Optics and Lasers in Engineering 48 (2010) 605–615

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Image encryption using radial Hilbert transform filter bank as an additional key in the modified double random fractional Fourier encoding architecture

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

[a] The International Centre for Automotive Technology, 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 30 May 2009
Received in revised form
24 September 2009
Accepted 25 September 2009
Available online 23 October 2009

Keywords:
Encryption
Decryption
Fractional Fourier transform
Hilbert transform
Filter bank

ABSTRACT

We propose a method for image encryption using a radial Hilbert transform (RHT) filter bank in the factional Fourier transform (FRT) domain. The filter bank comprises of multiple integral order RHT filters. The scheme is implemented using the well-known double random phase encoding technique. The random phase functions, fractional orders of the FRT, and integral orders of the multiple RHT filters forming the filter bank are used as key parameters for encryption and decryption. Simulation results have been presented to analyze the performance of the proposed scheme with respect to variation in key parameters, and the schematic for its optical implementation has been presented. Effectiveness of the scheme is also shown against the noise, occlusion and attacks using partially correct random phase keys. The effect on decryption, of rotation of the RHT filter bank as well as some of the RHT filters of the filter bank has been studied. Simulation results are also presented to exhibit the performance of the technique against reshuffling the positions of the RHT filters during the decryption. Investigations have also been carried out to analyze the proposed technique against the chosen- and the known-plain-text attacks.

1. Introduction

Quest to ensure information security has become a very important subject with the rapid development of communication technologies. Several methods have been proposed [1–7] for optical image encryption including the most popular double random phase encoding (DRPE) [8]. Using the DRPE, the image to be encrypted is changed to noise-like patterns and exact recovery of the image is possible only when the correct random phase functions and other key parameters are correctly used during the decryption. An extension of this technique to the fractional Fourier domain [9–12] has been presented by Unnikrishnan et al. [13] and recently significant work has been done in this area by other researchers [14–27]. Mathematically, the fractional Fourier transform (FRT) is a generalization of the conventional Fourier transform and can be physically interpreted as the quadratic phase modulated near-field diffraction of light, and hence a powerful tool in optical information processing.

The Hilbert transform (HT) [28] has been widely used for signal and image processing applications. The radial Hilbert transform (RHT) is a radially symmetric version of the HT and the fractional HT [29–31]. Davis et al. [32] have proposed its application for the edge enhancement of images through spatial filtering operations. Recently, an application of the RHT for image encryption has been proposed [33] in the FRT domain. In this technique, the RHT mask has been used as a spatial filter to segregate the spatial frequencies into two channels, and subsequently the encryption is performed using the DRPE algorithm. The fractional orders of the FRT and the random phase masks have been used as keys for encryption.

In the present paper, an effective technique for optical image encryption using the integral order RHT filter bank has been proposed in the FRT domain. The integral orders of the RHT, fractional orders of the FRT, and the random phase masks used during the process are the keys for encryption and decryption. Simulation results have been presented to show that the presence of the RHT filter bank provides a better security to the system. Robustness of the proposed technique has been checked against variation of the key parameters like fractional orders of the FRT, integral order of the RHT filter bank, and random phase masks. The performance of the proposed scheme has also been analyzed against occlusion, noise and attacks using partial windows of the correct random phase keys [34,35]. Mean-square-error (MSE) between the input image and the decrypted image is plotted in presence of noise in the FRT plane random phase mask. MSE and signal-to-noise ratio (SNR) between the input image and the

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

0143-8166/$ - see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.optlaseng.2009.09.014

decrypted image are also calculated with respect to the variation in fractional orders of the FRT, respectively. The sensitivity of the scheme has also been investigated against the change of orientation of the RHT filters during the decryption. Simulation results for the conventional DRPE in Fourier and fractional Fourier domain are also presented for comparison. Investigations have also been carried out to analyze the technique against the chosen- and the known-plain-text attacks [35]. The technique can be realized on a conventional 4-f set-up for implementing the DRPE algorithm and does not require any special optical arrangement.

2. Theory

2.1. Hilbert transform, fractional Hilbert transform and RHT

The Hilbert transform (HT) [28] has numerous applications in image processing, selective edge enhancement, phase observation, etc. Generalization of the HT to the fractional domain has been presented by Lohmann et al. [29]. Both HT and fractional HT, selectively emphasize the features of the input image during the spatial filtering operations [30,31]. The HT of an image produces its edge-enhanced version, whereas the fractional HT changes the nature of the edge enhancement. The conventional Hilbert filter produces an edge-enhanced image only along one dimension. It is also possible to produce two-dimensional edge enhancement of the image by combining two orthogonal Hilbert filters. However, these masks retain the basic x, y symmetry [32]. A uniformly edge-enhanced image can be produced if radial version [32] of the Hilbert mask is used and it is given as

$$H_P(r,\theta) = \exp(iP\theta), \tag{1}$$

where the variables (r,θ) represent the polar coordinates and P represents the 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. Recently, an extension of the RHT to fractional field has also been carried out by Xie and Daomu [36]. The Fourier transform of the radial mask is a Hankel transform of order P [32]. The convolution with the mask results in high-frequency spectra of the input image that depends upon the order of the Hankel transform.

The first-order RHT corresponds to a continuous phase variation from 0 to 2π, whereas its higher orders would lead to such multiple changes. Figs. 1 (i) and 1(ii) show the RHT for P=1 and 4, respectively. It can be observed that the RHT for P=4 leads to four phase variations from 0 to 2π. Besides this, a negative order of the RHT would produce a reverse phase change, e.g. from 2π to 0 for $P=-1$ (Fig. 1 (iii)). This negative-order RHT is termed as the inverse RHT (IRHT). The numbers of phase jumps as mentioned are used as a key during the encryption and the recovery of the image during decryption is possible only when the number of phase variations are equal as well as reversed. It is also possible to design a filter bank using multiple RHT masks. An RHT filter bank can be mathematically expressed as $H_{pn}(r, \theta)$, where P and n are integers representing order of a given RHT mask and number of the RHT masks used for making a filter bank. A typical RHT filter bank with n=4 and P=3, 5, 7 and 9, respectively, is shown in Fig. 1(iv).

2.2. Double random Fourier plane encoding

Figs. 2(i) and (ii), respectively, show the encryption and decryption schemes for the well-known DRPE application, in the absence of the RHT filter bank and with all d_1, d_2, d_3, and d_4 equal to focal length (f) of the Fourier transforming lenses used in the set-up. Here (x, y) denote the space coordinates, and (u, v) the coordinates in the Fourier domain. 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. The Fourier transformed data is then 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 is a stationary white noise.

During the decryption process, 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 [8].

2.3. Double random fractional Fourier plane encoding

It is quite possible to perform double random encoding in the input- and fractional Fourier planes. The method is the generalization of DRPE method where the input-, encryption- and the output-planes are related to each other by FRT [9–12]. This technique is relatively more secure as compared to its Fourier counterpart, as the fractional orders of FRT relating the input-, encryption-, and the output planes act as encryption keys in addition to the random phase masks. The digital as well as the optical implementation of the FRT are simple and can be calculated in the same order of time as the Fourier transform. For the sake of simplicity, steps involved in the encryption are presented in one dimension only, and are as follows.

The primary image $f(x)$ is multiplied by the random phase function $\phi_1(x)$. An ath order FRT of $f(x)\phi_1(x)$ is taken and multiplied with $\phi_2(u)$ in the fractional domain. A subsequent bth order FRT gives the encrypted signal in the $(a+b)$th fractional domain; the encrypted signal being a stationary white noise. The symbols have usual meaning as described in the previous section except that u is a coordinate in the ath fractional domain. The decryption can be done in two ways. In the first approach

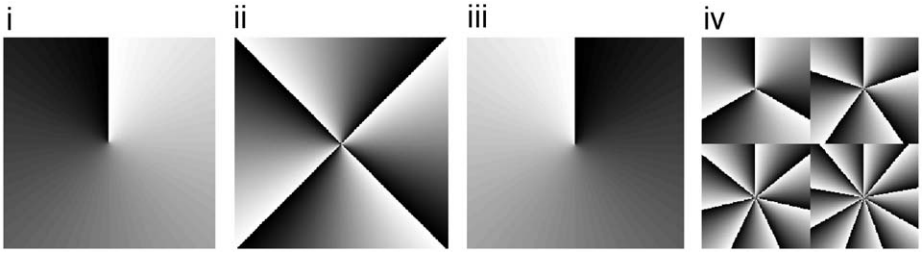

Fig. 1. (i) RHT for P=1; (ii) RHT for P=4; (iii) RHT for $P=-1$, (iv) typical RHT filter bank $H_{pn}(r, \theta)$ (with p=3, 5, 7, 9 and n=4).