Rev. Acad. Colomb. Cienc. Ex. Fis. Nat. 46(178):68-89, enero-marzo de 2022
doi: https://doi.org/10.18257/raccefyn.1597

Artículo de revisión

Encriptación de información mediante procesamiento óptico

Information encryption using optical processing

John Fredy Barrera-Ramírez

Grupo de Óptica y Fotónica, Instituto de Física, Facultad de Ciencias Exactas y Naturales, Universidad de Antioquia, Medellín, Colombia

Artículo de posesión como miembro correspondiente de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales

Resumen

En esta contribución se discuten los avances más significativos en el campo de la encriptación de información mediante procesamiento óptico con énfasis en los adelantos en la reducción y la eliminación del ruido. Se hace la descripción teórica de un sistema de encriptación compacto y se presentan los resultados de su implementación experimental. Además, se demuestra que la inclusión de contenedores de información personalizados permite la protección de la información y su recuperación libre de ruido, evidenciando el potencial del sistema de seguridad compacto. Por último, se presentan las perspectivas en el área de investigación.

Palabras clave: Encriptación de información; Procesamiento óptico; Protección de datos; Recuperación libre de ruido.

Abstract

In this contribution, the most significant advances in the area of information encryption using optical processing are discussed with an emphasis on advances in noise reduction and elimination. The theoretical description of a compact encryption system and the results of its experimental implementation are presented. Additionally, the inclusion of personalized information containers to protect information and retrieve it free of noise is also explained evidencing the potential of the compact security system. Finally, the perspectives of the research area are presented.

Keywords: Information encryption; Optical processing; Data protection; Noise-free retrieval.

Introducción

El estudio de las propiedades de la luz y de la forma en que puede manipularse la información mediante su uso es una de las áreas de investigación con grandes avances en los últimos años, impulsados por el gran interés científico que suscita y por sus aplicaciones tecnológicas que han permitido mejorar la calidad de vida de la sociedad actual y que, según las previsiones, ayudará a solucionar algunos de los problemas tecnológicos, sociales, económicos y ambientales avizorados para los próximos años. El avance en esta área ha tenido un impacto notable en temas como las energías nuevas y renovables, el desarrollo sostenible, la innovación industrial, la salud y la seguridad, entre otros. En cuanto al manejo seguro de la información específicamente, ha habido un desarrollo significativo de los protocolos y sistemas que garantizan la protección de la privacidad y los recursos de los ciudadanos, instituciones y empresas, lo que es de gran importancia dada la creciente cantidad de información privada que se intercambia.

Conforme aumenta el uso de los sistemas digitales y electrónicos en diversos ámbitos, también se han incrementado los crímenes relacionados. Solo en el 2017, los distintos tipos de 'cibercrímenes' representaron el 15 % de todos los delitos cometidos contra compañías en Colombia, generando un daño económico cercano a los 600 millones de

Citación: Barrera-Ramírez JF. Encriptación de información mediante procesamiento óptico. Rev. Acad. Colomb. Cienc. Ex. Fis. Nat. 46(178):68-89, enero-marzo de 2022. doi: https://doi.org/10.18257/raccefyn.1597

Editor: Román Eduardo Castañeda-Sepúlveda

Correspondencia:
John Fredy Barrera Ramírez;
john.barrera@udea.edu.co

Recibido: 11 de noviembre de 2021
Aceptado: 14 de marzo de 2022
Publicado: 23 de marzo de 2022

dólares (**Hernández, *et al*.,** 2018). Con el objetivo de evitarlos, en el primer trimestre del 2020 la inversión total en ciberseguridad en Colombia alcanzó los 10.400 millones de dólares (**Asociación Colombiana de Ingenieros de Sistemas-ACIS,** 2020) y es previsible que, a medida que aumente la actividad económica relacionada con los servicios digitales, mayor será el incentivo de los criminales para atacar las entidades que los proveen. Dada la necesidad de protección contra este tipo de crímenes, en los próximos años el mercado de la protección de datos resulta prometedor. En este sentido, vale la pena mencionar que el mercado del *software* de encriptación global en el 2020 se valoró en 8.49 billones de dólares y se proyecta que alcance los 59.5 billones de dólares en el 2028, con un incremento anual compuesto del 27,57 % entre el 2021 y 2028 (**Verified Market Research-VMR,** 2021).

Entre los principales sectores de aplicación de los sistemas de protección de información se pueden mencionar el financiero y el bancario, por su interés en la custodia de la información y las transacciones; el sector de la salud, por la necesidad de garantizar la seguridad de las imágenes de uso médico como las tomografías computarizadas, las imágenes de resonancia magnética o por ultrasonido y las tomografías de emisión de positrones, con el fin de ofrecer a los pacientes la confidencialidad, la integridad y la autenticación necesarias (**Lima, *et al*.,** 2015); el sector industrial y comercial, por las aplicaciones en tecnologías de autenticación de productos y contra las falsificaciones (hologramas, impresión de seguridad, etiquetas de seguridad, biometría, y mecanismos de identificación de productos originales, entre otros) mediante la detección óptica y la identificación de características de seguridad (**Kwok, *et al*.,** 2010); en el área de los bienes de lujo, por la necesidad de tecnologías de autenticación de bienes de alto valor y contra las falsificaciones (**Jiao, *et al*.,** 2019; **Ting, *et al*.,** 2013); en el sector gubernamental, por los requerimientos de mecanismos de seguridad para los programas del gobierno en la nube (pasaportes, información privada de los ciudadanos, registradurías y notarías, y aplicaciones, registros, e imágenes de terrenos y propiedades, entre otros); en la industria del entretenimiento para la adición de imágenes encriptadas en el contenido audiovisual y la recuperación de la información con contenido sobre titulares de derechos, y, por último, en el sector militar y de las fuerzas armadas del estado, y en el comercio electrónico.

En este contexto, la encriptación de la información mediante procesamiento óptico se presenta como una herramienta poderosa para la protección de datos (**Alfalou,** 2018; **Alfalou & Brosseau,** 2009; **Ambs,** 2010; **Carnicer & Javidi,** 2017; **Chen, *et al*.,** 2014; **Graydon,** 2013; **Javidi, *et al*.,** 2016; **Li, *et al*.,** 2017a; **Liang, *et al*.,** 2015; **Lim, *et al*.,** 2019; **Liu, *et al*.,** 2014; **Nomura, *et al*.,** 2009; **Paganin,** 2011; **Pile,** 2010; **Qu, *et al*.,** 2020; **Treacy,** 2013; **Zhu, *et al*.,** 2021), ya que los sistemas de encriptación de *software* (algoritmos digitales) (**Kaur, *et al*.,** 2021) y *hardware* (dispositivos electrónicos) comercialmente disponibles, que en un principio se pensaron invulnerables, ya pueden quebrantarse (**Karimi, *et al*.,** 2021; **Lázaro, *et al*.,** 2021; **Mughaid, *et al*.,** 2021). Los sistemas de protección basados en el procesamiento óptico han demostrado su potencialidad, versatilidad y aplicabilidad principalmente por su capacidad inherente de procesar en paralelo y la gran confiabilidad de sus grados de libertad, así como el uso de llaves de seguridad físicas en lugar de llaves digitales (**Barrera-Ramírez, *et al*.,** 2015a; **Gluckstad & Riso,** 2005; **Javidi,** 2003; **Javidi, *et al*.,** 2010; **Javidi & Tajahuerce,** 2007; **Wang & Schipf,** 2019a).

La codificación de información por medio de sistemas ópticos fue propuesta en 1975 (**Françon,** 1975), cuando se sugirió codificar un mensaje mediante los cambios aleatorios de fase producidos por un difusor, el cual permitiría codificar la información y, a su vez, extraer el mensaje codificado. Así, el difusor actuaría como llave de codificación y decodificación. Una década más tarde, e independientemente de esta primera propuesta, se implementó una técnica de codificación de información usando distribuciones aleatorias (**Kafri & Keren,** 1987) y se recurrió por primera vez a la palabra "encriptación" para describir la codificación de datos en el contexto de la óptica.

Rev. Acad. Colomb. Cienc. Ex. Fis. Nat. 46(178):68-89, enero-marzo de 2022
doi: https://doi.org/10.18257/raccefyn.1597

Más tarde, en lo que constituyó un trabajo pionero, se propuso un método de encriptación de datos usando una arquitectura óptica 4f y dos máscaras aleatorias de fase (**Refregier & Javidi,** 1995). Dicha arquitectura se había usado hasta ese momento para el procesamiento óptico de información, particularmente para correlacionar dos funciones (**Goodman,** 1996; **Vander-Lugt,** 1964), con el fin de detectar, localizar e identificar la presencia de un objeto de interés (**Millán,** 2012), pero en el contexto de la encriptación óptica el objetivo es la protección de la información. En este método de encriptación (**Refregier & Javidi,** 1995) una de las máscaras se ubica en el plano de entrada, en contacto con el dato que se desea proteger, en tanto que la segunda máscara se ubica en el primer plano de Fourier del sistema 4f. Esta propuesta se pudo comprobar mediante simulaciones computacionales y, posteriormente, se hizo la primera implementación experimental, registrando la imagen encriptada en una película holográfica (**Javidi, *et al.*,** 1996). Para solucionar las desventajas de esa primera implementación, se presentó una segunda demostración experimental que incluyó un cristal fotorrefractivo como medio de registro (**Unnikrishnan, *et al.*,** 1998).

La propuesta e implementación experimental de este trabajo pionero incentivaron el surgimiento de una nueva línea de investigación, la encriptación óptica. Desde ese momento y, hasta la fecha, esta nueva línea ha dado lugar a múltiples investigaciones cuyos resultados han permitido un gran número de interesantes desarrollos, demostrando la gran confiabilidad y versatilidad de los sistemas ópticos de encriptación (**Alfalou & Brosseau,** 2009; **Carnicer & Javidi,** 2017; **Chen, *et al*.,** 2014; 2009; **Graydon,** 2013; **Javidi, *et al*.,** 2016; **Li, *et al*.,** 2017a; **Liang, *et al*.,** 2015; **Lim, *et al*.,** 2019; **Liu, *et al*.,** 2014, **Nomura, *et al*.,** 2009; **Paganin,** 2011; **Pile,** 2010; **Qu, *et al*.,** 2020; **Treacy,** 2013; **Zhu, *et al*.,** 2021). Los sistemas ópticos de encriptación más desarrollados, los cuales tienen más variantes y han demostrado ser más seguros y tener mayor potencial para aplicaciones prácticas, son los que emplean dos máscaras aleatorias de fase, por lo que usualmente reciben el nombre de sistemas de codificación de doble máscara de fase (**Barrera-Ramírez, *et al.*,** 2006a; **Javidi, *et al.*,** 1996; **Refregier & Javidi,** 1995).

Es importante tener en cuenta que la mayoría de las propuestas de sistemas ópticos de encriptación publicadas en revistas científicas son virtuales, es decir, simulaciones computacionales que buscan replicar las condiciones físicas de un sistema experimental. A pesar de dichas comprobaciones, se ha demostrado que bajo ciertas condiciones estos sistemas son vulnerables (**Barrera-Ramírez, *et al.,*** 2010a; **Barrera-Ramírez, *et al.,*** 2010b; **Peng, *et al.,*** 2006). Por su parte, los procesadores ópticos experimentales que tienen como llave de seguridad un elemento físico y aleatorio tienen un alto grado de seguridad (**Barrera-Ramírez, *et al.,*** 2006a; **Barrera-Ramírez, *et al.,*** 2006b; **Barrera-Ramírez, *et al.,*** 2006c; **Jaramillo, *et al.*,** 2020a; **Unnikrishnan, *et al.,*** 1998; **Velez-Zea,** 2016a). Su gran confiabilidad se debe, principalmente, a que las propiedades físicas de la llave la hacen única y los grados de libertad del sistema permiten aumentar su seguridad.

Algunos sistemas ópticos no solo han demostrado ser muy seguros, sino que también pueden proteger adecuadamente un gran rango de información: información bidimensional y binaria (**Velez-Zea, *et al.*,** 2016b), información bidimensional en tonos de gris (**Tanha, *et al.*,** 2012) y estructurada (**Velez-Zea, *et al.*,** 2017a), e información de objetos tridimensionales (**Velez-Zea, *et al.,*** 2016a) y a color (**Tanha, *et al.*,** 2012; **Tebaldi, *et al.*,** 2011; **Velez-Zea, *et al.*,** 2019).

Además, en la literatura especializada se pueden encontrar muchas contribuciones que proponen diferentes sistemas ópticos para llevar a cabo procesos de protección de datos, entre las que se destacan los que usan la arquitectura 4f (**Barrera-Ramírez, *et al.*,** 2005a; **Barrera-Ramírez, *et al.*,** 2005b; **Javidi, *et al.*,** 1996; **Mosso, *et al.*,** 2011a), los de correlador de transformada conjunta (*joint transform correlator*, JTC) en el dominio de Fourier (**Nomura & Javidi,** 2000; **Velez-Zea, *et al.*,** 2018), los de Fresnel (**Barrera-Ramírez, *et al.*,** 2016; **Jaramillo-Osorio, *et al.*,** 2022b; **Vilardy, *et al.*,** 2014) y los de transformada fraccional (**Jaramillo-Osorio, *et al.*,** 2018; **Jaramillo-Osorio, *et al.*,** 2022a). Otras variantes incluyen el procesamiento mediante otras transformadas, entre ellas, la

de Hartley (**Chen & Zhao,** 2006), la giratoria (**Liu, *et al.*,** 2010; **Vilardy, *et al.*,** 2017), la de Arnold (**Shi, *et al.*,** 2011), la de Mellin (**Zhou, *et al.*,** 2015), la jigsaw (**Vilardy, *et al.*,** 2019a), y la de Collins (**Vilardy, *et al.*,** 2019b). Muchas de las propuestas basadas en estas transformadas no han sido comprobadas experimentalmente debido a que usan arquitecturas ópticas que involucran muchos elementos o tienen grandes exigencias de potencia, alineación o estabilidad.

Los avances científicos de los últimos años evidencian que los sistemas ópticos de encriptación son una gran alternativa a los sistemas digitales y de *hardware* que actualmente se comercializan. Esta área de trabajo concentra los esfuerzos de varios grupos alrededor del mundo y permite vislumbrar la transición desde el entorno académico hacia el tecnológico en busca de su adopción comercial. Además de los elementos y desarrollos descritos, vale la pena mencionar los avances en la reducción y la eliminación del ruido en los datos recuperados y el impacto que ello tiene en este campo. En ese sentido, a continuación se presentan el análisis teórico y los resultados de la implementación experimental de un sistema óptico compacto que admite un protocolo de protección de información con recuperación libre de ruido, y se muestran las perspectivas de trabajo más promisorias en el área.

Ruido en los datos recuperados

Uno de los aspectos que más atención ha recibido en el área de encriptación es el ruido que presentan los datos recuperados. En este sentido se pueden distinguir tres vertientes de investigación: la principal, dedicada a disminuir el ruido que presentan los datos desencriptados debido al procesamiento con sistemas ópticos; otra, centrada en evitar el ruido que generan los datos no desencriptados en aquellos recuperados en procesos de multiplexado, y, por último, la técnica mediante la cual cierto rango de información puede recuperarse completamente libre de ruido. En esta sección se discutirán los avances en estas tres vertientes.

Reducción de ruido

A medida que se publicaban las contribuciones que demostraban la gran potencialidad del área, también se fueron evidenciando importantes limitaciones cuya resolución se convirtió en un reto que atrajo la atención de muchos investigadores. Una de las principales limitaciones es el ruido que afecta los datos recuperados, generado principalmente por las máscaras aleatorias y por las dimensiones y características de los elementos que determinan el límite de resolución del sistema. Además, un sistema experimental está expuesto a otras fuentes de ruido como la suciedad (polvo) y las fluctuaciones del índice de refracción, por mencionar solo dos de ellas.

Dado al alto grado de seguridad de los sistemas de encriptación experimentales que emplean máscaras aleatorias, la reducción del ruido en los datos desencriptados ha motivado el desarrollo de una línea de trabajo (**Javidi, *et al.*,** 2000; **Javidi, *et al.*,** 2016) en la que se destacan las contribuciones de **Velez-Zea, *et al.*** (2017a), **Velez-Zea, *et al.*** (2017b) y **Vilardy, *et al.*** (2013). En el 2013 se propuso un método que permite reducir el ruido de *speckle* que presentan los datos recuperados en el sistema de encriptación JTC (**Vilardy, *et al.*,** 2013). Este método consiste en dividir el dato encriptado por la información de la intensidad de la llave de seguridad, lo cual permite reducir el ruido en el dato desencriptado. Las simulaciones computacionales muestran que el método conduce efectivamente a una reducción de ruido en la recuperación.

Más tarde, se presentó un análisis que demuestra que el ruido depende de la distribución espacial del objeto y pone en evidencia la existencia de un ruido de correlación aleatoria que no había sido tenido en cuenta y que, en gran medida, es el culpable del deterioro de la imagen desencriptada (**Velez-Zea, *et al.*,** 2017b). Para evitar este ruido, se reorganiza la entrada introduciendo pixeles negros entre los pixeles de la imagen original, es decir, se separan los pixeles del objeto. El objeto modificado se encripta y

Rev. Acad. Colomb. Cienc. Ex. Fis. Nat. 46(178):68-89, enero-marzo de 2022
doi: https://doi.org/10.18257/raccefyn.1597

desencripta siguiendo el procedimiento habitual y, por último, la separación entre los píxeles se revierte para obtener el objeto desencriptado con una reducción significativa de ruido. Los resultados experimentales muestran que la aplicación de la técnica conduce a una mejora notable en la fidelidad de la reconstrucción. Se debe destacar que esta técnica permite proteger y recuperar apropiadamente objetos que, si se procesan sin aplicarla, no podrían reconocerse apropiadamente.

Otro avance significativo es un protocolo mediante el cual es posible alcanzar una reducción adicional y significativa del ruido (**Velez-Zea, *et al.*,** 2017a). Este protocolo usa los avances anteriores en reducción de ruido (**Vilardy, *et al.*,** 2013; **Velez-Zea, *et al.*,** 2017b) e introduce el uso de una máscara de referencia para eliminar el ruido debido a la máscara aleatoria que está en contacto con el objeto en el sistema de encriptación de doble máscara de fase (**Velez-Zea, *et al.*,** 2017a). Se demostró experimentalmente que es posible proteger datos estructurados en tonos de gris con una recuperación óptima, evidenciando que la reducción de ruido aumenta efectivamente el rango dinámico de los datos descifrados y conserva los valores de escala de grises en mayor medida, con lo que abre la posibilidad de nuevas aplicaciones.

La combinación de los avances en la reducción del ruido prueba que se puede proteger y recuperar apropiadamente la información de objetos bidimensionales, tridimensionales, estructurados, en tonos de gris y a color. Esta línea de trabajo se sigue desarrollando y se espera que después de reducir todas las fuentes de ruido, finalmente el sistema de encriptación solo se vea limitado por las dimensiones físicas del montaje experimental.

Manejo seguro de múltiples datos

Los sistemas de protección de datos deben admitir protocolos que involucran múltiples usuarios. En la encriptación óptica se emplean técnicas de multiplexado para almacenar la información de múltiples datos encriptados en un único bloque de información, ese único dato se denomina "multiplexado" y contiene la suma de todos los datos encriptados. Para llevar a cabo un proceso destinado a múltiples usuarios, cada uno de los datos es encriptado independientemente y luego se obtiene su multiplexado. La información del multiplexado es enviada a todos los usuarios por el mismo canal, asegurando un manejo eficiente de la información, ya que se evita el envío de un dato encriptado por cada uno de los usuarios. De esta forma, cada usuario recibe por otro canal la llave o llaves de seguridad que le permiten recuperar el dato de interés a partir del multiplexado.

Inicialmente se propuso un procedimiento de multiplexado en el que se encriptan múltiples datos utilizando iluminación de diferente longitud de onda para posteriormente sumar los datos encriptados y obtener el multiplexado (**Situ & Zhang,** 2005). Para recuperar la información de uno de los datos, además de poseer la información del multiplexado y de la llave de seguridad, se debe usar una fuente de iluminación con la misma longitud de onda con que fue encriptado ese dato. La propuesta pudo verificarse en simulaciones computacionales y, posteriormente, se presentaron implementaciones experimentales de procesos de multiplexado mediante el desplazamiento lateral de la llave de seguridad (**Barrera-Ramírez, *et al.*,** 2006a), la polarización de la luz (**Barrera-Ramírez, *et al.*,** 2006b) y la pupila del sistema (**Barrera-Ramírez, *et al.*,** 2006c).

Asimismo, se han generado procedimientos que permiten el manejo seguro de varios datos y el aumento de la seguridad del sistema de encriptación, por ejemplo, con técnicas que tienen como objetivo engañar a posibles intrusos introduciendo un procedimiento de ocultamiento (**Barrera-Ramírez, *et al.*,** 2007), mediante la modificación del tamaño de una pupila (**Barrera-Ramírez, *et al.*,** 2008), usando versiones escaladas de una máscara aleatoria de fase (**Barrera-Ramírez, *et al.*,** 2009a), empleando llaves complejas (**Barrera-Ramírez, *et al.*,** 2009b) y encriptación de datos complejos (**Barrera & Torroba,** 2009c). Otros incluyen el multiplexado con dos difusores y un conjunto de pupilas como llave de seguridad (**Singh, *et al.*,** 2008), dos patrones de *speckle* elongados y superpuestos (**Singh, *et al.*,** 2009), un algoritmo de recuperación de fase en cascada (**Yong-Liang, *et al.*,** 2009) y dos estaciones de seguridad independientes (**Alfalou & Mansour,** 2009).

La inclusión de técnicas de multiplexado en el área de la encriptación óptica representa grandes ventajas. En primer lugar, mediante estas técnicas se generan procesos para múltiples usuarios. Además, el multiplexado de datos permite aumentar la seguridad global del proceso mediante la inclusión de llaves de seguridad adicionales y protocolos de distracción y engaño. Dichos protocolos pueden llegar a evitar la vulnerabilidad del sistema cuando un usuario no autorizado llegue a interceptar parte de la información involucrada en el proceso.

Desde el principio, los protocolos de multiplexado evidenciaron una limitación en el número de datos que se podían multiplexar debido al ruido que generan los datos no desencriptados en el dato que se desencripta. A medida que el número de datos encriptados y multiplexados aumenta, se incrementa el ruido sobre cualquier dato desencriptado (**Situ & Zhang,** 2005). Si se encriptan n datos usando llaves diferentes, al tratar de desencriptar uno de ellos con la llave que se usó para su encriptación, se recupera ese dato, pero los $n - 1$ datos que no son desencriptados representan un ruido que se superpone con el objeto recuperado. A medida que el número de objetos encriptados y multiplexados aumenta, el ruido también lo hace, hasta que para cierto número de datos no se puede reconocer el objeto recuperado. Este hecho representó una gran limitación para la encriptación óptica, pues restringía los procesos con múltiples usuarios. Según algunos investigadores alrededor del mundo, esta limitación conducía al estancamiento de la encriptación óptica, por lo que era evidente y absolutamente necesario sobrepasar dicha dificultad. Con esa motivación se presentaron contribuciones que no solo permitieron evitar la superposición entre el dato recuperado y los datos no desencriptados, sino que, además, generaron aplicaciones que extendieron la aplicabilidad de los sistemas de encriptación.

Como en las técnicas de multiplexado arriba mencionadas cada uno de los datos es encriptado y desencriptado secuencialmente, en la primera propuesta de solución se usó una estructura diferente. En esta propuesta, se implementó un proceso de multiplexado que usa una arquitectura 4f conjuntamente con la propagación en el espacio libre para generar un proceso de multiplexado en un solo paso (**Barrera & Torroba,** 2010c). En este caso, todos los datos son encriptados simultáneamente con diferentes llaves de seguridad y distintas distancias de propagación. La recuperación de los datos puede hacerse individualmente o se pueden desencriptar todos a la vez, evitándose cualquier tipo de superposición. Paralelamente a esta propuesta se presentó un desarrollo experimental por el cual el ángulo de la onda de referencia en el proceso de registro permite separar el dato desencriptado de los datos que permanecen encriptados en el plano de recuperación (**Henao, *et al.,*** 2010), solucionando de esta forma el solapamiento de los datos.

Un año más tarde, se presentó una solución al problema de superposición en el plano de construcción (**Mosso, *et al.,*** 2011a). En el sistema propuesto e implementado cada dato es encriptado y luego modulado separadamente y, por último, todos los datos encriptados y modulados son multiplexados. El sistema de recuperación contiene una estación de filtrado para seleccionar la información que se desea desencriptar y luego ésta se usa como entrada del sistema de desencriptación, de manera que en el plano de recuperación se obtiene el dato que estaba encriptado sin la influencia de los otros. Además, en esta investigación se presentó por primera vez el concepto de "encriptación dinámica por medios ópticos" (**Mosso, *et al.,*** 2011a), lo cual es posible dado que se pueden generar procesos que involucren múltiples datos, que un proceso dinámico está compuesto por múltiples escenas y que cada una constituye un dato para el sistema de encriptación. Estos conceptos condujeron a la primera implementación óptica de un video encriptado, en la cual cada uno de los cuadros del video es un dato para el sistema de encriptación. Así, al encriptar cada uno de los cuadros del video y aplicar la modulación en el proceso de encriptación para luego sincronizar el proceso del filtrado durante la recuperación, por primera vez se logró encriptar y desencriptar en tiempo real un video por medio de un procesador óptico. Una ventaja notable del proceso de multiplexado es que la información del video encriptado ópticamente está contenida en un solo dato.

Rev. Acad. Colomb. Cienc. Ex. Fis. Nat. 46(178):68-89, enero-marzo de 2022
doi: https://doi.org/10.18257/raccefyn.1597

A partir de estas contribuciones, con las que se encripta y desencripta un video binario (**Paganin,** 2011), se desarrolló un protocolo completamente óptico para encriptar y desencriptar un video a color (**Mosso *et al.,*** 2011b). En el proceso de encriptación de un video a color cada una de las escenas que lo componen son divididas en sus tres canales cromáticos y cada uno de ellos es encriptado y modulado. Con este procedimiento se obtiene por separado la información encriptada, modulada y multiplexada de cada uno de los tres canales cromáticos de todas las escenas que componen el video. Durante la recuperación, los tres canales que componen cada una de las escenas se desencriptan simultáneamente sin la influencia de las otras escenas, de manera que se puede recuperar una sola escena de color. Por lo tanto, al sincronizar la etapa de filtrado para cada uno de los canales correspondientes a una escena, es posible recuperar un video a color.

Los desarrollos y avances posteriores condujeron a técnicas que permiten la encriptación experimental de múltiples videos (**Barrera-Ramírez, *et al.,*** 2012), la encriptación computacional de un video usando la transformada de Fourier fraccional (**Zhong, *et al.,*** 2014), la compresión y encriptación simultánea aplicada a secuencias de video (**Aldossari, *et al.,*** 2014) y la protección de videos usando máscaras caóticas (**Saini & Sinha,** 2015).

Recuperación libre de ruido

A pesar de los avances en la reducción del ruido, los usuarios requieren que su información esté protegida y que la información recuperada sea fiel a la original. Con este objetivo, a principios del 2013 se publicó un artículo en el que se planteó por primera vez que era posible cifrar información usando un sistema óptico y recuperarla sin ningún tipo de ruido o degradación. Dicho desarrollo estaba respaldado por resultados obtenidos mediante un sistema óptico-virtual integrado a un sistema con dos máscaras aleatorias de fase, una arquitectura óptica 4f y un procedimiento de codificación gráfica (**Barrera-Ramírez, *et al.,*** 2013a). En este caso, la información que se pretende cifrar se convierte en un código de respuesta rápida, conocido ampliamente como código QR (*quick response code*, *QR code*) (**International Organization for Standardization-ISO,** 2006). Por lo tanto, en lugar de cifrar el dato original, se cifra su respectivo código QR. Al realizarse el proceso de desencriptación, el código QR recuperado presentará el ruido generado por el procesamiento óptico; y cuando el código QR recuperado es decodificado se obtiene la información original libre de ruido. En este sentido, el código QR actúa como un contenedor de información y la recuperación libre de ruido es posible gracias a la tolerancia al ruido que presenta la decodificación de los códigos QR, en tanto que el sistema óptico es el responsable de la seguridad del proceso.

Esta contribución demostró por primera vez que era posible proteger datos mediante sistemas ópticos y recuperarlos completamente libres de ruido. Posteriormente, se hizo la demostración experimental (**Barrera-Ramírez, *et al.,*** 2014a) utilizando una arquitectura óptica de correlador de transformada conjunta, una llave de seguridad aleatoria y física, y, como contenedor de información, un código QR (**Barrera-Ramírez, *et al.,*** 2011; **Barrera-Ramírez & Torroba,** 2015a; **Nomura & Javidi,** 2000; **Torroba & Barrera-Ramírez,** 2015).

Estas dos contribuciones demostraron que los sistemas ópticos de protección de información son una alternativa a los sistemas de protección digitales y de *hardware* (**Barrera-Ramírez, *et al.,*** 2013a; **Barrera-Ramírez, *et al.,*** 2014a), generando un gran impacto en la comunidad científica internacional y revitalizando el área de los sistemas ópticos de encriptación (**Graydon,** 2013; **Treacy,** 2013). Se debe destacar que estas contribuciones dieron lugar al inicio de una línea de investigación en encriptación óptica de información empleando contenedores de información, la cual ha generado aportes respaldados por sistemas experimentales coherentes (**Barrera-Ramírez, *et al.,*** 2014b; **Jaramillo, *et al.,*** 2018; **Trejos, *et al.,*** 2015) e incoherentes (**Cheremkhin, *et al.,*** 2017; **Cheremkhin, *et al.,*** 2021a; **Evtikhiev, *et al.,*** 2020; **Wang, *et al.,*** 2020;), y sistemas ópticos-virtuales (**Lin, *et al.,*** 2015; **Sui, *et al.,*** 2017). Además, motivaron el surgimiento de nuevas líneas de investigación y desarrollo en torno al procesamiento óptico usando contenedores en procesos

de autenticación de información (**Blau, *et al.,*** 2020; **Carnicer, *et al.,*** 2015; **Chen, *et al.,*** 2018; **Qin, *et al.,*** 2018a) y a la implementación de diferentes técnicas y materiales para la fabricación de contenedores (**Li, *et al.,*** 2017c; **Meng, *et al.,*** 2021a; **Petriashvili, *et al.*,** 2018; **Ponjavidze, *et al.,*** 2018; **Wang, *et al.,*** 2021). También incentivaron el desarrollo de aplicaciones en diferentes tópicos y áreas, por ejemplo, para la formación integral de imágenes (**Markman, *et al.,*** 2014), la protección de hologramas con marcas de agua (**Li, *et al.,*** 2018), la pictografía (**Zhu, *et al.,*** 2019), y la esteganografía (**Alajmi, *et al.,*** 2020).

A pesar sus ventajas, un código QR no es un contenedor ideal para los sistemas ópticos, ya que su diseño está optimizado para ser resistente a un daño localizado (**ISO,** 2006), en tanto que el ruido introducido por los sistemas de encriptación que usan máscaras aleatorias afecta casi uniformemente el objeto desencriptado (**Barrera-Ramírez, *et al.,*** 2013a; **Barrera-Ramírez, *et al.,*** 2014a; **Barrera-Ramírez, *et al.,*** 2014b; **Barrera-Ramírez & Torroba,** 2015b). Además del espacio que ocupa la información codificada, los códigos QR contienen estructuras de posición, alineamiento, sincronización, de formato y de versión que hacen que el tamaño del código sea considerable.

Un contenedor ideal debe tener frecuencias espaciales bajas para minimizar las pérdidas por difracción, el tamaño de píxel necesario en el medio de registro, y un nivel de tolerancia al ruido controlable, de manera que se pueda garantizar una lectura eficiente. Asimismo, el contenedor debe diseñarse de manera que requiera el menor espacio posi-ble y pueda codificar la mayor cantidad de información según las limitaciones físicas de los elementos usados en los montajes ópticos.

Siguiendo este razonamiento, se desarrolló el primer contenedor de información específicamente para sistemas ópticos, denominado *customized container for optical security* (CCOS). El CCOS satisface los criterios de un contenedor óptimo, pues su contenido espectral puede deducirse a partir de la separación y el tamaño de los bloques, y la tolerancia al ruido está directamente relacionada con el tamaño de los bloques. Además, la lectura del CCOS se lleva a cabo con tres operaciones sencillas sin necesidad de estructuras de sincronización, de formato y de versión. Además, las estructuras de posición y lineamiento en el CCOS son provistas por un borde que delimita el área de lectura (**Velez-Zea, *et al.,*** 2016b).

Los resultados computaciones y experimentales mostraron que un CCOS permite un gran aumento en la tolerancia al ruido en comparación con un código QR, a la vez que su encriptación satisfactoria requiere de menos espacio en el plano de entrada, aumentando la cantidad de información que puede ser procesada simultáneamente (**Jaramillo-Osorio, *et al.***, 2020a; **Velez-Zea, *et al.***, 2016b). Estas contribuciones demuestran que diseñar contenedores específicamente para las características del sistema óptico ayuda a superar algunas de las limitaciones causadas por el ruido.

Este nuevo contenedor ha servido de base para novedosas aplicaciones con operaciones XOR (**Qin & Zhang,** 2017), algoritmos de recuperación de fase (**Qin, *et al.,*** 2018b), imágenes fantasmas (**Liansheng, *et al.,*** 2019), criptosistemas asimétricos (**Kumar & Nishchal,** 2019) e, inclusive, implementaciones en el dominio de Fresnel (**Jaramillo-Osorio, *et al.,*** 2020a). Es importante tener en cuenta que la recuperación libre de ruido está limitada a los caracteres que se puedan codificar y decodificar usando los contenedores de información. Por lo tanto, cuando se trata de objetos que están por fuera de ese rango, la reducción de ruido se obtiene aplicando las técnicas mencionadas en la sección Reducción de ruido.

Los avances en estas tres vertientes están relacionados y potencian la encriptación óptica; por ejemplo, todos los avances en la reducción de ruido en un dato recuperado son fundamentales para aumentar el número de caracteres que pueden recuperarse sin ruido, ya que, al reducir significativamente el ruido en el contenedor desencriptado, es posible decodificar contenedores con un número significativo de información.

A partir de los avances en la reducción y eliminación del ruido, se han generado técnicas y métodos que han permitido expandir el rango de aplicabilidad de la encriptación óptica. Por ejemplo, se han presentado aplicaciones novedosas que demuestran que mediante

Rev. Acad. Colomb. Cienc. Ex. Fis. Nat. 46(178):68-89, enero-marzo de 2022
doi: https://doi.org/10.18257/raccefyn.1597

una técnica de multiplexado se pueden encriptar objetos que superan el límite de resolución del sistema (**Barrera-Ramírez, *et al.,*** 2011), implementar experimentalmente un teclado encriptado ópticamente (**Barrera-Ramírez, *et al.,*** 2013b) y aumentar la seguridad del sistema mediante un procedimiento de salteado (**Velez-Zea, *et al.,*** 2017c). Incluso, se presentó una contribución que aprovecha todos los avances en reducción de ruido, recuperación libre de ruido y encriptación dinámica para la protección y recuperación de mensajes libres de ruido (**Trejos, *et al.,*** 2015).

Sistema óptico compacto para la protección de datos

Aunque los sistemas ópticos de encriptación han demostrado un alto desempeño, su puesta en funcionamiento es muy exigente, lo que restringe su implementación en ambientes de investigación básica y limita su potencial para el uso en entornos prácticos. Esto evidencia la necesidad de desarrollar sistemas que preserven los niveles de seguridad hasta ahora alcanzados por los procesadores ópticos para la protección de datos y permitan una reducción del volumen físico que ocupa el sistema, la cantidad de elementos ópticos empleados y las exigencias de estabilidad y alineamiento, de manera que se cuente con protocolos de seguridad basados en esquemas ópticos compactos que permitan reducir los requerimientos de los sistemas convencionales. Además, estos sistemas deben admitir protocolos de seguridad en que los datos recuperados estén libres de cualquier ruido o degradación.

Uno de los sistemas ópticos de encriptación más desarrollados y estudiados, y que posee más variantes, es el sistema 4f (**Refregier & Javidi,** 1995). Este sistema emplea una arquitectura óptica 4f con dos lentes positivas y dos máscaras aleatorias de fase para convertir el dato original en un patrón de ruido blanco, conocido como dato encriptado. En la primera implementación experimental, la información del dato encriptado se registró usando un montaje interferométrico fuera de eje, en el cual uno de los brazos contiene el sistema 4f y el otro, una onda de referencia. En el proceso de recuperación es necesario emplear un sistema holográfico fuera de eje que permita el registro de la llave; posteriormente, la llave es multiplicada por el dato encriptado y, mediante un proceso inverso al de encriptación, es posible recuperar la información original. Una gran cantidad de elementos ópticos son necesarios para llevar a cabo el proceso de encriptación y de registro de la llave, lo que conduce a que el montaje experimental tenga grandes exigencias de alineación y estabilidad (**Javidi, *et al.,*** 1996).

Con el propósito de disminuir los requerimientos experimentales planteados por la arquitectura 4f, y tomando como base la arquitectura óptica JTC (**Goodman,** 1996; **Lu, *et al.,*** 1990; **Millán,** 2012; **Vander-Lugt,** 1964; **Weaver & Goodman,** 1966), se propuso el sistema de encriptación JTC (**Nomura & Javidi,** 2000). El plano de entrada del criptosistema JTC contiene el producto entre el objeto que se desea proteger y una máscara aleatoria de fase y, a una distancia determinada, se ubica otra máscara aleatoria de fase que actúa como llave de seguridad.

Experimentalmente, el plano de entrada se genera proyectando el objeto y la ventana de la llave en un modulador espacial de luz (MEL) (*spatial light modulator*, SLM), que luego se pone en contacto con un difusor (**Figura 1**). Esta arquitectura posee una sola lente ubicada entre los planos de entrada y de salida, de modo que ambos quedan ubicados en los puntos focales de dicha lente. En el plano de salida se registra la intensidad de la transformada de Fourier conjunta de las funciones que forman el plano de entrada y, a partir de esa intensidad, se obtiene el dato encriptado. Esto implica que el sistema JTC es más compacto, pues requiere solo de una lente, lo que reduce algunas de las exigencias del sistema 4f, característica que ha llevado a que se haya estudiado y desarrollado notablemente (**Jaramillo, *et al.,*** 2018; **Jaramillo, *et al.,*** 2020a; **Rueda, *et al.,*** 2009a; **Rueda, *et al.,*** 2009b; **Vilardy, *et al.,*** 2017).

Aunque en el criptosistema JTC no es necesario implementar un montaje interferómetrico con un brazo de referencia para registrar la intensidad que permite obtener el dato encriptado, este montaje es necesario para registrar la información de la llave de seguridad

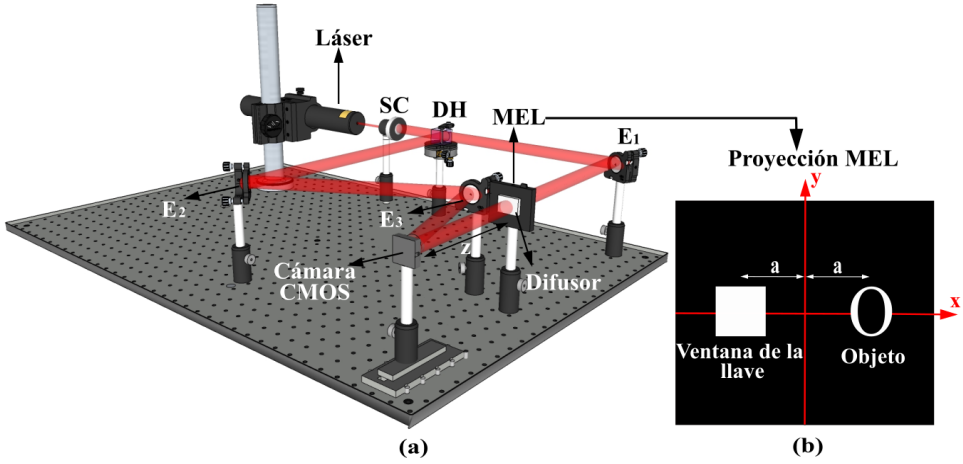

Figura 1. (a) Sistema de encriptación JTC en el dominio de Fresnel con brazo de referencia. *z*: separación entre el plano de entrada y el sensor de la cámara CMOS; MEL: modulador espacial de luz; SC: sistema de colimación; DH: divisor de haz; E: espejo. **(b)** Proyección en el MEL. 2*a*: separación entre el objeto y la ventana de la llave

(Barrera-Ramírez, *et al.,* 2011; Barrera-Ramírez, *et al.,* 2012; Barrera-Ramírez, *et al.,* 2013b; Barrera-Ramírez, *et al.,* 2013c; Barrera-Ramírez, *et al.,* 2014a; Barrera-Ramírez, *et al.,* 2016; Jaramillo, *et al.,* 2018; Rueda, *et al.,* 2009a; Rueda, *et al.,* 2009b) (Figura 1)**. Esto implica que el sistema JTC conserva los altos requerimientos experimentales y de implementación y funcionamiento asociados con el brazo de referencia (brazo con espejos E_2 y E_3). Con el fin de evitar estos requerimientos, recientemente se desarrolló un sistema de encriptación compacto que se describe a continuación.

Obtención del dato encriptado y la llave de seguridad

El sistema compacto de protección de datos utiliza una arquitectura de encriptación de correlador de transformada conjunta en el dominio de Fresnel (**Jaramillo-Osorio, *et al.,*** 2020a; **Jaramillo-Osorio, *et al.,*** 2020b). En esta arquitectura, la información que se va a proteger y la ventana de la llave se proyectan en un MEL y se ponen en contacto con un difusor (**Figura 2 a, b**). Considerando que $c(x, y) = o(x, y)r(x, y)$, donde $o(x, y)$ se denomina objeto y representa la información que se desea proteger y $r(x, y)$ es la máscara aleatoria correspondiente al área del difusor que está en contacto con la información que se va a encriptar, la transmitancia del plano de entrada del sistema se puede escribir como (**Figura 2 a**),

$$f(x, y) = c(x, y) \otimes \delta(x - c, y + d) + l(x, y) \otimes \delta(x + c, y + d) \quad (1),$$

donde la llave de seguridad $l(x, y)$ es la región del difusor limitada por la ventana de la llave, la separación entre el objeto y la llave de seguridad es $2c$ (**Figura 2 b**), $\otimes$ representa la operación de convolución y δ es la función delta de Dirac.

En el proceso de encriptación, el plano de entrada se ilumina con una onda plana monocromática y el campo que emerge del plano de entrada se propaga libremente hasta el plano de registro. Luego, en una cámara CMOS se registra la intensidad de la transformada de Fresnel (TFr) de la transmitancia del plano de entrada, intensidad que se conocida como espectro conjunto de potencias de Fresnel (ECPF),

$$F(u, v) = |C_z(u, v)|^2 + |L_z(u, v)|^2 + C_z^*(u, v)L_z(u, v)\, exp(4\pi icu) + C_z(u, v)L_z^*(u, v)\, exp(-4\pi icu) \quad (2),$$

donde z es la distancia entre el plano de entrada y el plano de registro (**Figura 2 a**), (u, v) son las coordenadas en el dominio de Fresnel; $C_z(u, v)$ y $L_z(u, v)$ son las TFrs de $c(x, y)$ y $l(x, y)$, respectivamente, y $*$ representa el complejo conjugado.

Rev. Acad. Colomb. Cienc. Ex. Fis. Nat. 46(178):68-89, enero-marzo de 2022
doi: https://doi.org/10.18257/raccefyn.1597

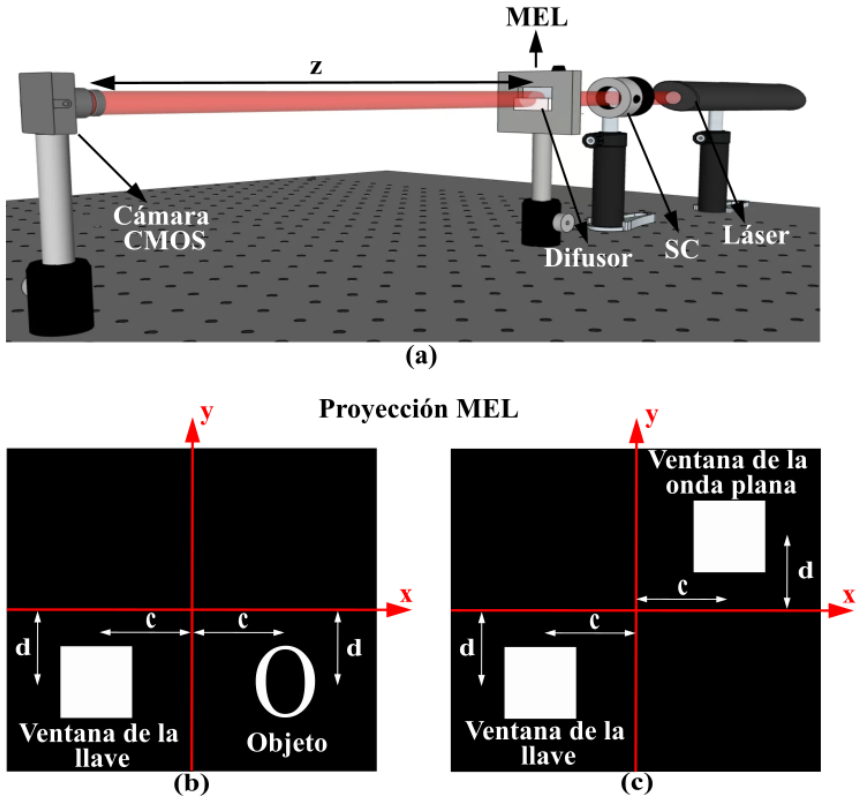

Figura 2. a) Sistema compacto de encriptación. *z*: separación entre el plano de entrada y el sensor de la cámara CMOS; MEL: modulador espacial de luz; SC: sistema de colimación. Proyección en el MEL para registrar: **b)** el objeto encriptado y **c)** la información de la llave de seguridad. 2*c*: separación entre el objeto y la ventana de la llave; 2*d*: separación entre la ventana llave y la ventana de la onda plana. El difusor cubre el área inferior del modulador donde se proyectan la ventana de la llave y el objeto

Para extraer el dato encriptado del ECPF (ecuación 2), se realiza un proceso de filtrado que consiste en registrar el término $|C_z(u,v)|^2$ proyectando en el SLM solo la ventana de la llave y $|L_z(u,v)|^2$ proyectando solo el objeto, para luego restar las intensidades $|C_z(u,v)|^2$ y $|L_z(u,v)|^2$ del ECPF y obtener

$$G(u,v) = C_z^*(u,v)L_z(u,v)\,exp(4\pi icu) + C_z(u,v)L_z^*(u,v)\,exp(-4\pi icu) \quad (3).$$

Al realizar la transformada de Fourier (FT) de la ecuación (3) se obtiene

$$g(\xi,\eta) = FT\{C_z^*(u,v)L_z(u,v)\} \otimes \delta(\xi - 2c) + FT\{C_z(u,v)L_z^*(u,v)\} \otimes \delta(\xi + 2c) \quad (4).$$

Como los dos términos en la ecuación (4) están separados espacialmente, es posible filtrar el primer término y retener el segundo. Luego, al posicionar el segundo término en las coordenadas (0, 0) y realizar una TF inversa, se obtiene el objeto encriptado (**Barrera-Ramírez, *et al.*,** 2013c),

$$E(u,v) = C_z(u,v)\,L_z^*(u,v) \quad (5).$$

Recuperación del objeto

Un usuario autorizado debe poseer la información del objeto encriptado y de la llave de seguridad para poder acceder a la información original. Para la obtención de la información de la llave de seguridad se utiliza el mismo montaje experimental empleado para obtener el dato encriptado, pero se cambia la proyección en el MEL. En este caso, en el MEL se proyecta la ventana de la llave y una ventana que permite generar una onda plana (**Figura 2 c**). Con esta proyección, la transmitancia del plano de entrada está dada por:

doi: https://doi.org/10.18257/raccefyn.1597

$$p(x, y) = w(x, y) \otimes \delta(x - c, y - d) + l(x, y) \otimes \delta(x + c, y + d) \quad (6),$$

donde $w(x, y)$ representa la ventana de la onda plana y $2d$ es la separación entre la ventana de la llave y la ventana de la onda plana (**Figura 1 c**). En la cámara CMOS se registra la intensidad de la TFr del plano de entrada,

$$P(u, v) = |W_z(u, v)|^2 + |L_z(u, v)|^2 + L_z^*(u, v)W_z(u, v)\, exp[-4\pi i(cu + dv)] + L_z(u, v)W_z^*(u, v)\, exp[4\pi i(cu + dv)] \quad (7),$$

donde $W_z(u, v)$ es la TFr de $w(x, y)$. Con un procedimiento de filtrado similar al aplicado en la ecuación (2) para obtener el objeto encriptado (ecuación 5), se accede a la información de la llave de seguridad $L_z(u, v)$ (**Barrera-Ramírez, *et al.*,** 2011).

El proceso de recuperación consiste en multiplicar el dato encriptado $E(u, v)$ por la información de la llave de seguridad $L_z(u, v)$,

$$e_d(u, v) = C_z(u, v)L_z^*(u, v)L_z(u, v) \quad (8).$$

Lo ideal es que $L_z(u, v)$ sea una función solo de fase, sin embargo, en la implementación experimental un difusor provee la llave y, por lo tanto, es una función aleatoria compleja. A pesar de esto, podemos aplicar la aproximación de ancho de banda donde $L_z^*(u, v)L_z(u, v) \approx 1$ (**Unnikrishnan, *et al.*,** 1998). Con esta aproximación y realizando la TFr inversa se obtiene el objeto desencriptado,

$$d(x, y) = c(x, y) = o(x, y)r(x, y) \quad (9).$$

Por último, la información del objeto original se recupera al calcular la intensidad del objeto desencriptado. Por otro lado, si un usuario no autorizado intenta acceder a la información original usando una llave incorrecta, una TFr inversa producirá un patrón de *speckle*, pues la información permanece encriptada.

Este sistema compacto reduce la cantidad de elementos utilizados y el volumen ocupado por el montaje experimental, manteniendo las características de seguridad presentes en los sistemas ya establecidos (**Figura 1 a, b**). Al excluir el brazo de referencia, se reducen las exigencias experimentales de estabilidad, alineación y potencia de la fuente de iluminación. Además, se evitan las aberraciones que pueden introducir los elementos ópticos asociados con el brazo de referencia.

Resultados experimentales

El montaje experimental está constituido por un láser de helio-neón con $\lambda = 632{,}8\ nm$ como fuente de iluminación y un MEL de transmisión SLM Holoeye LC2002 con 800 × 600 píxeles y un tamaño de pixel de 32 μm × 32 μm para proyectar el objeto, la ventana de la llave y la ventana de la onda plana (**Figura 2**). Las máscaras aleatorias de fase son generadas por medio de un difusor y se emplea una cámara CMOS EO-1002M con una resolución de 3840 × 2748 pixeles y un tamaño de píxel de 1,67 μm × 1,67 μm para registrar la información procesada ópticamente. El tamaño del objeto, la ventana de la llave y la ventana de la onda plana es de 8 *mm* × 6,4 *mm*, 3,2 *mm* × 3,2 *mm* y 4,8 *mm* × 4,8 *mm*, respectivamente. $c = 3{,}2\ mm$, $d = 2{,}6\ mm$ y la distancia entre el plano de entrada y el plano de registro es $z = 23\ cm$.

En la **figura 3** se presentan los resultados experimentales obtenidos por medio del sistema compacto. El objeto corresponde a las letras UDEA (**Figura 3 a**); como era de esperarse el objeto encriptado (ecuación 5) es un patrón aleatorio debido al uso de las máscaras aleatorias de fase (**Figura 3 b**). Para recuperar el objeto a partir de la información encriptada se debe tener acceso a la llave de seguridad empleada en el proceso de encriptación, pues si se utiliza una llave diferente, el dato permanecerá encriptado (**Figura 3 c**), en cambio, utilizando la llave de seguridad empleada en el proceso de encriptación se recupera la información original (**Figura 3 d**). Evidentemente, la información recuperada contiene el ruido asociado con los sistemas ópticos de encriptación que usan máscaras aleatorias de fase.

Rev. Acad. Colomb. Cienc. Ex. Fis. Nat. 46(178):68-89, enero-marzo de 2022
doi: https://doi.org/10.18257/raccefyn.1597

Como se mencionó al inicio de esta sección, los sistemas compactos deben admitir procesos de protección de información que brinden un dato recuperado libre de ruido. Para comprobar que el sistema de compresión de datos cumple este requisito, se emplea un CCOS como contenedor de información. El CCOS es un arreglo binario cuadrado de 3x3 celdas donde cada celda contiene un bloque. La lectura del código se hace calculando la intensidad promedio de cada celda de izquierda a derecha y de arriba abajo, y luego se compara con un valor límite que depende del sistema óptico (**Velez-Zea, *et al.,*** 2016b). En la **figura 4** se presenta el código CCOS correspondiente al texto UDEA (**Figura 4 a**) y el respectivo código desencriptado (**Figura 4 b**). La lectura del código CCOS brinda la información libre de ruido y de cualquier degradación (**Figura 4 c**) por su tolerancia al ruido.

Los resultados presentados en las **figuras 3** y **4** demuestran que con el sistema óptico compacto no solo se protege la información, sino que, además, se puede obtener una recuperación libre de ruido. La línea de trabajo en sistemas ópticos compactos para la protección

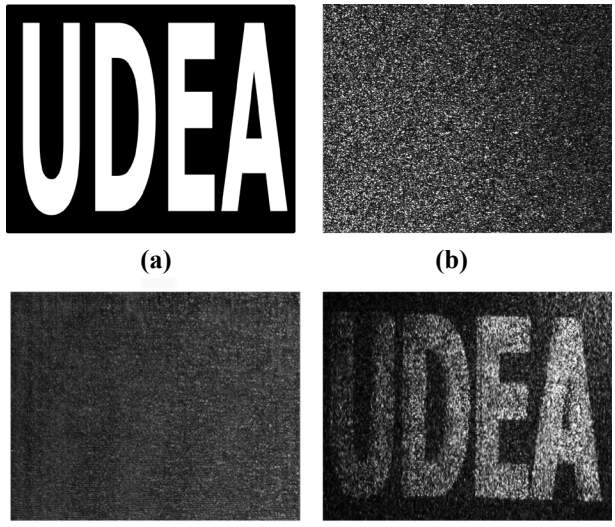

Figura 3. a) Objeto, resultados experimentales: **b)** objeto encriptado, objeto desencriptado con **c)** una llave incorrecta y **d)** la llave correcta

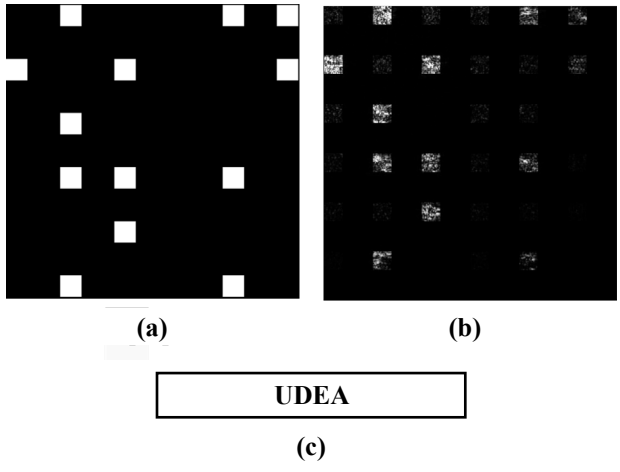

Figura 4. Resultado de la encriptación de información con recuperación libre de ruido. **a)** Código CCOS del texto UDEA, **b)** código desencriptado, y **c)** lectura del código desencriptado

de datos es una línea en desarrollo que contribuye significativamente a la potencial adopción de sistemas ópticos de seguridad. Aunque esta línea aprovecha todos los avances que se han generado en torno a los criptosistemas ópticos, óptico-digitales y óptico-virtuales, se requieren investigaciones que muestren que este tipo de sistemas pueden alcanzar un rendimiento similar al demostrado por los criptosistemas convencionales.

Perspectivas

A pesar de los grandes avances que se han logrado hasta ahora, aún hay retos que están siendo motivo de investigaciones en varios laboratorios alrededor del mundo, estudios en los que se definen las perspectivas del área de protección de la información mediante procesadores ópticos. Entre las líneas de trabajo recientes se destacan el desarrollo de sistema ópticos compactos (**Jaramillo-Osorio, *et al.,*** 2020a; **Jaramillo-Osorio, *et al.,*** 2020b), en el que se advierten futuras aplicaciones basadas en criptosistemas ópticos que permitirán dinamizar el área de la encriptación óptica de información. También se sigue trabajando para aumentar y mejorar la seguridad (**Dou, *et al.,*** 2019), en algunos casos implementando experimentalmente esquemas en diferentes dominios ópticos y transformadas que involucran nuevos parámetros de seguridad (**Jaramillo-Osorio, *et al.,*** 2020b; **Vilardy, *et al.,*** 2019a; **Vilardy, *et al.,*** 2019b). Otras líneas que se siguen desarrollando activamente son las encaminadas a lograr una reducción de ruido para mejorar la calidad de los datos recuperados y la encriptación óptica con recuperación libre de ruido (**Cheremkhin, *et al.,*** 2021a; **Cheremkhin, *et al.,*** 2021b; **Evtikhiev, *et al.,*** 2020; **Wang, *et al.,*** 2020), la encriptación de múltiples datos (**He, *et al.,*** 2020; **Wu, *et al.,*** 2019; **Zhang, *et al.,*** 2022) e incluso, la combinación de técnicas de multiplexado y recuperación libre de ruido (**Jaramillo-Osorio, *et al.,*** 2020b; **Yan, *et al.,*** 2019).

Debido a que los sistemas ópticos de encriptación han demostrado su gran potencialidad para aplicaciones prácticas, una de las líneas más activas actualmente es el criptoanálisis, en la cual se busca probar la seguridad de los sistemas ópticos de encriptación adaptando en el dominio óptico algunos de los ataques que se usan exclusivamente en el dominio digital (**Hai, *et al.,*** 2019; **Jiao, *et al.,*** 2020; **Wang, *et al.,*** 2019b; **Wu, *et al.,*** 2021; **Zhang, *et al.,*** 2021). Esta es un área en desarrollo y consolidación, ya que los ataques a los sistemas ópticos experimentales están en sus primeras etapas y se prevén futuros avances que permitan fortalecer el área de la protección de datos por medio de procesadores ópticos.

Se espera que en los próximos años se produzcan desarrollos que generen sistemas ópticos aptos para proteger la información mediante un amplio espectro de posibilidades que trasciendan el trabajo realizado hasta ahora. En ese sentido, los nuevos criptosistemas deberían ser lo suficientemente flexibles para incluir todos los desarrollos en las áreas de trabajo mencionadas. Además, se pueden prever avances científicos que permitan el desarrollo de dispositivos ópticos de encriptación ultracompactos mediante, por ejemplo, dispositivos fotónicos integrados y metateriales (**Abdollahramezani, *et al.,*** 2020; **Li, *et al.,*** 2017b; **Meng, *et al.,*** 2021b; **Reshef, *et al.,*** 2021; **Wang, *et al.,*** 2016). Obviamente, su implementación dependerá del campo en el que se obtengan los mejores desarrollos frente a las dificultades científicas y tecnológicas, así como del interés de los centros de investigación y las grandes compañías.

Conclusiones

Las contribuciones de los últimos años han permitido resolver limitaciones fundamentales del campo de la encriptación óptica, lo que ha demostrado su gran confiabilidad y efectividad para la protección de la información. Además, dichas investigaciones han dado lugar a novedosos avances y al surgimiento de diversas líneas de desarrollo en torno al procesamiento óptico de la información. En particular, el área de reducción y eliminación del ruido ha presentado un gran dinamismo y sigue vigente debido al impacto que tiene en la eventual adopción de los criptosistemas ópticos. El desarrollo teórico y los resultados experimentales presentados en esta exposición demuestran la validez del sistema óptico

Rev. Acad. Colomb. Cienc. Ex. Fis. Nat. 46(178):68-89, enero-marzo de 2022
doi: https://doi.org/10.18257/raccefyn.1597

de encriptación compacto y la real posibilidad de implementar protocolos de recuperación libre de ruido cuando se usan contendores de información personalizados. Estos resultados evidencian la potencialidad del sistema y permiten visualizar el desarrollo de una línea de trabajo en esta dirección dadas las ventajas prácticas de los criptosistemas compactos. Se prevé que los desarrollos actuales y futuros en el área no solo inspiren el surgimiento y desarrollo de líneas y tópicos relevantes, sino que, además, posibiliten una transición desde el ámbito científico y académico al de la aplicación tecnológica.

Agradecimientos

Esta investigación se llevó a cabo con el apoyo del Comité para el Desarrollo de la Investigación-CODI y la Estrategia de Sostenibilidad 2020-2021 de la Universidad de Antioquia (Colombia). El autor agradece la colaboración del estudiante de Doctorado en Física M.Sc. John Alexis Jaramillo Osorio (Instituto de Física, Universidad de Antioquia), por su ayuda en los montajes experimentales que permitieron obtener los resultados aquí presentados.

Conflicto de intereses

El autor del artículo declara que no existe conflicto de intereses con relación a la publicación de este artículo.

Referencias

Abdollahramezani, S., Hemmatyar, O., Adibi, A. (2020). Meta-optics for spatial optical analog computing. Nanophotonics. **9:** 4075-4095. DOI: 10.1515/nanoph-2020-0285

Asociación Colombiana de Ingenieros de Sistemas-ACIS. (2020). Cifras de ciberseguridad en Colombia prenden alarmas al cierre del 2020. Fecha de consulta: noviembre de 2021. Disponible en: https://acis.org.co/portal/content/noticiasdelsector/cifras-de-ciberseguridad-en-colombia-prenden-alarmas-al-cierre-del-2020

Alajmi, M., Elashry, I., El-Sayed, H.S., Farag, O.S. (2020). Steganography of Encrypted Messages Inside Valid QR Codes. IEEE Access. **8:** 27861-27873. https://doi.org/10.1109/ACCESS.2020.2971984

Aldossari, M., Alfalou, A., Brosseau, C. (2014). Simultaneous compression and encryption of closely resembling images: application to video sequences and polarimetric images. Opt. Express. **22:** 22349-22368. https://doi.org/10.1364/OE.22.022349

Alfalou, A. (Ed.). (2018). Advanced Secure Optical Image Processing for Communications. (8-1-8-33). Bristol: United Kingdom: Institute of Physics Publishing.

Alfalou, A. & Brosseau, C. (2009). Optical image compression and encryption methods. Adv. Opt. Photon. **1:** 589-636. https://doi.org/10.1364/AOP.1.000589

Alfalou, A. & Mansour, A. (2009). Double random phase encryption scheme to multiplex and simultaneous encode multiple images. Appl. Opt. **48:** 5933-5947. https://doi.org/10.1364/AO.48.005933

Ambs, P. (2010). Optical computing: a 60-year adventure. Adv. Opt. Technol. **2010:** 372652. https://doi.org/10.1155/2010/372652

Barrera-Ramírez, J.F., Henao, R., Torroba, R. (2005a). Optical encryption method using toroidal zone plates. Opt. Commun. **248:** 35-40. https://doi.org/10.1016/j.optcom.2004.11.086

Barrera-Ramírez, J.F., Henao, R., Torroba, R. (2005b). Fault tolerances using toroidal zone plate encryption. Opt. Commun. **256:** 489-494. https://doi.org/10.1016/j.optcom.2005.06.077

Barrera-Ramírez, 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. https://doi.org/10.1016/j.optcom.2005.09.027

Barrera-Ramírez, J.F., Henao, R., Tebaldi, M., Torroba, R., Bolognini, N. (2006b). Multiplexing encrypted data by using polarized light. Opt. Commun. **260:** 109-112. https://doi.org/10.1016/j.optcom.2005.10.053

Barrera-Ramírez, 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. https://doi.org/10.1016/j.optcom.2005.11.055

Barrera-Ramírez, J.F., Henao, R., Tebaldi, M., Torroba, R., Bolognini, N. (2007). Multiple-encoding retrieval for optical security. Opt. Commun. **276:** 231-236. https://doi.org/10.1016/j.optcom.2007.04.040

Barrera-Ramírez, J.F., Henao, R., Tebaldi, M., Torroba, R., Bolognini. N. (2008). Code retrieval via undercover multiplexing. Optik. **119:** 139-142. https://doi.org/10.1016/j.ijleo.2006.07.008

Barrera-Ramírez, J.F., Henao, R., Tebaldi, M., Torroba, R., Bolognini, N. (2009a). Digital encryption with undercover multiplexing by scaling the encoding mask. Optik. **120:** 342-346. https://doi.org/10.1016/j.ijleo.2007.10.002

Barrera-Ramírez, J.F., Tebaldi, M., Torroba, R., Bolognini, N. (2009b). Multiplexing encryption technique by combining random amplitude and phase masks. Optik. **120:** 351-355. https://doi.org/10.1016/j.ijleo.2007.10.001

Barrera-Ramírez, J.F. & Torroba, R. (2009c). Efficient encrypting procedure using amplitude and phase as independent channels to display decoy objects. Appl. Opt. **48:** 3121-3129. https://doi.org/10.1364/AO.48.003121

Barrera-Ramírez, J. F., Vargas, C., Tebaldi, M., Torroba, R. (2010a). Chosen-plaintext attack on a joint transform correlator encrypting system. Opt. Commun. **283:** 3917-3921. https://doi.org/10.1016/j.optcom.2010.06.009

Barrera-Ramírez, J.F., Vargas, C., Tebaldi, M., Torroba, R., Bolognini, N. (2010b). Known plaintext attack on a joint transform correlator encrypting system. Opt. Lett. **35:** 3553-3555. https://doi.org/10.1364/OL.35.003553

Barrera-Ramírez, J.F. & Torroba, R. (2010c). One step multiplexing optical encryption. Opt. Commun. **283:** 1268-1272. https://doi.org/10.1016/j.optcom.2009.11.083

Barrera-Ramírez, 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. https://doi.org/10.1016/j.optcom.2011.05.035

Barrera-Ramírez, J.F., Tebaldi, M., Ríos C., Rueda E., Bolognini, N., Torroba R. (2012). Experimental multiplexing of encrypted movies using a JTC architecture. Opt. Express. **20:** 3388-3393. https://doi.org/10.1364/OE.20.003388

Barrera-Ramírez, J.F., Mira-Agudelo, A., Torroba, R. (2013a). Optical encryption and QR codes: Secure and noise-free information retrieval. Opt. Express. **21:** 5373-5378. https://doi.org/10.1364/OE.21.005373

Barrera-Ramírez, J.F., Velez-Zea, A., Torroba. R. (2013b). Experimental multiplexing protocol to encrypt text of any length. J. Opt. **15:** 055404. https://doi.org/10.1088/2040-8978/15/5/055404

Barrera-Ramírez, J.F., Trejos, S., Tebaldi, M., Torroba. R. (2013c). Experimental protocol for packaging and encrypting multiple data. J. Opt. **15:** 055406. https://doi.org/10.1088/2040-8978/15/5/055406

Barrera-Ramírez, J.F., Mira-Agudelo, A., Torroba, R. (2014a). Experimental QR code optical encryption: noise-free data recovering. Opt. Lett. **39:** 3074-3077. https://doi.org/10.1364/OL.39.003074

Barrera-Ramírez, J.F. Velez-Zea, A., Torroba, R. (2014b). Experimental scrambling and noise reduction applied to the optical encryption of QR codes. Opt. Express. **22:** 20268-20277. https://doi.org/10.1364/OE.22.020268

Barrera-Ramírez, J.F., Mira-Agudelo A., Torroba, R. (Diciembre 18, 2015a). Aparato óptico-físico y procedimientos para la encriptación y recuperación de información libre de ruido. Patente de invención 14 98035.

Barrera-Ramírez, J.F. & Torroba, R. (2015b). Encriptación óptica de información con recuperación libre de ruido. Rev. Acad. Colomb. Cienc. Ex. Fis. Nat. **39:** 48-54. https://doi.org/10.18257/raccefyn.259

Barrera-Ramírez, J.F., Jaramillo-Osorio, A., Velez-Zea, A., Torroba, R. (2016). Experimental analysis of a joint free space cryptosystem. Opt. Lasers Eng. **83:** 126-130. https://doi.org/10.1016/j.optlaseng.2016.03.010

Blau, Y., Bar-On, O., Hanein, Y., Boag, A., Scheuer, J. (2020). Meta-hologram-based authentication scheme employing a speckle pattern fingerprint. Opt. Express. **28:** 8924-8936. https://doi.org/10.1364/OE.388233

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. https://doi.org/10.1364/OL.40.000135

Carnicer, A. & Javidi, B. (2017). Optical security and authentication using nanoscale and thin-film structures. Adv. Opt. Photon. **9:** 218-256. https://doi.org/10.1364/AOP.9.000218

Rev. Acad. Colomb. Cienc. Ex. Fis. Nat. 46(178):68-89, enero-marzo de 2022
doi: https://doi.org/10.18257/raccefyn.1597

Chen, J., Bao, N., Zhang, L.Y., Zhu, Z. (2018). Optical information authentication using optical encryption and sparsity constraint. Opt. Lasers Eng. **107:** 352-363. https://doi.org/10.1016/j.optlaseng.2018.04.0

Chen, L. & Zhao, D. (2006). Optical image encryption with Hartley transforms. Opt. Lett. **31:** 3438-3440. https://doi.org/10.1364/ol.31.003438

Chen, W., Javidi, B., Chen, X. (2014). Advances in optical security systems. Adv. Opt. Photon. **6:** 120-155. https://doi.org/10.1364/AOP.6.000120

Cheremkhin, P.A., Krasnov, V.V., Rodin, V.G., Starikov, R.S. (2017). QR code optical encryption using spatially incoherent illumination. Laser Phys. Lett. **14:** 026202. https://doi.org/10.1088/1612-202X/aa5242

Cheremkhin, P.A., Evtikhiev, N.N., Krasnov, V.V., Rodin, V.G., Ryabcev, I.P., Shifrina, A.V., Starikov, R.S. (2021a). Lensless optical encryption with speckle-noise suppression and QR codes. Appl. Opt. **60:** 7336-7345. https://doi.org/10.1364/AO.430968

Cheremkhin, P.A., Evtikhiev, N.N., Krasnov, V.V., Ryabcev, I.P., Shifrina, A.V., Starikov., R.S. (2021b). New customizable digital data container for optical cryptosystems. J. Opt. **23:** 115701. https://doi.org/10.1088/2040-8986/ac2166

Dou, S., Shen, X., Zhou, B., Lin, C., Lin, Y., Cheng, Y. (2019). Security-enhanced nonlinear cryptosystem based on joint transform correlator. Opt. Commun. **445:** 211-221. https://doi.org/10.1016/j.optcom.2019.04.011

Evtikhiev, N.N., Krasnov, V.V., Kuzmin, I.D., Molodtsov, D.Y., Rodin, V.G., Starikov, R.S., Cheremkhin, P.A. (2020). QR-code optical encryption in the scheme with spatially incoherent illumination based on two micromirror light modulators. Quantum Electron. **50:** 195-196. https://doi.org/10.1070/QEL17139

Françon, M. (1975). Information processing using speckle patterns. En Dainty, C. Laser speckle and related phenomena (183-185). New York, Estados Unidos: Springer-Verlag Berlin Heidelberg.

Goodman, J.W. (1996). Introduction to Fourier Optics (232-2467) (2da Ed.). New York, Estados Unidos: McGraw-Hill.

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. Nat. Photon. **7:** 343. https://doi.org/10.1038/nphoton.2013.127

Hai, H., Pan, S., Liao, M., Lu, D., He, W., Peng, X. (2019). Cryptanalysis of random-phase-encoding-based optical cryptosystem via deep learning. Opt. Express. **27:** 21204-21213. https://doi.org/10.1364/OE.27.021204

He, X., Jiang, Z., Kong, Y., Wang, S., Liu, C. (2020). Optical multi-image encryption based on focal length multiplexing and multimode phase retrieval. Appl. Opt. **59:** 7801-7812. https://doi.org/10.1364/AO.398459

Henao, R., Rueda, E., Barrera-Ramírez, J.F., Torroba. R. (2010). Noise-free recovery of opto-digital encrypted and multiplexed images. Opt. Lett. **35:** 333-335. https://doi.org/10.1364/OL.35.000333

Hernández, M., Baquero, L., Gil, C., Cardenas, D.A., Gil, A. (2018). Approach to the State of the Art of Ciberdelincuence in Colombia. Int. J. Appl. Eng. Res. **13:** 16648-16655.

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

Jaramillo-Osorio, A., Barrera-Ramírez, J.F., Velez-Zea, A., Torroba, R. (2018). Fractional optical cryptographic protocol for data containers in a noise-free multiuser environment. Opt. Lasers Eng. **102:** 119-125. https://doi.org/10.1016/j.optlaseng.2017.10.008

Jaramillo-Osorio, A., Barrera-Ramírez, J.F., Mira-Agudelo, A, Velez-Zea, A., Torroba, R. (2020a). High performance compact optical cryptosystem without reference arm. J. Opt. **22:** 035702. https://doi.org/10.1088/2040-8986/ab68f0

Jaramillo-Osorio, A., Mira-Agudelo, A., Velez-Zea, A., Barrera-Ramírez, J.F., Torroba, R. (2020b). Secure selective recovery protocol for multiple optically encrypted data. Opt. Laser Eng. **137:** 106383. https://doi.org/10.1016/j.optlaseng.2020.106383

Jaramillo-Osorio, A., Torres-Sepúlveda, W., Velez-Zea, A., Mira-Agudelo, A., Barrera-Ramírez, J.F., Torroba, R. (2022a). Focus-tunable experimental optical cryptosystem. Opt. & Laser Technol. **148:** 107689. https://doi.org/10.1016/j.optlastec.2021.107689

Jaramillo-Osorio, A., Velez-Zea, A., Cabrera, H., Niemela, J., Barrera-Ramírez, J.F., Torroba, R. (2022b). Optical encryption using phase modulation generated by thermal lens effect. J. Opt. **24:** 025702. https://doi.org/10.1088/2040-8986/ac4412

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

Javidi, B., Carnicer, A., Yamaguchi, M., Nomura, T., Pérez-Cabré, E., Millán, M.S., Nishchal, N.K., *et al.* (2016). Roadmap on optical security. J. Opt. **18:** 083001. https://doi.org/10.1088/2040-8978/18/8/083001

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

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

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. https://doi.org/10.1364/AO.39.004117

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. https://doi.org/10.1117/1.600854

Jiao, S., Gao, Y., Lei, T., Yuan, X. (2020). Known-plaintext attack to optical encryption systems with space and polarization encoding. Opt. Express. **28:** 8085-8097. https://doi.org/10.1364/OE.387505

Jiao, S., Zhou, C., Shi, Y., Zou, W., Li, X. (2019). Review on optical image hiding and watermarking techniques. Opt. Laser Technol. **109:** 370-380. https://doi.org/10.1016/j.optlastec.2018.08.011

Kafri, O. & Keren, E. (1987). Encryption of pictures and shapes by random grids. Opt. Lett. **12:** 377-379. https://doi.org/10.1364/OL.12.000377

Karimi, N., Basu, K., Chang, C.H., Fung, J.M. (2021). Hardware Security in Emerging Technologies: Vulnerabilities, Attacks, and Solutions. IEEE Trans. Emerg. Sel. Topics Circuits Syst. **11:** 223-227. https://doi.org/10.1109/JETCAS.2021.3084498

Kaur, M., Singh, S., Kaur, M. (2021). Computational Image Encryption Techniques: A Comprehensive Review. Math. Probl. Eng. **2021:** 5012496. https://doi.org/10.1155/2021/5012496

Kumar, A. & Nishchal, N. (2019). Quick response code and Interference-based optical asymmetric cryptosystem. J. Inf. Secur. Appl. **45:** 35-43. https://doi.org/10.1016/j.jisa.2019.01.004

Kwok, S.K., Ting, J.S.L., Tsang, A.H.C., Lee, W.B., Cheung, B.C.F. (2010). Design and development of a mobile EPC-RFID-based self-validation system (MESS) for product authentication. Comput. Ind. **61:** 624-35. https://doi.org/10.1016/j.compind.2010.02.001

Lázaro, J., Astarloa, A., Rodríguez, M., Bidarte, U., Jiménez, J. (2021). A Survey on Vulnerabilities and Countermeasures in the Communications of the Smart Grid. Electronics. **10:** 1881. https://doi.org/10.3390/electronics10161881

Li, H., Guo, C., Muniraj, I., Schroeder, B.C., Sheridan, J.T., Jia, S. (2017a). Volumetric Light-field Encryption at the Microscopic Scale. Sci. Rep. **7:** 40113. https://doi.org/10.1038/srep40113

Li, L., Jun Cui, T., Ji, W., *et al.* (2017b). Electromagnetic reprogrammable coding-metasurface holograms. Nat. Commun. **8:** 197. https://doi.org/10.1038/s41467-017-00164-9

Li, W.S., Shen, Y., Chen, Z.J., Cui, Q., Li, S.S., Chen, L.J. (2017c). Demonstration of patterned polymer-stabilized cholesteric liquid crystal textures for anti-counterfeiting two-dimensional barcodes. Appl. Opt. **56:** 601-606. https://doi.org/10.1364/AO.56.000601

Li, X., Zhao, M., Zhou, X., Wang, Q.H. (2018). Ownership protection of holograms using quick-response encoded plenoptic watermark. Opt. Express. **26:** 30492-30508. https://doi.org/10.1364/OE.26.030492

Liang, J., Gao, L., Hai, P., Li, C., Wang, L.V. (2015). Encrypted Three-dimensional Dynamic Imaging using Snapshot Time-of-flight Compressed Ultrafast Photography. Sci. Rep. **5:** 15504. https://doi.org/10.1038/srep15504

Liansheng, S., Cong, D., Minjie, X., Ailing, T., Anand. A. (2019). Information encryption based on the customized data container under the framework of computational ghost imaging. Opt. Express. **27:** 16493-16506. https://doi.org/10.1364/OE.27.016493

Lim, K.T.P., Liu, H., Liu, Y., Yang, J.K.W. (2019). Holographic colour prints for enhanced optical security by combined phase and amplitude control. Nat. Commun. **10:** 25. https://doi.org/10.1038/s41467-018-07808-4

Lima, J.B., Madeiro, F., Sales, F.J.R. (2015). Encryption of medical images based on the cosine number transform. Signal Process. Image Commun. **35:** 1-8. https://doi.org/10.1016/j.image.2015.03.005

Lin, C., Shen, X., Hua, B., Wang, Z. (2015). Three-dimensional polarization marked multiple-QR code encryption by optimizing a single vectorial beam. Opt. Commun. **352:** 25-32. https://doi.org/10.1016/j.optcom.2015.04.068

Liu, S., Guo, C., Sheridan, J.T. (2014). A review of optical image encryption techniques. Opt. Laser Technol. **57:** 327-342. https://doi.org/10.1016/j.optlastec.2013.05.023

Liu, Z., Xu, L., Lin, C., Liu, S. (2010). Image encryption by encoding with a nonuniform optical beam in gyrator transform domains. Appl. Opt. **49:** 5632-5637. https://doi.org/10.1364/AO.49.005632

Lu, X.J., Yu, F.T.S., Gregory, D.A. (1990). Comparison of Vander Lugt and joint transform correlators. Appl. Phys. B. **51:** 153-164. https://doi.org/10.1007/BF00326017

Markman, A., Wang, J., Javidi, B. (2014). Three-dimensional integral imaging displays using a quick-response encoded elemental image array. Optica. **1:** 332-335. https://doi.org/10.1364/OPTICA.1.000332

Meng, F., Umair, M.M., Zhang, S, Meng, Y., Tang, B. (2021a). Facile fabrication of encryption composite materials with trilayer quasi-amorphous heterostructure. Sci China Mater. **64:** 909-919. https://doi.org/10.1007/s40843-020-1500-9

Meng, Y., Chen, Y., Lu, L., *et al.* (2021b). Optical meta-waveguides for integrated photonics and beyond. Light Sci. Appl. **10:** 235. https://doi.org/10.1038/s41377-021-00655-x

Millán, M.S. (2012). Advanced optical correlation and digital methods for pattern matching-50th anniversary of Vander Lugt matched filter. J. Opt. **14:** 10300. https://doi.org/10.1088/2040-8978/14/10/103001

Mosso, F., Tebaldi, M., Barrera-Ramírez, J.F., Bolognini, N., Torroba, R. (2011a). All-optical encrypted movie. Opt. Express. **19:** 5706-5712. https://doi.org/10.1364/OE.19.005706

Mosso, F., Tebaldi, M., Barrera-Ramírez, J.F., Bolognini, N., Torroba, R. (2011b). Pure optical dynamical color encryption. Opt. Express. **19:** 13779-13786. https://doi.org/10.1364/OE.19.013779

Mughaid, A., Al-Arjan, A., Rasmi, M., AlZu'bi, S. (2021). Intelligent security in the era of AI: The key vulnerability of RC4 algorithm. International Conference on Information Technology (ICIT) (691-694). https://doi.org/10.1109/ICIT52682.2021.9491709.

Nomura, T. & Javidi B. (2000). Optical encryption using a joint transform correlator architecture. Opt. Eng. **39:** 2031-2035. https://doi.org/10.1117/1.1304844

Nomura, T., Pérez-Cabré, E., Millán, M.S., Javidi, B. (2009). Optical Techniques for Information Security. Proc. IEEE. **97:** 1128-1148. https://doi.org/10.1109/JPROC.2009.2018367

Paganin, D.M. (2011). Spotlight on Optics: All-optical encrypted movie. Optica Publishing Group. Fecha de consulta: noviembre de 2021. Disponible en: https://www.osapublishing.org/spotlight/summary.cfm?uri=oe-19-6-5706

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. https://doi.org/10.1364/OL.31.001044

Petriashvili, G., Devadze, L., Chanishvili, A., Zurabishvili, C., Sepashvili, N., Ponjavidze, N., De Santo, M.P., Barberi, R. (2018). Spiropyran doped rewritable cholesteric liquid crystal polymer film for the generation of quick response codes. Opt. Mater. Express. **8:** 3708-3716. https://doi.org/10.1364/OME.8.003708

Pile, D. (2010). Optical encryption: The ghost holds a secret. Nat. Photon. **4:** 587. https://doi.org/10.1038/nphoton.2010.206

Ponjavidze, N., De Santo, M.P., Barberi, R. (2018). Spiropyran doped rewritable cholesteric liquid crystal polymer film for the generation of quick response codes. Opt. Mater. Express. **8:** 3708-3716. https://doi.org/10.1364/OME.8.003708

Qin, Y., Gong, Q., Wang, H., Wang, Z. (2018a). Authentication-based optical cryptosystem with noise-free information retrieval. Opt. Commun. **426:** 325-332. https://doi.org/10.1016/j.optcom.2018.05.079

Qin, Y., Wang, Z., Wang, H., Gong, Q., Zhou, N. (2018b). Robust information encryption diffractive-imaging-based scheme with special phase retrieval algorithm for a customized data container. Opt. Lasers Eng. **105:** 118-124. https://doi.org/10.1364/OE.27.016493

Qin., Y. & Zhang, Y. (2017). Information Encryption in Ghost Imaging with Customized Data Container and XOR Operation. IEEE Photon. J. **9:** 1-8. https://doi.org/10.1109/JPHOT.2017.2690314

Qu, G., Yang, W., Song, Q., Liu, Y., Qiu, C.W., Han, J., Tsai, D.P., Xiao, S. (2020). Reprogrammable meta-hologram for optical encryption. Nat. Commun. **11:** 5484. https://doi.org/10.1038/s41467-018-07808-4

Refregier, P. & Javidi, B. (1995). Optical image encryption based on input plane and Fourier plane random encoding. Opt. Lett. **20:** 767-769. https://doi.org/10.1364/OL.20.000767

Reshef, O., DelMastro, M.P., Bearne, K.K.M. *et al.* (2021). An optic to replace space and its application towards ultra-thin imaging systems. Nat. Commun. **12:** 3512. https://doi.org/10.1038/s41467-021-23358-8

Rueda, E., Barrera-Ramírez J.F., Henao, R., Torroba, R. (2009a). Optical encryption with a reference wave in a joint transform correlator architecture. Opt. Commun. **282:** 3243-3249. https://doi.org/10.1016/j.optcom.2009.05.022

Rueda, E., Barrera-Ramírez J.F., Henao, R., Torroba, R. (2009b). Lateral shift multiplexing with a modified random mask in a joint transform correlator encrypting architecture. Opt. Eng. **48:** 27006. https://doi.org/10.1117/1.3080753

Saini, N. & Sinha, A. (2015). Video encryption using chaotic masks in joint transform correlator. J. Opt. **17:** 035701. https://doi.org/10.1088/2040-8978/17/3/035701

Shi, X. & Zhao, D. (2011). Color image hiding based on the phase retrieval technique and Arnold transform. Appl. Opt. **50:** 2134-2139. https://doi.org/10.1364/AO.50.002134

Singh, M., Kumar, A., Singh, K. (2008). Multiplexing in optical encryption by using an aperture system and a rotating sandwich random phase diffuser in the Fourier plane. Opt. Lasers Eng. **46:** 243-251. https://doi.org/10.1016/j.optlaseng.2007.10.001

Singh, M., Kumar, A., Singh, K. (2009). Encryption and decryption using a sandwich phase diffuser made by using two speckle patterns and placed in the Fourier plane: Simulation results. Optik. **120:** 916-922. https://doi.org/10.1016/j.ijleo.2008.03.025

Situ, G. & Zhang, J. (2005). Multiple-image encryption by wavelength multiplexing. Opt. Lett. **30:** 1306-1308. https://doi.org/10.1364/OL.30.001306

Sui, L., Xu, M., Tian, A. (2017). Optical noise-free image encryption based on quick response code and high dimension chaotic system in gyrator transform domain. Opt. Laser Eng. **91:** 106-114. https://doi.org/10.1364/AO.59.000474

Tanha, M., Kheradmand, R., Ahmadi-Kandjani, S. (2012). Gray-scale and color optical encryption based on computational ghost imaging. Appl. Phys. Lett. **101:** 28-31. https://doi.org/10.1063/1.4748875

Tebaldi M., Horrillo, S., Pérez-Cabré, E., Millán, M.S., Amaya, D., Torroba. R. *et al.* (2011). Experimental color encryption in a joint transform correlator architecture. J. Phys. Conf. Ser. **274:** 012054. https://doi.org/10.1088/1742-6596/274/1/012054

Ting, S.L. & Tsang, A.H.C. (2013). A two-factor authentication system using Radio Frequency Identification and watermarking technology. Comput. Ind. **64:** 268-79. https://doi.org/10.1016/j.compind.2012.11.002

Torroba, R. & Barrera-Ramírez, J.F. (2015). Protección de datos usando un sistema experimental de encriptación de correlador de transformada conjunta. Rev. Acad. Colomb. Cienc. Ex. Fis. Nat. **39:** 55-60. https://doi.org/10.18257/raccefyn.263

Treacy, S. (2013). The creative power of Colaboration. The world Academy of Sciences TWAS. Fecha de consulta: noviembre de 2021. Disponible en: https://twas.org/article/creative-power-collaboration

Trejos, S., Barrera-Ramírez, J.F., Torroba, R. (2015). Optimized and secure technique for multiplexing QR code images of single characters: Application to noiseless messages retrieval. J. Opt. **17:** 085702. https://doi.org/10.1088/2040-8978/17/8/085702

Unnikrishnan, G., Joseph, J., Singh, K. (1998). Optical encryption system that uses phase conjugation in a photorefractive crystal. Appl. Opt. **31:** 8181-8186. https://doi.org/10.1364/AO.37.008181

Vander-Lugt, A. (1964). Signal detection by complex spatial filtering. IEEE Trans. Inf. Theory. **10:** 139-145. https://doi.org/10.1109/TIT.1964.1053650

Velez-Zea, A., Barrera-Ramírez, J.F., Torroba, R. (2016a). Three-dimensional joint transform correlator cryptosystem. Opt. Lett. **41:** 599-602. https://doi.org/10.1364/OL.41.000599

Velez-Zea A., Barrera-Ramírez J.F., Torroba, R. (2016b). Customized data container for improved performance in optical cryptosystems. J. Opt. **18:** 125702. https://doi.org/10.1088/2040-8978/18/12/125702

Velez-Zea, A., Barrera-Ramírez, J.F., Torroba, R. (2017a). Experimental optical encryption of grayscale information. Appl. Opt. **56:** 5883-5889. https://doi.org/10.1364/AO.56.005883

Rev. Acad. Colomb. Cienc. Ex. Fis. Nat. 46(178):68-89, enero-marzo de 2022
doi: https://doi.org/10.18257/raccefyn.1597

Velez-Zea, A., Barrera-Ramírez, J.F., Torroba, R. (2017b). Innovative speckle noise reduction procedure in optical encryption. J. Opt. **19:** 055704. https://doi.org/10.1088/2040-8986/aa6526

Velez-Zea, A., Barrera-Ramírez, J.F., Torroba, R. (2017c). Cryptographic salting for security enhancement of double random phase encryption schemes. J. Opt. **19:** 105703. https://doi.org/10.1088/2040-8986/aa8738

Velez-Zea, A., Barrera-Ramírez, J.F., Torroba, R. (2018). Optimized random phase encryption. Opt. Lett. **43:** 3558-3561. https://doi.org/10.1364/OL.43.003558

Velez-Zea, A., Barrera-Ramirez, J.F., Torroba, R. (2019). Secure real-time generation and display of color holographic movies. Opt. Lasers Eng. **122:** 239-244. https://doi.org/10.1016/j.optlaseng.2019.06.010

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. https://doi.org/10.1088/2040-8978/15/2/025401

Vilardy, J.M., Millán, M.S., Pérez-Cabré, E. (2014). Nonlinear optical security system based on a joint transform correlator in the Fresnel domain. Appl. Opt. **53:** 1674. DOI: 10.1364/AO.53.001674

Vilardy, J.M., Millán, M.S., Pérez-Cabré, E. (2017). Nonlinear image encryption using a fully phase nonzero-order joint transform correlator in the Gyrator domain. Opt. Lasers Eng. **89:** 88-94. https://doi.org/10.1016/j.optlaseng.2016.02.013

Vilardy, J.M., Barba, L., Torres, C.O. (2019a). Image Encryption and Decryption Systems Using the Jigsaw Transform and the Iterative Finite Field Cosine Transform. Photonics. **6:** 121 (2019a). https://doi.org/10.3390/photonics6040121

Vilardy, J.M., Pérez, R.A., Torres, C.O. (2019b). Optical Image Encryption Using a Nonlinear Joint Transform Correlator and the Collins Diffraction Transform. Photonics. **6:** 115. https://doi.org/10.3390/photonics6040115

Verified Market Research-VMR. Encryption Software Market Size And Forecast to 2025. Fecha de consulta noviembre de 2021. Disponible en: https://www.verifiedmarketresearch.com/product/global-encryption-software-market-size-and-forecast-to-2025/

Wang, C.H., Hwang, Y.S., Wang, H.C., Wang, Y.L, Tsai, K.Y. (2020). Microstructure overlapping image application with optical decryption. J. Opt. Soc. Am. A **37:** 1361-1368. https://doi.org/10.1364/JOSAA.393182

Wang, K., Liang, J., Chen, R., Gao, Z., Zhang, C., Yan, Y., Yao, J., Zhao, Y.S. (2021). Geometry-Programmable Perovskite Microlaser Patterns for Two-Dimensional Optical Encryption. Nano Lett. **21:** 6792-6799. https://doi.org/10.1021/acs.nanolett.1c01423

Wang, W.C. & Schipf, D.R. (Junio 13, 2019). Fluid-optical encryption system and method thereof. US patent 0182407 A1.

Wang, L., Wu, Q., Situ, G. (2019). Chosen-plaintext attack on the double random polarization encryption. Opt. Express **27:** 32158-32167. https://doi.org/10.1364/OE.27.032158

Wang, Q., Rogers, E., Gholipour, B. *et al.* (2016). Optically reconfigurable metasurfaces and photonic devices based on phase change materials. Nat. Photon. **10:** 60-65. https://doi.org/10.1038/nphoton.2015.247

Weaver, C.S., Goodman, J.W. (1966). A Technique for Optically Convolving Two Functions. Appl. Opt. **5:** 1248-1249. https://doi.org/10.1364/AO.5.001248

Wu, H., Li, Q., Meng, X., Yang, X., Liu, S., Yin, Y. (2021). Cryptographic analysis on an optical random-phase-encoding cryptosystem for complex targets based on physics-informed learning. Opt. Express. **29:** 33558-33571. https://doi.org/10.1364/OE.441293

Wu, J., Wang, J., Nie, Y., Hu. L. (2019). Multiple-image optical encryption based on phase retrieval algorithm and fractional Talbot effect. Opt. Express. **27:** 35096-35107. https://doi.org/10.1364/OE.27.035096

Yan, A., Lu, C., Yu, J., Tang, M., Dong, J., Hu, Z., Zhang, H. (2019). Multiple-image encryption based on angular-multiplexing holography with quick response code and spiral phase keys. Appl. Opt. **58:** G6-G10.

Yong-Liang, X., Xin, Z., Sheng, Y., Qiang, L., Yang-Cong, L. (2009). Multiple-image optical encryption: an improved encoding approach. Appl. Opt. **48:** 2686-2692. https://doi.org/10.1364/AO.48.002686

Zhang, L., Wang, Y., Li, D-H, Li, Q., Zhao, W., Li, X. (2021). Cryptanalysis for a light-field 3D cryptosystem based on M-cGAN. Opt. Lett. **46:** 4916-4919. https://doi.org/10.1364/OL.436049

Zhang, L., Wang, Y., Zhang, D. (2022). Research on multiple-image encryption mechanism based on Radon transform and ghost imaging. Opt. Commun. **504:** 127494. https://doi.org/10.1016/j.optcom.2021.127494

Zhong, Z., Zhang, Y., Shan, M., Wang, Y., Zhang, Y., Xie, H. (2014). Optical movie encryption based on a discrete multiple-parameter fractional Fourier transform. J. Opt. **16:** 125404. https://doi.org/10.1088/2040-8978/16/12/125404

Zhou, N., Li, H., Wang, D., Pan, S., Zhou, Z. (2015). Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform. Opt. Commun. **343:** 10-21. https://doi.org/10.1016/j.optcom.2014.12.084

Zhu, L., Wang, A., Deng, M., Lu, B., Guo, X. (2021). Experimental demonstration of multiple dimensional coding decoding for image transfer with controllable vortex arrays. Sci. Rep. **11:** 12012. https://doi.org/10.1038/s41598-021-91553-0

Zhu, Y., Xu, W., Shi, Y. (2019). High-capacity encryption system based on single-shot-ptychography encoding and QR code. Opt. Commun. **435:** 426-432. https://doi.org/10.1016/j.optcom.2018.11.040