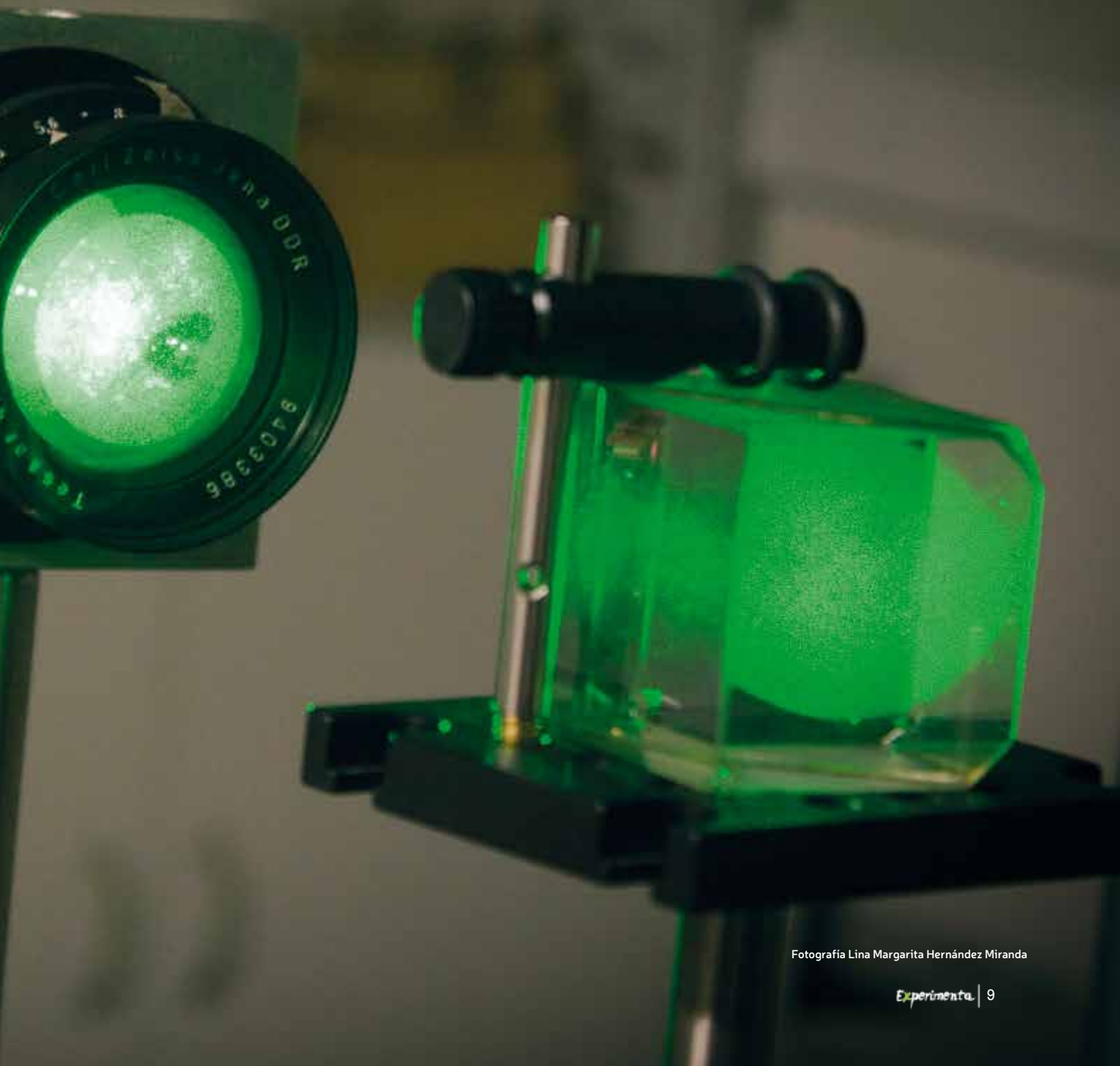
ENCRIPTANDO INFORMACIÓN

Gobiernos, bancos, empresas, enamorados furtivos y hasta espías... Muchos tienen información que quisieran que solo su destinatario conozca. Buscando proteger datos, los investigadores de la UdeA exploran la más impensada herramienta: la luz.

*Por: Sergio A. Urquijo Morales**



Fotografía Lina Margarita Hernández Miranda

Si yo fuera un espía, necesitaría enviarles a mis jefes claves de cajas fuertes, fotos comprometedoras, diagramas de complejos dispositivos, mapas, planos de la sala del museo donde está el diamante y, por qué no, cartas de amor furtivo... aunque esas probablemente no irían para mis jefes.

Lo cierto es que, sea una imagen, un texto, un video o una lista de datos, me importaría que fueran tan secretos que nadie no autorizado pudiera verlos. Es decir: tendría que encriptarlos.

El profesor John Fredy Barrera, coordinador del Grupo de Óptica y Fotónica (GOF) de la Universidad de Antioquia, señala para la criptografía usos esenciales en nuestro mundo de información, como "protección de claves de bancos y datos relativos a la privacidad de las personas, que necesitan ser encriptados antes de ser enviados, especialmente si se usa un medio tan vulnerable como es internet". Porque, como sabemos, en el mundo digital pululan los hackers, esas personas que logran romper las barreras de seguridad más tenaces que las instituciones han desarrollado para proteger datos.

Por eso la idea de encriptación óptica ha sido bienvenida en el mundo. Es muy segura, pues usa un sistema físico compuesto por una fuente de iluminación láser, lentes, espejos, difusores (vidrios esmerilados), entre otros elementos. El más temible hacker del mundo no podría descifrar un mensaje así encriptado a menos que tenga la llave. Y esa llave depende de características físicas, no digitales, que solo el equipo de investigadores conoce.

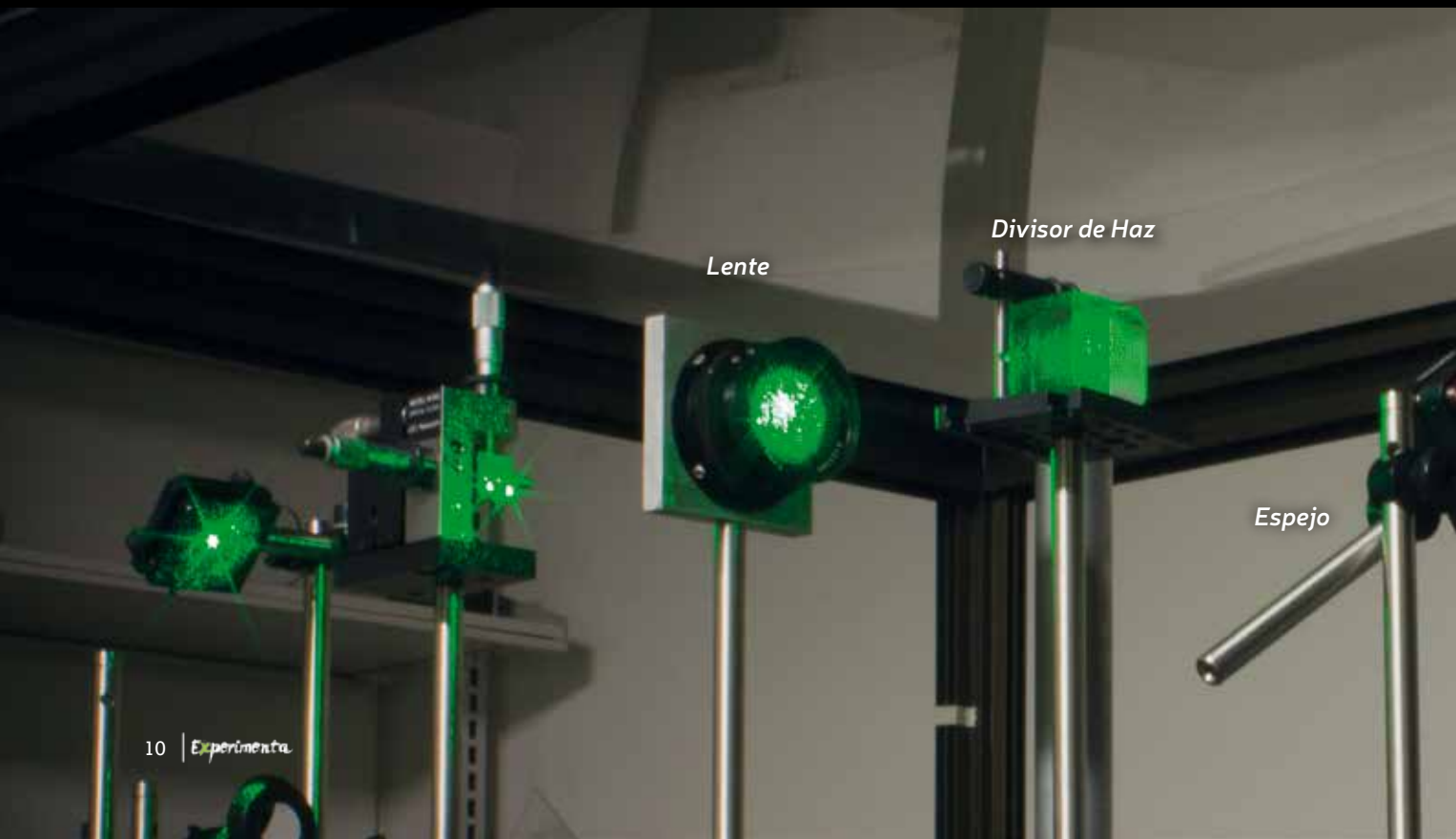
Lo que ocurre en el laboratorio del Grupo de Óptica y Fotónica parece sencillo, pero es sofisticado. La imagen que se quiere encriptar se proyecta en un montaje de laboratorio que recuerda los primeros pasos de la holografía, pero con toda la potencia del siglo XXI.

Lo que ocurre en el laboratorio del grupo de Óptica y Fotónica parece sencillo, pero es sofisticado. La imagen que se quiere encriptar se proyecta en el montaje de laboratorio, que es similar a un montaje clásico para hacer holografía, pero con toda la potencia del siglo XXI.

"Digitalmente se proyecta una imagen o un código visual sobre un elemento", explica el profesor Barrera. "Este se ilumina con luz láser y la luz que sale es procesada por el sistema físico de encriptación. Al final hay una cámara que recoge la información procesada".

El sistema óptico transforma la imagen en un patrón aleatorio. "Los elementos que componen el sistema procesan la luz que proviene de la imagen para convertirla en el dato encriptado". explica Barrera.

Los parámetros físicos de la iluminación y los demás elementos del sistema definen la seguridad y las características de la imagen encriptada. En particular, la rugosidad de los vidrios despulidos que posee el sistema es completamente aleatoria, por lo que es imposible que alguien que no tenga acceso



al vidrio específico usado, o a sus características exactas, pueda encontrar el patrón de difusión. "No hay dos vidrios iguales, aunque los pulan de la misma manera", comenta el profesor Barrera.

Cuando la información obtenida en el sistema físico se procesa digitalmente se obtienen dos elementos digitales: la imagen ya codificada y una 'llave', la clave para decodificar. Eso se envía por correo al usuario, que podrá recuperar la información con una aplicación sencilla para computador. "Así, hay una parte óptica y una digital, que permiten que el usuario autorizado recupere la información sin necesidad de contar con un sistema óptico", indica el profesor Barrera.

El desarrollo de esta línea en la Universidad comenzó hace diez años, alentado por una fructífera relación con el profesor Roberto Torroba, investigador del Centro de Investigaciones Ópticas (CIOp) en La Plata, Argentina, centro que ha colaborado activamente en la obtención del doctorado de varios profesores del GOF. "El grupo de la Universidad de Antioquia fue muy receptivo a propuestas que representaban un audaz cambio de dirección en las investigaciones", comenta Torroba. Y esa audacia creció hacia el desarrollo de soluciones para los desafíos que iban apareciendo, porque la investigación es así: una respuesta te genera otra pregunta, repleta de conocimiento por explorar.

Pero ¿y si el mensaje que quiero encriptar no es una imagen o un texto breve, sino una carta?

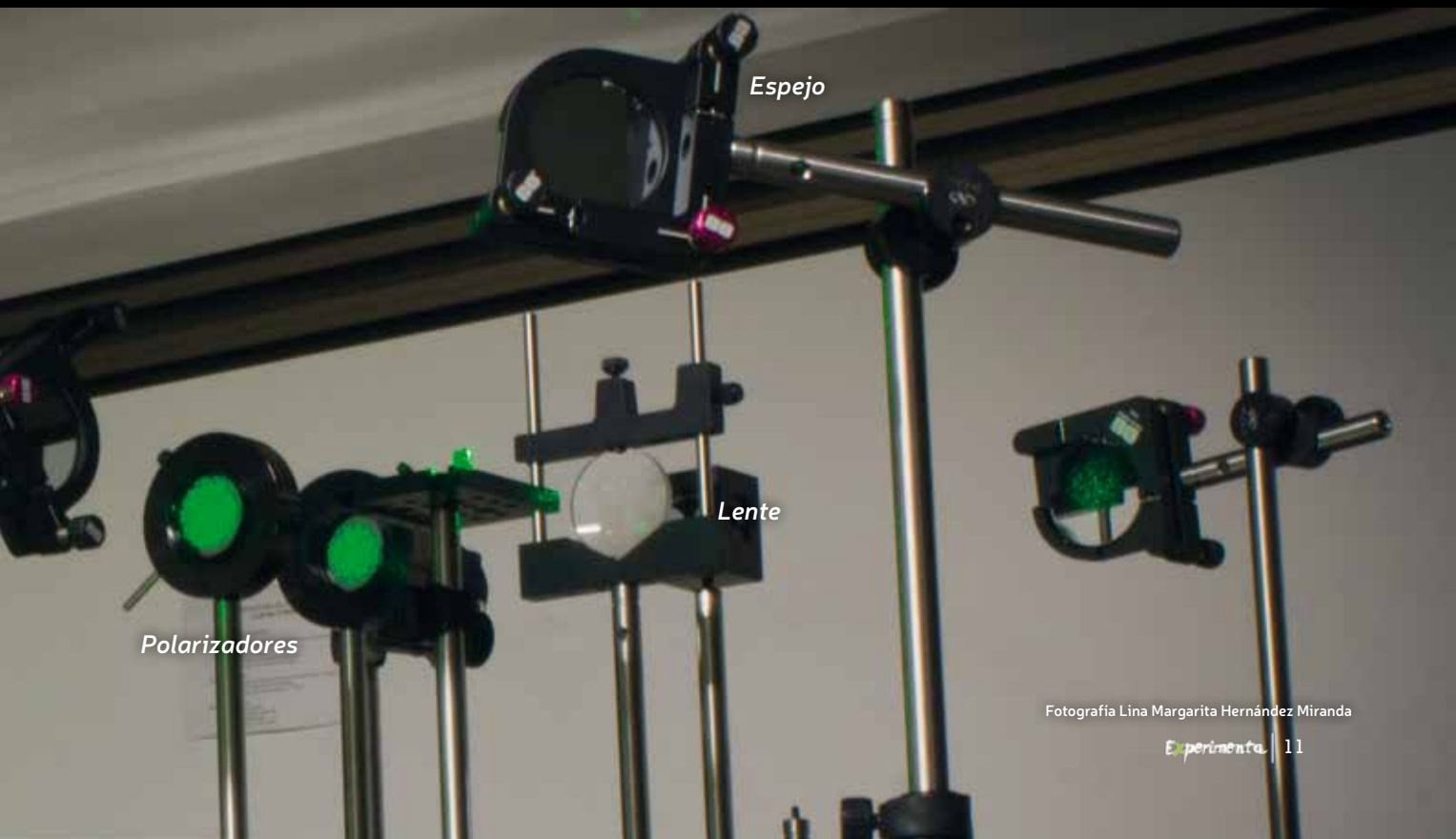
Al inicio, debido a efectos de difracción de la luz, un texto para encriptar debía ser corto, pues mientras más elementos pequeños hubiera en la imagen más complejo sería el encriptamiento y conduciría a distorsión. Pero los profesores Barrera y Torroba, con la participación de un estudiante del grupo, Alejandro Vélez, idearon y desarrollaron un teclado virtual que permite encriptar textos de cualquier longitud.

La idea es esta: si necesitamos proteger un texto, digamos, una carta, puede encriptarse letra por letra, caracter por caracter, con el sistema óptico ya probado. "Al encriptar cada letra por separado, en vez de todo el teclado al mismo tiempo, se asegura la recuperación clara de cada caracter", indica Vélez.

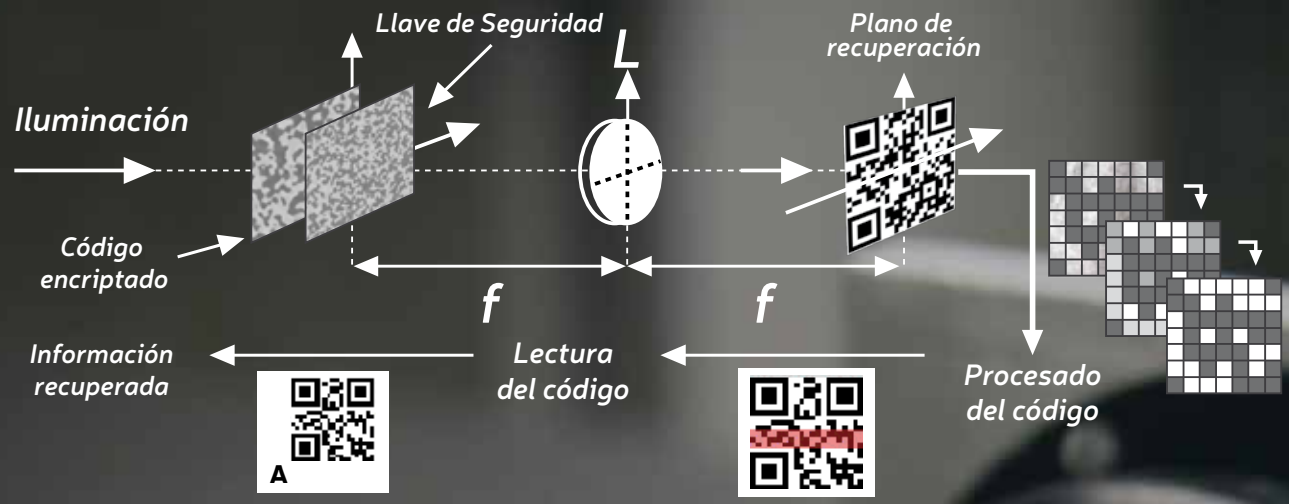
Luego los caracteres son reunidos en un solo archivo digital por medio de un procedimiento que se usa en muchas áreas de la tecnología: el multiplexado. Multiplexar significa combinar, y es el método por el que varias señales se combinan para ser enviadas por un solo canal o, como en este caso, para constituir un solo archivo.

Además, para aumentar la seguridad, estos caracteres ya encriptados y digitalizados estarán repartidos aleatoriamente gracias a un algoritmo digital. Así, quien lograra tener la primera llave no podría, aun así, reconstruir el mensaje, a menos que tuviera el orden de los caracteres para poder reconstruir un texto que recibirá desordenado.

De este modo podrían encriptarse y protegerse todas las novelas de Balzac o una secreta carta de amor. Y por supuesto, instrucciones, códigos, una



Fotografía Lina Margarita Hernández Miranda



Sistema de Recuperación. f: longitud focal de la lente L. Ilustración Grupo de Óptica y Fotónica

lista de claves bancarias y otros textos largos menos románticos, pero influyentes en nuestra era de la información.

Muy bien, pero no me gusta esa apariencia borrosa de las imágenes luego de ser desencriptadas.

Ese es el efecto que llamamos ruido. "Como no es un sistema digital sino físico, hay limitaciones que no podemos evitar" comenta el profesor Barrera. "Por eso al recuperar la imagen o el mensaje encriptado, queda con esa distorsión".

Eso me causaría problemas si yo quiero encriptar un delicado mensaje al presidente chino. ¿Qué tal si no puede leerlo bien y entiende otra cosa? ¿Causaré un conflicto internacional?
Afortunadamente, en las universidades de Antioquia y de La Plata pensaron en un recurso muy práctico: los códigos QR. Son esos cuadrados que en ciertos productos o empaques pueden ser leídos con un smartphone y remiten normalmente a un sitio web. Son un tipo de código de barras, pero dispuesto en una matriz rectangular. Los inventó la Denso Corporation, una empresa japonesa que elabora partes para autos, con el fin de reconocer rápidamente las piezas y organizarlas.

"Un código QR tiene muchas ventajas: se puede leer en cualquier posición, incluso si tiene algo de ruido o si le falta un pedazo, si está sucio, o detrás de un vidrio", explica John Fredy Barrera.

Denso Corporation patentó el invento pero lo dejó libre, de modo que no hay que pagar la propiedad intelectual para usarlo. Se hizo muy popular en todo el mundo, especialmente en mercadeo, publicidad y logística. Sus propiedades lo hacen perfecto para contener información (como la url de un sitio web, cifras y datos).

En el grupo de Óptica y Fotónica vieron la potencia de este sistema y fueron los primeros en traer el concepto de contenedor a la encriptación óptica. Se puede leer un texto aunque tenga ruido óptico. Y he ahí la solución: antes de encriptar mi información, la codifico en un QR y es esa imagen la que será encriptada ópticamente.

"Como el código se lee bien incluso si hay ruido, la información contenida podrá recuperarse sin ninguna distorsión", concluye Barrera.

Me da por querer encriptar una fotografía con este sistema, pero el profesor Barrera me explica que hay limitaciones en la cantidad de información: "El código QR, mientras más tolerante al ruido sea, es más complicado y requiere más capacidad de procesamiento y algoritmos que aún están poco desarrollados. Por eso no se logra todavía convertir eficientemente una imagen a QR, así que seguimos trabajando con datos, como números". Quién sabe en un futuro no lejano...

¿Y si quiero encriptar un video?

Para aumentar la seguridad, los caracteres encriptados y digitalizados se distribuyen aleatoriamente con otro algoritmo digital. Quien lograse tener la primera llave no podría reconstruir el mensaje, a menos que tuviera el orden de los caracteres para poder reconstruir un texto que recibiría desordenado.

Porque ahora se me ocurre que enviaría mis declaraciones secretas en video. Y si fuera un productor de cine o TV, tal vez quisiera proteger mis productos de la piratería, de forma que sólo quien tenga la clave pueda verlos.

Ese problema ya fue atendido por el grupo. En general, un video es una secuencia de imágenes

fijas, que al pasar con cierta frecuencia es visto como un continuo. Así se creó el cine: tomando y luego proyectando fotografías a gran velocidad; si pasan más de 25 imágenes por segundo, el cerebro es incapaz de darse cuenta que se están proyectando imágenes secuencialmente y tenemos la ilusión de estar viendo una escena con movimiento.

"En la encriptación óptica se protege un dato: una imagen o una foto. Cuando son muchos datos, hay limitaciones, aparece un ruido", señala Barrera. "Nosotros logramos solucionar ese problema y encriptar primero videos a blanco y negro, y luego a color. Para color se necesita encriptar tres canales diferentes". Por esto, en este proceso también se requiere multiplexar.

Varios artículos donde el grupo comunicó al mundo científico sus avances sobre encriptación óptica de video y de códigos QR, disminución de ruido al recuperar el dato y encriptación de textos largos, fueron destacados por revistas y entidades como la revista Nature Photonics y la Academia Mundial de las Ciencias. "La clave fue haber atendido una necesidad del mundo real, con muchas aplicaciones, lo que atrae interés de otros investigadores", opina Barrera.

En la línea de encriptación óptica han participado John Fredy Barrera, Alejandro Mira, Alejandro Vélez, Edgar Rueda, Rodrigo Henao, Carlos Ríos y Sorayda Trejos del GOF; y Roberto Torroba, Myrian Tebaldi y Roberto Bolognini, del CIOp. Pura cooperación suramericana para la ciencia mundial. Como Torroba lo indica, "estamos en permanente evolución y actualización, listos para seguir creciendo en conjunto. La gran ventaja de ser pioneros en un tema es que se marca el rumbo".

Bueno, ya podré ser un espía más eficiente. ¿Qué seguirá en el grupo?

Con tantos avances en tan poco tiempo, se puede esperar que vendrán muchos más. Más investigación en temas como encriptar datos tridimensionales, y quizás llegar al mercado. "Si uno crea un sistema de seguridad y quiere patentarlo y venderlo hay que probarlo", explica John Fredy Barrera. "Se permite que un hacker introduzca diferentes señales en el sistema. Si él no es capaz de recuperar la llave, el sistema es seguro".

Si el material encriptado que yo envíe fuera capturado por agentes enemigos, y ellos quisieran reconstruir el sistema óptico para revelarlo, sería prácticamente imposible. Como indica el investigador, "cuando uno tiene el sistema no solo tiene que conocer la llave, sino también otros elementos, como la iluminación y los demás parámetros del sistema físico".

La idea del grupo es hacer estos sistemas más compactos, para poderlos comercializar. Me imagino una especie de encriptador óptico portátil, y no veo la hora de que sea desarrollado por el Grupo de Óptica y Fotónica. Eso me haría un espía muy sofisticado, todo un James Bond. Pero por ahora, conocer los sistemas ópticos de encriptación y el poder de la luz para proteger la información es una aventura más que suficiente.

* Periodista

GLOSARIO:

Óptica: Es el área de la física que estudia la luz, su comportamiento y sus interacciones con la materia y otras formas de energía. También genera instrumentos de producción, control y medición de la luz. Los primeros trabajos de óptica datan de hace 1000 años, cuando el científico árabe Al-Haytam estudió fenómenos como la visión y los espejos.

Fotónica: Es el campo que estudia la luz desde sus fundamentos cuánticos, y aplica estos conocimientos a su generación, detección y comportamiento, y a la construcción de instrumentos para estudiarla. Algunos la entienden como una etapa contemporánea de la óptica.

Láser: Láser es el dispositivo que emite luz amplificada y coherente, es decir, luz generada de modo que todas sus partículas van con la misma frecuencia y fase y en la misma dirección. Su potencia y precisión hace que se use en campos tan variados como telecomunicaciones, cirugías y espectáculos.

Holografía: Es la técnica de generar imágenes tridimensionales. Un holograma, la imagen generada por el proceso, es como una fotografía, pero no tiene un soporte físico sino de luz misma, y al ser observado desde cualquier ángulo guarda la tridimensionalidad del objeto representado.

Difracción: Es un tipo de interferencia que se da cuando una onda encuentra un obstáculo o pasa por una rendija. Se da en cualquier tipo de onda, desde el sonido a la radiación electromagnética e incluso en la materia, a escala subatómica.

Criptografía: Es el desarrollo de técnicas para ocultar mensajes de manera que solo su destinatario pueda leerlos. A la vez es la búsqueda de métodos matemáticos y físicos para describir mensajes encriptados por otros.

Fotografía Lina Margarita Hernández Miranda