Optics & Laser Technology 57 (2014) 343–349

Contents lists available at ScienceDirect

Optics & Laser Technology

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

Multiple-image encryption based on optical wavelet transform and multichannel fractional Fourier transform

Dezhao Kong*, Xueju Shen

Department of Electronic and Optics, Ordnance Engineer College, Shijiazhuang 050003, China

ARTICLE INFO

Available online 10 September 2013

Keywords:
Optical image encryption
Optical wavelet transform
Multichannel fractional Fourier transform

ABSTRACT

A multiple-image encryption scheme based on the optical wavelet transform (OWT) and the multichannel fractional Fourier transform (MFrFT) is proposed. The scheme can make full use of multiresolution decomposition of wavelet transform (WT) and multichannel processing of MFrFT. The mentioned properties can achieve the encryption of multi-image and the encryption of single image. When encryption finished, each image gets its own fractional order and independent keys. Analysis of encrypted effects has been completed. Furthermore, the influence of WT type and order are analyzed, and the application and analysis of MFrFT are accomplished as well. Numerical simulation verifies the feasibility of the scheme and shows that the problem of insufficient capacity is better solved, and the flexibility of scheme increases. A simple opto-electronic mixed device to realize the scheme is proposed.

Crown Copyright © 2013 Published by Elsevier Ltd. All rights reserved.

1. Introduction

Fractional Fourier transform (FrFT) is widely used in image encryption, which is the expansion of Fourier transform in the fields of mathematics and optics. Fractional Fourier transform, as the expansion of Fourier transform in the fields of mathematics and optics, is widely used in image encryption. Since Unnikrishnan et al. proposed the fractional Fourier image encryption system [1], large numbers of researches in the field have been done [1–12]. Typically, Liu et al. proposed image encryption algorithm based on multi-stage and multichannel [2], and Liu et al. proposed random fractional Fourier transform encryption algorithm by making eigenvectors and kernel function random [3,4]. Tao et al. defined a multiple-parameter fractional Fourier transform and proposed the corresponding optical image encryption algorithm [10,11]. It has become a routine method that FrFT is applied in image encryption.

The MFrFT is mainly used in the multichannel optical information processing, such as multi-target recognition system [13], information on anti-counterfeiting [14], and image encryption [15]. MFrFT takes full advantage of the inherent parallelism of the optical system and has characteristics as following: (1) MFrFT for multiple objects can be completed, and each channel is independent of each other; (2) The lens focal length can be varied, which means the order of fractional Fourier transform (FrFT) in the corresponding channel can be different; and (3) The FrFT can be completed simultaneously. Therefore, based on the characteristics, MFrFT can be applied in multi-image encryption appropriately. Wavelet transform is widely used in image processing, including image compression, fusion, filtering, coding, and target recognition [16,17]. At the same time, on account of parallel and high-speed real-time of the optical method, optical wavelet transform has been a hot spot of research. WT's multi-resolution decomposition characteristics make it become a new attempt that OWT is used in image encryption. The fractional wavelet transform is used to encrypt gray image [18], which has been used in the color image encryption as well [19,20].

Based on the relations of the encryption keys and decryption keys, the cryptography can be divided into symmetric cryptography and asymmetric cryptography. The basic characteristic of symmetric cryptosystem is that encryption key and decryption key are the same [21,22]. Its advantages are high security strength, encryption speed, but the keys must be transmitted via a secure and reliable way. Keys management becomes critical factor on system security. The main feature of asymmetric cryptosystem is the difference between the encryption keys and decryption keys [23,24]. It can adapt to the environment where keys management is relatively simple. It can implement digital signatures and verification easily and safely.

Therefore, a multiple-image encryption scheme that combines OWT with MFrFT is proposed. Due to the properties of WT's multiresolution decomposition, images can be decomposed into subimages of different frequencies, and the WT can focus the image's energy on the low-frequency parts as far as possible. Therefore, low-frequency parts obtained by WT can be reassembled into an image. Through corresponding channels, MFrFT are implemented

* Corresponding author. Tel.: +86 311 8799 4222.
E-mail addresses: xiaowu89511@126.com, 529250039@qq.com (D. Kong).

0030-3992/$ - see front matter Crown Copyright © 2013 Published by Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.optlastec.2013.08.013

in the fractional domain encoding for different low-frequency parts. Finally, with the random phase masks used in the process, the encryption scheme is completed. Encrypted images can be obtained in the reverse process. The method can not only solve the problem of insufficient capacity of images better, but also make each image have its own fractional order and keys, which increases the flexibility of the scheme.

2. Wavelet transform

2.1. Basic theory

Optical wavelet transform is the WT realized in optical method. So the WT is introduced firstly.

WT is an inner product between a signal $f(x)$ and a set of wavelets $h^*((x–b)/a)$.

$$W_f(a,b)=\frac{1}{\sqrt{a}}\int_{-\infty}^{\infty} f(x)h^*(\frac{x-b}{a})dx \tag{1}$$

where * denotes the complex conjugate. A mother wavelet $h(x)$ is a finite-duration window function that can generate a family of daughter wavelets $h^*((x–b)/a)$ by varying dilation a and translation b. The mother wavelet must satisfy the admissibility condition that it must be oscillatory to have a zero-integrated area. Extended to the case of two-dimensional, the WT of a two-dimensional signal $f(x,y)$ can be defined as

$$W_f(a_1,a_2,b_1,b_2)=\frac{1}{\sqrt{a_1a_2}}\int\int_{-\infty}^{\infty} f(x,y)h^*(\frac{x-b_1}{a_1},\frac{x-b_2}{a_2})dx\,dy \tag{2}$$

In the frequency domain the wavelets are expressed as:

$$W_f(a_1,a_2,b_1,b_2)=\sqrt{a_1a_2}\int\int_{-\infty}^{\infty} F(u,v)h^*(a_1u,a_2v)e^{j2\pi(b_1u+b_2v)}du\,dv \tag{3}$$

In addition, it can be seen that for any one-dimensional signal, wavelet transform is a function of dilation a and translation b. Therefore two-dimensional signal WT is theoretically a four-dimensional function.

2.2. Discrete wavelet transform (DWT)

In order to illustrate the feasibility of numerical calculation and simplicity of theoretical analysis, discrete processing is necessary for the wavelet transform. Therefore, by making values of a and b in Eq. (1)–(3) discrete, the expressions of the general DWT can be obtained. Generally, the dilation a is made discrete in binary format, and translation b is made discrete in multiple-binary format, then binary WT is created. When $a_k=2^{-k}$, the function of Binary DWT is

$$W_f^k(b)=\int f(x)h^*(2^{-k},b)(x)dx \tag{4}$$

$\varphi^*(2^{-k},b)$ is the conjugate of the wavelet mother function, and $b$is the middle number of$a$. The inverse transform of $W_f^k(b)$:

$$f(x)=\sum_{-\infty}^{\infty}2^k\int W_f^k(b)h_{(2^{-k},b)}(x)db \tag{5}$$

The corresponding expression of the two-dimensional discrete wavelet can be obtained from the Eq. (4) and Eq. (5), and we do not elaborate here. In a general two-dimensional DWT, the data are decomposed into four parts firstly, shown as Fig. 1(a). LL_1 is the low-frequency part; HH_1 is the high-frequency part; and the other two are the diagonal parts. Above is the WT with the order n ($n=1$). LL_1 can be divided into four parts LL_2, HH_2, LH_2 and HL_2, shown as Fig. 1(b). In the third level decomposition, LL_2 is divided. However, the high-frequency parts and diagonal parts will not be decomposed into deeper sub-bands. It is the same to other orders.

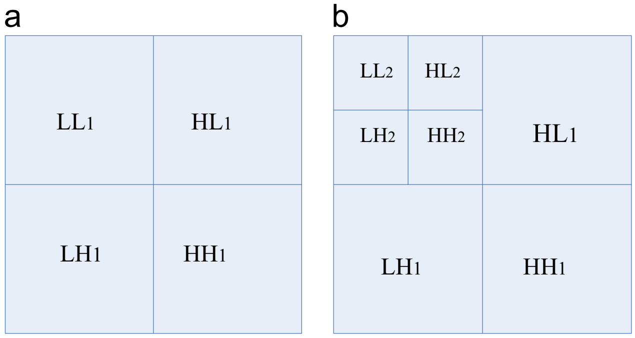

Fig. 1. Discrete wavelet decomposition. (a) $n=1$, and (b) $n=2$.

3. Introduction of scheme

3.1. Basic theory

The scheme is implemented by combining the OWT with MFrFT. WT can focus most energy of the original images on the low-frequency parts. So the sizes of images become smaller as far as possible without loss of image quality. Multi-image encryption can be implemented by using multichannel of MFrFT. Specific scheme is organized as follows:

(1) By completing the wavelet transform of original images $A_i(x,y)$ $(0<i\le n)$ in turn, the corresponding low-frequency parts $B_i(u,v)(0<i\le n)$ are obtained.

(2) The total spectral distribution$A(u,v)$ composed of $B_i(u,v)$ is shown as

$$A(u,v)=\begin{cases} B_1(u,v),\text{if } (u,v)\in S_1 \\ B_2(u,v),\text{if } (u,v)\in S_2 \\ \ldots\ldots \end{cases}$$
$$B_n(u,v),\text{if } (u,v)\in S_n \tag{6}$$

where S_1, S_2, …, S_n are areas of $A(u,v)$.

(3) $B_i(u,v)$ is overlapped with corresponding random phase $\varphi_i(u,v)$. Then the single complex amplitude output $C_i(u,v)=B_i(u,v)\times\varphi_i(u,v)$and the total complex amplitude output $A_p(u,v)$ are obtained as

$$A_p(u,v)=\sum_{i=1}^{n}\{B_i(u,v)\times\varphi_i(u,v)\}=\sum_{i=1}^{n}C_i(u,v) \tag{7}$$

(4) $C_i(u,v)$ $(0<i\le n)$ fulfill FrFT with an order of P_i in different channels, and $F^{P_i}[C_i(u,v)]$ is the result of FrFT with different orders. The $F^{P_i}[C_i(u,v)]$ is overlapped with corresponding random phase $\theta_i(g,h)$. Then the single complex amplitude output $D_i(g,h)=F^{P_i}[C_i(u,v)]\times\theta_i(g,h)$ and the total complex amplitude output $A_m(g,h)$ are obtained as

$$A_m(g,h)=\sum_{i=1}^{n}\{F^{P_i}[C_i(u,v)]\times\theta_i(g,h)\}=\sum_{i=1}^{n}D_i(g,h) \tag{8}$$

$F^{P_i}(C_i)$ denotes the FrFT of $C_i(u,v)$ with an order of P_i. g and h denote the horizontal and vertical coordinates respectively.

(5) After the FrFT is completed based on $D_i(g,h)$ $(0<i\le n)$ in order of Q_i, $O_i(r,t)$ $(0<i\le n)$ and $A_o(r,t)$ are obtained finally. $O_i(r,t)$ is the encrypted image of $A_i(x,y)$, and $A_o(r,t)$ is the total of encrypted image. Finally the encryption is achieved.

$$A_o(r,t)=\sum_{i=1}^{n}(F^{Q_i}\{F^{P_i}[(C_i(u,v)]\times\theta_i(g,h)\})=\sum_{i=1}^{n}O_i(r,t) \tag{9}$$

where $F^{Q_i}(\bullet)$ is a FrFT operator with an order Q_i. r and t denote the horizontal and vertical coordinates respectively.

Download English Version:

https://daneshyari.com/en/article/734421

Download Persian Version:

https://daneshyari.com/article/734421

Daneshyari.com