Rev. Acad. Colomb. Cienc. Ex. Fis. Nat. 39(Supl.):55-60, 2015
doi: http://dx.doi.org/10.18257/raccefyn.263

Protección de datos usando un sistema experimental de encriptación de correlador de transformada conjunta

Roberto Torroba[1], John Fredy Barrera-Ramírez[2,*]

[1]Centro de Investigaciones Ópticas (CONICET La Plata-CIC) and UID OPTIMO,
Facultad de Ingeniería, Universidad Nacional de La Plata, La Plata, Argentina
[2]Grupo de Óptica y Fotónica, Instituto de Física, Facultad de Ciencias Exactas y Naturales, Universidad de Antioquia

Resumen

En esta contribución se presenta la implementación experimental un sistema de protección de información basado en el procesamiento óptico y se analiza la fidelidad de la información recuperada cuando hay pérdida de datos durante la transmisión. La información es encriptada empleando una arquitectura óptica de correlador de transformada conjunta y una técnica de codificación de doble máscara de fase. Un usuario autorizado puede recuperar la información original cuando tiene acceso a la información del dato encriptado y de la llave de seguridad; si un intruso puede interceptar la imagen encriptada, pero no accede la información de la llave de seguridad, no podrá acceder a la información contenida en el dato encriptado. La descripción teórica y los resultados experimentales demuestran la habilidad que tiene el sistema de seguridad para proteger y recuperar información por medio de procesadores ópticos, y su tolerancia a la pérdida de información durante la transmisión.

Palabras clave: procesamiento óptico de información, protección de datos, seguridad óptica, correlador de transformada conjunta, encriptación, desencriptación.

Data protection using a joint transform correlator experimental system

Abstract

In this contribution the implementation of an experimental data protection system based on optical processing is presented, and the reliability of the recovered information when there is data loss during transmission is analyzed. The information is encrypted using an optical joint transform correlation architecture together with a double phase mask encoding technique. An authorized user recovers the original information when accessing the encoded data and the security key; if an intruder intersects the encoded image but does not possess the security key there is no possibility to access to the information contained in the encrypted image. The theoretical description and the experimental results show the ability the security systems exhibits to protect and recover the information by optical means, including the tolerance to data loss during transmission.

Key words: Optical information processing, data protection, optical security, joint transform correlator, encryption, decryption.

Introducción

Día a día aumenta en forma significativa la cantidad de información pública y privada disponible en el mundo, y en esa misma medida se incrementa el número de personas que intercambian datos (caracteres, archivos binarios, imágenes, videos, etc). Esto implica que se tiene un gran número de personas enviando y recibiendo información que en muchos casos es secreta o sensible. Por lo tanto, hoy en día para muchas personas alrededor del mundo es cotidiano el uso de protocolos y sistemas que garantizan que los datos privados sean accesibles sólo para los usuarios autorizados.

Las empresas invierten miles de millones de dólares alrededor del mundo sólo para evitar el fraude en la información. Además, las comunicaciones electrónicas y el almacenamiento de datos en computadores están bajo riesgo dado que las comunicaciones en línea y a través de redes inalámbricas pueden ser interceptadas o intervenidas. Riesgo que se incrementa con la alta capacidad de procesamiento de los computadores, capaces de reducir el tiempo requerido para codificar y decodificar mensajes, incluso las más sofisticadas técnicas de codificación digital pueden llegar a ser vulnerables.

Teniendo en cuenta lo antes mencionado y considerando que muchos sistemas de seguridad que en un momento se

***Correspondencia:**
John Fredy Barrera-Ramírez, john.barrera@udea.edu.co
Recibido: 16 de julio de 2015
Aceptado: 23 de octubre de 2015

consideraron seguros finalmente fueron vulnerados (**Bellare, Desai, Pointcheval & Rogaway,** 1998; **Camp-Winget, Housley, Wagner & Walker,** 2003; **Shannon,** 1949), todas las áreas relacionadas con la seguridad en la información han presentado un gran desarrollo. Este desarrollo incluye la consolidación y surgimiento de nuevas alternativas para el manejo seguro de datos. En particular, la encriptación óptica ha demostrado ser una importante alternativa a los sistemas actualmente disponibles (**Graydon,** 2013; **Pile,** 2010).

A los diferentes procedimientos ópticos usados para cifrar u ocultar información se les conocen en la literatura como métodos de encriptación, y a los usados para recuperar o acceder a la información oculta por parte de personas autorizadas se les conoce como métodos de desencriptación. Los códigos o valores de los parámetros con los cuales se oculta la información se conocen como llave(s) de seguridad, lo que implica que la información solo puede ser recuperada si el usuario autorizado posee la(s) llave(s) de seguridad correcta(s).

Los sistemas ópticos de encriptación más usados son los que emplean dos máscaras aleatorias de fase, los cuales son llamados usualmente sistemas de encriptación de doble máscara de fase. Como la seguridad del sistema es proporcionada por una máscara aleatoria, la posibilidad de construir una máscara para tratar de violar el sistema de encriptación sería un trabajo infructuoso, pues existen millones de combinaciones que se deben probar.

La propuesta e implementación del primer sistema óptico de encriptación de doble máscara de fase fue respaldada en primera instancia por simulaciones computacionales (**Refregier & Javidi,** 1995) usando una arquitectura óptica 4f. Posteriormente, se llevó a cabo su demostración experimental (**Javidi, Zhang & Li,** 1996) registrando la imagen encriptada 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. Más tarde, se publicó una contribución donde se usaba un cristal fotorrefractivo para registrar la imagen encriptada (**Unnikrishnan, Joseph & Singh,** 1998). En este caso la encriptación y la desencriptación se efectúan en tiempo real, sin necesidad de emplear el complejo conjugado de la llave de seguridad y sin el requerimiento de posicionar elementos durante la desencriptación.

Motivado por el gran número de grados de libertad que posee el procesamiento óptico de información, varios investigadores alrededor del mundo llevaron a cabo investigaciones que condujeron a la implementación de diferentes esquemas de encriptación de doble máscara de fase. Por un lado se desarrollaron sistemas de encriptación en el dominio fraccional de Fourier (**Unnikrishnan, Joseph & Singh,** 2000) y en el dominio de Fresnel (**Situ & Zhang,** 2004), además se publicó un artículo donde se combina un sistema óptico 4f y la propagación en espacio libre para la protección de múltiples datos (**Barrera & Torroba,** 2010), y se mostró que la posición axial de la llave encriptadora representa una llave extra de seguridad (**Matoba & Javidi,** 1999). Asimismo, se llevaron a cabo investigaciones que permitieron concluir que la longitud de onda (**Situ & Zhang,** 2005), el desplazamiento lateral de la llave de seguridad (**Barrera, Henao, Tebaldi, Torroba & Bolognini,** 2006a), la polarización de la luz (**Barrera, Henao, Tebaldi, Torroba & Bolognini,** 2006b), la pupila del sistema (**Barrera, Henao, Tebaldi, Torroba & Bolognini,** 2006c) y el uso de llaves complejas (**Barrera, Tebaldi, Torroba & Bolognini,** 2009) permiten encriptar múltiples datos y aumentar la seguridad global del proceso.

Dada la gran potencialidad de los procesos ópticos de seguridad basados en la codificación de doble máscara de fase, estos se han puesto a prueba usando los protocolos establecidos. Se ha mostrado que al igual que los sistemas digitales, los sistemas ópticos virtuales, que son simulaciones computacionales de los sistemas ópticos experimentales, pueden llegar a ser vulnerables bajo ciertas condiciones (**Barrera, Vargas, Tebaldi, Torroba & Bolognini,** 2010; **Carnicer, Montes-Usategui, Arcos & Juvells,** 2005; **Wang & Zhao,** 2012). Estas vulnerabilidades han conducido, al igual que en el resto de sistemas de seguridad, a la generación de protocolos que permiten eliminar las fallas de seguridad (**Carnicer, *et al.*,** 2005; **Wang & Zhao,** 2012).

Hasta el momento no se ha reportado ninguna vulnerabilidad de los sistemas de seguridad experimentales que emplean como llaves de seguridad un elemento físico y aleatorio. Por lo tanto, aunque todos los sistemas de encriptación comerciales que se usan en la actualidad son digitales, la encriptación óptica representa una atractiva y potencialmente poderosa herramienta para el manejo seguro de la información debido a su alto grado de seguridad, robustez, aplicabilidad y flexibilidad (**Alfalou & Brosseau,** 2009; **Javidi, Esmail & Zhang,** 2012; **Nomura, Pérez-Cabré, Millán & Javidi,** 2009).

A pesar de que existen muchas arquitecturas para el procesamiento seguro de datos bajo la codificación de doble máscara de fase; la disminución de los requerimientos de alineación con respecto a otras arquitecturas para obtener la imagen encriptada, el no requerir del conjugado de la llave de seguridad o de la imagen encriptada, y lo compacto de la arquitectura de correlador de tranformada conjunta o arquitectura JTC (por las siglas en inglés de joint transform correlator), la convierten en una gran alternativa para el manejo seguro de datos. Si a lo anterior se suma la posibilidad de incluir en el proceso una técnica de holografía digital que permita almacenar digitalmente la información procesada ópticamente, se podrá contar con un sistema seguro y práctico donde la información se puede transmitir por los canales actuales de comunicación.

Teniendo en cuenta lo antes expuesto, en esta contribución se presenta la descripción teórica y la implementación experimental de un sistema óptico de encriptación de doble máscara de fase bajo una arquitectura de correlador de transformada conjunta, donde la componente experimental incluye una técnica de holografía digital. Adicionalmente, se presenta un análisis del comportamiento de la información recuperada a medida que la información de la imagen encriptada y la llave de recuperación se van deteriorando en la transmisión.

Descripción teórica e implementación experimental del sistema de seguridad

El sistema de encriptación de correlador de transformada conjunta o JTC utiliza dos máscaras aleatorias de fase para proteger información (**Nomura & Javidi,** 2000). En este sistema el plano de entrada está compuesto por el dato a encriptar $f(x_0, y_0)$ en contacto con una máscara aleatoria de fase $m(x_0, y_0)$, y otra máscara aleatoria de fase que representa la llave de seguridad $k(x_0, y_0)$ del sistema (Figura 1).

Por lo tanto, si el objeto de entrada y la llave de seguridad están separados por una distancia $2a$, la entrada del sistema encriptador será de la forma (Figura 1):

$$u_0(x_0,y_0)=\left[f(x_0,y_0)m(x_0,y_0)\right]\otimes\delta\left(x_0-(-a),y_0\right) + k(x_0,y_0)\otimes\delta(x_0-a,y_0) \quad (1)$$

donde ⊗ representa la operación convolución y δ ( ) es la función delta de Dirac. Durante el proceso de encriptación, la entrada del sistema es iluminada con una onda plana monocromática. Luego, en el plano de salida se registra la intensidad de la transformada de Fourier del plano de entrada, patrón de intensidad conocido como espectro conjunto de potencias o JPS (por las siglas en inglés de joint power spectrum),

$$JPS(u,v)=\left|F(u,v)\right|^2+\left|K(u,v)\right|^2+F(u,v)K^*(u,v)\exp(4\pi iau) + F^*(u,v)K(u,v)\exp(-4\pi iau) \quad (2)$$

donde * es el complejo conjugado, $F(u, v)$ y $K(u, v)$ son las transformadas de Fourier de $f(x_0, y_0)$ $m(x_0, y_0)$ y $k(x_0, y_0)$, respectivamente. El JPS contiene cuatro términos, los primeros dos corresponden a la intensidad de $F(u, v)$ y $K(u, v)$, respectivamente; el tercer y cuarto término son la imagen encriptada y su complejo conjugado. Para extraer la información encriptada del JPS, primero se bloquea la llave de seguridad y se registrar en el plano de salida $|F(u, v)|^2$; asimismo al bloquear el objeto se obtiene $|K(u, v)|^2$. Restando estos dos términos del JPS se obtiene,

$$JPS'(u,v)=F(u,v)K^*(u,v)\exp(4\pi iau) + F^*(u,v)K(u,v)\exp(-4\pi iau) \quad (3)$$

Finalmente, la información encriptada se obtiene filtrando el segundo término y reposicionando el primero (**Barrera, Rueda, Ríos, Tebaldi, Bolognini & Torroba,** 2011),

$$E(u,v)=F(u,v)K^*(u,v) \quad (4)$$

Para acceder a la información original a partir del dato encriptado se debe poseer la información de la llave de seguridad. Para la obtención experimental de la información encriptada y de la llave de seguridad se utilizó un interferómetro que posee en un brazo el sistema de encriptación JTC y en el otro una onda plana de referencia (Figura 2). En el proceso de encriptación, el JPS se generó experimentalmente usando solo el brazo que contiene el sistema encriptador, es decir, se bloqueó la onda de referencia, y se registró en JPS (ecuación (2)) usando una cámara CCD. El objeto de entrada $f(x_0, y_0)$ y la abertura cuadrada que define el área de la llave de seguridad se proyectaron en un modulador espacial de luz SLM (por las siglas en inglés de Spatial Light Modulator), donde las máscaras aleatorias de fase $m(x_0, y_0)$ y $k(x_0, y_0)$ se generan al poner en contacto el SLM con un difusor (vidrio despulido que es un elemento aleatorio y físico). De esta forma se obtiene la información del plano de entrada (ecuación (1)) del sistema de encriptación JTC.

Una vez se tiene la imagen encriptada (ecuación (4)), se procede con el registro de holográfico de la información de la llave de seguridad. Al bloquear la información del objeto, es decir proyectando en el modulador solo la abertura cuadrada que define el área de la llave de seguridad, y usando la onda de referencia, en la cámara CCD se puede almacenar el holograma de la transformada de Fourier de la llave de seguridad (Figura 2), que en esta arquitectura actúa como llave de recuperación (**Barrera, Rueda, Ríos, Tebaldi, Bolognini & Torroba,** 2011),

$$HK(u,v)=|K(u,v)|^2+|P(u,v)|^2+P(u,v)K^*(u,v)\exp(2\pi iau) + P^*(u,v)K(u,v)\exp(-2\pi iau) \quad (5)$$

donde $P(u, v)$ representa la onda plana de referencia. Al filtrar los primeros tres términos y reposicionar el último término de la ecuación (5), se obtiene la llave de recuperación $K(u, v)$.

En el proceso de recuperación se emplea un sistema óptico virtual de desencriptación (Figura 3), donde en el plano de entrada se ubican la imagen encriptada $E(u, v)$ (ecuación (4)) y la llave desencriptadora $K(u, v)$,

$$S(u,v)=F(u,v)K^*(u,v)K(u,v) \quad (6)$$

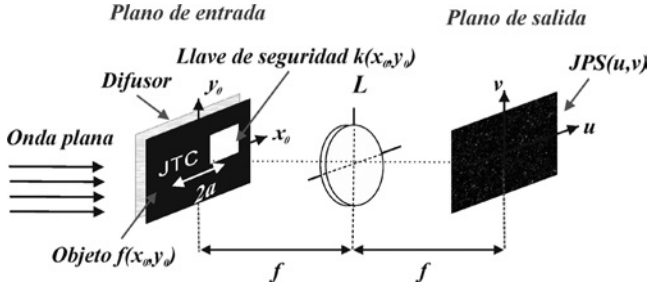

Figura 1. Sistema de encriptación JTC.

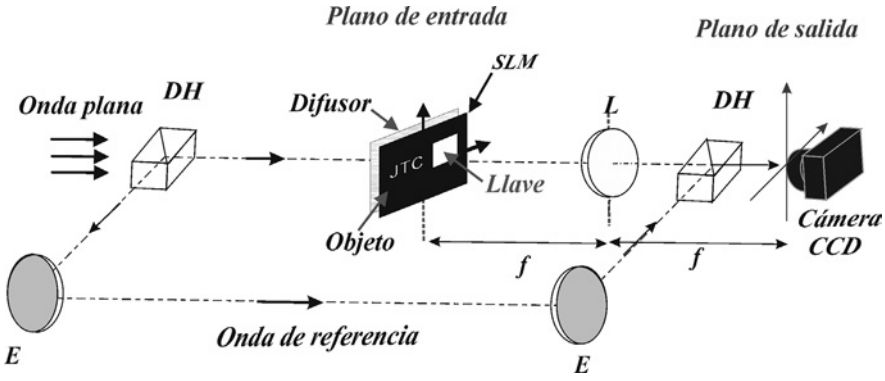

Figura 2. Montaje experimental (DH: divisor de haz; E: espejo; L: lente; SLM: modulador espacial de luz).

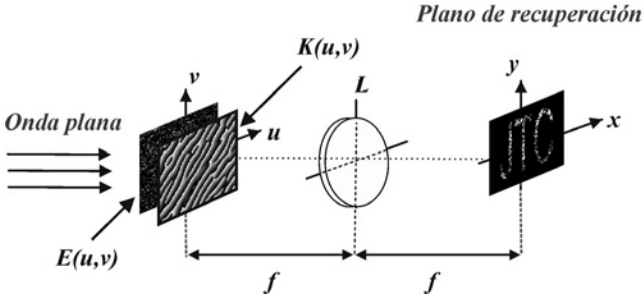

Figura 3. Sistema de recuperación.

Finalmente al realizar la transformada de Fourier sobre el plano de entrada del sistema desencriptador, en el plano de salida se obtiene un campo óptico dela forma:

$$d(x, y) = f(x, y)\, m(x, y) \otimes [k^{*}(-x, -y) \otimes k(x, y)] \quad (7)$$

La expresión se puede simplificar bajo la aproximación $k^{*}(-x, -y) \otimes k(x, y) \approx \delta(x, y)$ (**Unnikrishnan, *et al.,*** 1998), y por lo tanto la imagen desencriptada se puede expresar como

$$r(x, y) = f(x, y)\, m(x, y) \quad (8)$$

Como $m(x, y)$ es una máscara aleatoria de fase, la información del objeto de entrada se recupera al calcular la intensidad de la imagen desencriptada.

Se debe resaltar que a diferencia de otros sistemas de encriptación (**Javidi, *et al.,*** 1996; **Unnikrishnan, *et al.,*** 1998), cuando se usa un correlador de transformada conjunta no se requiere generar el complejo conjugado de la llave de seguridad, lo que representa una ventaja adicional de este sistema. Además, los sistemas ópticos de encriptación y desencriptación son compactos.

Resultados experimentales

En el montaje experimental se utiliza un modulador espacial de transmisión SLM Holoeye LC2002 con 800×600 pixeles de 32 μm para proyectar el objeto y la abertura cuadrada que limita el área de la llave de seguridad, un láser de Helio Neón (λ = 632.8 *nm*) como fuente de iluminación y una cámara CCD PULNIX TM6703 de 640×480 pixeles de área 9 μm × 9 μm (Figura 2) para almacenar la información procesada ópticamente. El tamaño del objeto y la llave es 1.92 *mm* × 1.92 *mm*, y la distancia entre el objeto y la llave es 2.6 *mm*. La lente empleada para generar el JPS tiene una longitud focal de 200 *mm* y las máscaras aleatorias de fase son generadas por medio de un difusor.

La Figura 4 presenta los resultados experimentales de los procesos de encriptación y desencriptación. Como objeto se eligió las letras JTC (Figura 4(a)), en la Figura 4(b) se presenta el dato encriptado (ecuación (4)), como era de esperarse la información encriptada es un patrón aleatorio debido al uso de las máscaras aleatorias de fase. Para recuperar la información original, el usuario autorizado ingresa el dato encriptado y la llave de recuperación al sistema desencriptador. La intensidad del campo óptico

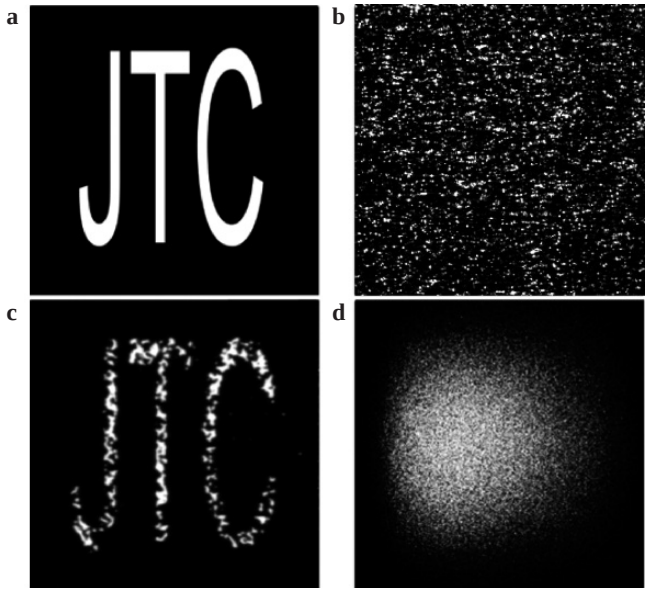

Figura 4. (a) Información original, (b) dato encriptado, (c) dato recuperado con la llave de seguridad correcta, y (d) dato desencriptado con una llave diferente a la empleada durante la encriptación.

a la salida del sistema permite recuperar la información original (Figura 4(c)). Por otro lado, si la información encriptada es interceptada por un intruso, no podrá acceder a la información del objeto si usa una llave diferente a la original (Figura 4(d)). Aunque la seguridad del proceso recae principalmente en la llave original, se debe tener en cuenta que los parámetros y grados de libertad del sistema óptico pueden verse como llaves extras de seguridad, por lo tanto para recuperar la información original un usuario también debe conocer la información de dichas llaves.

Como la imagen encriptada y la llave de recuperación son digitalizadas y posteriormente transmitidas, pueden estar sometidas a factores que alteran la información que contienen. Para simular la pérdida de información durante la transmisión, se hacen algunos píxeles, de la imagen encriptada y la llave de recuperación, simultánea y aleatoriamente iguales a cero en un porcentaje creciente, y se procede a evaluar la fidelidad de los datos recuperados. A cada una de las imágenes desencriptadas se le calcula el error cuadrático medio normalizado NMSE (siglas en ingles de normalized mean square error) definido como

$$NMSE = \frac{\sum_{i,j=1}^{N,M} |I'_{ij} - I_{ij}|^2}{\sum_{i,j=1}^{N,M} |I^{w}_{ij} - I_{ij}|^2} \quad (9)$$

donde $N \times M$ es el número total de píxeles de las imágenes, I'_{ij} representa la intensidad del píxel ij de cada imagen desencriptada cuando se pierde información, I^{w}_{ij} representa la imagen con la máxima pérdida y I_{ij} representa la imagen recuperada sin ninguna pérdida.

En la Figura 5 se presenta la gráfica del NMSE en función de la pérdida de información de la imagen encriptada y la llave de recuperación. En este caso, el porcentaje de pérdida es el mismo tanto para la llave como para el objeto encriptado, ya que se supone que la información es enviada por el mismo canal y por ello el ruido afecta los datos en igual porcentaje. Se puede notar que la correlación entre la imagen recuperada cuando no hay pérdida de información y las imágenes desencriptadas con pérdida, decrece a medida que la porcentaje de píxeles iguales a cero se incrementan sobre la imagen encriptada y la llave de desencriptación. Lo anterior implica que a medida que aumenta la pérdida, la calidad de la imagen desencriptada se reduce, lo cual se evidencia en la pérdida gradual sobre el dato recuperado y en un incremento del ruido que lo afecta. Cuando la pérdida de información es igual o superior al 50%, la imagen recuperada muestra una muy pobre correlación con la imagen original. Por lo tanto, a pesar de la degradación que presenta la imagen recuperada debido a la pérdida de información de la llave de seguridad y la imagen encriptada, se puede afirmar que el sistema de encriptación de doble máscara de fase basado en una arquitectura JTC es bastante tolerante a las pérdidas en la trasmisión de información.

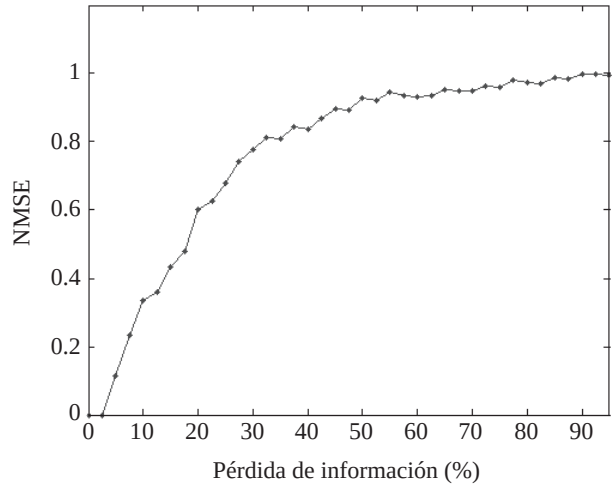

Figura 5. Curva que muestra la influencia de la pérdida de información en la llave de seguridad y el objeto encriptado sobre la imagen recuperada.

Conclusiones

En esta contribución se presenta la descripción teórica y la implementación experimental de un sistema de encriptación de doble máscara de fase en una arquitectura de transformada conjunta. El sistema de protección emplea una llave física, lo que garantizar un alto grado de seguridad. El análisis teórico y los resultados experimentales muestran que la información es recuperada satisfactoriamente cuando un usuario autorizado posee el dato encriptado y la llave de recuperación, de manera que el objeto no puede obtenerse bajo la interceptación del dato encriptado. Además, se muestra que el proceso de recuperación es tolerante a las pérdidas de la información transmitida en el proceso. Como comentario adicional debe mencionarse que hoy en día los computadores son básicamente sistemas electrónicos. Puede vislumbrarse en el futuro el desarrollo de computadoras ópticas (almacenamiento holográfico, interconectores ópticos no lineales, compuertas lógicas ópticas, etc.) y por ende la necesidad de proveer seguridad en el manejo de la información. En este contexto será de vital importancia profundizar las investigaciones en encriptación óptica de información.

Agradecimientos

Esta investigación fue llevada a cabo con el apoyo del Comité para el Desarrollo de la Investigación -CODI- (Universidad de Antioquia-Colombia), COLCIENCIAS (Colombia), Estrategia de Sostenibilidad 2014-2015 (Universidad de Antioquia-Colombia), MINCyT-COLCIENCIAS CO/13/05, CONICET Nos. 0863/09 y 0549/12 (Argentina), y la Facultad de Ingeniería, Universidad Nacional de La Plata No. 11/I168 (Argentina). John Fredy Barrera Ramírez agradece el apoyo

del Centro Internacional de Física Teórica (The International Centre for Theoretical Physics - ICTP) y la Academia Mundial de las Ciencias (The World Academy of Sciences - TWAS). Los autores agradecen la colaboración de Alexis Jaramillo (Instituto de Física, Universidad de Antioquia) por su ayuda en la realización de las experiencias que permitieron obtener los resultados presentados en este artículo.

Conflicto de intereses

Los autores del artículo declaramos que no existe conflicto de intereses con relación a la publicación de este artículo.

Referencias

Alfalou, A., Brosseau, C. 2009. Optical image compression and Optical image compression and encryption methods. Adv. Opt. Photon **1:** 589-636.

Barrera, J.F., Henao, R., Tebaldi, M., Torroba, R., Bolognini, N. 2006a. Multiplexing encryption-decryption via lateral shifting of a random phase mask. Opt. Commun. **259:** 532-536.

Barrera, J.F., Henao, R., Tebaldi, M., Torroba, R., Bolognini, N. 2006b. Multiplexing encrypted data by using polarized light. Opt. Commun. **260:** 109-112.

Barrera, J.F., Henao, R., Tebaldi, M., Torroba, R., Bolognini, N. 2006c. Multiple image encryption using an aperture-modulated optical system. Opt. Commun. **261:** 29-33.

Barrera, J.F., Tebaldi, M., Torroba, R., Bolognini, N. 2009. Multiplexing encryption technique by combining random amplitude and phase masks. Optik **120:** 351-355.

Barrera, J.F., Rueda, E., Ríos, C., Tebaldi, M., Bolognini, N., Torroba, R. 2011. Experimental opto-digital synthesis of encrypted sub-samples of an image to improve its decoded quality. Opt. Commun. **284:** 4350-4355.

Barrera, J.F., Torroba, R. 2010. One step multiplexing optical encryption. Opt. Commun. **283:** 1268-1272.

Barrera, J.F., Vargas, C., Tebaldi, M., Torroba, R., Bolognini, N. 2010. Known-plaintext attack on a joint transform correlator encrypting system. Opt. Lett. **35:** 3553-3555.

Bellare, M., Desai, A., Pointcheval, D., Rogaway, P. 1998. Relations Among Notions Security for Public-Key Encryption Schemes. Lecture Notes in Computer **1492:** 26-46.

Carnicer, A., Montes-Usategui, M., Arcos, S., Juvells, I. 2005. Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys. Opt. Lett. **30:** 1644-1646.

Camp-Winget, N., Housley, R., Wagner, D., Walker, J. 2003. Security flaws data links protocols. Communications of the ACM **46:** 35-39.

Graydon, O. 2013. Cryptography: Quick response codes, Nature Photonics **7:** 343**.**

Javidi, B., Zhang, G., Li, J. 1996. Experimental demonstration of the random phase encoding technique for image encryption and security verification. Opt. Eng. **35:** 2506-2512.

Javidi, B., Esmail, A., Zhang, G. (Abril 3, 2012). Optical security system using Fourier plane encoding. U.S. patent 8,150,033 B2.

Matoba, O., Javidi, B. 1999. Encrypted optical memory system using three-dimensional keys in the Fresnel domain. Opt. Lett. **24:** 762-764.

Nomura, T., Javidi B. 2000. Optical encryption using a joint transform correlator architecture. Opt. Eng. **39:** 2031-2035.

Nomura, T., Pérez-Cabré, E., Millán, M.S., Javidi, B. 2009. Optical Techniques for Information Security. Proc. IEEE **97:** 1128-1148.

Pile, D. 2010. Optical encryption: The ghost holds a secret. Nature Photonics **4:** 587.

Refregier, P., Javidi, B. 1995. Optical image encryption based on input plane and Fourier plane random encoding. Opt. Lett. **20:** 767-769.

Shannon, C. 1949. Communication Theory of Secrecy Systems. Bell Systems Technical Journal **28:** 656-715.

Situ, G., Zhang, J. 2004. Double random-phase encoding in the Fresnel domain. Opt. Lett. **29:** 1584-1586.

Situ, G., Zhang, J. 2005. Multiple-image encryption by wavelength multiplexing. Opt. Lett. **30:** 1306-1308.

Unnikrishnan, G., Joseph, J., Singh K. 1998. Optical encryption system that uses phase conjugation in a photorefractive crystal. Appl. Opt. **31:** 8181-8186.

Unnikrishnan, G.; Joseph, J.; Singh, K. 2000. Optical encryption by double-random phase encoding in the fractional Fourier domain. Opt. Lett. **25:** 887-889.

Wang, X., Zhao, D. 2012. Double images encryption method with resistance against the specific attack based on an asymmetric algorithm. Opt. Express **20:** 11994-12003.