Optics & Laser Technology 64 (2014) 82–93

Contents lists available at ScienceDirect

Optics & Laser Technology

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

New fractional matrix with its applications in image encryption

Feng Zhang *, Yang Hu, Ran Tao, Yue Wang

Department of Electronic Engineering, 5 South Zhongguancun Street, Haidian District, Beijing Institute of Technology, Beijing 100081, China

A R T I C L E I N F O

Article history:
Received 15 December 2013
Received in revised form
5 March 2014
Accepted 19 March 2014

Keywords:
Time–frequency analysis
Eigendecomposition
Discrete Fourier transform
Discrete fractional Fourier transform
Fractional-order matrix

A B S T R A C T

In this paper, new fractional matrix generation by using different the periodic matrix sequences are considered. For a periodic matrix with period P, its integer forms and fractional forms can constitute different periodic matrix sequences. The series of the periodic matrix sequence can be used to compute and construct different fractional matrices, which is depended on the relationship between the period and the size of the periodic matrix sequence. The proposed fractional matrix generation method is general and can be used to any periodic matrices. Then, we extend the new fractional matrices to multi-order forms, which can be used in image encryption. Simulation results and the application example in image encryption using the obtained new fractional matrix are also presented.

1. Introduction

As the generalization of a conventional Fourier transform, the fractional Fourier transform (FRFT) was originally introduced in 1980 by Namias as a mathematical tool for solving theoretical physical problems [1], but did not gain much attention until its reintroduction to optics in 1993 by Mendlovic and Ozaktas [2–4] and Lohmann [5]. Since then a lot of work has been done on its properties and optics implementations [6–9], and it has been widely studied and advances into application areas, such as beam shaping, signal processing and image processing [10–19].

Due to the fact that the FRFT is a useful tool in solving problems in the above areas, the discrete FRFT (DFRFT) has become an important issue recently. In [20], Pei et al. defined the DFRFT based on the eigendecomposition of the DFT matrix **F** where the eigenvectors are Hermite–Gaussian-like functions. In [21], Candan et al. consolidated and provided discussions on this definition of the DFRFT. In [22–24], Hanna et al. considered the generation of Hermite–Gaussian-like eigenvectors of **F** using the singular value decomposition and direct batch evaluation to obtain the DFRFT. Other **F**-commuting matrices whose eigenvectors are better approximate the continuous Hermite–Gaussian functions are introduced in [25–28]. In [29], Yeh and Pei developed a novel method to compute the DFRFT, by which the DFRFT of any order (angle) can be computed by a linear combination of the DFRFTs with special orders. Following Yeh and Pei's work, we have investigated properties and generalized aspects about a linear summation of fractional matrices [30].

In fact, the linear summation of a fractional matrix sequence implies a construction method for new fractional matrices. In this paper, we explore this method systematically and obtain some interesting properties of the periodic matrix sequence. We firstly present the physical meaning of the rotational angle for fractional matrices. Then, we derive some new fractional matrices by the series of different periodic matrix sequences, including some typical periodic matrices used in signal processing. Some simulations of new fractional matrices and an application of image encryption using these new fractional matrices are presented.

2. Preliminaries

2.1. The continuous FRFT

The continuous FRFT of a signal $x(t)$ with angle α is defined as [8,9]

$$X_\alpha(u) = \sqrt{1-j\cot\alpha} \times \int_{-\infty}^{\infty} x(t) e^{j\pi(t^2+u^2)\cot\alpha - j2\pi ut\csc\alpha} dt. \tag{1}$$

The transform angle $\alpha = \mathbf{a} \times \pi/2$ indicates the rotation angle in the time–frequency plane. Obviously, the FRFT reduces to the identity transform and the conventional Fourier transform (FT) for $\alpha = 0$ and $\alpha = \pi/2$, respectively. The fundamental property of the FRFT is the angle additivity property, i.e., two successive FRFTs with angles α and η is another FRFT with angle $\alpha+\eta$, and consequently the inverse FRFT is given by the FRFT with angle $-\alpha$.

* Corresponding author. Tel.: +86 10 68916130.
E-mail address: oUo@bit.edu.cn (F. Zhang).

http://dx.doi.org/10.1016/j.optlastec.2014.03.020

2.2. The definition of DFRFT

The ath-order $\mathbf{N} \times \mathbf{N}$ DFRFT kernel defined through the eigendecomposition method is [20,21]

$$\mathbf{F^a} = \mathbf{VD^aV}^T = \sum_{\mathbf{k}=0}^{\mathbf{N}-2} e^{-j\frac{\pi}{2}\mathbf{ka}}\mathbf{v_k}\mathbf{v_k}^T + e^{-j\frac{\pi}{2}\mathbf{Ma}}\mathbf{v_k}\mathbf{v_k}^T \tag{2}$$

where $\mathbf{V} = [\mathbf{v}_0|\mathbf{v}_1|\cdots\mathbf{v}_{\mathbf{N}-2}|\mathbf{v}_{\mathbf{N}-1}]$, $\mathbf{M} = \mathbf{N}-1$ when N is odd and $\mathbf{V} = [\mathbf{v}_0|\mathbf{v}_1|\cdots\mathbf{v}_{\mathbf{N}-2}|\mathbf{v}_{\mathbf{N}}]$, $\mathbf{M} = \mathbf{N}$ when N is even, and $\mathbf{v_k}$ is the kth Hermite–Gaussian-like eigenvector. $\mathbf{D}^a$ is a diagonal matrix with diagonal entries corresponding to the eigenvalues for column eigenvectors in matrix $\mathbf{V}$.

2.3. Linear summation of fractional matrices

When we compute the DFRFT based on the eigendecomposition method, the transform kernel needs to be recomputed while the transform order is changed. This computation cost is very large in practical situation of the DFRFT computation with multiple orders such as signal detection and estimation, noise filtering, and pattern recognition. In [29], a new computation method for the eigendecomposition-based DFRFT is developed. The ath-order $N \times N$ DFRFT matrix $\mathbf{F}^a$ can be computed as $\mathbf{F}^a = \sum_{n=0}^{N-1} B_{n,a}\mathbf{F}^{nb}$ where $b = 4/N$. The weighting coefficients are computed as $B_{n,a} = (1/N)(1-e^{j\times N\times(\pi/2)(nb-a)})/(1-e^{j\times(\pi/2)(nb-a)})$. With this method, the DFRFT of any order can be computed by a linear combination of the DFRFTs with special orders.

In fact, this computation method for the DFRFT implies the idea of linear summation of multiple fractional matrices. Note that the sizes and the periods of these matrices are equal. In [30], the linear summation of fractional matrices is generated to any diagonalizable periodic matrix.

Proposition 1. Assume that $\mathbf{L}$ is a $\mathbf{N} \times \mathbf{N}$ periodic matrix satisfying $\mathbf{L}^P = \mathbf{I}$ and its diagonalized form is $\mathbf{L} = \mathbf{VDV}^H$. Then, the matrix $\mathbf{L}^a = \mathbf{VD}^a\mathbf{V}^H$ and the matrix $\mathbf{L}_S^a = \sum_{n=0}^{P-1} C_{n,a}\mathbf{L}^n$ are equal when $\mathbf{N} = \mathbf{P}$, where the coefficients are given by $\mathbf{C_{n,a}} = (1/\mathbf{P})(1-\mathbf{e}^{\mathbf{j}2\pi(\mathbf{n}-\mathbf{a})})/(1-\mathbf{e}^{\mathbf{j}(2\pi/\mathbf{P})(\mathbf{n}-\mathbf{a})})$.

Proposition 2. Assume that $\mathbf{L}$ is a $\mathbf{N} \times \mathbf{N}$ periodic matrix satisfying $\mathbf{L}^P = \mathbf{I}$ and its diagonalized form is $\mathbf{L} = \mathbf{VDV}^H$. Let $b = P/N$ and $\mathbf{K} = \mathbf{L}^b = \mathbf{L}^{P/N} = \mathbf{VD}^{P/N}\mathbf{V}^H$. Then, $\mathbf{L}^a$ can be expressed as $\mathbf{L}^a = \mathbf{K}_S^{a/b} = \sum_{n=0}^{N-1} C_{n,a/b}\mathbf{K}^n$.

Proofs of Propositions 1 and 2 can be referred in [30].

In Proposition 1, the size and the period of the periodic matrix $\mathbf{L}$ are equal, i.e., $\mathbf{N} = \mathbf{P}$. In this case we can use the linear summation $\sum_{n=0}^{P-1} C_{n,a}\mathbf{L}^n$ to compute $\mathbf{L}^a$. Specially, for any vector $\mathbf{x}$ whose length is 4, we have $\mathbf{F}^a\mathbf{x} = \sum_{n=0}^{3} C_{n,a}\mathbf{F}^n\mathbf{x}$. For the case that $\mathbf{N} \neq \mathbf{P}$, we denote the matrix $\mathbf{K} = \mathbf{L}^{P/N} = \mathbf{VD}^{P/N}\mathbf{V}^H$ as is shown in Proposition 2. Then we have $\mathbf{K}^N = \mathbf{I}$ which has the property that the size and the period of the constructed matrix $\mathbf{K} = \mathbf{L}^{P/N}$ are equal. Therefore, we can compute $\mathbf{L}^a$ as $\sum_{n=0}^{N-1} C_{n,a/b}\mathbf{K}^n$.

3. New fractional matrix generation by periodic matrix sequences and its applications in image encryption

3.1. Order and angle parameters representation for fractional periodic matrices in the time–frequency plane

The Fourier transform of a signal can be viewed as a counterclockwise rotation by an angle of $\pi/2$ in the time–frequency plane, and the FRFT corresponds to a rotation by an angle α [8,9]. Similar to the continuous case, the DFT and the DFRFT can be regarded as a $\pi/2$ and an α rotation for the discrete signal, respectively. Therefore, the DFT matrix $\mathbf{F}$ and the DFRFT matrix $\mathbf{F^a}$ can be described both by their orders and rotational angles equivalently, where the rotation angle α and the order a of the transform matrix have a relation $\alpha = \mathbf{a} \times \pi/2$.

For the FRFT, it has the following important properties: (1) marginal property, i.e., reduction to the FT and identity operator when $a = 1$ and $a = 0$, respectively; (2) additivity property, i.e., $\mathbf{F}^a\mathbf{F}^b = \mathbf{F}^{a+b}$. Moreover, the Wigner distribution of the FRFTed signal with angle $\alpha = \mathbf{a} \times \pi/2$ is a counterclockwise rotated version of the Wigner distribution of the original signal by the same angle in the time–frequency plane. That is $W_{X_\alpha}(t,f) = W_x(t\cos\alpha - f\sin\alpha, t\sin\alpha + f\cos\alpha)$ where $W_{X_\alpha}(t,f)$ and $W_x(t,f)$ denotes the Wigner distributions of the FRFTed signal X_α and the original signal x, respectively. These important properties confirm the view of the FRFT as a rotation of the signal in the time–frequency plane.

Besides the DFRFT, fractional version of other signal transforms based on eigendecomposition method and these applications are proposed and discussed, such as the discrete cosine transform (DCT), the discrete sine transform (DST), and the discrete Hartley transform (DHT) [31–36]. Unlike the FRFT, these fractional transforms cannot be viewed as the rotation of the signal in the time–frequency plane. However, since these fractional transforms satisfy the additivity property and marginal property, these fractional transforms are viewed as the "fractional" versions of the original transforms and use the order a or angle α as the transform parameter. Similarly, for a periodic matrix $\mathbf{L}$ we also use its order a or angle α as the transform parameter, though it cannot be considered as a rotation with angle α in the time–frequency plane. Note that the DFT matrix $\mathbf{F}$ is a periodic matrix with period 4. In order to make the DFT matrix $\mathbf{F}$ as a special case for the transform matrix with period 4, we use an angle of $2\pi/\mathbf{P}$ to denote the transform parameter for a periodic transform matrix $\mathbf{L}$ with period P. Then we denote the matrix $\mathbf{L}$ in the time–frequency plane according to its angle parameters α.

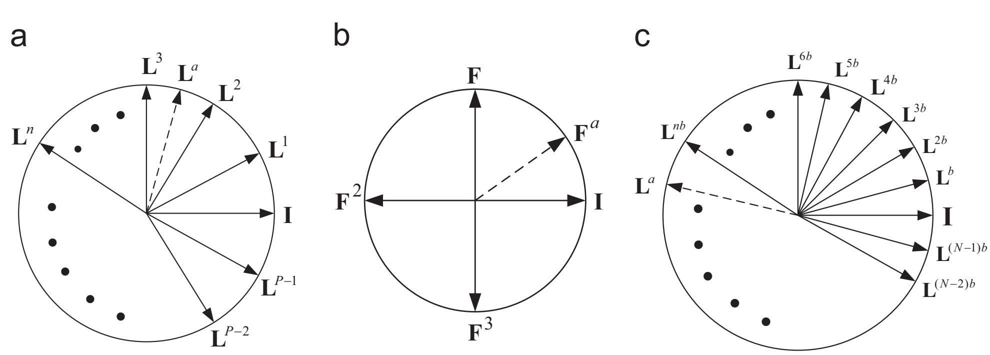

Fig. 1. (a) Denotation of $\mathbf{L^n}$, (b) $\mathbf{F^n}$ with size 4×4, and (c) $\mathbf{K}^n$ with angle parameters.