CRIPTOGRAFÍA ÓPTICA MEDIANTE DIFRACCIÓN DE FRESNEL Y CONJUGACIÓN DE FASE

OPTICAL CRYPTOGRAPHY USING FRESNEL DIFFRACTION AND PHASE CONJUGATION

JORGE ENRIQUE RUEDA-PARADA

PhD Física, Grupo Óptica Moderna, Universidad de Pamplona, Colombia, e-mail: jorgeenriquerueda@gmail.com

ANA LUDIA ROMERO-BECERRA

MSc Física, Grupo Óptica Moderna, Universidad de Pamplona, Colombia, e-mail: ludiaromero@hotmail.com

Recibido para revisar Marzo 4 de 2013, aceptado Julio 29 de 2013, versión final Agosto 2 de 2013

RESUMEN: Se implementó un procesador óptico para cifrar imágenes usando difracción de Fresnel en el espacio libre. Utilizamos mezcla de cuatro ondas para grabar la imagen cifrada en un cristal fotorrefractivo BSO y decodificamos la misma por conjugación de fase. En cada imagen cifrada sólo utilizamos una llave. Nosotros caracterizamos el procesador en términos de los valores de fase de la llave, y determinamos el límite inferior del valor medio de la fase en el cual se obtuvo un cifrado total. El procesador opera en tiempo real.

PALABRAS CLAVE: Criptografía, Mezclado de Ondas, Fotorrefractivos, Holografía, Difracción.

ABSTRACT: Optical processor was implemented to encrypt images using Fresnel diffraction in free space. We use four-wave mixing to record encrypted image into a photorefractive crystal BSO and decode it by phase conjugation. In each image encrypted only use a key. We characterize the processor in terms of the phase values of the key, and determine the lower limit of the average value of the phase in which we obtained a full encryption. The processor operates in real time.

KEYWORDS: Cryptography, Wave Mixing, Photorefractive, Holography, Diffraction.

1. INTRODUCCIÓN

La criptografía es una técnica de cifrado de información. En cuanto a esquemas de cifrado de imágenes, las diferentes contribuciones reportan arreglos puramente digitales, solo ópticos, o híbridos en los cuales se combinan las dos anteriores [3-22]. En términos generales, la implementación óptica de procesadores de cifrado se fundamentan en la arquitectura del Correlador Vander Lugt (VLC)[1] o del Correlador de Transformación Conjunta (Joint Transform Correlator -JTC-)[2]. En este sentido, no encontramos reportes de implementación óptica donde no se utilicen lentes para la obtención óptica de las transformadas de Fresnel que se requieren en el proceso de cifrar-descifrar [20]. Encontramos dos trabajos que utilizan el dominio de Fresenel sin el uso de lentes, sin embargo estas propuestas son modelos teóricos sustentados con simulaciones numéricas [21,22].

Nosotros implementamos un procesador óptico de cifrado en el dominio de difracción de Fresnel, con la particularidad de que no utilizamos lentes en los procesos cifrar-descifrar; además utilizamos las ventajas de la mezcla de cuatro ondas en un material fotorrefractivo [23,24]. Esta mezcla de ondas permite la conjugación de fase, operación necesaría para decodificar la imagen cifrada. La conjugación de fase también es responsable de que el procesador funcione en tiempo real. Es de anotar, que existen reportes donde se utiliza la conjugación de fase en medios fotorrefractivos [4,9], pero sin la particularidad de nuestra implementación. De otra parte, incluimos en el procesador un modulador de luz de cristal líquido –TN-LCR2500- que utilizamos para sintetizar las llaves de cifrado, dándo así mayor robustez al procesador.

2. PROCESADOR IMPLEMENTADO

Un esquema del Procesador de Cifrar-Descifrar en el dominio de Fresnel (PEF) se muestra en la Figura 1. Utilizamos una fuente láser de Argón, sintonizado en la longitud de onda 514nm/45mW, y un cristal BSO de 6mm de espesor, de cara principal $(\bar{1}10)$ de

10x10mm². Se utilizó la configuración holográfica transversal [23,24]. Ajustamos un ángulo interhaz 2θ≈90° para generar una red de frecuencia espacial de ≈7044 líneas/mm, garantizando así que el cristal BSO trabajara en el régimen de portadores de carga por difusión.

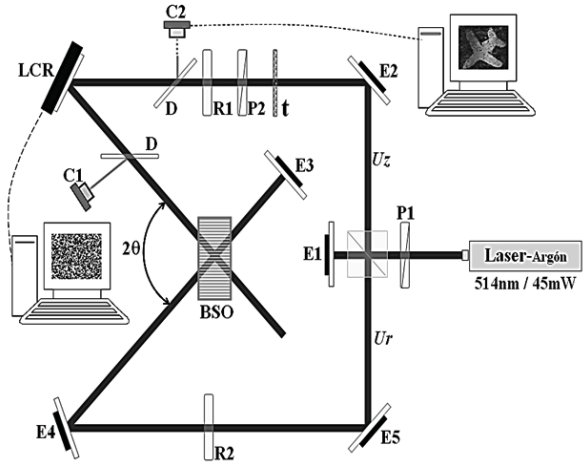


Figura 1. Esquema del PEF implementado. R: retardadores de media onda; P: polarizadores lineales; D: láminas divisoras de haz. BSO: cristal fotorrefractivo; E: espejos; C: cámaras CCD; **t**: plano objeto; LCR: modulador de cristal líquido TN-LCR2500; *Ur*: onda de referencia; *Uz*: onda objeto.

Cuatro ondas se mezclan en el cristal BSO: la onda objeto *Uz*, la onda de referencia *Ur*, la onda plana reflejada del espejo E3 (onda de lectura *UR*) y la onda conjugada de *Uz*. La onda de lectura produce la onda conjugada U_z^*; esta onda es contrapropagante a la onda *Uz*. Entre el plano objeto **t** y el 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, marca Holoeye, de resolución 1024(H)× 768(V) *pixels*; la función de distribución de la llave se calcula computacionalmente y se registra luego en este modulador; la respuesta de la llave (solo fase, solo amplitud ó amplitud-fase) es un modo de operación del modulador, que se ajusta mediante el retardador de media onda R1. Nosotros utilizamos llaves de solo fase, en este sentido, la precisión en el cálculo de este tipo de llave depende del conocimiento de la función de modulación en fase del dispositivo LCR2500 (ver Fig.2); la función de modulación de fase fue determinada utilizando un interferómetro Mach-Zehnder [25]. El retardador de media onda R2, en conjunto con R1, permiten controlar el estado de modulación del holograma fotorrefractivo.

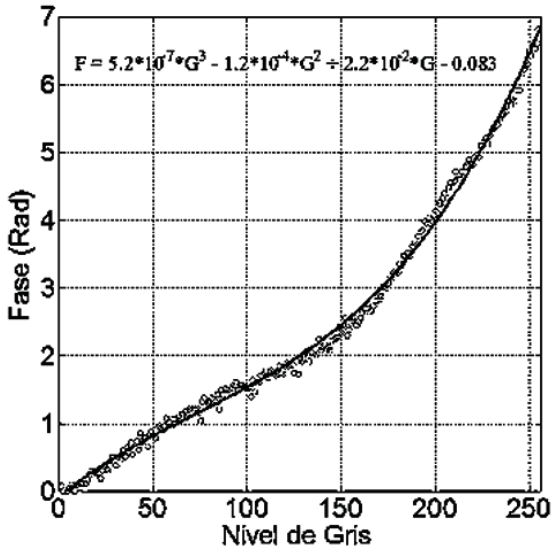


Figura 2. Función de modulación en fase (F) del LCR2500 para la longitud de onda 514nm; G es el Nivel de Gris aplicado [25].

El procesador PEF tiene dos salidas, una a través de la cámara C2 que registra la intensidad del plano de descifrado y la cámara C1 que permite verificar el estado de ocultamiento de la imagen cifrada registrada holográficamente en el BSO. El plano objeto **t** es una diapositiva, cuya función de transmitancia se requiere cifrar; en nuestro experimento la diapositiva despolariza el haz de entrada, razón por la cual se utiliza el polarizador P2, dado que para sintonizar el modulador en modo de operación de solo fase se requiere polarización lineal.

2.1. Modelo matemático del procesador

El modelo se presenta en términos de la difracción de Fresnel [26,27]; esta formulación propone para la propagación en el espacio libre la siguiente respuesta impulso:

$$h(x_o,y_o;z)=\exp(-jk_oz)\cdot\exp\left[\frac{-jk_o\left(x_o^{\,2}+y_o^{\,2}\right)}{2z}\right] \quad (1)$$

donde **z** es la distancia entre el plano objeto y el plano de observación. $k_o=\frac{2\pi}{\lambda}$ es el número de onda; $U(x_o,y_o;0)$ representa una onda que se difracta en el objeto $t(x_o,y_o)$, así, el campo $Uz(x,y;z)$ difractado es

de la forma:

$$Uz(x,y;z) = U(x_o,y_o;0)\cdot t(x_o,y_o;0) * h(x_o,y_o;z) \quad (2)$$

donde "*****" denota el operador convolución. Si suponemos que *U* es una onda plana de amplitud la unidad, $Uz(x,y;z) = t(x_o,y_o;0) * h(x_o,y_o;z)$. A partir de esta formulación, a continuación se modela en dos etapas el funcionamiento del procesador.

2.1.1. Etapa de cifrado:

Propagación de la onda $Uz(x,y;z_1)$ entre el plano objeto $t(x_o,y_o)$ y la superficie de reflexión del LCR2500, que en nuestro caso denominamos llave de cifrado $K(x_1,y_1;z_1) = \exp[-j\phi(x_1,y_1)]$, donde *f* es una distribución de fase aleatoria; entonces:

$$\begin{aligned} U_K(x_1,y_1;z_1) &= [t(x_o,y_o) * h_1(x_o,y_o;z_1)]\cdot K(x_1,y_1) \\ &= T(x_1,y_1)\cdot K(x_1,y_1) \end{aligned} \quad (3)$$

1) Propagación $z_2 = z_1$ entre el plano de la llave y el plano de cifrado BSO$(x_2,y_2;z_2 = z_1)$; el campo en este plano se puede denotar por:

$$U_C(x_2,y_2;z_2) = U_k * h_2(x_1,y_1;z_2) \quad (4)$$

De las ecuaciones (3) y (4) se concluye que la fase de h_2 será aleatoria siempre que lo sea la fase de la llave K. Si el campo U_C es tal, que la relación Señal/ Ruido tiende a cero, consecuencia de la convolución $U_k * h_2$, entonces este campo será ruido blanco; en otras palabras, se tendrá una imagen cifrada del objeto $t(x_o,y_o)$. Esta condición de cifrado depende de las características de la llave K, en términos de la distribución de sus valores aleatorios de fase.

En nuestra implementación, el campo U_C se registró holográficamente en un cristal fotorrefractivo BSO, via mezcla de cuatro ondas. Este tipo de mezclado permite, en la reconstrucción del holograma obtener la onda U_C^*, que corresponde a la onda conjugada de la onda U_C. La ecuación (5) es una representación aproximada de esta onda conjugada, consecuencia de la lectura del registro holográfico por la onda *UR*:

$$U_C^* \approx \frac{\pi\cdot d}{\lambda\cos\theta_B}\delta n\cdot UR \quad (5)$$

donde d es el espesor del cristal BSO, λ la longitud de onda de lectura, θ_B el ángulo de Bragg o de lectura, que en nuestro caso corresponde a θ/2; δn es la birrefringencia (holograma de la imagen cifrada) causada mediante efecto fotorrefractivo [23,24].

2.1.2. Etapa de descifrado:

1) Propagación de la onda U_C^* entre el plano de cifrado y el plano de la llave:

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

2) Propagación de U'_K una distancia z_1 entre el plano de la llave y el plano de la cámara C2. Este es el proceso final de decodificación de la información, esto es:

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

De la ecuación (6) se puede inferir que el efecto de la llave de cifrado K se eliminará solo cuando la llave de descifrado tenga la misma fase de K. En conclusión, el modelo muestra que el procesador PEF permite cifrar-descifrar imágenes.

3. RESULTADOS

En la Fig. 3 se muestra un histograma característico de la distribución de fase de una de las llaves utilizadas en las pruebas del PEF.

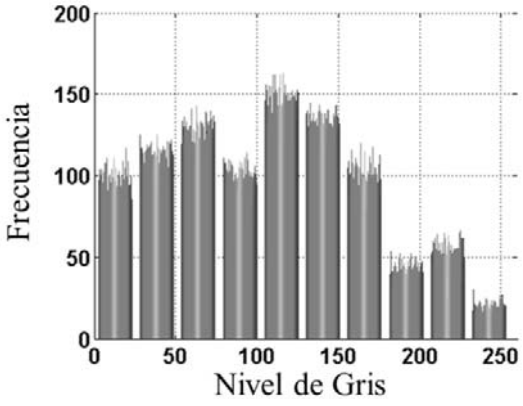


Figura 3. Histograma característico de la distribución de fase de las llaves utilizadas.

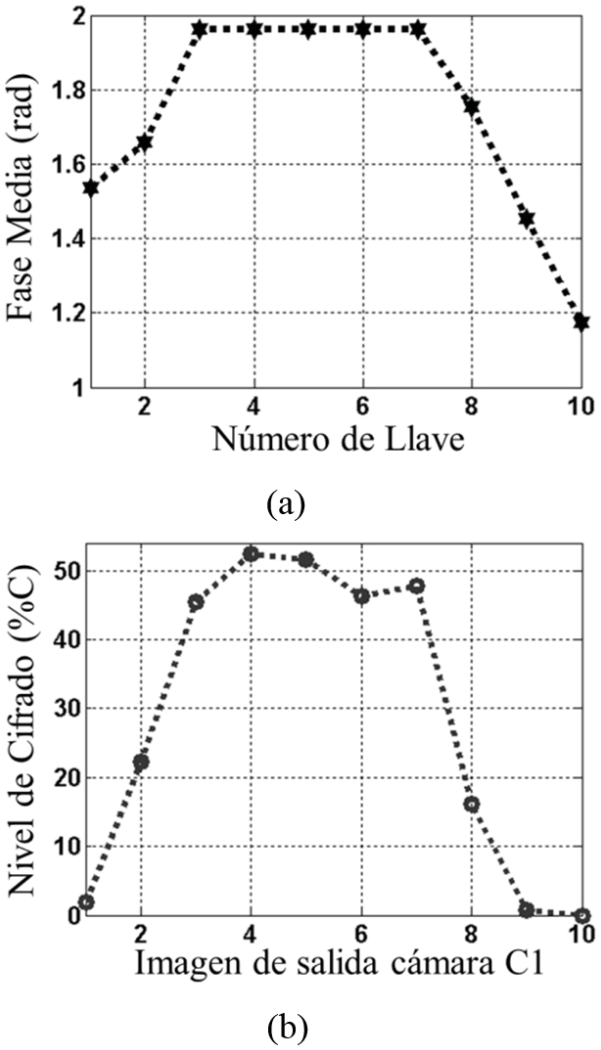
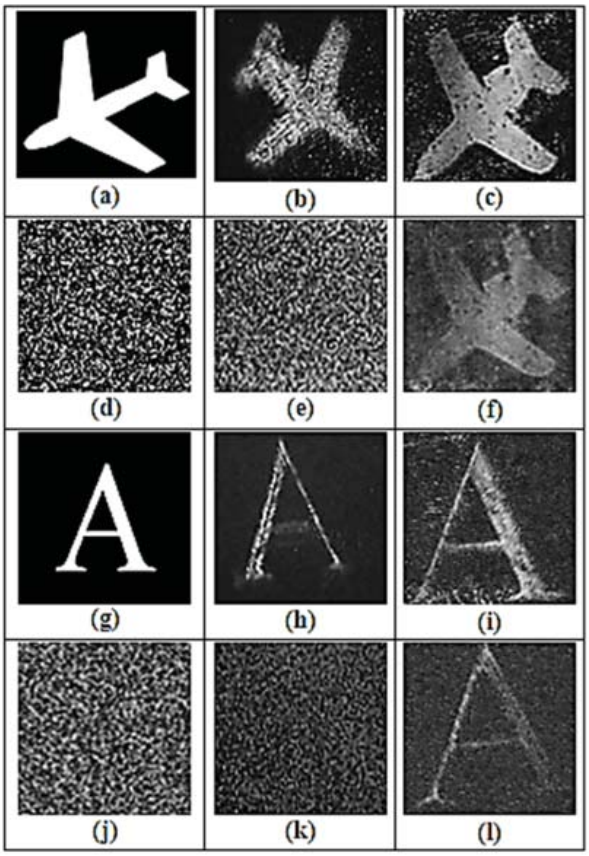


Figura 4. Características de las llaves de cifrado utilizadas.

En la Fig. 4(a) se relacionan los valores medios de fase de diez de las llaves utilizadas; la Fig. 4(b) es la relación de las mismas llaves en términos del nivel de cifrado. A partir de este análisis, se determinó que los niveles de cifrado aceptables son aquellos que estén por encima del 30%, los cuales ocurren para volores de fase media de la llave superior a 1.8 rad; así por ejemplo, en la Fig. 4 las llaves K1, K2, K8, K9 y K10 tienen valores de fase por debajo del umbral 1.8rad y con nivel de cifrado por debajo del 30%, en cuyos casos no se cifró la imagen de entrada.

Tabla 1. Resultados experimentales de validación del PEF. (a) Objeto de Prueba de 1.5 mm×1.5 mm. (b) Intensidad registrada por la cámara C1 sin llave de cifrado. (c) Intensidad registrada por la cámara C2 sin llave de cifrado. (d) Distribución de Fase de K4. (e) Intensidad registrada por la cámara C1 usando la llave K4. (f) Intensidad registrada por la cámara C2 usando la llave K4. (g) Objeto de Prueba de 1.5 mm×1.5 mm. (h) Intensidad registrada por la cámara C1 sin llave de cifrado. (i) Intensidad registrada por la cámara C2 sin llave de cifrado. (j) Distribución de Fase de K5. (k) Intensidad registrada por la cámara C1 usando la llave K5. (l) Intensidad registrada por la cámara C2 usando la llave K5.



Estos resultados dados en la Fig. 4 son los dos criterios de caracterización o validación del PEF implementado. El nivel de cifrado (*%C*) se refiere al cálculo porcentual de similitud entre la imagen cifrada y la imagen sin cifrar, según la siguiente expresión:

$$\%C = \left| \frac{IC - ISC}{IC} \right| \times 100 \qquad (8)$$

,

donde *ISC* es la imagen registrada por la cámara C1 cuando la llave tiene un plano de fase uniforme

e *IC* es la imagen registrada por la misma cámara C1 cuando la llave tiene un plano de fase aleatoria. En la Tabla 1 se presentan imágenes de dos resultados de prueba del procesador PEF. Es claro en estos resultados que la relación Señal/Ruido en las imágenes descifradas no es la mejor, sin embargo, mediante un tratamiento óptico ó digital se puede mejorar esta relación.

4. CONCLUSIONES

Se construyó un procesador óptico para cifrar-descifrar imágenes, el cual funciona en tiempo real a partir de la mezcla de cuatro ondas en un cristal fotorrefractivo de BSO. A diferencia de los procesadores ópticos de cifrado clásicos basados en las arquitecturas VLC o JTC, en nuestra implementación no utilizamos lentes para obtener las transformadas de Fresnel requeridas, es decir que el procesador trabaja por difracción de Fresnel en el espacio libre; esta propuesta puede favorecer la compactación del procesador. Esta particularidad marca la diferencia principal de nuestro valor agregado respecto a otros reportes. De otra parte, el procesador implementado es totalmente óptico en el sentido de que todas las operaciones dadas por las ecuaciones (1)-(7) son 100% ópticas. Comprobamos experimentalmente la efectividad de la conjugación de fase en el funcionamiento en tiempo real del PEF. El LCR2500 es un dispositivo con excelentes ventajas para registrar llaves de cifrado de fase, a la vez que facilita el funcionamiento del procesador, en cuanto a que la fase de la llave se puede calcular y registrar sin dificultad, y tan rápido como se requiera dentro del rango de 75Hz, que es la frecuencia de respuesta del modulador. Si bien la llave se obtiene mediante un cálculo digital, su funcionamiento es óptico. Las llaves se calcularon mediante software desarrollado en MatLab. Se establecieron dos criterios para caracterizar el PEF en términos de la distribución de valores del plano de fase de la llave de cifrado; de esta manera, determinamos que el límite inferior para el criterio nivel de cifrado aceptable es aproximadamente del 30%, que corresponde a un valor medio de los valores de la distribución de fase de la llave igual a 1.8 rad; comprobamos que por debajo de estos límites el procesadar no cifra. El tiempo de respuesta del cristal fotorrefractivo BSO utilizado, permitió un buen desempeño del procesador óptico implementado, aún bajo perturbaciones mecánicas externas de frecuencias bajas comparadas con el inverso del tiempo de respuesta del material.

REFERENCIAS

[1] Vanderlugt, A., Signal detection by complex spatial filter, IEEE Transactions on Information Theory, IT-10, pp. 139-146,1964.

[2] Weaver, C. S., Goodman, J. W., A technique for optically convolving two functions, Applied Optics, 5, pp. 1248-1249,1966.

[3] Javidi, B., Zhang, G., LI, J., Experimental demonstration of the random phase encoding technique for image encryption and security verification, Optical Engineering, 35, pp. 2506-2512,1996.

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

[5] Matoba, O. and Javidi, B., Encrypted optical storage with angular multiplexing, Applied Optics, 38, 7288,1999.

[6] Tajahuerce, E., Matoba, O., Verrall, S.C., Javidi, B., Optoelectronic information encryption with phase-shifting interferometry, Applied Optics, 39, pp. 2313-2320, 2000.

[7] Unnikrishnan, G., Joseph, J. and Singh, K., Optical encryption by double-random phase encoding in the fractional Fourier domain, Optics Letters, 25 (12), pp. 887-889, 2000.

[8] Hennelly, B. and Sheridan, J.T., Optical image encryption by random shifting in fractional Fourier domains, Optics Letters, 28, Issue 4, pp. 269-271, 2003.

[9] Salazar, A., Rueda, J.E. and Lasprilla, M., Encriptación por conjugación de fase en un BSO utilizando señales ópticas de baja potencia, Revista Colombiana de Física, 34, pp. 636-640, 2002.

[10] Nishchal, N.K., Joseph, J. and Singh, K., Optical phase encryption by phase contrast using electrically addressed spatial light modulator, Optics Communications, 42, pp. 117-122, 2003.

[11] Mela, C. and Lemmi, C., Optical encryption using phase-shifting interferometry in a joint transform correlator, Optics Letters, 31, pp. 2562-2564, 2006.

[12] Amaya, D., Tebaldi, M., Torroba, R., Bolognini, N., Wavelength multiplexing encryption using joint transform correlator architecture, Applied Optics, 48, pp. 2099-2104, 2009.

[13] Rueda, E., Tebaldi, M., Torroba, R., Bolognini, N., Three-dimensional key in a modified joint transform correlator encryption scheme, Optics Communications , 284, pp. 4321-4326, 2011.

[14] Ding, L. and Weimin, J., Color image encryption based on joint fractional Fourier transform correlator, Optical Engineering, 50, 2011.

[15] Situ, G. and Zhang, J., Multiple-image encryption by wavelength multiplexing Optics Letters, 30, pp. 1306-1308, 2005.

[16] Barrera, J.F., Henao, R., Tebaldi, M., Torroba, R., Bolognini, N., Multiplexing encrypted data by using polarized light, Optics Communications, 260, pp. 109-112, 2006.

[17] Singh, M., Kumar, A. and Singh, K., Securing multiplexed information by in-plane rotation of random phase diffusers constituting a sandwich diffuser placed in the Fourier plane of a double random phase encoding system, Optics and Laser Technology, 41, pp. 32-41, 2009.

[18] Nomura, T. and Javidi, B., Optical encryption using a joint transform correlator architecture, Optical Engineering, 39, pp. 2031-2035, 2000.

[19] Refregier, P., Javidi, B., Optical image encryption based on input plane and Fourier plane random encoding, Optics Letters, 20, pp. 767-769,1995.

[20] Matoba, O. and Javidi, B., Encrypted optical memory system using three-dimensional keys in the Fresnel domain, Optics Letters, 24, pp. 762-764, 1999.

[21] Situ, G. and Zhang, J., Double random-phase encoding in the Fresnel domain, Optics Letters, 29, pp. 1584-1586, 2004.

[22] Sudheesh, K., Raput, Y. and Naveen, K.N., Known-plaintext attack-based optical cryptosystem using phase-truncated Fresnel transform, Applied Optics, 52, pp. 871-878, 2013.

[23] Yeh, P., Introduction to photorefractive nonlinear optics, John Wiley & Sons,1993.

[24] Frejlich, J., Photorefractive Materials, Fundamental Concepts, Holographic recording and Materials Characterization, John Wiley & Sons, 2007.

[25] Rueda, J.E., Romero, A.L. and Guerra, L.A., Characterization of Reflective TN-LCD, Tuned in Phase-Only Modulation and to Six Wavelengths, Photonics Letters Of Poland, 2, pp. 174-176, 2010.

[26] Goodman, J.W., Introduction to Fourier Optics, McGraw-Hill, 1996.

[27] Lora, G. J., Munera, N. and Garcia, J., Modelling and reconstruction of gabor-type holograms, DYNA, 166, pp. 81-88, 2011.