Revista Colombiana de Física, vol. 44, No. 3, 2012

Encriptación óptico-digital usando una arquitectura 4f

Optical-Digital Encryption in a 4f Arquitecture

C. A. Vargas[1*], J. F. Barrera[1], R. Torroba[2]

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

Recibido mayo 12 de 2010; aceptado febrero 9 de 2011.

Resumen

En este trabajo se presenta un método óptico-digital para llevar a cabo un proceso de encriptación con doble máscara de fase usando una arquitectura 4f, el proceso de encriptación se realiza ópticamente y el proceso de desencriptación se hace en forma digital. Para recuperar la información original se registra la información de amplitud y fase del objeto encriptado y la fase de la llave de seguridad. Se utiliza el método holográfico de dos pasos que consiste en obtener dos hologramas de un elemento complejo con el fin de registrar su información de amplitud y fase, hologramas que difieren entre sí por un desfase adicional introducido en la onda de referencia durante cada registro. Como aporte original se propone un algoritmo que permite extraer la información de fase del dato encriptado, a partir de sus hologramas, sin necesidad de conocer el valor del desfase introducido entre estos, lo cual lo hace más eficiente que otros algoritmos. Se presentan resultados de simulaciones computacionales que muestran la eficiencia del método.

Palabras claves: encriptación, holografía digital.

Abstract

In this work an optical-digital method to carry out an encryption process, with double phase mask using a 4f architecture, is presented. The encryption process is optically performed, and the decryption is digitally done. To recover the original information, we register amplitude and phase of the encrypted object, as well as the phase of the security key. A two-step holographic method is employed. It consists in obtaining two holograms of a complex element in order to register its amplitude and phase information. These holograms differ by a delay introduced in the reference wave during each register. We propose an original algorithm that allows to extract the phase information of the encrypted data starting from its holograms, without needing to know the value of the delay introduced between them, making it more efficient than other algorithms. To probe the efficiency of the method, computational simulations are presented.

Keywords: encryption, digital holography.

1. Introducción

El sistema de encriptación de doble máscara de fase es la técnica de encriptación óptica más antigua [1], la que tiene más variantes [2,3] y la más avanzada en términos de su implementación comercial [4,5]. En la implementación experimental de la técnica se han usados cristales fotorefractivos [6], donde la encriptación y desencriptación se hacen sobre el montaje y a tiempo real. Luego se presentó un sistema que emplea holografía digital y una arquitectura 4f, con la particularidad de usar una lente en lugar de una máscaraaleatoria, como llave de seguridad, [7], hecho que representa una falla en la seguridad del sistema.

Recientemente se propuso un montaje interferométrico para la encriptación y desencriptación de datos por medio de un sistema de doble máscara de fase y la propagación en el espacio libre [8]. En dicha propuesta, para recuperar la información original es necesario usar el método de dos pasos, pero el algoritmo implementado para este fin posee algunas restricciones.

Debido a que las técnicas óptico digitales presentan ventajas en cuanto al manejo de la información, ya que permiten

* cavargas87@gmail.com

llevar a cabo procesos con una eficiente transmisión y recepción de datos, y a la gran potencialidad que tienen las técnicas antes mencionadas, se ha incentivado el estudio y perfeccionamiento de métodos que permitan el mejoramiento de las técnicas ya existentes y la implementación de nuevas propuestas. En esa línea, se presentó una contribución que emplea holografía digital y una arquitectura de correlador de transformada conjunta, usualmente llamada "arquitectura JTC" por sus sigla en inglés (JTC - Joint Transform Correlator) [9]. Al igual que las técnicas anteriores, se utiliza la codificación de doble máscara de fase pero combinando un procesamiento óptico-digital con una arquitectura JTC.

En esta contribución se propone e implementa un método para la encriptación de información que está basado en holografía digital y que usa un sistema de encriptación de doble máscara de fase bajo arquitectura 4f. Se propone un algoritmo que a diferencia de otros métodos, permite extraer la información de fase de un campo complejo sin el conocimiento del valor del desfase introducido entre los hologramas que serán usados en el método de dos pasos. Se implementa el sistema virtual óptico del montaje propuesto para mostrar la validez y aplicabilidad de la propuesta.

2. Marco teórico

2.1 Encriptación y desencriptación óptica en una arquitectura 4f

En el proceso de encriptación el objeto $f(x_0, y_0)$ se pone en contacto con una máscara de fase $\alpha(x_0, y_0) = \exp[2i\pi a(x_0, y_0)]$ donde $a(x_0, y_0)$ es un valor aleatorio entre $[0,1]$, de modo que la transmitancia en el plano de entrada está dado por [1]:

$$U_0(x_0, y_0) = f(x_0, y_0)\alpha(x_0, y_0), \tag{1}$$

al iluminar con una onda plana y monocromática de amplitud 1, en el plano focal de la lente L1 se obtiene la transformada de Fourier óptica del plano de entrada:

$$U_1(x_1, y_1) = \frac{1}{i\lambda f} F\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right) \otimes A\left(\frac{x_1}{\lambda f}, \frac{y_1}{\lambda f}\right), \tag{2}$$

donde $F(x_1, y_1)$ y $A(x_1, y_1)$ corresponde a la transformada de Fourier de $f(x_0, y_0)$ y $\alpha(x_0, y_0)$ respectivamente, f es la distancia focal de la lente y λ la longitud de onda incidente. La transformada de Fourier incide sobre la máscara de fase 2 o llave de seguridad cuya transmitancia es $\beta(x_1, y_1) = \exp[2i\pi b(x_1, y_1)]$ con $b(x_1, y_1)$ aleatoria y distribuida en el rango [0,1]. Luego la lente L_2 permite llevar a cabo una segunda transformada de Fourier y, por lo tanto en el plano de salida del sistema 4f, se obtiene la imagen encriptada [10]:

$$U_2(x_2, y_2) = \frac{e^{i\pi}}{(\lambda f)^2} f(-x_2, -y_2)\alpha(-x_2, -y_2) \otimes B\left(\frac{x_2}{\lambda f}, \frac{y_2}{\lambda f}\right), \tag{3}$$

donde $B(x_2, y_2)$ es la transformada de Fourier de la llave de seguridad en [10].

Para realizar el proceso de desencriptación, se obtiene el complejo conjugado del objeto encriptado, por ejemplo usando cristales fotorefractivos, y se genera su transformada de Fourier con una lente:

$$U_3(x_3, y_3) = \frac{i}{(\lambda f)^3} F^*\left(-\frac{x_3}{\lambda f}, -\frac{y_3}{\lambda f}\right) \otimes A^*\left(-\frac{x_3}{\lambda f}, -\frac{y_3}{\lambda f}\right) \times \beta^*(x_3, y_3), \tag{4}$$

donde * representa el complejo conjugado. Cuando este campo pasa a través de la llave de seguridad y se genera una última transformada de Fourier, se genera una distribución de campo de la forma:

$$U_4(x_4, y_4) = \frac{1}{(\lambda f)^4} f^*(x_4, y_4)\alpha^*(x_4, y_4), \tag{5}$$

notemos que esta última expresión corresponde al complejo conjugado de la transformada de Fourier del plano de entrada durante la encriptación (Ecuación 1) multiplicada por un factor constante.

2.2 Técnica de doble paso en holografía digital

Como el proceso de desencriptación es digital, se debe registrar la información de la imagen encriptada que se obtiene en el procesador óptico. Para recuperar la información original es necesario poseer la información de amplitud y fase asociada al objeto encriptado y a la llave de seguridad. Si se dispone de un elemento sensible a la intensidad (por ejemplo, una cámara CCD), se propone realizar 3 medidas de intensidad sobre el elemento al que se le quiere extraer la información.

Sea

$$f(x, y) = |f(x, y)| \exp[i\phi(x, y)] \tag{6}$$

la distribución de campo complejo sobre la cual se desea conocer tanto su amplitud $|f(x, y)|$ como fase $\phi(x, y)$.

Primero se mide su intensidad, dada por $I_1(x, y) = |f(x, y)|^2$ de donde se sigue que:

$$\left| f(x,y) \right| = \sqrt{I_1(x,y)}, \tag{7}$$

a partir de la información anterior se obtiene la amplitud del objeto deseado.

Para hallar la información asociada a la fase $\phi(x,y)$ se toma inicialmente un holograma usando como referencia una onda plana $U_p(x,y) = U_o \exp\left[i\vec{k} \cdot \vec{r} \right]$ cuyo vector de propagación $\vec{k}$ sea perpendicular al objeto sobre el que se está tomando la información o sea que sobre todo el objeto su valor de fase sea constante dada por $\phi_0 = \vec{k} \cdot \vec{r}$, por lo tanto el campo asociado a este holograma será:

$$U_p(x,y) = \left| f(x,y) \right| \exp\left[i\phi(x,y) \right] + U_o \exp\left[i\phi_0 \right], \tag{8}$$

luego, la intensidad del holograma estará entonces dada por:

$$\begin{aligned} I_2(x,y) &= \left| f(x,y) \right|^2 + \left| U_o \right|^2 \\ &+2\sqrt{\left| f(x,y) \right| \left| U_o \right|} \cos\left[\phi(x,y) - \phi_0 \right] \end{aligned} \tag{9}$$

Se hace necesario tomar un segundo holograma usando el mismo haz de referencia pero añadiendo a éste un valor de fase δ tal que $0 < \delta << \pi$. La intensidad asociada a este nuevo holograma estará dada por:

$$\begin{aligned} I_3(x,y) &= \left| f(x,y) \right|^2 + \left| U_o \right|^2 \\ &+2\sqrt{\left| f(x,y) \right| \left| U_o \right|} \cos\left[\phi(x,y) - \phi_0 - \delta \right]. \end{aligned} \tag{10}$$

2.3 Determinación de la información de fase

A partir de la información contenida en las 3 intensidades mostradas en las ecuaciones (7), (9) y (10) se puede determinar la información asociada a la diferencia de fase $\Delta(x,y) = \phi(x,y) - \phi_0$ usando el algoritmo que se mostrara a continuación.

Supongamos que tenemos 2 distribuciones de intensidad correspondientes a la interferencia de 2 rayos con I_1, I_2 y $\Delta = \phi_1 - \phi_2$ sus intensidades y diferencia de fase respectivamente, la primera de las distribuciones está dada por:

$$I^{(1)} = I_1 + I_2 + 2\sqrt{I_1 I_2} \cos\Delta, \tag{11}$$

y la segunda de ellas corresponde a la anterior solo que a uno de los rayos se le ha introducido un valor de fase adicional δ, supondremos en este caso, sin pérdida de generalidad, que se le introduce a I_2; por lo tanto la nueva distribución de intensidad estará dada ahora por:

$$I^{(2)} = I_1 + I_2 + 2\sqrt{I_1 I_2} \cos\Delta', \tag{12}$$

dónde $\Delta' = \Delta - \delta$. Se desea conocer la información de la diferencia entre los dos haces Δ usando la información de las diferentes distribuciones de intensidad y la asociada a cada haz. De la ecuación (12) se sigue que:

$$\Delta = \cos^{-1}\left\{ \frac{I^{(1)} - I_1 - I_2}{2\sqrt{I_1 I_2}} \right\}, \tag{13}$$

en la ecuación anterior existe un problema al evaluar la función coseno inverso ya que el rango de esta función está en el intervalo $[0,\pi]$, pero en general los valores de fase están en el rango de $[0,2\pi]$. Para eliminar esta ambigüedad se usa la información de fase obtenida del segundo interferograma que está dada por:

$$\Delta' = \Delta - \delta = \cos^{-1}\left\{ \frac{I^{(2)} - I_1 - I_2}{2\sqrt{I_1 I_2}} \right\}, \tag{14}$$

si $0 < \delta << \pi$ es posible determinar el valor exacto de Δ al realizar una comparación entre los valores arrojados por las ecuaciones (13) y (14), usando el siguiente criterio:

- Si $\Delta' > \Delta$, esto implica que el coseno del ángulo decreció lo cual es de esperarse si Δ está en el rango $[0,\pi]$, entonces, el valor correcto es el arrojado por la ecuación (13).
- Si $\Delta' < \Delta$, implica que el coseno del ángulo creció al disminuir el ángulo lo cual es de esperarse si Δ está en el rango $[\pi,2\pi]$, lo anterior implica que para hallar el valor correcto de la diferencia de fase, al valor arrojado por la ecuación (13) es necesario hacerle la corrección: $\Delta = \pi - \Delta$.

Si el valor del desfase Δ es cercano a los valores extremos como 0, π o 2π, se usa el hecho de que la diferencia entre los desfases en cada uno de los hologramas debe ser del orden del desfase introducido, si al compararlas se llega a esta dificultad, se concluye que se tomaron valores cercanos a estos extremos y se elige ese valor.

Al aplicar este algoritmo para el objeto de la ecuación (4) se obtiene:

$$f'(x,y) = \left| f(x,y) \right| \exp\left[i\phi(x,y) - i\phi_0 \right], \tag{15}$$

distribución de campo que difiere difiere del objeto original solo en el valor de fase constante asociado a la onda plana de referencia, que para nuestras aplicaciones no aporta información relevante.

3. Montaje

Se propone un montaje intereferométrico tipo Mach-Zender para la implementación experimental de la propuesta.

En uno de los brazos del interferómetro se ubica el sistema encriptador 4f que usa dos lentes, L_1 y L_2, de igual distancia focal f, en la salida del sistema encriptador se ubica la cámara CCD con la cual se harán los registros de intensidad de los diferentes hologramas. En el otro brazo del montaje

se ubica un haz de referencia para generar los hologramas, los cuales servirán para encontrar los valores de fase asociados al objeto encriptado y la llave de seguridad. Para llevar a cabo el procedimiento de doble paso, se ubicó una lámina delgada transparente sobre una base que permite rotaciones muy pequeñas. De esta forma se le puede añadir un valor de fase a la onda plana de referencia.

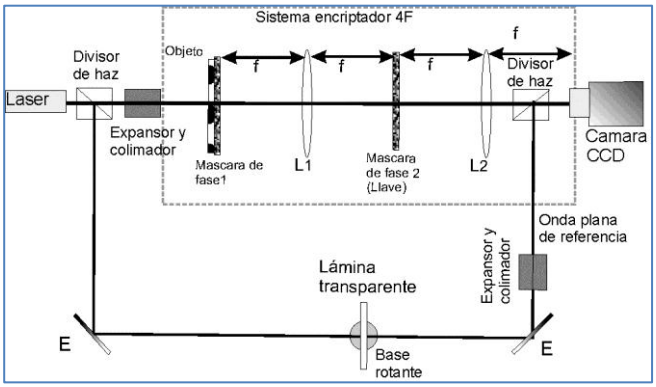

Fig. 1: Montaje propuesto.

4. Procedimiento de encriptación y desencriptación óptico-digital

A la salida del sistema 4f se obtiene el objeto encriptado (Fig. 1). Para el proceso de desencriptación es necesario tomar la información de amplitud y fase del objeto encriptado, para esto se toma su intensidad bloqueando el haz de referencia y 2 hologramas, los cuales difieren en un valor de fase constante introducido al rotar la lámina transparente un ángulo pequeño, tal como lo exige el método de doble paso. Adicionalmente se debe registrar la información de la llave de seguridad. Para ello se deben retirar del montaje el objeto, la primera máscara de fase y la lente L_1. De esta forma, la llave de seguridad estará iluminada por una onda plana y por lo tanto en el plano focal de la lente L_2 se obtiene:

$$B\left(\frac{x_2}{\lambda f},\frac{y_2}{\lambda f}\right), \qquad (16)$$

correspondiente a la transformada de Fourier óptica de la llave de seguridad. Luego se toma su intensidad y los 2 hologramas, de igual forma como se procedió para el objeto encriptado.
Durante el proceso digital, se reconstruye el objeto encriptado y la transformada de Fourier óptica de la llave usando el algoritmo propuesto en la sección 2.2, la información de estos elementos difiere de los reales solo en un valor de fase según la ecuación (13).
Con la información arrojada, primero se halla la llave de seguridad usando un proceso digital de transformada de Fourier inversa y se procede a la desencriptación como se muestra en la sección 2.1.

5. Simulación

Usando el software MatLab se simuló el sistema óptico virtual propuesto en la Figura 1, para esto se emplearon matrices de 512x512, con un muestreo de 10µm, lentes de un diámetro de 5cm, distancia focal de 15cm y longitud de onda de 632.8nm, la fase asociada a la onda plana se introdujo aleatoriamente y su amplitud fue constante.
Los resultados obtenidos en el proceso de desencriptación se muestran en la Figura.2, en ésta se muestra el objeto y uno de los hologramas asociados a la técnica de doble paso en holografía digital.

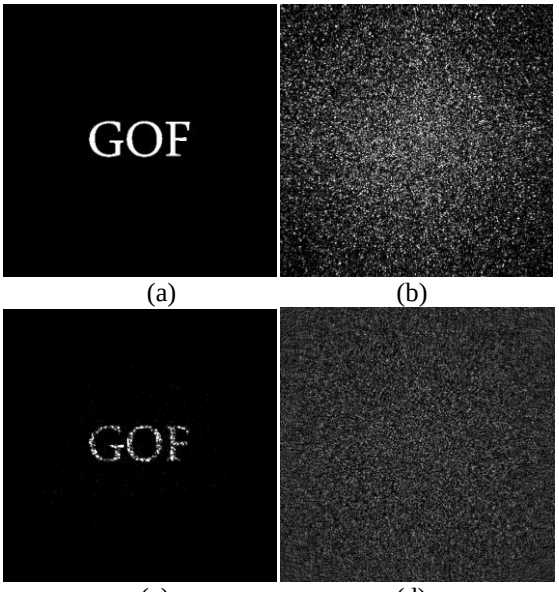

Fig. 2: Resultados simulación: (a) objeto, (b) intensidadel objeto encriptado, (c) objeto desencriptado usando el método propuesto y (d) holograma de la transformada de Fourier óptica de la llave de seguridad.

Los resultados presentados en la figura 2 demuestran que el método permite la encriptación y desecriptación de datos.

6. Conclusiones

Se presenta un método de encriptación basado en una codificación que usa la arquitectura 4f y la codificación por medio de dos máscaras de fase, usando además un procesamiento óptico-digital. En la propuesta, el proceso de encriptación se realiza en un procesador óptico mientras que la desencriptación es completamente digital. Para la implementación de la técnica se usa un procesador óptico virtual y la técnica de dos pasos con un algoritmo novedoso y eficiente. Los resultados demuestran que la técnica propuesta tiene gran potencialidad para ser puesta a prueba en un

montaje experimental. Como perspectiva del trabajo se busca implementar experimentalmente el procesador óptico propuesto.

Agradecimientos

Esta investigación fue realizada con apoyo de Colciencias (Colombia), CODI, Universidad de Antioquia (Colombia), TWAS-UNESCO Associateship Scheme at centres of Excellence in the South, CONICET No. 112-200801-00863 (Argentina), ANCYT PICT 1167 (Argentina) y Facultad de Ingeniería, Universidad Nacional de La Plata No.11/I105 (Argentina).

Referencias

[1] P. Refregier, B. Javidi, *Optics Letters*, **20**, 1995, pp.767-769..
[2] P. C. Mogensen, J. Gluckstad, *Optics Letters*, **25**, 2000, pp. 566-568.
[3] W. Hang, C. S. Park, D. H. Ryu, E. S. Kim. *Optical Enginiering*, **38**, 1999, pp. 47-54.
[4] B. Javidi, *Methods and apparatus for encryption.* Patente US6002773, diciembre 14, 1999.
[5] B. Javidi, *Methods and apparatus for encryption using partial information.* Patente US6519340, febrero 11, 2003.
[6] G. Unnikrishnan, J. Joseph, K. Singh, *Applied Optics*, **37**, 1998, 8181-8186.
[7] B. Javidi, T. Nomura, *Optics Letters*, **25**, 2000, pp. 28-31.
[8] X. F. Meng, et al., *Optics Letters*, **31**, 2006, 1414-1416.
[9] E. Rueda, J. F. Barrera , R. Henao, R. Torroba, *Optics Communications*, **282**, 2009, 3243-3249.
[10] E. Rueda, *Encriptación y desencriptación dinámica de información por medios óptico-digitales.* Medellín, 2009, pag. 192. Trabajo de grado (Doctor en Física). Universidad de Antioquia. Instituto de Física.