Rev. Acad. Colomb. Cienc. Ex. Fis. Nat. 39(Supl.):48-54, 2015
doi: http://dx.doi.org/10.18257/raccefyn.259

Encriptación óptica de información con recuperación libre de ruido

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

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

Resumen

Los sistemas de protección de información basados en procesadores ópticos y que emplean una técnica de codificación de doble máscara aleatoria de fase permiten el manejo seguro de los datos, pero su recuperación no está libre de ruido. Si bien la seguridad del sistema es provista por el procesador óptico que habilita encriptar la información, en este trabajo se demuestra que la recuperación libre de ruido es posible mediante la inclusión de la codificación de respuesta rápida, sin alterar el proceso de protección de datos. La información que se desea proteger es previamente convertida en un código de respuesta rápida o código QR, y posteriormente el código es encriptado ópticamente. El código QR recuperado contendrá el ruido habitual producido por el uso de las máscaras aleatorias de fase y el procesamiento óptico-digital involucrado en el proceso. Finalmente, al escanear el código QR desencriptado se puede recuperar la información original completamente libre de ruido. Se incluye la descripción teórica del procesador óptico y se presentan resultados experimentales que demuestran la validez y aplicabilidad del sistema de protección.

Palabras clave: protección de información, procesadores ópticos, recuperación libre de ruido

Optical encryption with noise-free recovery

Abstract

The information protection systems based on optical processors, employing a double random phase mask encryption technique, allow data securely handling, but the recovery is not noise-free. Although the system security is provided by the optical processor enabling the information encoding, we demonstrate in this contribution that noise-free recovery is indeed possible by including the quick response coding, without altering the data protection process. The information to be protected is first converted into a quick response code or QR code, and then this code is optically encrypted. The decrypted QR code exhibits the usual noise produced by the random phase masks along with the involved opto-digital processing. Finally, when scanning the decrypted QR code we recover the original information without noise. We include the theoretical description of the optical processor, as well as we show experimental results that corroborate the validity and applicability of the security system.

Key words: information protection, optical processors, noise-free recovery.

Introducción

Los sistemas de seguridad tienen como objetivo asegurar la protección de la información (privacidad) y bienes (recursos) de los ciudadanos, instituciones y empresas. Estos sistemas ofrecen alternativas fiables para, por ejemplo, proteger las claves de seguridad que se usan para ingresar a las cuentas de correo electrónico, las cuentas en las redes sociales o para realizar pagos o transacciones electrónicas vía internet. Lo antes mencionado evidencia que la seguridad de la información ha entrado a formar un papel primordial en todos los ámbitos del quehacer diario de nuestra sociedad.

Los sistemas que permiten proteger la información, usualmente llamados "sistemas de encriptación" comercialmente disponibles, son algoritmos digitales. Pero se ha demostrado a lo largo del tiempo que los sistemas de seguridad digitales que en un momento se pensaron invulnerables, finalmente fueron quebrantados. A medida que los proveedores de seguridad generan nuevos sistemas digitales, en esa misma medida, otras personas trabajan en la búsqueda de una forma de vulnerar esos sistemas. Es por esto, que aunque se busca reforzar los sistemas de encriptación que se comercializan en la actualidad, basados en algoritmos digitales, el área de la seguridad en la información también busca alternativas que permitan aumentar la seguridad en el manejo de la información.

***Correspondencia:**
Roberto Daniel Torroba, robertot@ciop.unlp.edu.ar
Recibido: 7 de julio de 2015
Aceptado: 17 de septiembre de 2015

En este contexto, la encriptación óptica aparece como una atractiva y poderosa herramienta para el manejo seguro de la información, debido principalmente a su gran confiabilidad, su gran número de grados de libertad y su inherente capacidad de procesar en paralelo. Para encriptar información ópticamente los datos se introducen, en forma de haces luminosos, a un sistema óptico; el paso de dichos haces a través de uno o varios elementos logran transformarlos en un grado tal que la información obtenida a la salida del sistema no guarda ninguna semejanza con la original. No obstante, la información se encuentra allí codificada y sólo si se conocen todos los pasos del sistema y los elementos introducidos (llave(s) de encriptación y/o parámetro(s)), el proceso se puede revertir y los datos pueden ser recuperados. Los sistemas ópticos más seguros son los que usan llaves de fase aleatorias y físicas para proteger la información, pues hasta el momento han sido inmunes a cualquier tipo de ataque.

En los últimos 10 años se han llevado a cabo múltiples investigaciones que han demostrado que el área de protección de información usando procesadores ópticos tiene una gran potencialidad para aplicaciones prácticas (**Graydon,** 2013; **Treacy,** 2013; **Barrera, Vélez & Torroba,** 2013b; **Javidi,** 2003; **Gluckstad & Riso,** 2005; **Javidi & Tajahuerce**, 2007; **Javidi, Esmail & Zhang,** 2010). Se han desarrollado sistemas completamente ópticos, sistemas ópticos híbridos donde se utiliza un sistema óptico experimental para la encriptación y un sistema óptico virtual para la recuperación de la información, y sistemas ópticos virtuales para la protección de información (**Graydon,** 2013; **Treacy,** 2013; **Barrera, *et al.*,** 2013b; **Javidi,** 2003; **Gluckstad & Riso,** 2005; **Javidi & Tajahuerce,** 2007; **Javidi, *et al.*,** 2010; **Matoba & Javidi B.,** 1999; **Barrera, Henao, Tebaldi, Torroba & Bolognini,** 2006a; **Barrera, Henao, Tebaldi, Torroba & Bolognini,** 2006b; **Javidi, Towghi, Maghzi & Verrall,** 2000; **Vilardy, Millán & Peréz-Cabre,** 2013; **Barrera, Mira & Torroba,** 2013a; **Barrera, Mira & Torroba,** 2014a; **Barrera, Vélez & Torroba,** 2014b; **Lin, Shen & Li,** 2014; **Wang, Zhang, Liu, & Qin,** 2014; **Fan, *et al.*,** 2013; **Qin & Gong,** 2014; **Markman, Javidi & Tehramipoor,** 2014; **Carnicer, Hassanfiroozi, Latorre-Carmona, Huang, & Javidi,** 2015).

Los sistemas ópticos de encriptación virtuales, que son simulaciones computacionales de los sistemas experimentales, han demostrado su vulnerabilidad. Dicha vulnerabilidad es debida a que en general estos sistemas no contienen el mismo número de grados de libertad que los sistemas experimentales (polarización, longitud de onda, pupilas, etc) y a que las llaves de seguridad, aunque en algunos casos son aleatorias, por su naturaleza digital son diseñadas en un arreglo regular de píxeles de tamaño definido y donde los píxeles tienen un número limitado de variaciones de fase, características que hacen que los sistemas virtuales sean vulnerables a cierto tipo de ataques **(Carnicer, Montes-Usategui, Arcos & Juvells,** 2005; **Peng, Zhang, Wei & Yu,** 2006; **Barrera, Vargas, Tebaldi & Torroba,** 2010a; **Barrera, Vargas, Tebaldi, Torroba & Bolognini,** 2010b; **Zhang, Xiao, Wen & Liu,** 2013a; **Zhang, Liao, He & Peng,** 2013b). Asimismo, algunos sistemas experimentales usan llaves aleatorias generadas por medios digitales u óptico-digitales, características que también los hace vulnerables a pesar de contar con los grados de libertad de un procesador experimental.

En contraste con lo anterior, los sistemas ópticos de encriptación experimentales que usan como llave de seguridad un elemento físico y aleatorio presentan un alto grado de seguridad (**Graydon,** 2013; **Treacy,** 2013; **Barrera, *et al.*,** 2013b; **Javidi,** 2003; **Gluckstad & Riso,** 2005; **Javidi & Tajahuerce,** 2007; **Javidi, *et al.*,** 2010). Su gran confiabilidad se basa principalmente en la utilización de un difusor (vidrio despulido que es un elemento aleatorio y físico), ya que a este tipo de llaves no se le pueden definir parámetros como el tamaño de píxel o el número de píxeles, y no presentan un número definido y limitado de variaciones de fase. Además, los grados de libertad del sistema experimental pueden actuar como llaves de seguridad adicionales; se ha demostrado que longitud de onda (**Matoba & Javidi,** 1999), la pupila del sistema óptico (**Barrera, *et al.*,** 2006b) o la polarización (**Barrera, *et al.*,** 2006a) hacen las veces de llaves complementarias. Por lo tanto, para recuperar la información original un usuario autorizado deberá poseer la información de la llave aleatoria y física, y las llaves de seguridad adicionales, estas últimas permitiendo que la seguridad global del sistema se incremente. Las características de la llave física en conjunto con los grados de libertad de un procesador óptico experimental, han permitido que hasta ahora los sistemas experimentales de encriptación óptica no hayan sido vulnerados.

Con esta motivación, el desarrollo y la optimización de sistemas de protección basados en procesadores ópticos experimentales y que empleen elementos físicos y aleatorios como llaves de seguridad, han concentrado la atención de muchos grupos de investigación alrededor del mundo. Los cientos de artículos científicos publicados hasta el año 2012 en el área de la encriptación óptica evidenciaron una limitación que no permitía vislumbrar una aplicación real y masiva de los sistemas ópticos de encriptación (**Barrera, *et al.*,** 2013b; **Javidi,** 2003; **Gluckstad & Riso,** 2005; **Javidi & Tajahuerce,** 2007; **Javidi, *et al.*,** 2010; **Matoba & Javidi B.,** 1999; **Barrera, *et al.*,** 2006a; **Barrera, *et al.*,** 2006b; **Javidi, *et al.*,** 2000; **Vilardy, *et al.*,** 2013**)**. Dicha limitación era el ruido que afectaba los datos recuperados, y que paradójicamente es debido en su mayoría al elemento que le brinda la mayor parte de la seguridad al sistema, el elemento aleatorio y físico que actúa como llave de seguridad. Este ruido, se debe principalmente al límite de resolución natural de los procesadores ópticos que depende de las dimensiones físicas y las características de los elementos que lo componen.

Además, hay otras causas de ruido como la suciedad (polvo) y las fluctuaciones del índice de refracción a las que está expuesto un procesador óptico experimental, por mencionar dos de ellas.

Ya que los usuarios exigen sistemas de seguridad donde la información recuperada sea fiel a la original, se debía eliminar este ruido para que la encriptación por medio ópticos se pudiera vislumbrar como una alternativa viable. Con esta motivación, se han presentan algunas contribuciones donde se presentan métodos para reducir en cierta medida el ruido generado en los datos desencriptados, y aunque dichos métodos permiten obtener alguna disminución del ruido, ninguno de ellos permite eliminarlo completamente (**Javidi, *et al.,*** 2000; **Vilardy, *et al.,*** 2013).

Teniendo como marco de referencia lo antes mencionado, para sobrepasar esa gran limitación se integraron un sistema óptico de encriptación de doble máscara de fase en una arquitectura 4f y la codificación de gráfica, logrando por primera vez recuperar los datos sin ningún tipo de ruido (**Barrera, *et al.,*** 2013a). En esta demostración, la información que se pretende proteger se convierte en un código de respuesta rápida (CRR), conocido ampliamente como código QR (*en inglés quick response code o QR code*). Por lo tanto, en lugar de encriptarse el dato original, se encripta su respectivo código QR. Si un usuario autorizado posee el código encriptado y la(s) llave(s) de seguridad, usando el sistema de desencriptación podrá acceder al código desencriptado, el cuál presentará el ruido convencional. Finalmente, el código QR desencriptado es decodificado para recuperar la información original libre de ruido. En este contexto, la codificación y decodificación de respuesta rápida es la principal responsable de la ausencia de ruido, mientras que el procesador óptico es el principal responsable de la seguridad del proceso (**Graydon,** 2013; **Treacy,** 2013; **Barrera, *et al.,*** 2013a).

Aunque en esta propuesta los procesos de encriptación y recuperación de la información fueron llevados a cabo por medio de sistemas óptico virtuales **(Barrera, *et al.,*** 2013a**)**; esta contribución despertó el interés de la comunidad internacional especializada gracias a que soluciona un problema fundamental para la adopción práctica de sistemas de protección basados en procesadores ópticos, y a que usa herramientas tecnológicas ampliamente disponibles y con un gran rango de aplicaciones como los códigos QR **(Graydon,** 2013; **Treacy,** 2013; **Barrera, *et al.,*** 2013b**, Barrera, *et al.,*** 2013a; **ISO, IEC 18004,** 2006; **Liao & Lee,** 2010). Estos códigos pueden ser escaneados con teléfonos inteligentes o tabletas usando programas gratuitos y ampliamente usados **(Graydon,** 2013; **Treacy,** 2013; **ISO, IEC 18004,** 2006; **Liao & Lee,** 2010).

Teniendo como motivación el impacto de la contribución **(Graydon,** 2013; **Treacy,** 2013; **Barrera, *et al.,*** 2013a), se presentó la primera demostración experimental de un sistema de protección de información que usa un procesador óptico experimental y permite la recuperación libre de ruido (**Barrera, *et al.,*** 2014a). Esta primera implementación mediante un sistema óptico virtual y su posterior demostración experimental, representaron el inicio de una nueva línea de investigación en lo que respecta a la protección de información por medios ópticos y con una recuperación libre de ruido (**Barrera, *et al.,*** 2014b; **Lin, *et al.,*** 2014; **Wang, *et al.,*** 2014; **Fan, *et al.,*** 2013; **Qin & Gong,** 2014). Además, se ha expandido esta propuesta a procesos de validación por medios ópticos (**Markman, *et al.,*** 2014; **Carnicer, *et al.,*** 2015).

Lograr una recuperación libre de ruido revitalizó el área de los sistemas ópticos de seguridad, con base en la propuesta original (**Barrera, *et al.,*** 2013a) y su posterior implementación experimental (**Barrera, *et al.,*** 2014a), impulsando un grupo de contribuciones basadas en sistemas virtuales (**Lin, *et al.,*** 2014; **Wang, *et al.,*** 2014; **Fan, *et al.,*** 2013; **Qin & Gong,** 2014; **Markman, *et al.,*** 2014; **Carnicer, *et al.,*** 2015). Adicionalmente, se presentaron dos técnicas que permitieron reforzar la encriptación óptica que emplea códigos QR (**Barrera, *et al.,*** 2014b), una de ellas consiste en cambiar de posición de los elementos que componen el código QR aumentando la seguridad del proceso. Además, se implementa una técnica de normalización no lineal que permite reducir el ruido sobre los códigos recuperados e incrementa la seguridad contra ataques (**Vilardy, *et al.,*** 2013; **Barrera, *et al.,*** 2014a). Otras investigaciones incluyen llaves multidimensionales (**Lin, *et al.,*** 2014**),** procedimientos de recuperación de fase (**Wang, *et al.,*** 2014; **Fan, *et al.,*** 2013), superposición incoherente (**Qin & Gong,** 2014), y validación óptica (**Markman, *et al.,*** 2014; **Carnicer, *et al.,*** 2015).

De acuerdo a todo lo expuesto, es evidente que el estudio, desarrollo y optimización de sistemas ópticos de protección es de gran importancia para la comunidad científica debido a sus grandes implicaciones académicas y tecnológicas (**Graydon,** 2013; **Treacy,** 2013; **Barrera, *et al.,*** 2013b). Dichos sistemas deben incluir métodos que permitan la recuperación de la información libre de ruido, un procesador óptico experimental con una llave de seguridad física y aleatoria y un sistema óptico virtual de recuperación; todo lo anterior para garantizar un sistema de protección seguro, práctico y versátil.

En esta contribución se presentará la descripción teórica del sistema de seguridad y su implementación experimental. Se incluirán resultados experimentales que permitirán comparar los datos recuperados con el método convencional y la recuperación libre de ruido al incluir los códigos de respuesta rápida.

Descripción del sistema de seguridad

El primer paso para lograr la encriptación óptica de datos y su recuperación libre de ruido es la conversión de la

información que se pretende proteger en un código QR. Luego, este código es insertado en el plano de entrada del sistema de encriptación y en el plano de salida se produce el código QR encriptado. El proceso de recuperación posee dos etapas, la desencriptación del código QR y su lectura para obtener la información original libre de ruido.

Aunque existen muchas arquitecturas disponibles para implementar el sistema de codificación de doble máscara de fase (**Javidi,** 2003; **Gluckstad & Riso,** 2005; **Javidi & Tajahuerce,** 2007; **Barrera, *et al.*,** 2013a) se eligió la arquitectura óptica de encriptación JTC (por las siglas en ingles de joint transform correlator) debido a que la encriptación y la recuperación de la información se llevan a cabo utilizando procesadores ópticos compactos (**Barrera, Vélez & Torroba,** 2013c).

El montaje experimental es un interferómetro Mach-Zehnder que en un brazo contiene el sistema encriptador JTC y en el otro un haz de referencia (Figura 1). Para encriptar el código QR se bloquea el brazo de referencia, de manera que solo se ilumina el procesador JTC. El sistema de encriptación contiene un modulador espacial de luz SLM (por las siglas en inglés de spatial light modulator) donde se proyecta el código correspondiente a la información que se desea proteger y una abertura cuadrada que limitará el tamaño de la llave de seguridad (Figura 1). Al poner en contacto el SLM con un difusor se obtiene la transmitancia del plano de entrada del sistema encriptador. En una de las ventanas del JTC se obtiene el producto $\rho(x, y) = o(x, y)\, r(x, y)$ entre el código QR y una máscara aleatoria y física $r(x, y)$, está máscara aleatoria corresponde a la porción del difusor que está en contacto con el código. La otra ventana contiene la llave de seguridad $l(x, y)$, que es la porción del difusor limitada por la abertura cuadrada proyectada en el modulador. Cuando el sistema de encriptación se ilumina con una onda plana y monocromática, la lente L genera la transformada de Fourier de la transmitancia del plano de entrada en el plano de la cámara CCD, y en ese plano se registra su JPS (por las siglas en inglés de joint power spectrum), indicado por $J(v, w)$ (**Barrera, *et al.*,** 2013c),

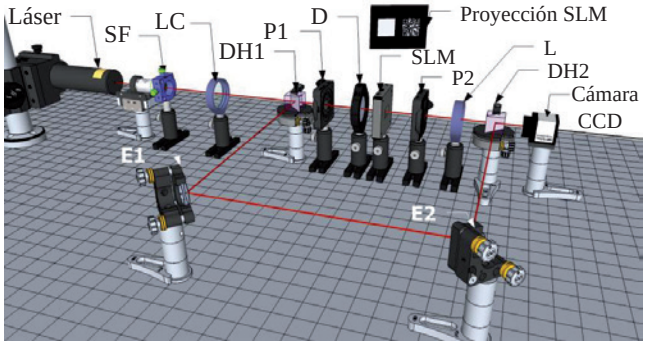

Figura 1. Montaje experimental: SF: Sistema de filtrado; LC: lente colimadora; DH: divisor de haz; P: polarizador; D: Difusor; SLM: modulador espacial de luz; L: lente; E: espejos.

$$J(v, w) = |C(v, w)|^2 + |L(v, w)|^2 + C(v, w)\, L^*(v, w)e^{-4\pi ibv} + C^*(v, w)\, L(v, w)e^{4\pi ibv} \quad (1)$$

donde $C(v, w)$ and $L(v, w)$ son las transformadas de Fourier de $\rho(x, y)$ y $l(x, y)$ respectivamente, $2b$ es la separación entre la ventana que contiene el código QR y la ventana de la llave y * representa la operación complejo conjugado. El tercer y el cuarto término del JPS contienen la información del código encriptado y su complejo conjugado. Por lo tanto al filtrar el primer, segundo y cuarto término del JPS, y al reposicionar el tercer término se obtiene el código encriptado $E(v, w)$ centrado en las coordenadas (0, 0) (**Barrera, *et al.*,** 2013c),

$$E(v, w) = C(v, w)\, L^*(v, w) \quad (2)$$

El paso siguiente es registrar la información de la llave de seguridad desbloqueando el brazo de referencia y bloqueando el objeto. De esta forma se almacena el interferograma de la transformada de Fourier de la llave de seguridad por medio de la cámara CCD (Figura 1). Aplicando un procedimiento similar al utilizado para obtener el código encriptado y centrado por medio del JPS, luego de procesar el interferograma se llega a la transformada de Fourier de la llave de seguridad $L(v, w)$.

El proceso de recuperación consta de dos etapas, en la primera el código QR encriptado y la información de la transformada de Fourier de la llave de seguridad se insertan en el plano de entrada de un procesador óptico 2f (Figura 2). Cuando el procesador óptico es iluminado con una onda plana y monocromática, realiza la operación transformada de Fourier sobre la transmitancia del plano de entrada, de esta manera en el plano de salida del sistema se obtiene,

$$d(x, y) = o(x, y)\, r(x, y) \quad (3)$$

Esta ecuación representa el producto entre el código QR $o(x, y)$ y la máscara $r(x, y)$. Por lo tanto, la intensidad del campo óptico a la salida del procesador 2f brinda la información del código QR, el cual presenta el ruido típico generado por los procesos de encriptación y desencriptación. Se debe tener en cuenta que para recuperar el código QR es absolutamente necesario poseer su par encriptado y la información de seguridad; si un usuario no autorizado intercepta el código encriptado, pero no puede acceder a la llave de seguridad, dicho usuario no podrá acceder a la información de dicho código.

En la etapa final del proceso de recuperación, al escanear el código QR desencriptado se accede a la información original totalmente libre de ruido. Lo anterior es posible debido a la tolerancia al ruido característica del proceso de lectura de los códigos de respuesta rápida (**ISO, IEC 18004,** 2006; **Liao & Lee,** 2010). De acuerdo a lo anterior, la seguridad del sistema y la recuperación libre de ruido se debe a la acción combinada del sistema óptico de seguridad y de los códigos gráficos. Un atractivo adicional de este

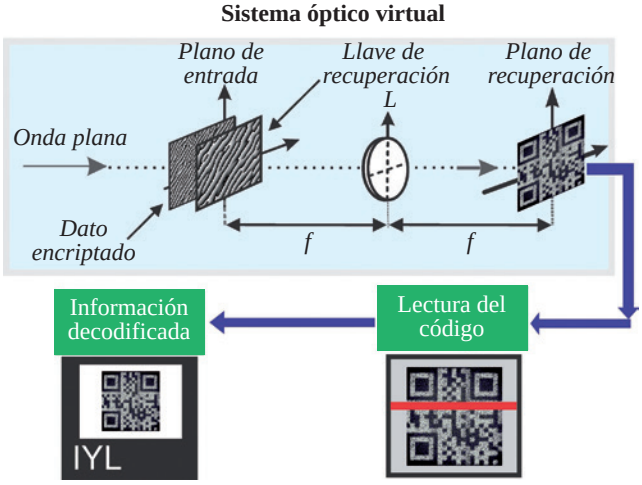

Figura 2. Sistema óptico virtual de recuperación.

procedimiento, es que los códigos QR pueden ser leídos por dispositivos que actualmente son de uso masivo y están ampliamente disponibles, como los smartphones o las tablets (**Graydon,** 2013).

Como se ha explicado ampliamente, la seguridad del sistema de protección de datos se basa principalmente en la utilización de un procesador óptico experimental para la encriptación de la información. Por lo tanto, existen dos opciones para el desarrollo del sistema de recuperación; la primera opción es contar con un sistema óptico experimental de recuperación, mientras que la segunda es la puesta a punto de un sistema óptico virtual. En esta contribución se elige la segunda opción pues es la más desarrollada, aceptada e investigada ya que es práctica y versátil, donde los usuarios del sistema no requieren de un montaje óptico experimental para recobrar la información.

Resultados experimentales

En el montaje experimental se emplea como fuente de iluminación un láser de Helio Neón (λ = 632.8 *nm*) y como medio de registro una cámara CCD PULNIX TM6703 de 640 × 480 pixeles de área $9\mu m \times 9\mu m$ (Figura 1). El objeto y la ventana de la llave son proyectadas en un SLM Holoeye LC2002, el tamaño del objeto y la llave es 1.92 *mm* × 1.92 *mm*, y la distancia entre el objeto y la llave es 3.84 *mm*. Las máscaras aleatorias de seguridad son generadas por medio de un difusor y la lente empleada para generar el JPS tiene una longitud focal de 200 *mm*.

En la figura 3 se pueden observar los resultados experimentales obtenidos con el sistema óptico-virtual descrito en la sección 2, pero usando el método convencional de encriptación, es decir, sin incluir la códigos QR. En este caso la información que se desea proteger corresponde al texto *IYL*, que son las iniciales del año internacional de la luz (por las siglas en ingles de *International Year of Light*) (Figura 3(a)). La Figura 3(b) es el resultado experimental del proceso de encriptación, como se puede apreciar es un patrón aleatorio ya que se está empleando una técnica de codificación de doble máscara de fase. En el proceso de recuperación, el código encriptado y la llave de seguridad se ubican en el plano de entrada del procesador 2f (Figura 2), de manera que en el plano de salida aparece el código desencriptado (Figura 3(c)). Como era de esperarse, si en la recuperación se utiliza una llave diferente a la asociada al proceso de encriptación, el dato desencriptado es un patrón aleatorio, es decir que el código no se puede recuperar (Figura 3(d)). Evidentemente, la información recuperada con el método convencional contiene el ruido habitual de los sistemas óptico-digitales que usan máscaras aleatorias de fase (Figura 3(c)).

En esta propuesta, para eliminar el ruido presente en los datos recuperados se combinará el procedimiento convencional con la codificación de respuesta rápida. En lugar de proyectar el texto que se desea proteger en el sistema de encriptación, se proyecta su correspondiente código QR (Figuras 1 y 4(a)) y se obtiene el correspondiente código encriptado (Ecuación (2)-Figura 4(b)). Como es de esperarse, tanto en el sistema convencional (Figuras 3(b) y 3(d)) como en la propuesta actual (Figuras 4(b) y 4(c)), los datos encriptados y los recuperados con una llave incorrecta son patrones aleatorios, hecho en el cual se basa la seguridad del método. La figura 4(d) muestra el código recuperado apropiadamente, en el cual puede reconocerse el código QR a pesar del ruido. Finalmente, al escanear el código desencriptado con un teléfono inteligente se puede acceder al texto original sin ningún tipo de ruido o distorsión (Figura 4(e)).

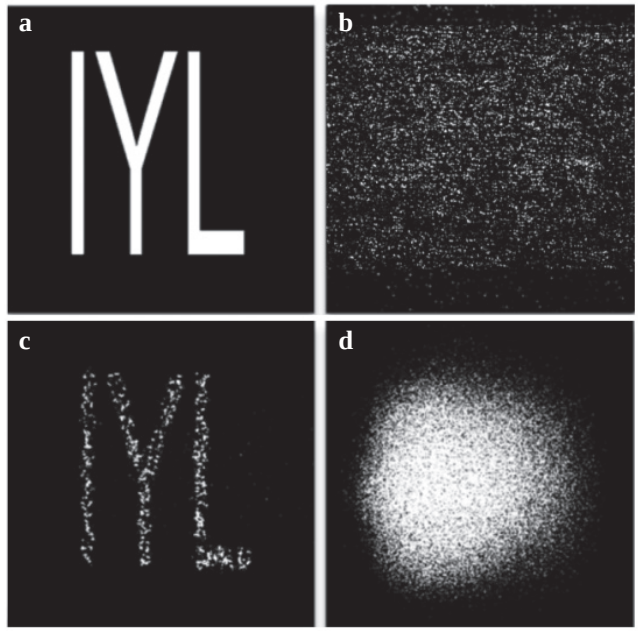

Figura 3. (a) Objeto original, (b) objeto encriptado, desencriptación con: (c) la llave de seguridad correcta y (d) otra llave.

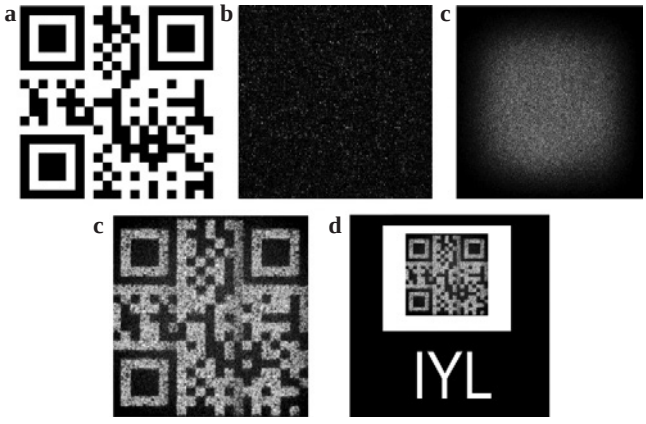

Figura 4. (a) Código QR del texto "IYL", (b) código QR encriptado, (c) recuperación usando una llave diferente a la original, (d) desencriptación con la llave de seguridad, y (e) lectura del código QR recuperado usando un teléfono inteligente.

Conclusiones

La descripción teórica y los resultados experimentales demuestran que es posible manipular información de manera segura empleando un procesador óptico y una técnica experimental de codificación de doble máscara de fase. Además, la combinación entre los sistemas ópticos de encriptación convencionales y la codificación de respuesta rápida permite la protección de información y a su vez una recuperación completamente libre de cualquier tipo de ruido o deterioro. Este avance permite revitalizar las investigaciones en el área de los sistemas de seguridad basados en procesadores ópticos, es evidente que esta área está más vigente que nunca y que se han abierto nuevos interrogantes que conducirán a futuras aplicaciones.

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, 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 apoyo en la realización de las experiencias que permitieron obtener los resultados experimentales 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

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

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

Barrera, J. F., Vargas, C., Tebaldi, M., Torroba, R. 2010a. Chosen-plaintext attack on a joint transform correlator encrypting system. Opt. Commun. **283:** 3917-3921.

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

Barrera, J.F., Mira, A., Torroba, R. 2013a. Optical encryption and QR codes: Secure and noise-free information retrieval. Opt. Express **21:** 5373-5378.

Barrera, J.F., Vélez, A., Torroba, R. (Agosto, 2013)b. Information security through light: Protecting information with optical processors. Sección Labtalk, J. Opt. Recuperado de http://iopscience.iop.org/2040-8986/labtalk-article/54457.

Barrera, J.F., Vélez, A., Torroba, R. 2013c. Experimental multiplexing protocol to encrypt messages of any length. Journal of Optics **15:** 055404.

Barrera, J.F., Mira, A., Torroba, R. 2014a. Experimental QR code optical encryption: noise-free data recovering. Opt. Lett. **39:** 3074-3077.

Barrera, J.F., Vélez, A., Torroba R. 2014b. Experimental scrambling and noise reduction applied to the optical encryption of QR codes. Opt. Express. **22:** 20268-20277.

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

Carnicer, A., Hassanfiroozi, A., Latorre-Carmona, P. Huang, Y. P., Javidi B. 2015. Security authentication using phase-encoded nanoparticle structures and polarized light. Opt. Lett. **40:** 135-138.

Fan, D., Meng, X., Wang, Y., Yang, X., Peng, X., He, W., Dong, G., Chen, H. 2013. Optical identity authentication scheme based on elliptic curve digital signature algorithm and phase retrieval algorithm. Appl. Opt. **52:** 5645-5652.

Gluckstad, G., Riso F. (Junio 14, 2005). Optical encryption and decryption method and system. U.S. patent 6907124.

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

ISO, IEC 18004. 2006. Information technology - Automatic identification and data capture techniques – QR Code 2005 bar code symbology specification. International Organization for Standardization, Geneva, Switzerland.

Javidi, B., Towghi, N., Maghzi, N., Verrall S. C. 2000. Error-reduction techniques and error analysis for fully phase- and amplitude-based encryption. Appl. Opt. **39:** 4117-4130.

Javidi, B. (Febrero, 2003). Method and Apparatus for Encryption Using Partial Information. U.S. Patent Number 6519340 B1.

Javidi, B., Tajahuerce, E. (Mayo 22, 2007). Information security using digital holography. U.S. patent 7221760 B2.

Javidi, B., Esmail, A., Zhang, G. (Marzo 23, 2010). Optical Security system using Fourier plane encoding. U.S. patent 7684098.

Liao, K. C., Lee, W. H. 2010. A novel user authentication scheme based on QR-Code. J. Netw. **5:** 937-941.

Lin, C., Shen, X., Li, B. 2014. Four-dimensional key design in amplitude, phase, polarization and distance for optical encryption based on polarization digital holography and QR code. Opt. Express **22:** 20727-20739.

Markman, A., Javidi, B., Tehramipoor, M. 2014. Photon-counting security tagging and verification using optically encoded QR codes. IEEE Photonics Journal **6:** 6800609.

Matoba, O., Javidi, B. 1999. Encrypted optical storage with wavelength-key and random phase codes. Appl. Opt **38:** 6785-6790.

Peng, X., Zhang, P., Wei, H., Yu B. 2006. Known-plaintext attack on optical encryption based on double random phase keys. Opt. Lett. **31:** 1044-1046.

Qin, Y., Gong, Q. 2014. Optical information encryption based on incoherent superposition with the help of the QR code. Opt. Commun. **310:** 69-74.

Treacy, S. (agosto de 2013). The creative power of Colaboration. The world Academy of Sciences TWAS. Recuperado de http://twas-old.ictp.it/news-in-home-page/news/the-creative-power-of-collaboration.

Vilardy, J. M., Millán, M. S., Peréz-Cabre, E. 2013. Improved decryption quality and security of a joint transform correlator-based encryption system. J. Opt. **15:** 025401.

Wang, Z., Zhang, S., Liu, H., Qin, Y. 2014. Single-intensity-recording optical encryption technique based on phase retrieval algoritm and QR code. Opt. Commun. **332:** 36-41.

Zhang, Y., Xiao, D., Wen, W., Liu, H. 2013a. Vulnerability to chosen-plaintext attack of a general optical encryption model with the architecture of scrambling-then-double random phase encoding. Opt. Lett. **38:** 4506-4508.

Zhang, C., Liao, M., He, W., Peng, X. 2013b. Ciphertext-only attack on a joint transform correlator encryption system. Opt. Express **21:** 28523-28530.