Optik 125 (2014) 5309–5315

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Image encryption using fractional Mellin transform, structured phase filters, and phase retrieval

Sunanda Vashisth, Hukum Singh, A.K. Yadav*, Kehar Singh

Department of Applied Sciences, ITM University, Sector 23-A, Gurgaon 122 017, Haryana, India

ARTICLE INFO

Article history:
Received 24 September 2013
Accepted 25 May 2014

Keywords:
Fractional Mellin transform
Structured phase masks
Toroidal zone plate
Radial Hilbert mask
Phase retrieval algorithm

ABSTRACT

An image encryption scheme has been presented by using two structured phase masks in the fractional Mellin transform (FrMT) plane of a system, employing a phase retrieval technique. Since FrMT is a non-linear integral transform, its use enhances the system security. We also add further security features by carrying out spatial filtering in the frequency domain by using a combination of two phase masks: a toroidal zone plate (TZP) and a radial Hilbert mask (RHM). These masks together increase the key space making the system more secure. The phase key used in decryption has been obtained by applying an iterative phase retrieval algorithm based on the fractional Fourier transform. The algorithm uses amplitude constraints of secret target image and the ciphertext (encrypted image) obtained from multiplication of fractional Mellin transformed arbitrary input image and the two phase masks (TZP and RHM). The proposed encryption scheme has been validated for a few grayscale images, by numerical simulations. The efficacy of the scheme has been evaluated by computing mean-squared-error (MSE) between the secret target image and the decrypted image. The sensitivity analysis of the decryption process to variations in various encryption parameters has also been carried out.

1. Introduction

Image encryption and decryption have attracted attention of researchers and practitioners in the area of image processing for information security during the last few decades. It is now well-known that optical techniques for information security [1–3] have several advantages over digital techniques. A combination of optical and digital (i.e., hybrid) techniques can provide advantages inherent in both of them. A large number of papers have been published based on the double random phase encoding (DRPE) and its variants. DRPE based encryption schemes have been devised using various integral transforms and their fractionalized versions. For example, Fourier transform [4–8], Gyrator transform [9,10], Hartley transform [11,12], Arnold transform [13], and Mellin transform [14–16], etc. have been used extensively.

The two most extensively used techniques so far are based on the DRPE and fractional Fourier transforms (FrFT). However, these are based on linear transforms and are vulnerable to attacks such as known-plaintext attack [17,18]. There are increasing efforts to test the vulnerability of different encryption techniques against various types of attacks such as brute force-, known and chosen plain-text-, and cipher-text attacks, etc. [19–24]. But when FrFT is preceded by transformation of input image to log-polar coordinates, it constitutes fractional Mellin transform (FrMT) technique. FrMT is a non-linear transform and could potentially provide security against most known attacks [17]. The security of an encryption scheme depends on the key space. The larger key space makes it increasingly difficult to break the system by at least brute force attack.

In symmetric cryptosystems, decryption keys are the same as encryption keys. On the other hand, asymmetric cryptosystems have decryption keys different from encryption keys. Asymmetric systems are generally considered more secure than the symmetric ones. The encryption scheme proposed in this paper is based on the FrMT [14–16] and is an asymmetric one. Here, we have used FrMT on an arbitrary input image transformed to an annular domain. The fractional Mellin transformed image is subjected to two structured phase-filters in the frequency domain. Here, the introduction of phase-filters is mainly aimed at enhancing the security by increasing the key space. Structured phase-filters additionally offer some advantages in an optical set-up. This is followed by phase retrieval

* Corresponding author. Tel.: +91 124 2365811–13; fax: +91 124 2367488.
E-mail address: akyadav@itmindia.edu (A.K. Yadav).

http://dx.doi.org/10.1016/j.ijleo.2014.06.068
0030-4026/© 2014 Elsevier GmbH. All rights reserved.

algorithm [25,26] to generate the phase key that will be required in decryption.

2. The encryption scheme

In this section, prior to presenting a schematic diagram of the encryption scheme, a brief description of the associated mathematical transforms and the structured phase masks is given for the sake of continuity and recapitulation. The security of an optical encryption technique depends on several factors including the non-linearity of transform and the enlarged key space used. The proposed scheme is based on the FrMT, a non-linear integral transform [14–16]. According to this, an arbitrary image is first transformed to log-polar coordinates and is then subjected to FrFT, which is a generalization of Fourier transform in fractional order [5] and provides additional degree of freedom for encryption. It is the most widely used tool in signal-, and optical information processing. The FrFT of order α of an input function $f(x)$ can be defined in terms of kernel function as follows (for simplicity, a one-dimensional input function is considered):

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

where the kernel function $K_{\alpha}(x,u)$ is expressed as:

$$K_{\alpha}(x,u)=\begin{cases}A\exp[i\pi(x^2\cot\Phi-2xu\,csc\Phi+u^2\cot\Phi & \alpha\neq n\pi\\ \delta(x-u) & \alpha=2n\pi\\ \delta(x+u) & \alpha=(2n+1)\pi\end{cases} \tag{2}$$

$A=(\exp[-i(\pi(sgn(\Phi)/4)-(\Phi/2))])/\sqrt{|\sin\Phi|}$ and $\Phi=\alpha\pi/2$. Whenever α is an integer multiple of π, the kernel function is expressed in terms of Dirac delta function. In the particular case of transform order $\alpha=1$, FrFT reduces to the conventional full Fourier transform. FrFT is a linear integral transform and its optical implementation is done by using Lohmann's Type I and Type II setups [4,27–29]. A simple extension of FrFT to two-dimensions can be written as:

$$F^{\alpha_1,\alpha_2}\{f(x,y)\}(u,v)=\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}K_{\alpha_1,\alpha_2}(x,y;u,v)f(x,y)dxdy \tag{3}$$

2.1. Fractional Mellin transform

The FrMT is inspired by the fractional Fourier transform. A two-dimensional FrMT of order (p_1,p_2) is the FrFT of the same order (p_1,p_2) of a function in its log-polar transformation. In log-polar representation, the Cartesian space coordinates are converted to polar coordinates relative to the origin of coordinate system where:

$$x=r\cos\theta;\quad y=r\sin\theta;\quad \rho=\ln\sqrt{x^2+y^2=\ln r};\quad \theta=\tan^{-1}\left(\frac{y}{x}\right)$$

In a Cartesian coordinate system, the two-dimensional FrMT of order (p_1,p_2) of an image $f(x,y)$ is given by [16]

$$\begin{aligned}M^{p_1,p_2}(u,v)=&\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}f(x,y)\times x^{-(2iu\pi/\sin\Phi_1)-1}\\&\times\exp\left[\frac{i\pi(u^2+\ln^2 x)}{\tan\Phi_1}\right]\times y^{-(2iv\pi/\sin\Phi_2)-1}\\&\times\exp\left[\frac{i\pi(v^2+\ln^2 y)}{\tan\Phi_2}\right]dxdy\end{aligned} \tag{4}$$

where $\Phi_1=p_1\pi/2$ and $\Phi_2=p_2\pi/2$. When the image is transformed to an annular domain by log-polar transformation, its FrMT of order (p_1,p_2) can be written [16] as:

$$\begin{aligned}M^{p_1,p_2}(u,v)=C&\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}f(\rho,\theta)\\&\times\exp\left\lfloor-2i\pi\left|\left(\frac{u\rho}{\sin\Phi_1}+\frac{v\theta}{\sin\Phi_2}\right)+\frac{i\pi(u^2+\rho^2)}{\tan\Phi_1}\right.\right.\\&\left.\left.+\frac{i\pi(v^2+\theta^2)}{\tan\Phi_2}\right|d\rho d\theta\right\rfloor=F^{p_1,p_2}\{f(\rho,\theta)\}\end{aligned} \tag{5}$$

where C is a constant.

Since, FrMT involves log-polar transformation of the input image prior to its transformation by FrFT, it requires setting up of parameters for transforming the input image to an annular domain. Hence, a few parameters are set in advance such as center position of annular domain, c_x, c_y, the radii of the innermost (r_{in}) and outermost (r_{out}) rings of annular domain and the number of sampling points along distance axis n_r and along angle axis n_w.

2.2. Structured phase masks

Some recent studies [30–35] have used structured phase masks, such as toroidal zone plate (TZP) and radial Hilbert mask (RHM) in their encryption schemes. The structured phase masks have some advantages over the commonly used random phase masks (RPM). Since phase TZPs are the diffractive optical elements, it is difficult to replicate them. TZPs have the advantage of overcoming the problem of axis alignment in an optical setup and possess characteristics of various keys in a single mask as additional security parameters [30–32].

Unlike the DRPE scheme, where RPMs are used in the encryption, here we have used structured phase masks such as TZP and RHM. In this context, one may argue on the relevance of TZP and RHM keys when the FrMT based scheme is considered secure due to its non-linearity. However, we believe that with the increase in computational power and development of new techniques, the security due to non-linearity may be at risk. Hence, we feel that there is a need to enhance the security by increasing the key space by introducing structured phase masks.

The complex amplitude distribution produced by a converging toroidal wave front can be written [30] as:

$$U(r)=\exp\left\{\frac{-ik(r-r_0)^2}{2f}\right\} \tag{6}$$

where f is focal length and r_0 is ring focus radius. The optical axis is assumed to coincide with the z-direction, and propagation constant is $k=2\pi/\lambda$, λ being the wavelength. The TZP corresponding to the sample values of various parameters ($\lambda=632.8$ nm, $f=4$ cm) in Eq. (6) is shown in Fig. 1.

The radial Hilbert transform is another structured phase mask which can serve to make an image edge-enhanced relative to the input image in addition to increasing the key space. The radial Hilbert phase function in log-polar coordinates (ρ,θ) can be written as:

$$H(\rho,\theta)=\exp(iP\theta) \tag{7}$$

where P denotes the order of transformation. It is apparent that 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 radial Hilbert transform can be helpful in aligning the axis of the optical setup [33–35]. The RHM of order $P=6$ has been displayed in Fig. 2.