Matrizes Geradoras de Autovetores para Construção de Transformadas de Hartley Fracionárias

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

***Resumo*— Neste artigo, propõe-se um método baseado em matrizes geradoras para construir autovetores da transformada discreta de Hartley (DHT). Os conjuntos de autovetores obtidos são caracterizados e empregados na definição de uma DHT fracionária (DFrHT). Uma versão real e multiordem da DFrHT é então apresentada; como o número de parâmetros livres dessa transformada é maior que o das transformadas de Fourier correspondentes, seu uso em cifragem de imagens pode prover vantagens relacionadas à robustez contra certos ataques criptográficos. Uma avaliação preliminar de tal possibilidade é realizada na parte final do trabalho.**

***Palavras-Chave*— transformada discreta de Hartley, matrizes geradoras, autovetores, transformadas fracionárias.**

***Abstract*— In this paper, we propose a method based on generating matrices for constructing eigenvectors of the discrete Hartley transform (DHT). The obtained eigenvector sets are characterized and employed in the definition of a fractional DHT (DFrHT). A real-valued version of the DFrHT is then presented; since the number of free parameters of such a transform is greater than that of the corresponding Fourier transforms, its usage in image encryption may provide advantages related to the robustness against certain cryptographic attacks. A preliminary evaluation regarding this possibility is performed in the final part of this work.**

***Keywords*— discrete Hartley transform, generating matrices, eigenvectors, fractional transforms.**

I. Introdução

Transformadas discretas são ferramentas matemáticas essenciais em diversos cenários de aplicação e, em particular, no campo de processamento digital de sinais [1]. Em geral, uma transformada discreta $\mathbf{X}$, de uma sequência $\mathbf{x}$ com N pontos, pode ser calculada de acordo com

$$\mathbf{X} = \mathbf{T}\,\mathbf{x}, \tag{1}$$

em que $\mathbf{T}$, identificada como matriz de transformação, tem suas entradas dependentes do núcleo da transformada correspondente.

Autoestruturas de matrizes de transformação têm sido extensivamente estudadas [2], [3]. Mais especificamente, a construção de bases formadas por autovetores de uma transformada é um ponto-chave no seu processo de fracionarização. Se $\mathbf{T}$ for diagonalizável, pode-se escrever

$$\mathbf{T} = \mathbf{V}\mathbf{\Lambda}\mathbf{V}^T, \tag{2}$$

em que $\mathbf{V}$ é uma matriz cujas colunas constituem um conjunto ortonormal de autovetores de $\mathbf{T}$, $\mathbf{\Lambda}$ é uma matriz diagonal cujas entradas são os autovalores correspondentes e $\mathbf{V}^T$ denota a transposta de $\mathbf{V}$. O respectivo operador fracionário é dado por

$$\mathbf{T}^a = \mathbf{V}\mathbf{\Lambda}^a\mathbf{V}^T, \tag{3}$$

em que $a \in \mathbb{R}$ é a ordem fracionária. Devido a este parâmetro, transformadas fracionárias podem ser vistas como generalizações das transformadas ordinárias correspondentes e podem ser aplicadas numa extensa gama de cenários práticos [3], [4]. Apenas para mencionar alguns exemplos, transformadas fracionárias podem ser empregadas em cifragem e extração de características de imagens, reconstrução e filtragem de sinais, comunicação subaquática, classificação de distúrbios em sistemas de potência etc. [5]–[10].

Se $\mathbf{T}$ for a matriz da transformada discreta de Fourier (DFT, do inglês *discrete Fourier transform*), propriedades específicas relacionadas aos autovetores usados em sua diagonalização podem ser desejáveis. Pode-se construir, por exemplo, autovetores da DFT cujas componentes aproximem numericamente amostras das funções Hermite-Gaussianas contínuas. Neste caso, a DFT fracionária obtida aproximaria a transformada fracionária de Fourier contínua. Usualmente, a construção dos referidos autovetores é realizada empregando métodos baseados em matrizes que comutam com a matriz da DFT [4].

Em [11], uma nova técnica para obter autovetores da DFT foi introduzida. Tal procedimento requer uma matriz $\mathbf{A}$ que satisfaça

$$\mathbf{F}^2\mathbf{A}\mathbf{F}^2 = \lambda\mathbf{A}, \tag{4}$$

em que $\mathbf{F}$ é a matriz da DFT e λ é uma constante; $\mathbf{A}$ é então usada para construir a matriz geradora

$$\mathbf{S}_\mathbf{A} = \lambda^{\frac{1}{2}}\mathbf{F}^{-1}\mathbf{A}\mathbf{F} + \mathbf{A}. \tag{5}$$

Se $\mathbf{v}_\mathbf{F}$ for um autovetor de $\mathbf{F}$ com autovalor $\lambda_\mathbf{F}$, então $\mathbf{S}_\mathbf{A}\mathbf{v}_\mathbf{F}$ será um autovetor de $\mathbf{F}$ com autovalor $\lambda^{\frac{1}{2}}\lambda_\mathbf{F}$. Enquanto métodos baseados em matrizes comutantes normalmente requerem $\mathcal{O}(N^3)$ operações aritméticas para obter N autovetores, a abordagem baseada em matrizes geradoras requer $\mathcal{O}(N^2 \log N)$.

Neste artigo, estende-se o método descrito acima, introduzindo matrizes para geração de autovetores da transformada discreta de Hartley (DHT, do inglês *discrete Hartley transform*) [12]. Conforme se demonstra ao longo do trabalho, a referida extensão envolve matrizes com um número maior de parâmetros livres, quando comparadas a matrizes $\mathbf{A}$ que satisfaçam (4). Dessa forma, conjuntos de autovetores gerados segundo a metodologia proposta podem ser empregados na obtenção de versões fracionárias da DHT, as quais, por sua vez, são propícias a aplicações relacionadas à Criptografia.

Ravi B. D. Figueiredo, Juliano B. Lima e José R. de Oliveira Neto. Departamento de Eletrônica e Sistemas, Universidade Federal de Pernambuco, Recife-PE, Brasil, E-mails: ravibdf@gmail.com, juliano_bandeira@ieee.org, joserodrigues.oliveiraneto@ufpe.br.

Na próxima seção, os principais resultados relacionados a autoestrutura da DHT são brevemente revisados. Na Seção III, descreve-se a abordagem proposta, caracterizando os autovetores obtidos e explicando como eles podem ser usados na fracionarização da DHT. Na Seção IV, usa-se a teoria desenvolvida para definir DHT fracionárias com múltiplas ordens; é feita, então, uma prévia da aplicação de tais transformadas ao cenário de cifragem de imagens. O trabalho é concluído com a exposição de considerações finais na Seção V.

II. Autoestrutura da Transformadas Discreta de Hartley

A matriz $\mathbf{H}$, da transformada discreta de Hartley, tem sua componente na k-ésima linha e na n-ésima coluna dada por

$$H_{k,n} = \frac{1}{\sqrt{N}}\text{cas}\left(\frac{2\pi}{N}kn\right), k, n = 0, 1, \ldots, N-1, \quad (6)$$

em que $\text{cas}(\cdot) = \cos(\cdot) + \text{sen}(\cdot)$. Essa transformada corresponde a uma involução, isto é, a expressão para o cálculo da DHT inversa é a mesma usada no cálculo da transformada direta. Equivalentemente, tem-se que $\mathbf{H}^{-1} = \mathbf{H}$ e $\mathbf{H}^2 = \mathbf{I}$, em que $\mathbf{I}$ é a matriz identidade. Isso permite deduzir que os autovalores de $\mathbf{H}$ são, possivelmente, $\lambda = \pm 1$. Na Tabela I, as multiplicidades $\#\{\cdot\}$ desses autovalores são apresentadas [12].

Outro resultado importante, o qual é enunciado a seguir, diz respeito à construção de autovetores associados a um autovalor específico da DHT.

Proposição 1: Seja $\mathbf{v}$ um vetor arbitrário com N pontos. Então, o vetor $\mathbf{v}^+ = \mathbf{v} + \mathbf{Hv}$ e o vetor $\mathbf{v}^- = \mathbf{v} - \mathbf{Hv}$ são, respectivamente, autovetores da matriz da DHT com os autovalores $\lambda^+ = 1$ e $\lambda^- = -1$.

Demonstração: Considerando que $\mathbf{H}^2 = \mathbf{I}$, tem-se o seguinte desenvolvimento:

$$\mathbf{Hv}^+ = \mathbf{H}(\mathbf{v} + \mathbf{Hv}) = \mathbf{Hv} + \mathbf{H}^2\mathbf{v} = \mathbf{v} + \mathbf{Hv} = \mathbf{v}^+.$$

Um desenvolvimento análogo pode ser obtido para $\mathbf{v}^-$. ■

III. Matrizes Geradoras de Autovetores da DHT

Nesta seção, são introduzidas matrizes geradoras de autovetores da matriz $\mathbf{H}$ da DHT; é descrito um procedimento sistemático para construir conjuntos desses autovetores que constituam, possivelmente, uma base para $\mathbb{R}^N$. O principal resultado nesse contexto é dado pela proposição a seguir.

Proposição 2: Seja $\mathbf{H}$ a matriz $N \times N$ de uma DHT, $\mathbf{A}$ uma matriz $N \times N$ arbitrária e $\mathbf{v}$ um autovetor de $\mathbf{H}$ com autovalor λ. Portanto $\mathbf{v}' = \mathbf{S_A v}$, em que $\mathbf{S_A}$ é e matriz geradora

$$\mathbf{S_A} = \pm\mathbf{HAH} + \mathbf{A}, \quad (7)$$

é um autovetor de $\mathbf{H}$ com autovalor $\lambda' = \pm\lambda$.

TABELA I: Multiplicidades dos autovalores da DHT.

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

Demonstração: Multiplicando $\mathbf{H}$ e $\mathbf{v}'$, obtém-se o seguinte desenvolvimento:

$$\begin{aligned}\mathbf{Hv}' &= \mathbf{HS_A v} = \mathbf{H}(\pm\mathbf{HAH} + \mathbf{A})\mathbf{v} = \\ &= \pm\mathbf{AHv} + \mathbf{HAv} = \pm\mathbf{A}\lambda\mathbf{v} + \mathbf{HAH}^2\mathbf{v} = \\ &= \pm\mathbf{A}\lambda\mathbf{v} + \mathbf{HAH}\lambda\mathbf{v} = \pm\lambda(\pm\mathbf{HAH} + \mathbf{A})\mathbf{v} \\ &= \pm\lambda\mathbf{S_A v} = \pm\lambda\mathbf{v}'.\end{aligned}$$

■

Ao passo em que a matriz $\mathbf{A}$ na Proposição 2 tem N^2 componentes livres, é possível mostrar que uma matriz $\mathbf{A}$ que satisfaça (4) e que, assim, possa originar uma matriz geradora de autovetores da DFT, tem $N^2/4$ componentes livres. Tal diferença, que fora observada anteriormente, desempenha um papel importante no cenário de aplicação descrito na Seção IV.

Usando a Proposição 2, pode-se construir um conjunto com N autovetores $\{\mathbf{v}_r\}_{r=0,1,\ldots,N-1}$ de $\mathbf{H}$ escolhendo uma matriz $\mathbf{A}$, um autovetor de partida $\mathbf{v}_0$ e calculando, para $r = 1, 2, \ldots, N-1$,

$$\mathbf{v}_r = \mathbf{S_A v}_{r-1}. \quad (8)$$

Se desejarmos que o referido conjunto de autovetores seja linearmente independente (LI) e, consequentemente, uma base para $\mathbb{R}^N$, aspectos adicionais precisam ser considerados; em particular, a seguinte condição deve ser observada.

Proposição 3: Se o conjunto $\{\mathbf{v}_r\}_{r=0,1,\ldots,N-1}$ for linearmente independente, então o polinômio mínimo de $\mathbf{S_A}$ possui grau N.

Demonstração: O conjunto $\{\mathbf{v}_r\}_{r=0,1,\ldots,N-1}$ é linearmente independente se, e somente se

$$\begin{aligned}c_0\mathbf{v}_0 + c_1\mathbf{v}_1 + \cdots + c_{N-1}\mathbf{v}_{N-1} &= \mathbf{0} \\ c_0\mathbf{v}_0 + c_1\mathbf{S_A v}_0 + \cdots + c_{N-1}\mathbf{S_A}^{N-1}\mathbf{v}_0 &= \mathbf{0} \\ c_0\mathbf{I} + c_1\mathbf{S_A} + \cdots + c_{N-1}\mathbf{S_A}^{N-1} &= \mathbf{0}\end{aligned}$$

requer $c_r = 0$, $r = 0, 1, \ldots, N-1$. Tal requisito, aplicado à última igualdade, implica que o grau mínimo de um polinômio que possua $\mathbf{S_A}$ como raiz é N. ■

Como a condição dada na Proposição 3 é necessária, mas não suficiente, ainda que ela seja satisfeita por uma matriz $\mathbf{S_A}$, deve-se verificar se o conjunto de autovetores correspondente é LI. Adicionalmente, deve-se considerar uma particularidade da autoestrutura de $\mathbf{H}$ quando $N = 4m$: a diferença entre as multiplicidades de $\lambda^+ = 1$ e $\lambda^- = -1$ é igual a 2 (vide Tabela I). Assim, seria impossível obter um conjunto LI com N autovetores de $\mathbf{H}$ usando, por exemplo, um autovetor de partida $\mathbf{v}_0$ com o autovalor $\lambda^+ = 1$ e a matriz $\mathbf{S_A} = -\mathbf{HAH} + \mathbf{A}$ para gerar, conforme (8), autovetores associados a $\lambda^- = -1$ e a $\lambda^+ = 1$ de forma alternada; além de $\mathbf{v}_0$, outros N autovetores precisariam ser gerados, a fim de totalizar $2m+1$ autovetores com $\lambda^+ = 1$ e $2m-1$ autovetores com $\lambda^- = -1$ (o autovetor $\mathbf{v}_{N-1}$, relacionado a $\lambda^- = -1$ seria descartado). Obviamente, o conjunto resultante seria linearmente dependente. Diante disso, propõe-se o seguinte procedimento, por meio do qual é possível gerar uma base ortonormal de $\mathbb{R}^N$ formada por autovetores de $\mathbf{H}$:

1) Construa um vetor arbitrário $\mathbf{v}$ com N pontos;

2) Utilizando a Proposição 1, construa dois autovetores de partida: $\mathbf{v}_0^+$, associado a $\lambda^+ = 1$ e $\mathbf{v}_0^-$, associado a $\lambda^- = -1$.
3) Construa uma matriz $N \times N$ arbitrária $\mathbf{A}$ e obtenha a matriz geradora $\mathbf{S_A} = \mathbf{HAH} + \mathbf{A}$;
4) Obtenha $\mathbf{v}_r^+ = \mathbf{S_A}\mathbf{v}_{r-1}^+$, $r = 1, 2, \ldots, \#\{\lambda^+\} - 1$ e $\mathbf{v}_r^+ = \mathbf{S_A}\mathbf{v}_{r-1}^-$, $r = 1, 2, \ldots, \#\{\lambda^-\} - 1$, e verifique se os conjuntos $\{\mathbf{v}_r^+\}_{r=0,1,\ldots,\#\{\lambda^+\}-1}$ e $\{\mathbf{v}_r^-\}_{r=0,1,\ldots,\#\{\lambda^-\}-1}$ são LI;
5) Se os conjuntos gerados no passo 4) forem LI, faça-os ortogonais por meio da aplicação de algum processo que tenha esta finalidade (o algoritmo de Gram-Schmidt, por exemplo). Denote os vetores dos conjuntos resultantes por $\{\tilde{\mathbf{v}}_r^+\}_{r=0,1,\ldots,\#\{\lambda^+\}-1}$ e $\{\tilde{\mathbf{v}}_r^-\}_{r=0,1,\ldots,\#\{\lambda^-\}-1}$;
6) Forme uma base ortonormal de $\mathbb{R}^N$ unindo, no mesmo conjunto, os vetores obtidos no passo 5).

Observe que alguns dos passos descritos podem ser modificados. No passo 1), por exemplo, dois vetores arbitrários distintos poderiam ser escolhidos; eles seriam usados, no passo 2), para construir cada um dos autovetores de partida; a geração recursiva de cada um dos dois conjuntos de autovetores no passo 4) também poderia ser feita usando matrizes geradoras diferentes, construídas no passo 3). Independentemente disso, o conjunto ortonormal de autovetores resultante pode ser usado na fracionarização de $\mathbf{H}$. Mais especificamente, esses autovetores são dispostos como colunas de $\mathbf{V}$ em

$$\mathbf{H}^a = \mathbf{V}\mathbf{\Lambda}^a\mathbf{V}^T, \tag{9}$$

em que $a \in \mathbb{R}$ é a ordem fracionária e $\mathbf{\Lambda}$ é uma matriz diagonal contendo apenas $\lambda^+ = 1$ e $\lambda^- = -1$ em números condizentes com suas respectivas multiplicidades. Diferentes ordenações podem ser empregadas para dispor esses autovalores ao longo da diagonal de $\mathbf{\Lambda}$; é suficiente que a disposição escolhida coincida com a disposição dos autovetores correspondentes em $\mathbf{V}$. Transformadas fracionárias construídas dessa maneira têm operador matricial inverso dado por $\mathbf{H}^{-a}$. Assim, são satisfeitas propriedades como aditividade de ordens, ou seja, $\mathbf{H}^a\mathbf{H}^b = \mathbf{H}^{a+b}$, redução à DHT ordinária quando $a = 1$ e periodicidade, ou seja, $\mathbf{H}^{a+2t} = \mathbf{H}^a$, $t \in \mathbb{Z}$.

Conforme comentado anteriormente, a construção de uma base ortonormal formada por autovetores de $\mathbf{H}$ e a consequente obtenção de $\mathbf{H}^a$ dependem, basicamente, de três parâmetros: (i) vetor inicial $\mathbf{v}$, (ii) matriz $\mathbf{A}$, a partir da qual se obtém a matriz geradora $\mathbf{S_A}$ e (iii) ordem fracionária a. A flexibilidade na escolha desses parâmetros sugere o uso da DFrHT em cenários relacionados à Criptografia. Na próxima seção, essa possibilidade é investigada de forma preliminar.

IV. DHT Fracionária Multiordem e Aplicação em Cifragem de Imagens

Nas últimas décadas, transformadas fracionárias têm sido amplamente usadas como fundamento de esquemas para cifragem de imagens [6], [13]. Alguns desses esquemas têm implementações ópticas e empregam lentes, moduladores espaciais de luz, sensores etc.; nesses casos, a decifragem requer um sistema óptico complementar dependente de parâmetros derivados de uma chave-secreta. Outros esquemas admitem implementações em *software* e combinam as transformadas com diversas outras estratégias. Com o propósito de ilustrar o uso da DFrHT construída de acordo com o método dado na Seção III, é definida a seguir uma DFrHT multiordem e sugerido um esquema de cifragem baseado nessa transformada.

A. DHT fracionária multiordem

De maneira geral, uma DHT fracionária multiordem é obtida substituindo, em (9), a ordem fracionária escalar a por um vetor $\mathbf{a} = (a_0, a_1, a_2, \ldots, a_{N-1}) \in \mathbb{R}^N$, de modo que se tenha

$$\mathbf{H}^{\mathbf{a}} = \mathbf{V}\mathbf{\Lambda}^{\mathbf{a}}\mathbf{V}^T, \tag{10}$$

em que o elemento na $(n+1)$-ésima linha e na $(n+1)$-ésima coluna de $\mathbf{\Lambda}^{\mathbf{a}}$ é $\Lambda_{n+1,n+1}^{a_n} = \lambda^{a_n}$, $\lambda \in \{-1, +1\}$, $n = 0, 1, \ldots, N-1$.

A questão é que, escrevendo $\lambda^+ = 1 = e^{i2\pi}$ e $\lambda^- = -1 = e^{i\pi}$, tem-se $\lambda^{a_n} = e^{ia_n 2\pi}$ ou $\lambda^{a_n} = e^{ia_n\pi}$, o que resulta num número complexo sempre que a_n for não-inteiro; assim, a matriz $\mathbf{H}^{\mathbf{a}}$ em (10) será, normalmente, complexa, o que é inconveniente para aplicação em cifragem de imagens. Por outro lado, se $\mathbf{H}^{\mathbf{a}}$ for uma matriz com componentes reais, conforme se esclarecerá posteriormente, uma imagem cifrada também com componentes reais será produzida; isso permite uma avaliação mais consistente de aspectos relacionados à robustez do método de cifragem contra ataques criptográficos.

Estratégias para produzir matrizes reais de transformadas fracionárias têm sido investigadas [14]–[16]. Um dos métodos propostos em [16], por exemplo, que é restrito a $N = 4m+1$, emprega, no lugar de $\mathbf{\Lambda}^{\mathbf{a}}$ em (10), a matriz bloco-diagonal

$$\mathbf{\Lambda}^{\mathbf{e},\mathbf{g}} = \begin{bmatrix} \mathbf{E}_1 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \ddots & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{E}_m & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & 1 & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{G}_1 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \ddots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{G}_m \end{bmatrix}, \tag{11}$$

em que os vetores $\mathbf{e} = (e_1, e_2, \ldots, e_m)$ e $\mathbf{g} = (g_1, g_2, \ldots, g_m)$ em $\mathbb{R}^N$ são usados para calcular

$$\mathbf{E}_n = \begin{bmatrix} \cos(2e_n\pi) & \text{sen}(2e_n\pi) \\ -\text{sen}(2e_n\pi) & \cos(2e_n\pi) \end{bmatrix} \tag{12}$$

e

$$\mathbf{G}_n = \begin{bmatrix} \cos(g_n\pi) & \text{sen}(g_n\pi) \\ -\text{sen}(g_n\pi) & \cos(g_n\pi) \end{bmatrix}, \tag{13}$$

$n = 1, 2, \ldots, m$. Além disso, da primeira até a $((N+1)/2)$-ésima coluna de $\mathbf{V}$, são colocados autovetores com o autovalor $\lambda^+ = 1$; nas demais colunas, são colocados autovetores com o autovalor $\lambda^- = -1$. A transformada multiordem definida dessa forma possui todas as propriedades mencionadas na Seção III e permite escolher $(N-1)$ parâmetros correspondentes às componentes dos vetores $\mathbf{e}$ e $\mathbf{g}$.

Se $N = 4m$, o método descrito acima pode ser ajustado conforme explicado a seguir. Os vetores $\mathbf{e} = (e_1, e_2, \ldots, e_m)$ e $\mathbf{g} = (g_1, g_2, \ldots, g_{m-1})$, com componentes reais, são usados para calcular $\mathbf{E}_n$, $n = 1, 2, \ldots, m$, e $\mathbf{G}_n$, $n = 1, 2, \ldots, m-$

1, como em (12) e (13), respectivamente. A matriz $\mathbf{\Lambda}^{\mathbf{e},\mathbf{g}}$ é construída como em (11), porém, tendo o número $\lambda^- = -1$ na posição (N, N). Da primeira até a $((N+2)/2)$-ésima coluna de $\mathbf{V}$, são colocados autovetores com o autovalor $\lambda^+ = 1$; nas demais colunas, são colocados autovetores com o autovalor $\lambda^- = -1$. Assim, obtém-se a seguinte matriz real para a DHT fracionária multiordem:

$$\mathbf{H}^{\mathbf{e},\mathbf{g}} = \mathbf{V}\mathbf{\Lambda}^{\mathbf{e},\mathbf{g}}\mathbf{V}^T. \tag{14}$$

B. Esquema de cifragem

Seguindo uma abordagem semelhante à apresentada noutros trabalhos [5], [17], o que se propõe é cifrar uma imagem $\mathbf{Im}$ aplicando uma versão bidimensional da DHT fracionária multiordem. A respectiva imagem cifrada é obtida por

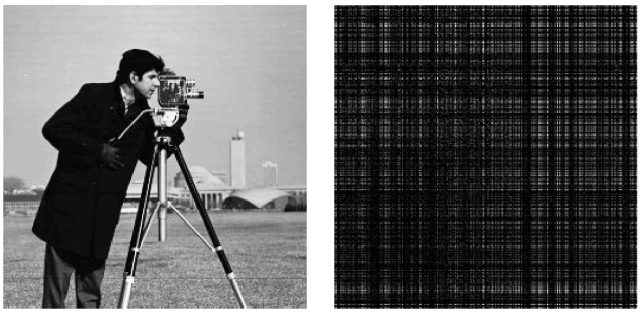
$$\mathbf{Im^c} = \mathbf{H}^{\mathbf{e}',\mathbf{g}'} \cdot \mathbf{Im} \cdot \mathbf{H}^{\mathbf{e}'',\mathbf{g}''}. \tag{15}$$

Na última equação, em vez de se usar $\mathbf{e}$ e $\mathbf{g}$ simplesmente, pode-se usar $\mathbf{e}'$ e $\mathbf{e}''$, e $\mathbf{g}'$ e $\mathbf{g}''$, que, sendo todos possivelmente distintos, indicam que as transformadas aplicadas às colunas e às linhas de $\mathbf{Im}$ podem ser diferentes. A decifragem é realizada pela aplicação das respectivas transformadas inversas a $\mathbf{Im^c}$, isto é, empregando, em vez dos parâmetros de ordem fracionária originais, seus simétricos aditivos.

O ponto principal na operação descrita, e que permite empregá-la efetivamente como uma cifragem, é o fato de haver diversos parâmetros que podem ser tomados como componentes de uma chave-secreta. De maneira mais específica, considerando $N = 4m$, podem ser escolhidos os seguintes parâmetros:

i. m componentes de cada um dos vetores $\mathbf{e}'$ e $\mathbf{e}''$, e $m-1$ componentes de cada um dos vetores $\mathbf{g}'$ e $\mathbf{g}''$, totalizando $4m - 2 = N - 2$ parâmetros;
ii. $2m+1$ componentes do autovetor de partida $\mathbf{v}_0^+$ e $2m-1$ componentes do autovetor de partida $\mathbf{v}_0^-$, para cada uma das transformadas aplicadas às colunas e às linhas de $\mathbf{Im}$, totalizando $8m = 2N$ parâmetros (supõe-se que, no passo 2 descrito na Seção III, esses vetores foram construídos a partir de vetores arbitrários $\mathbf{v}$ distintos);
iii. $4N^2$ componentes das quatro matrizes arbitrárias $\mathbf{A}$ utilizadas na obtenção de quatro matrizes geradoras $\mathbf{S_A}$ empregadas na geração dos conjuntos de autovetores associados a $\lambda^+ = 1$ e $\lambda^- = -1$, na transformada aplicada às colunas e naquela aplicada às linhas de $\mathbf{Im}$.

Somando os números de parâmetros de cada um dos itens acima, obtém-se um total de $4N^2 + 3N - 2$ parâmetros reais. A conversão deste número para binário, a fim de avaliar o tamanho do espaço de chaves que o método de cifragem permite, requer considerar determinada precisão para representar cada um dos parâmetros. Isso, por sua vez, depende da sensibilidade da cifragem a desvios impostos a cada um desses parâmetros; noutras palavras, escolhendo certo conjunto de parâmetros como chave, ao tentar decifrar uma imagem usando, por exemplo, $e'_1 + \delta$, $\delta \in \mathbb{R}$, em vez de e'_1, como primeira componente do vetor $\mathbf{e}'$ (as demais componentes da chave estariam corretas), seria preciso saber que valor mínimo de δ levaria a uma decifragem incorreta. Uma análise detalhada desse aspecto se encontra sob investigação e requer o uso de outras estratégias que fogem ao escopo do presente trabalho, cujo foco é apresentar o método introduzido na Seção III. Em todo caso, a fim de validar as ideias discutidas nesta seção, são apresentados a seguir alguns resultados preliminares de simulações relativas ao método de cifragem proposto.



(a) (b)

Fig. 1: Imagem "cameraman" (a) original e (b) cifrada.

C. Experimentos computacionais

Nos experimentos realizados, foram consideradas imagens em escala de cinza com dimensão 256×256 e, portanto, construídas DHT fracionárias multiordem reais com $N = 256$. Tal construção foi feita segundo o método descrito na subseção IV-B, porém empregando $\mathbf{H}^{\mathbf{e}',\mathbf{g}'} = \mathbf{H}^{\mathbf{e}'',\mathbf{g}''}$ e utilizando uma matriz $\mathbf{A}$ única para obter as matrizes geradoras de todos os autovetores necessários. Todos os parâmetros previamente mencionados foram escolhidos de forma aleatória. A matriz $\mathbf{A}$, em particular, teve seus elementos escolhidos segundo uma distribuição uniforme no intervalo $[0, 1]$.

Na Figura 1, apresenta-se uma das imagens utilizadas nas simulações, bem como a sua versão transformada segundo (15). É possível observar, na imagem cifrada, que o conteúdo visual da imagem original foi completamente corrompido. Um resultado semelhante é obtido se outras imagens forem consideradas. Utilizando os parâmetros corretos, pôde-se recuperar a imagem original sem erro significativo.

Com relação à segurança do método, realizou-se uma análise preliminar acerca da sua sensibilidade a variações nos parâmetros que podem integrar a chave-secreta. Mais especificamente, adicionou-se à matriz $\mathbf{A}$ empregada na cifragem uma matriz $\mathbf{\Delta}$ com todos os elementos iguais a $\delta = 0{,}05$. Ao se tentar recuperar a imagem original, utilizando a matriz $\mathbf{A} + \mathbf{\Delta}$ no lugar de $\mathbf{A}$ e mantendo os demais parâmetros inalterados, obteve-se como resultado a imagem da Figura 2. Embora se verifique alguma correlação visual com a imagem original (Figura 1a), a referida imagem já se apresenta bastante degradada. Um gráfico que reflete a diferença entre a imagem recuperada e a original é apresentado na Figura 3. Ele contém uma curva do erro médio quadrático entre as duas imagens, em função de desvios δ que compõem a matriz $\mathbf{\Delta}$. Na curva, observa-se que, se $|\delta| > 10^{-4}$, são obtidos erros maiores que 20.000, o que, normalmente, sugere que não se pode inferir, a partir da imagem resultante da tentativa de decifragem, conteúdo relevante da imagem original correta. De qualquer forma, ainda é necessário confrontar este resultado com a análise visual que se fez com base na Figura 2.

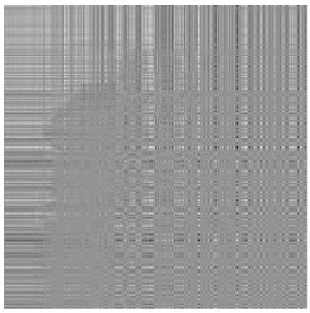


Fig. 2: Imagem obtida após tentativa de decifragem com parâmetros incorretos.

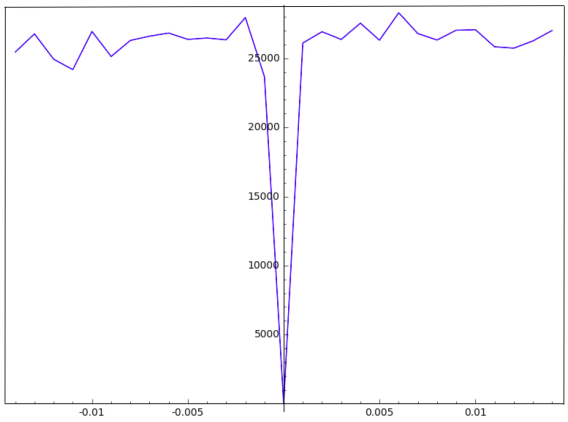


Fig. 3: Curva do erro entre a imagem recuperada e a original, em função de desvios δ que compõem a matriz constante $\mathbf{\Delta}$, adicionada à matriz $\mathbf{A}$ quando da tentativa de uma decifragem.

Embora se espere que um comportamento semelhante ocorra, quando desvios sobre outros parâmetros forem considerados na decifragem, tal possibilidade precisa ser confirmada, a fim de que se possa calcular o espaço de chaves do método. De qualquer forma, como o número de parâmetros livres é grande (vide Subseção IV-B), não deve haver problemas para se alcançar espaços de chaves grandes o suficiente para inviabilizar ataques de força-bruta. Além desse aspecto, encontra-se sob investigação a robustez do método a outros tipos de ataques criptográficos.

V. Conclusões

Neste artigo, foi introduzido um método baseado em matrizes geradoras para construção de autovetores da transformada discreta de Hartley. Os conjuntos de autovetores obtidos por meio do referido método foram caracterizados e empregados na definição de uma DHT fracionária. Uma DFrHT real e multiordem foi apresentada. Motivados pelo número de parâmetros livres dessa transformada, que é maior que o das transformadas de Fourier correspondentes, realizou-se uma avaliação preliminar de sua aplicação ao cenário de cifragem de imagens. Os resultados iniciais sugerem que, no referido cenário, a decifragem é suficientemente sensível a desvios impostos aos parâmetros necessários à construção da transformada. Uma análise mais detalhada acerca da segurança do método de cifragem considerado têm sido realizada. Além disso, outras aplicações da DFrHT proposta têm sido investigadas e o emprego de matrizes geradoras para construir autovetores de outras transformadas discretas e obter suas respectivas versões fracionárias tem sido estudado.

Agradecimentos

Os autores agradecem ao Conselho Nacional de Desenvolvimento Científico e Tecnológico, CNPq (processos 56744/2014-2, 307686/2014-0, 142428/2015-9) e à Fundação de Amparo à Ciência e Tecnologia do Estado de Pernambuco, FACEPE (processo IBPG-0100-3.04-15), por terem financiado este trabalho, e ao apoio do Programa de Pós-Graduação em Engenharia Elétrica, PPGEE / UFPE.

Referências

[1] Alan V. Oppenheim and Ronald W. Schafer, *Discrete-Time Signal Processing*, Pearson, New Jersey, USA, 3 edition, 2010.

[2] J.H. McClellan and T.W. Parks, "Eigenvalue and eigenvector decomposition of the discrete Fourier transform," *IEEE Transactions on Audio and Electroacoustics*, vol. 20, no. 1, pp. 66–74, 1972.

[3] S.-C. Pei and M.-H. Yeh, "The discrete fractional cosine and sine transforms," *IEEE Transactions on Signal Processing*, vol. 49, no. 6, pp. 1198–1207, June 2001.

[4] C. Candan, M. Alper Kutay, and H. M. Ozaktas, "The discrete fractional Fourier transform," *IEEE Transactions on Signal Processing*, vol. 48, no. 5, pp. 1329–1337, May 2000.

[5] X. Kang, R. Tao, and F. Zhang, "Multiple-parameter discrete fractional transform and its applications," *IEEE Transactions on Signal Processing*, vol. 64, no. 13, pp. 3402–3417, July 2016.

[6] Y. Zhang, D. Xiao, W. Wen, and Y. Tian, "Edge-based lightweight image encryption using chaos-based reversible hidden transform and multiple-order discrete fractional cosine transform," *Optics & Laser Technology*, vol. 54, pp. 1–6, December 2013.

[7] Y. Hu, F. Zhang, L. Xu, R. Tao, and Y. Wang, "Reconstruction of uniformly sampled signals from non-uniform short samples in fractional Fourier domain," *IET Signal Processing*, vol. 10, no. 2, pp. 140–149, April 2016.

[8] X. Zhi, D. Wei, and W. Zhang, "A generalized convolution theorem for the special affine Fourier transform and its application to filtering," *Optik - International Journal for Light and Electron Optics*, vol. 127, no. 5, pp. 2613–2616, Mar. 2016.

[9] Y. Zhao, H. Yu, G. Wei, F. Ji, and F. Chen, "Parameter estimation of wideband underwater acoustic multipath channels based on fractional Fourier transform," *IEEE Transactions on Signal Processing*, vol. 64, no. 20, pp. 5396–5408, October 2016.

[10] U. Singh and S. N. Singh, "Application of fractional Fourier transform for classification of power quality disturbances," *IET Science, Measurement & Technology*, vol. 11, no. 1, pp. 67–76, January 2017.

[11] S.-C. Pei and K.-W. Chang, "Generating matrix of discrete fourier transform eigenvectors," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing*, Taipei, Taiwan, April 2009, pp. 3333–3336.

[12] S.-C. Pei, C.-C. Tseng, M.-H. Yeh, and J.-J. Shyu, "Discrete fractional Hartley and Fourier transforms," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 45, no. 6, pp. 665–675, June 1998.

[13] Y. Liu, J. Du, J. Fan, and L. Gong, "Single-channel color image encryption algorithm based on fractional Hartley transform and vector operation," *Multimedia Tools and Applications*, vol. 74, no. 9, pp. 3171–3182, May 2015.

[14] I. Venturini and P. Duhamel, "Reality preserving fractional transforms," in *IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP'2004)*, 2004, vol. 5, pp. 205–208.

[15] W. L. Hsue and W. C. Chang, "Multiple-parameter real discrete fractional Fourier and Hartley transforms," in *International Conference on Digital Signal Processing*, August 2014, pp. 694–698.

[16] W. L. Hsue and W. C. Chang, "Real discrete fractional Fourier, Hartley, generalized Fourier and generalized Hartley transforms with many parameters," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 62, no. 10, pp. 2594–2605, October 2015.

[17] S.-C. Pei and W. L. Hsue, "Random discrete fractional fourier transform," *IEEE Signal Processing Letters*, vol. 16, no. 12, pp. 1015–1017, December 2009.