Type: Original Research Paper / Tipo: Artículo Original de Investigación
Section: Imaging Techniques / Sección: Técnicas de Imagen

Images encryption system based on a fractional joint transform correlator and nonlinear filtering

Sistema de cifrado de imágenes basado en un correlador de transformadas conjuntas fraccionario y filtrado no lineal

Juan M. Vilardy O.(*,S), María S. Millán(S), Elisabet Pérez-Cabré(S)

Grupo de Óptica Aplicada y Procesado de Imagen, Departamento de Óptica y Optometría, Universitat Politècnica de Catalunya, 08222 Terrassa (Barcelona), Spain

(*) Email: juan.manuel.vilardy@estudiant.upc.edu S: miembro de SEDOPTICA / SEDOPTICA member

Received / Recibido: 20/12/2013. Revised / Revisado: 28/02/2014. Accepted / Aceptado: 03/03/2014.

DOI: http://dx.doi.org/10.7149/OPA.47.1.35

ABSTRACT:

A new optical security system for image encryption based on a fractional joint transform correlator and nonlinear filtering is proposed. The position of the lens in the proposed optical encryption setup can be chosen, so that an additional key is introduced in the security system. The distributions at the input and output planes of the encryption system are related by a fractional Fourier transform (FrFT) at a given fractional order that is defined, among other parameters, by the focal length and the position of the lens in the setup; this fractional order acts as an additional key of the security system. The optical intensity of the complex distribution in the fractional Fourier domain (output plane) is captured by a CCD camera. The nonlinearity introduced in the last step of the encryption process, maintains the encrypted function as a real-valued function. The security system proposed in this work is an generalization of the encryption system based on a conventional joint transform correlator (JTC), from the Fourier domain to the fractional Fourier domain. Additional advantages of the proposed system are: new degrees of freedom for the optical setup, alleviated alignment requirement, and the introduction of an additional key (the fractional order of the FrFT) that improves security. Numerical simulations verify the validity of this new optical security system.

Key words: Image Encryption, Decryption, Joint Transform Correlator, Fractional Fourier Transform, Random Phase Mask, Nonlinear Filter.

RESUMEN:

En este trabajo se propone un sistema de seguridad óptico para cifrar imágenes, basado en un correlador de transformadas conjuntas fraccionario y filtrado no lineal. La posición de la lente en el montaje óptico de cifrado propuesto puede ser seleccionada, lo cual añade una llave al sistema de seguridad. Las distribuciones en los planos de entrada y salida del sistema de cifrado se relacionan por medio de una transformada fraccionaria de Fourier (*fractional Fourier transform*, FrFT) con un orden fraccionario específico, que viene definido entre otros parámetros por la distancia focal y la posición de la lente en el montaje, y que actúa como llave adicional en el sistema de seguridad. La intensidad óptica de la distribución compleja en el dominio fraccionario de Fourier (plano de salida) es captada usando una cámara CCD. La no linealidad introducida en el último paso del proceso de cifrado, mantiene el carácter real de la función cifrada. El sistema de seguridad propuesto en este trabajo es una generalización del sistema de cifrado basado en el correlador de transformadas conjuntas (*joint transform correlator*, JTC) convencional, desde el dominio de Fourier al dominio fraccionario de Fourier. Las ventajas adicionales del sistema propuesto son: nuevos grados de libertad para el montaje óptico, requerimiento de alineación mitigado y la introducción de una clave adicional (el orden fraccionario de la FrFT) que mejora la seguridad. Simulaciones numéricas verifican la validez de este nuevo sistema óptico de seguridad.

Palabras clave: Cifrado de Imágenes, Descifrado, Correlador de Transformadas Conjuntas, Transformada Fraccionaria de Fourier, Máscara Aleatoria de Fase, Filtrado no Lineal.

REFERENCES AND LINKS / REFERENCIAS Y ENLACES

[1]. M. S. Millán, E. Pérez-Cabré, "Optical data encryption", pp. 739–767 in *Optical and Digital Image Processing: Fundamentals and Applications*, G. Cristóbal, P. Schelkens, H. Thienpont, Edts., , Wiley-VCH Verlag GmbH & Co. (2011).

[2]. P. Réfrégier, B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding", *Opt. Lett.* **20**, 767–769 (1995). DOI

[3]. G. Situ, J. Zhang, "Double random-phase encoding in the Fresnel domain", *Opt. Lett.* **29**, 1584–1586 (2004). DOI

[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). DOI

[5]. J. W. Goodman, *Introduction to Fourier Optics*, McGraw-Hill (1996).

[6]. T. Nomura, B. Javidi, "Optical encryption using a joint transform correlator architecture", *Opt. Eng.* **39**, 2031–2035 (2000). DOI

[7]. E. Rueda, J. F. Barrera, R. Henao, R. Torroba, "Optical encryption with a reference wave in a joint transform correlator architecture", *Opt. Commun.* **282**, 3243–3249 (2009). DOI

[8]. M. N. Islam, M. S. Alam, "Optical security system employing shifted phase-encoded joint transform correlation", *Opt. Commun.* **281**, 248–254 (2008). DOI

[9]. J. M. Vilardy, M. S. Millán, E. Pérez-Cabré, "Improved decryption quality and security of a joint transform correlator-based encryption system", *J. Opt.* **15**, 025401 (2013). DOI

[10]. J. M. Vilardy, M. S. Millán, E. Pérez-Cabré, "Joint transform correlator-based encryption system using the Fresnel transform and nonlinear filtering", *Proc. SPIE* **8785**, 87853J (2013). DOI

[11]. D. Lu, W. Jin, "Color image encryption based on joint fractional Fourier transform correlator", *Opt. Eng.* **50**, 068201 (2011). DOI

[12]. S. K. Rajput, N. K. Nishchal, "Image encryption and authentication verification using fractional nonconventional joint transform correlator", *Opt. Commun.* **50**, 1474-1483 (2012).

[13]. H. M. Ozaktas, Z. Zalevsky, M. A. Kutay, *The Fractional Fourier Transform: with Applications in Optics and Signal Processing*, John Wiley & Sons Ltd (2001).

[14]. R. C. Gonzalez, R. E. Woods, S. L. Eddins, *Digital Image Processing Using Matlab*, Gatesmark Publishing (2009).

[15]. E. Pérez, K. Chałasińska-Macukow, K. Styczyński, R. Kotyński, M. S. Millán, "Dual nonlinear correlator based on computer controlled joint transform processor: Digital analysis and optical results", *J. Mod. Opt.* **44**, 1535–1552 (1997). DOI

[16]. M. Tebaldi, S. Horrillo, E. Pérez-Cabré, M. S. Millán, D. Amaya, R. Torroba, N. Bolognini, "Experimental color encryption in a joint transform correlator architecture", *J. Physics: Conf. Ser.* **274**, 012054 (2011).

[17]. J. A. Rodrigo, T. Alieva, M. L. Calvo, "Programmable two-dimensional optical fractional Fourier processor", *Opt. Express* **17**, 4976–4983 (2009). DOI

1. Introducción

En las dos últimas décadas, el procesamiento de la información por medios ópticos ha mostrado un gran potencial en su aplicación al campo de la seguridad. Varias técnicas de cifrado óptico han sido propuestas aprovechando su capacidad de procesamiento en paralelo, alta velocidad de cómputo y también por la gran variedad de parámetros físicos controlables que brindan los sistemas de procesamiento óptico, todo esto permite obtener sistemas con un alto grado de seguridad [1].

Un método muy conocido para el cifrado óptico de imagen es el método de cifrado por doble máscara de fase aleatoria (*double random phase encoding*, DRPE) propuesto por Réfrégier y Javidi [2]. El método de cifrado DRPE emplea dos máscaras de fase aleatorias (*random phase mask*, RPM), una RPM en el plano de entrada y otra RPM en el plano de Fourier, con el fin de obtener una imagen cifrada de ruido blanco

estacionario. Posteriormente, el DRPE fue extendido adicionalmente desde el dominio de Fourier al dominio de Fresnel [3] y al dominio fraccionario de Fourier (*fractional Fourier domain*, FrFD) [4], con el propósito de incrementar la seguridad del método de cifrado óptico. Inicialmente, el DRPE propuesto en [2] fue implementado por medio de un procesador óptico 4f [5], y dado que dicho procesador necesita un sistema holográfico para registrar la función cifrada de valores complejos, su implementación física requiere un alineamiento óptico estricto. Por otra parte, el proceso de descifrado necesita una copia exacta del complejo conjugado de una de las RPM usadas como llave del método de cifrado. Para mitigar los requerimientos físicos que impone el procesador óptico 4f, Nomura y Javidi propusieron alternativamente el uso del correlador de transformadas conjuntas (*joint transform correlator*, JTC) para la implementación óptica del DRPE [6]. En la propuesta realizada en [6], la imagen cifrada es la distribución de intensidad dada por el espectro de potencia conjunto (*joint power spectrum*, JPS), la cual es captada por una cámara CCD en el plano de Fourier. Además, el método de descifrado usa exactamente la misma llave de seguridad previamente usada en el método de cifrado. Otras modificaciones del DRPE implementado por medio del JTC han sido propuestas por varios autores [7-9].

La implementación del DRPE basado en un JTC también ha sido extendida desde el dominio de Fourier [6] al domino de Fresnel [10] y al FrFD [11,12]. Las implementaciones del DRPE por medio de un JTC en el FrFD propuestas en [11,12] no reproducen exactamente el algoritmo del DRPE como fue propuesto en [2,6], ya que la imagen descifrada obtenida en [11,12] es diferente a la obtenida en [2,6], tal como se detalla en [9]. Dicha diferencia conlleva una degradación de la calidad de la imagen descifrada. Los sistemas de seguridad propuestos en [11,12] son una generalización del sistema propuesto en [7] desde el dominio de Fourier al FrFD.

En este trabajo se presenta una generalización del sistema de cifrado de imagen basado en un JTC desde el dominio de Fourier al FrFD, con el fin de incrementar la seguridad del sistema y adicionar nuevos grados de libertad para el montaje óptico. En particular, se considera el esquema de cifrado basado en un JTC no lineal propuesto en [9]. El esquema de cifrado propuesto en este trabajo es un sistema óptico con nuevos grados de libertad para su montaje (ya que la posición de la lente en el montaje óptico de cifrado puede ser seleccionada) con respecto a los anteriores sistemas de cifrado basados en la arquitectura JTC [6-9]. El filtrado no lineal que se introduce en la etapa de cifrado es necesario para una implementación más precisa del DRPE por medio del JTC, tal como fue originalmente formulado en [2]. Además, dicho filtrado no lineal mejora la calidad de la imagen descifrada. La no linealidad introducida en la etapa de cifrado no incrementa la cantidad de información a ser almacenada o transmitida, ya que la función cifrada resultante tiene el mismo tamaño que su contraparte sin filtrado no lineal. Finalmente, se presenta una posible implementación óptica de los sistemas de cifrado y descifrado propuestos.

El resto del artículo está organizado de la siguiente forma: la sección 2 muestra la definición y propiedades importantes de la transformada fraccionaria de Fourier. En la sección 3 se presenta el sistema de cifrado propuesto basado en un JTC en el FrFD y filtrado no lineal; en esta sección, también se detallan simulaciones numéricas que ilustran y verifican la propuesta del sistema de cifrado. Finalmente, las conclusiones del artículo son descritas en la sección 4.

2. Transformada fraccionaria de Fourier

La transformada fraccionaria de Fourier (*fractional Fourier transform*, FrFT) de orden α es un operador lineal integral que transforma una función dada $f(x)$ para obtener una función $f_\alpha(u)$ así [13]:

$$f_\alpha(u) = \mathcal{F}^\alpha\{f(x)\} = \int_{-\infty}^{+\infty} f(x) K_\alpha(u,x)\, dx, \quad (1)$$

con

$$K_\alpha(u,x) = C_\alpha e^{i\pi[(u^2+x^2)\cot\alpha - 2ux\csc\alpha]}, \quad (2a)$$

$$C_\alpha = \frac{e^{-i\left(\frac{\pi}{4}\mathrm{sgn}(\alpha)-\frac{\alpha}{2}\right)}}{\sqrt{|sin\alpha|}}, -\pi < \alpha \leq +\pi, \quad (2b)$$

donde K_α es el kernel fraccionario de Fourier y $\mathrm{sgn}(\alpha)$ es la función signo. Para $\alpha = 0$, la FrFT se corresponde a la transformada identidad. Para $\alpha = \pi/2$, la FrFT se reduce a la transformada de Fourier directa. Para $\alpha = \pi$, la FrFT es el operador paridad. Para $\alpha = -\pi/2$, la FrFT se corresponde a la transformada de Fourier inversa. La FrFT inversa corresponde a la FrFT con orden fraccionario $-\alpha$.

Algunas propiedades de la FrFT relevantes en este trabajo son:

$$\mathcal{F}^\alpha\left\{\mathcal{F}^\beta\{f(x)\}\right\} = \mathcal{F}^{\alpha+\beta}\{f(x)\}, \quad (3)$$

$$\mathcal{F}^\alpha\{e^{-i2\pi x_0 x\cot\alpha} f(x-x_0)\} = \\ = e^{-i\pi(2x_0 u\,\csc\alpha + x_0^2\cot\alpha)} f_\alpha(u), \quad (4)$$

donde x_0 es una constante real.

3. Sistema de cifrado de imágenes basado en una arquitectura JTC en el FrFD y filtrado no lineal

La imagen de valor real, con valores en el intervalo de [0,1], a ser cifrada es representada por medio de la función $f(x)$ (la notación matemática es escrita en una dimensión por simplicidad) y las dos RPMs $r(x)$ y $h(x)$ son dadas por:

$$r(x) = \exp\{i2\pi s(x)\}, \quad (5a)$$

$$h(x) = \exp\{i2\pi n(x)\}, \quad (5b)$$

donde $s(x)$ y $n(x)$ son funciones aleatorias, normalizadas, positivas, estadísticamente independientes y uniformemente distribuidas en el intervalo [0,1]. La Fig. 1 (parte I) muestra el esquema óptico de cifrado basado en un arquitectura JTC no lineal en el FrFD. Para el proceso de cifrado, el plano de entrada del JTC está compuesto por dos distribuciones de datos no superpuestas ubicadas lado a lado. La primera distribución de datos está dada por la

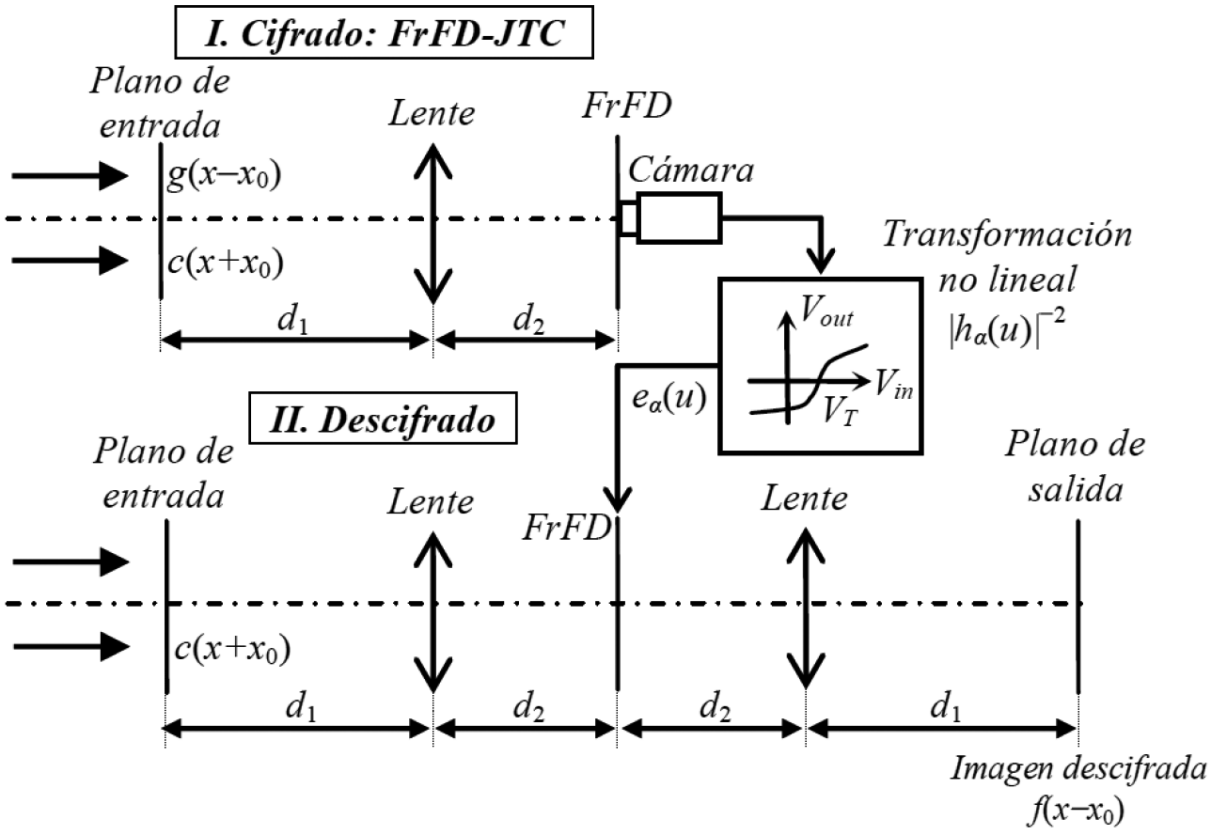

Fig. 1. Representación esquemática del montaje óptico. El sistema de cifrado está basado en una arquitectura JTC no lineal en el FrFD y el sistema de descifrado es compuesto por dos FrFT sucesivas.

imagen real a cifrar $f(x)$ superpuesta sobre la RPM $r(x)$ y dicho producto es modulado por un término de fase pura lineal:

$$g(x) = e^{-i2\pi x_0(x+x_0)\cot\alpha} r(x)f(x), \qquad (6)$$

donde x_0 es una constante real y α es el orden fraccionario de la FrFT. La segunda distribución de datos del plano de entrada del JTC es representada por la RPM $h(x)$ modulada por otro término de fase pura lineal:

$$c(x) = e^{i2\pi x_0(x-x_0)\cot\alpha} h(x). \qquad (7)$$

Las FrFT con orden fraccionario α de las funciones $r(x)f(x)$ y $h(x)$ son representadas por:

$$t_\alpha(u) = \mathcal{F}^\alpha\{r(x)f(x)\}, \qquad (8a)$$

$$h_\alpha(u) = \mathcal{F}^\alpha\{h(x)\}. \qquad (8b)$$

En el proceso de cifrado, $g(x)$ y $c(x)$ son ubicadas lado a lado en el plano de entrada del JTC en las coordenadas $x = x_0$ y $x = -x_0$, respectivamente. El espectro de potencia conjunto fraccionario (*joint fractional power spectrum*, JFPS) de orden α es determinado por:

$$\mathrm{JFPS}_\alpha(u) = |\mathcal{F}^\alpha\{g(x-x_0) + c(x+x_0)\}|^2. \qquad (9)$$

Con el fin de obtener la imagen cifrada, el JFPS es filtrado usando el término no lineal $|h_\alpha(u)|^{-2}$. El resultado de esta transformación no lineal es:

$$\begin{aligned} e_\alpha(u) &= \frac{\mathrm{JFPS}_\alpha(u)}{|h_\alpha(u)|^2} = \frac{|t_\alpha(u)|^2}{|h_\alpha(u)|^2} + 1 + \\ &+ t_\alpha^*(u)\frac{h_\alpha(u)}{|h_\alpha(u)|^2} e^{i2\pi(2x_0)u\,\csc\alpha} + \\ &+ t_\alpha(u)\frac{h_\alpha^*(u)}{|h_\alpha(u)|^2} e^{-i2\pi(2x_0)u\,\csc\alpha}, \end{aligned} \qquad (10)$$

donde la Ec. (4) ha sido usada para obtener la expresión completa de la imagen cifrada. Si $|h_\alpha(u)|^2$ es igual a cero para un valor particular de u, este valor de intensidad es sustituido por una constante de valor pequeño y así evitar singularidades en el cálculo de $e_\alpha(u)$. La imagen cifrada resultante de la Ec. (10) es una función de valor real, por lo tanto dicha imagen cifrada puede ser registrada y almacenada por un dispositivo de adquisición convencional de intensidad óptica, tal como una cámara CCD. A diferencia del DRPE implementado por medio del JTC en el dominio de Fourier, las llaves del sistema de cifrado/descifrado propuesto en este trabajo son dadas por la RPM $h(x)$ y el orden fraccionario α. El orden fraccionario de la FrFT, α, es definido en función de la distancia focal de la lente y las distancias d_1 y d_2 usando relaciones simples [13]. La RPM $r(x)$ es empleada para esparcir el contenido de la información de la imagen original $f(x)$ sobre la imagen cifrada $e_\alpha(u)$. Comparando el sistema de cifrado propuesto en este trabajo con los anteriores sistemas de cifrado basados en el JTC [6-9], el sistema de cifrado no lineal implementado por medio del JTC en el FrFD presenta nuevos grados de libertad para el montaje óptico, ya que la lente presente en el sistema de cifrado puede ser ubicada en diferentes posiciones con respecto al plano de entrada del JTC y el plano del JFPS (plano de salida del JTC).

Para el método de descifrado, la distribución de datos $c(x)$ es ubicada en la coordenada $x = -x_0$ del plano de entrada y consecuentemente, la imagen cifrada $e_\alpha(u)$, localizada en el FrFD, es iluminada por $\mathcal{F}^\alpha\{c(x+x_0)\}$. Usando las Ecs. (4), (7) y (10), el paso inicial del proceso de descifrado puede ser expresado de la siguiente forma:

$$\begin{aligned} d_\alpha(u) &= e_\alpha(u)\mathcal{F}^\alpha\{c(x+x_0)\} = \\ &= e^{i\pi(2x_0u\,\csc\alpha - x_0^2\cot\alpha)}\frac{h_\alpha(u)}{|h_\alpha(u)|^2}|t_\alpha(u)|^2 + \\ &+ e^{i\pi(2x_0u\,\csc\alpha - x_0^2\cot\alpha)}h_\alpha(u) + \\ &+ e^{i\pi(6x_0u\,\csc\alpha - x_0^2\cot\alpha)}t_\alpha^*(u)\frac{h_\alpha^2(u)}{|h_\alpha(u)|^2} + \\ &+ e^{-i\pi(2x_0u\,\csc\alpha + x_0^2\cot\alpha)}t_\alpha(u). \end{aligned} \qquad (11)$$

El cuarto término sobre el miembro derecho de la Ec. (11) retiene la información que se desea descifrar. Por lo tanto, si la FrFT con orden fraccionario $-\alpha$ se aplica al cuarto término de la Ec. (11) y luego se toma el valor absoluto, se obtiene la imagen descifrada en la coordenada $x = x_0$:

$$\begin{aligned} &\tilde{f}(x-x_0) = \\ &\quad = \left|\mathcal{F}^{-\alpha}\left\{e^{-i\pi(2x_0u\,\csc\alpha + x_0^2\cot\alpha)}t_\alpha(u)\right\}\right| \end{aligned} \qquad (12)$$

Nótese como la no linealidad introducida en el cálculo de la imagen cifrada (Ec. (10)) facilita la recuperación de la imagen original en el proceso de descifrado (Ec. (12)). Otras no linealidades podrían usarse en el proceso descrito, pero la división por el módulo al

cuadrado de $h_\alpha(u)$ es la que asegura la recuperación de la imagen original con la mejor calidad [9]. La Fig. 1 (parte II) también muestra el esquema óptico del montaje para la etapa de descifrado, el cual está basado en dos FrFT sucesivas.

Los resultados de la simulación numérica de los procesos de cifrado y descifrado, siguiendo los pasos descritos anteriormente en esta sección, son mostrados con un ejemplo en la Fig. 2. La imagen original a ser cifrada y el código de distribución aleatoria $n(x)$ de la RPM $h(x)$ son presentados en las Figs. 2(a) y 2(b), respectivamente. La imagen cifrada para el orden fraccionario $\alpha = 0.327\pi$ es mostrada en la Fig. 2(c). La Fig. 2(d) es el valor absoluto del plano de salida para el procedimiento de descifrado con las llaves correctas del orden fraccionario α y la RPM $h(x)$. Observamos en la Fig. 2(d) que aparecen 3 términos espacialmente diferenciados. Para que ello sea así, es necesario seleccionar adecuadamente la distancia x_0 en el plano de entrada del JTC y así evitar solapamientos de las distribuciones en el plano de salida del sistema de descifrado. La imagen descifrada presentada en la Fig. 2(e) es la región de interés ampliada, centrada en la coordenada $x = x_0$, del plano de salida del procedimiento de descifrado (Fig. 2(d)). Con el fin de evaluar la calidad de la imagen descifrada, se emplea la raíz cuadrada del error cuadrático medio (*root mean square error*, RMSE), definido de la siguiente manera [14]:

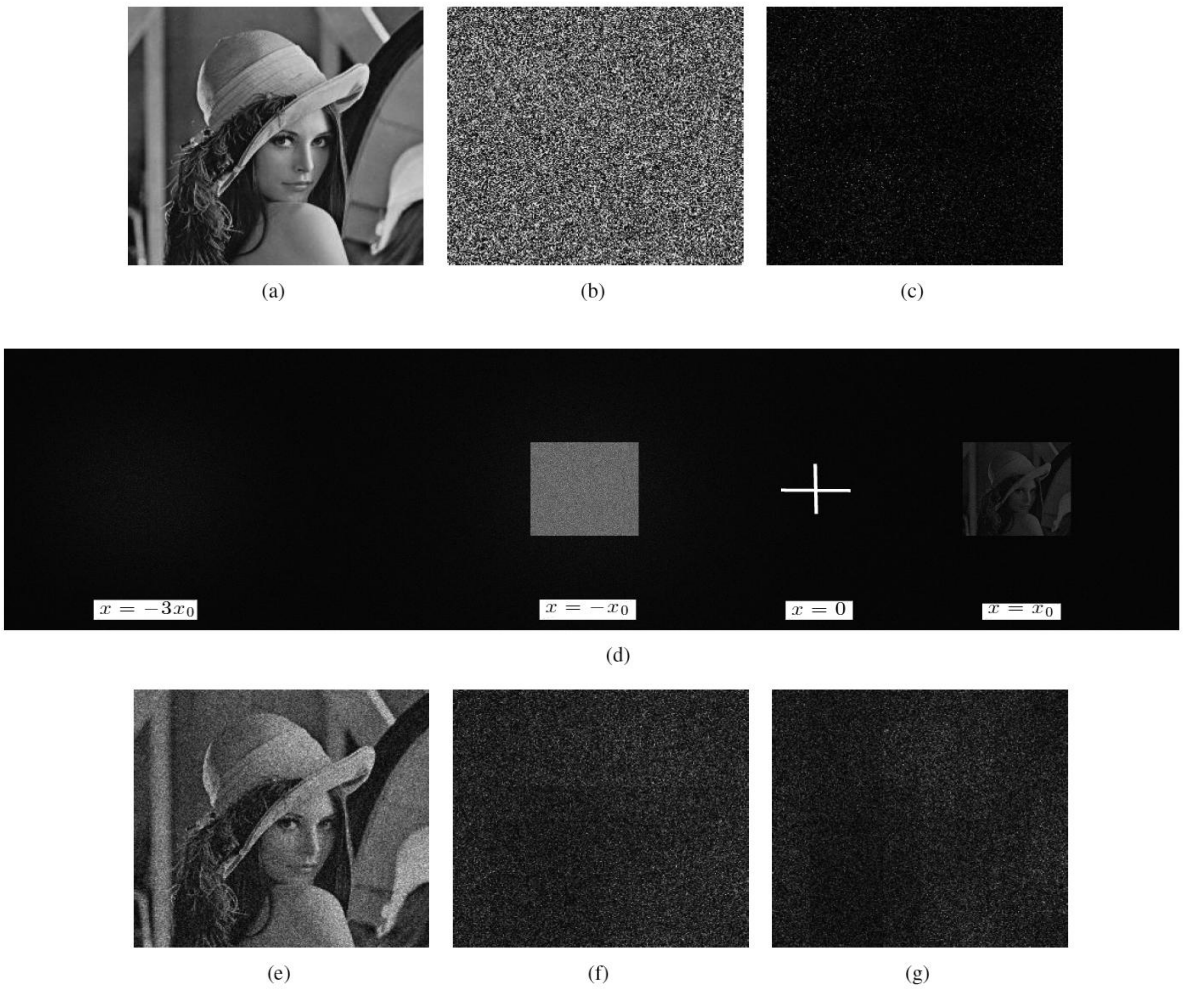

Fig 2. (a) Imagen original a ser cifrada $f(x)$ de 256×256 píxeles, (b) Código de distribucción aleatoria $n(x)$ de la RPM $h(x)$, (c) Imagen cifrada $e_\alpha(u)$ para la llave $\alpha = 0.327\pi$, (d) Valor absoluto del plano de salida para el procedimiento de descifrado con las llaves correctas α y la RPM $h(x)$, (e) Región de interés ampliada de (d), correspondiente a la imagen descifrada $\tilde{f}(x)$. Imágenes descifradas: (f) cuando el filtrado no lineal de la Ec. (10) no es introducido sobre la función de cifrado y las llaves correctas son usadas, y (g) después de usar un valor incorrecto del orden fraccionario $\alpha = 0.337\pi$, el filtrado no lineal y la RPM $h(x)$ correcta.

$$\mathrm{RMSE} = \left(\frac{\sum_{x=1}^{M} \left[f(x) - \tilde{f}(x) \right]^2}{\sum_{x=1}^{M} [f(x)]^2} \right)^{1/2}, \qquad (13)$$

donde $f(x)$ y $\tilde{f}(x)$ representan la imagen original y la imagen descifrada, respectivamente. El RMSE entre la imagen original de la Fig. 2(a) y la imagen descifrada de la Fig. 2(e) es 0.147. La Fig. 2(f) muestra la imagen descifrada cuando el filtrado no lineal no es aplicado en la Ec. (10) y se emplean las llaves correctas en la etapa de descifrado.

La imagen resultante es ruidosa y por lo tanto se hace muy difícil discernir la imagen original en la imagen descifrada obtenida. El resultado de la Fig. 2(f) demuestra que el filtrado no lineal aplicado en la etapa de cifrado es importante para la recuperación de la imagen original en la etapa de descifrado. Cuando una imagen original es cifrada con un valor muy cercano a $\alpha = \pi/2$ (dominio de Fourier) y sin emplear el filtrado no lineal, en el resultado del proceso de descifrado es posible distinguir la imagen original con una mala calidad, tal como fue demostrado en [9].

Finalmente, se evalúa la influencia de las llaves correctas sobre la calidad de la imagen descifrada del sistema de seguridad propuesto usando simulaciones numéricas. La imagen descifrada a partir de la imagen cifrada de la Fig. 2(c) usando un valor incorrecto del orden fraccionario $\alpha = 0.337\pi$, el filtrado no lineal y la RPM $h(x)$ correcta, es mostrada en la Fig. 2(g). La imagen descifrada resultante tiene una apariencia de ruido sin ninguna información de la imagen original. Si la RPM $h(x)$ es incorrecta para el procedimiento de descifrado, se obtiene una imagen descifrada muy ruidosa, similar a la presentada en la Fig. 2(g).

El procedimiento de cifrado propuesto en este trabajo puede ser implementado usando el montaje optoelectrónico esquematizado de la Fig. 1 (parte I) y siguiendo el procedimiento propuesto en [15,16] con una extensión al FrFD. La imagen cifrada dada por la Ec. (10) puede ser ópticamente implementada por medio de un JTC de dos pasos [15] en el FrFD. En el primer paso, $|h_\alpha(u)|^2$ es captada por una cámara CCD, donde dicha función de intensidad es igual a $|h_\alpha(u)|^2 = |\mathcal{F}^\alpha\{c(x + x_0)\}|^2$. Luego, el JFPS representado por la Ec. (9) es captado en el segundo paso [15,16]. Por último, el JFPS es filtrado no linealmente de forma digital por medio de $|h_\alpha(u)|^{-2}$ y así de esta manera, se obtiene la imagen cifrada. La imagen cifrada es la única información que debe ser almacenada o transmitida, por lo tanto la cantidad de información que se necesita para iniciar el procedimiento de descifrado no se incrementa [9,10]. La FrFT óptica puede ser implementada por medio del montaje optoelectrónico descrito en [17].

4. Conclusiones

En este trabajo se ha presentado un método de cifrado-descifrado de imágenes basado en una arquitectura JTC en el FrFD y filtrado no lineal. El sistema de cifrado propuesto es un montaje óptico con nuevos grados de libertad (en relación con la posición de la lente) en comparación con los sistemas de seguridad convencionales basados en el JTC. Se introdujo una llave adicional, la cual es el orden fraccionario α, que incrementa el nivel de seguridad del sistema propuesto. El filtrado no lineal aplicado en el FrFD permitió la recuperación de la imagen original en el proceso de descifrado y de la misma forma también mejoró la seguridad de la imagen cifrada. Dado que el filtrado no lineal del JFPS es aplicado justo antes de la generación de la imagen cifrada, no se obtiene un incremento adicional de la información a ser almacenada o transmitida. Finalmente, la realización experimental del sistema de cifrado no lineal y el sistema de descifrado es adecuada para una implementación optoelectrónica: una arquitectura JTC de dos pasos puede ser usada para la etapa de cifrado y para la etapa de descifrado se pueden emplear dos FrFT ópticas sucesivas.

Agradecimientos

Esta investigación ha sido parcialmente financiada por el Ministerio Español de Ciencia e Innovación y Fondos FEDER (Project DPI2009-08879). El primer autor también desea agradecer al Departamento Administrativo de Ciencia, Tecnología e Innovación de Colombia, COLCIENCIAS, por la beca de estudios doctorales concedida.

