Sistema Óptico de Encriptación de Doble Máscara de Fase bajo Arquitectura 4f

Carlos A. Ríos[1]
Edgar A. Rueda[2]
John F. Barrera[3]

Resumen

Actualmente el área de la encriptación óptica de información concentra los esfuerzos de muchos investigadores en diferentes laboratorios del mundo, esto debido a que las contribuciones presentadas en las dos últimas décadas han mostrado la confiabilidad, versatilidad y aplicabilidad de los sistemas ópticos de encriptación. Uno de los sistemas ópticos de encriptación más antiguo, más usado y que actualmente está protegido por varias patentes se basa en la utilización de dos máscaras aleatorias de fase y una arquitectura 4f. En esta contribución se hace una revisión bibliográfica de este sistema óptico de encriptación. Se presenta la teoría y el funcionamiento básico explicando los montajes y técnicas que permiten su implementación experimental. Con el fin de mostrar la validez del método, se presentan los resultados obtenidos mediante la simulación computacional del sistema óptico virtual.

1 Grupo de Óptica y Fotónica, Instituto de Física, Universidad de Antioquia, carios@barlai.udea.edu.co
2 Grupo de Óptica y Fotónica, Instituto de Física, Universidad de Antioquia, erueda@fisica.udea.edu.co
3 Grupo de Óptica y Fotónica, Instituto de Física, Universidad de Antioquia, jbarrera@fisica.udea.edu.co

Fecha de recepción: 17 de Agosto de 2010
Fecha de aceptación: 31 de Octubre de 2010

Palabras clave

Arquitectura 4f, desencriptación, encriptación, máscara de seguridad, procesamiento óptico.

Abstract

Nowadays the area of optical encryption of information concentrates the efforts of many researchers in laboratories around the world, mainly because contributions presented in the last two decades have shown the reliability, versatility and applicability of such systems. One of the most successful systems, which is currently protected by several patents, is based on the use of two random phase masks and a 4f architecture. In this contribution we do a review of this optical encryption system. We present the theory and the basic procedure explaining the setups and techniques that allow its experimental implementation, and we present results obtained by computational simulations of the optical virtual system to show the validity of the method.

Keywords

4f architecture, decryption, encryption, optical processing, security mask.

1. INTRODUCCIÓN

Desde la antigüedad, el hombre se ha visto en la necesidad de transmitir información a grupos privilegiados de personas y para ello se ha apoyado en el uso de códigos. Uno de los primeros códigos fue la escritura misma, en una época en que sólo un reducido grupo de personas sabía leer y escribir. Con el tiempo, a medida que más gente conocía la escritura los códigos se volvieron cada vez más complejos.

En la era moderna, el advenimiento de las comunicaciones por radio llevó a un aumento de la complejidad de los códigos debido a que la información era ahora transmitida por canales abiertos. Se empieza entonces a hablar de "encriptación de la información" la cual requiere de una llave para poder descifrar la información oculta, y que sólo conocerán aquellas personas que estén autorizadas a acceder a la información. En la actualidad, con la aparición de la era digital y la dependencia en aumento de la humanidad a la información, han sido creados nuevos métodos de encriptación cada vez más seguros. Casi en su totalidad, todos los métodos de encriptación de información corresponden a protocolos computacionales que buscan hacer la información codificada altamente indescifrable, pero tienen sus desventajas, entre ellas están el tiempo de procesamiento y su vulnerabilidad bajo ciertas condiciones (Cam-Winget et al., 2003; Bellare et al., 1988)

Existen muy buenas razones para considerar el uso de técnicas de procesamiento óptico en sistemas de encriptación de información. A diferencia de los computadores, los dispositivos ópticos tienen una inherente capacidad para procesar en paralelo. Por lo tanto, cuando hay un gran volumen de información a ser procesada, el procesamiento en paralelo presenta una velocidad de transmisión superior a sus contrapartes electrónicas.

Además de la rápida transmisión de la información, los procesadores ópticos ofrecen otras ventajas en cuanto a seguridad. La información puede ser codificada en dimensiones como la fase, longitud de onda, frecuencia espacial o la polarización de la luz; un dispositivo sensible a la intensidad como una cámara CCD no puede copiar todas estas dimensiones (por ejemplo la fase). Asimismo, en un montaje óptico se puede usar como llave de

seguridad un difusor, que es un elemento físico que le introduce fluctuaciones aleatorias de fase a un frente de onda incidente. Cuando se juntan todas las propiedades de las técnicas ópticas de encriptación, se incrementa sustancialmente el número de posibilidades matemáticas que se deben tener en cuenta cuando se desea romper el código; lo que hace que estos sistemas sean de gran confiabilidad (Javidi, 1997).

La propuesta de la utilización de sistemas ópticos que usan distribuciones aleatorias para codificar información se remonta cuando menos a 1976, cuando Françon & May (1996) sugieren codificar un mensaje usando los cambios aleatorios de fase producidos por un difusor. Para extraer el mensaje que esta codificado es absolutamente necesario poseer la información del difusor, que actuaría en este caso como llave de codificación y decodificación.

Una década más tarde e independientemente de la primera propuesta, la idea de codificar información usando distribuciones aleatorias fue aplicada por Kafri & Keren (1987); usando por primera vez la palabra "encriptación" para describir la codificación de datos en el contexto de la óptica. En este método se utilizaron dos distribuciones de amplitud dispuestas al azar para codificar información, donde las áreas de las distribuciones que poseen la información encriptada están correlacionadas. Por lo tanto, al superponer las distribuciones de amplitud las áreas correlacionadas son resueltas del fondo y debido a la diferencia de luz transmitida se puede observar el objeto que estaba codificado. Lo más interesante y notable del método es que mientras la encriptación es local el proceso de decodificación es global.

En un trabajo pionero, Refregier & Javidi (1995) proponen un método de encriptación de datos en el cual se usan dos máscaras aleatorias de fase, una en el plano de entrada y otra en el plano de Fourier, para encriptar la información. Método que se denominó "sistema de encriptación de doble máscara de fase". Para decodificar un dato complejo es necesario generar el complejo conjugado de las dos máscaras aleatorias, mientras que para el caso de datos de amplitud solo es necesario poseer el complejo conjugado de la máscara que se situó en el plano de Fourier durante la encriptación. Por lo tanto el sistema de encriptación se

basa en el uso de máscaras aleatorias de fase como llaves de seguridad. Éste trabajo pionero incentivó el crecimiento de una nueva línea de investigación, "la encriptación óptica"; desde ese momento y hasta la fecha, esta nueva línea ha dado lugar a múltiples investigaciones y como resultados de éstas, se han presentado un gran número de interesantes desarrollos en esta área.

En la primera implementación experimental (Javidi et al., 1996) del sistema de encriptación de doble máscara de fase (SEDMF) bajo arquitectura 4f, la imagen encriptada era registrada en una película holográfica. Luego, para recuperar la información, tanto el complejo conjugado de la llave de seguridad como el holograma de la información encriptada debían ser insertados en un montaje holográfico que servía de estación desencriptadora. Para aliviar las desventajas que presentaba esta primera implementación, Unnikrishnan et al. (1998) presentaron la demostración experimental de un sistema de encriptación que incluye un cristal fotorrefractivo como medio de registro y vidrios esmerilados como llaves de seguridad. En esta implementación, la encriptación y desencriptación se efectúa en tiempo real, sin necesidad de emplear el complejo conjugado de la llave de seguridad y sin el requerimiento de posicionar ningún elemento durante la desencriptación.

La propuesta e implementación experimental de este sistema de encriptación incentivaron un notable crecimiento de las investigaciones en el área de la encriptación óptica de información. Todas las contribuciones presentadas a la fecha han demostrado la gran potencialidad que tienen los sistemas ópticos de encriptación para ser implementados en aplicaciones prácticas.

Debido a las características de seguridad y a sus ventajas en implementación, una de las arquitecturas ópticas de encriptación más usadas es la 4f. Por esta razón, el resto de esta contribución se centrará en la descripción de las técnicas experimentales y de los sistemas ópticos virtuales que hacen uso de esta arquitectura para la encriptación de la información y para el manejo seguro de múltiples datos.

2. SISTEMA ÓPTICO DE ENCRIPTACIÓN DE DOBLE MÁSCARA DE FASE QUE USA UNA ARQUITECTURA 4f

Una arquitectura *4f* es un sistema óptico que utiliza dos lentes, usualmente de igual distancia focal f (lo cual no es estrictamente necesario) y tiene una longitud total igual a *4f*, de ahí su nombre. Esta arquitectura es usualmente usada como sistema formador de imágenes o como correlador (Gaskill, 1978), gracias a las propiedades de las lentes para realizar de manera óptica la transformada de Fourier del campo que incide sobre ella (Goodman, 1996).

La aplicación de esta arquitectura en la encriptación óptica de información fue inicialmente propuesta por Réfrégier & Javidi (1995), siendo así la propuesta pionera en este tema. Su idea fundamental es encriptar la información como ruido blanco por medio del uso de dos máscaras aleatorias de fase, ubicadas en el plano de entrada y en el plano de Fourier de la primera lente. Este proceso es completamente reversible sólo en el caso que se conozcan la máscara del plano de Fourier cuando la información es de amplitud, y ambas máscaras si la información es compleja o de fase (Barrera, 2006).

2.1 Modelo Teórico del Sistema

Sea $o(x_0, y_0)$ la información a encriptar y sea $\alpha(x_0, y_0) = \exp(i2\pi\, b(x_0, y_0))$ la máscara aleatoria de fase del plano de entrada (Fig. 1a y Fig. 2), donde $b(x_0, y_0)$ es una función aleatoria uniformemente distribuida entre los valores [0, 1], el campo en el plano de entrada corresponde al producto entre el objeto a encriptar y la máscara de fase.

$$u_0(x_0, y_0) = o(x_0, y_0)\alpha(x_0, y_0) \tag{1}$$

Cuando una onda plana monocromática y coherente, lo que correspondería experimentalmente a un haz láser colimado (Siegman, 1986), ilumina el plano de entrada, la lente L realiza la transformada de Fourier de $u_0(x_0, y_0)$ en el plano K (Fig. 1a). Para lograr encriptar la información en forma de ruido blanco se

multiplica el campo de este plano por otra máscara de fase aleatoria $\beta(x_1, y_1) = \exp(i2\pi\, h(x_1, y_1))$, con $h(x_1, y_1)$ aleatoria y uniformemente distribuida en el intervalo [0, 1]. Así, utilizando las propiedades de la transformada de Fourier aplicada sobre un producto de funciones y multiplicando por la segunda máscara, el campo resultante en el plano K es

$$u_1(x_1, y_1) = \frac{1}{i\,\lambda\, f_L}\left[O\left(\frac{x_1}{\lambda\, f_L}, \frac{y_1}{\lambda\, f_L}\right) \otimes A\left(\frac{x_1}{\lambda\, f_L}, \frac{y_1}{\lambda\, f_L}\right)\right] \beta(x_1, y_1) \tag{2}$$

donde $O(x_1, y_1)$ y $A(x_1, y_1)$ son los espectros de Fourier de las funciones $o(x_0, y_0)$ y $\alpha(x_0, y_0)$ respectivamente, $\boldsymbol{\lambda}$ es la longitud de onda del láser usado, f_L es la distancia focal de la lente L, (x_1, y_1) son las nuevas coordenadas del plano de Fourier y $\otimes$ representa el producto convolutivo. El montaje de encriptación es mostrado en la Fig. 1a.

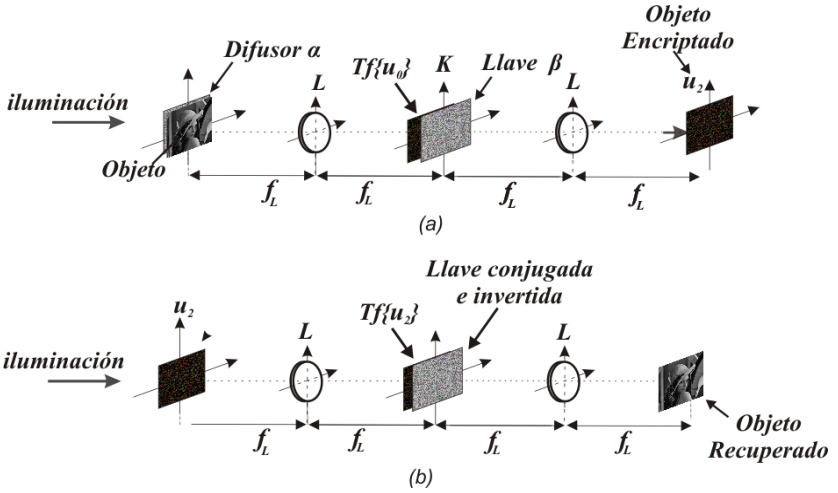

Fig. 1. Codificación de doble máscara de fase en una arquitectura 4f. Sistemas de (a) encriptación y (b) desencriptación. *K:* plano de Fourier; u_2*:* objeto encriptado. *L:* lente de distancia focal f_L*;* $Tf\{\cdot\}$: transformada de Fourier

Finalmente, se toma la transformada de Fourier de $u_1(x_1, y_1)$ por medio de la segunda lente, obteniendo como

resultado la imagen encriptada en forma de ruido blanco (Fig. 2c) (Kishk & Javidi, 2002)

$$u_2(x_2, y_2) = \frac{e^{i\,\pi}}{(\lambda\, f_L)^2}[o(-x_2, -y_2)\alpha(-x_2, -y_2)] \otimes B\left(\frac{x_2}{\lambda\, f_L}, \frac{y_2}{\lambda\, f_L}\right) \tag{3}$$

La ecuación (3) representa la imagen encriptada, nótese que la encriptación está dada por el producto convolutivo entre el plano de entrada en la estación encriptadora (Fig. 1a) y la función aleatoria $B\left(\frac{x_2}{\lambda\, f_L}, \frac{y_2}{\lambda\, f_L}\right)$.

Para el proceso de desencriptación se ubica la imagen encriptada en el plano de entrada de un sistema 4f (Fig. 1b), se ilumina con un haz monocromático colimado de luz coherente y se realiza la transformada de Fourier con la lente L, obteniéndose en el plano K una distribución de campo de la forma

$$u_3(x_3, y_3) = \frac{e^{i\,\pi}}{i(\lambda\, f_L)}\left[O\left(-\frac{x_3}{\lambda\, f_L}, -\frac{y_3}{\lambda\, f_L}\right) \otimes A\left(-\frac{x_3}{\lambda\, f_L}, -\frac{y_3}{\lambda\, f_L}\right)\right] \beta(-x_3 -, y_3) \tag{4}$$

multiplicando $u_3(x_3, y_3)$ por el complejo conjugado de la máscara $\beta(x_3, y_3)$ invertida, la cual tiene la forma

$$\beta^*(-x_3, -y_3) = e^{-i2\pi\, h(-x_3, -y_3)} \tag{5}$$

y realizando una segunda transformada de Fourier, en el plano de desencriptación (Fig. 2a) se obtiene

$$u_4(x_4, y_4) = o(x_4, y_4)\ \alpha(x_4, y_4). \tag{6}$$

Si la información es real al encontrar la intensidad $\sqrt{|u_4(x_4, y_4)|^2}$ desencriptamos exitosamente la información (Fig. 2e), pero cuando la información del objeto que esta encriptado es compleja se debe multiplicar $u_4(x_4, y_4)$ por el complejo conjugado de la máscara $\alpha(x_4, y_4)$.

Si se multiplica $u_3(x_3, y_3)$ por una máscara de fase distinta $\gamma(x_3, y_3)$ con transformada de Fourier $D(x_4, y_4)$, en un intento de

descifrar la información encriptada, en el plano de desencriptación se obtendría

$$u_4(x_4, y_4) = o(x_4, y_4)\ \alpha(x_4, y_4) \otimes B(x_4, y_4) \otimes D(x_4, y_4). \quad (7)$$

Por lo tanto, la información no es recuperada ya que sigue siendo ruido blanco debido al producto convolutivo de la información con dos funciones de fase aleatoria (Fig. 2d). Es precisamente por este hecho que la seguridad del sistema recae en la máscara aleatoria de fase que es empleada como llave. En la figura 2 se presentan simulaciones computacionales del sistema de encriptación.

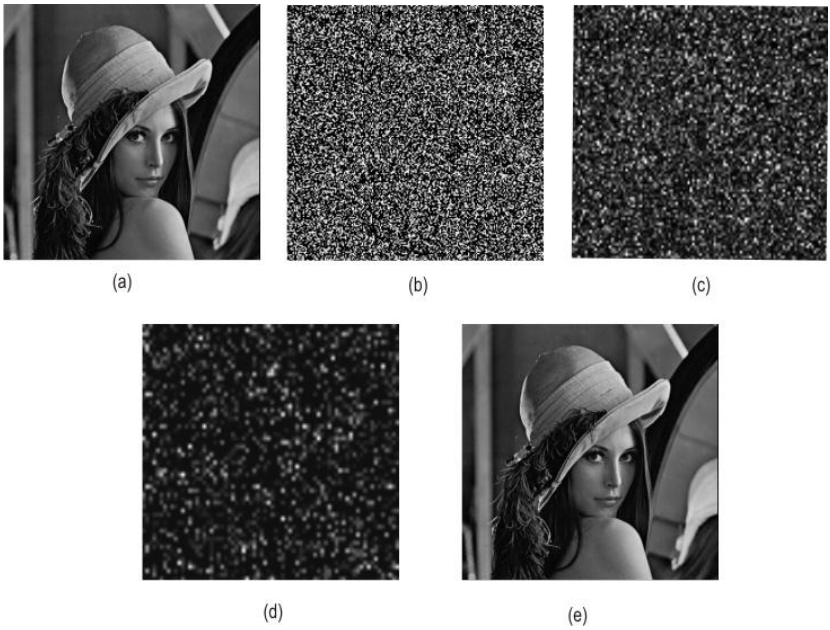

Fig. 2. (a) Imagen original, (b) llave de seguridad (máscara aleatoria de fase), (c) imagen encriptada, (d) imagen desencriptada cuando se usa una llave distinta a la usada en la encriptación y (e) imagen desencriptada cuando se usa la llave adecuada

3. IMPLEMENTACIÓN EXPERIMENTAL

En la primera implementación experimental del sistema 4f de encriptación con doble máscara de fase, realizada por Javidi et al. (1996), la imagen encriptada es registrada usando un montaje holográfico. En el montaje experimental el haz colimado es dividido por el divisor de haz DH_1 en un haz de referencia y un haz objeto (Fig. 3). El haz objeto ilumina el sistema de encriptación para generar la imagen encriptada, información que es registrada en una película holográfica usando la onda de referencia.

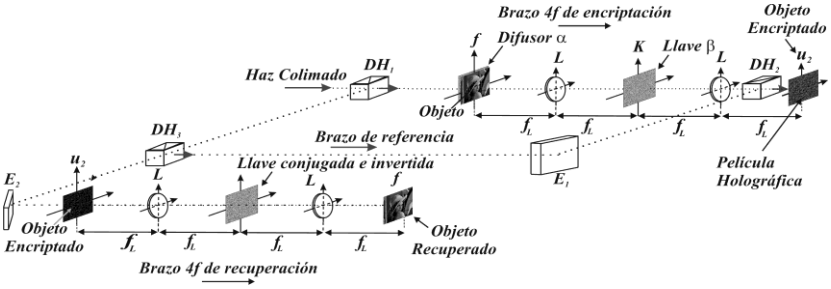

Fig. 3. Montaje experimental. DH_1, DH_2, DH_3: divisores de haz, o: objeto a encriptar; α: primera máscara aleatoria de fase; β: segunda máscara aleatoria de fase; L: lente de longitud focal f_L; E_1, E_2: espejos planos.

Para la desencriptación, la película holográfica que contiene la imagen encriptada y la llave de seguridad conjugada e invertida son insertadas en un sistema 4f. De manera que al iluminar el sistema con la onda de referencia que sale de DH_3, a la salida del sistema 4f se recupera el objeto que estaba encriptado.

Esta implementación experimental presenta varias desventajas: no trabaja en tiempo real, la precisión del posicionamiento de los elementos durante la desencriptación exige bajas tolerancias para que el proceso sea exitoso y se tiene que producir el complejo conjugado de la llave de seguridad, eliminando la posibilidad de usar como llaves elementos con alta complejidad como vidrios esmerilados.

Para aliviar las desventajas antes mencionadas, Unnikrishnan et al. (1998) presentaron un montaje que utiliza cristales fotorrefractivos para la encriptación y desencriptación de

información en tiempo real. A diferencia de la primera implementación, la utilización de los cristales permite obtener el complejo conjugado de la llave de seguridad por medio del mezclado de cuatro ondas, y por lo tanto la información es recuperada sin necesidad de generar el complejo conjugado de la llave de seguridad.

Un esquema del montaje que usa cristales fotorrefractivos es mostrado en la Fig. 4 (Barrera et al., 2005; Boyd, 2003), dónde se usa un láser de Nd YAG de 150 mW de potencia y 532 nm de longitud de onda como fuente de luz. La luz proveniente de la fuente láser es expandida y colimada para generar un haz plano y monocromático, que es dividido por el divisor de haz DH_1 en un haz de referencia y un haz objeto. El haz objeto ilumina el sistema 4f, que a su salida permite obtener la imagen encriptada, la cual puede registrase en la cámara CCD_2 por medio de DH_3.

Sobre el cristal incide un patrón de intensidad correspondiente a la interferencia entre el haz de referencia y el haz del objeto encriptado. Esta distribución de intensidad genera un campo de cargas espaciales en el cristal debido a la redistribución de portadores. El campo espacial de cargas resultante produce una perturbación del índice refractivo, el cual replica y almacena la información encriptada. Por lo tanto la información encriptada es registrada holográficamente, como variaciones del índice de refracción dentro del cristal.

Parte del haz de referencia transmitido por el cristal, se refleja sobre el espejo E_2 e incide de nuevo sobre éste, en la misma dirección pero en sentido contrario, al haz de referencia A_2. Cuando el haz reflejado A_2 pasa a través del cristal, genera un haz A_3 con amplitud de campo proporcional al complejo conjugado del objeto encriptado. Este haz conjugado se propaga en la misma dirección, pero en sentido contrario, al haz que contiene la información encriptada. Luego de pasar a través de la lente positiva L incide sobre la llave de seguridad ß. Finalmente, el objeto original es recuperado por medio de la lente L. Como se observa en la Fig. 4, para el registro del objeto de salida se usa la cámara CCD_1 junto con el divisor de haz DH_2.

Note que cuando el haz conjugado pasa a través de la máscara aleatoria de fase M_2, que en este caso es la llave de encriptación y

reconstrucción, compensa los cambios aleatorios de fase introducidos durante la encriptación. De esta forma el objeto puede ser desencriptado. Pero si el haz conjugado incide sobre una máscara de fase distinta, no existe tal compensación y por lo tanto no se puede recobrar la información original. Es importante resaltar que a diferencia del primer montaje experimental, el esquema que utiliza cristales fotorrefractivos permite encriptar y desencriptar utilizando el mismo sistema 4f.

En el montaje experimental se usa como máscara aleatoria de fase un vidrio con una de sus caras despulida, usualmente llamado difusor. Cuando una onda coherente ilumina un difusor, éste introduce fluctuaciones aleatorias de fase. Entonces, delante del difusor se obtiene una distribución de aspecto granular que constituye un patrón aleatorio (Danti, 1975; Erf, 1978). De acuerdo con esto y dado que el sistema de encriptación usa dos máscaras aleatorias de fase, la imagen encriptada es codificada en un patrón de speckle (Fig. 2c).

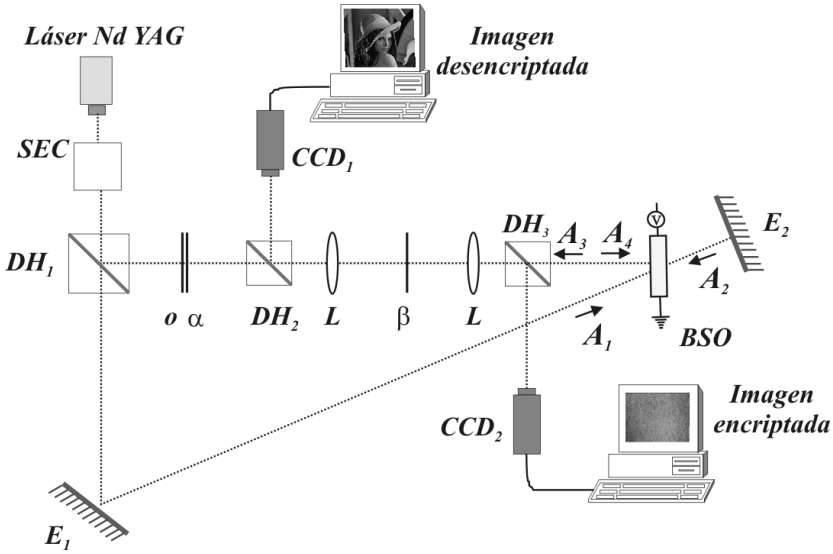

Fig. 4. Montaje experimental. (SEC: Sistema de Expansión y Colimación; CCD_1 y CCD_2: cámaras CCD; BSO: cristal fotorrefractivo; A_1: haz de referencia, A_2: haz reflejado por E_2, A_3: haz conjugado, A_4: haz que contiene el objeto encriptado)

Después de la primera implementación experimental del SEDMF, se utilizó la longitud de onda como llave de seguridad adicional (Matoba & Javidi, 1999a). En el esquema experimental, se forma la imagen del dato encriptado sobre un cristal fotorrefractivo y se muestra que para recuperar el objeto que está encriptado, además de poseer la llave de seguridad, se debe iluminar con la misma longitud de onda que se usó para encriptar el objeto.

Javidi & Nomura (2000) realizaron la primera implementación del sistema 4f usando holografía digital, lo que significa que la información se almacena en formato digital usando una cámara CCD, permitiendo así su integración a los sistemas de transmisión de información digitales. La inclusión de un esquema de holografía digital hace que la encriptación sea óptica y la desencriptación sea digital, por lo que esta contribución representa la primera implementación experimental de un sistema de encriptación óptico-digital. A diferencia de los montajes y procedimientos experimentales presentados a esa fecha, adicional al holograma del dato encriptado se debe registrar la información de la intensidad del espectro del dato encriptado y el haz de referencia del holograma.

En esa misma línea de desarrollo, se presentó un sistema experimental de encriptación y desencriptación usando holografía digital y moduladores espaciales de luz (Matoba & Javidi, 2002a). En el proceso de encriptación la imagen encriptada y la transformada de Fourier de la llave de seguridad son registradas holográficamente, y durante la desencriptación ambos datos son proyectados uno al lado del otro empleando un modulador espacial de luz. La intensidad de la transformada de los datos es proyectada en un modulador de luz, de manera que al generar la transformada de la información contenida en éste se puede recuperar el dato original.

4. TÉCNICAS DE MULTIPLEXADO Y AUMENTO DE LA SEGURIDAD

Una de las aplicaciones más importantes de los sistemas de encriptación son los procesos que involucran múltiples usuarios.

En este contexto las técnicas de múltiple almacenamiento de datos, usualmente llamadas técnicas de multiplexado, juegan un papel protagónico. Usando SEDMF bajo arquitectura 4f y diferentes técnicas de multiplexado, se han generado procedimientos que permiten el manejo seguro de varios datos y el aumento de la seguridad del sistema de encriptación, por ejemplo con técnicas que tienen como objetivo engañar a posibles intrusos (Barrera et al., 2007; 2009).

Un primer ejemplo, implica introducir un procedimiento de ocultamiento para reforzar la seguridad global del método (Barrera et al., 2007). En el procedimiento se usa una máscara de fase virtual para camuflar la máscara de decodificación original, de forma tal que si el intruso puede tener acceso a las dos informaciones (multiplexado y llave de seguridad) recuperará un dato falso, mientras que la información real permanece escondida.

De la misma manera, se introdujo una técnica de múltiple ocultamiento usando versiones escaladas de una máscara aleatoria de fase (Barrera et al., 2009a). En esta ocasión un objeto falso es encriptado usando una máscara aleatoria de fase, mientras que el resto de objetos son encriptados empleando una versión aumentada de dicha máscara. Al usuario autorizado, se le envían por canales separados la información del multiplexado (que contiene la suma de todas las imágenes encriptadas), la máscara original y la información del aumento; para que con estos datos pueda desencriptar todos los objetos contenidos en el mensaje. Mientras que si un usuario no autorizado intercepta el multiplexado y la máscara original, sólo desencriptará el dato falso y de esta forma será engañado.

Para incrementar la seguridad en la transmisión de datos se han propuesto varios métodos, en uno de ellos el principio de operación es la descomposición de la información de entrada en diferentes secciones (Amaya et al., 2008). Cada una de las secciones es encriptada usando un SEDMF, pero con una llave de seguridad, una polarización y una longitud de onda diferentes, luego esas imágenes encriptadas son multiplexadas. Para recuperar el dato encriptado, se debe recuperar cada una de las secciones por separado y luego superponerlas. Esta técnica representa un incremento en la seguridad del método ya que la

desencriptación de cada sección implica el conocimiento de su llave de seguridad, polarización y longitud de onda características. En un segundo método (Rueda et al., 2008) se generan llaves de seguridad a partir de sistemas dinámicos en régimen caótico, que junto a un sistema de sincronización permite la modificación constante de la llave de seguridad, dificultando así el acceso a la información al tener cada llave de seguridad un tiempo de vida muy corto. Una ventaja adicional está en que la información necesaria para la construcción de la llave de seguridad en la estación desencriptadora puede ser transmitida usando canales abiertos. Dentro de esta línea de trabajo, se ha propuesto la utilización de llaves de seguridad generadas mediante transformadas afines (Mosso et al., 2010). A partir de una imagen fuente y aplicando sobre ésta sucesivas operaciones de reflexión, traslación, rotación, recortes, escalamientos y algunas operaciones aritméticas, controladas por una serie de parámetros conocidos, se obtiene la llave de seguridad. Por lo tanto, en lugar de enviarle al usuario autorizado la máscara de fase aleatoria que representa la llave de seguridad, se le envía la imagen fuente y los parámetros de la transformación afín. La imagen fuente puede ser enviada por un canal abierto sin poner en riesgo la seguridad del método, pues un error en cualquiera de los parámetros de la transformada afín impide la recuperación de la información.

Asimismo, se desarrolló una técnica de multiplexado de ocultamiento para proporcionarle protección adicional al proceso de recuperación de la información (Barrera et al., 2009b). El proceso de ocultamiento se basa en la inclusión de una máscara de amplitud en la segunda lente del procesador 4f, de manera que cada vez que se desea encriptar un dato se debe cambiar dicha máscara. En este método, si la información del multiplexado de las imágenes encriptadas y la llave de seguridad son interceptadas por un intruso, éste recobrará un dato falso; mientras que el usuario autorizado al usar la información de las máscaras de amplitud empleadas durante la encriptación puede recuperar los datos verdaderos.

En otra contribución se encriptaron datos complejos, donde cada uno de ellos contiene diferente información en su amplitud y en su fase (Barrera & Torroba, 2009c). Las imágenes encriptadas

de los datos complejos es multiplexada y enviada como un solo dato a los usuarios autorizados. Para recuperar uno de los datos contenidos en el multiplexado, el usuario debe poseer la información de la llave de seguridad si desea recuperar la información de la amplitud, y adicionalmente la primera máscara aleatoria si desea obtener la información de fase. Por lo tanto, si el dato de interés es la información de fase y un usuario no autorizado intercepta el multiplexado y la llave de seguridad, recuperará la información de amplitud que no es la información válida.

Además, se emplearon llaves complejas en los procesos de encriptación y desencriptación de múltiples datos (Barrera et al., 2009d). En este método, la llave de seguridad está compuesta por la superposición de una máscara aleatoria de fase y una máscara de amplitud. En el proceso de multiplexado cada uno de los datos es encriptado usando la misma máscara de fase, pero una máscara de amplitud diferente. Si durante la recuperación de los datos sólo se emplea la máscara de fase, todos los objetos se recuperarán al mismo tiempo, lo que impedirá la discriminación de la información. Por lo tanto, la recuperación adecuada de cada uno de los datos requiere la utilización de la máscara de amplitud con que se encriptó cada dato.

Desde otra perspectiva, se pueden utilizar un conjunto de estaciones del sistema de encriptación 4f para propósitos de multiplexado seguro de datos (Yong-Liang et al., 2009). Para lograr la recuperación de la información que esta encriptada, es necesario implementar un algoritmo de recuperación de fase tipo cascada. Las simulaciones del sistema óptico virtual muestran que el conjunto de procesadores permite mejorar la seguridad del método. Siguiendo con la idea de aumentar la seguridad del sistema de encriptación, se desarrolló una aplicación que utiliza dos estaciones de seguridad independientes (Alfalou & Mansour, 2009). En la primera estación, el objeto a encriptar se multiplica por una función de fase y se lleva a cabo una transformada de Fourier, posteriormente se realizan transformadas de Fourier sucesivas donde en cada iteración se modifica la fase hasta que se obtenga un elemento de amplitud. Luego, a la salida de la primera estación se tendrá un elemento de amplitud modulado por una

fase. La salida de la primera estación se ingresa en la segunda estación, la cual es un sistema de encriptación de doble máscara de fase con arquitectura 4f. Finalmente, la salida de la segunda estación será la imagen encriptada. Esta técnica permite encriptar y recuperar múltiples datos con un alto grado de seguridad y de eficiencia.

En general, si la variación en un parámetro o en un elemento del sistema impide la recuperación de la información que esta encriptada, éste puede ser considerado como una llave de seguridad adicional, y por lo tanto podrá ser utilizado para el multiplexado de la información. Es así como se propuso la utilización de la longitud de onda como llave extra de seguridad (Situ et al., 2005). Cada uno de los datos es encriptado empleando una fuente de iluminación de diferente longitud de onda, y posteriormente todos los datos encriptados son multiplexados. Para recuperar la información de uno de los datos, además de poseer la información del multiplexado y de la llave de seguridad, se debe conocer la longitud de onda con que fue encriptado ese dato.

Con el propósito de aumentar la seguridad en el proceso y ampliar la capacidad de multiplexado, se usan dos difusores y un conjunto de pupilas como llave de seguridad en el sistema de encriptación (Singh et al., 2008). Los difusores y las máscaras de amplitud están en contacto en el plano de la primera transformada, donde las llaves adicionales de seguridad son la rotación de uno de los difusores y las pupilas que componen la máscara de amplitud. Usando la idea de emplear como llave de seguridad varios elementos en contacto, se demostró que dos patrones de speckle elongados y superpuestos pueden representar un llave de seguridad (Singh et al., 2009).

En las técnicas de multiplexado arriba mencionadas cada uno de los datos es encriptado y desencriptado secuencialmente. A diferencia de esto, se implementó un proceso de multiplexado que usa una arquitectura 4f junto con propagación en espacio libre para generar un proceso de multiplexado en un solo paso (Barrera & Torroba, 2010). Todos los datos son encriptados en el mismo instante, con diferentes llaves de seguridad y distintas distancias de propagación en espacio libre. La recuperación de los datos

puede hacerse individualmente o se pueden desencriptar todos los datos a la vez. Esta es una aplicación novedosa pues representa la primera técnica de "encriptación en un solo paso".

Se debe tener presente que la inclusión de técnicas de multiplexado en el área de la encriptación óptica representa grandes ventajas. En primer lugar, mediante estas técnicas se generan procesos multiusuario. Además, el multiplexado de datos permite aumentar la seguridad global del proceso mediante protocolos de distracción y engaño. Dichos protocolos pueden llegar a evitar la vulnerabilidad del sistema cuando un usuario no autorizado puede interceptar parte de la información involucrada en el proceso.

5. OTRAS APLICACIONES DEL SEDMF

El sistema de encriptación de doble máscara de fase también ha sido utilizado e integrado en otras líneas de trabajo, por ejemplo, en el domino temporal para evaluar su potencial aplicación en la transmisión segura de múltiples datos por medio de fibra óptica (Cuadrado-Laborde et al., 2008). En esta contribución se encontró que de acuerdo a la capacidad de multiplexado de las fibras ópticas, el contenido de ruido de la señal crece linealmente con el número de canales empleados. En una de las más recientes y novedosas aplicaciones se demuestra que es posible alcanzar super-resolución con una sola exposición, siempre y cuando se combine el sistema de encriptación de doble máscara de fase bajo arquitectura 4f y una técnica de compresión de detección (Rivenson et al., 2010).

6. CONCLUSIONES

Todas las contribuciones mencionadas en esta revisión evidencian la implementación y perfeccionamiento de sistemas ópticos, óptico-digitales y ópticos virtuales para la encriptación óptica de información, y demuestran la gran potencialidad que tienen los sistemas ópticos de encriptación para su

implementación práctica (Matoba & Javidi, 2002b; Matoba et al., 2009). Esto ha llevado a que estos sistemas estén protegidos por varias patentes (Javidi, 1999a; 1999b; Javidi & Matoba, 2002; Javidi, 2003). Es claro que el tema de investigación es de gran interés para la comunidad científica nacional e internacional, por lo tanto se advierten futuras aplicaciones que permitirán dinamizar el área de la encriptación óptica de información.

Para finalizar, es importante mencionar que este trabajo busca presentar una revisión, lo más completa posible, de lo que ha sido la encriptación óptica con doble máscara de fase y arquitectura 4f. Por esto se incluyen las contribuciones más importantes, representativas y que han generado líneas de desarrollo, según el criterio de los autores.

7. AGRADECIMIENTOS

Los autores le agradecen a Colciencias, a la Vicerrectoría de Investigación y al CODI (Universidad de Antioquia). J.F. Barrera le agradece el apoyo al programa "TWAS-UNESCO Associateship Scheme at Centres of Excellence in the South".

8. REFERENCIAS

Alfalou, A., Mansour, A., (2009); Double random phase encryption scheme to multiplex and simultaneous encode multiple images. Applied Optics, 48(31), 5933-5947.

Amaya, D., Tebaldi, M., Torroba, R., Bolognini, N., (2008); Multichanneled puzzle-like encryption. Optics Communications, 281(13), 3434–3439.

Barrera, J.F., Henao, R., Tebaldi, M., Bolognini, N., Torroba, R., (2005); Encryption-Decryption in a four-wave mixing arrangement. Proceedings of International conference on Optics and Optoelectronics PP-OIP-4.

Barrera, J.F., (2006); Encriptación óptica: estudio y desarrollo de arquitecturas alternativas, Instituto de Física, Universidad de Antioquia, Medellín, Colombia.

Barrera, J.F., Henao, R., Tebaldi, M., Torroba, R., Bolognini, N., (2007); Multiple-encoding retrieval for optical security. Optics Communications, 276(2), 231-236.

Barrera, J.F., Henao, R., Tebaldi, M., Torroba, R., Bolognini, N., (2009a); Digital encryption with undercover multiplexing by scaling the encoding mask, Optik 120(7), 342-346.

Barrera, J.F., Serna, J.H., Tebaldi, M., Bolognini, N., Torroba, R., (2009b); Manejo seguro de múltiples datos mediante una técnica de multiplexado de ocultamiento. Revista de la Sociedad Colombiana de Física, 41(3), 645-647.

Barrera, J.F., Torroba, R., (2009c); Efficient encrypting procedure using amplitude and phase as independent channels to display decoy objects. Applied Optics 48 (17), 3121-3129.

Barrera, J.F., Henao, R., Tebaldi, M., Bolognini, N., (2009d); Multiplexing encryption technique by combining random amplitude and phase masks. Optik 120(8), 351-355.

Barrera, J.F., Torroba, R., (2010); One step multiplexing optical encryption. Optics Communications, 283(7), 1268-1272.

Bellare, M., Desai, A., Pointcheval, D., Rogaway, P., (1988); Relations among notions of security for public-key encryption. Lect. Notes Compt. Sci. 1462, 26-45.

Boyd, R.W., (2003); Nonlinear Optics, 2ª edición, 4-17, Elsevier, San Diego, Estados Unidos.

Cam-Winget, N., Housley, R., Wagner, D., Walker, J., (2003); Security flaws in 802.11 data link protocols. Commun. ACM 46 (5), 35-39.

Cuadrado-Laborde, C., Duchowicz, R., Torroba, R., Sicre, E., (2008); Dual random phase encoding: a temporal approach for fiber optic applications. Applied Optics, 47(11), 1940-1946.

Danty, J.C., (1975); Laser speckle and related phenomena. Springer-Verlag, New York, Estados Unidos.

Erf, R.K., (1978); Speckle Metrology. Academic Press, New York, Estados Unidos.

Françon, M., May, M., (1975); Correlation and Information Processing Using Speckle Patterns.JOSA 66 (11), 1275-1282.

Gaskill, J.D., (1978); Linear Systems, Fourier Transform, and Optics, 449-521,Wiley-Interscience, New York, Estados Unidos.

Goodman, J.W., (1996); Introduction to Fourier optics, 2ª edición, 96-125, McGraw –Hill, Boston, Estados Unidos.

Javidi, B., Zhang, G., Li, J., (1996); Experimental demonstration of the random phase encoding technique for image encryption and security verification. Optical Engineering, 35(9), 2506-2512.

Javidi, B., (1997); Securing information with Optical Technologies. Physics Today 50(3), 27-32.

Javidi, B., (1999a); Methods and apparatus for encryption. U.S. patent 5,903,648.

Javidi, B., (1999b); Methods and apparatus for encryption. U.S. patent 6,002,773.

Javidi, B., Nomura, T., (2000); Securing information by use of digital holography. Optics Letters, 25(1), 28-30.

Javidi, B., Matoba, O., (2002); Methods and apparatus for secure ultrafast communication. U.S. patent 6,519,340.

Javidi, B., (2003); Methods and apparatus for encryption using partial information. U.S. patent 6,519,340.

Kafri, O., Keren, E., (1987); Encryption of pictures and shapes by random grids. Optics Letters 12 (6), 377-379.

Kishk, S., Javidi, B., (2002); Information hiding technique with double phase encoding. Applied Optics, 41(26), 5462–5470.

Matoba, O., Javidi, B., (1999a); Encrypted optical storage with wavelength-key and random phase codes. Applied Optics, 38(32), 6785-6790.

Matoba, O., Javidi, B., (2002a); Optical retrieval of encrypted digital holograms for secure real-time display. Optics Letters, 27(5), 321-323.

Matoba, O., Javidi, B., (2002b); Secure Ultrafast Data Communication and Processing. Optics and Photonics News , 13(5),71-73.

Matoba, O., Nomura, T., Pérez-Cabré, E., Millán, M., Javidi, B. (2009); Optical techniques for information security. Proceedings of IEEE, 57(6), 1128-1148.

Mosso, F., Tebaldi, M., Torroba, R., Bolognini, N., (2010); Double random phase encoding method using a key code generated by affine transformation. Optik, en prensa.

Réfrégier, P., Javidi, B., (1995); Optical image encryption based on input plane Fourier plane random encoding. Optics Letters, 20(7), 767-769.

Rivenson, Y., Stern, A., Javidi, B., (2010); Single exposure super-resolution compressive imaging by double phase encoding. Optics Express, 18(14), 15094-15103.

Rueda, E., Vera, C.A., Rodríguez, B., Torroba, R., (2008); Synchronized chaotic phase masks for encrypting and decrypting images. Optics communications, 281(23), 5750–5755.

Siegman A.E., (1986); Lasers, 2-76, University Science Books, Sausalito, Estados Unidos.

Singh, M., Kumar, A., Singh, K. (2008); Multiplexing in optical encryption by using an aperture system and a rotating sandwich random phase diffuser in the Fourier plane. Optics and Lasers Engineering, 46(3), 243–251.

Singh, M., Kumar, A., Singh, K., (2009); Encryption and decryption using a sandwich phase diffuser made by using two speckle patterns and placed in the Fourier plane : Simulation results. Optik, 120(17), 916–922.

Situ, G., Zhang, J., (2005); Multiple-image encryption by wavelength multiplexing. Optics Letters, 30(11), 1306-1308.

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

Yong-Liang, X., Xin, Z., Sheng, Y. Qiang, L., Yang-Cong, L., (2009); Multiple-image optical encryption: an improved encoding approach. Applied Optics 48(14), 2686-2692.