ESTUDIO DE LAS LIMITACIONES DE LOS DISPOSITIVOS DE ENCRIPTACIÓN ÓPTICA MÚLTIPLE

Myrian Tebaldi[1], John Fredy Barrera[2], Néstor Bolognini[1], Roberto Torroba[1]

[1]UID OPTIMO, Facultad de Ingenieria, Universidad Nacional de La Plata y Centro Investigaciones Ópticas (CONICET La Plata-CIC), La Plata, Argentina

[2]Grupo de Óptica y Fotónica, Instituto de Física, Universidad de Antioquia, Medellín, Colombia

Email: robertot@ciop.unlp.edu.ar

Palabras Claves: encriptación, óptica, 4f, ruido, solapamiento

Resumen

En los últimos años ha aumentado notablemente el número de transacciones financieras realizadas por internet y conjuntamente se han incrementado los problemas de seguridad. En este contexto, se han propuesto e implementado sistemas ópticos para el cifrado de datos, los cuales han demostrado que el procesamiento óptico permite una manipulación segura de la información. Entre ellos, los dispositivos más usados y desarrollados se basan en el empleo de máscaras aleatorias de fase para transformar los datos en una distribución de ruido blanco (imagen encriptada). El proceso de desencriptación se realiza con la máscara de fase correcta (llave de seguridad), sin la cual se hace imposible recuperar el dato original.

En la actualidad se buscan nuevas estrategias para aumentar la cantidad de datos codificados a ser almacenados. Los resultados obtenidos en arreglos de encriptación múltiple permitieron verificar que a medida que se incrementa el número de datos, en esa misma medida se degradan los datos recuperados en la etapa de decodificación. Este deterioro se debe al solapamiento y al ruido generado por los datos no desencriptados. Este hecho representa una gran limitación para la aplicación práctica de los sistemas ópticos de seguridad cuando se involucran múltiples datos. En ese sentido, se esboza una solución que permite eliminar el deterioro a través del reposicionado de la información asociada a cada uno de los datos de entrada.

1. Introducción

Los datos convencionales de uso masivo trasmitidos a traves de los sistemas informáticos son factibles de ser falsificados. La idea de los dispositivos codificación es que permitan que la información a ser transmitida y almacenada sea accesible solo a personas autorizadas. A los procedimientos ópticos usados para cifrar información se les conocen como técnicas de encriptación. La encriptación es la transformación de los datos e imágenes de forma que sea imposible recuperarlos sin el adecuado conocimiento de la llave de seguridad con la cual se codificado. A la transformación del dato encriptado de nuevo en una forma inteligible se la conoce con el nombre de desencriptación. Cabe destacar que para acceder a la información el usuario autorizado debe poseer la imagen encriptada y la llave de seguridad. Las técnicas ópticas evidencian un gran potencial para el desarrollo de sistemas de seguridad basados en la encriptación [1-3].

Los sistemas de cifrado de información comercialmente disponibles son digitales. Sin embargo, se ha mostrado la vulnerabilidad de estos sistemas. Un sistema encriptador es seguro si a pesar de que un usuario no autorizado tiene conocimiento del sistema encriptador, pero desconoce las llaves de seguridad, le es imposible acceder a la información cifrada por este sistema u obtener por algún método las llaves de seguridad. Justamente, en estos aspectos de seguridad se ha demostrado en los últimos años que el procesamiento óptico provee ventajas en aplicaciones que involucren técnicas de encriptación en comparación con los sistemas digitales. La seguridad en un sistema de

encriptación se centra en la seguridad de la llave. En los últimos años, se diseñaron varios ataques para vulnerar dicha llave [8]. A pesar de esto, los sistemas ópticos de seguridad son más seguros dado que para romper un sistema óptico, un hacker necesita utilizar sofisticadas técnicas menos accesibles y flexibles en comparación con métodos digitales.
Los sistemas ópticos de encriptación más usados son los que emplean dos máscaras aleatorias de fase, los cuales son usualmente llamados sistemas de encriptación de doble máscara de fase. Los arreglos ópticos están basados fundamentalmente en correladores 4f [3, 4] y de transformada conjunta (JTC) [5]. Ademas de la seguridad ya mencionada, debemos mencionar que los sistemas ópticos ofrecen muchos grados de libertad para codificar los datos de forma segura (longitud de onda [6], polarización de la luz [7], etc). Asimismo, los sistemas ópticos implican procesos que transmiten una gran cantidad de información en paralelo y aumentando en consecuencia la velocidad del procesamiento en comparación con los sistemas electrónicos que se limitan, en general, al procesamiento en serie. Todos estas caracteristicas permiten advertir que las arquitecturas opticas representan una alternativa de lograr sistemas que compitan en la tarea de otorgar seguridad a la información a ser transmitida.

En la actualidad se buscan estrategias para aumentar la cantidad de datos codificados a ser almacenados. En ese sentido es de interés desarrollar técnicas de multiplexado que permitan almacenar muchos datos en un único bloque de información que contiene la suma de todos los datos encriptados. El multiplexado se puede implementar modificando la llave de codificación y/ó los parámetros ópticos del sistema [9], por ejemplo desplazando la máscara llave [10], cambiando al longitud de onda [11], etc.

Los sistemas de encriptación múltiple presentan la ventaja de que a partir de un único bloque de datos, un usuario que recibe diferentes llaves en diferentes momentos pueda recuperar diferentes datos. Asimismo, estos sistemas permiten el manejo de múltiples usuarios cada uno de los cuales a través de una llave diferente podrán acceder a diferente información. En el procedimiento de desencriptación, la información del multiplexado es enviada a todos los usuarios, lo que asegura un manejo eficiente de la información ya que se evita el envío por separado de un dato encriptado por cada uno de los usuarios. Asimismo, por separado, a cada usuario se le envía la llave de seguridad y/ó los parámetros del sistema que le permiten, a partir del multiplexado, recuperar el dato de interés. Aunque un usuario no autorizado pueda interceptar la información del multiplexado, si no tiene acceso a la llave de seguridad y/o los parámetros del procesador, no podrá acceder a la información de ninguno de los datos encriptados.

Cabe mencionar que a la ventaja antes mencionada debemos agregar que la seguridad de los datos encriptados aumenta gracias al multiplexado por ejemplo mediante el multiplexado encubierto [12].

En la Sección 2 de este trabajo, se mostrará que en los arreglos de encriptación múltiple a medida que se incrementa el número de datos almacenados en un único bloque, en esa misma medida se degradan los datos recuperados. El mencionado deterioro se debe al solapamiento y al ruido generado por los datos no desencriptados. Este hecho representa una gran limitación para la aplicación práctica de los sistemas ópticos de encriptación de múltiples datos. En ese sentido, se esboza una solución que permite eliminar el deterioro a través del reposicionado de la información asociada a cada uno de los datos de entrada.

2. Encriptación múltiple de datos

En el sistema de encriptación de doble máscara de fase basado en la arquitectura 4f, el dato a ser encriptado se adosa a una máscara aleatoria de fase R_1 (ver Figura 1). Luego se realiza una transformada de Fourier de este producto y en el plano de Fourier se coloca una

segunda máscara aleatoria de fase ó llave de seguridad del sistema R_2. Finalmente se realiza otra transformada de Fourier para obtener el dato encriptado [3],

$$E = O_1 R_1 * \Im[R_2] \quad (1)$$

donde $*$ denota la operación de convolución, $\Im$ la transformada de Fourier, O_1 el objeto de entrada.

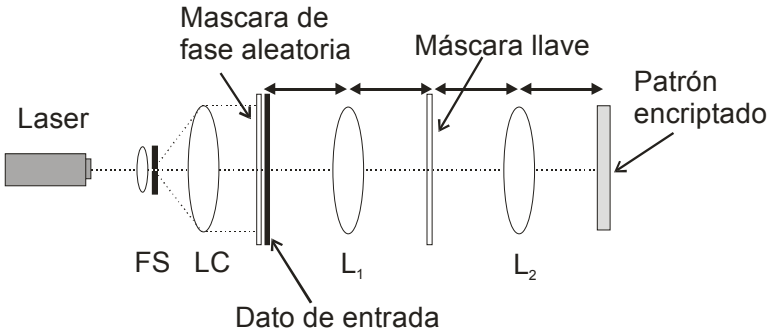


Figura 1. Esquema del sistema óptico de encriptación (FS: filtro espacial; LC: lente colimadora, L_1 y L_2: lente).

Este patrón encriptado multiplexado es enviado al usuario final junto con la máscara llave R_2. Para recuperar el dato de entrada, se realiza la transformada de Fourier del complejo conjugado de la imagen encriptada y se lo multiplica por la llave del sistema R_2.

$$\Im[E^*]\, R_2 = \Im[(O_1 R_1)^*]\, R_2^*\, R_2 \quad (2)$$

Luego, se realiza una segunda transformada de Fourier obteniéndose el dato desencriptado (ver esquema del dispositivo de desencriptación de la Figura 2).

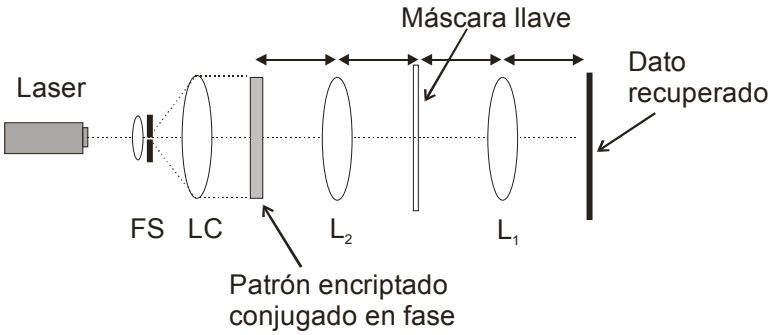


Figura 2. Esquema del sistema óptico de desencriptación (FS: filtro espacial; LC: lente colimadora, L_1 y L_2: lente).

Las técnicas de multiplexado permiten que múltiples datos encriptados sean almacenados en un único medio de almacenamiento que contiene la suma de todos los datos (ver el esquema presentado en la Figura 3). Para llevar a cabo el mencionado proceso, en primer lugar se encripta uno de los datos de entrada O_1 con la máscara llave R_2, posteriormente se encripta un segundo dato O_2 cambiando la llave de seguridad o algún parámetro del sistema (dicha máscara la denotaremos como R_3) y luego se suma este patrón encriptado con el primero; obteniéndose el multiplexado entre el primer y segundo dato encriptado. A continuación se encripta el tercer dato con una máscara llave R_4 y se suma con el multiplexado del primero y el segundo, repitiéndose el procedimiento con el resto de datos a

procesar. Entonces, una operación de multiplexado implica generar un patrón multiplexado resultante $M = E_1 + E_2 + E_3$.

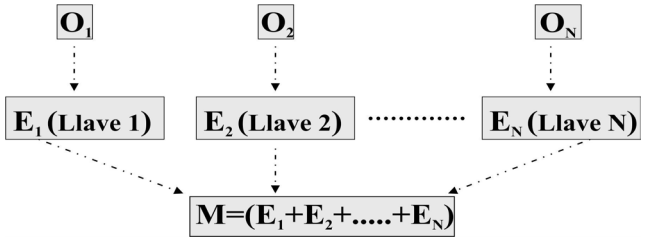


Figura 4 Esquema multiplexado

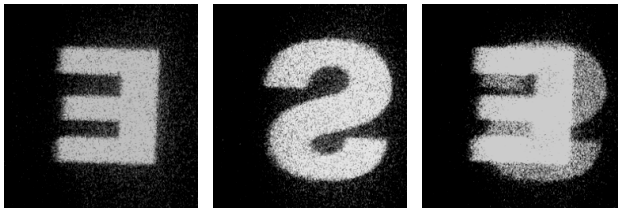
Una característica novedosa y singular de nuestras propuesta, es la presencia simultánea en el frente de onda de todas las señales encriptadas. Para la desencriptación en la configuración de multiplexado, a los usuarios finales autorizados se les envía la información del multiplexado y por separado se les envía la llave de seguridad, por ejemplo R_2 y el conjunto de parámetros ópticos empleados durante la encriptación. Para desencriptar la información, el usuario realiza la transformada de Fourier del dato multiplexado conjugado en fase y multiplica por la llave R_2, resultando:

$$\Im\left[M^*\right] R_2 = \Im\left[\left(O_1 R_1\right)^*\right] R_2{}^* R_2 + \Im\left[\left(O_2 R_1\right)^*\right] R_3{}^* R_2 + +\Im\left[\left(O_3 R_1\right)^*\right] R_4{}^* R_2 \qquad (3)$$

Cuando se emplea la máscara de fase R_2, el usuario recupera el objeto O_1 y el ruido asociado a los datos encriptados correspondientes a los objeto O_2 y a O_3 que no fueron desencriptados. Entonces, luego de una nueva transformada de Fourier se obtiene,

$$\begin{aligned} K &= \Im\left[\left(O_1 R_1\right)^*\right] + \Im\left[\left(O_2 R_1\right)^*\right] R_3{}^* R_2 + \Im\left[\left(O_3 R_1\right)^*\right] R_4{}^* R_2 \\ \Rightarrow \quad \Im^{-1}[K] &= \left(O_1 R_1\right)^* + N_3 + N_4 \Rightarrow \quad O_1 R_1 \end{aligned} \qquad (4)$$

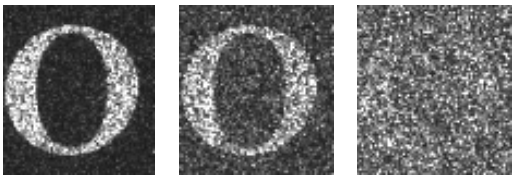
Donde N_3 y N_4 representan el ruido adicionado por los objetos no desencriptados. Un sistema de encriptación múltiple adecuado debe permitir recuperara aisladamente cada dato almacenado. Entendemos por solapamiento a la superposición de datos correctamente decodificados. La presencia de solapamiento se traduce en la incorrecta visualización de la información recuperada. En la Figura 3 a) y 3 b) se muestran los datos recuperados aisladamente mientras que en la Figura 3 c) se muestra la información recuperada cuando hay solapamiento entre los datos correspondientes a diferentes registros. El solapamiento se puede eliminar eligiendo mascaras llave estadísticamente independientes o seleccionando adecuadamente los parámetros ópticos, como se puede ver en las Ref. [6, 7, 10]. En suma, en todos los casos que se utilice el cambio de algún parámetro óptico para le multiplexado es requerido un adecuado estudio de la sensibilidad del sistema al cambio de los parámetros ópticos permite almacenar información múltiple eliminando el solapamiento.



(a) (b) (c)

Figura 3: a) y (b) Imágenes desencriptadas correspondientes a datos encriptados con mascaras llave estadísticamente independientes (c) Imagen desencriptada correspondientes a datos encriptados con la misma máscara llave

El cambio adecuado del parámetro óptico permite recuperar aisladamente la información de cada registro. Sin embargo, como se puede ver en la ecuación (4) los datos no desencriptado correspondientes a O_2 y O_3 pueden ser considerado como ruido de fondo sobre la información de O_1. Entonces, por ruido entendemos la contribución de imágenes no desencriptadas sobre una imagen correctamente recuperada. El origen de este ruido se debe básicamente a que el frente de onda contiene toda la información almacenada como ay fue mencionado. Entonces, una imagen no desencriptada se comporta sobre ruido blanco sobre los datos de interés. Cuando el número de imágenes a ser multiplexadas en un único bloque de datos es pequeño el peso de estos términos no es importante. Sin embrago, a medida que se incrementa el número de datos en el proceso de multiplexado, aumenta el número de términos que contribuyen al ruido en el plano de desencriptación, hasta llegar un momento en que no se puede discriminar el dato desencriptado debido al ruido generado por los no desencriptados. Esto se puede confirmar en los resultados presentados en la Figura 4, donde se observa que cuando se almacenan 30 imágenes el ruido supera a la información. Lo anterior implica que para cierto número de datos multiplexados, a pesar de que se use una de las llaves de seguridad correcta, no se podrá discriminar el dato desencriptados.



(a) (b) (c)

Figura 4: Imagen desencriptada cuando se almacenaron en un único medio de registro (a) 4 imágenes, (b) 10 imágenes y (c) 30 imágenes.

Cabe mencionar que tanto el ruido debido a los datos no desencriptados como el solapamiento pueden aparecer simultáneamente. Si bien los estudios presentados en als Ref. [6, 7,10] permiten eliminar el solapamiento, aparece en la reconstrucción ruido de fondo debido a la presencia de los datos no desencriptados. En ese sentido, recientemente hemos desarrolado para la arquitectura 4f una técnica basada en la "tetha modulation" para eliminar este ruido y por lo tanto aumentar la capacidad de procesamiento de los sistemas ópticos de encriptación. La técnica propuesta consiste en modular cada uno de los datos encriptados con una red con diferente frecuencia y/o orientación [13-15]. Este procedimiento permite separar cada uno de los datos encriptados y filtrarlos adecuadamente en la etapa de desencriptación, obteniéndose cada uno de los datos de entrada libres del ruido.

3. Conclusiones

Las técnicas de encriptación múltiple permiten que la información de varios de datos de entrada sea almacenada en un único medio que contenga la suma de todos los datos individuales. En este trabajo se muestra que si bien se ha verificado la aplicabilidad de los sistemas ópticos en procesos de seguridad, sin embargo los procesos de multiplexado presentaban una gran limitación debido al solapamiento y al ruido debido a los datos no desencriptados. Ambos hechos pueden aparecer simultáneamente. Entonces, a medida que se incrementa el número de datos en el proceso multiusuario, aumenta el número de términos que contribuyen al ruido en el plano de recuperación, hasta llegar un momento en que no se puede discriminar el dato desencriptado debido al ruido generado por los no desencriptados. Para eliminar el ruido generado por los datos no desencriptados y por lo tanto aumentar la capacidad de procesamiento de los sistemas ópticos de encriptación

basados en la arquitectura 4*f*, recientemente se propuso la implementación de la técnica "tetha modulation". Esta técnica se basa en un reposicionado inteligente al momento de desencriptar la información multiplexada, mediante mecanismos accesorios al montaje encriptador básico.

Bibliografía

1. A. Alfalou, C. Brosseau. Optical image compression and encryption methods. Adv. Opt. Photon. **1**, 589–636 (2009).
2. O. Matoba, T. Nomura, E. Perez-Cabre, M.S. Millan, B. Javidi. Optical techniques for information security. Proc. of IEEE 97, 1128-1148 (2009).
3. P. Refregier, B. Javidi. Optical image encryption using input and Fourier plane random phase encoding. Opt. Lett. 20, 767-769 (1995).
4. G. Unnikrishnan, J. Joseph, K. Singh, Optical encryption by double-random phase encoding in the fractional Fourier domain, Opt. Lett. 25, 887-889 (2000).
5. T. Nomura, B. Javidi. Optical encryption using a joint transform correlator architecture. Opt. Eng. 39, 2031-2035 (2000).
6. D. Amaya, M. Tebaldi, R. Torroba, N. Bolognini. Wavelength multiplexing encryption using JTC architecture. Appl. Opt., 48, 2099-2104 (2009).
7. J. F. Barrera, R. Henao, M. Tebaldi, N. Bolognini, R. Torroba. Multiplexing encrypted data by using polarized light. Opt. Commun., 260, No.1, 109-112 (2006).
8. Y. Frauel, A. Castro, T.J. Naughton, B. Javidi. Resistance of the double random phase encryption against various attacks, Opt. Express 15, 10253-10265 (2007).
9. D. Amaya, M. Tebaldi, R. Torroba, N. Bolognini. Multichanneled puzzle-like encryption. Opt. Commun., 281, 3434–3439 (2008).
10. J. F. Barrera, R. Henao, M. Tebaldi, N. Bolognini, R. Torroba. Multiplexing encryption-decryption via lateral shifting of a random phase mask. Opt. Commun., 259, No. 2, 532-536 (2006)
11. D. Amaya, M. Tebaldi, R. Torroba, N. Bolognini. Digital color encryption using a multi-wavelength approach and a joint transform correlator. J. Opt. A: Pure Appl. Opt., 10, 104031 (5pp) (2008)
12. J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, N. Bolognini. Multiple-encoding retrieval for optical security. Opt. Commun., 276, 231–236 (2007).
13. F. Mosso, J. F. Barrera, M. Tebaldi, N. Bolognini, R. Torroba. All-optical encrypted movie. Opt. Express, 19, 5706-5712 (2011).
14. F. Mosso, M. Tebaldi, J. F. Barrera, N. Bolognini, R. Torroba. Pure optical dynamical color encryption. Opt. Express, 19, 13779- 13786 (2011).
15. J. F. Barrera, M. Tebaldi, C. Ríos, E. Rueda, N. Bolognini, R. Torroba. Experimental multiplexing of encrypted movies using a JTC architecture. Opt. Express **20**, 3388–3393 (2012).