Optik 165 (2018) 388–394

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Short note

A unified approach for defining random discrete fractional transforms

Juliano B. Lima*, José R. Oliveira Neto, Ravi B.D. Figueiredo

Department of Electronics and Systems, Federal University of Pernambuco, 50740-550 Recife, PE, Brazil

ARTICLE INFO

Article history:
Received 22 February 2018
Accepted 27 March 2018

Keywords:
Discrete fractional transforms
Eigenvectors
Generating matrices
Image encryption

ABSTRACT

In this paper, we introduce a systematic procedure for defining random discrete fractional transforms of Fourier, Hartley, cosine and sine types. The procedure is based on an extension of the generating matrix method for constructing eigenvectors of such transforms. We give multiorder reality-preserving versions of the referred transforms, characterizing them with respect to the number of free parameters and illustrating their applicability in image encryption.

1. Introduction

Discrete transforms are mathematical tools applicable in several practical scenarios. In general, the N-point discrete transform of a sequence $\mathbf{x}$ can expressed as

$$\boldsymbol{X} = \boldsymbol{M}\mathrm{x}, \tag{1}$$

where $\mathbf{M}$ is a $N \times N$ matrix whose entries depend on the type of transform being considered; $\mathbf{M}$ may be related to discrete Fourier, cosine, sine or Hartley transform, for example. If $\mathbf{M}$ is diagonalizable (this is the case of the transforms we just mentioned), its ath power can be obtained as

$$\mathbf{M}^a = \mathbf{V}\boldsymbol{\Lambda}^a\mathbf{V}^T, \quad a \in \mathbb{R}, \tag{2}$$

where $\mathbf{V}$ is a matrix whose columns form an orthonormal set $\{\mathbf{v}_m\}$, $m = 0, 1, \ldots, N-1$, of eigenvectors of $\mathbf{M}$ and $\boldsymbol{\Lambda}$ is a diagonal matrix whose entries are the corresponding eigenvalues; $\mathbf{M}^a$ is the matrix of the fractional version of the transform being considered.

In the last decades, discrete fractional transforms have been widely investigated and employed in a range of applications in the fields of signal processing, optics, communications and information security, for instance (see [1] and references therein). There is a particular interest in discrete fractional transforms whose definition uses randomly constructed eigenvectors as columns of $\mathbf{V}$ in (2) [2,3]; such a construction usually requires the choice of multiple parameters, making the respective fractional transform suitable for cryptography [4].

* Corresponding author.
E-mail addresses: juliano_bandeira@ieee.org (J.B. Lima), joserodrigues.oliveiraneto@ufpe.br (J.R. Oliveira Neto), ravi.bdf@gmail.com (R.B.D. Figueiredo).

https://doi.org/10.1016/j.ijleo.2018.03.116
0030-4026/

Table 1
Multiplicities of eigenvalues of the discrete Fourier transform matrix.

N	$\#\{1\}$	$\#\{-i\}$	$\#\{-1\}$	$\#\{i\}$
$4m$	$m+1$	m	m	$m-1$
$4m+1$	$m+1$	m	m	m
$4m+2$	$m+1$	m	$m+1$	m
$4m+3$	$m+1$	$m+1$	$m+1$	m

Table 2
Multiplicities of eigenvalues of discrete trigonometric transform matrices.

N	DHT		DCT/DST	
	$\#\{1\}$	$\#\{-1\}$	$\#\{1\}$	$\#\{-1\}$
$4m$	$2m+1$	$2m-1$	$2m$	$2m$
$4m+1$	$2m+1$	$2m$	$2m+1$	$2m$
$4m+2$	$2m+1$	$2m+1$	$2m+1$	$2m+1$
$4m+3$	$2m+2$	$2m+2$	$2m+2$	$2m+1$

Among the techniques for systematically constructing the referred eigenvectors, we highlight the one based on generating matrices [5]. In such a method, it is shown that, if $\mathbf{v}$ is an eigenvector of the discrete Fourier transform (DFT) matrix $\mathbf{F}$ with eigenvalue λ, the vector $\mathbf{v}' = \mathbf{S}_A\mathbf{v}$, where

$$\mathrm{S_A} = \alpha^{1/2}\boldsymbol{F}^{-1}\boldsymbol{A}\mathrm{F} + \boldsymbol{A}$$

and $\mathbf{A}$ satisfies $\mathbf{F}^2\mathbf{A}\mathbf{F}^2 = \alpha\mathbf{A}$, is an eigenvector of $\mathbf{F}$ with eigenvalue $\lambda' = \alpha^{1/2}\lambda$; $\mathbf{S}_A$ is identified as a generating matrix. In this paper, we extend this result to discrete trigonometric transforms (DTT), which refers to discrete cosine transforms (DCT) and discrete sine transforms (DST) of types I and IV, and to discrete Hartley transform (DHT). We then propose a unified methodology to construct random eigenbases used in the fractionalization of such transforms. Moreover, we explain how to construct real-valued random fractional DTT and DFT for any N and provide some illustrative results regarding the use of such transforms in image encryption. We demonstrate that the number of free parameters involved in the proposed construction is greater than that provided by other approaches; this is relevant for the mentioned application scenario.

2. Generating eigenbases of discrete transforms

The eigenstructures of discrete transform matrices have been widely investigated [6–9]. It is a well-known fact, for example, that the only eigenvalues of $\mathbf{F}$ are $(-i)^k$, for $k = 0, \ldots, 3$ and $i = \sqrt{-1}$; given an even-symmetric vector $\mathbf{e}$ (resp. odd-symmetric vector $\mathbf{o}$), one constructs the eigenvector $\mathbf{e} \pm \mathbf{Fe}$ (resp. $\mathbf{o} \mp i\mathbf{Fo}$) related to the eigenvalues ± 1 (resp. $\pm i$) [6]. On the other hand, the only eigenvalues of any DTT matrix are $(-1)^k$, $k = 1, 2$ [7–9]. The multiplicity of any of these eigenvalues is known and has some peculiarities depending on N. If $N = 4n$, for example, the multiplicities of eigenvalues 1 and -1 of the discrete Hartley transform matrix are respectively $2n+1$ and $2n-1$. In our text, we denote the multiplicity of the eigenvalue λ by $\#\{\lambda\}$. See Tables 1 and 2 for details.

An eigenvector of a DTT matrix $\mathbf{T}$ can be obtained from an arbitrary vector according to the following proposition.

Proposition 1. *Let* $\mathbf{u}$ *be an arbitrary vector. The vector* $\mathbf{v} = \mathbf{u} \pm \mathbf{Tu}$ *is an eigenvector of* $\mathbf{T}$ *with eigenvalue* $\lambda = \pm 1$.

Proof. The DTT considered in this paper are all involutions, that is $\mathbf{T}^2 = \mathbf{I}$. Therefore, one has

$$\boldsymbol{T}\mathrm{v} = \boldsymbol{T}(\boldsymbol{u} \pm \boldsymbol{T}\mathrm{u}) = \boldsymbol{T}\mathrm{u} \pm \boldsymbol{T}^2\boldsymbol{u} = \pm\boldsymbol{u} + \boldsymbol{T}\mathrm{u} = \pm\boldsymbol{v}.$$

Proposition 2. *Let* $\mathbf{A}$ *be a* $N \times N$ *matrix and* $\mathbf{v}$ *a* N*-point eigenvector of the DTT matrix* $\mathbf{T}$ *with eigenvalue* λ. *Therefore* $\mathbf{v}' = \mathbf{S}_A\mathbf{v}$, *where* $\mathbf{S}_A = \pm\mathbf{TAT} + \mathbf{A}$, *is an eigenvector of* $\mathbf{T}$ *with eigenvalue* $\lambda' = \pm\lambda$.

Proof

$$\begin{aligned}\boldsymbol{T}\boldsymbol{v}' &= \mathrm{TS_A}\mathrm{v} = \boldsymbol{T}(\pm\boldsymbol{T}\mathrm{AT} + \boldsymbol{A})\boldsymbol{v} = \pm\boldsymbol{A}\boldsymbol{T}\boldsymbol{v} + \boldsymbol{T}\boldsymbol{A}\boldsymbol{v}\\ &= \pm\boldsymbol{A}\lambda\boldsymbol{v} + \boldsymbol{T}\boldsymbol{A}\boldsymbol{T}^2\boldsymbol{v} = \pm\boldsymbol{A}\lambda\boldsymbol{v} + \boldsymbol{T}\boldsymbol{A}\boldsymbol{T}\lambda\boldsymbol{v}\\ &= \pm\lambda(\pm\boldsymbol{T}\mathrm{AT} + \boldsymbol{A})\boldsymbol{v} = \pm\lambda\mathrm{S_A}\mathrm{v} = \pm\lambda\boldsymbol{v}'.\end{aligned}$$

Remark: a less general version of Proposition 2 was introduced in [10]. In that paper, one considers cosine and sine transforms only and presents an eigenbases construction method not extensible to other transform types.

The generating matrix method can be recursively applied to obtain a set of eigenvectors of a given transform. We exploit this possibility in our approach, which requires constructing, for each eigenvalue, one *seed* eigenvector and one generating matrix. Since we are interested the referred set to be an orthonormal basis, we have to verify its linear independence and