ISSN: 1692-7257 - Volumen 1 - Número 19 - Año 2012

Revista Colombiana de Tecnologías de Avanzada

Recibido: 17 de febrero de 2011
Aceptado: 29 de marzo de 2011

OPTICAL CRYPTOSYSTEM: AN IMPLEMENTATION USING PHOTOREFRACTIVE HOLOGRAPHY AND LCR2500 MODULATOR

CRIPTOSISTEMA ÓPTICO: UNA IMPLEMENTACIÓN UTILIZANDO HOLOGRAFÍA FOTORREFRACTIVA Y UN MODULADOR LCR2500

PhD. Jorge Enrique Rueda, Fís. Ana Ludia Romero

Universidad de Pamplona. Grupo Óptica Moderna, Departamento de Física
Ciudadela Universitaria. Pamplona, Norte de Santander, Colombia.
Tel.: 57-7-5685303, Fax: 57-7-5685303, Ext. 144
E-mail: jorgeenriquerueda@gmail.com

Abstract: This paper presents the results of the implementation of optical encryption-decryption processor in real-time, using diffraction in free propagation as mechanism of correlation and convolution operations, and the use of a liquid crystal modulator (LCR2500) and a photorefractive crystal ($Bi_{12}SiO_{20}$). We used the advantages of four-wave mixing in the photerefractive crystal, firstly to store encrypted data holographically, and also phase conjugation was used to decrypt the information in parallel to the encryption process.

Keywords: Cryptography, Holography, Wave Mixing, Photorefractive Crystals, Twisted Nematic Crystals.

Resumen: En este trabajo se presentan los resultados de la implementación de un procesador de encriptación-descencriptación óptica en tiempo real, utilizando difracción en propagación libre como mecanismo de operaciones de correlación y convolución, y el uso de un modulador de cristal líquido (LCR2500) y un cristal fotorrefractivo ($Bi_{12}SiO_{20}$). Utilizamos las ventajas de la mezcla de cuatro ondas en el cristal fotorrefractivo, por un lado, para almacenar holográficamente la información encriptada, y de otra parte se aprovecha la conjugación de fase para descencriptar la información en paralelo al proceso de encriptación.

Palabras clave: Criptografía, Holografía, Mezcla de Ondas, Cristales Fotorrefractivos, Cristales Twisted Nematic.

1. INTRODUCCIÓN

La criptografía es una técnica de ocultamiento de información. Diferentes técnicas se han propuesto para este propósito, que van desde el uso de algoritmia matemática, hasta las de última generación mediante el uso de tecnología óptica, que es también la base del trabajo que presentamos. En términos generales, la implementación óptica de los criptosistemas propuestos hasta hoy tienen como nucleo fundamental, o bien la arquitectura del Correlador óptico Vander Lugt (VLC) (Vander Lugt, 1964) o el Correlador óptico de Transformación Conjunta (Joint Transform Correlator -JTC-) (Goodman, 1996); en los dos casos se requiere el uso de lentes convergentes para calcular, ópticamente, las transformadas de Fourier necesarias. Así, Francon (Francon, 1975) propone un sistema óptico para encriptar información usando llaves bidimensionales de fase aleatoria, siendo esta llave una placa difusora. Los trabajos de (Refregier, 1995), (Javidi, 1996), utilizan el

concepto de la transformada de Fourier mediante un procesador 4f y proponen el uso de doble llave aleatoria de fase, una multiplicando la entrado y la otra en el plano de Frecuencias del procesador 4f; también (Javidi, 1996) hace uso de la holografía fotorrefractiva. En 1999 Matoba y Javidi (Matoba, 1999) (Matoba, 1999a), proponen el almacenamiento de imágenes encriptadas usando un cristal de $LiNbO_3$. En 2000 Tan et al. (Tan, 2000), presentan la implementación de un dispositivo experimental de encriptación llamado totalmente en fase. En este caso, múltiples imágenes de fase son almacenadas en el cristal LiNbO3 utilizando multiplexado angular. Tajahuerce et al (Tajahuerce, 2000), proponen utilizar un sistema óptico-digital basado en un interferómetro MachZender y la técnica de holografía digital de corrimiento de fase para encriptar y digitalizar la información original. (Unnikrishnan, 2000) propone el uso de doble llave y la transformada fraccinaría de Fourier. En 2003 Hennelly et al. (Hennelly, 2003), demostraron un nuevo método basado en cambios aleatorios de secciones diferentes de la imagen original en el dominio fraccionario de Fourier. Nishchal et al. (Nishchal, 2003), proponen un sistema de encriptación de solo fase, donde la encriptación de la imagen es un holograma grabado en un cristal fotorrefractivo de titanato. Matoba y Javidi (Matoba, 2004), utilizan un sistema óptico-digital que almacena la información encriptada y la llave de forma holográfica usando una cámara CCD. Chang-Mok Shin et al. (Shin, 2005), presentaron un criptosistema digital basado en el uso del operador lógico XOR, donde las entradas son la imagen a encriptar y una imagen randómica binaria; así, el resultado es una imagen de solo fase. Li-Chien Lin et al. (Lin, 2006), propusieron un criptosistema de transformación conjunta, y proponen un algoritmo digital para calcular la llave de fase óptima, que permite aumentar la relación Señal/Ruido en la imagen descencriptada. Mela et al. (Mela, 2006), presentan un algoritmo de corrimiento de fase donde solo es necesario adquirir dos interferogramas. Chen et al. (Chen, 2008), proponen un criptosistema tipo JTC en el que utilizan una cámara CCD en el proceso de encriptación y en la descencriptación un SLM.

En este artículo presentamos los resultados de la implementación de un procesador de encriptación-descencriptación de imágenes en tiempo real; utilizamos el fenómeno de descomposición espectral mediante difracción de la luz sin el uso de lentes. Incluimos en el procesador un modulador de cristal líquido -LCR2500- para generar llaves de encriptación de solo fase. De otra parte, este dispositivo constituye una interfase híbrida entre un ordenador digital y un procesador holográfico fotorrefactivo. El procesador fotorrefractivo (Yeh, 1993) es un mezclador de cuatro ondas ópticas, mediante el cual son posibles dos operaciónes fundamentales para el procesamiento en tiempo real, la primera es el registro holográfico dinámico de la información encriptada, y la segunda operación es la conjugación de fase para descencriptar la información; así, se logra en paralelo, la encriptación y descencriptación de la imagen de entrada.

2. DISCUSIÓN DEL PROCESADOR IMPLEMENTADO

Un esquema del Procesador de Encriptación-Descencriptación en propagación Libre (*PEDL)* implementado se muestra en la Fig.1. La fuente óptica es un láser de Argón, sintonizado en la longitud de onda 514nm/50mW. El cristal fotorrefractivo es un BSO de 6mm de espesor y cara principal de área 10x10mm^2, de talla Huignard, trabajado en configuración holográfica transversal; se ajustó un ángulo de registro de 57.78°. Obsérvese que cuatro ondas se mezclan en el cristal BSO, las ondas U, Ur, la onda reflejada del espejo E4 (onda de lectura) y la onda conjugada de U que se genera por auto-difracción (acoplamiento en fase y amplitud entre los haces que entran al medio fotorrefractivo).

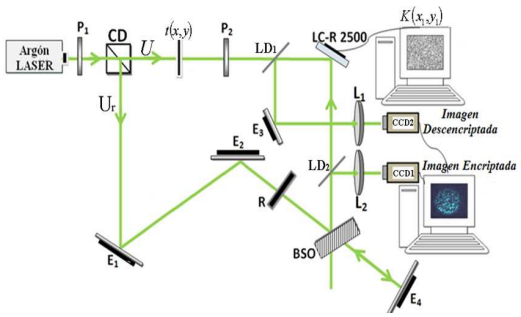


Fig. 1. Esquema del PEDL implementado. R: retardador de media onda; P1,2: polarizadores lineales; CD: cubo divisor de haz; LD: láminas divisoras de haz. BSO: cristal fotorrefractivo; E1,2,3,4: espejos; CCD1,2: cámaras digitales; t(x,y):función de tramitancia de la imagen a encriptar.

Entre el plano objeto y plano del cristal BSO se ajustó una distancia de 120cm. El dispositivo LCR2500 es un modulador de luz de cristal líquido reflectivo Twisted Nematic 45º Holoeye de resolución 1024(H) x 768(V) *pixels*; en este

dispositivo se registran llaves de encriptación de solo fase y distribución aleatoria de la misma; para la adecuada generación de este tipo de llaves es necesario conocer la función de modulación de fase del dispositivo LCR2500; nosotros determinamos la función de modulación, de este dispositivo para seis longitudes de onda, entre ellas la línea 514nm (Rueda, 2010). El procesador tiene dos salidas, la cámara CCD1 registra la salida Plano de encriptación y la CCD2 registra la salida Plano de descencriptación.

La función $t(x,y)$ es una diapositiva (plano de la imagen a encriptar) que despolariza el haz de entrada, razón para utilizar el polarizador P1, mediante el cual podemos ajustar el tipo de modulación; el retardador de media onda R cumple la función de permitir ajustar el contraste máximo de la distribución de intensidad que registra el cristal BSO.

2.1 Modelo físico –matemático del PEDL

El modelo físico-matemático se presenta en términos de la formulación de difracción de Fresnel (Goodman, 1996); así, esta formulación propone la respuesta impulso Ecuación 1, para la propagación en el espacio libre de una onda:

$$h(x,y;z)=\exp(-jk_o z)\cdot\exp\left[\frac{-jk_o(x^2+y^2)}{2z}\right] \qquad (1)$$

Siendo Z la distancia entre el plano de la pupila y el plano de observación; $k_o=\frac{2\pi}{\lambda}$ es el número de onda. Así, si $U(x,y;0)$ es la onda que se difracta en una pupila de tramitancia $t(x,y)$, entonces el campo $U_z(x,y;z)$ es:

$$U_z(x,y;z)=U(x,y;0)*h(x,y;z) \qquad (2)$$

Si U es una onda plana de amplitud la unidad, entonces podemos escribir $U = t(x,y)$; el operador $*$ es de convolución.

2.1.1 Etapa de encriptación

1) Propagación $Z1$ entre el plano objeto $t(x,y)$ (información a encriptar) y el plano de la llave $K(x_1,y_1;z_1)$, entonces:

$$\begin{aligned}U_K(x_1,y_1;z_1)&=[t(x,y)*h_1(x,y;z_1)]\cdot K(x_1,y_1)\\&=\mathrm{T}(x_1,y_1)\cdot K(x_1,y_1)\end{aligned} \qquad (3)$$

2) Propagación $Z2 = Z1$ entre el plano de la llave y el plano de encriptación $(x_2,y_2;z_2=z_1)$, el campo en este plano es:

$$U_E(x_1,y_1;z_2)=U_k*h_2(x_1,y_1;z_1) \qquad (4)$$

Si el campo U_E es tal, que la relación Señal/Ruido tiende a cero, entonces este campo será un ruido blanco, en otras palabras, la imagen de entrada está encriptada. Esta relación depende de las características de la llave, en cuanto al los valores medios de la distribución aleatoria de la fase.

Este campo U_E se registra holográficamente en el cristal fotorrefractivo BSO mediante un mezclado de cuatro ondas; siendo así posible, en la reconstrucción del holograma obtener la onda conjugada U_E^*, que es una onda contra propagante a la onda U_E; la Ecuación 5 es una representación aproximada de esta onda; en esta expresión se observan parámetros que representan el medio de registro holográfico y de la radiación de lectura:

$$U_E^*\approx\frac{\pi d}{\lambda\cos\theta}\delta n\cdot U_{-r} \qquad (5)$$

Donde d es el espesor del cristal BSO, λ la longitud de onda de lectura, θ es el ángulo de Bragg o de lectura, δn es la birrefringencia (holograma) causada por efecto fotorrefractivo. U_{-r} es la onda de lectura que se obtine mediante el espejo $E4$.

2.1.2 Etapa de descencriptación

3) Propagación de U_E* entre el plano de encriptación y el plano de la llave:

$$\begin{aligned}U'_K&=U_E^**h_2=\left[U_K^**h_2^*\right]*h_2\\&=U_K^**\delta(x_1,y_1)=[\mathrm{T}\cdot\mathrm{K}]^*\cdot K\\&=[T]^*=t^**h_1^*\end{aligned} \qquad (6)$$

Para que la llave se elimine es necesario que la llave de descencriptación sea la misma de encriptación, solo así, la información se descencripta.

4) Propagación de U'_K una distancia $Z1$; estamos entonces en el proceso final de descencriptación de la información, esto es:

$$U'(x',y';z_1)=\left[t^**h_1^*\right]*h_1=t^*(x',y') \qquad (7)$$

De otra parte, en paralelo al proceso de registro del holograma de la información encriptada, se genera

también la onda conjugada, que se contra-propaga hacia el modulador LCR2500, dispositivo donde está codificada la llave utilizada para encriptar la imagen del objeto de entrada. Entonces, justo después de la llave, el haz conjugado pierde la información de la llave, es decir que la onda que se refleja del modulador, porta la imagen descencriptada; esta imagen la registra la cámara CCD2.

3. RESULTADOS

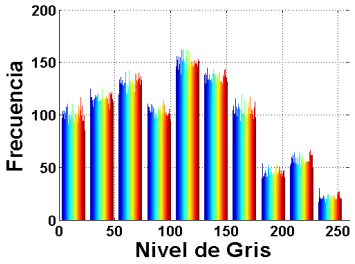
En la Fig.2 se muestran las características y el comportamiento de diez llaves de prueba; para la interpretación de las Fig.2. (b) y (c), las llaves K1, K2, K8 y K10, no encriptaron la imagen de entrada; la Fig.2.(a) es el histograma característico de la distribución de fase de las llaves utilizadas en la validación del criptosistema. Utilizamos dos criterios para caracterizar el comportamiento de las llaves:

1). El nivel de encriptación (%E): se refiere al cálculo del porcentual de similitud entre la imagen encriptada y la imagen sin encriptar, es decir:

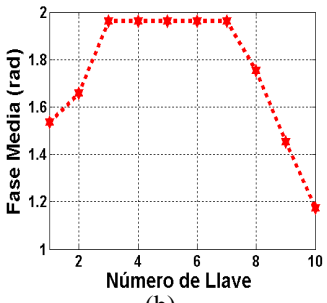
$$\%E = \left| \frac{IE - ISE}{IE} \right| * 100 \qquad (8)$$

Donde *ISE* es la imagen sin encriptar registrada por la *CCD1* (sin la llave) e *IE* la imagen encriptada registrada por la *CCD1*.

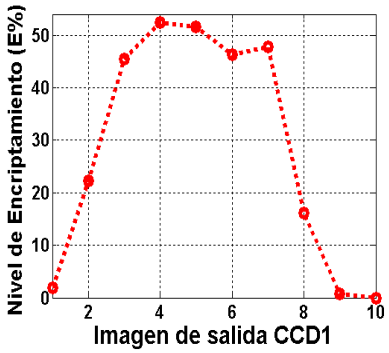
2). Valor medio de fase en la distribución.



(a). Histograma de la distribución de fase de las llaves.



(b).



(c).

Fig. 2. Características de las llaves de encriptación utilizadas.

Este tipo de llave mostró un comportamiento aceptable de encriptación solo para valores de fase media superiores a 1.8 rad. De otra parte, determinamos que el nivel encriptación aceptable debe ser superior al 30%.

La Fig.3 son imágenes de dos de los resultados de prueba del procesador. La relación Señal/Ruido en las imágenes descencriptadas no es la óptima, sin embargo, mediante un tratamiento óptico ó digital se puede aumentar esta relación, eliminando la presencia del ruido óptico, el cual es causado, en buena medida, por los dispositivos que utilizamos.

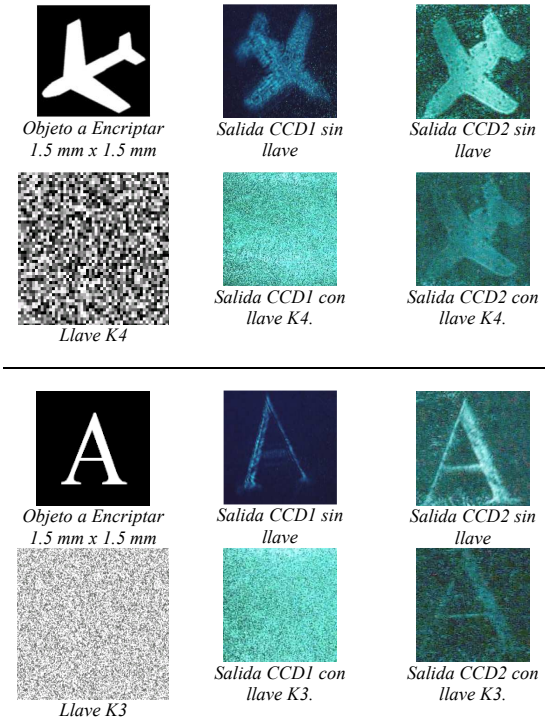


Fig. 3. Pruebas del PEDL

5. CONCLUSIONES

Se construyó un sistema de encriptación-decriptación óptico de imágenes en tiempo real, posible mediante el mezclado de ondas ópticas en un cristal fotorrefractivo de BSO. De otra parte, a diferencia de los criptosistemas ópticos clásicos, nosotros no utilizamos lentes transformadoras de Fourier, así como tampoco utilizamos doble llave de fase.

Se comprobó que la conjugación de fase efectivamente permite el proceso de descencriptación.

Se utilizó un modulador LCR2500 para registrar llaves de encriptación de solo fase. Se establecieron dos criterios para caracterizar las llaves; determinamos que el límite inferior para el criterio nivel de encriptación aceptable es aproximadamente del 30% que corresponde también a un valor medio de la distribución de fase de 1.8 rad; comprobamos que por debajo de estos límites la llave no encripta.

REFERENCIAS

Chen C. L. (2008). Design and implementation of an optical joint transform encryption system using complex-encoded key mask. Opt. Eng. , 47, 068201.

Francon, M. (1975). Information processing using speckle patterns, in Laser speckle and related phenomena. Springer-Verlag, New York .

Goodman J. W. (1996) Introduction to Fourier Optics. New York: McGraw-Hill, 2da Ed.

Hennelly B. (2003) Optical image encryption by random shifting in fractional Fourier domains. Opt. Lett. , 28, 269.

Javidi B. (1996) Experimental demonstration of the random phase encoding technique for image encryption and security verification. Opt. Eng. , 2506-2512.

Li-Chien L. (2006) Optimal key mask design for optical encryption based on joint transform correlator architecture. Department of Communications Engineering, Feng Chia University, Taichung, Taiwan.

Matoba O. (1999) Encrypted optical storage with angular multiplexing. Appl. Opt, 38, 7288.

Matoba O. (1999a) Encrypted optical storage with wavelength-key and random phase codes. Appl. Opt. , 38, 6785.

Matoba O. (2004) Secure three-dimensional data transmission and display. Appl. Opt. , 43, 2285–2291.

Mela C. (2006) Optical encryption using phase-shifting interferometry in a joint transform correlator. Opt. Lett. , 31, 2562-2564.

Nishchal N. (2003) Optical phase encryption by phase contrast using electrically addressed spatial light modulator. Opt. Eng. , 42, 1583.

Nomura T. (2000) Optical encryption using a joint transform correlator arquitecture. Opt. Eng., 39, 2031–2035.

Refregier P. (1995) Optical image encryption based on input plane Fourier plane random encoding. Opt. Lett., Vol. 20 , 767.

Refregier P. (1995) Optical image encryption based on input plane and Fourier plane random encoding. Optics Letters , 767-769 .

Rueda J. E., Romero A. L. and Guerra L. A (2010) Characterization of Reflective TN-LCD, Tuned in Phase-Only Modulation and to Six Wavelengths Photonics. Letters Of Poland, Vol. 2, No. 4, 174-176.

Shin C. (2005) Image encryption using modified exclusive-or rules and phase-wrapping technique. School of Electrical Engineering and Computer Science, Kyungpook National University, 1370 Sangyuk-Dong, Buk-Gu, Daegu 702-701.

Tajahuerce E. (2000) Optoelectronic information encryption with phase-shifting interferometry. Appl. Opt. , 39, 2313–2320.

Tan X. (2000) Secure optical storage that uses fully phase encryption. Appl. Opt. , 39, 6689.

Tan X. (2000) Secure optical storage that uses fully phase encryption. Appl. Opt. , 39, 6689.

Unnikrishnan G.. (2000) Optical encryption by double-random phase encoding in the fractional Fourier domain. Opt. Lett. , 25, 887.

Vander Lugt A. (1964) Signal detection by complex spatial filtering. IEEE transactions on Information , 10, 139.

Yeh P. (1993) Introduction to photorefractive nonlinear optics. New York : John Wiley & Sons.