Optics and Lasers in Engineering 46 (2008) 522–526

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

journal homepage: www.elsevier.com/locate/optlaseng

Image encryption and decryption using fractional Fourier transform and radial Hilbert transform

Madhusudan Joshi [a,*], Chandra Shakher [b], Kehar Singh [c]

[a] The International Centre for Automotive Technology, Plot No. 26, Sector 3, IMT Manesar, Gurgaon-122050, Haryana, India
[b] Instrument Design and Development Centre, Indian Institute of Technology Delhi, New Delhi-110016, India
[c] Department of Physics, Indian Institute of Technology Delhi, New Delhi-110016, India

ARTICLE INFO

Article history:
Received 19 January 2008
Received in revised form
16 February 2008
Accepted 3 March 2008
Available online 16 April 2008

Keywords:
Encryption
Decryption
Fractional Fourier transform
Hilbert transform

ABSTRACT

A technique for image encryption using fractional Fourier transform (FRT) and radial Hilbert transform (RHT) is proposed. The spatial frequency spectrum of the image to be encrypted is first segregated into two parts/channels using RHT, and image subtraction technique. Each of these channels is encrypted independently using double random phase encoding in the FRT domain. The different fractional orders and random phase masks used during the process of encryption and decryption are the keys to enhance the security of the proposed system. The algorithms to implement the proposed encryption and decryption scheme are discussed, and results of digital simulation are presented.

1. Introduction

The threat of illegal data access has made the data encryption an important subject. Out of the several techniques proposed for optical image encryption [1–16], the double random phase encoding [17] is the most well-known. This technique uses two statistically independent random phase masks in the input and the Fourier planes to encrypt the input image into a stationary white noise. An extension of this technique to the fractional Fourier domain [18,19] has been presented by Unnikrishnan et al. [20] and later significant work has been done in this area by other researchers [21–26]. Optical encryption offers several image parameters, e.g. phase, amplitude, color, spatial frequency, polarization, etc., that can be exploited to perform a robust and highly secure encryption.

In this paper, we propose a technique for a spatial frequency-based image encryption in the fractional Fourier domain using the properties of radial Hilbert transform (RHT) [31]. The image to be encrypted is multiplied with a random phase function, and a two-dimensional fractional Fourier transform (FRT) of some order is calculated to obtain its randomized spatial frequency spectrum in the fractional domain. This spatial frequency spectrum of the image is then multiplied with a RHT mask to get the high-frequency part [31]. The remaining part of the spatial frequency spectrum of the image under consideration is calculated by performing image subtraction technique in the fractional Fourier domain. The frequency spectra of the image obtained as mentioned above are multiplied with two different random phase functions and two independent FRTs are calculated to obtain the encrypted images. The whole process would require an extra random phase function and two extra fractional orders that make this technique more secure and robust as compared to conventional double random phase encoding technique in the fractional Fourier domain. It is also possible to vary the distribution of spatial frequencies in the two channels mentioned above by changing the fractional order of the RHT, and its impact on the quality of encryption can also be understood.

The MATLAB 7.0 platform has been used to perform the simulations to demonstrate the proposed idea. It is shown that the decrypted image matches with the input image only when the correct fractional orders as well as correct random phase functions are used during the process of decryption. The mean-square-error (MSE) is calculated for different fractional orders in the high-frequency channel, and the channel corresponding to the rest of the frequencies. The effect of changing the fractional order of RHT has also been discussed.

2. Principle

2.1. Definition of FRT

Conventionally, the nth order FRT [17], $f_n(x_n)$, of a function $f(x)$ is calculated using integral transform kernel given by

$$K_n(x,x_n) = \begin{cases} \xi_\phi \exp\{j\pi(x^2\cot\phi - 2xx_n + x_n^2\cot\phi\}, & 0<|n|<2, \\ \delta(x-x_n), & n=0, \\ \delta(x+x_n), & n=\pm 2, \end{cases}$$

* Corresponding author. Tel.: +91 9810777619.
E-mail address: madhusudanjoshi@gmail.com (M. Joshi).

0143-8166/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.optlaseng.2008.03.001

where
$\xi_\phi = \exp[-j\pi \mathrm{sgn}(\sin\phi)/4 + j\phi/2]$ and $\phi = a\pi/2$.

Here, x and x_n represent the coordinate systems, respectively, for the input (zeroth order) domain and the output (nth order) fractional domain. The FRT is linear and has the property that it is index additive,

$F^a\{F^b\{f(x)\}\} = F^{a+b}\{f(x)\}$, where a and b are different fractional orders of FRT.

It is possible to extend the definition of the FRT order beyond ± 2:

$$F^a\{f(x)\} = F^{a+4m}\{f(x)\}, \quad \text{where } m \text{ is an integer}.$$

The extension of the definition to 2-dimensional signals is straightforward and simple.

2.2. Hilbert transform, fractional Hilbert transform and RHT

The Hilbert transform [27] has been widely used in image processing and phase observation on account of its edge-enhancing properties. The generalization of the conventional Hilbert transform to fractional counterpart has been explained by Lohmann et al. [28]. Both of its forms are useful to selectively emphasize the features of the input image during the spatial filtering operations [29]. The Hilbert transform forms an edge-enhanced version of the input image, whereas the fractional Hilbert transform changes the nature of the edge enhancement. The classic Hilbert filter enhances the image only along one dimension. Although it is possible to create two-dimensional masks by performing the product of two Hilbert masks, these masks retain the basic x, y symmetry only [30]. However, it is possible to maintain the basic concept of the Hilbert mask and avoid the x, y symmetry by making a radial counterpart [31] given by

$$H_P(r,\theta) = \exp(iP\theta),$$

where the variables (r,θ) represent the polar coordinates and P represents the fractional order of the radial Hilbert transform. The opposite halves of any radial line of the mask have a relative phase difference of $P\pi$ radian. Therefore, for each radial line we have the equivalent of a one-dimensional Hilbert transform of order P.

The Fourier transform of the radial mask is a Hankel transform of order P [31]. The convolution with the mask results in high-frequency spectra of the input image that depends upon the order of the Hankel transform. Recently, an extension of the RHT to fractional field has also been carried out by Xie et al. [32]

2.3. Double random Fourier plane encoding

Let (x,y) denote the space coordinates, and (u,v) the coordinates in the Fourier domain (Fig. 1(a)). The real-valued function $f(x,y)$ denotes the original two-dimensional image to be encrypted. The original image $f(x,y)$ is multiplied by a random phase function $\phi_1(x,y)$ and is subsequently Fourier transformed. In the next step, the Fourier transformed data are multiplied with another phase mask $\phi_2(u,v)$, which is statistically independent of $\phi_1(x,y)$. An inverse Fourier transform is then performed on this image to obtain the encrypted image in space domain. The encrypted image is recorded using a CCD camera. It can be shown that the encrypted data are a stationary white noise.

During the decryption process (Fig. 1(b)), the encrypted image is Fourier transformed and multiplied with the complex conjugate of $\phi_2(u,v)$. The image thus obtained is inverse Fourier transformed to get the decrypted image. The two random phase functions used during the process of encryption act as keys for data security during decryption [16].

2.4. Double random fractional Fourier plane encoding

The application of this method is motivated by the fact that it is quite possible to perform double random encoding in the input and fractional Fourier planes. The method may be regarded as a generalization of the previous method in the sense that the input encryption and the output planes are related to each other by the FRT [17,18]. This technique [19] is established to be more secure as compared to its Fourier counterpart, because one needs to know the fractional orders relating the input encryption and the output planes in addition to the random phase mask. It is also important

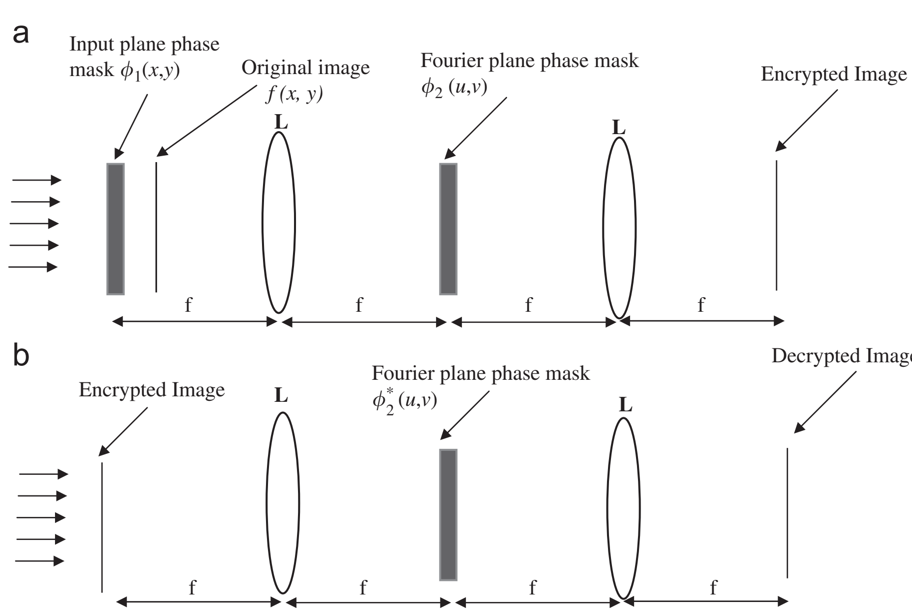

Fig. 1. Schematic for double random Fourier plane encoding. (a) Encryption process; (b) decryption process. 'L' is Fourier transforming lens (FTL), 'f' is focal length of FTL, '*' denotes complex conjugate.