Contents lists available at SciVerse ScienceDirect

Optics & Laser Technology

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

# Image encryption scheme based on fractional Mellin transform and phase retrieval technique in fractional Fourier domain

Nanrun Zhou [a,b,c,]*, Xingbin Liu [a], Ye Zhang [a], Yixian Yang [b,c]

[a] Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China
[b] Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China
[c] National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China

ARTICLE INFO

*Article history:*
Received 19 July 2012
Received in revised form
27 August 2012
Accepted 27 August 2012
Available online 12 October 2012

*Keywords:*
Fractional Mellin transform
Phase retrieval algorithm
Optical image encryption

ABSTRACT

An image encryption scheme is proposed based on fractional Mellin transform and phase retrieval technique. Any image can be chosen as ciphertext, the selected annular domain of the specified image is first transformed by fractional Mellin transform. With the transformed result and original image, phase-key can be extracted by using phase retrieval technique in fractional Fourier domain. The proposed scheme can reduce the burden of transmission, enlarge key space, and can be extended to multiple-image encryption. Simulation results demonstrate the feasibility and effectiveness of the proposed scheme.

© 2012 Elsevier Ltd. All rights reserved.

## 1. Introduction

With the rapid development of multimedia and network, information security plays an important role and has attracted more and more attention. Image encryption technique is one of the hottest topics. Optical information process developed much further due to its intrinsic parallelism and extra-high processing speed. By combining optical information processing with image encryption technique, various optical image encryption and hiding algorithms have been proposed during the past two decades [1–14]. Most of the schemes are based on Fourier transform or fractional Fourier transform (FrFT). In recent years, some transforms as new tools are employed in the image encryption system, such as fractional Hartley transform [15], fractional cosine transform [16], fractional Mellin transform (FrMT) [17], and so on. Among them, fractional Mellin transform is a nonlinear transform and can be realized by optoelectronic hybrid system [17]. Before processing image with FrMT, some parameters should be set in advance, such as center position, radii of annular image, and fractional orders. Therefore, FrMT can provide more degrees of freedom in the encryption process than FrFT. These characteristics of FrMT can strengthen the security of the encryption system and make it an excellent tool in image encryption. In addition, Some optical image encryption algorithm based on phase retrieval technique [18–21], information prechoosing [22], and other techniques [23–25] have been proposed recently, which can be widely used in protecting confidential information. Multiple-image encryption (MIE) as a newly developed image encryption technique demonstrates tremendous potential, a lot of algorithms of MIE had been proposed during the last few years [26–31].

In this paper, we propose an image encryption scheme based on fractional Mellin transform (FrMT) and phase retrieval technique. The annular domain should be chosen in advance for FrMT is carried out in annular domain. Thus, different annular domains can be chosen from the selected ciphertext to achieve multiple-image encryption. Any image can be chosen as ciphertext, the annular domain of ciphertext is first transformed by FrMT. With transformed result and original image, phase-key can be generated in the phase retrieval process. During the decryption process, the original image can be recovered with parameters of FrMT, phase-key and the order of FrFT. In general, images processed by FrMT will increase data. This algorithm can take advantages of this characteristic of FrMT to encrypt a larger image than the ciphertext by choosing proper parameters. The keys of the encryption system include the orders of FrMT and FrFT, and phase-key function generated in the iterative process. This encryption scheme is free of using random phase masks and the classical image can be selected as ciphertext which will reduce the burden of transmission. Moreover, the scheme implemented by optoelectronic devices is presented correspondingly.

The rest of this paper is organized as follows. The basic principle of the proposed encryption scheme is introduced in Section 2. Simulation results are presented and analyzed in Section 3. A brief conclusion is given in Section 4.

* Corresponding author at: Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China. Tel.: +86 791 83969670; fax: +86 791 83969679.
*E-mail addresses:* znr21@163.com, nrzhou@163.com (N. Zhou).

0030-3992/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.optlastec.2012.08.033

## 2. Image encryption scheme based on FrMT and phase retrieval technique

FrFT is one of the powerful tools widely used in signal and optical information processing. Conventionally, the $\alpha$ order FrFT of input function $f(x)$ can be defined by using kernel function as follows:

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

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

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

and

$$A=\frac{\exp\left[-\mathrm{i}\left(\pi\mathrm{sgn}(\phi)/4-\phi/2\right)\right]}{\sqrt{|\sin\phi|}}, \tag{3}$$

$\phi=\alpha\pi/2$ is the transform angle, when $\alpha=1$, the FrFT reduces to the conventional Fourier transform. The definition of two-dimensional FrFT is straightforward and shown as follows

$$F^{\alpha_1,\alpha_2}\{f(x,y)\}(u,v)=\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}K_{\alpha_1,\alpha_2}(x,y;u,v)f(x,y)\mathrm{d}x\mathrm{d}y, \tag{4}$$

where

$$K_{\alpha_1,\alpha_2}(x,y;u,v)=K_{\alpha_1}(x,u)K_{\alpha_2}(y,v) \tag{5}$$

FrFT satisfies the Paseval energy conservation theorem, i.e., the energy of $f(x,y)$ is equivalent in the time domain and frequency domain

$$\int\int_{-\infty}^{+\infty}\left|F^{\alpha}[f(x,y)]\right|^2dudv=\int\int_{-\infty}^{+\infty}\left|F^{\alpha}[f(x,y)]\right|^2dxdy \tag{6}$$

In a rectangular Cartesian coordinate system, the two-dimensional FrMT [32] of $f(x,y)$ with orders $(p_1,p_2)$ is

$$\begin{aligned} M^{(p_1p_2)}(u,v)=&\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}f(x,y)x^{-(2iu\pi/\sin\Phi_1)-1}\times\exp\left[\frac{i\pi(u^2+\ln^2x)}{\tan\Phi_1}\right],\\ &\times y^{-(2iv\pi/\sin\Phi_2)-1}\exp\left[\frac{i\pi(v^2+\ln^2y)}{\tan\Phi_2}\right]dxdy \end{aligned} \tag{7}$$

where $\Phi=(p_1\pi/2)$ and $\Phi=(p_2\pi/2)$.

In general case, FrMT with order $(p_1,p_2)$ of an image is FrFT with the same orders $(p_1,p_2)$ of the image in its log-polar representation, which is expressed as

$$\begin{aligned} M^{(p_1,p_2)}(u,v)&=C\cdot\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}f(\rho,\theta)\\ &\quad\times\exp\Big[-2\pi i((u\rho/\sin\Phi_1)+(v\theta/\sin\Phi_2))\\ &\quad+\pi i(u^2+\rho^2/\tan\Phi_1)+(v^2+\theta^2/\tan\Phi_2))\Big]d\rho d\theta\\ &=F^{(p_1,p_2)}(f(\rho,\theta)), \end{aligned} \tag{8}$$

where $C$ is a constant and $\rho=\ln\sqrt{x^2+y^2}$, $\theta=\arctan\frac{y}{x}$.

In the process of implementing FrMT, log-polar transformation process is involved, so the image transformed by FrMT should be annular domain. Before the image transformation, some parameters should be set in advance, such as the center position of the annular domain $(c_x,c_y)$, the radii of the innermost and outermost rings of the annular domain $(r_{\mathrm{in}},r_{\mathrm{out}})$, and the number of discrete sampling points along distance axis and along angle axis (denoted as $n_r$ and $n_w$). The $n_r$ and $n_w$ can determine the size of transformed image.

The phase retrieval algorithm (PRA) involving iterative process is shown in Fig. 1. The initial amplitude is known and the initial phase is randomly generated with the distribution in [0,2π]. The PRA starts with FrFT of initial input and then obtains the complex function in the transform plane, the amplitude of the complex function is approximation to target image. Next keep the phase of the complex function unchanged and the amplitude changed to the target image, and then the composite image is transformed by inverse fractional Fourier transform (IFrFT). The phase of the transformed result substitutes the phase of input and next loop starts. Repeat the above described process until the algorithm is convergence or reaches the pre-set number of iterations.

The schematic of encryption and decryption processes are shown in Fig. 2(a) and (b), respectively. In the proposed encryption scheme, we can choose an arbitrary image as ciphertext. As shown in Fig. 2(a), assuming a real valued image $C(x,y)$ is selected as ciphertext and $C_r(x,y)$ is the selected annular domain of $C(x,y)$ with inner radius $r_{\mathrm{in}}$ and outer radius $r_{\mathrm{out}}$. Then the annular domain is fractional Mellin transformed with order $p$, thus we obtain transformed result $g(x,y)$, which is a complex-valued image and can be written as

$$g(x,y)=A(x,y)\exp\left[\mathrm{i}\varphi(x,y)\right]=M^p\{C_r(x,y)\}, \tag{9}$$

$M^p\{\cdot\}$ represents fractional Mellin transform of order $p$. The size of transformed image is determined by $n_r$ and $n_w$. If the plaintext has the size of $M\times N$ pixels, one can set $n_r=M$ and $n_w=N$, the size of the transformed image $g(x,y)$ will be $M\times N$.

The next step is the main process of the proposed scheme, which is to find the correct phase function under the constraint of the amplitude of FrMT transformed image and original image by using phase retrieval technique. The amplitude of transformed image $g(x,y)$ is extracted first:

$$A(x,y)=\left|g(x,y)\right|, \tag{10}$$

where $|\cdot|$ represents calculating amplitude information of the complex-valued image. Suppose the original image to be encrypted is $I_o(x,y)$, the ultimate goal is to make $I_o(x,y)$ and $A(x,y)$ satisfy the following relationship:

$$I_o(x,y)\exp[\mathrm{i}n(x,y)]=F^{\alpha}\{A(x,y)\exp\left[\mathrm{i}\phi(x,y)\right]\}, \tag{11}$$

where $F^{\alpha}\{\cdot\}$ represents fractional Fourier transform of order $\alpha$, $n(x,y)$ and $\phi(x,y)$ are phase functions which can be obtained by PRA.

The phase retrieval process has been illustrated in Fig. 1, $I_o(x,y)$ is regarded as the target image and $A(x,y)$ is the source image.

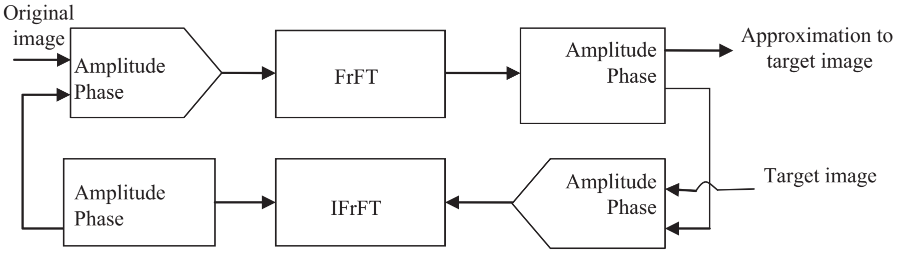

**Fig. 1.** Flowchart of phase retrieval algorithm in FrFT domain.

Download English Version:

https://daneshyari.com/en/article/734582

Download Persian Version:

https://daneshyari.com/article/734582

Daneshyari.com