ESTUDIO DE MÉTODOS ANÁLOGO - DIGITALES DE CODIFICACIÓN ÓPTICA. APLICACIONES AL MULTIPLEXADO

Dafne C. Amaya Robayo

Facultad de Ciencias Exactas de la Universidad Nacional de La Plata

Departamento de Física

La Plata, abril de 2012.

UNIVERSIDAD NACIONAL DE LA PLATA

Facultad de Ciencias Exactas

Departamento de Física

ESTUDIO DE MÉTODOS ANÁLOGO - DIGITALES DE CODIFICACIÓN ÓPTICA. APLICACIONES AL MULTIPLEXADO

Tesis para optar al grado de Doctor

Presentada por

Dafne C. Amaya Robayo

Director: Dr. Néstor Bolgnini

Codirector: Dr. Myrian Tebaldi

Abril de 2012.

"En el nombre de Dios, de mis mayores y de la libertad. Ni un paso atrás, siempre adelante, y lo que fuere menester...sea",

José Antonio Galán

AGRADECIMIENTOS

Después de emprender la travesía salir de mi país para doctorarme sin saber lo que iba a encontrar en el lugar a donde llegaba, es muy grato saber lo afortunada que he sido. En esta etapa final sería imposible plasmar en un papel el profundo agradecimiento que siento por muchas personas, quienes hicieron que esta experiencia de vida, haya sido sin lugar a duda, la mejor que he tenido. En lo que sigue trataré de dar algunos agradecimientos personales, porque sería imposible nombrarlos a todos.

Ante todo debo expresar un profundo agradecimiento al doctor Néstor Bolognini y a la doctora Myrian Tebaldi por la gran dedicación que tuvieron y el esfuerzo que les implicó la dirección de esta Tesis. Aprecio todas y cada una de las enseñanzas que me quedan, las académicas, profesionales y personales. Gracias por hacerme sentir más que una estudiante de doctorado, por ayudarme a solucionar cosas que nada tenían que ver con lo académico, por darme el tiempo que necesité, por permitirme crecer y formar parte, en el amplio sentido la frase, de su equipo de trabajo. Gracias los demás integrantes del grupo, al Dr. Roberto por sus siempre acertadas palabras, a Alberto, Gustavo, Fabián, Luisa y Daniel.

Alberto, aunque te mereces todo un capítulo, aquí te dedico solo unas palabras. Tenías razón " sos un fenómeno". Gracias por ser mi amigo, mi compañero de oficina, por darme la mano y hasta el codo... cada vez que lo necesité. Sabes que además del cariño que te tengo, te admiro y respeto por tu multifacética capacidad profesional.

A mi madre, a mi padre, a mis adorados hermanos Andrés, Diana y Nathalia, además de agradecerles, les pido disculpas por todo el tiempo que no he estado. No fueron solo cumpleaños, navidades, etc., lo que me perdí. Nacieron tres sobrinos, Michelle, Juan Camilo y Valentina. Andrés se recibió y por suerte puede estar para el matrimonio de Natis. Esa es la parte dura de esta experiencia, pero ustedes con su amor y generosidad, saben comprender y esperar. Los amo.

En general les agradezco a todos los integrantes del CIOp que hacen de este lugar de trabajo un sitio tan especial. A Fabían Videla, Laureano y Ricardo valoro su linda amistad, a Jesi no la olvidaré por la grata compañía de aquellos tiempos. A Jorge Tocho, y a Faustico muchas gracias por hacerme más fácil el camino siendo excelentes caseros. Sepan todos en general que me han hecho sentir en familia.

Por otro lado fuera del ambiente del CIOp también me he cruzado con personas maravillosas a las que les quiero agradecer por todo el afecto y compañía que me han brindado estos años: a Antonia y Pochito, a Martha Lencina, a Ceci, a mis amigos del barrio, Andre, Migue, Nelson, Yurani, Ivan y Edu... ah y a Sebas que también es del barrio. Como dijo un famoso cantautor argentino, ¡GRACIAS TOTALES!.

INDICE GENERAL

CAPÍTULO I

Introducción General

CAPÍTULO II

Conceptos teóricos básicos

CAPÍTULO III

Análisis de la distribución de los datos encriptados. Arquitectura 4f.

CAPÍTULO IV

Análisis de la distribución de los datos encriptados. Arquitectura JTC

CAPÍTULO V

Almacenamiento múltiple de la información encriptada

CAPÍTULO VI

Aplicaciones de multiplexado. Canales de información.

CAPÍTULO VII

Conclusiones generales

CAPÍTULO I

Introducción General

I.1 Introducción

Desde que existe el ser humano ha existido también la necesidad de comunicarse con sus semejantes, pero en ocasiones es necesario que esa comunicación sea privada. Las razones son evidentes, imaginemos por ejemplo que en tiempos de guerra el enemigo lograse interceptar un mensaje que detalle la estrategia a seguir. Por esta razón, desde las primeras civilizaciones se desarrollaron técnicas de ocultamiento para enviar mensajes durante las guerras, de forma que si el mensajero era interceptado, la información que portaba no corriera el peligro de ser descifrada.

La criptografía, del griego kryptós que significa “escondido”, y graphos, “escritura”, es el arte de alterar las representaciones lingüísticas de un mensaje mediante una clave secreta. El proceso de transformación del texto original (mensaje), en el texto cifrado (criptograma), se conoce como cifrado, y su proceso contrario, es decir, el de recuperación del texto original, descifrado. El cifrado se lleva a cabo con una serie de parámetros, conocidos como clave, que son indispensables para la recuperación del mensaje. Si no se conoce dicha clave, es deseable que sea imposible recuperar el mensaje.

Hay registros que muestran que las primeras civilizaciones que usaron la criptografía fueron la Egipcia, la Mesopotámica, la India y la China. Los espartanos, en Grecia, desarrollaron en el 400 a.C. ''la Scitala'', primer sistema criptográfico por transposición. Julio Cesar utilizó un método basado en la sustitución de cada letra por una que ocupa otra posición en el alfabeto, creando así el conocido cifrado que lleva su nombre [1.1].

En la edad media, León Battista Alberti creó el sistema de cifrado polialfabético, que

emplea varios abecedarios, cambiando de uno a otro cada tres o cuatro palabras. Posteriormente, el abad Johannes Trithemius escribió un libro, Poligrafía (Polygraphia), que fue el primer tratado publicado sobre el tema (1518). En este trabajo se describe un método para cifrar y descifrar utilizando una tabla que en la primera fila contiene todas las letras del abecedario; en la siguiente fila, las letras están desplazadas una posición, y así sucesivamente. El mensaje cifrado se forma empleando para la primera letra, la primera fila, la posición correspondiente a la segunda fila para la segunda letra y así sucesivamente. Más adelante, Giovanni Battista Belaso en 1533, presenta una versión mejorada de la técnica propuesta por Trithemius que incluye una palabra ó frase *clave*. A este método se le conoce como "Cifrado de Vigenère".

El siglo XVIII no fue una época de grandes avances criptográficos. Sin embargo, el telégrafo, inventado por Samuel Morse a principios del siglo XIX, y la aparición de la radio revolucionaron las comunicaciones y obligaron a la criptografía a desarrollarse como ciencia. Estas nuevas formas de comunicación eran fáciles de interceptar, lo que dio lugar en los ámbitos militares y diplomáticos a buscar nuevas maneras de mantener en secreto mensajes importantes. En esta época surgen importantes criptoanalistas como Charles Babbage (decodificó el cifrado de Vigenère), Friedrich Kasiski, William Friedman.

Durante las dos guerras mundiales, la criptografía adquirió un alto grado de de desarrollo, especialmente en el último conflicto. En esta etapa se optimizaron las técnicas de cifrado, al convertirse en un proceso automatizado mediante el uso de las máquinas de cálculo. Esta nueva herramienta permitió que los procesos de cifrado y descifrado fueran más complejos, rápidos y seguros. La más conocidas de esta generación de máquinas fueron la MarkII (SIGABA) americana y la famosa ENIGMA alemana (que cambiaba a diario la palabra clave, para producir un nuevo código de cifrado). Para vencer al ingenio alemán fue necesario el concurso de los mejores matemáticos de la época y un gran esfuerzo computacional. Fue el matemático y criptógrafo polaco Marian Adam Rejewski quien pudo solucionar el mecanismo de cifrado principal usado por ENIGMA. El éxito de Rejewski y sus colegas permitieron a Inglaterra leer los mensajes alemanes. A este tipo de inteligencia se le llamó código "ultra" y contribuyó, quizás decisivamente, a la derrota de la Alemania nazi [1.1].

Actualmente, con el advenimiento de la era digital y el avance de la tecnología de las comunicaciones, somos cada día más dependientes de internet. Cada vez con mayor frecuencia, la red es usada por organizaciones y personas para realizar compras en línea, transacciones bancarias y enviar información privada. Para transmitir estos datos en forma segura es necesario enviarlos codificados, requiriéndose el uso de llaves ó claves sin las cuales sea imposible recuperar la información. Por esta razón se desarrollaron sistemas más seguros que la trasposición y la sustitución como el DES, (Data Encriptation Standart), que es un criptosistema de clave privada que posteriormente fue vulnerado. Diffie y Hellman propusieron utilizar criptosistemas cuyo criptoanálisis fuese equivalente a la resolución de un problema computacionalmente difícil. De esta manera, a pesar de conocer los algoritmos que generan el texto cifrado, no es posible recuperar el mensaje en un tiempo razonable. Este es el principio de los sistemas de clave pública, como el RSA (1978). En 1991 Philip Zimmermann desarrolló un sistema criptográfico, aparentemente inviolable, el P.G.P (Pretty Good Privacy) y lo distribuyó libremente en las redes de comunicación [1.2]. Actualmente, es uno de los más utilizados para la protección de los correos electrónicos. Sin embargo, permanentemente hay usuarios no autorizados buscando interceptar y decodificar los datos de la red, desde un acceso remoto. Esto ha producido en los últimos años un creciente interés en desarrollar sistemas de codificación que involucren nuevos algoritmos y mejorar la seguridad de los existentes. En la actualidad, se pretende que los sistemas criptográficos sean, rápidos, seguros y sencillos de implementar.

Las tecnologías ópticas representan una alternativa válida para dotar de seguridad a la información [1.3-1.6], es decir, para que la misma sea accesible sólo a los usuarios autorizados. Los sistemas ópticos presentan importantes ventajas respecto a los electrónicos, debido a la inherente capacidad de procesar en paralelo de la luz, lo que permite aumentar la velocidad de transmisión de los datos, siendo esta una característica de gran importancia para aplicaciones en tiempo real. Otro rasgo destacable es que la información puede ser codificada empleando cualquiera de los grados de libertad que ofrece la óptica, tales como la fase, la polarización, la longitud de onda, etc.

En el campo de la codificación de datos, la propuesta de utilizar sistemas ópticos fue

hecha en el año 1975 por M. Françon [1.7], quien sugiere codificar un mensaje usando los cambios aleatorios de fase producidos por un difusor. En este caso, para extraer el mensaje es absolutamente necesario poseer la información del difusor, que actúa como llave. La idea de codificar información usando distribuciones aleatorias fue implementada por O. Kafri y E. Keren [1.8]. En dicha propuesta se acuña el término "encryption" para hacer referencia a la codificación óptica de datos. Precisamente, a partir de allí para referirnos al mismo proceso utilizamos el vocablo "encriptación".

Los esquemas de codificación óptica más utilizados, se basan en las arquitecturas de correlación. La primera arquitectura de correlación óptica, el correlador $4f$ propuesto por VanderLugt () [1.9], se basa en el uso de un filtro complejo adaptado. En 1966, una nueva arquitectura experimental, fue propuesta por Weaver y Goodman [1.10] y se denominó Correlador de Transformada Conjunta (Joint Transform Correlator), también conocido como JTC.

En 1995, P. Refregier y B. Javidi introducen por primera vez un sistema de encriptación óptica basado en la arquitectura $4f$ [1.11]. Este arreglo permite trasformar los datos de entrada en ruido blanco estacionario mediante el uso de dos máscaras de fase aleatorias. Por esta razón se le llama a esta configuración, arquitectura de doble máscara de fase aleatoria (Double Random Phase Encoding, conocida como DRPE). Las máscaras deben ser estadísticamente independientes y están ubicadas, una en el plano de entrada adosada a los datos a encriptar y la otra (máscara llave) se ubica en el plano de frecuencias. En esta primera versión, en el proceso de desencriptación, la información original se recupera a partir de los datos encriptados y del complejo conjugado de la máscara llave, cuando los datos de entrada son de amplitud. En el caso que los datos de entrada sean en fase pura se necesitan el complejo conjugado de las dos máscaras. Un año después, B. Javidi, G. Zhang y J. Li [1.12] implementan experimentalmente el proceso de encriptación-desencriptación con la arquitectura DRPE usando como medio de registro una placa holográfica y máscaras aleatorias generadas empleando moduladores de fase. En 1997, B. Javidi, G. Zhang y J. Li [1.13] extienden la propuesta anterior al almacenamiento múltiple de datos encriptados. En este trabajo se almacenan en una única placa holográfica dos imágenes encriptadas empleando máscaras llaves

estadísticamente independientes. En 1998, G. Unnikrishnan, J. Joseph y K. Singh [1.14] implementaron la técnica usando un cristal fotorrefractivo como medio de de almacenamiento. Mediante el mezclado de cuatro ondas dentro del cristal se genera el complejo conjugado de los datos encriptados. Con esta nueva variante no se requiere emplear el complejo conjugado de la máscara llave para decodificar los datos, es decir se usan las mismas máscaras empleadas que en la etapa de encriptación. Este cambio facilitó la implementación experimental del método DRPE. A partir de ese momento se desarrollaron muchas investigaciones encaminadas a analizar el desempeño del método [1.15-1.17], sus vulnerabilidades [1.18-1.120], el desarrollo de variantes en la configuración del DRPE, tales como, la propagación en el espacio libre [1.21-1.22], la transformada fraccional de Fourier [1.23]. Las aplicaciones de encriptación que emplean el DRPE continúan siendo un tema de interés actual. Este sistema presenta una alta sensibilidad a los problemas de alineamiento del sistema óptico. Por otra parte los datos encriptados son de amplitud compleja, es decir contienen información tanto de amplitud cuanto de fase, requiriendo el empleo de alguna técnica holográfica y un medio de registro apropiado para su almacenamiento. También es necesario utilizar en la etapa de desencriptación, como fue mencionado, el complejo conjugado de los datos encriptados ó de las máscaras llaves. Con el objetivo de aliviar estas dificultades, se implementó una nueva arquitectura de encriptación, basada en el correlador de transformada conjunta.

El uso de la arquitectura JTC fue propuesta por T. Nomura y B. Javidi [1.24] en el año 2000. En esta configuración, la imagen a encriptar adosada a una máscara de fase aleatoria y la máscara llave están ubicadas a lado y lado en el plano de entrada del sistema. Estos datos son transformados conjuntamente por una lente obteniéndose en su plano focal la información encriptada. En este caso, a diferencia del DRPE, la información encriptada es la intensidad del campo, es decir, el espectro conjunto de energía (Joint Power Spectrum conocido como JPS). Por esta razón, en el registro no se requiere utilizar un haz de referencia, ya que este sistema es holográfico en sí, lo cual hace que esta arquitectura sea fácil de implementar. Además, presenta la ventaja de no requerir en la etapa de desencriptación la generación del complejo conjugado de la máscara llave ó de la información encriptada. En este caso es suficiente iluminar el JPS con un campo que

sea proporcional a la transformada de Fourier de la máscara llave. Para obtener la información original, el campo resultante es transformado nuevamente por una segunda lente. Si el objeto a ser encriptado es sólo de amplitud, se puede detectar con un sensor de intensidad. Por otro lado, el correlador JTC es invariante a las traslaciones siendo por lo tanto menos sensible a los problemas de alineamiento.

Las investigaciones en la línea de la encriptación óptica están encaminadas en encontrar la manera de incrementen la seguridad de estos sistemas. Una alternativa interesante, que mejora significativamente la seguridad, es el almacenamiento múltiple de datos (multiplexado) encriptados en un único medio de registro. Los primeros trabajos en esta dirección, O. Matoba y B. Javidi [1.25, 1.26], aprovechan la selectividad angular de los medios de volumen, para almacenar múltiples datos encriptados. Luego, C. C. Sun et al. [1.27] implementan un proceso de múltiple almacenamiento de información encriptada que combina el multiplexado angular y desplazamientos laterales del difusor. Estos trabajos pioneros llevaron a indagar el empleo de diferentes parámetros ópticos para multiplexar datos encriptados [1.28-1.33]. Aunque los primeros trabajos usan medios de volumen para el registro, también es posible almacenar múltiples datos encriptados en un medio plano. Esto es posible, debido a que los datos encriptados ópticamente, tienen redundancia de información tal como los hologramas, luego no se requiere el total del patrón para recuperar los datos de entrada. Para llevar a cabo el multiplexado en un único medio plano, se necesita variar de algún (ó algunos) parámetro óptico [1.28-1.33] que asegure que los patrones encriptados correspondientes a distintos objetos de entrada sean estadísticamente independientes. Si existe algún grado de correlación entre los patrones encriptados, a la imagen decodificada se le superpone la información correspondiente a otro (otros) objeto de entrada. Este efecto no deseado se conoce con el nombre de *"cross talk"* ó solapamiento. Por esta razón, cuando se implementa un proceso de multiplexado, es necesario hacer una calibración de la sensibilidad del sistema a la variación del parámetro que se va a utilizar. Los valores de los parámetros ópticos, que aseguren que no exista solapamiento, en cada registro del multiplexado, definen un posible canal de información. Cuando se recupera la información de un canal en un proceso de multiplexado, a la información desencriptada

se le superpone ruido correspondiente a los objetos de entrada que no son correctamente desencriptados. Naturalmente el ruido en los datos recuperados aumenta cuando se incrementa la cantidad de canales. Este hecho impone un límite a la cantidad de datos encriptados que pueden ser multiplexados en un medio para un sistema dado. No tenemos conocimiento de investigaciones encaminadas a estudiar dicho límite. Por esta razón, este aspecto será analizado en el desarrollo de este trabajo.

Los sistemas de encriptación óptica han sido vulnerados. Los métodos de ataque propuestos en la literatura involucran un único patrón encriptado. No existen antecedentes de ataques exitosos a sistemas que involucren el multiplexado de información encriptada. Una de las razones de esta resistencia frente a los ataques se debe a que es muy difícil determinar a partir del patrón encriptado multiplexado el número de objetos codificados. Esto se debe a la naturaleza de la información encriptada, dado que la suma patrones de ruido blanco aleatorio dan como resultado un nuevo patrón de ruido blanco donde las distribuciones encriptadas individuales asociadas a cada canal son indistinguibles. Por lo tanto, las aplicaciones que involucran múltiple almacenamiento de información encriptada son de gran interés. Si bien hace más de diez años que se implementan procesos de multiplexado, hasta ahora no se han estudiado los mecanismos que posibilitan dichos procesos.

Todos los antecedentes antes mencionados nos motivan a desarrollar investigaciones que permitan caracterizar, mejorar e implementar procesos de multiplexado de datos encriptados. Como etapa previa al estudio de procesos de multiplexado, es necesario caracterizar y optimizar las arquitecturas de encriptación óptica 4f y JTC. Es importante tener presente que una imagen desencriptada experimentalmente ó en simulaciones que buscan replicar condiciones reales, siempre se presenta ruido. Sin embargo, la mayoría de los trabajos publicados en esta línea, son realizados digitalmente y presentan imágenes desencriptadas sin ruido. Es llamativo que las condiciones reales (dimensión finita de las pupilas, tamaño finito del medio de almacenamiento, etc) de los sistemas de encriptación no sean motivo de investigación en dichas propuestas. De esta manera, se evoluciona en arquitecturas digitales que aumentan más la brecha respecto a una genuina implementación experimental. En

nuestro concepto se necesita hacer investigaciones que disminuyan esa brecha. Al tener en cuenta las condiciones reales, los resultados de los sistemas digitales se hacen más comparables a los experimentales. Bajo estas condiciones, las simulaciones se pueden aprovechar para optimizar los arreglos experimentales.

En la siguiente sección se presenta un resumen del contenido por capítulos desarrollado en este trabajo de tesis.

I.2 Contenido por capítulos

En el Capítulo II de este trabajo se presentan los conceptos teóricos básicos necesarios para comprender los resultados que se presentan a partir del Capítulo III. Se presentan las configuraciones básicas que condujeron al desarrollo de los arreglos de encriptación, es decir los correladores 4*f* y JTC. Luego se presentan los sistemas de encriptación de doble máscara de fase aleatoria 4*f* y JTC. Dado que los datos encriptados ópticamente son esencialmente patrones de speckle se introduce las principales características de estas distribuciones.

En el Capítulo III se estudia como es la distribución de la información del patrón encriptado en términos de los tamaños de los centros dispersores de las máscaras de fase objeto y llave para la arquitectura 4*f*. Este estudio provee las herramientas que permiten controlar la distribución espacial de los datos encriptados, de manera que la mayor cantidad de información pueda ser almacenada en el medio de registro disponible. Por otra parte, se analiza la degradación de la imagen desencriptada debido a la pérdida de información originada por el área finita del medio de almacenamiento. A partir de estos estudios se determina la mínima cantidad de datos encriptados necesarios para obtener una imagen desencriptada que permita reconocer el objeto de entrada.

En el Capítulo IV se estudia como es la distribución de la información del patrón encriptado en términos de los tamaños de los centros dispersores de las máscaras objeto y llave para la arquitectura JTC. Siguiendo el mismo procedimiento que en el Capítulo III, se analiza el deterioro de la imagen desencriptada debido a la pérdida de datos encriptados por efecto del tamaño finito del medio de registro. Se demuestra que para

esta arquitectura las imágenes desencriptadas presentan un ruido adicional debido a la no uniformidad de la amplitud del espectro de la máscara llave. Con el fin de solucionar este problema, se presenta una propuesta de un JTC optimizado para operar en sistemas de óptica virtual. Se demuestra a partir de resultados simulados que las imágenes se recuperan sin la degradación que exhiben las obtenidas en el JTC no optimizado. Por último, se demuestra que controlando adecuadamente el ancho de banda de la señal de entrada (objeto de entrada, máscara objeto) se puede mejorar significativamente la salida desencriptada para un medio de registro fijo.

En el Capítulo V se analizan aspectos relevantes del almacenamiento múltiple de información encriptada. Se estudia la capacidad de multiplexado en los sistemas 4*f* y JTC en función del tamaño del objeto de entrada para un área fija del medio de registro. El multiplexado de datos encriptados se lleva a cabo mediante la variación de algún (ó algunos) parámetro óptico, tales como la longitud de onda, la polarización, etc., que asegure que los patrones encriptados correspondientes a distintos objetos de entrada sean estadísticamente independientes. Se presenta un método de evaluación de la sensibilidad del sistema al parámetro elegido. A partir de estos estudios, se implementa un multiplexado en longitud de onda para una arquitectura JTC y su aplicación para la encriptación de imágenes a color. También, se presentan resultados experimentales.

En el Capítulo VI se proponen dos técnicas de encriptación óptica de información que utilizan el almacenamiento múltiple de datos encriptados como herramienta para aumentar la seguridad de un dato altamente confidencial y para crear canales que proporcionan diferentes niveles de acceso a la información encriptada.

Finalmente, en el Capítulo VII se presentan las conclusiones y las perspectivas para futuros trabajos.

I.3 Referencias

[1.1] J. C. Galende Díaz, “Criptografía: historia de la escritura cifrada”, editorial complutense S.A, Madrid, 1ª edición septiembre (1995).

[1.2] M. Á. López Guerrero, E. C. García del Castillo Crespo, “Introducción a la criptografía:

historia y actualidad", ediciones de la universidad de castilla, La Mancha, España (2006).

[1.3] B. Javidi, J. L. Horner, "Optical pattern recognition for validation and security verification", Opt. Eng. 33, 1752–1756 (1994).

[1.4] B. Javidi, G. S. Zhang, J. Li, "Experimental demonstration of the random phase encoding technique for image encryption and security verification", Opt.Eng. 35, 2506-2512 (1996).

[1.5] B. Javidi, E. Ahouzi, "Optical security system with Fourier plane encoding", Appl. Opt. 37, 6247–6255 (1998).

[1.6] R. K. Wang, I. A. Watson, C. Chatwin, "Random phase encoding for optical security", Opt. Eng. 35, 2464–2469 (1996).

[1.7] M. Francon, "Information Processing Using Speckle Patterns", en Laser speckle and related phenomena, J. C. Dainty Ed., Springer-Verlag, New York (1975).

[1.8] O. Kafri, E. Keren, "Encryption of pictures and shapes by random grids", Opt. Lett. 12, 377-379 (1987).

[1.9] A. VanderLugt, "Signal detection by complex spatial filtering", I.E.E.E. Trans. Info. Theory, IT-10,139-145 (1964).

[1.10] C. S. Weaver, J. W. Goodman, "Technique for Optically Convolving Two Functions", Appl. Opt. 5, 1248-1249 (1966).

[1.11] P. Réfrégier, B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding", Opt. Lett. 20, 767-797 (1995).

[1.13] B. Javidi, G. Zhang, J. Li, "Experimental demonstration of the random phase encoding technique for image encryption and security verification", Opt. Eng. 35, 2506–2512 (1996).

[1.13] B. Javidi, G. Zhang, J. Li, "Encrypted optical memory using double-random phase encoding", Appl. Opt. 36, 1054-1058 (1997).

[1.14] G. Unnikrishnan, J. Joseph, K. Singh, "Optical encryption system that uses phase

conjugation in a photorefractive crystal", Appl. Opt. 37, 8181–8186 (1998).

[1.15] B. Javidi, A. Sergent, G. Zhang, L. Guibert, "Fault tolerance properties of a double phase encoding encryption technique," Opt. Eng. 36, 992–998 (1997).

[1.16] B. Wang, C. Sun, W. Su, A. Chiou, "Shift-tolerance property of an optical double random phase encoding encryption system," Appl. Opt. 39, 4788–4793 (2000).

[1.17] C. Sun, W. Su, "Three dimensional shifting selectivity of random phase encoding in volume holograms", Appl. Opt. 40, 1253–1260 (2001).

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

[1.19] 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).

[1.20] L. Neto, Y. Sheng, "Optical implementation of image encryption using random phase encoding", Opt. Eng. 35, 2459–2463 (1996).

[1.21] G. Situ, J. Zhang, "Double random-phase encryption in the Fresnel domain", Opt. Lett. 29, 1584–1586 (2004).

[1.22] A. Nelleri, J. Joseph, K. Singh, "Digital Fresnel field encryption for three dimensional information security", Opt. Eng. 46, 045801 (2007).

[1.23] G. Unnikrishnan, K. Singh, "Double random fractional Fourier domain encoding for optical security", Opt. Eng. 39, 2853–2859 (2000).

[1.24] T. Nomura, B. Javidi, "Optical encryption using a joint transform correlator architecture", Opt. Eng. 39, 2031–2035 (2000).

[1.25] O. Matoba, B. Javidi. "Encrypted optical memory system using three-dimensional keys in the Fresnel domain". Opt Lett. 24, 762-764 (1999).

[1.26] O. Matoba, B. Javidi, "Encrypted optical storage with angular multiplexing", App. Opt. 38, 7288-7293 (1999).

[1.27] C. C. Sun, W. C. Su, B. Wang, A. E.T. Chiou. “Lateral shifting of a ground glass for holographic encryption and multiplexing using phase conjugate readout algorithm”, Opt. Commun. 191, 209–224 (2001).

[1.28] J. Barrera, M. Tebaldi, R. Torroba, N. Bolognini, “Multiplexing encryption-decryption via lateral shifting of a random phase mask”, Opt. Comm. 259, 532–536 (2006).

[1.29] J. Barrera, R. Henao, M. Tebaldi, R. Torroba, N. Bolognini, “Multiplexing encrypted data by using polarized light”, Opt. Comm. 260, 109–112 (2006).

[1.30] J. Barrera, R. Henao, M. Tebaldi, R. Torroba, N. Bolognini, “Multiple image encryption using an aperture-modulated optical system,” Opt. Comm. 261, 29–33 (2006).

[1.31] R. Henao, E. Rueda, J. F. Barrera, R. Torroba, "Noise-free recovery of optodigital encrypted and multiplexed images", Opt. Lett. 35, 333-335 (2010).

[1.32] F. Mosso, J. F. Barrera, M. Tebaldi, N. Bolognini, R. Torroba, "All-optical encrypted movie", Opt. Express 19, 5706-5712 (2011).

[1.33] L. Cabezas, M. Tebaldi, J. F. Barrera, N. Bolognini, R. Torroba, "Optical smart packaging to reduce transmitted information", Opt. Express 20, 158-163 (2012).

CAPÍTULO II

Conceptos teóricos básicos

I.1 Introducción

En este capítulo se abordan los principales conceptos teóricos básicos necesarios para la comprensión de los resultados a ser analizados en los capítulos siguientes. En los procesos de encriptación y multiplexado a ser estudiados se usan las arquitecturas ópticas de doble máscara de fase aleatoria y la de correlador de transformada conjunta. La descripción de estos dos esquemas se aborda a partir del desarrollo histórico que condujo a su implementación. Recordemos que la operación de convolución entre dos señales es implementada en óptica principalmente por dos tipos de arquitecturas: el correlador de Vander Lugt ó procesador 4f [2.1] y el correlador de trasformada conjunta ó JTC [2.1]. Entre otras aplicaciones estos arreglos permiten manipular los datos de entrada de tal manera que se puedan resaltar características de las imágenes, filtrar información, mejorar la relación señal ruido, etc. [2.2]. En Sección II.2.1 se describe el funcionamiento de ambos procesadores y en la Sección II.2.2 su uso en múltiples aplicaciones para el reconocimiento de datos. Finalmente, en la Sección II.2.3 se presentan las adaptaciones que requieren los mencionados correladores para su empleo como sistemas de encriptación. Estos dispositivos se basan en la introducción de difusores aleatorios de fase para codificar datos como ruido blanco estacionario, tanto en la arquitectura DRPE [2.3] cuanto en la JTC [2.4]. La encriptación analógica y digital será el objetivo general de este trabajo.

II.2 Procesador 4f

Como es bien conocido, una de las principales propiedades de una lente convergente es su capacidad para realizar la transformada óptica de Fourier, o

distribución espectral de un campo de entrada [2.1], cuando éste se ubica en el plano focal anterior de la lente y se observa en el plano focal posterior. A esta arquitectura se le llama sistema $2f$. Por otra parte, la arquitectura $4f$ se obtiene mediante el uso de dos sistemas $2f$ contiguos, de tal manera que entre el plano de salida del sistema y el de entrada hay justamente una distancia equivalente a 4 veces la distancia focal f de la lente utilizada. En la **Figura 2.1** se esquematiza un procesador óptico $4f$. La primera lente L_1 realiza la transformada de Fourier del campo que emerge del plano objeto (x_0, y_0), localizada en el plano espectral (x_1, y_1). La distribución en el plano de salida (x_2, y_2) se obtiene mediante una segunda transformada de Fourier generada por la lente L_2.

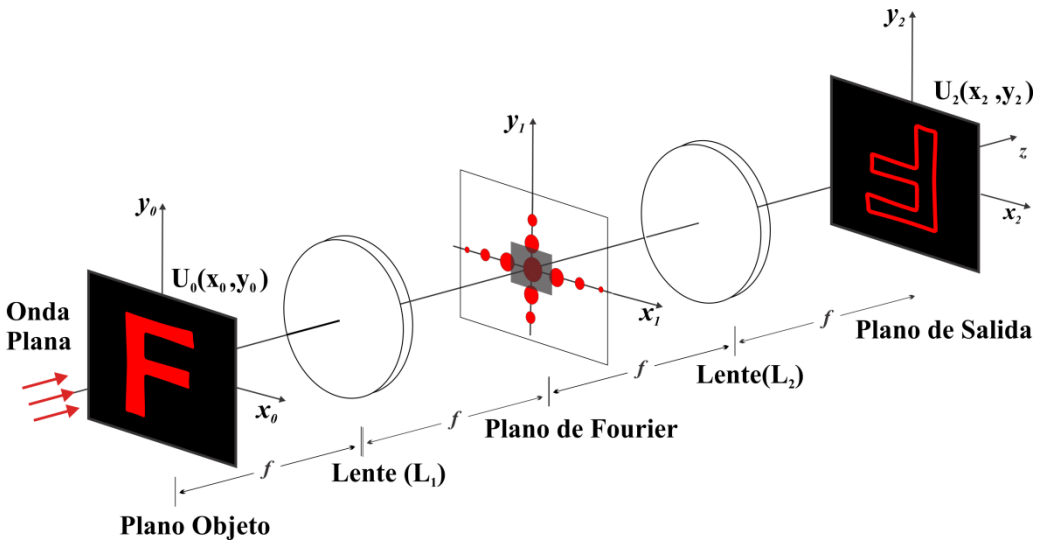


Figura 2.1 Procesador óptico $4f$.

Si la distribución de entrada está representada por la función $U_0(x_0, y_0)$, e incide sobre ella una onda plana de amplitud unitaria y longitud de onda λ, la distribución de campo $U_1(x_1, y_1)$ en el plano espectral es:

$$U_1(x_1, y_1) = \frac{1}{i\lambda f} \iint_{-\infty}^{\infty} U_0(x_0, y_0) e^{\frac{-i2\pi}{\lambda f}(x_0 x_1 + y_0 y_1)} \, dx_0 \, dy_0$$

$$U_1(x_1, y_1) = \frac{1}{i\lambda f} \, \Im\left\{U_0\left(\frac{x_0}{\lambda f}, \frac{y_0}{\lambda f}\right)\right\} \qquad (2.1)$$

donde $\Im$ representa el operador transformada de Fourier. Al realizar la segunda transformada de Fourier se obtiene el campo a la salida $U_2(x_2, y_2)$ representado por:

$$U_2(x_2, y_2) = \Im\left\{\frac{1}{i\lambda f} U_1\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right)\right\}$$

$$= \Im\{\Im\{U_0(x_0, y_0)\}\}$$

$$= U_0(-x_0, -y_0) \tag{2.2}$$

La tercera fila de la ecuación (2.2) representa a la función de entrada, pero invertida debido a la doble transformada y con magnificación unitaria, dado que las dos lentes tienen la misma distancia focal. Está configuración es una herramienta muy adecuada para el procesamiento óptico de información, ya que permite manipular los datos en el espacio de frecuencias de tal manera que se obtenga en la salida la distribución deseada. Un ejemplo se muestra en la **Figura 2.1**, donde se utiliza un filtro pasa-altos en el plano de Fourier para obtener en el plano de salida, sólo la información de alta frecuencia de la imagen de entrada.

II.3 Correladores ópticos

La operación de correlación entre dos funciones da cuenta del grado de similitud que existe entre ellas, por esta razón es una herramienta clave para las aplicaciones de reconocimiento, identificación, validación de objetos patrones e imágenes, etc. [2.5]. Mediante el uso de las propiedades de la transformada de Fourier, la operación de correlación se simplifica a una multiplicación en el dominio de frecuencias y una transformada inversa de Fourier para volver a las coordenadas espaciales. Como mencionamos, las lentes delgadas convergentes tienen la propiedad de llevar a cabo ópticamente la transformada de Fourier, lo que permitió implementar algunas arquitecturas ópticas que realicen la operación de correlación. En estas arquitecturas se pretende detectar si en la escena de entrada está contenido el objeto que queremos reconocer (objeto patrón ó referencia), u otro con un cierto grado de semejanza con respecto a nuestro objeto patrón. El sistema debe dar una respuesta que permita según algún criterio (por ejemplo un umbral en la intensidad del pico de correlación) tomar decisiones. Esto se logra mediante el uso de un filtro adecuado diseñado específicamente para reconocer el objeto que buscamos detectar.

II.3.1 Correlador 4f

La información del objeto referencia en la arquitectura 4*f* está embebida en un filtro que se ubica en el plano de Fourier. Estos filtros usualmente contienen información tanto de amplitud cuanto de fase. Las primeras versiones de estos filtros tenían algunas limitaciones. Antes de 1963 la forma convencional de introducir esta información era usar máscaras independientes para la amplitud y la fase. La transmitancia de amplitud se elaboraba con técnicas fotográficas. La transmitancia de fase era una placa transparente con una apropiada variación de espesor que produjera la diferencia de fase requerida. Tales placas podían ser elaboradas en un substrato, por métodos de grabado, ó por deposición de películas delgadas. Es fácil imaginarse que con la tecnología de la época, el uso de estos métodos era bastante complicado y funcionaban bien sólo si el patrón de fase deseado era sencillo, por ejemplo, un patrón binario de simple estructura geométrica. A partir de 1963 con la invención de los filtros grabados interferometricamente esta limitación fue superada y se pudieron fabricar filtros con información más compleja.

En 1963 Vander Lugt propone una nueva técnica para sintetizar filtros para procesadores ópticos coherentes. Los filtros generados por esta técnica tienen la importante propiedad que pueden controlar la amplitud y la fase de una función de transferencia [2.6], a pesar de consistir sólo de patrones de absorción. Por medio de esta técnica, fue posible solucionar las limitaciones que tenían los sistemas ópticos coherentes. El filtro es sintetizado con ayuda de un sistema interferométrico. Tal como se muestra en la **Figura 2.2**, una lente colima la luz proveniente de la fuente puntual S. Una parte del frente de onda incide sobre la máscara M_1, la cual tiene una transmitancia proporcional a la respuesta impulso deseada h. La lente L_1 realiza la transformada de Fourier de la distribución de amplitud de h, resultando una amplitud de distribución de campo:

$$\frac{1}{\lambda f} H\left(\frac{x_2}{\lambda f}, \frac{y_2}{\lambda f}\right) \tag{2.3}$$

donde H es la transformada de Fourier de h. Este campo incide sobre el medio de almacenamiento, usualmente una película fotográfica. Además, otra porción del haz colimado pasa a través de un prisma P ubicado por encima de la máscara M_1 y finalmente la luz emergente incide en el plano de almacenamiento (x_1, y_1) con un ángulo θ, como se muestra en la **Figura 2.2**. Esta onda plana inclinada incidente produce una distribución de campo:

$$U_1(x_1, y_1) = r_0 e^{-i2\pi\alpha y_1} \tag{2.4}$$

donde r_0 es la amplitud de la onda incidente y α la frecuencia espacial dada por:

$$\alpha = \frac{\text{Sen}\,\theta}{\lambda} \tag{2.5}$$

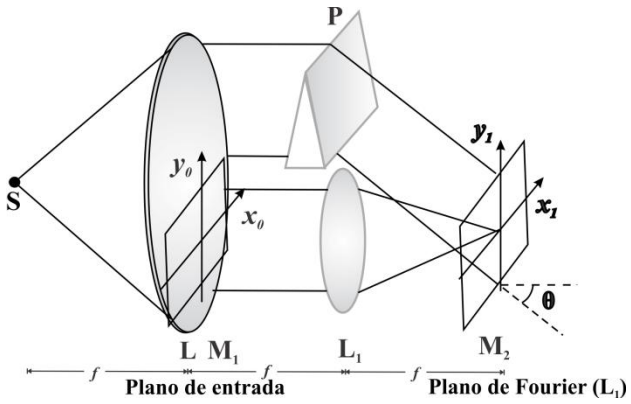


Figura 2.2. Grabado de una máscara de frecuencia plana para un filtro VanderLugt.

La intensidad total incidente en cada punto del medio de almacenamiento está determinada por la interferencia de dos distribuciones de amplitud mutuamente coherentes. Entonces, la distribución de intensidad resultante es:

$$I(x_1, y_1) = \left| r_0 e^{-i2\pi\alpha y_1} + \frac{1}{\lambda f} H\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right) \right|^2 = r_0^2 + \frac{1}{\lambda^2 f^2} \left| H\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right) \right|^2 +$$

$$\frac{r_0}{\lambda f} H\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right) e^{i2\pi\alpha y_1} + \frac{r_0}{\lambda f} H^*\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right) e^{-i2\pi\alpha y_1} \tag{2.6}$$

Nótese que si la función compleja H tiene una distribución de amplitud A y una distribución de fase ψ, esto es, si:

$$H\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)=A\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)e^{i\psi\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)} \tag{2.7}$$

entonces la expresión para la intensidad I, dada por la ecuación (2.6), puede ser reescrita como:

$$I(x_1,y_1)=r_0^2+\frac{1}{\lambda^2 f^2}A^2\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)+\frac{2r_0}{\lambda f}A\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)\cos\left[2\pi\alpha y_1+\psi\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)\right] \tag{2.8}$$

Esta expresión ilustra el hecho que un proceso interferométrico permite el almacenamiento de una función compleja H sobre un detector sensible a la intensidad. La información de amplitud y fase son almacenadas respectivamente como modulaciones de amplitud y fase de una portadora de alta frecuencia que es introducida por el ángulo relativo de inclinación de la onda de referencia que emerge del prisma. Existen otros sistemas ópticos que producirían la misma distribución de intensidad [2.1].

Como paso final en la síntesis del filtro, la película fotográfica registrada es revelada resultando una transparencia cuya transmitancia en amplitud es proporcional a la distribución de intensidad que incidió durante el proceso de exposición. Entonces, la transmitancia en amplitud del filtro es de la forma:

$$t_A(x_1,y_1)\propto r_0^2+\frac{1}{\lambda^2 f^2}|H|^2+\frac{1}{\lambda f}He^{i2\pi\alpha y_1}+\frac{r_0}{\lambda f}H^*e^{-i2\pi\alpha y_1} \tag{2.9}$$

Nótese que, el tercer término de la transmitancia en amplitud es proporcional a H que es la forma requerida para sintetizar un filtro con respuesta impulso h.

Una vez que el filtro ha sido sintetizado, este es insertado en un sistema 4f, como se muestra en la **Figura 2.3**.

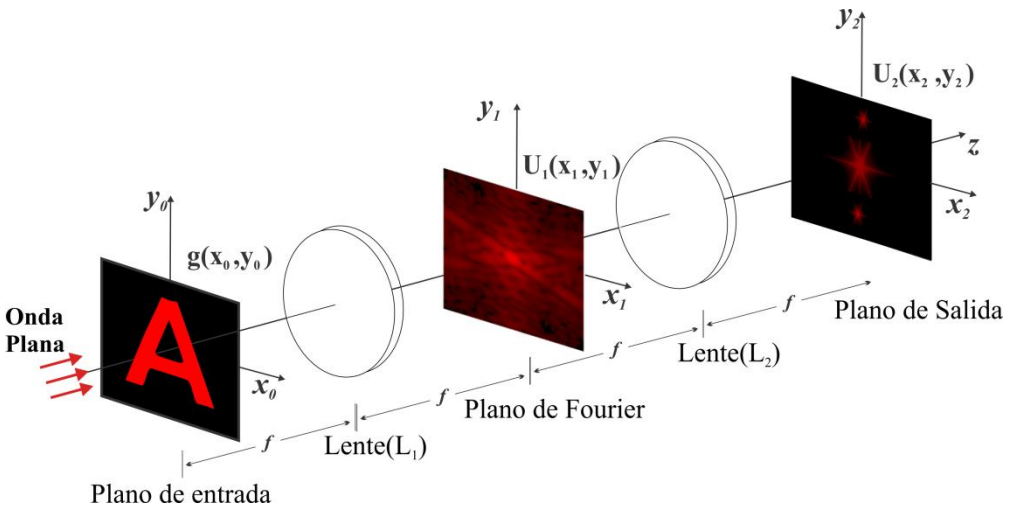


Figura 2.3. Correlador 4*f* con filtro VanderLugt.

La distribución de amplitud compleja, que incide en el filtro, es la transformada de la imagen $g(x_0, y_0)$, y esta dada por:

$$\frac{1}{\lambda f} G\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right) \tag{2.10}$$

El campo transmitido por el filtro entonces es proporcional a:

$$U_1(x_1, y_1) \propto \frac{{r_0}^2 G}{\lambda f} + \frac{1}{\lambda^3 f^3}|H|^2 G + \frac{r_0}{\lambda^2 f^2} H G e^{i2\pi\alpha y_1} + \frac{r_0}{\lambda^2 f^2} H^* G e^{-i2\pi\alpha y_1} \tag{2.11}$$

La lente L_2 de la **Figura 2.3** hace la transformada óptica de Fourier del campo $U_1(x_1, y_1)$. Teniendo en cuenta las constantes de escalamiento y que el sistema de coordenadas está reflejado en el plano de salida (x_2, y_2), el valor del campo en este plano es proporcional a:

$$\begin{aligned} U_2(x_2, y_2) \quad \propto\ & r_0^2 g(x_2, y_2) + \frac{1}{\lambda^2 f^2}[h(x_2, y_2) \otimes h^*(-x_2, -y_2) \otimes g(x_2, y_2)] \\ & + \frac{r_0}{\lambda f}[h(x_2, y_2) \otimes g(x_2, y_2) \otimes \delta(x_2, y_2 + \alpha\lambda f)] \ + \\ & \frac{r_0}{\lambda f}[h^*(-x_2, -y_2) \otimes g(x_2, y_2) \otimes \delta(x_2, y_2 - \alpha\lambda f)] \end{aligned} \tag{2.12}$$

donde $\otimes$ representa la operación de convolución.

El primer y segundo término de la ecuación (2.12), no son de utilidad para la operación de filtrado, en cambio el tercer y cuarto término son de particular interés. Nótese que el tercer término:

$$h(x_2, y_2) \otimes g(x_2, y_2) \otimes \delta(x_2, y_2 + \alpha\lambda f) =$$

$$= \iint_{-\infty}^{\infty} h(x_2 - \xi, y_2 + \alpha\lambda f - \eta)\, g(\xi, \eta)\, d\xi\, d\eta \qquad (2.13)$$

es la *convolución* entre h y g, centrada en las coordenadas $(0, -\alpha\lambda f)$ en el plano (x_2, y_2). Asimismo, el cuarto término puede ser reescrito como:

$$h^*(-x_2, -y_2) \otimes g(x_2, y_2) \otimes \delta(x_2, y_2 - \alpha\lambda f) =$$

$$= \iint_{-\infty}^{\infty} g(\xi, \eta) h^*(\xi - x_2, \eta - y_2 + \alpha\lambda f)\, d\xi\, d\eta \qquad (2.14)$$

que es la *correlación cruzada* entre g y h centrada en las coordenadas $(0, \alpha\lambda f)$ en el plano (x_2, y_2).

Es claro que si *la frecuencia portadora* α es suficientemente alta, los términos de correlación y convolución estarán suficientemente separados en direcciones opuestas del eje óptico, pudiéndose detectarlos de forma independiente, es decir sin superposición. Para encontrar la *convolución* entre h y g, simplemente se debe observar la distribución de luz centrada en las coordenadas $(0, -\alpha\lambda f)$. Para encontrar la *correlación cruzada* entre g y h , la observación debe realizarse en las coordenadas centradas en $(0, \alpha\lambda f)$.

Para tener una idea más precisa de los requisitos que debe cumplir α, consideremos el ancho de los términos de salida ilustrados en la **Figura 2.4**. Si el máximo ancho de h en la dirección y es W_h y de g es W_g, entonces el ancho de los términos de salida son respectivamente:

1. $r_0^2 g(x_2, y_2) + \frac{1}{\lambda^2 f^2} \rightarrow W_g$

2. $\frac{1}{\lambda^2 f^2}[h(x_2, y_2) \otimes h^*(-x_2, -y_2) \otimes g(x_2, y_2)] \rightarrow 2W_h + W_g$

3. $\frac{r_0}{\lambda f}[h(x_2,y_2) \otimes g(x_2,y_2) \otimes \delta(x_2,y_2+\alpha\lambda f)] \rightarrow W_h + W_g$

4. $\frac{r_0}{\lambda f}[h^*(-x_2,-y_2) \otimes g(x_2,y_2) \otimes \delta(x_2,y_2-\alpha\lambda f)] \rightarrow W_h + W_g$ (2.15)

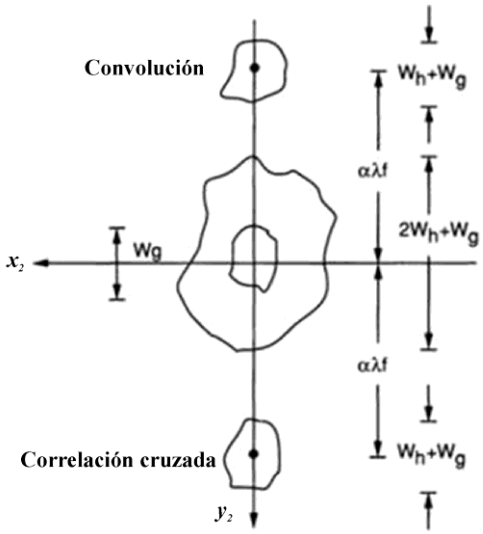


Figura 2.4. Localización de los términos de salida del procesador.

A partir de la **Figura 2.4** es claro que se obtiene la separación necesaria para discriminar los órdenes de la convolución y la correlación si:

$$\alpha > \frac{1}{\lambda f}\left(\frac{3W_h}{2} + W_g\right) \tag{2.16}$$

o equivalentemente, bajo la aproximación de ángulos pequeños:

$$\theta > \frac{2}{3}\frac{W_h}{f} + \frac{W_g}{f} \tag{2.17}$$

Si bien la introducción del filtro Vander Lugt solucionó algunos de los principales inconvenientes que los procesadores ópticos coherentes tenían en ese momento, seguía presentando algunas debilidades. La respuesta del procesador es muy sensible a la posición del filtro, por lo que se requiere una alta precisión en la ubicación de todos los componentes ópticos. Este filtro requiere una modulación de alta frecuencia, por lo cual es necesario utilizar un medio de registro de alta resolución que permita resolver estas franjas para su correcto funcionamiento.

II.3.2 Correlador de transformada conjunta

El correlador de transformada conjunta (JTC) es una arquitectura, propuesta por Weaver y Goodman en 1966 que permite realizar de manera óptica la correlación entre dos funciones. Desde su aparición el JTC ha sido ampliamente usado en muchas aplicaciones; por ejemplo, en sistemas de localización de trayectorias, sistemas dirigidos autónomamente, de reconocimiento de formas en tiempo real, entre otras [2.5]. Este correlador presenta ventajas respecto al esquema de Vander Lugt, dado que no necesita la síntesis de un filtro complejo para modular la amplitud y la fase de la transformada de Fourier de la función a ser procesada y asimismo es menos sensible a las vibraciones y a la desalineación de los elementos ópticos.

En la **Figura 2.5** se muestra un esquema de la etapa de registro para un correlador de transformada conjunta. En una de las ventanas del plano de entrada del correlador se ubica la función de referencia $h(x_0 - Y, y_0)$ y en la otra la función escena $g(x_0 + Y, y_0)$, ambas desplazadas del origen en la cantidad Y. Luego la función de entrada es:

$$U_0(x_0, y_0) = h(x_0 - Y, y_0) + g(x_0 + Y, y_0) \tag{2.18}$$

La densidad espectral conjunta de energía (JPS), la cual corresponde al módulo al cuadrado de la transformada de Fourier de la función de entrada $U_0(x_0, y_0)$, se registra empleando un medio sensible a la intensidad (por ejemplo, una placa holográfica, una cámara CCD, un cristal fotorrefractivo, etc.) ubicado en el plano focal posterior de la lente L_1

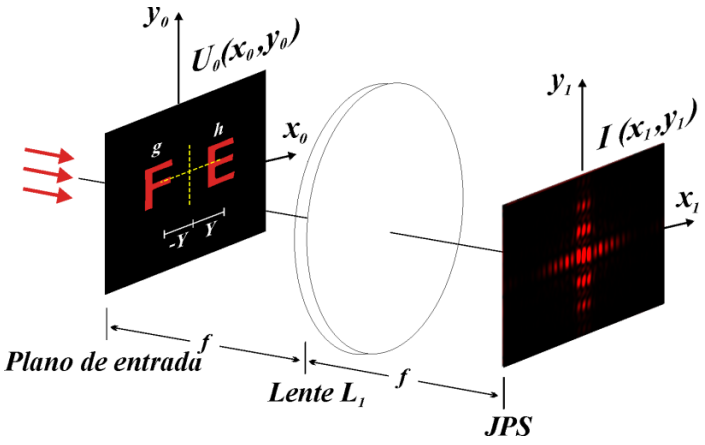


Figura 2.5. Etapa de registro de un correlador de transformada conjunta JTC

En el plano de Fourier, la amplitud compleja del campo electromagnético es proporcional a:

$$U_1(x_1, y_1) = \frac{1}{\lambda f} H\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right) exp\left(-j2\pi x_1 \frac{Y}{\lambda f}\right) + \frac{1}{\lambda f} G\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right) exp\left(j2\pi x_1 \frac{Y}{\lambda f}\right) \quad (2.19)$$

donde λ es la longitud de onda de la onda que ilumina el sistema óptico, *f es* la distancia focal de la lente L_1, H y G representan la transformada de Fourier de las funciones *h* y *g,* respectivamente. Entonces, el espectro de potencia conjunto está dado por:

$$I(x_1, y_1) = |U_1(x_1, y_1)|^2 =$$

$$= {}^{1}/_{\lambda^2 f^2} \left[\left| H\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right) \right|^2 + \left| G\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right) \right|^2 \right] +$$

$$+ {}^{1}/_{\lambda^2 f^2} \left[H\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right) G^*\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right) exp\left(-j2\pi x_1 \frac{2Y}{\lambda f}\right) \right] +$$

$$+ {}^{1}/_{\lambda^2 f^2} \left[H^*\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right) G\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right) exp\left(j2\pi x_1 \frac{2Y}{\lambda f}\right) \right] \quad (2.20)$$

Para hallar la correlación entre las funciones h y g es necesario realizar la transformada de Fourier de la densidad espectral conjunta de energía (JPS). La distribución de amplitud en el plano de salida del correlador $U_2(x_2, y_2)$ es:

$$u_2(x_2, y_2) = {}^{1}/_{\lambda f} [h(x_2, y_2) \otimes h^*(-x_2, -y_2) + g(x_2, y_2) \otimes g^*(-x_2, -y_2)]$$

$$+ {}^{1}/_{\lambda f} [h(x_2, y_2) \otimes g^*(-x_2, -y_2) \otimes \delta(x_2 - 2Y, y_2)]$$

$$+ {}^{1}/_{\lambda f} [h^*(-x_2, -y_2) \otimes g(x_2, y_2) \otimes \delta(x_2 + 2Y, y_2)] \quad (2.21)$$

donde los dos primeros términos corresponden a las autocorrelaciones de las funciones h y g respectivamente, y los dos últimos términos son las correlaciones cruzadas de las funciones *h* y *g*, centradas en (-2Y ,0,) y (2Y, 0) del plano de salida como se observa en la **Figura 2.6**.

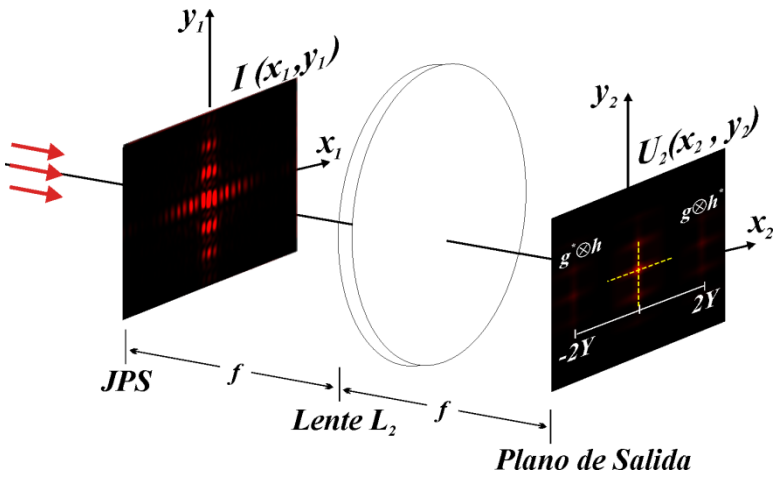
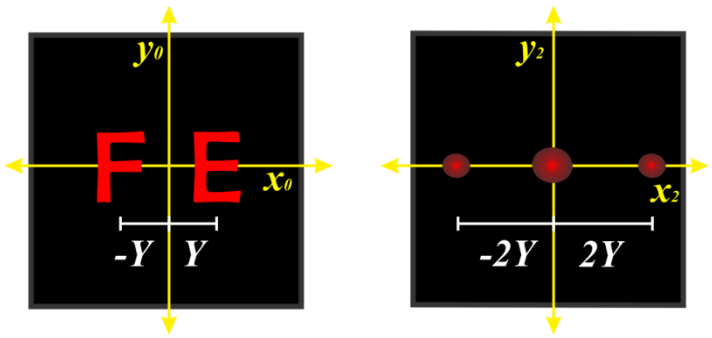


Figura 2.6. Correlador de transformada conjunta JTC. Etapa Lectura.

El JTC óptico convencional tiene como inconveniente que presenta una componente de orden cero de difracción. Para evitar que los picos de correlación se solapen con el orden cero (ver **Figura 2.7**) se debe imponer sobre la separación entre la escena y la referencia la siguiente restricción: $Y > max\{R_{y_1}, E_{y_1}\} + (R_{y_1} + E_{y_1})/2$, donde R_{y_1} es el ancho de la referencia y E_{y_1} de la escena a lo largo del eje y_1 [2.1].



(a) (b)

Figura 2.7. (a) Plano de entrada del correlador JTC, (b) Plano de salida. Localización de los picos de correlación en términos de la separación de las ventanas en el plano de entrada.

II.4 Sistemas de encriptación

II.4.1 Sistema de doble máscara de fase aleatoria ($4f$).

La técnica de codificación DRPE está basada en la arquitectura del correlador $4f$. En el arreglo se emplean dos máscaras para transformar los datos de entrada en ruido

blanco estacionario. Dichas máscaras son funciones complejas de amplitud unitaria y fase aleatoria uniformemente distribuida entre 0 y 2π, que a su vez deben ser estadísticamente independientes entre ellas. Una de las máscaras es adosada a los datos a encriptar en el plano de entrada del 4*f*, lo que resulta en una redistribución aleatoria de la información en el dominio de frecuencias. La otra máscara (*máscara llave o encriptadora*) se ubica en el plano de Fourier multiplicando al campo resultante de la primera transformada. La radiación que emerge es transformada al dominio espacial por la lente L_2 (Ver **Figura 2.8**). En el plano de salida del procesador 4*f* se obtiene la imagen codificada en una distribución compleja estacionaria de ruido blanco. Este proceso sólo es reversible si se conoce la máscara encriptadora M_2 cuando los datos a encriptar son reales y ambas máscaras si son complejos.

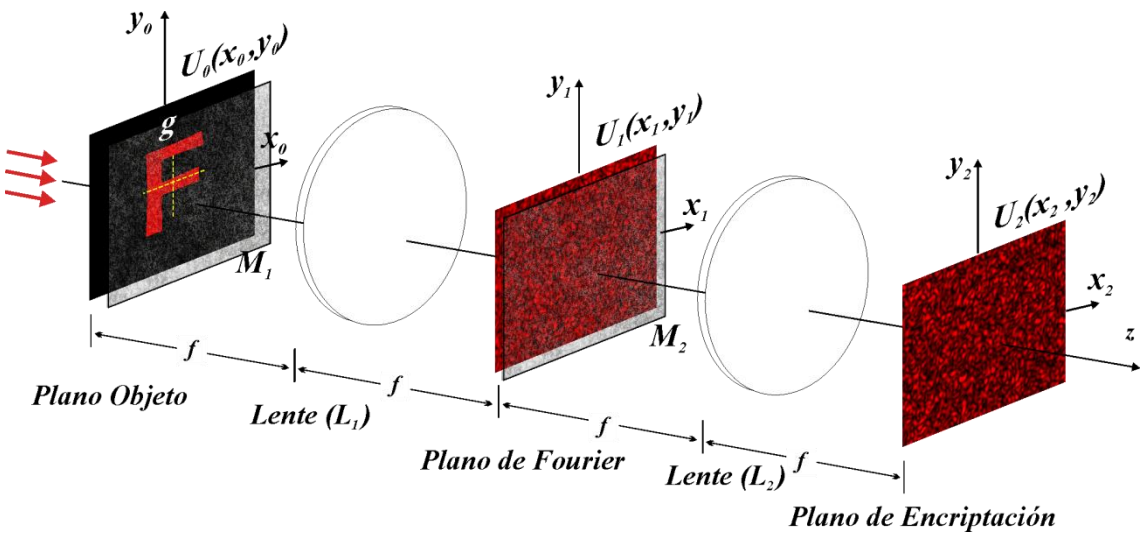


Figura 2.8. Esquema de encriptación basado en una arquitectura 4*f*.

Sea la información a encriptar una función real positiva $g(x_0, y_0)$, y sea la máscara de fase aleatoria M_1 definida en el plano de entrada $r(x_0, y_0) = e^{i2\pi p(x_0,y_0)}$, donde $p(x_0, y_0)$ es una distribución aleatoria uniformente distribuida entre los valores 0 y 1. El campo en el plano de entrada se representa por:

$$U_0(x_0, y_0) = g(x_0, y_0)r(x_0, y_0) \tag{2.22}$$

Se ilumina este plano con un haz de luz coherente colimado de longitud de onda λ y amplitud unitaria. El campo emergente se propaga a través de la lente L_1 de distancia

focal f tal que en su plano focal se obtenga la transformada de Fourier de los datos de entrada representada por:

$$U_1(x_1, y_1) = \left(\frac{1}{i\lambda f}\right) \Im\{U_0(x_0, y_0)\} \tag{2.23}$$

Por las propiedades de la transformada de Fourier una multiplicación en el espacio directo equivale a una convolución en el espacio de frecuencias, entonces la ecuación (2.23) resulta:

$$U_1(x_1, y_1) = \left(\frac{1}{i\lambda f}\right) G\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right) \otimes R\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right) \tag{2.24}$$

donde G y R representan la transformada de Fourier de g y r respectivamente.

Como fue mencionado, $r(x_0, y_0)$ es una función aleatoria de sólo fase que al ser multiplicada por los datos de entrada, cumple la función de redistribuir la información en el plano de Fourier como ruido blanco representados por $U_1(x_1, y_1)$. Sin embargo, los datos no están aún encriptados en este plano, ya que haciendo una simple transformada de Fourier inversa y observando con un detector de intensidad se recuperan los datos de entrada. Para que la información quede realmente encriptada, se utiliza en el plano de Fourier la máscara M_2 representada por $H(x_1, y_1) = \frac{1}{i\lambda f} e^{i2\pi Q\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right)}$, donde $Q\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right)$ es una distribución aleatoria uniformente distribuida entre 0 y 1, que debe ser estadísticamente independiente de $p(x_0, y_0)$. La información emergente del plano de Fourier es:

$$\left(\frac{1}{i\lambda f}\right)\left[G\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right) \otimes R\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right)\right] H(x_1, y_1) \tag{2.25}$$

La lente L_2 realiza una segunda trasformada de Fourier óptica, obteniéndose en el plano focal posterior el campo complejo que corresponde a los datos encriptados. La expresión para la información encriptada contenida en el plano (x_2, y_2), en un sistema 4f es proporcional a:

$$U_2(x_2, y_2) = [g(x_2, y_2) r(x_2, y_2)] \otimes h(x_2, y_2) \tag{2.26}$$

Esta ecuación representa la información encriptada como ruido blanco estacionario. Si hacemos una transformada de Fourier obtendríamos también ruido blanco. Para desencriptar la información, se requiere utilizar la función complejo conjugada de la máscara llave ó de la información encriptada.

En nuestro caso, para describir el proceso de desencriptación se utilizará la segunda opción. En los arreglos experimentales generar la función complejo conjugada de un campo, se logra mediante el empleo de materiales no lineales tales como los medios fotorrefractivos. Una vez obtenido el patrón encriptado conjugado, lo ubicamos en el plano de entrada del $4f$ con la misma configuración óptica del proceso de registro, tal como se muestra en la **Figura 2.9**. Este plano se ilumina con un haz colimado coherente de la misma longitud de onda que se empleó para encriptar. El campo emergente es transformado al dominio de Fourier mediante la lente L_2, resultando:

$$\Im[U_2(x_2,y_2)^*] = U_3(x_3,y_3) = \left(\frac{1}{-i\lambda f}\right)\left[G\left(\frac{x_3}{\lambda f},\frac{y_3}{\lambda f}\right) \otimes R^*\left(\frac{x_3}{\lambda f},\frac{y_3}{\lambda f}\right)\right] H^*\left(\frac{x_3}{\lambda f},\frac{y_3}{\lambda f}\right) \quad (2.27)$$

Esta expresión es equivalente a la función conjugada de este mismo plano (x_1, y_1) en la etapa de encriptación.

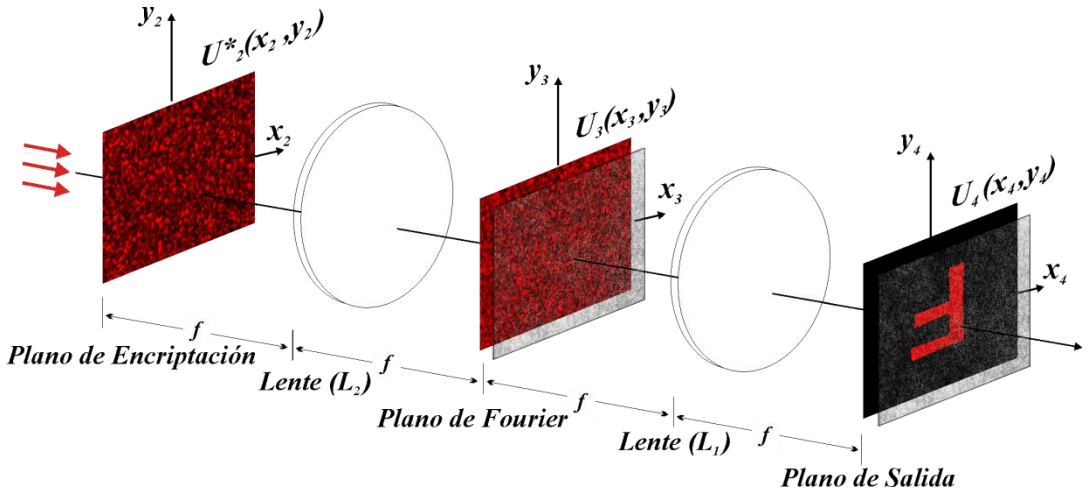


Figura 2.9. Esquema de desencriptación basado en una arquitectura $4f$.

En este plano se multiplica a $U_3(x_3, y_3)$ por la máscara llave $H(x_1, y_1)$ para compensar en uno de sus términos el efecto de $H^*\left(\frac{x_3}{\lambda f},\frac{y_3}{\lambda f}\right)$, dado que $H(x_1, y_1)$ fue definida antes como una función de sólo fase cuyas coordenadas son equivalentes

$\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)=\left(\frac{x_3}{\lambda f},\frac{y_3}{\lambda f}\right)$. Si la máscara M_2 que se utiliza en el proceso de desencriptación es exactamente igual a la que se usó en el proceso de encriptación y no se cambian los parámetros del sistema óptico, entonces se cumple que:

$$H^*\left(\frac{x_3}{\lambda f},\frac{y_3}{\lambda f}\right)H\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)=\left|H\left(\frac{x_3}{\lambda f},\frac{y_3}{\lambda f}\right)\right|^2=1 \tag{2.28}$$

Si multiplicamos al campo dado por la ecuación (2.27) por la máscara llave y utilizando la propiedad dada por la ecuación (2.28) obtenemos:

$$H\left(\frac{x_3}{\lambda f},\frac{y_3}{\lambda f}\right)U_3(x_3,y_3)=\left(\frac{1}{-i\lambda f}\right)\left[G\left(\frac{x_3}{\lambda f},\frac{y_3}{\lambda f}\right)\otimes R^*\left(\frac{x_3}{\lambda f},\frac{y_3}{\lambda f}\right)\right] \tag{2.29}$$

Si se utiliza una máscara llave diferente representada por $k\left(\frac{x_3}{\lambda f},\frac{y_3}{\lambda f}\right)$, las distribuciones de fase no se compensarían ya que: $H^*\left(\frac{x_3}{\lambda f},\frac{y_3}{\lambda f}\right)k\left(\frac{x_3}{\lambda f},\frac{y_3}{\lambda f}\right)\neq 1$ lo que provocaría que no se pueda recuperar la información original.

Por otro lado, resulta de interés analizar lo que ocurre si se utiliza en la etapa de desencriptación la máscara llave correcta pero desplazada con respecto a la posición original en la etapa de encriptación. Si el desplazamiento es tal que las máscaras estén decorrelacionadas, tampoco se puede recuperar la información original dado que no se cumple la condición dada por la ecuación (2.28). De manera análoga, el cambio de algún parámetro óptico del sistema modificaría el campo en el plano de Fourier $U_3(x_3,y_3)$, no permitiendo reconstruir los datos de entrada.

Si se satisfacen las condiciones necesarias sobre la máscara llave para cumplir la condición de la ecuación (2.28), entonces nos quedaría de la ecuación (2.29) sólo la parte correspondiente a la convolución:

$$\left(\frac{1}{-i\lambda f}\right)\left[G\left(\frac{x_3}{\lambda f},\frac{y_3}{\lambda f}\right)\otimes R^*\left(\frac{x_3}{\lambda f},\frac{y_3}{\lambda f}\right)\right] \tag{2.30}$$

Para recuperar la información original, se realiza otra transformada de Fourier mediante la lente L_1, para que esta convolución pase a ser una multiplicación en las coordenadas espaciales (x_4,y_4), las cuales son equivalentes a las coordenadas del plano de entrada (x_0,y_0). Finalmente, mediante un detector de intensidad se pueden

recuperar los datos de entrada $g(x_4, y_4)$. Esto es posible porque la información correspondiente a $r(x_4, y_4)$ no es visible con un detector de intensidad, debido a que contiene sólo información de fase, es decir:

$$\left|\Im\left\{\left(\frac{1}{-i\lambda f}\right)\left[G\left(\frac{x_3}{\lambda f}, \frac{y_3}{\lambda f}\right) \otimes R^*\left(\frac{x_3}{\lambda f}, \frac{y_3}{\lambda f}\right)\right]\right\}\right|^2 = |g(x_4, y_4) r^*(x_4, y_4)|^2 = |g(x_4, y_4)|^2 \quad (2.31)$$

II.4.2 Encriptación Óptica en una arquitectura JTC

Nomura y Javidi [2.4] en el 2000 presentan un método para encriptar información basado en la arquitectura JTC, que emplea dos mascaras de fase aleatorias como en la configuración 4*f*. En esta propuesta, la información encriptada corresponde al espectro conjunto de potencia (JPS) el cual se registra en un medio sensible a la intensidad. En la etapa de desencriptación no se necesita el complejo conjugado de ninguna de las máscaras, o de la información encriptada. Estas características representan una clara ventaja de esta arquitectura frente a la 4*f*.

Sea la función real positiva $g(x_0, y_0)$ la información a encriptar, y sea $r(x_0, y_0) = e^{i2\pi p(x_0, y_0)}$ una máscara de fase aleatoria definida en el dominio espacial, donde $p(x_0, y_0)$, es una distribución aleatoria uniformente distribuida entre los valores 0 y 1. La máscara $r(x_0, y_0)$ está adosada a la imagen a encriptar $g(x_0, y_0)$ y componen una de las ventanas del plano de entrada del JTC. En la otra ventana se ubica la máscara llave que definimos como $h(x_0, y_0)$, la cual es sintetizada como la transformada inversa de Fourier de una máscara en el dominio de frecuencias $H(x_1, y_1) = \frac{1}{i\lambda f} e^{i2\pi Q\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right)}$, donde $Q\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right)$ es una distribución aleatoria uniformemente distribuida entre 0 y 1, que debe ser estadísticamente independiente de $p(x_0, y_0)$.

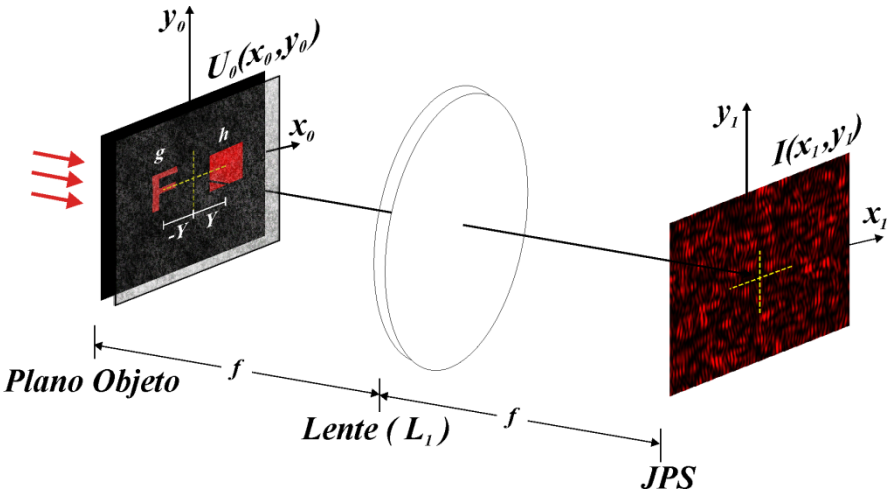


Figura 6.10. Esquema de desencriptación basado en una arquitectura 4f. Etapa de Lectura.

El campo en el plano de entrada es proporcional a:

$$U_0(x_0,y_0) = g(x_0,y_0)r(x_0,y_0) \otimes \delta(x_0+Y,y_0) + h(x_0,y_0) \otimes \delta(x_0-Y,y_0) \quad (2.32)$$

siendo $2Y$ la distancia de centro a centro de las ventanas en el plano de entrada del JTC.

Se ilumina el plano de entrada con un haz colimado coherente de longitud de onda λ. El campo emergente se transforma al dominio de Fourier mediante la lente L_1, quedando representado por:

$$U_1(x_1,y_1) = \frac{1}{i\lambda f}\left[G\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right) \otimes R\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)\right] e^{i\pi 2Y\frac{x_1}{\lambda f}} + \frac{1}{i\lambda f} H\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right) e^{-i2\pi Y\frac{x_1}{\lambda f}} \quad (2.33)$$

Como se mencionó en la Sección II.2.2, en la arquitectura JTC la información encriptada es el espectro de potencia, es decir el valor absoluto al cuadrado de la ecuación (2.33).

$$I(x_1,y_1) = |U_1(x_1,y_1)|^2 = \frac{1}{(\lambda f)^2}\left[\left|G\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right) \otimes R\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)\right|^2 + \left|H\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)\right|^2\right]$$

$$+\frac{1}{(\lambda f)^2}\left[G\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right) \otimes R\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)\right] H^*\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right) e^{i2\pi(2Y)\frac{x_1}{\lambda f}} +$$

$$+\frac{1}{(\lambda f)^2}\left[G^*\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right) \otimes R^*\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)\right] H\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right) e^{-i2\pi(2Y)\frac{x_1}{\lambda f}} \quad (2.34)$$

El primer término en la ecuación anterior sólo representa ruido, es decir, es energía que se distribuye alrededor del orden cero y no contribuyendo en la reconstrucción de los

datos de entrada en el proceso de desencriptación. El segundo término, dado que $H(x_1, y_1)$ fue definida como una función de sólo fase es igual a 1. En el tercer término está contenida la información que va a producir la imagen desencriptada y el cuarto es igual al término anterior pero complejo conjugado. Este espectro de potencia se almacena en un medio sensible a la intensidad, para generar un patrón de absorción que sea proporcional a la información encriptada.

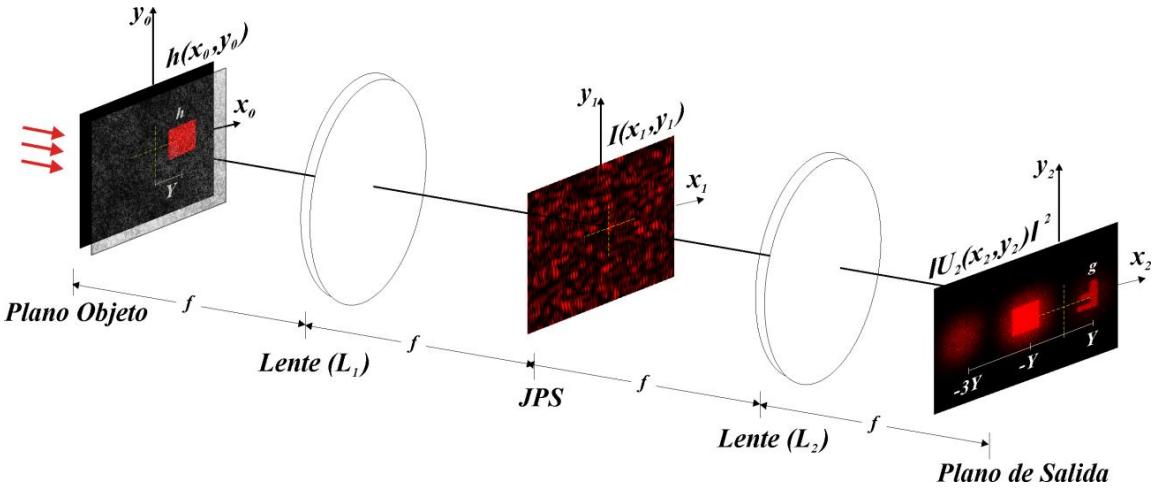


Figura 2.11 Esquema de desencriptación basado en una arquitectura 4f. Etapa de Lectura.

En la **Figura 2.11** se muestra un esquema de la etapa de desencriptación. En este proceso se requiere iluminar el JPS registrado con un campo complejo que sea proporcional a la trasformada de Fourier de la máscara llave usada en el proceso de registro. Es decir, que la onda que ilumina al registro de los datos encriptados (JPS) debe ser proporcional a:

$$\frac{1}{i\lambda f} H\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right) e^{-i2\pi Y \frac{x_1}{\lambda f}} \tag{2.35}$$

El campo que emerge del plano espectral después de ser iluminado quedaría representado por la ecuación

$$S(x_1, y_1) = I(x_1, y_1) \frac{1}{i\lambda f} H\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right) e^{-i\pi Y \frac{x_1}{\lambda f}} =$$

$$= \frac{1}{i(\lambda f)^3} \left[\left| G\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right) \otimes R\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right) \right|^2 + \left| H\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right) \right|^2 \right] H\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right) e^{-i\pi Y \frac{x_1}{\lambda f}} +$$

$$+\frac{1}{i(\lambda f)^3}\left[G\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)\otimes R\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)\right]H^*\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)e^{i2\pi(2Y)\frac{x_1}{\lambda f}}H\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)e^{-i2\pi Y\frac{x_1}{\lambda f}}+$$

$$+\frac{1}{i(\lambda f)^3}\left[G^*\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)\otimes R^*\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)\right]H\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)e^{-i2\pi(2Y)\frac{x_1}{\lambda f}}H\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)e^{-i2\pi Y\frac{x_1}{\lambda f}} \quad (2.36)$$

Teniendo en cuenta la ecuación (2.34), vemos que el tercer término contiene dos factores que son el complejo conjugado de la ecuación (2.35). Como ya hemos mencionado $H(x_1,y_1)$ es una función de sólo fase, entonces el producto de estas dos distribuciones resulta:

$$H\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)e^{-i2\pi Y\frac{x_1}{\lambda f}}H^*\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)e^{i2\pi Y\frac{x_1}{\lambda f}}=\left|H\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)\right|^2=1 \quad (2.37)$$

En el tercer término de la ecuación (2.36) nos queda además del factor constante, la convolución $G\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)\otimes R\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)$ multiplicado por $e^{i2\pi Y\frac{x_1}{\lambda f}}$. Es casi intuitivo ver que para recuperar los datos encriptados se debe hacer una trasformada de Fourier para que este término sea el producto entre $g(x_2,y_2)r(x_2,y_2)$ siendo el plano (x_2,y_2) equivalente a (x_0,y_0). Mediante la lente L_2 realizamos la trasformada óptica del campo de la ecuación (2.36) como se puede ver en la **Figura 2.11**. El campo en el plano de salida es proporcional a:

$$\begin{aligned}\Im\{S(x_1,y_1)\}=\ U_2(x_2,y_2)=&\frac{e^{i\pi}}{(\lambda f)^2}[g(-x_2,-y_2)r(-x_2,-y_2)]\\&\otimes[g^*(x_2,y_2)r^*(x_2,y_2)]\otimes h(-x_2,-y_2)\otimes\delta(x_2+Y,y_2)\\&+\frac{e^{i\pi}}{(\lambda f)^2}h(-x_2,-y_2)\otimes\delta(x_2+Y,y_2)\\&+\frac{e^{i\pi}}{(\lambda f)^2}g(-x_2,-y_2)r(-x_2,-y_2)\otimes\delta(x_2-Y,y_2)\\&+\frac{e^{i\pi}}{(\lambda f)^2}[g^*(x_2,y_2)r^*(x_2,y_2)]\otimes h(-x_2,-y_2)\\&\otimes h(-x_2,-y_2)\otimes\delta(x_2-3Y,y_2)\end{aligned} \quad (2.38)$$

El primer término corresponde a la autocorrelación de la ventana que contiene la imagen de entrada convolucionada con la llave. El segundo término es la llave. Ambos términos están centrados en la misma posición $(-Y, 0)$. El cuarto es un término de ruido ubicado en la posición $(-3Y, 0)$.

Finalmente, el tercer término corresponde a la información desencriptada $g(x_2, y_2)$ adosada a la máscara de fase $r(x_2, y_2)$ centrada en la posición $(Y, 0)$ si observamos en el plano de salida en esta posición con un detector de intensidad de manera que la máscara de fase $r(x_2, y_2)$ no se pueda ver, se recupera la información desencriptada $|g(x_2, y_2)|^2$.

II.5 Propiedades del Speckle

II.5.1 Origen del speckle

La luz coherente transmitida por un difusor aleatorio, ó reflejada por una superficie rugosa, produce un patrón de interferencia granular, conocida como patrón speckle. Es muy común observar este fenómeno cuando se utiliza como fuente de iluminación un láser, debido su alta coherencia.

En los años 60, cuando se dispuso por primera vez de láseres, se observo que la luz reflejada desde una superficie como un papel o el muro del laboratorio, tenía el aspecto de un patrón granular con un alto contraste al ser visto por un observador. Además, la medida de la intensidad de la luz reflejada por la superficie mostró que estas fluctuaciones de intensidad existían en el espacio, a pesar de que la iluminación era relativamente uniforme. Este tipo de granularidad se dio a conocer como “speckle.”

Posteriormente, se descubrió que estas fluctuaciones se debían a la rugosidad aleatoria de las superficies desde la cual la luz era reflejada [2.7]. En efecto la mayoría de los objetos en el mundo real son rugosos en la escala de una longitud de onda óptica, es por esa razón que este fenómeno usualmente aparece en óptica, de hecho es la regla más que la excepción.

El patrón de speckle se observa también cuando la luz láser es transmitida a través de difusores, por la misma razón básica: el camino óptico de diferentes rayos de luz pasando

a través de este tipo de objetos varia significativamente en la escala de la longitud de onda.

En principio este era un efecto no deseado y lo que se buscaba era la forma de suprimirlo, por eso las primeras investigaciones estaban encaminadas a encontrar técnicas orientadas a la reducción de speckle en sistemas ópticos y holográficos. Una vez que se fue conociendo la naturaleza de su origen y se busco una representación matemática de algunas de sus propiedades, comenzaron a desarrollarse muchas aplicaciones aprovechando la información que contenían estos patrones de luz y su sensibilidad a pequeños desplazamientos, rotaciones y deformaciones. Para mencionar solo algunas de ellas, la medición de rugosidad en superficies, interferometría speckle estelar, interferometría holográfica y DSPI.

II.5.2 Formación de un patrón de Speckle

En esta sección se presentan dos configuraciones ópticas bajo las cuales se genera un patrón de speckle. La geometría de propagación en el espacio libre llamado speckle objetivo y la que usa un sistema de formación de imagen llamado speckle subjetivo.

II.5.2.1 Speckle Objetivo

Primero consideramos el caso cuando una fuente de iluminación coherente ilumina una superficie rugosa plana, y la luz dispersada es observada a alguna distancia Z desde la superficie como se ilustra en la **Figura 2.12**. Este resultado aplica igual para el caso de transmisión a través de un difusor. En ambos casos se asume que las perturbaciones de fase sufridas por la onda incidente son al menos varias veces 2π radianes la longitud de onda.

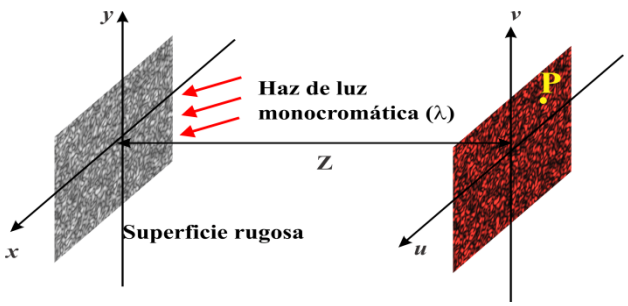


Figura 2.12 Formación de un patrón de speckle objetivo por reflexión.

Se asume que la longitud de onda de la radiación incidente es λ, se asume que la superficie dispersora es estacionaria en el tiempo y la forma de los centros dispersores que componen el difusor ó la superficie rugosa por el momento no se especifica. Asumiendo aproximación paraxial (solo pequeños ángulos dispersores está envueltos). Bajo estas condiciones, la propagación de la luz desde la superficie hasta un punto de observación P a la distancia Z, es el resultado de la superposición coherente de una gran cantidad de contribuciones independientes, asociadas con los centros dispersores de la región iluminada por el haz láser. Ocurre cuando el ángulo de dispersión hace que la diferencia de caminos relativos entre la luz dispersada desde el centro del área iluminada al borde difiera en una longitud de onda. En ese caso, la intensidad no está correlacionada.

El estudio de la estadística de segundo orden es importante para determinar el tamaño transversal del patrón de speckle que coincidirá con los límites de detección del método. Así para un speckle objetivo el diámetro de speckle medio para el modelo supuesto es función únicamente de la distancia a la superficie Z, del área de la zona iluminada L y la longitud de onda λ.

II.5.2.2 Speckle subjetivo

La **Figura 2.13** ilustra una configuración para obtener un patrón se speckle subjetivo. También se puede obtener un patrón de speckle, cuando se forma la imagen del difusor (lámina transparente rugosa) con una lente ó con algún otro sistema óptico como el ojo humano ó una cámara fotográfica.

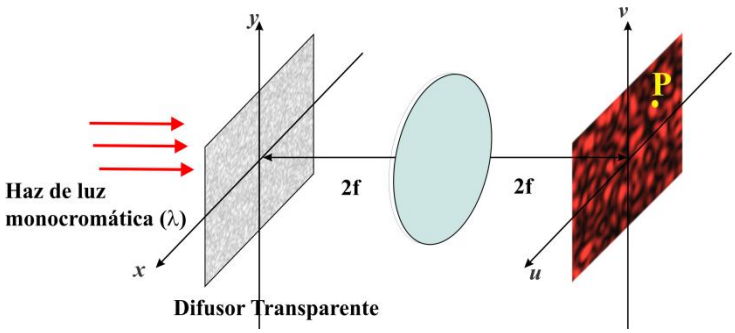


Figura 2.13 Formación de un patrón de speckle objetivo por transmisión.

El patrón de speckle generado así se denomina speckle subjetivo o speckle imagen. Para un speckle subjetivo el diámetro de speckle medio es función únicamente de la distancia de la lente al plano de observación, el diámetro de la pupila D y la longitud de onda λ.

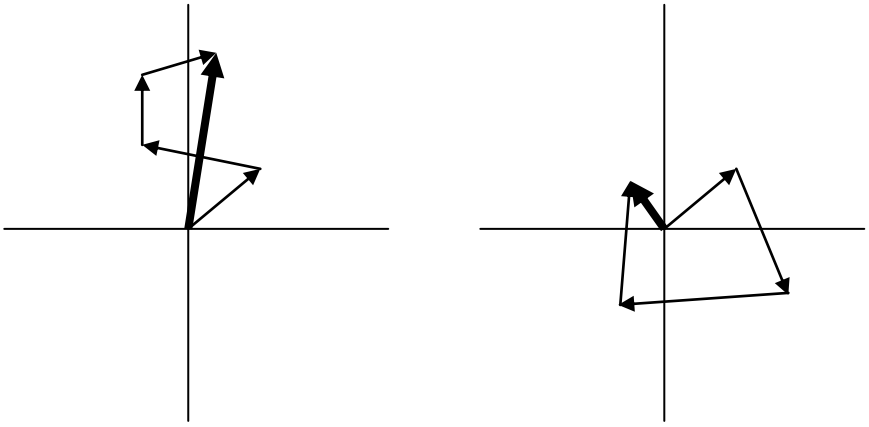
II.5.3 Speckle como un fenómeno de camino aleatorio

Cuando una superficie está iluminada por una onda de luz, según la teoría de la difracción, cada punto de una superficie iluminada actúa como una fuente de ondas secundarias esféricas. El campo resultante en un punto se compone de la superposición las ondas dispersada por cada punto de la superficie iluminada. Si la superficie tiene una rugosidad de un orden suficiente para crear diferencias camino óptico de más de una longitud de onda, dando lugar a cambios de fase superior a 2π, la amplitud, y por lo tanto la intensidad la distribución luz resultante tiene un comportamiento aleatorio.

Las propiedades del speckle no están determinadas por las características macroscópicas del objeto difusor, sino que están determinadas por su micro estructura [2.3]. Debido a que no se conocen las características microscópicas de la superficie desde la cual, la luz coherente está siendo dispersada, se hace necesario discutir las propiedades de los patrones de speckle en términos estadísticos. Esto implica que si ponemos un detector en un punto (x, y, z) en el plano de observación, la medida de la irradiancia no es predecible de manera exacta, pero podemos describir sus propiedades estadísticas sobre un ensamble de superficies rugosas. Por esta razón modelamos nuestro objeto como un ensamble de difusores, que tienen una posible distribución de amplitud compleja, y una probabilidad de ocurrencia [2.4].

El speckle aparece en una señal cuando esta señal se compone de una multitud de componentes aditivas de fases independientes (es decir, que dichas componentes tengan amplitud y fase). Las componentes pueden tener ambas longitudes (amplitudes) y direcciones (fases) aleatorias. Cuando estas componentes se suman, constituyen lo que se conoce como un camino aleatorio. La resultante de la suma puede

ser grande o pequeña, dependiendo las fases relativas de las componentes de la suma, y en particular si en la suma domina la interferencia constructiva ó destructiva. La longitud al cuadrado de la resultante es lo que usualmente llamamos "intensidad" de la onda observada.



(a) (b)

Figura 2.14.Muestra de caminos aleatorios que al ser sumados generan una resultante grande, donde domina la interferencia (a) constructiva y (b) destructiva.

En los casos ilustrados ambas longitudes y direcciones son aleatorias y múltiples contribuciones dominan la suma. El vector con flecha más gruesa representa el resultado de la suma compleja.

II.5.3.1 Estadística de primer orden.

Para utilizar una representación matemática simplificada para el modelo estadístico del speckle, se hacen las siguientes suposiciones, el campo incidente en el punto (x,y,z) es perfectamente polarizado y perfectamente monocromático. Bajo tales condiciones podemos representar este campo complejo por un valor analítico de la forma:

$$u(x,y,z;t) = A(x,y,z)\cos(i2\pi\nu t) \tag{2.39}$$

donde ν es la frecuencia óptica y $A(x,y,z)$es un fasor de amplitud compleja,

$$A(x,y,z) = |A(x,y,z)|e^{i\theta(x,y,z)} \tag{2.40}$$

El observable de este campo es la irradiancia en (x,y,z) la cual se puede representar por:

$$I(x,y,z) = \lim_{T\to\infty} \frac{1}{T} \int_{-T/2}^{T/2} |u(x,y,z;t)|^2 dt \qquad (2.41)$$

Quizá la más importante propiedad estadística de un patrón de speckle es la probabilidad de distribución de la irradiancia I. ¿Qué probabilidad hay de observar un pico brillante ó uno oscuro en la irradiancia hacia un dado punto?. Esta pregunta se puede resolver usando la similitud que tiene este problema con el problema de los caminos aleatorios que ha sido estudiado por cerca de 100 años [6]

La amplitud compleja del campo hacia (x,y,z) puede ser considerada como el resultado de la suma de contribuciones desde muchas pequeñas aéreas de dispersión desde la superficie rugosa.

Este fasor de amplitud del campo puede ser representado por,

$$A(x,y,z) = Ae^{i\theta} = \frac{1}{\sqrt{N}} \sum_{k=1}^{N} |a_k| \, e^{i\phi_k} \qquad (2.42)$$

Donde $|a_k|$ y ϕ_k representan la amplitud y la fase de la contribución desde la k-esima área de dispersión y N es el número total de tales contribuciones. La siguiente **Figura** ilustra este fasor de adición.

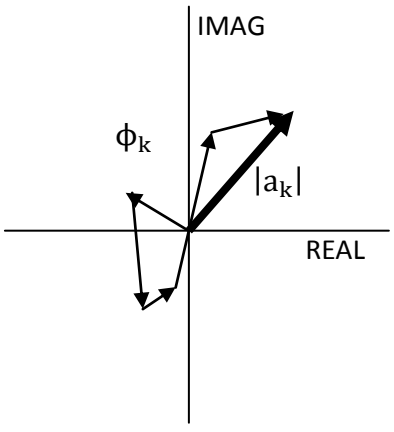


Figura 2.15.Muestra de caminos aleatorios que al ser sumados generan una resultante grande, donde domina la interferencia (a) constructiva y (b) destructiva.

Ahora se hacen algunas suposiciones sobre las contribuciones desde las aéreas primarias de dispersión, es decir las componentes de la sumatoria de la expresión (2.42).

Estas suposiciones son más fáciles de entender si se considera la parte real e imaginaria del fasor resultante,

$$\Re = \mathrm{Re}\{A\} = \frac{1}{\sqrt{\mathrm{N}}}\sum_{\mathrm{k}=1}^{\mathrm{N}} |\mathrm{a_k}| \cos \phi_\mathrm{k}$$

$$\Im = \mathrm{Im}\{A\} = \frac{1}{\sqrt{\mathrm{N}}}\sum_{\mathrm{k}=1}^{\mathrm{N}} |\mathrm{a_k}| \,\mathrm{sen}\, \phi_\mathrm{k} \qquad (2.43)$$

Donde los símbolos $\mathrm{Re}\{\ \}$ y $\mathrm{Im}\{\ \}$ representan la parte real e imaginaria de la cantidad compleja ente los paréntesis. Las suposiciones son:

- Las amplitudes y fases $|\mathrm{a_k}|$ y ϕ_k del *k*-ésimo fasor elemental son estadísticamente independientes de las amplitudes y fases $|\mathrm{a_m}|$ y ϕ_m del *m*-ésimo fasor elemental siempre que $m \neq k$. Esto es, el conocimiento de los valores de amplitud y/o fase de un componente del fasor no nos permite conocer la amplitud y/o fase de otra componente del fasor. (En nuestro caso esto se debe a que suponemos que la superficie del objeto desde la cual la luz está siendo dispersada tiene una rugosidad aleatoria, por lo tanto las aéreas de dispersión primaria no están correlacionadas)
- Para cualquier *k* , $\mathrm{a_k}$ y ϕ_k son estadísticamente independientes. Esto quiere decir que el conocimiento del componente de fase del fasor, no permite conocer la amplitud del mismo fasor y viceversa.
- Las contribuciones de fase ϕ_k son igualmente probables en el intervalo $[-\pi, \pi]$, es decir la fase está uniformemente distribuida en dicho intervalo. Esto se da porque la superficie es rugosa, es decir que sus irregularidades son muy grandes en comparación con una longitud de onda, resultando así que.

Bajo estas suposiciones, la similaridad de nuestro problema con el clásico de las trayectorias aleatorias es completa [2.4]. Siempre que se cumpla que el número N de las contribuciones elementales es grande, nos encontramos con: las partes real e imaginaria del campo complejo en (x, y, z) tienen media cero, sus varianzas son iguales y son independientes (es decir que estas variables no se hallan correlacionadas). Estas conclusiones se pueden representar matemáticamente por las siguientes relaciones,

$$\langle \Re \rangle = \langle \Im \rangle = 0 \tag{2.44}$$

$$\sigma^2 = \langle [\Re]^2 \rangle = \langle [\Im]^2 \rangle = \frac{1}{N} \sum_{k=1}^{N} \frac{\langle |a_k|^2 \rangle}{2} \tag{2.45}$$

$$\langle \Re \, \Im \rangle = 0 \tag{2.46}$$

Donde $\langle \dots \rangle$ representa el promedio sobre las todas contribuciones desde las áreas de dispersión. Esta operación puede interpretarse como el promedio espacial sobre un área suficientemente extensa del difusor. Bajo estas condiciones la función de densidad de probabilidad asociada a la irradiancia del campo complejo I y a la fase θ, obedece a una estadística exponencial negativa, esto es, la función de densidad de probabilidad es de la forma:

$$p_I(I) = \begin{cases} \dfrac{I}{\langle I \rangle} - exp\left\{\dfrac{I}{\langle I \rangle}\right\}, & I > 0 \\ 0, & \text{en otro caso} \end{cases} \tag{2.47}$$

$$p_\theta(\theta) = \begin{cases} \dfrac{1}{2\pi}, & -\pi \leq \theta > \pi \\ 0, & \text{en otro caso} \end{cases} \tag{2.48}$$

donde $\langle \boldsymbol{I} \rangle$ es el valor promedio de la irradiancia.

La función de densidad de probabilidad para irradiancia dada por ecuación (9) se ajusta a una exponencial negativa que es representada en la siguiente figura:

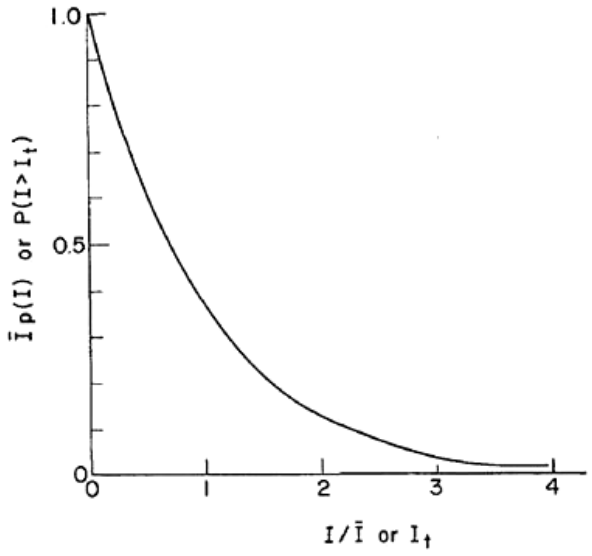


Figura 2.16.Funcion de densidad de probabilidad de un patrón de speckle

Un patrón de speckle con esta distribución de intensidad es usualmente llamado como un *patrón de Speckle bien desarrollado*. La varianza y la desviación estándar para la densidad de probabilidad de la irradiancia está dada por:

$$\sigma_I^2 = \langle I^2 \rangle - \langle I \rangle^2 = \langle I \rangle^2 \tag{2.49}$$

$$\sigma_I = \langle I \rangle \tag{2.50}$$

Esta es una de las más importantes características de la distribución exponencial negativa, que su desviación estándar es precisamente igual al promedio. Entonces, si definimos el contraste un patrón de speckle polarizado como:

$$C = \frac{\sigma_I}{\langle I \rangle} \tag{2.51}$$

Se puede fácilmente notar de reemplazar (2.50) en (2.51), que el contraste para un patrón de Speckle bien desarrollado es siempre igual a la unidad.

En la siguiente sección se detalla cómo se forma en la práctica un patrón de speckle

II.5.3.2 Estadística de segundo orden.

Anteriormente se han estudiado las propiedades del speckle en un único punto (estadística de primer orden). Esta estadística es suficiente para describir dicho fenómeno en lo que se refiere a su generación y fluctuaciones de brillo, pero es insuficiente para describir otras propiedades del speckle como, por ejemplo, su estructura espacial o el diámetro del speckle. Por esta razón necesitamos estudiar la estadística de segundo orden del speckle. Vamos ahora a calcular la función de autocorrelación de la intensidad de un patrón de speckle objetivo.

Supongamos que iluminamos una superficie rugosa con un haz de luz monocromática, y la luz dispersada desde la misma es observada a una distancia, sin intervención de elementos ópticos según se muestra en la **Figura 2.12.** Los campos difractados por la superficie rugosa se estudian en un plano infinitamente próximo (adyacente) a la superficie por la función $\boldsymbol{\alpha(x_0, y_0)}$ de valor complejo. El campo complejo $\boldsymbol{A(x, y)}$ observado en un plano paralelo al plano $(\boldsymbol{x_0}, \boldsymbol{y_0})$ y a una distancia Z de él, representa el campo de speckle. Queremos calcular la función de autocorrelación $\boldsymbol{R_I}$ de la

distribución de intensidad $\boldsymbol{I(x,y) = |A(x,y)|^2}$ en el plano $(\boldsymbol{x_0, y_0})$ para dos puntos del mismo patrón de speckle,

$$R_I(x_1, y_1, x_2, y_2) = \langle I(x_1, y_1) I(x_2, y_2) \rangle \tag{2.52}$$

El ancho de esta función de autocorrelación proporciona una medida razonable del diámetro medio de la dimensión transversal del speckle. Ahora, se calcula la función de autocorrelación de la intensidad usando el hecho de que la superficie, desde la cual la luz fue dispersada, es rugosa comparada con la longitud de onda y el campo $\boldsymbol{A(x,y)}$ es una variable compleja aleatoria circular gaussiana en cada punto del plano $(\boldsymbol{x,y})$. Para estos campos, la función de autocorrelación de la intensidad $\boldsymbol{R_I}$ puede expresarse en términos de la función de autocorrelación de los campos $\boldsymbol{J_A}$, la cual se representa por,

$$J_A(x_1, y_1, x_2, y_2) = \langle A(x_1, y_1) A^*(x_2, y_2) \rangle \tag{2.53}$$

la relación entre las ecuaciones (2.52) y (2.53) es,

$$R_I(x_1, y_1, x_2, y_2) = \langle I(x_1, y_1) \rangle \langle I(x_2, y_2) \rangle \, |J_A(x_1, y_1, x_2, y_2)|^2 \tag{2.54}$$

donde $J_A(x,y) = \langle I(x,y) \rangle$. El problema del cálculo de R_I se reduce por lo tanto al cálculo de J_A. Es importante recalcar que esta aproximación es válida para superficies rugosas a escala de longitud de onda λ. Para superficies lisas no se puede aplicar la distribución circular Gaussiana para $A(x,y)$.

Para resolver el problema se puede emplear la teoría de la difracción escalar de una onda monocromática. Aplicando la aproximación de Fresnel [2.4], la amplitud de la onda dispersada es,

$$A(x,y) = \frac{1}{\lambda \mathrm{Z}} e^{-i\frac{\pi}{\lambda z}(x,y)} \iint_{-\infty}^{\infty} \alpha(x_0, y_0) e^{-i\frac{\pi}{\lambda z}(x_0^2, y_0^2)} \, e^{i\frac{\pi}{\lambda z}(x x_0, y y_0)} dx_0 dy_0 \tag{2.55}$$

Particularizando este resultado para $A(x_1, y_1)$ y $A(x_2, y_2)$, y reemplazando en la ecuación (2.53) podemos encontrar la relación entre la función de autocorrelación de la amplitud en la pantalla de observación J_A y la función de autocorrelación de la amplitud en la superficie rugosa J_α,

$$J_A(x_1, y_1, x_2, y_2) = \frac{1}{\lambda^2 z^2} e^{-i\frac{\pi}{\lambda z}(x_1^2 - x_2^2, + y_1^2 - y_2^2)} \iiint_{-\infty}^{\infty} J_\alpha(x_{01}, y_{01}; x_{02}, y_{02})$$

$$e^{-i\frac{\pi}{\lambda z}(x_{01}^2 - x_{02}^2 + y_{01}^2 - y_{02}^2)} e^{-i\frac{\pi}{\lambda z}(x_1 x_{01} - x_2 x_{02} + y_1 y_{01} - y_2 y_{02})} dx_{01} dx_{02} dy_{01} dy_{02} \quad (2.56)$$

Cómo sólo nos interesa el módulo de J_A se puede eliminar el factor exponencial que aparece fuera de la integral. Por otra parte, si se supone que la micro-estructura de la superficie es suficientemente fina, se puede hacer la aproximación:

$$J_\alpha(x_{01}, y_{01}; x_{02}, y_{02}) = \langle \alpha(x_{01}, y_{01}) \alpha^*(x_{02}, y_{02}) \rangle$$

$$\cong k P(x_{01}, y_{01}) P^*(x_{02}, y_{02}) \delta(x_{01} - x_{02}, y_{01} - y_{02}) \quad (2.57)$$

donde k es una constante de proporcionalidad, la función $P(x_0, y_0)$ es la amplitud del campo incidente sobre los centros dispersores y $\delta(x_0, y_0)$ es la distribución bidimensional delta de Dirac. El resultado de todas estas simplificaciones es,

$$J_A(x_1, y_1, x_2, y_2) = \frac{k}{\lambda^2 z^2} \iint_{-\infty}^{\infty} |P(x_{01}, y_{01})|^2 e^{-i\frac{\pi}{\lambda z} x_{01}(x_1 - x_2) + y_{01}(y_1 - y_2)} \, dx_{01} dy_{01} \quad (2.58)$$

En esta expresión J_A depende sólo de la diferencia de coordenadas en el plano (x_0, y_0) y su cálculo se reduce a una transformada de Fourier de la distribución de la intensidad $|P(x_{01}, y_{01})|^2$. Es conveniente dejar el resultado de una forma más compacta. Concretamente, la versión normalizada de la intensidad, conocida como el factor de coherencia complejo, se define por,

$$\mu_A(\Delta x, \Delta y) = \frac{J_A(x_1, y_1; x_2, y_2)}{\sqrt{J_A(x_1, y_1; x_1, y_1) J_A(x_2, y_2; x_2, y_2)}} \quad (2.59)$$

Finalmente, la función de autocorrelación de la intensidad R_I toma la forma,

$$R_I(\Delta x, \Delta y) = \langle I \rangle^2 [1 + |\mu_A(\Delta x, \Delta y)|^2] =$$

$$= \langle I \rangle^2 \left[1 + \left| \frac{\iint_{-\infty}^{\infty} |P(x_0, y_0)|^2 e^{i\frac{2\pi}{\lambda z}(x_0 \Delta x + y_0 \Delta y)} \, dx_0 dy_0}{\iint_{-\infty}^{\infty} |P(x_0, y_0)|^2 \, dx_0 dy_0} \right|^2 \right] \quad (2.60)$$

La función de autocorrelación R_I depende de $\mu_A(\Delta x, \Delta y)$, es decir, de la forma geométrica de la superficie dispersora. Por tanto, es proporcional al cuadrado del módulo de la transformada de Fourier de la intensidad en superficie del objeto.

Supongamos el caso especial de una superficie difusora uniforme y cuadrada con unas dimensiones de L X L m^2, entonces tenemos una función de distribución de intensidad igual a $P(x_0, y_0) = rect\left(\frac{x_0}{\mathrm{L}}\right) rect\left(\frac{x_0}{\mathrm{L}}\right)$, donde $rect(x) = 1$ para $|x| \leq \frac{1}{2}$ y cero en otro caso para la coordenada x, para la coordenada y sería análogo. La función de autocorrelación de la intensidad en este caso es igual a

$$R_I(\Delta x, \Delta y) = \langle I \rangle^2 \left[1 + \mathrm{sinc}^2 \frac{L\Delta y}{\lambda \mathrm{Z}} \mathrm{sinc}^2 \frac{L\Delta y}{\lambda \mathrm{Z}}\right] \tag{2.60}$$

Como diámetro medio del speckle, puede razonablemente tomarse el valor de Δx donde $\mathrm{sinc}^2 \frac{L\Delta x}{\lambda \mathrm{Z}}$ se hace por primera vez cero. Llamando a esta distancia $\langle S_x \rangle$, tenemos que es igual a

$$\langle S_x \rangle = \frac{\lambda \mathrm{Z}}{L} \tag{2.61}$$

donde el diámetro medio de speckle es función de la distancia a la superficie Z, de la magnitud de la zona iluminada L y de la longitud de onda λ de la onda de la radiación incidente [2.4]. Así en fuentes no monocromáticas se tiene un patrón de speckle para cada longitud de onda λ_j con un diámetro medio diferente. Para el caso en el que interviene una lente para formar el patrón de speckle (speckle subjetivo), también es de utilidad determinar el diámetro medio del speckle, ya que la magnitud de dicho diámetro está relacionada con el desplazamiento mínimo que se puede detectar en un experimento de translación, rotación ó deformación. Para determinar este diámetro, repetimos, el procedimiento empleado en el apartado anterior, esto es, la determinación de la función de autocorrelación de la intensidad, cuando aparece una lente.

Una región del objeto es iluminada uniformemente, la lente empleada debe cumplir que la unidad de resolución asociada sea mucho menor que la región iluminada, de esta forma el tamaño del speckle incidente sobre la lente es extremadamente pequeño comparado con el la lente.

Una aproximación de la intensidad mutua J_α en el plano de la lente (x_0, y_0)es la ecuación (2.57) siendo $P(x_0, y_0)$ la función de la pupila de la lente. Se tratará el plano de la pupila

de la lente como una supuesta superficie rugosa unifórmente brillante. Así para calcular la propagación en el espacio desde el plano de la pupila de la lente (x_0, y_0) hasta el plano de la imagen (x, y) separado una distancia Z, se puede usar el desarrollo utilizado para el speckle objetivo hasta llegar a la ecuación (2.60) para la expresión de la función de autocorrelación de la intensidad R_I en el plano de la imagen (x, y) con la única diferencia en la interpretación de $P(x_0, y_0)$. De acuerdo a esta expresión la función de autocorrelación de la intensidad del patrón de speckle consiste en un término constante más el cuadrado de la transformada de Fourier de la transmitancia de intensidad $|P(x_0, y_0)|^2$ de la pupila de la lente. La función de autocorrelación es independiente de aberraciones que puedan estar asociados al sistema de imagen, afectando estas únicamente a la fase de $P(x_0, y_0)$.

Para el caso particular de una lente de pupila de diámetro D, la función de autocorrelación en el plano de la imagen del patrón de speckle es

$$R_I(r) = \langle I \rangle^2 \left[1 + \left| 2 \frac{\mathcal{J}_1\left(\frac{\pi D_r}{\lambda \mathrm{Z}}\right)}{\frac{\pi D_r}{\lambda \mathrm{Z}}} \right|^2 \right] \tag{2.62}$$

donde $r = \sqrt{(\Delta x)^2 + (\Delta y)^2}$, Z es la distancia del plano de la pupila al plano de la imagen y $\mathcal{J}_1$ es la función de Bessel de primera especie.

Para el cálculo del diámetro medio del speckle cuando se interpone entre la superficie difusora y el plano de observación una lente, se puede tomar el valor más pequeño de r para el cual $\mathcal{J}_1$ tiene su primer valor nulo. Llamando a el diámetro medio del speckle $\langle S_r \rangle$, tenemos que

$$\langle S_r \rangle = 1{,}2 \frac{\lambda \mathrm{Z}}{D} \tag{2.63}$$

donde λ es la longitud de onda del láser, Z la distancia de la lente al plano de observación y D el diámetro de la lente. Teniendo en cuenta que se define el número del sistema óptico F como $F = \frac{f}{D}$, donde f es la distancia focal, y que en óptica geométrica la distancia Z del sistema óptico al objeto es igual a, $\mathrm{Z} = (1 + \mathrm{M})f$, donde M es el aumento lateral, tenemos otra expresión análoga del diámetro medio del speckle subjetivo

$$\langle S_r \rangle = 1{,}2\lambda(1+M)F \tag{2.64}$$

Es importante apreciar en la ecuación (2.63) que el diámetro de speckle para estos sistemas es función de la lente y no de la superficie iluminada para la teoría desarrollada.

II.6 Referencias

[2.1] J. Goodman, "Introduction to Fourier Optics", McGraw-Hill, New York, (1996).

[2.2] A. B. Vander Lugt, "Optical Signal Processing", John Wiley and Sons, New York (1992).

[2.3] C. S. Weaver and J. W. Goodman, "Technique for Optically Convolving Two Functions" Appl. Opt. 5, 1248-1249 (1966)

[2.4] P. Réfrégier, B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding", Opt. Lett. 20, 767-797 (1995).

[2.5] T. Nomura and B. Javidi, "Optical encryption using a joint transform correlator architecture," Opt. Eng. 39, 2031–2035 (2000).

[2.6] F. T. S Yu., S. Jutamulia, Optical Pattern Recognition, Cambridge University Press (1998).

[2.7] A. B. Vander Lugt, "Signal detection by complex spatial filtering" I.E.E.E. tans. Info. Theory, IT-10, 139-145 (1964).

[2.8] J.D. Rigden and E.I. Gordon. "The granularity of scattered optical maser light," Proc. IRE 50, 2367–2368 (1962).

[2.9] J. W. Goodman, "Statistical Optics", Wiley-Interscience, New York, (1985)

[2.10] J. W. Goodman, "Speckle Phenomena in Óptics: Theory and application" Robers and Company, Greenwood Village, CO, (2007).

[2.11] L.I. Goldfisher, "Autocorrelation function and power spectral density of laser-produced speckle patterns" J Opt. Soc. Am. 55, 247-253 (1965).

[2.12] J. C. Dainty**,** "Laser Speckle and Related Phenomena", Topics in Applied Physics Vol. 9 , Springer, Berlin(1975).

CAPÍTULO III

Análisis de la distribución de los datos encriptados. Arquitectura 4f.

III.1 Introducción

El sistema de encriptación de doble máscara de fase aleatoria fue uno de los primeros sistemas ópticos implementados para codificar datos ópticamente. Ya hemos descripto en el capitulo anterior cómo mediante las arquitecturas JTC y 4*f* los datos de una imagen de entrada pueden ser codificados en una distribución de ruido blanco aleatorio estacionario. En el presente y el siguiente capítulo vamos a tratar los aspectos que se presentan y se deben tener en cuenta cuando se quieren implementar estas arquitecturas de encriptación en forma analógica ó digital.

Existen en la actualidad otras arquitecturas además de las clásicas 4*f* y JTC ó nuevas variantes de las mismas para encriptar datos ópticamente, sin embargo muchas de estas aunque se basan en sistemas ópticos, son implementadas digitalmente. Nosotros hemos notado que en los sistemas de encriptación óptica convencionales aún existen muchos aspectos a ser estudiados para poder hacer un uso eficiente de dichas técnicas. Es bien conocido que cuando se quiere implementar alguna propuesta que emplea una técnica de encriptación óptica, en especial cuando se ha sustentado sólo con datos simulados, los resultados suelen ser deficientes, ó incluso resulta imposible de reproducir experimentalmente. Esto se debe, entre otras razones, a un desequilibrio entre las condiciones de las simulaciones y las experimentales. Por un lado los sistemas digitales se diseñan de forma ideal, sin tener en cuenta las condiciones experimentales reales, por

otro lado, no se ha estudiado en profundidad, cómo los parámetros ópticos de los sistemas de encriptación afectan a la calidad de los datos recuperados. Es decir, podemos estar utilizando unas condiciones experimentales muy deficientes y resulta difícil contrastar los resultados obtenidos con los datos idealmente simulados. La imagen desencriptada "ideal" debería contener la información completa del objeto en el plano de entrada. Muchas de las imágenes desencriptadas que se muestran en las publicaciones científicas que usan técnicas digitales para la arquitectura 4*f*, cumplen con esta recuperación ideal de los datos de entrada. Sin embargo, en los casos de simulaciones en que se pretende representar condiciones experimentales (óptica virtual) y en los arreglos experimentales, la pérdida de información es casi inevitable. Desde un principio, las técnicas de encriptación se han empleado para codificar los datos como ruido blanco, difusores de fase, que son un arreglo aleatorio de pequeños centros dispersores que introducen diferencias de fases aleatorias en el campo incidente. El tamaño de los centros dispersores es del orden de los micrómetros. Por esta razón, en los sistemas de encriptación, la información de la imagen de entrada es redistribuida, en un área que contiene información alta frecuencia. Es de esperarse entonces que se tenga especial cuidado en la selección de los parámetros ópticos del dispositivo de encriptación, para evitar ó reducir la pérdida de información en la imagen desencriptada por efecto del ancho de banda del sistema.

En 1996 Lohmann [3.1] muestra que el producto del ancho de banda espacial de las señales y sistemas ópticos puede producir pérdidas o degradaciones de información. En el 2005 Hennelly y Sheridan [3.2] realizan un análisis matemático del producto espacial ancho de banda señal-sistema aplicado a los sistemas de encriptación óptica, mediante el formalismo de la función de distribución de Wigner. Para un sistema 4*f*, Nomura et al. [3.3] muestran que cuando el ancho de banda de la señal de entrada es mayor que la extensión espacial de la máscara encriptadora del sistema, se produce una degradación en la imagen desencriptada. Para mejorar esta limitación, proponen el diseño de una máscara de fase aleatoria optimizada para el plano de entrada mediante algoritmos de recuperación de fase. De esta manera, la mayor cantidad de información proveniente del plano de entrada queda contenida dentro del ancho de banda del sistema.

También para una arquitectura 4*f* Javidi et al. [3.4] estudiaron la degradación de los datos desencriptados, por efecto de: adicionar ruido aditivo a la máscara llave, a los datos encriptados y también por el efecto de binarizar la información encriptada.

En este capítulo se estudia como es la distribución espacial de los datos encriptados debido a las características de las máscaras de fase aleatorias, para arquitectura 4*f*. En particular, nosotros analizamos la distribución de la información del patrón encriptado en términos de los tamaños de los centros dispersores. Este parámetro puede ser controlado en un modulador de fase, controlando la cantidad de pixeles a los cuales se les asigna la misma fase y en los difusores fabricados por ablación, cambiando el tamaño promedio de las partículas abrasivas, de manera que se incremente ó disminuya la rugosidad promedio del difusor, etc.

Estudiaremos la distribución espacial de la información en el plano de encriptación de un procesador 4*f*, con la finalidad de controlar el área en la cual está distribuida la información de los datos encriptados, sin modificar el tamaño promedio del speckle, para que la mayor cantidad de información pueda ser almacenada en el medio de registro disponible. Para entender la importancia de la relación entre el área en la que está distribuida la información encriptada y el área del medio de registro, estudiamos la degradación de la imagen desencriptada debido a esta pérdida de información.

III.2 Ancho de banda espacial para un sistema de encriptación 4f.

La calidad de la señal de salida de un sistema óptico, está conectada con los requerimientos del producto espacio-ancho de banda entre la señal de entrada y el sistema [3.1]. Para un dado grupo de señales ó imágenes, la idea de hacer el estudio sobre los requerimientos del ancho de banda del sistema, para reducir la degradación de la señal de salida al mínimo posible. En ese sentido, en esta Sección plantearemos las desigualdades necesarias para garantizar la trasferencia de información desde el plano de entrada hasta el plano de encriptación.

Para estudiar el rol que desempeñan las máscaras aleatorias del objeto y llave en un sistema de encriptación 4*f*, debemos hacer algunas consideraciones sobre los anchos de banda del sistema, de dichas máscaras y del objeto de entrada.

Según la notación del capítulo II, sean $g(\mathrm{x}_0, \mathrm{y}_0)$, $r(\mathrm{x}_0, \mathrm{y}_0)$ y $\mathrm{H}(\mu, \nu)$ la imagen a ser encriptada, la máscara del objeto, y la máscara llave respectivamente.

En las siguientes ecuaciones se expresan las condiciones que vamos a imponer al sistema. La señal de entrada debe ser finita en el espacio, su ancho de banda frecuencial debe ser limitado y la máscara llave debe ser finita en el espacio:

$$g(x_0, y_0) = 0, \text{ fuera del rango: } |x_0| \leq \frac{\Delta x_{0g}}{2}, |y_0| \leq \frac{\Delta y_{0g}}{2} \tag{3.1}$$

$$r(x_0, y_0) = 0, \text{ fuera del rango: } |x_0| \leq \frac{\Delta x_{0r}}{2}, |y_0| \leq \frac{\Delta y_{0r}}{2} \tag{3.2}$$

$$G(\mu, \nu) = 0, \text{ fuera del rango: } |\mu| \leq \frac{\Delta \mu_G}{2}, |\nu| \leq \frac{\Delta \nu_G}{2} \tag{3.3}$$

$$R(\mu, \nu) = 0, \text{ fuera del rango: } |\mu| \leq \frac{\Delta \mu_R}{2}, |\nu| \leq \frac{\Delta \nu_R}{2} \tag{3.4}$$

$$H(\mu, \nu) = 0, \text{ fuera del rango: } |\mu| \leq \frac{\Delta \mu_H}{2} |\nu| \leq \frac{\Delta \nu_H}{2} \tag{3.5}$$

Donde $\mathrm{G}(\mu, \nu)$ y $\mathrm{R}(\mu, \nu)$ son las transformadas de Fourier de $\mathrm{g}(\mathrm{x}_0, \mathrm{y}_0)$ y $\mathrm{r}(\mathrm{x}_0, \mathrm{y}_0)$, respectivamente, $(\Delta \mathrm{x}_{0\mathrm{g}}, \Delta \mathrm{y}_{0\mathrm{g}})$ y $(\Delta \mathrm{x}_{0\mathrm{r}}, \Delta \mathrm{y}_{0\mathrm{r}})$ representa el ancho de banda espacial de $g(x_0, y_0)$ y $r(x_0, y_0)$, respectivamente, $(\Delta \mu_{\mathrm{G}}, \Delta \nu_{\mathrm{G}})$, $(\Delta \mu_{\mathrm{R}}, \Delta \nu_{\mathrm{R}})$, $(\Delta \mu_{\mathrm{H}}, \Delta \nu_{\mathrm{H}})$ son los anchos de banda de frecuencia espacial de $G(\mu, \nu)$, $\mathrm{R}(\mu, \nu)$ and $\mathrm{H}(\mu, \nu)$, respectivamente.

El ancho de banda espacial del sistema, suponemos que está a su vez determinado por la extensión de la máscara de fase $\mathrm{H}(\mu, \nu)$ en el plano de Fourier.

Bajo estas condiciones, el patrón encriptado contiene toda la información del objeto si se cumple las siguientes condiciones:

$$\Delta \mu_G + \Delta \mu_R \leq \Delta \mu_H \tag{3.6}$$

$$\Delta \nu_G + \Delta \nu_R \leq \Delta \nu_H \tag{3.7}$$

En otras palabras, bajo estas condiciones se tiene un sistema “perfecto” sin pérdida de energía, donde se cumple que tanto en los planos espaciales cuanto en los

frecuenciales, la energía total se conserva, es decir se cumple el teorema de Parseval:

$$\iint_{-\infty}^{\infty}|U_0(x_0,y_0)|^2dx_0dy_0 = \iint_{-\infty}^{\infty}|U_1(\mu,\nu)|^2d\mu d\nu \qquad (3.8)$$

donde $U_0(x_0,y_0) = \mathrm{g(x_0,y_0)r(x_0,y_0)}$, representa el campo en el plano de entrada y $U_1(\mu,\nu) = \left(\frac{1}{i\lambda f}\right)\Im\{U_0(x_0,y_0)\}\mathrm{H}(\mu,\nu)$, representa el campo en el plano frecuencial de la etapa de encriptación.

Antes de dar comienzo al análisis del rol de las máscaras, necesitamos hacer una acotación adicional a la descripción hecha para esta arquitectura en la Sección II.3.1.

III.3 Análisis de la distribución de los datos encriptados. Influencia del área finita del medio de Registro.

En esta Sección se analiza cómo se distribuye la información encriptada en el plano de Fourier de una arquitectura 4*f* en función de las características de la máscara llave. También se estudia la degradación que se presenta en la imagen desencriptada cuando no se puede registrar la información encriptada en su totalidad debido al área finita del medio de almacenamiento. Se consideran dos condiciones, cuando la información está uniformemente distribuida y cuando no.

III.3.1. Esquema 4f con área finita del medio de registro.

Para el estudio pertinente a este capítulo vamos a adicionar una condición, al sistema de encriptación de doble máscara de fase aleatorio, descripto en la Sección II.3.1 del capítulo II. Suponemos que se tiene un medio finito de almacenamiento (ver **Figura 3.4**). Sea la señal de entrada en el plano $(\mathrm{x_0,y_0})$ compuesta por el objeto a ser encriptado, $\mathrm{g(x_0,y_0)}$ multiplicado por la máscara del objeto, $\mathrm{r(x_0,y_0)} = \mathrm{e^{i2\pi p(x_0,y_0)}}$ iluminada por una onda plana de longitud de onda λ y amplitud unitaria. El campo propagado es transformado Fourier por la lente $\mathrm{L_1}$ de distancia focal ***f.*** En el plano (μ,ν) este campo es multiplicado por la máscara llave representada por $\mathrm{H}(\mu,\nu) = \frac{1}{\mathrm{i\lambda f}}\mathrm{e^{i2\pi Q(\mu,\nu)}}$. Las fases aleatorias $\mathrm{p(x_0,y_0)}$ y $\mathrm{Q}(\mu,\nu)$ están uniformemente distribuidas entre 0 y 2π y son estadísticamente independientes. Una segunda lente $\mathrm{L_2}$ transforma Fourier el campo

del plano de frecuencias obteniéndose en su plano focal (x_2, y_2) la información encriptada:

$$U_2(x_2, y_2) = \mathrm{Rect}(\frac{x_2}{D_x}, \frac{y_2}{D_y})\big[[g(x_2, y_2)r(x_2, y_2)] \otimes \Im\{H(\mu, \nu)\}\big] \tag{3.9}$$

Esta ecuación describe el patrón encriptado que es almacenado en un medio de registro de dimensiones D_x y D_y.

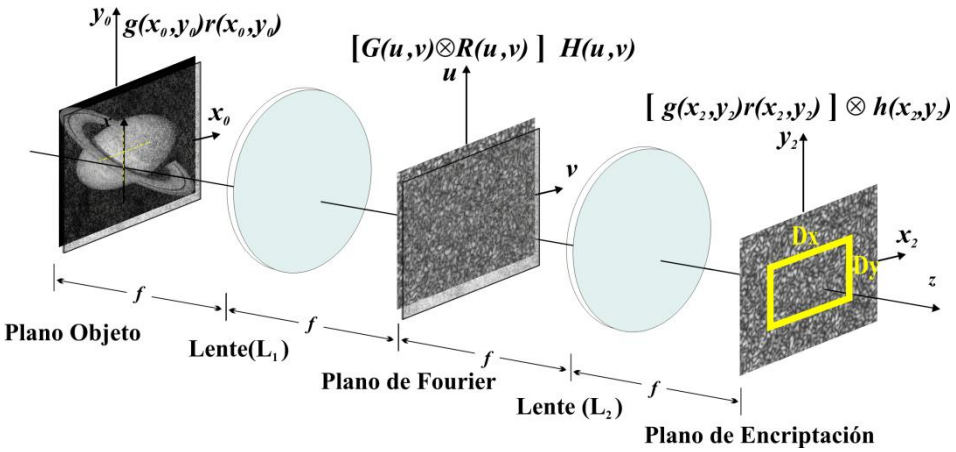


Figura 3.4. Arquitectura de encriptación 4*f* con medio de registro finito.

En la etapa de desencriptación, se requiere el campo conjugado de la información encriptada. Este campo propagado hacia atrás a través del mismo sistema óptico produce una réplica exacta de la imagen de entrada, si la máscara de fase aleatoria introducida en el proceso de encriptación (como máscara llave) es totalmente compensada. Esta condición es cumplida si la máscara llave, su posición y todos los parámetros del sistema óptico son iguales que en la etapa de encriptación. Por otra parte, la réplica del objeto se logra con un medio de almacenamiento sin limitaciones físicas.

III.3.2 Difusores utilizados en los sistemas de encriptación.

En los sistemas clásicos de encriptación, la máscara de fase aleatoria y la máscara llave son difusores. Estos difusores pueden ser considerados como un arreglo de pequeños centros dispersores con distribuciones aleatorias de fase, posición y forma. Idealmente un difusor sería un arreglo de fuentes puntuales (pequeñas dimensiones) con fases iniciales estadísticamente independientes una de la otra (aleatoria). En la práctica se

usan como difusores de fase, transparencias que tienen micro-topografía con perfil aleatorio. La rugosidad debe ser de una dimensión dada, para que en el orden de las longitudes de onda del visible introduzca diferencias de fase aleatorias en el frente de onda incidente, por efecto de la variación del espesor en cada punto. También es común el uso de los moduladores espaciales de luz (SLM), funcionando en régimen de sólo fase, para introducir variaciones de fase aleatorias en un frente de onda incidente. En este caso, el difusor es generado como un arreglo de MxN pixeles. En cada pixel se controla el valor del índice de refracción del cristal líquido, introduciendo de esta manera los cambios de fase deseado en el frente de onda. Una representación matemática de este tipo de difusores equivale a tener la convolución de una función **rect**, con la dimensión de un pixel, con una muestra de funciones aleatorias, donde cada muestra está dada por una función delta de Dirac, la cual ha sido modulada por algún valor de fase aleatorio, ver **Figura 3.5**.

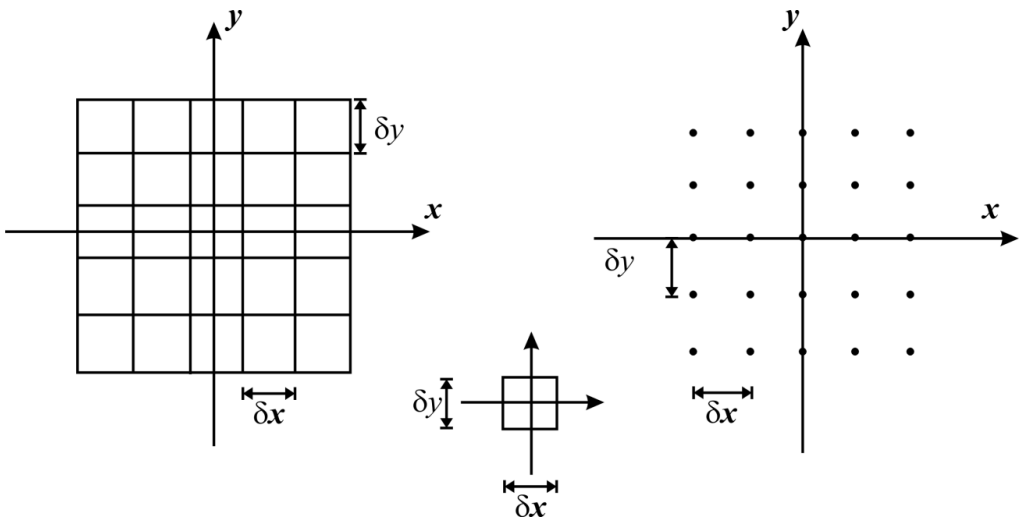


Figura 3.5. Representación del modelo de un difusor digital como la convolución de una función rect (área de un pixel) con un arreglo periódico bidimensional de valores de fases aleatorias.

Esta representación es válida también para los sistemas de encriptación ópticos simulados por computador, ya que se tiene la misma situación de muestreo por el arreglo de pixeles.

En nuestro caso disponemos de un SLM con tamaño de pixel de 32 micrómetros, vamos a tomar este valor como cota superior para nuestro análisis debido a que los SLM

de última generación tienen en promedio un tamaño de pixel inferior. El tamaño transversal promedio de la rugosidad de los vidrios esmerilados utilizados como difusores, en nuestro caso tiene dimensiones inferiores a los 100 micrómetros. De ahora en adelante, nos referiremos a estas dimensiones, ya sea pixel ó rugosidad promedio, como: Tamaño de Grano (**TG**) del difusor. Este orden de magnitud de la dimensión transversal de los centros dispersores produce portadores de información de alta frecuencia espacial. Si parte de la información de alta frecuencia (que corresponde a cualquier lugar del objeto de entrada) es bloqueada por alguna limitación física (pupila, medio de almacenamiento, etc.), este hecho producirá en la imagen desencriptada pérdida aleatoria de información, de manera que la imagen contiene speckle. La dimensión transversal del grano de speckle obedece a algún parámetro específico del sistema óptico y la cantidad de información perdida, se ve reflejada en un aumento del speckle en la imagen.

Teniendo en cuenta que los sistemas ópticos tienen un ancho de banda finito, es indispensable controlar la relación entre los **TG** de los difusores, las frecuencias espaciales de las imágenes a encriptar y el ancho de banda del sistema, para que las arquitecturas de encriptación sean lo más eficiente posible, es decir, desencriptar las imágenes con la menor pérdida de información.

III.3.3. Efecto de la máscara llave en la distribución espacial de la información en el plano de encriptación.

Recordemos que la señal de salida de cualquier sistema $4f$ exhibe la imagen geométrica de la entrada convolucionada con la respuesta impulsiva del sistema. En la ecuación (3.9) podemos notar que la respuesta impulsiva del sistema de encriptación bajo las condiciones impuestas, corresponde a la transformada de Fourier de la máscara llave $H(\mu, \nu)$.

Para visualizar el efecto que la máscara llave produce sobre la distribución del campo en el plano de encriptación, se presenta en la **Tabla 3.1** las imágenes encriptadas obtenidas mediante simulaciones en condiciones de óptica virtual en términos del

tamaño del objeto de entrada y tamaño de grano de la máscara llave (**TGll**).

En las simulaciones presentadas a continuación se utilizan los siguientes parámetros: el tamaño del área de trabajo es de 4096 x 4096 pixeles, la resolución de pixel en la dimensión x e y son de 5 micrómetros, la longitud de onda es de 632 nanómetros, las distancias focales, en todos los casos son iguales y son de 162 milímetros, la pupila del sistema está determinada por el área de trabajo. Una vez fijada el área de trabajo, la resolución de píxel y la longitud de onda, la distancia focal se calcula de tal manera que el área del plano de Fourier coincida con el área de trabajo.

Para todos los resultados mostrados en la **Tabla 3.1**, el difusor del plano de entrada es mantenido constante. Cada fila corresponde a un objeto de tamaño fijo y diferentes valores de **TGll.**

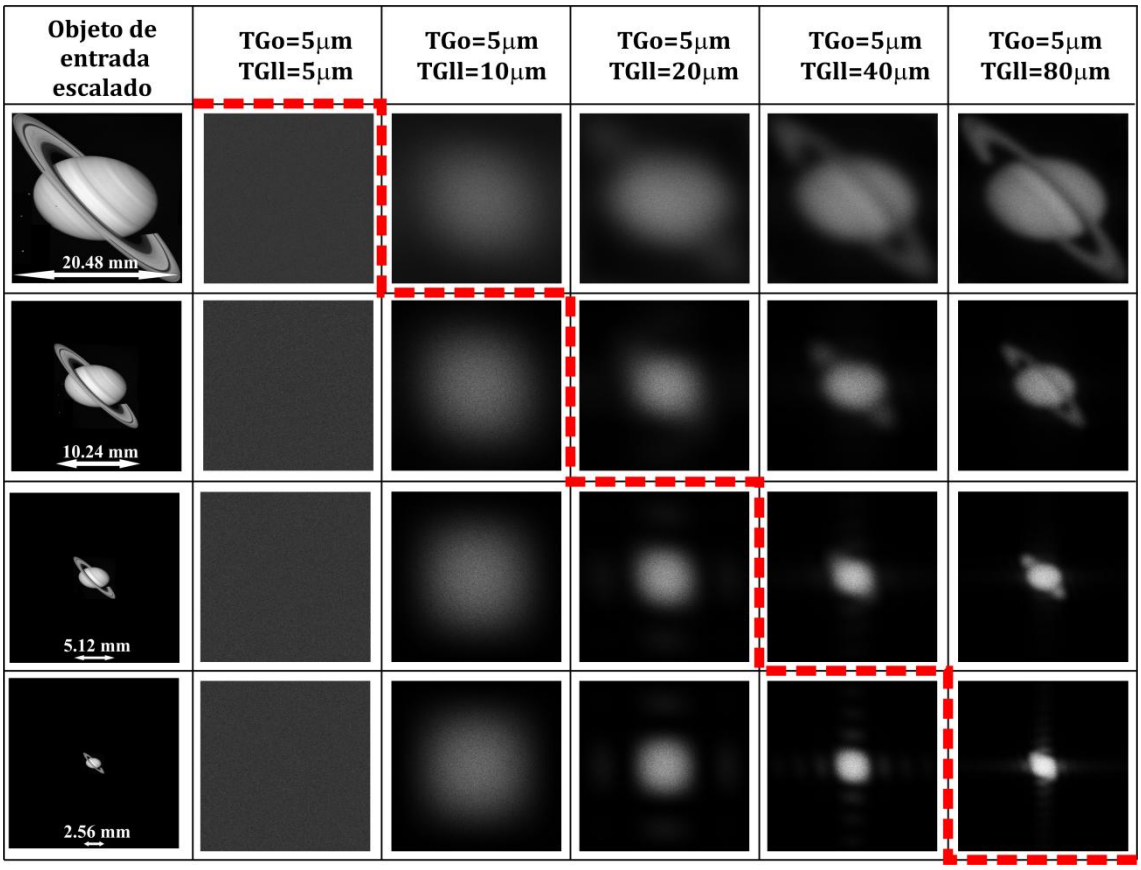


Tabla 3.1. Distribución del patrón encriptado en términos del tamaño del objeto de entrada y del **TGll**.

Como se puede en la **Tabla 3.1**, bajo determinadas condiciones, la distribución del patrón encriptado revela información del objeto de entrada. En la primera fila desde la

segunda columna en adelante, el patrón encriptado comienza a dar algún tipo información sobre el objeto de entrada, y este comportamiento se acentúa cada vez más a medida que el **TGll** incrementa hasta el punto que se reconoce completamente la imagen conjugada del objeto de entrada. Aunque este comportamiento se repite para tamaños menores de objeto de entrada, observándose para valores mayores de **TGll**. De hecho en la última columna se revela información correspondiente a la imagen conjugada del objeto para todos los tamaños entrada percibiéndose con menos detalles a medida que disminuye su dimensión. La **Tabla 3.1** nos proporciona información muy importante. Es evidente que una vez fijado el sistema óptico, para un objeto de un tamaño dado, la arquitectura 4*f* encripta el objeto de entrada correctamente hasta cierto valor umbral de **TGll**.

A partir de este umbral el sistema da como patrón encriptado una distribución de campo que revela información del objeto. En los casos en que el objeto de entrada se visualiza, es evidente que el proceso de encriptación falló, pero hay situaciones intermedias, en las cuales, a simple vista la imagen no se revela, pero se requiere de una análisis más exhaustivo para establecer el TG límite para un objeto de una tamaño dado resulte "bien encriptado".

La respuesta impulsiva del sistema es constante a lo largo de cada columna de la **Tabla 3.1**, es evidente sin embargo, a partir de estos resultados, que la capacidad de encriptación del sistema depende claramente del tamaño del objeto de entrada. En efecto, en el plano de encriptación, la proyección geométrica del objeto debe ser más pequeña que el área correspondiente a la respuesta impulsiva del sistema (que depende del **TGll**) para que la información quede "bien encriptado".

Para profundizar más la compresión del comportamiento del sistema de encriptación, vamos a analizar los casos que están por debajo de la línea a trazos roja de la **Tabla 3.1** los cuales llamamos "bien encriptados" y los casos por arriba de ella que llamamos "mal encriptados".

En esta arquitectura, la máscara llave es iluminada por una distribución de speckle, la cual proviene de la transformada óptica de Fourier del campo de entrada. Y teniendo en cuenta que el tamaño transversal promedio del speckle es:

$$\langle S_x \rangle \propto \frac{\lambda f}{D} \tag{3.10}$$

Como en el caso de las simulaciones presentadas en la **Tabla 3.1,** el sistema óptico se fijó (λ, f) y además es libre de pérdidas (se cumplen las condiciones representadas por las ecuaciones (3.1) - (3.8)) y la pupila efectiva del sistema D es la dimensión del objeto de entrada. Es decir, el tamaño del objeto de entrada determina el valor de $\langle S_x \rangle$. En la **Tabla 3.2** se verifica esta dependencia, mediante las funciones de auto correlación (3^{era} fila) de los patrones de speckle (2da fila) generados a partir de objetos de prueba con diferentes dimensiones (1^{era} fila), adosados a la máscara del objeto.

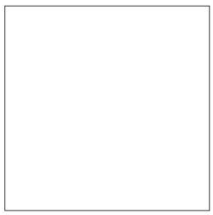
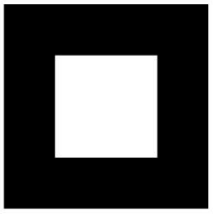
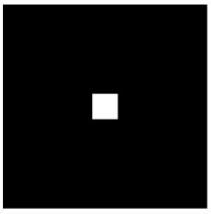
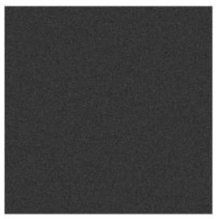
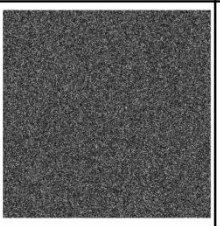
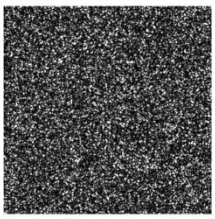
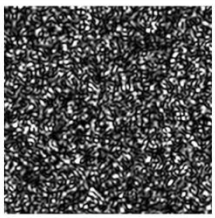
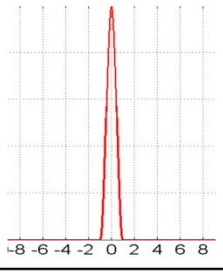
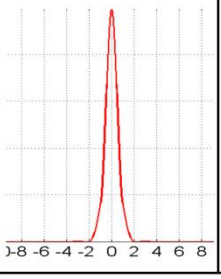
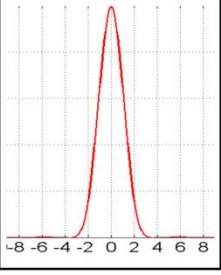
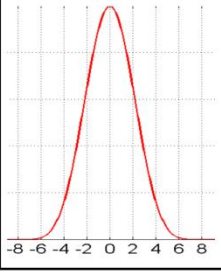
	Tamaño del objeto de entrada			
	20,48 mm	**10,24 mm**	**5,12 mm**	**2,56 mm**
a				
b				
c				

Tabla 3.2. Verificación de la relación entre $\langle S_x \rangle$ en el plano (μ, ν) y la dimensión del objeto de entrada (D). a) Objeto de entrada. b) Patrón de speckle en el plano de Fourier. c) Perfil de **autocorrelación** del patrón de speckle.

En los casos en que $\langle S_x \rangle$ es más pequeño que **TGII**, el proceso de encriptación falla. Estos casos corresponden a las imágenes mostradas sobre la línea roja a trazos de la **Tabla 3.1**. Por el contrario cuando $\langle S_x \rangle$ es más grande, de tal manera que entre más de un centro dispersor de la máscara llave por grano de speckle, la información estará bien

encriptada. Estos casos corresponden a los patrones mostrados por debajo de la línea roja en la **Tabla 3.1**.

El elemento que tiene la dimensión más pequeña (**TGll** ó $\langle S_x \rangle$) en el plano (μ, ν) es quien controla la distribución macroscópica (envolvente) de la información en el plano de encriptación (x_2, y_2). En un sistema de encriptación bajo esta arquitectura se requiere que el elemento de dimensión más pequeña sea el **TGll**. En esta situación la información en el plano (x_2, y_2) estará "bien encriptada", y el área en la cual se distribuye se corresponde con la transformada de Fourier del centro dispersor característico de la máscara llave.

Para un tamaño de objeto fijo a ser encriptado, dada la máscara aleatoria del plano de entrada a la cual se le adosa esta imagen, primero se debe buscar una configuración de sistema óptico 4*f* adecuada, de manera que haya la menor pérdida de información posible. Una vez fijado el sistema óptico, se debe utilizar una máscara llave, que además de cumplir las ya conocidas condiciones de este sistema de encriptación (ser de sólo fase, distribuida aleatoriamente y estadísticamente independiente de la primera). Recordemos que el tamaño del objeto de entrada determina el valor de $\langle S_x \rangle$ de la distribución de campo que ilumina la máscara llave. Este análisis sugiere que se puede determinar un criterio para escoger el máximo valor de **TGll**, para que la distribución de campo en el plano de salida se considere "bien encriptado". A partir de nuestro análisis sugerimos que **TGll** debe cumplir:

$$\mathbf{TGll} \leq \frac{\langle S_x \rangle}{2} \tag{3.11}$$

Este valor límite será válido para tamaños de objetos iguales ó menores.

Contrariamente cuando en el en el plano (μ, ν) el elemento más pequeño es el speckle, es de esperarse que se revele información del objeto de entrada, debido a que $\langle S_x \rangle$ es controlado por el tamaño del objeto de entrada. A medida que más granos de speckles pasen a través de un sólo elemento dispersor de la máscara llave, más información del objeto se aprecia en el patrón encriptado (Ver primera fila de la **Tabla 3.1**).

III.3.4. Efecto de la máscara del objeto en la distribución espacial de la información en el plano de encriptación.

En la Sección anterior estudiamos como el **TGII** controla la envolvente de la distribución de campo en el plano de encriptación. En esta Sección vamos a estudiar como el tamaño de los centros dispersores de la máscara del objeto afecta la distribución espacial del campo en el plano de encriptación.

Se muestra en la **Tabla 3.3** las imágenes encriptadas en términos de la variación del **TGo.** En estos resultados se puede apreciar el efecto que tiene el aumento del **TGo** y el tamaño del objeto de entrada en la distribución del patrón encriptado. Se observa que el tamaño promedio del grano de speckle aumenta en consonancia con **TGo** mientras que el cambio del tamaño del objeto de entrada no modifica el tamaño del grano de speckle.

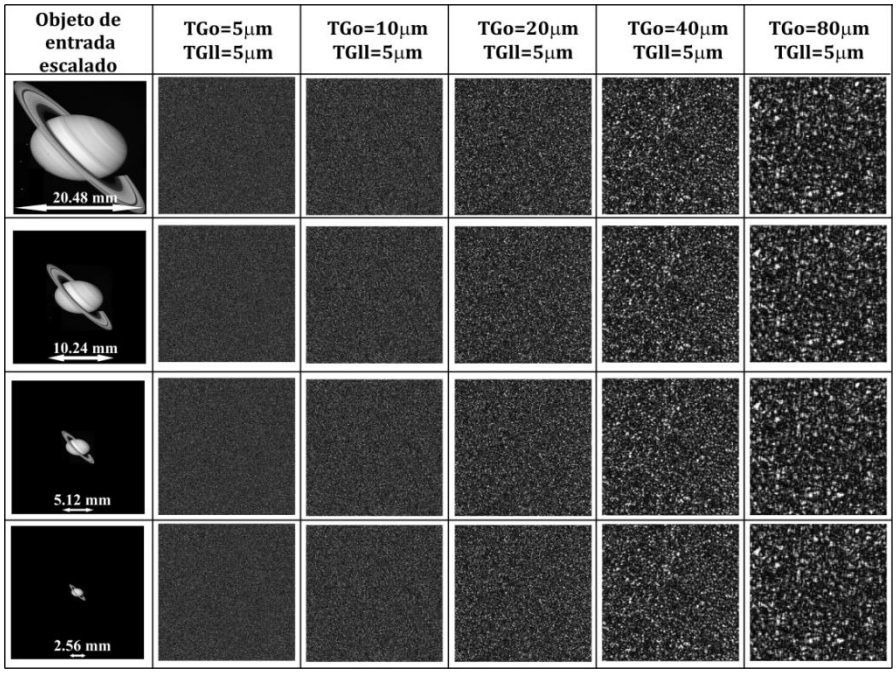


Tabla 3.3. Patrones encriptados en términos del tamaño del objeto de entrada y el **TGo**.

Es importante aclarar que para los resultados mostrados en la **Tabla 3.3**, los parámetros del sistema ópticos no cambian y **TGII** es mantenido constante en 5 micrones. Este **TGII** corresponde a una situación en la cual todos los tamaños de objetos presentados en la **Tabla 3.3** resultan en un patrón bien encriptado, es decir se cumple la condición impuesta por la ecuación (3.11). Por esta razón, aunque el tamaño del objeto

cambia a lo largo de las filas, el área y la envolvente en la cual está contenida la información encriptada no cambia. Como se puede ver a simple vista, a medida que se incrementa el **TGo**, el tamaño promedio transversal del speckle en el plano de encriptación (x_2, y_2) se incrementa también. Nótese que a lo largo de cada columna se obtienen distribuciones de speckles equivalentes, no obstante que a lo largo de dicha columna el tamaño del objeto ha variado, lo que evidencia la no dependencia de la dimensión del objeto en la distribución espacial del patrón encriptado. Cabe mencionar que la energía que aporta cada objeto al sistema no se evidencia porque todos los patrones han sido normalizados.

Para determinar cómo el tamaño promedio transversal del speckle en el plano de encriptación está relacionado con **TGo**, se evaluó para diferentes valores de **TGo**, la función de auto-correlación de la máscara objeto y del tamaño de speckle generado en el plano de encriptación (x_2, y_2). Los resultados se muestran en la **Tabla 3.4.**

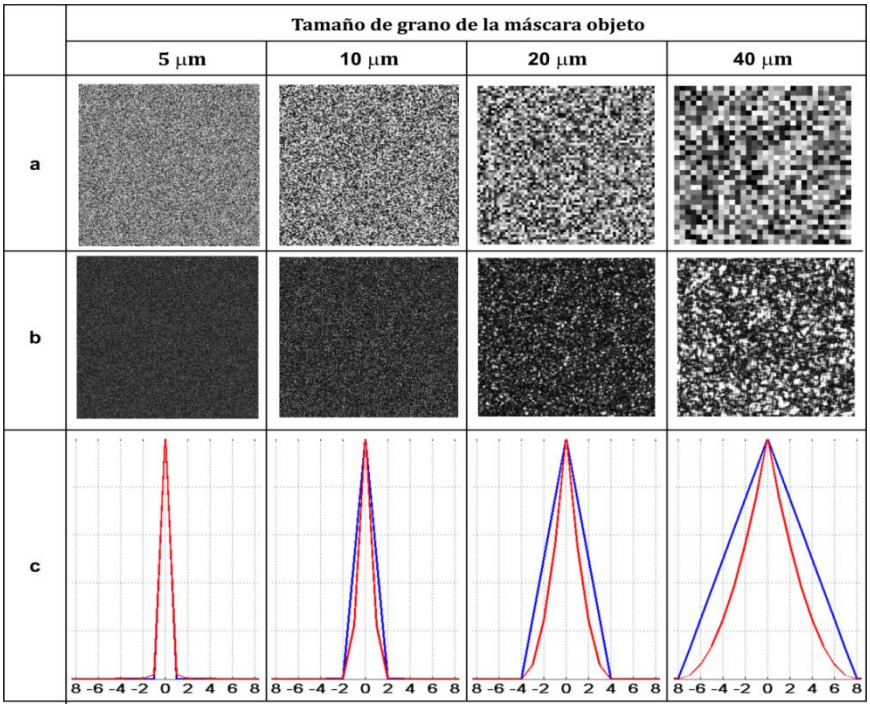


Tabla 3.4. Relación entre $\langle S_x \rangle$ en el plano de encriptación y el **TGo.** a) Representación en niveles de gris de la fase del difusor objeto. b) Intensidad de los datos encriptados (256 niveles de gris). c) Perfil de autocorrelación de la fase del difusor (azul) y la intensidad (rojo) de los datos encriptados.

La primera fila de la **Tabla 3.4** muestra las imágenes que son una representación en niveles de gris de la distribución de fase de la máscara objeto. La segunda fila muestra

las imágenes en intensidad del respectivo patrón encriptado. En la tercera fila se presenta el perfil de autocorrelación de las imágenes correspondientes a las dos filas anteriores.

Las funciones de autocorrelación de la **Tabla 3.4** nos permite concluir que hay una relación directa entre el cambio del **TGo** y el tamaño promedio del speckle en el plano de encriptación. Podemos decir que el **TGo** de la máscara de fase del plano de entrada controla el tamaño promedio del speckle en el plano de encriptación.

Bajo las condiciones de este capítulo, la distribución espacial de la información encriptada depende de **TGll** y **TGo**, que controlan el área en la cual está contenida la información y su envolvente y el tamaño promedio del speckle de dicha distribución, respectivamente. Analizaremos en la Sección siguiente el efecto que tiene el medio de almacenamiento finito en el sistema.

III.3.5. Efecto del tamaño finito del medio de registro en la imagen desencriptada.

En esta Sección analizaremos el efecto que tiene el tamaño finito del medio de almacenamiento en la arquitectura de encriptación 4*f.* Este estudio resulta pertinente, dado que el medio de almacenamiento en dispositivos experimentales, suele ser el elemento más pequeño del todo el sistema óptico, por lo tanto es allí donde se pierde gran parte de los datos encriptados. La información no almacenada en el medio de registro se ve reflejada en la pérdida de información de la imagen desencriptada. En qué medida se ve afectada la información recuperada, depende del tamaño relativo entre el medio de almacenamiento y la distribución de la información en el plano de encriptación. Es evidente que cuanto mayor porcentaje de la información quede registrada en el medio de almacenamiento, mejor será la calidad de los datos desencriptados. En esta Sección se estudiaran con más detalle estos aspectos.

Con el fin de poder determinar la cantidad de información que se pierde en los datos desencriptados, debido al efecto del área finita del medio de registro, se presentan resultados en el marco de la óptica virtual, en la **Tabla 3.5**.

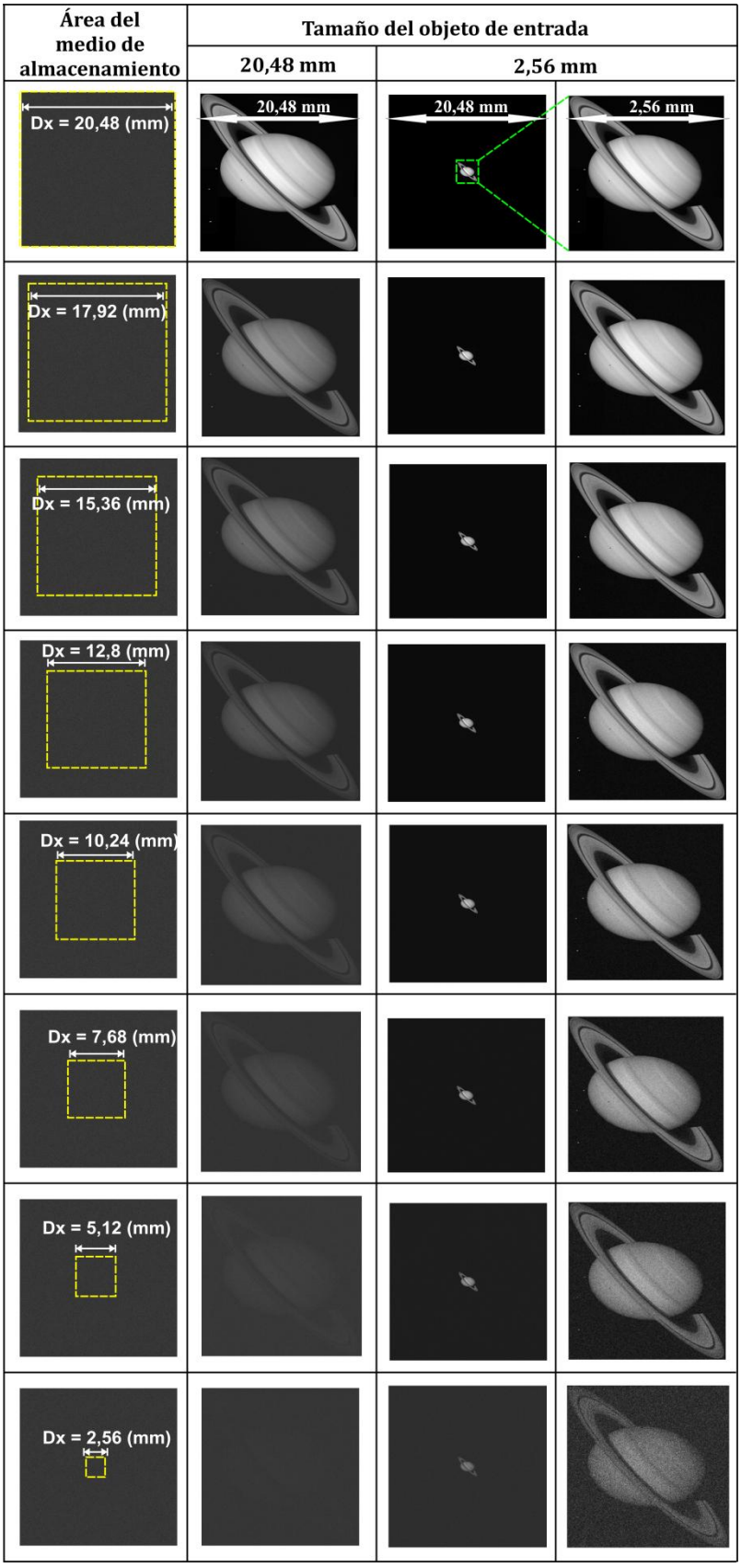


Tabla 3.5. Imágenes desencriptadas en función del área del medio de almacenamiento, para dos tamaños de objeto de entrada, para un sistema óptico con **TGo** y **TGII** de 5 μm.

Las imágenes desencriptadas mostradas en la **Tabla 3.5**, fueron obtenidas variando el área del medio de almacenamiento (representado por el cuadro amarillo en línea punteada) y el tamaño del objeto de entrada. Todos los demás parámetros del sistema óptico permanecen constantes, donde **TGo** y **TGII** se fijan en 5 micrones. Para este **TGII** ambos tamaños de objetos de entrada resultan en un patrón "bien encriptado", es decir se cumple el criterio definido por la ecuación (3.11). Bajo estas condiciones, la información encriptada para los dos tamaños de objetos presenta las mismas características de distribución espacial (área, envolvente y tamaño promedio de speckle). Cuando se cambia la imagen de entrada por otra que tenga diferente energía ó tamaño, la energía promedio del patrón cambia, pero no su distribución espacial.

La degradación en las imágenes desencriptadas presentadas en las columnas 2 y 3 de la **Tabla 3.5** es consecuencia del área finita del medio de registro. Asimismo, a medida que se hace más pequeña el área de registro, (es decir, menos cantidad de información queda registrada) se pierde más información en la imagen recuperada en el proceso de desencriptación. Es importante notar que no se pierde información adicional en el proceso de desencriptación. Resulta de interés en este momento buscar alguna métrica para determinar la calidad de la información recuperada. En nuestro caso elegimos el Error cuadrático medio (MSE) para esta evaluación, que se define como:

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{M}[I(x,y) - \tilde{I}(x,y)]^2 \qquad (3.12)$$

En la **Figura 3.6** se muestra una curva del MSE normalizado en función del área de registro para los dos tamaños de imágenes de entrada mostrados en la **Tabla 3.5.**

La información encriptada se encuentra contenida en un área de 20,48 x 20,48 mm^2, para los dos casos. Al observar la **Figura 3.6**, es claro que para la imagen de 20.48 mm, la curva del error cuadrático medio aumenta mucho más rápido que la correspondiente a la imagen de 2.56 mm. Es decir, que se obtiene el mismo nivel de degradación en la imagen desencriptada de 2,56 mm en comparación con la imagen desencriptada de 20,48 mm, aunque el área del medio de registro sea menor. Por ejemplo, si elegimos como máximo nivel de degradación un MSE=0.24, observamos que

se requiere un medio de registro de 5,12 x 5,12 mm^2 (1024 píxeles) para la imagen de 20,48 x 20,48 mm^2 (4096 píxeles) y de 17,92 x 17,92 mm^2 (3584 píxeles) para la imagen de 2.56 x 2.56 mm^2 (512 píxeles).

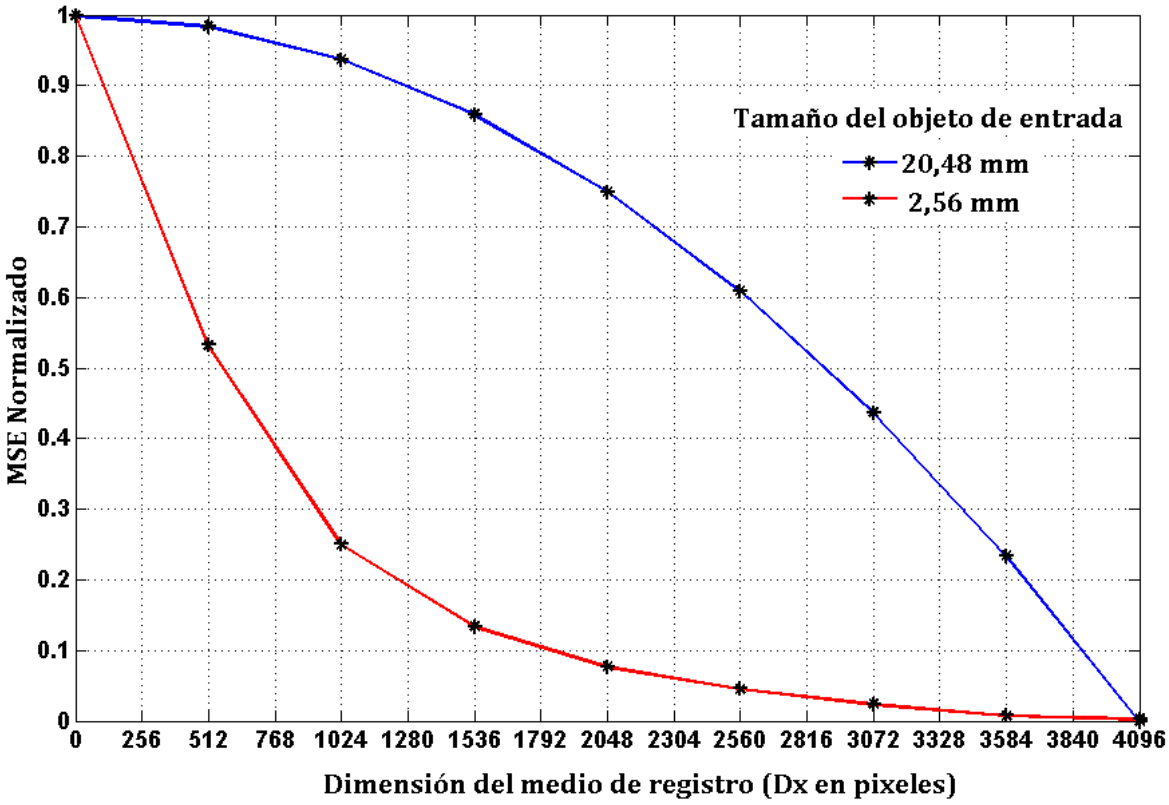


Figura 3.6. MSE normalizado en función de la cantidad de información registrada debido al tamaño finito del medio de almacenamiento.

Los resultados presentados en la **Tabla 3.5** corresponden a dos situaciones límite de tamaño de imágenes para las condiciones de nuestra simulación. En la **Tabla 3.6** se muestran las imágenes desencriptadas para el mismo sistema óptico que el utilizado en el caso de la **Tabla 3.5**, pero en este caso mantenemos constante el área del medio de almacenamiento, siendo esta a su vez menor que el área en la cual están distribuidos los datos encriptados. Se consideran cinco tamaños diferentes de objeto de entrada.

A partir de los resultados anteriores es evidente que a medida que el objeto de entrada disminuye, mejora la calidad de la imagen recuperada como se puede verificar a partir de la **Figura 3.7**, donde se presenta el MSE en función del tamaño de objeto de entrada.

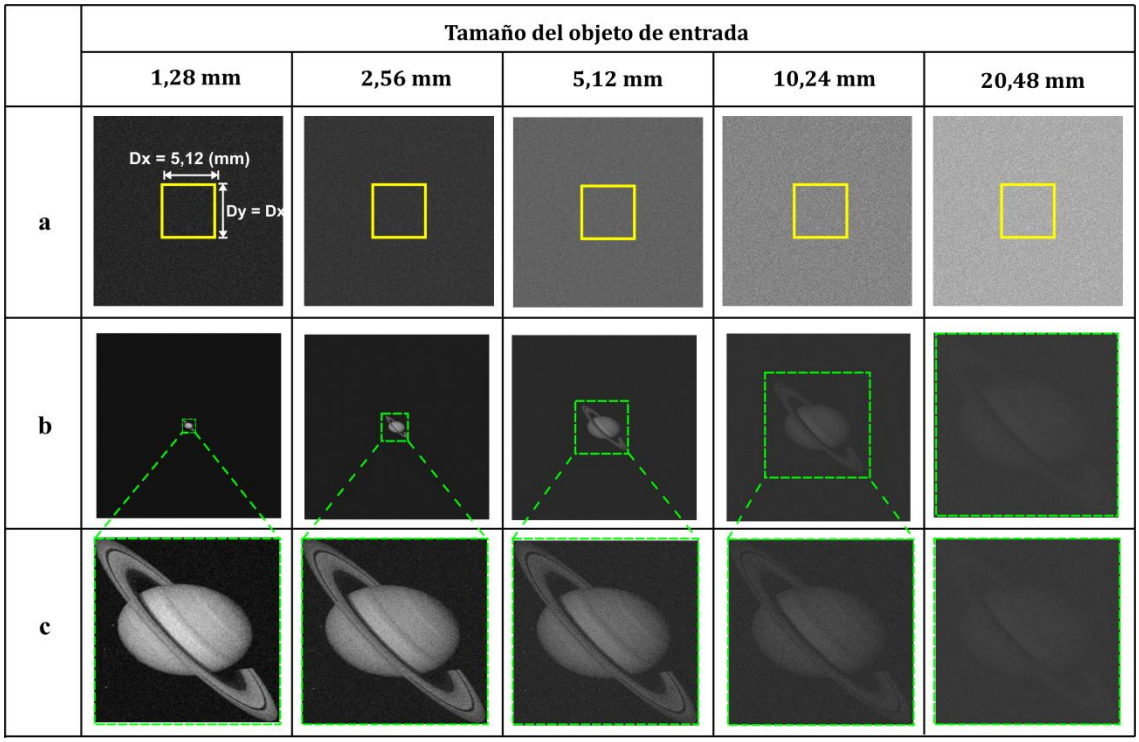


Tabla 3.6. Imagen desencriptada en términos del tamaño del objeto de entrada. a) Patrón encriptado mostrando el área del medio de almacenamiento; b) Imágenes desencriptadas; c) Versión ampliada de las imágenes desencriptadas correspondientes al área indicada por la línea a trazos amarilla de la fila b.

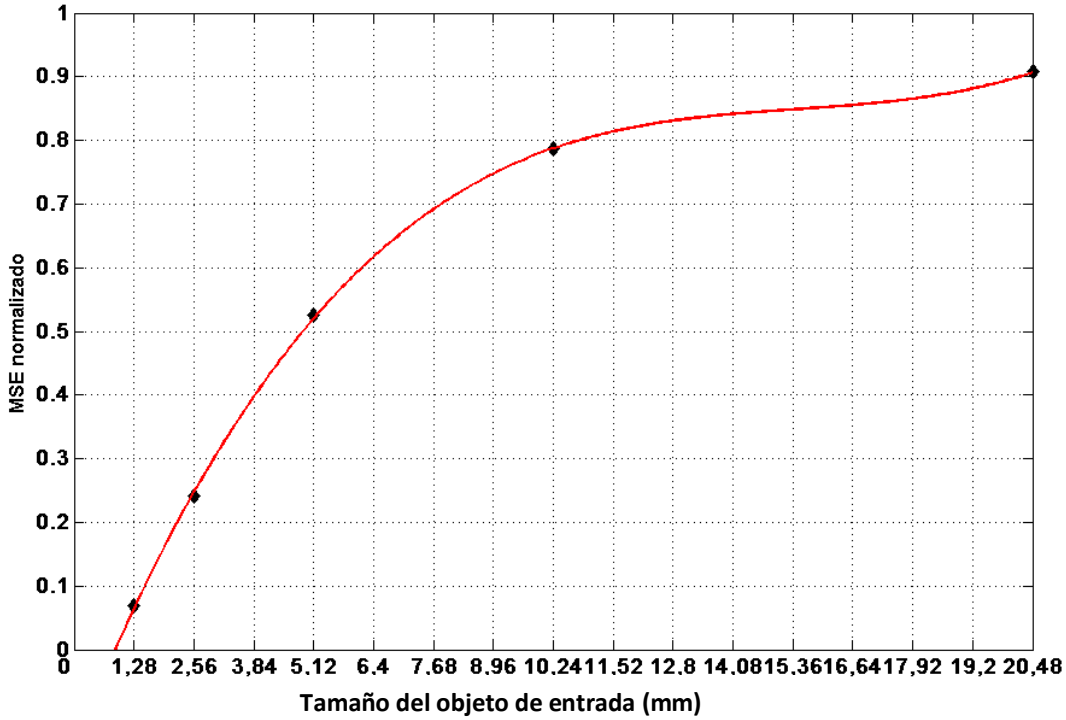


Figura 3.7. Error cuadrático medio de la imagen desencriptada en función del tamaño del objeto de entrada.

Es decir, se requiere un área de almacenamiento mayor para una imagen mayor si se desea tener la misma calidad de imagen desencriptada.

Como observamos a partir de los resultados de la **Tabla 3.6** y la **Figura 3.7**, para un determinado sistema de encriptación y área de almacenamiento, la calidad de la imagen desencriptada depende del tamaño del objeto de entrada. Es evidente, que se requiere una mínima cantidad de información encriptada para cada tamaño de objeto de entrada tal que produzca una imagen desencriptada "identificable". Para cuantificarla, se diseñó una prueba, que consiste en medir el contraste de la imagen desencriptada que proporcione el mínimo contraste detectable para una entrada binaria. El contraste para una imagen de intensidad I se define como:

$$C = \frac{\max(I) - \min(I)}{\max(I)} \tag{3.13}$$

En esta prueba los objetos de entrada son réplicas escaladas de una imagen binaria. Para cada tamaño de objeto, se presentan las imágenes desencriptadas obtenidas a partir del registro de diferentes porcentajes de información encriptada (lo que implica variar el área del medio de almacenamiento). Los resultados de la prueba se presentan en la **Tabla 3.7.**

La imagen en intensidad de los datos encriptados se presenta en la primera columna, es importante recordar que el área en la cual se distribuyen los datos encriptados es la misma para todos los tamaños de objetos de entrada. Para cada fila de la **Tabla 3.7** el área del medio de almacenamiento es la misma, mientras que a lo largo de cada columna se varía (representada por el cuadro amarillo de la primera columna).

A partir de estos resultados se ve que para una determinada área de medio de almacenamiento, a medida que el tamaño del objeto de entrada disminuye, mejora el contraste de la imagen recuperada. Fijado el tamaño del objeto de entrada, es decir a lo largo de cada columna, para obtener un determinado contraste en la imagen desencriptada, es aparente que el área del medio de almacenamiento disminuye cuando disminuye el tamaño del objeto de entrada.

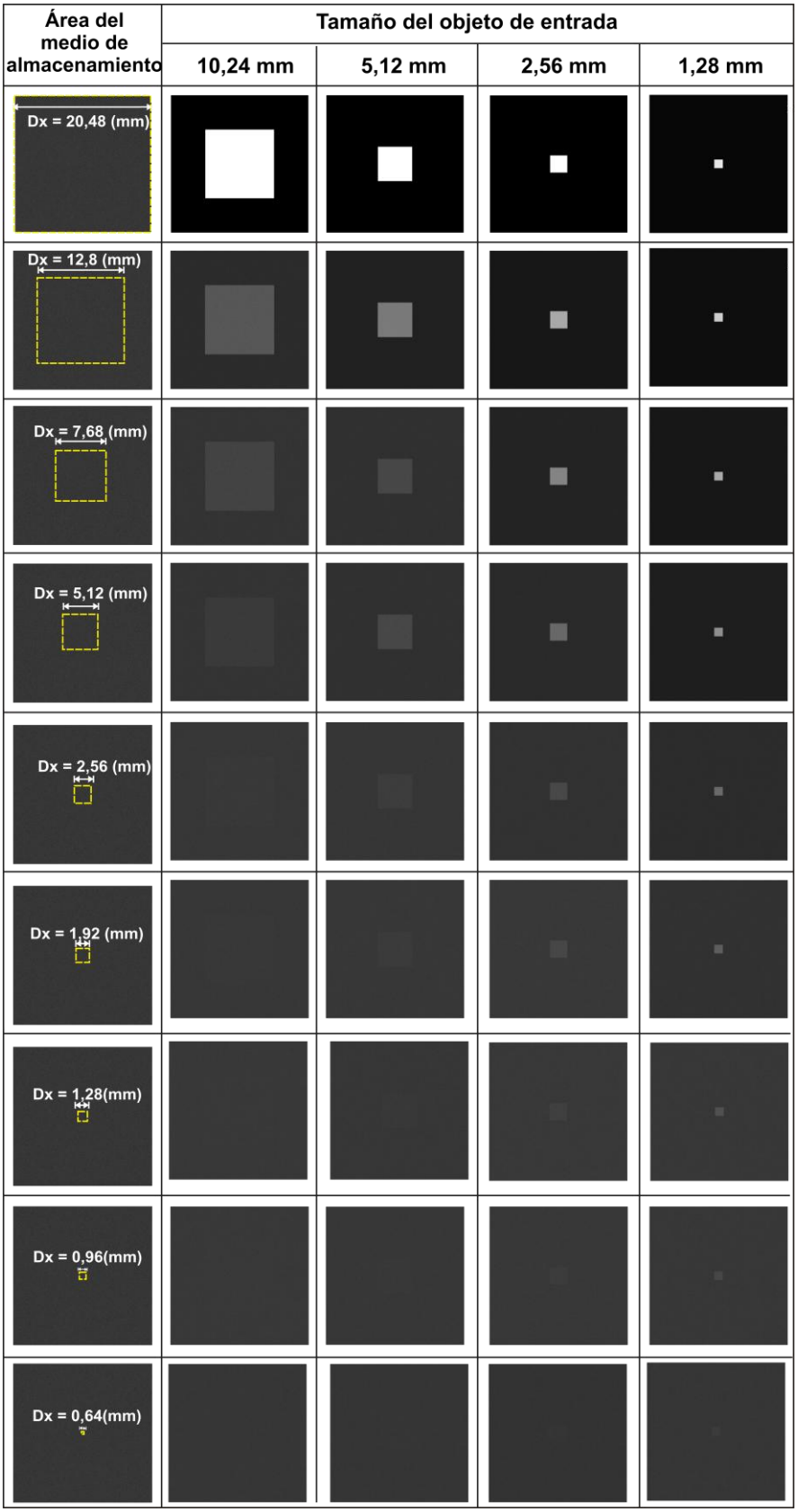


Tabla 3.7. Imágenes binarias desencriptadas en función del área del medio de almacenamiento, para cuatro tamaños de objeto de entrada, para un sistema óptico con **TGo** y **TGII** de 5 micrómetros.

Para cuantificar este comportamiento se presenta en la **Figura 3.8** el contraste de las imágenes desencriptadas en términos del área del medio de almacenamiento para los cuatro tamaños de objeto de entrada de la **Tabla 3.7**

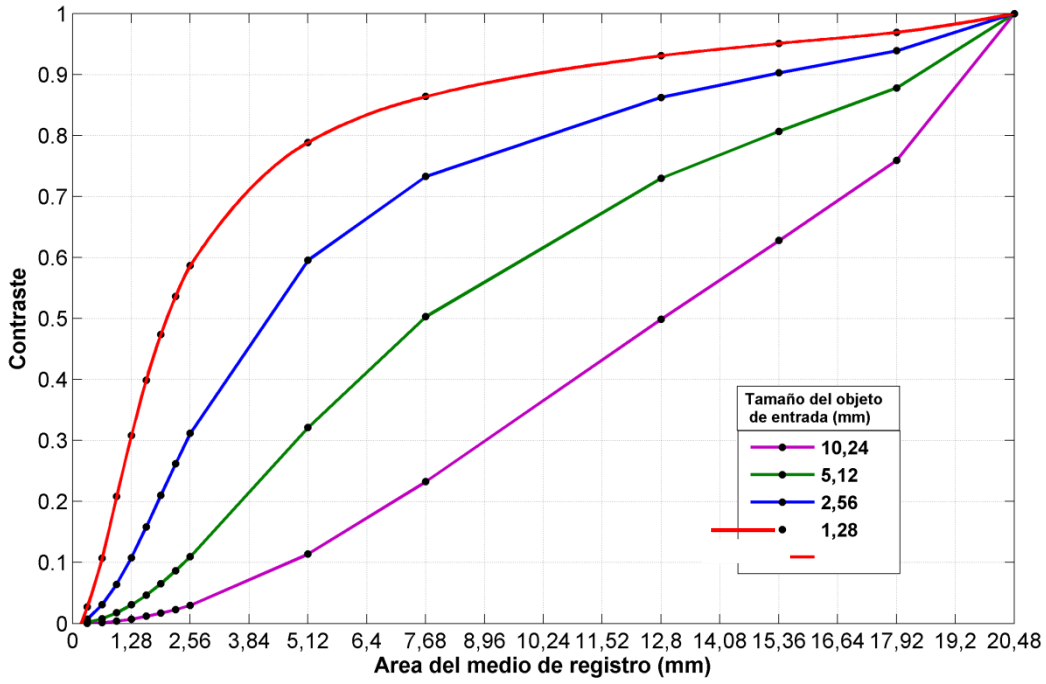


Figura 3.8. Contraste de las imágenes desencriptadas de la **Tabla 3.7** en función del tamaño del medio de almacenamiento.

Seleccionamos de la **Tabla 3.7** las imágenes desencriptadas para cada tamaño de objeto de entrada, que a nuestro criterio son "identificables". Para el objeto de entrada de 10,24 x 10,24 mm^2, 5,12 x 5,12 mm^2, 2,56 x 2,56 mm^2 y 1,28 x 1,28 mm^2, dicha imagen corresponde a un área de almacenamiento de 5,12 x 5,12 mm^2, 2,56 x 2,56 mm^2 y 1,28 x 1,28 mm^2 y 0,64 x 0,64 mm^2, respectivamente. Al localizar estos cuatro casos en las curvas de la **Figura 3.8** observamos que corresponden a un contraste de 0.1.

Hasta este punto hemos analizado el efecto que provoca en la imagen desencriptada el hecho de que el medio de almacenamiento sea más pequeño que el área en la cual la información encriptada está distribuida, pero en todos los casos la información estaba uniformemente distribuida. En esta Sección se analiza el efecto que produce en los datos recuperados, información no uniformemente distribuida en el plano de encriptación, cuando sólo se registra una parte de aquella debido al tamaño finito del medio de registro.

Enfaticemos que para esta arquitectura, la información en el plano de encriptación (x_2, y_2) corresponde a la proyección geométrica del objeto de entrada convolucionada con la respuesta impulsiva del sistema. Por otra parte, en la Sección III.3.3 se demostró que la distribución macroscópica espacial de la información depende **TGll**. En la primera columna de la **Tabla 3.8** se hacen evidentes estas consideraciones.

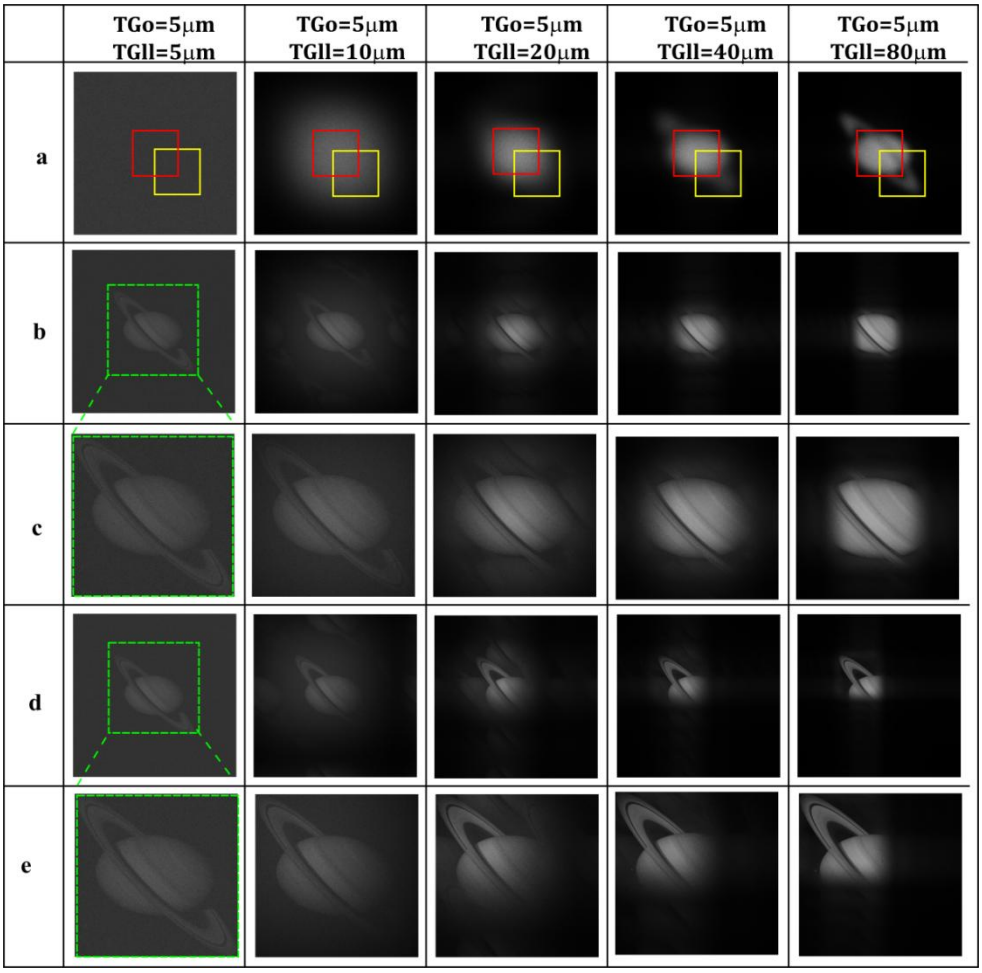


Tabla 3.8. Imagen desencriptada cuando se registra solo una porción de la información encriptada en función de **TGll** y la posición del medio de registro. a) Patrón encriptado mostrando el área del medio de almacenamiento en dos localizaciones distintas. b) Imágenes desencriptadas cuando el medio de almacenamiento está ubicado en la posición delimitada por el cuadro rojo de la fila a). c) Versión ampliada de las imágenes desencriptadas de la fila b). d) Imágenes desencriptadas cuando el medio de almacenamiento está ubicado en la posición delimitada por el cuadro amarillo de la fila a). e) Versión ampliada de las imágenes desencriptadas de la fila c).

En la primera fila de la **Tabla** 3.8 se muestra el patrón encriptado para una imagen cuadrada de 10,24 mm de lado que ocupa el centro de un fondo negro cuadrado de 20,48 mm de lado. A lo largo de cada fila se controla la distribución de los datos encriptados mediante el cambio de **TGll**. Como el valor de **TGll** aumenta a lo largo de las filas, se

observa que a partir de la tercera columna, se deja de cumplir el criterio impuesto por la ecuación (3.11) necesario para que la información esté uniformemente distribuida. Las imágenes mostradas en la fila b de la **Tabla 3.7** corresponden a las imágenes desencriptadas cuando se ha registrado sólo la parte de la información encriptada en un medio de almacenamiento cuyo tamaño y posición están representados por el cuadro rojo. Como se puede ver claramente, si la información está distribuida de manera uniforme en el plano de encriptación (deslocalizada), entonces la información obtenida en el proceso reconstrucción contiene información de todos los puntos objetos en el plano de entrada, con el mismo peso. Por el contrario, si en el plano de encriptación los datos están modulados por alguna envolvente (localizados), los datos recuperados van a tener diferentes pesos para cada zona de la imagen desencriptada, que se corresponden con las coordenadas conjugadas de las que ocupa el medio de almacenamiento y el perfil de la envolvente que modulaba los datos. Se puede ver en la fila b**,** que a medida que aumenta el valor de **TGII**, la información desencriptada corresponde de una manera mucho más local a la ubicación conjugada del cuadro de almacenamiento. En la fila d, se evidencia el efecto de la localización cuando se registra una porción no centrada del patrón encriptado. Las filas c y e muestran una versión ampliada de las filas b y d respectivamente.

III.4 Conclusiones

Para que la imagen desencriptada en un sistema de encriptación 4*f*, sea recuperada con la menor pérdida de información, garantizando que la información esté bien encriptada, es necesario tener en cuenta los anchos de banda espacial y frecuencial de la señal de entrada y del sistema óptico. Para una señal de entrada, su ancho de banda frecuencial, debe ser menor que el ancho de banda espacial de la máscara llave que a su vez determina el ancho de banda del sistema para toda la información de entrada sea transferida al plano de encriptación. Si se garantiza que el área del medio de almacenamiento registra toda la información encriptada, entonces únicamente bajo estas

condiciones el proceso resulta reversible y los datos desencriptados replican la información de entrada.

El hecho de que la información encriptada esté uniformemente distribuida en el plano de encriptación, que denominamos información bien encriptada, está determinado por **TGII**. Para lograr este objetivo, el criterio que se determinó indica que el tamaño promedio del grano de speckle del campo que ilumina el difusor llave, debe al menos duplicar el **TGII.**

Otro aspecto a tener en cuenta está relacionado con el área de almacenamiento. En ese sentido si el tamaño del medio de almacenamiento relativo al área en la que está contenida la información encriptada disminuye, se incrementa el deterioro de la imagen desencriptada. Asimismo si la distribución de la información en el plano de encriptación no es uniforme, los datos recuperados van a tener diferentes pesos para cada zona de la imagen desencriptada, que se corresponden con las coordenadas conjugadas de las que ocupa el medio de almacenamiento y del perfil que tenga la envolvente que modulaba los datos.

La pérdida de información en los sistemas de encriptación óptica es casi inevitable. Sin embargo es posible caracterizar esa pérdida en función de los parámetros del sistema. Para un dado sistema óptico, incluyendo los difusores, la mínima cantidad de datos encriptados requeridos para obtener una imagen desencriptada identificable dependerá del tamaño del objeto de entrada. Asimismo, hay una relación directa entre el tamaño del objeto de entrada y el área del medio de almacenamiento. Un análisis más profundo involucraría tener en cuenta objetos no binarios y objetos con distintos contenido en frecuencias espaciales. Asimismo otro aspecto a considerar el rango dinámico del medio de adquisición.

III.5 Referencias

[3.1] A.W. Lohmann, R. G. Dorsch, D. Mendlovic and Z. Zalevsky, C. Ferreira. ”Space–bandwidth product of optical signals and systems”, J. Opt. Soc. Am. A. 13, 470-473 (1996).

[3.2] BM Hennelly, J.T. Sheridan. **“**Optical encryption and the space bandwidth product”, Opt. Comm. 247, 291-305 (2005).

[3.3] T. Nomura, E. Nitanal, T. Numata and B. Javidi. “Design of input phase mask for the space bandwidth of the optical encryption system”, Opt Eng. 45, 017006 (2006)

[3.4] B. Javidi, A. Sergent, G. Zhang, and L. Guibert, “Fault tolerance properties of a double phase encoding encryption technique”, Opt. Eng. 36, 992–998 (1997)

[3.5] B. Javidi, G.S. Zhang, and J. Li, “Experimental demonstration of the random phase encoding technique for image encryption and security verification”, Opt.Eng. 35, 2506-2512 (1996).

[3.6] B. Javidi and E. Ahouzi, “Optical security system with Fourier plane encoding,” Appl. Opt. 37, 6247–6255 (1998).

[3.7] R.K.Wang, I.A.Watson, and C. Chatwin, “Random phase encoding for optical security,” Opt. Eng. 35, 2464–2469 (1996).

[3.8] O. Kafri, E. Keren, “Encryption of pictures and shapes by random grids”, Opt. Lett. 12, 377-379 (1987).

[3.9] B. Javidi, L. Horner, “Optical Pattern recognition for validation and security verification”, Op. Eng. 33, 1752-1756 (1994).

[3.10] P. Réfrégier, B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding”, Opt. Lett. 20, 767-797 (1995).

[3.11] B. Javidi, G. Zhang, and J. Li, “Experimental demonstration of the random phase encoding technique for image encryption and security verification,” Opt. Eng. 35, 2506–2512 (1996)

[3.12] B. Javidi, G. Zhang, and J. Li, “Encrypted optical memory using double-random phase encoding” Appl. Opt. 36, 1054-1058 (1997).

[3.13] G. Unnikrishnan, J. Joseph, and K. Singh, “Optical encryption system that uses phase conjugation in a photorefractive crystal,” Appl. Opt. 37, 8181–8186, 1998.

[3.14] G. Situ and J. Zhang, “Double random-phase encryption in the Fresnel domain,” Opt. Lett. 29, 1584-1586, 2004.

[3.15] T. Nomura and B. Javidi, "Optical encryption using a joint transform correlator architecture," Opt. Eng. 39, 2031-2035 (2000).

[3.16] J. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, "Multiplexing encrypted data by using polarized light," Opt. Comm. 260, 109-112, 2006.

[3.17] J. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, "Multiple image encryption using an aperture-modulated optical system," Opt. Comm. 261, 29–33, 2006.

[3.18] O. Matoba, B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain", Opt. Lett. 24, 762-764 (1999).

[3.19] O. Matoba, B. Javidi, "Encrypted optical storage with angular multiplexing", App. Opt. 38, 7288-7293 (1999).

[3.20] Li-Chien Lin, Chau-Jern Cheng, "Optimal Key mask design for optimal encryption based on joint trasform correlator architecture" (2005)

[3.21] See O. Lummer and F. Reiche, Die Lehre von der Bildentstehung im Mikroskop von E. Abbe (Vieweg, Braunschweig, 1910).

[3.22] M. von Laue, Ann. Phys. (Leipzig) 44, 1197 (1914).

[3.23] W. Lukosz, "Optical systems with resolving powers exceeding the classical limit," J. Opt. Soc. Am. 56, 1463–1472 (1996).

[3.24] A. W. Lohmann, "The space–bandwidth product, applied to spatial filtering and holography," Research Paper RJ-438 (IBM San Jose Research Laboratory, San Jose, Calif., 1967), pp. 1–23.

[3.25] A. VanderLugt, Optical Signal Processing (Wiley, New York, 1992), pp. 10, 50.

[3.21] C. Cuadrado-Laborde, J. Lancis, "The space-bandwidth product in the joint transform correlator optical encryption setup", Opt. Commun. (2011), doi:10.1016/j.optcom.2011.05.012.

CAPÍTULO IV

Análisis de la distribución de los datos encriptado. Arquitectura JTC.

IV.1 Introducción

El sistema de encriptación basado en la arquitectura JTC [4.1] representa una alternativa a las exigencias de alineación propias de la arquitectura 4*f* [4.2-4.3]. Si bien la arquitectura JTC ha sido menos estudiada que la basada en el 4*f,* hay algunas investigaciones en la que se analiza la degradación de los datos recuperados para estos dispositivos de codificación. Primero Nomura at al. [4.4] y luego Li-Chien y Chau-Jern [4.5] muestran que la imagen desencriptada mejora significativamente cuando se garantiza que se cumpla la condición impuesta en la teoría, es decir que la máscara llave tenga una ancho de banda espacial limitado a la ventana del JTC y que sea de sólo fase en el dominio de la frecuencia. Usualmente, tanto en las simulaciones cuanto en los experimentos, se utiliza en el plano de entrada del JTC un difusor de sólo fase aleatorio, razón por la cual la condición mencionada no se cumple. Se puede verificar que si bloqueamos la ventana del objeto y observamos sólo la transformada de Fourier de la máscara llave, no se obtiene una distribución de sólo fase en el plano de Fourier, resultando un patrón en intensidad no uniforme. En estas condiciones las imágenes desencriptadas resultan afectadas debido a esta distribución no uniforme en intensidad, aunque no exista pérdida de información debido a los productos de ancho de banda del sistema y la señal. Por otro lado, R. Henao et al. [4.6] muestran que mediante la manipulación digital de los datos encriptados, se pueden eliminar algunas componentes en intensidad de ciertos términos del JPS resultando en una imagen desencriptada menos ruidosa.

Como se analizó en el capítulo III, las imágenes desencriptadas (obtenidas mediante simulaciones) basadas en la arquitectura 4*f* logran reconstruirse sin ruido. Sin embargo, en la arquitectura JTC el speckle está presente en la imagen desencriptada, en el mejor de los casos, puede reducir su tamaño de tal manera que en comparación a las frecuencias espaciales del objeto, resulte en ruido de alta frecuencia. Por esta razón, el sistema JTC no es el más empleado a pesar ser más fácil de implementar experimentalmente por ser más robusto a la alineación y no requerir una conjugación de fase.

En este capítulo analizaremos la influencia de los parámetros ópticos del sistema de encriptación en la calidad de la imagen desencriptada. Asimismo, abordamos el problema del ruido en las imágenes obtenidas mediante el arreglo JTC con el fin de optimizarlo y obtener mediante simulaciones imágenes de calidad comparable a las de la arquitectura 4*f.*

También, se analizará el rol que desempeña el tamaño de los centros dispersores de la máscara de fase aleatoria en la distribución de la información en el plano de encriptación y cómo esto afectará la calidad de la imagen desencriptada. Para realizar este estudio, será necesario hacer algunas precisiones respecto a los anchos de banda de la imagen a encriptar, la máscara objeto, la máscara llave y el sistema óptico.

Debemos recordar algunas de las ventajas que la configuración JTC presenta frente al clásico sistema 4*f*. La imagen encriptada es un patrón en intensidad razón por la cual puede ser registrada directamente empleando una cámara CCD, un cristal fotorrefractivo de volumen, etc [4.7]. En esta arquitectura, el registro de los datos encriptados tiene lugar en un plano de Fourier, resultando en consecuencia menos sensible a los desalineamientos, por la invariancia a las traslaciones.

En trabajos previos se ha demostrado que cuando el medio de registro es de volumen, la eficiencia de difracción de un patrón de speckle modulado (JPS en una arquitectura JTC) depende del volumen del grano promedio de speckle dentro del cristal [4.8]. En el caso de la arquitectura JTC (régimen de campo lejano) las dimensiones promedio del patrón de speckle son independientes de la naturaleza del difusor. En este caso, la pupila del sistema y la distancia focal son los parámetros que controlan el tamaño

del speckle para una longitud de onda dada. Por esta razón existe una configuración, dependiendo de las dimensiones del medio de almacenamiento, que permite obtener una óptima eficiencia de difracción, resultando una imagen desencriptada de mayor energía. Esto nos restringe a emplear lentes dentro de cierto rango de distancias focales y dimensión de pupila. Estos dos aspectos son de vital importancia en la calidad de la imagen desencriptada. Por otra parte, el tamaño de los centros dispersores que componen el difusor no afecta el volumen del speckle, sin embargo controla otras características del patrón encriptado.

Otro aspecto a tener en cuenta se vincula con el área finita del medio de almacenamiento (cámaras CCD, cristales fotorrefractivos, etc). En algunos de los resultados experimentales que presentaremos en los siguientes capítulos, empleamos cristales fotorrefractivos, cuya área no supera el centímetro cuadrado. Por este motivo, al igual que en el capítulo anterior, resulta de interés analizar la influencia del área finita del medio de registro.

IV.2 Ancho de banda espacial de un sistema de encriptación óptico JTC.

Para un sistema de encriptación JTC, siguiendo la notación del capítulo II, se denota como $g(\mathrm{x}_0, \mathrm{y}_0)$ y $r(\mathrm{x}_0, \mathrm{y}_0)$, a la imagen a encriptar y a la máscara de fase aleatoria del plano de entrada, respectivamente. La máscara llave del sistema está representada por $h(\mathrm{x}_0, \mathrm{y}_0)$. Ahora vamos a imponer la condición de que la señal de entrada sea finita en el espacio y tenga ancho de banda frecuencial limitado y que la máscara llave tenga un ancho de banda frecuencial limitado también:

$$g(x_0, y_0) = 0, \text{ fuera del rango: } |x_0| \leq \frac{\Delta x_{0g}}{2}, |y_0| \leq \frac{\Delta y_{0g}}{2} \tag{4.1}$$

$$r(x_0, y_0) = 0, \text{ fuera del rango: } |x_0| \leq \frac{\Delta x_{0r}}{2}, |y_0| \leq \frac{\Delta y_{0r}}{2} \tag{4.2}$$

$$h(x_0, y_0) = 0, \text{ fuera del rango: } |x_0| \leq \frac{\Delta x_{0h}}{2}, |y_0| \leq \frac{\Delta y_{0h}}{2} \tag{4.3}$$

$$G(\mu, \nu) = 0, \text{ fuera del rango: } |\mu| \leq \frac{\Delta \mu_G}{2}, |\nu| \leq \frac{\Delta \nu_G}{2} \tag{4.4}$$

$$R(\mu,\nu)=0, \text{ fuera del rango: } |\mu| \leq \frac{\Delta\mu_R}{2},\ |\nu| \leq \frac{\Delta\nu_R}{2} \tag{4.5}$$

$$H(\mu,\nu)=0, \text{ fuera del rango: } |\mu| \leq \frac{\Delta\mu_H}{2} |\nu| \leq \frac{\Delta\nu_H}{2} \tag{4.6}$$

donde $\mathrm{G}(\mu,\nu)$, $\mathrm{R}(\mu,\nu)$ y $H(\mu,\nu)$ son las transformadas de Fourier de $\mathrm{g}(\mathrm{x}_0,\mathrm{y}_0)$, $\mathrm{r}(\mathrm{x}_0,\mathrm{y}_0)$ y $h(x_0,y_0)$ respectivamente, $(\Delta\mathrm{x}_{0\mathrm{g}},\Delta\mathrm{y}_{0\mathrm{g}})$, $(\Delta\mathrm{x}_{0\mathrm{r}},\Delta\mathrm{y}_{0\mathrm{r}})$ y $(\Delta\mathrm{x}_{0\mathrm{h}},\Delta\mathrm{y}_{0\mathrm{h}})$ representa el ancho de banda espacial de $g(x_0,y_0)$, $r(x_0,y_0)$ y $h(x_0,y_0)$, respectivamente, $(\Delta\mu_{\mathrm{G}},\Delta\nu_{\mathrm{G}})$,$(\Delta\mu_{\mathrm{R}},\Delta\nu_{\mathrm{R}})$, $(\Delta\mu_{\mathrm{H}},\Delta\nu_{\mathrm{H}})$ son los anchos de banda de frecuencia espacial de $\mathrm{G}(\mu,\nu)$, $\mathrm{R}(\mu,\nu)$ and $\mathrm{H}(\mu,\nu)$, respectivamente.

El ancho de banda espacial del sistema, está determinado por la extensión de la transformada de Fourier de la máscara llave en el plano de Fourier, $\mathrm{H}(\mu,\nu)$. Esto debe ser garantizado mediante la selección adecuada de los parámetros ópticos del sistema.

El patrón encriptado contiene toda la información del objeto si se cumple la siguiente condición:

$$\Delta\mu_G + \Delta\mu_R \leq \Delta\mu_H \tag{4.7}$$

$$\Delta\nu_G + \Delta\nu_R \leq \Delta\nu_H \tag{4.8}$$

esto coincide con lo establecido para el sistema 4*f* en las ecuaciones (3.6) y (3.7) de la Sección III.2 del capítulo III).

Está condición para el sistema de encriptación JTC no siempre se cumple, dado que al estar la máscara objeto y la máscara llave en el mismo plano, usualmente se utiliza un único difusor para ambas ventanas. Esto implica que el ancho de banda de las máscaras sean iguales, es decir: $(\Delta\mu_R,\Delta\nu_R)$ =$(\Delta\mu_H,\Delta\nu_H)$, con lo cual la desigualdad planteada en las ecuaciones (4.7) y (4.8) no se cumple. Si el objeto sólo tiene bajas frecuencias se perderá poca información debido al ancho de banda del objeto, pero si contiene altas frecuencias, una porción importante de la información encriptada se perderá debido al corte de frecuencias (que impone las ecuaciones (4.7) y (4.8)). Remarquemos que para este sistema no basta con cumplir la mencionada condición para tener una imagen desencriptada sin ruido, sino que $\mathrm{H}(\mu,\nu)$ debe ser de sólo fase, es decir, su amplitud debe ser uniforme como se impuso en la ecuación (2.37) del capítulo II:

$$\left|H\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)\right|^2 = 1 \tag{4.9}$$

Para el sistema 4*f* esta es una condición fácil de cumplir, porque la máscara de sólo fase $\mathrm{H}(\mu,\nu)$ está físicamente ubicada en el plano de Fourier. En cambio, para el caso del JTC la máscara llave $h(x_0,y_0)$ está ubicada en el plano espacial y acotada por una ventana del plano de entrada, y no resulta trivial tener la distribución de amplitud uniforme en el plano de Fourier que se requiere según la ecuación (4.9).

IV.3 Esquema JTC con área finita del medio de registro

En nuestro estudio vamos a adicionar una condición al sistema de encriptación JTC descripto en la Sección (II.4.2) del capítulo II: la finitud del medio de registro.

En efecto, el medio que se utiliza para almacenar los datos encriptados tiene dimensión finita. Sea $g(\mathrm{x}_0,\mathrm{y}_0)$, la imagen a ser encriptada multiplicada por la máscara de fase del plano de entrada $r(\mathrm{x}_0,\mathrm{y}_0)=\mathrm{e}^{\mathrm{i}2\pi\mathrm{p}(\mathrm{x}_0,\mathrm{y}_0)}$ ubicada en la posición (0, -Y) del plano de entrada del JTC. En la otra ventana ubicada en la posición (0, +Y), se localiza la máscara llave $\mathrm{h}(\mathrm{x}_0,\mathrm{y}_0)$. La entrada es iluminada por una onda plana de longitud de onda λ y amplitud unitaria. El campo propagado es transformado Fourier por la lente $\mathbf{L_1}$ de longitud focal ***f.*** Como se mencionó en la Sección II.4.2, en la arquitectura JTC la información encriptada es el espectro de potencia, es decir el valor absoluto al cuadrado de la ecuación (2.33). Al considerar la extensión finita del medio de registro, el patrón encriptado estará representado por:

$$I(x_1,y_1)=\mathbf{Rec}(\frac{\mathbf{x_2}}{\mathbf{D_x}},\frac{\mathbf{y_2}}{\mathbf{D_y}})|U_1(x_1,y_1)|^2 =$$

$$\mathbf{Rec}\left(\frac{\mathbf{x_2}}{\mathbf{D_x}},\frac{\mathbf{y_2}}{\mathbf{D_y}}\right)\left\{\frac{1}{(\lambda f)^2}\left[\left|G\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)\otimes R\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)\right|^2+\left|H\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)\right|^2\right]+\right.$$

$$\left.\frac{1}{(\lambda f)^2}\left[G\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)\otimes R\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)\right]H^*\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)e^{i2\pi(2Y)\frac{x_1}{\lambda f}}+\right.$$

$$\frac{1}{(\lambda f)^2}\left[G^*\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)\otimes R^*\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)\right]H\left(\frac{x_1}{\lambda f},\frac{y_1}{\lambda f}\right)e^{-i2\pi(2Y)\frac{x_1}{\lambda f}}\Big\} \qquad (4.10)$$

Esta ecuación describe el patrón encriptado que es almacenado en un medio de registro de dimensiones D_x y D_y. El esquema de la etapa de encriptación considerando el medio de registro finito se muestra en la **Figura 4.1.**

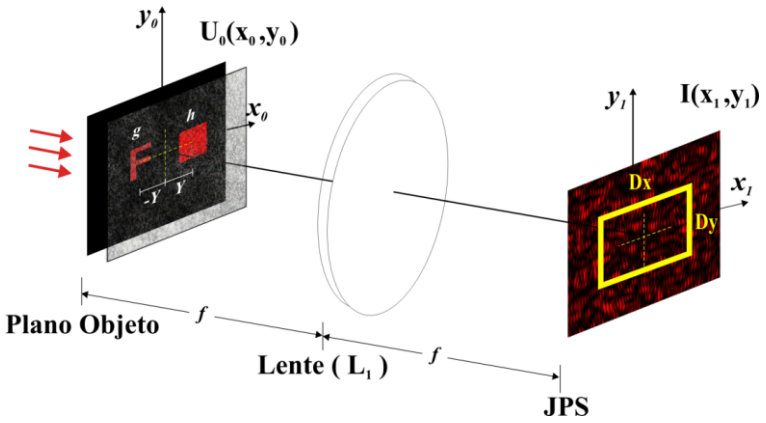


Figura 4.1. Arquitectura de encriptación JTC con medio de registro finito.

En la etapa de desencriptación, se ilumina el JPS con el campo correspondiente a la transformada de Fourier de la máscara llave utilizada en el proceso de encriptación. El campo emergente es nuevamente transformado Fourier para recuperar la imagen desencriptada. Esta imagen replica al objeto de entrada, si la máscara llave utilizada en el proceso de desencriptación es idéntica a la utilizada en el proceso de encriptación y además todos los parámetros del sistema óptico son iguales que en la etapa de encriptación. Por otra parte, la réplica del objeto se logra con un medio de almacenamiento sin limitaciones físicas.

IV.4 Ancho de banda de la máscara objeto, del objeto de entrada y del producto entre ellos.

Cuando se adosa una máscara objeto a un objeto en el dominio espacial se genera en el espacio de frecuencias la convolución entre la transformada de Fourier del objeto y la transformada de Fourier de la máscara. La distribución resultante en el dominio de

Fourier (ancho de banda de la señal de entrada) se extiende $\Delta\mu_G + \Delta\mu_R$ en x_1 y $\Delta\nu_G + \Delta\nu_R$ en y_1.

IV.4.1 Distribución de la información del objeto de entrada cuando se utiliza una máscara objeto con centros dispersores cuadrados.

En esta Sección se muestra como es la distribución de la información espectral de un objeto en función del ancho de banda de la máscara objeto, cuyos centros dispersores son cuadrados es decir que poseen una fase uniforme en toda el área (cuadrado). Este tipo de máscaras se presentan en la simulaciones de óptica virtual y cuando se utiliza moduladores espaciales de luz en régimen de fase.

En la **Tabla 4.1** se observa para el objeto (un cuadro de amplitud uniforme) de la primera fila su transformada de Fourier en la segunda fila. En las siguientes filas impares se muestra una representación en niveles de gris de la distribución aleatoria de fase correspondiente a la máscara que se adosa al objeto, cuando se incrementa el tamaño de los centros dispersores (TGo). En las siguientes filas pares se muestra la distribución en amplitud en el plano de Fourier correspondiente al producto del objeto (primera fila) y la máscara objeto (representado en la fila impar inmediata anterior) que componen la señal de entrada. Se puede notar que la modulación de la distribución la controla la transformada de Fourier del centro dispersor. Es evidente que a medida que aumenta el TGo se reduce el ancho de la distribución (ver **Tabla 4.1**). Notemos que el tamaño del centro dispersor nos permite controlar el ancho de banda, mientras que su forma determina la modulación macroscópica del espectro de la señal de entrada. Esto constituye una herramienta útil para escoger una máscara objeto que cumpla las condiciones impuestas por las ecuaciones (4.7) y (4.8).

Dado que el centro dispersor es un cuadrado, la modulación macroscópica del espectro de la señal de entrada se corresponde con una función seno cardinal (sinc), como se evidencia en los resultados de la **Tabla 4.1**. Aprovechando esta correspondencia

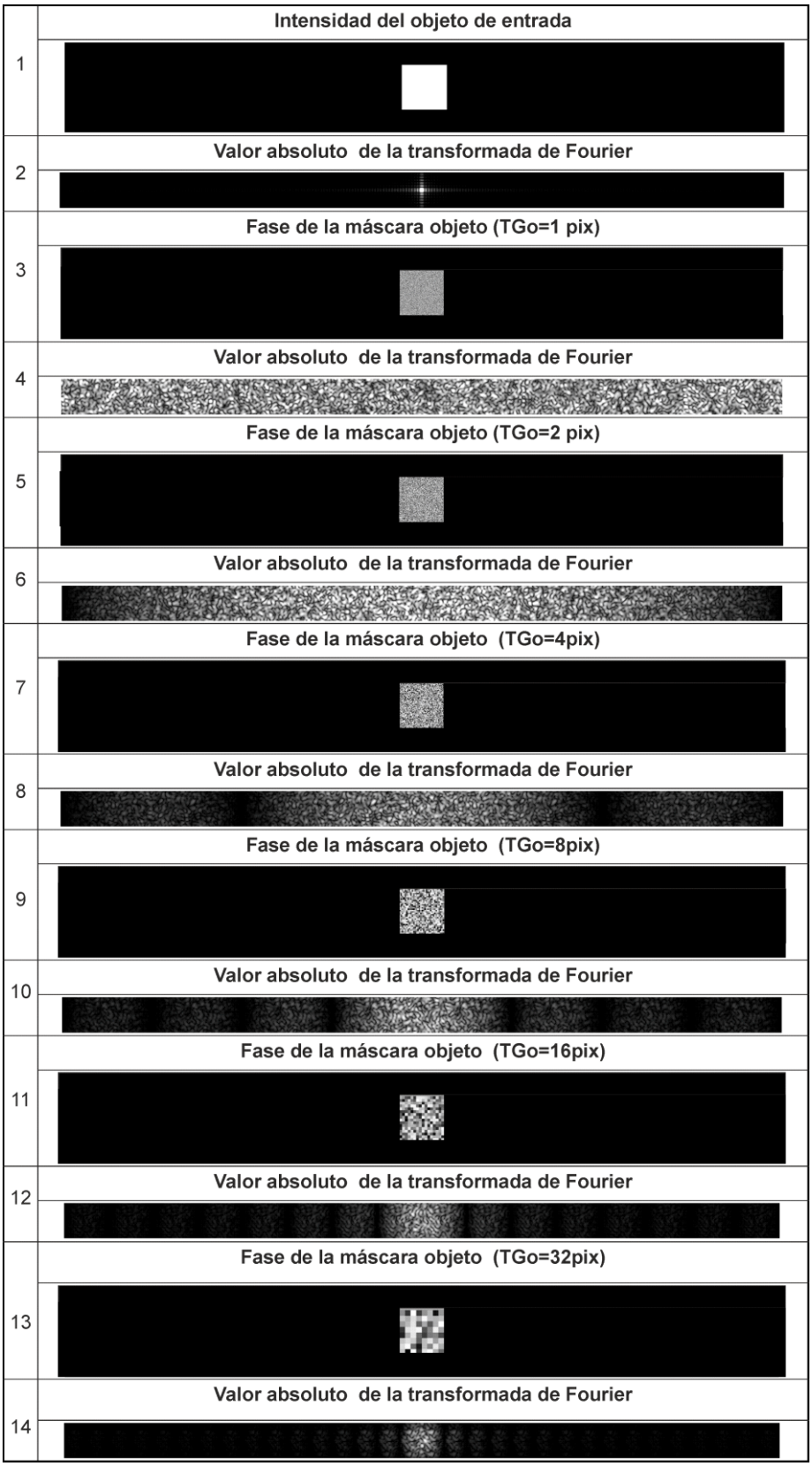


Tabla 4.1. Distribución de la información en el plano de Fourier de la imagen de entrada en función del ancho de banda de la máscara objeto.

biunívoca, se puede diseñar un elemento dispersor que tenga un perfil sinc en fase, tal que la distribución macroscópica sea un cuadrado uniforme [4.9].

IV.4.2 Diseño de una máscara objeto compuesta de elementos dispersores con perfil sinc()

Cuando una máscara de fase aleatoria compuesta de centros dispersores con perfil sinc () bidimensional (es decir, el área del centro dispersor, no es uniforme) es adosada a una imagen en intensidad, el espectro del producto será un patrón de speckle uniformemente distribuido dentro de un cuadrado (ancho de banda limitado y bien definido). Nótese que el uso de máscaras aleatorias de fase con esta característica (compuesta de centros dispersores con el mencionado perfil no produce una modulación macroscópica del espectro de la señal de entrada, como sí ocurre en los casos tratados en la Sección IV.4.1. Recordemos que la dimensión del área en el dominio de Fourier que contiene a toda la energía proveniente del plano de entrada (ancho de banda de la señal de entrada), es igual a la suma de los anchos de banda de la máscara de fase adosada al objeto y del objeto.

En la arquitectura de encriptación JTC, en nuestro caso consideraremos la señal de entrada está compuesta por la máscara objeto (solo fase) y la imagen a ser encriptada (amplitud), ambas ubicadas en una de las ventanas de entrada. Si utilizamos una máscara objeto con espectro limitado, conocido y bien definido, solo restaría conocer el ancho de banda del objeto de entrada para tener el ancho de banda de la señal de entrada. Para que toda la información del objeto esté contenida en el patrón encriptado (JPS), se requiere, que el ancho de banda de la señal de entrada sea menor ó igual al ancho de banda de la máscara llave, $(\Delta\mu_G + \Delta\mu_R\ ,\ \Delta\nu_G + \Delta\nu_R) \leq\ (\Delta\mu_H, \Delta\nu_H)$, así todo el campo que proviene del plano de entrada queda modulado por el espectro de la llave.

Los objetos a ser encriptados pueden tener diferente contenido frecuencial. Este aspecto en las publicaciones sobre técnicas ópticas de encriptación, no es tenido en cuenta [4.1-4.5]. En este capítulo se pretende obtener máscaras de fase, que produzcan la menor pérdida de información en la imagen recuperada después del proceso de

desencriptación. Si se desea encriptar imágenes con diferente contenido frecuencial en un único sistema óptico, hay que diseñar la máscara objeto y la máscara llave para que los requerimientos sobre sus anchos de banda sean cumplidos. En cambio, si se dispone una máscara objeto dada (por ejemplo un vidrio esmerilado), entonces de debe determinar su ancho de banda y limitar el sistema de encriptación a objetos de entrada con una máxima frecuencia espacial.

Es evidente que controlando el ancho de banda de la máscara objeto (máscaras diseñadas), el sistema será más flexible en cuanto a los espectros de los objetos de entrada sin perder calidad en la imagen desencriptada. Estas máscaras objeto de solo fase $r(x_0, y_0)$se van a utilizar en un sistema de encriptación JTC. Para diseñar máscaras de fase con ancho de banda limitado a un cuadrado se implementó un algoritmo iterativo de recuperación de fase [4.9]. Para su diseño se tuvieron en cuenta las siguientes condiciones:

- La fase de $r(x_0, y_0)$, debe estar acotada en el plano espacial a una ventana de tamaño igual al tamaño del objeto de entrada, es decir, deber tener un ancho de banda espacial $(\Delta \mathrm{x_{0r}}, \Delta \mathrm{y_{0r}})$. En nuestro caso se escogió a $\Delta \mathrm{x_{0r}} = \Delta \mathrm{y_{0r}} = 2.56\ \mathrm{mm}$ y $r(x_0, y_0)$=0, fuera del rango: $|x_0| \leq \frac{\Delta x_{0r}}{2}, |y_0| \leq \frac{\Delta y_{0r}}{2}$. El área de trabajo está comprendida en el rango $|x_0| \leq 10.24\ mm$, $|y_0| \leq 10.24\ mm$.

- Debe tener el ancho de banda limitado (deseado), es decir, la amplitud de su transformada de Fourier, $|R(\mu, \nu)|$, debe estar limitada al rango$(\Delta \mu_R, \Delta \nu_R)$ y $R(\mu, \nu) = 0$, fuera de él: $|\mu| \leq \frac{\Delta \mu_R}{2}, |\nu| \leq \frac{\Delta \nu_R}{2}$. Se diseñaron tres máscaras con anchos de banda limitados a $\Delta \mu_R = \Delta \nu_R = 20.48, 10.24, 5.12$ mm, respectivamente.

En la **Tabla 4.2** se presentan los resultados de las tres máscaras diseñadas con las condiciones anteriores. En la primera fila se muestra una representación en niveles de gris de la transmitancia en amplitud y en fase de las máscaras diseñadas en el plano de entrada. En la segunda fila se muestra la distribución en amplitud y en fase en el plano de Fourier correspondiente a cada una de las máscaras diseñadas con el ancho de banda indicado. Para producir estos tres espectros se usa una distribución distinta de fase en cada caso para el plano de entrada aunque visualmente no se percibe.

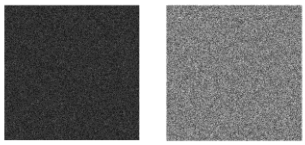
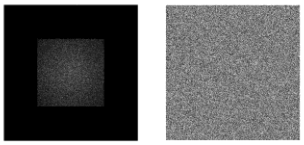
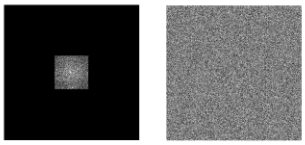
Primera máscara	Segunda máscara	Tercera máscara
Plano de entrada		
 **ANCHO DE BANDA 2,56 mm**	 **ANCHO DE BANDA 2,56 mm**	 **ANCHO DE BANDA 2.56 mm**
Plano de Fourier		
 **E=97%** **ANCHO DE BANDA 20,48 mm**	 **E=98%** **ANCHO DE BANDA 10,24 mm**	 **E=100%** **ANCHO DE BANDA 5,12 mm**

Tabla 4.2. Máscaras objeto de fase diseñadas con un ancho de banda limitado a 20.48, 10.24 y 5.12 mm, respectivamente.

Nótese que para la máscara diseñada con ancho de banda de 5,12 mm, el 97 % de la energía queda contenida dentro del ancho de banda mencionado. Por otra parte, para las máscaras con ancho de banda de 10,24 mm y 20,48 mm, el 98 % y el 100% de la energía queda contenida en dichos anchos de banda, respectivamente.

Presentamos en la **Tabla 4.3** la comparación de la información en el plano de Fourier cuando se usan máscaras con centros dispersores cuadrados (ver Sección IV.4.1) adosadas a un objeto en intensidad y aquellas en las que se emplean máscaras diseñadas de acuerdo a lo detallado, con centros dispersores con perfil sinc (), en ambos casos se emplean las máscaras objetos con ancho de banda bien definido dentro de un cuadrado.

En la **Tabla 4.3**, el objeto de entrada mostrado en la primera fila, tiene un espectro de muy baja frecuencia (ver fila 2). En las filas 3, 6 y 9, se muestran en cada caso una imagen que es una representación en niveles de gris de la máscara objeto de fase con centros dispersores cuadrados de dimensión 10, 20, 40 micras, respectivamente.

Dicha máscara es adosada al objeto de la primera fila y la amplitud de la transformada de Fourier del producto se presenta en las filas 4, 7 y 10, respectivamente. El primer cero de la envolvente de la función sinc() que modula la amplitud de las transformadas de las

imágenes de las filas 4, 7 y 10 está ubicado en las posiciones$|10.24|$, $|5.12|$ y $|2.56|$, respectivamente, en la dirección horizontal del plano de frecuencias.

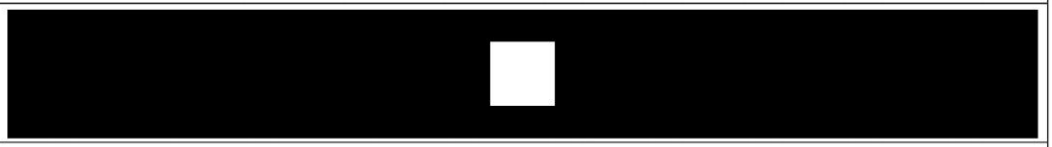
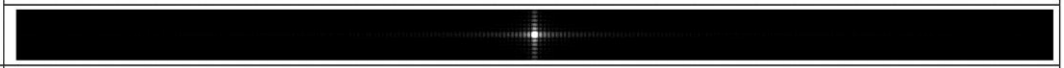
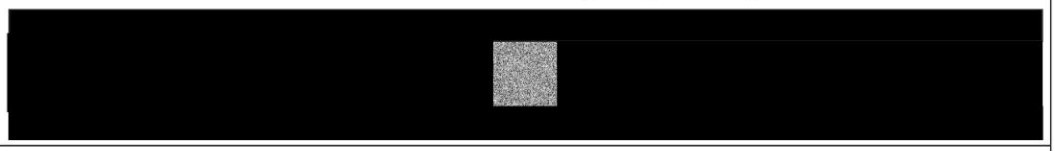
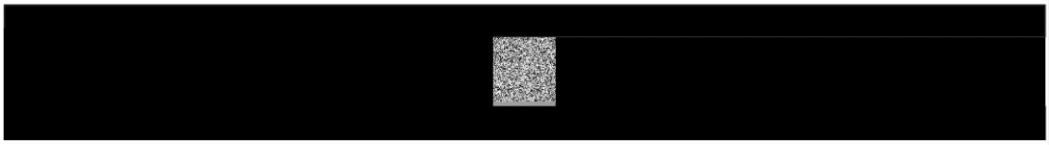
1	Objeto de entrada 
2	Valor absoluto de la transformada de Fourier 
3	Fase de la máscara objeto (TGo=2 pix) 
4	Valor absoluto de la transformada de Fourier 
5	
6	Fase de la máscara objeto (TGo=4pix) 
7	Valor absoluto de la transformada de Fourier 
8	
9	Fase de la máscara objeto (TGo=8pix) 
10	Valor absoluto de la transformada de Fourier 
11	

Tabla 4.3. Distribución de la información en el plano de Fourier cuando se usa una máscara objeto con centros dispersores: cuadrados y con perfil sinc () .

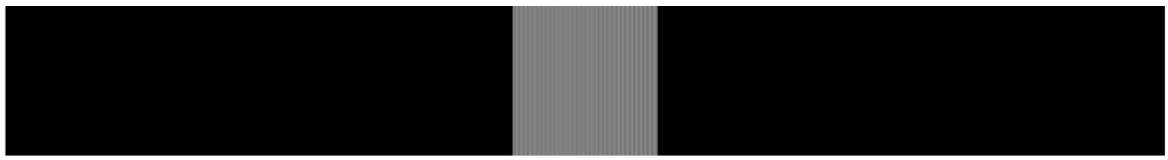
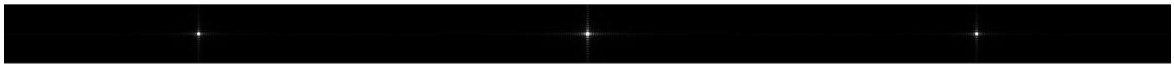
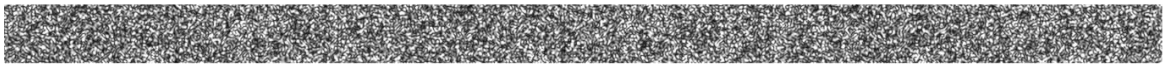
Cómo ya sabemos el lóbulo central de la función sinc() contiene el 90 % de la energía total, el resto se distribuye en los órdenes superiores. Las imágenes de las filas 5,

8 y 11 corresponden a la amplitud de la transformada de Fourier cuando se emplea las máscaras diseñadas con ancho de banda 20.48, 10.24, 5.12 mm, respectivamente. Es decir, los anchos de banda de las filas 4, 7 y 10 y las filas 5, 8 y 11 son comparables, pero es evidente que el límite está perfectamente establecido para las máscaras diseñadas (fila 5, 8 y 11) y que para las de centros dispersores cuadrados (fila 4,7 y 10) el borde no está bien definido y además la energía total contenida en el lóbulo central del sinc es menor que la energía dentro del ancho de banda de las máscaras diseñadas.

Por otro lado, si el ancho de banda de la máscara objeto es pequeño en comparación con el del objeto, la distribución de la información en el plano de Fourier puede revelar información del espectro del objeto, debido a que cada frecuencia está convolucionada con la transformada de Fourier de la máscara objeto (que se distribuye en un área con la dimensión del ancho de banda). Recordemos que en la Sección III.3.3 mostramos que a partir de cierto umbral, a medida que aumenta el tamaño de TGll se revela información del objeto en el plano de encriptación. En la arquitectura JTC el plano de encriptación es un plano de frecuencias, entonces, a medida que aumenta el tamaño de los centros dispersores de la máscara objeto (TGo), el ancho de banda de la máscara disminuye. A partir de cierto umbral, se revela información del espectro del objeto, aumentando a medida que se incrementa TGo. Para poner en evidencia este comportamiento, se presenta en la **Tabla 4.4** los espectros para una señal de entrada compuesta por una función coseno en amplitud, de paso 3 píxeles acotada en una ventana de 512 x 512 píxeles dentro de un fondo de 4096 x 4096 píxeles. Como función de fase se utilizan las máscaras diseñadas con ancho de banda limitado de 4096, 2048 y 1024 píxeles, respectivamente.

A partir de los resultados de la **Tabla 4.4** podemos verificar que cada frecuencia del espectro del objeto es convolucionada con la transformada de Fourier de la máscara de fase. Cuando se utiliza la máscara con ancho de banda de 4096 píxeles, que coincide con la dimensión del área de trabajo, la energía correspondiente a la frecuencia de orden cero se distribuye en todo el plano de Fourier. Asimismo, la energía correspondiente a las frecuencias del coseno utilizado como objeto de entrada (orden +1 y -1) se distribuye en

un área de 4096 x 4096 píxeles centrada en cada una de ellas, pero esto implica que parte de la energía de las frecuencias más altas se sale del área de trabajo.


Valor absoluto de la transformada de Fourier del objeto

Valor absoluto de la transformada de Fourier de la señal de entrada, cuando se adosa al objeto, la máscara objeto de ancho de banda:
4096 píxeles

2048 píxeles

1024 píxeles


Tabla 4.4 Ancho de banda de la señal de entrada, cuando el objeto de entrada tiene frecuencias altas y es adosado a máscaras objeto de diferentes anchos de banda.

Debido al muestreo y las propiedades de simetría del algoritmo de la transformada rápida de Fourier (FFT), en el caso digital, la energía que sale fuera del área de trabajo del lado derecho "reingresa" por el lado izquierdo del plano mientras que la de la izquierda "reingresa" por el lado derecho. *Este es un hecho muy importante a tener en cuenta cuando se comparan sistemas digitales con sistemas reales*, porque en el caso digital tenemos, por las razones anteriormente mencionadas, un ancho de banda de sistema "extendido". En el caso real, debido a la dimensión del medio de almacenamiento, la distribución de energía que excede al medio conllevaría a la pérdida de parte de la energía correspondiente a las frecuencias del coseno y esto se vería reflejado en ruido speckle en la imagen desencriptada. En el caso de la máscara de ancho de banda 2048 píxeles (penúltima fila de la **Tabla 4.4**), parte de la energía de las frecuencias laterales, aunque en una menor proporción, también se perdería. Como en el caso anterior estos datos "reingresan" en el lado opuesto de la imagen, de hecho si se observa en detalle la

imagen, se puede ver que la parte izquierda y derecha tienen un sutil aumento de energía debido a este fenómeno. En el último caso, para la máscara con ancho de banda 1024 píxeles se ve claramente, dado que la energía de cada frecuencia no se superpone con la de la otra, el efecto de la convolución entre el espectro del objeto y la transformada de Fourier de la máscara objeto. En este caso, no se perdería energía de ninguna frecuencia debido al área finita de trabajo y el caso digital sería equivalente al caso experimental.

En este punto, si bien estamos tratando la arquitectura JTC, las ideas involucradas nos permitirá entender con claridad, porqué en los sistemas de encriptación digitales basados en la arquitectura 4*f,* se obtienen imágenes desencriptadas sin pérdida de información debido al área finita de trabajo, aunque se utilicen difusores de fase donde cada píxel tiene una fase diferente, lo que implica que el ancho de banda de la máscara llave es alrededor de dos veces el área de trabajo. Si se replica la misma configuración en una simulación y en un caso real, en este último se perdería casi la mitad de la energía de la información encriptada correspondiente a los portadores de alta frecuencial.

Si bien existen otros inconvenientes en las implementaciones experimentales, el corte frecuencial debido a los anchos de banda, en los sistemas de encriptación que usan difusores de fase, representa una importante pérdida no uniforme de energía, que implica perdida de información (speckle) y esto se traduce en ruido en la imagen desencriptada. Por eso consideramos que cuando se requiere tener la menor pérdida posible de información en los sistemas de encriptación, es de vital importancia tener conocimiento sobre los anchos de banda de las máscaras, del objeto a encriptar y del sistema.

IV.4.3 Ancho de banda del objeto de entrada.

En las secciones siguientes de este capítulo, en el análisis del JTC, utilizaremos tres objetos de entrada que exhiben diferentes características. La elección de estos objetos está motivada en evidenciar que la calidad de la imagen desencriptada depende de los parámetros del sistema además de las características del objeto.

En nuestro sistema de óptica virtual, cada píxel equivale a $5\mu m$. Cada objeto de entrada tiene 512 x 512 píxeles y está embebido en un fondo de 4096 x 4096 píxeles (esta será la extensión del plano de encriptación en los casos a considerar). Una vez realizada la transformada rápida de Fourier, se procede a calcular la energía de la imagen asociadas a intervalos en el origen del plano de frecuencias, con el fin de encontrar el ancho de banda frecuencial de la imagen. En las **Figura 4.2**, **Figura 4.5** y **Figura 4.8**, se muestran: un objeto binario, un objeto de 256 niveles de gris de bajas frecuencias y un objeto de 256 niveles de gris de altas frecuencias, respectivamente**.** En las **Figura 4.3**, **Figura 4.6** y **Figura 4.9**, se muestra el espectro de los objetos mostrados en la **Figura 4.2**, **Figura 4.5** y **Figura 4.8**, respectivamente. Por último en las **Figura 4.4**, **Figura 4.7** y **Figura 4.10**, se muestran las gráficas de la energía normalizada en función de ventanas centradas en el plano de Fourier de los espectros de los objetos mostrados en la **Figura 4.2**, **Figura 4.5** y **Figura 4.8**, respectivamente.

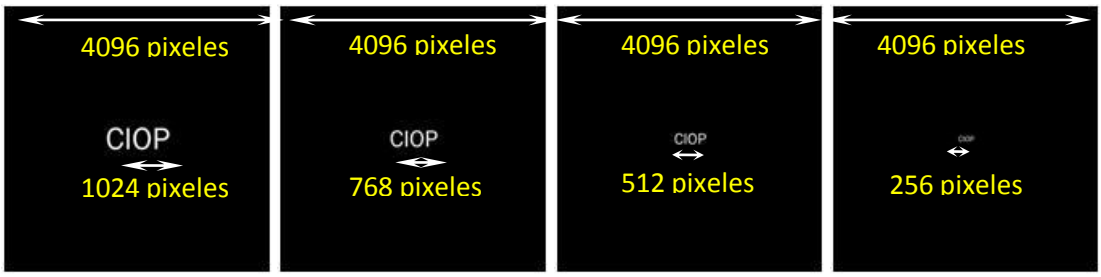


Figura 4.2. Objeto de entrada binaria de tamaño: 1024, 768, 512, 256 píxeles.

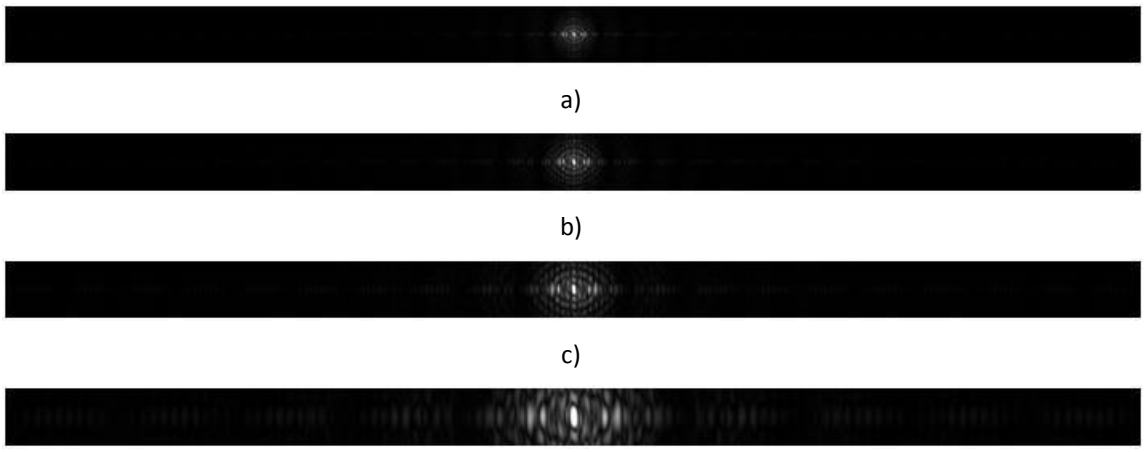


Figura 4.3 Transformada de Fourier de la imagen de la Figura 4.2. a) b) c) d) respectivamente.

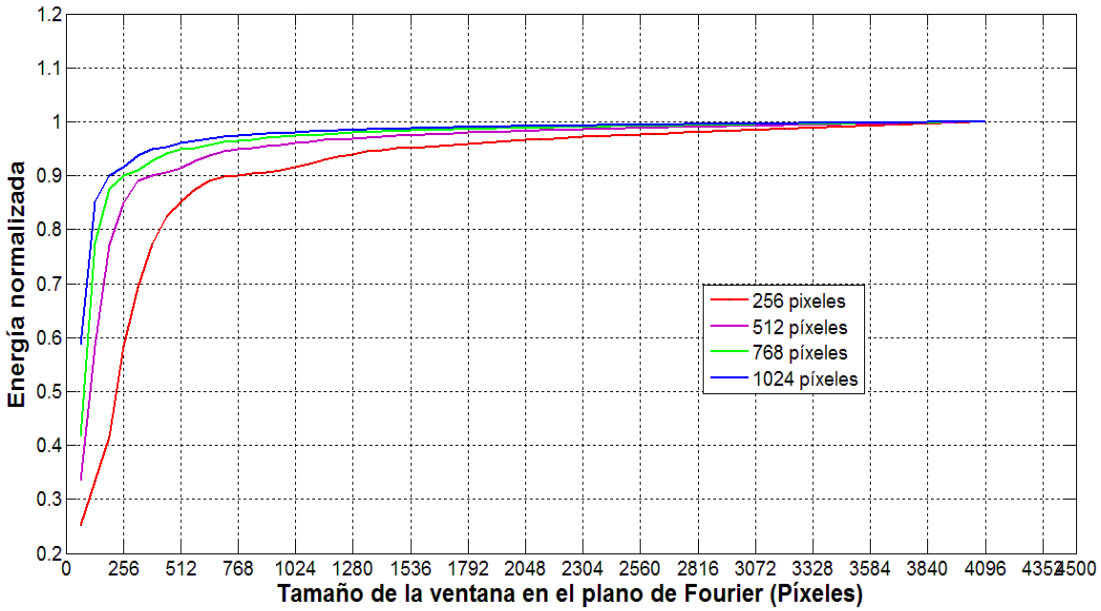


Figura 4.4. Energía normalizada de las imágenes de la **Figura 2** en función de una ventana centrada en el plano de Fourier (1 píxel= 5 µm).

A partir de los datos de la **Figura 4.4** surge que el ancho de banda de las imágenes binarias es $\Delta\mu = \Delta\nu = 3392,\ 2816,\ 2304,\ 1856$ píxeles, ya que el 99.0% de la energía total está contenida dentro de esta ventana para la imagen de 256, 512, 768, 1024 (mostradas en la **Figura 4.2**), respectivamente.

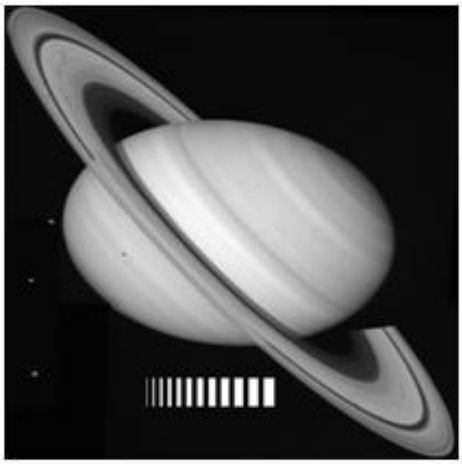


Figura 4.5. Objeto de 256 niveles de gris de bajas frecuencias.

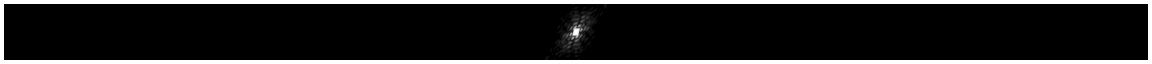


Figura 4.6 Transformada de Fourier de la imagen de la Figura 4.5.

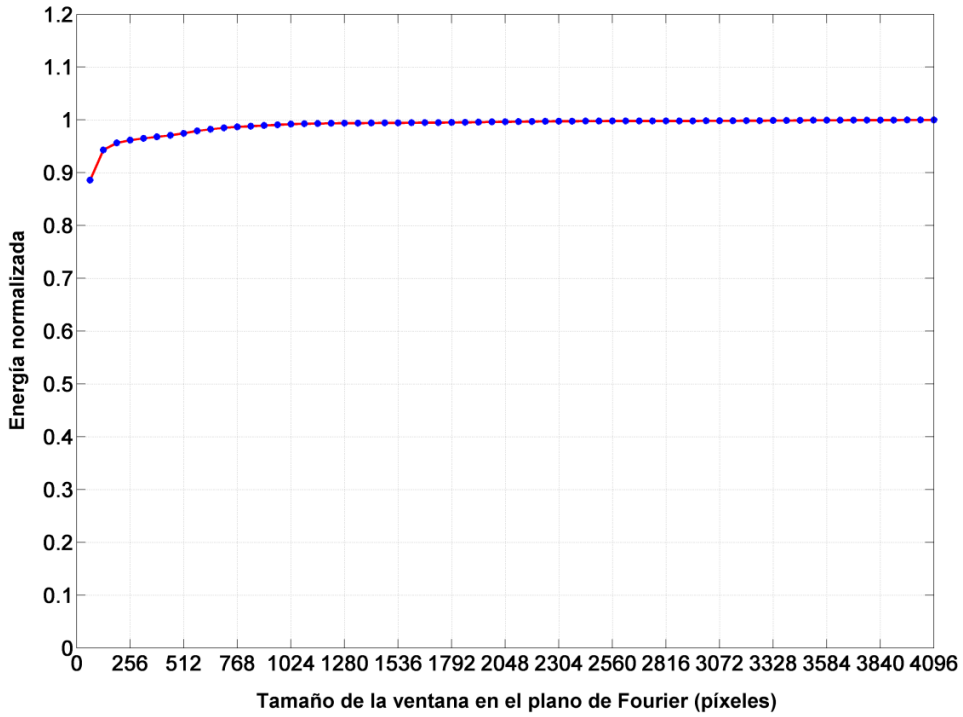


Figura 4.7. Energía normalizada de la imagen de la Figura 4 en función de una ventana centrada en el plano de Fourier.

A partir de los datos de la **Figura 4.7** surge que el ancho de banda de la imagen en niveles de gris es $\Delta\mu = \Delta\nu = 960$, dado que el 99.09 % de la energía total está contenida dentro de esta ventana.

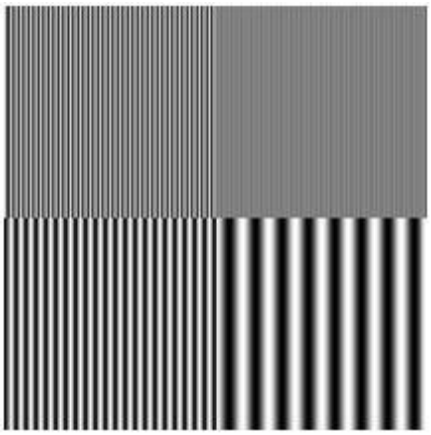


Figura 4.8. Objeto de 256 niveles de gris de altas frecuencias.

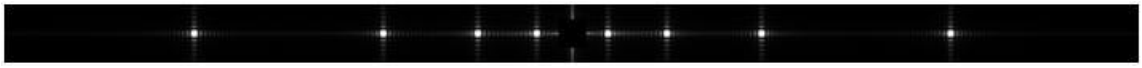


Figura 4.9. Transformada de Fourier de la imagen de la Figura 4.8

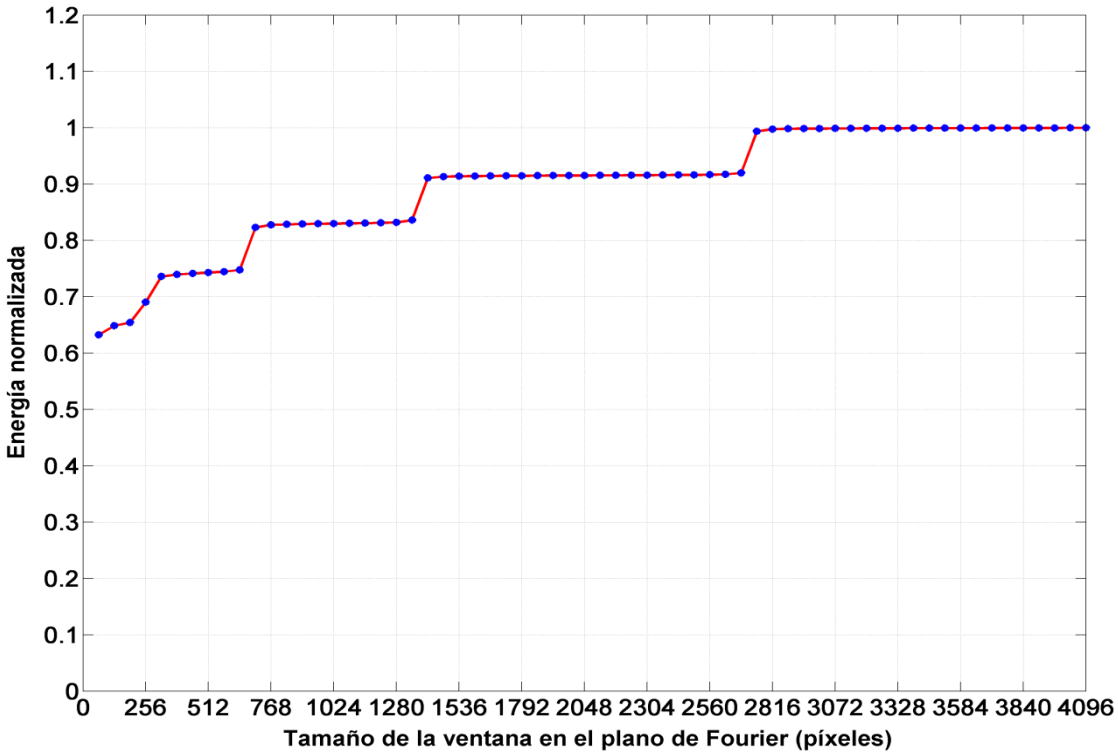


Figura 4.10. Energía normalizada de la imagen de la Figura 6 en función de una ventana centrada en el plano de Fourier.

A partir de los datos de la Figura 4.7 surge que el ancho de banda de la imagen en niveles de gris de alta frecuencia es $\Delta\mu = \Delta\nu = 2688$ píxeles, ya que el 91.98 % de la energía está contenida dentro de esta ventana.

IV.5 Efecto de la máscara llave en la distribución espacial de la información encriptada.

Recordemos que el plano de encriptación en un sistema JTC está ubicado en el plano de Fourier como se puede ver el **Figura 4.1.** En este plano interfieren el campo que emerge de las dos ventanas del plano de entrada del JTC. Dado que cada ventana tiene una máscara aleatoria de fase, el espectro conjunto (JPS) resulta en un patrón de speckle modulado. Esta distribución de intensidad descripta por la ecuación (4.10) representa la imagen encriptada.

En las simulaciones a ser presentadas se utilizan los siguientes parámetros: el tamaño del área de trabajo es de 4096 x 4096 pixeles, la resolución de pixel en la

dimensión x_0 y y_0 son de 5 μm, la longitud de onda es de 632 nm, las distancias focales, en todos los casos es igual a 162 mm, la pupila del sistema está determinada por el área de trabajo 20,48 x 20,48 mm. Una vez fijada el área de trabajo, la resolución de píxel y la longitud de onda, la distancia focal se calcula de tal manera que el área del plano de Fourier coincida con el área de trabajo.

Con los valores de parámetros utilizados para las simulaciones, el máximo tamaño de imagen que podemos encriptar sin que se superponga ruido sobre la imagen en el plano de salida es de 3,84 mm y la más pequeña es de 1,92 mm.

En la **Tabla 4.11** se muestra en la primera fila el plano de entrada de un JTC, para 4 versiones escaladas del objeto mostrado en la **Figura 4.5,** con dimensiones de 3.84, 3.20, 2.56 y 1.92 mm, respectivamente**.** En todos los casos se usa como separación entre los centros de las ventanas del JTC el doble de la dimensión de la imagen, lo cual garantiza obtener en promedio tres franjas por speckle. Esta separación también evita, que el ruido alrededor del orden cero en el plano de salida, no se superponga al orden que contiene la imagen desencriptada. En la segunda fila de la **Figura 4.5** se muestra una porción (igual para todos los casos) del JPS**,** donde se puede notar claramente que el tamaño promedio del speckle aumenta a medida que disminuye el tamaño del objeto de entrada y que el número de franjas por speckle no cambia, debido a que la separación entre las ventanas se aumenta de manera proporcional.

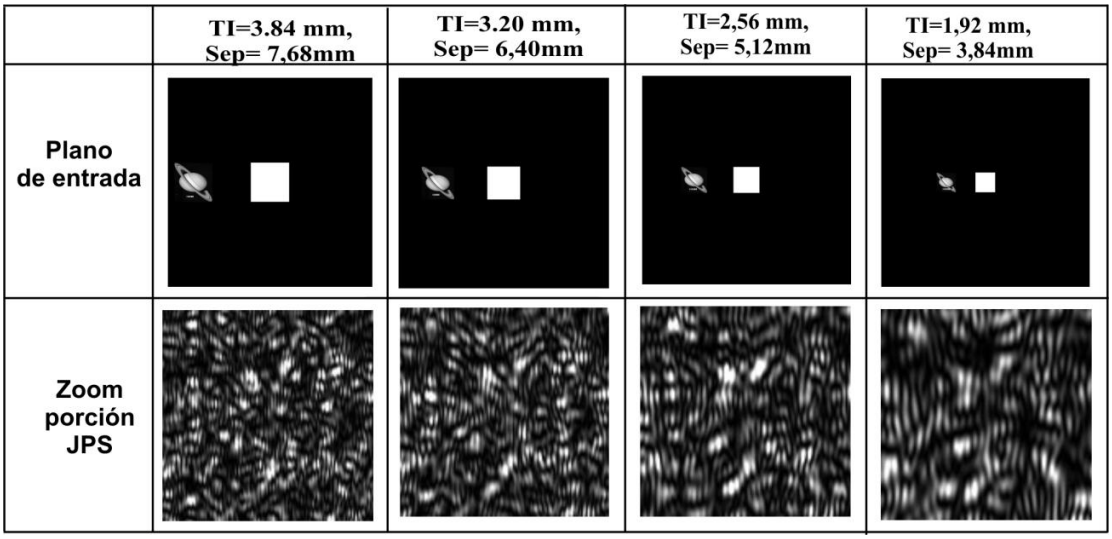


Figura 4.11. Plano de entrada del JTC y detalle de su espectro de potencia.

Para visualizar el efecto que la máscara llave (**TGll**) produce sobre la distribución del campo en el plano de encriptación, se presenta en la **Tabla 4.12** las imágenes encriptadas obtenidas mediante simulaciones en condiciones de óptica virtual en términos del tamaño de grano de la máscara llave (**TGll**) para dos tamaños de objeto de entrada.

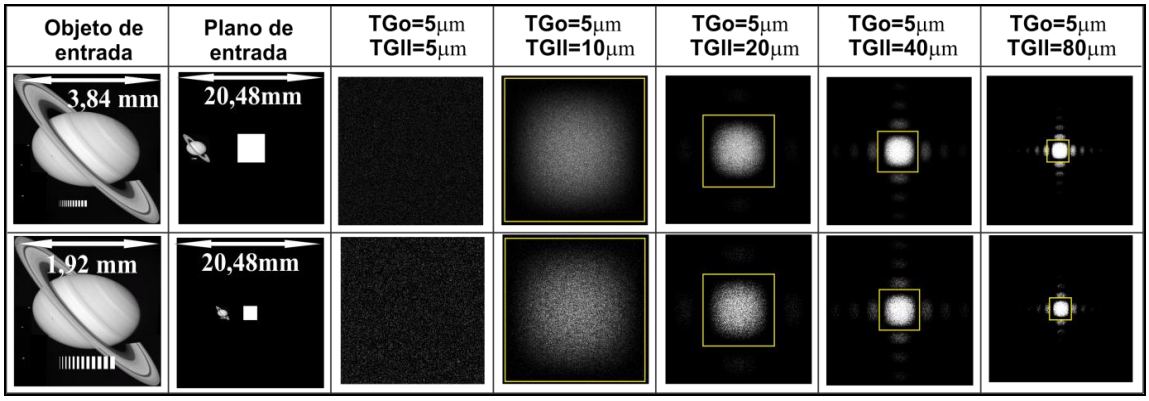


Tabla 4.12. Distribución del patrón encriptado en términos del tamaño del objeto de entrada y del **TGll**.

En los resultados mostrados en la **Tabla 4.12**, el difusor utilizado cómo máscara objeto es mantenido constante y el tamaño de los centros dispersores es de 5 μm . Esto implica que la información del objeto de entrada está distribuida en todo el plano de Fourier. Cada fila corresponde a un objeto de tamaño fijo y diferentes valores de **TGll.** A medida que se aumenta el valor de **TGll** (ver **Tabla 4.12**), la energía que proviene de la máscara llave se va distribuyendo en un área cada vez más pequeña (disminuye el ancho de banda de la máscara llave, marcada por el cuadro amarillo). Recordemos que la transformada de Fourier de la máscara llave modula al espectro de la señal de entrada que se extiende en todo el plano de frecuencias. A partir de la columna 4 de la **Tabla 4.12** la amplitud de la transformada de Fourier de la llave está contenida en un área que es más pequeña que el área del espectro de la señal de entrada. Esto significa que no toda la información del objeto queda modulada y en la etapa de lectura sólo las zonas del JPS que estén moduladas contribuyen a la imagen desencriptada y toda la información que quede por fuera del espectro de la llave será información que no aparece en los datos recuperados.

En la etapa de desencriptación, como se trató en la Sección II.4.2, la imagen encriptada (JPS) se ilumina con la transformada de Fourier de la máscara llave que se usó en la etapa de registro. El campo emergente del plano (x_1, y_1) es transformado Fourier

para obtener la salida desencriptada, representada por la ecuación (2.38). Si observamos en el plano de salida con un detector de intensidad de manera que la fase del campo complejo no se registra, se obtiene una salida como la presentada en la **Figura 4.12**. Está imagen corresponde a la salida desencriptada para el caso del JPS que se muestra en la segunda fila y tercera columna de la **Tabla 4.4**, es decir, para la imagen de 1.92 mm y un TGo=TGll= 5 μm . En la **Figura 4.12**, el recuadro amarillo marca el área de la imagen desencriptada, que se corresponde al tercer término de la ecuación (2.38). Cómo estamos observando la intensidad y $r(x_2, y_2)$ (máscara objeto en coordenadas del plano de salida), es una función de solo fase, solo nos queda el tercer término $|g(x_2, y_2)|^2$, que es la imagen en intensidad de los datos encriptados.

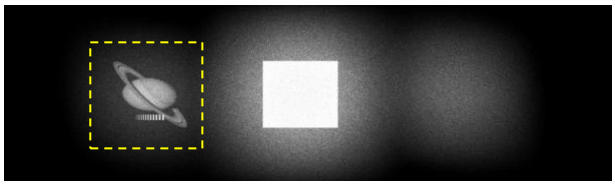


Figura 4.11. Intensidad del plano de salida para un sistema de encriptación JTC

Para visualizar el efecto que causa el aumento del tamaño de grano de los centros dispersores de la máscara llave **TGll**, se presentan en la **Tabla 4.13** las imágenes desencriptadas empleando la llave y todos los parámetros ópticos correctos correspondientes a los JPS mostrados en la **Tabla 4.12**.

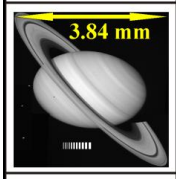
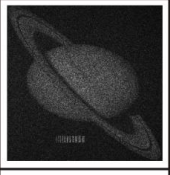
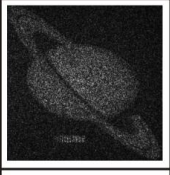
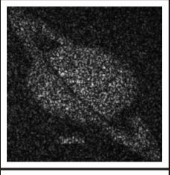
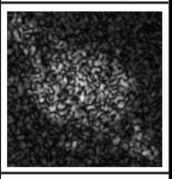
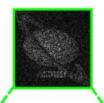
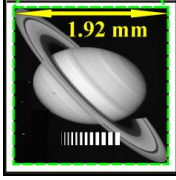
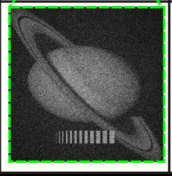
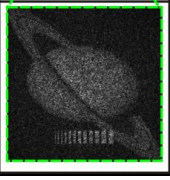
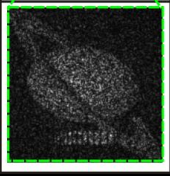
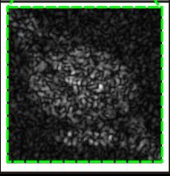
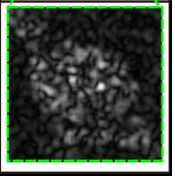
Objeto de entrada	TGo=5μm TGll=5μm	TGo=5μm TGll=10μm	TGo=5μm TGll=20μm	TGo=5μm TGll=40μm	TGo=5μm TGll=80μm
					
					
					

Tabla 4.13. Imágenes desencriptadas correspondientes a la Tabla 4.12.

En la primera y segunda fila de la **Tabla 4.13** se muestran las imágenes desencriptadas para el tamaño de objeto de 3.84 mm y de 1.92 mm, respectivamente. Para ambas filas se puede ver que a medida que aumentan las columnas (incrementa el valor de TGll) el tamaño de grano (la frecuencia espacial) del ruido de speckle aumenta también. Este comportamiento se corresponde con la disminución del ancho de banda de la máscara llave a medida que aumenta el TGll.

Para evaluar la similitud entre la imagen desencriptada (I') y la imagen de entrada (I), se calcula el coeficiente de correlación mediante la ecuación:

$$CC = \frac{\sum_x \sum_y \left(I_{x,y} - \langle I \rangle\right)\left(I'_{x,y} - \langle I' \rangle\right)}{\sqrt{\left[\sum_x \sum_y \left(I_{x,y} - \langle I \rangle\right)^2\right]\left[\sum_x \sum_y \left(I'_{x,y} - \langle I' \rangle\right)^2\right]}} \tag{4.11}$$

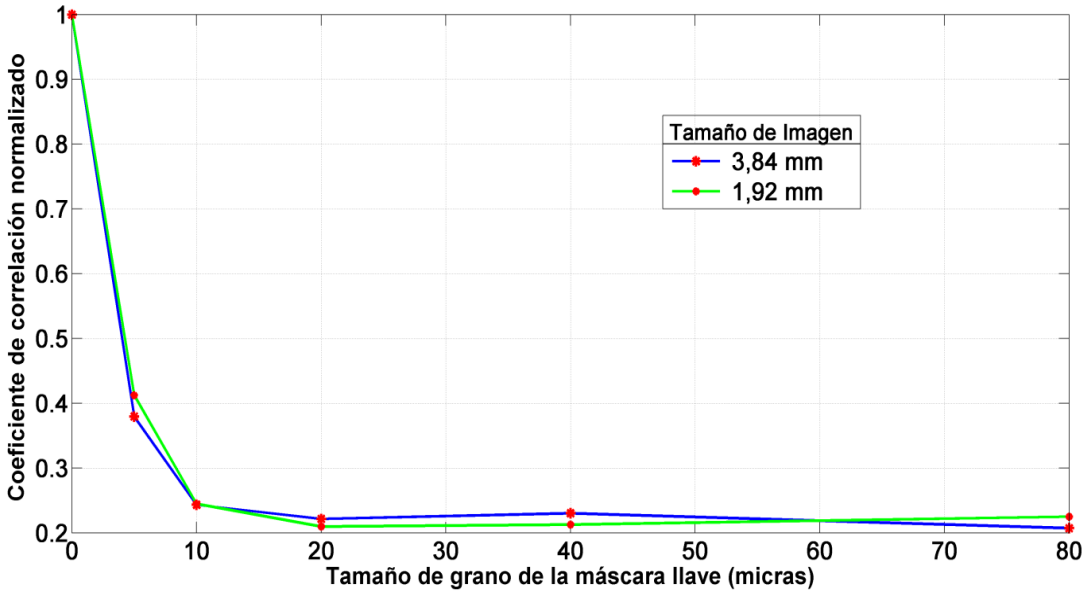


Figura 4.12. Coeficiente de correlación para las imágenes desencriptadas de la Tabla 4.13.

La **Figura 4.12** está normalizada por el valor de autocorrelación de la imagen de entrada, que está representado en el valor correspondiente al TGll= 0. Si analizamos esta gráfica, veremos que brinda el nivel de degradación de la imagen desencriptada en comparación con el objeto de entrada. Sin embargo, para las tres últimas columnas de la **Tabla 4.13** el valor del coeficiente de correlación prácticamente no varía, pero se observa que la pérdida frecuencial es mayor para la imagen de la última columna que para la penúltima y así sucesivamente. Resulta complicada la elección de un método para evaluar

la calidad de la imagen desencriptada en una arquitectura JTC, porque en nuestra opinión ni el coeficiente de correlación, ni el error cuadrático medio (MSE) representan realmente la pérdida frecuencial de información, cómo se puede evidenciar del análisis anterior. Más adelante trataremos este aspecto con más detalle.

Para cerrar esta Sección, es claro que si el ancho de banda de la máscara llave es menor que el ancho de banda de la señal de entrada, la imagen desencriptada tendrá una pérdida de información frecuencial, equivalente a un proceso de filtrado pasa bajos. Para las condiciones impuestas en esta Sección, es decir, si la información del objeto está distribuida en todo el plano de Fourier (TGo fijo en la dimensión adecuada), a medida que aumenta el TGll, la imagen desencriptada va perdiendo cada vez mas información de altas frecuencias.

En la siguiente Sección se estudiar el efecto de variar el TGo, cuando se fija el TGll y todos los demás parámetros del sistema.

IV.6 Efecto de la máscara objeto en la distribución espacial de la información encriptada.

En las secciones IV.4.1 y IV.4.2 tratamos el efecto que causa en la distribución de la información de un objeto de entrada en el plano de Fourier, el hecho controlar los centros dispersores (perfil cuadrado ó perfil con función sinc) en la máscara aleatoria de fase adosada al objeto. Por otra parte, sabemos que controlando el ancho de banda de la máscara objeto (variando el TGo), podemos controlar el ancho de banda de la señal de entrada, para un objeto dado. Ahora vamos a analizar cómo influye el cambio del TGo en la calidad de las imágenes desencriptadas. Para facilitar nuestro análisis presentamos en la **Figura 4.14** las imágenes encriptadas obtenidas mediante simulaciones en condiciones de óptica virtual en términos del tamaño de grano de la máscara objeto (**TGo**) para dos tamaños de objeto de entrada.

En los resultados mostrados en la **Tabla 4.14**, el difusor utilizado cómo máscara llave es mantenido constante y el **TGll** es de 5 μm. Cada fila corresponde a un objeto de tamaño fijo y diferentes valores de **TGo.**

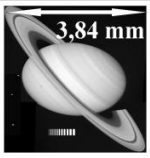
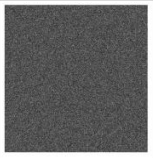
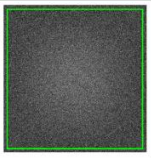
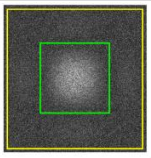
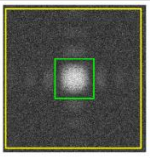
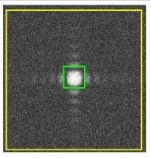
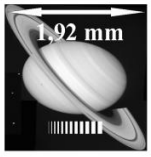
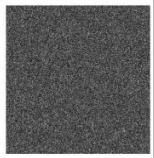
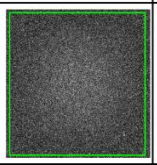
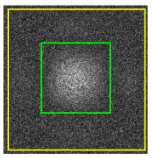
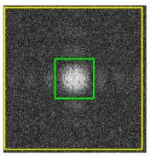
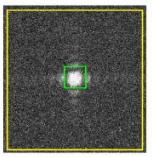
Objeto de entrada	Plano de entrada	TGo=5μm TGII=5μm	TGo=10μm TGII=5μm	TGo=20μm TGII=5μm	TGo=40μm TGII=5μm	TGo=80μm TGII=5μm
						
						

Tabla 4.14. Distribución del patrón encriptado en términos del tamaño del objeto de entrada y del **TGo**.

A medida que se aumenta el valor de **TGo**, la energía que proviene de la señal de entrada se va distribuyendo en un área cada vez más pequeña (disminuye el ancho de banda de la señal de entrada, marcada por el cuadro verde). Recordemos que la transformada de Fourier de la máscara llave modula al espectro de la señal de entrada que se extiende en un área determinada por el ancho de banda de la señal de entrada. Como el **TGII** es mantenido constante en todos los casos en 5 μm, esto implica (en las condiciones de nuestro sistema de óptica virtual) que la transformada de Fourier de la llave en todos los casos está distribuida en todo el plano de Fourier (marcado por el cuadro amarillo), luego toda la información que esté en este plano proveniente del la ventana objeto estará modulada, siempre y cuando el ancho de banda de la señal de entrada sea menor que el área del plano de Fourier, que en la **Tabla 4.14** se cumple en todos los casos. A partir de la columna 4 de la tabla anterior la amplitud de la transformada de Fourier de la señal de entrada está contenida en un área que es más pequeña que el área del espectro de la máscara llave. Para todos los casos presentados en la Tabla anterior, toda la información del objeto queda modulada. Como en la etapa de lectura sólo las zonas del JPS que estén moduladas (área común entre el recuadro amarillo y verde) contribuyen a la imagen desencriptada, entonces se espera que para estos casos no haya perdida frecuencial. En la siguiente Tabla se muestran las imágenes desencriptadas para los JPS mostrados en la **Tabla 4.14** y el coeficiente de correlación para evaluar la similitud entre la imagen recuperada y el objeto de entrada, se evalúa y su grafica se presenta en la **Figura 4.13**.

Como podemos observar a diferencia de las imágenes desencriptadas de la **Tabla 4.13**, las imágenes recuperadas no tienen perdida de información frecuencial, sin

embargo tienen un patrón de ruido superpuesto que aumenta (el tamaño de grano) a medida que disminuye el TGo. Este ruido es el patrón en intensidad no uniforme que está presente en la imágenes desencriptadas para un sistema JTC cuando la transformada de Fourier de la máscara llave no tiene amplitud uniforme. La frecuencia espacial de dicho ruido cambia porque el área del plano de Fourier que está modulada (y es la que contribuye a la difracción de los ordenes en uno de los cuales está la imagen desencriptada) disminuye a medida que aumenta TGo. El tamaño y la forma de un elemento promedio de patrón de ruido (speckle) presente en la imagen recuperada, está determinado por la transformada de Fourier la envolvente que modula el JPS en el plano de encriptación.

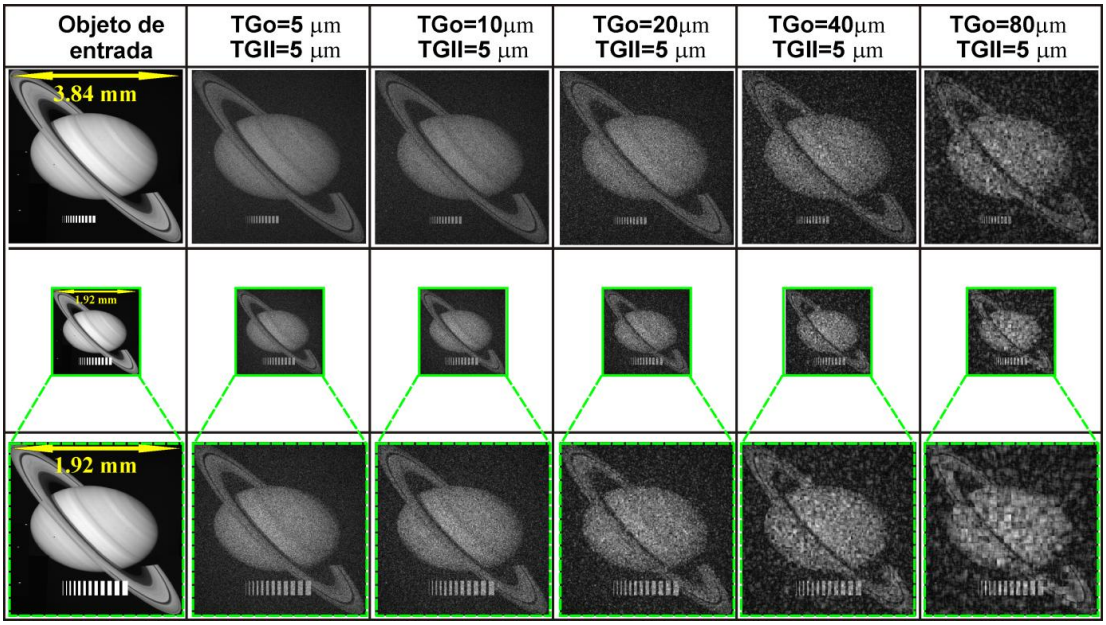


Tabla 4.15. Imágenes desencriptadas cuando se varia el TGo y el TGll se fija en 5 micrómetros.

Para los casos presentados en la **Tabla 4.15**, aunque la disminución del ancho de banda de la señal de entrada no se traduzca en la perdida de frecuencias en la imagen recuperada, el ruido debido al patrón no uniforme de la amplitud del espectro de la máscara llave deteriora la imagen desencriptada, siendo este efecto más notorio a medida que aumenta TGo. Por esta razón es conveniente ajustar el ancho de banda de la máscara objeto (TGo) de manera que no se pierda información frecuencial del objeto de entrada, pero no aumentarlo al punto que se presente en las imágenes recuperadas este patrón de ruido con una frecuencia que resulte en una "contaminación visual" en

comparación con las frecuencias espaciales del objeto, como se puede observar en las columnas finales de la **Tabla 4.15**.

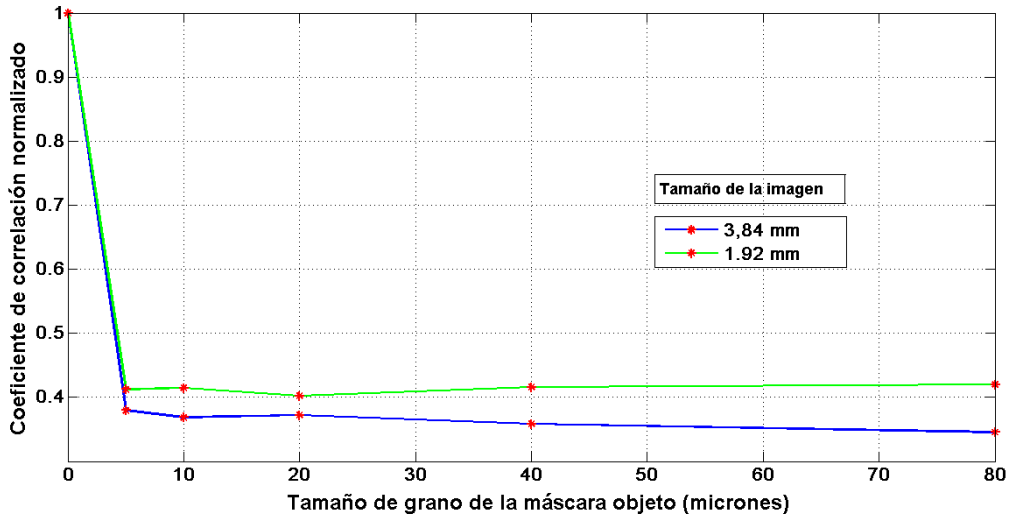


Figura 4.13. Coeficiente de correlación para las imágenes desencriptadas de la Tabla 4.13.

Enfaticemos que en este punto estamos en condiciones de obtener en el sistema de encriptación JTC imágenes desencriptadas de calidad comparables a las del 4*f.* Para ello además de cuidar todas las condiciones necesarias para que no haya pérdida frecuencial de los datos de entrada, se debe enfrentar el problema de cumplir con la condición de que la amplitud del espectro de la máscara llave sea uniforme. Si todo lo detallado se logra, la imagen desencriptada para un sistema de encriptación JTC mejorará significativamente.

IV.7 Optimización de un sistema de encriptación JTC en condiciones de óptica virtual.

En unos pocos trabajos se ha tratado el problema de optimizar la máscara llave para la arquitectura JTC. En el 2002, Nomura at al [4.4], diseñan un algoritmo iterativo que permite obtener una máscara llave optimizada (compuesta de valores de solo amplitud) para un JTC. La máscara llave así diseñadas cumple que tenga un ancho de banda limitado y que la amplitud de su transformada de Fourier sea lo más uniforme posible dentro del ancho de banda escogido. En la **Figura 4.14 a)** se muestra el objeto de entrada y la imagen desencriptada mediante el sistema JTC optimizado, lo cual confirma lo propuesto

en [4.4]**.** En el 2006 Li-Chien y Chau-Jern presentan otro diseño de máscara llave optimizada [4.5] donde se incorpora a las condiciones mencionadas en [4.4] que la máscara sea de solo fase. Esta propuesta satisface con una buena aproximación las condiciones impuestas mediante un algoritmo iterativo que busca la mejor interpolación sinc() entre los valores de fase de la transformada de Fourier de la máscara llave (la cual tiene amplitud uniforme). En este método sin embargo la fase de la transformada de Fourier de la máscara llave no es una función aleatoria uniformemente distribuida en todo el plano. El objeto de entrada y la imagen desencriptada obtenida mediante simulaciones con esta optimización se presentan en la **Figura 4.14 b**) para una imagen binaria**.**

(a)

(b)

Figura 4.14 Imágenes desencriptadas obtenidas mediante sistemas de óptica virtual JTC optimizados por: a) Nomura et al [4.4]; b) Li-Chien y Chau-Jern [4.5].

IV.7.1 Diseño optimizado de la máscara llave.

Como ya fue mencionado en la Sección anterior para optimizar el desempeño del JTC es necesario además de cumplir las condiciones sobre los anchos de banda de la señal de entrada, la máscara y el sistema, cumplir que $|H(x1/\lambda f, y1/\lambda f)$ |^2 $= 1$.

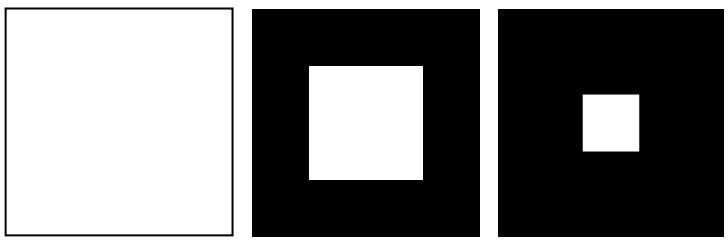
- Para lograr este objetivo, siguiendo un procedimiento similar al de la Sección 4.4.2, se implementó un algoritmo iterativo de recuperación de fase y amplitud para diseñar máscaras de fase con ancho de banda limitado a un cuadrado y

donde la amplitud de su espectro sea uniforme dentro del ancho de banda elegido. Es importante mencionar que para la máscara llave, a diferencia de la del objeto, no es una condición que sea una función de solo fase. En efecto puede ser una función compleja con amplitud, porque la imposición de solo fase es para su transforma de Fourier no para el plano espacial.

La máscara llave $h(x_o, y_o)$ se va a utilizar en un sistema de óptica virtual basado en la arquitectura JTC según las siguientes condiciones:

- la fase de $h(x_o, y_o)$, debe estar acotada en el plano espacial a una ventana de tamaño comparable al tamaño del objeto de entrada, es decir, debe tener un ancho de banda espacial $(\Delta x_{0h}, \Delta y_{0h})$ limitado. En nuestro caso se escogió a $\Delta x_{0h} = \Delta y_{0h} = 2.56$ mm y $h(x_o, y_o) = 0$, fuera del rango: $|x_0| \leq \frac{\Delta x_{0h}}{2}$, $|y_0| \leq \frac{\Delta y_{0h}}{2}$. El área de trabajo está comprendida en el rango $|x_0| \leq 10.24$mm y $|y_0| \leq 10.24$mm.
- debe tener dentro del ancho de banda en frecuencia (deseado), amplitud uniforme. Es decir que la amplitud de su transformada de Fourier sea uniforme, $|H(\mu, \nu)| = 1$, dentro del ancho de banda frecuencial elegido, $(\Delta\mu_H, \Delta\nu_H)$ y $|H(\mu, \nu)| = 0$ fuera del rango : $|\mu| \leq \frac{\Delta\mu_H}{2}$ $|\nu| \leq \frac{\Delta\nu_H}{2}$. Se diseñaron tres máscaras con $\Delta\mu_H = \Delta\nu_H = 20.48, 10.24\ y\ 5.12$ mm.
- la fase de $H(\mu, \nu)$ debe ser aleatoria y uniformemente distribuida dentro del ancho de banda frecuencial elegido.

Teniendo en cuenta las condiciones anteriores, el algoritmo utiliza una imagen objetivo para $|H(\mu, \nu)|$ a la cual designaremos como TFh_obj. En la **Figura 4.15** se presentan las TFh_obj para los anchos de banda frecuenciales deseados.



a) b) c)

Figura 4.15 Imagen objetivo para un ancho de banda de a) 20.48 mm b) 10.24 mm c) 5.12 mm

Para evaluar en el algoritmo la similitud entre el valor absoluto de la transformada de Fourier de la máscara diseñada para la N-ésima iteración $|H_N(\mu,\nu)|$ y TFh_obj, se utiliza la siguiente función de energía:

$$E = \sum_{Area\ total}\left\{|\Im\{h_N(x_o,y_o)\}| - TFh_{obj}\right\}^2 \qquad (4.12)$$

En las pruebas realizadas se minimizó el valor E incluyendo tanto los valores de fase cuanto los de amplitud en el algoritmo para $h_N(x_o,y_o)$. Es importante remarcar que no existe la restricción que $h(x_o,y_o)$ sea de solo fase ó de solo amplitud. La máscara llave optimizada asó obtenida para el sistema de óptica virtual basado en la arquitectura JTC, es una función compleja, lo cual no representa una limitación en sistemas digitales.

En la **Tabla 4.16** se presentan los resultados de las tres máscaras diseñadas con las condiciones anteriores.

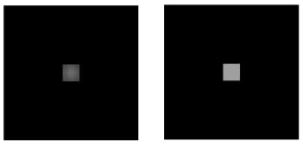
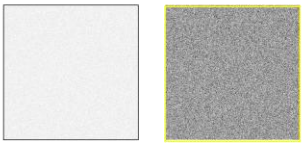
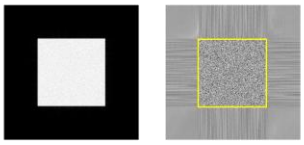
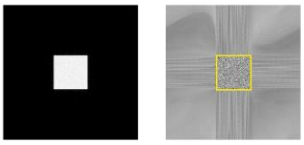
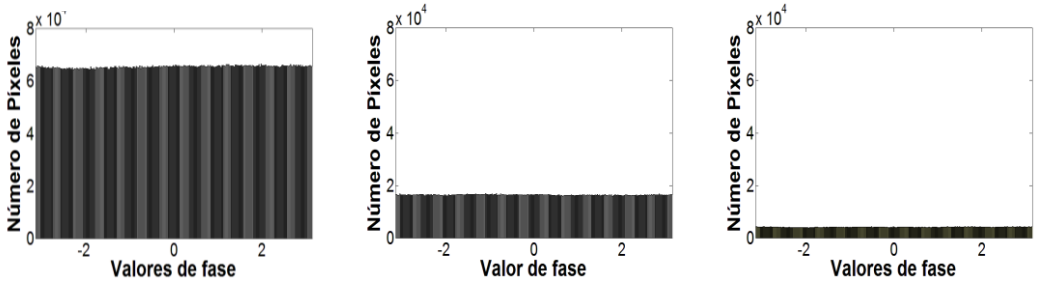
Primera máscara	Segunda máscara	Tercera máscara
Plano de entrada		
 **ANCHO DE BANDA 2,56 mm**	 **ANCHO DE BANDA 2,56 mm**	 **ANCHO DE BANDA 2.56 mm**
Plano de Fourier		
 **E=0.0363 ANCHO DE BANDA 20,48 mm**	 **E=0.0093 ANCHO DE BANDA 10,24 mm**	 **E=0.0024 ANCHO DE BANDA 5,12 mm**

Tabla 4.16. Máscaras de fase diseñadas con un ancho de banda limitado a 20.48, 10.24 y 5.12 mm optimizadas para la ventana llave de un sistema JTC virtual.

En las imágenes de la primera fila se muestra una representación en niveles de gris de la transmitancia en amplitud y en fase de las máscaras diseñadas puesta en el plano de entrada (espacial). Para los tres casos la extensión espacial de las máscaras es de 2,56 mm. En la siguiente fila se muestra la distribución en amplitud y en fase en el plano de frecuencias correspondiente a la transformada de Fourier de cada una de las máscaras diseñadas con ancho de banda de 20,48 mm para el caso de la primera columna, 10,24

mm de la segunda y 5,12 mm de la tercera. El valor de la de la función energía se indica debajo de cada imagen.

Para demostrar que la fase dentro del ancho de banda elegido de las tres máscaras está uniformemente distribuido entre $-\pi \; y \; \pi$ se presenta en la **Figura 4.16** el histograma de las fases de las máscaras diseñadas. Para el histograma solo se tuvieron en cuenta los valores de fase contenidos dentro del ancho de banda de cada máscara cuya área está marcada por el cuadro amarillo sobre las imágenes de fase de la última fila de la **Tabla 4.16**.



a) b) c)

Figura 4.16. Distribución de fase en el rango [$-\pi \; y \; \pi$], para las máscaras llave diseñadas con ancho de banda: a) 20,48 mm b) 10,24 y c) 5,12.

IV.7.2 Resultados de la optimización.

Para visualizar la potencialidad de las máscaras de fase objeto y llave diseñadas, ver Sección IV.4.2 y IV.7.1 respectivamente, para un JTC, se presenta en la **Tabla 4.17** la comparación entre las imágenes desencriptadas en un sistema de JTC virtual cuando se emplean mascaras de fase tradicionales y las optimizadas para distintos anchos de banda medios. Es evidente que el mejor resultado corresponde a la máscara optimizada con el mayor ancho de banda medio.

Por otro lado en la **Figura 4.17** se presentan los objetos de entrada y las imágenes desencriptadas mediante simulaciones para sistemas encriptación JTC virtuales optimizados por Li-Chien y Chau-Jern [4.5]. y resultado de la optimización propuesto en este trabajo.

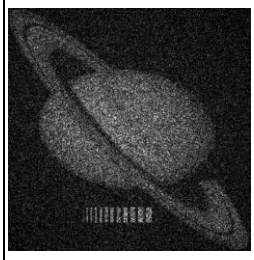
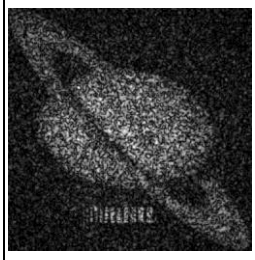
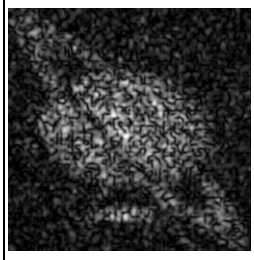
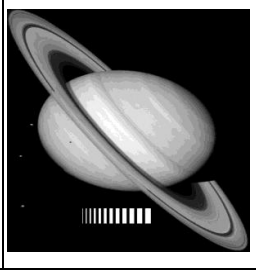
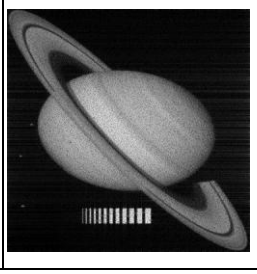
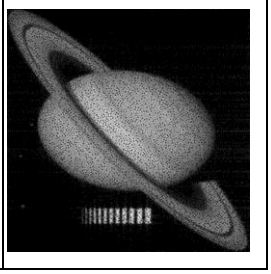
	Tamaño del centro dispersor(TGo=TGll)		
	10x10 micrones ABM=20.48 mm	**20x20 micrones ABM=10.24 mm**	**40x40 micrones ABM=5.12 mm**
JTC no optimizado			
JTC optimizado			

Tabla 4.17 Comparación entre las imágenes desencriptadas en un sistema de óptica virtual convencional (primera fila) y optimizado (segunda fila), cuando los anchos de banda de la máscara objeto y llave son iguales a 20.48 (segunda columna), 10.24 (tercera columna) y 5.12mm (cuarta columna) optimizadas para la ventana llave de un sistema JTC virtual. El tamaño de objeto de entrada es de 2.56 mm y el área de trabajo 20.48 mm para todos los casos. ABM es el ancho de banda de las máscaras llave y objeto debido al tamaño del centro dispersor que las componen.

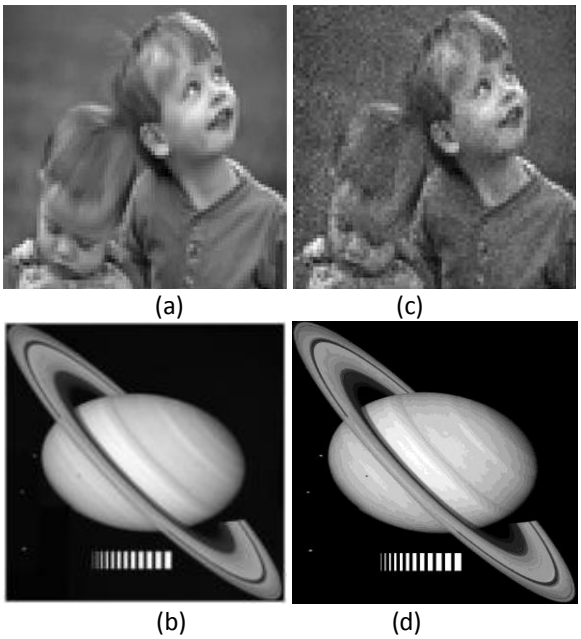


Figura 4.17 Imágenes desencriptadas obtenidas mediante sistemas de óptica virtual optimizados por: a)- b) Li-Chien y Chau-Jern [4.5], c)-d) resultado de la optimización propuesta en este trabajo

En la siguiente Sección vamos analizar el efecto que tiene en un sistema de encriptación JTC el hecho de que le medio de almacenamiento tiene un área finita.

IV.8. Efecto del tamaño finito del medio de registro en la imagen desencriptada.

En esta Sección analizaremos el efecto que produce el tamaño finito del medio de almacenamiento en las imágenes desencriptadas cuando se emplea una arquitectura de encriptación JTC.

Las imágenes desencriptadas presentados en la **Tabla 4.18** fueron obtenidas empleando en todos los casos los siguientes parámetros: el tamaño del área de trabajo es de 4096 x 4096 pixeles, la resolución de pixel en las dimensiones x e y es de 5 μm, la longitud de onda es de 632 nm, la distancia focal es de 162 mm y la pupila del sistema está determinada por el área de trabajo. Una vez fijada el área de trabajo, la resolución de píxel y la longitud de onda, la distancia focal fue elegida de manera que el área del plano de Fourier coincida con el área de trabajo. **TGll** y **TGo** se fijan en 5 μm, lo cual implica que el JPS se extienda en todo el plano de Fourier, es decir los datos encriptados están contenidos en un área de 20.48 x 20.48 mm^2. Los resultados corresponden a un sistema JTC no optimizado (columnas 2 y 4) y optimizado (columnas 3 y 5) empleado dos tipos de objetos de entrada los cuales se presentan en la primera fila de imágenes: un objeto de entrada binario (columnas 2 y 3) y un objeto en 256 niveles de gris (columnas 4 y 5).

En el optimizado se emplean las máscaras objeto y llave diseñadas con ancho de banda igual a 20.48 mm. A partir de la segunda fila se varía el tamaño del medio de almacenamiento, representado por el cuadro verde en el patrón encriptado de la primera columna. Si observamos las imágenes desencriptadas se puede observar que a medida que el área del medio de registro disminuye se va perdiendo cada vez mas información frecuencial en la imagen desencriptada. Recordemos que en esta arquitectura el plano de encriptación es un plano de frecuencias, los resultados muestran que a pesar de que la

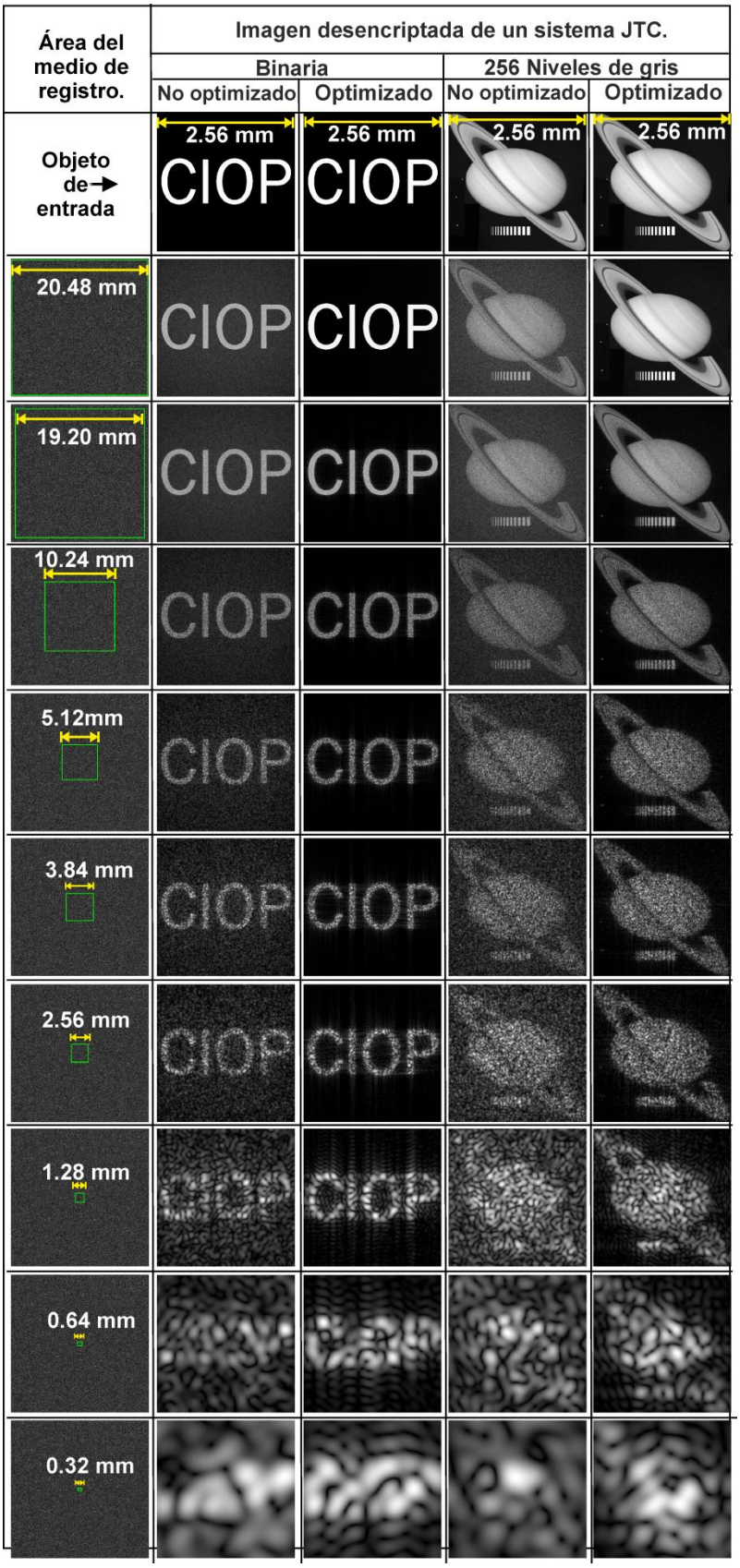


Tabla 4.18 Imágenes desencriptadas en función de la dimensión finita del medio de almacenamiento.

información esta uniformemente distribuida en un patrón aleatorio, el tamaño finito del medio de almacenamiento actúa como una ventana de filtro pasa bajos, cuando su área es menor a la del patrón encriptado. La información no almacenada en el medio de registro se ve reflejada en pérdida de frecuencias en la imagen desencriptada. El tamaño relativo entre el medio de almacenamiento y la distribución del JPS en el plano de encriptación determina como se ve afectada la información recuperada. Es evidente que cuanto mayor porcentaje de la información quede registrada en el medio de almacenamiento, mayor será el contenido en frecuencias en la imagen desencriptada.

La calidad de la imagen desencriptada en términos del objeto de entrada se evalúa mediante el coeficiente de correlación en función de la dimensión del medio de almacenamiento. Las correlaciones presentadas en la **Figura 4.18** para el objeto en niveles de gris y en la **Figura 4.19** para el objeto binario fueron obtenidas a partir de los resultados de la **Tabla 4.18**.

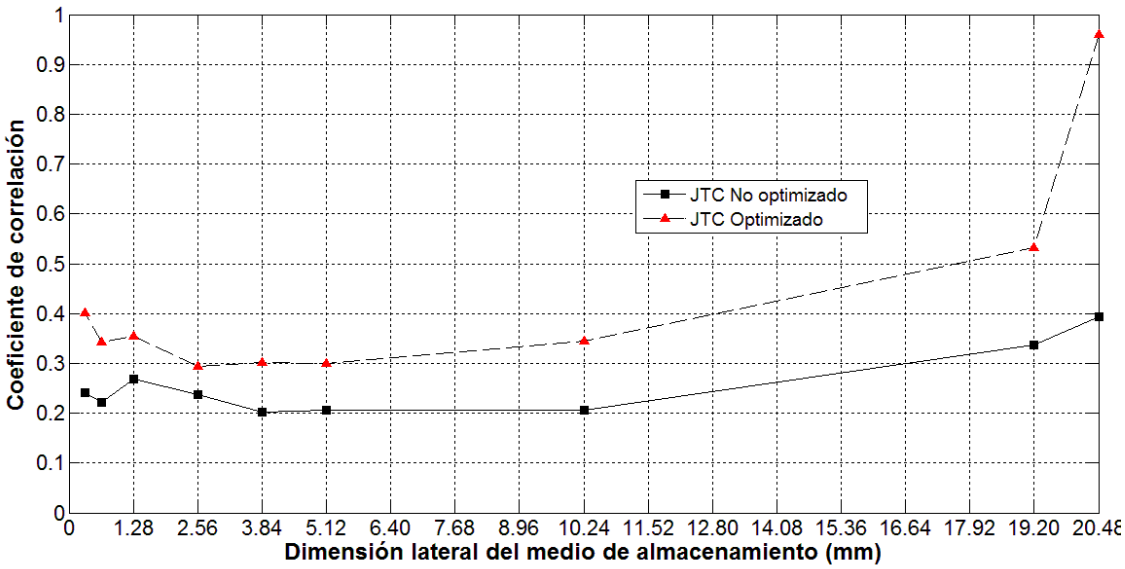


Figura 4.18 Coeficientes de correlación para la imagen desencriptada de 256 niveles de gris (Saturno) recuperada de un sistema JTC convencional y optimizado, en función del área del medio de almacenamiento.

Como se puede ver en las graficas de las **Figuras 4.18** y **4.19**, las imágenes desencriptadas con el JTC optimizado tienen mayor similitud con el objeto de entrada que las imágenes recuperadas con el JTC no optimizado y esta diferencia se acentúa para tamaños mayores del medio de almacenamiento. Por ejemplo para la imagen en niveles

de gris cuando el medio de almacenamiento (dimensión del medio 20.48) registra el patrón encriptado completo, el coeficiente de correlación entre la imagen desencriptada con el JTC optimizado es de 0.97 mientras que para la misma situación, en el JTC convencional el coeficiente de correlación es de 0.39. A medida que disminuye el área de almacenamiento, se va perdiendo información frecuencial en la imagen desencriptada para los dos sistemas, pero la diferencia entre los coeficientes de correlación disminuye. Si observamos la **Tabla 4.18**, queda en evidencia que a partir del área de 5.12 x 5.12 mm los detalles de la imagen (Saturno), lucen similares para las zonas dentro de la imagen, sin embargo para el JTC convencional aparece ruido por fuera de Saturno con la misma frecuencia espacial haciendo que se pierdan los bordes de la imagen. Este comportamiento se refleja en las curvas de correlación. También para la imagen binaria el comportamiento es similar, pero es evidente que para esta imagen, el sistema tolera un medio de almacenamiento de dimensiones menores sin que se pierda información frecuencial en la imagen desencriptada, ya que el ancho de banda de este objeto es menor que para el objeto en niveles de gris.

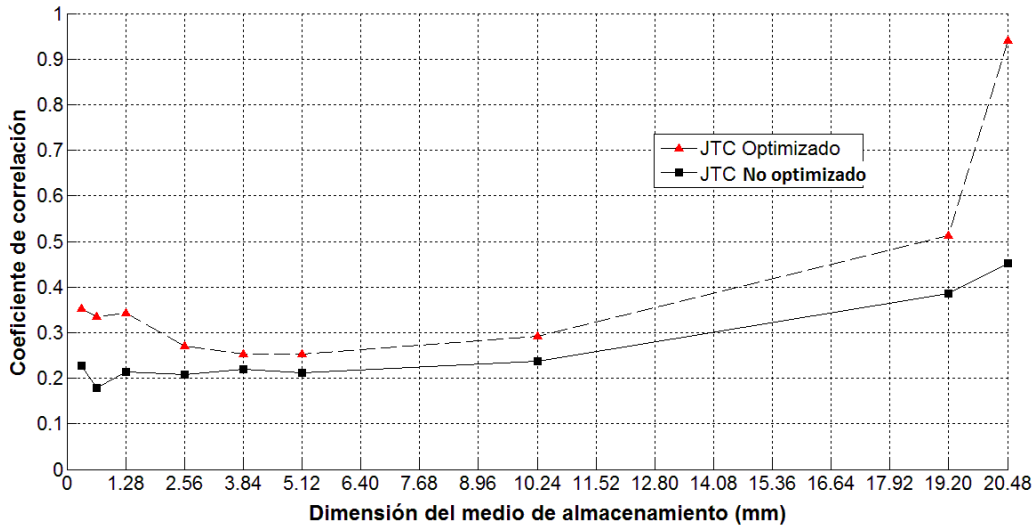


Figura 4.19 Coeficientes de correlación para la imagen desencriptada binaria (CIOP) recuperada de un sistema JTC convencional y optimizado, en función del área del medio de almacenamiento.

Para evaluar la pérdida de frecuencias en la imagen desencriptada debido al tamaño finito del medio de almacenamiento, se diseño el objeto de entrada presentado en la **Figura 4.8**. Este objeto está compuesto por cuatro cosenos de diferente frecuencia,

de manera que su espectro tiene frecuencias bien definidas. Un detalle del objeto y su espectro se muestra en la **Figura 4.20**. La dimensión de la imagen es de 2.56 mm.

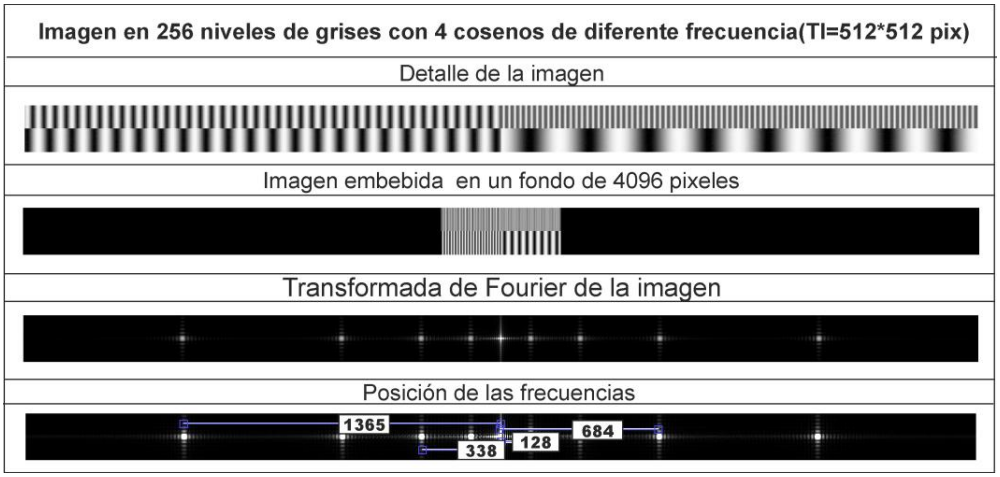


Figura 4.20 Objeto en niveles de gris con cuatro frecuencias y su espectro. TI: tamaño del objeto de entrada.

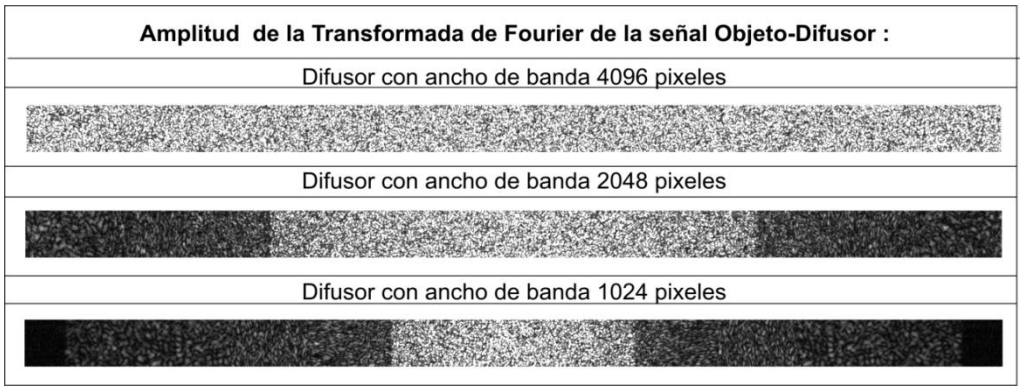


Figura 4.21 Imagen de la amplitud del espectro de la señal de entrada para el objeto presentado en la figura 4.18, cuando se le adosa una máscara objeto con distintos anchos de banda.

Al adosar al objeto de entrada una máscara de fase objeto diseñada con ancho de banda limitado, el espectro del objeto de entrada, se redistribuye como se muestra en la **Figura 4.21**. Las imágenes desencriptadas a medida que disminuye la dimensión del medio de almacenamiento se presentan en la **Tabla 4.19**. Para estudiar la pérdida de frecuencias en función del tamaño del medio de almacenamiento, se escoge la máscara objeto de ancho de banda igual a 4096 píxeles, es decir 20.48 mm. Como parámetros del sistema, se utiliza la misma configuración utilizada para las imágenes presentadas en la **Tabla 4.18**.

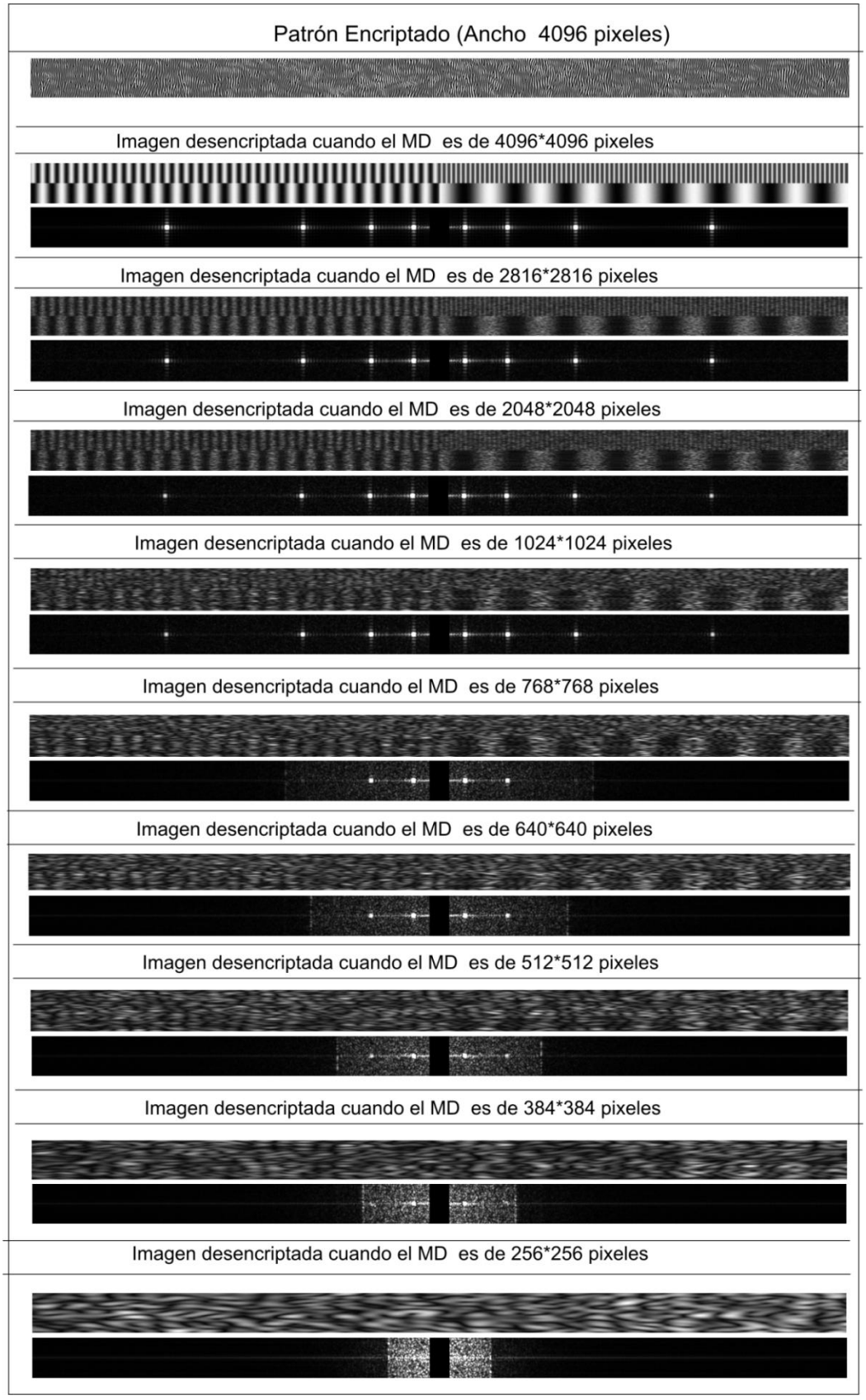


Tabla 4.19. Pérdida frecuencial debido a la dimensión del medio de almacenamiento (MD) para un objeto que contiene altas frecuencias.

A partir de estos resultados, se concluye que a medida que se disminuye el tamaño del medio de registro la imagen desencriptada perderá información correspondiente a las altas frecuencias.

Debe enfatizarse que si se requiere encriptar un objeto y se dispone de un medio de almacenamiento dado, se pueden diseñar máscaras objeto y llave con un ancho de banda acorde a la dimension del medio, teniendo en cuenta también el ancho de banda del objeto de entrada, de manera que se pierda la menor cantidad de informacion posible. Esto se puede verificar a aprtir de los resultados de la la **Tabla 4.20** donde se muestran las imágenes desencriptadas cuando se usa como objeto de entrada la imagen de Saturno (dimension 512 píxeles= 2.56 mm)

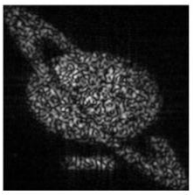
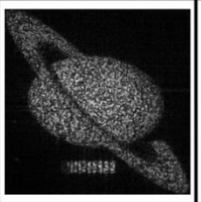
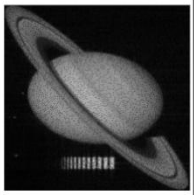
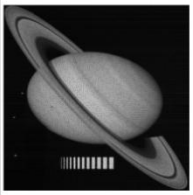
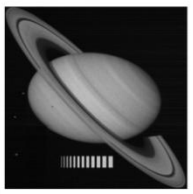
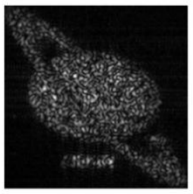
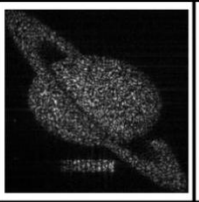
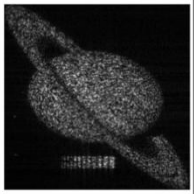
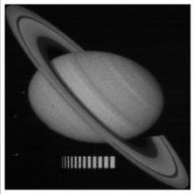
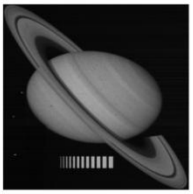
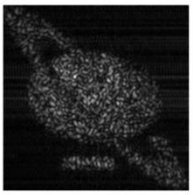
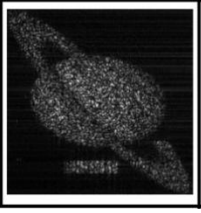
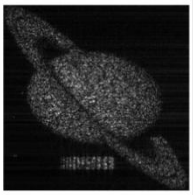
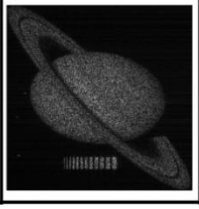
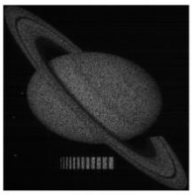
	Medio de Registro 512*512	Medio de Registro 768*768	Medio de Registro 1024*1024	Medio de Registro 2048*2048	Medio de Registro 3072*3072
Ancho de banda máscara objeto 1024*1024					
Ancho de banda máscara objeto 2048*2048					
Ancho de banda máscara objeto 4096*4096					

Tabla 4.20 Imágenes desencriptadas en un sistema JTC optimizado, cuando se varia el tamaño relativo del ancho de banda de la señal de entrada (mediante el ancho de banda de la máscara objeto) y la dimensión del medio de almacenamiento

Los resultados de la **Tabla 4.20** son obtenidos empleando los mismos parámetros ópticos que en los casos anteriores. La dimensión del área de trabajo es de 20.48 mm equivalente a 4096 pixeles para nuestra simulación. Cada columna de la tabla representa un tamaño fijo de medio de almacenamiento. Se utilizó para todos los casos la misma máscara llave, la cual se diseñó con un ancho de banda igual a 20.48 mm para el JTC optimizado. En este caso, toda la información dentro de esta área queda modulada. Cada

fila corresponde a un ancho de banda diferente de la máscara objeto y de esa forma modificar el ancho de banda de la señal de entrada y controlar el área del plano de encriptación que va a contener la información del objeto encriptado. A medida que incrementan las filas, el espectro de la señal de entrada se distribuye en un área cada vez mayor. La relación entre el área del medio de almacenamiento y el área que contiene la información de la señal de entrada, determina si hay pérdida frecuencial ó no. En la primera fila de la Tabla, las imágenes desencriptadas cuando se utiliza un medio de almacenamiento de una dimensión mayor a 5.12 mm, no sufren pérdida de frecuencia, ya que toda la información del objeto está contenida dentro de esa área. Para la segunda fila está condición se logra cuando el medio de almacenamiento supera los 10.24 mm. En cambio, para la tercera fila no se alcanza a conseguir esta situación, debido a que la máxima dimensión del medio de registro que utilizamos fue de 15.36 mm y los datos encriptados para este caso están distribuidos en un área de 20.48 mm.

IV.9 Conclusiones

De la misma forma que en el capítulo III se establecieron las condiciones necesarias de los anchos de banda de las máscaras llave, objeto y del objeto de entrada, para que toda la información de la señal de entrada quede contenida en el patrón encriptado en la arquitectura JTC.

Por otro lado, se analizó el rol que desempeñan el tamaño de los centros dispersores de las máscaras llave y objeto en la distribución de la información en el plano de encriptación y cómo esto afecta la calidad de la imagen desencriptada.

En la arquitectura JTC la información encriptada se registra en un plano frecuencial. La información encriptada es el JPS del plano de entrada y consiste en un diagrama de speckle modulado en las regiones que ambos patrones (el espectro de la señal de entrada objeto y de la llave) se interceptan. La extensión en la cual se distribuye la información del objeto de entrada en el plano de Fourier, está determinada por el ancho de banda de señal de entrada. Mientras que para el campo que proviene de la ventana llave la extensión está determinada por el ancho de banda de la máscara llave. Se determinó que

si el ancho de banda de la máscara llave es menor que el ancho de banda de señal de entrada, la imagen desencriptada tendrá pérdida de información frecuencial, equivalente a un proceso de filtrado pasa bajos, incluso si el área del medio de almacenamiento contiene al área en la cual está distribuida la señal de entrada. Se probó que este mismo proceso tiene lugar si el área del medio de registro es menor que el patrón de speckle modulado. Se demuestra que la menor dimensión entre el ancho de banda de la máscara llave y el medio de registro en relación al área determinada por el ancho de banda de la señal de entrada, determina la máxima frecuencia espacial de la imagen desencriptada y es a su vez la frecuencia espacial del ruido speckle. Esto tiene una implicancia crucial en la calidad de imagen desencriptada, provocando un rápido deterioro de la información a medida que el área del medio de registro (ó el ancho de banda de la máscara llave) disminuye. Este estudio nos permite afirmar que para preservar la información de alta frecuencia y la distribución en niveles de gris en la imagen desencriptada en esta arquitectura se debe optimizar el registro del patrón encriptado. Estos estudios permitirán diseñar adecuadamente los esquemas experimentales para evitar el deterioro de la información desencriptada.

Se demuestra que a diferencia de la arquitectura 4*f*, para esta arquitectura aunque se registre la información completa del plano de encriptación, la imagen desecriptada presenta ruido speckle. Se demuestra que el origen de este ruido se debe a que no se cumple con la condición teórica de que la amplitud del espectro de la máscara llave sea uniforme. En ese sentido, si no se utiliza una máscara llave optimizada, a lo sumo este ruido puede controlarse de tal manera que su tamaño en comparación con las frecuencias espaciales del objeto, sea de alta frecuencia. Como una alternativa a este problema, se propone para la implementación digital del JTC, una arquitectura optimizada que se basa en el diseño de una máscara llave adecuada para la perfecta recuperación de la imagen desencriptada, como supone el análisis teórico. Con esta versión optimizada, se logra tener imágenes de salida comparables en ambas arquitecturas.

Por último, se demostró que cuando se tiene un medio de registro dado (menor que en ancho de banda de la máscara llave), se puede controlar la relación entre el área de dicho

medio y el área que contiene la información de la señal de entrada, ajustando el ancho de banda de la máscara objeto. Esto se debe a que dicha relación determina la pérdida frecuencial.

IV.10 Referencias

[4.1] T Nomura and B Javidi. “Optical encryption using a joint transform correlator architecture”, Opt. Eng. 39, 2031–2035 (2000).

[4.2] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical Encryption System That Uses Phase Conjugation in a Photorefractive Crystal", Appl. Opt. 37, 8181-8186 (1998).

[4.3] B. Javidi, G. Zhang, and J. Li, “Experimental demonstration of the random phase encoding technique for image encryption and security verification”, Opt. Eng. 35, 2506–2512 (1996).

[4.4] T. Nomura, S. Mikan, Y. Morimoto y B. Javidi. ”Secure optical data storage with random phase key codes by use of a configuration of a joint transform correlator”, Appl. Opt. 42, 1508-1514 (2003).

[4.5] Li-Chie and Chau-Jern. “Optimal Key mask desing for optimal encryption based on joint trasform correlator architecture”. Opt. Comm. 258, 144–154 (2006).

[4.6]R. Henao, E. Rueda, J. F. Barrera, and R. Torroba, “Noise-free recovery of optodigital encrypted and multiplexed images”, Opt. Lett. 35, 333-335 (2010).

[4.7] D. Amaya, M. Tebaldi, R. Torroba, and N. Bolognini, "Multichanneled encryption via a joint transform correlator architecture", Appl. Opt. 47, 5903-5907 (2008).

[4.8] M. Tebaldi, A Lencina y N. Bolognini. “Analysis and applications of the speckles patterns registered in a photorefractive BTO crystal”, Opt. Comm. 202, 257–270 (2002).

[4.9] T. Nomura, E. Nitanai, T. Numata and B. Javidi, “Design of input phase mask for the space bandwidth of the optical encryption system”, Opt. Eng. 45, 017006 (2006).

[4.10] E. Rueda, J. F. Barrera, R. Henao and R. Torroba, “Lateral shift multiplexing with a modified random mask in a JTC encrypting architecture”, Opt. Eng. 48, 027006 (2009).

[4.11] E. Rueda, C. A. Vera, B. Rodrıguez and R. Torroba, “Synchronized chaotic phase masks for encrypting and decrypting images”, Opt. Comm. 281, 5750−5755 (2008).

[4.12] E. Rueda, J. F. Barrera, R. Henao and R. Torroba, “Optical encryption with a reference wave in a joint transform correlator architecture,” Opt. Comm. 282, 3243-3249 (2009).

[4.13]R. Henao, E. Rueda, J. F. Barrera, and R. Torroba, "Noise-free recovery of optodigital encrypted and multiplexed images" , Opt. Lett. 35, 333-335 (2010).

CAPÍTULO V

Almacenamiento múltiple de información encriptada

V.1 Introducción

La multiplexación es un procedimiento muy empleado en telecomunicaciones que consiste en combinar dos o más canales de información en un único medio usando un dispositivo llamado multiplexor. Multiplexar es la transmisión simultánea de varios canales de información separados en el mismo circuito de comunicación sin que interfieran entre sí. Cuando la transmisión llega al usuario se requiere realizar el proceso inverso que se conoce como demultiplexación, con el fin de separar la información correspondiente a los canales independientes. Si existe algún tipo de acoplamiento entre dos (ó más) canales de transmisión, cuando se recupere la información deseada aparecerá además de los datos correctos los que corresponden a otros canales. A este efecto no deseado se lo conoce como "cross-*talk*" ó solapamiento. El objetivo de multiplexar información es compartir la capacidad de transmisión de datos sobre un mismo enlace para aumentar la eficiencia, minimizar la cantidad de líneas físicas requeridas, maximizando el uso del ancho de banda del enlace. El multiplexado de información no solo se emplea en el campo de las telecomunicaciones. Al observar el holograma de seguridad de una tarjeta de crédito, se puede ver que la imagen cambia a medida que cambiamos el ángulo de visión ó de iluminación, lo que implica que hay almacenado en el mismo soporte físico más de un holograma.

El procedimiento de multiplexar datos también se ha empleado en óptica con el fin de aprovechar la capacidad de almacenamiento de algunos tipos de memorias ópticas. Por ejemplo, cuando se requiere almacenar múltiples hologramas en un cristal fotorrefractivo (memoria óptica de volumen), es usual emplear el multiplexado angular

(diferente ángulo de registro para cada dato)[5.1]. La alta selectividad angular de esos medios de registro permite reconstruir selectivamente y sin solapamiento cada uno de los datos multiplexados.

Con el fin de incrementar la seguridad de la información a ser transmitida, como ya fue mencionado en capítulos anteriores, se emplea el esquema de encriptación con doble máscara de fase. En este caso, la información encriptada es esencialmente un patrón de speckle. C. C. Sun et al [5.2] demuestran que los patrones encriptados almacenados holográficamente en un material fotorrefractivo de volumen, presentan selectividad al desplazamiento horizontal del difusor utilizado para codificar la información. Posteriormente, C. C. Sun et al [5.3] demuestran que los datos encriptados presentan selectividad al desplazamiento tridimensional del difusor y no sólo lateral. En Ref [5.4], C. C. Sun et al. proponen un algoritmo para el almacenamiento múltiple de información encriptada utilizando multiplexado angular y el desplazamiento del difusor. Se muestran resultados experimentales de multiplexado de ocho patrones en un cristal fotorrefractivo (tres se almacenaron utilizando multiplexado angular y cinco mediante el desplazamiento lateral del difusor). En este trabajo se demostró que se aumenta la capacidad de almacenamiento en un cristal fotorrefractivo cuando se registran patrones de ruido blanco y se multiplexan mediante el desplazamiento del difusor.

O. Matoba y B. Javidi proponen un dispositivo de encriptación que emplea dos máscaras de fase aleatorias en el dominio de Fresnel [5.5] ubicadas entre el plano del objeto de entrada y el cristal. En esta propuesta el parámetro que permite multiplexar es la posición longitudinal de los difusores. En la etapa de desencriptación si los difusores no están ubicados exactamente en la misma posición que tenían en la etapa de registro, no se compensan las fases aleatorias introducidas en la posición de la etapa registro y como consecuencia no se puede recuperar los datos de entrada.

Posteriormente, aprovechando la dependencia del speckle de otros parámetros ópticos como la polarización, la longitud de onda, etc se desarrollaron otras técnicas de multiplexado [5.6-5.7, 5.9]. La óptica tiene muchos grados de libertad que pueden ser usados como parámetros de multiplexado, sin embargo es necesario estudiar para la arquitectura óptica elegida, la viabilidad de dicho parámetro. Por ejemplo, mientras que

para una arquitectura 4*f*, pequeños desplazamientos laterales de la máscara llave permiten el almacenamiento de múltiples datos encriptados, para el JTC no es un parámetro adecuado debido a la invariancia ante traslaciones inherente a esta arquitectura. Otro aspecto muy importante que debe ser tenido en cuenta, es la sensibilidad del parámetro elegido, es decir, el mínimo cambio que se debe producir, para garantizar que no haya solapamiento entre la información de canales adyacentes.

Esta problemática surge cuando se registran múltiples datos encriptados en un único medio en N canales distintos y se desencripta la información de un canal. La información no desencriptada de los N-1 canales restantes aparece solapada como ruido a la imagen recuperada del canal. Naturalmente el ruido en los datos recuperados aumenta cuando se incrementa la cantidad de canales, al punto que para un número dado de patrones encriptados no se puede reconocer el dato recuperado en un determinado canal. Esto impone un límite, determinado por la relación señal ruido tolerable, en el número de patrones encriptados que pueden ser multiplexados, para una dada configuración.

En resumen, la dificultad esencial de los procesos de multiplexado radica en que un aumento en el número de datos encriptados incrementa el ruido en la información desencriptada, limitando así la cantidad de datos a ser codificados ópticamente. Para solucionar este problema, recientemente se han propuesto diversas alternativas [5.13, y 5.25]. Ambas propuestas se basan en estrategias de reposicionado. En la Ref. [5.13], los datos encriptados son modulados mediante una red sinusoidal y posteriormente son multiplexados en un único medio. La modulación permite eliminar el ruido durante la desencriptación a través de la separación de los datos encriptados. Basados en esta idea Mosso et al. [5.14], proponen encriptar ópticamente fenómenos dinámicos tales como videos monocromáticos y a color en una arquitectura basada en el correlador 4*f*.

Otro aspecto que aumenta el interés en las técnicas de multiplexado se relaciona con la posibilidad de trasmitir gran cantidad de información en un único paquete, reduciendo en consecuencia el peso del paquete en comparación con el peso de cada envío individual [L. Cabezas et al. [5.15]].

En este capítulo se presenta un estudio de la capacidad de multiplexado en los sistemas de encriptación basados en las arquitecturas 4*f* y JTC en función del tamaño del objeto de entrada. Asimismo, se analiza la implementación del multiplexado en longitud de onda para una arquitectura JTC [5.10] y su aplicación para la encriptación de imágenes a color [5.11]. Se presenta un método de evaluación de la sensibilidad de la longitud de onda para el multiplexado y se exhiben resultados experimentales [5.12]

V.2 Capacidad de multiplexado.

En la actualidad es de interés almacenar múltiple información encriptada en un único medio. Es evidente que si se emplea una memoria de volumen (cristales fotorrefractivos) es posible multiplexar gran cantidad de información, sin embargo resulta de interés estudiar si es posible multiplexar datos encriptados cuando se emplea un medio de registro plano (cámaras digitales). Es pertinente avanzar sobre el estudio de los mecanismos que hacen posible en este último caso el multiplexado. En ese sentido, estudiaremos la redundancia de los patrones encriptados que permitirá aprovechar al máximo la capacidad de almacenamiento (es decir, multiplexar la máxima cantidad de información que el sistema tolere).

En el capítulo III y IV analizamos la degradación en la imagen desencriptada debido a la pérdida de información encriptada que produce el área finita del medio de registro. Se demostró que no es necesario disponer del 100% del patrón encriptado para obtener en la etapa de desencriptación una imagen reconocible del objeto de entrada. En esta Sección se determinará la mínima porción del patrón encriptado (seleccionado de manera aleatoria) necesaria para recuperar una imagen reconocible. Para lograr este objetivo se diseñó una serie de pruebas utilizando como objeto de entrada imágenes binarias escaladas. Una vez determinado el mínimo porcentaje de datos encriptados necesario para obtener una información reconocible, se lo vinculará con la "capacidad de multiplexado", es decir la cantidad de imágenes (canales de encriptación) que un dado sistema óptico permite almacenar y recuperar. Debemos mencionar que los datos desencriptados en estos casos contienen ruido y bajo contraste, sin embargo mediante

operaciones que realcen el brillo y el contraste es posible reconocer la información desencriptada. Estos estudios se realizarán para las arquitecturas de encriptación 4*f* y JTC.

V.2.1. Estudio de la redundancia de información como herramienta para predecir la capacidad de multiplexado.

En esta Sección se determinará en las arquitecturas de encriptación 4*f* y JTC el menor porcentaje de información encriptada necesario para que la imagen desencriptada sea reconocible. Para nuestro análisis se emplean como objetos de entrada distintas imágenes binarias *I* de 4096x4096 píxeles. El contraste se define como: $C = (\max(I) - \min(I))/(\max(I))$. El objeto binario de entrada propuesto tiene máximo contraste, C=1, sin embargo en la imagen desencriptada el contraste decae debido a la pérdida de información encriptada. Por esta razón, definiremos un mínimo contraste de la imagen desencriptada, que a nuestro criterio nos permite reconocer la información del objeto de entrada, para determinar la mínima cantidad de datos encriptados necesarios. En nuestra propuesta emplearemos el contraste, dado que el MSE y el coeficiente de correlación no resultaron una métrica adecuada para determinar la calidad de la imagen desencriptada. El contraste permitió comparar los resultados para distintos tamaños de objeto de entrada.

V.2.1.1 Estudio en la arquitectura 4*f*

A partir del análisis de la Sección 3.4.5 sabemos que la mínima proporción de área del patrón encriptado necesaria para que en la imagen recuperada sea reconocible, depende del tamaño del objeto de entrada, cuando todos los restantes parámetros del sistema permanecen constantes. En nuestro análisis consideramos cuadros blancos de tamaños: 10.24x10.24 mm^2, 5.12x5.12 mm^2, 2.56x2.56 mm^2, 1.28x1.28 mm^2 embebidos en un fondo 20.48x20.48 mm^2. La mínima área de los datos encriptados requerida para obtener en la imagen desencriptada un contraste C=0.1, es 5.12x5.12 mm^2, 2.56x2.56 mm^2, 1.28x1.28 mm^2, 0.64x0.64mm^2, respectivamente. Estos valores representan el 6.250%, 1.563%, 0.39%, 0.098% de los datos, respectivamente.

Se diseñaron una serie de pruebas con el fin de relacionar la capacidad de multiplexado de un sistema óptico dado con la mínima cantidad (área) de datos encriptados necesaria para reconocer al objeto de entrada en la imagen desencriptada para un sistema de encriptación 4*f.* Los resultados se presentan en la **Tabla 5.1**. En la primera columna se muestra el objeto de entrada. Para cada objeto de entrada, se extrae del patrón encriptado el área necesaria para obtener un contraste de 0.1 en la imagen desencriptada. El área del patrón encriptado se selecciona de dos formas: extrayendo los datos ubicados en un cuadro centrado y extrayendo los datos de forma aleatoria en todo el plano de encriptación. En la segunda columna se muestra un detalle del plano de encriptación al que se le superpone una máscara binaria que selecciona el porcentaje del patrón (distinto para cada tamaño de objeto de entrada), que se emplea en el proceso de desencriptación. La imagen desencriptada en cada caso se presentan en la tercera columna. A partir de la evaluación del contraste en la tercera columna de la **Tabla 5.1**, podemos observar que para la arquitectura 4*f*, si la información está uniformemente distribuida en el plano de encriptación, el efecto es el mismo cuando se extrae la información mediante un área centrada ó de forma aleatoria.

Posteriormente, se diseñó una nueva prueba con el fin de determinar la capacidad de multiplexado. Los resultados se presentan en la **Tabla 5.2**. En este caso se determinó el número de imágenes que el sistema permite multiplexar, encontrando la relación entre el área total de trabajo y la mínima área de cada dato encriptado definida teniendo en cuenta la **Tabla 5.1**. Las imágenes presentadas en la **Tabla 5.2** tienen un contraste de 0.1, es decir que poseen el mismo nivel de "degradación". Sabemos que a medida que disminuye la cantidad de áreas blancas del objeto de entrada, para un área de trabajo constante (área total de la imagen), se requiere un porcentaje menor de datos encriptados y eso se traduce en un aumento del número de imágenes a multiplexar. Los datos de la **Tabla 5.2** fueron multiplexados utilizando máscaras llaves estadísticamente independientes para encriptar cada canal de información. Esto garantiza que los patrones encriptados en el mismo medio no presenten solapamiento entre los distintos canales en la etapa de desencriptación.

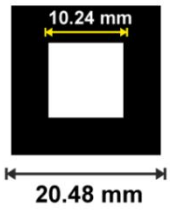
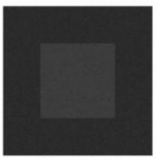
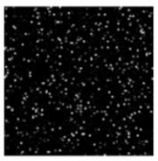
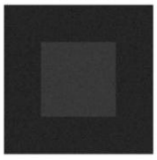
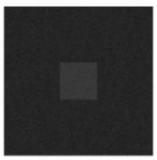
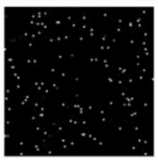
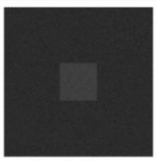
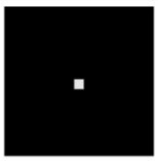
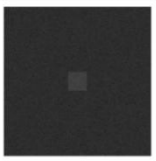
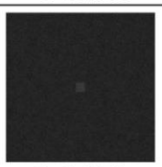
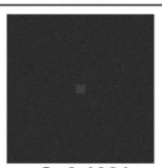
Objeto de entrada	Área y localización de las regiones del plano de encriptación	Imagen desencriptada
	 6.25%	 C=0.1139
	 6.25%	 C=0.1097
	 1.563%	 C=0.1095
	 1.563%	 C=0.1100
	 0.390%	 C=0.1079
	 0.390%	 C=0.1098
	 0.098%	 C=0.1071
	 0.098%	 C=0.1081

Tabla 5.1. Imágenes desencriptadas con contraste de aproximadamente 0.1 considerando distintos tamaños de objeto de entrada y seleccionado una porción de los datos encriptados. (el brillo-contraste de la imagen desencriptada fue modificado para facilitar la visualización). Las máscaras aleatorias de la segunda columna abarcan 100 x 100 pixeles del total 4096 x 4096 píxeles.

Por ejemplo, para un cuadro blanco de 10.24x10.24 mm^2 embebido en un fondo de 20.48x20.48 mm^2, la relación, área mínima requerida-área total, predice que se pueden multiplexar 16 patrones encriptados para que el contraste de la imagen recuperada de un canal sea 0.1 ± 0.02. Por otra parte, para un cuadro blanco de 1.28x1.28 mm^2 se pueden multiplexar 1024 patrones para obtener en cada canal una imagen recuperada con el mismo nivel de contraste. Comparando los resultados de la segunda fila (imagen desencriptada con el porcentaje mínimo) y la tercera fila (imagen desencriptada correspondiente a un canal cuando se multiplexan N patrones), notamos que las imágenes desencriptadas para la misma columna (es decir igual tamaño de objeto de entrada) tienen un contraste comparable. A partir de estos resultados podemos verificar que la relación, área mínima requerida-área total, permite predecir la capacidad de multiplexado para un sistema 4*f* considerando un tamaño de objeto y una configuración dados.

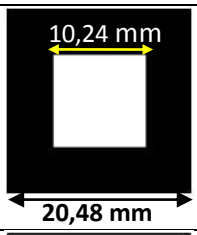
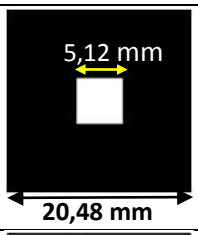
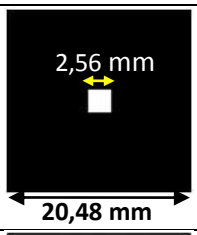
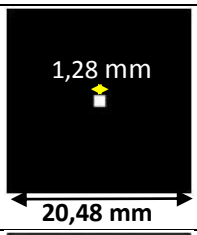
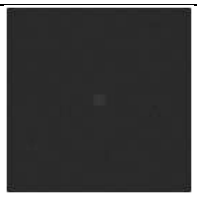
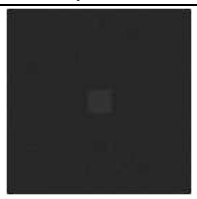
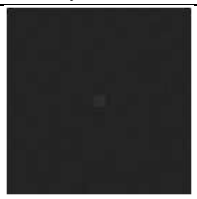
Objeto de entrada				
a)	 **6,25%**	 **1,56%**	 **0,39%**	 **0,097%**
b)	 **N=16**	 **N=64**	 **N=256**	 **N=1024**

Tabla 5.2 Imágenes desencriptadas con un valor de contraste de 0.1 ± 0.02. **a)** cuando se extrae un porcentaje aleatorio de los datos encriptados. **b)** cuando se recupera un canal del patrón encriptado que contiene N imágenes encriptadas multiplexadas.

Estos resultados ponen en evidencia un aumento de la capacidad de multiplexado cuando el tamaño del objeto de entrada disminuye si el área del medio del almacenamiento y todos los demás parámetros del sistema permanecen constantes.

Por otro lado la predicción de la cantidad de imágenes que se pueden multiplexar en términos del tamaño del objeto de entrada se hizo para el caso ideal que no se pierde información en el sistema de encriptación-desencriptación.

VI.2.1.2 Estudio en la arquitectura JTC

La mínima región del patrón encriptado que se requiere en una arquitectura JTC para que se pueda reconocer el objeto de entrada en la imagen desencriptada para un determinado tamaño de objeto de entrada, no surge directamente del análisis de la Sección 4.8. En este caso, se debe tener en cuenta que el plano de encriptación es un plano de frecuencias, lo cual implica que la modalidad de extracción de los datos encriptados afecta el contenido frecuencial de la imagen desencriptada. El efecto de extraer los datos en forma de un cuadro centrado se puede ver en la **Tabla 4.8** del capítulo anterior. Se verificó que si se limita el medio de almacenamiento la imagen desencriptada va perdiendo información de alta frecuencia, es decir, equivale a un filtrado pasa bajos.

Si consideramos un procedimiento de multiplexado, el patrón encriptado de un canal se superpone al patrón de los restantes canales. En esta Sección intentaremos verificar que la redundancia el patrón encriptado está directamente relacionada con el multiplexado. En ese sentido, se diseña una prueba para verificar la redundancia de los datos encriptados en la arquitectura JTC. En la **Tabla 5.3** se muestran las imágenes desencriptadas cuando se extrae un porcentaje cada vez menor del patrón encriptado. La máscara binaria, que selecciona aleatoriamente los datos encriptados, tiene una celda de tamaño de un pixel y se muestra en la segunda columna. Las pruebas fueron realizadas para dos tamaños de objetos de entrada de 5,12 x 5,12 mm^2 y 1,28 x 1,28 mm^2 y las correspondientes imágenes desencriptadas se presentan en la tercera y cuarta columna, respectivamente. A partir de las imágenes desencriptadas de la **Tabla 5.3** se puede notar que se requiere un porcentaje menor del patrón encriptado cuando el tamaño de objeto de entrada es más pequeño.

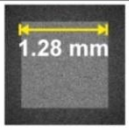
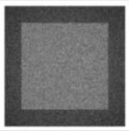
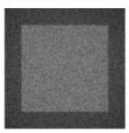
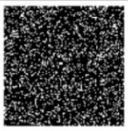
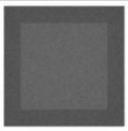
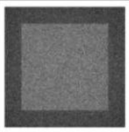
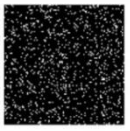
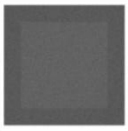
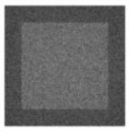
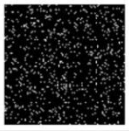
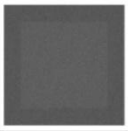
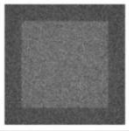
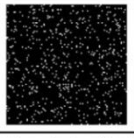
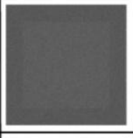
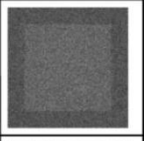
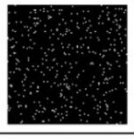
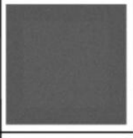
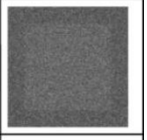
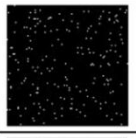
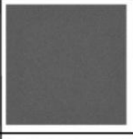
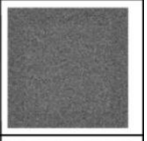
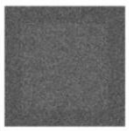
Área y localización de las regiones del plano de encriptación		Imagen desencriptada. TOE:	
		5.12 mm	1.28mm
100%			
40%			
30%			
20%			
10%			
8%			
6%			
4%			
2%			
1%			

Tabla 5.3. Imágenes desencriptadas cuando se utiliza solo una región del patrón encriptado considerando dos tamaños de objeto de entrada**.** La máscara que muestra la selección aleatoria de los datos encriptados en la segunda columna, es una versión ampliada de 100x100 pixeles del total 4096 x4096 pixeles.

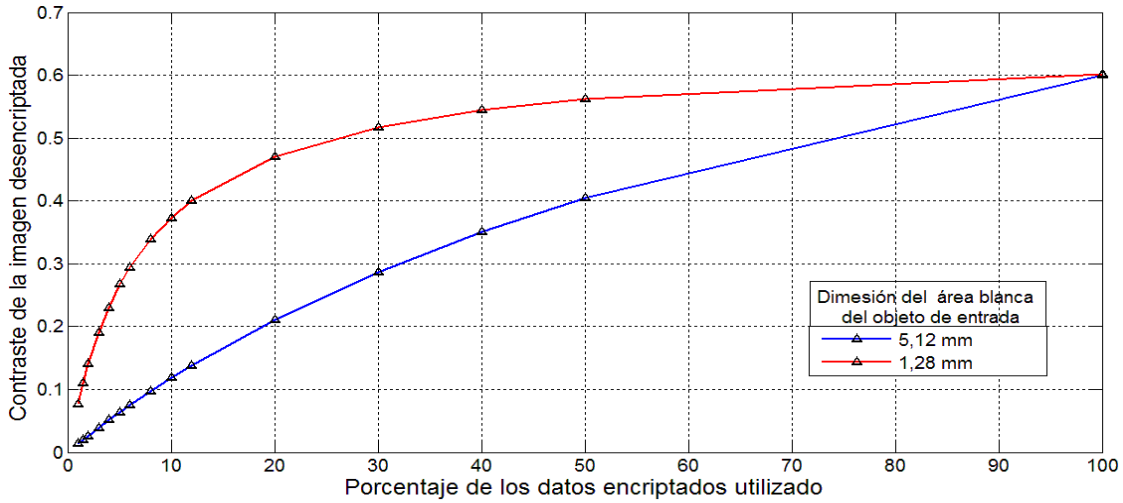


Figura 5.1 Contraste de la imagen desencriptada en función del porcentaje aleatorio de los datos encriptados empleados en la etapa de desencriptación para dos tamaños de objeto de entrada. El tamaño de la celda de la máscara binaria que selecciona los datos encriptados es de 1 píxel.

Las curvas de la **Figura 5.1** confirman que se presenta mayor redundancia en los datos encriptados cuando el objeto de entrada es más pequeño. Por ejemplo, si se considera una imagen de 5,12 x 5, 12 mm^2 se necesita el 50 por ciento de los datos encriptados para obtener en la imagen de salida un contraste de 0.4. Mientras, cuando se considera una imagen de 1,28 x 1,28 mm^2, se requiere aproximadamente el 12 por ciento del patrón encriptado.

En importante resaltar en los resultados de la **Tabla 5.3** que el tamaño de celda de la máscara binaria empleada para extraer los datos encriptados es un píxel. Sin embargo, nuestra idea es relacionar la cantidad de datos encriptados necesarios con la capacidad de multiplexado. Para el plano de encriptación del JTC podemos imaginar que la perdida de información debido al multiplexado tiene una frecuencia espacial del orden del tamaño promedio del speckle en el plano de encriptación. Recordemos que el tamaño promedio transversal del speckle en el plano focal de una lente es: $\langle Sx \rangle \propto \lambda f / D$ donde λ es la longitud de onda, f la distancia focal y D es dimensión del objeto de entrada. En este contexto nos parece pertinente analizar la perdida de información cuando se extrae el porcentaje de los datos encriptados empleando mascaras binarias con tamaño de celda igual al tamaño promedio del speckle del patrón encriptado.

El tamaño promedio del speckle es 20 μm para un objeto de entrada de D = 5,12 mm mientras que el tamaño es de 80 μm para un objeto de D=1,28 mm, considerando una longitud de onda de 632 nm y una distancia focal de 162 mm. La resolución de píxel es de 5 μm, luego el tamaño de speckle es de 4 y 16 píxeles para los objetos de 5,12 y 1,28 mm, respectivamente. Las imágenes desencriptadas cuando la máscara empleada para seleccionar un porcentaje de la información encriptada tiene un tamaño de celda de 4 y 16 píxeles para los objetos de 5,12 y 1,28 mm, respectivamente, se presentan en la Tabla 5.4.

Si comparamos las imágenes de la tercera y quinta columna de la **Tabla 5.4** con las de la tercera y cuarta columna de la **Tabla 5.3**, se puede notar que el comportamiento del sistema cambia, cuando los datos encriptados se seleccionan considerando una máscara con tamaño de celda que coincide con el tamaño promedio del speckle. En la **Tabla 5.4** a diferencia de lo que se observa en las imágenes de la **Tabla 5.3**, las imágenes desencriptadas correspondientes a la misma fila (es decir cuando se selecciona el mismo porcentaje del patrón encriptado), parecen tener la misma calidad de salida. Para verificar este comportamiento, en la **Figura. 5.2** se presentan las curvas del contraste de la imagen desencriptada en función del porcentaje de información del patrón encriptado utilizado en la etapa de desencriptación, para los dos tamaños de objeto de entrada.

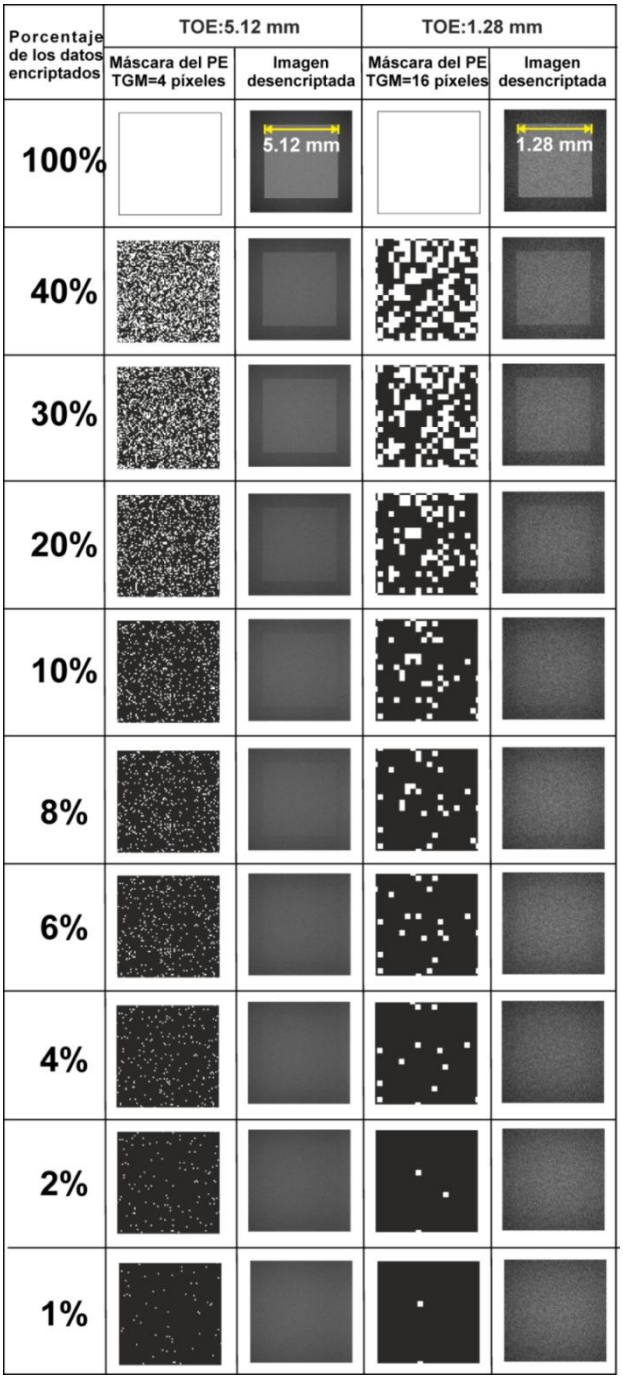


Tabla 5.4. Las imágenes desencriptadas cuando la máscara empleada para seleccionar un porcentaje de la información encriptada tiene un tamaño de celda de 4 y 16 píxeles para los objetos de 5,12 y 1,28 mm, respectivamente**.** La máscara binaria es una versión ampliada de 100 x 100 pixeles^2 del total 4096x4096 pixeles^2

Como se puede ver en la **Figura 5.2** las curvas para las dos imágenes en comparación con las correspondientes a las de la **Figura 5.1** se acercan y tienen la misma tendencia. Se verificó que en la arquitectura 4f se requería menor porcentaje de datos encriptados a medida que se disminuye el tamaño del objeto de entrada.

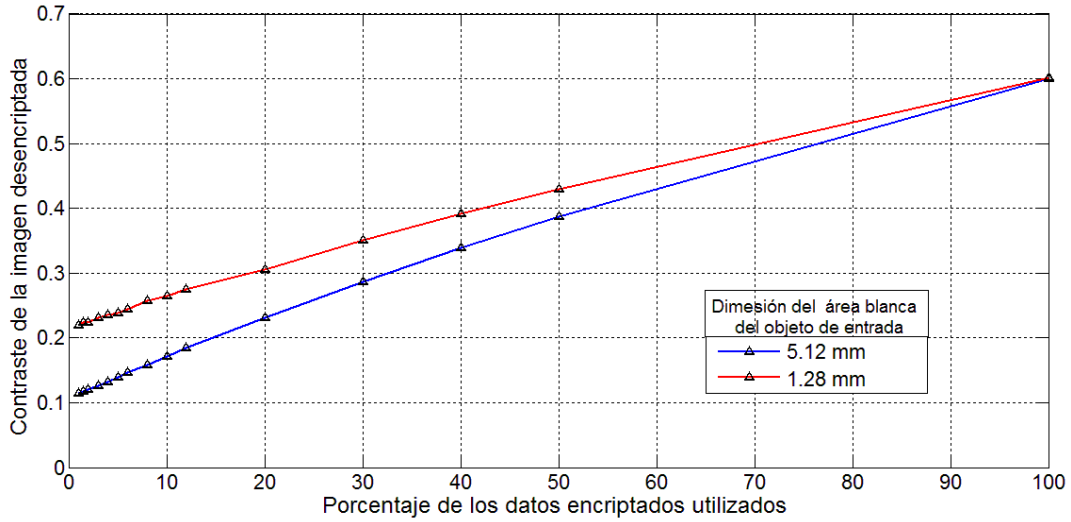


Figura 5.2 Contraste de la imagen desencriptada en función del porcentaje aleatorio de los datos encriptados empleados en la etapa de desencriptación para dos tamaños de objeto de entrada. El tamaño de la celda de la máscara binaria que selecciona los datos encriptados es de 1 píxel.

Este comportamiento se observa también para la arquitectura JTC cuando se utiliza una máscara binaria con tamaño de celda de 1 pixel. Sin embargo, cuando se modifica el tamaño de celda de la máscara binaria de manera que coincida con el tamaño promedio del speckle ese comportamiento no se observa dado se percibe en las imágenes un nivel de degradación similar para los dos tamaños de objetos de entrada cuando se emplea el mismo porcentaje de datos encriptados. Este comportamiento no nos permite hacer una predicción respecto a la capacidad de multiplexado en la arquitectura JTC. Para clarificar este comportamiento, se implementó un multiplexado en un sistema JTC para distintos tamaños de objeto de entrada.

En la **Tabla 5.5** se presentan la comparación entre las imágenes desencriptadas obtenidas extrayendo un porcentaje aleatorio de los datos encriptados con una máscara con tamaño de celda igual al tamaño del speckle.

	100%	50%	30%	10%	5%
(a)					
(b)					

Tabla 5.5 Imagen de 2,56 mm desencriptada cuando se utiliza un porcentaje de los datos encriptados en una arquitectura JTC. a) no optimizada; b) optimizada.

Las simulaciones fueron obtenidas considerando una máscara llave de fase pura (no optimizada) y una máscara llave optimizada (Sección del capítulo IV). Las columnas corresponden a diferentes porcentajes de datos encriptados. Obsérvese que el empleo de una máscara llave optimizada mejora la calidad de las imágenes desencriptadas.

Figue 5.3 Imagen binaria a ser encriptada.

El plano de entrada del JTC donde se localizan las ventanas objeto y llave tiene una dimensión de 20,48 x 20,48 mm^2. El objeto de entrada utilizado es una imagen binaria de la palabra CIOp (ver Figura 5.3). El objeto es adosado a la máscara objeto y en la otra ventana se localiza una máscara llave de solo fase (para el JTC no optimizado). El objeto de entrada utilizado para la implementación del multiplexado son versiones escaladas cuyos tamaños son: 5,12 x 5,12 mm^2, 3,84 x 3,84 mm^2, 2,56 x 2,56 mm^2 y 1,28 x 1,28 mm^2. Las ventanas del JTC están separadas una distancia igual al doble del tamaño del objeto de entrada, resultando en el JPS speckles modulados por al menos 3 franjas. Esta separación es la mínima que garantiza que la imagen desencriptada este espacialmente separada de restantes términos en el plano de salida. Con el fin de asegurar que haya 3 franjas por grano de speckle, un cambio en el tamaño del objeto de entrada implica un

cambio de la separación entre las ventanas del JTC. En la **Figura 5.4** se muestran los planos de entrada, plano de encriptación (JPS) y plano de salida del JTC, para los cuatro tamaños de objetos de entrada considerados. El cuadro amarillo en la última fila de la Tabla 5.5, indica el área y la localización de la imagen desencriptada. Los resultados presentados en la Tabla 5.5 corresponden a la encriptación y desencriptación de un único objeto de entrada.

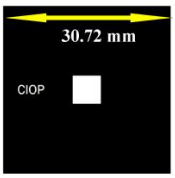
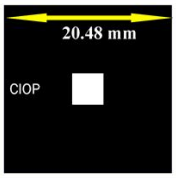
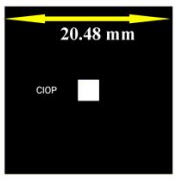
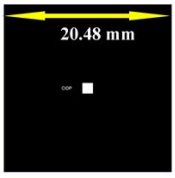
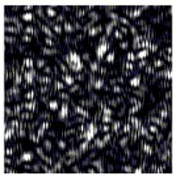
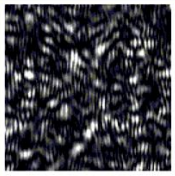
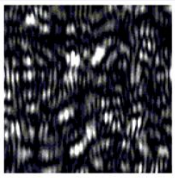
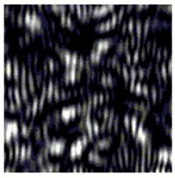
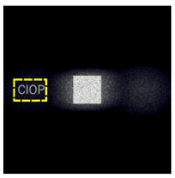
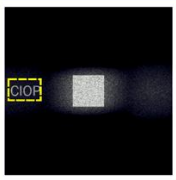
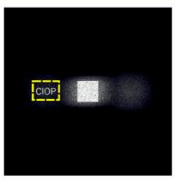
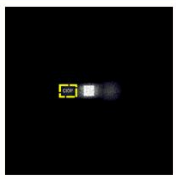
	TI=5,12 mm, Sep= 10,24mm	TI=3.84 mm, Sep= 7,68mm	TI=2,56 mm, Sep= 5,12mm	TI=1,28 mm, Sep= 2,56mm
Plano de entrada				
Versión ampliada plano de encriptación				
Plano de salida				

Tabla 5.5 Plano de entrada, versión ampliada del plano de encriptación (JPS) y plano de salida, para cuatro tamaños de objeto de entrada.

Para la implementación del multiplexado, se encripta N veces el mismo objeto de entrada, utilizando en cada caso máscaras llaves estadísticamente independientes, para asegurar que los N patrones encriptados resulten no haya solapamiento entre los canales. En la **Tabla 5.6** se presentan las imágenes desencriptadas correspondientes a un canal, cuando se almacenan 10, 20, 30 y 40 patrones encriptados en una arquitectura JTC para diferentes tamaños de objeto de entrada. A partir de los resultados de la **Tabla 5.6**, podemos notar que la calidad de la imagen desencriptada independiente del tamaño del objeto de entrada. Estos resultados sugieren que la capacidad de multiplexar información encriptada, no depende del tamaño del objeto de entrada para la arquitectura JTC.

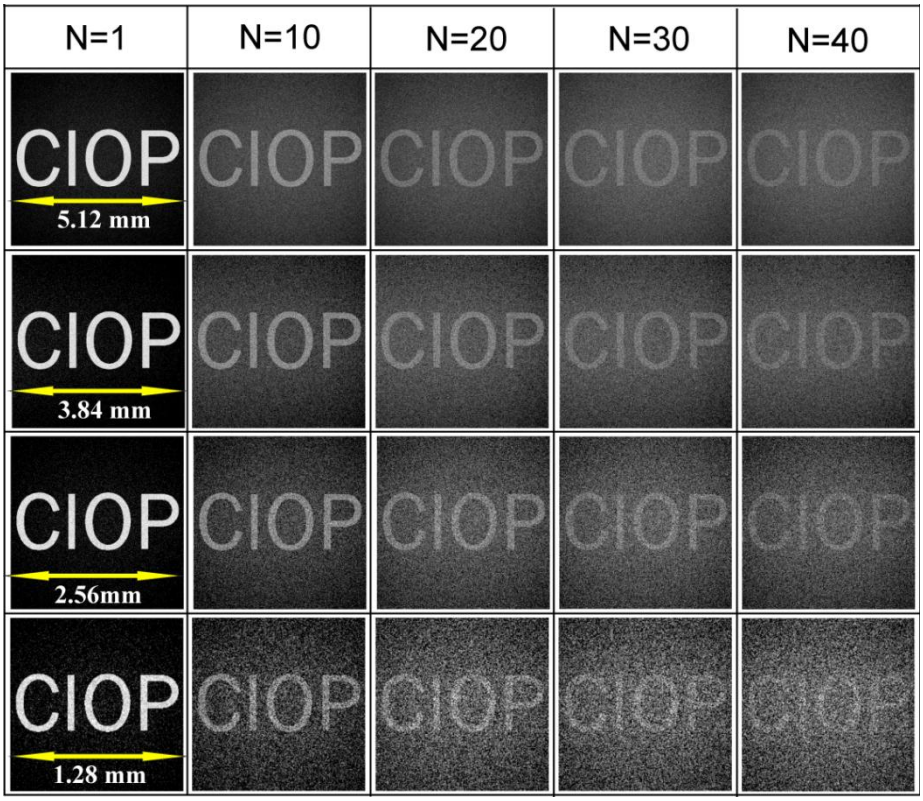


Tabla 5.6 Imagen desencriptada correspondiente a un único canal cuando se almacena en el plano de encriptación 10, 20, 30 y 40 patrones encriptados, para cuatro tamaños de objeto de entrada. La dimensión de los objetos de entrada está indicado sobre la imagen de la primera columna.

Con el fin de marcar la diferencia en la capacidad de multiplexado en las arquitecturas 4f y JTC, se presenta en la Tabla 5.7 las imágenes desencriptadas de un único canal, cuando se almacena N objetos encriptados para tres tamaños de objeto de entrada. El numero de objetos a ser multiplexado en ambas arquitecturas se determino con objetivo de obtener contrastes (C = 0. 47+-0.2) comparables en la imagen desencriptada de un canal. Es evidente para el tamaño de objeto de 1,28 mm que la capacidad de multiplexado depende fuertemente de la arquitectura elegida.

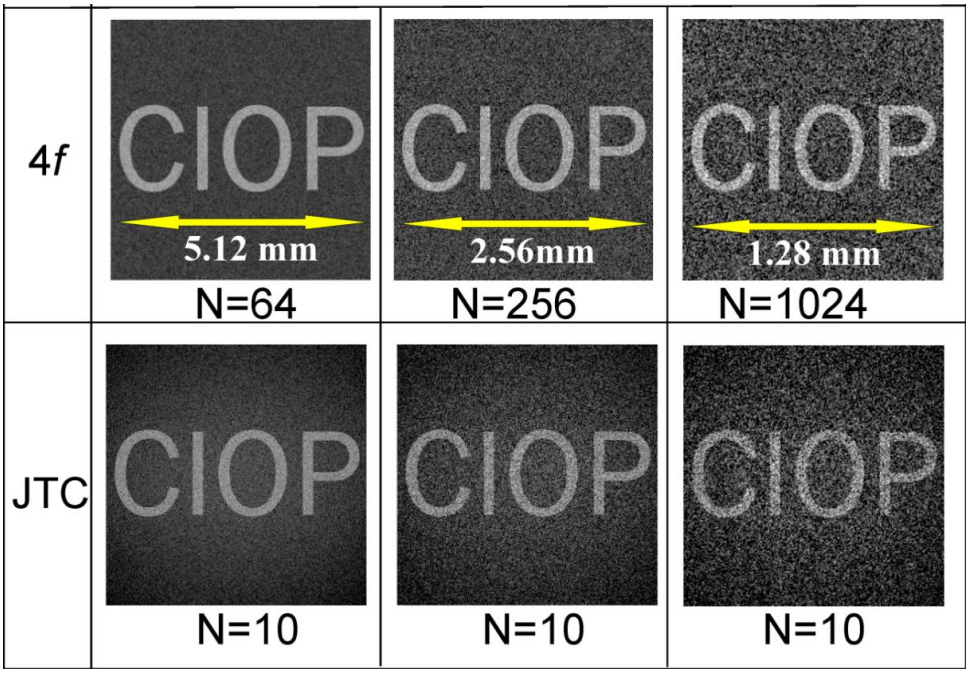


Tabla 5.7. Imágenes desencriptadas de un único canal cuando se multiplexan N patrones encriptados en las arquitecturas 4 f y JTC, para tres tamaños de objeto de entrada

V.3 Sensibilidad del sistema de encriptación a un parámetro de multiplexado.

La capacidad de multiplexado a la que nos referimos en la Sección 5.2 depende de la redundancia de los datos encriptados con respecto al tamaño del objeto de entrada para la arquitectura de encriptación 4*f* y JTC. Es decir que en la Sección anterior se analizó la máxima cantidad de patrones encriptados que se pueden multiplexar asegurando que no haya solapamiento. Cuando se utiliza máscaras llaves estadísticamente independientes para cada objeto a ser encriptado en el proceso de multiplexado, los patrones encriptados están decorrelacionados lo que garantizada que no haya solapamiento entre las imágenes recuperadas. Sin embargo, otra alternativa para multiplexar datos encriptados consiste en empleando distintos parámetros ópticos. Algunos de los parámetros empleados para el almacenamiento múltiple de datos encriptados son: el desplazamiento tridimensional de la máscara llave (para sistemas basados en 4*f*) [5.4-5.5, 5.6, 5.19], rotaciones de la máscara llave (4*f* y JTC) [5.18], cambio de la longitud de onda [5.9], cambio del estado de polarización de la luz incidente [5.7,

5.20], empleo de máscaras de amplitud para seleccionar porciones independientes de la máscara llave [5.16], escalamientos digital de la máscara codificadora [5.17].

En este caso, para llevar a cabo un almacenamiento múltiple de datos encriptados $E_N(x_2)$, donde N es la cantidad de patrones que se desea almacenar en el medio es necesario que cada patrón encriptado $E_i(x_2)$ este decorrelacionado de todos los demás $E_{N\neq i}(x_2)$, para así evitar el mencionado solapamiento entre canales independientes.

La variación del parámetro que se utilice en un proceso de multiplexado, se nombrará de aquí en adelante como "*parámetro de multiplexado*" y la mínima variación necesaria para que no se produzca solapamiento entre registros de datos encriptados sucesivos se llamará "*sensibilidad del sistema al parámetro de multiplexado*". La sensibilidad es el umbral a partir del cual los datos codificados correspondientes a registros distintos están decorrelacionados. Si se desea realizar un proceso de multiplexado variando algún parámetro óptico del sistema y no empleando máscaras independientes, se requiere un estudio sobre la sensibilidad del sistema ante el cambio del parámetro óptico con el fin de evitar el solapamiento.

Con el objetivo de medir la sensibilidad del sistema al cambio del parámetro de multiplexado (ΔP_{min}) sé pueden utilizar dos estrategias: una consiste en medir el pico de correlación entre los patrones encriptados con el valor de parámetro igual a P_0 y a $P_0 + \Delta P$, la otra consiste en medir el coeficiente de correlación (ó el MSE) entre la imagen desencriptada $I(P_0)$ con el parámetro correcto y la imagen desencriptada $I(P_0 + \Delta P)$ obtenida empleando el parámetro desplazado. El coeficiente de correlación que mide la similitud entre dichas imagen desencriptadas, se calcula mediante la ecuación:

$$CC = \frac{\sum_x \sum_y \left(IP_{x,y} - \langle IP \rangle\right)\left(I\Delta P_{x,y} - \langle I\Delta P \rangle\right)}{\sqrt{\left[\sum_x \sum_y \left(IP_{x,y} - \langle IP \rangle\right)^2\right]\left[\sum_x \sum_y \left(I\Delta P_{x,y} - \langle I\Delta P \rangle\right)^2\right]}} \qquad (4.12)$$

V.3.1 Análisis de la sensibilidad a la longitud de onda.

Si bien los sistemas de encriptación basados en la arquitectura 4f resultan ventajosos en cuanto a la capacidad de multiplexado, la arquitectura JTC presenta ventajas experimentales. Entre las ventajas que incrementan el interés en el desarrollo de las investigaciones en esta arquitectura, podemos mencionar que el sistema es más compacto que un sistema holográfico ordinario (dado que el objeto y el haz de referencia se localizan en el mismo plano) a lo que se suma que este sistema es menos sensible a los problemas de alineamiento. Por estas razones tenemos interés en el desarrollo de la presente investigación de aprovechar los grados de libertad que la óptica ofrece para multiplexar datos en una arquitectura JTC. En particular las aplicaciones que se presentarán en este capítulo utilizan el parámetro de multiplexado en longitud de onda. En la primera parte de esta Sección se hace un estudio teórico de la sensibilidad a este parámetro en la arquitectura JTC. Después se evalúa la sensibilidad en términos del coeficiente de correlación y se incluyen resultados para la arquitectura 4*f* que permiten comparar el comportamiento ante el cambio en la longitud de onda entre ambos sistemas.

V.3.1.1. Análisis teórico de la sensibilidad a la longitud de onda en la arquitectura JTC.

Si bien, en la Sección II.4.2 se realizó un análisis teórico del sistema de encriptación JTC, se va retomar en la presente Sección con el objetivo de profundizar el estudio de la sensibilidad a la longitud de onda.

Recordemos que denominamos $g(\mathrm{x}_0, \mathrm{y}_0)$ a la imagen a ser encriptada multiplicada por la máscara de fase del plano de entrada $r(\mathrm{x}_0, \mathrm{y}_0) = \mathrm{e}^{\mathrm{i}2\pi \mathrm{p}(\mathrm{x}_0, \mathrm{y}_0)}$ ubicada en la posición (0, -Y) del plano de entrada del JTC. En la otra ventana ubicada en la posición (0, +Y), se localiza la máscara llave $h(\mathrm{x}_0, \mathrm{y}_0)$. La entrada es iluminada por una onda plana de longitud de onda λ y amplitud unitaria. El campo propagado es transformado Fourier por la lente L_1 de distancia focal ***f.*** Como se mencionó en la Sección II.4.2, en la arquitectura

JTC la información encriptada es el espectro de potencia, es decir el valor absoluto al cuadrado de la ecuación (2.33), luego el patrón encriptado estará representado por:

$$JPS_\lambda = I(x_1) = |U_1(x_1)|^2 =$$

$$\left\{\frac{1}{(\lambda f)^2}\left[\left|G\left(\frac{x_1}{\lambda f}\right)\otimes R\left(\frac{x_1}{\lambda f}\right)\right|^2 + \left|H\left(\frac{x_1}{\lambda f}\right)\right|^2\right] + \right.$$

$$\frac{1}{(\lambda f)^2}\left[G\left(\frac{x_1}{\lambda f}\right)\otimes R\left(\frac{x_1}{\lambda f}\right)\right]H^*\left(\frac{x_1}{\lambda f}\right)e^{i2\pi(2Y)\frac{x_1}{\lambda f}} +$$

$$\left.\frac{1}{(\lambda f)^2}\left[G^*\left(\frac{x_1}{\lambda f}\right)\otimes R^*\left(\frac{x_1}{\lambda f}\right)\right]H\left(\frac{x_1}{\lambda f}\right)e^{-i2\pi(2Y)\frac{x_1}{\lambda f}}\right\} \qquad (5.1)$$

Suponemos en este análisis que la dimensión del medio de almacenamiento es mayor que el área en la cual está distribuido el patrón encriptado.

Recordemos que en la etapa desencriptación se requiere iluminar el JPS registrado con la transformada de Fourier de la máscara llave. El tercer término de la ecuación (5.1) permite obtener la imagen desencriptada y está espacialmente separado de los otros tres términos en el plano de salida del sistema. Denotamos al tercer término del JPS como $S_3(x_1, y_1)$:

$$S_3\left(\frac{x_1}{\lambda f}\right) = \frac{1}{i\lambda f}H\left(\frac{x_1}{\lambda f}\right)e^{-i2\pi Y\frac{x_1}{\lambda f}}\,JPS_3 =$$

$$\frac{1}{i(\lambda f)^3}\left[G\left(\frac{x_1}{\lambda f}\right)\otimes R\left(\frac{x_1}{\lambda f}\right)\right]H^*\left(\frac{x_1}{\lambda f}\right)e^{i2\pi(2Y)\frac{x_1}{\lambda f}}H\left(\frac{x_1}{\lambda f}\right)e^{-i2\pi Y\frac{x_1}{\lambda f}} \qquad (5.2)$$

Si se cumple que la transformada de Fourier de la máscara llave es una función de solo fase y amplitud uniforme y es la misma empleada en el proceso de encriptación, entonces se cumple la igualdad mostrada en la ecuación (2.37). Al compensarse algunos de los términos de fase de la parte derecha de la ecuación (5.2), $S_3(x_1, y_1)$ queda reducida a:

$$S_3\left(\frac{x_1}{\lambda f}\right) = \frac{1}{i(\lambda f)^3}\left[G\left(\frac{x_1}{\lambda f}\right)\otimes R\left(\frac{x_1}{\lambda f}\right)\right]e^{i2\pi(Y)\frac{x_1}{\lambda f}} \qquad (5.3)$$

Finalmente el campo que emerge del plano de frecuencias se transforma Fourier de nuevo para obtener en el plano de salida la imagen desencriptada:

$$\Im\left\{S_3\left(\frac{x_1}{\lambda f}\right)\right\} = \frac{e^{i\pi}}{(\lambda f)^2}[g(-x_2)\ \mathrm{r}(-\mathrm{x}_2)] \otimes \delta(-x_2 - Y) \tag{5.4}$$

Si observamos en el plano se salida con un detector de intensidad de manera que la máscara objeto de solo fase $\mathrm{r}(-\mathrm{x}_2)$ no se pueda ver, se recupera la información desencriptada $|g(-x_2)|^2$.

Un esquema del proceso de encriptación y desencriptación para el sistema JTC se presenta en la **Figura 2.10** y **Figura 2.11** del capítulo II, respectivamente.

En este análisis, se asume que la máscara llave $h(x_0)$ es correcta. Si se usa la longitud de onda λ correcta en el proceso de desencriptación, la imagen es correctamente desencriptada. De otra manera, el ruido aleatorio introducido por $h(x_0)$ no puede ser removido, y puede afectar la información recuperada en el sistema. Asumamos que la longitud de onda en el proceso de lectura difiere en $\Delta\lambda$ de la longitud de onda usada en el proceso de encriptación. En este caso, la respuesta impulso (IR), en notación unidimensional, del sistema de desencriptación se transforma en:

$$IR(x, x_0, f, \lambda + \Delta\lambda) = \frac{1}{i(\lambda + \Delta\lambda)f} \exp\left\{\frac{i2\pi f}{\lambda + \Delta\lambda}\right\} \exp\left\{\frac{i\pi}{\lambda + \Delta\lambda}[x - x_0]^2\right\} \tag{5.5}$$

donde f es la longitud focal de la lente L y x, x_0 son variables espaciales. En este caso, se asume que la distancia focal no depende de la longitud de onda. Es posible demostrar que:

$$\frac{1}{\lambda + \Delta\lambda} = \frac{1}{\lambda} - \frac{\Delta\lambda}{\lambda^2} \tag{5.6}$$

Usando la ecuación (5.6), el primer factor de fase de la ecuación (5.5) puede ser expresado como $\exp[i2\pi f/\lambda]\exp[-i2\pi f\Delta\lambda/\lambda^2]$. Esto es, el efecto de $\Delta\lambda$ es adicionar una fase hacia la distribución de fase en el plano transformado. Mediante un análisis similar se puede demostrar que el segundo factor de fase también afecta la distribución en el plano de transformación. Es decir, el empleo de la máscara llave correcta, no puede remover la fase introducida por $\Delta\lambda$. Esta fase se suma a la distribución aleatoria original

en la etapa de desencriptación como otra distribución aleatoria, la cual no coincide con la primera. Por lo tanto, al no poder compensar ese término de fase, el proceso de desencriptación falla.

Ahora consideremos la sensibilidad a la longitud de onda cuando se tiene la máscara llave correcta en el proceso desencriptación. En la siguiente ecuación escribimos la reconstrucción del tercer término de la ecuación (5.1) cuando se ilumina con el campo erróneo $\frac{1}{i(\lambda+\Delta\lambda)f} H\left(\eta\frac{x_1}{\lambda f}\right) e^{-i2\pi Y\eta\frac{x_1}{\lambda f}}$ como sigue:

$$S_3\left(\frac{x_1}{\lambda f}\right)_{\lambda+\Delta\lambda} = \frac{1}{i(\lambda+\Delta\lambda)f} H\left(\eta\frac{x_1}{\lambda f}\right) e^{-i2\pi Y\eta\frac{x_1}{\lambda f}} JPS_3 =$$

$$\frac{1}{i(\lambda+\Delta\lambda)\lambda^2 f^3}\left[G\left(\frac{x_1}{\lambda f}\right)\otimes R\left(\frac{x_1}{\lambda f}\right)\right] H^*\left(\frac{x_1}{\lambda f}\right) e^{i2\pi(2Y)\frac{x_1}{\lambda f}} H\left(\eta\frac{x_1}{\lambda f}\right) e^{-i2\pi Y\eta\frac{x_1}{\lambda f}} \qquad (5.7)$$

donde $H^*\left(\frac{x_1}{\lambda f}\right) = e^{-i2\pi Q\left(\frac{x_1}{\lambda f}\right)}$ y la distribución aleatoria de la transformada de la llave cuando se ilumina con una longitud de onda $\lambda+\Delta\lambda$ queda escalada por η, así $H\left(\eta\frac{x_1}{\lambda f}\right) = e^{i2\pi Q\left(\eta\frac{x_1}{\lambda f}\right)}$, siendo $\eta = \frac{\lambda}{\lambda+\Delta\lambda}$ el radio entre la longitud de onda registro-lectura y $Q\left(\frac{x_1}{\lambda f}\right)$ una distribución de valores aleatorios uniformemente distribuidos entre 0 y 1.

Podemos reescribir a (5.7) de la siguiente manera:

$$S_3\left(\frac{x_1}{\lambda f}\right)_{\lambda+\Delta\lambda} = A\left(\frac{x_1}{\lambda f}, Y, \eta\right)\left[G\left(\frac{x_1}{\lambda f}\right)\otimes R\left(\frac{x_1}{\lambda f}\right)\right]\exp\left\{-i2\pi\left[Q\left(\frac{x_1}{\lambda f}\right) - Q\left(\eta\frac{x_1}{\lambda f}\right)\right]\right\} \qquad (5.8)$$

donde $A\left(\frac{x_1}{\lambda f}, Y, \eta\right) = \frac{1}{i(\lambda+\Delta\lambda)\lambda^2 f^3} e^{i2\pi(2Y)\frac{x_1}{\lambda f}} e^{-i2\pi Y\eta\frac{x_1}{\lambda f}}$

Este campo es transformado Fourier siguiendo el proceso de desencriptación y se obtiene en el plano de salida, para el término que contiene la imagen desencriptada:

$$w(x_2, \lambda+\Delta\lambda) = \Im\left\{S_3\left(\frac{x_1}{\lambda f}\right)_{\lambda+\Delta\lambda}\right\} =$$

$$[g(-x_2)\ \mathrm{r}(-\mathrm{x}_2)]\ \otimes \Im\left\{\exp\left\{-i2\pi\left[Q\left(\frac{x_1}{\lambda f}\right) - Q\left(\eta\frac{x_1}{\lambda f}\right)\right]\right\}\right\} \qquad (5.9)$$

Se ha omitido el efecto de $A\left(\frac{x_1}{\lambda f}, Y, \eta\right)$en la transformación, debido a que no afecta directamente la imagen desencriptada.

Dependiendo de la configuración del sistema, existe un umbral en la longitud de onda de lectura $\lambda + \Delta\lambda$ a partir del cual, el escalamiento producido por η, provoca que las distribuciones de fase aleatorias $Q\left(\frac{x_1}{\lambda f}\right)$ y $Q\left(\eta\frac{x_1}{\lambda f}\right)$ estén decorrelacionadas, es decir que son estadísticamente independientes. Este hecho, no permite recuperar la imagen desencriptada, como se puede evidenciar en la ecuación (5.9). En realidad debido a la longitud finita de la correlación de la máscara, habrá un parcial solapamiento entre $Q\left(\frac{x_1}{\lambda f}\right)$ y $Q\left(\eta\frac{x_1}{\lambda f}\right)$ como una función de la longitud de correlación y el cambio de escala.

El análisis presentado en esta Sección permite demostrar que un cambio en la longitud de onda (Δλ) en la etapa de decodificación afecta la reconstrucción de la imagen desencriptada, introduciendo un factor de fase aleatorio. A partir de cierto umbral (Δλ) no es posible recuperar el objeto de entrada. Este valor límite dependerá de la configuración particular del sistema de encriptación y se puede evaluar mediante el coeficiente de correlación ó el MSE entre la imagen desencriptada con la longitud de onda de registro y una longitud de onda desplazada.

V.3.1.2. Evaluación de la sensibilidad a la longitud de onda. Arquitecturas JTC y $4f$.

En esta Sección además de evaluar la sensibilidad al parámetro longitud de onda para la arquitectura JTC, se incluye un análisis similar para el $4f$ con el fin de comparar dicha sensibilidad entre los dos sistemas. Con este objetivo en las simulaciones se considera un área de trabajo de 4096 x 4096 pixeles^2 (que equivalen a 20,48 x 20,48 mm^2), una resolución de pixel de 5x5 μm^2, una longitud de onda en la etapa de registro de 632.8 nm, distancias focales de 162 mm y un tamaño de pupila que está determinado por el área de trabajo. Una vez fijada el área de trabajo, la resolución de píxel y la longitud de onda, la distancia focal fue calculada de tal manera que el área del plano de Fourier coincidiera con el área de trabajo.

En la **Figura 5.4** se presenta, para el sistema 4*f*, el coeficiente de correlación entre la imagen desencriptada con la longitud de onda correcta ($\lambda = 632\ nm$) y la desencriptada con una longitud de onda desplazada una cantidad $\Delta\lambda$ con respecto a la de registro. Estos resultados se obtienen utilizando como objeto de entrada una imagen binaria de 2,56 x2,56 mm^2.

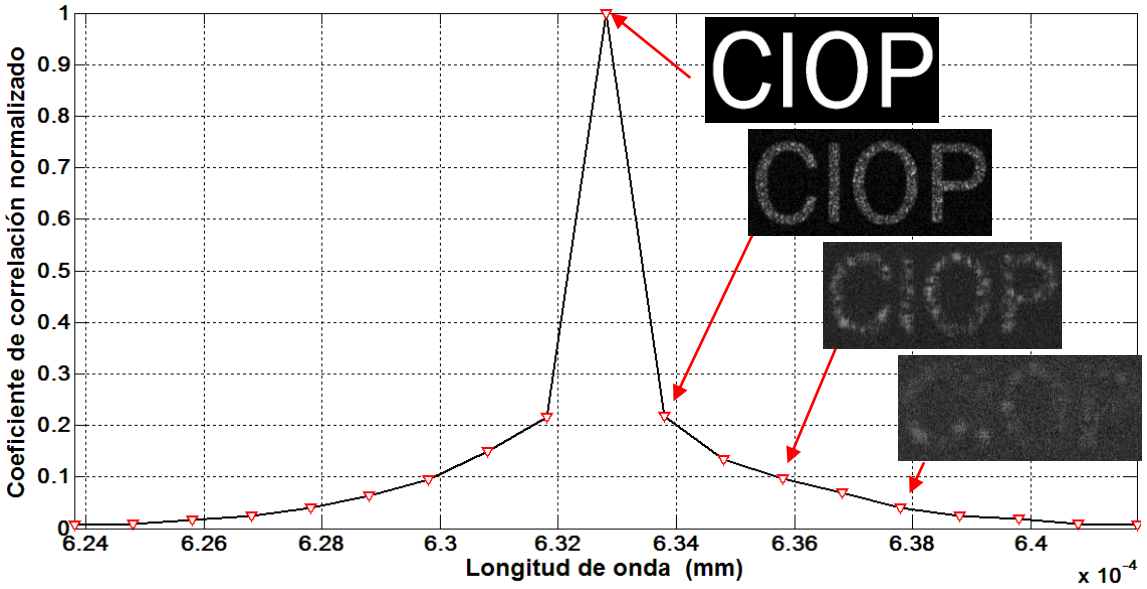


Figura 5.4 Coeficiente de correlación normalizado entre la imágenes desencriptadas empleando la longitud de onda de registro y una longitud de onda desplazada respecto a la de encriptación para un tamaño de objeto de entrada de 2,56 x2,56 mm^2 en un sistema de encriptación 4*f*.

Se presenta en la **Figura 5.4** algunas imágenes desencriptadas correspondientes a las longitudes de onda indicadas. Se puede observar que para un desplazamiento de 5 nm en la longitud de onda la imagen desencriptada no es reconocible.

Para verificar si este comportamiento cambia cuando se varía el tamaño del objeto de entrada, se repitió la prueba para la imagen escalada a 5,12 x 5,12 mm^2 y a 1.28x 1,28 mm^2. En la **Figura 5.5** se presentan las curvas de correlación en término de la longitud de onda en la etapa de desencriptación. En esta figura se puede notar que el coeficiente de correlación cae más abruptamente para la imagen más grande que para la más pequeña. Sin embargo, para desplazamientos mayores que $6nm$ las curvas caen al mismo nivel de decorrelación. Asimismo, en la grafica se muestran las imágenes desencriptadas cuando la longitud de onda en el proceso de desencriptación se ha desplazado 6 nm con respecto

a la de registro, para los tres tamaños de imágenes. Nótese que no se puede reconocer en ninguna de las tres imágenes desencriptadas el objeto de entrada.

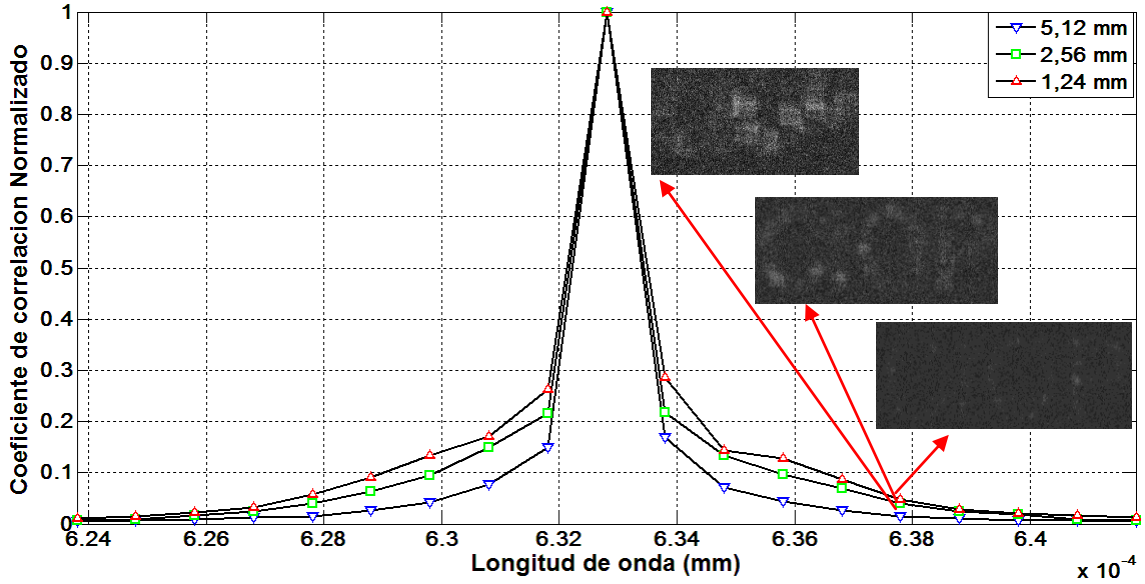
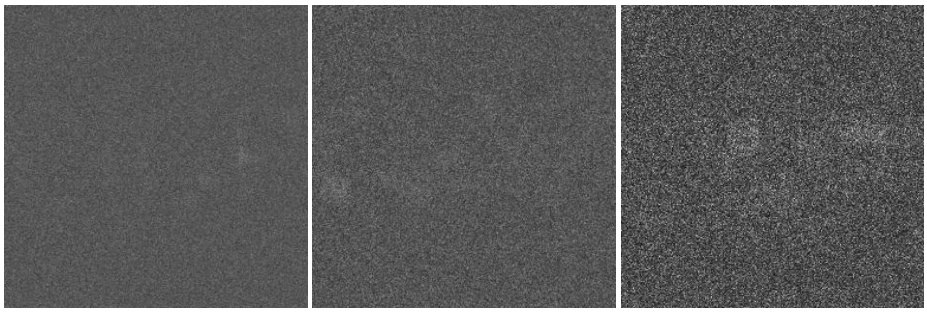


Figura 5.5 Coeficiente de correlación normalizado entre la imágenes desencriptadas empleando la longitud de onda de registro y una longitud de onda desplazada respecto a la de encriptación, para tres tamaños de objeto de entrada en un sistema de encriptación 4*f*



a) b) c)

Figura 5.6 Imagen desencriptada en un sistema de encriptación 4*f*, cuando la longitud de onda del proceso de desencriptación se ha desplazado 8 nm con respecto a la de registro para un tamaño de objeto de entrada de: a) 5,12 x 5,12 mm^2 b) 2,56 x 2,56 mm^2 c) 1,28 x 1,28 mm^2.

Luego, se realizó una prueba de sensibilidad al parámetro de multiplexado longitud de onda (λ) para la arquitectura JTC. Las gráficas del coeficiente de correlación entre la imagen desencriptada con la longitud de onda correcta ($\lambda = 632\ nm$) y la longitud de onda desplazada ($\lambda = 632 \pm \Delta\lambda\ nm$), para dos tamaños de objeto de entrada, 2,56 x 2,56 mm^2 y 1,28 x 1,28 mm^2, se presentan en la **Figura5.7.** El desplazamiento en longitud de onda de la etapa de decodificacion para obtener un nivel de decorrelacion que evite el

solapamiento entre las imágenes desencriptadas es de 14 nm para un objeto de entrada de 2,56 x 2,56 mm^2 y de 22 nm para un objeto de entrada de de 1,28 x 1,28 mm^2. Las imágenes desencriptadas correspondientes los valores límites mencionados se presentan en la Figura 5.8.

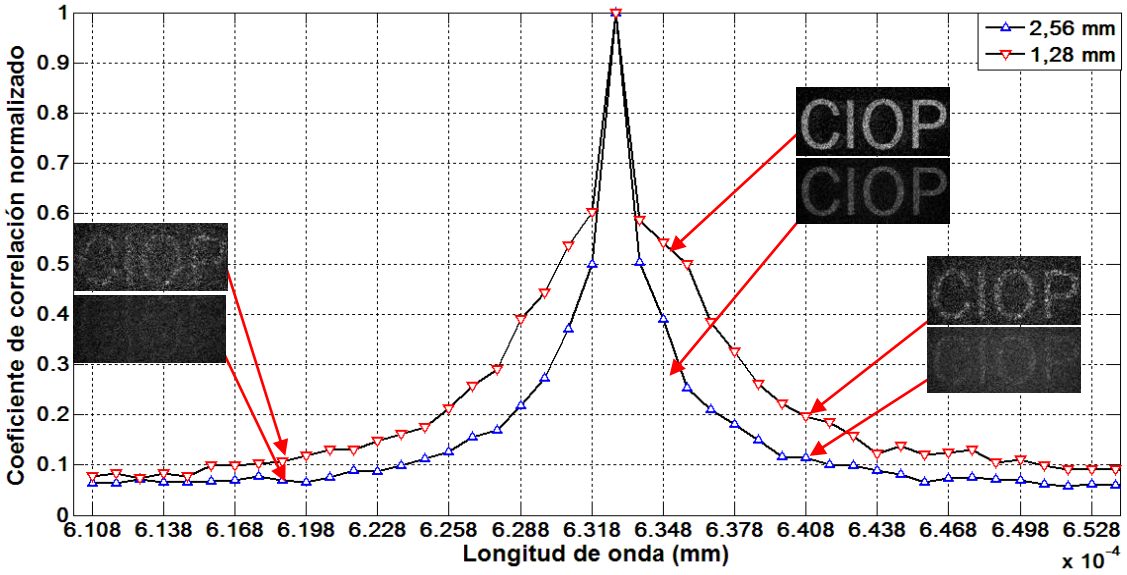
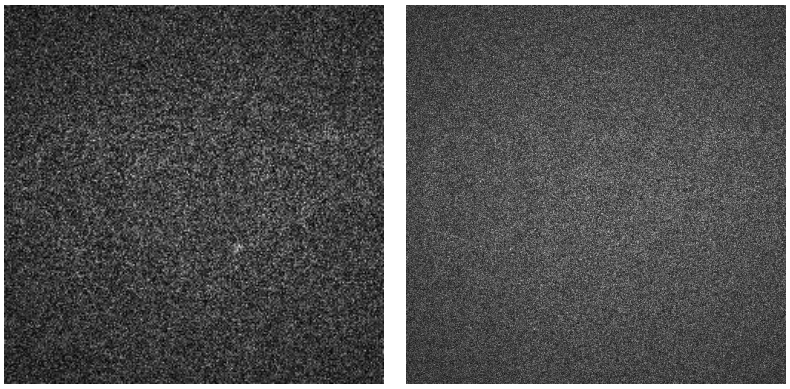


Figura 5.7 Coeficiente de correlación normalizado entre las imágenes desencriptadas empleando la longitud de onda de registro y una longitud de onda desplazada respecto a la de encriptación, para dos tamaños de objeto de entrada en un sistema de encriptación JTC.



a) b)

Figura 5.8 Imágenes desencriptadas correspondientes a una longitud de onda en la etapa de desencriptación de: a) $\lambda = 632\ nm + 14\ nm$ para el objeto de entrada de 2,56 x 2,56 mm^2 y b) $\lambda = 632\ nm + 22\ nm$ para el objeto de entrada 1,28 x 1,28 mm^2

En la **Figura 5.9** se muestran las curvas del coeficiente de correlación para el sistema JTC y 4*f* para un objeto de entrada de 2,56 x 2,56 mm^2. Se puede notar que el coeficiente de correlación tiene valores más bajos, en el sistema 4*f* respecto al JTC, para el mismo desplazamiento en la longitud de onda en el proceso de decodificación. Esto significa que

el sistema 4*f* es más sensible ante el cambio en longitud de onda, es decir se requiere un desplazamiento $\Delta\lambda$ menor en comparación con el que se requiere en un JTC, para que no se pueda recuperar la imagen desencriptada.

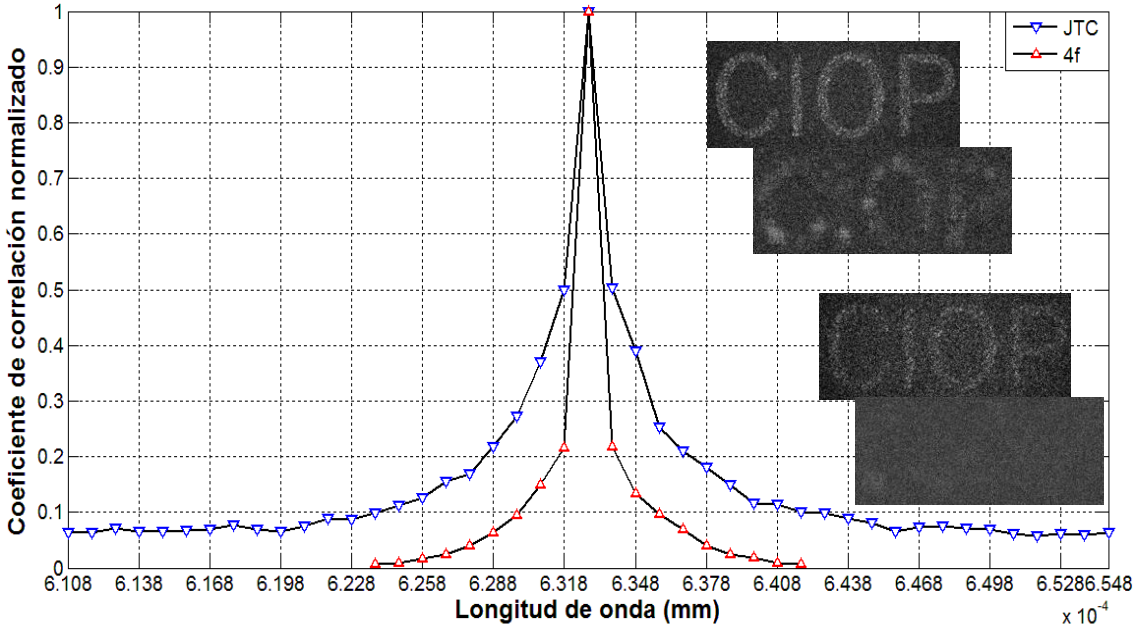
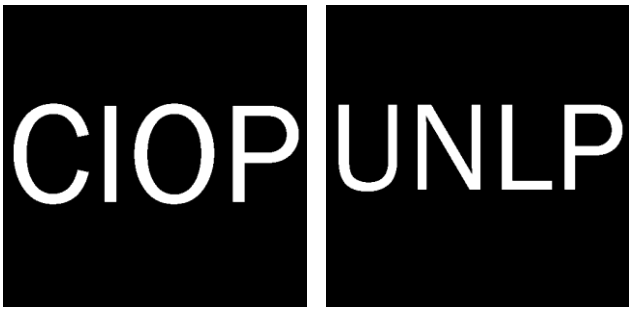


Figura 5.9 Coeficiente de correlación normalizado entre las imágenes desencriptadas empleando la longitud de onda de registro y una longitud de onda desplazada respecto a la de encriptación cuando el objeto de entrada tiene un tamaño de 2,56 x 2,56 mm^2 para las arquitecturas 4*f* y JTC.

A partir de los resultados anteriores, se implementó un multiplexado en longitud de onda para las imágenes mostradas en la **Figura 5.10 a)** y **b)** tanto para el sistema JTC cuanto para el 4*f*.



a) b)

Figura 5.10 a) y b) Imágenes binarias de 2,56 x2,56 mm^2 a ser encriptadas y almacenadas en un único medio de almacenamiento.

En la **Tabla 5.8** se presentan las imágenes desencriptadas en los sistemas JTC y 4*f* cuando se multiplexan la información encriptada de los objetos mostrados en la **Figura 5.10** y para tres desplazamientos de la longitud de onda ($\Delta\lambda$) en la etapa de encriptación.

La primera columna de la **Tabla 5.8** muestra el caso en que ambas arquitecturas el desplazamiento en la longitud de onda está por debajo del umbral de sensibilidad observándose en consecuencia solapamiento entre las imágenes reconstruidas. El solapamiento observado en la primera columna pone en evidencia la mayor sensibilidad a este parámetro en la arquitectura 4f que en la JTC, confirmado lo observado en la **Figura 5.9.** Es importante notar que para obtener un estado similar de entrecruzamiento de información entre canales consecutivos se necesita un $\Delta\lambda$ mayor para el JTC que para el 4f .

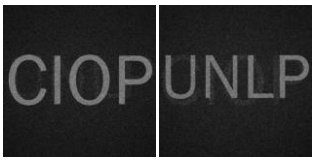
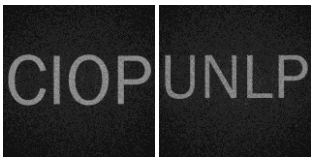
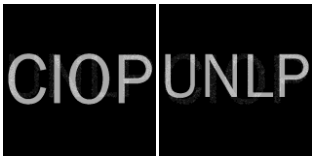
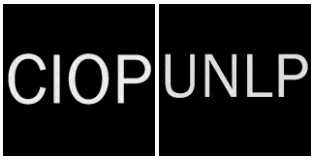
JTC	 $\Delta\lambda = 2\ nm$	 $\Delta\lambda = 4\ nm$	 $\Delta\lambda = 8\ nm$
4f	 $\Delta\lambda = 0.5\ nm$	 $\Delta\lambda = 1\ nm$	 $\Delta\lambda = 4\ nm$

Tabla 5.8 Imágenes desencriptadas cuando se multiplexan la información encriptada de los objetos mostrados en la Figura 5.10 y para tres desplazamientos de la longitud de onda en la etapa de encriptación en los sistemas JTC y 4*f*.

En el análisis anterior se evaluó la sensibilidad a la longitud de onda en términos del coeficiente de correlación. Sin embargo, también es posible el análisis utilizando el error cuadrático medio como se realizará a continuación.

Se evaluará un proceso de encriptación en la arquitectura JTC para codificar objetos de entrada en términos de la longitud de onda. En todos los casos la longitud de onda en la etapa de encriptación es de 640 nm. Dado que las curvas de correlación de la **Figura 5.7** muestran una dependencia con tamaño del objeto de entrada, en nuestro estudio consideraremos objetos con los siguientes tamaños: 400 x 400 píxeles, 300 x 300 píxeles y 200 x 200 píxeles. En la **Tabla 5.9**, se muestran las imágenes desencriptadas para los tres tamaños objetos mencionados y diferentes longitudes de onda en la etapa de recuperación.

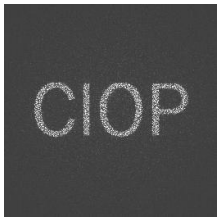
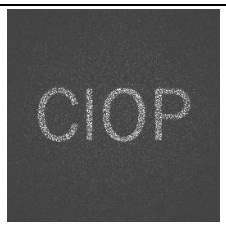
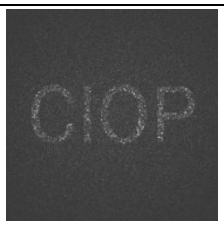
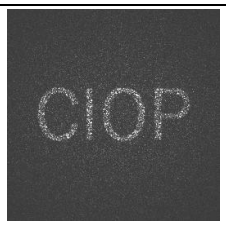
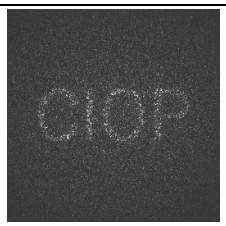
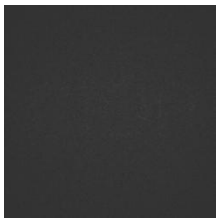
$\lambda_{\text{Lectura}}\,(nm)$	400 x 400 pix^2	300 x 300 pix^2	200 x 200 pix^2
640 nm			
636 nm	 MSE = 0.8003	 MSE = 0.6249	 MSE = 0.4334
632 nm	 MSE = 0.9676	 MSE = 0.9046	 MSE = 0.8036
628 nm	 MSE = 0.9789	 MSE = 0.97	 MSE = 0.923
624 nm	 MSE = 0.9708	 MSE = 0.9792	 MSE = 0.9934

Tabla 5.9) Resultados mostrando la reconstrucción del objeto de entrada encriptado, la palabra CIOP, para diferentes tamaños en píxeles y para una longitud de onda de lectura corrida con respecto a la que se usó en la etapa de registro. En los casos de la reconstrucción con la longitud de de onda corrida se indica el valor del MSE.

En la primera fila de la **Tabla 5.9**, se presentan las imágenes desencriptadas para la longitud de onda de encriptación (λ= 640 nm). Las imágenes desencriptadas de las

siguientes filas fueron obtenidas con una longitud de onda desplazada respecto a la empleada en la etapa de encriptación.

Para evaluar de manera cuantitativa la sensibilidad del sistema se analiza el error cuadrático medio (MSE) entre la imagen desencriptada con la longitud de onda correcta y aquella obtenida empleando una longitud de onda desplazada (ver **Figura 5.12**). Para la evaluación del MSE se emplearon los resultados mostrados en la **Tabla 5.9.**

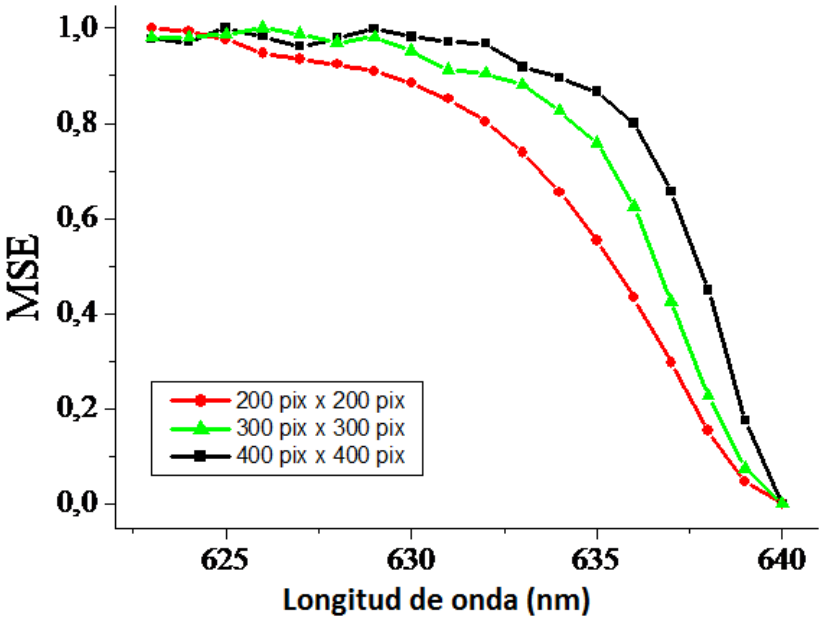


Figura 5.12 MSE en términos de la longitud de onda de lectura, cuando la longitud de onda de registro fue 640 nm.

Cada curva de la **Figura 5.12** muestra el comportamiento de la sensibilidad al desplazamiento en longitud de onda del sistema. En la curva correspondiente al objeto de 400 x 400 píxeles se observa que si $\Delta\lambda$= 4 nm el MSE=0.9. Para el mismo $\Delta\lambda$, el MSE=0.5 para el objeto de 200 x 200 píxeles. Este resultado confirma la dependencia de la sensibilidad con el tamaño del objeto de entrada. En resumen para un determinado valor del MSE de la imagen reconstruida existe una relación inversa entre el objeto de entrada y la sensibilidad del sistema.

La evaluación desarrollada en la Sección V.3.1 será el punto de partida para implementar procesos de multiplexado en longitud de onda sin solapamiento entre las imágenes desencriptadas.

V.4. Multiplexado en longitud de onda en una arquitectura JTC.

Como ya mencionamos la arquitectura JTC presenta ventajas en comparación con la 4f en su implementación óptica. Además, en el JTC la información encriptada tiene un carácter inherentemente holográfico y no requiere una onda de referencia adicional, lo que conllevaría a la conjugación de fase en la etapa de desencriptación. Asimismo el dispositivo es menos sensible al alineamiento lo que facilita la implementación experimental [5.10].

En esta Sección proponemos y estudiamos una técnica de multiplexado de longitud de onda en una arquitectura JTC. El empleo de técnicas de almacenamiento y recuperación de patrones encriptados que tienen dependencia espectral, reducen la necesidad de usar múltiples máscaras u otro tipo de mecanismos de posicionamiento para llevar a cabo el proceso de multiplexado facilitando la manipulación de imágenes en paralelo.

V.4.1. Principio del sistema

El proceso de multiplexado en la arquitectura JTC, implica almacenar varias imágenes encriptadas en el mismo medio de almacenamiento. El parámetro de multiplexado en este caso es la longitud de onda, por lo tanto cada imagen de entrada es encriptada con una longitud de onda diferente. Es evidente que el rendimiento de un sistema de múltiple almacenamiento de datos encriptados mejora si se disminuye el solapamiento.

Consideremos la encriptación de cuatro imágenes en el mismo medio. Los objetos de entradas son cuatro caracteres de 400 x 400 píxeles. Cada imagen encriptada es desencriptada con la misma longitud de onda que se empleó en la etapa de encriptación. Las imágenes desencriptadas se muestran en la **Tabla 5.10**. A lo largo de cada columna se muestran las imágenes desencriptadas para el mismo carácter de entrada. Para la salida desencriptada ubicada en la fila $\boldsymbol{m}$ y columna $\boldsymbol{i}$, la longitud de onda de encriptación

empleada es $\lambda_{mi} = \lambda_0 + (i-1)\Delta\lambda_{0\mathrm{m}}$ donde $m, i = 1, 2, 3, 4$ y $\Delta\lambda_{01} = 0$ nm , $\Delta\lambda_{02} = 2$ nm, $\Delta\lambda_{03} = 4$ nm, $\Delta\lambda_{04} = 8$ nm. Por lo tanto, las imágenes desencriptadas mostradas en la primera fila ($m = 1$) corresponden al caso en el que los caracteres de entrada son encriptados empleando la misma la longitud de onda $\lambda_0 = 640\ nm$ en todos los canales.

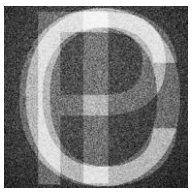
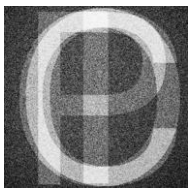
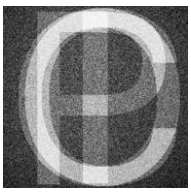
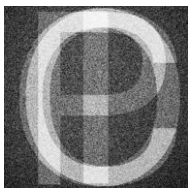
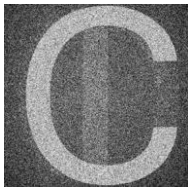
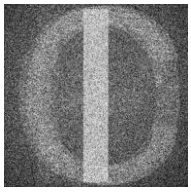
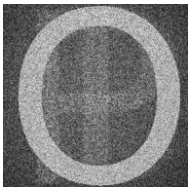
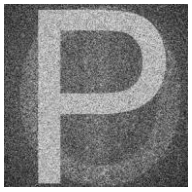
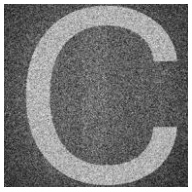
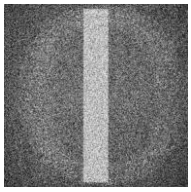
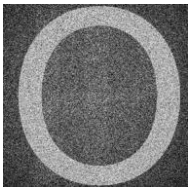
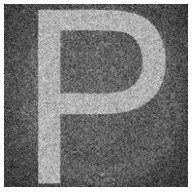
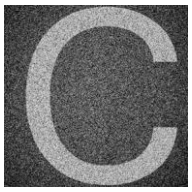
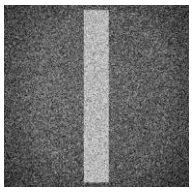
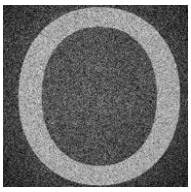
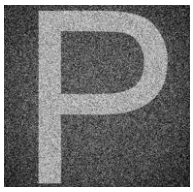
	i = 1	*i* = 2	*i* = 3	*i* = 4
m = 1 $\Delta\lambda_{01} = 0$ nm				
m =2 $\Delta\lambda_{02} = 2$ nm				
m = 3 $\Delta\lambda_{03} = 4$ nm				
m = 4 $\Delta\lambda_{04} = 8$ nm				

Tabla 5.10. Imágenes multiplexadas desencriptadas, cuando cara una fue desencriptada con la misma longitud de onda que fue encriptada. Estas salidas muestran que se revela la correcta información, a pesar de que se presenta un severo solapamiento porque cada carácter desencriptado es mostrado simultáneamente con los caracteres remanentes y todos ellos tienen la misma fidelidad.

En la segunda fila, $\Delta\lambda_{02} = 2\mathrm{nm}$ y cada imagen desencriptada presenta solapamiento aunque es menor que el presentado en la primera fila. En la tercera fila $\Delta\lambda_{03} = 4\mathrm{nm}$ el solapamiento es aún menor. En la cuarta fila que corresponde a un desplazamiento de 8 nm en la longitud de onda entre los caracteres correspondiente a caracteres adyacentes, se observa que el solapamiento desaparece y únicamente se presenta el ruido debido a las imágenes no desencriptadas.

Otra manera de ver el comportamiento de la sensibilidad consiste en observar el solapamiento entre los diferentes canales. Por ejemplo, para el caso m= 2, el desplazamiento en longitud de onda entre el carácter **C** e **I** es $\Delta\lambda = 2\,\text{nm}$, entre los caracteres **C** y **O** es $\Delta\lambda = 4\,\text{nm}$, mientras entre **C** y **P** es $\Delta\lambda = 6\,\text{nm}$, es evidente al reconstruir **C** una disminución gradual del solapamiento de los caracteres **I**, **O** y **P**. En resumen, se puede observar una disminución del solapamiento entre los caracteres en la imágenes desencriptadas cuando se aumenta el desplazamiento entre los diferentes caracteres encriptados (ver el comportamiento en **Tabla 5.10**).

Por lo tanto, en general, en un procedimiento de múltiple encriptación cuando se desencripta con la longitud de onda λ_i, la i^{esima} imagen desencriptada puede ser expresada,

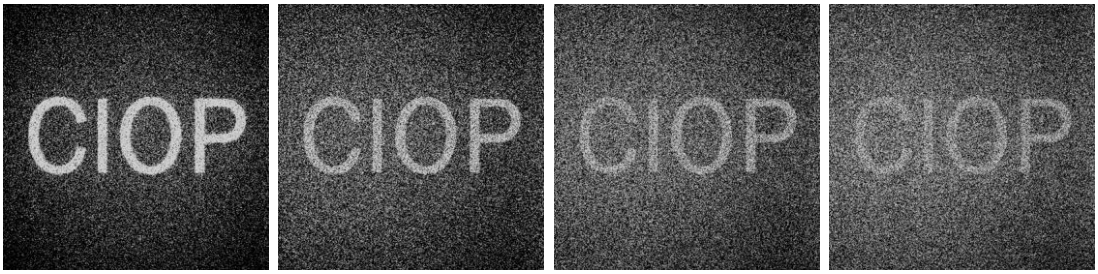
$$\hat{g}_i(x_2) = g_i(x_2) + n(x_2) \tag{5.10}$$

donde

$$n(x) = \sum_{j=1}^{N} W_j\left(x_2, \lambda_i + \Delta\lambda_{ij}\right) \quad i = 1 \ldots\ldots N \tag{5.11}$$

con $W_j\left(x_2, \lambda_i + \Delta\lambda_{ij}\right)$ es definida en la ecuación (5.9), $\Delta\lambda_{ij} = \lambda_j - \lambda_i \; y \; N$ es el número de imágenes multiplexadas. La mínima separación entre las longitudes de onda $\Delta\lambda_{min}$ para canales independientes en el proceso de multiplexado, debe tomar el valor que hace que el solapamiento $n(x)$ se vuelva ruido aleatorio para todos los canales. Desde este punto de vista, el solapamiento es determinado por la respuesta impulsiva de cada estado del sistema ó los parámetros del sistema y el tamaño del objeto de entrada. En nuestro caso, para un objeto de 400 x 400 píxeles resulta $\Delta\lambda_{min} = 8nm$.

La **Figura13** muestra los imágenes desencriptadas cuando un objeto de entrada de 400 x 400 pixeles es multiplexado N veces con N=10, 20 y 30 y un desplazamiento en longitud de onda $\Delta\lambda = 8nm$ entre canales adyacente que ausencia la ausencia de solapamiento. Se puede observar que el ruido se incrementa a medida que aumenta el número de imágenes multiplexadas. Esto establece un límite al número de imágenes que se pueden multiplexar compatible con una relación señal-ruido establecida por el usuario.



N=1 (a) N=2 (b) N=20 (c) N=30 (d)

Figura 13: Secuencia de imágenes de un canal desencriptado correspondiente al multiplexado de N imágenes encriptadas a) N=1, b) N=10, c) N=20 y d) N=30. (el tamaño de la imagen de entrada es de 400 x 400 píxeles).

Cuando se quiere caracterizar el rendimiento de un sistema de multiplexado de información encriptada, es necesario determinar el máximo número N_{max} que el sistema tolera. El criterio para determinar el valor de N_{max} se determina a partir del MSE y el coeficiente de correlación entre la imagen desencriptada para el N ^{esimo} canal y el objeto de entrada.

V.5. Encriptación digital de imágenes a color empleando una arquitectura JTC.

El multiplexado en longitud de onda permite la encriptación de imágenes a color. Recordemos que una imagen en color verdadero está compuesto por tres canales, uno rojo, otro verde y otro azul (RGB). La combinación de estos tres canales de color producen una imagen final a color. En esta Sección presentamos un método de encriptación de imágenes a color, en el cual cada canal de color es encriptado independientemente y multiplexado en un único medio de registro [5.11]. El multiplexado se realiza con las mismas máscaras llave y modificando para cada canal de color la longitud de onda.

V.5.1. Descripción de la técnica

La **Figura 5.13 a)** se muestra el esquema para encriptar imágenes en color en una arquitectura JTC. Una de las aberturas del JTC contiene la información de la imagen

correspondiente a un determinado canal de color adosado a una máscara de fase pura aleatoria, mientras que la otra abertura contiene la máscara llave. Los canales de color, asociados a las longitudes de onda 640 nm, 520 nm y 470 nm, son encriptado independientemente en el mismo medio de almacenamiento. El speckle modulado (JPS), generado por las máscaras aleatorias del plano de entrada depende de la longitud de onda, entonces la variación en la longitud de onda de iluminación producirá un cambio correspondiente en el JPS. El procedimiento descrito en la Sección V.3.1.1 es aplicado a la encriptación de cada canal de color.

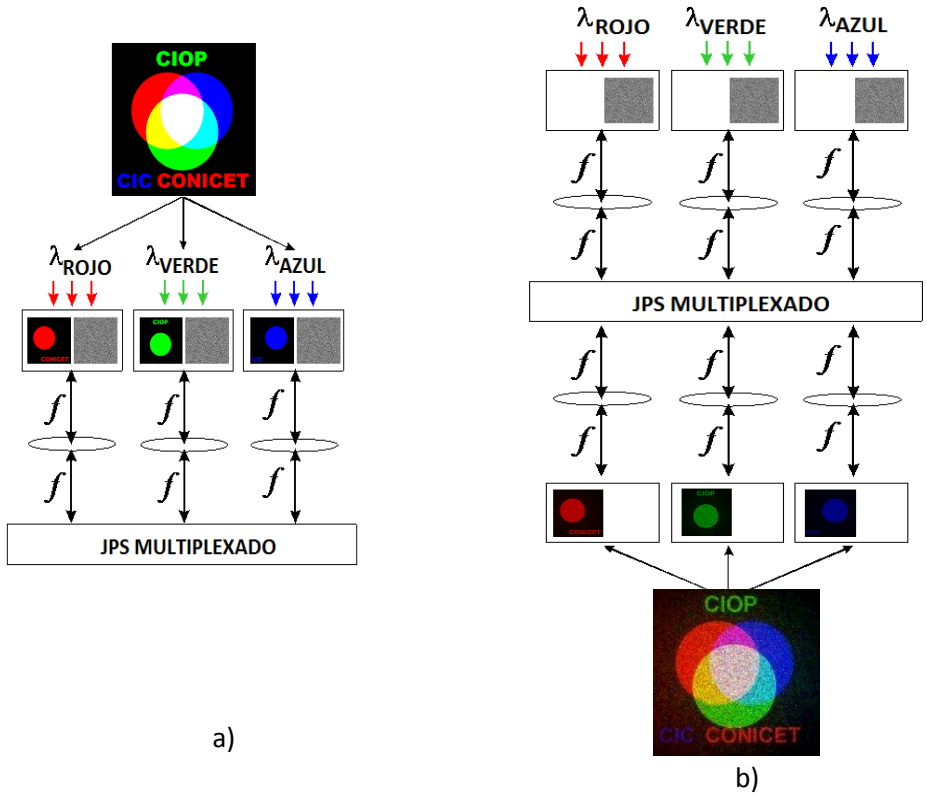


Figura 5.13. Esquema del proceso de encriptación de imágenes en color, usando un multiplexado en longitud de onda en una arquitectura JTC. a) Etapa de ecnriptación y multiplexado. b) Etapa de desencriptación y composición de la imagen en color.

Es importante puntualizar que la diferencia de longitud de onda de encriptación de los canales de color (verde-rojo $\Delta\lambda_{\mathrm{GR}} = 120\ \mathrm{nm}$ y azul-verde es $\Delta\lambda_{\mathrm{AG}} = 50\ \mathrm{nm}$) garantiza que no existe solapamiento entre las imágenes desencriptadas. Entonces, los patrones encriptados para cada canal $JPS(rojo)$ $JPS(verde)$ y $JPS(azul)$ no estén correlacionados. Esto permite almacenar en el mismo medio los tres patrones, es decir el JPS multiplexado, $MJPS = JPS(rojo) + JPS(verde) + JPS(azul)$. El medio de almacenamiento, debe ser un dispositivo que responda linealmente a la intensidad, de tal

manera que el patrón encriptado sea una transmitancia, proporcional al $MJPS$. La ecuación (5.1) de la Sección 5.3.1 muestra una representación matemática del JPS. En la siguiente ecuación se muestra el tercer que proporciona la imagen desencriptada del $MJPS$ con un multiplexado RGB.

$$MJPS_3(R,G,B) = \sum_{C=R,\ G,\ B} \frac{1}{(\lambda_C f)^2}\left[G_i\left(\frac{x_1}{\lambda_C f}\right) \otimes R\left(\frac{x_1}{\lambda_C f}\right)\right] H^*\left(\frac{x_1}{\lambda_C f}\right) e^{i2\pi(2Y)\frac{x_1}{\lambda_C f}} \quad (5.12)$$

En la etapa de desencriptación, representada por el esquema de la **Figura 5.13 b)** se requiere iluminar el $MJPS$ con la transformada de Fourier de la máscara llave. Para obtener la imagen desencriptada de cada componente de color, la longitud de onda de iluminación debe coincidir con la empleada en la etapa de encriptación para que la información de dicho canal se recupere. Es decir, la distribución de fase aleatoria de la transformada de Fourier de la llave generada con la longitud de onda λ_C, $H\left(\frac{x_1}{\lambda_C f}\right)$, solo puede compensar la distribución de fase $H^*\left(\frac{x_1}{\lambda_C f}\right)$ correspondiente al término de la sumatoria de la ecuación (5.12) que corresponde al canal C. Por ejemplo, cuando se ilumina la máscara llave con la longitud de onda del canal rojo λ_R, el campo en el plano de encriptación sería:

$$S_3(\lambda_R) = \frac{1}{i(\lambda_R)f} H\left(\frac{x_1}{\lambda_R f}\right) e^{-i2\pi Y\frac{x_1}{\lambda_R f}}\, MJPS_3(R,G,B) =$$

$$\frac{1}{i(\lambda_R f)^3}\left[G_R\left(\frac{x_1}{\lambda_R f}\right) \otimes R\left(\frac{x_1}{\lambda_R f}\right)\right] e^{i2\pi(Y)\frac{x_1}{\lambda_R f}} +$$

$$\sum_{C=G,B} MJPS_3(G,B)\frac{1}{i(\lambda_R)f} H\left(\frac{x_1}{\lambda_R f}\right) e^{-i2\pi Y\frac{x_1}{\lambda_R f}} \quad (5.13)$$

donde el último término de la ecuación (5.13), corresponde a los patrones encriptados de los dos canales restantes, G y B , donde la distribución de fase de la transformada de la llave $H\left(\frac{x_1}{\lambda_R f}\right)$, no puede compensar las fases del canal G, $H^*\left(\frac{x_1}{\lambda_G f}\right)$ y del canal B, $H^*\left(\frac{x_1}{\lambda_B f}\right)$. Para obtener la información del canal rojo desencriptada, se transforma Fourier $S_3(\lambda_R)$ y se obtiene:

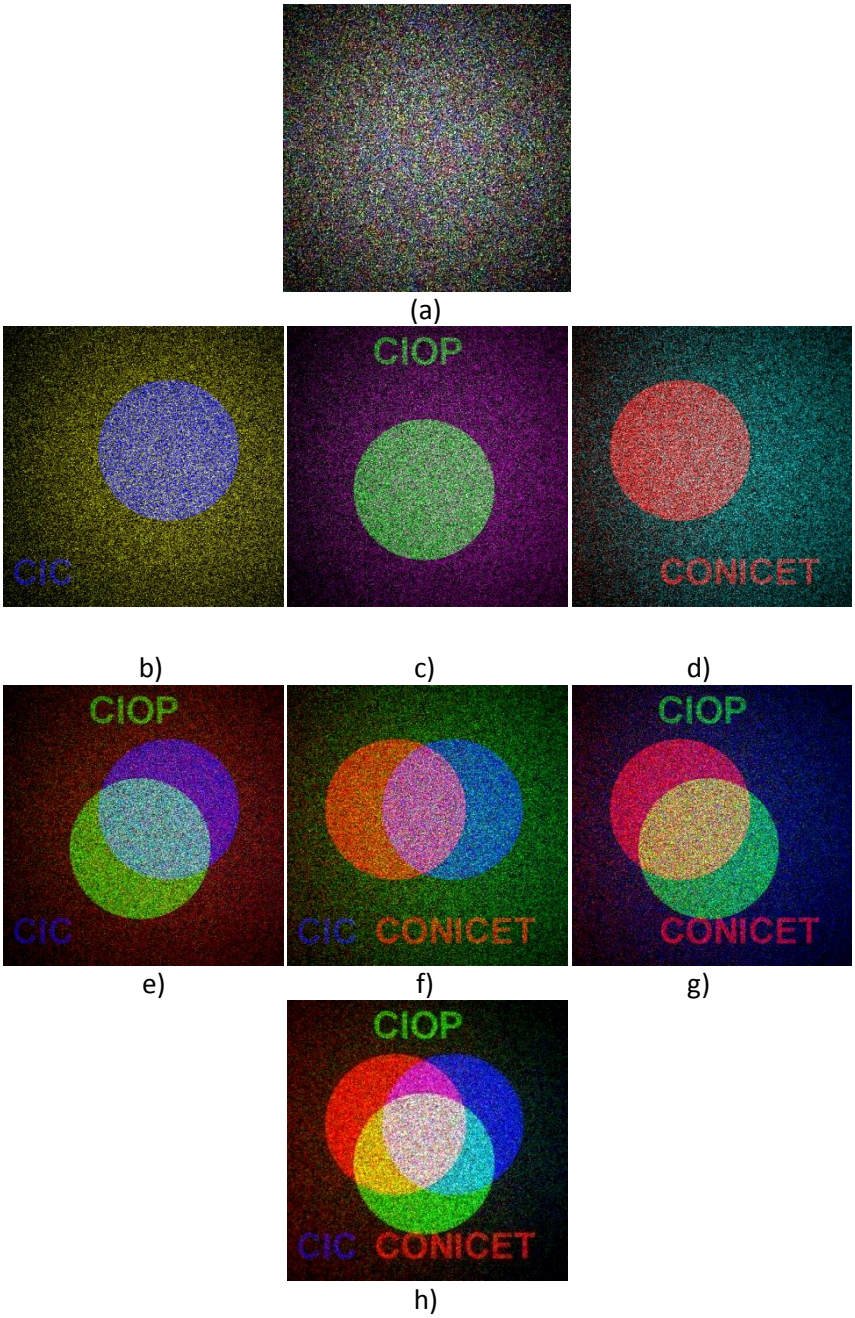
$$\Im\{S_3(\lambda_R)\} = \frac{e^{i\pi}}{(\lambda_R f)^2}\left[g_R(-x_2)\ \mathrm{r}(-\mathrm{x}_2)\right] \otimes \delta(-x_2 - Y) + \Im\left\{\sum_{C=G,B} MJPS_3(G,B)\frac{1}{i(\lambda_R)f} H\left(\frac{x_1}{\lambda_R f}\right) e^{-i2\pi Y\frac{x_1}{\lambda_R f}}\right\} \qquad (5.14)$$

Cuando se observa con un detector sensible a la intensidad, de manera que $\mathrm{r}(-\mathrm{x}_2)$ no pueda ser observada, se obtiene la imagen desencriptada correspondiente al canal rojo $g_R(-x_2)$ y el ruido debido a las imágenes no desencriptadas del canal G y B, representado por el último término de la ecuación (5.14). Siguiendo el mismo procedimiento, al iluminar secuencialmente el $MJPS$ con la longitud de onda del canal G y B se obtienen las imágenes desencriptadas de dichos canales. Finalmente, se compone a partir de las imágenes recuperadas de los canales de color la imagen en color verdadero.

Como demostramos, durante el proceso de desencriptación de un canal, se debe utilizar la misma máscara llave y la misma longitud de onda, que se usó en la etapa de encriptación. Cuando se usa una máscara llave incorrecta y/o una longitud de onda incorrecta en la reconstrucción, los datos de entrada no pueden ser recuperados y solamente aparece ruido en el plano de salida. En resumen, la longitud de onda actúa como una llave extra de codificación de la misma manera que la máscara llave.

En la **Figura 5.14 a)** a la **Fig 5.14 g)** se muestran los resultados de la implementación digital del multiplexado cuando la máscara de fase es correcta y al menos una de las longitudes de onda de desencriptación es incorrecta. Esto implica que al menos uno de los canales de color produzca una señal de ruido. Los datos recuperados correspondientes a la primera fila fueron obtenidos cuando todas las longitudes de onda son incorrectas.

Las imágenes de la segunda y la tercera fila, de la **Figura 5.14** fueron obtenidas cuando la longitud de onda asociada a sólo uno ó dos canales es correcta, respectivamente.



(a)

b) c) d)

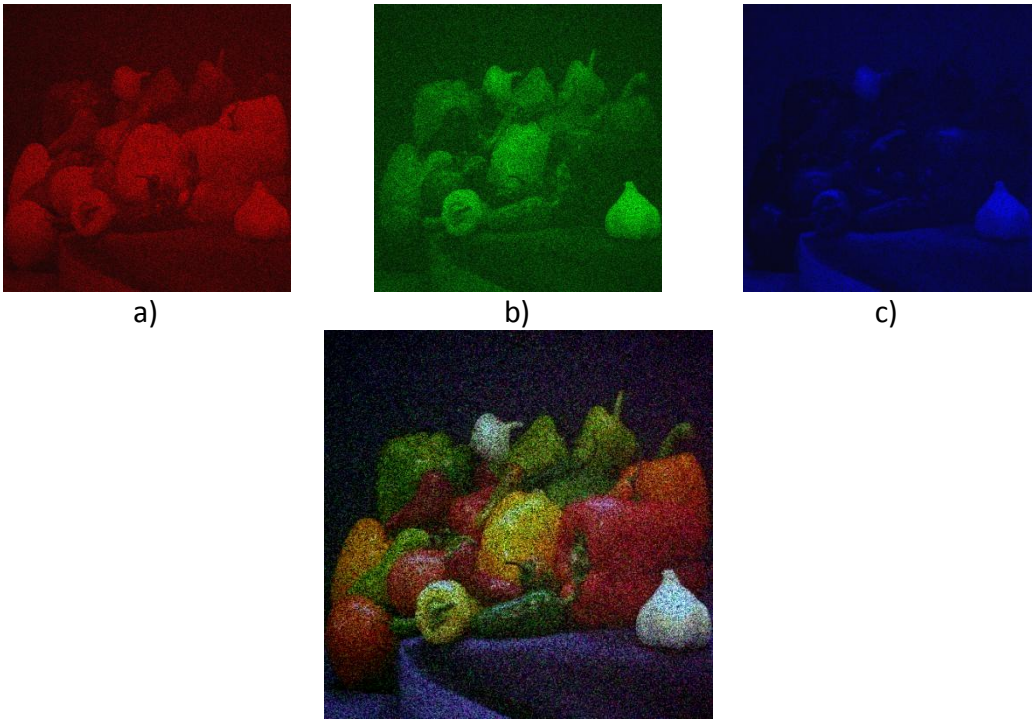
e) f) g)

h)

Figura 5.14 Imágenes desencriptadas en color verdadero cuando se obtiene solo ruido en el canal: a) rojo, verde y azul; b) rojo y verde; c) rojo y azul; d)verde y azul; e) rojo; f) verde; g) azul; h) ninguno.

En estos casos no se puede recuperar la información completa de color del objeto de entrada. Es decir, la información de color de la imagen se modifica. Cuando se emplea una longitud de onda incorrecta, aparece ruido en el plano de salida. Se pude observar en la segunda fila de la **Figura 5.14** que el color del ruido, coincide con la longitud de onda correspondiente al canal mal desencriptado. En el caso de dos canales de color incorrectos, fila 3 **Figura 5.14,** el color del ruido corresponde a la combinación de las

longitudes de onda de los canales mal desencriptados. Estos resultados corresponden a una imagen en color verdadero, donde la información de los canales corresponde a imágenes binarias. En la **Figura 5.15** se muestra un multiplexado digital de una imagen en color verdadero, compuesta por imágenes en niveles de gris para cada canal.



a) b) c)

d)

Figura 5.15. Imagen en verdadero color compuesta a partir de las imágenes desencriptadas del canal a) rojo, b) verde, c) azul, cuando se hace un multiplexado RGB en longitud de onda.

En este caso se empleó JTC optimizado descrito en la Sección IV.7.2 capítulo IV.

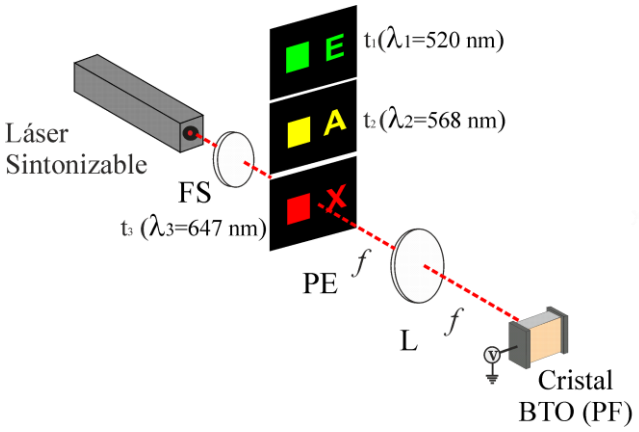
V.6. Multiplexado experimental usando múltiples longitudes de onda en una arquitectura JTC.

El análisis de la Sección anterior reveló que se puede usar la longitud de onda como un parámetro de multiplexado de datos encriptados en una arquitectura JTC. En esta Sección se verificará experimentalmente el empleo de la longitud de onda como parámetro de codificación [5.12], lo que constituye el principio básico para el almacenamiento seguro de imágenes en color. En nuestro conocimiento no hay

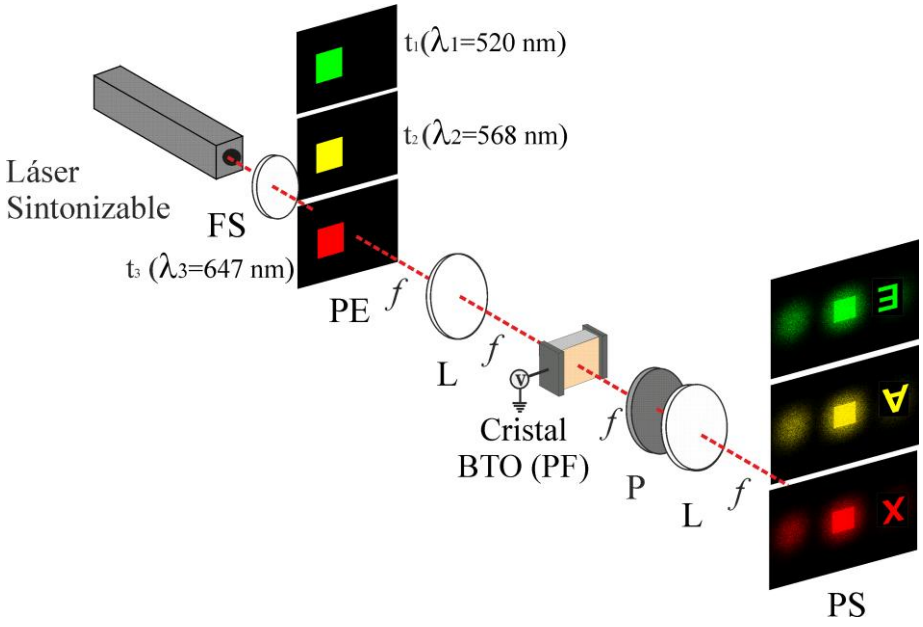
comunicaciones que reporten resultados experimentales de múltiple encriptación en longitud de onda.

V.6.1. Descripción del montaje experimental

El esquema experimental de encriptación en longitud de onda basada en la arquitectura JTC coincide con lo propuesto en la Sección anterior. Un medio de almacenamiento holográfico representa una interesante opción para implementar experimentalmente el mencionado esquema de codificación. En particular, los materiales fotorrefractivos con su capacidad de lectura y escritura en paralelo, alta velocidad de recuperación de información, alta capacidad de almacenamiento es una alternativa válida. En esta propuesta se emplea como medio de almacenamiento un cristal fotorrrefractivo. El sistema experimental utilizado es esquematizado en la **Figura 5.16.** Las diferentes longitudes de onda de la fuente de iluminación son provistas mediante un láser sintonizable de Ar-Kr. En el experimento de las líneas disponibles del láser, se seleccionaron las longitudes de onda 647nm, 568 nm y 520 nm. La eficiencia de difracción en un cristal BTO incluye un factor de absorción. No se seleccionaron longitudes de onda en la región azul del espectro dado que en este rango el coeficiente de absorción es muy alto.



a)



b)

Figura 5.16 Esquema experimental para el multiplexado en color usando un cristal fotorrefractivo como medio de almacenamiento. a) Etapa de encriptación, b) Etapa de desencriptación. (FS: filtro espacial, PE: plano de entrada, L: lente, P: polarizador, PS: plano de salida. *f:* distancia focal (100 mm)).

La implementación óptica realizada emplea como medio de almacenamiento un cristal tipo selenita BTO. El cristal está cortado en la configuración electro-óptica transversal. Las direcciones $(1\bar{1}0)$, (001) y (110) del cristal coinciden con los ejes XYZ del sistema y sus dimensiones lineales son $L_x = L_y = L_z = 8$ mm, respectivamente.

Como se había mencionado, si se cambia la longitud de onda de iluminación y se mantiene la máscara llave, el patrón encriptado (JPS) se modifica. Para proceder con el multiplexado, cada objeto de entrada es encriptado con una longitud de onda diferente y es secuencialmente almacenado en el mismo cristal, generando un JPS multiplexado.

Las tres imágenes en color fueron encriptadas independientemente usando las longitudes de onda del láser seleccionadas. El proceso de encriptación se muestra en el esquema de la **Figura 5.16 a).**

Durante el proceso de decodificación, la máscara llave es localizada en el plano de entrada e iluminada con un haz colimado cuya longitud de onda coincide con la empleada en la etapa de encriptación del canal que se desea recuperar (ver **Figura 5.16 b))**. De esta manera se logra que el JPS multiplexado sea iluminado con la Transformada de Fourier de

la llave y la longitud de onda correcta permitiendo obtener en el plano de salida la imagen desencriptada deseada.

Si alguna de las llaves (difusor llave, ó longitud de onda de iluminación) no es la correcta, la distribución de intensidad en la CCD es un patrón de ruido. La imagen desencriptada solo aparece cuando se usa la correcta combinación de llaves. Sin embargo, aparecerá en cada imagen correctamente desencriptada ruido debido a los restantes canales no desencriptados. Es inevitable que se presente ruido debido a las imágenes no desencriptadas.

En la **Figura 5.17 a)** se muestran tres imágenes desencriptadas empleando la longitud de onda correcta en la implementación experimental del multiplexado en longitud de onda propuesto. En la **Figura 5.17 b)** se presentan los resultados simulados de la misma implementación, pero obtenidos mediante un sistema de óptica virtual.

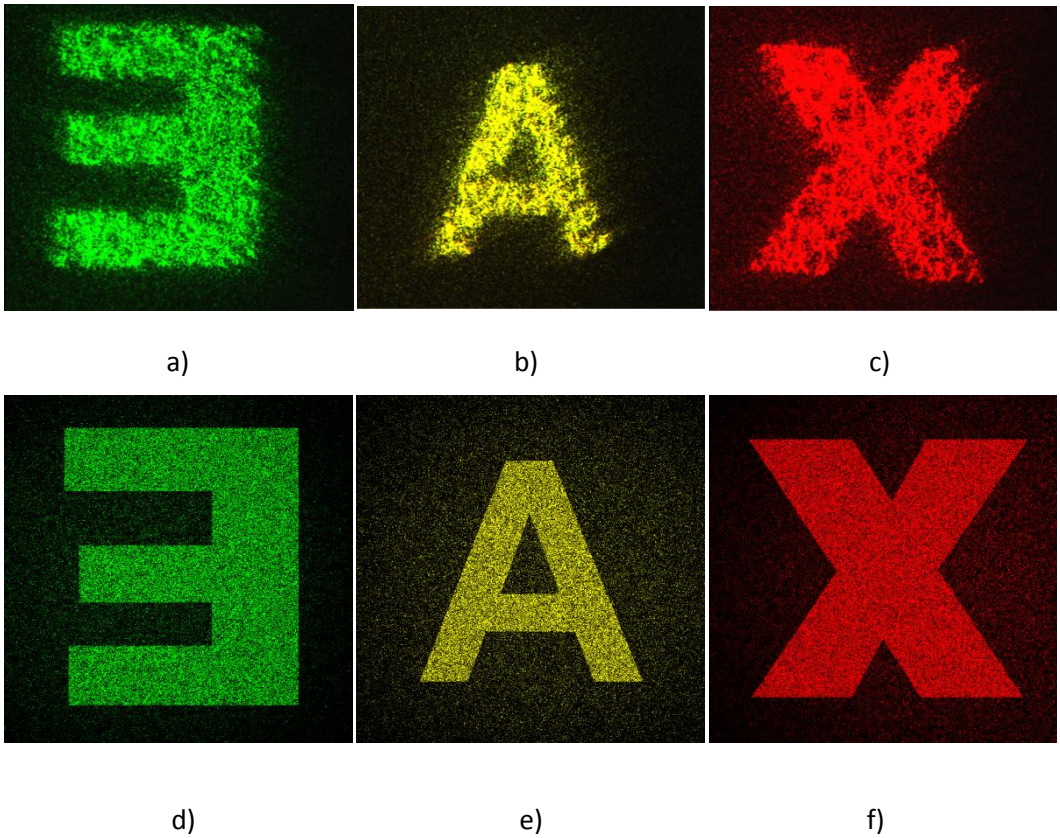


Figura 5.17 Imágenes experimentales y simuladas desencriptadas para tres canales de color. Canal verde ($\lambda_1 = 520$)nm a) experimental y d) simulada; canal amarillo ($\lambda_2 = 568$)nm: b) experimental y e) simulada; canal rojo ($\lambda_3 = 647$) c): experimental, f) simulada.

V.7. Conclusiones.

Multiplexar es almacenar múltiple información en un único medio. En este capítulo se estudió el múltiple almacenamiento de información encriptada cuando se emplea un medio de registro plano. En particular, se analizo de que manera las condiciones de trabajo (arquitecturas, tamaño objeto de entrada, parámetros ópticos) afectan los procesos de multiplexado.

Cuando se decodifica la información de un canal en un proceso de multiplexado, aparece ruido en la imagen desencriptada debido a las imágenes no desencriptadas. Esto determina un límite en el número de objetos que se puede almacenar en un dado medio. Por otro lado, en el estudio de capítulos anteriores se demostró que no es necesario disponer del 100% del patrón encriptado para obtener en la etapa de decodificación una imagen desencriptada donde se pueda reconocer el objeto de entrada, lo que indica que existe redundancia de información en el patrón encriptado. La redundancia es la razón fundamental que permite almacenar múltiples datos encriptados en un medio de registro plano. Aun más, la redundancia es el factor determinante del número máximo de objetos que se pueden multiplexar.

Se determinó en las arquitecturas 4f y JTC el mínimo porcentaje de datos encriptados necesarios para que en la imagen desencriptada se pueda reconocer la información del objeto. Se comprobó, que existe una relación entre el total de la información encriptada y el mínimo porcentaje de datos encriptados que condiciona el número máximo de imágenes encriptadas que el sistema permite multiplexar.

Se debe destacar que el mínimo porcentaje de datos encriptados depende fuertemente del tamaño del objeto de entrada para la arquitectura 4f, en cambio en la arquitectura JTC no se observa esa dependencia. En consecuencia, la capacidad de multiplexado para un sistema de encriptación 4f aumenta significativamente a medida que el tamaño de objeto de entrada disminuye para un medio de almacenamiento fijo. Esto implica que en un proceso de multiplexado, el sistema 4*f* es más versátil y permite

incrementar significativamente la capacidad de almacenamiento de datos en comparación con el JTC.

Para la correcta implementación de un proceso de multiplexado, es necesario que los patrones encriptados correspondientes a diferentes canales estén decorrelacionados, esto garantiza que no haya solapamiento de información en las imágenes desencriptadas. Una opción para obtener patrones encriptados decorrelacionados es cambiar la longitud de onda. En ese sentido estudió la sensibilidad a la longitud de onda y esto habilitó la implementación de un multiplexado con este parámetro.

Se realizó un multiplexado en longitud de onda en la arquitectura JTC. En esta propuesta, se verificó digital y experimentalmente que para la correcta recuperación de la información de cada canal, es necesario conocer la máscara llave y la longitud de onda asociada a ese canal.

Dado que una imagen en color verdadero es posible descomponerla en canales puros de color, se implementó una encriptación de imágenes en color usufructuando el multiplexado en longitud de onda.

V.8. Referencias.

[5.1] Fai H. Mok, “Angle-multiplexed storage of 5000 holograms in lithium niobate”, Opt. Lett. 18, 915-917 (1993).

[5.2] C. C. Sun, W. C. Su, B. Wang, Y. Ouyang. “Diffraction sensitivity of holograms with random phase encoding”, Opt. Commun. 175, 67–74 (2000)

[5.3] C. C. Sun, W. C. Su. “Three dimensional shifting selectivity of random phase encoding in volume holograms”, App. Opt. 40, 1253-1260 (2001)

[5.4] C. C. Sun, W. C. Su, B. Wang, A. E.T. Chiou. “Lateral shifting of a ground glass for holographic encryption and multiplexing using phase conjugate readout algorithm”, Opt. Commun. 191, 209–224 (2001).

[5.5] O. Matoba, B. Javidi. “Encrypted optical memory system using three-dimensional keys in the Fresnel domain”. Opt Lett. 24, 762-764 (1999) .

[5.6] 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).

[5.7] J. F. Barrera, R. Henao, M. Tebaldi, N. Bolognini, R. Torroba, “Multiplexing encrypted data by using polarized light”, Opt. Commun. 260, 109-112 (2006).

[5.8] R. Henao, E. Rueda, J. F. Barrera, R. Torroba, "Noise-free recovery of optodigital encrypted and multiplexed images", Opt. Lett. 35, 333-335 (2010).

[5.9] G. Situ, J. Zhang. “Multiple-image encryption by wavelength multiplexing”, Opt. Lett. 30, 1306-1308 (2005).

[5.10] D. Amaya, M. Tebaldi, R. Torroba, N. Bolognini, “Wavelength multiplexing encryption using joint transform correlator architecture”, Appl. Opt. 48, 2099-2104 (2009)

[5.11] D. Amaya, M. Tebaldi, R. Torroba, N. Bolognini. “Digital color encryption using a multi-wavelength approach and a joint transform correlator”, J. Opt. A: Pure Appl. Opt. 10, 104031 (2008)

[5.12] M. Tebaldi, S. Horrillo, E. Pérez-Cabré, M. Millán, D. Amaya, R. Torroba, N. Bolognini."Experimental color encryption in a joint transform correlator architecture", J. Phys. : Conf. Ser. 274, 12054-12059 (2011).

[5.13] F. Mosso, J. F. Barrera, M. Tebaldi, N. Bolognini, R. Torroba, "All-optical encrypted movie", Opt. Express 19, 5706-5712 (2011)

[5.14] F. Mosso, M. Tebaldi, J.F. Barrera, N. Bolognini, R. Torroba, "Pure optical dynamical color encryption", Opt. Express 19, 13779-13786 (2011)

[5.15]L. Cabezas, M. Tebaldi, J. F. Barrera, N. Bolognini, R. Torroba, "Optical smart packaging to reduce transmitted information", Opt. Express 20, 158-163 (2012).

[5.16] J.F. Barrera R., M. Tebaldi, R. Torroba, N. Bolognini. "Multiplexing encryption technique by combining random amplitude and phase masks", Optik 120, 351-355 (2009).

[5.17] J.F. Barrera, R. Henao, M. Tebaldi, R. Torroba, N. Bolognini "Digital encryption with undercover multiplexing by scaling the encoding mask", Optik 120, 342-346 (2009).

[5.18] Yong-Liang X, et al. "Key rotation multiplexing for multiple-image optical encryption in the Fresnel domain", Opt Laser Technol 43, 889‑894 (2011).

[5.19] E. Rueda, J. F. Barrera, R. Henao, R. Torroba, "Lateral shift multiplexing with a modified random mask in a joint transform correlator encrypting architecture", Opt. Eng. 48, 027006 (2009).

[5.20] U. Gopinathan, T. J. Naughton, J. T. Sheridan, "Polarization encoding and multiplexing of two-dimensional signals: application to image encryption", Appl. Opt. 45, 5693–5700 (2006).

[5.21] G. Situ, J. Zhang, "Double random-phase encoding in the Fresnel domain", Opt. Lett. 29, 1584-1586 (2004).

[5.22] J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, N. Bolognini, "Code retrieval via undercover multiplexing", Optik. 119, 139-142 (2008).

[5.23] L. Chen, D. Zhao. "Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms", Opt. Express 14, 8552-8560 (2006).

[5.24] M. Joshi, Chandrashakher, K. Singh. "Color image encryption and decryption using fractional Fourier transform", Opt. Commun. 279 ,35-42 (2007).

[5.25] R. Henao, E. Rueda, J. F. Barrera, R. Torroba, "Noise-free recovery of optodigital encrypted and multiplexed images" , Opt. Lett. 35, 333-335 (2010).

CAPÍTULO VI

Aplicaciones de multiplexado canales de información

VI.1 Introducción

El objetivo de los ataques a los métodos ópticos de encriptación es obtener la información de la máscara llave o máscara de encriptación y se basan en la linealidad de estos sistemas. En la literatura se demuestra que conociendo un par objeto de entrada-información encriptada, se puede obtener la máscara llave y así decodificar la información de entrada a partir de los datos encriptados, tanto para la arquitectura 4f [6.1] cuanto para la JTC [6.2]. Las estrategias de ataque suponen que para la relación objeto de entrada-información encriptada existe una única máscara llave. Es claro que cuando se implementa un procedimiento de multiplexado (en un medio plano), a múltiples objetos de entrada les corresponde un único patrón encriptado. El multiplexado implica el uso de múltiples máscaras llaves ó el cambio de algún parámetro si se usa la misma máscara llave, lo que hace el sistema mucho más complejo. En el proceso de desencriptación la información deseada es recuperada mediante la selección adecuada de los parámetros asociados a cada canal. El multiplexado mejora la seguridad de los sistemas ópticos de codificación, debido a que es muy difícil identificar el número de imágenes encriptadas que están almacenadas en el medio de registro. Esto se debe a la naturaleza de la información encriptada, dado que la suma patrones de ruido blanco aleatorio dan como resultado un nuevo patrón de ruido blando donde las distribuciones encriptadas individuales asociadas a cada canal son indistinguibles. No tenemos conocimiento de reportes de ataques exitosos a sistemas ópticos de múltiple almacenamiento de información encriptada.

Por otro lado, existen algunas estrategias basadas en el multiplexado que buscan aumentar aún más la seguridad en los sistemas ópticos de codificación. Una de las estrategias se basa en confundir a un usuario no autorizado que haya tenido acceso a la información encriptada y a una llave pública. Dicha llave da acceso a información de entrada incorrecta, mientras que el verdadero mensaje está escondido y se requiere conocer una llave extra (llave privada) para recuperar la información. En Ref. [6.3] la máscara llave es pública y el escalamiento representa la llave privada. El usuario que intercepta la máscara recuperara la imagen incorrecta y no el mensaje encubierto para el que necesito conocer el escalamiento de la máscara. También para un sistema 4*f* J. Barrera et al [6.4], utilizan la variación del tamaño de la pupila del sistema óptico como parámetro extra de multiplexado. La información encubierta está contenida en uno de los canales generados con el tamaño de pupila escalada, razón por la cual, se debe conocer el escalamiento además de tener la máscara llave correcta para poder acceder al mensaje verdadero. Dentro de las estrategias de ocultamiento, J.Rosen y B. Javidi [6.5], proponen una técnica donde se codifica un mensaje dentro de una variación de una imagen "*halftone"*. La manera de recuperar la información oculta es mediante una correlación espacial con una única función filtro. Posteriormente, D. Abookasis et al. [6.6] utilizan este principio de ocultamiento, para codificar un mensaje tipo marca de agua, dentro de dos imágenes ("*halftone"*). Una de ellas está codificada por el mensaje oculto y la otra por el filtro. Para recuperar la información escondida se requiere utilizar una arquitectura tipo JTC para correlacionar las dos imágenes y obtener en los órdenes cruzados del plano de salida el mensaje decodificado.

Por otra parte, es necesario en algunos casos controlar el acceso a lugares seguros. Asimismo, en los sistemas donde hay múltiples usuarios, es necesario proteger la información de manera que sea accesible solo a determinados usuarios. En este sentido, los sistemas de multiplexado de información encriptada representan una alternativa válida, dado que permiten utilizar los diferentes canales de información para controlar el nivel de acceso por parte de los usuarios. En ese sentido, J.F. Barrera y R. Torroba [6.7], proponen el uso de máscaras de amplitud superpuesta a la máscara llave de fase pura en un sistema 4*f* para generar canales independientes de información. El uso de las máscaras

de amplitud, permiten seleccionar porciones distintas de la máscara llave para cada registro de un objeto de entrada en la epata de encriptación. En la etapa de desencriptación, la información recuperada dependerá de la combinación entre la máscara de amplitud y la máscara llave utilizada. Con estas estrategias se logra mediante el empleo de un conjunto de parámetros adicionales y de un único patrón encriptado, que diferentes usuarios tengan acceso a distinta información en el plano de salida del sistema.

En este capítulo, se presentan dos técnicas de multiplexado que permiten generar seguridad adicional en los sistemas de encriptación (sección 6.2) y crear diferentes niveles de acceso a la información encriptada (sección 6.3).

VI.2 Encriptación multicanal tipo rompecabezas.

El sistema de codificación con doble máscara de fase aleatoria requiere de un preciso alineamiento en el proceso de desencriptación, cuya sensibilidad depende de las características de la máscara llave. En este caso, una imagen no puede ser recuperada si la posición de la máscara de fase aleatoria no coincide con la utilizada en el proceso de encriptación. Aunque esta característica podría ser interpretada como una desventaja, puede ser utilizada para múltiple encriptación [6.8]. Otros ejemplos de parámetros llave extra en sistemas de encriptación son el estado de polarización [6.9], el uso de diferentes pupilas en la lente de codificación [6.10] ó diferentes longitudes de onda [6.11] para encriptar cada imagen de entrada. Todos estos parámetros mejoran la robustez del sistema y son adecuados para el almacenamiento de múltiples imágenes encriptadas en un único medio de registro. En estos sistemas ópticos de encriptación, los datos de entrada se codifican de tal forma que solo el uso de la llave correcta y el conjunto correcto de parámetros ópticos en la etapa de desencriptación permite revelar la información de entrada.

El principio básico de nuestra propuesta consiste en disociar una imagen de entrada en varias partes (descomponer la imagen tipo rompecabezas), cada una de estas imágenes

es encriptada independientemente y finalmente todas son multiplexadas en un único medio con el fin de incrementar la seguridad de los datos. Para evitar el solapamiento entre las la información desencriptada correspondiente a cada canal, es necesario caracterizar la respuesta del sistema a cada uno de los parámetros ópticos. Para recuperar con éxito la información de entrada completa es necesario no solo desencriptar correctamente todas las componentes (piezas del rompecabezas), sino también componer todos los canales.

VI.2.1 Descripción del método

La propuesta se lleva a cabo usando la clásica arquitectura de doble máscara de fase aleatoria tipo 4f. En primer lugar la imagen de entrada se descompone en partes no superpuestas de la imagen original (componentes) y después se encriptan cada una de las componentes en canales separados. Cada componente contiene un conjunto de píxeles cuyos valores y posiciones replican los valores de los píxeles y las posiciones de la imagen de entrada. Definimos estos píxeles como píxeles activos. La parte restante de la componente se completa con pixeles de valor nulo. Estos pixeles nulos se definen como pixeles pasivos. Cada componente contiene la misma cantidad de píxeles que la imagen de entrada.

Matemáticamente, definiremos la imagen de entrada como:

$$I_I = \sum_{(i,j)=(1,1)}^{(N,M)} P_i\,(i,j) \tag{6.1}$$

donde (i,j) representa la posición de los pixeles, $N\,x\,M$ es el tamaño de la imagen y $P(i,j)$ es el elemento de la matriz de valores en la posición (i,j). Por otra parte, se define una imagen con valores nulos:

$$I_B = \sum_{(i,j)=(1,1)}^{(N,M)} P_B\,(i,j)\ \forall\,(i,j) \Longrightarrow P_B\,(i,j) = 0 \tag{6.2}$$

Para implementar la técnica, la $r^{\text{ésima}}$ componente de la imagen de entrada se expresa como:

$$I_C^{(r)} = \sum_{(i,j)=(1,1)}^{(N,M)} P^r(i,j) \tag{6.3}$$

donde $P^r(i,j)$ es el elemento de la matriz de valores en la posición (i,j) de la componente y está dada por:

$$P^r(i,j) = \begin{cases} P^r(i,j) = P_I\,(i,j)\ para\ un\ grupo\ de\ posiciones\ (i,j) \\ P^r(i,j) = \ (i,j)\ para\ las\ posiciones\ restantes \end{cases} \tag{6.4}$$

Nótese que $P_I\,(i,j)$ representa el pixel activo mientras $P_B\,(i,j)$ representa el pixel pasivo.

El conjunto de píxeles $L = \{P_I\,(i,j)\}$ que forman la imagen de entrada son los píxeles activos. A continuación se describe el procedimiento mediante el cual se determinan los elementos pasivos ó activos de cada imagen componente.

Vamos a construir el conjunto de píxeles activos que constituyen cada una de las componentes para $r = 1 \ldots K$, donde K es el número de componentes en el cual la imagen original fue disociada. Ahora se selecciona un conjunto de píxeles activos que conforman un subconjunto estricto L_1 tal que $L_1 = \{P_I\,(i,j)\}_1 \subset \{P_I\,(i,j)\}$. Subconjunto estricto quiere decir que existe al menos un elemento del el grupo $L = \{P_I\,(i,j)\}$ no contenido en el subconjunto $L_1 = \{P_I\,(i,j)\}_1$. Para la componente $r = 2$, el subconjunto estricto L_2 cumple la condición $L_2 = \{P_I\,(i,j)\}_2 \subset L - L_1 = [\{P_I\,(i,j)\} - \{P_I\,(i,j)\}_1]$. Para la imagen componente $r = K$, el subconjunto estricto $L_k = \{P_I\,(i,j)\}_k \subset [\{P_I\,(i,j)\} - \sum_{r=1}^{k-1}\{P_I\,(i,j)\}_r]$. Además para cualquier par de subconjuntos L_n y L_m se cumple que, $L_n = \{P_I\,(i,j)\}_n \cap L_m = \{P_I\,(i,j)\}_m = \emptyset\ (conjunto\ vacio)$, para $n \neq m$ y $n,m = 1 \ldots . K$. Esto significa que los píxeles activos de la $r^{ésima}$ imagen componente, no están contenidos en ninguna otra imagen componente. Es decir que un píxel activo de una imagen componente se convierte en pasivo para todas las restantes imágenes componentes.

Se debe remarcar que el conjunto de píxeles activos que componen cada sub conjunto $L_n = \{P_I\,(i,j)\}_n$ se determina por medio de una función aleatoria. Los valores aleatorios se obtienen mediante un algoritmo basado en el generador Marsaglia-Zaman [6.12].

Claramente la suma de todos los píxeles activos de todas las imágenes componentes da como resultado la imagen original, esto es:

$$I_I = \sum_{(i,j)=(1,1)}^{(N,M)} P_I(i,j) = \sum_{r=1}^{K} I_C^{(r)} \tag{6.5}$$

Una vez que la imagen de entrada es disociada en las imágenes componente, se encripta cada una empleando un sistema de encriptación $4f$ convencional. La información encriptada correspondiente a cada componente está dada por:

$$E^{(r)} = I_C^{(r)} R_1 \otimes \Im[R_2] \tag{6.6}$$

donde R_1 y R_2 son las máscaras de fase aleatorias, $\otimes$ denota la operación de convolución y $\Im$ representa la transformada de Fourier. El procedimiento de multiplexado implica superponer las k componentes encriptadas $E^{(r)}$en el mismo medio. Luego, la información encriptada multiplexada E se puede expresar como $E = \sum_{r=1}^{k} E^{(r)}$.

Como ya fue mencionado en capítulos anteriores, para multiplexar se requiere introducir un cambio adecuado de alguno de los parámetros ópticos en el dispositivo encriptador. De esta manera, cada imagen componente $I_C^{(r)}$ será asociada a un único grupo de valores de los parámetros ópticos $OP^{(r)}$ Cada conjunto $OP_i^{(r)}$materializa un canal donde la componente $I_C^{(r)}$es apropiadamente operada.

Bajo la técnica descrita previamente, la imagen encriptada asociada a cada componente $E^{(r)}$ toma la forma de un patrón de speckle. Una vez se cumple el proceso de encriptación, todos los patrones codificados se suman en única imagen representada por E Como ya mencionamos en la imagen encriptada multiplexada no es posible distinguir los patrones individuales. Entonces, el usuario no puede distinguir en cuantas imágenes componentes se separó la entrada.

En la etapa de desencriptación se requiere de una operación de conjugación de fase de los datos encriptados, E, para recobrar la información de entrada original. Además en esta implementación se deben conocer los parámetros $OP_i^{(r)}$para recuperar la componente encriptada en dicho canal. Cuando en el proceso de desencriptación se emplea un parámetro erróneo, aparece ruido en el plano de salida y no la imagen componente. La información completa de la imagen original se obtiene sumando la información correctamente desencriptada de todos los canales. Es importante mencionar que en la información desencriptada de un único canal aparece ruido blanco de fondo como consecuencia de la información no desencriptada correspondiente a todos los canales restantes. Cuando se compone la información final, este ruido se adiciona reduciendo la calidad del la imagen resultante final. Esta situación representa un límite en el número de canales en el que se puede disociar la imagen de entrada sin deteriorar apreciablemente imagen desencriptada final.

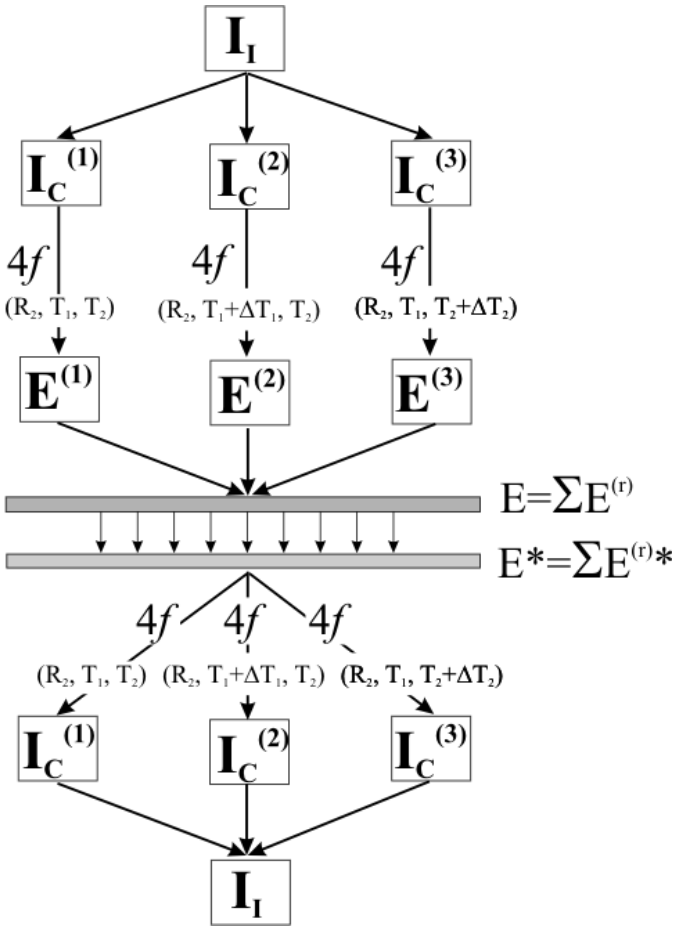


Figura 6.1. Diagrama de bloque mostrando las etapas del procedimiento de la técnica propuesta.

La propuesta de multiplexado tipo rompecabezas descrito se esquematiza en la **Figura 6.1**, donde una imagen de entrada $\mathrm{I_I}$ es descompuesta en tres componentes $\mathrm{I_C^{(i)}}$ $i = 1,2,3$. Para este caso, se escogió un conjunto de parámetros ópticos: la longitud de onda, la polarización y la posición en el plano de la máscara llave. Los valores de este conjunto de parámetros de encriptación definen un canal. Por ejemplo, el conjunto de valores $(OP_1^1,\ OP_2^1,\ OP_3^1)$ establecen el canal (1), los cuales son utilizados para encriptar la componente $\mathrm{I_C^{(1)}}$ como E^1. Cambiando al menos uno de los parámetros del conjunto que definen el canal, se encriptan las dos componentes restantes. Luego, se almacenan las tres imágenes encriptadas en un único medio de registro. Como es usual en el arreglo 4f, se implementa una operación de conjugación de fase de la información encriptada multiplexada, y se desencriptan las componentes individuales cambiando adecuadamente el conjunto de parámetros que define cada canal.

VI.2.2. Discusión de los resultados

En esta sección se verifica la validez del método propuesto en un sistema de óptica virtual. En la **Figura 6.2** y **Figura 6.3** se muestran los resultados para una imagen en niveles de gris de 384 x 512 pixeles y una imagen binaria de 479 x 399 píxeles, respectivamente. En nuestro casos, se utiliza una distancia focal f de 7 mm y una pupila de 5 mm para el sistema de encriptación. En la segunda fila de la **Figura 6.2** se muestra la descomposición de la imagen de entrada en niveles de gris disociada en tres componentes. Como ya mencionamos en la sección anterior, cada componente sólo contiene un conjunto de pixeles activos, mientras que los restantes pixeles son pasivos. Luego, cada componente es encriptada utilizando un conjunto de parámetros ópticos, de manera que resulten canales de información independientes. En este caso para implementar el multiplexado se utilizan tres parámetros: la longitud de onda, el desplazamiento de la máscara llave y la polarización. En nuestro caso particular, el cambio necesario en cada parámetro para generar los canales independientes, es decir que no se solapen entre sí, es de $\Delta\lambda = 10nm$ para la longitud de onda, $\Delta x = \Delta y = 8\ píxeles$ para

los desplazamientos horizontales y verticales de la máscara llave respectivamente y 5 grados de rotación en el estado de polarización de la luz incidente para la polarización.

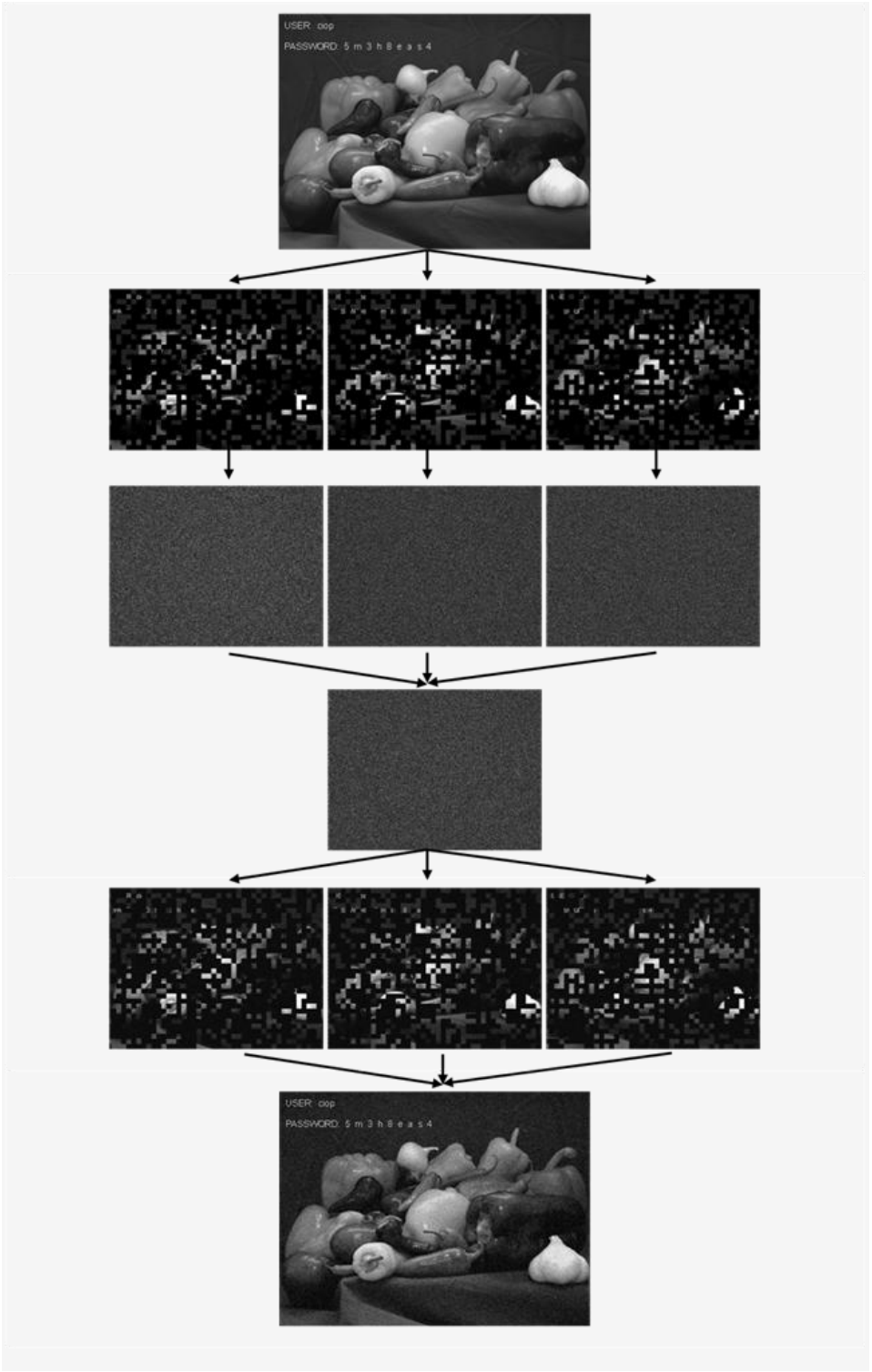
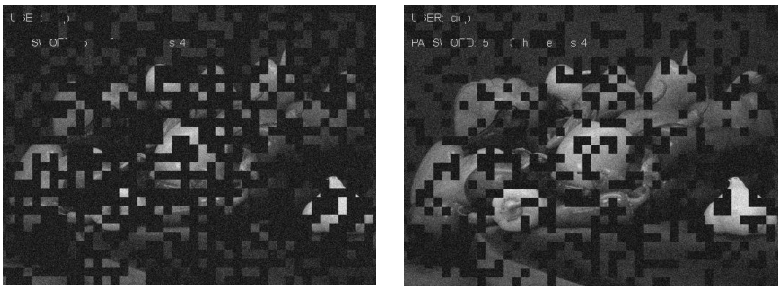


Figura 6.2. Diagrama de la técnica de encriptación multicanal tipo rompecabezas cuando se disocia la imagen de entrada en tres imágenes componentes.

Se procede a encriptar las tres imágenes componentes, y posteriormente se las almacena en el mismo medio. Si observamos la imagen encriptada multiplexada de la cuarta fila de la **Figura 6.2**, podemos notar que es imposible distinguir que está compuesta por la suma de los datos encriptados. Si la máscara llave y los demás parámetros de encriptación adicionales asociados a cada canal son conocidos por el usuario final, cada imagen componente será recuperada en el procedimiento de desencriptación como se muestra en la quinta fila de la **Figura 6.2.** Finalmente, en la última fila, se muestra la imagen recompuesta a partir de las componentes desencriptadas. Si únicamente uno ó dos canales están correctamente desencriptados, la información de entrada no puede ser completamente recuperada como se puede observar en la **Figura 6.3**. Esta información perdida en el procedimiento de desencriptación conduce a una imagen recuperada incompleta, aumentando la robustez de la técnica de codificación.



(a) (b)

(c)

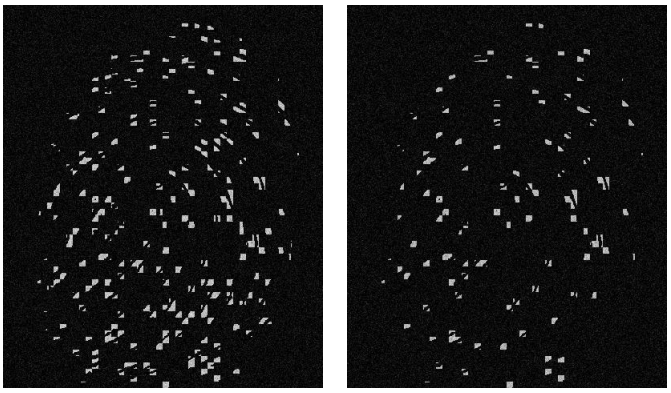
Figura 6.3 Imagen desencriptada compuesta cuando a) 1; b) 2; c) 3; canales son correctamente decodificados.

Con el fin de mostrar la potencialidad del multiplexado tipo rompecabezas, se presentan la imagen final recuperada correspondientes a una imagen binaria de entrada descompuesta en diez (**Figura 6.4 (b)**) y veinte (**Figura 6.4 (c)**) imágenes componentes, respectivamente.

(a) (b) (c)

Figura 6.4 (a) imagen de entrada. Imagen desencriptada-compuesta, cuando el objeto de entrada se descompone en: (b) diez y (c) veinte imágenes componentes.

En la **Figura 6.5** se muestran los datos desencriptados correspondiente a un único canal cuando la imagen binaria de entrada fue dividida en diez (ver **Figura 6.5 a)**) y veinte (ver **Figura 6.5 b)**) imágenes componentes, respectivamente. Como es de esperarse, la imagen desencriptada de un único canal contiene menos información del objeto de entrada cuando es descompuesta en mayor número de imágenes componentes. Como consecuencia un mayor número de canales reduce la probabilidad de que un intruso recupere la información completa.



(a) (b)

Figura 6.5 Imagen desencriptada de un único canal, cuando el objeto de entrada se descompone en (a) diez y (b) veinte imágenes componentes, respectivamente.

VI.3 Encriptación multicanal vía una arquitectura modificada del correlador de transformada conjunta.

Los sistemas de seguridad garantizan que la información confidencial sea accesible únicamente a los usuarios autorizados. Un problema relacionado con los sistemas multi-usuarios, radica en dar acceso a diferente información a cada usuario. En particular, es de interés tener un dispositivo en el cual exista un administrador con acceso a la información completa. En esta sección, se presenta un método de encriptación múltiple que permite controlar el nivel de acceso de cada usuario, permitiendo a su vez que el administrador disponga de la información completa del sistema.

La técnica consiste en la manipulación adecuada de los canales de multiplexado en un arreglo de codificación basado en una versión modificada de la arquitectura JTC, que emplea múltiples máscaras llaves en el plano de entrada. Cada máscara llave genera un canal de datos encriptados. La propuesta se aplicó a la encriptación secuencial de dos objetos de entrada en un único medio. Cada objeto se codifica empleando simultáneamente dos máscaras llaves en cada registro. Las máscaras asociadas a cada exposición, se seleccionan de manera que existan una máscara llave común y una no común. De esta manera, para cada máscara llave en la etapa de desencriptación, se recupera la información de un único ó a ambos objetos de entrada dependiendo de si se emplea una máscara común ó no común, respectivamente. En la siguiente sección se describe en detalle la técnica y se incluyen simulaciones que confirman su potencialidad.

VI.3.1. Principio de la técnica

La propuesta consistió en la encriptación secuencial de dos objetos de entrada en un único medio empleando múltiples máscaras llaves. En la **Figura 6.6** se presenta un diagrama de bloques del arreglo de aperturas en el plano de entrada del JTC modificado. Se denota a la máscara de fase objeto, localizada en las coordenadas (-a, 0), como r(x, y), a los objetos de entrada, localizados ambos en las coordenadas (-a, 0), como $O_A(x, y)$ y

$O_B(x,y)$ y a las máscaras llaves, ubicados en las coordenadas (a, b), (a, -b) y (a, 0), como $h_A(x,y)$, $h_B(x,y)$ y $h(x,y)$, respectivamente. En la **Figura 6.6** se puede notar que $h(x,y)$ está presente en ambos registros, por lo cual la denominaremos como la máscara común. Por otra parte, $h_A(\mathrm{x},\mathrm{y})$ y $\mathrm{h_B(x,y)}$ se utilizan en una única exposición por lo cual las llamaremos máscaras no comunes. El cuadrado de línea a trazos en la **Figura 6.6** indica la posición de la máscara llave bloqueada. Los difusores empleados para las simulaciones son estadísticamente independientes y tienen sus valores de fase aleatorios uniformemente distribuidos en el intervalo entre $[0\ 2\pi]$ con una transmitancia en amplitud uniforme.

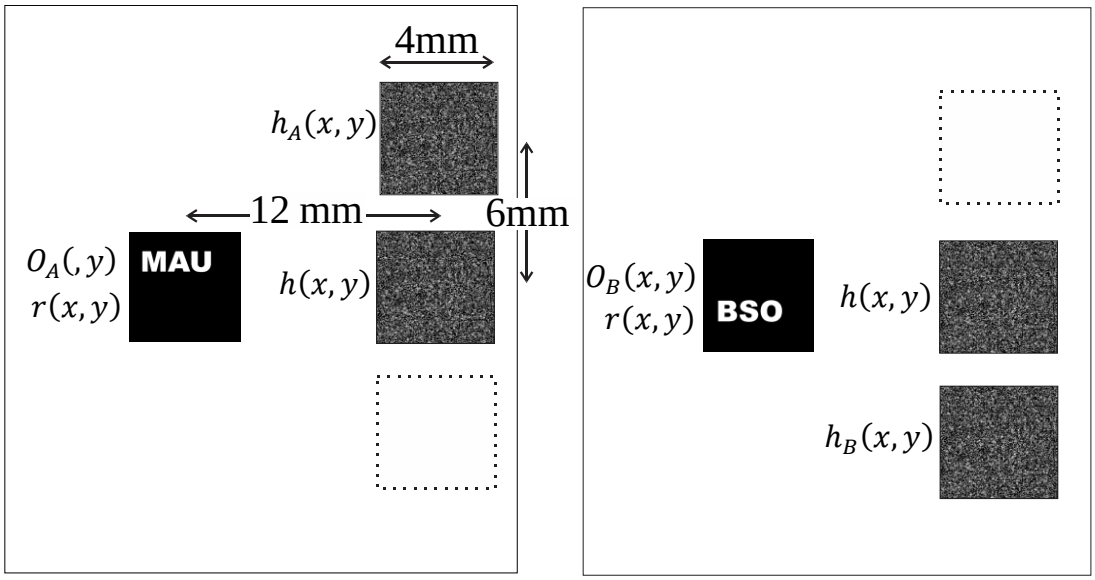


Figura 6.6 Esquema del plano de entrada del JTC modificado para los dos objetos de entrada..(a) primera exposición, (b) segunda exposición.

El espectro conjunto de energía (JPS) correspondiente a la señal encriptada de O_A está dada por,

$$JPS_A(v_x,v_y) = |\Im[r(x+a,y)O_A(x+a,y) + h(x-a,y) + h_A(x-a,y-b)]|^2$$
$$= |R \otimes A|^2 + 1 + 1 + (R \otimes A)^* H e^{-i4\pi a v_x} + (R \otimes A) H^* e^{i4\pi a v_x}$$
$$+ (R \otimes A)^* H_A e^{-i2\pi(2av_x + bv_y)} + (R \otimes A) H_A^* e^{i2\pi(2av_x + bv_y)}$$
$$+ H^* H_A e^{-i2\pi b v_y} + H H_A^* e^{i2\pi b v_y} \qquad (6.7)$$

donde $\Im[\ ]$, $R(v_x, v_y)$, $H_A(v_x, v_y), H(v_x, v_y)$ y $O_A(v_x, v_y)$ representan el operador transformada de Fourier y las transformadas de Fourier de $r(x, y)$, $h_A(x, y)$, $h(x, y)$ y $O_A(x, y)$, respectivamente. El símbolo * denota el complejo conjugada y $\otimes$ denota la operación de convolución. Como fue mencionado, $H(v_x, v_y)$y. $H_A(v_x, v_y)$.solo contienen información de fase, luego $\left| H(v_x, v_y)\right|^2 = \left| H_A(v_x, v_y)\right|^2 = 1$, condición que es requerida para la perfecta recuperación de la imagen desencriptada.

A continuación consideraremos el almacenamiento únicamente del $JPS_A(v_x, v_y)$ que representa una distribución de ruido blanco en el dominio de frecuencias. Cuando en la etapa de desencriptación la máscara llave $h(x, y)$ se ubica en las coordenadas $(x, y) = (a, 0)$ el espectro de potencias encriptado asociado al objeto $O_A(x, y)$, $JPS_A(v_x, v_y)$, es iluminado por $H(v_x, v_y)\, e^{-i2\pi a v_x}$. En este caso, en el quinto término de la ecuación (6.7) se compensan las fases, $H^* e^{i4\pi a v_x} H(v_x, v_y)\, e^{-i2\pi a v_x} = e^{i2\pi a v_x}$. Finalmente, después de una transformada de Fourier inversa, se obtiene en el plano de salida $r(x, y)O_A(x, y) \otimes \delta(x + a, y)$, permitiendo en consecuencia recuperar el objeto de entrada. Dado que $O_A(x, y)$ es una imagen en amplitud, un dispositivo sensible a la intensidad permite recuperar el objeto de entrada sin ser afectado por la información de fase correspondiente a la máscara objeto, $r(x, y)$. Los restantes términos del JPS aparecen en el plano de salida como ruido y están espacialmente separados. Si se emplea en la etapa de desencriptación la máscara llave $h_A(x, y)$, se recupera la misma imagen en el plano de salida. El objeto de entrada $O_A(x, y)$ no puede ser recuperado si no se posee las máscaras $h(x, y)$ y/ó $h_A(x, y)$.

Hasta ahora hemos considerado el almacenamiento del $JPS_A(v_x, v_y)$ asociado a $O_A(x, y)$. Análogamente se puede representar el $JPS_B(v_x, v_y)$ asociado a $O_B(x, y)$. Ambos JPS fueron registrados en el mismo medio.

Recordemos que en nuestra propuesta, los canales de salida de la información, se generan mediante el cambio del objeto de entrada y del arreglo de máscaras llaves en cada exposición de la etapa de codificación. Cada una de estas máscaras genera un canal de datos encriptados. Los patrones encriptados, $JPS_A(v_x, v_y)$ y $JPS_B(v_x, v_y)$ obtenidos

secuencialmente son almacenados en el mismo medio. Para las simulaciones se emplean objetos de entrada de 470 x 470 píxeles. El objeto $O_A(x,y)$ es encriptado con las dos máscaras llaves esquematizadas en la **Figura 6.6 a)**. Asimismo, se almacena la información encriptada del objeto $O_B(x,y)$ empleando en este caso las máscaras llaves esquematizadas en la **Figura 6.6 b)**. Como ya fue mencionado a partir de la comparación de la **Figura 6.6 a)** y **b)**, hay aperturas comunes y no comunes para las máscaras llaves empleadas en ambas exposiciones.

Se puede verificar a partir de los resultados de la **Figura 6.7** que el uso de diferentes arreglos de múltiples máscaras llaves en un arreglo de múltiples exposiciones, permite desencriptar diferentes información, a partir de cada máscara llave. En la **Figura 6.7 a),** se esquematiza la máscara llave empleada para desencriptar cada canal de información. En la **Figura 6.7 b)** se muestra las imágenes desencriptadas cuando se emplean la máscara llave indicada en la **Figura 6.7 a)**. Los objetos $O_A(x,y)$ y $O_B(x,y)$ se recuperan aisladamente, a partir del JPS multiplexado, mediante el uso de las máscaras llave $h_A(x,y)$ y $h_B(x,y)$, respectivamente. Mientras que el empleo de la máscara $h(x,y)$ en la etapa de desencriptación, permite recuperar simultáneamente los objetos $O_A(x,y)$ y $O_B(x,y)$.

a)

b)

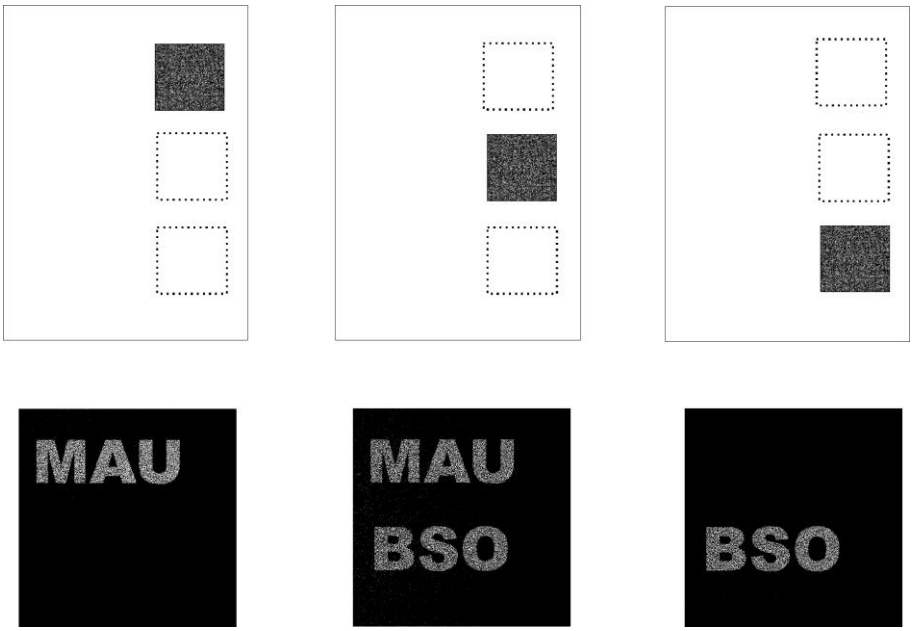


Figura 6.7. (a) Esquema de la máscara llave empleada en la etapa de desencriptación, (b) imágenes desencriptadas mediante la llave mostrada en a),

De acuerdo con la máscara llave empleada se puede recuperar una imagen sin rastros de la otra, ó se pueden recuperar ambas imágenes simultáneamente. En consecuencia, las máscaras llaves en sí mismas se comportan como canales de información.

VI.3.2 Implementación experimental.

La propuesta descripta se implementa utilizando como medio de registro un cristal fotorrefractivo tipo silenita BTO en la configuración transversal donde las direcciones $(1\bar{1}0), (001), (110)$, coinciden con los ejes $X, Y\ y\ Z$, respectivamente (ver **Figura 6.8)**. Las dimensiones del cristal son $8\ mm\ x\ 8\ mm\ x\ 8\ mm$. Se emplea un láser de $He\ Ne$ ($\lambda = 632{,}8\ nm$). En la **Figura 6.8 a)** se representa una de las dos exposiciones del proceso de multiplexado. La **Figura 6.8 b)** corresponde a la desencriptación de uno de los canales de información.

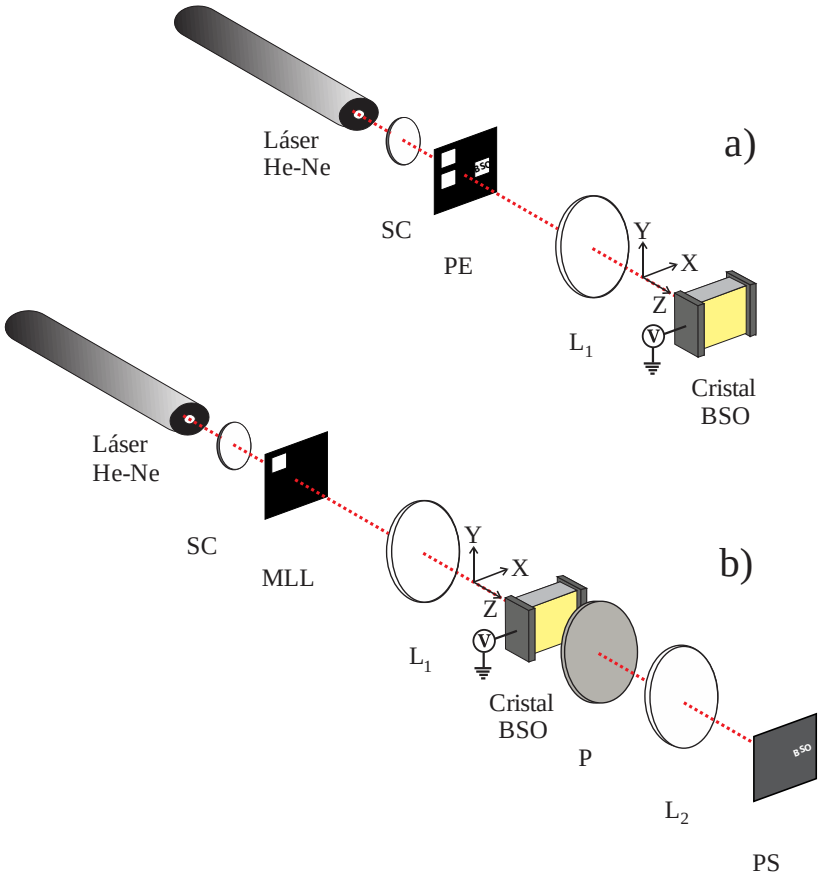


Figura 6.8. Esquema experimental: (a) etapa de encriptación y (b) etapa de desencriptación. (SC: sistema de colimación; PE: Plano de de entrada; L_1 y L_2: lentes; **MLL** : Una máscara llave ; P: polarizador, PS: plano de salida)

En cada exposición, se emplean tres aperturas en el plano de entrada. Las dimensiones de las aperturas de las máscaras y del objeto son de $4mm\ x\ 4mm$. Como máscara llave y objeto se utilizan difusores. En el cristal fotorrefractivo se almacena el patrón de interferencia entre la transformada de Fourier del arreglo de máscaras llave y el producto de la máscara objeto y el objeto a ser encriptado. Esta operación es realizada por medio de la lente L_1 que tiene una distancia focal de $100\ mm$. En cada exposición el cristal recibe tres contribuciones, una de cada apertura del plano de entrada. Entonces en el patrón resultante aparece la interferencia de las mencionadas contribuciones. En estos patrones de speckles modulados, las franjas son ortogonales a la línea que une los centros entre las aperturas. En particular, se producen tres sistemas de franjas de bajas frecuencias: verticales, diagonales y horizontales con periodos de aprox. $5\ \mu m$, $7\ \mu m$ y $10\ \mu m$, respectivamente. Para comprender el resultado, es necesario considerar el particular comportamiento de almacenamiento y lectura en este cristal, para las modulaciones de baja frecuencia [6.25, 6.26]. La distribución de intensidad que ilumina el cristal crea fotocargas. Existen para este tipo de materiales dos mecanismos de transporte: deriva y difusión. En los patrones de interferencia de nuestro experimento debido a las bajas frecuencias de las franjas el mecanismo de transporte de difusión es despreciable. Por lo tanto, el mecanismo de trasporte en este caso es el de deriva debido al campo eléctrico externo aplicado a lo largo de la dirección $(1\bar{1}0)$ del cristal. Se aplica un voltaje de $8\ \mathrm{kV}$ entre las caras del cristal separadas 8 mm, produciendo un campo eléctrico de $10\ \mathrm{kV/cm}$. Las fotocargas se mueven de las regiones altamente iluminadas a las menos iluminadas, donde quedan atrapadas. La tasa de generación de fotocargas es proporcional al patrón que ilumina el cristal. Estas cargas generan un campo de cargas espaciales que compensa parcialmente el campo externo. Se obtiene un campo interno resultante en cada punto y el sistema llega a una situación estacionaria. De esta manera, la distribución de la intensidad recibida por el cristal queda codificada como una distribución espacial de campo eléctrico resultante en cada punto. Este campo induce a través del efecto electro óptico lineal, que el cristal exhibe, la correspondiente variación del índice Δn. Por lo tanto el JPS es almacenado en cada exposición como una distribución de índices de refracción.

En la etapa de desencriptación, un obturador bloquea el haz objeto de tal manera que el cristal fotorrefractivo es iluminado solo por la trasformada de Fourier de una de las máscaras llaves. La luz difractada desde el plano de encriptación es colectada hacia el plano focal de la lente L_2, reconstruyendo así la entrada correspondiente a la máscara llave seleccionada. La distancia focal de la lente L_2 es de 50 mm y tiene un diámetro de 50 mm. Es importante notar que la eficiencia de difracción de la red de índices en las condiciones del experimento depende fuertemente de la dirección de las franjas que modulan el patrón de speckle [6.25, 6.26]. Como se demuestra en la Ref. [6.26], el campo externo introduce un comportamiento anisotrópico cuando se construye la red de índices. Es decir, la proyección del campo en la dirección del vector de red determina la contribución de los portadores de deriva. Como consecuencia, la eficiencia de difracción cambia con la dirección de la red de índices. En resumen, este comportamiento anisotrópico debe ser tenido en cuenta en la implementación del sistema de encriptación JTC modificado dado que determina la eficiencia de difracción asociada a cada sistema de franjas. En particular, en la configuración diseñada, los términos cruzados correspondientes a la interferencia entre las máscaras llaves son despreciables, debido a que tienen una modulación de franjas en la dirección vertical y el campo externo es aplicado en la dirección horizontal, por lo tanto su eficiencia de difracción es nula.

Figura 6.9. Imágenes desencriptadas experimentalmente**.**

Los resultados experimentales que se presentan en la **Figura 6.9,** muestran una evidente concordancia con su contrapartes simuladas, **Figura 6.8 b)**. Es importante mencionar que para obtener eficiencias de difracción comparables en las múltiples exposiciones, se ha tenido en cuenta la respuesta del cristal en este régimen de operación.

Nótese que el esquema propuesto mantiene las ventajas inherentes a la versión convencional del JTC y permite el acceso selectivo a distintos canales de información. Esta propuesta puede ser extendida para un mayor número de objetos de entrada aumentando el número de máscaras llave y de exposiciones ó bien incorporando nuevas llaves de multiplexado tales como la longitud de onda.

VI.4 Conclusiones.

En este capítulo se presentaron dos técnicas de múltiple encriptación con el fin de aumentar la seguridad de datos confidenciales y crear canales de información que proporciones diferentes niveles de acceso a la información encriptada.

En la primera propuesta, el multiplexado se utiliza para aumentar la seguridad de una imagen encriptada en una arquitectura 4f. El método se basa en la descomposición de la imagen de entrada en múltiples imágenes componentes. Cada imagen componente es encriptada individualmente en un canal representado por un conjunto de parámetros del sistema. Para multiplexar se cambia al menos uno de los parámetros del sistema en el registro de cada componente encriptada. Para desencriptar adecuadamente la imagen sin solapamiento, se tuvo en cuenta la sensibilidad del sistema a la variación de los parámetros de multiplexado. Esto implica que se debe conocer el conjunto de llaves de encriptación para todos los canales. Con el método de descomposición propuesto, se descifra parcialmente la imagen de entrada cuando se desencripta un número parcial de canales. La imagen de entrada completa sólo se puede recuperar mediante la composición de todas las imágenes componentes desencriptadas. La separación de una imagen de entrada en componentes disjuntas dificulta la recuperación por parte de un intruso de la verdadera imagen, dado que requiere recuperar todas las componentes individuales. Cuanto mayor sea el número de canales que se utilizan, menor es la posibilidad recuperar la imagen original de entrada si no se conocen el conjunto de parámetros.

Además de mejorar la seguridad de la encriptación, el procesamiento multicanal aumenta la complejidad del sistema. De hecho, para sistemas de múltiple almacenamiento de información encriptada, no tenemos conocimiento de reportes de ataques que se basan en la existencia de un par de imágenes, entrada-encriptada. En este sentido, el multiplexado hace el sistema más seguro contra los ataques.

Por otro lado, en la segunda aplicación propuesta, la versión modificada de la arquitectura JTC permite generar diferentes niveles de acceso a los datos encriptados. Nótese que este esquema modificado mantiene las ventajas inherentes a la versión convencional del JTC. El cristal fotorrefractivo es un medio de almacenamiento valido para implementar la alternativa propuesta. Cuando se emplea un cristal tipo silenita, el comportamiento anisotrópico en el registro de las franjas moduladoras de baja frecuencia actúa como un filtro eliminando la contribución de la interferencia entre las máscaras llaves en cada registro.

Otra característica que es importante enfatizar, cuando se utiliza un cristal fotorrefractivo como medio de registro, es la diferencia entre las direcciones de polarización lineal que exhiben el orden cero y los órdenes difractados bajo determinadas condiciones [6.29]. Este hecho, es aprovechado en la implementación experimental para reducir el ruido del orden cero en la etapa de desencriptación utilizando un polarizador lineal para seleccionar la información de interés.

VI.5 Referencias

[6.1] X. Peng, P. Zhang, H. Wei, and B. Yu, “Known-plaintext attack on optical encryption based on double random phase keys”, Opt. Lett. 31, 1044-1046 (2006).

[6.2] J. F. Barrera, C. Vargas, M. Tebaldi, R. Torroba, and N. Bolognini, “Known-plaintext attack on a joint transform correlator encrypting system”, Opt. Lett. 35, 3553-3555 (2010).

[6.3] J.F. Barrera R., R. Henao, M. Tebaldi, R. Torroba, N. Bolognini "Digital encryption with undercover multiplexing by scaling the encoding mask", Optik 120, 342-346 (2009).

[6.4] J.F. Barrera R., R. Henao, M. Tebaldi, R. Torroba, N. Bolognini, "Code retrieval via undercover multiplexing", Optik 119, 139-142 (2008).

[6.5] J. Rosen and B. Javidi, "Hidden Images in Halftone Pictures", Appl. Opt. 40, 3346-3353 (2001).

[6.6] D. Abookasis, O. Montal, O. Abramson, and J. Rosen, "Watermarks encrypted in a concealogram and deciphered by a modified joint-transform correlator", Appl. Opt. 44, 3019-3023 (2005).

[6.7] J.F. Barrera R., R. Torroba, "Efficient encrypting procedure using amplitude and phase as independent channels to display decoy objects", Appl. Opt. 48, 3121-3129 (2009).

[6.8] 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).

[6.9] J. F. Barrera, R. Henao, M. Tebaldi, N. Bolognini, R. Torroba, "Multiplexing encrypted data by using polarized light", Opt. Commun. 260, 109-112 (2006).

[6.10] 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).

[6.11] G. Situ, J. Zhang, "Multiple-image encryption by wavelength multiplexing", Opt. Lett. 30, 1306-1308 (2005).

[6.12] G. Marsaglia and A. Zaman, "A New Class of *Random Number Generators*", Annals of Applied Probability 3, 462-480 (1991).

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

[6.15] P. Refregier, B. Javidi, "Optical image encryption using input and Fourier plane random phase encoding", Opt. Lett. 20, 767-769 (1995).

[6.16] F. H. Mok, "Angle-multiplexed storage of 5000 holograms in lithium niobate", Opt. Lett. 18, 915-917(1993).

[6.17] D. L. Staebler, W.J. Burke, W. Phillips, J.J. Amodei, "Multiple storage and erasure of fixed holograms in Fe-doped LiNbO", Appl. Phys. Lett. 26, 182-184 (1975).

[6.18] G. A. Rakuljik, V. Leyva, A. Yariv, "Optical data storage using orthogonal wavelength multiplexed volume holograms", Opt. Lett. 17, 1471-1473 (1992).

[6.19] C. Denz, G. Pauliat, G. Roosen, T. Tschudi, "Volume hologram multiplexing using a deterministic phase encoding method", Opt. Commun. 85, 171-176 (1991).

[6.20] D. Psaltis, M. Levene, A. Pu, G. Barbastathis, "Holographic storage using shift multiplexing"**,** Opt. Lett. 20, 782-784 (1995).

[6.21] G. Unnikrishnan, J. Joseph, K. Singh, "Optical encryption system that uses phase conjugation in a photorefractive crystal", Appl. Opt. 37, 8181–8186 (1998).

[6.22] Songcan Lai, "Security holograms using an encoded reference wave", Opt. Eng. 35 2470-2472 (1996).

[6.23] E. Tajahuerce, B. Javidi, "Encrypting three-dimensional information with digital holography"**,** Appl. Opt. 39 6595 (2000).

[6.24] L. Yu, X. Peng, L. Cai, "Parameterized multi-dimensional data encryption by digital optics", Opt. Commun. 203, 67-77 (2002).

[6.25] Jong-Wook Han, Choon-Sik Park, Dae-Hyun Ryu, Eun-Soo Kim, "Optical image encryption based on XOR operations", Opt. Eng. 38, 47–54 (1999).

[6.26] G. Unnikrishnan, J. Joseph, K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain"**,** Opt. Lett. 25, 887-889 (2000).

[6.27] G. Unnikrishnan, K. Singh, "Double random fractional Fourier-domain encoding for optical security", Opt. Eng. 39, 2853-2859 (2000).

[6.28] Wei-Chia Su, Chien-Hong Lin, "Enhancement of the angular selectivity in encrypted holographic memory'', Appl. Opt. 43, 2298-2304 (2004).

[6.29] M. Tebaldi, M. C. Lasprilla N. Bolognini. "Analysis of birrefringence encoded images", Optik 110, 127-136 (1999).

CAPÍTULO VII

Conclusiones generales

VII.1 Conclusiones generales y perspectivas

El estudio contenido en este trabajo de tesis estuvo encaminado a optimizar las arquitecturas de codificación ópticas 4*f* y JTC para aplicaciones de múltiple almacenamiento de información encriptada.

En las arquitecturas JTC y 4*f* los datos de una imagen de entrada son codificados en una distribución de ruido blanco estacionario que es esencialmente un patrón de speckle. Multiplexar es almacenar múltiple información en un único medio. En un patrón encriptado multiplexado los patrones individuales que lo componen son indistinguibles. Por esta razón, los esquemas basados en el multiplexado de datos encriptados son inmunes a los procedimientos de ataque conocidos que se basan en la existencia de un par objeto de entrada-imagen encriptada. De este modo, el multiplexado incrementa la seguridad de las técnicas de codificación óptica.

Una imagen desencriptada experimentalmente ó en simulaciones que buscan replicar condiciones reales, siempre presenta ruido speckle. El origen de este ruido puede deberse principalmente a pérdidas de información a través del sistema ó si existe un multiplexado al ruido de las imágenes no desencriptadas. Asimismo, para la arquitectura JTC se identificó que otra fuente de ruido se origina en la no uniformidad de la amplitud del espectro de la máscara llave.

El ruido speckle en una imagen recuperada en un único proceso de encriptación en sistemas reales es casi inevitable. Sin embargo, si se conocen los factores que lo generan, se puede encontrar las condiciones para minimizarlo. En los sistemas ópticos de encriptación las máscaras usualmente son difusores compuestos de centros

dispersores de dimensión transversal inferior a los 100 μm, produce portadores de información de alta frecuencia espacial. Si parte de la información de alta frecuencia es bloqueada por alguna limitación física (pupila, medio de almacenamiento, etc.), se producirá en la imagen desencriptada pérdida de información que se traducirá en la aparición de speckle. Por un lado, la dimensión transversal del speckle obedece a parámetros específicos del sistema óptico y por otro la cantidad de información perdida se ve reflejada en un aumento de la cantidad de speckle en la imagen desencriptada. Con el fin de dilucidar de cuales parámetros depende el ruido speckle, se estudió el rol que desempeñan las máscaras llave y objeto en la distribución espacial de la información encriptada tanto para la arquitectura 4f cuanto para la JTC. Asimismo, se analizó la degradación de la imagen desencriptada cuando el área del medio de registro es menor que el área en la cual está distribuido el patrón encriptado.

La mayoría los trabajos en codificación óptica, son realizados digitalmente y se han encaminado a desarrollar nuevos esquemas de codificación y a incrementar la seguridad en los procesos de encriptación. Es llamativo que las condiciones reales (dimensión finita de las pupilas y del medio de almacenamiento, etc.) de los sistemas de encriptación no sean motivo de investigación en estas propuestas. De esta manera, se evoluciona en arquitecturas digitales que cada vez ensanchan más la brecha respecto a una genuina implementación experimental. En nuestro concepto se necesita hacer investigaciones que disminuyan esa brecha. Al tener en cuenta las condiciones reales en los sistemas digitales se posibilita la implementación de las nuevas propuestas y la optimización de los arreglos experimentales.

Para que la imagen en un sistema de encriptación sea recuperada con la menor pérdida de información, garantizando que la información este bien encriptada, es necesario tener en cuenta la relación entre los anchos de banda de la señal de entrada y el sistema óptico. Se determinó para un sistema $4f$ que el ancho de banda frecuencial de la señal de entrada, debe ser menor que el ancho de banda espacial de la máscara llave. que a su vez determina el ancho de banda del sistema. De esta manera toda la información de entrada es transferida al plano de encriptación. Si se garantiza que el área del medio de almacenamiento registra toda la información encriptada, la imagen

desencriptada es una réplica del objeto de entrada. Estas condiciones son muy difíciles de materializar en un experimento, por esta razón se estudió la degradación de la imagen desencriptada cuando no se registra todo el patrón encriptado debido al área finita del medio de almacenamiento. Se determinó que si el tamaño del medio de almacenamiento relativo al área en la que está contenida la información encriptada disminuye, se incrementa el ruido en la imagen desencriptada. En nuestro estudio se probó que si la información en el plano de encriptación está uniformemente distribuida, la imagen desencriptada es insensible a la posición del medio de registro y el ruido en ella es uniforme en todo el plano de salida. Por otra parte, si la distribución de la información en el plano de encriptación no es uniforme, los datos recuperados van a tener diferentes pesos para cada zona de la imagen desencriptada. Dichos pesos se corresponden con las coordenadas conjugadas del patrón encriptado en el medio finito de almacenamiento. Este resultado se debe a la naturaleza del plano de encriptación del sistema 4f, dado que exhibe la operación de convolución entre la señal de entrada y la máscara llave.

Siempre se parte del supuesto que la información encriptada está uniformemente distribuida en plano de encriptación. Sin embargo, demostramos que bajo ciertas condiciones reales, aquello no se cumple. De hecho, hemos demostrado que la distribución espacial de la información en el plano de encriptación para una arquitectura 4*f*, está gobernada principalmente por la relación entre el tamaño de grano de los centros dispersores de la máscara llave y la dimensión transversal del patrón de speckle que incide sobre ella. Dicha dimensión, para las condiciones establecidas en este trabajo, es determinada por el tamaño del objeto de entrada. En ese sentido, se encontró un criterio para garantizar la distribución uniforme de la información encriptada que establece que el tamaño promedio del grano de speckle del campo que ilumina el difusor llave, debe al menos duplicar el tamaño de los centros dispersores que lo compone.

El análisis del rol que desempeñan el tamaño de los centros dispersores de las máscaras objeto y llave en la distribución de la información encriptada y cómo se ve afectada la calidad de la imagen desencriptada también se consideró en la arquitectura JTC. Recordemos que en la arquitectura JTC la información encriptada se registra en un plano frecuencial. Dicha información consiste en el patrón de interferencia de las

transformadas de Fourier de los datos contenidos en las dos ventanas del plano de entrada. Una de las ventanas contiene el objeto a encriptar adosado a una máscara de fase objeto (señal de entrada), en la otra está la máscara llave. La información proveniente de cada ventana llega al plano frecuencial como un patrón de speckle. Por lo tanto la información encriptada consiste en un diagrama de speckle modulado en las regiones que ambos patrones se interceptan. La extensión de la información de la señal de entrada en el plano de frecuencias, es la suma del ancho de banda frecuencial del objeto y del ancho de banda frecuencial de la máscara objeto. Mientras que para el campo que proviene de la ventana llave la extensión está determinada por el ancho de banda de la máscara llave. Se determinó que si el ancho de banda de la máscara llave es menor que el ancho de banda de señal de entrada, la imagen desencriptada tendrá pérdida de información frecuencial. Esto es equivalente a un proceso de filtrado pasa bajos. Se probó que este mismo proceso tiene lugar si el área del medio de registro es menor que el patrón de speckle modulado. Consideremos que la extensión del ancho de banda de la señal de entrada es mayor que la dimensión del medio de registro y la dimensión del ancho de banda de la máscara llave. Bajo esta condición, la menor entre las dimensiones mencionadas determina la máxima frecuencia espacial de la imagen desencriptada que es a su vez la frecuencia espacial del ruido speckle. Esto tiene una implicancia crucial en la calidad de imagen desencriptada, provocando un rápido deterioro de ella a medida que la dimensión del medio de registro ó del espectro de la máscara llave disminuye. Este estudio nos permite afirmar que para preservar la información de alta frecuencia y de niveles de gris en la imagen desencriptada se debe optimizar el registro del patrón encriptado. Estos estudios permitirán diseñar adecuadamente los esquemas experimentales para evitar el rápido deterioro de la información desencriptada en esta arquitectura.

Debemos destacar que en la implementación digital de la arquitectura 4*f*, si se registra la información completa en el plano de encriptación, es posible encontrar una imagen desencriptada “perfecta”, tal como puede observarse en la literatura. Sin embargo, en la implementación digital de la arquitectura JTC, aún si se registra la información completa en el plano de encriptación, se obtiene una imagen desencriptada

"imperfecta". En este caso, el speckle está presente en la imagen desencriptada y a lo sumo puede reducirse su tamaño de tal manera que en comparación con las frecuencias espaciales del objeto, sea ruido de alta frecuencia. Para lograr que la imagen desencriptada sea una réplica del objeto de entrada en la arquitectura JTC, además de cuidar todas las condiciones necesarias para que no haya pérdida de información, se debe enfrentar el problema de cumplir con la condición teórica de que la amplitud del espectro de la máscara llave sea uniforme. Esta no es una condición fácil de cumplir teniendo en cuenta que si se usa un difusor(con sólo información de fase) como máscara llave, la amplitud de su espectro es un patrón de speckle y no una amplitud uniforme como se requiere. Es ese sentido, hemos propuesto una arquitectura optimizada para la implementación digital del JTC que se basa en el diseño de una máscara llave adecuada para la perfecta recuperación de la imagen desencriptada. Con esta versión optimizada, se logra tener imágenes de salida comparables en ambas arquitecturas.

Es importante aclarar que el análisis realizado en este trabajo no tuvo en cuenta las pérdidas debido al tamaño finito de las pupilas de las lentes y para la arquitectura 4f de la máscara llave. Consideramos que es necesario extender el estudio incluyendo estos aspectos que también introducen ruido en las imágenes desencriptadas.

Se debe destacar que si bien la arquitectura 4f es su formato digital proporciona imágenes desencriptadas de mejor calidad en comparación con las obtenidas en la arquitectura JTC no optimizada, su implementación experimental es más exigente debido a la necesidad de generar un frente onda conjugado. Debemos mencionar que en las simulaciones del 4f, no se tiene en cuenta la baja reflectividad de conjugación de fase que se obtiene en experimentos de mezclado de cuatro ondas fotorrefractivos. Por otra parte, la arquitectura JTC presenta ventajas en su implementación. Una de ellas es que este esquema (donde el objeto de entrada y el haz de referencia se localizan en el mismo plano) es más compacto que un sistema holográfico ordinario. Otra ventaja es que este sistema es menos sensible a los problemas de alineamiento. Por otra parte, cuando se utiliza un cristal fotorrefractivo como medio de registro en un JTC, la diferencia entre la direcciones de polarización que exhiben el orden cero y los órdenes difractados puede ser aprovechado para reducir el ruido del orden cero en la etapa de desencriptación. Cuando

se desea implementar experimentalmente un dispositivo de encriptación, se presenta una degradación de la imagen desencriptada como consecuencia del rango dinámico del medio de registro. Si bien esta limitación no fue tenida en cuenta en nuestro trabajo, será de relevancia considerarla en un futuro.

El análisis del proceso de encriptación en las arquitecturas $4f$ y JTC cuando se almacena un único patrón encriptado, fue el punto de partida para el estudio de procesos de multiplexado.

Debemos enfatizar el interés en el desarrollo de aplicaciones de codificación óptica que involucren múltiple información ó múltiples usuarios. Al emplear memorias de volumen (cristales fotorrefractivos) se puede multiplexar gran cantidad de información encriptada aprovechando la selectividad angular. Es importante destacar que también este proceso se puede llevar a cabo empleando un medio de registro plano. Para la correcta implementación de un proceso de multiplexado, es necesario que los patrones encriptados correspondientes a diferentes canales estén decorrelacionados. Se garantiza así que no haya solapamiento de información en las imágenes desencriptadas. Esto se puede lograr mediante el uso de máscaras llaves estadísticamente independientes para el registro de cada patrón encriptado. También se puede lograr variando algún parámetro óptico en una cantidad que asegure dicha decorrelación. Si bien la condición anterior garantiza que no haya solapamiento de información, las imágenes desencriptadas presentan ruido. Este ruido en la imagen recuperada de un determinado canal se debe a la información no desencriptada de los canales restantes. La dificultad esencial en los procesos de multiplexado para dado sistema, radica en que un aumento en el número canales incrementa el ruido en la información desencriptada, limitando así la cantidad de datos encriptados a multiplexar.

En nuestra propuesta hemos aprovechado la redundancia propia de los datos encriptados para el almacenamiento de múltiple información en un medio plano. Esta propiedad es la razón fundamental que nos habilita a multiplexar información y en ese sentido, se la estudió con el fin de aprovechar al máximo la capacidad de almacenamiento de un medio dado. Dentro de ese análisis se encontró que la redundancia es el factor determinante del número máximo de objetos que se pueden multiplexar.

Hemos verificado que existe una relación entre la redundancia en la información encriptada y el mínimo porcentaje de esta información necesario para que en la imagen desencriptada se pueda reconocer la información del objeto. En ese sentido se determinó para las arquitecturas 4f y JTC ese mínimo porcentaje de datos encriptados. Se comprobó, que la razón entre el total y el mínimo porcentaje de datos encriptados condiciona el número máximo de imágenes encriptadas que el sistema permite multiplexar.

Se debe destacar que el mínimo porcentaje de datos encriptados depende fuertemente del tamaño del objeto de entrada para la arquitectura 4f, en cambio en la arquitectura JTC no se observa esa dependencia. En consecuencia, la capacidad de multiplexado para un sistema de encriptación 4f aumenta significativamente a medida que el tamaño de objeto de entrada disminuye para un medio de almacenamiento fijo. Esto nos permitió establecer que en un proceso de multiplexado, el sistema 4f permite incrementar significativamente la capacidad de almacenamiento de datos en comparación con el JTC.

Este estudio será el punto de partida para caracterizar el comportamiento de la redundancia de datos encriptados en términos de los parámetros ópticos del sistema, de los niveles de fase de las máscaras, dado que en nuestro caso sólo se analizó la influencia debido al tamaño del objeto de entrada. Asimismo consideramos que es necesario profundizar en las características particulares de cada arquitectura ante el multiplexado para dilucidar la marcada diferencia en la capacidad de multiplexado.

Como ya mencionamos otro aspecto muy importante que debe ser tenido en cuenta, es la sensibilidad del sistema de encriptación al parámetro de multiplexado elegido, es decir, el mínimo cambio que se debe producir para garantizar que no haya solapamiento entre la información de canales adyacentes.

Una opción para obtener patrones encriptados decorrelacionados es cambiar la longitud de onda. En ese sentido, se estudió la sensibilidad a la longitud de onda y esto habilitó la implementación de un multiplexado con este parámetro. Como herramienta para su evaluación se utilizó el coeficiente de correlación y el error cuadrático medio. Se determinó que la arquitectura 4f es más sensible al cambio en la longitud de onda.

Se implementó un multiplexado en longitud de onda en la arquitectura JTC. Se verificó digital y experimentalmente que para la correcta recuperación de la información de cada canal, es necesario conocer la máscara llave y la longitud de onda asociada a ese canal. Así mismo, se comprobó que cuando se aumenta el tamaño del objeto de entrada, el sistema se torna más sensible al cambio en la longitud de onda.

Dado que una imagen en color verdadero es posible descomponerla en canales puros de color, se implementó una encriptación de ese tipo imágenes usufructuando el multiplexado en longitud de onda. El usuario debe entonces recibir la información encriptada, la máscara llave, y la longitud de onda utilizada en cada canal de color para recuperar los datos de entrada. Para un canal dado, cuando alguna ó todas las llaves del sistema son incorrectas, aparece ruido en el plano de salida. Si intentamos recuperar la información con solo uno o dos canales correctos, no se puede obtener la información de color completa.

El estudio de algunos de los parámetros de multiplexado permitió la implementación de aplicaciones que involucran almacenamiento de múltiples datos codificados.

Las propuestas están relacionadas con el aprovechamiento de los múltiples canales disponibles en los proceso de multiplexado. En una de las propuestas esta fue una herramienta para amentar la seguridad de datos confidenciales de una sola imagen de entrada a ser encriptada en la arquitectura 4*f*. El método se basó en la descomposición del objeto de entrada en múltiples imágenes componentes, que fueron encriptadas independientemente y multiplexadas en un único medio. La imagen de entrada completa sólo se puede recuperar mediante la composición de todas las imágenes desencriptadas correspondientes a las imágenes componentes. Esto implica que se debe conocer todo el conjunto de llaves de encriptación para todos los canales. La selección de la información de entrada asociada a cada una de las imágenes componentes fue realizada con una función aleatoria, lo que dificulta el reconocimiento del objeto de entrada si no se tiene la información de todos los canales.

La segunda propuesta se basó en la manipulación adecuada de los canales de multiplexado en un arreglo de encriptación basado en una versión modificada de la arquitectura JTC. Esta manipulación se realiza mediante el empleo de un arreglo de múltiples mascaras llaves que se modifican entre los diferentes registros que contribuyen al multiplexado. En nuestra propuesta cada máscara llave genera un canal de datos encriptados. Cada objeto de entrada se codifica empleando simultáneamente dos máscaras llaves. Entre exposiciones se emplea una máscara llave común y una no común. De esta manera, cuando se emplea una de las máscaras llaves en la etapa de desencriptación, se recupera la información de un único ó ambos objetos de entrada dependiendo de si se emplea una máscara común ó no común, respectivamente. Este esquema modificado mantiene las ventajas inherentes a la versión convencional del JTC y permite el acceso selectivo a distintos niveles de información. Esta propuesta puede ser extendida para un mayor número de objetos de entrada aumentando el número de máscaras llaves y de exposiciones ó bien incorporando nuevas llaves de multiplexado tales como la longitud de onda.

Es importante remarcar que en los últimos años se ha verificado que los sistemas de encriptación óptica son vulnerables a los ataques. En ese aspecto, el multiplexado mejora la seguridad de los sistemas ópticos de codificación, debido a que es muy difícil identificar el número de imágenes encriptadas que están almacenadas en el medio de registro. Esto se debe a la naturaleza de la información encriptada, dado que la suma de patrones de ruido blanco aleatorio dan como resultado un nuevo patrón de ruido blanco donde las distribuciones encriptadas individuales asociadas a cada canal son indistinguibles. Las aplicaciones que involucran múltiple almacenamiento de información encriptada son de gran interés debido a que incrementan la seguridad frente a los ataques.

Los resultados obtenidos en esta Tesis relativos a la degradación de la imagen recuperada cuando hay pérdida de datos encriptados por efecto del multiplexado y/ó del área finita del medio de almacenamiento mostraron marcadas diferencias para los sistemas 4*f* y JTC. Esto se debe a la naturaleza espacial y frecuencial del plano de encriptación para el 4*f* y JTC, respectivamente. Por esta razón, será de relevancia

investigar la respuesta a la pérdida de datos encriptados en los dominios de Fresnel y de Fourier fraccionario.

La caracterización de un sistema de encriptación implica utilizar alguna métrica para determinar el nivel de degradación en la imagen desencriptada. La métrica más usual es el error cuadrático medio, sin embargo hemos verificado que no es una métrica adecuada para evaluar imágenes desencriptadas con bajos niveles de relación señal ruido. En ese sentido, en un futuro será importante establecer nuevas métricas de desempeño que tengan en cuenta las características de los arreglos de codificación óptica.

VII.2 Lista de publicaciones

Algunos aspectos originales de este trabajo fueron la base de las siguientes publicaciones

- D. Amaya, M. Tebaldi, R. Torroba, and N. Bolognini, "Wavelength multiplexing encryption using joint transform correlator architecture," Appl. Opt. 48, 2099-2104 (2009).
- D. Amaya, M. Tebaldi, R. Torroba and N. Bolognini. “Digital color encryption using a multi-wavelength approach and a joint transform correlator”. *J. Opt. A: Pure Appl.* Opt. 10 104031 (2008).
- Myrian Tebaldi, S. Horrillo, E. Pérez-Cabré, M. Millán, D. Amaya, R. Torroba and N. Bolognini."Experimental color encryption in a joint transform correlator architecture". 2011 J. Phys.: Conf. Ser. 274 012054.
- D. Amaya, M. Tebaldi, R. Torroba and N. Bolognini.'' Multichanneled puzzle-like encryption'', Optics Communications, 281, 3434-3439 (2008).
- D. Amaya, M. Tebaldi, R. Torroba, and N. Bolognini, "Multichanneled encryption via a joint transform correlator architecture," Appl. Opt. 47, 5903-5907 (2008).
- D. Amaya, M. Tebaldi, R. Torroba and N. Bolognini, " Encoding degree testing in a 4f architecture", Proc. SPIE 8011, 801179 (2011); http://dx.doi.org/10.1117/12.902172