Available online at www.sciencedirect.com
SCIENCE DIRECT®
Optics Communications 255 (2005) 357–365
OPTICS COMMUNICATIONS
www.elsevier.com/locate/optcom

A discrete fractional random transform

Zhengjun Liu, Haifa Zhao, Shutian Liu *

Harbin Institute of Technology, Department of Physics, Harbin 150001, PR China

Received 25 April 2005; received in revised form 14 June 2005; accepted 14 June 2005

Abstract

We propose a discrete fractional random transform based on a generalization of the discrete fractional Fourier transform with an intrinsic randomness. Such discrete fractional random transform inheres excellent mathematical properties of the fractional Fourier transform along with some fantastic features of its own. As a primary application, the discrete fractional random transform has been used for image encryption and decryption.

PACS: 42.30.−d; 42.40.−i; 02.30.Uu

Keywords: Fractional Fourier transform; Discrete random transform; Cryptography; Image encryption and decryption

1. Introduction

It is well known that the mathematical transforms from time (or space) to frequency domain or joint time–frequency domain, such as Fourier transform, Winger distribution function, wavelet transform and more recent fractional Fourier transform, etc. have long been powerful mathematical tools in physics and information processing. For instance, Fourier transform has been the basic tool for signal representation, analysis and processing, image processing and pattern recognition. In physics the Fourier transform describes well the Fraunhofer (far field) diffraction of light and thus has been the fundamental of information optics [1]. More recently, in the research of quantum information, Fourier transform algorithm has been adopted as an effective and fundamental algorithm in quantum computer [2]. Wavelet transform is a kind of windowed Fourier transform (Gabor transform), however with variable size of the windows [3]. Therefore wavelet transform has been an extremely powerful tool in signal representation in time–frequency joint domain with multi-resolution capability, and has been extensively used in image compression, segmentation, fusion and optical pattern recognitions.

The significance of mathematical transforms manifests itself further when the fractional Fourier

* Corresponding author. Tel.: +86 451 86418042; fax: +86 451 86414335.
E-mail address: stliu@hit.edu.cn (S. Liu).

0030-4018/$ - see front matter
doi:10.1016/j.optcom.2005.06.031

transform was re-invented in 1980s [4,5] and became active from 1990s after its physical interpretations were found in optics [6–8]. Actually at the beginning, Namias tried to solve Schrödinger equations in quantum mechanics using fractional Fourier transform as a tool with little notice in community. However, the fractional Fourier transform has found itself in real physical processes of light propagation in a graded index (GRIN) fiber, which is equivalent to a near field diffraction of light, Fresnel diffraction, with a quadratic factor. Thus the fractional Fourier transform can be easily realized in a bulk optical setup consisting of lenses. The fractional Fourier transform provides various of new mathematical operations which are useful in the field of optical information processing. And because fractional Fourier transform also is a kind of time–frequency joint representation of a signal [9], it has found extensive applications in signal and image processing [10].

The discrete forms of mathematical transforms have been extremely useful in applications, especially in signal processing and image manipulations. In fact, discrete transforms can approximate their continuous versions with high precision, meanwhile with high computation speed and lower complexities. Needless to say, Discrete Fourier transform (or FFT) and discrete wavelet transform have been widely used in different kinds of applications. Recently, discrete fractional Fourier transform (DFrFT) and the relevant discrete fractional cosine transform (DFrCT) have been proposed [11,12]. We have used this fast algorithm of fractional Fourier transform in the numerical simulations of image encryption and optical security [13,14].

As we have demonstrated that the extension of fractional Fourier transform have many different kinds of definitions according to how we fractionalize the Fourier transform [15], the DFrFT may also have different kinds of versions. In our researches of optical image encryption, we ask naturally the question, is there any possibility that the DFrFT be random? We have been motivated in searching such a random transform because then the image encryption process could be simplified by a single step of transform. Recently we found that, from the generalization of DFrFT, we can construct a discrete fractional random transform (DFRNT) with an inherent randomness. We demonstrate that such DFRNT has excellent mathematical properties as the fractional Fourier transforms have. And moreover it has some fantastic features of its own. We have also demonstrated that the DFRNT is a very efficient tool in digital image encryption and decryption with a very high speed of computation. The open questions left are concerning with the physical analogies of DFRNT and its further applications, which we are considering now.

We discuss the mathematical definition and properties of DFRNT and provide numerical simulation results of the DFRNT's for one-dimensional and two-dimensional signals in the following sections in details.

2. Mathematics of the discrete fractional random transform

We begin our discussions from the definition of DFrFT proposed by Pei et al. [11]. A one-dimensional DFrFT can be expressed as a matrix–vector multiplication

$$\mathbf{X}_{\alpha}(n) = \mathbf{F}^{\alpha}\mathbf{x}(n), \tag{1}$$

where $\mathbf{x}(n)$ is the input vector which has N elements, $\mathbf{F}^{\alpha}$ is the kernel transform matrix and α is the fractional order. When $\alpha = 1$, the DFrFT becomes the DFT as $\mathbf{X}(n) = \mathbf{F}\mathbf{x}(n)$, with matrix $\mathbf{F}$ indicating the kernel matrix of DFT.

The transform matrix is defined as follows. Firstly, because the fractional Fourier transform has the same eigenfunctions with the Fourier transform, we can calculate the eigenvectors $\{\mathbf{V}_j\}$ $(j = 1, 2, \ldots, N)$ of DFrFT with a real transform matrix $\mathbf{S}$ of discrete Fourier transform which is defined as follows [16]where $\omega = 2\pi/N$. The matrix $\mathbf{S}$ actually is not the kernel transform matrix $\mathbf{F}$ of the discrete Fourier transform (DFT). However, the matrix $\mathbf{S}$ commutes with matrix $\mathbf{F}$, i.e. $\mathbf{SF} = \mathbf{FS}$. Thus the eigenvectors of $\mathbf{S}$ are also the eigenvectors of $\mathbf{F}$, only they correspond to different eigenvalues. Because the matrix $\mathbf{S}$ is symmetrical, the eigenvectors $\{\mathbf{V}_j\}$ are all real and orthonormal to