía promedio de las imágenes encriptadas en un medio de registro plano. Estos resultados demuestran que existe una deficiencia al aplicar esta técnica en algunos aspectos. 1) la cantidad de información que se quiere transmitir en un multiplexado se ve restringida, ya que a mayor número de imágenes encriptadas multiplexadas mayor grado de deterioro en la imagen recuperada. 2) el contenido energético de la imagen influye directamente en el ruido del multiplexado, consecuentemente, las mismas características de la información a transmitir definen el grado de deterioro en la etapa de recuperación. Desde este enfoque, la técnica convencional de multiplexado en medios de registro planos es ineficiente para la transmisión de grandes volúmenes de información.

Los anteriores resultados permiten concluir lo siguiente. 1) el ruido promedio de multiplexado adicionado a una imagen descryptada no tiene dependencia con la forma del objeto de entrada si al cambiar la forma se conserva la energía total de la imagen. Esto se comprueba con los resultados obtenidos al usar las permutaciones aleatorias de la palabra “CIOP” y las permutaciones de las imágenes en niveles de gris las cuales no tienen una forma definida. Lo único que tienen en común es una energía total promedio. 2) la densidad y distribución del ruido de multiplexado no depende del número de píxeles de la imagen de entrada que interacciona con la primera máscara sino de su energía total. Esto se comprueba al evaluar el ruido de las imágenes recuperadas al multiplexar imágenes binarias y al multiplexar imágenes en niveles de gris. Cada uno de estos multiplexados

tiene la misma energía total pero el número de píxeles involucrados en el proceso de encriptación es mayor cuando se codifica imágenes de niveles de gris. Sin embargo, los órdenes del ruido obtenido son independientes de este hecho.

Los anteriores resultados son soportados por la Ecuación (4.19). El número de términos de la sumatoria del ruido aumenta con la cantidad de imágenes multiplexadas, lo cual indica que existen más términos sobre los cuales se distribuye la energía de entrada en el proceso de recuperación. Si se emplea la llave de seguridad correcta, en la Ecuación (4.17) siempre estará la imagen correctamente decodificada, sin embargo, si existen muchos términos de ruido de multiplexado la calidad de la imagen recuperada estará comprometida. El deterioro depende explícitamente de la cantidad de energía que contribuya en cada término de ruido. Por lo tanto, a mayor energía total multiplexada, mayor será el deterioro en la imagen recuperada.

En resumen, el solapamiento de información está presente al aplicar la técnica convencional de multiplexado de imágenes encriptadas en un medio de registro plano. Las imágenes recuperadas se ven afectadas por el ruido debido a dos casos: 1) la superposición de imágenes desencriptadas correctamente al usar una única llave de codificación $e^{i\varphi_m}$ para encriptar todos los objetos o 2) la superposición de imágenes desencriptadas incorrectamente al usar diferentes llaves de codificación $e^{i\varphi_m}$ para encriptar todos los objetos. En los dos casos, las imágenes recuperadas muestran un deterioro visual.

Consecuentemente para incrementar el número de datos procesados en un multiplexado lineal se tiene la necesidad de crear una nueva estrategia para evadir estos dos tipos de solapamiento de información. Pese a esta necesidad, no se han presentado soluciones eficientes para solucionar este problema que permita recuperar eficientemente grandes volúmenes de información.

Teniendo en cuenta este objetivo se introduce la técnica de modulación theta la cual es presentada en la siguiente sección como una herramienta para multiplexar información y como técnica de modulación para evadir la problemática del solapamiento presente en un multiplexado de imágenes encriptadas en un medio de registro plano.

4.5 Técnica de modulación theta

La técnica de modulación theta [4.22] es ampliamente conocida y ha sido empleada para realizar procesamiento óptico de información, algunas aplicaciones han sido en pseudocoloreado, composición de color, multiplexado de información, filtrado de componentes espaciales y frecuenciales [4.22]-[4.27], entre otras. La idea básica de estas propuestas es realizar una codificación de la información de sectores de una imagen por medio de la modulación de una estructura periódica de amplitud. De esta manera, se consigue una separación simple en el espacio de frecuencias ya que este tipo de redes difractan en posiciones que no se solapan sobre el plano de Fourier. Esto brinda la ventaja de poder modificar el espectro de frecuencias por medio de un filtrado espacial. Sin embargo, el precio a pagar es un incremento de resolución del material de registro y un incremento de ancho de banda espacial.

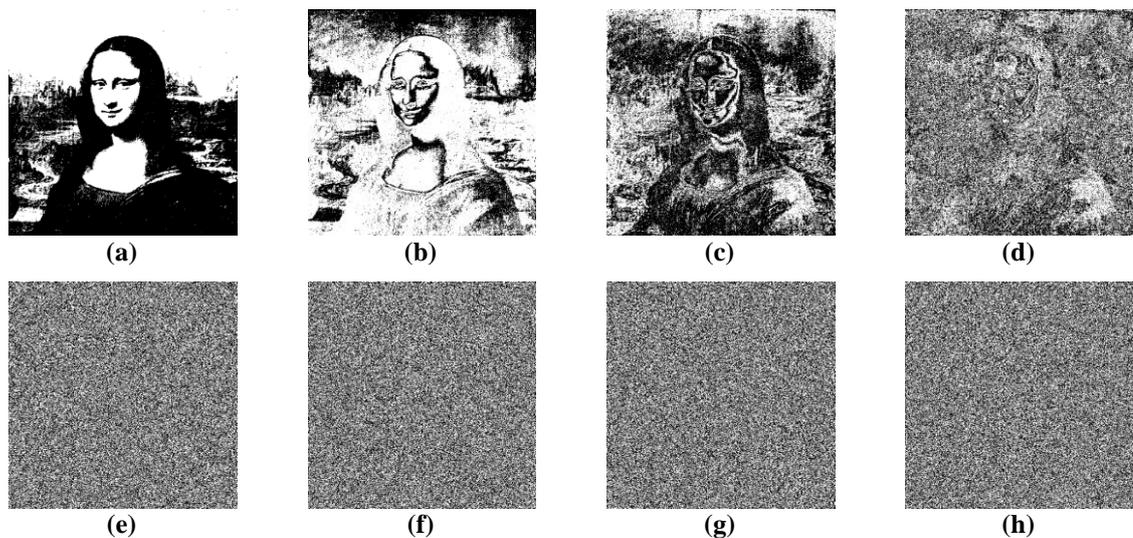


Figura 4.13: Descomposición de una imagen en 8 bits. (a) 1, (b) 2, (c) 3, (d) 4, (e) 5, (f) 6, (g) 7 y (h) 8 bits.

Para su aplicación, un objeto de entrada puede ser seccionado en sub-objetos de diferentes características, por ejemplo, una imagen puede ser separada en áreas de diferente forma, también se pueden crear sub-objetos que contengan un rango determinado de niveles de gris, o sub-objetos que definan el número de bits de la imagen, tal como se muestra en la Figura 4.13 donde una imagen ha sido seccionada en 8 bits. Al aplicar la técnica de modulación theta cada una de estas secciones es modulada por una red periódica

de amplitud en el dominio espacial. De esta forma, la difracción del objeto modulado producirá un espectro que consiste de un orden central y dos órdenes difractados. Esto gracias a la modulación de la red periódica sinusoidal de amplitud.

Consecuentemente, el objeto $O(x, y)$ puede ser representado como una composición de sub-objetos $\{O_1(x, y), O_2(x, y), \dots, O_n(x, y)\}$, los cuales son modulados por redes $\{G_1(x, y; u_1, v_1), G_2(x, y; u_2, v_2), \dots, G_n(x, y; u_n, v_n)\}$, donde u_n y v_n son las frecuencias espaciales de la red en las direcciones del *eje x* y del *eje y*, respectivamente.

Matemáticamente cada red sinusoidal de amplitud puede ser expresada como:

$$G_n(x, y; u_n, v_n) = \left\{ \frac{1}{2} + \frac{m}{2} \cos[2\pi(u_n x + v_n y)] \right\} \text{rect}\left(\frac{x}{a}\right) \text{rect}\left(\frac{y}{b}\right) \quad (4.20)$$

donde m es la amplitud entre picos consecutivos, a , b , son las dimensiones que limitan la red en el *eje x* y en el *eje y*, respectivamente y u_n , v_n son las frecuencias espaciales de la red en las direcciones del *eje x* y del *eje y*, respectivamente.

Por lo tanto, el objeto total modulado I_M puede ser escrito como una suma del producto de cada red periódica G_n y el sub-objeto O_n . Esto es:

$$I_M(x, y) = \sum_{k=1}^n O_k(x, y) G_k(x, y; u_k, v_k) \quad (4.21)$$

En la Figura 4.14 se muestra la representación de un objeto modulado $I_M(x, y)$ por cinco redes periódicas de amplitud.

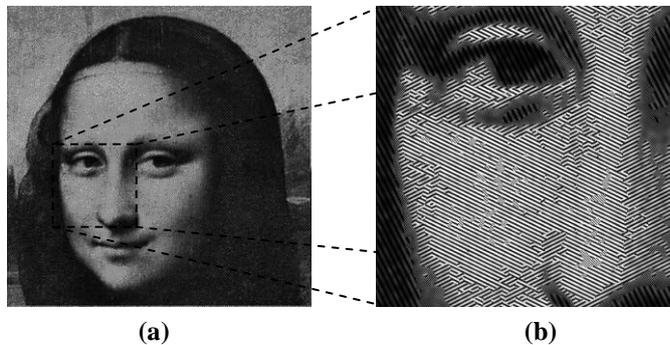


Figura 4.14: Objeto modulado por redes periódicas de amplitud. **(a)** Objeto modulado por cinco redes periódicas de amplitud de diferente frecuencia y dirección. **(b)** Parte aumentada de la imagen modulada.

El objeto fue seccionado en cinco sub-objetos $O_k(x, y)$, con $k = 1, 2 \dots, 5$, donde cada uno contiene un intervalo de niveles de gris de la imagen original. Posteriormente cada sub-objeto fue modulado con una red periódica de amplitud de diferente frecuencia y orientación $G_k(x, y; u_k, v_k)$. Finalmente fue recompuesto para obtener el objeto original modulado en diferentes secciones del plano.

Al introducir esta imagen theta modulada en un procesador $4f$ de dos lentes de igual distancia focal f , en el plano de Fourier de la primera lente se encontrará el plano de filtrado donde se puede manipular la información para recuperar convenientemente cualquier información que ha sido modulada con las redes de amplitud.

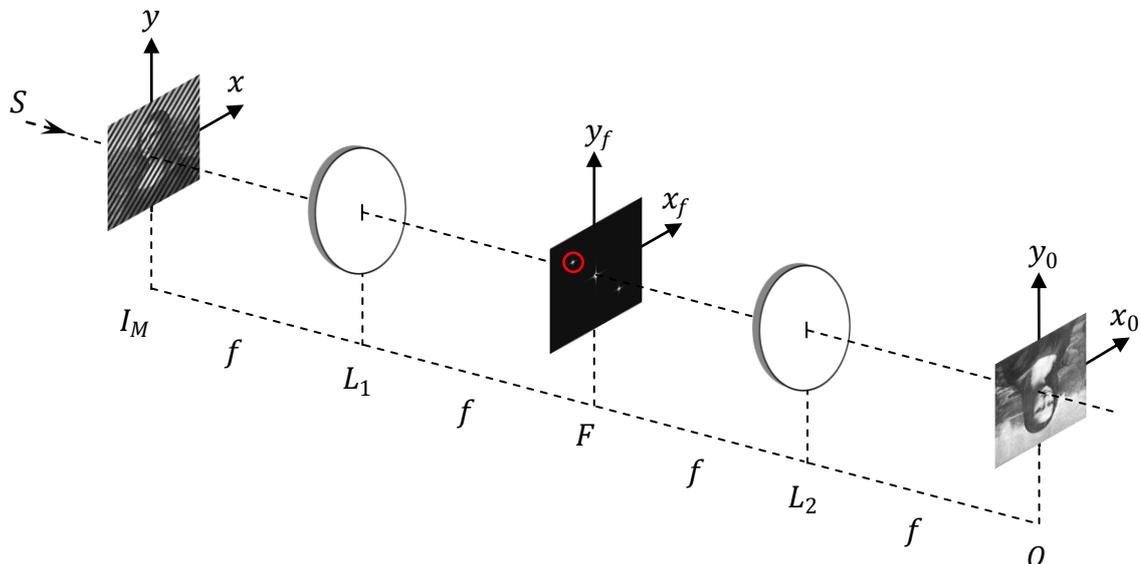


Figura 4.15: Técnica de modulación theta en un sistema $4f$. S es la fuente de iluminación, L_1 y L_2 son lentes de distancia focal f , I_M es la imagen theta modulada, F es el plano de filtrado y O es el objeto recuperado sin modulación.

Tal como se muestra en la Figura 4.15, en el plano de Fourier se producirá un orden central y dos órdenes difractados los cuales pueden ser filtrados independientemente. Si uno de estos órdenes se deja transmitir (representado por el círculo rojo), tras una nueva transformada de Fourier se obtendrá el objeto de entrada sin modulación.

Para un conjunto de sub-objetos que componen una imagen theta modulada representada por la Ecuación (4.21), matemáticamente, su espectro en frecuencias en el plano de Fourier puede ser escrito como:

$$\mathcal{F}[I_M(x, y)] = \sum_{k=1}^n \mathcal{F}[O_k(x, y)] \otimes \mathcal{F}[G_k(x, y; u_k, v_k)] \quad (4.22)$$

donde \mathcal{F} es la transformada de Fourier y \otimes es el operador de convolución. Debido a que la transformada de Fourier de las redes periódicas puede ser expresada como:

$$\mathcal{F}[G_k(x, y; u_k, v_k)] = \mathcal{F}\left\{\frac{1}{2} + \frac{m}{2} \cos[2\pi(u_n x + v_n y)]\right\} \otimes \mathcal{F}\left[rect\left(\frac{x}{a}\right)rect\left(\frac{y}{b}\right)\right] \quad (4.23)$$

se tiene que la Ecuación (4.22) puede ser escrita como:

$$\begin{aligned} \mathcal{F}[I_M(x, y)] = \sum_{k=1}^n \left\{ \left[\frac{1}{2} \delta(f_x, f_y) + \frac{m}{4} \delta(f_x + u_k, f_y + v_k) + \frac{m}{4} \delta(f_x - u_k, f_y - v_k) \right] \right. \\ \left. \otimes ab \operatorname{sinc}(af_x) \operatorname{sinc}(bf_y) \otimes \mathcal{F}[O_k(x, y)] \right\} \end{aligned} \quad (4.24)$$

donde $f_x = x/\lambda z$ y $f_y = y/\lambda z$ son frecuencias espaciales. De esta forma, la contribución de cada espectro de los sub-objetos modulados (un orden central y dos órdenes difractados) están superpuestos en el plano de Fourier. El orden central está dado por:

$$S_{central} = \sum_{k=1}^n \frac{ab}{2} \operatorname{sinc}(af_x) \operatorname{sinc}(bf_y) \otimes \mathcal{F}[O_k(x, y)] \quad (4.25)$$

y las parejas de órdenes difractados están determinados por:

$$\begin{aligned} S_{difractados} = \sum_{k=1}^n \frac{abm}{4} \left\{ \operatorname{sinc}[a(f_x + u_k)] \operatorname{sinc}[b(f_y + v_k)] \right. \\ \left. + \operatorname{sinc}[a(f_x - u_k)] \operatorname{sinc}[b(f_y - v_k)] \right\} \otimes \mathcal{F}[O_k(x, y)] \end{aligned} \quad (4.26)$$

La Ecuación (4.25) indica que los órdenes centrales están superpuestos y está contenida toda la información de cada una de las secciones de los objetos. Si se filtra el orden central, al hacer una nueva transformada de Fourier se recupera el objeto completo

sin modulación. De la Ecuación (4.26) se puede observar que cada orden difractado estará distribuido en posiciones diferentes del plano de frecuencias. Cada orden contiene la información particular que ha sido modulada por la red periódica sinusoidal. Al dejar transmitir un único orden difractado se recuperará esa información sin modulación.

En la Figura 4.16 se muestra el espectro de un objeto theta modulado por cinco redes de diferente orientación e igual frecuencia. Como se puede observar, las frecuencias de las redes periódicas hacen que los órdenes difractados estén a una posición equidistante del orden central. Como se mencionó, la superposición de los espectros de los sub-objetos está determinada por la Ecuación (4.25) y cada par de órdenes difractados en el plano de Fourier están determinados por la Ecuación (4.26).

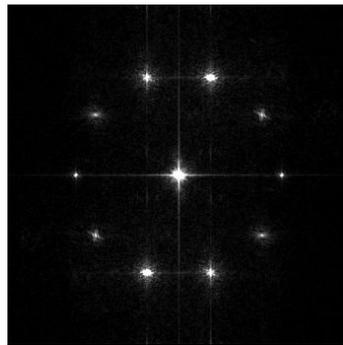


Figura 4.16: Difracción de un objeto modulado por cinco redes periódicas de amplitud de diferente orientación e igual frecuencia.

A continuación se presentan dos procedimientos para procesar información usando esta técnica de modulación y usando el concepto de multiplexado de información.

4.5.1 Composición de color

Una aplicación directa de la técnica de modulación theta es la técnica de multiplexado de información. Como se mostró en la sección anterior, la entrada puede ser modulada por varias redes periódicas sinusoidales de amplitud. Este procedimiento puede ser asemejado al multiplexado de diferentes características del objeto de entrada las cuales pueden ser moduladas y multiplexadas para luego ser recuperadas y procesadas independientemente.

En la contribución realizada por Armitage y Lohmann [4.22] se presenta la técnica de modulación theta para realizar la producción de color de una imagen a partir de transparencias binarias. El esquema del montaje experimental original es mostrado en la Figura 4.17 y la técnica se basa en un procesador óptico en configuración $4f$. Este procedimiento consiste en modular un objeto de entrada con redes de Ronchi. El plano de filtrado se encuentra en el plano focal posterior de la primera lente donde se filtra un orden difractado para recuperar el objeto sin modulación, tal como se explicó en la sección anterior.

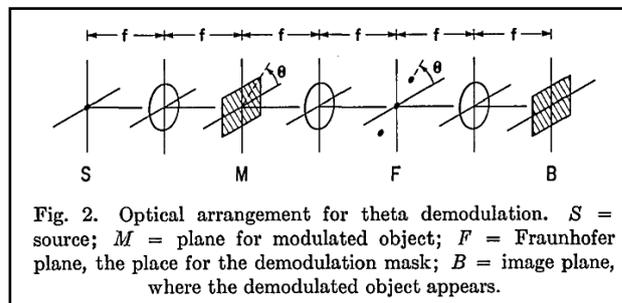


Figura 4.17: Arreglo experimental de la técnica de modulación theta introducida por Armitage y Lohmann, imagen tomada de la referencia [4.22].

En la presente sección se implementa en un SOV la experiencia de Armitage y Lohmann con el fin de ejemplificar los resultados obtenidos con la técnica de modulación theta para la construcción de color. Esta técnica será empleada en capítulos subsecuentes para generar secuencias policromáticas. Se aclara que se reproduce el sistema óptico analógico empleado por Armitage y Lohmann explicando únicamente lo que se considera relevante y realizando algunos análisis propios para las aplicaciones prácticas realizadas en esta Tesis. Para el lector interesado en profundizar en el detalle del origen de estas experiencias se recomienda ver las referencias [4.22]-[4.24].

La experiencia virtual consiste del siguiente procedimiento. Inicialmente, para realizar el procesamiento de una imagen policromática, se considera que el objeto está compuesto de tres canales de color que son separados para ser procesados independientemente. De esta forma cada canal de color modulado por una red periódica sinusoidal de amplitud puede ser expresado como:

$$I_M(x, y, c) = O_c(x, y)G_c(x, y; u_c, v_c) \quad (4.27)$$

donde $c = 1, 2, 3$ representan las componentes de color de la imagen. En este texto se trabajarán imágenes compuestas de canales de color rojo (R), verde (G) y azul (B), llamadas imágenes RGB. En la Figura 4.18 se ejemplifica la composición digital de color para una imagen RGB. Las imágenes (a), (b) y (c) son los canales rojo, verde y azul, respectivamente, representadas como imágenes binarias. La imagen (d) es la composición de color usando los tres canales.

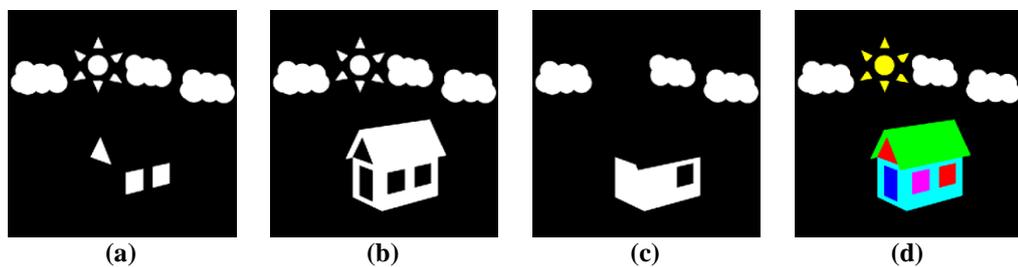


Figura 4.18: Composición de color de una imagen usando tres canales independientes rojo verde y azul. (a) canal de color rojo, (b) canal de color verde, (c) canal de color azul y (d) imagen con composición de color usando (a), (b) y (c).

Si bien el ejemplo anterior es sobre imágenes binarias, que representan colores puros, la aplicación puede ser extendida a colores compuestos de combinaciones de valores de niveles de gris en 8 bits en los tres canales de color. Esto define precisamente imágenes de 256 colores, 24 bits de color, etc.

Al considerar las tres componentes de color como tres mensajes independientes se puede referir como si fuera un multiplexado de tres señales. Es decir, el color compuesto puede ser visto como el multiplexado de los canales RGB, donde cada uno puede ser theta modulado independientemente. En este sentido, todos los sub-elementos del color verde por ejemplo, constituyen juntos una señal, la cual en principio puede ser completamente independiente y ser modulada con redes de diferentes orientaciones si se quisiera.

En la experiencia virtual, cada componente de color es iluminada con una única longitud de onda para realizar el procesamiento óptico. Una de las razones para realizar este procedimiento son las aberraciones cromáticas presentes al realizar un procesado de los tres canales con una fuente policromática o al iluminar cada canal de color con una longitud de onda diferente. Esto se observa en la Figura 4.19.

La superficie de la Figura 4.19 es el espectro obtenido a partir de un SOV que realiza la transformada de Fourier de una red periódica sinusoidal de amplitud usando una lente de 150 mm. La red está contenida en un área de $1.3 \times 1.3 \text{ mm}^2$ y tiene un pitch de aproximadamente $184 \text{ }\mu\text{m}$. Esta red es iluminada con longitudes de onda $\lambda_1 = 633 \text{ nm}$, $\lambda_2 = 514 \text{ nm}$ y $\lambda_3 = 405 \text{ nm}$. Cada patrón de difracción es normalizado y superpuesto en esta superficie.

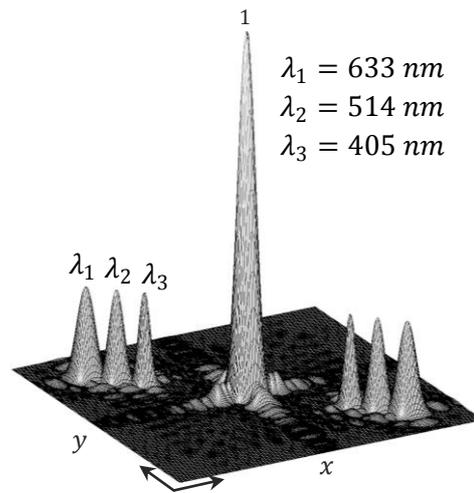


Figura 4.19: Difracción de una red periódica de amplitud usando luz monocromática de diferentes longitudes de ondas λ_c . Las superficies normalizadas son superpuestas observando el solapamiento de los órdenes difractados de una red periódica sinusoidal iluminada con longitudes de onda $\lambda_1 = 633 \text{ nm}$, $\lambda_2 = 514 \text{ nm}$ y $\lambda_3 = 405 \text{ nm}$.

Nótese como el ancho de los lóbulos de los órdenes difractados tienen diferentes tamaños y como están ubicados en posiciones distintas respecto al orden central. La iluminación de esta red con luz policromática que contiene diferentes longitudes de onda, $\lambda_{c=1,2,3}$ produce órdenes de difracción de varios tamaños que se superponen en el plano de Fourier. Esto se debe a que las frecuencias de la red (u_c, v_c) , la longitud de onda de iluminación λ_c y la distancia focal de la lente f , definen el tamaño de los órdenes difractados según la relación $\lambda f/w$. Del mismo modo, estos parámetros definen la distancia de separación medida desde el orden central a cada orden difractado según la relación $\lambda f(u_k^2 + v_k^2)^{1/2}$. Por lo tanto, si se quiere realizar un procesamiento óptico con luz policromática se deben usar filtros para cada longitud de onda eliminando las contribuciones de las otras dos restantes.

Volviendo a la aplicación del procesamiento de imágenes de color por canales independientes. Cada componente de color es modulada con una red de diferente orientación para obtener imágenes descritas por la Ecuación (4.27). Cada componente de color theta modulada es ubicada en el procesador óptico $4f$ de la Figura 4.20.

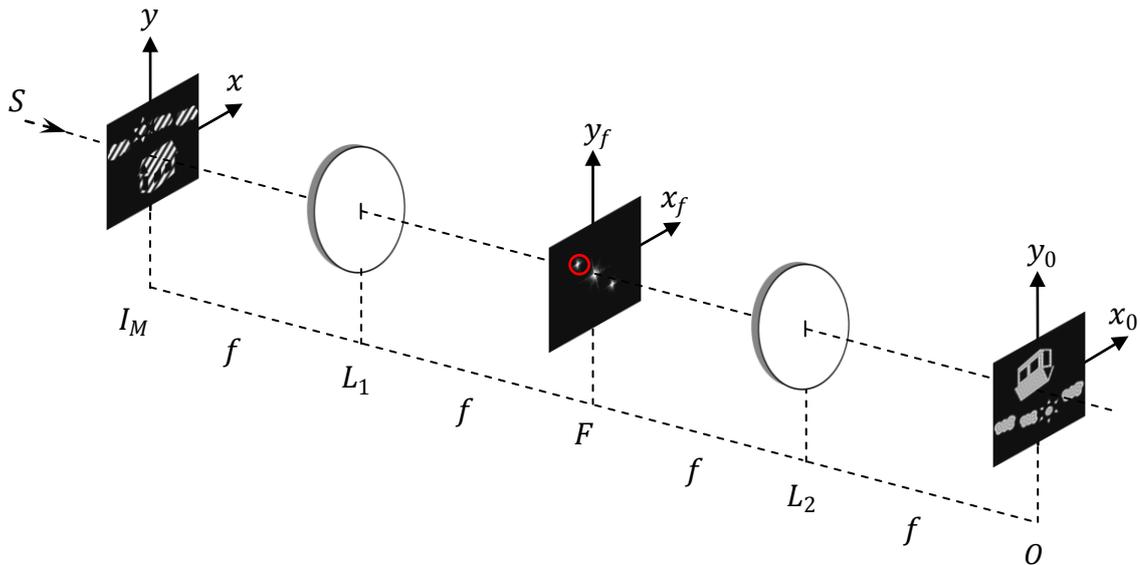


Figura 4.20: Técnica de modulación theta implementada en un SOV. S es la fuente de iluminación, L_1 y L_2 son lentes de distancia focal f , I_M es el canal de color theta modulado, F es el plano de filtrado y O es el canal de color recuperado sin modulación.

En el plano de Fourier de la lente L_1 de distancia focal f , se introduce la imagen theta modulada de cada color. El espectro consiste de un orden central y dos órdenes difractados definidos por las frecuencias espaciales de la red, la distancia focal de la lente y la longitud de onda de iluminación. Posteriormente uno de estos órdenes es filtrado en el plano de Fourier F , finalmente, la lente L_2 realiza una transformada de Fourier para obtener la componente de color sin modulación.

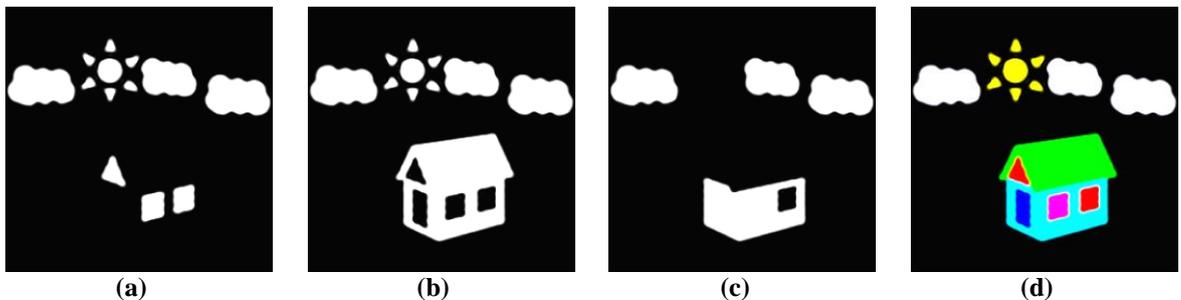


Figura 4.21: Composición de color de una imagen usando tres canales cromáticos, rojo, verde y azul. El procesado óptico se ha realizado en un SOV en configuración $4f$. (a) Canal de color rojo, (b) canal de color verde, (c) canal de color azul y (d) imagen con composición de color usando (a), (b) y (c).

Realizando este proceso en un SOV para los tres canales de color se obtienen los resultados mostrados en la Figura 4.21. Las imágenes (a), (b) y (c) son los canales de color procesados por separado y la composición se logra uniendo los tres canales cromáticos para obtener la imagen de la Figura 4.21 (d).

4.5.2 Multiplexado de información

Desde el punto de vista del procesamiento de información, los aspectos más relevantes de la técnica de modulación theta tienen lugar en el proceso de demodulación al recuperar características de la imagen a partir de la etapa de filtrado. Esta técnica puede ser usada para generar “niveles” de acceso en la recomposición de la imagen. En este sentido, se puede hablar de multiplexado.

Nuevamente, en un SOV en configuración $4f$ se realiza la implementación para el multiplexado de información.

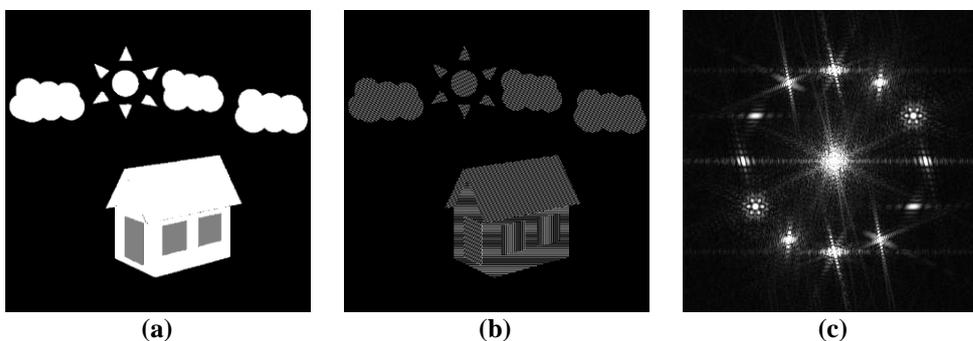


Figura 4.22: Modulación de imágenes con redes de diferente orientación. (a) imagen original, (b) imagen thetamodulada y (c) transformada de Fourier del objeto modulado.

La Figura 4.22 (a) muestra una imagen de tres niveles de gris, la imagen es segmentada en seis partes, nubes, sol, techo, puerta, ventanas y pared. Cada sección es modulada por una red de amplitud periódica de diferente orientación e igual frecuencia. Posteriormente el objeto es recompuesto como lo muestra la Figura 4.22 (b). El objeto theta modulado es la entrada en el SOV $4f$. Al encontrar el espectro del objeto, en el plano de filtrado se logran visualizar seis parejas de órdenes difractados correspondientes a cada segmento modulado como lo muestra la Figura 4.22 (c). En el plano de filtrado se puede observar como cada par de parejas de órdenes difractados tienen diferente forma

correspondiendo cada una a los objetos que representan las nubes, el sol, el techo, la puerta, las ventanas y la pared.

En el plano de Fourier de la primera lente del SOV $4f$ (Figura 4.20), se pueden diseñar todo tipo de máscaras para filtrar la información de interés. En este caso se han empleado aperturas circulares que limitan las frecuencias de cada orden difractado, como se observa en las Figuras 4.23 (a), (b) y (c).

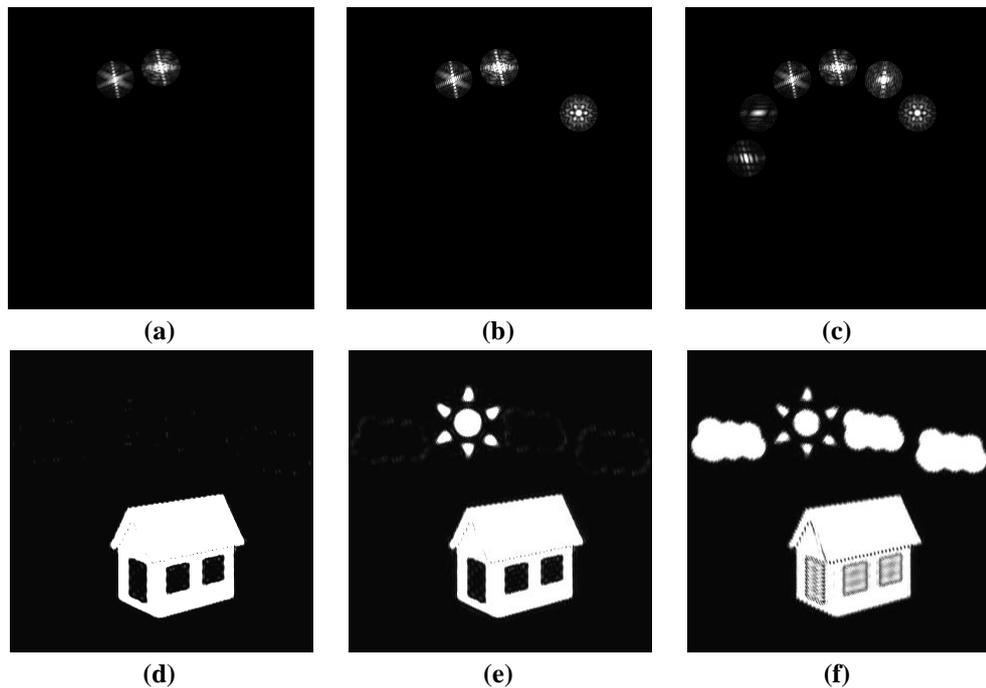


Figura 4.23: Proceso de filtrado de órdenes difractados por un objeto tehetta modulado. (a), (b) y (c) filtrado de dos órdenes, tres órdenes y seis órdenes, respectivamente. (d), (e) y (f) imágenes recuperadas a partir de los órdenes filtrados mostrados en (a), (b) y (c), respectivamente.

De esta experiencia virtual se pudo observar que la información multiplexada se encuentra en el plano de frecuencias donde se generan “niveles” de acceso a los segmentos de cada imagen modulada. Al filtrar los dos órdenes mostrados en la Figura 4.23 (a) se recupera el techo y la pared de la casa, Figura 4.23 (d). Al filtrar los tres órdenes de la Figura 4.23 (b) se recupera el techo la pared y el sol, Figura 4.23 (e). Por último, al filtrar los seis órdenes de la Figura 4.23 (c) se obtiene toda la imagen sin modulación, Figura 4.23 (f).

Las experiencias de filtrado espacial han mostrado que al limitar la información transmitida en el plano de frecuencias se puede realizar operaciones típicas de detección de

bordes o realces de detalles en la imagen, etc. También es conocido que regularmente filtrar en el plano de frecuencias de una imagen lleva a la pérdida de detalles finos en el objeto recuperado. Esto mismo ocurre en las Figuras 4.23 (d), (e) y (f). Aquí se pueden notar los efectos de pérdidas de bordes en todas las imágenes recuperadas, también son visibles la superposición de bordes de otros objetos que contribuyen en el campo complejo que se deja transmitir en la etapa de filtrado, por último se presenta el efecto de franjas de Moiré en los bordes de las imágenes recuperadas.

Las dos experiencias virtuales expuestas en los dos ejemplos anteriores muestran la gran ventaja de la técnica de modulación theta en la descomposición de un objeto en el plano de frecuencias y la recomposición del objeto sin modulación filtrando los órdenes de difracción. Ahora, recordando las deficiencias que posee un multiplexado lineal, se puede pensar en aprovechar la gran ventaja de re-direccionamiento de frecuencias que realiza la técnica de modulación theta para evadir la presencia de solapamiento de información en un multiplexado de imágenes encriptadas.

La inserción de esta técnica de modulación theta en el sistema de encriptación de doble máscara de fase en configuración $4f$ resulta en una técnica novedosa que permite transmitir un mayor volumen de información sin que existan restricciones referentes al objeto que se va a encriptar. Por otro lado, brinda la ventaja adicional de poder recuperar la información sin solapamiento al filtrar cada orden de difracción. Consecuentemente, optimizar la capacidad de transmisión de imágenes en un multiplexado y asegurar una eficiente recuperación de la información significa una optimización en la etapa del emisor y en la etapa de recepción en un sistema de comunicaciones clásico. Esto abre un amplio abanico de aplicaciones que hasta el momento no eran posibles de realizar con los sistemas convencionales de encriptación.

4.6 Bibliografía

- [4.1] A. Carnicer, M. Montes-Usategui, S. Arcos, I. Juvells, "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," *Opt. Lett.* 30, 1644–1646 (2005).

- [4.2] X. Peng, P. Zhang, H. Wei, B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," *Opt. Lett.* 31, 1044-1046 (2006).
- [4.3] X. Peng, H. Wei, P. Zhang, "Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain," *Opt. Lett.* 31, 3261-3263 (2006).
- [4.4] Y. Frauel, A. Castro, T. J. Naughton, B. Javidi, "Resistance of the double random phase encryption against various attacks," *Opt. Express* 15, 10253–10265 (2007).
- [4.5] G. Situ, U. Gopinathan, D. S. Monaghan, J. T. Sheridan, "Cryptanalysis of optical security systems with significant output images," *Appl. Opt.* 46, 5257-5262 (2007).
- [4.6] X. C. Cheng, L. Z. Cai, Y. R. Wang, X. F. Meng, H. Zhang, X. F. Xu, X. X. Shen, G. Y. Dong, "Security enhancement of double-random phase encryption by amplitude modulation," *Opt. Lett.* 33, 1575-1577 (2008).
- [4.7] X. Yong-Liang, Z. Xin, Y. Sheng, L. Qiang, L. Yang-Cong, "Multiple-image optical encryption: an improved encoding approach," *Appl. Opt.* 48, 2686-2692 (2009).
- [4.8] Y. Chen, J. Chen, "Cryptosystem for plaintext messages utilizing optical properties of gratings," *Appl. Opt.* 49, 2041-2046 (2010).
- [4.9] A. J. Menezes, P. C. Van Oorschot, y S. A. Vanstone. *Handbook of Applied Cryptography*, CRC Press, (1997). pp. 41-44.
- [4.10] T. G. Pencheva, M. P. Petrov, S. I. Stepanov, Selective properties of volume phase holograms in photorefractive crystals, *Optics Communications*, Volume 40, Issue 3, 1 January (1982), Pages 175-178.
- [4.11] J. Goltz, T. Tschudi, Angular selectivity of volume holograms recorded in photorefractive crystals; An analytical treatment, *Optics Communications*, Volume 67, Issue 3, 1 July (1988), Pages 164-166.
- [4.12] K. Nonaka, "Off-Bragg Analysis of the Diffraction Efficiency of Reflection Photorefractive Holograms," *Appl. Opt.* 37, 3215-3221 (1998).

- [4.13] T. Kume, K. Nonaka, M. Yamamoto, S. Yagi, "Wavelength-Multiplexed Holographic Data Storage by Use of Reflection Geometry with a Cerium-Doped Strontium Barium Niobate Single-Crystal Structure and a Tunable Laser Diode," *Appl. Opt.* **37**, 334-339 (1998).
- [4.14] S. G. Kim, H. S. Lee, K. T. Kim, E. S. Kim, B. Lee, "Angular multiplexed holographic memory system based on moving window on liquid crystal display and its crosstalk analysis," *Optical and Quantum Electronics* Vol. 32, No. 3, (2000), 419-430.
- [4.15] C. C. Chang, G. W. Hu, C. Y. Lin, K. L. Russell, "Encrypted holographic memory using rotationally random phase encoding," G. Salamo, A. Siahmakoun, in *Photorefractive Effects, Materials, and Devices*, Vol. 62 of OSA Trends in Optics and Photonics (Optical Society of America, 2001), paper 188.
- [4.16] W. Su, C. Lin, "Enhancement of the Angular Selectivity in Encrypted Holographic Memory," *Appl. Opt.* **43**, 2298-2304 (2004).
- [4.17] J. S. Courtney-Pratt, *J. Soc. Motion Picture Television Engrs.* **72**, 876 (1963).
- [4.18] G. Situ, J. Zhang, "Multiple-image encryption by wavelength multiplexing," *Opt. Lett.* **30**, 1306–1308 (2005).
- [4.19] J. F. Barrera, R. Henao, M. Tebaldi, N. Bolognini, R. Torroba, "Multiplexing encryption-decryption via lateral shifting of a random phase mask," *Opt. Commun.* **259**, 532–536 (2006).
- [4.20] J. F. Barrera, R. Henao, M. Tebaldi, N. Bolognini, R. Torroba, "Multiplexing encrypted data by using polarized light," *Opt. Commun.* **260**, 109–112 (2006).
- [4.21] J. F. Barrera, R. Henao, M. Tebaldi, N. Bolognini, R. Torroba, "Multiple image encryption using an aperture modulated optical system," *Opt. Commun.* **261**, 29–33 (2006).
- [4.22] J. D. Armitage, A. W. Lohmann, "Theta Modulation in Optics," *Appl. Opt.* **4**, 399-403 (1965).

- [4.23] A. G. Apostolidis, J. Spyridelis, "Image multiplexing and color images with theta modulation of the speckle patterns," *Optics Communications*, Volume 40, Issue 4, 15 January (1982), Pages 249-253.
- [4.24] P. Andres, C. Ferreira, A. Pons, C. Hernandez, "Colour mixtures through theta-modulation technique," *Optics Communications*, Volume 48, Issue 2, 15 November (1983), Pages 103-106.
- [4.25] H. Bartelt, A. W. Lohmann, E. E. Sicre, "Optical logical processing in parallel with theta modulation," *J. Opt. Soc. Am. A* 1, 944-951 (1984).
- [4.26] A. Kumar, R. M. Vasu, "Multiplexing in multiple imaging through the theta modulation technique," *Optics Communications*, Volume 66, Issue 1, 1 April (1988), 6-8.
- [4.27] K. W. Wong, L. M. Cheng, "A new theta modulation multiplexing scheme for computer-generated holograms," *Optics and Laser Technology*, Volume 24, Issue 2, April (1992), 89-92.

Capítulo 5

Técnica de encriptación de eventos dinámicos

5.1 Introducción

Se ha enfatizado que el procesado óptico coherente de información ha contribuido al desarrollo de las comunicaciones en tiempo real y en la transmisión de imágenes, además, el avance significativo de las redes de comunicaciones ha permitido aumentar la cantidad de información soportada por los canales de comunicación. En la actualidad se requiere que estos grandes volúmenes de datos sean resguardados requiriendo que en los procesos de transmisión se asegure la información de forma tal que al ser interceptada por usuarios no autorizados no se revelen datos confidenciales.

Como se ha expuesto, las tecnologías ópticas son grandes candidatas para procesar y transmitir grandes volúmenes de datos de manera segura. Existen diferentes arquitecturas de encriptación con las cuales se puede resguardar información usando como llaves de seguridad diferentes grados de libertad del sistema óptico (longitud de onda, polarización, distancias de propagación, etc.), parámetros que se deben conocer para recuperar los datos encriptados.

Hasta ahora, los estudios realizados en la protección de datos por métodos ópticos se han limitado a trabajar con eventos estáticos o información representada por imágenes, códigos, textos, etc. Antes del desarrollo aquí propuesto, no existían reportes de una técnica óptica eficiente que permitiera encriptar una escena en movimiento y recuperarla a tiempo real.

La contribución más cercana fue realizada por Alfalou y Mansour [5.1]. Estos autores proponen la encriptación de tres imágenes combinándolas linealmente con parámetros de mezclado que producen otras imágenes codificadas. Estas refuerzan la seguridad en la transmisión de la información en un canal de comunicación digital. Con un proceso inverso en la etapa de desencriptación, reconstruyen una escena de tres imágenes que representa la escena en movimiento. Más allá de esta referencia no se encuentran registros de encriptación y transmisión de información de eventos que evolucionan en el tiempo.

La importancia de transmitir eventos dinámicos reproducibles en aplicaciones multimedia acoplando texto, imagen, sonido y video radica en la necesidad de transmitir información que permita una comunicación más eficiente y más minuciosa en la descripción de un evento o múltiples eventos, es decir, existe la necesidad de transmitir ideas complejas que con una simple imagen no se pueden representar. En este sentido, es muy importante desarrollar una técnica que brinde la posibilidad de manejar y transmitir grandes volúmenes de datos en forma confidencial.

En el Capítulo 4 se presentó la técnica de multiplexado como una opción para codificar grandes volúmenes de información. Sin embargo, se mostró que esta técnica presenta solapamiento de información cuando se recupera una imagen a partir del multiplexado. Esto impone restricciones sobre la información que se va a encriptar ya que el ruido en la imagen recuperada depende de la cantidad de energía total de la información multiplexada. Para resolver esta dificultad se usufructuó la característica de redireccionamiento de las frecuencias espaciales que genera la técnica de modulación theta.

La propuesta que se plantea en este capítulo combina la arquitectura convencional de codificación $4f$ y la técnica de modulación theta. El objetivo consiste en modular cada imagen encriptada con redes sinusoidales de amplitud de diferente orientación y diferente frecuencia. De esta manera, en la etapa de desencriptación se introducirá un plano de filtrado donde se puede recuperar convenientemente cada elemento de información encriptada y evitar así cualquiera de los dos tipos de solapamiento de información presentes en un multiplexado convencional. Al procedimiento desarrollado se lo denomina

técnica de encriptación de eventos dinámicos y constituye una contribución original en esta línea de investigación.

En la Sección 5.2 se presenta las etapas que involucran la técnica de encriptación de eventos en una arquitectura *4f*. En la Sección 5.3 se formula su implementación. Finalmente, en la Sección 5.4 se plantean algunas consideraciones relativas a la seguridad del sistema propuesto.

5.2 Sistema de encriptación de eventos dinámicos en la arquitectura *4f*

Un evento dinámico es una situación que evoluciona en el tiempo. Un conjunto de imágenes visualizadas consecutivamente y en forma sincronizada constituye una escena en movimiento. La técnica de encriptación de eventos dinámicos permite codificar y decodificar esta secuencia sincronizada de imágenes. El usuario al aplicar el proceso de desencriptación reproduce la escena en movimiento y en tiempo real.

Para llevar a cabo este procedimiento, la técnica de encriptación de eventos dinámicos se divide en cinco etapas: 1) etapa de encriptación, 2) etapa de modulación, 3) etapa de multiplexado, 4) etapa de filtrado y sincronización y 5) etapa de desencriptación. Estos cinco procesos que se describen a continuación, posibilitan codificar varias imágenes y evitan el solapamiento de información en las imágenes recuperadas.

5.2.1 Etapa de encriptación

Se ha seleccionado como protocolo de encriptación el sistema convencional de codificación de doble máscara de fase basado en una arquitectura *4f*. Como se explicó en la Sección 2.2, este sistema emplea dos máscaras de fase con valores distribuidos uniformemente en el rango entre 0 y 2π . La primera se sitúa en el plano del objeto y la segunda se ubica en el plano de Fourier de la primera lente actuando como llave de seguridad.

La etapa de encriptación consta de un único sistema de codificación $4f$ con el cual se encripta cada una de las imágenes de la secuencia dinámica. La encriptación de la escena se puede hacer de dos maneras, usando una única llave de seguridad para codificar todas las imágenes o usando una llave de seguridad diferente para codificar cada imagen de la película. Estos dos casos son exactamente los mismos que conducen al solapamiento de información en la técnica convencional de multiplexado (Capítulo 4).

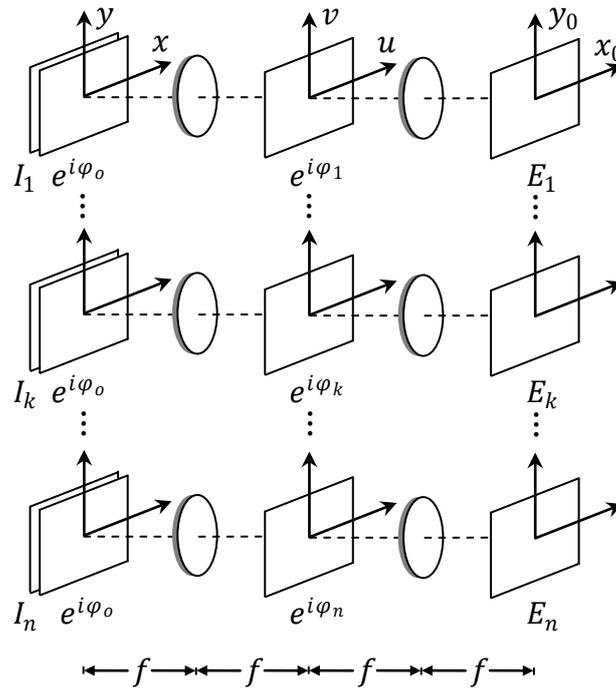


Figura 5.1: Etapa de encriptación de un evento dinámico. El sistema es un sistema $4f$ compuesto de dos lentes de distancia focal f , I_k es la k -ésima imagen de la secuencia dinámica, $e^{i\phi_0}$ es la primera máscara de fase, $e^{i\phi_k}$ es la k -ésima llave de seguridad y E_k es la k -ésima imagen encriptada.

Haciendo referencia a la Figura 5.1, la k -ésima imagen encriptada de la escena dinámica puede ser descrita matemáticamente como:

$$E_k(x_0, y_0) = \mathcal{F}\{\mathcal{F}[I_k(x, y)e^{i\phi_0(x, y)}]e^{i\phi_k(u, v)}\} \quad (5.1)$$

donde $I_k(x, y)$ es una imagen de la película, $e^{i\phi_0(x, y)}$ es la primera máscara de fase, $e^{i\phi_k(u, v)}$ es la llave de codificación, $E_k(x_0, y_0)$ es la imagen encriptada y \mathcal{F} representa la transformada de Fourier.

Si en esta instancia se realiza un multiplexado convencional de las imágenes encriptadas, se producirá degradación en la información recuperada en la etapa de

decodificación, tal como se mostró en la Sección 4.3 y en la Sección 4.4. Para dar solución a este problema se introduce en el sistema de encriptación la técnica de modulación theta.

5.2.2 Etapa de modulación

Al utilizar la técnica de modulación theta introducida en la Sección 4.5, se modulan las imágenes codificadas con redes sinusoidales de amplitud, antes de aplicar la operación de multiplexado.

La modulación realizada por una red de amplitud puede ser interpretada como un proceso de discretización. Ya que la información encriptada es una distribución de *speckle*, se debe asegurar un mínimo de dos franjas por grano de *speckle* en la modulación de la imagen encriptada. Según el teorema de muestreo de Nyquist-Shannon [5.2], esta condición de discretización asegura que la información puede ser transmitida y recuperada a partir de la imagen modulada.

La aplicación de la técnica de modulación theta sobre las imágenes encriptadas antes del multiplexado, permite recuperar cada imagen codificada a partir de un proceso de filtrado de los órdenes difractados (ver Sección 5.2.4). También brinda la ventaja adicional de poder recuperar cada imagen sin la influencia de las imágenes restantes que aún se mantienen encriptadas.

La transmitancia de la red de amplitud sinusoidal $G_k(x_0, y_0; u_k, v_k)$ que modula la k -ésima imagen encriptada $E_k(x_0, y_0)$ es representada por la ecuación:

$$G_k(x_0, y_0; u_k, v_k) = \left\{ \frac{1}{2} + \frac{m}{2} \cos[2\pi(u_k x_0 + v_k y_0)] \right\} \text{rect} \left(\frac{x_0}{a} \right) \text{rect} \left(\frac{y_0}{b} \right) \quad (5.2)$$

donde m es la amplitud entre máximos sucesivos de la red, a , b , son las dimensiones que la limitan y (u_n, v_n) son sus frecuencias espaciales. La separación entre máximos de cada franja d_i satisface la relación $d_i \ll S_t$, donde S_t es el promedio transversal del tamaño de *speckle*, el cual es inversamente proporcional al tamaño de la pupila de salida del sistema.

De esta manera, la k -ésima imagen encriptada modulada E_{kM} , puede ser expresada como:

$$E_{kM}(x_0, y_0) = E_k(x_0, y_0)G_k(x_0, y_0; u_k, v_k) \quad (5.3)$$

La Figura 5.2 muestra una versión ampliada del proceso de modulación theta descrito por la Ecuación (5.3).

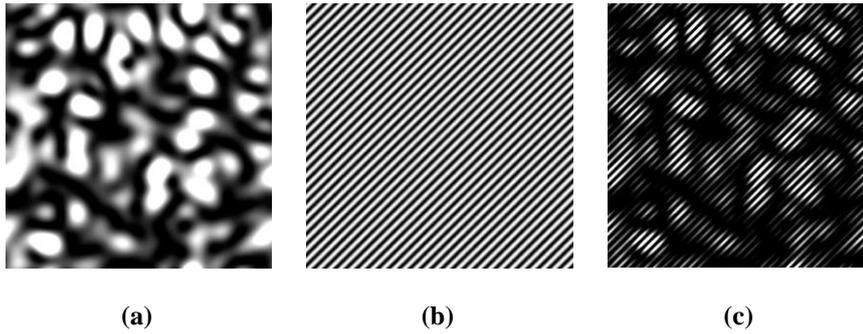


Figura 5.2: Versión ampliada de la modulación de una imagen encriptada. (a) imagen encriptada $E_k(x_0, y_0)$, (b) Red periódica de amplitud $G_k(x_0, y_0; u_k, v_k)$ y (c) imagen encriptada modulada $E_{kM}(x_0, y_0)$.

En síntesis, se codifica cada imagen de la película y posteriormente se modula mediante una red periódica de amplitud. A medida que se codifican las imágenes, van siendo moduladas por redes que tienen diferentes frecuencias espaciales y diferentes direcciones. Una vez realizado este proceso se procede con la operación de multiplexado de las imágenes encriptadas moduladas.

5.2.3 Etapa de multiplexado

Inmediatamente después de aplicar la modulación a cada imagen encriptada, se realiza un proceso de multiplexado y adicionalmente se efectúa una operación de conjugación de fase. Estas operaciones pueden ser expresadas como:

$$M^*(x_0, y_0) = \left[\sum_{k=1}^n E_k(x_0, y_0) G_k(x_0, y_0; u_k, v_k) \right]^* \quad (5.4)$$

Dado que el medio de registro es un detector plano, estas operaciones se realizan digitalmente. La operación de conjugación de fase, se efectúa cambiando el signo de la parte imaginaria del multiplexado.

En la Figura 5.3 (d) se muestra una versión amplificada del multiplexado de tres imágenes encriptadas moduladas. En las Figuras 5.3 (a), (b) y (c) cada distribución de *speckle* ha sido modulada por una red de amplitud de diferente orientación y diferente frecuencia espacial, respectivamente.

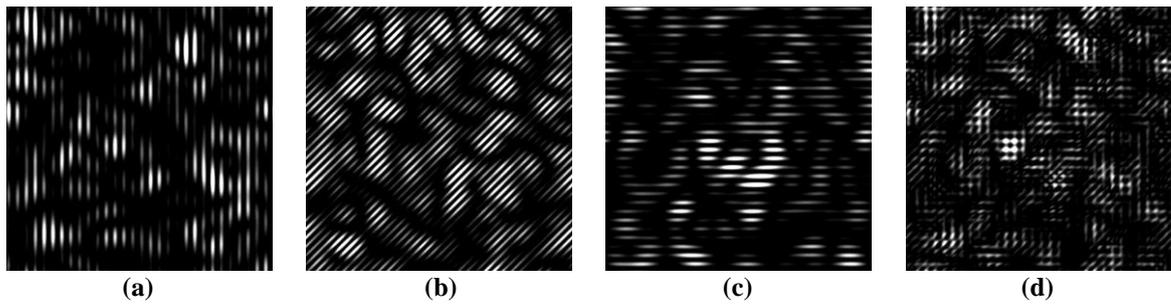


Figura 5.3: Multiplexado de imágenes encriptadas moduladas. (a), (b) y (c) son versiones amplificadas de tres imágenes encriptadas moduladas por diferentes redes de amplitud y (d) es la versión amplificada del multiplexado resultante de sumar (a) (b) y (c).

Finalmente, al usuario se le envía por medio de un canal de comunicación el multiplexado $M^*(x_0, y_0)$ y una copia de la llave o llaves de seguridad. El usuario podrá acceder a la información aplicando una etapa de sincronización, una etapa de filtrado secuencial y una etapa de desencriptación convencional $4f$.

En la implementación analógica, se pueden presentar dos estrategias para la modulación. La primera requiere usar redes físicas para modular el frente de onda antes de realizar un registro holográfico. Finalmente, los hologramas digitales pueden ser multiplexados. La segunda estrategia consiste en realizar los registros de cada imagen encriptada mediante holografía digital. A partir de estos hologramas se recupera la información compleja encriptada, se modula digitalmente y se procede con la operación de multiplexado. Esta última estrategia es la adoptada con SOV, donde se asume una recuperación completa del campo complejo de cada holograma digital de las imágenes encriptadas.

5.2.4 Etapa de sincronización y filtrado secuencial

Cuando el usuario ha recibido el multiplexado y la llave o llaves de seguridad, procede a la etapa de recuperación de la información. Haciendo referencia a la Figura 5.4, la etapa de

filtrado y sincronización consta de un procesador $4f$ donde la primera lente de distancia focal f realiza el espectro del multiplexado exhibiendo en el plano de Fourier parejas de órdenes difractados.

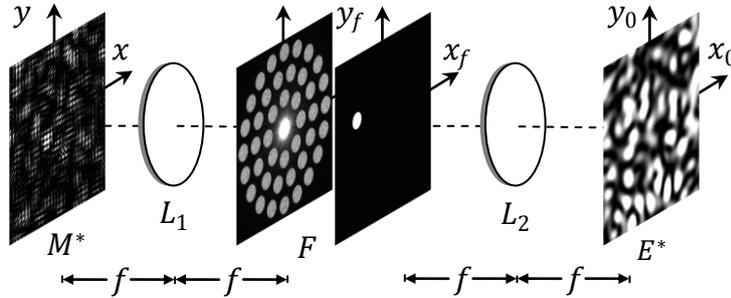


Figura 5.4: Etapa de filtrado y sincronización. Procesador $4f$ con ambas lentes de distancia focal f , M^* es el multiplexado, F es el plano de filtrado y E^* es el complejo de la imagen encriptada recuperada.

Como se analizó en la Sección 4.5, la transformada de Fourier de una imagen modulada con una red de amplitud sinusoidal descrita por la Ecuación (5.2) produce dos órdenes de difracción. La distancia que separa a cada orden difractado y el orden cero es $\lambda f(u_k^2 + v_k^2)^{1/2}$, donde, (u_k, v_k) son las frecuencias espaciales de la red, λ es la longitud de onda de la luz y f es la distancia focal de la lente.

Como se observa en la Figura 5.4, los órdenes producidos por las diferentes redes se encuentran separados entre sí y distribuidos sobre el plano de Fourier. En ese sentido, la información de las distintas imágenes encriptadas de la película ha sido separada y exceptuando al orden central, no hay presencia de solapamiento de información.

El espectro en el plano de filtrado puede ser expresado como:

$$\mathcal{F}[M^*(x, y)] = \sum_{k=1}^N \left\{ \frac{ab}{2} \text{sinc}(af_x) \text{sinc}(bf_y) + \frac{ab}{4} \left\{ \text{sinc}[a(f_x + u_k)] \text{sinc}[b(f_y + v_k)] \right. \right. \\ \left. \left. + \text{sinc}[a(f_x - u_k)] \text{sinc}[b(f_y - v_k)] \right\} \right\} \otimes \mathcal{F}[E_k^*(x, y)] \quad (5.5)$$

El proceso de filtrado consiste en dejar transmitir un orden de cada pareja de órdenes difractados. Este procedimiento se realiza mediante una máscara o una pupila representada por la Ecuación (3.40) que se ubica en el plano de filtrado F , como lo muestra

la Figura 5.4. Finalmente, el complejo conjugado de la imagen encriptada se obtiene al realizar una transformada de Fourier del campo transmitido.

El proceso de sincronización consiste en seleccionar la información del plano de filtrado en el orden cronológico correcto. La secuencia para escoger los órdenes difractados puede servir como llave de seguridad. Si esta secuencia no se aplica correctamente, las imágenes recuperadas en la etapa de desencriptación formarán una escena dinámica que no tiene un movimiento natural.

Volviendo a la Figura 5.4, las máscaras circulares dejan transmitir uno de los órdenes de difracción. Estos órdenes son representados por los últimos dos términos en la Ecuación (5.5).

Así, un orden filtrado puede ser descrito como:

$$S_k(x_f, y_f) = \frac{ab}{4} \{ \text{sinc}[a(f_x + u_k)] \text{sinc}[b(f_y + v_k)] \} \otimes \mathcal{F}[E_k^*(x, y)] \quad (5.6)$$

o con signos de resta en la función *sinc*. Al aplicar el teorema de convolución, la Ecuación (5.6) puede ser reescrita de la forma:

$$S_k(x_f, y_f) = \mathcal{F} \left(\left\{ \frac{1}{4} \exp[-i2\pi(u_k x + v_k y)] \text{rect} \left(\frac{x}{a} \right) \text{rect} \left(\frac{y}{b} \right) \right\} E_k^*(x, y) \right) \quad (5.7)$$

A partir de la Ecuación (5.6), la etapa de sincronización y filtrado está definida por la variable k que escoge los órdenes de una manera cronológica correcta para reconstruir la escena en movimiento.

Finalmente la lente L_2 realiza una última transformada de Fourier del orden transmitido para recuperar el complejo conjugado de la imagen encriptada, esto es:

$$\mathcal{F}\{S_f(x_f, y_f)\} = C(-x, -y) E_k^*(-x, -y) \quad (5.8)$$

donde $C(-x, -y)$ es la imagen invertida de:

$$C(x, y) = \frac{m}{4} \exp[-i2\pi(u_k x + v_k y)] \text{rect} \left(\frac{x}{a} \right) \text{rect} \left(\frac{y}{b} \right) \quad (5.9)$$

a esa imagen encriptada. Posteriormente, una segunda lente realiza una última transformada de Fourier y se produce el campo complejo $I_{r_k}(x_0, y_0)$. Este proceso es realizado para cada una de las imágenes encriptadas obtenidas del proceso de filtrado y sincronización.

El campo complejo de la imagen recuperada en el proceso de desencriptación puede ser escrito como:

$$I_{r_k}(x_0, y_0) = \mathcal{F}\left(\left\{\mathcal{F}\left[I_k(x, y)e^{i\varphi_o(x, y)}\right]\right\}^* e^{-i\varphi_{km}(u, v)}\right) \quad (5.10)$$

donde $e^{-i\varphi_{km}(u, v)} = e^{-i[\varphi_k(u, v) - \varphi_m(u, v)]}$. Se ha colocado en forma general el producto de la llave de desencriptación $e^{i\varphi_m(u, v)}$ con la llave de encriptación $e^{i\varphi_k(u, v)}$. Se puede notar que cada objeto recuperado es correctamente decodificado sólo si las llaves de encriptación y desencriptación son iguales. En caso contrario, la imagen decodificada se verá como otra imagen encriptada, ya que la Ecuación (5.10) tiene la misma forma que la Ecuación (5.1). Cuando la llave de seguridad no realiza la compensación de fase adecuada, es decir, cuando $\varphi_k(u, v) \neq \varphi_m(u, v)$, el objeto permanece encriptado.

Ahora, cuando se usa la llave de seguridad correcta en la Ecuación (5.10), la amplitud compleja del objeto decodificado es $I_{r_k}(x_0, y_0) = [I_k(x, y)e^{i\varphi_o(x, y)}]^*$. De esta forma se recupera el objeto original. La intensidad de cada objeto recuperado es:

$$I_{r_k}(x_0, y_0)I_{r_k}^*(x_0, y_0) = I_k^*(x, y)I_k(x, y) \quad (5.11)$$

De esta manera, todas las imágenes de la escena dinámica que fueron encriptadas, moduladas y multiplexadas, se recuperan de a una por vez en el orden cronológico correcto con la adecuada sincronización y haciendo uso de una única llave de seguridad.

Con esta última etapa finaliza la técnica de encriptación de eventos dinámicos. Este método representa una solución al problema de un único usuario con una sola llave de encriptación tratando de visualizar un conjunto de imágenes encriptadas. Sin la red externa que modula cada imagen encriptada y sin el subsecuente proceso de filtrado y sincronización, la visualización de cada imagen por separado sería infructuosa ya que para cada imagen desencriptada existiría la superposición de las imágenes restantes.

Adicionalmente, debe mencionarse que se reconstruye toda la secuencia con la misma calidad. Esto es demostrado en las aplicaciones expuestas en el Capítulo 6.

Esta técnica conlleva a la idea de que cada imagen recuperada puede ser asociada a un fenómeno que evoluciona en el tiempo. Desplegando consecutivamente las imágenes recuperadas en un orden secuencialmente correcto y sincronizado se logra reconstruir la película del fenómeno dinámico. En este sentido, por medio de esta técnica se desarrolla el primer concepto de una película encriptada por medios ópticos.

5.3 Consideraciones generales de implementación

Como se mostró en la sección anterior, la técnica propuesta consiste de cinco etapas: 1) etapa de encriptación, 2) etapa de modulación, 3) etapa de multiplexado, 4) etapa de sincronización y filtrado secuencial y 5) etapa de desencriptación.

Cada una de ellas se implementó como un SOV realizando las consideraciones que se exponen a continuación.

5.3.1 Extensión finita de las lentes en un SOV

En los SOV se consideran lentes delgadas que tienen un diámetro finito y constante. El tamaño de la pupila de la lente es asignada dependiendo de los parámetros del SOV, estos son: el muestreo de entrada, distancia focal y longitud de onda. Al incluir la pupila se limita las componentes del campo que la lente acepta. Esto se asemeja a colocar de forma analógica una pupila para eliminar contribuciones de luz espurias.

Como se está evaluando la técnica de encriptación propuesta y se compara con las técnicas convencionales, en los SOV el diámetro de la pupila de la lente es ajustada para todas las aplicaciones al valor constante de 1 cm. Así, las distribuciones incidentes en el plano de la lente que tengan un área de difracción por fuera de ese diámetro se verán limitadas.

De esta manera, por ejemplo, se permite comparar el sistema de encriptación $4f$ implementado con sólo transformadas rápidas de Fourier, implementado como un SOV

convencional o como un SOV utilizando redes de modulación. En la Figura 5.6 se muestra el resultado de esta comparación.

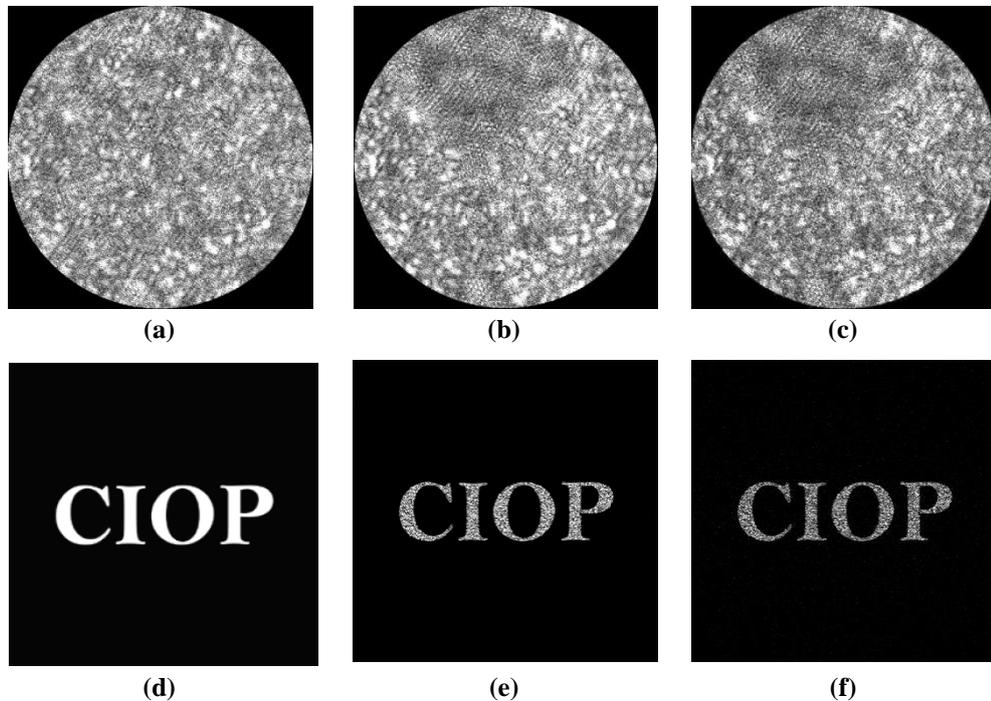


Figura 5.6: Imágenes encriptadas al emplear: (a) un sistema de encriptación implementado con transformadas rápida de Fourier, (b) un SOV de encriptación $4f$ y (c) un SOV de encriptación de eventos dinámicos. (d), (e) y (f) muestran las imágenes recuperadas a partir de las imágenes de (a), (b) y (c), respectivamente.

Las Figuras 5.6 (a), (b) y (c) muestran una porción aumentada de una imagen encriptada en los tres sistemas. Se ha colocado una abertura circular para tenerla de referencia y poder comparar puntos equidistantes en estas tres imágenes.

La Figura 5.6 (a) muestra la distribución resultante para una imagen encriptada usando únicamente transformadas rápidas de Fourier. A partir de este resultado se recupera el objeto original sin ruido mostrado en la Figura 5.6 (d). Este sistema considera que todo el campo difractado se vuelve a recuperar al final del proceso de encriptación. Esto es equivalente a tener lentes infinitas donde no existen pérdidas de frecuencias de ningún tipo. Por otro lado, las Figura 5.6 (b) y Figura 5.6 (c), obtenidas usando SOV, son ligeramente distintas, estas imágenes han sido ajustadas en contraste, ya que la red de difracción periódica limita el 50 % del campo. En los dos SOV se considera la extensión finita de las lentes. La diferencia es producida por el uso de las redes de modulación que hace que las

interferencias aleatorias produzcan distribuciones de *speckle* levemente diferentes. Las imágenes recuperadas a partir de estos sistemas son las imágenes de la Figura 5.6 (e) y Figura 5.6 (f). Note como esta última presenta más ruido *speckle*. Sin embargo, se mostrará que las imágenes recuperadas con el sistema propuesta tienen una calidad constante al multiplexar más de dos imágenes.

Otra consideración de suma importancia y que se debe analizar se vincula con las redes de modulación.

5.3.2 Escalamiento del objeto para su modulación

Una buena modulación por parte de las redes de amplitud hace que se transmita correctamente la información del objeto a los órdenes difractados. Esta consideración debe ser tomada en cuenta en la parte analógica como en la implementación con SOV. Una correcta modulación con redes de amplitud permite recuperar el objeto encriptado con mejor calidad. Por supuesto, siempre se tiene como referencia el ruido que es obtenido en la encriptación de una única imagen.

Para realizar una modulación adecuada en un SOV se debe hacer un escalamiento de la imagen que se va a modular. Por ejemplo, esto equivale a representar por ejemplo, un objeto encriptado de tamaño 5 mm en una matriz de 512×512 píxeles o en una matriz de 4096×4096 píxeles. Las dos matrices representan las mismas dimensiones físicas, pero después de su transmisión digital, la mejor imagen recuperada se obtendrá de la mejor modulación, en este caso de la matriz de 4096×4096 píxeles. Realizar el escalamiento adecuado permite producir una mejor modulación con las redes de amplitud.

Para aplicar este procedimiento, se debe asegurar que las distribuciones escaladas brindan la información física correcta. Esto se puede comprobar analizando el diámetro del disco de Airy $d = 1.22\lambda f/R$ que forma la difracción de una apertura circular de diámetro $2R$ donde λ es la longitud de onda de la luz y f es la distancia focal de la lente.

Para hacer esto, en un SOV se obtienen los patrones de difracción de una apertura usando tres lentes de diferente distancia focal, $f=100$ mm, $f=150$ mm y $f=200$ mm. La apertura tienen un radio de ~ 0.3 mm y es iluminada con una longitud de onda de 632.8

nm. La difracción es obtenida en una matriz de 512×512 píxeles y la distribución escalada en una matriz de 4096×4096 píxeles. Los resultados se muestran en la Figura 5.7.

El contraste de las imágenes ha sido aumentado para realizar la medición del disco de Airy en píxeles en cada caso. La primera fila muestra las distribuciones obtenidas en matrices de tamaño 512×512 píxeles. La segunda fila muestra las distribuciones obtenidas en matrices de tamaño 4096×4096 píxeles. Note el escalamiento al usar cada lente de diferente distancia focal. Note también que para las dos filas los patrones correspondientes a la misma distancia focal son los mismos.

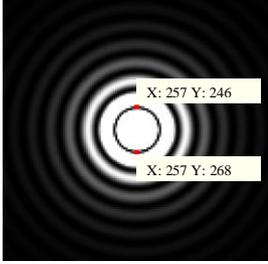
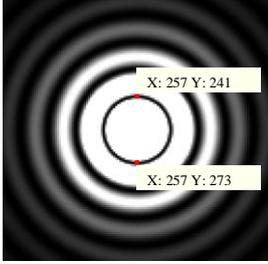
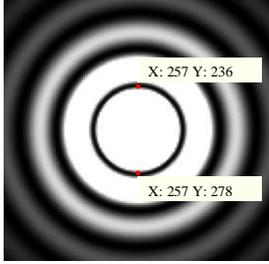
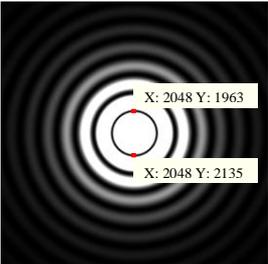
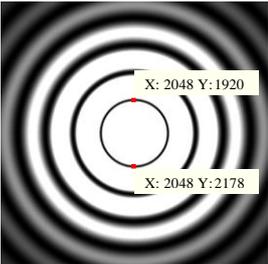
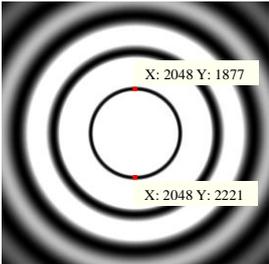
| $\lambda=632.8 \text{ nm}, s_{in}=12 \mu\text{m}, R=0.3 \text{ mm}, \text{ tamaño de imágenes } 512 \times 512$ | | |
|---|---|---|
| $f=100 \text{ mm}$ | $f=150 \text{ mm}$ | $f=200 \text{ mm}$ |
|  |  |  |
| $d=0.2573 \text{ mm}$ Valor Teórico: 21.4449 píxeles Medición: 22 píxeles. | $d=0.3860 \text{ mm}$ Valor Teórico: 32.1673 píxeles Medición: 32 píxeles. | $d=0.5147 \text{ mm}$ Valor Teórico: 42.8898 píxeles Medición: 42 píxeles. |
| $\lambda=632.8 \text{ nm}, s_{in}=12 \mu\text{m}, R=0.3 \text{ mm}, \text{ tamaño de imágenes } 4096 \times 4096$ | | |
| $f=100 \text{ mm}$ | $f=150 \text{ mm}$ | $f=200 \text{ mm}$ |
|  |  |  |
| $d=0.2573 \text{ mm}$ Valor Teórico: 171.5591 píxeles Medición: 172 píxeles. | $d=0.3860 \text{ mm}$ Valor Teórico: 257.3387 píxeles Medición: 258 píxeles. | $d=0.5147 \text{ mm}$ Valor Teórico: 343.1182 píxeles Medición: 344 píxeles. |

Figura 5.7: Difracción de una abertura circular. Las distribuciones de la primera fila son representadas en una matriz de 512×512 píxeles. Las distribuciones de la segunda fila son representadas en una matriz de 4096×4096 píxeles. s_{in} es el muestreo de entrada, λ es la longitud de onda

La medición ha sido realizada ubicando los píxeles sobre la imagen que definen el diámetro del disco de Airy y han sido comparados con el valor teórico que también es

representado en píxeles, como lo muestra la Figura 5.7. Con esta experiencia se comprueba que se puede producir la distribución escalada que representa la misma información física.

De esta forma, se puede proceder con la etapa de modulación. Por ejemplo, un grano de *speckle* que se representa por 4 píxeles en una matriz de 512×512 ahora es representado por 32 píxeles en una matriz de 4096×4096 como lo muestra la Figura 5.8.

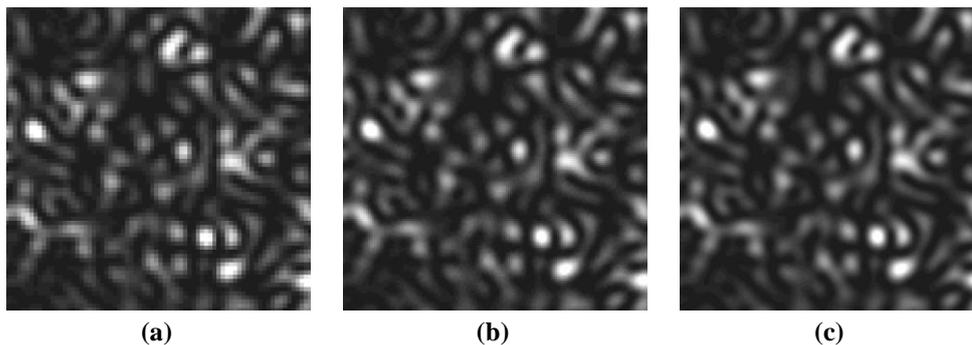


Figura 5.8: Distribuciones de *speckle* en una matriz de: (a) 512×512 píxeles, (b) 2048×2048 píxeles y (c) 4096×4096 píxeles.

Note el pixelado de los granos de *speckle* a medida que la matriz se hace más pequeña. Cabe enfatizar que no se debe confundir este proceso con una mejora de la imagen. En una experiencia analógica, el detector digitaliza la señal óptica y se realiza un proceso de cuantización y no se puede obtener más información que la colectada. No obstante, es válido asegurar que el proceso de modulación digital se puede hacer correctamente para los datos ya registrados, que es lo que se está discutiendo en este punto.

El procedimiento anterior es importante para que el usuario final pueda recuperar la información original con la mejor calidad posible. Se debe enfatizar que la reconstrucción analógica está restringida por la resolución del medio que despliega la información. Esto implica contar con un dispositivo de alta resolución para desplegar el multiplexado de información encriptada, lo cual impone un límite a la aplicación. Sin embargo, sería factible usar un sistema híbrido para la reconstrucción de la información. Se puede realizar la etapa de filtrado y sincronización en forma digital y desplegar en un SLM la información encriptada recuperada de esta etapa para proceder con un proceso de desencriptación convencional. Al realizar este procedimiento se dispone de la capacidad de modular adecuadamente la información en forma digital.

5.3.3 Optimización de las redes de modulación

La etapa de modulación consiste en introducir una red periódica de amplitud sinusoidal que module las imágenes encriptadas. El campo complejo a la distancia z puede ser escrito como:

$$U(x, y) = \frac{e^{jkz}}{j\lambda z} e^{j\frac{k}{2z}(x^2+y^2)} \left\{ \frac{ab}{2} \text{sinc}(af_x) \text{sinc}(bf_y) \right. \\ \left. + \frac{ab}{4} \left\{ \text{sinc}[a(f_x + u_k)] \text{sinc}[b(f_y + v_k)] + \text{sinc}[a(f_x - u_k)] \text{sinc}[b(f_y - v_k)] \right\} \right\} \quad (5.12)$$

Al tratarse de una red de amplitud sinusoidal, que puede ser producida por un patrón de interferencia de bajo contraste, su transmitancia varía suavemente y producen sólo un par de órdenes difractados, uno a cada lado del orden central. Esto se observa en los tres términos de la Ecuación (5.12). Ya que la transmitancia varía entre 0 y 1, el valor 1/2 en la Ecuación (5.2) asegura que no existan transmitancias negativas. Este valor define la eficiencia de difracción del orden central que es del 25% de la energía incidente mientras que la de los órdenes difractados es del 6.5%. El resto de la energía es absorbida por la red.

Al realizar una modulación en forma digital se debe asegurar la buena modulación del objeto encriptado, como se explicó en la sección anterior. En un SOV la modulación depende del número de valores de amplitud que se tenga por franja. Al tener más valores mejor será la modulación. Consecuentemente, se recupera mejor la información en el proceso de descryptación.

Una red de amplitud optimizada tiene un número mayor de valores por franja que modula el mismo grano de *speckle*. Esto se puede ver en los resultados de la Figura 5.9. En ella se muestra la modulación de una imagen encriptada representada en una matriz de 4096×4096 píxeles y 8192×8192 píxeles, respectivamente. La frecuencia de la red es la misma en ambos casos, pero al tener la representación del objeto en frecuencias en una matriz más grande, el número de píxeles por franja será mayor. Así, el número de píxeles

por franja en la matriz de 8192×8192 pixeles duplica al de la matriz de 4096×4096 . Esto produce una mejor modulación de los granos de *speckle* como se observa en la Figura 5.9 (b) en comparación a la Figura 5.9 (a).

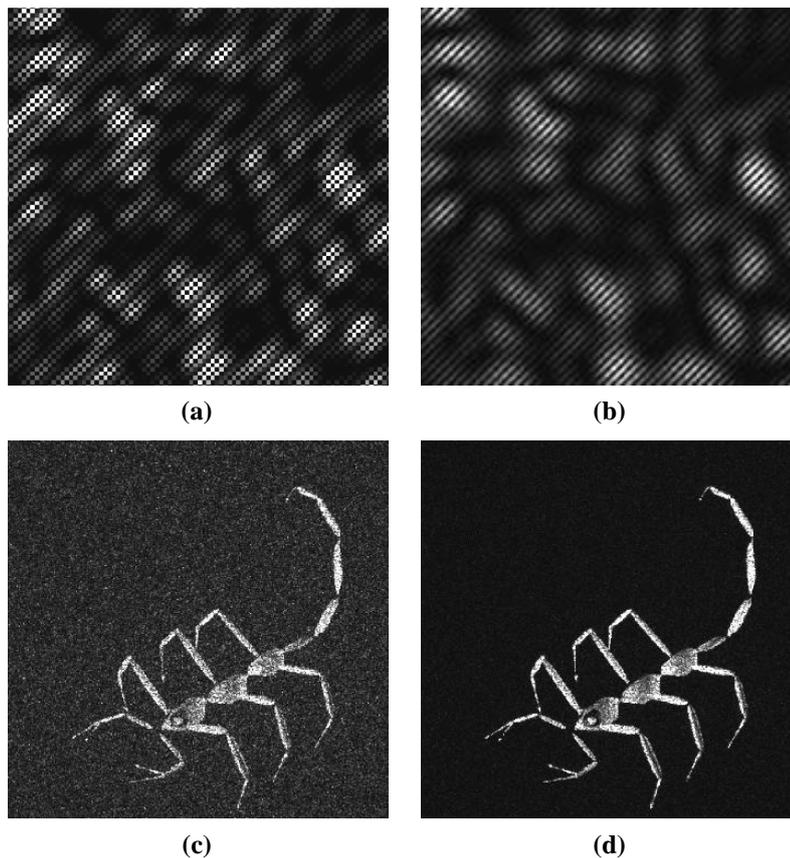


Figura 5.9: Recuperación de información de una imagen encriptada representada en diferentes tamaños de matriz. Imagen encriptada modulada en una matriz de: (a) 4096×4096 , (b) 8192×8192 . (c) y (d) imágenes recuperadas de (a) y (b), respectivamente.

En la Figura 5.9 (c) se puede observar que el objeto recuperado tiene más ruido *speckle* que el de la Figura 5.9 (d). Una modulación con franjas bien definidas, como la Figura 5.9 (b), direcciona correctamente la información hacia los órdenes difractados sin dispersarse en el resto del plano de frecuencias. En cambio, al no ser uniforme la modulación como en la Figura 5.9 (a), la información en el plano de filtrado se dispersará en mayor medida fuera de los órdenes de difracción. Por lo tanto, al filtrar un orden y al recuperar la información, las frecuencias que no fueron direccionadas correctamente adicionarán ruido *speckle* en el proceso de reconstrucción de la imagen.

En los SOV, las frecuencias de las redes con las cuales se trabajan resultan restringidas por los parámetros ópticos del sistema según la relación $d = \lambda f(u_k^2 + v_k^2)^{1/2}$, donde d es la distancia entre el orden difractado y el orden central, (u_k, v_k) son las frecuencias espaciales de la red, λ es la longitud de onda de la luz y f es la distancia focal de la lente. Al ajustar el área del plano de filtrado, en la etapa de sincronización y filtrado secuencial se encuentra que existe una relación entre los parámetros ópticos del sistema y el número de líneas por milímetro de las redes. Los valores encontrados deben tenerse en cuenta en el caso de una implementación experimental. Así, una determinada separación de un orden difractado del orden central, se obtiene a partir de una combinación dada de valores del muestreo de entrada (tamaño finito del display), de la distancia focal de las lentes y de la longitud de onda de iluminación, los cuales definen el número de líneas/mm de cada red de amplitud sinusoidal.

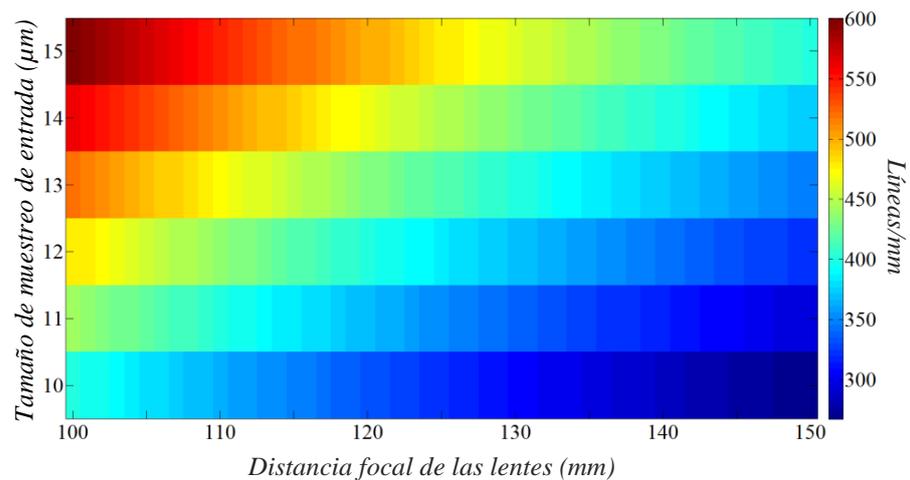


Figura 5.10: Relación entre parámetros ópticos del sistema y número de líneas por milímetros de la red.

Así, por ejemplo, la gráfica en la Figura 5.10 muestra que si el orden difractado más alejado se encuentra a ~ 38 mm, para un muestreo de entrada de ~ 15 μm , lentes de 100 mm y una longitud de onda de 632.8 nm, el número de líneas/mm de la red es 600. Ahora, si se cambia la distancia focal a 150 mm y se conservan los otros parámetros ópticos, se requerirá una red de difracción de 400 líneas/mm para que el orden difractado más alejado se encuentre a la misma distancia de ~ 38 mm. Consecuentemente, para difractar a distancias más cercanas se necesitarán redes con menor número de líneas/mm. Estos

aspectos considerados permiten tener una visión integral de los elementos necesarios para una implementación ya sea analógica o en SOV.

5.4 Comentarios sobre la seguridad del sistema

No existe una técnica de encriptación que provea una seguridad absoluta en la protección de datos. Evidentemente este es un tema que podría abordarse y desarrollarse exhaustivamente para encontrar las condiciones bajo las cuales la aplicación de la técnica de encriptación de eventos dinámicos no brinda el grado de seguridad adecuado. Sin embargo, al ser una técnica nueva de encriptación, no existe en la literatura un procedimiento o un protocolo para atacarla.

Cabe comentar algunos aspectos generales de la seguridad. La técnica de encriptación de eventos dinámicos se sustenta en los procesos de multiplexado que hace que los sistemas convencionales de encriptación sean más resistentes ante diversos ataques del criptoanálisis. No obstante, el grado de seguridad en la técnica propuesta, bajo ciertas condiciones, podría no ser mayor a la seguridad obtenida en un sistema convencional *4f*.

Esto es debido al re-direccionamiento que permite codificar un mayor volumen de información hace que la etapa de decodificación se comporte como múltiples sistemas *4f*. A partir de cada orden difractado se recupera una imagen con la llave de seguridad correcta. En este sentido, la seguridad no se incrementa y aquí es donde el sistema podría ser vulnerado como un sistema de encriptación convencional. Sin embargo, como se mencionó, se necesitaría otro protocolo, ya que se debe acceder a la etapa interna del sistema de decodificación y además acceder a la etapa de sincronización y filtrado secuencial.

Se ha señalado que la secuencia para seleccionar cada orden de difracción también actúa como parámetro de seguridad. Por lo tanto, el usuario no autorizado debería hacer un barrido completo sobre el plano de filtrado para poder aplicar cada ataque convencional. Sin mencionar que esta etapa de filtrado es otro sistema óptico que puede presentar variantes como por ejemplo, un parámetro que introduzca una magnificación de los ordenes difractados en el plano de Fourier. En este sentido, la técnica propuesta es más

segura al hacer que los ataques del criptoanálisis no puedan funcionar adecuadamente. Se necesitaría otra estrategia para tratar de dilucidar si existe alguna manera que permita efectivizar estos ataques convencionales sobre la técnica de encriptación de eventos dinámicos.

Dentro de las consideraciones realizadas, también se encuentran los tamaños de las llaves de codificación. Ya que se necesitan que las llaves de seguridad sean de tamaños grandes, la seguridad del sistema es resistente ante algunos ataques convencionales, por ejemplo ante una búsqueda exhaustiva de la llave de codificación o un ataque de fuerza bruta.

Desde el punto de vista del criptoanálisis, se estima que el tiempo para encontrar una llave de seguridad que tienen una dimensión de $\sim 10^{30}$ (posibles combinaciones), realizando un ataque de fuerza bruta, está en el orden de 1.6×10^{10} años. Esto es realizando un millón de procesos de encriptación por microsegundo en un sistema DES (Data Encryption Standar) de 56 bits [5.3]. Por lo tanto, al considerar ese tiempo de ejecución, un ataque que realice una búsqueda exhaustiva de la llave de seguridad no es una opción válida para vulnerar el sistema de encriptación propuesto. Esto resulta al considerar que si la llave de encriptación es, por ejemplo, de tamaño 512×512 pixeles de 8 bits, esto equivale a tener una llave de seguridad de tamaño $2^{8 \times 512 \times 512}$. Al aplicar un ataque de búsqueda exhaustiva, el tiempo de ejecución sería incalculable, para encontrar la combinación correcta de fases que permita decodificar una secuencia dinámica.

Adicionalmente se considera que se usan llaves de seguridad descartables. Entonces a cada usuario se le puede asignar una llave de seguridad que le permite recuperar una única escena dinámica. Si el usuario requiere más información, se le vuelve a enviar dicha información codificada con otra llave de encriptación. De esta forma, si se intercepta alguna llave de codificación, esa llave no servirá para recuperar otra información codificada con el mismo sistema de seguridad.

5.3 Bibliografía

- [5.1] A. Alfalou, A. Mansour, “All-optical video-image encryption with enforced security level using independent component analysis,” *J. Opt. A. Pure Appl. Opt.* 9, 787–796 (2007).
- [5.2] B. Jähne, *Digital image processing*, Springer-Verlag Berlin Heidelberg 2005, pp. 243-255.
- [5.3] D. E. R. Denning, *Cryptography and data security*, Addison-Wesley, (1983).

Capítulo 6

Encriptación de eventos dinámicos: Aplicaciones

6.1 Introducción

La técnica de encriptación de eventos dinámicos implementada en el Capítulo 5 brinda la posibilidad de encriptar ópticamente diferentes tipos de señales. Por medio de esta técnica se pueden transmitir eficientemente grandes volúmenes de información como videos, varias secuencias de texto, textos dinámicos, señales compuestas de imágenes y sonido, etc., representando un avance significativo en esta línea de investigación.

De forma general, se debe tener presente la calidad de recuperación de las señales encriptadas por métodos ópticos. En el procesado óptico coherente de información siempre se va a tener la presencia del ruido de *speckle*, por lo tanto, la recuperación de las señales no va a tener un cien por ciento de fidelidad. A menos que las señales se vean reducidas desde un principio a un flujo de bits, donde se pueden realizar procesos de detección y compensación de errores en la transmisión, eliminación de ruidos, etc., las imágenes recuperadas no son fieles reproducciones de los objetos originales.

Es claro que la aplicación final de un sistema justifica su implementación, por lo tanto, si se requiere transmitir imágenes o sonidos en alta definición de manera segura, lo más probable es que las técnicas de encriptación óptica y en general el procesado óptico coherente no sean los procedimientos más adecuados para esta tarea. Por el contrario, si con la recuperación de datos de calidad aceptable, por ejemplo códigos, textos, etc., se

consigue obtener una información relevante, es muy probable que la encriptación óptica y el procesado óptico coherente suplan eficientemente las necesidades requeridas. Por ejemplo, un sistema de correlación óptica permite identificar patrones de una escena, sin embargo esta técnica no brinda detalles de la escena misma, no obstante se ha aplicado en procesos industriales y hasta en aplicaciones militares.

En este sentido, las técnicas de seguridad óptica pueden ser aplicadas donde el ruido inherente de *speckle* sea permisible. Por ejemplo, en la transmisión de un breve mensaje de sonido que defina una instrucción específica o códigos que permitan acceder a información más delicada. En otro ejemplo, la conjunción de las técnicas de encriptación con el procesamiento de patrones biométricos hace que aquellas resulten más relevantes para realizar procesos de verificación de identidad, control de acceso, etc.

Bajo estos lineamientos, la información que se manipula en las aplicaciones siguientes ya no son elementos estáticos (imagen o textos únicos). En este caso, la información manipulada de relevancia son secuencias dinámicas compuestas de un conjunto de imágenes que constituyen una o varias escenas en movimiento. Cada escena representa un mensaje importante para un usuario en particular el cual requiere que su transmisión por un canal digital mantenga su grado de confidencialidad.

Este capítulo presenta tres aplicaciones específicas de la técnica de encriptación de eventos dinámicos. Cada una de estas aplicaciones permite resguardar, transmitir y recuperar mayor volumen de información que las técnicas actuales de encriptación. La Sección 6.2 presenta la aplicación de encriptación de eventos dinámicos de secuencias monocromáticas. La Sección 6.3 detalla la aplicación de esta técnica en secuencias policromáticas y por último la Sección 6.4 muestra su aplicación en procesos multiusuario.

6.2 Encriptación de escenas dinámicas monocromáticas

En esta sección se presenta la encriptación de una secuencia de imágenes monocromáticas que representan un evento dinámico que evoluciona a través del tiempo. Cada imagen de la escena contiene información de 8 bits por pixel y cada una tiene 512×512 pixeles. Los

cinco procesos que componen la técnica de encriptación de eventos dinámicos fueron implementados en un SOV.

6.2.1 Descripción general

En esta sección se introduce el concepto de encriptar ópticamente un evento dinámico. La película se compone de varios marcos codificados correspondientes a una situación que evoluciona en el tiempo representando una escena en movimiento. Cada una de las imágenes que componen la escena ha sido codificada en el sistema de encriptación en configuración *4f*. Todos los cuadros se codificaron con una única máscara de fase que actúa como llave única de seguridad. Convencionalmente por medio de la operación de multiplexado se puede almacenar la información de la película en un único elemento para su transmisión. Como se analizó en el Capítulo 4, la recuperación de la información a partir de este multiplexado implica la existencia de solapamiento de información de dos tipos. 1) La existencia de superposición de imágenes correctamente decodificadas al usar una única llave de encriptación, hecho descrito por la Ecuación (4.12). 2) La existencia de superposición de una imagen correctamente decodificada con ruido de imágenes incorrectamente recuperadas, hecho descrito por la Ecuación (4.17). En este sentido, si no se realiza un pre-procesado a los marcos encriptados antes de realizar el proceso de multiplexado, las imágenes recuperadas estarán degradadas en calidad por la superposición de información.

Teniendo en cuenta estas consideraciones, se aplica la técnica de modulación theta presentada en la Sección 4.5 antes de realizar el multiplexado. De esta forma, cada imagen encriptada es modulada con redes periódicas de amplitud las cuales son descritas por la Ecuación (4.20). Posteriormente estas imágenes encriptadas theta moduladas son multiplexadas por medios digitales. Al usuario final se le transmite la única llave de encriptación y el paquete multiplexado. Finalmente, en la etapa de recuperación, una etapa apropiada de sincronización y filtrado secuencial realizada sobre el espectro del multiplexado logra obtener las imágenes encriptadas sin la influencia de la modulación. De esta forma se recuperan correctamente los marcos de la película en su posición original

después de un proceso convencional de decodificación. La escena de movimiento original es recuperada únicamente cuando el usuario posee la llave de seguridad correcta.

6.2.2 Descripción del método

Se ha seleccionado como protocolo de encriptación al sistema de codificación de doble máscara de fase en configuración $4f$. Haciendo referencia a la Figura 6.1, inicialmente, la imagen $O_1(x, y)$ es multiplicada por una primera máscara de fase $e^{i\varphi_0(x, y)}$, posteriormente la lente L_1 de distancia focal f realiza una primera transformada de Fourier, el espectro resultante es multiplicado por una segunda máscara de fase $e^{i\varphi_1(x_f, y_f)}$ y finalmente la lente L_2 realiza una nueva transformada de Fourier para obtener el objeto encriptado $E_1(x_0, y_0)$. Este procedimiento es realizado para todas las imágenes que componen la secuencia en movimiento.

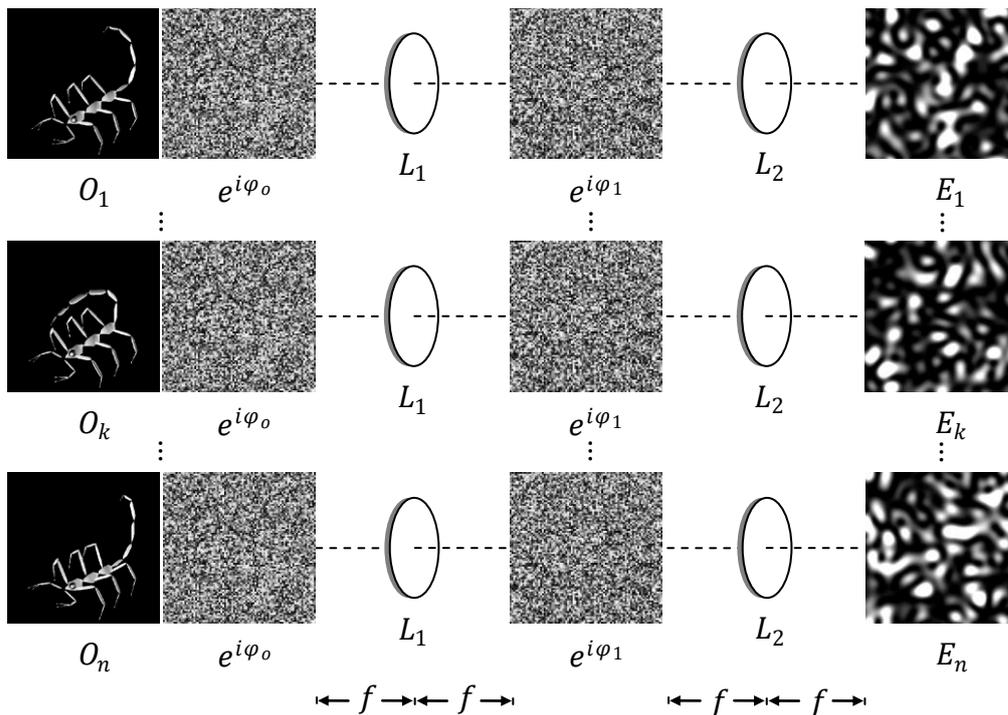


Figura 6.1: Encriptación de una secuencia dinámica monocromática compuesta de n imágenes. O_k es la k -ésima imagen de la escena en movimiento, $e^{i\varphi_0}$ es la primera máscara de fase, L_1 y L_2 son lentes de distancia focal f , $e^{i\varphi_1}$ es la segunda máscara de fase y E_k es la k -ésima imagen encriptada.

Como se describió en el Capítulo 2, cada una de las imágenes encriptadas es representada matemáticamente por la Ecuación (2.1):

$$E_k(x_0, y_0) = \{O_k(-x, -y) \exp[i\varphi_0(-x, -y)]\} \otimes \mathcal{F}\{\exp[i\varphi_1(x_f, y_f)]\} \quad (6.1)$$

donde \otimes denota la operación de convolución, los signos negativos indican la inversión de coordenadas de la función correspondiente y \mathcal{F} es la operación de transformada de Fourier. Luego del proceso de encriptación, a las imágenes codificadas se les aplica la técnica de modulación theta. Posteriormente son multiplexadas y finalmente se realiza una operación de conjugación de fase.

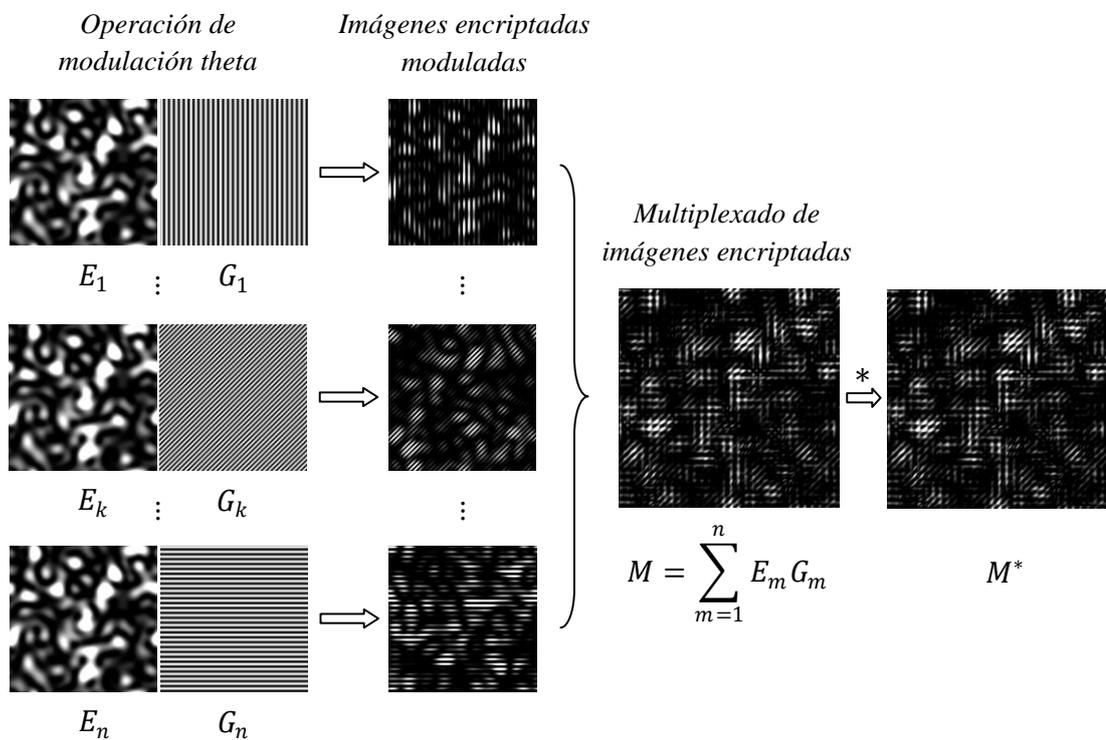


Figura 6.2: Técnica de modulación theta, técnica de multiplexado y operación de conjugación de fase. E_k representa la k -ésima imagen encriptada, G_k es la red sinusoidal de amplitud, M es el multiplexado de imágenes encriptadas moduladas, $*$ representa la operación de conjugación de fase y M^* es la fase conjugada de M .

Haciendo referencia a la Figura 6.2, la primera imagen codificada $E_1(x_0, y_0)$ es multiplicada por una red sinusoidal de amplitud $G_1(x_0, y_0; u_1, v_1)$ de frecuencias espaciales (u_1, v_1) . Este procedimiento es realizado para todas las imágenes encriptadas de la secuencia dinámica y el resultado son imágenes encriptadas moduladas como lo muestra la tercera columna de la Figura 6.2. Se puede notar mediante una ampliación de estas imágenes que la estructura de los granos de *speckle* está modulada como mínimo con dos franjas por grano de *speckle* para que la información pueda ser transmitida y recuperada

correctamente. Finalmente, todas las imágenes encriptadas moduladas son multiplexadas digitalmente para luego aplicar una operación de conjugación de fase.

Este conjunto de operaciones puede ser expresado como:

$$M^*(x_0, y_0) = \left[\sum_{k=1}^n E_k(x_0, y_0) G_k(x_0, y_0; u_k, v_k) \right]^* \quad (6.2)$$

donde $M(x_0, y_0)$ es el multiplexado de las imágenes encriptadas $E_k(x_0, y_0)$ que son moduladas con las redes periódicas de amplitud $G_k(x_0, y_0; u_k, v_k)$. De esta manera, al usuario final se le envía por medio de un canal de comunicación digital el multiplexado, $M^*(x_0, y_0)$ y la llave de seguridad $e^{i\varphi_1(x_f, y_f)}$.

Cabe aclarar que el registro de los patrones encriptados pueden realizarse mediante holografía digital [6.2] (ver Apéndice A). A la información recuperada de los hologramas digitales se le aplica una modulación theta para luego proceder con la operación de multiplexado. Siempre teniendo presente que las redes periódicas de modulación deben de tener varios valores de amplitud por franja y que debe haber en promedio por lo menos dos franjas que modulen el grano de *speckle*.

Volviendo a la aplicación con el SOV, la técnica de multiplexado brinda la ventaja de poder transmitir múltiples imágenes encriptadas de la escena dinámica en un único patrón complejo. Por otro lado, la aplicación de la técnica de modulación theta sobre las imágenes encriptadas antes de aplicar la técnica de multiplexado brinda la ventaja adicional de poder separar el espectro de la información modulada en un plano de filtrado.

De esta manera, el proceso de recuperación de la información consiste de dos etapas fundamentales: 1) recuperar la información sin modulación de cada imagen encriptada teniendo en cuenta el orden de encriptación y 2) realizar el proceso de decodificación de las imágenes de la escena dinámica que ya deberá estar sincronizada en un orden cronológico correcto. Esto con el fin de poder recuperar la película en su orden natural.

La primera etapa se muestra en la Figura 6.3. Este esquema representa la etapa de filtrado y sincronización. Aquí se recupera la información encriptada sin modulación seleccionando adecuadamente la información separada en el plano de filtrado.

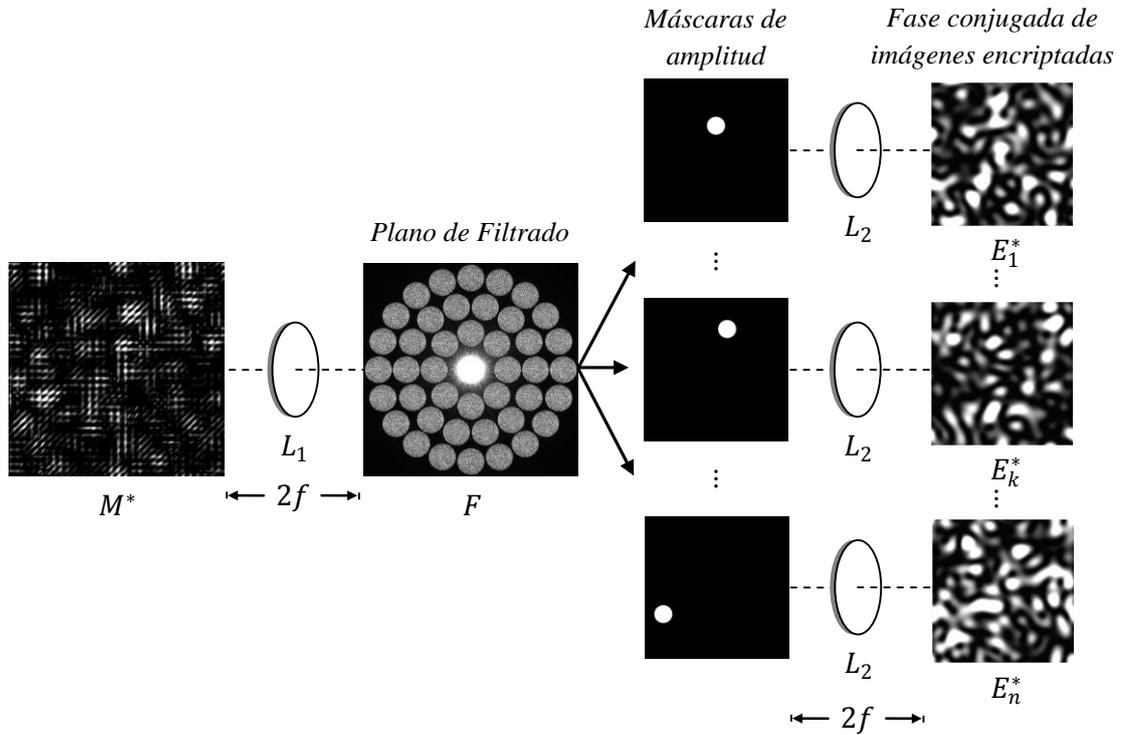


Figura 6.3: Proceso de filtrado secuencial para recuperar la información encriptada sin modulación. M^* es el multiplexado enviado al usuario, L_1 y L_2 son lentes de distancia focal f , F es el plano de filtrado, E_k^* , es el campo complejo de la imagen encriptada a la cual se le debe realizar un proceso de inversión.

Inicialmente el usuario introduce el multiplexado en un procesador $4f$, la primera lente L_1 realiza una transformada de Fourier separando la información encriptada en el plano de filtrado. Dependiendo de las frecuencias espaciales y la orientación de las redes periódicas de modulación, los órdenes difractados tendrán una posición espacial sin solapamiento en este plano.

En el caso de la Figura 6.3, los órdenes difractados están distribuidos sobre líneas circulares. En este caso, una red de franjas con orientación inicial vertical se hace rotar diferentes ángulos de tal manera que los órdenes no se solapen. Para generar órdenes difractados sobre otra circunferencia de mayor radio, se aumenta convenientemente la frecuencia de la red y se procede a rotarla. El proceso se repite hasta modular todos los marcos encriptados de la escena en movimiento. Para la reconstrucción de la escena

dinámica se debe mantener este orden para conservar la secuencia cronológica que permitirá ver en orden natural la escena en movimiento. Por otro lado, para optimizar el área disponible en el plano de filtrado, se pueden variar las orientaciones de las redes de amplitud y se pueden variar sus frecuencias espaciales. Estos parámetros se ajustan para maximizar el número de órdenes difractados que pueden confinarse en una área determinada del plano de filtrado.

Matemáticamente, el espectro en el plano de filtrado puede ser expresado por la Ecuación (5.5):

$$\mathcal{F}[M^*(x, y)] = \sum_{k=1}^N \left\{ \frac{ab}{2} \text{sinc}(af_x) \text{sinc}(bf_y) + \frac{ab}{4} \left\{ \text{sinc}[a(f_x + u_k)] \text{sinc}[b(f_y + v_k)] \right. \right. \\ \left. \left. + \text{sinc}[a(f_x - u_k)] \text{sinc}[b(f_y - v_k)] \right\} \right\} \otimes \mathcal{F}[E_k^*(x, y)] \quad (6.3)$$

La etapa de filtrado espacial se realiza utilizando máscaras de amplitud circulares esquematizadas en la tercera columna de la Figura 6.3. Cada orden filtrado es representado por la Ecuación (5.6). El proceso de sincronización permite seleccionar la información en el orden cronológico correcto para recuperar en la etapa de descryptación la escena dinámica original. De esta manera, todo el proceso de reconstrucción que experimenta el usuario es en tiempo real.

La segunda etapa del proceso de recuperación consiste de un sistema de descryptación convencional en configuración $4f$. Haciendo referencia a la Figura 6.4, el complejo conjugado de una imagen encriptada sin modulación se ubica en la entrada de un procesador $4f$. La lente L_1 de distancia focal f genera el espectro que es multiplicado por la llave de seguridad $e^{i\varphi_1(u,v)}$. Por último, la lente L_2 de distancia focal f realiza una nueva transformada para encontrar en el plano de salida el campo complejo de la imagen recuperada $O_{rk}(x_0, y_0)$. Este proceso es realizado para cada una de las imágenes encriptadas sin modulación obtenidas a partir del proceso de filtrado.

El campo complejo de la imagen decodificada en el proceso de descryptación está descrito por la Ecuación (5.10):

$$O_{r_k}(x_0, y_0) = \mathcal{F}(\{\mathcal{F}[O_k(x, y)e^{i\varphi_o(x, y)}]\}^* e^{-i\varphi_{km}(u, v)}) \quad (6.4)$$

Al usar la llave de seguridad correcta, la amplitud compleja del objeto decodificado es $O_{r_k}(x_0, y_0) = [O_k(x, y)e^{i\varphi_o(x, y)}]^*$ y la intensidad está dada por:

$$O_{r_k}(x_0, y_0)O_{r_k}^*(x_0, y_0) = O_k^*(x, y)O_k(x, y) \quad (6.5)$$

De esta forma se descriptan las imágenes de la secuencia dinámica de a una por vez en el orden cronológico correcto con la adecuada sincronización y haciendo uso de una única llave de seguridad.

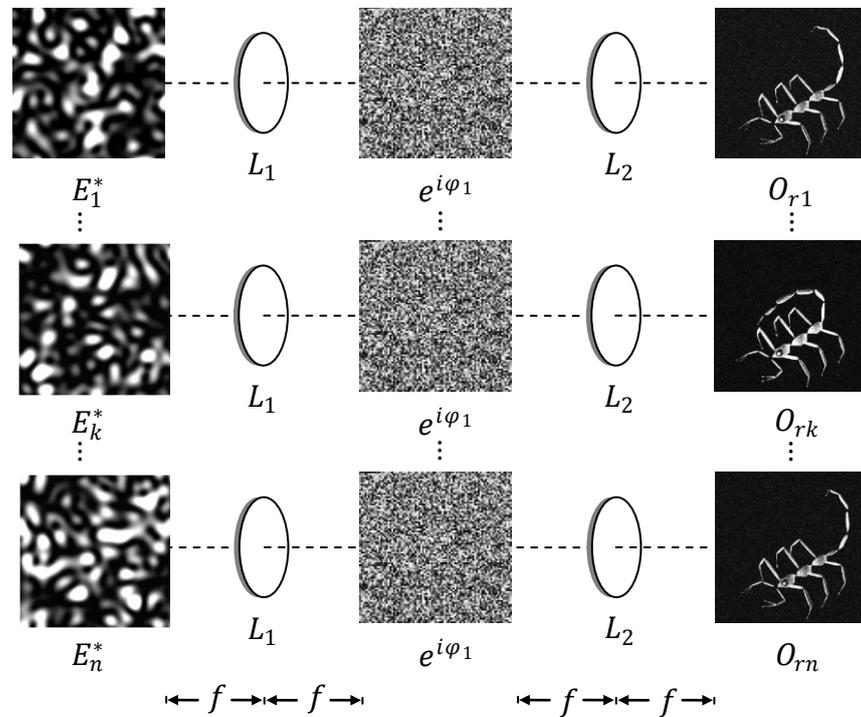


Figura 6.4: Etapa de recuperación de la información. Se emplea un procesador $4f$ cuyas dos lentes L_1 y L_2 tienen distancia focal f . En el plano de Fourier de la lente L_1 se encuentra la llave de seguridad $e^{i\varphi_1}$ y en el plano de Fourier de la lente L_2 se recupera el objeto O_{rk} el cual es registrado en intensidad.

Se demuestra así que el método desarrollado constituye una solución al problema de visualizar un conjunto de imágenes encriptadas mediante el empleo de una única llave de seguridad a partir de un multiplexado. Sin el uso de las redes de amplitud que modulan las imágenes encriptadas y sin el subsecuente proceso de filtrado, la visualización de cada marco estaría degradada. Adicionalmente, esta técnica permite reconstruir cada imagen codificada con la misma calidad, característica que no se presenta en las imágenes

desencriptadas a partir de un multiplexado convencional de imágenes encriptadas, según se detalló en el Capítulo 4.

En la sección siguiente se discuten los resultados obtenidos a partir del SOV. Se realiza un análisis de la calidad de las imágenes recuperadas de una secuencia dinámica y se comparan con los sistemas convencionales de encriptación. Los estadísticos empleados para ello son el máximo de la relación señal ruido ($PSNR$) y la raíz cuadrada del error cuadrático medio normalizado ($NRMSE$) (ver Apéndice B).

6.2.3 Discusión de resultados

En el experimento virtual se han tomado 22 imágenes de una película original las cuales han sido sometidas al proceso descrito anteriormente. A continuación del proceso de desencriptación, el despliegue de las imágenes para su visualización se sincroniza a razón de 10 marcos por segundo para obtener una película de 2.2 segundos, (ver Apéndice C.2). Después del proceso de recomposición, se puede observar un movimiento fluido de las imágenes correctamente recuperadas. Por el contrario, al reproducir la película sin la llave correcta de decodificación, se obtiene una secuencia de imágenes incorrectamente desencriptadas las cuales son patrones de *speckle* de-correlacionados. En la Figura 6.5 se muestra la imagen número diez de la película original. La Figura 6.5 (a) muestra la imagen desencriptada correctamente y la Figura 6.5 (b) muestra la imagen recuperada incorrectamente.

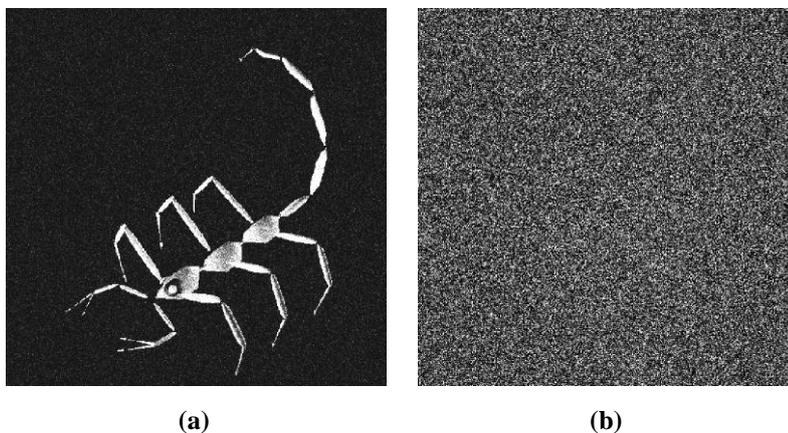


Figura 6.5: Resultados de la recuperación de información al emplear: (a) la llave de seguridad correcta y (b) una llave de seguridad incorrecta. La llave de seguridad correcta desencripta todas las imágenes de la escena dinámica. La llave de seguridad incorrecta no recupera información y las imágenes se mantienen encriptadas.

Para realizar el experimento se utilizó un objeto de $5.7 \times 5.7 \text{ mm}^2$ y una longitud de onda de iluminación de 632.8 nm. Las lentes delgadas empleadas en el proceso tienen distancia focal de 100 mm. El área del plano de filtrado es de $45 \times 45 \text{ mm}^2$, cada orden difractado tiene diámetro de 5.7 mm y la separación entre órdenes adyacentes es en promedio 6.5 mm. Esta última medida es relativa a la dirección y frecuencia de cada red.

Nótese que al tener todas las lentes la misma distancia focal, el plano de filtrado es un plano imagen del plano de la llave de seguridad. Así es posible filtrar un orden y hacer que interactúe directamente con la llave de codificación y recuperar la información sin la necesidad de realizar dos transformadas de Fourier adicionales. Sin embargo, para explicar adecuadamente la técnica de encriptación de eventos dinámicos se trabajan con estas dos transformadas de Fourier.

Al emplear los parámetros ópticos mencionados y atendiendo a la optimización del espacio en el plano de filtrado, las redes de difracción resultan con un espaciado máximo de $7 \text{ }\mu\text{m}$ o 142 líneas/mm. Así, el orden de difracción más cercano dista 9 mm del orden central. Y si el orden más alejado se ubica a 28.2 mm, el espaciado de las redes debe de ser de $2.25 \text{ }\mu\text{m}$ o tener 445 líneas/mm, por lo tanto, para que la información sea transmitida a los órdenes de difracción, como mínimo, el grano de *speckle* debe tener tamaño promedio de $14 \text{ }\mu\text{m}$.

Si el haz ilumina un diámetro promedio de la imagen de entrada de 5.7 mm, el grano de *speckle* tendrá en promedio $13.5 \text{ }\mu\text{m}$. Si el objeto es de menor tamaño actúa entonces como una pupila de menor diámetro formando un grano de *speckle* más grande. En este caso, su tamaño es calculado con la función de autocorrelación que define la región de coherencia [6.3]-[6.4].

Al tener menos franjas en un grano de *speckle* se tienen más valores de fase por franja, por lo que en promedio contribuye a que los órdenes difractados contengan la información relevante para realizar una buena reconstrucción. En un SOV la buena modulación de las redes depende del número de franjas que tenga en promedio el grano de *speckle*. Usar redes de frecuencias muy altas influye en la calidad de las imágenes

recuperadas tal como se mostró en la Sección 5.3.3. Consecuentemente, es de importancia evaluar la calidad de cada información descriptada.

Para realizar este análisis se aplican las métricas de *NRMSE* y *PSNR* barriendo cada imagen en diferentes direcciones. La ventaja de esta propuesta radica en que las medidas extraídas de cada imagen tienen un grado de dispersión en cada dirección respecto al valor promedio de cada estadístico utilizado. Esto no lo brindan directamente las métricas al comparar dos imágenes ya que arrojan un único valor sin saber realmente que representa respecto a toda la imagen. Este análisis que muestra dispersión de los datos se realizará únicamente para la aplicación en secuencias monocromáticas. La razón es que el procesado en color y la aplicación multiusuario están basados en esta primera experiencia, por lo tanto, el comportamiento de estos dos últimos es similar.

Para establecer la calidad de una imagen recuperada después de aplicarle un determinado proceso, (este caso, el de descriptación) se compara una imagen de referencia y la imagen observada después de la decodificación. A cada imagen de referencia y la observada se le realiza un promediado de intensidades de los píxeles que están en una dirección de ángulos iguales respecto al centro de la imagen (ver Apéndice B). Y a los valores que contribuyen a cada promediado angular de intensidades en una determinada dirección se les aplican las dos métricas antes mencionadas. Se emplea como imágenes de referencia a aquellas que se descriptan de un sistema convencional de codificación de doble máscara de fase en configuración $4f$ y como objetos observados se toman las imágenes de la escena dinámica descriptadas al utilizar la técnica de encriptación de eventos dinámicos.

Cada medida de las métricas en todas las direcciones arroja una curva a la cual se le puede encontrar el grado de dispersión respecto al valor promedio. Al realizar el diagrama de cajas (*DC*) de la información de *NRMSE* y *PSNR* en todas las direcciones angulares se interpreta la calidad de todas las imágenes recuperadas con la técnica de encriptación de eventos dinámicos. Es primordial hacer un análisis estadístico detallado, ya que la técnica propuesta debe asegurar que brinda ventajas sobre el multiplexado convencional.

Al realizar el procedimiento descrito anteriormente para las 22 imágenes recuperadas mediante la técnica de encriptación de eventos dinámicos, se obtienen los resultados de la Figura 6.6. Cada una de estas gráficas muestra el DC del $NRMSE$ encontrado entre la imagen de referencia y la imagen recuperada de la técnica propuesta. Cada DC muestra la dispersión de los datos graficados en color azul, donde el marcador (x) indica que hasta ese punto se han realizado el 99% de las medidas. Los marcadores con signo (+) indican el valor mínimo y el valor máximo de cada medida y el marcador en cuadro rojo indica el valor promedio de la métrica en cada imagen.

La gráfica de la Figura 6.6 (a) muestra el DC del $NRMSE$ entre las imágenes de referencia y las imágenes de la secuencia dinámica recuperadas cuando se usa la llave de seguridad correcta. Este caso corresponde a la Figura 6.5 (a) y a todas las imágenes de la película. Los valores han sido normalizados a la unidad con constante de normalización 0.2, lo que indica que el $RMSE$ es muy pequeño indicando una gran similitud con las imágenes recuperadas del sistema convencional de encriptación 4f.

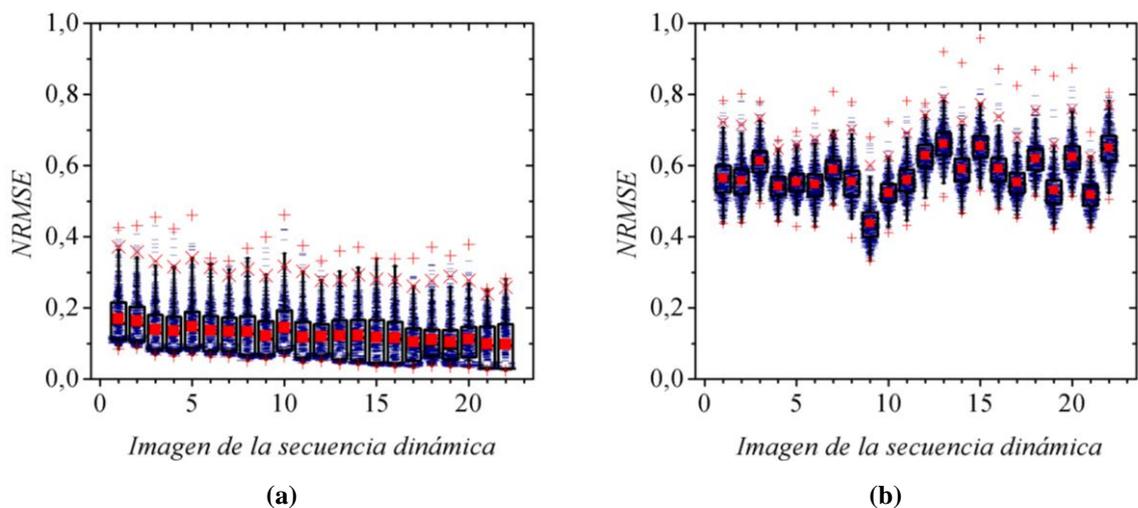


Figura 6.6: Raíz cuadrada del error cuadrático medio normalizado de las imágenes recuperadas de la película con (a) la llave correcta de seguridad y (b) la llave incorrecta de seguridad.

Nótese como la media del $NRMSE$ se mantiene constante a lo largo de todas las imágenes recuperadas concluyendo que se recuperan las imágenes con una calidad uniforme. Obsérvese que la dispersión en la información de cada $NRMSE$ está por encima del valor promedio, indicando que la imagen recuperada tiene la presencia de zonas que difieren mucho de la imagen de referencia. Esto es de esperarse y se le puede atribuir al ruido de *speckle* que siempre está presente en los procesos ópticos. Por último, los valores

atípicos que están por fuera del límite superior o límite inferior del DC no superan el 1% y no contribuyen al comportamiento general de las medidas de $NRMSE$ y $PSNR$.

La gráfica de la Figura 6.6 (b) muestra el DC del $NRMSE$ entre las imágenes de referencia y las imágenes recuperadas de la secuencia dinámica cuando se usa una llave de seguridad incorrecta. Este caso corresponde a la Figura 6.5 (b) y a todas las imágenes de la película. Se observa que el valor de $NRMSE$ de todas las imágenes es en promedio constante y es mucho mayor que los valores de $NRMSE$ de la Figura 6.6 (a). Nótese también como la dispersión de los valores es homogénea y simétrica en cada DC indicando que la distribución estadística de las imágenes recuperada es constante. Esto se le puede atribuir a que todas las imágenes recuperadas siguen encriptadas y tienen una distribución que siguen la misma estadística de un patrón de *speckle*.

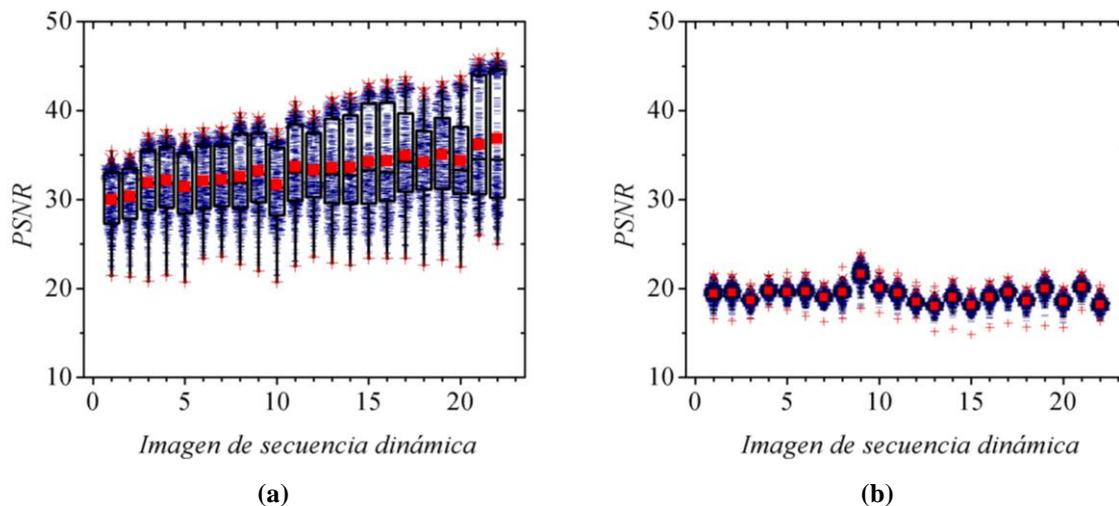


Figura 6.7: Pico de la relación señal ruido en dB de las imágenes recuperadas de la secuencia dinámica con (a) la llave correcta de seguridad y (b) la llave incorrecta de seguridad.

Para complementar las medidas de $NRMSE$, se acude a la métrica de $PSNR$. Cuanto más alto sea el valor de $PSNR$ se asegura que mejor es la calidad del objeto recuperado. Al comparar dos imágenes, los valores de $PSNR$ están usualmente entre 30 dB y 50 dB. En estos rangos se puede identificar el objeto original con alta calidad, valores por debajo indican que la imagen recuperada tiene calidad inferior en comparación a la imagen de referencia.

En la gráfica de la Figura 6.7 (a) se muestra el *DC* del *PSNR* entre las imágenes de referencia y las imágenes de la secuencia dinámica recuperadas cuando se usa una llave de seguridad correcta. La dispersión de los valores de *PSNR* indica que existen sectores de baja y alta calidad. Esto se le puede atribuir al ruido de *speckle*, por ejemplo en los sectores oscuros de la imagen se puede encontrar ruido. El valor *PSNR* indicará aquellos sectores de baja calidad.

Ya que el valor medio del *PSNR* está dentro de los rangos de buena calidad, se puede afirmar que las imágenes recuperadas del proceso de desencriptación de eventos dinámicos son muy aceptables. Los resultados son comparables a aquellos del sistema convencional de encriptación de doble máscara de fase en configuración 4f.

Otra información relevante que brinda el *PSNR* en todas las imágenes es la tendencia del aumento de este valor con el orden de las imágenes recuperadas. Este aumento se le puede atribuir a la modulación de las redes periódicas de amplitud. La información se encuentra mejor modulada al tener más elementos de fase por franjas. Como es de esperarse digitalmente, una red periódica de mayor frecuencia espacial tienen menos valores de amplitud por franja, estas son las que difractan en posiciones más alejadas del orden central en el plano de filtrado a diferencia de franjas de menor frecuencia que difractan en posiciones más cercanas al orden central. De esta forma, se deduce que ya que el *PSNR* aumenta con el orden de la imagen recuperada, inicialmente la modulación de las imágenes encriptadas se ha realizado con redes de frecuencias altas. A medida que va aumentando el número de imágenes encriptadas se va reduciendo la frecuencia de la red de modulación. Este detalle no se aprecia a simple vista, sin embargo las medidas de *PSNR* permiten deducir estos pequeños cambios que afectan la calidad de las imágenes desencriptadas.

Por último, la gráfica de la Figura 6.7 (b) muestra el diagrama de cajas del *PSNR* entre las imágenes de referencia y las imágenes de la secuencia dinámica recuperadas cuando se usa una llave de seguridad incorrecta. Se puede observar como la media del *PSNR* de todas las imágenes está por debajo de los valores aceptables de calidad. Por lo tanto, al usar una llave de seguridad incorrecta se degrada completamente la calidad de las

imágenes recuperadas. Los valores de $PSNR$ están distribuidos homogéneamente y son simétricos en el DC . De la misma manera que para el $NRMSE$, la dispersión de los valores no es muy grande indicando que las imágenes recuperadas tienen una distribución que tiene una estadística constante (*speckle*).

Evidentemente, cuando se usa la llave correcta de seguridad, la información recuperada con la técnica de encriptación de eventos dinámicos permite descryptar la información a partir de un multiplexado de 22 imágenes. No ocurre así en un multiplexado convencional donde se degrada la información recuperada. Este hecho se puede observar en las gráficas de la Figura 6.8, al comparar las dos curvas de $NRMSE$ y $PSNR$ de las imágenes descryptadas al utilizar los dos sistemas, a partir de un multiplexado convencional y a partir de la técnica de encriptación de eventos dinámicos desarrollada.

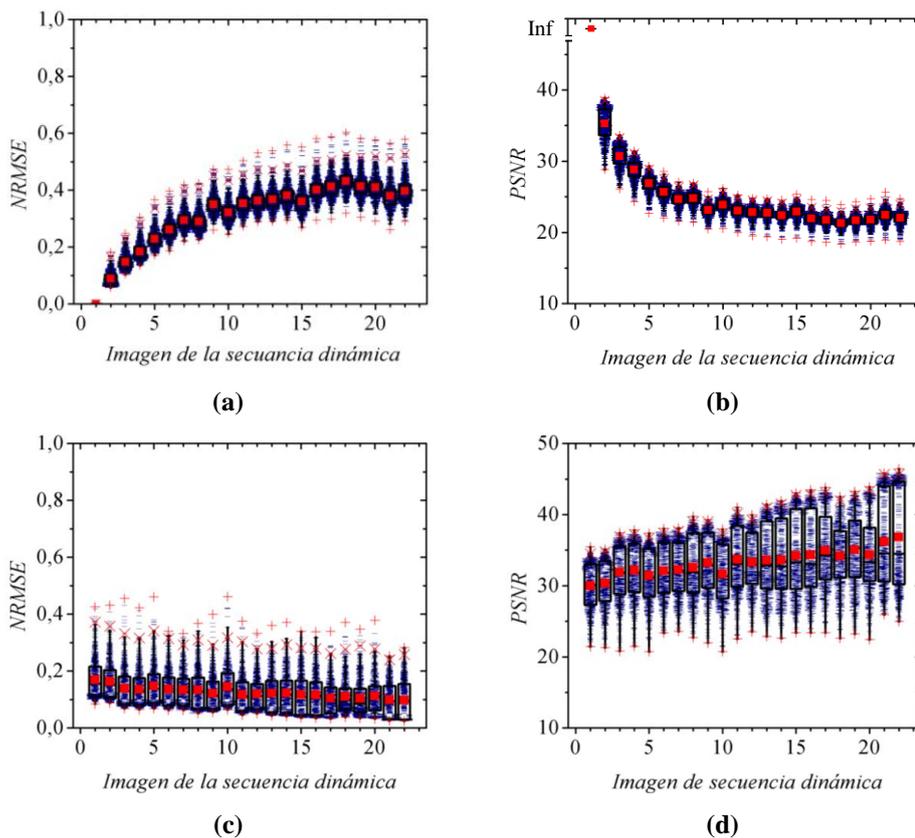


Figura 6.8: Curvas de $NRMSE$ y $PSNR$ de las imágenes recuperadas al aplicar: (a), (b) la técnica de convencional multiplexado y (c), (d) la técnica de encriptación de eventos dinámicos.

Nótese en la Figura 6.8 (a) y en la Figura 6.8 (b) como la calidad de las imágenes recuperadas en la técnica de multiplexado convencional se degrada a medida que se

aumenta el número de imágenes encriptadas. Por el contrario, como se observa en Figura 6.8 (c) y Figura 6.8 (d), con la técnica propuesta, la calidad de las imágenes recuperadas se mantiene en un valor promedio constante

En la Figura 6.9 se muestra la comparación de las imágenes recuperadas a partir de las tres técnicas, el sistema de codificación de doble máscara de fase en configuración $4f$, un multiplexado convencional y al utilizar la técnica de encriptación de eventos dinámicos.

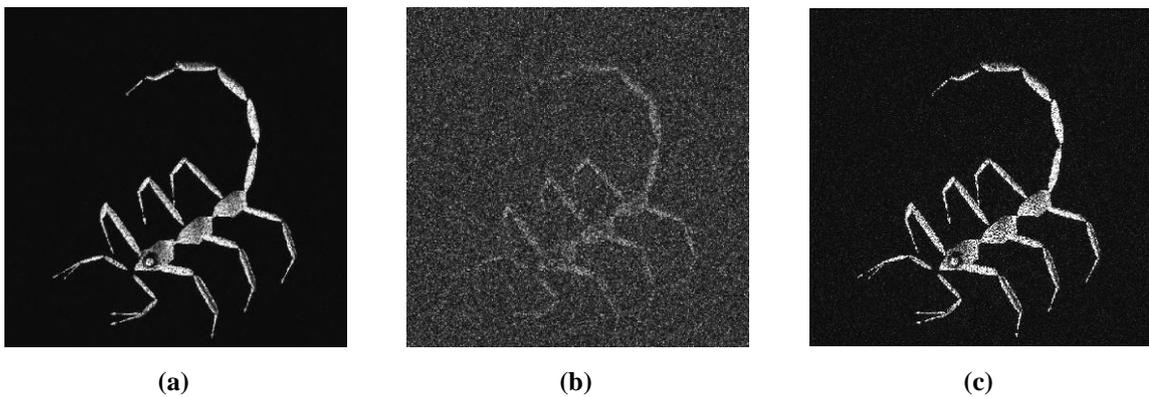


Figura 6.9: Comparación de imágenes recuperadas de los sistemas de encriptación: (a) de doble máscara de fase en configuración $4f$, (b) multiplexado convencional de información y (c) técnica de encriptación de eventos dinámicos.

Indudablemente se pueden observar los beneficios que tiene emplear la técnica de encriptación de eventos dinámicos en procesos que requieren transmitir grandes volúmenes de información. Esta técnica asegura que no existe un deterioro considerable en la información recuperada. En la técnica propuesta no se muestra una dependencia de la calidad de cada imagen recuperada respecto al número de imágenes multiplexadas, tal como ocurre en la técnica de multiplexado convencional.

Finalmente, en la Tabla 6.1 se muestra en detalle los valores de los pitch de las redes usadas para realizar el experimento virtual. Estos valores sirven como base para una posible implementación analógica junto a los parámetros ópticos del sistema óptico virtual. En la Tabla 6.1 también se muestra la correspondiente distancia de separación de los órdenes de difracción respecto al orden central y la relación que existe entre las medias de las métricas $NRMSE$, $PSNR$ de las imágenes recuperadas, relacionando las características de la red de modulación con la calidad de las imágenes recuperadas.

| Imágenes de la secuencia dinámica | Distancia desde el orden difractado al orden central | | Métricas de imágenes recuperadas con máscara de fase correcta | | Métricas de imágenes recuperadas con máscara de fase incorrecta | |
|-----------------------------------|--|-------------------------|---|-------|---|-------|
| | Imagen | Pitch (μm) | $d(\text{mm})$ | NRMSE | PSNR (dB) | NRMSE |
| 1 | 2.3 | 28.1742 | 0.17 | 29.98 | 0.54 | 19.43 |
| 2 | 2.6 | 24.4824 | 0.16 | 30.35 | 0.53 | 19.53 |
| 3 | 2.9 | 21.6747 | 0.14 | 31.92 | 0.58 | 18.69 |
| 4 | 3.1 | 20.1244 | 0.14 | 32.16 | 0.51 | 19.76 |
| 5 | 2.3 | 28.1742 | 0.15 | 31.42 | 0.53 | 19.57 |
| 6 | 2.6 | 24.4824 | 0.14 | 32.10 | 0.52 | 19.68 |
| 7 | 2.9 | 21.6747 | 0.13 | 32.24 | 0.56 | 19.04 |
| 8 | 3.1 | 20.1244 | 0.13 | 32.57 | 0.53 | 19.58 |
| 9 | 2.6 | 24.4824 | 0.12 | 33.23 | 0.42 | 21.65 |
| 10 | 2.9 | 21.6747 | 0.14 | 31.67 | 0.50 | 20.07 |
| 11 | 3.1 | 20.1244 | 0.12 | 33.72 | 0.53 | 19.50 |
| 12 | 2.6 | 24.4824 | 0.12 | 33.31 | 0.60 | 18.48 |
| 13 | 2.9 | 21.6747 | 0.12 | 33.57 | 0.63 | 18.03 |
| 14 | 3.1 | 20.1244 | 0.12 | 33.62 | 0.56 | 19.03 |
| 15 | 3.1 | 20.1244 | 0.12 | 34.24 | 0.62 | 18.12 |
| 16 | 3.8 | 16.5950 | 0.12 | 34.31 | 0.56 | 19.02 |
| 17 | 4.4 | 14.5119 | 0.10 | 34.95 | 0.53 | 19.59 |
| 18 | 3.1 | 20.1244 | 0.11 | 34.17 | 0.59 | 18.60 |
| 19 | 3.8 | 16.5950 | 0.10 | 35.04 | 0.50 | 19.96 |
| 20 | 4.4 | 14.5119 | 0.11 | 34.35 | 0.59 | 18.55 |
| 21 | 3.8 | 16.5950 | 0.10 | 36.21 | 0.49 | 20.17 |
| 22 | 4.4 | 14.5119 | 0.10 | 36.83 | 0.62 | 18.19 |

Tabla 6.1: Relación entre las métricas *NRMSE*, *PSNR* de las imágenes recuperadas, el pitch de cada red de amplitud usada en la modulación y la distancia de separación de los órdenes de difracción respecto al orden central

De la Tabla 6.1 se puede observar como en promedio, a medida que la distancia de separación de los orden difractados se reduce, la calidad de las imágenes recuperadas aumenta, esto indica que al modular digitalmente la información encriptada para una cierta configuración de parámetros ópticos, a menor pitch o mayor número de líneas por milímetro, la información recuperada tendrá menos calidad que al usar redes de pitch más grande o menor número de líneas por milímetro.

En resumen, se ha desarrollado el concepto de encriptación/desencriptación de eventos dinámicos permitiendo desplegar fenómenos que evolucionan en el tiempo. Se mostró que la técnica realiza un “etiquetado” de cada imagen encriptada para evadir el efecto de solapamiento de información presente en sistemas convencionales de multiplexado de imágenes encriptadas registradas en medio planos. El “etiquetado” que se evidencia en el plano de filtrado permite seleccionar apropiadamente información

encriptada para recuperarla sin superposición. Finalmente, aplicando la sincronización adecuada y al usar la llave de seguridad correcta es posible reconstruir y desplegar el movimiento natural del fenómeno dinámico.

En la sección siguiente se utilizan las ventajas que posee la técnica de encriptación de eventos dinámicos en la aplicación al procesamiento de secuencias dinámicas a color.

6.3 Encriptación de escenas dinámicas policromáticas

En la sección anterior se presentó la aplicación de la técnica de encriptación de eventos dinámicos en secuencias monocromáticas compuestas de imágenes en niveles de gris de 8 bits. La salida debía estar sincronizada para reconstruir el movimiento de la escena en el orden cronológico correcto a partir de la selección adecuada de información en la etapa de filtrado. Esta aplicación desplegó correctamente la información en tiempo real y en ese sentido ofrece nuevas perspectivas en la rama de encriptación óptica. Posibles extensiones del método sugieren diversas experiencias como el uso de transformaciones unitarias en reemplazo de la transformada de Fourier, incorporación de marcas de agua, adición de niveles de acceso, modulación de un objeto con redes de diferente periodicidad, recomposición parcial de información, estudios sistematizados de la influencia del ruido, el rol de la coherencia parcial, entre otras. En este punto, la extensión natural de la técnica conduce hacia su aplicación para encriptar/desencriptar secuencias policromáticas en tiempo real.

6.3.1 Descripción general

Cada imagen que compone la secuencia policromática es un arreglo matricial de $M \times N \times 3$ píxeles de color. Cada píxel tiene componentes correspondientes al rojo, verde y azul constituyendo una imagen RGB. Los canales cromáticos de la imagen RGB son imágenes en niveles de gris las cuales al ser desplegadas en un monitor que soporta estas tres componentes produce una imagen de 2^{24} colores, es decir, cada píxel puede soportar hasta 24 bits de información.

En años recientes, algunos esquemas de encriptación de imágenes a color [6.5]-[6.7] han sido propuestos y analizados. En ciertos casos, la estrategia de trabajo consiste en procesar por separado cada uno de sus canales cromáticos, realizar el proceso de encriptación, enviar la información al usuario y recuperar las imágenes a color realizando la composición con los canales procesados. En otras situaciones experimentales, se emplean sistemas opto-electrónicos para combinar los canales cromáticos, en estos casos se aumenta el número de elementos ópticos del sistema impidiendo implementaciones a tiempo real. El problema básico de la implementación a tiempo real, radica en ajustar la magnificación en la máscara de fase para compensar las aberraciones cromáticas cuando se trabaja con fuentes de iluminación compuestas de varias longitudes de onda.

Es importante resaltar que la propuesta que se presenta en esta sección emplea una única llave de codificación para encriptar los canales RGB de cada escena dinámica. Por otro lado, es de notar que la magnificación cromática es resuelta procesando independientemente los tres canales de color. De esta manera, indirectamente se está evitando el multiplexado de varios canales cromáticos en un único medio de registro. Esto permite la posibilidad de recombinar en tiempo real las imágenes recuperadas correspondientes a cada color, sin adicionar elementos ópticos que contribuyan a su degradación. Por lo tanto, se prefiere hacer tres procesados ópticos en paralelo y realizar la composición de las imágenes RGB al final del proceso en la etapa de desencriptación.

6.3.2 Descripción del método

El método consiste en aplicar en paralelo el procedimiento descrito en la Sección 6.2.2 para una secuencia monocromática a los tres canales de color RGB de la secuencia dinámica policromática. De esta forma, cada una de las imágenes que componen la escena a color es descompuesta en sus tres canales cromáticos como lo muestra la Figura 6.10. Un pixel de color rojo de la imagen de la Figura 6.10 (a) se obtiene con las componentes (255, 0, 0), un pixel de color verde de la Figura 6.10 (b) se obtiene con (0, 255, 0) y un pixel de color azul de la Figura 6.10 (c) se obtiene con (0, 0, 255). La ausencia de color (color negro) se obtiene cuando las tres componentes de un pixel son 0 (0, 0, 0). Mediante la mezcla por adición de los tres canales de color primarios se obtiene la imagen de la Figura

6.10 (d) donde se pueden observar pixeles que tienen contribuciones de cada color monocromático.

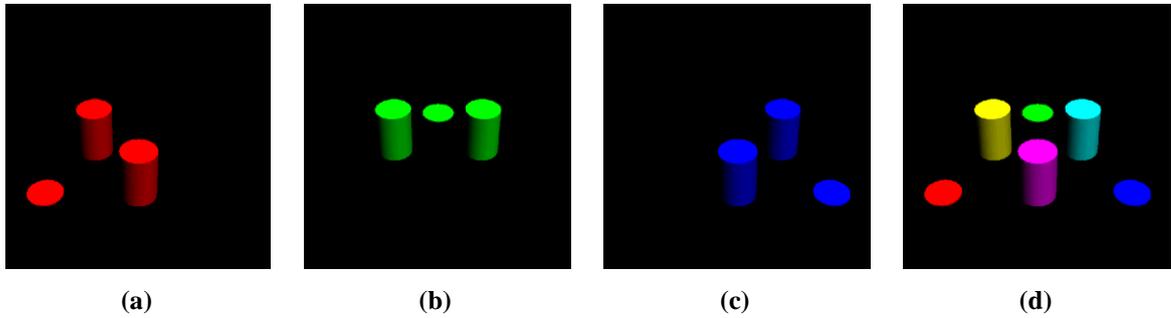


Figura 6.10: Componentes de color de una imagen RGB. Componente de color (a) rojo, (b) verde y (c) azul. Al desplegar las tres componentes en un dispositivo que soporte imágenes RGB se mostrará la imagen a color (d).

Cada una de las componentes de las imágenes RGB que constituyen la secuencia dinámica es codificada en un sistema de encriptación de doble máscara de fase en configuración $4f$, tal como lo muestra la Figura 6.11.

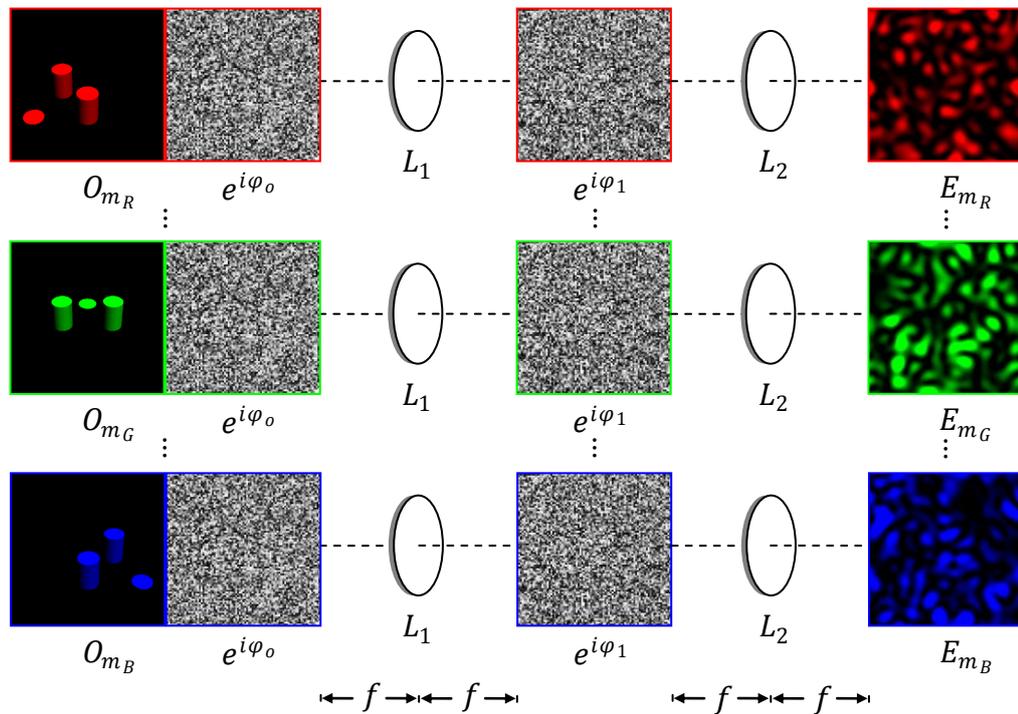


Figura 6.11: Etapa de encriptación de una secuencia policromática. L_1 y L_2 son lentes de distancia focal f , O_{m_C} es la componente de color $C: R, G, B$ del objeto O_m , $e^{i\varphi_0}$ es la primera máscara de fase, $e^{i\varphi_1}$ es la llave de seguridad, E_{m_C} es la componente de color encriptada.

Las componentes de color $O_{m_C}(x, y)$, donde $C: R, G, B$, de todas las imágenes de la escena en movimiento han sido encriptadas con una única máscara de fase $e^{i\varphi_1(x_f, y_f)}$ que actúa como llave única de seguridad para codificar y decodificar la información. Al final del proceso se obtienen las tres secuencias a color encriptadas, compuestas de las imágenes $E_{m_C}(x_0, y_0)$. Nótese que la representación de cada color se visualiza con la ausencia de las otras dos componentes y no como un canal monocromático. De hecho en la experiencia, las imágenes de componentes de color puro son representadas por imágenes binarias tal como se hace en las experiencias de pseudocoloreado. En la experiencia analógica cada componente es una imagen en niveles de gris o una transparencia que deja transmitir diferentes intensidades de luz representando una componente de color monocromática.

Seguido al proceso de encriptación, se aplica la técnica de modulación theta a cada una de las componentes cromáticas encriptadas. Finalmente, por medio de la operación de multiplexado se guarda la información de cada canal de color encriptado en un único elemento. De esta forma se obtienen tres multiplexados independientes.

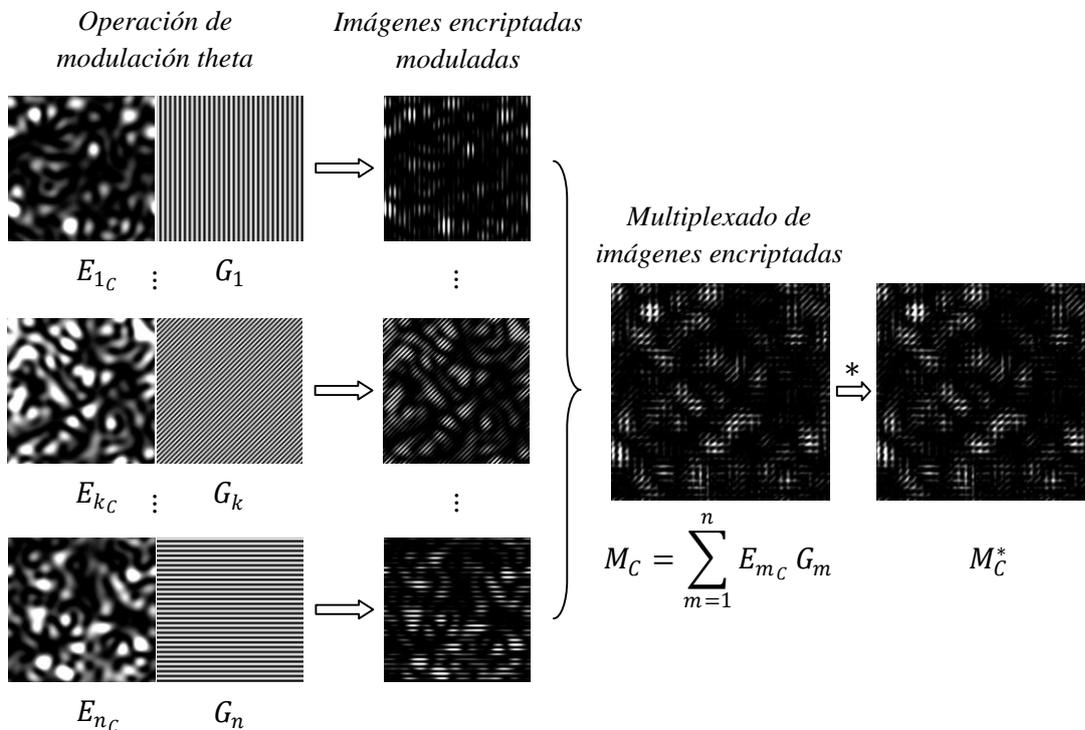


Figura 6.12: Técnica de modulación theta, técnica de multiplexado y operación de conjugación de fase. E_{k_C} es la imagen encriptada de una componente de color, $C: R, G, B$, G_k es la red sinusoidal de amplitud, M_C es el multiplexado de cada canal de color y (*) es la operación de conjugación de fase.

En referencia a la Figura 6.12, las imágenes encriptadas $E_{m_c}(x_0, y_0)$ son moduladas con las redes de amplitud $G_k(x_0, y_0; u_k, v_k)$. De esta forma, todas las imágenes encriptadas y moduladas son multiplexadas para luego realizarles la operación de conjugación de fase.

Este conjunto de operaciones puede ser expresado como:

$$M_C^*(x_0, y_0) = \left[\sum_{k=1}^N E_{m_c}^*(x_0, y_0) G_k(x_0, y_0; u_k, v_k) \right]^* \quad (6.6)$$

Al usuario final se le envía por medio de un canal de comunicación digital las cantidades $M_R^*(x_0, y_0)$, $M_G^*(x_0, y_0)$, $M_B^*(x_0, y_0)$ y la llave de seguridad $e^{i\varphi_1(x_f, y_f)}$ para que pueda recuperar la información en tiempo real. Es de aclarar que el usuario debe poseer tres copias de la llave de seguridad. Debido a que las llaves no son físicas, si no en formato digital, su copia no representa ningún inconveniente.

La etapa de recuperación consiste en realizar un proceso de filtrado de información que debe estar acompañada de una sincronización adecuada. La sincronización debe ser en los tres canales cromáticos simultáneamente para poder recombinarlos a tiempo real y poder visualizar la secuencia a color en el orden cronológico correcto.

Es de notar que los esquemas de cada etapa de encriptación son similares a los de la secuencia monocromática, por lo que la etapa de filtrado para cada canal cromático puede ser representada por el esquema de la Figura 6.13 que muestra el proceso para cada canal de color. En la entrada de la etapa de filtrado se ubica el complejo conjugado de cada uno de los multiplexados cromáticos, esto es $M_C^*(x_0, y_0)$, $C: R, G, B$. Una transformada de Fourier revelará los órdenes difractados para cada etapa de filtrado de los tres multiplexados. Posteriormente, se aplican las mismas máscaras que permiten seleccionar y transmitir un orden ubicado en la misma posición en los tres planos de filtrado asegurando la misma sincronización en los tres canales. Finalmente, por medio de otra transformada de Fourier aplicada a cada orden transmitido de cada canal, se obtiene el complejo conjugado de las imágenes encriptadas $E_C^*(x, y)$ (posterior a una operación de inversión). Esto es representado por la Ecuación (5.8) para cada canal de color.

El último paso de la etapa de desencriptación consiste en recuperar cada uno de los canales imágenes de la escena dinámica, al utilizar un proceso convencional de decodificación en arquitectura $4f$. Este proceso está esquematizado en la Figura 6.13.

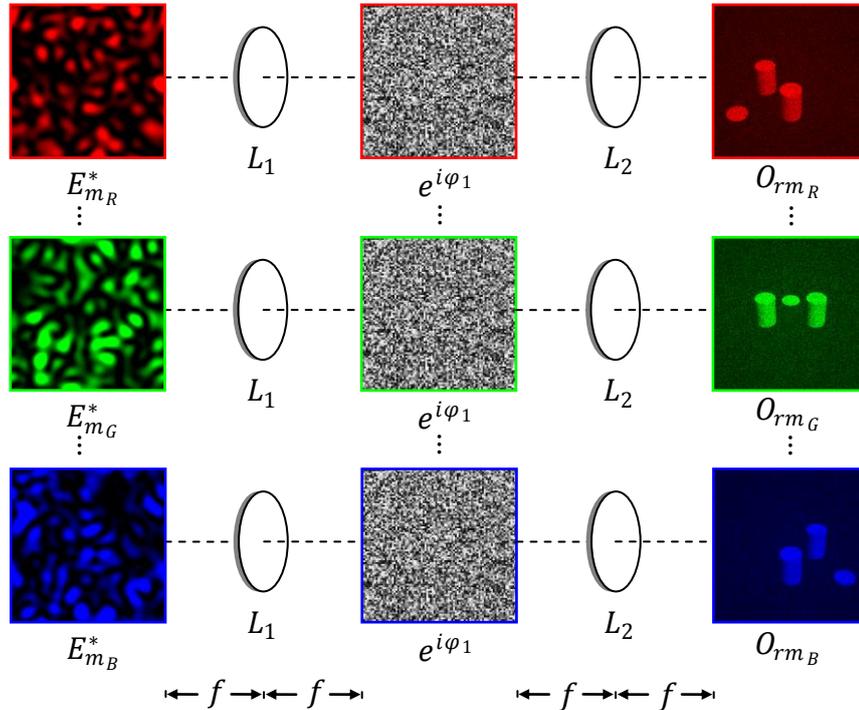


Figura 6.13: Etapa de recuperación de la información cromática de una imagen. L_1 y L_2 son lentes de distancia focal f , $e^{i\varphi_1}$ es la llave de seguridad, $E_{m_C}^*$ es la componente de color encriptada y O_{rm_C} es la componente de color $C: R, G, B$ recuperada del objeto O_m .

Finalmente, el proceso de recuperación concluye con la recomposición de las imágenes a color para visualizar la escena dinámica policromática

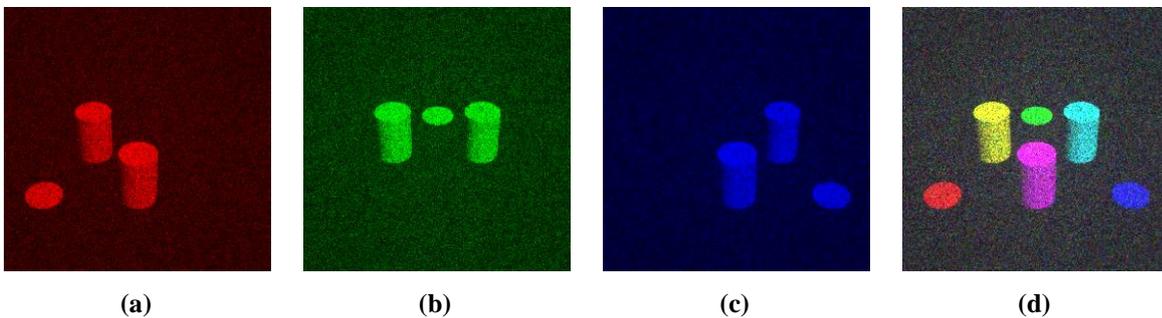


Figura 6.14: Componentes de color de una imagen RGB recuperada al utilizar la técnica propuesta. Componente de color (a) rojo, (b) verde y (c) azul. Al desplegar las tres componentes en un dispositivo que soporte imágenes RGB se mostrará la imagen a color (d).

La Figura 6.14 muestra el resultado de las imágenes recuperadas al procesar independientemente los tres canales cromáticos de la Figura 6.10 al utilizar la técnica de encriptación de eventos dinámicos. Las Figuras 6.14 (a), (b) y (c) muestran las componentes de color rojo, verde y azul, respectivamente y en la Figura 6.14 (d) se muestra la imagen resultante al combinar las imágenes de los tres canales de color recuperados. Nótese que las cuatro imágenes de la Figura 6.14 exhiben el fenómeno de *speckle* al igual que en un sistema óptico real.

En resumen, el proceso completo conlleva a la clara visualización de cada imagen de color sin la influencia de las otras de la escena dinámica. El usuario recibe la información de los tres multiplexados cromáticos junto a la única llave de seguridad. El éxito del procedimiento recae en la sincronización automática la cual está implícita como un sistema adicional en la estación de desencriptación. Además, la adecuada sincronización en la selección del orden cronológico de las imágenes y la selección adecuada de la información de cada canal de color en el plano de filtrado, permiten la correcta reconstrucción de la película de color a tiempo real.

Debe enfatizarse que la técnica de encriptación de eventos dinámicos evita el solapamiento de información recuperando las imágenes a partir de cada orden seleccionado en la etapa de filtrado donde la información de toda la escena dinámica es desplegada sin superposición. Esto se cumple si las redes de modulación difractan sus órdenes con una separación suficiente tal que no se superponen.

Se comprueba que el método desarrollado es aplicable para encriptar secuencias dinámicas policromáticas. Sin el uso de las redes periódicas de amplitud que modulen las imágenes encriptadas cromáticas y sin el subsecuente proceso de filtrado, la visualización de cada imagen a color estaría degradada. En este sentido, se realiza un análisis de la calidad de las imágenes recuperadas de la secuencia policromática y se comparan con los resultados obtenidos al emplear sistemas convencionales de encriptación. Los estadísticos empleados para este análisis son el pico de la relación señal ruido *PSNR* y la raíz cuadrada del error cuadrático medio normalizado *NRMSE*.

6.3.3 Discusión de resultados

Los procesos que involucran la encriptación y recuperación de una escena dinámica han sido implementados en un SOV. En el experimento virtual se han tomado 30 imágenes a color de una película original sometida al proceso descrito anteriormente. Se realizan dos ejemplos que contienen escenas dinámicas diferentes. El primero consiste en cilindros moviéndose y el segundo una animación de un pájaro bebedor. El despliegue de las imágenes recuperadas para su visualización se sincroniza a 10 imágenes por segundo para obtener una película de color de 3 segundos (ver Apéndice C.3)

Para realizar el experimento se emplearon los mismos parámetros de la secuencia monocromática, el objeto de entrada es de tamaño $5.7 \times 5.7 \text{ mm}^2$, la longitud de onda de iluminación es de 632.8 nm y las lentes involucradas en todo el proceso tienen distancia focal de 100 mm. Por lo tanto, se tienen los mismos valores que en la experiencia de la secuencia monocromática para el área del plano de filtrado, el diámetro de los órdenes y la distancia entre ellos.

| <i>Red</i> | <i>Pitch (μm)</i> | <i>Líneas/mm</i> |
|------------|---|------------------|
| 1 | 2.2 | 445 |
| 2 | 2.6 | 389 |
| 3 | 2.9 | 343 |
| 4 | 3.1 | 318 |
| 5 | 3.8 | 262 |
| 6 | 4.4 | 229 |
| 7 | 5.2 | 191 |
| 8 | 7.0 | 142 |

Tabla 6.2: Parámetros de las redes periódicas de amplitud usadas para encriptar 30 imágenes a color. Al iluminar cada imagen encriptada modulada con una longitud de onda de 632.8 nm y al usar lentes de 100 mm en todos los procesos involucrados, el tamaño del plano de filtrado tiene un área de $45 \times 45 \text{ mm}^2$

Nótese que ahora cada película es constituida por 30 imágenes de color, es decir 8 imágenes más que la secuencia monocromática y se utilizan los mismos parámetros ópticos. Esto implica que para la misma área del plano de filtrado se ubica un mayor número de órdenes de difracción. Esto se logra optimizando las relaciones entre el pitch y el ángulo de rotación de la red cuando se realiza la modulación. Los cálculos indican que para optimizar el espacio disponible de $45 \times 45 \text{ mm}^2$ del plano de filtrado, son necesarias ocho redes de diferente pitch asociadas a 30 pares de órdenes de difracción, cada uno de

área $5.7 \times 5.7 \text{ mm}^2$. Los valores de los pitch de las ocho redes de modulación se muestran en la Tabla 6.2.

Así, los tres canales de color de las imágenes que constituyen cada película son encriptadas con una única llave de seguridad y moduladas con las ocho redes descritas en de la Tabla 6.2. Las redes se rotan entre $\sim 8^\circ$ y $\sim 172^\circ$ para difractar órdenes en diferentes posiciones. La separación máxima del orden difractado al usar la red de menor pitch es ~ 28 mm y la separación mínima del orden difractado al usar la red de mayor pitch es de ~ 9 mm. Las distancias son medidas desde el orden central. Posteriormente a la modulación se realiza la operación de multiplexado y conjugación de fase para finalmente enviarle al usuario los tres canales de color multiplexados y la llave única de seguridad.

Para recuperar la información se aplica la sincronización correcta en los tres canales de color y se aplica el proceso de desencriptación en cada canal. Consecutivamente a un proceso de recomposición se puede observar un movimiento fluido de las imágenes desencriptadas al utilizar la llave de seguridad correcta. Por el contrario, al usar una llave de seguridad incorrecta, se obtiene una secuencia de imágenes que aun están encriptadas. Estas imágenes son patrones de *speckle* de color sin ninguna correlación.

En la Figura 6.15 se muestran imágenes de dos escenas diferentes recuperadas al aplicar la técnica propuesta. La Figura 6.15 (a) muestra una imagen de la película de cilindros en movimiento recuperada al utilizar la llave de seguridad correcta y (b) al usar la llave de seguridad incorrecta. La Figura 6.15 (c) muestra una imagen de la película del pájaro balanceándose desencriptada al usar la llave de seguridad correcta y (d) al utilizar la llave de seguridad incorrecta.

En la Figura 6.15 se puede observar la presencia de ruido de *speckle* cuyo color depende de las componentes cromáticas que tenga la imagen original. Por ejemplo, en la imagen del pájaro existen más componentes del color verde frente a las contribuciones del amarillo y cian, así el color predominante del *speckle* al desencriptar incorrectamente la imagen es el color verde. De la misma forma, el *speckle* de fondo en la imagen correctamente decodificada tiende a tener este color. Por el contrario, en la imagen recuperada de los cilindros se puede notar una distribución más uniforme de colores

indicando que las componentes de la imagen tienen en promedio el mismo porcentaje de componentes de color.

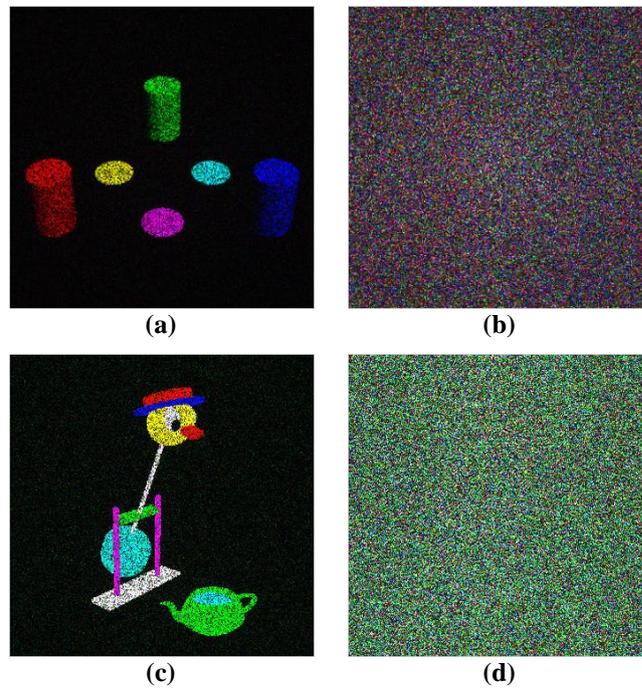


Figura 6.15: Imágenes recuperadas de las secuencias policromáticas. Recuperación de la película de cilindros en movimiento usando (a) llave de seguridad correcta y (b) llave de seguridad incorrecta. Recuperación de la película del pájaro balanceándose usando (c) llave de seguridad correcta y (d) llave de seguridad incorrecta.

En términos de calidad, es importante cuantificar el ruido de todas las imágenes recuperadas utilizando las métricas de *NRMSE* o *PSNR*.

En la Figura 6.16 se muestran los valores del pico de la relación señal-ruido de las 30 imágenes recuperadas de la secuencia del pájaro balanceándose. Para encontrar estos valores, cada imagen recuperada mediante la técnica de eventos dinámicos es comparada con la imagen recuperada de un sistema convencional *4f*. Esta última es tomada como imagen de referencia en el cálculo de las métricas.

Se puede observar en la Figura 6.16 que la calidad de las imágenes recuperadas es buena presentando un *PSNR* alto cuando se descrypta con la llave de seguridad correcta, a diferencia de cuando se emplea una llave de seguridad incorrecta. En este último caso se obtiene un valor de *PSNR* bajo.

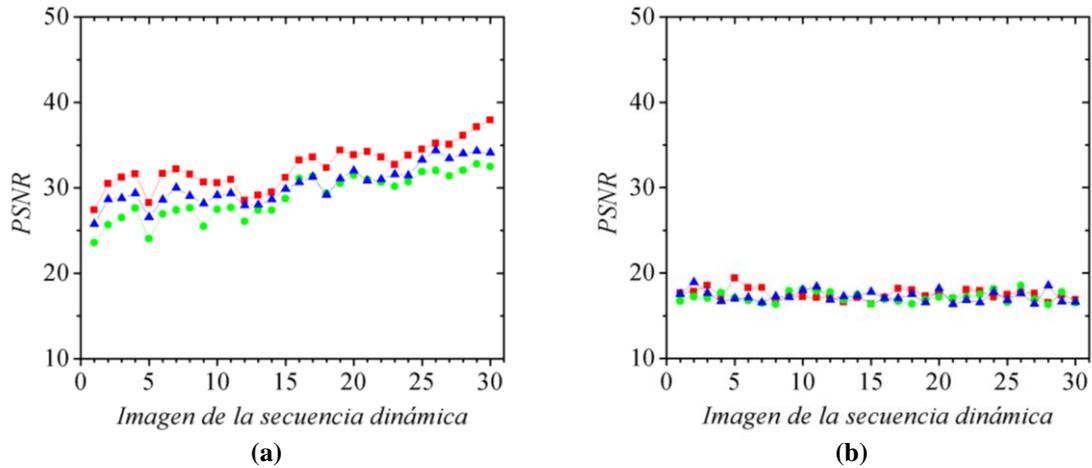


Figura 6.16: Pico de la relación señal-ruido de las imágenes recuperadas de los tres multiplexados cromáticos. La escena analizada es el pájaro balanceándose usando. *PSNR* al usar (a) la llave de seguridad correcta y (b) la llave de seguridad incorrecta en el proceso de desencriptación.

Nótese que el comportamiento de los tres canales de color es similar al comportamiento de la Figura 6.7, donde se muestra la calidad de las imágenes recuperadas de la secuencia monocromática. De la misma manera, se puede notar como el *PSNR* aumenta a medida que las imágenes se modulan con una red de menor pitch, a diferencia de las primeras imágenes recuperadas las cuales son moduladas con redes de pitch de mayor valor.

Ahora bien, haciendo referencia nuevamente a la Tabla 6.2, se debe observar que los valores del pitch de cada red, junto a los parámetros del sistema óptico (longitud de onda y distancia focal de las lentes involucradas) definen estrictamente las condiciones para que no se presente solapamiento de los órdenes difractados en el plano de filtrado. Esto implica una dependencia con el ángulo de rotación de cada red. Los parámetros de la Tabla 6.2 aseguran que el orden central está separado una distancia considerable de los órdenes difractados más cercanos. Esto evita que las frecuencias del orden central degraden los órdenes que están más cercanos.

Debe señalarse que todos los parámetros ópticos son establecidos para que se realice una transmisión de una secuencia dinámica de hasta 30 imágenes. El espacio en el plano de filtrado fue optimizando usando los valores de la Tabla 6.2 ubicando la mayor cantidad de órdenes sin solapamiento.

Ahora, si se quiere transmitir una escena dinámica de mayor extensión, sería poco práctico cambiar los parámetros ópticos y características de los procesos involucrados en la estación de desencriptación de todos los usuarios para poder visualizar una escena de mayor extensión. Además, usar redes de mayores frecuencias produciría cambios en el área del plano de filtrado teniendo que readecuar el sistema para realizar una buena sincronización. En este sentido, se requiere conservar los parámetros y el rango de los pitch de las redes de modulación para tener la misma área del plano de filtrado. En otras palabras, se requiere que el mismo sistema óptico ya pre-establecido en las estaciones de encriptación y de desencriptación soporte secuencias dinámicas de diferente extensión.

Con este objetivo, se investiga la posibilidad de realizar secuencias dinámicas policromáticas de mayor extensión sin variar el área de filtrado, aumentando el número de orden difractados y asegurando que no exista solapamiento entre sus componentes espectrales.

La pupila en el sistema óptico de encriptación limita el contenido espectral de cada imagen codificada. Nótese que el plano de filtrado y el plano de la llave de seguridad en el sistema de encriptación son planos imagen. Por lo tanto, las frecuencias espectrales de las imágenes encriptadas pueden ser limitadas tanto en la región de filtrado como en la región de la llave de seguridad.

Debido a que cada imagen de entrada está adosada a una primera máscara de fase $e^{i\varphi_0(x,y)}$, la información en el plano de la llave de seguridad esta uniformemente distribuida en todo el plano. Además, aprovechando las características de redundancia al realizar una modulación aleatoria con la primera máscara de fase, es permisible reducir el tamaño de la pupila en el plano de la llave de seguridad. Esto reduce el diámetro de los órdenes difractados en el plano de filtrado. Los dos procesos son equivalentes y se pueden llevar a cabo de dos maneras. 1) Limitando la llave de codificación y obtener así órdenes más pequeños. 2) Realizar la codificación con toda la llave de encriptación y limitar con máscaras de menor tamaño los órdenes difractados.

Por la naturaleza aleatoria del proceso de encriptación, limitar cualquiera de los dos planos genera resultados con distribuciones de ruido del mismo orden sobre la imagen

recuperada y no existe mejora en la calidad al usar un método o el otro. Por lo tanto, se decide limitar en el plano de la llave de seguridad. Esta estrategia, si bien reduce el número de elementos de la llave de codificación, el sistema se mantiene seguro por la operación de multiplexado.

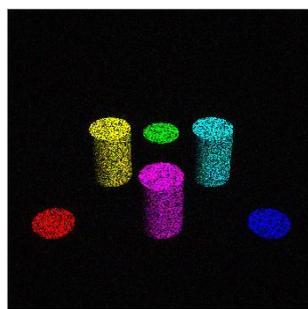
Para realizar la aplicación a escenas de mayor extensión, se usan diferentes tamaños de pupilas circulares en el plano de filtrado. La frecuencia de cada red de modulación es seleccionada tal que las componentes espectrales de cada imagen no se superpongan entre ellas en el plano de filtrado. De esta forma, el uso de diferentes tamaños de pupilas permite controlar la extensión de la película ubicando un número mayor de órdenes en la misma área de este plano. Este procedimiento permite recomponer una película de mayor longitud con el mismo sistema óptico.

El tamaño de la pupila determina la frecuencia de corte para el contenido espectral de la imagen de entrada, consecuentemente si se aumenta la extensión de una película los detalles del objeto se verán afectados en la recuperación de información. Este punto es evaluado en el siguiente ejemplo para dos objetos policromáticos de diferente complejidad.

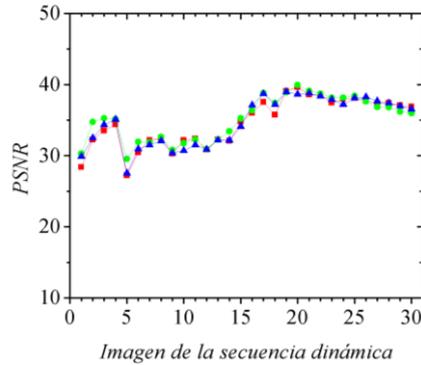
La primera escena dinámica posee pocos detalles y consiste de seis cilindros en movimiento, los cuales cambian su forma a medida que aumenta la longitud de la película. La película de mayor detalle consiste en un pájaro balanceándose hasta tomar agua un par de veces. En ambos casos, a medida que decrece el tamaño de la pupila, incrementa el grano de *speckle* que contribuye a la degradación de las imágenes recuperadas. Por otro lado, el mismo corte de frecuencias realizado por la disminución del diámetro de la pupila, impone una restricción sobre la calidad de las imágenes recuperadas limitando la extensión de la escena dinámica. Los diámetros de las pupilas en el plano de la llave de encriptación para lograr la extensión de 3 segundos, 4.8 segundos y 12.6 segundos son de ~ 5.70 mm, ~ 4.27 mm y ~ 2.85 mm, respectivamente. Se debe notar que para aumentar la extensión de una película y recuperarla exitosamente, se debe asegurar en la etapa de desencriptación que el tamaño de la máscara de filtrado sea variable, conservando los parámetros ópticos del sistema original. Si bien se debe aumentar el número de redes de modulación con diferente pitch para difractar un número mayor de órdenes en posiciones distintas del plano

de filtrado, no se presenta la necesidad de cambiar los parámetros ópticos del sistema en la etapa de recuperación.

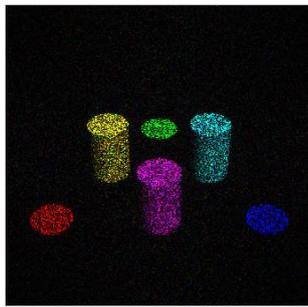
Las imágenes de la Figura 6.17 (a), (c) y (e) se han recuperado de tres películas de 3 segundos, 4.8 segundos y 12.6 segundos de duración.



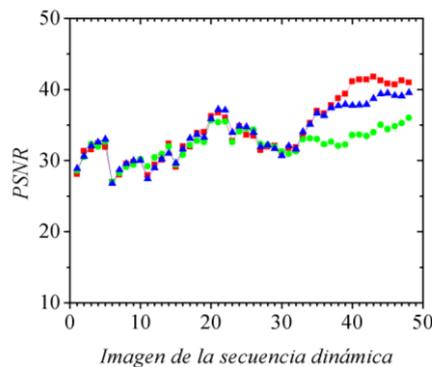
(a)



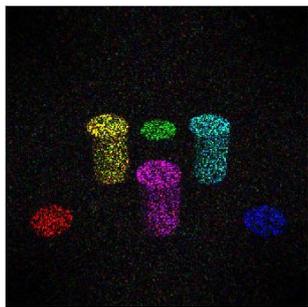
(b)



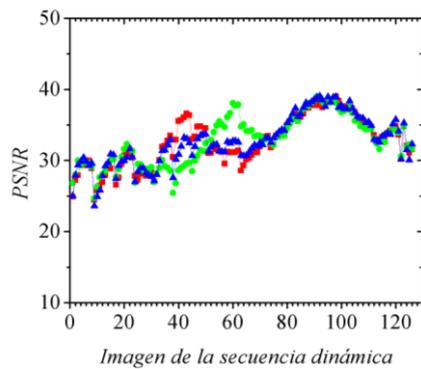
(c)



(d)



(e)



(f)

Figura 6.17: Calidad de las imágenes recuperadas en secuencias dinámicas policromáticas de diferente extensión. Las imágenes (a), (c) y (e) son descriptadas al utilizar la llave de seguridad correcta de escenas a color de 3 segundos, 4.8 segundos y 12.6 segundos de duración, respectivamente. Las curvas (b), (d) y (f) son el pico de la relación señal ruido en dB de las imágenes recuperadas de la secuencia dinámica a color de 3 segundos, 4.8 segundos y 12.6 segundos de duración, respectivamente.

Los valores de las curvas de *PSNR* de las Figuras 6.17 (b), (d) y (f) conservan su comportamiento pero decrecen en valor cuando la extensión de la película va aumentando y por lo tanto la calidad de las imágenes recuperadas disminuye. Esto es de esperarse ya que al recortar frecuencias en el plano de la llave de codificación se pierde información relevante del objeto en la reconstrucción y se adiciona ruido de *speckle*. Este comportamiento es corroborado con las imágenes recuperadas mostradas en las Figura 6.17 (a), (c) y (e). Por lo tanto, si se aumenta la extensión de la película encriptada, el precio a pagar es la pérdida de detalles en las imágenes recuperadas. La optimización de este procedimiento será una perspectiva para futuras contribuciones, teniendo como objetivo aumentar la extensión de la película conservando fijos los parámetros ópticos del sistema.

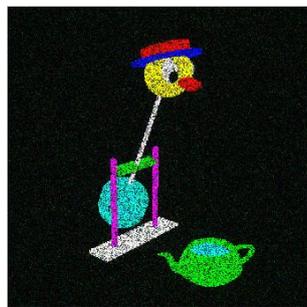
La pérdida de detalles en el objeto recuperado al aumentar la extensión de la película puede ser observada de una mejor forma al encriptar una secuencia donde el objeto tenga detalles más finos. La segunda escena consiste en un pájaro balanceándose una y otra vez. Los detalles como los ojos del pájaro, las líneas que definen el sombrero y la forma de la tetera se pierden a medida que se aumenta la extensión de la película. Al igual que en el ejemplo anterior se codificaron escenas de 3 segundos, 4.8 segundos y 12.6 segundos de duración, aplicando pupilas de diferentes tamaños en el plano de la llave de encriptación. Las pupilas fueron de diámetro ~ 5.70 mm, ~ 4.27 mm y ~ 2.85 mm, lográndose la extensión más larga con el diámetro de pupila más pequeño.

Las imágenes de la Figura 6.18 (a), (c) y (e) muestran una de las imágenes recuperadas de las tres películas del pájaro balanceándose de 3 segundos, 4.8 segundos y 12.6 segundos, respectivamente. Las curvas de las Figuras 6.18 (b), (d) y (f) muestran los valores de *PSNR* para cada una de estas imágenes.

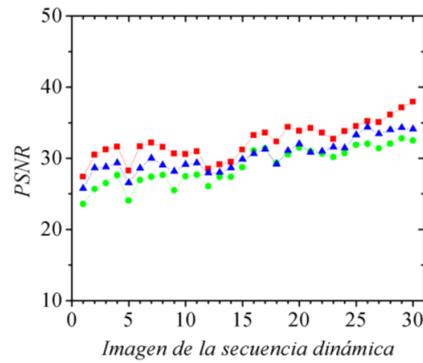
Se puede observar que el comportamiento de las curvas de *PSNR* de la Figura 6.18 es similar al comportamiento de las curvas de *PSNR* de la Figura 6.17. El mismo análisis de la dependencia de la calidad de la imagen en relación a la frecuencia de las redes aplica en este caso.

Al comparar estos dos conjuntos de curvas debería notarse que la calidad de las imágenes de los objetos de mayor detalle se ve más degradada al incrementar la longitud

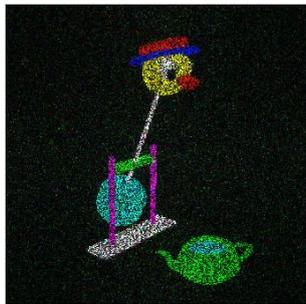
de las películas. Nótese como los valores de las curvas de $PSNR$ son menores en las gráficas de la Figura 6.18 en comparación las gráficas de la Figura 6.17.



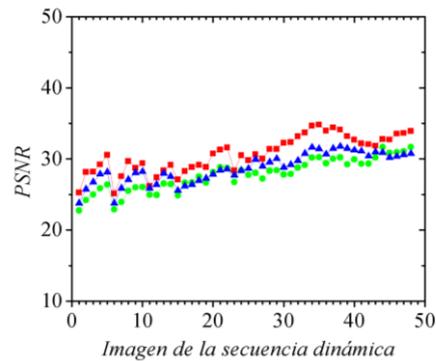
(a)



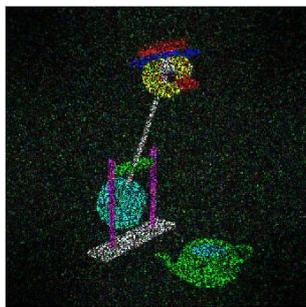
(d)



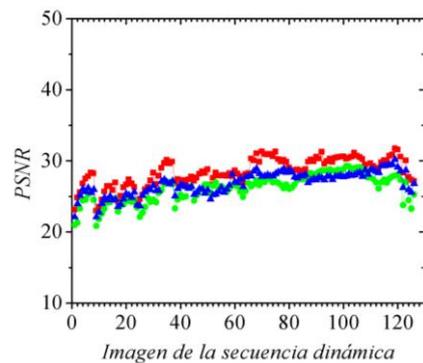
(b)



(e)



(c)



(f)

Figura 6.18: Calidad de las imágenes recuperadas en secuencias dinámicas policromáticas de diferente extensión. Las imágenes (a), (c) y (f) han sido recuperadas usando la llave de seguridad correcta y pertenecen a secuencias dinámicas de 3 segundos, 4.8 segundos y 12.6 segundos de duración, respectivamente. Las curvas (b), (d) y (f) son el pico de la relación señal ruido en dB de las imágenes recuperadas de la secuencia de 3 segundos, 4.8 segundos y 12.6 segundos de duración, respectivamente.

También se puede notar como los detalles de los ojos del pájaro y las líneas que definen la forma de la tetera prácticamente se han perdido en la Figura 6.18 (e), pero no ocurre en la imagen de la Figura 6.18 (a) donde se puede aún definir detalles de la escena. Por el contrario, al realizar esta misma comparación de las imágenes de la Figura 6.17 (a) y Figura 6.17 (e), los detalles gruesos de la imagen en la escena de los cilindros aún definen la escena en general y resulta una pérdida menor de calidad en las imágenes recuperadas al extenderse la longitud de la película.

Estas dos experiencias permiten concluir que el introducir una pupila que controle la extensión de la película es factible la información transmitida no es relevante en cuanto a la fidelidad de los detalles. Si esto no es posible, lo más probable es que se tengan que generar con la técnica propuesta conjuntos de multiplexados de secuencias de corta longitud para ampliar la información transmitida.

Más allá de la optimización del espacio del plano de filtrado y de la extensión de la duración de una escena dinámica, se debe señalar que indudablemente el avance significativo de la técnica de encriptación de eventos dinámicos radica en permitir multiplexar más volumen de información y recuperar con mejor calidad que un multiplexado convencionales de información encriptada. Se suprime la superposición de información en la descryptación y se elimina el uso de múltiples llaves de codificación. Esto es muy importante ya que en un canal de transmisión clásico se está optimizando la cantidad de llaves de seguridad que se requieren transmitir para recuperar la información con la misma calidad.

En la Figura 6.19 se muestran las curvas de *NRMSE* de las imágenes descryptadas de una escena policromática a partir de un multiplexado convencional y la técnica de encriptación de eventos dinámicos al usar la llave correcta de seguridad. Se puede observar que las curvas presentan un crecimiento en el *NRMSE* en las tres componentes de color a medida que aumentan el número de imágenes multiplexadas. Este caso corresponde a las imágenes recuperadas de un multiplexado convencional. Por el contrario, en Figura 6.19 (b) se muestra un *NRMSE* constante en las imágenes recuperadas a partir de la técnica de encriptación de eventos dinámicos.

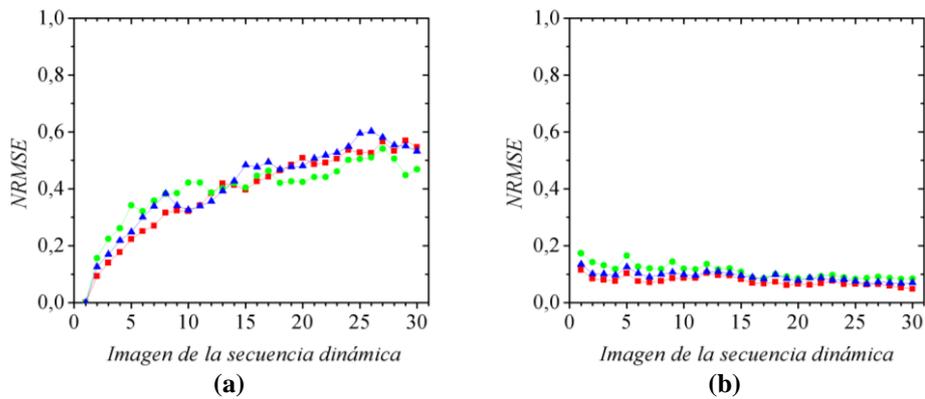


Figura 6.19: Curvas de $NRMSE$ de las imágenes recuperadas al usar (a) la técnica convencional de multiplexado y (b) la técnica de encriptación de eventos dinámicos.

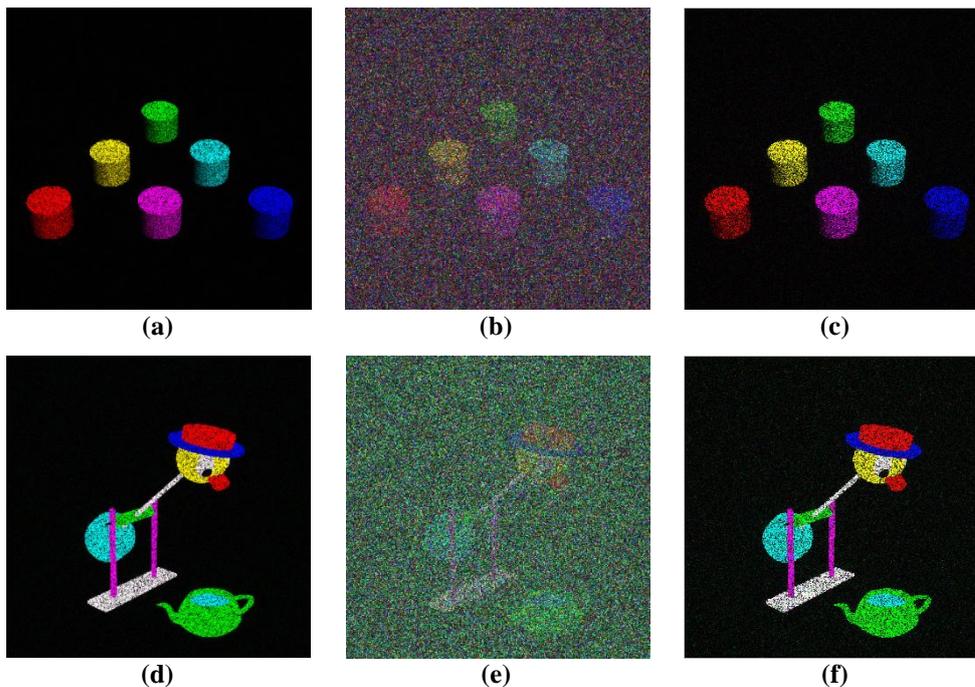


Figura 6.20: Comparación de imágenes recuperadas de los sistemas de encriptación (a) de doble máscara de fase en configuración $4f$, (b) multiplexado convencional de información y (c) técnica de encriptación de eventos dinámicos.

Por último, en la Figura 6.20 se muestra una comparación al recuperar una imagen de la secuencia dinámica en el sistema de codificación de doble máscara de fase en configuración $4f$, Figura 6.20 (a) y Figura 6.20 (d); al recuperar la misma imagen de un multiplexado de treinta imágenes usando la técnica de multiplexado convencional, Figura 6.20 (b) y Figura 6.20 (e); y al recuperar la misma imagen de un multiplexado de treinta

imágenes usando la técnica de encriptación de eventos dinámicos, Figura 6.20 (c) y Figura 6.20 (f).

En resumen, se ha presentado una aplicación de la técnica de encriptación de eventos dinámicos a secuencias dinámicas de color. La técnica se basa en aplicar la técnica de modulación theta a cada canal cromático de las imágenes de entrada que han sido encriptadas con una única llave de seguridad. A diferencia de otros métodos de procesamiento a color, cada canal cromático no se multiplexa en un único medio de registro. Esto permite que los canales de color se sincronicen simultáneamente durante el proceso de filtrado y etapa de decodificación realizando la composición del color y la reconstrucción de la escena en movimiento en tiempo real.

Esta técnica desarrollada es promisoria ya que aumenta la capacidad de multiplexado de imágenes encriptadas. También asegura la misma calidad de recuperación en las imágenes y evita la degradación debido a la superposición de información. Todas estas cualidades optimizan los procesos involucrados en un canal de información clásico. Por un lado, el emisor puede enviar mayores volúmenes de información teniendo la certeza que la información no resultara degradada como ocurre al usar la técnica de multiplexado convencional. Por otro lado, se optimiza la recuperación de la información según se ha demostrado en los análisis realizados. Esto es muy importante para el receptor ya que tiene la confianza de recibir la información requerida y de manera segura con altos grados de confidencialidad. Por último, el usuario final sólo necesita una única llave de seguridad y el multiplexado para recuperar toda la información. Gracias a esto, se reduce directamente la cantidad de datos requeridos para recuperar la información original ahorrando tiempos de transmisión, manejos de múltiples llaves, etc. Estas ventajas no las ofrecen los sistemas convencionales de encriptación.

6.4 Aplicación de la técnica de encriptación de eventos dinámicos a un proceso multiusuario

A continuación se presenta una última aplicación dirigida a procesos multiusuario que sigue la línea de encriptación de eventos dinámicos. Se propone la idea original de

multiplexar varias películas encriptadas y transmitir las a múltiples usuarios, donde cada película es decodificada exitosamente con una llave de seguridad distinta [6.8].

6.4.1 Descripción general

Como se expuso en el Capítulo 4, los procesos de encriptación que emplean operaciones de multiplexado exhiben un ruido inherente en la etapa de recuperación por la presencia del solapamiento de información. En estos procesos convencionales se emplea una llave para encriptar cada imagen, sin embargo el proceso de desencriptación revela la correcta recuperación de los datos encriptados pero degradados por el ruido debido a las imágenes incorrectamente desencriptadas. En principio, el usar diferentes llaves de seguridad que no estén correlacionadas entre sí hace posible multiplexar un gran número de imágenes encriptadas, sin embargo, el ruido reduce severamente el número de imágenes recuperadas que tienen una calidad aceptable.

La importancia del multiplexado recae en poder realizar el registro múltiple de datos y transmitirlos como un único elemento permitiendo que en la etapa de decodificación el frente de onda reconstruido contenga la información asociada a todos los datos encriptados.

Un modelo de un proceso de multiplexado ideal debería ser capaz de encriptar una gran cantidad de imágenes y poder recuperar cada una de ellas libre de ruido. Como se ha expuesto en las secciones anteriores, se ha propuesto la técnica de encriptación de eventos dinámicos, una nueva técnica de multiplexado, que elude el ruido debido al solapamiento de información. Este método ha permitido realizar aplicaciones en la encriptación de secuencias monocromáticas y policromáticas.

En esta sección se extiende su aplicación a un esquema para codificar y decodificar información incluyendo la posibilidad de transmitir diferentes escenas dinámicas que han sido codificadas con diferentes llaves de seguridad. Para recuperar exitosamente la información de una escena, el usuario debe tener el multiplexado y la llave de seguridad asignada para desencriptar cada escena de movimiento.

6.4.2 Descripción del método

Mediante la técnica de encriptación de eventos dinámicos se desarrolla la aplicación de transmitir información encriptada a múltiples usuarios. El esquema sigue el protocolo del sistema de codificación de doble máscara $4f$, la técnica de modulación theta y la técnica de multiplexado de imágenes encriptadas moduladas.

En esta aplicación multiusuario se emplean diferentes llaves de seguridad para codificar cada secuencia dinámica. A un conjunto de usuarios se le transmite en común la información multiplexada y a cada usuario en particular se le envía una llave diferente de decodificación. De esta manera, a partir de un multiplexado, los usuarios pueden descryptar una secuencia dinámica por cada llave de codificación. Al usuario se le podrá enviar otra llave de seguridad diferente a la primera para que pueda descryptar otra secuencia dinámica a partir del mismo multiplexado, si así lo requiere.

Para ejemplificar el proceso se emplean tres secuencias monocromáticas de igual extensión. Surge del análisis de la sección anterior, que se pueden codificar sin dificultades 30 imágenes en un multiplexado y recuperarlas con una calidad uniforme. En este sentido, empleando la encriptación de eventos dinámicos se codifican tres secuencias dinámicas, cada una constituida de 10 imágenes.

La primera etapa de esta técnica es el proceso de encriptación y se esquematiza en la Figura 6.21. Cada una de las imágenes $O_{a_1}(x, y) \dots O_{a_k}(x, y)$, $O_{b_1}(x, y) \dots O_{b_l}(x, y)$ y $O_{c_1}(x, y) \dots O_{c_n}(x, y)$, de las tres secuencias dinámicas es multiplicada por una primera máscara de fase $e^{i\varphi_0(x_f, y_f)}$. La lente L_1 realiza una primera transformada de Fourier y el espectro resultante es multiplicado por cada llave de seguridad correspondiente. Mediante la llave $e^{i\varphi_a(x_f, y_f)}$, $e^{i\varphi_b(x_f, y_f)}$, $e^{i\varphi_c(x_f, y_f)}$, se codifican las imágenes correspondientes a los objetos $O_a(x, y)$, $O_b(x, y)$ y $O_c(x, y)$, respectivamente. Finalmente se realiza una última transformada de Fourier usando la lente L_2 para encontrar las imágenes encriptadas $E_{a_1}(x_0, y_0) \dots E_{a_k}(x_0, y_0)$, $E_{b_1}(x_0, y_0) \dots E_{b_l}(x_0, y_0)$, $E_{c_1}(x_0, y_0) \dots E_{c_n}(x_0, y_0)$.

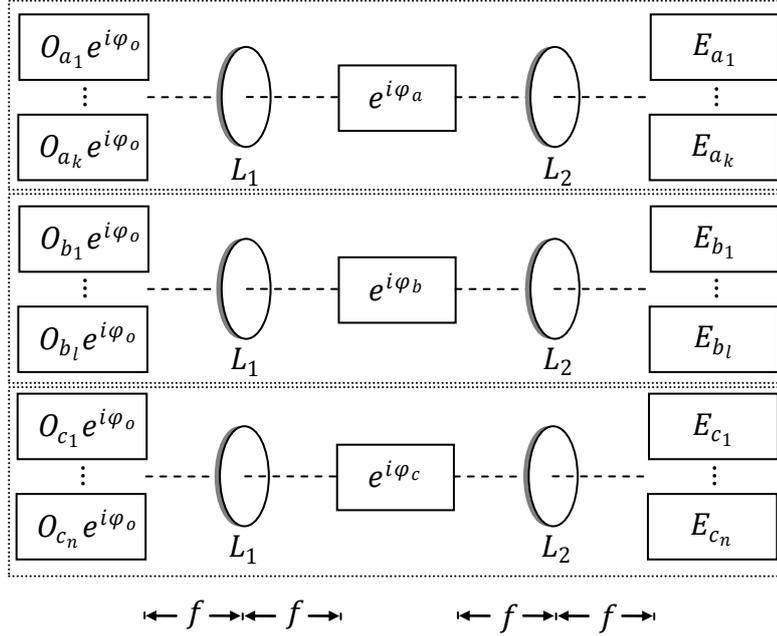


Figura 6.21: Esquema de aplicación multiusuario. Etapa de encriptación. L_1 y L_2 son lentes de distancia focal f , $O_{a_1} \dots O_{a_k}$, $O_{b_1} \dots O_{b_l}$ y $O_{c_1} \dots O_{c_n}$ son imágenes de las tres secuencias (a , b y c), $e^{i\varphi_0}$ es la primera máscara de fase, $e^{i\varphi_a}$, $e^{i\varphi_b}$ y $e^{i\varphi_c}$ son las llaves de seguridad para codificar cada película y $E_{a_1} \dots E_{a_k}$, $E_{b_1} \dots E_{b_l}$ y $E_{c_1} \dots E_{c_n}$ son las imágenes encriptadas de las tres secuencias dinámicas.

Después de este proceso, todas las imágenes codificadas son moduladas por redes periódicas de amplitud de diferente pitch para luego ser multiplexadas y realizar la operación de conjugación de fase. El patrón resultante de estas tres operaciones que se le envía a los múltiples usuarios se expresa:

$$M^*(x_0, y_0) = \left[\sum_{S=a,b,c} \sum_{m=1}^p E_{S_m}(x_0, y_0) G_{S_m}(x_0, y_0; u_m, v_m) \right]^* \quad (6.7)$$

donde p es el número de imágenes que constituyen cada una de la secuencia dinámica S . Por lo tanto, a cada uno de los tres usuarios se les envía la cantidad $M^*(x_0, y_0)$ y una única llave de seguridad diferente, $e^{i\varphi_a(x_f, y_f)}$, $e^{i\varphi_b(x_f, y_f)}$, $e^{i\varphi_c(x_f, y_f)}$, respectivamente, tal que cada usuario sólo descrypta su secuencia dinámica asignada.

En la etapa de descryptación, el plano de filtrado exhibe parejas de orden difractados que son filtrados teniendo en cuenta la etapa de sincronización para cada película. Esta vez se coloca atención a la secuencia de filtrado. Esta toma relevancia

presentándose como un parámetro adicional de encriptación. Si no se conoce la secuencia adecuada, la película de cada usuario no puede ser reconstruida en un orden cronológico correcto. Consecuentemente, al usuario se le debe enviar por otro canal la secuencia que tiene que introducir en el proceso de desencriptación. En los ejemplos anteriores este parámetros se consideraba implícito en la etapa de recuperación al ser un único usuario, ahora, cada usuario tendrá acceso a todo el plano de filtrado donde existe información que no puede recuperar con su llave de acceso. Por lo tanto, para la adecuada selección de información es relevante esta secuencia de filtrado. Se aumentan así los grados de libertad del sistema para recuperar la información adecuadamente.

La etapa final para recuperar la información es esquematizada en la Figura 6.22. Las imágenes encriptadas de todas las secuencias dinámicas son desencriptadas secuencialmente según la sincronización que debe introducir cada usuario para recuperar el orden cronológico natural de la película transmitida. En general, la imagen encriptada es la entrada del procesador $4f$. La lente L_1 realiza una primera transformada de Fourier, el espectro resultante de cada imagen es multiplicada con la llave de seguridad asignada a cada usuario y finalmente la lente L_2 produce la imagen desencriptada.

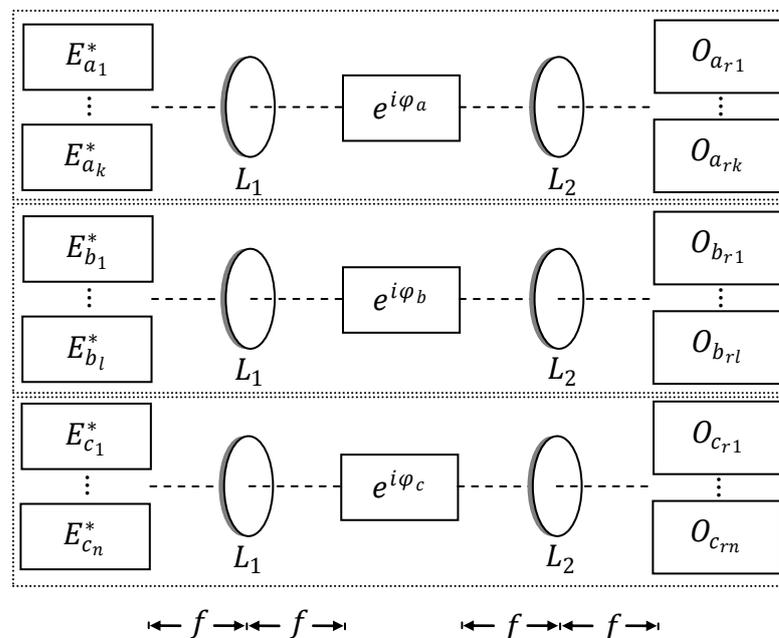


Figura 6.22: Esquema de aplicación multiusuario. Etapa de desencriptación. L_1 y L_2 son lentes de distancia focal f , $E_{a_1}^* \dots E_{a_k}^*$, $E_{b_1}^* \dots E_{b_l}^*$ y $E_{c_1}^* \dots E_{c_n}^*$ son las imágenes encriptadas recuperadas de la secuencia de filtrado. $(a, b$ y $c)$, $e^{i\varphi_a}$, $e^{i\varphi_b}$ y $e^{i\varphi_c}$ son las llaves de seguridad de las tres escenas.

A continuación se presenta el análisis de los resultados obtenidos de la aplicación multiusuario apelando a las métricas de *PSNR* y *RMSE* para evaluar la calidad de las tres secuencias recuperadas.

6.4.3 Discusión de resultados

Para mostrar la validez de la propuesta de la aplicación de la técnica de encriptación de eventos dinámicos a un sistema multiusuario se considera un ejemplo donde participan tres personas autorizadas. El procedimiento descrito en la anterior sección es utilizado para encriptar y multiplexar tres películas en el mismo medio de registro. Cada película es codificada usando tres llaves de seguridad diferentes, $e^{i\varphi_a}$, $e^{i\varphi_b}$ y $e^{i\varphi_c}$, de esta manera se generan accesos a la información por canales independientes.

Cada película está constituida por 10 imágenes las cuales están sincronizadas a seis marcos por segundo, es decir, cada película tiene 1.67 segundos de duración. Los parámetros de las redes periódicas de amplitud empleadas se especifican en la Tabla 6.3. El tamaño de las imágenes tienen un área $\sim 6.97 \text{ mm}^2$, se uso una fuente de iluminación de longitud de onda de 632.8 nm y las lentes involucradas en el sistema óptico virtual en las diferentes etapas tienen una distancia focal de 150 mm. De esta manera, con las redes empleadas para la modulación, el plano de filtrado tiene un área de $\sim 56 \times 56 \text{ mm}^2$, finalmente, los órdenes difractados son filtrados con pupilas de diámetro $\sim 6.97 \text{ mm}$. Nuevamente se enfatiza que el *speckle* está presente en todo el proceso realizado con sistemas ópticos virtuales. Para estos parámetros ópticos, el orden más alejado del orden central se encuentra a $\sim 34.5 \text{ mm}$ al usar la red de menor pitch. El orden difractado más cercano obtenido al usar la red de mayor pitch se encuentra a $\sim 11 \text{ mm}$ del orden central.

| <i>Red</i> | <i>Pitch (μm)</i> | <i>Líneas/mm</i> |
|------------|---|------------------|
| 1 | 2.8 | 364 |
| 2 | 3.2 | 315 |
| 3 | 3.6 | 280 |
| 4 | 3.9 | 260 |
| 5 | 4.7 | 214 |
| 6 | 5.3 | 187 |
| 7 | 6.4 | 156 |
| 8 | 8.6 | 116 |

Tabla 6.3: Parámetros ópticos de las redes periódicas de amplitud usadas para encriptar 3 escenas dinámicas, de 10 imágenes monocromáticas.

A los tres usuarios se les debe enviar el mismo patrón multiplexado de imágenes encriptadas moduladas y la correspondiente llave de seguridad para poder recuperar las imágenes de una determinada secuencia en la etapa de decodificación. A la secuencia de sincronización se le puede dar relevancia y generar así secuencias sofisticadas de filtrados. También pueden ser secuencias predeterminadas las cuales el usuario puede testear en la estación de decodificación, como si se tratara de canales de video en un televisor cuando se conecta un decodificador.

En la Figura 6.23 se muestra el plano de filtrado obtenido al aplicarle una transformada de Fourier al complejo conjugado del multiplexado de imágenes encriptadas moduladas de las tres secuencias dinámicas. Nótese como está optimizado el espacio en el plano de filtrado en comparación a la disposición de círculos concéntricos mostrados en la Figura 6.3. Y obsérvese como las frecuencias del orden central afectarían a los órdenes adyacentes si no se dejara un espacio prudente entre estos y el orden central.

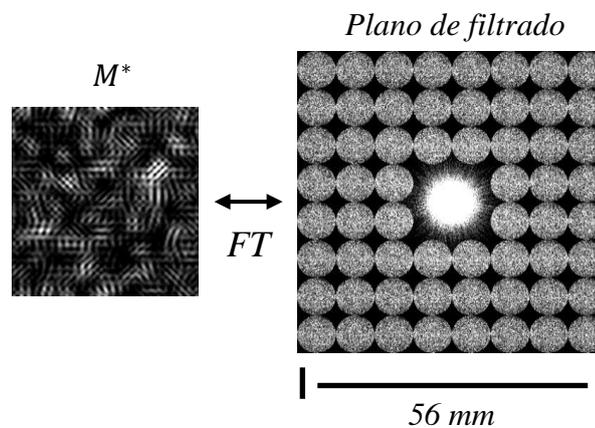


Figura 6.23: Etapa de Filtrado y sincronización. M es el multiplexado que se le envía a los tres usuarios. FT es la transformada de Fourier. Se puede observar que escoger aleatoriamente los órdenes en el plano de filtrado recuperaría una escena de movimiento en un orden temporal incorrecto.

Se concluye que al sistema se le adiciona un grado de seguridad al introducir el parámetro de la secuencia de filtrado. El número total de combinaciones posibles para formar una secuencia dinámica de 10 imágenes a partir del plano de filtrado de 30 parejas de órdenes difractados es del orden de $\sim 1 \times 10^{14}$, un número relativamente importante. Si se tiene en cuenta el orden de las 30 imágenes en una única secuencia, existen $\sim 2.65 \times 10^{32}$ formas de organizar la escena dinámica.

En esta aplicación, si un usuario desea acceder a otra información que contiene el multiplexado deberá requerir la llave de codificación y la secuencia de filtrado que permite recuperar la información original. Por el contrario, si la información no se encuentra en el paquete multiplexado, el usuario podrá conservar la llave de codificación así como el orden de la secuencia y se le transmitirá un nuevo multiplexado que contiene la información requerida.

Al tener en cuenta estas consideraciones, el usuario logra recuperar exitosamente una secuencia dinámica con la correspondiente llave de seguridad. La Figura 6.24 muestra tres imágenes diferentes las cuales corresponden a una de las imágenes de cada escena descryptada por cada usuario (ver Apéndice C.4). Por otro lado, si se emplea una llave de seguridad diferente a las llaves de seguridad autorizadas, se recupera sólo ruido en todo el proceso de descryptación, ya que todas las imágenes de las tres escenas se mantienen encriptadas. Esto se puede observar en la Figura 6.25, donde un usuario ha tratado de recuperar información de un multiplexado original con una llave de seguridad incorrecta.

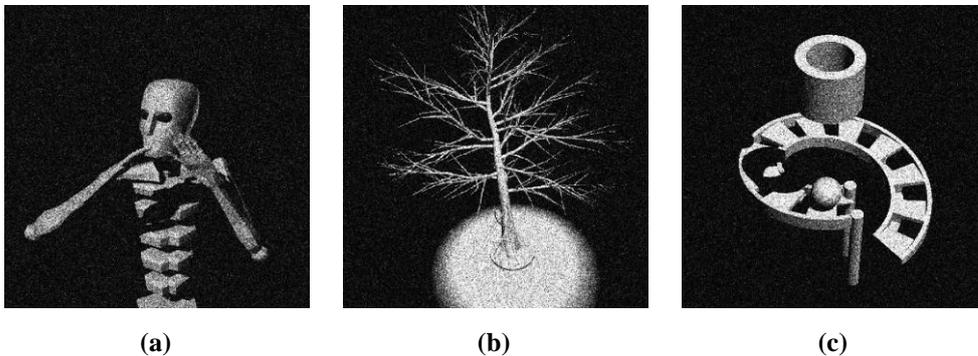


Figura 6.24: Imágenes descryptadas al utilizar la correcta llave de seguridad. Secuencia dinámica recuperada por (a) el primer usuario, (b) el segundo usuario y (c) el tercer usuario.

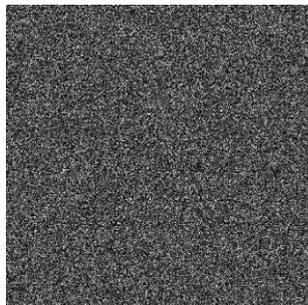


Figura 6.25: Imagen descryptada al usar una llave de seguridad incorrecta. La escena resultante es un conjunto de patrones de *speckle* que no están correlacionados.

Ahora, es importante evaluar la calidad de las tres secuencias recuperadas a partir de un multiplexado de imágenes encriptadas moduladas. Es de esperarse que el comportamiento general de las curvas de *PSNR* repita el de las curvas de *PSNR* de la experiencia en color y de la experiencia monocromática discutida en las secciones anteriores. También aquí se verifica que las imágenes recuperadas al usar la técnica de encriptación de eventos dinámicos tienen poca degradación.

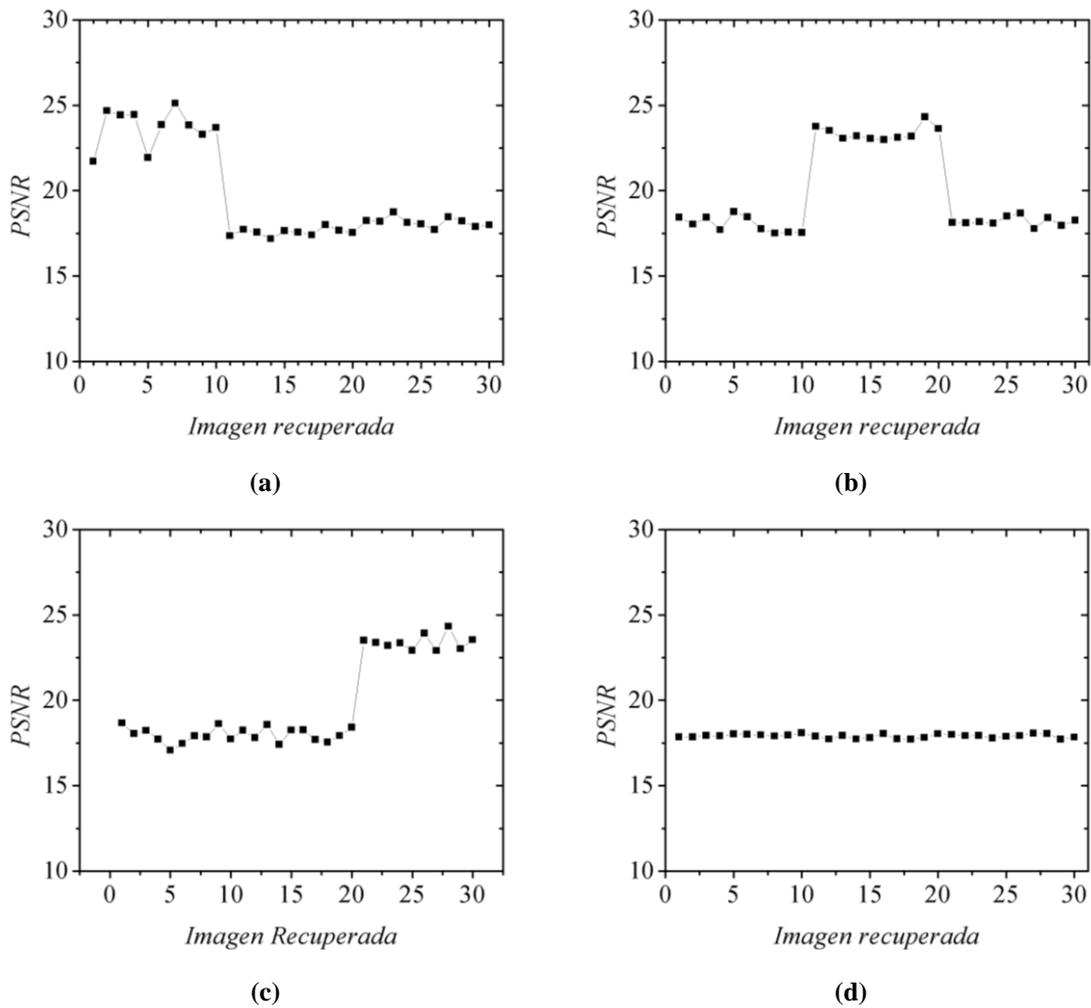


Figura 6.26: Pico de la relación señal-ruido de las imágenes recuperadas por diferentes usuarios al usar sus llaves de seguridad asignadas. A partir del multiplexado que es igual para cuatro usuarios, tres de ellos tienen una llave de seguridad correcta que decodifica una escena dinámica. El cuarto usuario ha usado una llave de seguridad incorrecta con la cual no recupera ninguna escena.

Por otro lado, de esta experiencia se puede evaluar el comportamiento de la etapa de decodificación cuando los usuarios tratan de recuperar con la única llave de seguridad asignada, todas las secuencias encriptadas y multiplexadas. En la Figura 6.26 se muestra

las curvas de la métrica de *PSNR* de las imágenes recuperadas en la aplicación multiusuario. En la curva de la Figura 6.26 (a), el primer usuario ha tratado de desencriptar todas las imágenes del multiplexado. La curva de *PSNR* revela que sólo ha conseguido recuperar las primeras 10 imágenes asignadas a esa llave de seguridad, mientras que las 20 imágenes restantes no han sido recuperadas manteniéndose encriptadas. De la misma manera, en las curvas de las Figuras 6.26 (b) y 6.26 (c), se puede observar como el segundo y el tercer usuario recuperan únicamente las 10 imágenes de las secuencias a las que tiene acceso su respectiva llave de seguridad. Por el contrario, la curva de la Figura 6.26 (d) revela que un usuario ha empleado una llave de seguridad incorrecta con la cual no recupera ningún tipo de información, mostrando las curvas de *PSNR* valores muy bajos.

Estos resultados comprueban que la técnica de encriptación de eventos dinámicos permite generar canales de acceso a partir de un único multiplexado. Con esta técnica se logra recuperar la información encriptada de una secuencia dinámica sin degradación y con valores muy aceptables de *PSNR* indicando medidas de calidad permisible en las imágenes recuperadas.

6.5 Bibliografía

- [6.1] A. Alfalou, A. Mansour, “All-optical video-image encryption with enforced security level using independent component analysis,” *J. Opt. A. Pure Appl. Opt.* **9**, 787–796 (2007).
- [6.2] U. Schnars, W. Jueptner. *Digital Holography, Digital hologram recording, Numerical reconstructions, and related techniques*. Springer Science+Business Media Inc. (2005). pp. 41-69.
- [6.3] G. S. Landsberg, *Óptica*, Mir, Moscú (1983) Tomo1, p.112.
- [6.4] J. W. Goodman. Statistical properties of laser *speckle* patterns p 35-42 en J.C. Dainty. *Laser speckle and related phenomena*, Springer-Verlag Berlin Heidelberg New York 1975.
- [6.5] L Chen, D. Zhao, “Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms.” *Opt Exp.* **14**, 8552–8560 (2006).

- [6.6] L. Chen, D. Zhao, “Color information processing (coding and synthesis) with fractional Fourier transforms and digital holography,” *Opt Exp.* 15, 16080–16089 (2007).
- [6.7] M. Joshi, Chandrashakher, K. Singh, “Color image encryption and decryption using fractional Fourier transform,” *Opt. Commun.* 279, 35–42 (2007).
- [6.8] F. Mosso, M. Tebaldi, J. Barrera, N. Bolognini, R. Torroba, “Multi-user multiplexed scheme for decoding modulated-encoded sequential information”, *Proc. SPIE* 8011, 801173 (2011);<http://dx.doi.org/10.1117/12.902124>

Capítulo 7

Generación de llaves de seguridad para técnicas de codificación óptica

7.1 Introducción

A lo largo de este trabajo se ha enfatizado que gracias a la inherente característica de los procesadores ópticos para manejar información en paralelo es posible procesar y encriptar ópticamente grandes flujos de datos. Esto permite almacenar o transmitir información de manera segura brindando acceso únicamente a personas autorizadas [7.1], [7.2]. Esta tarea es realizada eficientemente por las arquitecturas de encriptación óptica mostradas en el Capítulo 2. La mayoría de estas arquitecturas cumplen con tres criterios básicos necesarios para ser un sistema de encriptación eficiente, seguro y accesible para el usuario final. 1) Las funciones que definen las llaves de seguridad deben ser difíciles de encontrar. 2) Los datos encriptados y transmitidos deben ser manipulables para comunicaciones en internet. 3) El proceso de desencriptación debe ser relativamente sencillo para los usuarios autorizados que tengan las llaves correctas de decodificación.

Estas técnicas de encriptación óptica basan su efectividad en el uso de funciones que definen las llaves de codificación. Estas interactúan y transforman la información a un formato ilegible para que pueda ser transmitida de manera segura. Las máscaras de fase empleadas en las técnicas de encriptación óptica, pueden ser creadas a partir de difusores aleatorios, por ejemplo para formar un patrón de *speckle* que puede ser usado como llave de seguridad [7.3]. Se mencionó en la Sección 3.3.4 que un difusor aleatorio puede ser

considerado como un conjunto de elementos dispersores con distribuciones aleatorias de posición, forma y tamaño que introducen cambios aleatorios de fases (distribuidas uniformemente entre 0 y 2π) en la luz. Este elemento que se define como la máscara de seguridad, es el elemento principal que debe tener el usuario para recuperar la información original.

En los últimos años se han propuesto diferentes técnicas para codificar información. Para constituir llaves de seguridad, se ha recurrido a variaciones de los parámetros ópticos de las arquitecturas de encriptación (polarización, longitud de onda, distancias de propagación, modificación espacial de la llave de codificación, etc.). Estas variaciones permiten reforzar la seguridad de los sistemas de codificación aumentando los grados de libertad en el proceso de recuperación facilitando la implementación de técnicas de multiplexado de información encriptada [7.4]-[7.13].

Por otro lado, también se ha centrado la atención en el difusor aleatorio. Se han reportado contribuciones donde se logra generar máscaras de fase por diferentes métodos. Por ejemplo, se ha propuesto una técnica de cifrado donde la llave de encriptación es creada por un generador de números pseudoaleatorios [7.14]-[7.16]. Otra propuesta consiste en generar llaves de seguridad a partir de sistemas dinámicos en régimen caótico, que en conjunción con un sistema de sincronización permite modificarla a una frecuencia muy alta, dificultando el acceso a la información por el corto tiempo de vida de la máscara de codificación [7.17]. En otra contribución, se implementó un método óptico para generar secuencias de números pseudoaleatorios realizando transformaciones geométricas [7.18] sobre una imagen fuente [7.19]. Cada distribución pseudoaleatoria fue empleada para codificar digitalmente un mensaje por medio de una suma modular de orden n . El proceso de decodificación del mensaje original consiste en una resta modular de orden n entre el mensaje codificado y la imagen pseudoaleatoria. La ventaja de la suma modular es que produce un conjunto de valores en un rango determinado, además no es posible obtener de forma directa los números que fueron sumados. Empleando el teorema de Bézout [7.20] es posible encontrar un conjunto de ecuaciones lineales que permiten decodificar el mensaje cuando las ecuaciones sean resueltas. Sin embargo, se presenta una combinatoria de

ecuaciones diferenciales para cada uno de los píxeles, que dificulta severamente su resolución.

Todas estas contribuciones buscan establecer protocolos de codificación que brinden protección a la información transmitida al usuario final.

Estrictamente hablando, las máscaras de codificación generadas por difusores aleatorios no pueden ser duplicadas fielmente debido a que el mismo proceso de duplicación es fuente de ruido. Para realizar una réplica fidedigna de la máscara de fase, el usuario debe poseer el difusor y el sistema óptico bajo las mismas condiciones experimentales. Esto se asemeja a tratar de replicar una distribución de *speckle* en dos ambientes controlados diferentes [7.21], es muy difícil de conseguir. Por otro lado, si las llaves de codificación son superficies rugosas tangibles, como por ejemplo vidrios esmerilados, necesariamente al usuario se le debe transmitir físicamente la llave de encriptación. Esto hace ineficiente los procesos de decodificación hablando en términos de practicidad. Resulta oneroso transmitir grandes volúmenes de datos encriptados si cada información codificada tiene asociada por lo menos una llave física de encriptación.

Estos motivos tornan conveniente que las llaves de codificación sean manipuladas en un formato digital. Adicionalmente, esto permite usar un sistema opto-electrónico para su despliegue en un sistema analógico. Las tecnologías de moduladores espaciales de luz SLM [7.22] han permitido realizar grandes avances en la óptica. Las aplicaciones con estos dispositivos utilizan la rápida velocidad de reconfiguración para controlar la amplitud, fase y polarización de un campo incidente. Este proceso es realizado únicamente al desarrollar secuencias programables en el SLM [7.23]-[7.26]. En la encriptación óptica, esta tecnología permite desplegar una y otra vez una determinada distribución aleatoria de fase por medio de una interfaz A/D (análogo/digital). Esto permite controlar características de la luz por medio de comandos digitales. Si bien los SLM representan una ventaja en los procesos de encriptación también representan una herramienta para vulnerar la seguridad del sistema. Por ejemplo, se podría usar un SLM para probar llaves de fase recuperadas de algoritmos heurísticos [7.27]. De todas formas es un elemento opto-electrónico primordial para avanzar en las diversas aplicaciones de procesamiento óptico de información.

La propuesta más atractiva, de las mencionadas anteriormente concernientes a la manipulación de las máscaras de fase, es la generación óptica de secuencias de números pseudoaleatorios [7.18]. Sin embargo, realizar un montaje óptico para realizarlos experimentalmente en cada estación de decodificación aumentaría considerablemente los costos del sistema, sin mencionar lo impráctico que resultaría para el usuario final su manipulación. Una alternativa es usufructuar y optimizar esta técnica realizando su implementación digital.

Los avances originales mostrados en este capítulo muestran la optimización de la implementación puramente digital de la técnica de generación de números pseudoaleatorios por métodos ópticos usando transformaciones geométricas. Esta herramienta desarrollada permite generar imágenes pseudoaleatorias regidas por los parámetros de las transformaciones afines aplicadas. Estas imágenes son convertidas en máscaras de fase y pueden ser usadas como llaves de seguridad en un proceso de codificación de cualquier sistema de encriptación y pueden ser desplegadas en un SLM teniendo presente su rango de funcionamiento. Esto último es posible debido a que el proceso propuesto emplea una suma modular de orden n controlable para generar secuencia que tengan cualquier rango de niveles de gris.

Por otro lado, al usar un SOV de encriptación $4f$ y la técnica de generación de llaves de seguridad usando transformaciones afines, se desarrolla un protocolo de codificación que no transmite directamente la llave de encriptación al usuario final como se hace regularmente. El protocolo permite que el mismo usuario pueda generar su llave de seguridad directamente en la estación de descryptación. Se optimiza así la seguridad en los métodos actuales de transmisión de información encriptada. Una ventaja adicional de esta estrategia es la reducción en el tamaño de los elementos necesarios para recuperar la información original, lo que representa un proceso de transmisión más eficiente.

En el Capítulo 5 se desarrolló la técnica de encriptación de eventos dinámicos que permite encriptar múltiples datos y recuperar la imagen con la misma calidad mediante una única llave de codificación, sin la necesidad de usar múltiples llaves. Se recuperan así múltiples datos sin la influencia del solapamiento de información. Se observó en la

aplicación multiusuario que usar diferentes llaves de codificación genera niveles de acceso a la información. En este sentido, la técnica que se propone en este capítulo es aplicable a la desarrollada en el Capítulo 5. Simplemente donde se emplee un difusor aleatorio, se puede utilizar una imagen pseudoaleatoria obtenida con la técnica propuesta. Los resultados aquí mostrados se limitan al uso de la técnica a un SOV de encriptación 4f.

El presente capítulo se avoca a la solución de dos inconvenientes presentes en el proceso de transmisión de información encriptada. 1) transmitir la llave de seguridad por un único canal hace vulnerable al sistema ante posibles intrusos. 2) el uso de diferentes llaves de seguridad para codificar cada objeto viene acompañado de un aumento en el tamaño de los elementos necesarios para recuperar la información. Presentar una solución eficiente a estos problemas optimiza significativamente el proceso de transmisión en un canal de información clásico.

Inicialmente, en la Sección 7.2 se presentan las transformaciones geométricas en coordenadas homogéneas desde el punto de vista del procesamiento de imágenes. Posteriormente, en la Sección 7.3 se expone la representación matricial de la transformación de traslación, reflexión, rotación, contracción o escalamiento y *shearing*. En la Sección 7.4 se explica el proceso de generación de imágenes pseudoaleatorias al emplear transformaciones afines (PGI_{at}). En la Sección 7.5 se realiza una breve discusión de la aleatoriedad de las imágenes generadas en el PGI_{at} . En la Sección 7.6 se muestra la aplicación de estas imágenes como llaves de seguridad en un SOV de encriptación 4f. Finalmente, en la Sección 7.7 se muestran las ventajas adicionales que el nuevo protocolo desarrollado para recuperar la información original presenta sobre los actuales.

7.2 Transformaciones geométricas en coordenadas homogéneas

En esta sección se presentan los fundamentos básicos de las transformaciones aplicadas a una imagen para generar secuencias pseudoaleatorias. Una transformación lineal es una operación que se le realiza a un elemento de un sub-espacio para transformarlo en un elemento de otro sub-espacio. En ocasiones los vectores son fácilmente interpretados

dentro de un determinado contexto gráfico, otras veces es necesario transformar los vectores para manipularlos más fácilmente.

Las transformaciones lineales junto a las transformaciones afines y las transformaciones proyectivas son ampliamente usadas en diferentes campos de la ciencia e ingeniería, por ejemplo en robótica [7.28]-[7.29], en visión por ordenador [7.30], etc. Aquí sólo se trabaja únicamente con transformaciones lineales o afines. Las transformaciones proyectivas son más complejas que las dos primeras y por lo tanto no se emplearán para las aplicaciones subsecuentes.

En el área del procesamiento de imágenes, las transformaciones lineales modifican la forma y el tamaño de una imagen aplicando diferentes tipos de transformaciones sobre la base vectorial en la que se encuentre. Las transformaciones lineales se caracterizan principalmente por mantener el origen de coordenadas en un punto fijo del plano, preservan las rectas, conservan el paralelismo y las cónicas presentes en la imagen. Algunos ejemplos de transformaciones lineales son las rotaciones, contracciones, dilataciones, reflexiones y homotecias. Al aplicarle una transformación lineal a una imagen los vectores de su base se modifican y reubican los puntos de la imagen (píxeles) según las componentes del vector transformado. La Figura 7.1 (a) muestra una grilla con vectores de base en color rojo y la Figura 7.1 (b) muestra una transformación lineal de rotación cuyos vectores de base transformados están en color celeste

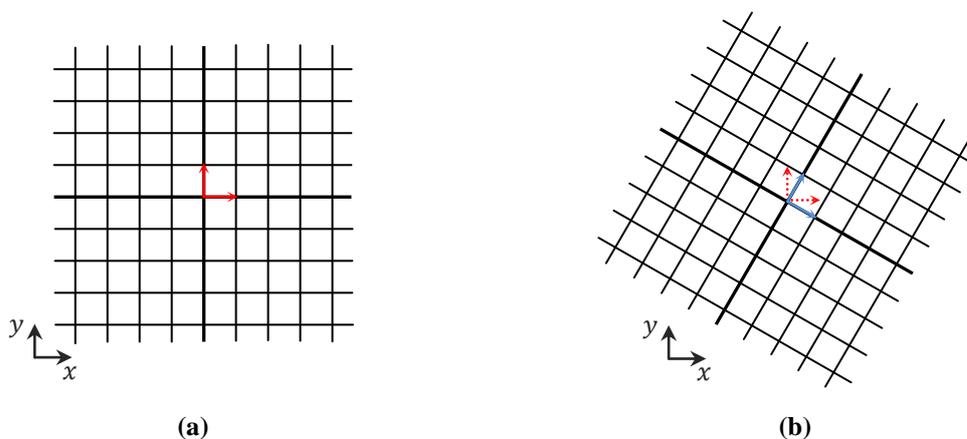


Figura 7.1: Transformaciones lineales. (a) Grilla cuadrada con vectores de base en color rojo y (b) rotación de la grilla cuadrada mostrando los vectores de la base transformados en color celeste.

Del mismo modo, las transformaciones afines preservan las rectas, conservan el paralelismo y las cónicas presentes en una imagen, sin embargo, generalmente el origen de coordenadas es desplazado después de la transformación lineal. Ejemplos de transformaciones afines son las rotaciones, contracciones dilataciones, reflexiones y homotecias, acompañadas de una traslación. La Figura 7.2 (a) muestra una grilla con vectores de base en color rojo y la Figura 7.2 (b) muestra una transformación afín compuesta de una rotación una contracción y una traslación. Se puede observar como la grilla cuadrada en la Figura 7.2 (b) es más pequeña y ha sido trasladada de su origen de coordenadas.

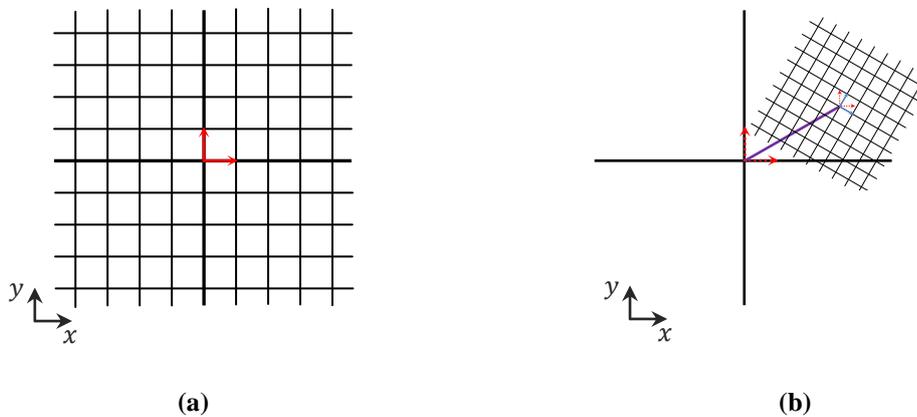


Figura 7.2: Transformaciones afines. (a) Grilla cuadrada con vectores de base con flechas de color rojo, (b) transformación afín de (a) compuesta de una rotación, una contracción y una traslación.

El vector desde el origen a un punto transformado (x, y) puede ser representado en el espacio por medio de coordenadas homogéneas de la forma (kx, ky, k) , para cualquier k distinto de cero [7.31]. Consecuentemente, un punto puede tener infinitas representaciones en estas coordenadas. Por ejemplo, el punto $(5,4)$ puede ser representado en coordenadas homogéneas como $(5,4,1)$, $(10,8,2)$, $(5/2,2,1/2)$, $(15,12,3)$, etc. En otras palabras, un punto (kx, ky, k) en coordenadas homogéneas representa al punto $(x/k, y/k)$. La convención que será usada para realizar las aplicaciones en este capítulo es $k = 1$.

Por lo tanto, una transformación lineal de un vector $(u, v, 1)$ puede ser expresado de la siguiente manera:

$$(x, y, 1) = (u, v, 1)A \quad (7.1)$$

donde $(x, y, 1)$ son las coordenadas homogéneas transformadas y \mathbf{A} es un operador que actúa sobre el vector $(u, v, 1)$. Debido a la forma lineal de las transformaciones, \mathbf{A} se puede expresar convenientemente en forma matricial como:

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & 0 \\ a_{21} & a_{22} & 0 \\ a_{31} & a_{32} & 1 \end{pmatrix} \quad (7.2)$$

así, la Ecuación (7.1) puede ser escrita como:

$$(x, y, 1) = (u, v, 1) \begin{pmatrix} a_{11} & a_{12} & 0 \\ a_{21} & a_{22} & 0 \\ a_{31} & a_{32} & 1 \end{pmatrix} \quad (7.3)$$

La aplicación repetitiva en una transformación compuesta de varias transformaciones lineales será el producto de los operadores de cada transformación individual las cuales obedecen al algebra matricial.

7.3 Representación matricial de transformaciones afines

Las transformaciones afines pueden ser representadas mediante operadores que actúan sobre los vectores de una base para transformar una imagen de entrada. A continuación se define la representación matricial de las transformaciones de traslación, reflexión, rotación, contracción y *shearing*.

7.3.1 Transformación de traslación

La traslación es una transformación rígida o isométrica congruente con la forma original de la imagen. Esta es la que combinada con otras transformaciones lineales o por sí misma, forman una transformación afín. El operador de traslación \mathbf{T} mueve los vectores de base en el plano coordenado. Cada punto o pixel de la imagen es trasladado una distancia constante en una dirección determinada por las componentes del vector transformado. La notación para el operador matricial que realiza una traslación está dada por:

$$\mathbf{T} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ T_x & T_y & 1 \end{pmatrix} \quad (7.4)$$

donde T_x, T_y son los parámetros de traslación en píxeles en la dirección x e y , respectivamente. Aplicando T a un vector fila $(u, v, 1)$, las componentes del vector transformado $(x, y, 1)$ están dadas por:

$$\begin{aligned} x &= u + T_x \\ y &= v + T_y \end{aligned} \quad (7.5)$$

Se puede observar que cuando los parámetros de traslación son iguales a cero, los vectores de la base permanecen inalterados. Por otro lado, cuando los parámetros de traslación son positivos, la imagen es trasladada en píxeles el valor del parámetro.

Como ejemplo, asignar valores positivos de los parámetros T_x y T_y hacen que la imagen resultante se traslade como la Figura 7.3 (a), (b) y (e). Asignar valores negativos de los parámetros de traslación hace que la imagen resultante se mueva como la Figura 7.3 (c), (d) y (f). Valores combinados de T_x y T_y hacen que la imagen resultante se desplace como las Figuras 7.3 (g) y (h).

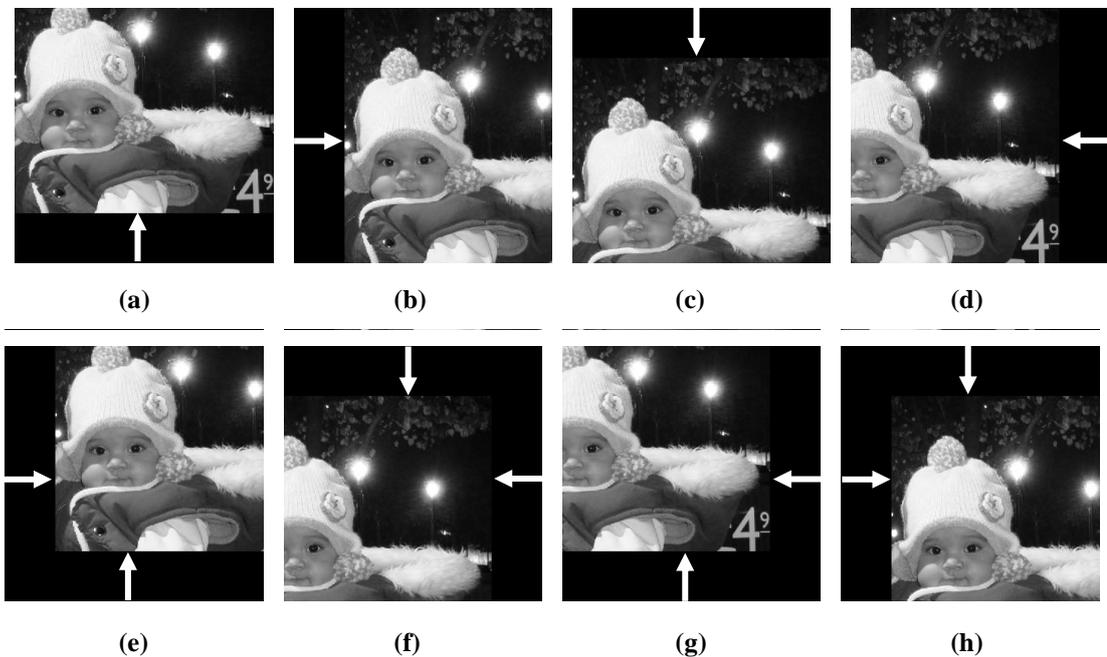


Figura 7.3: Transformación afín de traslación. Los parámetro de traslación (T_x, T_y) son: (a) $(0, 100)$, (b) $(100, 0)$, (c) $(0, -100)$, (d) $(-100, 0)$, (e) $(100, 100)$, (f) $(-100, -100)$, (g) $(-100, 100)$, (h) $(100, -100)$.

7.3.2 Transformación de reflexión

La reflexión es una transformación rígida o isométrica congruente con la forma original de la imagen. Esta transformación es representada por el operador \mathbf{R} . En forma matricial puede ser expresada como:

$$\mathbf{R} = \begin{pmatrix} i_x & 0 & 0 \\ 0 & i_y & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (7.6)$$

donde i_x e i_y son los parámetros de reflexión que pueden tomar valores 1 ó -1. El valor negativo produce la imagen reflejada según el *eje x* o el *eje y*, respectivamente. Al aplicar la matriz \mathbf{R} sobre el vector $(u, v, 1)$, las componentes del vector transformado $(x, y, 1)$ pueden ser expresadas como:

$$\begin{aligned} x &= ui_x \\ y &= vi_y \end{aligned} \quad (7.7)$$

La Figura 7.4 muestra el resultado de una transformación de reflexión aplicada a una imagen en el *eje x*.

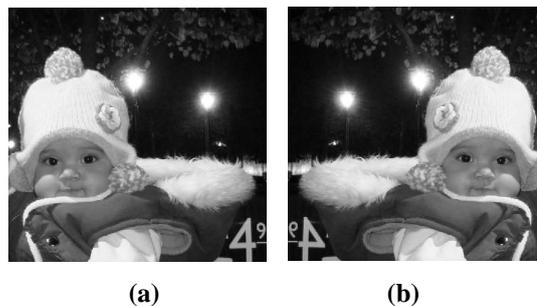


Figura 7.4: Reflexión de una imagen. (a) Parámetro afín de reflexión $i_x = 1$, (b) parámetro afín de reflexión $i_x = -1$.

7.3.3 Transformación de rotación

La rotación es una transformación rígida donde se mantiene la forma y el tamaño de las imágenes. La rotación puede ser en sentido horario o en sentido anti-horario. El operador matricial $\mathbf{\theta}$ que realiza una rotación puede ser expresado como:

$$\boldsymbol{\theta} = \begin{pmatrix} \cos \theta & -\sin \theta & 0 \\ \sin \theta & \cos \theta & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (7.8)$$

donde θ es el ángulo de rotación medido respecto al centro de la imagen. Este valor puede tomar valores entre 0 y 2π radianes. Al aplicar $\boldsymbol{\theta}$ sobre un vector $(u, v, 1)$, las componentes del vector transformado $(x, y, 1)$ pueden ser expresadas como:

$$\begin{aligned} x &= u \cos \theta + v \sin \theta \\ y &= -u \sin \theta + v \cos \theta \end{aligned} \quad (7.9)$$

La Figura 7.5 (a) muestra el resultado de aplicar sobre una imagen una transformación de rotación con $\theta = 45^\circ$, mientras la Figura 7.5 (b) muestra el resultado al aplicar una transformación de rotación con $\theta = -45^\circ$. Note que las dimensiones de la matriz resultante aumentan de tamaño para visualizar la imagen transformada.

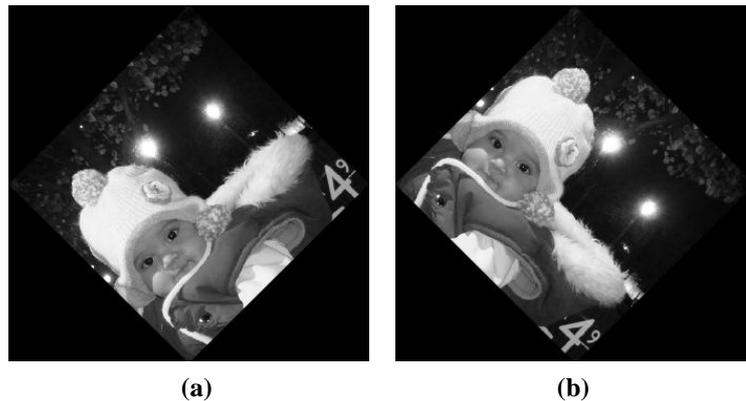


Figura 7.5: Rotación de una imagen. (a) Imagen rotada con el parámetro afín $\theta = 45$. (b) Imagen rotada con el parámetro afín $\theta = -45$.

7.3.4 Transformación de contracción o escalamiento

La contracción o escalamiento es una transformación no rígida que cambia el tamaño de la imagen. El operador de contracción \mathbf{C} que realiza un escalamiento está determinado por la siguiente matriz:

$$\mathbf{C} = \begin{pmatrix} S_x & 0 & 0 \\ 0 & S_y & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (7.10)$$

donde S_x y S_y son parámetros de escalamiento en el *eje x* y *eje y*, respectivamente. Al aplicar \mathbf{C} sobre un vector $(u, v, 1)$, las componentes del vector transformado $(x, y, 1)$ tienen la forma:

$$\begin{aligned} x &= uS_x \\ y &= vS_y \end{aligned} \quad (7.11)$$

En la Figura 4.9 (b) se muestra una contracción en las dos direcciones de la imagen de la Figura 4.9 (a). En la Figura 4.9 (c) se muestra un escalamiento en la dirección del *eje x* y una contracción de la imagen en la dirección del *eje y*.



Figura 7.6: Contracción de una imagen. (a) Imagen sin modificar, parámetros afines de contracción $(S_x, S_y) = (1,1)$, (b) y (c) imágenes transformadas con parámetros de contracción $(S_x, S_y) = (0.7,0.9)$ y $(S_x, S_y) = (1.2,0.9)$, respectivamente.

7.3.5 Transformación de *shearing*

El *shearing* es una transformación no rígida que mueve un lado de la imagen en el *eje x* o *eje y* mientras el otro lado permanece fijo. Se puede interpretar como un afilamiento de la imagen o una distorsión. No obstante se la llamará por su nombre en inglés para evitar la incorrecta traducción. El operador matricial \mathbf{Sh} puede ser expresado como:

$$\mathbf{Sh} = \begin{pmatrix} 1 & Sh_y & 0 \\ Sh_x & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (7.12)$$

donde Sh_x y Sh_y son los parámetros de *shearing*. Al aplicar \mathbf{Sh} sobre un vector $(u, v, 1)$, las componentes del vector transformado $(x, y, 1)$ tienen la forma:

$$\begin{aligned}x &= u + vSh_x \\ y &= uSh_y + v\end{aligned}\tag{7.13}$$

En la Figura 7.7 (a) se muestra como el lado izquierdo y el derecho de la imagen se van inclinando manteniendo fijos los puntos extremos inferiores. Por otro lado, en la Figura 7.7 (b) se muestra como el lado superior e inferior de la imagen se van inclinando manteniendo fijos los puntos extremos laterales.

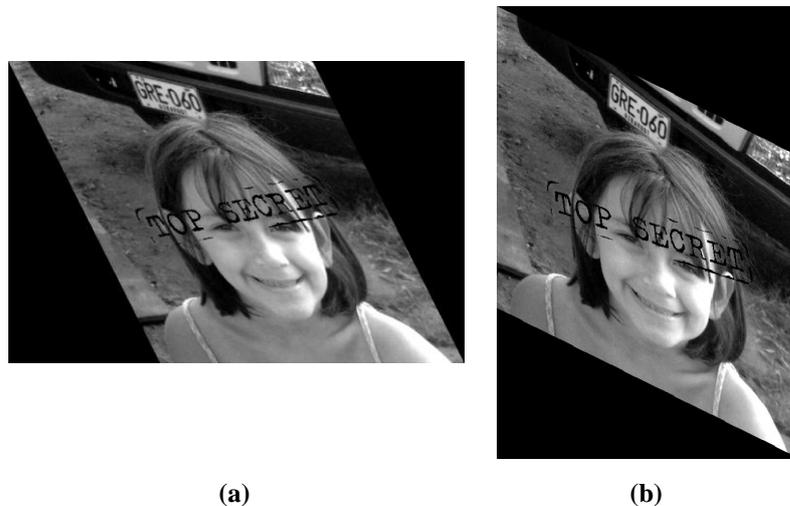


Figura 7.7: *Shearing* de una imagen. (a) Imagen modificada con parámetros de *shearing* $(Sh_x, Sh_y) = (0.5, 0)$ y (b) con parámetros $(Sh_x, Sh_y) = (0, 0.5)$.

A continuación se describe el proceso que combina estas transformaciones afines para generar imágenes pseudoaleatorias.

7.4 Generación de imágenes pseudoaleatorias

El proceso de generación de imágenes pseudoaleatorias por transformaciones afines (PGI_{at}), consiste de una suma de módulo n , entre dos imágenes que han sido transformadas geoméricamente. Una imagen de entrada llamada imagen fuente, es transformada por operadores de traslación, reflexión, rotación, contracción y *shearing*. Este proceso se aplica para la misma imagen dos veces con diferentes parámetros afines para proceder finalmente con la suma modular. La imagen resultante es llamada imagen AT (I_{at}).

En el PGI_{at} , la imagen fuente es transformada en una imagen AT usando los parámetros de las transformaciones afines. Ahora, si este procedimiento es realizado N veces, tomando como imagen fuente en cada PGI_{at} la imagen AT obtenida de un PGI_{at} anterior, el resultado será indicado como $I_{at}^{(N)}$. El subíndice N indica que la imagen resultante es producto de aplicar N procesos PGI_{at} . A esta distribución se la puede llamar imagen AT de orden N . Por ejemplo, después de aplicar cinco PGI_{at} a una imagen inicial, se indicará el resultado final como $I_{at}^{(5)}$ y se referirá a ella como imagen AT de orden cinco.

El PGI_{at} es realizado de la siguiente manera: inicialmente se tiene una imagen I_1 , que por simplicidad, es duplicada para obtener la imagen idéntica I_2 . A estas dos imágenes, I_1 e I_2 , se les realiza un conjunto de transformaciones con parámetros afines diferentes. El resultado de cada una de estas transformaciones aplicadas sobre las dos imágenes I_1 e I_2 son sumadas en módulo n . La imagen resultante de la suma modular es entonces la distribución $I_{at}^{(1)}$ que será la nueva imagen de entrada del PGI_{at} siguiente.

Para generar una imagen I_{at} de orden N , es decir $I_{at}^{(N)}$, se necesitan los siguientes parámetros:

- 1) T_{x1}, T_{y1}, T_{x2} y T_{y2} asociados a la operación de translación.
- 2) i_{x1}, i_{y1}, i_{x2} e i_{y2} asociados a la operación de reflexión.
- 3) θ_1 y θ_2 asociados a la operación de rotación.
- 4) S_{x1}, S_{y1}, S_{x2} y S_{y2} asociados a la operación de escalamiento.
- 5) $Sh_{x1}, Sh_{y1}, Sh_{x2}$ y Sh_{y2} asociados a la operación de *shearing*.

Los subíndices (1 o 2) en cada parámetro indican que imagen de entrada (I_1 o I_2) es transformada. En total, se involucran veinte parámetros, considerando la base n de la suma modular y el número de iteraciones N del PGI_{at} . Con estos parámetros se pueden generar unívocamente una imagen AT (I_{at}). Se debe notar que el mismo conjunto de parámetros afines es usado en cada iteración del proceso. También se debe destacar que el parámetro de la suma modular n es quien controla el rango de valores en niveles de gris que tienen las

$I_{at}^{(N)}$ generadas. De esta manera al cambiar n se puede controlar el número de fases de la llave de codificación generada a partir de estas imágenes pseudoaleatorias.

La forma lineal y la manera repetitiva de aplicar las transformaciones afines en un PGI_{at} permiten expresar el proceso entero como una única transformación de la imagen fuente. En el PGI_{at} intervienen las transformaciones de traslación, reflexión, rotación, contracción y *shearing*. El número total de permutaciones del orden de aplicación de sus operadores matriciales es $5!$, es decir 120 permutaciones posibles que generan imágenes $I_{at}^{(N)}$ diferentes.

Se debe mencionar que al usar una imagen fuente simétrica según el *eje x* o *eje y*, se reduce el número de permutaciones posibles de los operadores. Para este tipo de imágenes una transformación afín de reflexión no contribuye ya que no se altera la imagen con la transformación. Para este caso el número de permutaciones de aplicación de los operadores se reduce a $4!$ o 24 permutaciones posibles las cuales generan imágenes $I_{at}^{(N)}$ diferentes.

Para dar un ejemplo, si se considera el operador \mathbf{A}_t actuando sobre el vector $(u, v, 1)$, el vector transformado $(x, y, 1)$ estará dado por:

$$(x, y, 1) = (u, v, 1)\mathbf{A}_t \quad (7.14)$$

donde el operador \mathbf{A}_t es una de las 120 permutaciones posibles del orden de aplicación de las 5 transformaciones afines. Si se toma una de estas permutaciones, por ejemplo:

$$\mathbf{A}_t = \mathbf{R} \cdot \mathbf{C} \cdot \mathbf{Sh} \cdot \mathbf{T} \cdot \mathbf{\Theta} \quad (7.15)$$

los operadores que componen esta transformada actuarán de izquierda a derecha, primero actuara el operador de reflexión \mathbf{R} sobre el vector $(u, v, 1)$. Posteriormente, sobre este resultado, actuará el operador de contracción \mathbf{C} y así sucesivamente hasta actuar el operador de rotación $\mathbf{\Theta}$. Esto es equivalente a representar el operador \mathbf{A}_t como una única matriz:

$$\mathbf{A}_t = \begin{pmatrix} i_x \cdot S_x \cdot \cos \theta + i_x \cdot S_x \cdot Sh_y \cdot \sin \theta & i_x \cdot S_x \cdot Sh_y \cdot \cos \theta - i_x \cdot S_x \cdot \sin \theta & 0 \\ i_y \cdot S_y \cdot \sin \theta + i_y \cdot S_y \cdot Sh_x \cdot \cos \theta & i_y \cdot S_y \cdot \cos \theta - i_y \cdot S_y \cdot Sh_x \cdot \sin \theta & 0 \\ T_x \cdot \cos \theta + T_y \cdot \sin \theta & T_y \cdot \cos \theta - T_x \cdot \sin \theta & 1 \end{pmatrix} \quad (7.16)$$

actuando directamente según la Ecuación (7.14). Esto producirá una imagen AT que será diferente al resultado de aplicar cada operador en posición diferente.

Consecuentemente, debido a que las permutaciones transforman de manera diferente una imagen, se debe conocer el orden correcto de aplicación de cada operador para replicar una misma imagen de orden $I_{at}^{(N)}$, o que es lo mismo, replicar correctamente la llave de seguridad.

Analizando las 120 permutaciones de aplicación de los cinco operadores, se pueden encontrar valores de los parámetros afines para los cuales el orden de aplicación de los operadores no tiene importancia y produce una misma distribución, estos valores son:

$$\mathbf{A}_{t1} = \mathbf{A}_{t2} = \dots = \mathbf{A}_{t120} \begin{cases} i_x = i_y \\ S_x = S_y \\ \theta = 180^\circ \\ Sh_x = -Sh_y \\ T_x = 0 \text{ o } T_y = 0 \end{cases} \quad (7.17)$$

Se debe procurar no usar alguno de estos valores en los parámetros afines. De esta forma tiene relevancia el orden de aplicación de cada operador. Esto brinda un grado más de seguridad si un usuario no autorizado pretende generar la misma distribución pseudoaleatoria, pero no conoce la forma de aplicación de cada transformación afín.

Se va a suponer que el orden de aplicación de los operadores afines en el PGI_{at} es:

$$\mathbf{A}_t = \mathbf{C} \cdot \boldsymbol{\theta} \cdot \mathbf{R} \cdot \mathbf{Sh} \cdot \mathbf{T} \quad (7.18)$$

De esta forma, el operador \mathbf{A}_t puede ser escrito matricialmente de la forma:

$$\mathbf{A}_t = \begin{pmatrix} i_x \cdot S_x \cdot \cos \theta - i_y \cdot S_x \cdot Sh_x \cdot \sin \theta & i_x \cdot S_x \cdot Sh_y \cdot \cos \theta - i_y \cdot S_x \cdot \sin \theta & 0 \\ i_x \cdot S_y \cdot \sin \theta + i_y \cdot S_y \cdot Sh_x \cdot \cos \theta & i_y \cdot S_y \cdot \cos \theta + i_x \cdot S_y \cdot Sh_y \cdot \sin \theta & 0 \\ T_x & T_y & 1 \end{pmatrix} \quad (7.19)$$

Note que los operadores \mathbf{A}_t de la Ecuación (7.16) y la Ecuación (7.19) son diferentes. En esta última ecuación los parámetros de traslación T_x , T_y no son modificados por otros parámetros afines. Esto brinda la ventaja de poder decorrelacionar en el *eje x* o en el *eje y* y las imágenes que se van a sumar en forma modular.

Tomando la transformación de la Ecuación (7.19), las coordenadas del vector transformado $(x, y, 1)$ pueden ser expresadas como:

$$\begin{aligned} x &= u(i_x \cdot S_x \cdot \cos \theta - i_y \cdot S_x \cdot Sh_x \cdot \sin \theta) + v(i_x \cdot S_y \cdot \sin \theta + i_y \cdot S_y \cdot Sh_x \cdot \cos \theta) + T_x \\ y &= u(i_x \cdot S_x \cdot Sh_y \cdot \cos \theta - i_y \cdot S_x \cdot \sin \theta) + v(i_y \cdot S_y \cdot \cos \theta + i_x \cdot S_y \cdot Sh_y \cdot \sin \theta) + T_y \end{aligned} \quad (7.20)$$

La distribución resultante de cada proceso es de menor o mayor tamaño que la imagen fuente y depende exclusivamente de la combinación de los parámetros afines. Por lo tanto, la aplicación del PGI_{at} permite generar de forma controlada imágenes pseudoaleatorias. Se puede controlar el rango de valores de cada distribución con la suma modular y con las operaciones de contracción o escalamiento se pueden obtener distribuciones pseudoaleatorias del tamaño necesario para encriptar una imagen de un tamaño preestablecido.

En la Figura 7.8 se muestra la generación de distribuciones pseudoaleatorias con el proceso descrito en párrafos anteriores. Los parámetros afines están dados en la Tabla 7.1 y son aplicados según la Ecuación (7.18). La Figura 7.8 (a) es la imagen fuente y las imágenes de la Figura 7.8 (b) - Figura 7.8 (f) son el resultado de sucesivas iteraciones del PGI_{at} . Se puede observar como en la imagen correspondiente a la iteración $N = 1$ ($I_{at}^{(1)}$), se genera una distribución donde la imagen fuente es aun reconocida. A medida que se incrementa el número de iteraciones la imagen progresivamente va adquiriendo características pseudoaleatorias como se puede observar en las imágenes Figura 7.8 (c) - Figura 7.8 (f). Esta “aleatoridad” es esencial para poder encriptar información y será analizada en la Sección 7.5.

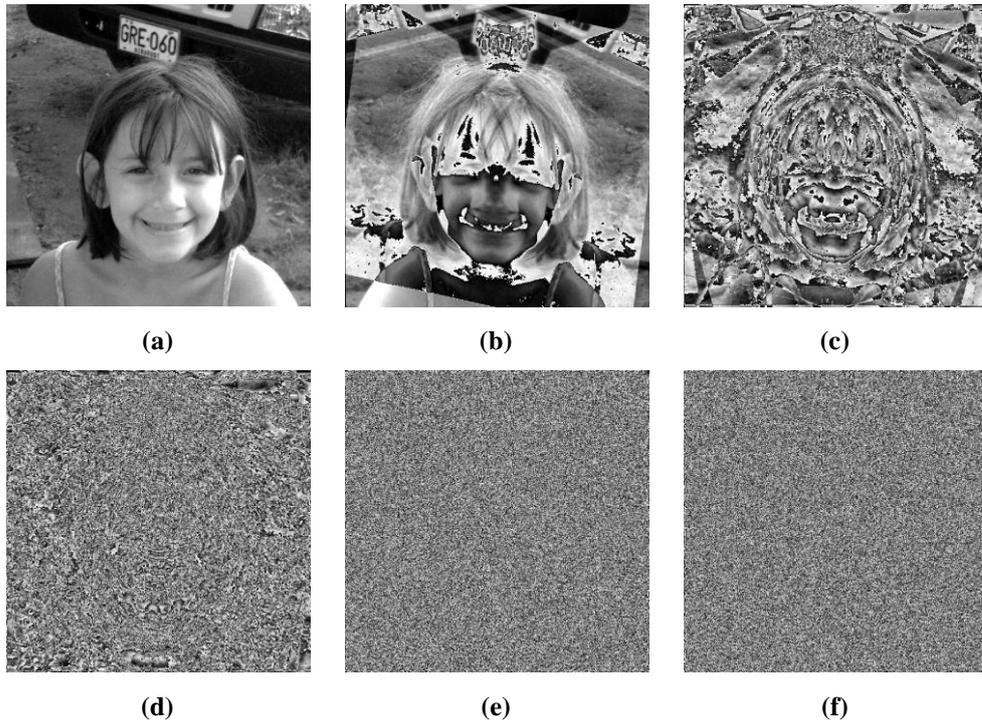


Figura 7.8: Imágenes generadas por transformaciones afines para diferentes órdenes de iteración. (a) Imagen fuente, (b) $I_{at}^{(1)}$, (c) $I_{at}^{(3)}$, (d) $I_{at}^{(5)}$, (e) $I_{at}^{(9)}$, (f) $I_{at}^{(15)}$.

| Imagen fuente | Reflexión (i_x, i_y) | Traslación (T_x, T_y) | Rotación (θ) | Contracción (S_x, S_y) | Shearing (Sh_x, Sh_y) | Módulo (n) | Iteración (N) |
|---------------|-----------------------------|------------------------------|--------------------------|-------------------------------|------------------------------|-------------------|----------------------|
| 1 | (1,1) | (0,0) | -10 | (1,1) | (0.05,0.05) | 256 | 15 |
| 2 | (-1,1) | (1,1) | 0 | (1,1) | (0,0) | | |

Tabla 7.1: Parámetros afines usados para generar los resultados de la Figura 7.8

A continuación, se realiza un estudio del comportamiento de estas distribuciones pseudoaleatorias cuando la imagen fuente se ve contaminada o alterada. Ya que la aplicación de estas imágenes $I_{at}^{(N)}$ es en sistemas de encriptación, estos estudios serán determinantes para evaluar su eficiencia como llaves de seguridad.

En primera medida se analiza cuando la imagen fuente pierde información en algunos de sus píxeles, ya sea por el proceso de transmisión o por otro proceso que deteriore la imagen. Un segundo análisis considera que la imagen fuente ha sido restaurada eliminando el ruido del primer caso. Un tercer análisis considera una imagen fuente que ha sido contaminada con ruido de *speckle* de diferentes varianzas y finalmente, se considera que la imagen fuente ha sido transmitida al usuario en diferentes formatos de compresión.

Estos estudios están encaminados a evaluar la técnica propuesta para ser aplicada en sistemas de codificación.

7.4.1 Sensibilidad de las imágenes $I_{at}^{(N)}$ ante la pérdida de información de píxeles en la imagen fuente

La pérdida de píxeles en la imagen fuente produce valores nulos donde antes existía información. Este es un ruido típico llamado “pimienta”. En la imagen se pierden píxeles de forma aleatoria y se puede considerar que la imagen está contaminada. La Figura 7.9 (b) muestra una imagen que ha sufrido pérdida de información presentándose como puntos negros en la imagen. En la Figura 7.9 (c) se muestra la $I_{at}^{(3)}$ obtenida al usar una imagen fuente sin pérdida de información y en la Figura 7.9 (d) se muestra la $I_{at}^{(3)}$ al usar la imagen fuente con pérdida de información.

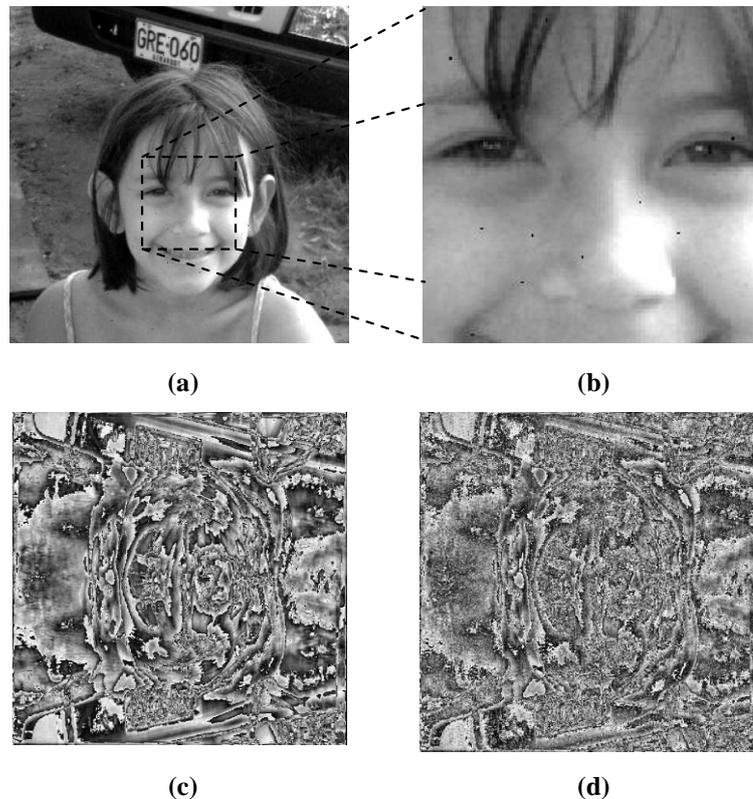


Figura 7.9: Generación de imágenes AT con pérdida de información en la imagen fuente. (a) Imagen con pérdida de píxeles, (b) región aumentada, (c) imagen $I_{at}^{(3)}$ obtenida de la imagen fuente sin pérdida de píxeles y (d) imagen $I_{at}^{(3)}$ obtenida de la imagen fuente con pérdida de 10000 píxeles.

Note la similitud entre la imagen de la Figura 7.9 (c) y la Figura 7.9 (d). A pesar de que la imagen fuente ha perdido una cantidad importante de píxeles, tienen una gran similitud. Si la pérdida de información fuera poca, las dos imágenes AT de orden tres, $I_{at}^{(3)}$, serían casi idénticas.

Para observar mejor este comportamiento, inicialmente se han generado 15 imágenes I_{at} usando los parámetros de la Tabla 7.2. La imagen fuente sin contaminación es la Figura 7.8 (a). Las $I_{at}^{(N)}$, con $N = 1, 2, \dots, 15$, generadas a partir de esta imagen sirven como distribuciones de referencia. Posteriormente, la imagen fuente es contaminada y se generan nuevamente 15 imágenes I_{at} . El número de píxeles contaminados introducidos aleatoriamente en la imagen varían de 1 hasta 10000 píxeles. Esto es solamente el $\sim 4\%$ de una imagen de tamaño 512×512 . Finalmente, se evalúa la similitud entre las imágenes AT de referencia y las imágenes AT obtenidas al contaminar la imagen fuente.

| Imagen fuente | Reflexión (i_x, i_y) | Traslación (T_x, T_y) | Rotación (θ) | Contracción (S_x, S_y) | Shearing (Sh_x, Sh_y) | Módulo (n) | Iteración (N) |
|---------------|-----------------------------|------------------------------|--------------------------|-------------------------------|------------------------------|-------------------|----------------------|
| 1 | (1,-1) | (10,0) | 2 | (1,1) | (0,0) | 256 | 15 |
| 2 | (1,1) | (-5,5) | 0 | (1,1) | (0,0) | | |

Tabla 7.2: Parámetros afines usados para generar los resultados de la Figura 7.9.

La gráfica de la Figura 7.10 muestra la raíz del error cuadrático medio ($RMSE$) en función del número de píxeles perdidos en la imagen fuente y en función del orden de iteración N del PGI_{at} .

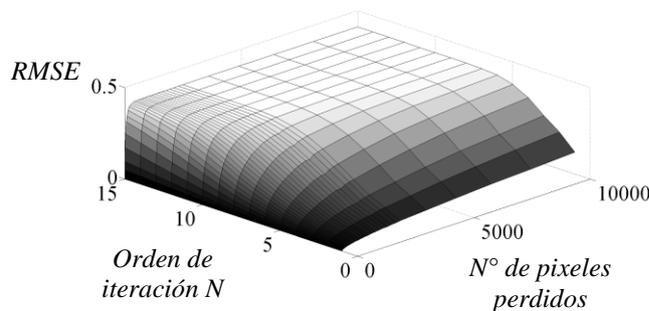


Figura 7.10: Superficie de $RMSE$ obtenida entre cada orden de las imágenes AT obtenidas a partir de la imagen fuente original y las imágenes AT obtenidas a partir de la imagen fuente que tiene pérdida de información aleatoria de 1 a 10000 píxeles.

La superficie de *RMSE* revela un valor de saturación a partir de un número determinado de píxeles y un dado orden de iteración N . Se calcula que a partir de la contaminación de 400 píxeles de una imagen de tamaño 512×512 píxeles y con un orden de iteración $N = 9$ o superior, las distribuciones obtenidas son totalmente diferentes a las distribuciones de referencia. Esta observación es muy importante ya que indica que si la imagen es contaminada en $\sim 0.15\%$, después de aplicar nueve procesos PGI_{at} no se puede replicar la distribución pseudoaleatoria.

Para verificar esto, se evalúan los picos de correlación cruzada entre la $I_{at}^{(15)}$ de referencia (obtenida de la imagen fuente sin pérdida de píxeles) y las $I_{at}^{(15)}$ obtenidas a partir de la imagen fuente con pérdida de 0 píxeles (auto-correlación), 16 píxeles, 100 píxeles, 256 píxeles, 400 píxeles y 10000 píxeles. Los resultados son mostrados en Figura 7.11. Note como después de perder 400 píxeles en la imagen original, las gráficas del pico de correlación son superficies de ruido estacionario. Esto muestra la decorrelación entre la $I_{at}^{(15)}$ obtenida de una imagen fuente original y la $I_{at}^{(15)}$ obtenida de una imagen fuente con 400 píxeles perdidos.

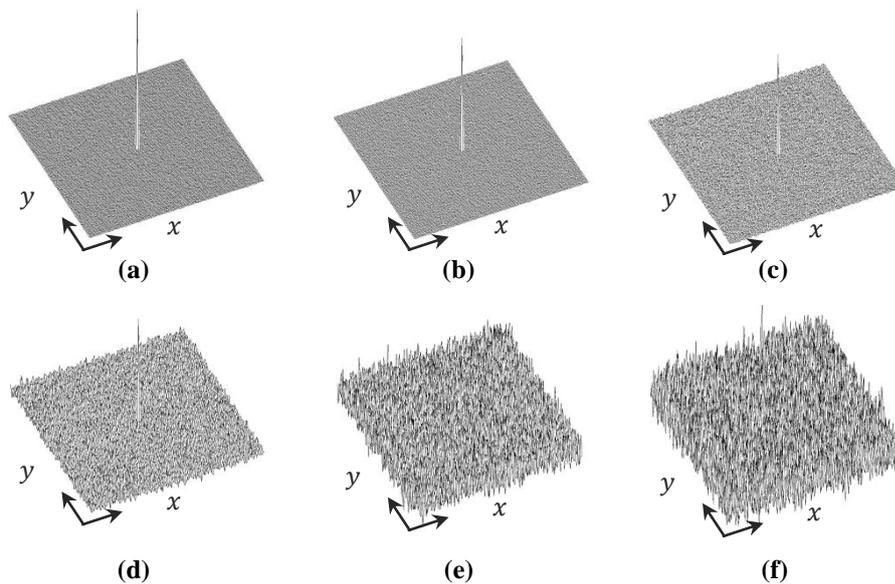


Figura 7.11: Correlación cruzada entre la $I_{at}^{(15)}$ obtenida de la imagen fuente sin pérdida de píxeles y las $I_{at}^{(15)}$ obtenidas de la imagen fuente con pérdida de píxeles de (a) 0 píxeles (auto-correlación), (b) 16 píxeles, (c) 100 píxeles, (d) 256 píxeles, (e) 400 píxeles y (f) 10000 píxeles.

En la Figura 7.11, se puede observar como la intensidad de los picos de correlación cruzada van disminuyendo a medida que aumenta la pérdida de píxeles en la imagen fuente. Nótese también como las variaciones de los coeficientes de correlación comienzan a fluctuar cada vez más, indicando una decorrelación.

El comportamiento de las intensidades máximas de cada superficie de correlación es graficado en la Figura 7.12. La intensidad de los picos de correlación cruzada no sólo disminuye, la función de correlación también tienden a una distribución de fluctuaciones de valor medio constante.

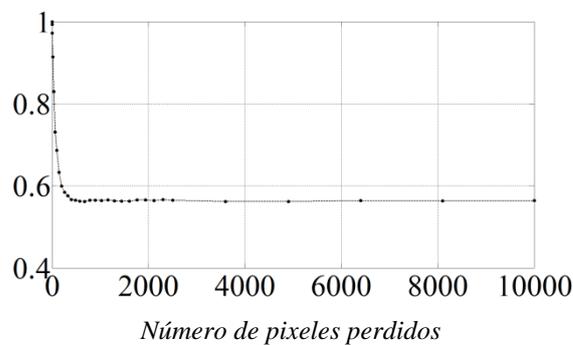


Figura 7.12: Máximos de la correlación cruzada entre la $I_{at}^{(15)}$ obtenida de una fuente sin pérdida de información y la $I_{at}^{(15)}$ obtenida con pérdida de información entre 1 y 10000 píxeles.

Esto demuestra que la generación de imágenes AT es un proceso extremadamente sensible a cambios producidos sobre la imagen fuente. Al usar estas distribuciones como máscaras de fase en un sistema de encriptación, al usuario autorizado se le deberá transmitir esta imagen con una contaminación menor a $\sim 0.15\%$. La imagen transmitida junto a los parámetros afines permitirá reconstruir la llave de seguridad en la estación de descryptación. Si la imagen fuente es transmitida con una contaminación superior a este porcentaje se estima que a partir de un orden de iteración $N \geq 9$ las distribuciones pseudoaleatorias no servirán como llaves de decodificación. Esto brinda un grado adicional de la técnica propuesta el cual se analizará en la Sección 7.6.

7.4.2 Sensibilidad de las imágenes $I_{at}^{(N)}$ al usar una imagen fuente restaurada

La adición de píxeles nulos representa un deterioro y una contaminación en la imagen fuente. Sin embargo, la imagen puede ser procesada digitalmente mediante filtros para obtener una imagen restaurada. Estos filtros pueden ser aplicados sobre la imagen en el dominio espacial y en el dominio de frecuencias. En el dominio espacial están los filtros de orden entre los cuales se destacan los filtros de mediana, moda, filtro máximo y filtro mínimo. También se pueden aplicar filtros de medias lineales como la media (filtro paso bajo espacial), media geométrica, media armónica, media contra-armónica, de Gauss y filtros de medias no lineales como el Outlier. Por otro lado, en el dominio de las frecuencias se pueden aplicar filtros paso bajo, paso banda, paso alto y rechazo de banda. Un estudio del ruido presente en imágenes y las técnicas de filtrado se encuentra en [7.32]-[7.34]. Para el ruido que consiste de mínimos de intensidad, es conveniente emplear un filtro de orden máximo el cual elimina el ruido pimienta o píxeles negros. Sin embargo, únicamente funciona cuando el ruido es exclusivamente tipo pimienta y el efecto global es que la imagen procesada tiende a ser más clara.

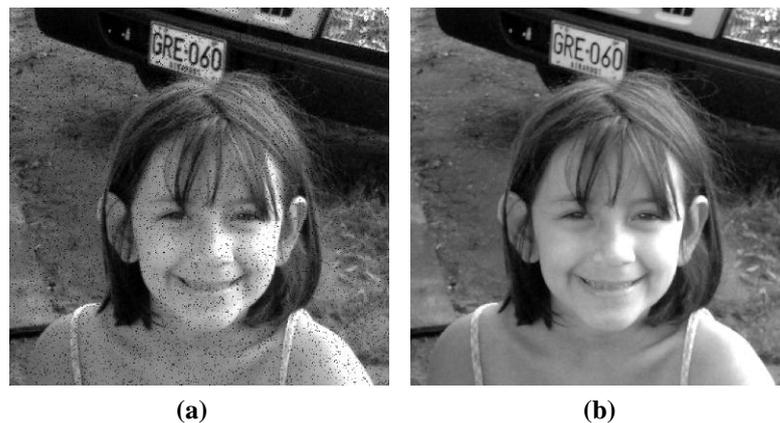


Figura 7.13: Filtrado de la imagen fuente. (a) Imagen fuente con pérdida de información y (b) imagen restaurada con un filtro de orden máximo.

En la Figura 7.13 se muestra un ejemplo de la aplicación de este filtro. Aquí, la Figura 7.13 (a) es una imagen que ha perdido 10000 píxeles y la Figura 7.13 (b) es la imagen restaurada. Claramente la imagen filtrada es un resultado de excelente calidad sin el ruido de pimienta.

Ahora, al usar la imagen restaurada como imagen fuente en el proceso PGI_{at} se encuentra que la $I_{at}^{(15)}$ obtenida a partir de esta imagen es totalmente diferente a la $I_{at}^{(15)}$ de referencia (distribución generada con la imagen fuente sin ruido).

Para evaluar si existe dependencia con la cantidad de píxeles filtrados, se restauró una imagen fuente con pérdida de 16 píxeles, 100 píxeles y 256 píxeles. Con cada imagen fuente restaurada se generó una $I_{at}^{(15)}$. Posteriormente, se encontraron las correlaciones cruzadas entre la $I_{at}^{(15)}$ de referencia y la $I_{at}^{(15)}$ obtenida de cada imagen fuente restaurada. Los resultados de estas correlaciones cruzadas son mostrados en la Figura 7.14. Se puede observar que no existe correlación entre estas imágenes a pesar que la imagen restaurada posee la mayoría de características generales de la imagen original. Sin embargo, no es suficiente para realizar una réplica de la distribución pseudoaleatoria.

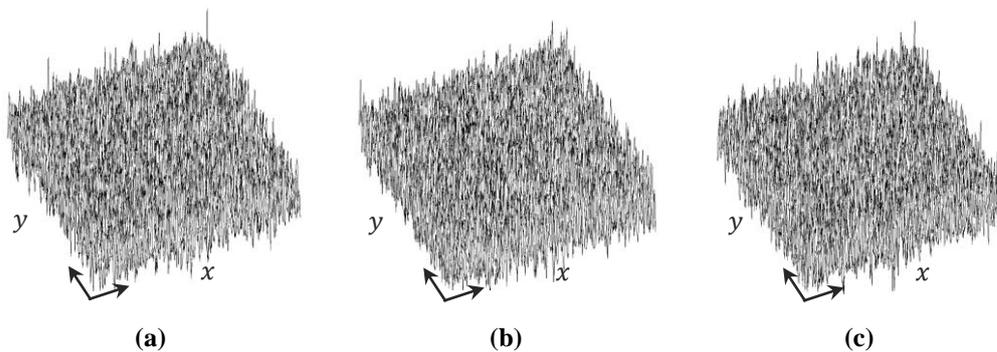


Figura 7.14: Correlación cruzada entre la $I_{at}^{(15)}$ de referencia y la $I_{at}^{(15)}$ obtenida de la imagen fuente restaurada. Esta imagen tenía pérdida de información de (a) 16 píxeles, (b) 100 píxeles y (c) 256 píxeles.

Es evidente la efectividad de los filtros para procesar y restaurar digitalmente imágenes. Sin embargo, cuando son empleadas como entradas en el PGI_{at} generan otro conjunto de distribuciones pseudoaleatorias diferentes a las obtenidas con la imagen fuente original. Esto está acorde con el análisis de la sección anterior, ya que filtrar una imagen producirá cambios globales que afectan la mayoría de los píxeles. Nótese que no se refiere a si un nivel de gris cambia más o menos, se refiere a la cantidad de píxeles que ya no son iguales. De esta forma, no es relevante si dos píxeles tiene valores de nivel de gris igual a

128 y 127, ellos dos son diferentes de la misma forma que dos pixeles de niveles de gris 1 y 255.

7.4.3 Sensibilidad de las imágenes $I_{at}^{(N)}$ al usar una imagen fuente con ruido *speckle*

El ruido *speckle* puede estar presente en varios procesos contaminando las imágenes fuente. Este ruido es adicionado a la imagen I de la forma $J = I + mI$, donde m es una función de ruido aleatorio uniformemente distribuida con media cero y varianza v . Este caso es de particular interés, un usuario no autorizado puede llegar a recuperar todos los parámetros afines, pero quizás no tenga acceso a la imagen fuente fidedigna, sino a una copia de cierta fidelidad.

En base a esto, se analiza cómo cambia la generación de distribuciones pseudoaleatorias debido a la presencia del ruido *speckle* en la imagen fuente. Inicialmente, con los parámetros de la Tabla 7.2 se generan 15 imágenes AT usando como imagen fuente la Figura 7.8 (a). Posteriormente, la imagen fuente es contaminada con ruido *speckle* de diferentes varianzas. Para cada varianza se generan nuevamente 15 imágenes AT.

La gráfica de la Figura 7.15 muestra los resultados del *RMSE* en función de la varianza del ruido *speckle* y del orden de iteración N del PGI_{at} . Cada valor de *RMSE* fue calculado para cada orden de iteración, entre las imágenes AT de referencia y las imágenes AT obtenidas a partir de la imagen fuente contaminada. La varianza del ruido *speckle* está entre los valores 0 y 0.01.

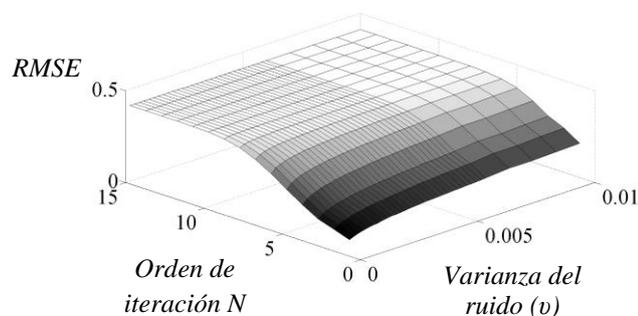


Figura 7.15: Superficie de *RMSE* obtenida entre cada orden de las imágenes AT de referencia y las imágenes AT obtenidas a partir de la imagen fuente contaminada con ruido *speckle*.

De la superficie de $RMSE$ de la Figura 7.15, se debe observar que la $I_{at}^{(10)}$ obtenida con la mínima varianza establecida en los análisis de 0.0002, ya está totalmente decorrelacionada de la $I_{at}^{(10)}$ de referencia. Esto corrobora los análisis de las dos secciones anteriores. En general, la adición de ruido *speckle* y la adición de otra contaminación en la imagen fuente hace que se produzcan sumas modulares distintas a lo largo de todas las iteraciones del PGI_{at} .

En la Figura 7.16 se muestran las correlaciones cruzadas entre la $I_{at}^{(9)}$ obtenida de la imagen fuente original y la $I_{at}^{(9)}$ obtenida de la imagen fuente contaminada con ruido *speckle* de varianza 0.0002, 0.0006 y 0.0012, respectivamente. Se puede notar un pico de correlación en la Figura 7.16 (a) obtenido con la menor varianza de ruido *speckle*, para valores mayores de varianza, las imágenes se decorrelacionan y las intensidades de los picos disminuyendo. Evaluando la correlación cruzada entre la $I_{at}^{(10)}$ de referencia y la $I_{at}^{(10)}$ obtenida de la imagen fuente que tiene la mínima varianza del ruido *speckle* el pico desaparece.

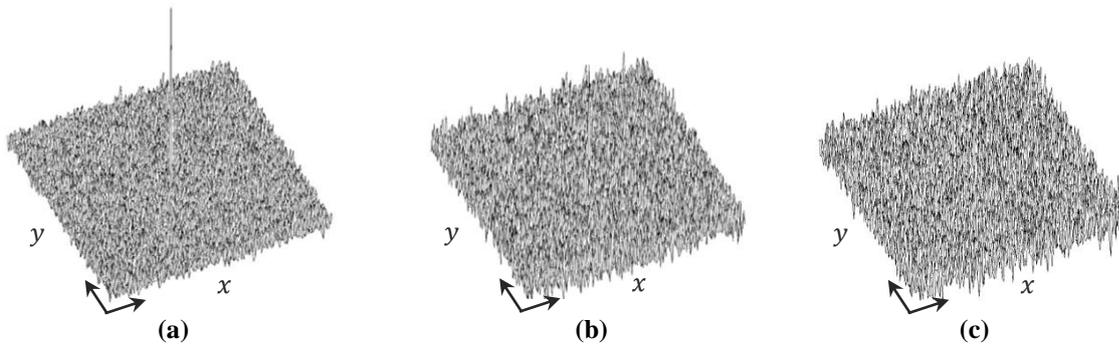


Figura 7.16: Correlación cruzada entre la imagen $I_{at}^{(9)}$ obtenida de la imagen fuente sin ruido *speckle* y la imagen $I_{at}^{(9)}$ obtenida de la imagen fuente con ruido *speckle* de varianza (a) 0.0002, (b) 0.0006 y (c) 0.0012.

Aplicando estas distribuciones como llaves de seguridad, las máscaras de codificación obtenidas con la imagen fuente bajo la influencia del ruido *speckle* cercano a las mínimas varianzas, no logran replicar las máscaras de fase originales aun teniendo los parámetros afines correctos.

7.4.4 Sensibilidad de las imágenes $I_{at}^{(N)}$ al usar una imagen fuente transmitida en formato comprimido

Para finalizar la evaluación de la susceptibilidad de la técnica de generación de imágenes AT por transformaciones afines, se muestra como la transmisión de la imagen fuente en diferentes formatos de compresión influye en la generación de estas distribuciones y consecuentemente en la generación de una réplica de la llave de seguridad.

Inicialmente la imagen fuente de la Figura 7.8 (a) es guardada con la extensión BMP (Bit Mapped Picture). Este es un formato que no usa compresión en las imágenes, permitiendo soportar hasta 24 bits en cada pixel. En segunda medida se guarda la imagen de la Figura 7.8 (a) con la extensión PNG (Portable Network Graphics). Este es un formato que emplea un algoritmo de compresión sin pérdida, lo que significa que siempre se mantendrá la calidad original de la imagen, la extensión PNG soporta datos de hasta 64 bits y posee otras características para aplicaciones en internet que no posee el formato BMP. Por último, la imagen de la Figura 7.8 (a) es guardada con extensión JPEG, JPG (Joint Photographic Experts Group). Este es un formato que emplea un algoritmo de compresión con pérdida, lo que significa que el nivel de compresión afecta directamente la calidad de la imagen produciendo la disminución en el tamaño de archivo, este formato soporta hasta 24 bits y es el más usado en aplicaciones de internet.

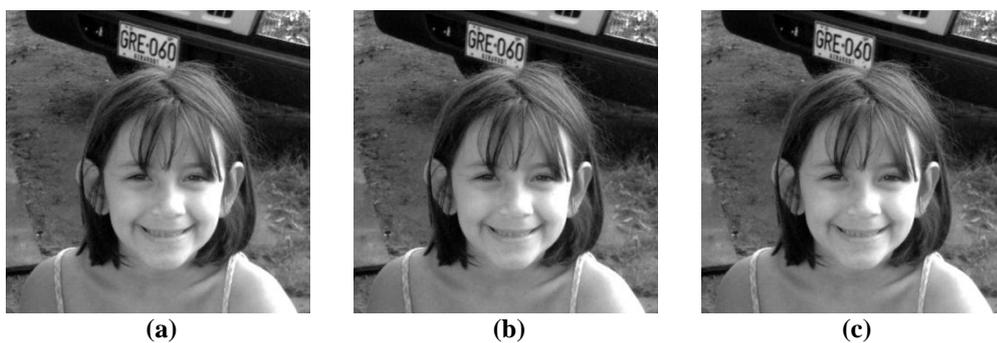


Figura 7.17: Imágenes guardadas en diferentes formatos. Formato (a) BMP, (b) jpg y (c) png.

La imagen guardada en los tres formatos es mostrada en la Figura 7.17. Se puede observar como la diferencia de los tres formatos al ojo humano es imperceptible. Sin embargo, existen diferencias entre las imágenes (a) y (b) y entre las imágenes (b) y (c), a

diferencia de las imágenes (a) y (c) que son iguales debido a que el formato BMP no usa algoritmos de compresión y el formato PNG emplea algoritmos de compresión pero sin pérdida.

A partir de cada una de estas imágenes se generan 15 imágenes AT y se realizan las curvas de *RMSE* comparando con las imágenes AT de referencia (imágenes que no han sido comprimidas). Realizando esta prueba para el formato BMP y el PNG es cero. Esto indica que las 15 imágenes AT generadas al usar la imagen fuente transmitida en formato PNG o BMP, son idénticas a las imágenes AT de referencia. Esto se debe a que las imágenes transmitidas contienen la misma información. Caso contrario al formato JPG.

La Figura 7.18 muestra la curva de *RMSE* entre las imágenes AT de referencia y las imágenes AT obtenidas de una imagen fuente en formato JPG. Se puede observar que la curva satura después del orden diez del PGI_{at} . Esto indica que las imágenes están decorrelacionadas a partir de este orden a pesar de ser la misma imagen fuente, con la salvedad de haber sido transmitidas en un formato JPG. Por lo tanto, una máscara de codificación no puede ser replicada incluso si el formato de la imagen fuente usa algoritmos de compresión con pérdida de información.

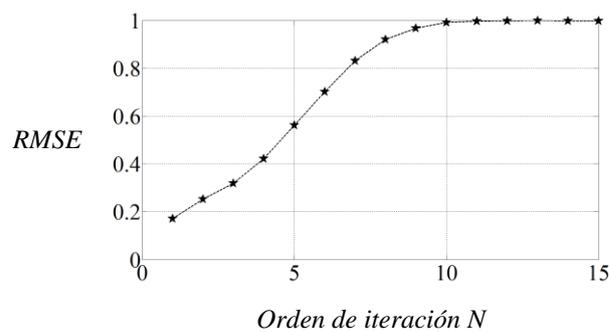


Figura 7.18: *RMSE* entre imágenes AT de referencia y las imágenes AT generadas de la imagen fuente transmitida en formato JPG.

En la Figura 7.19 se muestran las correlaciones cruzadas entre la $I_{at}^{(10)}$ obtenida de referencia y la $I_{at}^{(10)}$ obtenida de una imagen fuente guardada en formato PNG y JPG, respectivamente.

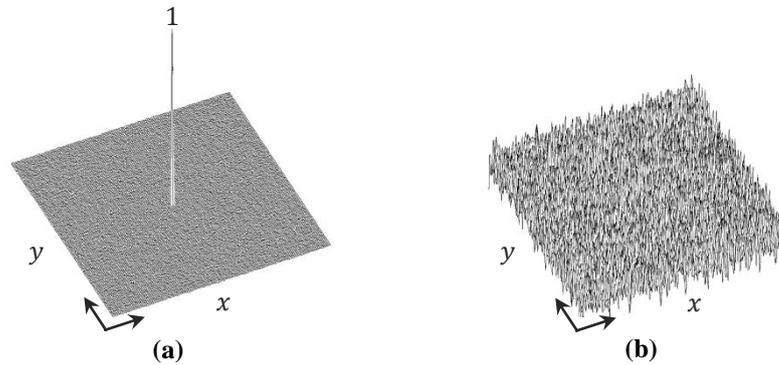


Figura 7.19: Correlación cruzada entre la $I_{at}^{(10)}$ de referencia y una $I_{at}^{(10)}$ obtenida de una fuente guardada en formato (a) PNG y (b) JPG.

Al aplicar estas distribuciones pseudoaleatorias como llaves de seguridad al usuario se le debe transmitir la imagen fuente y los parámetros afines por un canal de comunicación. El usuario en la estación de descryptación aplicará el proceso PGI_{at} para generar estas llaves. Si la imagen fuente es transmitida en formatos que emplean algoritmos de compresión con pérdida de información, se van a generar máscaras de decodificación incorrectas impidiendo la recuperación de la información encriptada. Este es el caso que se observa de la Figura 7.19 (b). La correlación cruzada de las dos distribuciones indica que son diferentes. Por otro lado, cuando la imagen fuente es transmitida con formatos de compresión que no tienen pérdida de información como el formato PNG, se generan llaves de fase correctas logrando recuperar la información en la etapa de descryptación. Este es el caso que se observa de la Figura 7.19 (a). La correlación cruzada de las dos distribuciones indica que son idénticas.

En resumen, los análisis anteriores muestran que la imagen fuente debe ser transmitida fielmente para poder reproducir de manera exacta una llave de seguridad. Cualquier contaminación o cambio mínimo en la imagen fuente producirá llaves incorrectas de decodificación. Se demostró que el sistema de generación de distribuciones pseudoaleatorias usando transformaciones afines es sensible a pequeños cambios en la imagen fuente. Las pérdidas de información influyen negativamente para replicar las llaves de seguridad en la estación de descryptación. Se mostró que al tratar de restaurar la imagen fuente y usarla en el proceso de generación contribuye a la decorrelación de las llaves de seguridad en la etapa de decodificación. En general, cualquier tipo de ruido que

degrade la imagen fuente hace que se generen llaves de seguridad incorrectas. Es importante notar que con aproximadamente un 0.15 % de error en la imagen fuente transmitida generan llaves de decodificación incorrectas, incluso si se tienen los parámetros afines correctos y el 99.8 % de la imagen fuente original. Por lo tanto, se debe asegurar la fidelidad en la imagen fuente transmitida para que el proceso funcione de forma óptima y se pueda recuperar exitosamente la información encriptada.

7.5 Aleatoriedad de las imágenes generadas en el PGI_{at}

El sistema de encriptación de doble máscara de fase basado en una arquitectura $4f$ mostrado en la Figura 7.20 y descrito en la Sección 2.2 requiere de dos máscaras de fase con distribución aleatoria para codificar adecuadamente la información.

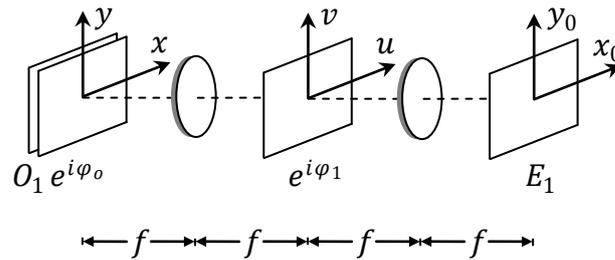


Figura 7.20: Sistema de encriptación de doble máscara de fase arquitectura $4f$. f es la distancia focal de las lentes, O_1 es el objeto de entrada, $e^{i\varphi_0}$ es la primera máscara de fase, $e^{i\varphi_1}$ es la llave de seguridad y E_1 es el objeto encriptado.

Se ha propuesto que estas máscaras de fase pueden ser generadas a partir de la imagen $I_{at}^{(N)}$, la cual es resultado de aplicar N veces el proceso PGI_{at} regido por los parámetros afines. Ya que las llaves de codificación deben tener una distribución de fase pseudoaleatoria con valores uniformemente distribuidos entre 0 y 2π , a la imagen $I_{at}^{(N)}$ se le asignan valores proporcionales de fase dependiendo de sus valores de intensidad.

Matemáticamente esta operación puede ser expresada como:

$$M_{at}^{(N)} = \exp\left(\frac{I_{at}^{(N)}}{(2^8 - 1)} 2\pi i\right) \quad (7.21)$$

donde $M_{at}^{(N)}$ es la máscara de fase pura que representa la llave de encriptación generada a partir de una $I_{at}^{(N)}$ de 8 bits. La constante de normalización $(2^8 - 1)$ asegura que los valores de fase están distribuidos entre 0 y 2π .

Una vez realizada esta asignación, se emplean estas máscaras de fase como llaves de encriptación en un SOV de encriptación $4f$ (Sección 7.6). Debido a que las llaves de seguridad generadas deben exhibir un comportamiento pseudoaleatorio, en esta sección se discute estas características de las $I_{at}^{(N)}$ de orden superior.

Para que estas máscaras de fase puedan ser utilizadas como llaves de encriptación, inicialmente el histograma de la imagen $I_{at}^{(N)}$ debe tener una distribución uniforme de niveles de gris entre 0 y 255, con media normalizada 1/2. Para verificar estas características, en la Figura 7.21 se muestran los histogramas de las diferentes imágenes $I_{at}^{(N)}$ mostradas en la Figura 7.8 que fueron obtenidas aplicando los parámetros afines de la Tabla 7.1.

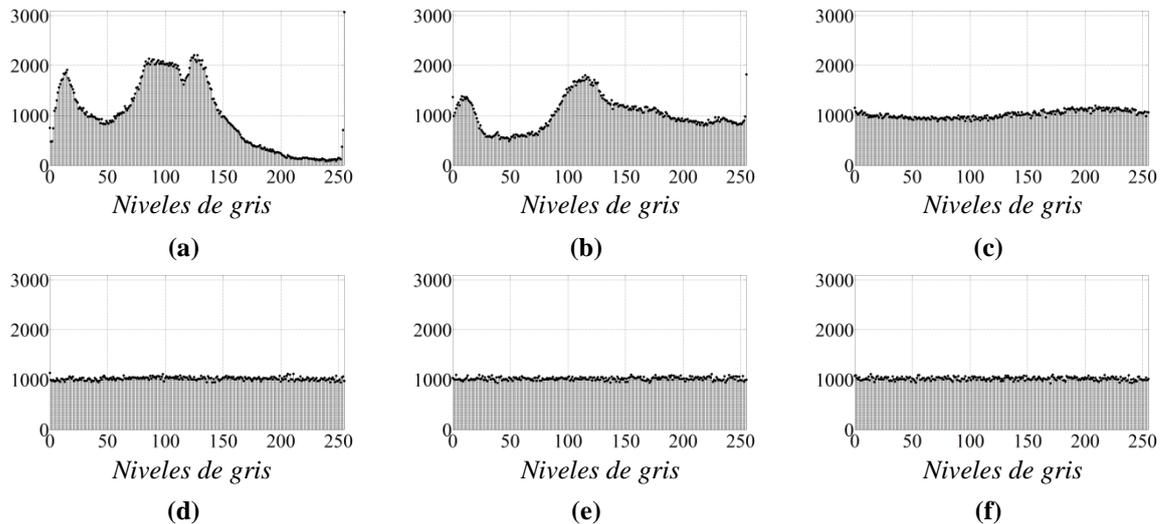


Figura 7.21: Histogramas de imágenes generadas por transformaciones afines para diferentes ordenes de iteración. (a) Imagen fuente, (b) $I_{at}^{(1)}$, (c) $I_{at}^{(3)}$, (d) $I_{at}^{(5)}$, (e) $I_{at}^{(9)}$, (f) $I_{at}^{(15)}$.

Se puede observar como a medida que el orden de iteración del PGI_{at} va aumentando, el histograma de la imagen va adquiriendo una distribución uniforme. Al

realizar la media normalizada de los valores se puede observar que tiende a $1/2$. El histograma indica que la población de los niveles de gris se iguala a medida que el orden de iteración aumenta. Para una imagen de tamaño 512×512 una distribución uniforme es una población de 1024 elementos por nivel de gris. Esta distribución produce una media normalizada de $1/2$. Sin embargo, una distribución uniforme en un histograma no asegura que la población de cada nivel de gris este distribuida homogéneamente en todo el plano de la imagen. Para verificar esta característica de las $I_{at}^{(N)}$, se evalúa la autocorrelación y el promediado angular de intensidades.

Por medio de la correlación se pueden identificar correspondencias de patrones entre dos imágenes. Debido a que una distribución aleatoria de pixeles no sigue un patrón particular y carece de periodicidad, el resultado de su autocorrelación es un pico agudo central. Cuando se realiza la autocorrelación de una imagen ordinaria cuyos pixeles no están distribuidos aleatoriamente, se podrá identificar un pico ancho. Esto indica que existen sectores o un gran número de pixeles de igual intensidad en posiciones seguidas en la imagen. Así, la distribución de la población de cada nivel de gris no es homogénea en todo el plano, por lo tanto es muy poco probable que la imagen tenga características de pseudoaleatoriedad.

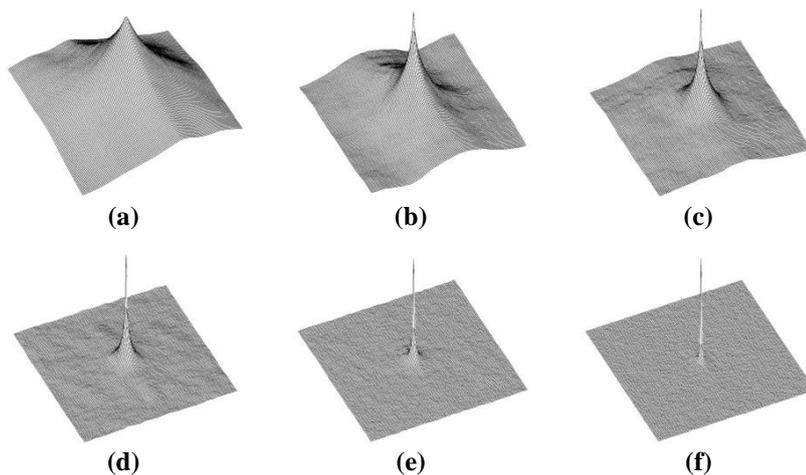


Figura 7.22: Autocorrelación de imágenes generadas por transformaciones afines para diferentes órdenes de iteración. (a) Imagen fuente, (b) $I_{at}^{(1)}$, (c) $I_{at}^{(3)}$, (d) $I_{at}^{(5)}$, (e) $I_{at}^{(9)}$, (f) $I_{at}^{(15)}$.

La Figura 7.22 muestra la autocorrelación para cada una de las imágenes de la Figura 7.8. Se puede observar que a medida que aumenta el orden de iteración N los picos

de autocorrelación tienden a ser más agudos. Esto está acorde con los histogramas de la Figura 7.21 los cuales tienden a una distribución uniforme.

Aplicando un promediado angular de intensidades a las imágenes de la Figura 7.8 se evalúa el valor medio de las intensidades de los píxeles que tienen una misma coordenada angular en el plano de la imagen. En la Figura 7.23 se muestran los resultados para los promediados angulares de intensidades medidos a lo largo de 1° a 360° en paso de 1° . Se puede observar como la Figura 7.23 (d) y Figura 7.23 (e) aún no tienen una media promedio constante. Si se sigue estrictamente esta condición sólo a partir del orden $N = 10$ se obtienen mejores características de distribución uniforme. Para el orden de iteración $N = 15$, Figura 7.23 (f), se puede observar que tienen una media promedio normalizada de aproximadamente $1/2$.

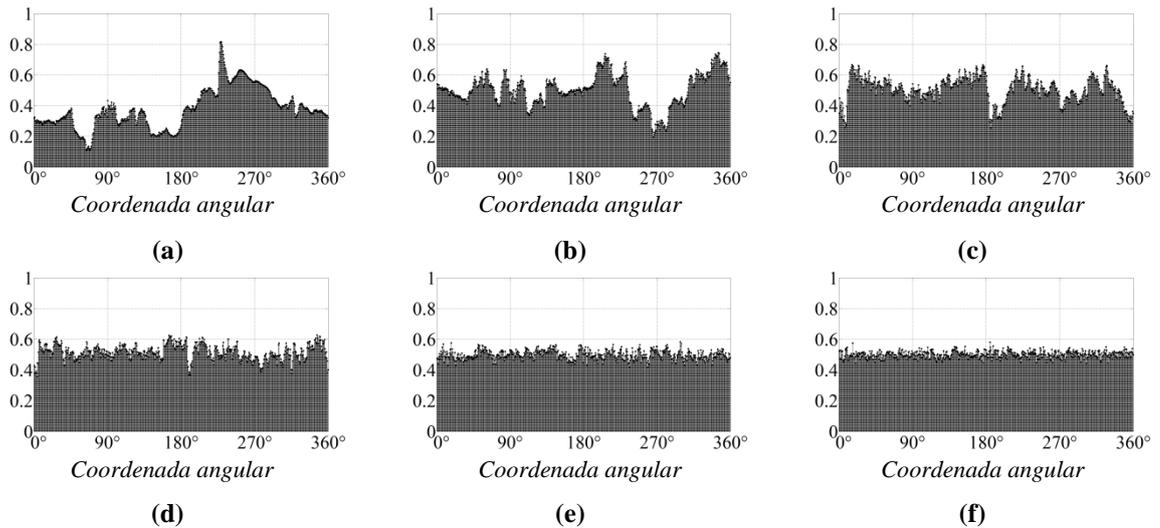


Figura 7.23: Promediado angular de intensidades de imágenes generadas por transformaciones afines para diferentes ordenes de iteración. (a) Imagen fuente, (b) $I_{at}^{(1)}$, (c) $I_{at}^{(3)}$, (d) $I_{at}^{(5)}$, (e) $I_{at}^{(9)}$, (f) $I_{at}^{(15)}$.

En resumen, una imagen $I_{at}^{(N)}$ de orden superior $N \geq 10$ asegura que las llaves de seguridad obtenidas a partir de estas distribuciones tienen valores de fase que están uniformemente distribuidos en el rango 0 y 2π y que están distribuidos homogéneamente en todo el plano. Estas características de pseudoaleatoriedad son comprobadas con sus picos de autocorrelación, con sus histogramas y sus promediados angulares de intensidad.

En la siguiente sección se presenta la aplicación de las imágenes AT como llaves de seguridad en un SOV de encriptación $4f$. Se discute la calidad de las imágenes recuperadas en términos de la variación de los parámetros afines.

7.6 Encriptación de información usando llaves de seguridad generadas a partir de imágenes $I_{at}^{(N)}$

Hasta ahora se ha evaluado el comportamiento de la pseudoaleatoriedad de las imágenes AT según el orden de iteración del proceso PGI_{at} . Se determinó que las $I_{at}^{(N)}$ de orden superior son las más adecuadas para que funcionen como llaves de seguridad. Sin embargo, esta afirmación ha sido heurística. Por lo tanto su comprobación se presenta a continuación.

En esta sección se evalúa el funcionamiento de las máscaras de fase obtenidas a partir de las imágenes AT al aplicarlas en un SOV de encriptación $4f$. En esta configuración se emplean dos máscaras de fase para codificar adecuadamente la información, una en el plano del objeto y otra en el plano de Fourier de la primera lente del sistema $4f$. Como los objetos de entrada son de amplitud, la primera máscara sólo es importante en la etapa de encriptación, más no en la etapa de decodificación. Consecuentemente para las pruebas la primera máscara de fase se considera constante. El procedimiento empleado para realizar el análisis es el siguiente:

1) Se genera un grupo de 15 imágenes AT a partir de una imagen fuente la cual se le ha aplicado una mínima transformación de traslación dada por la Tabla 7.3.

2) A cada imagen AT del procedimiento anterior se le asignan valores proporcionales de fase según la Ecuación 7.21. Estas son las máscaras de fase de referencia $M_{at}^{(N)}$.

3) Se codifica una imagen empleando cada una de las máscaras de fase generadas del ítem (2). De esta forma se obtienen 15 imágenes encriptadas. Estas 15 imágenes encriptadas son las distribuciones de referencia. A partir de estas imágenes se va a recuperar la información como se explica en los próximos ítems.

4) Con la imagen fuente, en el proceso PGI_{at} se empieza a variar individualmente cada uno de los parámetros de las transformaciones afines en pequeñas proporciones. Por ejemplo, el parámetro de traslación en el *eje* y de la transformación de la imagen I_1 varía 1, 5, 10, 20 y 35 píxeles. Con cada variación del parámetro se genera un nuevo grupo de 15 imágenes AT a las cuales se les asignan valores de fase para generar las llaves de decodificación.

5) Con cada llave de decodificación obtenida al variar el parámetro de traslación del ítem (4) se desencripta la información de las imágenes encriptadas de referencia del ítem (3). Esto es, la imagen encriptada con la $M_{at}^{(1)}$ de referencia es desencriptada con la $M_{at}^{(1)}$ obtenida al variar el parámetro de traslación 1 píxel en el PGI_{at} . Posteriormente, la imagen encriptada con la $M_{at}^{(2)}$ de referencia es desencriptada con la $M_{at}^{(2)}$ obtenida al variar el parámetro de traslación 1 píxel en el PGI_{at} . Así hasta que la imagen encriptada con la $M_{at}^{(15)}$ de referencia es desencriptada con la $M_{at}^{(15)}$ obtenida al variar el parámetro de traslación 1 píxel en el PGI_{at} . Finalmente este procedimiento es realizado para todas las variaciones de traslación, 5, 10, 20 y 35 píxeles.

6) Se realiza el procedimiento del ítem (4) y del ítem (5) variando los parámetros de rotación de la imagen I_1 en 1° , 5° , 10° , 20° y 35° . Variando los parámetros de contracción en el *eje* y de la imagen I_1 en 1.01, 1.03, 1.05, 1.07 y 1.09. Variando los parámetros de shearing en el *eje* y de la imagen I_1 en 0.01, 0.03, 0.05, 0.07 y 0.09. Variando el parámetro de reflexión en el *eje* x de I_1 y en el *eje* y de I_2 . Se reitera que únicamente se hace la variación de cada parámetro afín sin alterar los restantes. Es decir, los valores de los parámetros afines de referencia de la Tabla 7.3 se mantienen constantes y se realiza la variación de los parámetros de traslación, rotación, contracción, *shearing* y reflexión de a uno por vez.

| Imagen fuente | Reflexión (i_x, i_y) | Traslación (T_x, T_y) | Rotación (θ) | Contracción (S_x, S_y) | <i>Shearing</i> (Sh_x, Sh_y) | Módulo (n) | Iteración (N) |
|---------------|-----------------------------|------------------------------|--------------------------|-------------------------------|-------------------------------------|-------------------|----------------------|
| 1 | (1,1) | (2,0) | 0 | (1,1) | (0,0) | 256 | 15 |
| 2 | (1,1) | (0,2) | 0 | (1,1) | (0,0) | | |

Tabla 7.3: Parámetros afines usados para generar los máscaras de codificación de referencia.

Siguiendo este procedimiento se obtiene la imagen descriptada con diferentes llaves de seguridad generadas a partir de las variaciones descritas en el procedimiento anterior. Cada imagen recuperada es comparada con la imagen de referencia usando la métrica *NRMSE*. Los resultados son mostrados en la Figura 7.24.

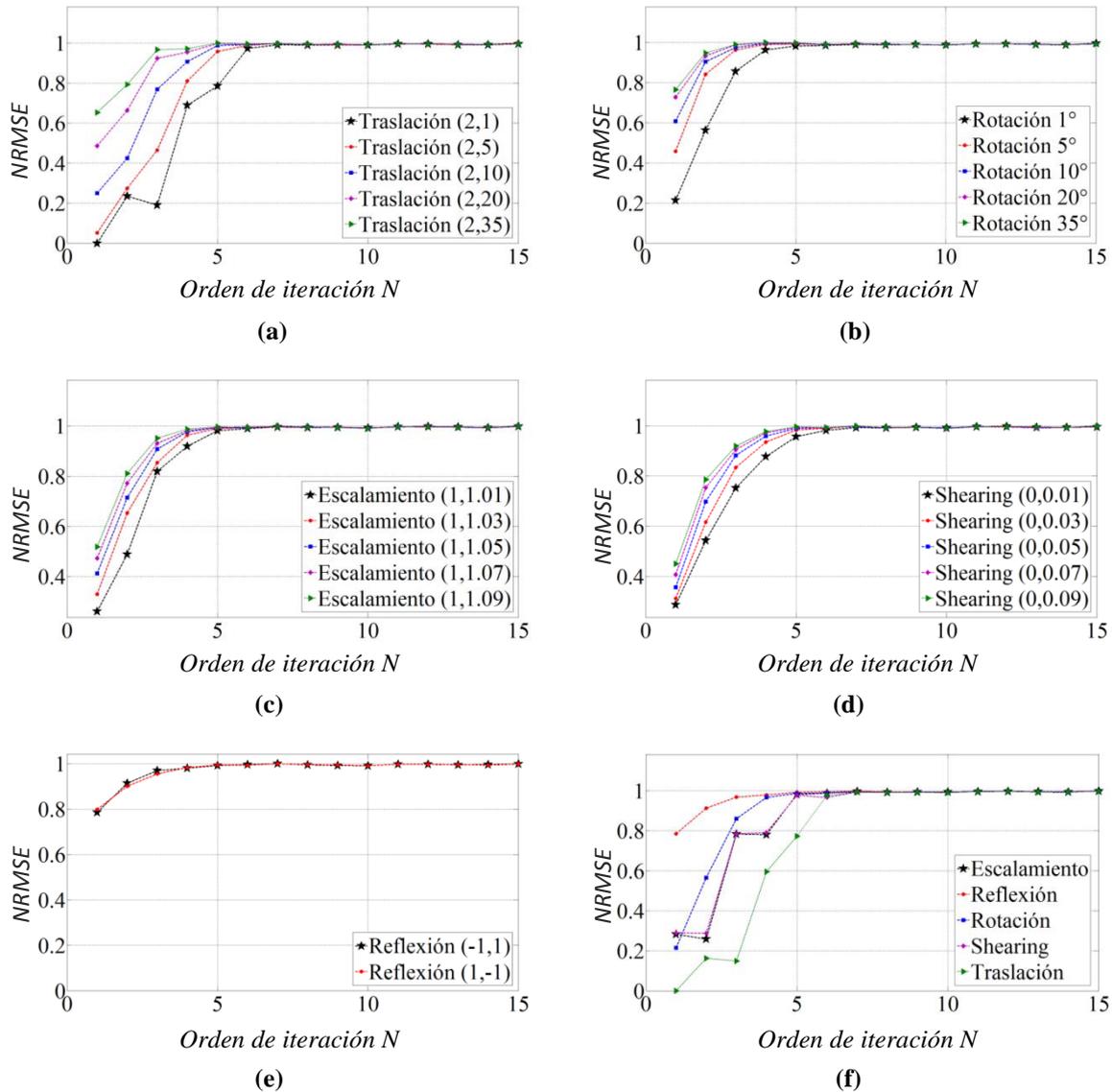


Figura 7.24: Curvas de error *NRMSE* calculadas entre la imagen de referencia y las imágenes recuperadas con máscaras de fase generadas al variar el parámetro de (a) traslación en el eje x y de la imagen I_1 en 1, 5, 10, 20 y 35 píxeles, (b) rotación de la imagen I_1 en 1°, 5°, 10°, 20° y 35°, (c) contracción en el eje x y de la imagen I_1 en 1.01, 1.03, 1.05, 1.07 y 1.09, (d) *shearing* en el eje x y de la imagen I_1 en 0.01, 0.03, 0.05, 0.07 y 0.09 y (e) reflexión en el eje x de I_1 y en el eje y de I_2 . (f) Comparación de *NRMSE* de las cinco transformaciones al recuperar la imagen con máscaras de fase generadas a partir del parámetro mínimo de variación de cada transformación.

Obsérvese como el primer valor de la curva de *NRMSE* del parámetro de traslación es cero, Figura 7.24 (a). Esto indica que la imagen recuperada y la de referencia son idénticas. Sin embargo, note que la llave de encriptación (llave de seguridad de referencia) y la llave generada con la primera traslación, deberían ser diferentes por ser dos parámetros afines distintos. Al ser las primeras imágenes AT iguales, deberían dar el mismo conjunto de transformaciones afines para todas las iteraciones y es claro que no es así ya que únicamente el primer valor del *NRMSE* en la curva de la Figura 7.24 (a) es cero. Esto es una corrección por emplear un algoritmo de optimización que selecciona la información relevante en la imagen AT antes de realimentarla en el PGI_{at} . Este proceso es incluido con el fin de realizar un manejo adecuado de memoria para no trabajar con tamaños grandes de matrices que contengan información que no haya sido el resultado de una suma modular. Por ejemplo, sumas de ceros empleados en el relleno de imágenes, de esta manera se evita un consumo innecesario de memoria.

Analizando las curvas *NRMSE*, note como tienen el mismo comportamiento y tienden a un mismo valor de saturación. Esto indica que la recuperación con llaves de seguridad incorrectas tiene una distribución constante (distribución de *speckle*).

Nótese como las imágenes recuperadas con las llaves de seguridad generadas con órdenes de iteración del PGI_{at} bajo tienen un *NRMSE* menor que el *NRMSE* de las imágenes recuperadas con llaves de seguridad de órdenes más altos. Esto indica que las máscaras de fase generadas en los órdenes más bajos aun recuperan información de la información encriptada. Esto no debería ser así ya que se emplean parámetros afines diferentes (variación de 1°). Esto justifica el hecho de no ser adecuadas las máscaras obtenidas de órdenes bajos de iteración para usarlas como llaves de seguridad en el proceso de encriptación/descriptación.

Por otro lado, para los órdenes superiores, los valores de error *NRMSE* tienden al valor de saturación. Esto indica que todas aquellas imágenes encriptadas con máscaras de fase obtenidas de órdenes superiores están correctamente protegidas y no pueden ser descriptadas con otras máscaras de fase obtenidas al realizar la mínima variación de un parámetro afín.

Note como las curvas de la Figura 7.24 (a) – Figura 7.24 (d), muestran que las imágenes recuperadas con máscaras generadas con parámetros afines de menor variación, por ejemplo 1° de rotación, tienen un *NRMSE* menor que las imágenes recuperadas con máscaras generadas con parámetros afines de mayor variación, por ejemplo 10° de rotación. Esto tiene sentido ya que un parámetro afín más alto produce una imagen de mayor diferencia que un parámetro afín más bajo. Esto produce llaves de seguridad cada vez mas decorrelacionada a medida que aumenta el valor del parámetro afín.

Esta misma característica se puede evidenciar en la curva de la Figura 7.24 (e). Aquí las dos curvas empiezan casi alcanzando el límite de saturación. Esto se atribuye a que el parámetro de reflexión invierte toda la imagen en el *eje x* o *eje y*. Al hacer una comparación pixel a pixel (*NRMSE*) de la imagen original y la imagen transformada es de esperarse que exista una gran diferencia si no es una imagen simétrica. Consecuentemente, las máscaras de fase generadas donde intervenga el parámetro de reflexión, producirán llaves de seguridad decorrelacionadas más rápidamente, que cuando no se usa esta transformación.

Por último, en la curva de la Figura 7.24 (f) muestra la comparación de las curvas de *NRMSE* entre la imagen de referencia y la imagen recuperada al usar las máscaras de fase realizando la variación mínima de los parámetros de traslación, rotación, escalamiento, *shearing* y reflexión. Se puede decir que bajo las variaciones mínimas de los parámetros afines, la transformación de reflexión es quien produce mayores cambios en los órdenes más bajos de iteración, seguida de esta curva, se encuentra la transformación de rotación la cual produce cambios más significativos en la imagen fuente en comparación con las transformaciones de contracción y *shearing*, las cuales tienden a un mismo comportamiento al usar los parámetros mínimos, sugiriendo que las dos transformaciones hacen cambios parecidos a la imagen bajo estos parámetros. Por último está la transformación de traslación que produce cambios menos significativos en la imagen fuente con los valores mínimos de variación.

Por lo tanto, para la generación de una buena máscara de codificación que proteja la información eficientemente, se puede variar cada parámetro afín de a uno por vez y

generar una llave de seguridad de los órdenes superiores de iteración. Como se observó de las curvas de la Figura 7.24, es recomendable que el orden de iteración del PGI_{at} sea $N \geq 10$. Esta condición asegura que se pueden generar llaves de codificación con características pseudoaleatorias con los valores mínimos de variación en los parámetros afines. Las llaves producidas bajo estas condiciones poseen todas las propiedades necesarias para codificar eficientemente información, al igual que un difusor convencional. Esto las hace propicias para su uso en sistemas de encriptación óptica.

En esta última sección se muestra como el uso del PGI_{at} puede redefinir el protocolo convencional de transmisión de datos encriptados.

7.7 Reducción del tamaño de las llaves de seguridad transmitidas en un canal de información clásico

En el Capítulo 2 se mostró el sistema de encriptación de doble máscara de fase en configuración $4f$. En este sistema, cada información encriptada tiene asociada una llave de seguridad. Esta pareja, imagen codificada – llave de encriptación, tiene que ser transmitida al usuario para poder recuperar la información original. Note que el tamaño de transmisión aumenta linealmente a medida que se codifica información con una llave de seguridad diferente. Esto es un inconveniente al querer enviar grandes volúmenes de datos encriptados a un mismo usuario. En este sentido se acude al almacenamiento múltiple de información.

En el Capítulo 4 se mostró como la técnica de multiplexado convencional brinda la posibilidad de codificar conjuntos de datos encriptados en un único medio de registro plano. Esta técnica es de utilidad siempre y cuando el ruido de solapamiento de información sea permisible y no de gran relevancia. Del mismo modo, al emplear diferentes llaves de seguridad en cada codificación, el tamaño de información transmitida al usuario aumenta en forma lineal.

En el Capítulo 5 se presentó una solución al inconveniente del solapamiento de información presente en un multiplexado convencional. La ventaja adicional es que se

emplea una única llave de decodificación para recuperar múltiple información con la misma calidad. Esta técnica se puede aplicar para generar niveles de acceso o procesos multiusuario. Aquí, es imprescindible usar diferentes máscaras de codificación. En este aspecto, el volumen de la información transmitida también aumenta.

En todos los casos, es necesario transmitirle al usuario la imagen encriptada o el multiplexado y las múltiples llaves de seguridad. El inconveniente radica en que las llaves de codificación enviadas son del mismo tamaño que la información a encriptar. Esto representa un problema de practicidad en la transmisión de grandes volúmenes de datos en un canal de información clásico.

En el Capítulo 7 se presentó la generación de imágenes pseudoaleatorias usando transformaciones afines. Las propiedades de estas distribuciones las hacen propicias para crear llaves de seguridad y ser aplicadas en procesos de encriptación como difusores. La ventaja de esta técnica es que al usuario no se le envía directamente la máscara de fase por un canal de información que tiene la posibilidad de ser intervenido. Al usuario, se le envían los parámetros afines y la imagen fuente para que realice una réplica de la llave de seguridad en la etapa de desencriptación.

Por medio de esta técnica es posible reducir el tamaño de la información transmitida que requiere el usuario para recuperar la información original. Una transformación afín de contracción o escalamiento es una transformación lineal espacial que puede modificar el área de la imagen transformada. El control del parámetro de contracción o escalamiento junto a la suma modular permiten generar imágenes AT de mayores dimensiones a partir de imágenes fuente de menores dimensiones. Por lo tanto, no es necesario que la imagen fuente transmitida sea del mismo tamaño que la información encriptada.

Para dar un ejemplo, se realiza la siguiente experiencia. Usando un SOV de encriptación $4f$ se codifican 30 imágenes con diferentes llaves de seguridad. Cada imagen codificada tiene un tamaño específico que no influirá en los cálculos. Esto es debido a que siempre se debe transmitir la información encriptada y el proceso de reducción es únicamente en el tamaño de transmisión de las llaves de encriptación.

Convencionalmente, cada llave de seguridad es transmitida como una imagen de 8 bits que representan 256 valores discretos de fase. Asumiendo que cada llave de seguridad tiene un tamaño promedio de 220 KB, el tamaño que se le debe transmitir al usuario asociado a las máscaras de descryptación es ~ 6600 kB (30 llaves de seguridad). Este tamaño aumenta al trabajar con un número mayor de bytes por elemento.

Ahora, aplicando la técnica propuesta, en la Figura 7.25 se muestran dos imágenes de dimensiones, 512×512 píxeles y 64×64 píxeles. La primera imagen tiene un tamaño ~ 215 KB y la segunda imagen un tamaño de ~ 6 KB.



Figura 7.25: Imágenes fuente de diferente tamaño. Imagen de 8 bits de tamaño (a) 512×512 píxeles y (b) 64×64 píxeles, las cuales tienen un tamaño de ~ 215 KB y ~ 6 KB, respectivamente.

Al aplicar el PGI_{at} usando los parámetros afines de la Tabla 7.4 y usando como imagen fuente la imagen de menor dimensión, Figura 7.25 (b) (6 KB), se generan imágenes AT de dimensiones 512×512 píxeles como lo muestra la Figura 7.26

| Imagen fuente | Reflexión (i_x, i_y) | Traslación (T_x, T_y) | Rotación (θ) | Contracción (S_x, S_y) | Shearing (Sh_x, Sh_y) | Módulo (n) | Iteración (N) |
|---------------|-----------------------------|------------------------------|--------------------------|-------------------------------|------------------------------|-------------------|----------------------|
| 1 | (1,1) | (30,25) | 45 | (1.2,1.2) | (0,0) | 256 | 15 |
| 2 | (-1,1) | (20,5) | -30 | (1.2,1.2) | (0,0) | | |

Tabla 7.4: Parámetros afines usados para generar los máscaras de codificación de la Figura 7.26.

En la Ecuación 7.20, los parámetros de contracción o escalamiento son los elementos principales que hacen posible que se aumente considerablemente el tamaño de la imagen transformada. En la Figura 7.26, el tamaño de todas las imágenes es de 512×512 píxeles. De esta manera se puede observar como la aplicación del proceso PGI_{at} iteradas veces va generando información en todo el espacio de la matriz. Note como en la parte central de las imágenes se producen valores que tienden a estar uniformemente

distribuidos. Como es regular, a partir del orden de iteración $N \geq 10$ la distribución posee características pseudoaleatorias. La Figura 7.26 (f) tiene valores de niveles de gris uniformemente distribuidos entre 0 y 255 y distribuidos homogéneamente en todo el plano.

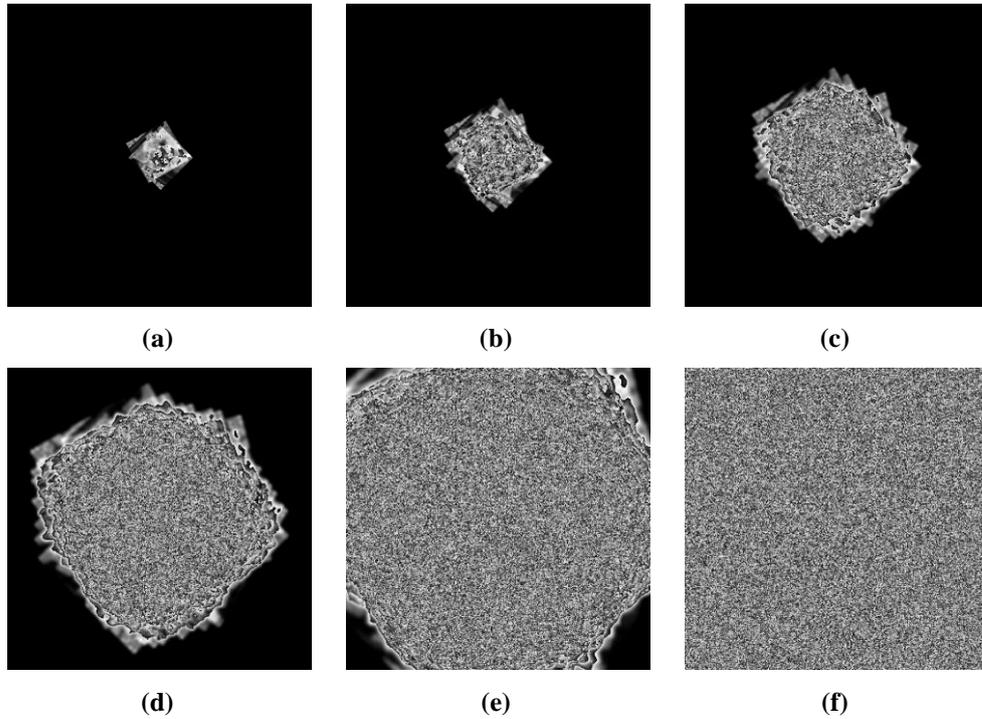


Figura 7.26: Generación de una imagen AT de tamaño 512×512 píxeles a partir de una imagen de tamaño 64×64 píxeles. Orden de iteración (a) 1, (b) 3, (c) 5, (d) 7, (e) 9 y (f) 12 del proceso PGI_{at} .

Estas características son comprobadas en la Figura 7.27. Aquí se muestra su autocorrelación y su promediado angular de intensidades.

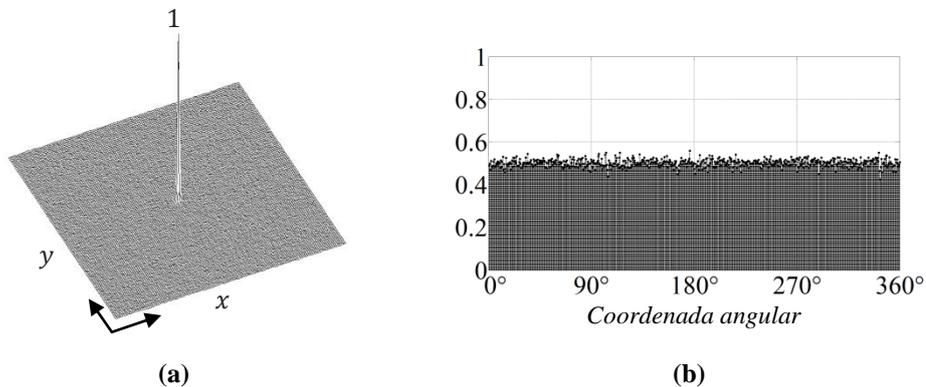


Figura 7.27: Características pseudoaleatorias que exhibe la distribución de la imagen de la Figura 7.26 (f). (a) autocorrelación y (b) promediado angular de valores de intensidad normalizados.

Consecuentemente, los tamaños de transmisión se reducen ya que las llaves de seguridad se generan a partir de imágenes fuente de menores dimensiones que la imagen encriptada.

En términos de tamaño, cada parámetro afín puede ser enviado independientemente pesando cada uno ~ 2 KB. Para generar 30 llaves de seguridad se requiere en el peor de los casos usar 600 parámetros afines. El tamaño de la información transmitida de estos parámetros afines, cada uno por canales independientes, sería ~ 1200 KB. Esto reduce ~ 5.5 veces el tamaño de la información transmitida para decodificar las 30 imágenes. Sería factible enviar los parámetros afines agrupando los 20 parámetros en una sola variable de ~ 3 KB. Por lo tanto la información transmitida sería aproximadamente ~ 100 KB incluyendo la imagen fuente. De esta forma, el tamaño se reduce ~ 66 veces en comparación a un sistema convencional de transmisión.

Este comportamiento se muestra en las curvas de la Figura 7.28. Aquí se muestra el tamaño de información total transmitido al usuario final en función del número de máscaras de decodificación transmitidas.

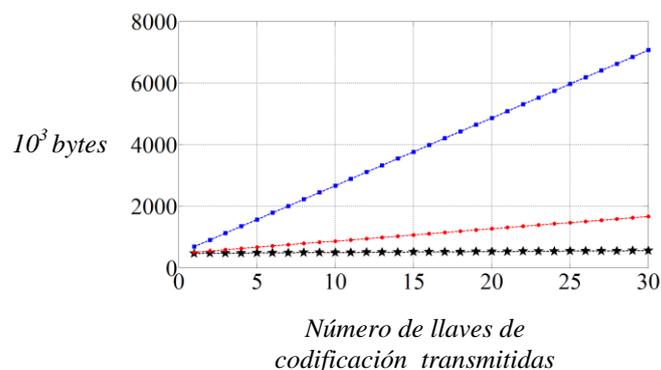


Figura 7.28: Tamaño de información en kilobytes en función del número de máscaras de fase transmitidas al usuario final.

Las curvas representan tres casos de transmisión de un multiplexado. La curva de color azul muestra el resultado de los tamaños de transmisión en un sistema convencional de encriptación al transmitir el multiplexado de información encriptada y las máscaras de decodificación por canales independientes.

Por otro lado, la curva de color rojo muestra los tamaños al transmitir el multiplexado, la imagen fuente de 64×64 píxeles y los 20 parámetros de las

transformaciones afines. En este caso, cada parámetro es transmitido por un canal independiente. Aquí se reduce el tamaño de transmisión ~ 5.5 veces respecto al primer caso.

Finalmente, la curva de color negro muestra los tamaños al transmitir el multiplexado, la imagen fuente de 64×64 píxeles y los 20 parámetros de las transformaciones afines. En este caso se transmiten los 20 parámetros afines como una sola variable en forma vectorial. De esta forma se logra reducir el tamaño de transmisión ~ 66 veces respecto al primer caso.

Cabe resaltar que independiente de la naturaleza del sistema de encriptación, si es un sistema óptico, un sistema óptico-digital o un sistema óptico virtual, esta técnica es aplicable. En los dos primeros casos el difusor puede ser un SLM al cual se le introduce una secuencia digital. Esta secuencia pseudoaleatoria introducida en el SLM puede ser producida por la técnica propuesta.

Por lo tanto, la generación de distribuciones pseudoaleatorias es aplicable a cualquier sistema de encriptación donde intervenga un difusor aleatorio. Su aplicación trae consigo ventajas en términos de transmisión. Vuelve al sistema de encriptación más seguro ante posibles intrusiones del canal de comunicación y reduce considerablemente el tamaño de la información necesaria para decodificar grandes volúmenes de información.

En resumen, esta técnica propone un nuevo protocolo en la transmisión de información encriptada en un canal de información clásico. La técnica propuesta emplea otra estrategia de transmisión de los datos requeridos para descryptar adecuadamente la información original. Por otro lado, esta técnica permite obtener una mayor velocidad de transmisión al minimizar el tamaño de las llaves de seguridad requeridas por el usuario. Por último, brinda un grado mayor de protección que los sistemas convencionales de encriptación en la transmisión de la información resguardada, esto es gracias a que no es necesario enviar por un único canal de comunicación la llave de seguridad como una sola unidad, por el contrario se puede enviar por diferentes canales de comunicación la información necesaria para que el usuario genere su llave de descryptación. Esto minimiza los riesgos de interceptación en la transmisión de la información.

7.8 Bibliografía

- [7.1] B. Javidi, *Optical and Digital Techniques for Information Security*, Springer Verlag, New York, (2005).
- [7.2] M. S. Millan, E. Pérez, *Optical Data Encryption*. pp. 739-767 en G. Cristóbal, P. Schelkens, H. Thienpont. *Optical and digital image processing fundamentals and applications*. WILEY-VCH Verlag GmbH & Co. KGaA, Boschstr. 12, 69469 Weinheim, Germany (2011).
- [7.3] A. Kumar, M. Singh, K. Singh, *Speckle Coding for Optical and Digital Data Security Applications*, Ch. 6, en G. H. Kaufmann *Advances in Speckle Metrology and Related Techniques*. WILEY-VCH Verlag & Co. KGaA, Boschstr. 12, 69469 Weinheim, Germany (2011).
- [7.4] O. Matoba, B. Javidi, “Encrypted optical storage with wavelength-key and random phase codes,” *Appl. Opt.* 38, 6785-6790 (1999).
- [7.5] O. Matoba, B. Javidi, “Encrypted optical memory system using three-dimensional keys in the Fresnel domain,” *Opt. Lett.* 24, 762-764 (1999).
- [7.6] G. Situ, J. Zhang, “Double random-phase encoding in the Fresnel domain,” *Opt. Lett.* 29, 1584-1586 (2004).
- [7.7] G. Situ, J. Zhang, “Multiple-image encryption by wavelength multiplexing,” *Opt. Lett.*, 30(11), 1306-1307 (2005).
- [7.8] G. Situ, J. Zhang, “Position multiplexing for multiple-image encryption,” *J. Opt. A: Pure Appl. Opt.*, 8, 391–397 (2006).
- [7.9] J. F. Barrera, R. Henao, M. Tebaldi, N. Bolognini, R. Torroba, “Multiplexing encryption-decryption via lateral shifting of a random phase mask,” *Opt. Commun.* 259, 532–536 (2006).
- [7.10] J. F. Barrera, R. Henao, M. Tebaldi, N. Bolognini, R. Torroba, “Multiplexing encrypted data by using polarized light,” *Opt. Commun.* 260, 109–112 (2006).

- [7.11] M. Singh, A. Kumar, K. Singh, “Multiplexing in optical encryption by using an aperture system and a rotating sandwich random phase diffuser in the Fourier plane,” *Optics and Lasers Engineering*, 46(3), 243–251 (2008).
- [7.12] M. Singh, A. Kumar, K. Singh, “Encryption and decryption using a sandwich phase diffuser made by using two *speckle* patterns and placed in the Fourier plane: Simulation results,” *Optik*, 120(17), 916–922 (2009).
- [7.13] H. T. Chang, H. E. Hwang, C. L. Lee, “Position multiplexing multiple-image encryption using cascaded phase-only masks in Fresnel transform domain,” *Opt. Commun.* 284(18), 4146–4151 (2011).
- [7.14] M. Madjarova, M. Kakuta, M. Yamaguchi, N. Ohya, “Optical implementation of a stream cipher based on the irreversible cellular automata algorithm,” *Opt. Lett.* 22 1624–1626 (1997).
- [7.15] S. Zhang, M. Karim, “High-security optical integrated stream ciphers,” *Opt. Eng.* 38, 20–24 (1999).
- [7.16] T. Sasaki, H. Togo, J. Tanida, Y. Ichikoka, “Stream cipher based on pseudorandom number generation with optical affine transformation,” *Appl. Opt.* 39, 2340–2346 (2000).
- [7.17] E. Rueda, C. Vera, B. Rodríguez, R. Torroba, “Synchronized chaotic phase masks for encrypting and decrypting images,” *Optics communications*, 281(23), 5750–5755 (2008).
- [7.18] B. Jähne, *Digital Image Processing*. Springer-Verlag Berlin Heidelberg (2005). pp. 275-279.
- [7.19] T. Sasaki, H. Togo, J. Tanida, Y. Ichikoka, “Stream cipher based on pseudorandom number generation with optical affine transformation,” *Appl. Opt.* 39 2340–2346 (2000).
- [7.20] R. Séroul, *The Bézout Theorem in Programming for Mathematicians*, Springer-Verlag, Berlin, 2000, p. 10.

- [7.21] P. Tuyls, B. Skoric, T. Kevenaer, *Security with Noisy Data On Private Biometrics, Secure Key Storage and Anti- counterfeiting*, Springer-Verlag London Limited (2007), pp. 277-297.
- [7.22] I. W. Jung, *Spatial Light Modulators and Applications Spatial Light Modulators for Applications in Coherent Communication, Adaptive Optics and Maskless Lithography* (VDM Verlag, 2009).
- [7.23] Y. Bitou, "Digital phase-shifting interferometer with an electrically addressed liquid-crystal spatial light modulator," *Opt. Lett.* 28(17), 1576–1578 (2003).
- [7.24] C. Kohler, T. Haist, X. Schwab, W. Osten, "Hologram optimization for SLM-based reconstruction with regard to polarization effects," *Opt. Express* 16, 14853-14861, (2008).
- [7.25] T. Meeser, C. Kopylow, C. Falldorf, "Advanced Digital Lensless Fourier Holography by means of a Spatial Light Modulator," in *3DTV-Conference: The True Vision - Capture, Transmission and Display of 3D Video (3DTV-CON)*, 2010 2010), 1–4.
- [7.26] C. Falldorf, M. Agour, C. V. Kopylow, R. B. Bergmann, "Phase retrieval by means of a spatial light modulator in the Fourier domain of an imaging system," *Appl. Opt.* 49(10), 1826–1830 (2010).
- [7.27] W. Liu, G. Yang, H. Xie, "A hybrid heuristic algorithm to improve known-plaintext attack on Fourier plane encryption," *Opt. Express* 17, 13928-13938 (2009).
- [7.28] J. Angeles, *Fundamentals of robotic mechanical systems: theory, methods, and algorithms*. Ed. Springer – Verlag (2003).
- [7.29] J. Craig, *Introduction to Robotics: Mechanics and Control* Ed. Addison – Wesley, (2005).
- [7.30] B. Jähne, *Digital Image Processing*. Springer-Verlag Berlin Heidelberg (2005). p. 17.

- [7.31] B. Jähne, Digital Image Processing. Springer-Verlag Berlin Heidelberg (2005). p. 212.
- [7.32] R. Gonzalez, R. Woods, Digital Image Processing, Prentice-Hall, Inc. (2007). p.333.
- [7.33] G. Blanchet, M. Charbir, Digital Signal and Image Processing using Matlab. ISTE Ltd, (2006). p. 101.
- [7.34] R. Gonzalez, R. Woods, S. Eddins, Digital Image Processing using Matlab, Prentice-Hall, Inc. (2003). p.141.

Capítulo 8

Conclusiones y perspectivas

Los desarrollos alcanzados en esta Tesis fueron realizados dentro del marco de la óptica virtual. Si bien los sistemas propuestos aun no han sido implementados analógicamente, se generaron sus representaciones físicas en forma digital. Esta propuesta permite obtener una representación visual de los resultados que arrojaría la experiencia real. Una extensión importante de esta metodología incluirá el desarrollo de elementos ópticos en aplicaciones gráficas optimizadas. Esto requiere de un amplio conocimiento en la manipulación de gráficos por computador así como de los conceptos ópticos involucrados que permitan agregar características detalladas del modelado del sistema analógico. El objetivo principal de este desarrollo sería manipular en un ambiente gráfico los elementos ópticos virtuales de manera interactiva, de tal manera que el experimentador se centralice únicamente en generar el modelo del sistema real con los elementos gráficos desarrollados.

Al inicio de este trabajo se implementaron elementos ópticos virtuales que se articulan entre sí para modelar sistemas analógicos complejos cuya descripción está dada por la teoría escalar de la difracción. La implementación de estos sistemas incluyó la programación del modelo, su calibración y caracterización, esto con el fin de asegurar el óptimo rendimiento en cada experiencia virtual. En esa instancia, se aseguró el correcto funcionamiento de los elementos ópticos implementados al presentar los resultados de experiencias básicas de diferente complejidad, desde transformadas ópticas de Fourier hasta la reconstrucción de un holograma digital. Al corroborarse el correcto funcionamiento del modelado de los elementos virtuales, el experimentador está en condiciones de diseñar, evaluar y depurar variantes de un sistema analógico. Con estos

fundamentos, se implementó el sistema de encriptación de doble máscara de fase en configuración 4f.

Con este sistema, en el Capítulo 4 se realizó un estudio de la técnica convencional de multiplexado de imágenes encriptadas en medios de registro planos. Se mostró como, a partir de este multiplexado, las imágenes recuperadas presentan una degradación en su calidad. También se comprobó que el deterioro de estas imágenes se debe a dos casos particulares. En el primero, se mostró que la imagen recuperada consiste en la superposición de todas las imágenes descryptadas correctamente. En el segundo caso, se comprobó que la imagen recuperada es la superposición de la imagen de interés con aquellas que permanecen aún codificadas. Del mismo modo, se demostró que la degradación en las imágenes no depende del número de imágenes multiplexadas, sino de la suma total de la energía de todas las imágenes de entrada. De esta forma se comprobó como la técnica de multiplexado convencional impone restricciones sobre las características de los objetos que se van a encriptar. Estos motivos conducen a calificar al multiplexado lineal como una técnica ineficiente en la manipulación de grandes volúmenes de información. Los resultados obtenidos en el Capítulo 4 evidenciaron la necesidad de investigar una nueva estrategia que permita procesar, transmitir y recuperar eficientemente un mayor volumen de datos al manipulado por las técnicas actuales de encriptación.

Con el objetivo de suplir las deficiencias del multiplexado lineal, se desarrolló la técnica de encriptación de eventos dinámicos. Esta técnica permitió recuperar múltiples imágenes a partir de un multiplexado, sin la influencia del solapamiento de información. Y se sustentó mediante la inclusión de la técnica de modulación theta que es aplicada sobre las imágenes encriptadas antes de efectuar el multiplexado convencional. Se mostró como esta variante permite desplegar en un plano de filtrado la información asociada a cada imagen codificada. Este hecho generó el concepto original de la realización de la primera película encriptada por medios puramente ópticos sobre la base que la técnica desarrollada permitió sincronizar a tiempo real las imágenes correctamente recuperadas. Se logró así mejorar diferentes aspectos respecto a los existentes en la línea de la encriptación óptica. En primera medida se aumentó la cantidad de imágenes codificadas que se pueden recuperar a partir de un multiplexado sin la presencia de solapamiento de información y

con calidad uniforme. Por otro lado se redujo el número de llaves de codificación a una única llave para acceder a toda la información del multiplexado. Este concepto permitió desarrollar tres aplicaciones importantes. En primer lugar, se realizó la encriptación de escenas dinámicas monocromáticas. Se codificó una escena compuesta de 22 imágenes de 8 bits sincronizada a 10 imágenes por segundo para constituir una película de 2.2 segundos de duración. En segundo lugar, se realizó la encriptación de escenas dinámicas policromáticas. Para ello se codificó una escena compuesta de 30 imágenes de 24 bits sincronizada a 10 imágenes por segundo para constituir una película a color de 3 segundos de duración. Se analizó entonces una estrategia para encriptar una película de mayor duración. Esto conllevó a variar el diámetro de la pupila en el plano de la llave de seguridad mientras se mantienen los valores de los restantes parámetros del sistema. De esta forma se encriptaron dos películas de 48 y 126 imágenes a color, respectivamente, ambas sincronizadas a 10 imágenes por segundo. Se encontró que visualmente, las escenas que contienen pocos detalles soportan ser descryptadas a partir del multiplexado de una película de mayor duración. Por el contrario, los detalles finos de los objetos (asociado a altas frecuencias espaciales) se pierden por la granularidad del speckle como consecuencia de reducir la pupila para aumentar la cantidad de imágenes multiplexadas. También se pudo verificar que las imágenes descryptadas de cada película mantienen siempre su calidad, demostrándose que la adición de ruido es debido a la variación de la pupila, mas no se produce por la técnica en sí. De esta manera, se comprueba que la técnica desarrollada no impone restricciones sobre las características de los objetos a codificar. Finalmente se comprobó la viabilidad de un proceso multiusuario para encriptar múltiples películas y transmitir las en un único multiplexado. En este caso, cada película (tres en total) compuesta de imágenes de 8 bits y de 1.6 segundos de duración es encriptada con una llave distinta. Se corroboró que todas las películas presentan en sus imágenes descryptadas la misma calidad.

Esta técnica desarrolla sugiere otras variantes que conduzcan a nuevas experiencias.

Una variante que redundaría en evitar pérdidas de energía consiste en introducir elementos ó redes de fase diseñados tal que difracten y escojan los órdenes tal como se

implementó para las redes de amplitud. Esto permitiría disminuir el ruido introducido por la modulación de las redes periódicas de amplitud.

Otra experiencia puede consistir en realizar la encriptación y recuperación de una escena dinámica con sonido. Como se muestra en el archivo (Media_15.avi), se puede generar una película monocromática o policromática sincronizando dos archivos multimedia. El primer archivo multimedia es la secuencia de imágenes correctamente descriptadas y el segundo archivo multimedia es la señal de sonido que debe ser post-procesada al haber sido multiplexada conjuntamente con las imágenes encriptadas. Para codificar una señal de sonido por medios ópticos se debe realizar un mapeo de la señal y reasignarla en una matriz bidimensional y proceder entonces con la etapa de encriptación. El post-procesado es necesario ya que los sistemas ópticos virtuales introducen speckle adicionándose como ruido de fondo. El inconveniente de este proceso radica en la imposibilidad de hacerlo a tiempo real. A menos que se evite el post-procesado y se acepte la recuperación de sonido degradado tal como se escucha en el archivo referenciado anteriormente. Sin embargo, esta propuesta es una buena alternativa para encriptar señales mixtas que combinan imágenes y sonido.

Otra experiencia sugerida puede consistir en realizar la encriptación y recuperación de una escena dinámica anaglífica. Una imagen anaglífica es realizada superponiendo dos capas de color de una misma escena vista con dos perspectivas diferentes para producir el efecto de profundidad. Al filtrar diferentes canales de cada perspectiva, al combinarlas en una sola imagen y al verlas con unas gafas anaglíficas, o con filtros de color apropiados dará como resultado que cada ojo observa una imagen levemente diferente. Como se muestra en el archivo (Media_16.avi), se reconstruiría una escena dinámica con sensación de profundidad. En este caso, el speckle parece imponerse en un plano frontal, dando la sensación que el objeto está detrás del ruido de speckle.

Otra posible implementación de encriptación de eventos dinámicos podría apelar al procesamiento con luz blanca. Para ello se debe recurrir a incluir en las arquitecturas ópticas filtros interferenciales, espejos dicróicos y combinadores de haz. Asimismo, las redes de modulación tendrían que ajustarse convenientemente en frecuencia para que los

órdenes de difracción no cambien su ubicación en el plano de filtrado. Una última variante en esta línea, podrían tener en cuenta el estado de polarización de la luz en la etapa de encriptación mediante la inclusión de elementos de polarización. De esta manera la imagen o imágenes recuperadas pueden ser construidas a partir de varios órdenes de difracción que contengan estados de polarización diferentes.

Más allá de la línea de encriptación de eventos dinámicos, esta técnica podría ser usada para generar secuencias de textos alfanuméricos al aprovechar la selección del orden de difracción en la etapa de filtrado. Dado que se genera un gran número de combinatorias, si cada orden difractado tiene asociado una letra, símbolo o número, la secuencia de filtrado actuará como llave de seguridad. Si por ejemplo, se tiene 32 órdenes difractados y el código consiste de 4 letras donde importa la secuencia de repetición se tendrían 652458240 códigos posibles, asumiendo que se tiene la llave de codificación correcta.

Finalmente, se pueden sugerir otras experiencias. Entre ellas están las propuestas por David M. Paganin en la sección "Spotlight on optics" de la OSA. Dentro de las aplicaciones propuestas se encuentra usar transformaciones unitarias en vez de transformadas rápidas de Fourier, incorporar marcas de agua, niveles adicionales de encriptación con la selección adecuada de redes de modulación no uniformes, realizar un estudio sistemático del ruido y la estabilidad del proceso de encriptación – desencriptación, la incorporación de técnicas de recuperación de fase y realizar estudios del rol de la coherencia parcial, entre otras.

En la parte final de esta Tesis se implementó un método para generar máscaras de fase pseudoaleatorias para aplicaciones en técnicas de seguridad óptica. El método desarrollado está basado en la aplicación de transformaciones geométricas sobre una imagen fuente. Las transformaciones aplicadas, de translación, rotación, reflexión, escalamiento y *shearing* son definidas por parámetros afines. Este proceso fue implementado digitalmente y se tomó ventaja del hecho que los actuales sistemas de encriptación óptica son sistemas híbridos donde participan dispositivos optoelectrónicos, principalmente moduladores espaciales de luz. Las máscaras de fase implementadas pueden ser utilizadas al desplegarse en fase en un SLM. El rango de las fases generadas

puede ser controlado por medio de una suma modular incluida en el proceso de generación de las imágenes, ajustándose a los rangos de operación en fase del SLM. Se comprobó que las imágenes generadas presentan gran sensibilidad en su distribución pseudoaleatoria al realizar cambios mínimos de cualquiera de los parámetros afines así como ante cambios locales en la imagen fuente. Se demostró que esta imagen fuente debe ser transmitida fielmente hasta en un 99% para generar la misma distribución pseudoaleatoria. La imagen fuente no puede presentar pérdidas de información, ni agregado de ruido aditivo o multiplicativo. Además no puede emplearse una imagen restaurada con filtros de procesamiento digital y no puede ser transmitida en un formato de compresión con pérdida de información. Todos estos factores optimizan la seguridad de las técnicas convencionales de codificación al aplicar estas máscaras como llaves de seguridad. Se demostró también que se puede obtener una máscara de fase de gran tamaño al aplicar el proceso de generación sobre una imagen fuente de tamaño reducido. Esto brinda una ventaja adicional en los procesos de transmisión clásicos de información encriptada. Convencionalmente se debía transmitir un conjunto de información codificada y sus llaves de seguridad que ocupan, por lo menos, el mismo tamaño que la información encriptada. Con la técnica desarrollada, el tamaño de las llaves de seguridad se reduce notoriamente al tener que transmitir sólo una imagen fuente de pequeñas proporciones y los parámetros afines de generación. Se propuso como aspecto original de esta técnica que el propio usuario genera la llave de seguridad en la estación de descifrado. De esta manera la llave de seguridad no es transmitida directamente por un canal de comunicación que siempre tiene la posibilidad de ser intervenido. En este método, las funciones que definen la llave de seguridad son los parámetros afines junto a la imagen fuente. Y cada uno de ellos pueden ser enviados independientemente por un canal de comunicación tornando más difícil para un intruso violar la seguridad alcanzada al aplicar esta técnica.

Las transformaciones afines aplicadas en el proceso de generación de imágenes pseudoaleatorias pueden extenderse para generar máscaras de fase en tres dimensiones. Esta optimización abre una variante interesante para generar a partir de una imagen fuente bidimensional de tamaño reducido arreglos tridimensionales que pueden aplicarse como llaves de seguridad. La efectividad de este método se basa en que para poder recuperar la

información original, la compensación de fases que realiza la llave de decodificación debe ser idéntica a las fases introducidas en el proceso de encriptación. Un arreglo de fases que actué como llave en tres dimensiones brindaría un grado adicional de seguridad ya que la máscara de encriptación no se encuentra únicamente en el plano de Fourier, invalidando ataques convencionales de texto plano o texto cifrado. Por otro lado, por su carácter tridimensional, cada llave estaría compuesta de planos paralelos de valores de fases. Esta característica permitiría generar niveles de acceso a información encriptada con uno o varios planos de una misma llave de seguridad. Adicionalmente, la información encriptada puede ser multiplexada usando la técnica de encriptación de eventos dinámicos. A partir de esta variante la llave en tres dimensiones puede actuar como llave única o como múltiples llaves de codificación. Lo más importante de este desarrollo radicaría en poder controlar la distribución pseudoaleatoria de una máscara tridimensional de fase a partir de un número reducido de parámetros afines.

Apéndice A

Conceptos básicos de holografía digital

A.1 Introducción

La holografía permite recuperar el campo complejo de un objeto (amplitud y fase) a partir de la reconstrucción de su holograma [A.1]. La reconstrucción se realiza usando un haz de iluminación que tiene las mismas propiedades del haz de referencia empleado en el registro holográfico. Cualquier cambio en su amplitud, fase, polarización, etc., resultan en la pérdida total o parcial de la información original. En este sentido, las características de la onda de referencia pueden ser vistas como parámetros de seguridad para reconstruir la información codificada en el holograma. Este es el principio básico de encriptación de información usando las técnicas de holografía y holografía digital como parámetros de seguridad [A.2], [A.3], [A.4].

De forma general, en la rama de la encriptación óptica las arquitecturas de codificación que están basadas en sistemas ópticos virtuales y sistemas ópticos-digitales están directamente relacionadas con la holografía digital. Esta herramienta permite registrar electrónicamente el campo complejo de la información encriptada y codificarlo en una distribución de intensidad. Posteriormente esta distribución es transmitida de manera segura por un canal de comunicación al usuario autorizado para que realice el proceso de desencriptación.

Específicamente, la holografía digital es la técnica empleada para realizar el registro digital de la información encriptada en un sistema de codificación de doble máscara de fase en configuración *4f*. Por lo tanto, todas las aplicaciones que han sido

propuestas en este trabajo podrán usar esta técnica para el registro del campo complejo de la información encriptada.

Básicamente la reconstrucción del objeto a partir del holograma digital es realizada usando la propagación descrita por la integral de Fresnel o por la propagación del espectro angular, conceptos que fueron implementados en sistemas ópticos virtuales. Por estas razones parece importante realizar una revisión simple de la técnica de holografía digital. Para profundizar en este tema se recomienda acudir a las referencias [A.5], [A.6].

Aunque esta técnica complementa el Capítulo 3, se prefiere incluirla en este apéndice para no dispersar los lineamientos que allí se presentan.

A.2 Registro y reconstrucción de un holograma digital

Cuando un objeto en tres dimensiones es fotografiado se registra únicamente su distribución de intensidad, como resultado se pierden la información de las fases relativas de las ondas provenientes de diferentes puntos del objeto. Por el contrario, la holografía permite registrar el campo complejo de la onda (amplitud y fase) codificándolo en variaciones de intensidad.

Según se muestra en la Figura A.1, el proceso de registro del holograma se realiza haciendo interferir el campo complejo del objeto $E_o(x, y) = a_o(x, y)\exp[i\varphi_o(x, y)]$ con el campo complejo de la onda de referencia $E_R(x, y) = a_R(x, y)\exp[i\varphi_R(x, y)]$, donde $a_R(x, y)$ y $a_o(x, y)$ son amplitudes y $\varphi_R(x, y)$ y $\varphi_o(x, y)$ son fases. Así, la intensidad de la superposición está dada por:

$$I(x, y) = a_o^2(x, y) + a_R^2(x, y) + E_o(x, y)E_R^*(x, y) + E_R(x, y)E_o^*(x, y) \quad (\text{A.1})$$

La diferencia entre la fase de la onda de referencia y la fase de la onda del objeto, $\varphi_R(x, y) - \varphi_o(x, y)$, es codificada en una distribución de intensidad dada por el término de interferencia $2a_o(x, y)a_R(x, y)\cos[\varphi_R(x, y) - \varphi_o(x, y)]$.

La amplitud de transmisión del holograma $h(x, y)$ registrada en la placa fotográfica, emulsión, etc., es proporcional a la intensidad y puede ser escrita como:

$$h(x, y) = h_0 + \beta\tau I(x, y) \quad (\text{A.2})$$

donde β es un parámetro que caracteriza la sensibilidad del material a la intensidad, τ es el tiempo de exposición y h_0 es la amplitud de transmisión del material sin exposición.

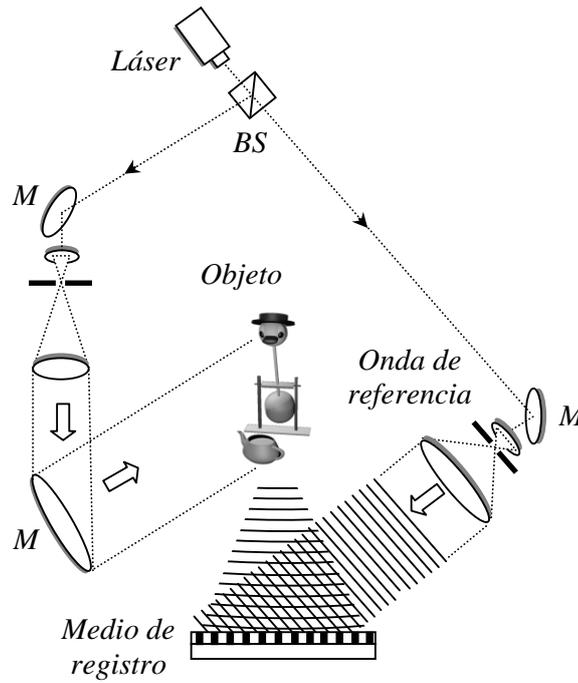


Figura A.1: Registro de un holograma. BS: divisor de haz, M: espejos. Un haz de iluminación se colima y se direcciona hacia el objeto que produce el campo complejo que interfiere en el medio de registro con la onda de referencia proveniente del segundo haz. En el medio de registro se forman franjas de interferencia que codifican la fase del objeto.

Ahora, para realizar la reconstrucción del objeto, Figura A.2, el holograma debe ser iluminado con la onda de referencia con la cual se realizó el registro holográfico. Así, multiplicando la amplitud de transmisión del holograma por la amplitud compleja del haz de referencia se tiene:

$$\begin{aligned} h(x, y)E_R(x, y) = & [h_0 + \beta\tau(a_R^2(x, y) + a_o^2(x, y))]E_R(x, y) + \beta\tau a_R^2(x, y)E_o(x, y) \\ & + \beta\tau E_R^2(x, y)E_o^*(x, y) \end{aligned} \quad (\text{A.3})$$

En el lado derecho de la igualdad, el primer término es el orden cero y representa la onda de referencia que no ha sido difractada por el holograma. El segundo término forma

la imagen virtual del objeto reconstruido, el factor $\beta\tau a_R^2$ influye únicamente en el brillo de la imagen. El tercer término genera una imagen real distorsionada del objeto la cual puede ser corregida usando el complejo conjugado del haz de referencia en la reconstrucción.

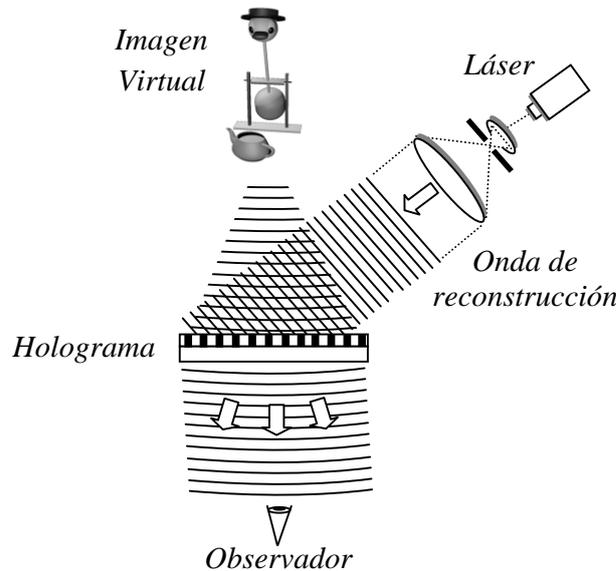


Figura A.2: Reconstrucción de un holograma. El haz de referencia usado en la etapa de registro holográfico es colimado e incide en el holograma formando la imagen virtual del objeto.

Si se reconstruye el holograma con una longitud de onda diferente a la empleada en el registro holográfico, la imagen reconstruida se verá alterada en tamaño, posición y con aberraciones. Para profundizar en estos aspectos se recomienda la referencia [A.7].

Ahora, el concepto de registrar un holograma digitalmente es ilustrado en la Figura A.3 (a). De la misma manera que en la holografía, una onda plana de referencia y el campo complejo de un objeto localizado a una distancia d del material de registro interfieren sobre una cámara CCD [A.8]. Así, el holograma $h(x, y)$ es registrado de forma discreta.

La reconstrucción a partir del holograma digital es ilustrada en la Figura A.3 (b). La imagen virtual aparece en la posición del objeto original y la imagen real es formada a una distancia d en dirección opuesta de la cámara CCD. En la reconstrucción digital, $E_R = E_R^*$ ya que son funciones sólo de amplitud, esto es $E_R = a_R + i0 = a_R$.

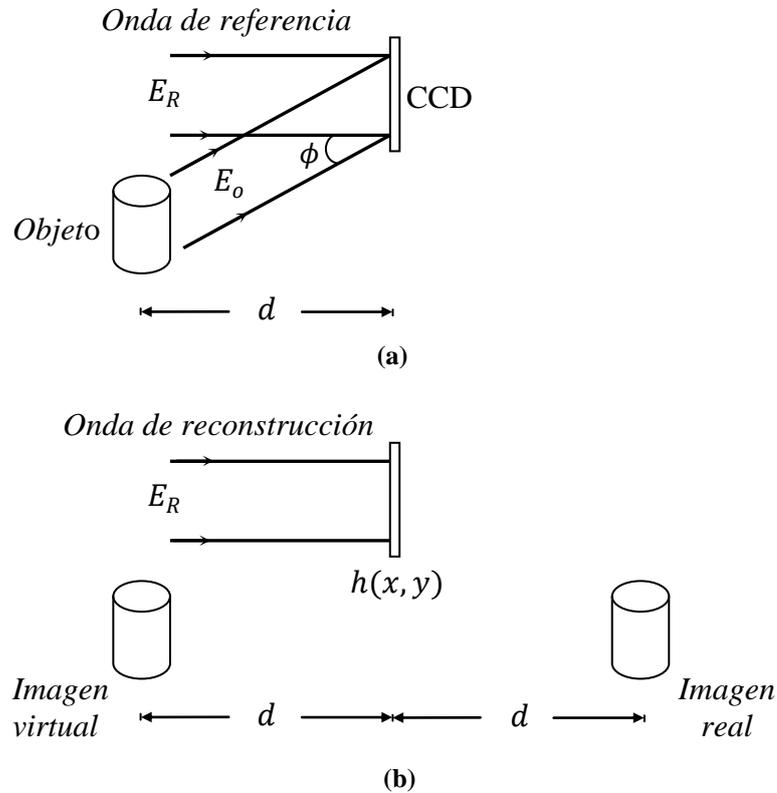


Figura A.3: Esquema básico de holografía digital. (a) Registro del holograma digital y (b) reconstrucción del objeto. E_o es la onda objeto, E_R es la onda de referencia, ϕ es el ángulo que forman E_o y E_R y $h(x, y)$ representa el holograma del objeto.

La difracción de la luz realizada por el holograma puede ser descrita por la propagación del espectro angular usando la Ecuación (3.25) o usando la integral de Fresnel, Ecuación (3.31). En una representación discreta, el holograma puede ser reconstruido como:

$$U(m_x, m_y, z) = \beta \Delta_x \Delta_y \sum_{n_x=0}^{M_x-1} \sum_{n_y=0}^{M_y-1} U(n_x, n_y, 0) e^{jk \frac{(n_x^2 \Delta_x^2 + n_y^2 \Delta_y^2)}{2z}} e^{-j2\pi \left(\frac{n_x m_x}{M_x} + \frac{n_y m_y}{M_y} \right)} \quad (\text{A.4})$$

donde $z = d$, λ es la longitud de onda, Δ_x , Δ_y , Δ_{0x} y Δ_{0y} son los intervalos de muestreo en el plano del objeto y en el plano de observación, respectivamente, n_x , n_y , m_x y m_y son números enteros entre 0 y $N - 1$, con $M_x = M_y = N$, siendo N el tamaño del holograma en pixeles. El factor β es definido por la Ecuación (3.32) y se tiene que la amplitud compleja en el plano $z = 0$ es $U(n_x, n_y, z = 0) = h(n_x, n_y) E_R(n_x, n_y)$, que es el

holograma multiplicado por la onda de referencia. Bajo otra configuración, $E_R(n_x, n_y)$ es una función compleja dependiente del ángulo de incidencia del haz de referencia [A.5].

En la Figura A.4 (a) se muestra un holograma digital y en la Figura A.4 (b) su reconstrucción numérica.

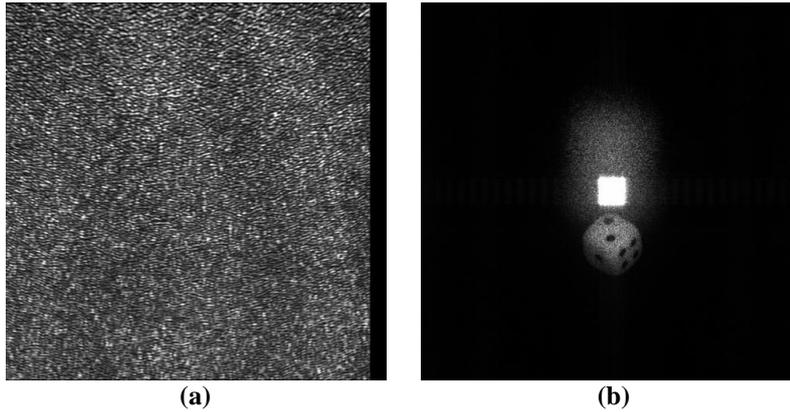


Figura A.4: (a) Holograma digital y su (b) reconstrucción numérica. Imágenes tomadas del libro *Digital Holography. Digital hologram recording, Numerical reconstructions and related techniques* [A.9]. El tamaño del holograma es de 1024×1024 píxeles, el tamaño de muestreo de entrada es $6.8 \mu\text{m}$, la longitud de onda es 632.8 nm y la distancia de registro del holograma es 1054 mm .

Ahora, para este mismo holograma se realizó la reconstrucción con los sistemas ópticos virtuales implementados de la propagación usando el espectro angular y la integral de Fresnel. La Figura A.5 (a) muestra la reconstrucción usando la integral de Fresnel y la Figura A.5 (b) y Figura A.5 (c) muestran la reconstrucción usando el espectro angular.

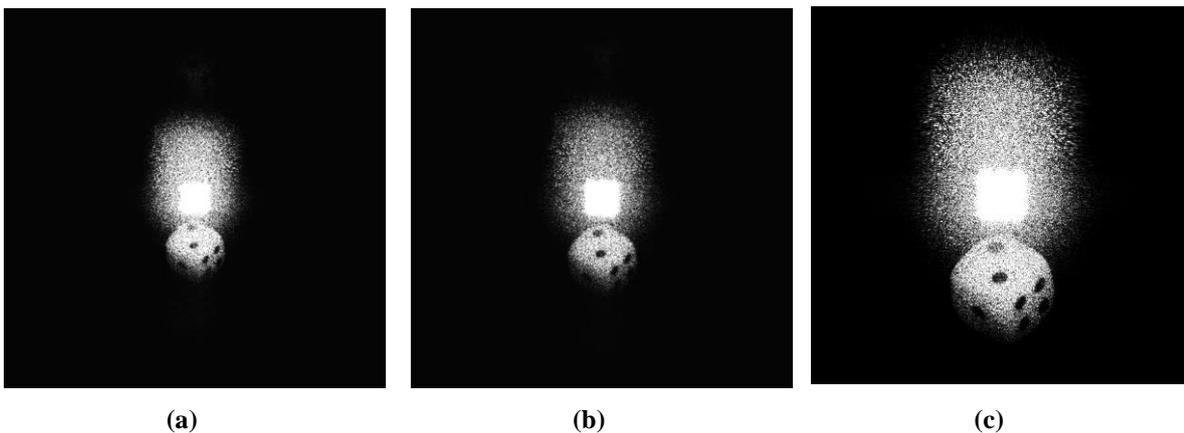


Figura A.5: Reconstrucción del holograma de la Figura A.5 (a) usando un sistema óptico virtual que realiza la propagación usando (a) la integral de Fresnel, (b) y (c) el espectro angular. El tamaño de las imágenes son: en (a) $98.1 \times 98.1 \text{ mm}^2$, en (b) $83.6 \times 83.6 \text{ mm}^2$ y en (c) $27.9 \times 27.9 \text{ mm}^2$.

Es de resaltar que las reconstrucciones corroboran que los sistemas ópticos virtuales funcionan correctamente. Básicamente este ejemplo describe como se comportaría el sistema virtual en la reconstrucción de un holograma digital realizado experimentalmente.

A.3 Bibliografía

- [A.1] P. Hariharan, *Optical Holography. Principles, techniques and applications.* Cambridge University Press (1996). pp. 1-6.
- [A.2] B. Javidi, T. Nomura, "Securing information by use of digital holography," *Opt. Lett.* 25, 28-30, (2000).
- [A.3] E. Tajahuerce and B. Javidi, "Encrypting three-dimensional information with digital holography," *Appl. Opt.* **39**, 6595-6601 (2000).
- [A.4] E. Tajahuerce, O. Matoba, S. C. Verrall, B. Javidi, "Optoelectronic information encryption with phase-shifting interferometry," *Appl. Opt.* **39**, 2313-2320 (2000).
- [A.5] U. Schnars, W. Jueptner, *Digital Holography. Digital hologram recording, Numerical reconstructions and related techniques.* Springer Science+Business Media Inc. (2005). pp. 5-69.
- [A.6] T. C. Poon, "Digital holography and three-dimensional display. Principles and Applications". Springer Science+Business Media Inc. (2006). pp. 51-57.
- [A.7] P. Hariharan, *Optical Holography. Principles, techniques and applications.* Cambridge University Press (1996). pp. 25-43.
- [A.8] U. Schnars, W. Jüptner, "Direct recording of holograms by a CCD target and numerical reconstruction," *Appl. Opt.* **33**, 179-181 (1994).
- [A.9] U. Schnars, W. Jueptner, *Digital Holography. Digital hologram recording, Numerical reconstructions and related techniques.* Springer Science+Business Media Inc. (2005). p. 49.

Apéndice B

Métricas para el análisis de resultados

B.1 Introducción

En el Capítulo 3 se mostró como la adecuada combinación de elementos ópticos virtuales permite el modelado de experiencias ópticas analógicas que involucran principalmente los fenómenos de difracción e interferencia de la luz. Haciendo uso de estos sistemas, en el Capítulo 4 se analizó el solapamiento de la información en las imágenes recuperadas a partir de un multiplexado convencional. De igual forma en el Capítulo 6 se aplicó la técnica de encriptación de eventos dinámicos y se analizó la calidad de las imágenes recuperadas de las secuencias dinámicas.

Se tiene que en los resultados obtenidos con sistemas ópticos virtuales se excluyen errores aleatorios, errores sistemáticos, errores instrumentales o errores de método que se presentan en un experimento analógico. Esto es debido a que el experimento óptico virtual arroja los mismos resultados al reproducir la experiencia digitalmente una y otra vez. Sin embargo, en la implementación de los sistemas virtuales se pueden presentar los llamados errores gruesos, los cuales surgen por la falta de cuidado, incapacidad, mala suerte, etc., del experimentador virtual. Por ejemplo, la inadecuada manipulación de la información, transposición de números al escribir, confusión de variables, cambios de signo, etc., producen errores que se manifiestan con resultados discordantes respecto a los resultados predichos por la teoría.

Considerando que en el Capítulo 3 se comprobó el buen funcionamiento de los sistemas ópticos virtuales mediante experiencias ópticas conocidas, se puede descartar la

idea de que existan errores gruesos en las implementaciones desarrolladas. Por lo tanto, en el caso que nos ocupa, queda únicamente evaluar mediante análisis estadísticos los resultados obtenidos de cada experiencia virtual.

En este apéndice se definen algunas métricas estadísticas [B.1] usadas para analizar los resultados obtenidos de los experimentos ópticos virtuales. Del mismo modo, se discute brevemente algunas consideraciones para interpretar los resultados obtenidos.

B.2 Estimadores estadísticos

En un experimento analógico la distribución de errores aleatorios da como resultado un histograma de las frecuencias relativas de las fluctuaciones de la medición. La reproducibilidad de un resultado define la *precisión* que describe la concordancia de los valores numéricos de dos o más mediciones bajo las mismas condiciones experimentales. Por otro lado la exactitud describe si los resultados experimentales son los correctos, convirtiendo la exactitud en un término relativo sujeto a las necesidades del investigador. Por lo tanto, todos los tipos de medidas son solo una aproximación al valor verdadero a excepción del recuento de objetos que es el único experimento completamente exacto.

Dependiendo de la información que se quiera extraer, existen diferentes elementos estadísticos que se pueden emplear para analizar un conjunto de datos. El utilizar herramientas estadísticas para deducir la probable exactitud de un resultado es parte fundamental en el análisis de cualquier experimento. Esto último es debido a que los datos con fiabilidad desconocida esencialmente no tienen utilidad. Algunos de los términos estadísticos empleados para el análisis de muestras que brindan fiabilidad y dan una descripción de la precisión en la medida son:

i) *Media de la muestra* (\bar{x}): da el promedio de un conjunto finito de datos y es expresada como:

$$\bar{x} = \frac{1}{N} \sum_{i=0}^N x_i \quad (\text{B.1})$$

donde x_i es el valor de la i -ésima medida y N es el número de medidas, cuando N tiende a infinito los datos analizados dejan de ser una muestra y se convierten en población.

ii) *Error absoluto* (E_a): brinda una diferencia entre la media de una muestra de un conjunto de mediciones y un valor de referencia que es tomado como el valor real de la magnitud medida.

$$E_a = \bar{x} - x_{ref} \quad (\text{B.1})$$

donde \bar{x} es la media o promedio y x_{ref} es el valor de referencia o el valor aceptado como verdadero.

iii) *Error relativo* (E_{rel}): da el valor porcentual de la relación del error absoluto y la medición y el valor de referencia.

$$E_{rel} = \frac{\bar{x} - x_{ref}}{x_{ref}} \times 100\% \quad (\text{B.2})$$

iv) *Desviación estándar de la muestra*: es la medida de la dispersión de los datos respecto a la media aritmética de una muestra, la desviación estándar para una muestra de datos limitado viene dada por:

$$s = \sqrt{\frac{1}{N-1} \sum_{i=1}^N (x_i - \bar{x})^2} \quad (\text{B.3})$$

v) *Coficiente de variación*: es la desviación estándar relativa expresada en porcentaje

$$CV = \frac{s}{\bar{x}} \times 100\% \quad (\text{B.4})$$

Ahora, las señales bidimensionales de entrada y de salida de un sistema óptico virtual tendrán una relación de señal-ruido que debe ser analizada. Este es el caso de las imágenes procesadas por los sistemas ópticos virtuales de encriptación. Los fenómenos de difracción involucrados ocasionan que una señal bidimensional no se recupere con un cien por ciento de fidelidad.

Dependiendo del uso de las imágenes involucradas, la calidad es un atributo que puede tener varias definiciones e interpretaciones. La clasificación de calidad puede variar de un observador a otro al no existir una escala universal de medición objetiva, por lo tanto, la percepción subjetiva del observador influye en la clasificación de la calidad de una imagen [B.2].

Dado que un sistema de encriptación debe ofrecerle al usuario la menor pérdida de calidad en la recuperación, es de interés analizar las diferencias entre las imágenes descriptadas y las imágenes de referencia.

Para analizar la diferencia entre dos imágenes se usan estadísticos como error absoluto medio (MAE), el error absoluto medio normalizado (NMAE), el sesgo (BIAS), la raíz cuadrada del error cuadrático medio (RMSE), la raíz cuadrada del error cuadrático medio normalizado (NRMSE) y el pico de la relación señal ruido. Las expresiones de algunas de estas métricas son:

i) *Error absoluto medio (MAE)*: es una medida para el cálculo de precisión que da la medición de las diferencias en promedio entre una imagen observada (imagen descriptada) y una imagen de referencia.

$$MAE = \frac{1}{MN} \sum_{n=1}^N \sum_{m=1}^M |I_{ref}(m, n) - I_{obs}(m, n)| \quad (B.5)$$

donde $I_{ref}(m, n)$ es el pixel de la imagen de referencia y donde $I_{obs}(m, n)$ es el pixel en la coordenada (m, n) de la imagen observada. Las imágenes comparadas son representadas en una matriz de tamaño $M \times N$.

ii) *Error absoluto medio normalizado (NMAE)*: es una medida que tiene en cuenta el peso del error en cada pixel de la imagen. Cada diferencia de cada pixel es normalizado al valor del pixel observado.

$$NMAE = \frac{1}{MN} \sum_{n=1}^N \sum_{m=1}^M \frac{|I_{ref}(m, n) - I_{obs}(m, n)|}{I_{obs}(m, n)} \quad (B.6)$$

iii) *Sesgo (BIAS)*: es una medida del error sistemático del modelo

$$BIAS = \frac{1}{MN} \sum_{n=1}^N \sum_{m=1}^M [I_{ref}(m, n) - I_{obs}(m, n)] \quad (B.7)$$

iv) *Raíz cuadrada del error cuadrático medio (RMSE)*: este estadístico brinda la medida del promedio de las diferencias entre una imagen observada y una imagen de referencia.

$$RMSE = \sqrt{\frac{1}{MN} \sum_{n=1}^N \sum_{m=1}^M [I_{ref}(m, n) - I_{obs}(m, n)]^2} \quad (B.8)$$

v) *Pico de la relación señal ruido (PSNR)*: es una medida de la razón entre el pico de la señal y la diferencia de dos imágenes. En procesamiento de imágenes el pico de la relación señal-ruido se mide en decibeles dB, puede verse que un incremento en 20 dB corresponde a un decrecimiento de una décima parte en la diferencia del *RMSE* y se considera que el *PSNR* debe ser mayor que 20 dB para considerar una imagen de alta calidad. El *PSNR* está dado por:

$$PSNR = 20 \cdot \log_{10} \left(\frac{2^q - 1}{RMSE} \right) \quad (B.9)$$

donde q es el número de bits de las imágenes.

B.3 Consideraciones de las métricas aplicadas en los análisis de resultados

Para realizar los análisis de la calidad de las imágenes descriptadas, se usa la raíz cuadrada del error cuadrático medio normalizado (*NRMSE*) y el pico de la relación señal-ruido (*PSNR*). El *NRMSE* es una medida normalizada del *RMSE* cuya constante de normalización puede ser el valor medio de la imagen observada, la diferencia entre el máximo y el mínimo de la imagen observada, o en muchos casos, el valor máximo que puede tomar el valor de un pixel, $(2^{bits} - 1)$.

En las aplicaciones se tomó como constante de normalización $(2^{\text{bits}} - 1)$ y en algún caso particular se renormaliza a un valor constante todas las imágenes de una misma secuencia para resaltar el comportamiento de la calidad de las imágenes descryptadas. Es de aclarar que esto se hace únicamente para el NRMSE, el valor de PSNR es encontrado según la Ecuación B.9, donde interviene la métrica *RMSE*.

Ahora, un único valor de *NRMSE* o de *PSNR* es una medición muy general. Es evidente que en todas las contribuciones que se emplean estas métricas, los análisis son complementados con las percepciones subjetivas del experimentador [B.3]. A partir de dos valores de *NRMSE*, por ejemplo 0.6 y 0.2, no se puede decir con certeza nada de las dos imágenes sin detallarlas visualmente y sin realizar una medida subjetiva de lo que representa ese valor.

Es por esto que se introduce un análisis diferente para medir la calidad de las imágenes descryptadas. La estrategia propuesta se basa en la idea de que el valor de *NRMSE* y del *PSNR* de cada imagen debe estar acompañado de un rango de valores de dispersión. Para realizar este análisis se emplea el promediado angular de intensidades el cual se define a continuación.

B.3.1 Promediado radial y angular de intensidades

Haciendo referencia a la Figura B.1, expresando la coordenada cartesiana (x, y) de un pixel en coordenadas polares, se tiene: $\rho = \sqrt{x^2 + y^2}$ y $\theta = \tan^{-1}\left(\frac{y}{x}\right)$. El promediado radial de intensidades a radios constantes consiste en realizar la media aritmética de los valores de los pixeles de la imagen ubicados a la misma distancia radial medida desde el centro de la imagen. Por otro lado, el promediado angular de intensidades consiste en realizar la media aritmética de los valores de los pixeles de la imagen que tienen la misma coordenada angular. Estas cantidades definen medidas direccionales que evalúan la calidad de la imagen a lo largo de las direcciones de los pixeles promediados.

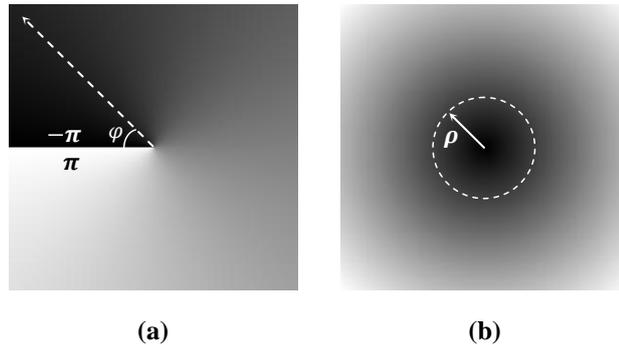


Figura B.1: Dirección de promediado de intensidades. **(a)** La media aritmética se hace con los píxeles que están en la línea punteada, todos ellos tienen la misma coordenada angular. **(b)** La media aritmética se hace con los píxeles que están en la línea punteada, todos ellos tienen la misma coordenada radial.

Usando este concepto, se aplican las métricas *NRMSE* y *PSNR* a los píxeles en estas direcciones particulares. De esta manera se obtendrá un conjunto de medidas sobre las direcciones angulares y radiales de la imagen. Finalmente con estos valores se puede realizar un diagrama de cajas mostrando la dispersión de la media del *NRMSE* y *PSNR*.

Por último, para evaluar la aleatoriedad de una imagen y el grado de semejanza entre dos imágenes con distribuciones randómicas vistas en el Capítulo 7, se utiliza las funciones de autocorrelación y correlación cruzada.

B.3.2 Correlación cruzada y autocorrelación

El teorema de Wiener-Khintchine [B.4] permite definir el espectro de una señal por medio de la autocorrelación. Los coeficientes de autocorrelación pueden ser encontrados como:

$$c_{hh} = \mathcal{F}^{-1}[|H(v)|^2] \quad (\text{B.10})$$

donde $H(v)$ es el espectro de la señal de entrada, \mathcal{F} denota la operación de transformada de Fourier y c_{hh} son los coeficientes de autocorrelación de la señal de entrada $h(x)$. Para determinar el grado de similitud entre dos señales $h(x)$ y $g(x)$ se usa la expresión que define la de correlación cruzada:

$$c_{gh} = \mathcal{F}^{-1}[G^*(v)H(v)] \quad (\text{B.11})$$

B.4 Bibliografía

- [B.1] D. Skoog, F. Holler, T. Nieman, Principios de análisis instrumental. McGRAW-HILL. (2001) pp. 919-939.
- [B.2] Z. Wang, A. Bovik, L. Lu, “Why is image quality assessment so difficult?” Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Proc., vol. 4, pp. 3313-3316, (2002).
- [B.3] B. Girod, “What's wrong with mean-squared error,” en Digital Images and Human Vision, A. B. Watson, pp. 207-220, MIT Press, (1993).
- [B.4] M. Born, E Wolf, Principles of optics: electromagnetic theory of propagation, interference and diffraction of light. Cambridge: Cambridge University Press, (1999). p. 567.

Apéndice C

Imágenes recuperadas

C.1 Introducción

En el Capítulo 6 se presentaron varias aplicaciones de la técnica de encriptación de eventos dinámicos. Esta técnica fue usada para multiplexar escenas dinámicas monocromáticas, policromáticas y múltiples escenas para un proceso multiusuario.

Como primer ejemplo, se codificó una secuencia monocromática compuesta de 22 imágenes de 8 bits sincronizada a 10 imágenes por segundo obteniendo 2.2 segundos de duración. La Figura C.1 muestra las 22 imágenes correctamente recuperadas al usar la llave de seguridad correcta y la Figura C.2 muestra las 22 imágenes incorrectamente recuperadas al usar una llave de seguridad incorrecta.

Como segundo ejemplo, se codificaron secuencias a color (cilindros en movimiento y pájaro balanceándose). En las Figuras C.3, C.4, C.5 y en las Figuras C.7, C.8 y C.9 se muestran las primeras 24 imágenes correctamente recuperadas de escenas de diferente duración. En las Figuras C.6 y C.10, se muestran las primeras 24 imágenes incorrectamente recuperadas de una escena de 3 segundos de duración.

Por último, se realizó un proceso multiusuario codificando diferentes secuencias monocromáticas en un único multiplexado. Las Figuras C.11, C.12 y C.13 muestran las imágenes recuperadas de la secuencia dinámica de cada usuario autorizado usando la llave de seguridad correcta. La Figura C.14 muestra imágenes recuperadas del multiplexado de las 3 secuencias dinámicas usando una llave de seguridad incorrecta.

C.2 Imágenes de la escena monocromática

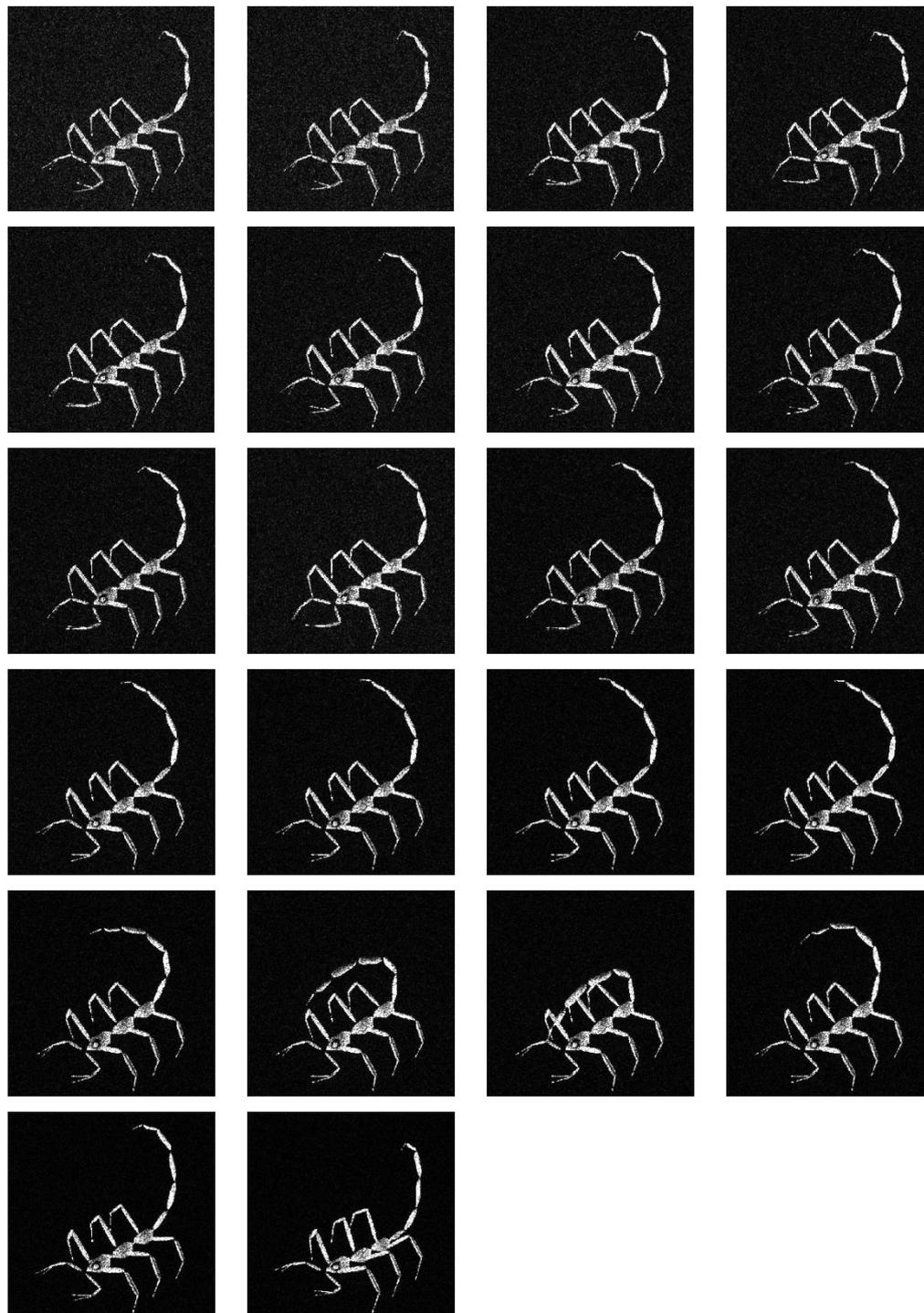


Figura C.1: Imágenes recuperadas de la secuencia monocromática usando la llave de seguridad correcta. Media 1.avi.

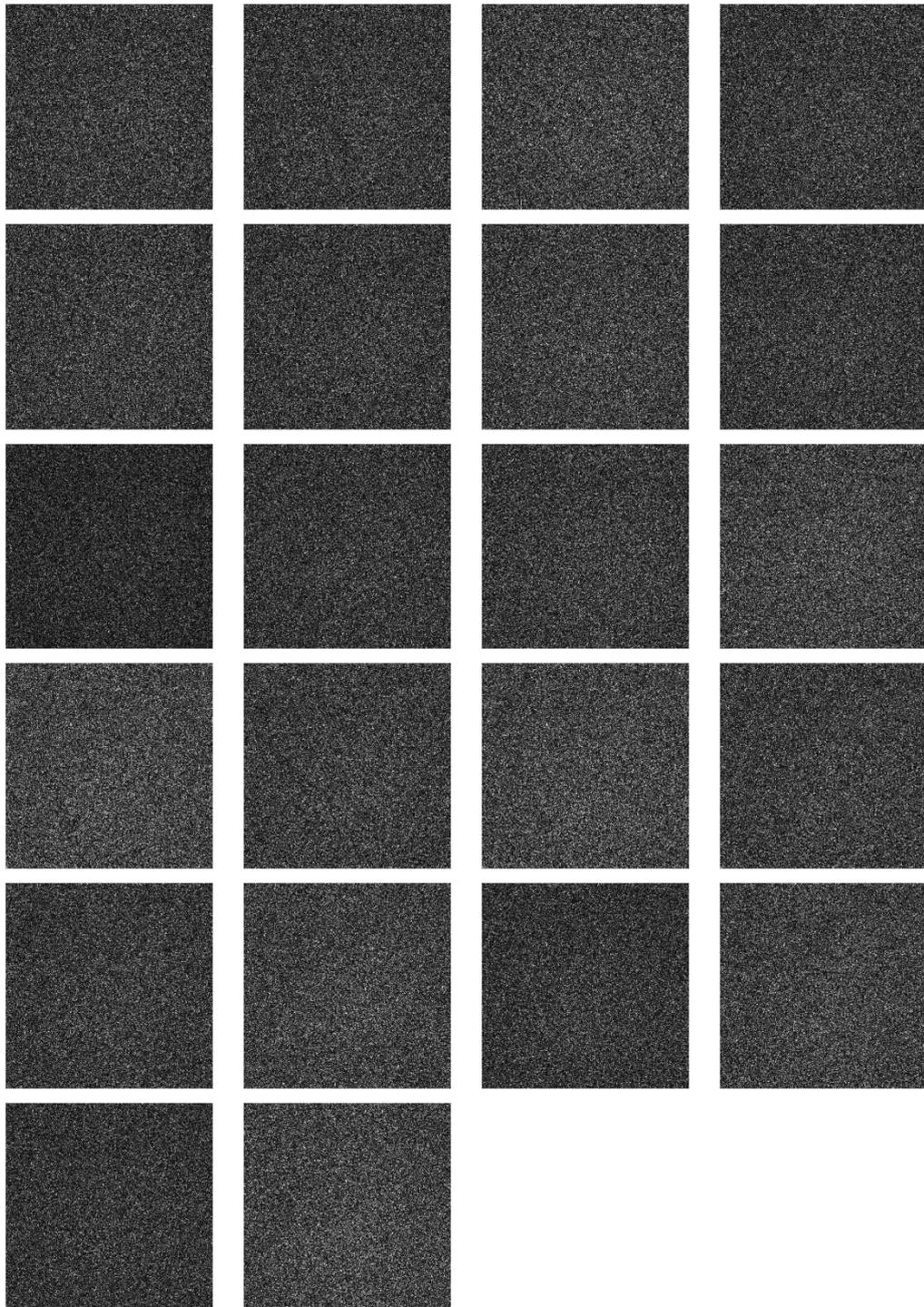


Figura C.2: Imágenes recuperadas de la secuencia monocromática usando una llave de seguridad incorrecta. Media 2.avi.

C.3 Imágenes de las escenas policromáticas

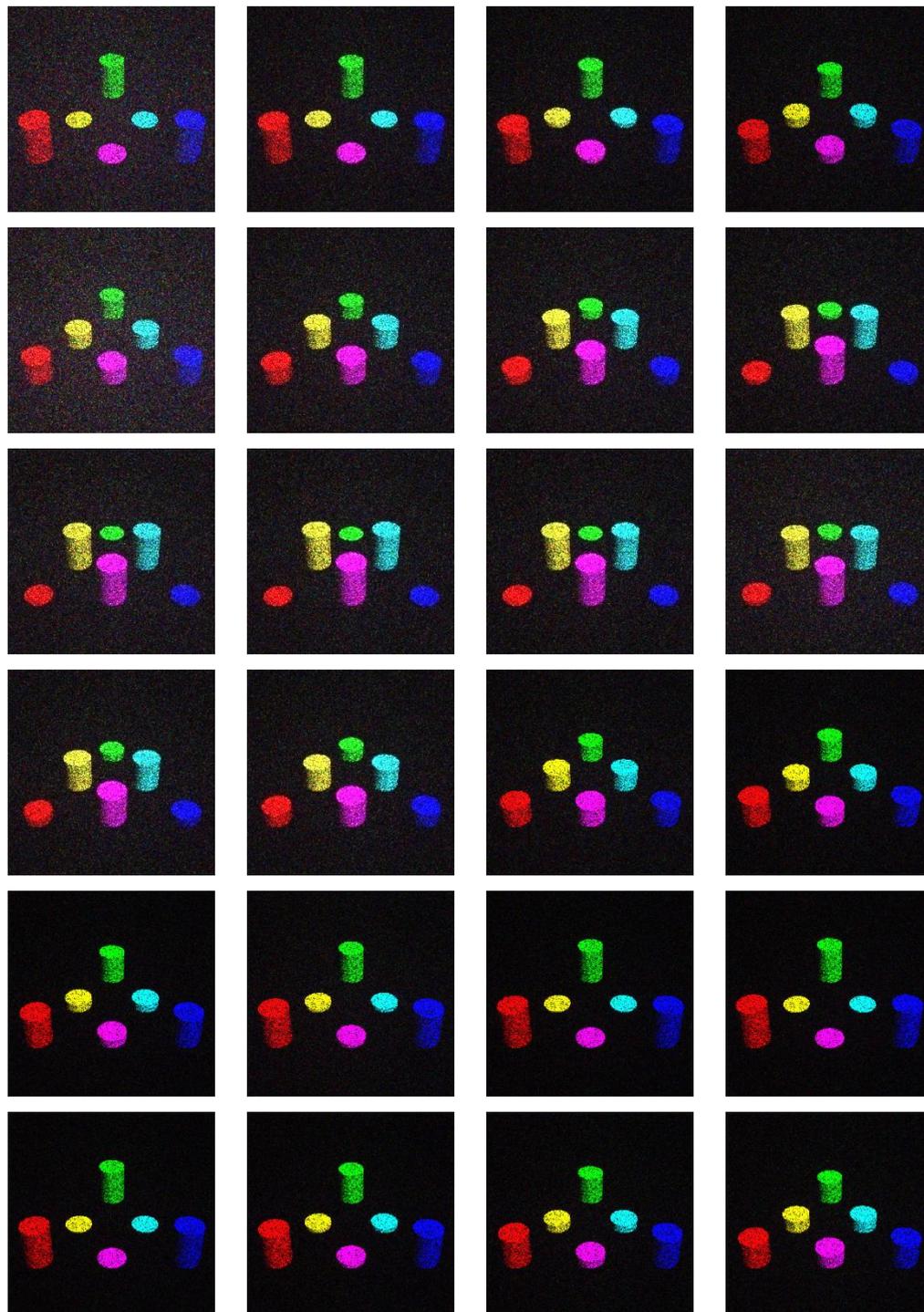


Figura C.3: Primeras 24 imágenes recuperadas de la secuencia poli-cromática de 3 segundos de duración de los cilindros en movimiento. Se usa la llave de seguridad correcta para realizar la descryptación de cada imagen. Media 3.avi.

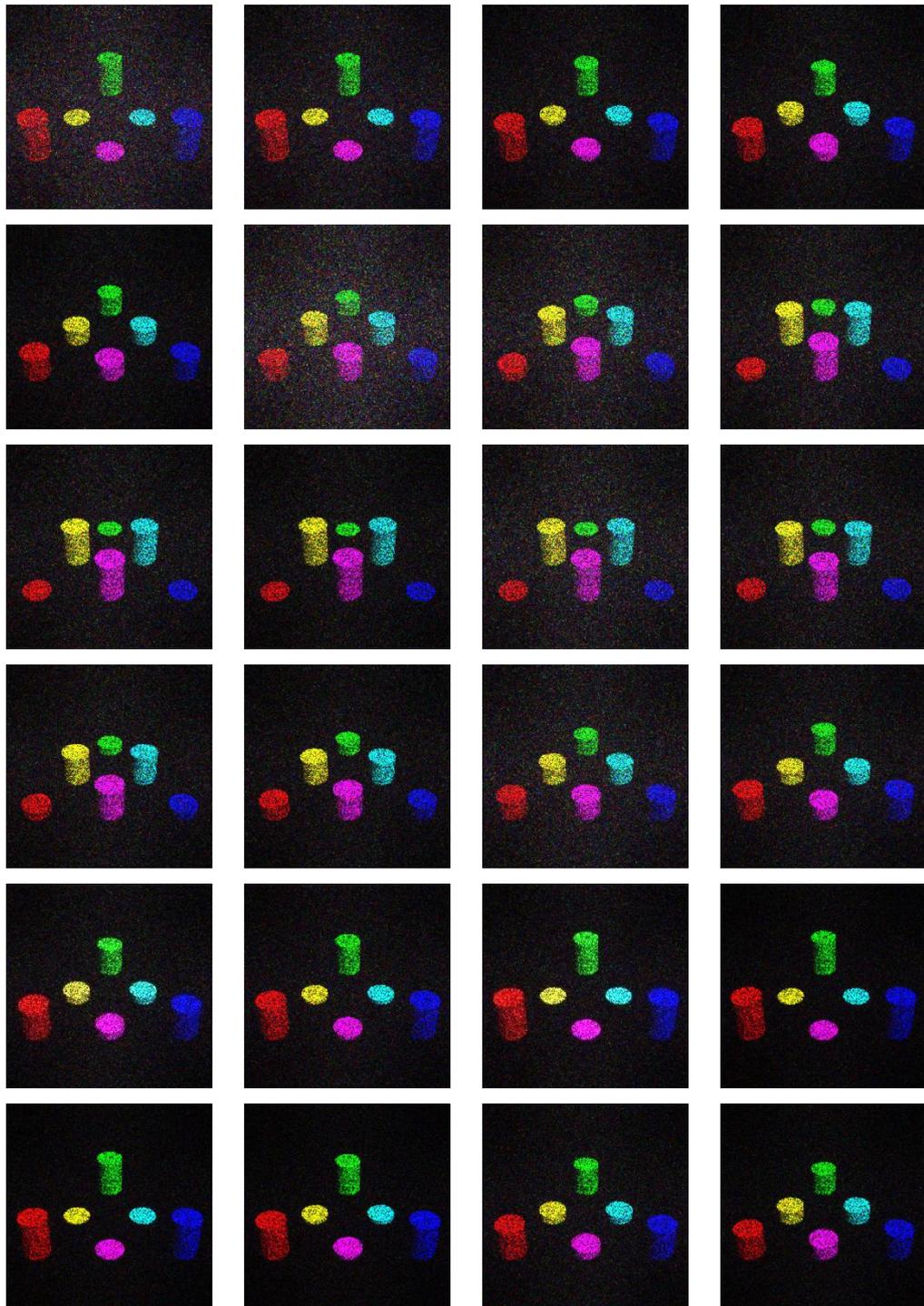


Figura C.4: Primeras 24 imágenes recuperadas de la secuencia poli-cromática de 4.8 segundos de duración de los cilindros en movimiento. Se usa la llave de seguridad correcta para realizar la descriptación de cada imagen. Media 4.avi.

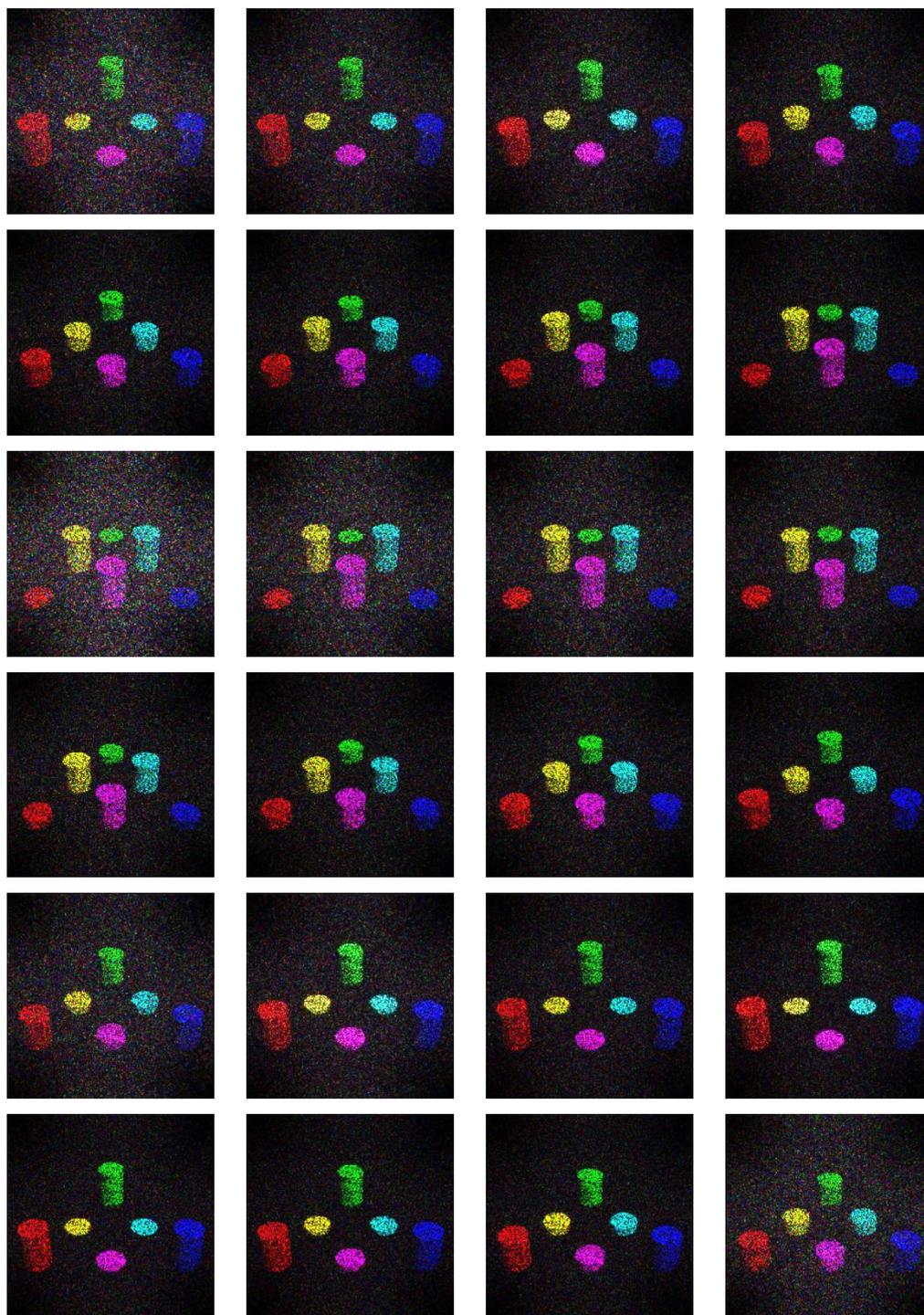


Figura C.5: Primeras 24 imágenes recuperadas de la secuencia poli-cromática de 12.6 segundos de duración de los cilindros en movimiento. Se usa la llave de seguridad correcta para realizar la descryptación de cada imagen. Media 5.avi.

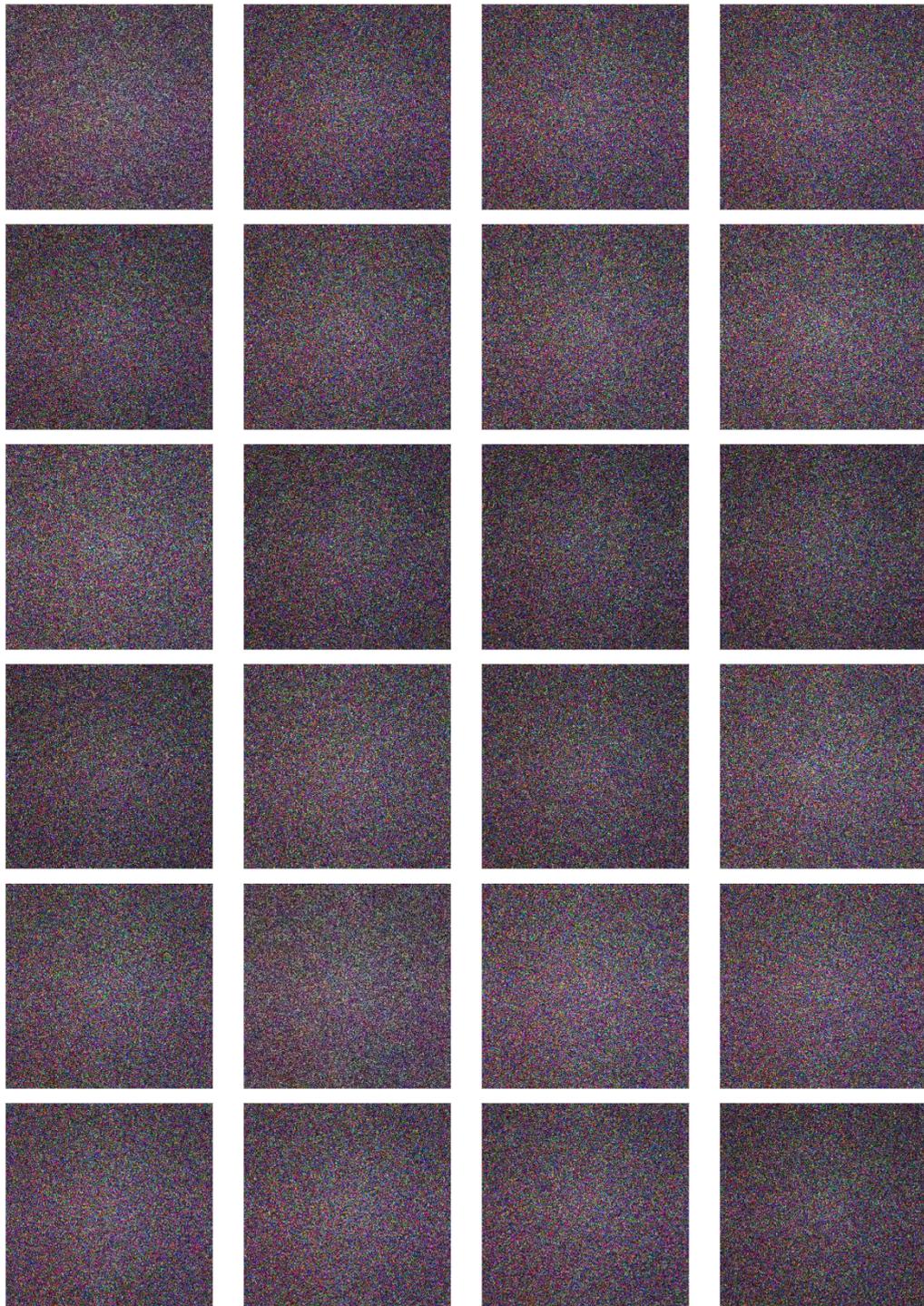


Figura C.6: Primeras 24 imágenes recuperadas de la secuencia poli-cromática de 3 segundos de duración de los cilindros en movimiento. Se usa la llave de seguridad incorrecta para realizar la descryptación de cada imagen. Media 6.avi.

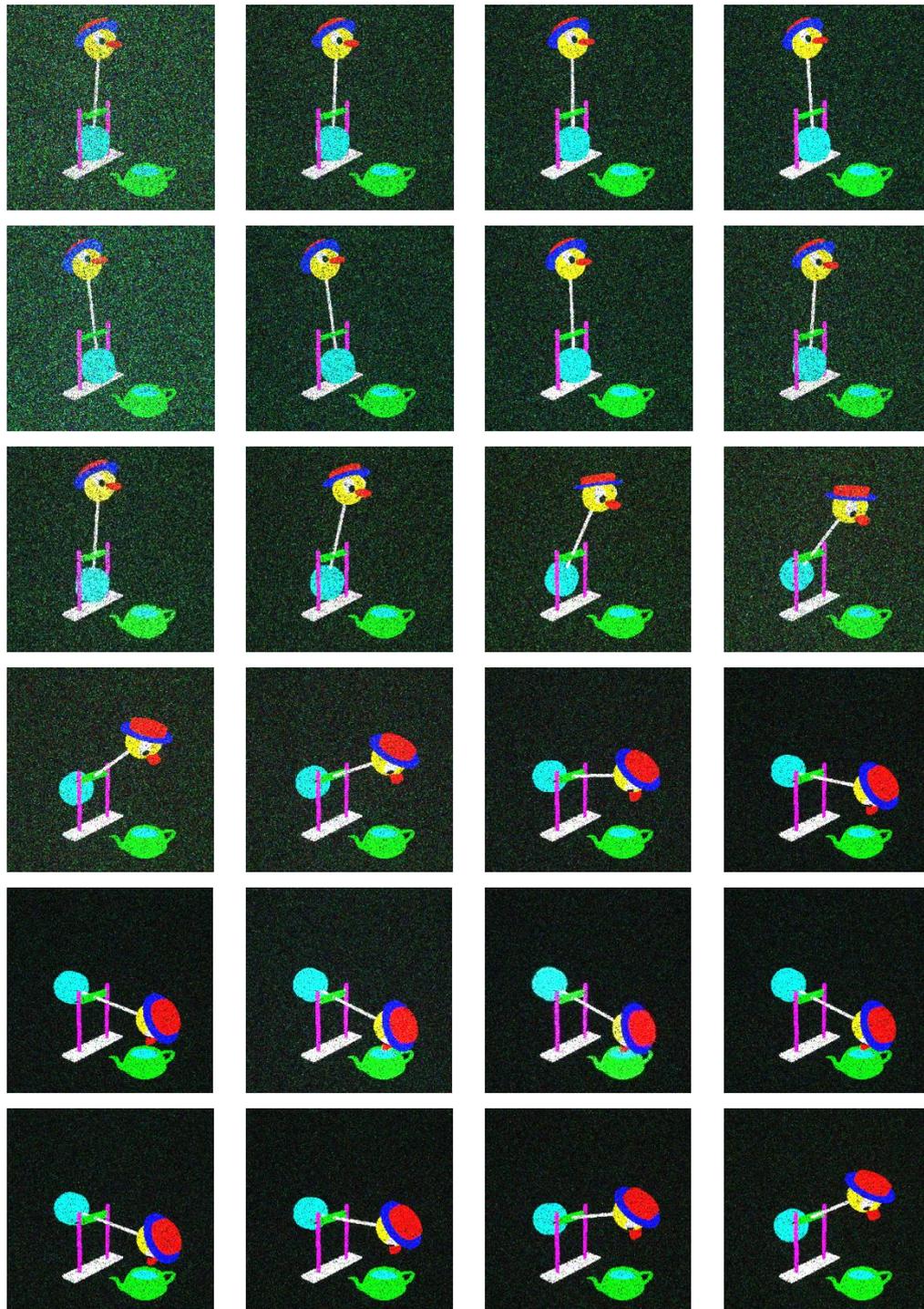


Figura C.7: Primeras 24 imágenes recuperadas de la secuencia poli-cromática de 3 segundos de duración del pájaro balanceándose. Se usa la llave de seguridad correcta para realizar la descryptación de cada imagen. Media 7.avi.

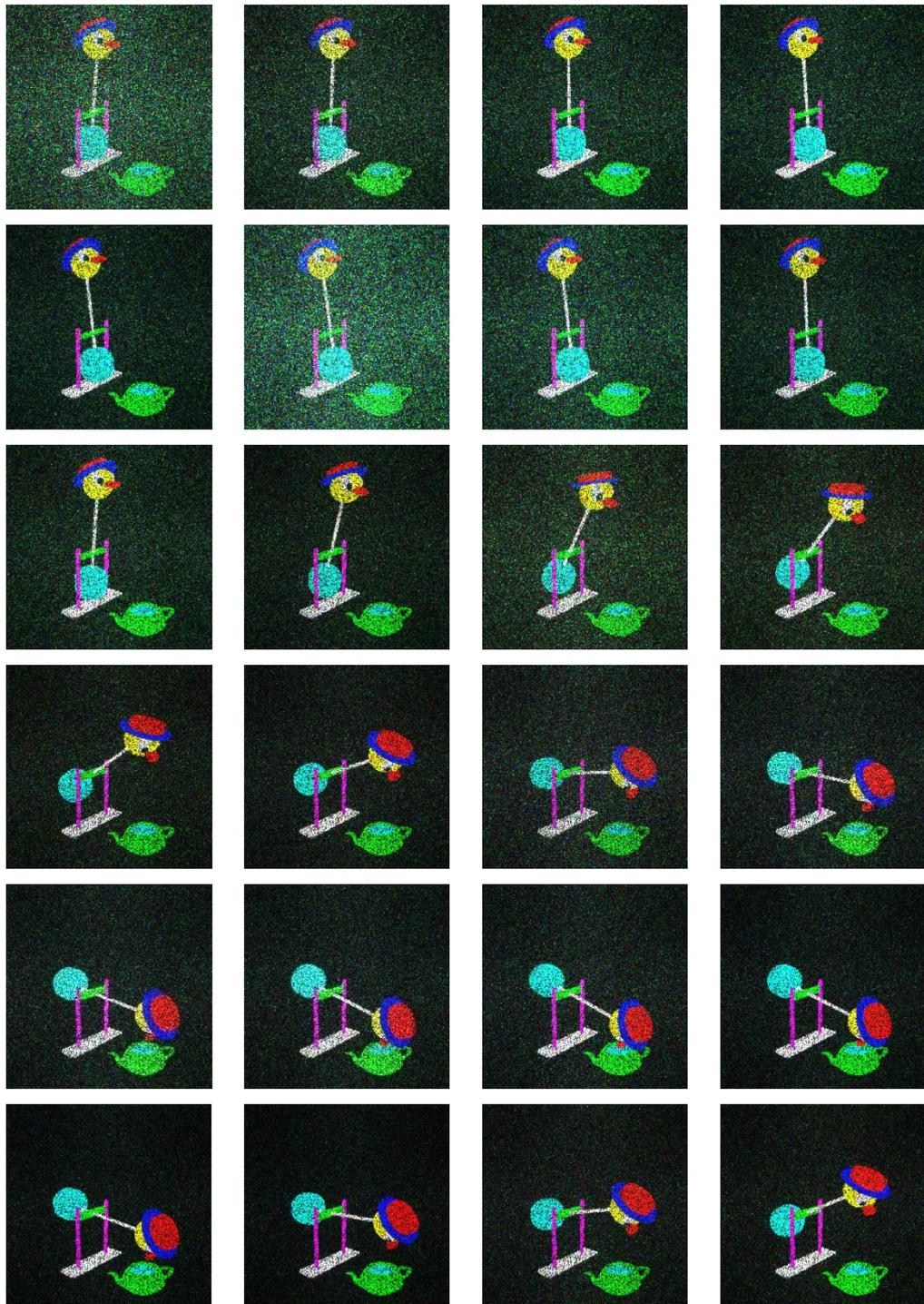


Figura C.8: Primeras 24 imágenes recuperadas de la secuencia poli-cromática de 4.8 segundos de duración del pájaro balanceándose. Se usa la llave de seguridad correcta para realizar la descriptación de cada imagen. Media 8.avi.

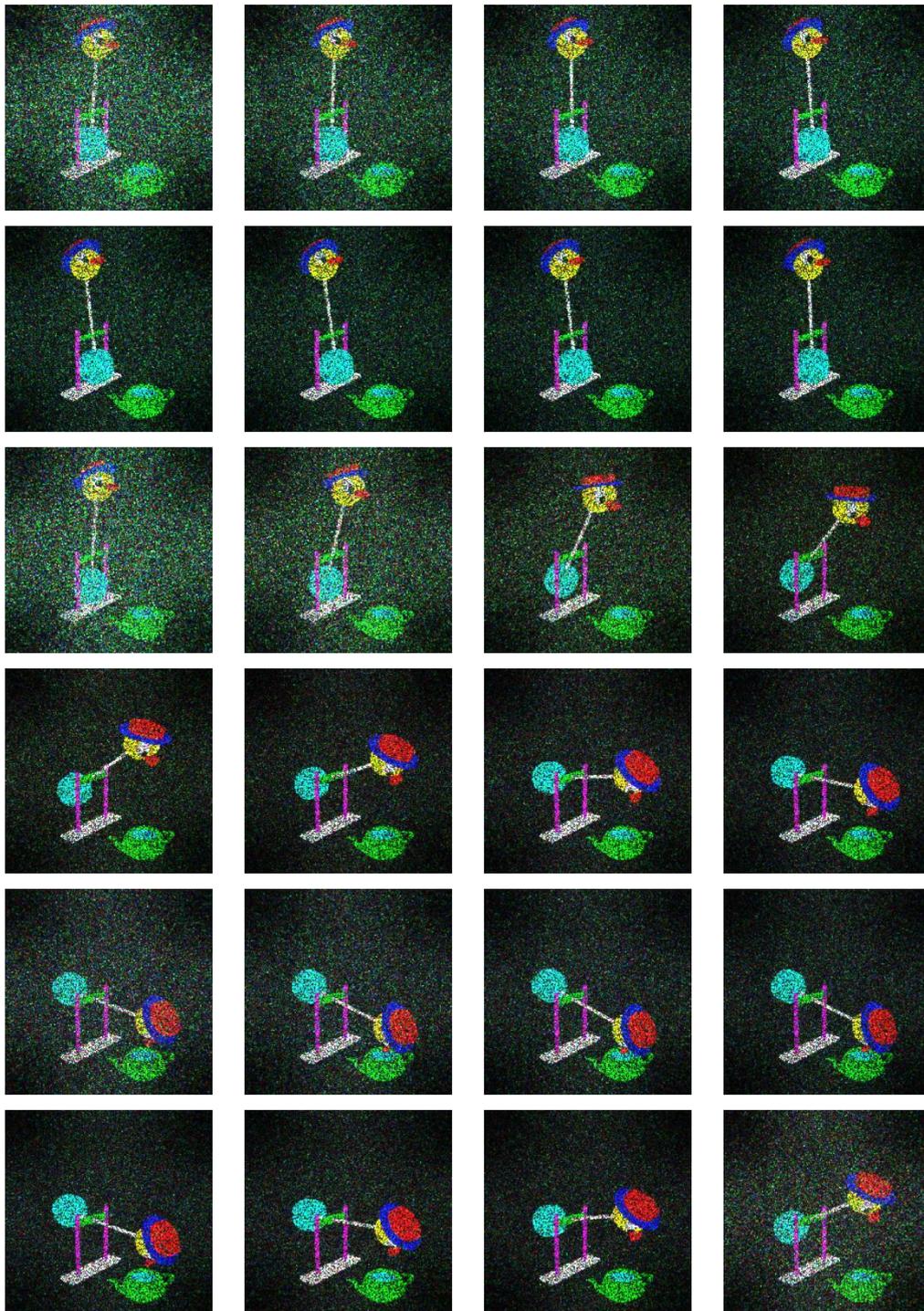


Figura C.9: Primeras 24 imágenes recuperadas de la secuencia poli-cromática de 12.6 segundos de duración del pájaro balanceándose. Se usa la llave de seguridad correcta para realizar la descryptación de cada imagen. Media 9.avi.

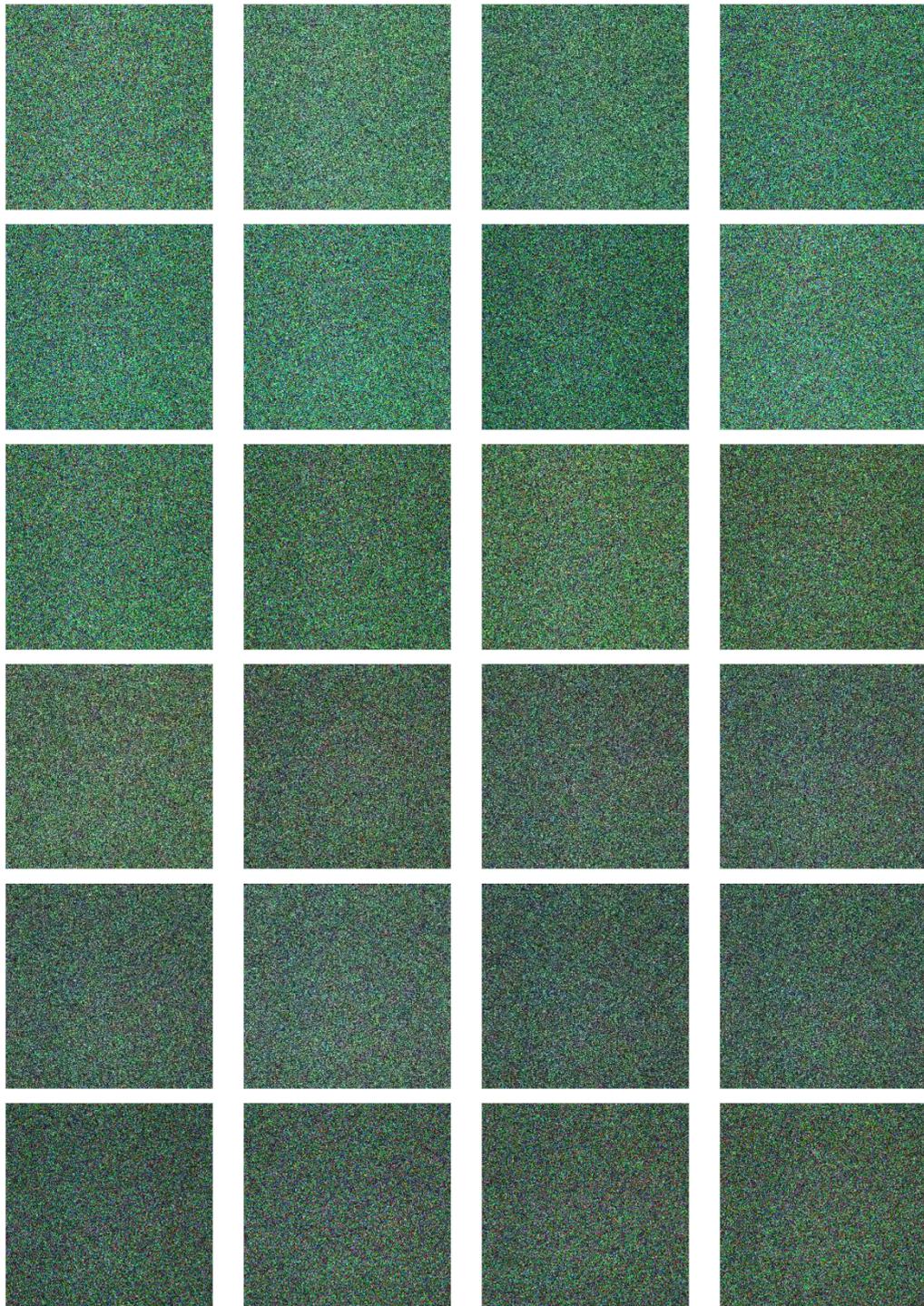


Figura C.10: Primeras 24 imágenes recuperadas de la secuencia poli-cromática de 3 segundos de duración del pájaro balanceándose. Se usa la llave de seguridad incorrecta para realizar la descryptación de cada imagen. Media 10.avi.

C.4 Imágenes descriptadas de un proceso multiusuario

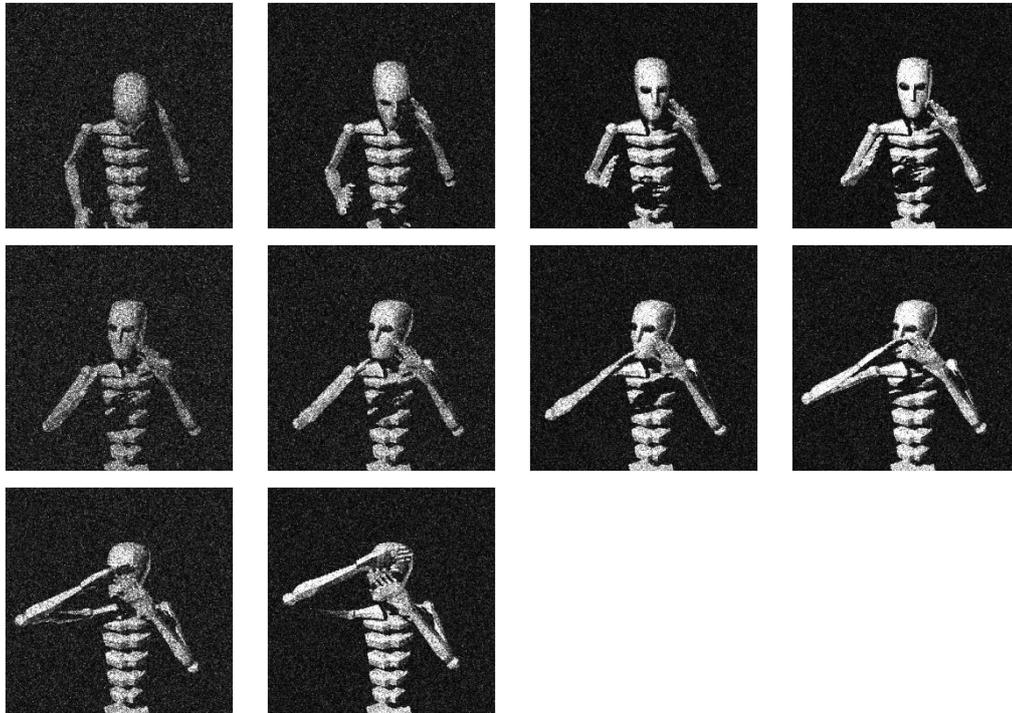


Figura C.11: Imágenes recuperadas de la secuencia dinámica del primer usuario usando la llave de seguridad correcta. Media 11.avi.

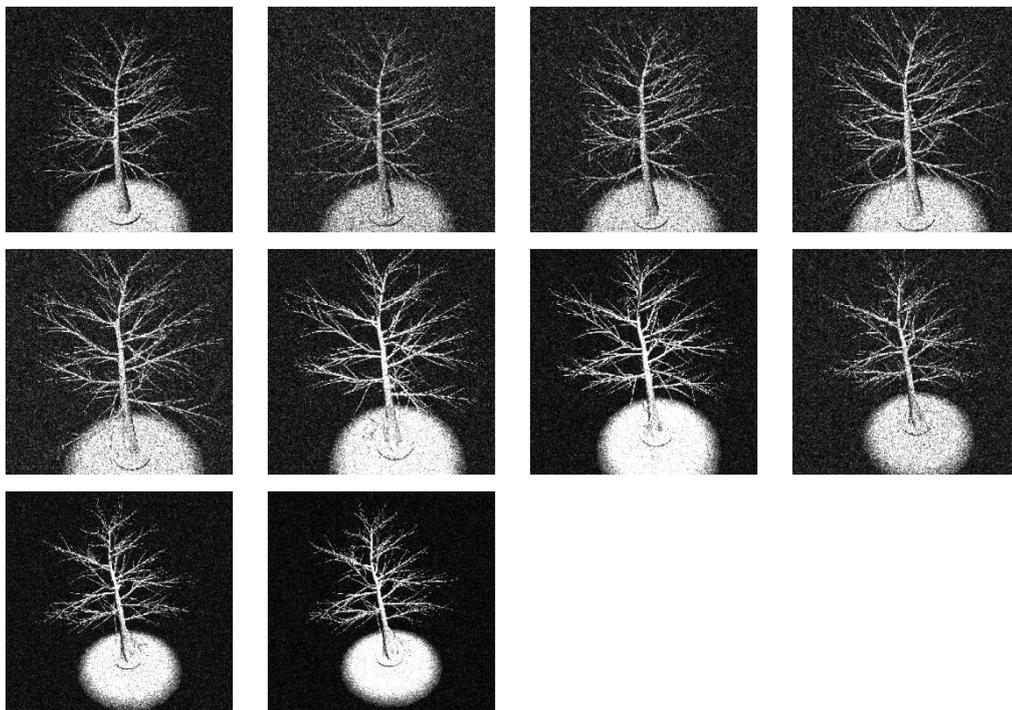


Figura C.12: Imágenes recuperadas de la secuencia dinámica del segundo usuario usando la llave de seguridad correcta. Media 12.avi.

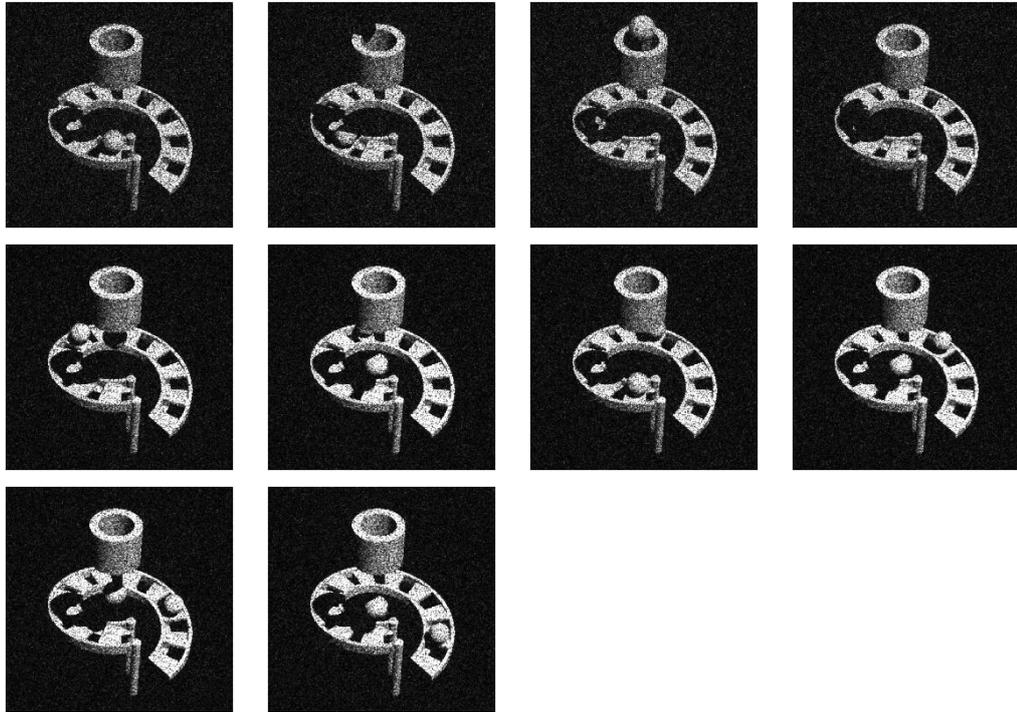


Figura C.13: Imágenes recuperadas de la secuencia dinámica del tercer usuario usando la llave de seguridad correcta. Media 13.avi.

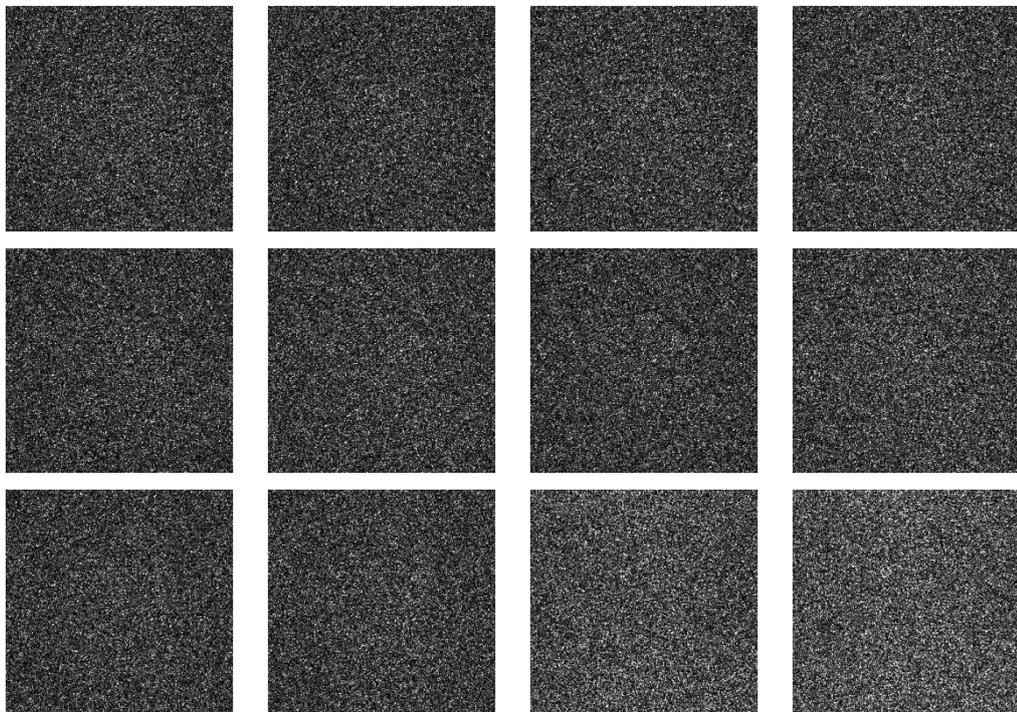


Figura C.14: Primeras 12 imágenes recuperadas del multiplexado de las 3 secuencias dinámicas usando una llave de seguridad que no es alguna de los tres usuarios autorizados. Todas las imágenes recuperadas restantes son ruido de *speckle*. Media 14.avi.

Lista de Publicaciones

Algunos de los aspectos originales presentados en este trabajo fueron reportados en las siguientes publicaciones:

F. Mosso, M. Tebaldi, F. Barrera, N. Bolognini, and R. Torroba, " Multi-user multiplexed scheme for decoding modulated-encoded sequential information " Proc. SPIE 8011, 801173 (2011).

F. Mosso, M. Tebaldi, F. Barrera, N. Bolognini, and R. Torroba, "Pure optical dynamical color encryption," Opt. Express 19, 13779-13786 (2011)
<http://www.opticsinfobase.org/oe/abstract.cfm?URI=oe-19-15-13779>

F. Mosso, F. Barrera, Myrian Tebaldi, Néstor Bolognini, and Roberto Torroba, "All-optical encrypted movie," Opt. Express 19, 5706-5712 (2011)
<http://www.opticsinfobase.org/oe/abstract.cfm?URI=oe-19-6-5706>

F. Mosso, M. Tebaldi, R. Torroba, N. Bolognini, "Double random phase encoding method using a key code generated by affine transformation", Optik - International Journal for Light and Electron Optics, Volume 122, Issue 6, March 2011, Pages 529-534, ISSN 0030-4026, 10.1016/j.ijleo.2010.03.018.
<http://www.sciencedirect.com/science/article/pii/S0030402610001592>

E. Mosso, M. Tebaldi, A. Lencina, N. Bolognini, "Cluster speckle structures through multiple apertures forming a closed curve", Optics Communications, Volume 283, Issue 7, 1 April 2010, Pages 1285-1290, ISSN 0030-4018, 10.1016/j.optcom.2009.12.016.
<http://www.sciencedirect.com/science/article/pii/S0030401809012899>

Comunicaciones a Congresos

F. Mosso, M. Tebaldi, F. Barrera, N. Bolognini, and R. Torroba, "Multi-user multiplexed scheme for decoding modulated-encoded sequential information" 22th Congress of the International Commission for Optic. Puebla, Mexico. (2011).

F. Mosso, M. Tebaldi, R. Torroba and N. Bolognini. "Optical encryption of sound signals". VII Ibero-American Conference on optics. X Latin-American Meeting on Optics, Lasers and Applications. RIAO-OPTILAS 2010, Memorias evento. ISBN: 978-612-4057-21-2

F. Mosso, M. Tebaldi, R. Torroba and N. Bolognini. "Optical accessing by using speckle patterns generated by the chirp-z transform". VII Ibero-American Conference on optics. X Latin-American Meeting on Optics, Lasers and Applications. RIAO-OPTILAS 2010, Memorias evento. ISBN: 978-612-4057-21-2

F. Mosso, M. Tebaldi, R. Torroba, N. Bolognini. "Empleo de máscaras de fase generadas a partir de transformaciones afines para dispositivos de seguridad". XI Encuentro Nacional de Óptica y II Conferencia andina y del caribe en óptica y sus aplicaciones, Pamplona, Colombia, Memorias evento, ISBN:978-958-44-4200-0 (2008).

F. Mosso, M. Tebaldi, R. Torroba, N. Bolognini. "Random phase images generated by affine transformations as optical coding masks". 21th Congress of the International Commission for Optic, Proc., p. 170 (2008).

Distinciones

Selección por parte de Optical Society of America (OSA) del artículo "All Optical Encrypted Movie" (Tapa de revista Optics Express), por ser la primera película encriptada por medios puramente ópticos. El reconocimiento se realiza por la excelente calidad científica y es destacado en la sección Spotlight on Optics - Marzo de 2011.

<http://www.opticsinfobase.org/oe/issue.cfm?volume=19&issue=6>

<http://www.opticsinfobase.org/spotlight/summary.cfm?uri=oe-19-6-5706>