Revista Bistua
ISSN 01204211
Universidad de Pamplona
Pamplona-Colombia

Métodos Ópticos Como Herramienta Para Encriptar-Desecriptar Información

Myrian Tebaldi
Centro de Investigaciones Ópticas (CONICET-CIC,) P.O. Box 124, La Plata (1900), Argentina, UID OPTIMO, Facultad Ingeniería y Facultad Ciencias Exactas, Universidad Nacional de La Plata, La Plata, Argentina.

RESUMEN

Los datos trasmitidos a través de los sistemas informáticos son factibles de ser falsificados. No obstante es posible implementar procesos de codificación para protegerlos. La idea central radica en el uso de claves ó llaves sin las cuales es imposible recuperar la información. Las técnicas ópticas evidencian un gran potencial para el desarrollo de tales sistemas empleando la correlación óptica.

Uno de los métodos más conocidos de encriptación esta basado en el uso de una doble máscara aleatoria de fase, una en el plano de entrada y la segunda en el plano de Fourier. Asimismo, se han desarrollado otros arreglos de encriptación usando usando arquitecturas de correlador JTC y técnicas de holografía digital. La encriptación mediante técnicas de correlación puede implementarse: en forma analógica, en memorias holográficas almacenadas en cristales fotorrefractivos y mediante técnicas digitales.

Los medios fotorrefractivos que no requieren procesamiento previo para leer la información en ellos registrada, permiten el almacenamiento holográfico múltiple (modificando el ángulo de registro, el estado de polarización, empleando pupilas de múltiples aberturas, etc).

Se estudiaron arreglos ópticos de encriptación basados en correladores 4f y de transformada conjunta (JTC). Una ventaja significativa de los correladores tipo JTC es que no requieren el cálculo de una nueva función filtro cada vez que la imagen de referencia cambia y por otra parte prácticamente no necesitan alineación. Es de destacar que actualmente la mayoría de las técnicas de almacenamiento de múltiples datos encriptados se basan en el uso de correladores convergentes tipo 4*f*, sin embargo en la arquitectura del JTC no ha sido aún aprovechada la alta capacidad de almacenamiento de los medios de registro volumétricos como los cristales fotorrefractivos.

Se estudiaron técnicas de encriptación múltiple que empleen las arquitecturas antes mencionadas. En particular, se analizaron la posibilidad de almacenar múltiples datos a partir del cambio de la longitud de onda de registro en la arquitectura JTC. Es esencial en este caso que todos los datos almacenados se puedan recuperar selectivamente y sin solapamiento de la información. Se analizaron los eventuales entrecruzamientos (solapamientos) e identificando los parámetros que controlan este proceso. Este estudio fue el punto de partida para el almacenamiento de imágenes a color. Otra propuesta consistió en el empleo de una versión modificada del correlador de transformada conjunta que emplea un arreglo de múltiples aberturas. Esta propuesta unida al almacenamiento múltiple, posibilitó tener diferentes niveles de acceso a la información codificada.

Palabras Claves: encriptación, multiplexado

ABSTRACT

The trasmitted data through electronic systems could be hacked. However, it is possible to implement codification procedures to protect them.The goal of this approach relay in using codes or keys so that without them it is not possible

to recover the information. Optical techniques exhibit a potential in order to develop such systems by using correlation optical approaches. One of the well known encryption methods is based on the use of double random phase masks, one of them located in the input plane and the second in the Fourier plane. Also, other encryption arrangements have been developed by using JTC correlation architecture as well as digital holography thechniques. Encryption implemented through correlation techniques implies analogical format in holographic memories stored in photorefractive crystals an also digital techniques. Photorefractive media do not require any processing to read-out the stored information allowing multiple holographic storage (modifiying the registering angle, different polarization states, different multiple aperture pupil arrangements, etc). Optical encryption arrangements based on both 4f and JTC correlation where investigated. A significant advantage of JTC correlators is that it does not require computing a new filtering function each time the reference input changes and on the other hand it does not require strict alignement. It should be highlighted that presently the most of the multiple encryption techniques are based on 4f convergent correlator. However, in the JTC architecture has not been profited the high storage capacity of photorefractive volume registering media.
In this contribution, multiple encryption techniques by employing the mentioned architectures are investigated. In particular, the possibility of multiple data storing based on wavelength changes in a JTC architecture is proposed. It is very important in this case that the stored data can be recovered selectively and without cross-talk. Possible cross-talks were analyzed by identifying those parameters that govern the process. This study was the starting point to color image storing technique. Another proposal consists in the use of a modified version of a JTC wich employs a multiple aperture arrangement. This proposal combined with the multiple storage approach enabled to have different accessibility levels to the codified data.

Keywords: multiplexing, encryption.

1. INTRODUCCIÓN

La encriptación es la transformación de datos de forma que sea imposible, leerlos sin el adecuado conocimiento de la clave mediante la cual se codificó dicha información. En cambio, desencriptación es la transformación del dato encriptado de nuevo a su forma original. Los sistemas de encriptación tiene como objetivo codificar la información de manera que sea difícil decodificarla si no se conoce la clave pero fácil si se la conoce.

Las técnicas ópticas evidencian un gran potencial para el desarrollo de sistemas de encriptación, mediante la correlación óptica. Es de destacar que la mayoría de las técnicas ópticas de almacenamiento de datos encriptados se basan en el uso de correladores convergentes tipo 4*f* [1], sin embargo la arquitectura del JTC ha sido exitosamernte utilizada en estos dispositivos [2, 3]. En la técnica de arquitectura 4f, una onda plana ilumina el conjunto objeto a ser encriptado-máscara de fase y una lente realiza la transformada de Fourier, en cuyo plano se ubica una segunda máscara aleatoria de fase ó mascara llave. Luego una segunda lente realiza la transformada de Fourier, resultando la información codificada. De esta forma la imagen de entrada queda codificada en una distribución estacionaria de ruido blanco. El método basado en la arquitectura JTC consiste en iluminar con una onda plana el conjunto máscara de fase-objeto a ser codificado y otra máscara de fase aleatoria que es la llave codificadora. La transformada de Fourier de esta entrada es almacenada en el medio fotosensible de registro.

La encriptación de la información mediante técnicas de correlación es posible implementarla: (a) en forma analógica, en memorias holográficas almacenadas en cristales fotorrefractivos y (b) mediante técnicas digitales. La encriptación mediante tecnicas ópticas permite almacenar y recuperar los datos en paralelo y a una gran velocidad favoreciendo así el desarrollo de dispositivos que trabajen en tiempo real. Otra de las las ventajas que ofrecen las técnicas ópticas reside en las múltiples formas de codificar la información de manera segura: en fase, en polarización [4], en longitud de onda [5], etc. Justamente estos parámetros de codificación también pueden ser aprovechados para el almacenamiento de múltiples datos encriptado [6- 8].

Anteriormente mencionamos que las técnicas de codificación pueden implementarse empleando como medio de almacenamiento cristales fotorrefractivos. Estos medios tienen la habilidad de registrar hologramas en términos de redes dinámicas de índice de refracción. Las memorias holográficas que usan materiales fotorrefractivos son adecuadas para aplicaciones que involucran la encriptación-desencriptación de datos debido a: su alta capacidad de almacenamiento [9]; su alta velocidad de acceso a la información, no requerir procesamiento previo para leer la información en ellos almacenada recuperar la información almacenada en paralelo y la posibilidad de borrar - reescribir la información.

Si se desea implementar dispositivos experimentales de encriptación-desencriptación se pone en evidencia el papel fundamental que cumplen los materiales fotorrefractivos. Una característica distintiva de los materiales

fotorrefractivos la constituye la habilidad de generar un frente de onda conjugado. En Ref. [10], por primera vez en una arquitectura 4f, la desencriptación es realizada a través de la generación del conjugado de la imagen encriptada a través de la conjugación de fase óptica. En este caso, la imagen codificada en fase se recuperará mediante el uso de la misma máscara de fase aleatoria empleada en la etapa de codificación, eliminando la necesidad de emplear una clave conjugada en fase.

Por otra parte, debemos destacar que los cristales fotorrefractivos en la etapa de reconstrucción ó desencriptación exhiben características de selectividad angular, permitiendo asi el almacenamiento de múltiples imágenes. Existen variadas formas de impementar el almacenamiento múltiple, por ejemplo en Ref. [11] se almacenaron múltiples datos encriptada variando el ángulo entre los haces de registro. Aprovechando la alta capacidad de almacenamiento de los medios fotorrefractivos y empleando alguno de los múltiples parámetros ópticos que pueden ser aprovechados para codificar información de manera segura, en nuestra contribución se presentarán técnicas para encriptar múltiples datos. Por ejemplo, en la arquitectura 4*f* se implementó la técnica de multiplexado por corrimiento de la máscara de fase [6], mediante el cambio en el estado de polarización [4] y mediante el uso de un arreglo de múltiples aberturas que cambian entre exposiciones [7, 8]. También, es posible el almacenamiento múltiple empleando la arquitectura de correlador JTC y empleando cristales fototorrefractivos tipo BSO-BTO como medio de registro. En este caso, mediante el cambio de la longitud de onda [12, 13], la rotación del arreglo de aberturas del plano de entrada del JTC ó bien el empleo de multiples aberturas en el plano de entrada del JTC que se modifican entre exposiciones [14] se implementaron técnicas de codificación de múltiples datos. En todas las técnicas mencionadas, es fundamental que todos los datos pueden ser recuperados independientemente sin solapamiento de la información.

2. MULTIPLEXADO DE DATOS ENCRIPTADOS

En la Figura 1 se presentan los esquemas experimentales empleados para el almacenamiento de multiples datos de entrada. Los esquemas de la Figura 1 a) y 1 b) estan basados en la arquitectura 4f y JTC, respectivamente.

2.1 Arquitectura tipo 4f

En el arreglo experimental de la Figura 1 a), la imagen es encriptada usando una doble máscara de fase aleatoria. La primera máscara de fase es localizada en el plano de entrada junto con el objeto a ser encriptado. Una segunda máscara de fase se ubica en el plano de Fourier de la entrada. Luego, una segunda lente realiza la transformada de Fourier, resultando la información codificada. De esta forma el objeto de entrada queda codificado en una distribución estacionaria de ruido blanco. En nuestro caso, se empleó como máscara aleatoria de fase pura un difusor. La implementación de este esquema requiere, como se observa en Figura 1 a), de la generación de un haz de fase conjugado. El mezclado de cuatro ondas es un método conveniente para la generación de un haz de fase conjugada. Es justamente la generación de este haz lo que permite la decodificación de la información de entrada sin la necesidad de emplear el conjugado de la máscara llave. Si la llave ó máscara de fase no es correcta, la imagen original no será reconstruída. Asimismo, si alguno de los parámetros ópticos utilizados para codificar los datos de entrada son modificados, aún empleando en la etapa de desencriptación la misma máscara de fase utilizada en la etapa de encriptacion, el objeto de entrada no podrá ser reconstruido. En resumen, es suficiente modificar alguno de los parámetros ópticos de registro para evitar la recuperación de la información. Entre los múltiples parámetros cuya modificación altera la correcta desencriptación, podemos mencionar la modificación de la longitud de onda, el estado de polarización [4], etc. En nuestro caso, estas ideas fueron aprovechadas para realizar almacenamiento múltiple mediante el cambio entre exposiciones de los parámetros mencionados.

Detallaremos a continuación diferentes técnicas de multiplexado basadas en el empleo de la arquitectura 4f. En la primera propuesta los diversos objetos de entrada fueron codificados modificando entre exposiciones la posición de la máscara de fase [6]. Para corroborar lo propuesto se empleó como medio de registro un cristal fotorrefractivo tipo silenita BSO cuyas dimensiones son 10 x 10 x 10 mm. En la etapa de desencriptación cada uno de los datos de entrada será recuperado con máxima fidelidad únicamente cuando la posicion de la máscara llave coincide exactamente con la que tenía en la etapa de encriptación. En las imágenes desencriptadas de la Figura 2, puede observarse que no hay solapamiento entre los datos correspondiente a cada uno de los registros.

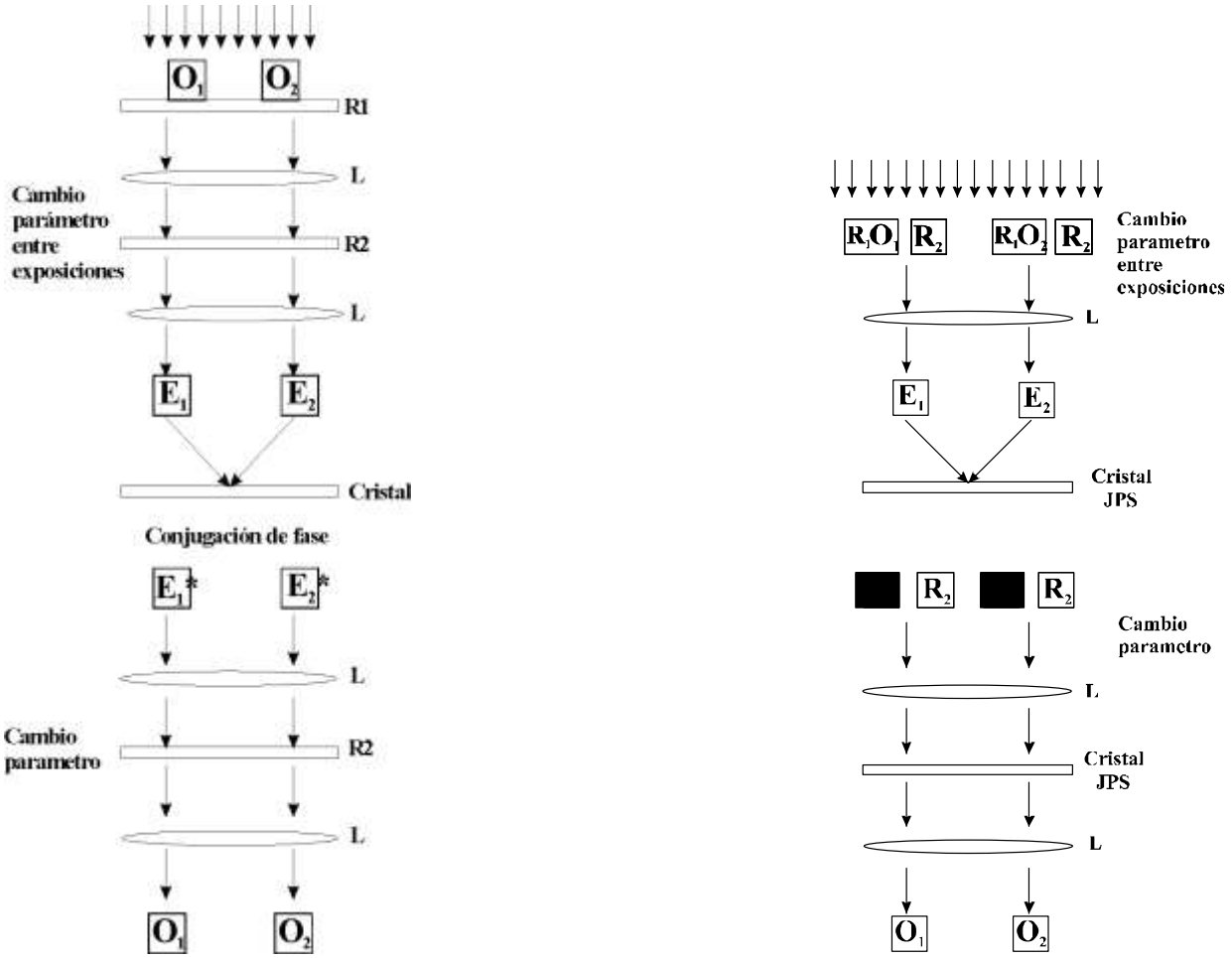
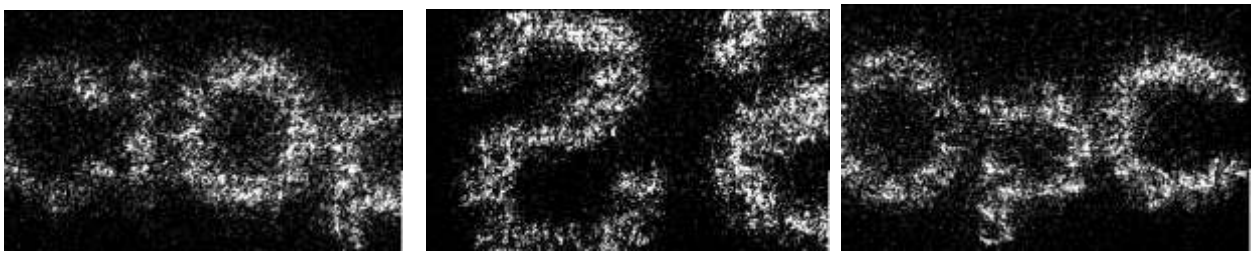


Figura 1: Esquema de los dispositivos de multiplexado empleando las arquitecturas (a) 4f (b) JTC (O_1, O_2: objetos a ser encriptados; R_1, R_2: máscaras aleatorias de fase pura (difusores); L: lentes; E_1, E_2: información encriptada; E_1* y E_2*: información encriptada conjugada en fase



Figuras 2: Multiples imágenes encriptadas empleando la aruitectura 4f. Se muestran las imágenes reconstruidas cuando se coloca la mascara de fase en la posición correcta.

Otra de las técnicas de multiplexado de imágenes encriptadas está basada en el uso de diferentes arreglos de aberturas en la segunda lente de la arquitectura 4*f* [7]. Aquí las imágenes son codificadas cambiando el arreglo de pupilas entre exposiciones. En este caso, además de las características propias de la máscara de fase, se incorpora al sistema como nuevo grado de seguridad del sistema, la información del arreglo de aberturas. En particular, si la máscara de fase es interceptada, el sistema no podrá ser violado sin el correcto conocimiento de los parámetros

geométricos de la pupila del sistema óptico.

Por otra parte, se investigó el empleo del estado de polarización como nuevo parámetro en el dispositivo de encriptación con arquitectura 4*f*. Cuando se modifica el estado de polarización en la etapa de decodificación, se induce una modificación del patrón encriptado que impide que el objeto de entrada sea reconstruido. Esto fue aprovechado para la encriptación de múltiple datos [4].

En todos los casos, una característica novedosa y singular de las propuestas antes mencionadas reside en la presencia simultánea en el frente de onda conjugado de todas las señales encriptadas. Entonces, las pupilas, la segunda máscara de fase y el estado de polarización actúan como elementos selectores de la imagen a desencriptar.

Otra técnica para incrementar la seguridad en la transmisión de datos se basó en un multiplexado tipo "rompecabezas". El principio básico del método se basa en la descomposición de una imagen de entrada, de igual manera que las piezas de un rompecabezas. Cada conjunto de partes de la imagen descompuesta es encriptada en canales separados pero en el mismo medio de almacenamiento. El uso de canales separados implica modificar alguno de los parámetros del sistema óptico (posición de la máscara de fase, longitud de onda, estado de polarización, etc). Para recuperar la información completa es necesario desencriptar adecuadamente y componer todos los diferentes canales [15].

Por otra parte, hemos demostrado que el concepto de multiplexado puede ser empleado según otro enfoque, con el fin de aumentar el grado de seguridad en los sistemas de protección de la información. El objetivo se centró en confundir ó engañar a quienes pretendan acceder a la información sin autorización y asegurarse que sólo los usuarios válidos la obtengan. En este caso, el multiplexado se empleó para generar una jerarquía de accesibilidad para acceder a la información verdadera [16- 18].

Una de las propuestas se baso en generar "encodegramas" que combinan una doble encriptación en una sola estructura de forma tal de incrementar el grado de seguridad en la transmisión de la información [18]. El arreglo experimental consistió en encriptar un primer objeto en un procesador convencional de doble máscara de fase. Un segundo objeto que es la clave realmente a proteger se encriptó empleando el mismo dispositivo anterior, reemplazando la llave de encriptación por la información de fase de la imagen encriptada del primer objeto. Finalmente, se multiplexaron las dos imágenes encriptada. Para recuperar la clave, el usuario autorizado recibirá las máscaras de fase y la información multiplexada. A partir de la segunda máscara de fase y la información multiplexada, se recuperará el primer objeto y a partir de la información de amplitud de él y mediante el empleo de ambas máscaras, se recuperará la imagen encriptada de aquel. Finalmente, con la información de fase del primer objeto y el multiplexado se accederá al verdadero objeto.

2.2 Arquitectura tipo JTC

La encriptación también es posible realizarla empleando la arquitectura JTC. La arquitectura convencional de estos procesadores consiste en localizar en un mismo plano dos señales ó ventanas: una sirve de referencia y la otra es la información ú objeto a procesar. En este caso, la transformada de Fourier óptica genera la correlación de la información contenida en ese plano de entrada. Esta información puede ser procesada con un filtro y posteriormente sujeta a otra transformación de Fourier óptica que proporcione la señal de correlación buscada.

Se estudiaron técnicas de encriptación múltiple en dispositivos de encriptación que empleen la arquitectura antes detallada [12-14]. Una de las ventanas del dispositivo contiene el objeto a ser encriptado y la máscara de fase aleatoria mientras la segunda ventana contiene otra máscara de fase. La transformada de Fourier de esta entrada se registra en el medio fotosensible. Esta transformada conjunta contiene la información del objeto de entrada codificada como ruido blanco. En la etapa de desencriptación, un cambio de alguno de los parametros ópticos de sistema trae como consecuencia evitar la recuperación del objeto de entrada. Esta idea es aprovechada para la encriptación de múltiples objetos sin solapamiento entre ellos. Es esencial en nuestra propuesta que todos los datos almacenados en un único medio de registro se puedan recuperar selectivamente y sin solapamiento. Se estudió la posibilidad de almacenar múltiples datos a partir del cambio de la longitud de onda de registro. Luego utilizando el mismo concepto de base, se propuso una técnica de almacenamiento de imágenes a color [13]. En el arreglo propuesto, la imagen a color a ser encriptada es separada en los tres canales de color (rojo, verde y azul). Cada canal de color es encriptado empleando la misma llave de codificación pero diferente longitud de onda. Recordemos que el espectro de potencia conjunta depende de la longitud de onda de la fuente de iluminación. Luego secuencialemente cada color es almacenado en el mismo medio y recuperado independientemente sin

solapamiento entre ellos.

Otra alternativa para multiplexar datos de entrada fue implementada a partir de la rotación entre exposiciones del arreglo de doble aberturas de la arquitectura JTC. Si en la etapa de desencriptación la máscara llave es rotada respecto al eje óptico del sistema, ya no se reconstruirá fidedignamente el objeto, ya que la transformada de Fourier que incide sobre el espectro de potencia no coincide con la de la llave. Esta idea será aprovechada para almacenar distintos objetos rotando deliberadamente entre exposiciones el arreglo de aberturas. Para verificar la propuesta se registro el espectro de potencia conjunto en un cristal fotorrefractivo tipo silenita BTO. Para la etapa de encriptación y desencriptación se empleó un láser de He-Ne de 10 mW, dado la buena sensibilidad de los cristales BTO en este rango espectral. Como es conocido, la distribución luminosa recibida sobre el cristal via el efecto fotorrefractivo queda almacenada como variación del índice de refracción. Dada las frecuencias espaciales involucradas en esta propuesta el mecanismo de transporte de cargas dominante es el de arrastre, motivo por el cual en nuestras experiencia se aplicó un campo eléctrico externo que favorece la generación de las redes de índice respectivas. En la Figura 3 se presentan las imágenes desencriptadas, obtenidas empleando en la etapa de desencriptacion la máscara en las mismas orientaciones que en la etapa de registro. A partir de los resultados es evidente que posible recuperar acada dato sin que exista solapamiento entre ellos.

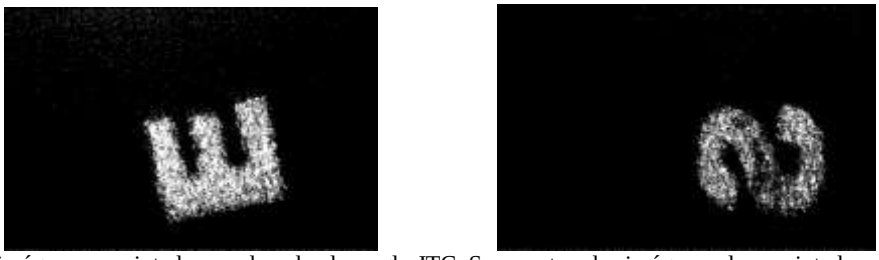


Figura 3. Multiples imágenes encriptadas empleando el arreglo JTC. Se muestran las imágenes desencriptadas cuando se emplea la orientación correcta de la mascara de fase en la etapa de decodifiaccion

3. CONCLUSIONES

En este trabajo se presentaron distintas técnicas de almacenamiento multiple de datos encriptados basadas en arquitecturas JTC y 4f. Para la implementación analógica de las técnicas propuestas se emplearon cristales fotorrefractivos para almacenar la información codificada. El empleo de cristales fotorrefractivos une las ventajas propias del procesamiento óptico a las introducidas por estos medios. Entre las características salientes se debe destacar la gran capacidad de almacenamiento de datos.

AGRADECIMIENTOS

Este trabajo fue realizado con el apoyo de los siguientes subsidios: CONICET No. 5995, ANCYT PICT 1167, Facultad Ingeniería, Universidad Nacional de La Plata (Argentina).

REFERENCIAS

1. P. Refregier, B. Javidi, “Optical image encryption using input and Fourier plane random phase encoding”, *Opt. Lett*. 20, pp. 767-769, 1995.
2. T. Nomura, B. Javidi, “Optical encryption system with a binary key code”, *Appl. Opt*. 39, pp. 4783- 4787, 2000.
3. T. Nomura, S. Mikan, Y. Morimoto, B. Javidi, “Secure optical data storage with random phase key codes by use of a configuration of a joint transform correlator”, *Appl. Opt*. 42, pp. 1508-1514, 2003.
4. J. F. Barrera, R. Henao, M. Tebaldi, N. Bolognini, R. Torroba “Multiplexing encrypted data by using polarized light” *Opt. Commun.* 260, pp. 109-112 (2006).
5. G. H. Situ, J. J. Zhang, “Multiple-image encryption by wavelength multiplexing”, *Opt. Lett.* 30, p 1306, 2005.
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, pp. 532-536, 2006.

7. J. F. Barrera, R. Henao, M. Tebaldi, N. Bolognini, R. Torroba, “Multiple image encryption using an aperture-modulated optical system”, *Opt. Commun*. 261, pp. 29-33, 2006.
8. J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, N. Bolognini, “Code retrieval via undercover Multiplexing”, *Optik* 119, pp. 139-142, 2008.
9. F. H. Mok, "Angle-multiplexed storage of 5000 holograms in lithium niobate," *Opt. Lett.* 18, p 915, 1993.
10. G. Unnikrishnan, J. Joseph, K. Singh, “Optical encryption system that uses phase conjugation in a photorefractive crystal”, *Appl. Opt*. 37, pp. 8181–8186, 1998.
11. O. Matoba, B. Javidi, "Encrypted Optical Storage with Angular Multiplexing,"*Appl. Opt*. 38, 7288-7293, 1999.
12. D. Amaya, M. Tebaldi, R. Torroba, N. Bolognini, “Wavelength multiplexing encryption using JTC architecture”, enviado para su publicación
13. 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 (5pp), 2008.
14. D. Amaya, M. Tebaldi, R. Torroba, N. Bolognini, “Multichanneled encryption via a modified Joint Transform Correlator architecture” *Appl. Opt*., en prensa
15. D. Amaya, M. Tebaldi, R. Torroba, N. Bolognini, “Multichanneled puzzle-like encryption” *Optics Communications*, 281 No 13, pp. 3434-3439, 2008.
16. J. F. Barrera and R. Henao, M. Tebaldi, R. Torroba, N. Bolognini “Digital encryption with undercover multiplexing by scaling the encoding mask”, *Optik*, en prensa.
17. J. F. Barrera, M. Tebaldi, R. Torroba, N. Bolognini, “Multiplexing encryption technique by combining random amplitude and phase masks”, *Optik*, en prensa.
18. J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, N. Bolognini, “Multiple-encoding retrieval for optical security”, *Optics Communications*, 276, pp. 231–236, 2007.