Revista Colombiana de Física, Vol. 42, No. 2 de 2010.

Análisis de la Sensibilidad de un Sistema Óptico de Encriptación Bajo Rotaciones de la Llave de Seguridad

Analysis of Sensibility Under Key Rotations for an Optical Encryption System

C.A. Ríos [*] [a], E. Rueda[a], J.F. Barrera[a]

[a] *Grupo de Óptica y Fotónica, Instituto de Física, Universidad de Antioquia, A.A. 1226, Medellín, Colombia.*

Recibido 02.03.10; Aceptado 19.08.10; Publicado en línea 17.01.11.

Resumen

Se simula un sistema de encriptación óptico de doble máscara de fase usando una técnica de holografía digital y un correlador de transformada conjunta. El sistema de encriptación utiliza como llave de seguridad una máscara aleatoria de fase. Se llevan a cabo simulaciones computacionales para generar un proceso de encriptación óptico y una desencriptación digital. Para simular la llave se utiliza el modelo de probabilidad de fase balanceada donde los dispersores tienen el mismo tamaño, son estadísticamente independientes, tienen transmitancia constante y están dispuestos en un arreglo cuadrado. Se estudia el efecto que genera la rotación de la llave de seguridad durante la desencriptación y se analiza el resultado de la recuperación cuando las llaves tienen dispersores de distintos tamaños, encontrándose una relación directa entre el tamaño del dispersor y la sensibilidad a las rotaciones de la llave; a menor tamaño mayor sensibilidad.

Palabras Clave: Encriptación, Correlador Transformada Conjunta, Llave de Seguridad.

Abstract

We simulated a double phase mask encoding optical system using a digital holography technique and a joint transform correlator architecture. The encryption system uses a random phase mask security key. We carried out computational simulations of an optical encryption and a digital decryption process. We studied the effect of rotating the phase key, in the decryption result, for different scatterers sizes. To simulate the phase key we used the balance-phase probability model with scatterers of the same size, statistically independent, constant transmittance and placed in a square arrangement.

Keywords: Encryption, Joint Transform Correlator, Security Key.
PACS: 42.30.-d, 42.30.Ms, 42.25.Fx.

1. Introducción

La mayoría de las arquitecturas ópticas de encriptación tienen como principio de operación la codificación de doble máscara de fase (CDMF), que consiste en utilizar dos máscaras de fase aleatorias en el proceso de encriptación de la información. El trabajo pionero en la encriptación óptica de datos se basa en la CDMF y en una arquitectura 4f, donde la primera máscara está ubicada en el plano de entrada del sistema y la segunda en el primer plano de Fourier [1]. En la primera implementación experimental del sistema de encriptación de doble máscara de fase la imagen encriptada es registrada en un holograma. Luego el complejo conjugado de la llave de seguridad y el holograma deben ser insertados en la estación desencriptadora para recobrar la información original [2]. Por lo anterior, este sistema no trabajaba a tiempo real. Además, la precisión del posicionamiento de los elementos durante la desencriptación exige bajas toleran-

[*] carlos.riosocampo@gmail.com

cias para que el proceso sea exitoso, y se tiene que producir el complejo conjugado de la llave de seguridad, eliminando la posibilidad de usar vidrios esmerilados (difusores que tienen un rango de fase continuo entre 0 y 2π). Para aliviar las desventajas antes mencionadas y con base en las características de los cristales fotorrefractivos, se realizó 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 a 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 [3].

Posterior a la propuesta e implementación experimental del sistema óptico de encriptación, se presentaron múltiples contribuciones que igualmente se basan en la CDMF. Se implementó un montaje experimental bajo arquitectura 2f y con cristales fotorrefractivos para registrar holográficamente el dato encriptado [4]. En otras aproximaciones las mascaras están situadas en planos de Fresnel [5], o en planos fraccionales de Fourier [6], o bajo arquitectura JTC (por sus siglas en inglés, JTC: Joint Transform Correlator) [7], o usando un sistema sin lentes [8], etc.

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. En particular, una de las propuestas emplea un sistema basado en una arquitectura JTC y una técnica de holografía digital para la encriptación de datos [9]. La encriptación se lleva a cabo en un procesador óptico mientras que la desencriptación es completamente digital, lo que representa una ventaja en cuanto a la transmisión, recepción y desencriptación de la información. Además de las ventajas del procesamiento óptico-digital, en la arquitectura JTC los requerimientos de alineación y resolución son menos estrictos que en otras arquitecturas y bajo algunas condiciones no se requiere un filtrado de la información. Todo lo antes mencionado hace que el sistema de encriptación basado en una arquitectura JTC y en técnicas de holografía digital sea atractivo para una futura implementación práctica de un sistema de seguridad basado en la encriptación óptica de información. Otra característica de este sistema es que utiliza vidrios esmerilados para generar las llaves de seguridad, lo que obliga a desplazar el difusor para poder generar llaves diferentes. Los desplazamientos podrán ser laterales (con una modificación del montaje [10]) o rotacionales, y en ambos casos será importante conocer la sensibilidad del sistema a dichos desplazamientos. Teniendo lo anterior en cuenta, en este trabajo se estudia el procesador óptico-digital de Rueda et al. [9] para investigar el efecto que la rotación de la llave de seguridad tiene sobre la desencriptación de la información. En particular se propone que la sensibilidad del sistema es directamente proporcional al tamaño del dispersor del difusor. Para mostrar la validez de la propuesta se simula un sistema óptico y se analiza la recuperación de la información para diferentes rotaciones y con varios tamaños de dispersores.

2. Proceso de Encriptación y Desencriptación

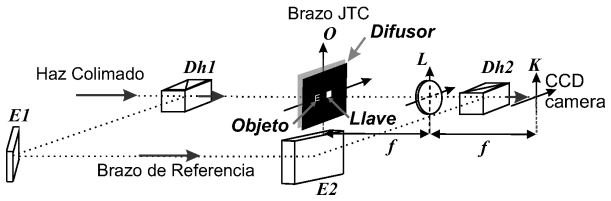

Fig. 1: Montaje experimental propuesto: $Dh1$ y $Dh2$: Divisores de Haz, E_1 y E_2: Espejos, O: plano de entrada con *Objeto* a ser encriptado, *Difusor*: Máscara de fase aleatoria, *Llave*: Máscara de fase aleatoria para la encriptación, L: lente de distancia focal f, K: plano de salida donde se ubica una cámara CCD.

Para llevar a cabo los procesos de encriptación y desencriptación se implementó un montaje óptico-digital basado en una arquitectura JTC. Para el montaje se usó un interferómetro de Mach-Zehnder (ver Fig. No. 1) [9].

En el plano de entrada O es ubicado el objeto a encriptar $o(x, y)$, separado una distancia $a + b$ de la llave de seguridad $h(x, y)$ que corresponde a una máscara de fase aleatoria, como se muestra en la Fig. No. 2.

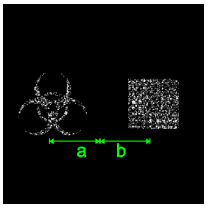

Fig. 2: Fase en niveles de gris del plano de entrada del sistema. Izquierda: Objeto, Derecha: Máscara de fase.

Así, la expresión para el plano de entrada es:

$$f(x_0, y_0)\otimes\delta(x_0-(-a), y_0)+h(x_0, y_0)\otimes\delta(x_0-b, y_0), \quad (1)$$

donde $f(x_0, y_0) = o(x_0, y_0)d(x_0, y_0)$ y $d(x, y)$ es una máscara de fase aleatoria. En el proceso de encriptación se bloquea el brazo de la onda de referencia y se registra el espectro conjunto de potencias, del plano de entrada, con una cámara CCD en el plano K:

$$\begin{aligned} T_1(u, v) = \quad & |F(u, v)|^2 + F^*(u, v)H(u, v)e^{-2i\pi(a+b)u} \\ & +F(u, v)H^*(u, v)e^{-2i\pi(-a-b)u} \\ & +|H(u, v)|^2, \end{aligned} \quad (2)$$

donde los términos constantes no se tienen en cuenta, $F(u, v)$ y $H(u, v)$ son los espectros de Fourier de $f(x, y)$

y $h(x,y)$ respectivamente, $u = \frac{x'}{\lambda f}$, $v = \frac{y'}{\lambda f}$, λ es la longitud de onda, f es la distancia focal de la lente, (x', y') son las coordenadas del plano K y $H^*(u,v)$ es el complejo conjugado de $H(u,v)$. Si además se registran las intensidades de la Transformada de Fourier (TF) del objeto $|F(u,v)|^2$ y la TF de la llave $|H(u,v)|^2$, y se realiza un proceso digital de restado, se eliminan los términos considerados ruido en la Ec. No. 2, y por lo tanto la imagen encriptada será:

$$T_1'(u,v) = F^*(u,v)H(u,v)e^{-2i\pi(a+b)u} + F(u,v)H^*(u,v)e^{-2i\pi(-a-b)u}. \quad (3)$$

Para desencriptar, se desbloquea la onda de referencia y se registra el holograma de la transformada de Fourier de la máscara de fase (TFMF):

$$T_2(u,v) = |P(u,v)|^2 + H'^*(u,v)P(u,v)e^{-2i\pi(-b)u} + H'(u,v)P^*(u,v)e^{-2i\pi bu} + |H'(u,v)|^2, \quad (4)$$

donde los términos constantes no se tienen en cuenta, $P(u,v)$ representa la onda plana de referencia y $H'(u,v)$ la TF de la máscara de fase aleatoria $h'(x,y)$ con la que se pretende desencriptar. Igual que para el caso de la imagen encriptada, se registran las intensidades de la TF de la llave $|H'(u,v)|^2$ y la intensidad de la onda plana $|P(u,v)|^2$, y se restan digitalmente en la Ec. No. 4:

$$T_2'(u,v) = H'^*(u,v)P(u,v)e^{-2i\pi(-b)u} + H'(u,v)P^*(u,v)e^{-2i\pi bu}. \quad (5)$$

Siguiendo con el proceso de desencriptación, digitalmente se multiplican $T_1'(u,v)$ y $T_2'(u,v)$ y se realiza la transformada de Fourier inversa, obteniéndose como resultado la suma de cuatro términos:

$$\begin{aligned} T_3(x,y) = {} & f(x,y) \otimes [h^*(-x,-y) \otimes h'(x,y)] \\ & \otimes \delta(x-(-a-\lambda f\alpha), y-(-\lambda f\beta)) \\ & + f(x,y) \otimes [h^*(-x,-y) \otimes h'^*(-x,-y)] \\ & \otimes \delta(x-(-a-2b-\lambda f\alpha), y-\lambda f\beta) \\ & + f^*(-x,-y) \otimes [h(x,y) \otimes h'(x,y)] \\ & \otimes \delta(x-(a+2b-\lambda f\alpha), y-(-\lambda f\beta)) \\ & + f^*(-x,-y) \otimes (h(x,y) \otimes h'^*(-x,-y)) \\ & \otimes \delta(x-(b-\lambda f\alpha), y-\lambda f\beta), \end{aligned} \quad (6)$$

donde no se tienen en cuenta las constantes que acompañan a cada término. La onda plana tiene cosenos directores $[cos\theta, cos\phi]$ tal que $P(x',y') = exp(-i2\pi(\alpha x' + \beta y'))$, donde $\alpha = \frac{cos\theta}{\lambda}$, $\beta = \frac{cos\phi}{\lambda}$, y θ y ϕ ángulos directores de la onda plana de referencia. El primer término corresponde al objeto, el cual está sujeto a que la correlación entre la llave de seguridad y la máscara de fase con la que se pretende desencriptar, $h^*(-x,-y) \otimes h'(x,y)$, se aproxime a una delta de Dirac [3]; la posición del objeto encriptado será $\delta(x-(-a-\lambda f\alpha), y-(-\lambda\beta))$. El cuarto término corresponde al complejo conjugado del primero, el segundo y tercer término corresponden a términos de ruido, ver Fig. No. 3.

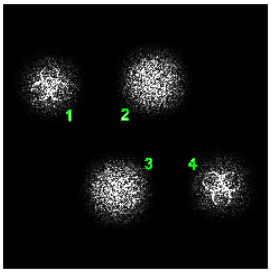

Fig. 3: Resultado del proceso de desencriptación. Término 1: objeto desencriptado, términos 2 y 3: ruido, término 4: complejo conjugado del objeto desencriptado.

3. Rotación de la Llave de Seguridad

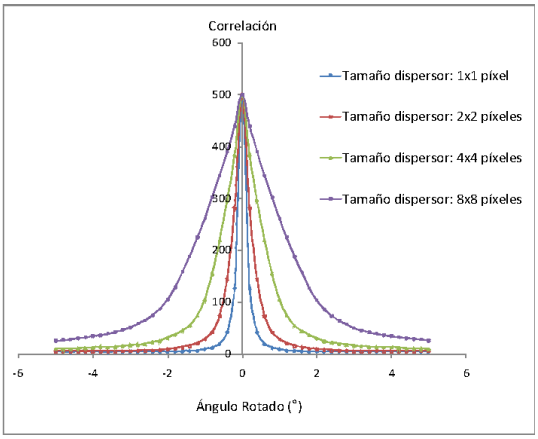

Fig. 4: Valores máximos de correlación entre la llave de seguridad y la llave de seguridad rotada para cuatro tamaños de dispersores

Para estudiar la sensibilidad del sistema bajo rotaciones de la llave de seguridad, y teniendo en cuenta la correlación $h^*(-x,-y) \otimes h'(x,y)$ en la Ec. No. 6, que da cuenta del éxito del proceso de desencriptación, se determinaron los valores máximos de correlación para distintos ángulos de rotación del difusor, y para distintos tamaños de dispersores. Es de esperarse que una tasa de cambio negativa y rápida del valor máximo de correlación corresponda a una mayor sensibilidad. Para simular las llaves, se usó un modelo de probabilidad de fase balanceada en el rango $[0, 2\pi]$ [3] donde todos los dispersores tienen el mismo tamaño, son estadísticamente independientes, tienen transmitancia constante y estaban dispuestos en un arreglo cuadrado de 500×500. Los resul-

tados se presentan en la Fig. No. 4, donde se aprecia que a mayor tamaño de dispersor, mayor debe ser el ángulo rotado para que la imagen no se desencripte correctamente, es decir, menor sensibilidad. Se simuló el sistema óptico virtual del montaje experimental con el fin de encontrar la relación entre el tamaño del dispersor y la calidad de la imagen desencriptada y compararla con la Fig. No. 4. Los resultados para las diferentes rotaciones de la llave de seguridad con los distintos tamaños de dispersores son mostrados en la Fig. No. 5, la Fig. No. 6 y la Fig. No. 7.

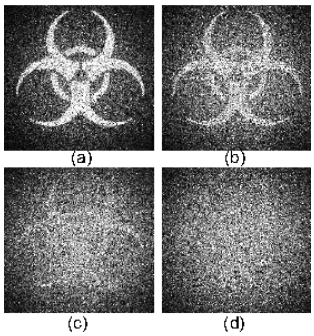

Fig. 5: Objetos desencriptados usando un dispersor de 1×1 píxel con una rotación de la llave de: (a) 0^o, (b) $0{,}2^o$, (c) $0{,}6^o$ y (d) 1^o

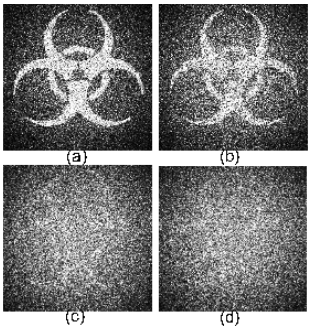

Fig. 6: Objetos desencriptados usando un dispersor de 2×2 píxeles con una rotación de la llave de: (a) 0^o, (b) $0{,}5^o$, (c) $1{,}2^o$ y (d) 2^o

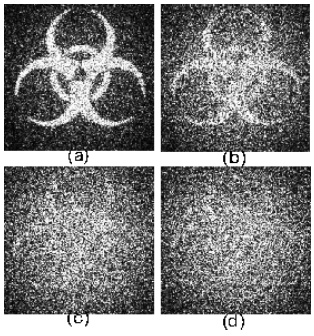

Fig. 7: Objetos desencriptados usando un dispersor de 4×4 píxeles con una rotación de la llave de: (a) 0^o, (b) 1^o, (c) $1{,}8^o$ y (d) $2{,}2^o$

Por último se obtuvo el error cuadrático medio normalizado (NMSE) de las imágenes desencriptadas, para cada rotación y cada tamaño de dispersor. El NMSE está definido por la siguiente ecuación:

$$\mathrm{NMSE}(I_0, I) = \frac{1}{K} \sum_{i,j}^{N} |I(i,j) - I_0(i,j)|^2 , \qquad (7)$$

donde $I_0(i,j)$ e $I(i,j)$ son la imágenes desencriptadas con el difusor sin rotar y rotado en el píxel (i,j), respectivamente. La imagen tiene un total de $N \times N$ píxeles y K es el error cuadrático medio entre I_0 y la imagen desencriptada bajo una rotación de 90^o. En la Fig. No. 8 se presentan los resultados.

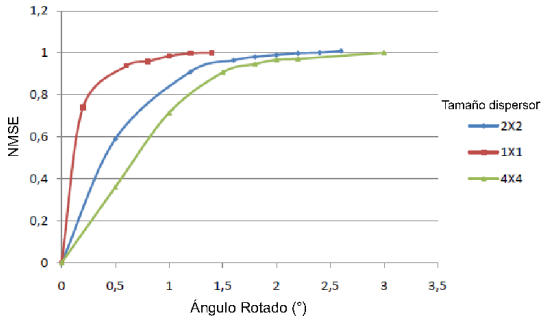

Fig. 8: Error cuadrático medio para tres tamaños distintos de dispersor: 1×1, 2×2 y 4×4 píxeles

Los resultados obtenidos en la simulación del sistema óptico virtual muestran que a medida que se rota la llave de seguridad en el proceso de desencriptación, la correlación se pierde en un ángulo mayor si se tiene una máscara de fase con dispersores grandes, es decir la imagen no es desencriptada. Esto se aprecia en la Fig. No. 4 donde la curva de los picos máximos de correlación de un difusor con un dispersor de 1×1 píxel cae al 2 % en un ángulo de aproximadamente 1^o, mientras que el de 2×2 píxeles cae en aproximadamente 2^o, el de 4×4 en aproximadamente 5^o y el de 8×8 en un ángulo superior a los límites de la gráfica. Estos mismos resultados pueden ser apreciados en la Fig. No. 8, donde el objeto no es desencriptado para un NMSE cercano a 1, es decir, para el ángulo en que ya las dos imágenes comparadas son prácticamente distintas. En la Fig. No. 8 se observa un comportamiento distinto para el difusor con tamaño de dispersor de 4×4, ya que para éste el objeto no se desencripta para un ángulo menor que el predicho por la gráfica de las correlaciones (Fig. No. 4). Igualmente en la Fig. No. 7 se observa que el objeto ya no es desencriptado para un ángulo menor.

4. Conclusiones

Se encontró que la sensibilidad del sistema a rotaciones del difusor depende del tamaño del dispersor del difusor: a mayor tamaño de dispersor, menor la sensibilidad. No obstante, la dependencia no es exactamente como la predice la correlación de los difusores, puesto que la simulación del sistema óptico virtual tiene en cuenta parámetros físicos como: tamaño de las pupilas, tamaño del objeto, tamaño de la llave, efectos difractivos de los distintos elementos, etc. Será necesario incluir en el análisis del montaje experimental los distintos parámetros físicos, con el fin de conocer su influencia en la sensibilidad del sistema ante rotaciones de la llave. Si se usa una llave con tamaño de dispersor pequeño, el sistema es más seguro ante posibles ataques y más apto para otras aplicaciones como la multiplexación de información.

Referencias

[1] Refregier, P., Javidi, B. Optical image encryption based on input plane Fourier plane random encoding. En: Opt. Lett., No. 20 (1995); p. 767-769. ISSN 0146-9592.

[2] Javidi, B., Zhang, G., Li, J. Experimental demonstration of the random phase encoding technique for image encryption and security verification. En: Opt. Eng., No. 35 (1996); p. 2506-2512. ISSN 0091-3286.

[3] Unnikrishnan, G., Joseph, J. y Singh, K. Optical encryption system that uses phase conjugation in a photorefractive crystal. En : Appl. Opt., No. 37 (1998); p. 8181-8186. ISSN 1539-4522.

[4] Matoba, O., Javidi, B. Encrypted optical storage with angular multiplexing. En: App. Opt., No. 38 (1999); p. 7288-7293. ISSN 1539-4522.

[5] Matoba, O., Javidi, B. Encrypted optical memory system using three-dimensional keys in the Fresnel domain. En: Opt. Lett., No. 24 (1999); p. 762-764. ISSN 0146-9592.

[6] Unnikrishnan, G., Joseph, J. y Singh, K. Optical encryption by double-random phase encoding in the fractional Fourier domain. En: Opt. Lett., No. 25 (2000); p. 887-889. ISSN 0146-9592.

[7] Nomura, T., Javidi, B. Optical encryption using a joint transform correlator architecture. En: Opt. Eng., No. 39 (2000); p. 2031-2035. ISSN 0091-3286.

[8] Situ, G., Zhang, J., Double random-phase encoding in the Fresnel domain. En: Opt. Lett., No. 29 (2004); p. 1584-1586. ISSN 0146-9592.

[9] Rueda, E., Barrera, J. F., Henao, R., Torroba, R. Optical encryption with a reference wave in a joint transform correlator architecture. En: Opt. Commun., No. 282 (2009); p. 3243-3249. ISSN 0030-4018

[10] Rueda, E., et al. Lateral shift multiplexing with a modified random mask in a joint transform correlator encrypting architecture. En : Opt. Eng. No. 48 (2009); p. 027006. ISSN 0091-3286.