MULTIPLEXADO EN COLOR PARA ESQUEMAS OPTICOS DE ENCRIPTACION

Sierra Sosa, Daniel[1], Tebaldi, Myrian[1], Horrillo, Sergi[2], Pérez-Cabré, Elisabet[2], Millán, María S.[2], Bolognini, Nestor[1], Torroba, Roberto[1]

1 Centro de Investigaciones Ópticas (CONICET La Plata-CIC) y UID OPTIMO, Departamento de Ciencias Básicas, Facultad de Ingeniería, Universidad Nacional de La Plata, P.O. Box 3, M. B. Gonnet (1897), La Plata, Argentina. Email: myrianc©ciop.unlp.edu.ar
2 Departamento de Óptica y Optometría de la Universidad Politécnica de Cataluña, Terrasa (España)

Palabras Claves: encriptación, multiplexado, speckles, fotorrefractivos.

1. Introduccion.

Las técnicas ópticas evidencian un gran potencial para el desarrollo de sistemas de encriptación de imágenes, mediante la operación de correlación. Dichas técnicas están basadas en las arquitecturas ópticas (4f [1] y JTC [2]) con herramientas de la holografía. En los esquemas mencionados, el uso de máscaras de fase permite la obtención de una distribución de ruido blanco aleatorio en el plano de encriptación. En la etapa de recuperación, la imagen codificada es reconstruida mediante el empleo de los mismos parámetros ópticos de la codificación [3-6].

Una imagen encriptada es un diagrama de speckle, y como es conocido, los speckles dependen de las propiedades geométricas del sistema óptico así como de la longitud de onda. Entonces, la longitud de onda será utilizada en nuestra propuesta como un parámetro extra necesario para recuperar las imágenes encriptadas y por lo tanto otorgar seguridad adicional a los datos almacenados. En este trabajo se presenta una técnica alternativa experimental de encriptación de imágenes en canales de color empleando cristales fotorrefractivos tipo silenitas (BSO y BTO) como medio de registro [7]. Para proceder a la implementación experimental del multiplexado de imágenes se analizará la sensibilidad espectral del medio de registro utilizado.

Adicionalmente, es de interés almacenar múltiples datos encriptados en un único medio de registro. Para dicho fin proponemos un esquema multiplexado en longitud de onda, libre de solapamiento y que por lo tanto hace que las diversas imágenes almacenadas en un único paquete puedan ser recuperadas individualmente, aun empleando la misma máscara encriptadora. Se realizará un estudio detallado de los mecanismos que permitan eliminar el solapamiento de la información en el plano de recuperación.

Para ello, se analizará una arquitectura óptica para la implementación del manejo seguro de múltiples imágenes por medio de canales de color. Las imágenes encriptadas y multiplexadas están constituidas por la suma de diagramas de speckle indistinguibles, por lo tanto no es posible determinar ni la cantidad ni la naturaleza de las imágenes almacenadas lo que establece el grado de seguridad de la información codificada.

2. Resultados experimentales

El esquema experimental básico en la etapa de encriptación consiste en una formación de imágenes simple en donde en el plano de entrada (plano M) se coloca un difusor de fase pura (vidrio despulido) y en el plano de la lente (plano L) se coloca una máscara consistente en dos pequeñas aberturas (pupilas) simétricas respecto al eje óptico. En una de las pupilas se posiciona el objeto a ser procesado y la otra sirve como referencia interferencial. Este esquema se muestra en la Figura 1 a). Este proceso genera en el plano imagen de la lente (plano C) el diagrama de speckle que codifica a nuestro objeto de entrada y por lo tanto la

encriptación del mismo. En este plano se encuentra el medio de registro (cristal fotorrefractivo) que nos permitirá almacenar la información encriptada y facilitar su posterior reconstrucción.

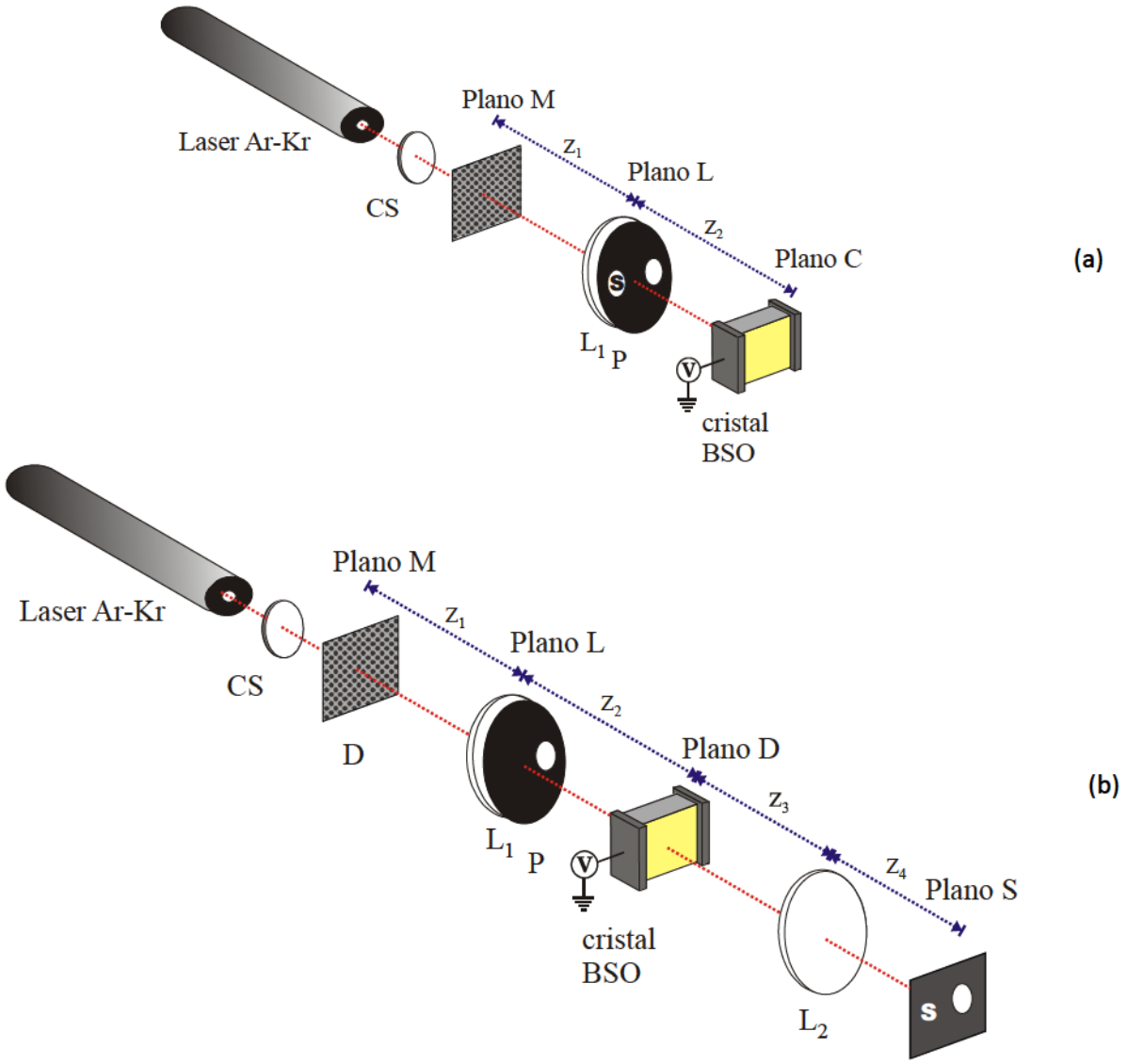

Figura 1 a) Esquema de encriptación de cada objeto de entrada (z_1= 40 cm, z_2= 40 cm, f_1= 20 cm), y b) Esquema de desencriptación (donde A: difusor, P: mascara con múltiples aberturas L_1: lente de distancia focal f_1 (f_1= 20 cm), L': lente de distancia focal f_2 (f_2= 35 cm,) y donde las distancias: z_1= 40 cm, z_2= 40 cm, , z_3=30 cm y z_4= 70 cm).

En la Figura 1 b) apreciamos el esquema de reconstrucción en donde basta una simple iluminación con la misma fuente de luz original, la misma mascara de entrada posicionada adecuadamente y la pupila de referencia en el plano de la lente sin el haz objeto. El cristal fotorrefractivo se ubica en el plano C de tal forma de ser iluminado en las mismas condiciones originales del proceso de codificación. Esta iluminación genera un frente de onda que contiene la información decodificada y que la lente L_2 se encargara de formar nuevamente la imagen en el plano de salida S. Los procesos de codificación con diagramas de speckle se anulan en la etapa de desencriptación, generando el proceso inverso en exactamente las mismas condiciones gracias a la reversibilidad de los caminos ópticos. La clave de este proceso está en el diagrama de speckle el cual es aleatorio e irreproducible

por medios mecánico ya que son distribuciones complejas de fase requiriendo de un proceso holográfico como el aquí expuesto para el almacenamiento y su posterior reconstrucción. Cuando decimos repetir exactamente las condiciones de registro implicamos utilizar al misma longitud de onda de la fuente de iluminación así como todos los parámetros geométricos del sistema óptico (distancia focal, pupila apertura del sistema óptico) y contar con exactamente el mismo diagrama de speckle.

El proceso descripto implica un único objeto de entrada pero las ventajas de los procesos holográficos residen en el almacenamiento de múltiple información. La adición en un único medio de registro como el mencionado no degrada los diagramas guardados en el mismo, dado que garantiza el mantenimiento de las mismas características relativas de fase de los frentes de onda incidentes. En base a esto en nuestra propuesta si cambiamos sucesivamente en el mismo esquema de la Figura 1 a) distintos objetos de entrada, es posible almacenar toda esta información en un único medio de registro tales como los cristales fotorrefractivos tipo silenitas (BSO, BTO). Esta idea introduce el concepto de multiplexado al cual aludimos en la presente contribución.

En un dispositivo de encriptación, si la máscara aleatoria de fase en la etapa de desencriptación no es correcta, la imagen original no será reconstruida. Esta característica permite almacenar múltiple información empleando por ejemplo diferentes mascaras de fase para encriptar cada objeto. Asimismo, si alguno de los parámetros ópticos utilizados para codificar los datos de entrada son incorrectos, aún empleando en la etapa de desencriptación la máscara de fase correcta, el objeto de entrada no podrá ser reconstruido. Por lo tanto los mencionados parámetro geométricos también son llaves extras de decodificación y pueden ser aprovechados para almacenar múltiples datos y/o imágenes. Surge en este punto la cuestión de que al momento de reconstruir toda esta información en la etapa de desencriptación se superpondrá en un mismo lugar espacialmente. La solución a este eventual solapamiento seria introducir una alteración en el esquema de registro que sea única para cada objeto de esta manera se mantiene las condiciones de seguridad y a su vez nos permite aislar cada objeto individual sin superposiciones con los restantes. Esto implica un análisis geométrico que determine que parámetro o parámetros sean adecuados alterar para estos fines. Esto requiere una calibración de estos parámetros que garantice reconstrucciones libres de solapamiento. Un parámetro inspeccionado es la longitud de onda de la fuente de iluminación que rige el tamaño de cada speckle individual que compone el diagrama desencriptador. En la Figura 3 exploramos esta dependencia para las longitudes de onda disponible experimentalmente utilizando un laser multilinea de ArK. Asi, para el caso que se encripto la letra X con la fuente emitiendo en 520 nm, solo se reconstruye para este caso y no para las longitudes de onda como se muestra en el ejemplo. Cabe aclarar que en esta experiencia no se alteraron los restantes parámetros del sistema de decodificación.

Si se almacenan múltiples datos con diferentes longitudes de onda se superpone espacialmente en la misma posición en el plano S, tanto los datos correctamente desencriptados como la información no desencriptada. La información correspondiente a la imagen no desencriptada se comporta como ruido blanco sobre los datos de interés. Entonces, a medida que se incrementa el número de datos, aumenta el número de términos que contribuyen al ruido en el plano de recuperación, hasta llegar un momento en que no se puede discriminar el dato desencriptado debido al ruido generado por los no desencriptados. Sin embargo, debemos destacar que utilizando este concepto, es posible llevar a cabo la encriptación de imágenes a color.

En la Figura 3 se muestra el análisis de la respuesta a la reconstrucción de la letra **X** utilizada como objeto de entrada cuando la pupila de referencia adopta otras posiciones en el plano de la lente. Se ve claramente que la reconstrucción es correcta solo cuando la pupila coincide con la posición original. Esto nos indica que es posible almacenar tantos

objetos como diferentes posiciones pueda adoptar esta pupila. Asimismo esto permite mediante el uso de diferentes arreglos de pupilas reconstruir cada objeto en el plano de salida (plano S) en una posición espacial distinta. En consecuencia, este objeto estará libre del ruido debido a los datos no desencriptados.

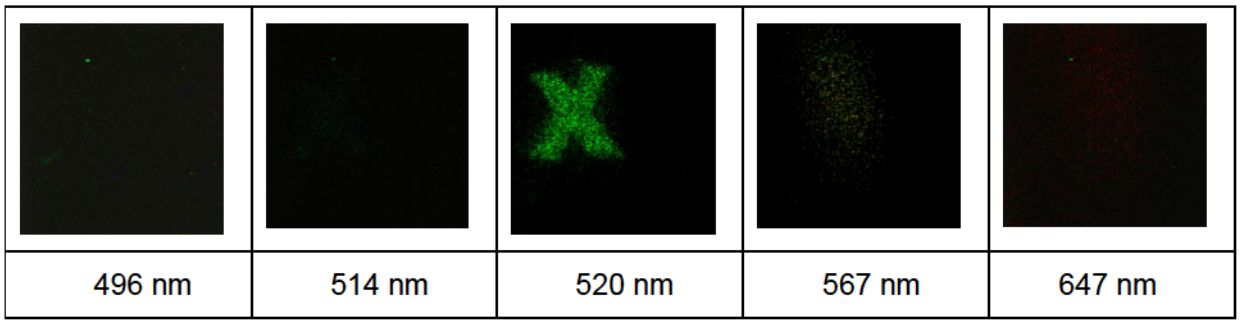

Figura 2 Imágenes desencriptadas con la misma máscara codificadora y la misma pupila que en la etapa de encriptación pero con diferentes longitudes de onda de la fuente luminosa.

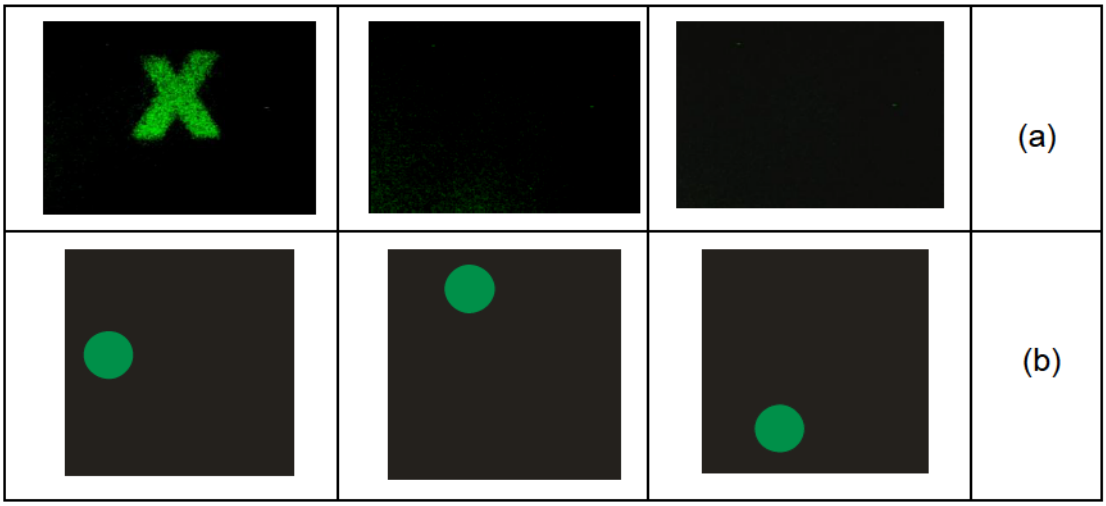

Figura 3 (a) Imágenes desencriptadas con la misma máscara de codificación y la misma longitud de onda de la fuente luminosa que en la etapa de registro, pero con pupilas en diferentes posiciones. (b) posición de la pupila utilizada en la etapa de desencriptación.

En la Figura 4 se presentan los objetos desencriptados según el procedimiento descripto más arriba. Cada uno de los objetos fue almacenado empleando simultáneamente diferentes posiciones de las pupilas y diferentes longitudes de onda. La selección adecuada de los distintos parámetros ópticos y geométricos evita el solapamiento es decir la superposición de datos correctamente decodificados, como se puede confirmar a partir de los resultados presentados en la Figura 4. Nuestra propuesta a través del empleo de las pupilas permite la decodificación de cada uno de los objetos sin la presencia de ruido proveniente de las restantes datos, dado que los mismos se localizan en posiciones espaciales diferentes.

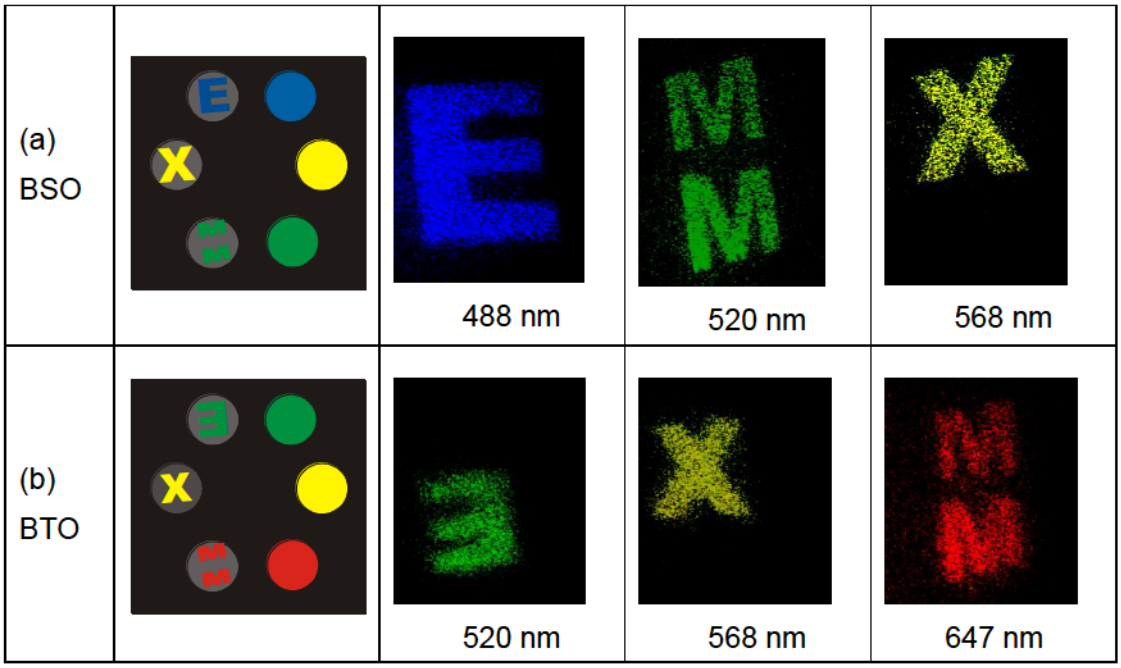

Figura 4 Imágenes desencriptadas experimentalmente correspondientes a letras almacenadas en un unico medio fotorrefractivo (cristales fotorrefractivos BSO y BTO) empleando difentes longitudes de onda de una fuente laser.

3. Conclusiones

En este trabajo se propone el empleo de una nueva arquitectura de encriptación basada en la formación de imagen para el multiplexado de datos codificados. Se emplean aberturas en el plano de la lente formadora de imagen en la etapa de registro para obtener, en la etapa de recuperación, datos individuales no afectados por el ruido debido a los datos no desencriptados. Además, se emplearon diferentes longitudes de onda tanto en la lectura como en la escritura, lo que proporciona un nivel adicional de seguridad.

En resumen nuestra propuesta se basa en un reposicionado inteligente mediante el empleo de aperturas múltiples que permite recuperar aisladamente los datos correspondientes a cada registro y además con la posibilidad de incluir a la longitud de onda como parámetro extra.

4. Bibliografía

1. P Refregier, B Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Optics Letters 20 (7), 767-769 (1995).
2. T Nomura, B Javidi, "Optical encryption using a joint transform correlator architecture," Optical Engineering 39 (8), 2031-2035 (2000).
3. G. Situ and J. Zhang, "Multiple-image encryption by wavelength multiplexing," Optics Letters 30, 1306-1308 (2005).
4. J. F. Barrera, R. Henao, M. Tebaldi, N. Bolognini, R. Torroba, "Multiple image encryption using an aperture-modulated optical system," Optics Communications 261(1), 29-33 (2006).

5. D. Amaya, M. Tebaldi, R. Torroba, N. Bolognini, "Wavelength multiplexing encryption using joint transform correlator architecture," Applied Optics 48(11), 2099-2104 (2009).

6. D. Amaya, M. Tebaldi, R. Torroba, N. Bolognini, "Multichanneled encryption via a joint transform correlator architecture," Applied Optics 47, 5903-5907 (2008).

7. G. Unnikrishnan, J. Joseph, K. Singh, "Optical encryption system that uses phase conjugation in a photorefractive crystal," Applied Optics, 37(35), 8181-8186 (1998).