Universidade Federal de Pernambuco
Centro de Tecnologia e Geociências
Departamento de Eletrônica e Sistemas
Programa de Pós-graduação em Engenharia Elétrica

Ravi Barreto Dória Figueiredo

Construção de Autovetores de Transformadas Trigonométricas Discretas Baseada em Matrizes Geradoras

RECIFE
2017

Ravi Barreto Dória Figueiredo

Construção de Autovetores de Transformadas Trigonométricas Discretas Baseada em Matrizes Geradoras

Dissertação submetida ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Pernambuco como parte dos requisitos para obtenção do grau de Mestre em Engenharia Elétrica.

Área de Concentração: Comunicações
Linha de Pesquisa: Processamento Digital de Sinais

Orientador: Prof. Dr. Juliano Bandeira Lima.

RECIFE
2017

Catalogação na fonte
Bibliotecária Valdicéa Alves, CRB-4 / 1260

F476c Figueiredo, Raví Barreto Dória

Construção de autovetores de transformadas trigonométricas discretas baseada em matrizes geradoras/ Raví Barreto Dória Figueiredo. – 2017.

76folhas, il.

Orientador: Prof. Dr. Juliano B. Lima

Dissertação(Mestrado) – Universidade Federal de Pernambuco. CTG. Programa de Pós-Graduação em Engenharia Elétrica, 2017.

Inclui Referências.

1. Engenharia Elétrica. 2. Transformadas trigonométricas discretas. 3. Autovetores. 4. Matrizes geradoras. 5. Cifragem de imagens. I. Lima, Juliano B.. (Orientador). II.Título.

621.3 CDD (22. ed.)

UFPE
BCTG/2018-124

Universidade Federal de Pernambuco

Pós-Graduação em Engenharia Elétrica

PARECER DA COMISSÃO EXAMINADORA DE DEFESA DE DISSERTAÇÃO DO MESTRADO ACADÊMICO DE

Ravi Barreto Doria Figueiredo

TÍTULO

"CONSTRUÇÃO DE AUTOVETORES DE *TRANSFORMADAS TRIGONOMÉTRICAS DISCRETAS BASEADA EM MATRIZES GERADORAS*"

A comissão examinadora composta pelos professores: JULIANO BANDEIRA LIMA, DES/UFPE; DANIEL PEDRO BEZERRA CHAVES, DES/UFPE e FRANCISCO MADEIRO BERNARDINO JÚNIOR, POLI/UPE, sob a presidência do primeiro, consideram o candidato RAVI BARRETO DORIA FIGUEIREDO **APROVADO**.

Recife, 31 de julho de 2017.

MARCELO CABRAL CAVALCANTI Coordenador do PPGEE	**JULIANO BANDEIRA LIMA** Orientador e Membro Titular Interno
FRANCISCO MADEIRO BERNARDINO JÚNIOR Membro Titular Externo	**DANIEL PEDRO BEZERRA CHAVES** Membro Titular Interno

Agradecimentos

Eu sou uma mini-peça nesse jogo, agradeço aos meus pais, Renan e Marizi, pelo apoio incondicional, e agradeço por ser integrante desta familia. Agradeço a minha irmã Isa, Paula e Daniel.

Agradeço a minha querida dupla evolutiva, Lucianna, que aprendemos tanto juntos. Nossa jornada apenas começou.

Aos meus grandes amigos, Diego Canterle, Bruno Vinicius, Carlos Eduardo, Jose Perez(Cubano), Veruska, Jamille, Guilherme Boaviagem, José Neto, Rodrigo Bernardino(Rodorigo), Darlinsson Santos, pelo apoio e pelas ótimas discussões que tivemos juntos, e claro, pela convivência.

Agradeço a meu orientador Juliano Bandeira, que me acolheu sem me conhecer, que me guiou da maneira mais correta que poderia imaginar, pela paciência e pela amizade. Me sinto muito orgulhoso de compartilhar esses momentos contigo.

Agradeço ao professor Ricardo Campello, por me mostrar como é ser professor, as lições passadas por ele foi além do assunto, adorei ter encontrado o senhor.

Agradeço a Facepe, por promover um aluno como eu, que não sabia de minha capacidade, graças a eles poderei seguir aquilo com que sonhei.

"As consciências se atraem por suas afinidades mais profundas."
(Waldo Vieira)

Resumo

Transformadas discretas são ferramentas bem conhecidas e que desempenham um papel importante em diversas aplicações de Engenharia e, em particular, de Processamento Digital de Sinais. O cálculo de uma transformada pode ser representado pelo produto entre a respectiva matriz de transformação e o vetor cuja transformada se deseja obter. Nas últimas décadas, diversas propriedades relacionadas às autoestruturas dessas matrizes têm sido investigadas; mais especificamente, têm sido propostos métodos para construir autovetores dessas matrizes, os quais podem ser empregados, por exemplo, na definição de versões fracionárias das respectivas transformadas. Nesta dissertação, são propostas metodologias baseadas em matrizes geradoras para construção de autovetores de transformadas trigonométricas discretas, as quais, no presente contexto, se referem às transformadas discretas do cosseno e do seno dos tipos I e IV, e à transformada discreta de Hartley; dado um autovetor de uma dessas transformadas, associado a certo autovalor, mostra-se como obter uma matriz que, ao ser multiplicada pelo referido autovetor, produz um novo autovetor, com autovalor possivelmente distinto do primeiro. São discutidos procedimentos para que, utilizando as metodologias propostas, sejam obtidas bases de autovetores. Essas bases são, então, empregadas na definição de versões fracionárias, multiordem e reais das transformadas correspondentes. Esquemas de cifragem de imagens baseados nas transformadas definidas são considerados e têm sua robustez avaliada de forma preliminar. Os resultados sugerem que os referidos esquemas preenchem alguns dos principais requisitos de segurança necessários à aplicabilidade em cenários práticos. Isso se deve, em parte, ao número de parâmetros livres envolvidos nos procedimentos introduzidos neste trabalho, que é maior que o de métodos similares encontrados na literatura.

Palavras-chave: Transformadas trigonométricas discretas. Autovetores. Matrizes geradoras. Cifragem de imagens.

Abstract

Discrete transforms are well-known mathematical tools and play an important role in several applications of Engineering and, in particular, in Digital Signal Processing. The computation of a transform can be represented as the product between the respective transform matrix and the vector whose transform one desires to obtain. In the last decades, several properties related to the eigenstructures of such matrices have been investigated; more specifically, methods devoted to the construction of eigenvectors of such matrices, which can be employed, for instance, in the definition of fractional versions of the respective transforms, have been proposed. In this dissertation, methodologies based on generating matrices for constructing eigenvectors of discrete trigonometric transforms are proposed (in the present context, such transforms refer to discrete cosine and sine transforms of types I and IV, and to the discrete Hartley transform); given an eigenvector of one of such transforms, associated to a certain eigenvalue, one demonstrates how to obtain a matrix which, being multiplied by the referred eigenvector, produces a new eigenvector with eigenvalue possibly different from the former. We discuss procedures for obtaining eigenvector bases using the proposed methodologies. Such bases are then employed in the definition of fractional, multiorder and real-valued versions of the corresponding transforms. Image encryption schemes based on the defined transforms are considered and have their robustness evaluated in a preliminary manner. The results suggest that the referred schemes complies with some of the main security requirements necessary to the applicability in practical scenarios. In part, this is due to the number od free parameters involved in the techniques introduced in this work, which is greater than that of similar methods found in the literature.

Keywords: Discrete trigonometric transforms. Eigenvectors. Generating matrices. Image encryption.

Lista de Ilustrações

Lista de Tabelas

Sumário

1 Introdução

As transformadas discretas são ferramentas matemáticas bem conhecidas e que possuem grande importância em diversas aplicações de Engenharia. A transformada discreta mais difundida é a de Fourier (DFT, do inglês *discrete Fourier transform*), cuja aplicação produz uma representação no domínio da frequência de sinais inerentemente digitais ou de sinais originalmente contínuos, que foram submetidos a processos como amostragem e quantização. Ao longo dos anos, outras transformadas discretas foram propostas, dentre as quais podem ser destacadas a do cosseno, a do seno, a de Hartley e a wavelet. Além disso, diferentes versões de cada uma dessas transformadas foram estabelecidas. Entre essas versões, encontram-se as transformadas fracionárias, que generalizam as transformadas ordinárias correspondentes no sentido de permitir que sejam calculadas potências não-inteiras dos respectivos operadores de transformação. A seguir, é apresentado o estado da arte a respeito das transformadas fracionárias, o que permite, nas seções subsequentes, elencar o objetivo geral e os objetivos específicos desta dissertação.

1.1 Autovetores de transformadas discretas

Desde 1960, as transformadas discretas têm desempenhado um papel essencial numa gama de aplicações de Engenharia e, em particular, em processamento digital de sinais. Tal abrangência se deve, dentre outros motivos, às diferentes propriedades das diversas transformadas discretas que têm sido definidas e à viabilização da implementação dessas transformadas em plataformas de *software* e *hardware* de vários tipos. A caracterização de uma transformada discreta envolve uma série de aspectos, sendo realizada a partir de interpretações específicas que se pode dar a essas ferramentas. O cálculo de uma transformada discreta pode ser expresso, por exemplo, como o produto entre uma matriz identificada como matriz de transformação e um vetor cuja transformada se deseja calcular; normalmente, um vetor $\mathbf{x} = (x[n])$ com comprimento N tem sua transformada $\mathbf{X} = (X[k])$ de mesmo comprimento calculada por

$$X[k] = \sum_{n=0}^{N-1} x[n]M[k,n],$$

$k = 0, 1, \ldots, N-1$, em que $\mathbf{M} = (M[k,n])$ corresponde à referida matriz de transformação e representa, também, o núcleo da transformada. O produto matriz-vetor que se mencionou seria, então, escrito como

$$\mathbf{X} = \mathbf{M} \cdot \mathbf{x}.$$

O estudo dos atributos da matriz associada a determinadas transformadas discretas tem sido bastante útil no desenvolvimento de questões teóricas e práticas a elas associadas. A fatoração de uma matriz de transformação pode auxiliar, por exemplo, no projeto de algoritmos rápidos para realizar o produto dado na última equação. Outro aspecto cuja investigação tem sido alvo de um grande número de trabalhos desde a década de 1970 é o das autoestruturas dessas matrizes, isto é, da determinação de seus autovalores e autovetores. Com respeito aos autovalores, além de determinar os seus valores propriamente ditos, o que usualmente se objetiva nos referidos trabalhos [2] é determinar suas multiplicidades algébrica e geométrica; com relação aos autovetores, o mais importante é determinar como esses podem ser construídos e, eventualmente, identificar propriedades interessantes sob algum critério em conjuntos formados por eles.

Quando se considera a transformada discreta de Fourier, uma lista de resultados e métodos relacionados à autoestrutura da respectiva matriz de transformação pode ser apresentada. A construção de autovetores da DFT, por exemplo, pode ser feita a partir de matrizes que comutam com a sua matriz de transformação. Isso é possível porque, quando duas matrizes são comutantes, elas possuem pelo menos um conjunto de autovetores em comum; isso tem sido usado para lidar com o fato de uma matriz da DFT, com dimensão $N \times N$, possuir infinitos conjuntos ortogonais distintos com N autovetores. Existem várias matrizes que possuem a propriedade de comutar com a matriz da DFT. Alguns dos principais exemplos são encontrados em [3], [4], [5] e [6]. Via de regra, a construção de conjuntos ortogonais formados por autovetores da DFT a partir de matrizes comutantes requer a execução de passos que não são baseados em fórmulas fechadas e possui complexidade aritmética $\mathcal{O}(N^3)$.

Em [7], Pei e Chang propuseram um método para geração de autovetores da matriz da DFT baseado em matrizes geradoras. A complexidade da técnica é de $\mathcal{O}(N^2 \log N)$ e emprega apenas fórmulas fechadas. Na proposta, indica-se como construir uma matriz geradora que possui a propriedade de, ao ser multiplicada por um autovetor da DFT, associado a certo autovalor, fornecer um novo autovetor, associado a um autovalor possivelmente

diferente do primeiro. Essa estratégia pode ser aplicada de forma recursiva até que um conjunto de autovetores seja obtido.

Técnicas dedicadas à construção de conjuntos de autovetores de transformadas discretas diferentes da de Fourier não têm sido muito exploradas. Na realidade, o que normalmente se faz é construir um autovetor da matriz da DFT e, a partir deste autovetor, derivar o autovetor correspondente da matriz da transformada discreta do cosseno ou do seno, por exemplo. De qualquer maneira, o principal uso desses autovetores tem sido a definição de transformadas fracionárias, as quais, conforme descrito a seguir, constituem uma espécie de generalização das transformadas ordinárias associadas.

1.2 Transformadas fracionárias

A origem dos estudos sobre transformadas fracionárias remonta ao início do século XX. Nesses estudos, a transformada de Fourier (ordinária) é interpretada como um operador integral aplicável a uma função ou sinal. Aplicar este operador várias vezes, de forma recursiva, a determinada função ou sinal corresponde a calcular potências do operador. A transformada fracionária de Fourier (FrFT, do inglês *fractional Fourier transform*) consiste numa generalização da transformada de Fourier, em que potências não inteiras do referido operador são aplicadas.

O cálculo de uma FrFT admite diferentes interpretações. É possível descrever o efeito desta transformação, por exemplo, empregando o plano tempo-frequência. O cálculo de uma transformada de Fourier ordinária gera uma representação de um sinal do domínio do tempo para o da frequência; se a transformada for aplicada novamente, a representação é transladada do domínio da frequência para o do tempo, porém com sentido invertido, e assim por diante. Cada aplicação da transformada pode, então, ser visto como uma rotação por um ângulo igual a $\pi/2$ no plano mostrado na Figura Figura - 1.1. Assim, o cálculo de uma FrFT pode ser interpretado como uma rotação, no sentido anti-horário, por um ângulo igual a $\alpha = a\pi/2$, em que $a \in \mathbb{R}$ é a ordem fracionária [1]; noutras palavras, sempre que o valor de a for não-inteiro, um sinal originalmente no domínio do tempo é levado para uma espécie de domínio intermediário, em que o tempo e a frequência estão de certa forma misturados.

A primeira referência relacionada a FrFT se encontra num artigo de Wiener, publicado em 1929 [8], o qual apresenta uma relação entre a expansão de uma série de Hermite e sua

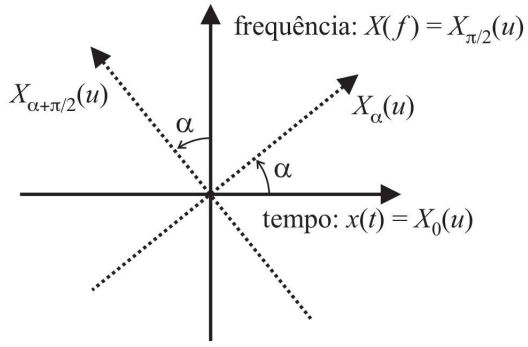


Figura Figura - 1.1 – *Representação da transformada fracionária de Fourier em um plano tempo-frequência [1].*

transformada de Fourier. Em 1937 [9], Condon demonstrou que o operador de Fourier gera um grupo cíclio de transformações de ordem 4, o qual é isomorfo a um grupo de rotações num plano com ângulo múltiplos de $\pi/2$; ele encontrou um grupo de transformadas gerado pelo operador Hermitiano, do qual o grupo gerado pelo operador da transformada de Fourier é um subgrupo.

O termo transformada fracionária de Fourier, especificamente, parece ter sido cunhado por Namias, em 1980, num artigo que define o operador de Fourier fracionário, apresenta algumas propriedades e fornece uma aplicação em Mecânica Quântica, mais precisamnete, na obtenção de uma solução da equação de Schrödinger para o oscilador harmônico. Em 1987, McBride e Kerr [10], percebendo certa ausência de rigor no trabalho de Namias, escreveram um artigo com finalidade de desenvolver uma formulação matemática mais rigorosa dos conceitos apresentados. Nos anos seguintes, em 1987, 1989 e em 1991, três artigos importantes relacionados à FrFT foram publicados; os trabalhos relacionam a FrFT ao Princípio da Incerteza e à distribuição tempo-frequência de Wigner [11], [12], [13].

Após o estabelecimento da FrFT, tornou-se natural a busca por versões discretas dessa transformada. A ideia seria obter um operador que generalizasse a transformada discreta de Fourier num sentido análogo ao que a FrFT generaliza a transformada de Fourier ordinária. Neste sentido, houve uma grande contribuição em 1982, quando Dickinson *et al*. [3], baseados, em parte, no trabalho que já havia sido realizado por Parks e McClellan em [14], analisaram a autoestrutura da matriz da DFT e propuseram um método para construir conjuntos ortogonais de autovetores dessa matriz (tal método é baseado numa matriz comutante com a matriz da DFT, possibilidade sobre a qual se escreveu na parte inicial deste

capítulo). Com isso, foi proposta, também, uma forma eficiente de computar potências fracionárias da matriz da DFT. Mais especificamente, denotando por $\mathbf{F}$ a matriz da DFT e sabendo que tal operador é diagonalizável, pode-se escrever

$$\mathbf{F} = \mathbf{V}\mathbf{\Lambda}\mathbf{V}^T, \tag{1.1}$$

em que $\mathbf{V}$ é uma matriz cujas colunas são dadas por vetores de um conjunto ortonormal de autovetores de $\mathbf{F}$, $\mathbf{\Lambda}$ é uma matriz diagonal contendo os autovalores de $\mathbf{F}$ na mesma sequência em que os respectivos autovetores são dispostos ao longo das colunas de $\mathbf{V}$ e $\mathbf{V}^T$ corresponde à versão transposta da matriz $\mathbf{V}$. Assim, a a-ésima potência de $\mathbf{F}$ é dada por

$$\mathbf{F}^a = \mathbf{V}\mathbf{\Lambda}^a\mathbf{V}^T. \tag{1.2}$$

É relevante observar que a equação 1.2 pode ser usada para calcular potências não-inteiras de um operador matricial qualquer ou, mais restritamente, de matrizes associadas a outros tipos de transformadas discretas. O ponto-chave neste processo, sobretudo se a matriz, ainda que seja diagonalizável, possuir autovalores repetidos, é a construção do conjunto de autovetores a serem empregados como colunas de $\mathbf{V}$.

Em paralelo às novidades que surgiam no campo das transformadas fracionárias discretas, os pesquisadores continuaram a avançar nas investigações relacionadas à transformada fracionária de Fourier (para sinais de variável contínua). Nos anos de 1993 e 1994, foram publicados estudos descrevendo a relação entre a FrFT e a propagação da luz em sistemas ópticos e novos resultados descrevendo a relação entre a FrFT e outras representações tempo-frequência, tais como a transformada de Fourier de curta duração, a função ambiguidade e o espectograma [15], [16], [17], [18].

Com a consolidação da FrFT e de suas propriedades, versões mais refinadas da DFrFT (do inglês *discrete fractional Fourier transform*) também foram propostas. A ideia era que uma formulação teórica mais consistente da DFrFT permitiria a implementação prática da FrFT, tornando-a viável inclusive para novos campos de aplicação, como o de imagens, vídeos, áudio e outras informações contidas em formato digital [19], [20], [21]. Muitos dos estudos sobre a DFrFT estão concentrados na construção de autovetores do tipo Hermite-Gaussiano da DFT, que reproduzem propriedades das respectivas funções de variável contínua empregadas na fracionarização da transformada de Fourier [3], [5], [6], [4], [7].

Alguns pesquisadores propuseram estender o conceito de transformada fracionária para outras transformadas diferentes da de Fourier, como, por exemplo, versões fracionárias das

transformadas discretas do cosseno, do seno e de Hartley [22], [23], [24], [25]. Tanto no cenário de variável contínua quanto no de variável discreta, as autoestruturas destas transformadas, ou seja, os autovalores e os autovetores, podem ser caracterizadas a partir da autoestrutura da transformada de Fourier. Com isso, as transformadas fracionárias correspondentes a essas transformadas podem ser definidas a partir da FrFT e da DFrFT, embora cada uma possua peculiaridades que as tornam menos ou mais atrativas para determinadas aplicações. Em lugar das transformadas fracionárias de Fourier, têm sido empregadas transformadas fracionárias do cosseno, do seno e de Hartley, por exemplo, em verificação *online* de assinaturas manuscritas [26], ocultação de dados em sinais de voz [27], cifragem de imagens coloridas [28], extração de características em reconhecimento de locutor [27] e em outros cenários de aplicação.

Cifragem de imagens

O histórico resumido que se acabou de apresentar dá indício da diversidade de cenários em que as transformadas fracionárias podem ser empregadas. Como parte deste rol, além das aplicações que já foram mencionadas, podem ser listadas como exemplos a filtragem de sinais[29**?** , 30], as técnicas modernas de comunicação, como aquelas que empregam a multiplexação por divisão de frequências ortogonais (OFDM, do inglês *orthogonal frequency-division multiplexing*) [31, 32], os sistemas de radar de abertura sintética (SAR, do inglês *synthetic aperture radar*) [33], a estimação cega da dispersão cromática em comunicações ópticas, a estimação de parâmetros de canais acústicos subaquáticos banda-larga com múltiplos percursos [34], o processamento de sinais linearmente modulados em frequência (LFM, do inglês *linear frequency modulation*) [35], a classificaçao de distúrbios na qualidade da energia (PQD, do inglês *power quality disturbance*) [36], o diagnóstico de imagem por ultrassom de dentes humanos [37], o desenvolvimento de uma transformada de Hough avançada com base numa FrFT multicamada [38], dentre outras.

Mais um dos cenários de aplicação das transformadas fracionárias é o de cifragem de imagens. Isso se deve, principalmente, ao fato de se poder utilizar a ordem fracionária como chave de segurança. A cifragem de uma imagem objetiva, por exemplo, a sua transmissão por um canal supostamente inseguro, de maneira que, caso um observador intercepte-a sem autorização, este não consiga extrair informação sobre a imagem; na prática, após passar por um processo de cifragem, uma imagem adquire aspecto visual ruidoso, o qual se reflete, também, em diversas métricas relacionadas à entropia, correlação entre pixels

vizinhos, entre outros. Liu *et al.* [39] mostra que a DFrFT pode ser usada diretamente em uma cifragem de imagem por meio do cálculo da respectiva transformada bidimensional. A partir deste estudo, várias técnicas para cifragem de imagem baseadas no mesmo princípio e envolvendo, adicionalmente, outras estratégias voltadas ao aperfeiçoamento de aspecros de segurança foram propostas [20], [40], [41].

1.3 Justificativa

Conforme se pode constatar pelo conteúdo apresentado nas primeiras seções deste capítulo e, particularmente, pela atualidade das referências citadas, técnicas para construção de autovetores de transformadas discretas, visando, sobretudo, à definicão das respectivas transformadas fracionárias e ao estudo de suas aplicações, continuam sendo um tema de grande interesse de diversos grupos de pesquisadores. Esta realidade serve como motivação principal para o desenvolvimento desta dissertação, em que se coloca como foco a extensão a certos tipos de transformadas trigonométricas discretas do método de matrizes geradoras de autovetores da transformada discreta de Fourier introduzido em [7]. O propósito é disponibilizar mais uma alternativa para construção de tais autovetores, a qual pode prover determinadas vantagens, em comparação às técnicas já estabelecidas na literatura; esses autovetores podem ser empregados na definição de novas transformadas fracionárias que, por sua vez, podem ser utilizadas em cenários de aplicação os mais diversos.

1.4 Objetivos

O objetivo geral desta dissertação é a proposição de um método para construção de autovetores de certos tipos de transformadas trigonométricas discretas empregando matrizes geradoras. As transformadas consideradas são a do cosseno e a do seno dos tipos I e IV, e a de Hartley.

Objetivos específicos

Como obejtviso específicos deste trabalho, podem ser elencados os seguintes:

1. Introduzir uma proposição que indique como construir matrizes geradoras de autovetores das transformadas discretas do cosseno e a do seno dos tipos I e IV, e a de Hartley;

2. Propor procedimentos sistemáticos para gerar conjuntos de autovetores das transformadas investigadas, os quais podem constituir bases a serem empregadas na expansão espectral dos respectivos operadores;
3. Empregar, efetivamente, as bases mencionadas para fracionarizar as transformadas consideradas e, mais especificamente, obter versões reais e multiordem destas ferramentas;
4. Aplicar os resultados teóricos obtidos ao cenário de cifragem de imagens digitais;
5. Realizar uma avaliação preliminar dos aspectos de segurança dos esquemas de cifragem propostos.

1.5 Estrutura e contribuições da dissertação

Esta dissertação se encontra organizada da seguinte forma:

- ▷ No Capítulo 1, é realizada uma contextualização do trabalho, sendo apresentado, de forma concisa, um apanhado histórico a respeito dos temas abordados e sendo colocados os principais motivos para a sua realização e os objetivos inicialmente delineados.
- ▷ O Capítulo 2 apresenta uma revisão bibliográfica sobre a transformada discreta de Fourier, as transformadas discretas do cosseno e do seno dos tipos I e IV, e a transformada discreta de Hartley. São apresentadas, basicamente, as definições de cada uma dessas transformadas e enunciados os principais resultados acerca das autoestruturas das respectivas matrizes de transformação.
- ▷ No Capítulo 3, é apresentado a contribuição central da dissertação: um método baseado em matrizes geradoras para construção de autovetores das transformadas discretas do cosseno e do seno dos tipos I e IV, e da transformada discreta de Hartley. São introduzidos procedimentos para que, empregando o referido método, sejam obtidas bases formadas pelos autovetores construídos, as quais são empregadas na fracionarização das transformadas correspondentes. Tal possibilidade é, então, estendida por meio da definição de transformadas fracionárias trigonométricas discretas com múltiplas ordens e representadas por operadores matriciais reais.
- ▷ No Capítulo 4, é discutido um método para cifragem de imagens baseado nas transformadas definidas no Capítulo 3. O método propriamente dito é similar a outros existentes na

literatura, porém, empregando as transformadas construídas nesta dissertação em substituição a outras transformadas fracionárias, tem-se um número maior de parâmetros livres; isso eleva, potencialmente, o espaço de chaves do esquema e, consequentemente, a sua robustez a ataques de força-bruta. Uma avaliação preliminar desse aspecto é realizada.

- ▷ O Capítulo 5 traz as conclusões do trabalho, indica sugestões para a continuidade da pesquisa e lista os artigos resultantes da pesquisa realizada.

2 Autoestruturas de transformadas discretas

Neste capítulo, são revisadas definições e proposições relacionadas a alguns tipos de transformadas trigonométricas discretas. Mais especificamente, são abordadas as transformadas discretas do cosseno e do seno dos tipos I e IV, e a transformada discreta de Hartley. A autoestrutura de cada uma dessas transformadas é apresentada, o que inclui a determinação de seus autovalores e a caracterização dos respectivos autovetores. Métodos voltados à construção desses autovetores também são discutidos. Mostra-se, por exemplo, como um autovetor da DFT ou de sua versão generalizada pode ser utilizado para obter um autovetor de uma das transformadas mencionadas.

2.1 Transformada discreta de fourier

Nesta seção, são apresentados os principais resultados relacionados à autoestrutura da transformada discreta de Fourier (DFT, do inglês *discrete Fourier transform*) [14]. Inicia-se pela definição dessa transformada, a qual é dada a seguir.

Definição 2.1 – Transformada discreta de Fourier

A DFT de um vetor $\mathbf{x} = (x[n])$*, com componentes* $x[n] \in \mathbb{C}$*,* $n = 0, 1, \ldots, N-1$*, é o vetor* $\mathbf{X} = (X[k])$ *com componentes*

$$X[k] = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x[n] W^{kn}, \tag{2.1}$$

$k = 0, 1, \ldots, N-1$*, em que* $W = e^{-i\frac{2\pi}{N}}$ *e* $i = \sqrt{-1}$*.* □

Teorema 2.1 – Transformada discreta de Fourier inversa

A DFT inversa de um vetor $\mathbf{X} = (X[k])$*, com componentes* $X[k] \in \mathbb{C}$*,* $k = 0, 1, \ldots, N-1$*, é o vetor* $\mathbf{x} = (x[n])$ *com componentes*

$$x[n] = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} X[k] W^{-kn}, \tag{2.2}$$

$n = 0, 1, \ldots, N-1$*.* □

Pode-se relacionar um vetor $\mathbf{x}$ e a sua DFT $\mathbf{X}$ por meio da equação matricial

$$\mathbf{X} = \mathbf{F}\mathbf{x}, \tag{2.3}$$

em que a entrada na k-ésima linha e na n-ésima coluna da matriz $\mathbf{F}$ da DFT é dada por

$$F[k,n] = \frac{1}{\sqrt{N}} e^{-i\frac{2\pi}{N}kn}, \tag{2.4}$$

$k, n = 0, 1, \ldots, N-1$.

Autoestrutura da matriz da DFT

Proposição 2.1

Os autovalores da matriz da DFT são as raízes de quarta ordem da unidade, 1, -1, i *e* $-i$. *Suas multiplicidades são apresentadas na Tabela Tabela - 2.1 .* □

Embora a matriz da DFT possua, no máximo, quatros autovalores distintos, o respectivo operador é diagonalizável, uma vez que as multiplicidades algébricas desses autovalores coincidem com suas multiplicidades geométricas (dimensão do autoespaço ao qual cada autovalor está associado). Com isso, é possível construir bases para $\mathbb{R}^N$ formadas por autovetores de $\mathbf{F}$; na realidade, em função da repetição dos autovalores, há uma infinidade dessas bases, as quais motivam, de alguma forma, a concepção de diferentes estratégias para obtenção de autovetores de $\mathbf{F}$ relacionados a um autovalor específico. Duas dessas estratégias são apresentadas nas subseções que seguem.

Tabela Tabela - 2.1 – *Multiplicidade dos autovalores da matriz da DFT (m é um número inteiro).*

N	Mult. 1	Mul. $-i$	Mult. -1	Mult. 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

Construção de Autovetores da DFT: Abordagem Geral

Nesta seção, descreve-se como obter autovetores da matriz da DFT, relacionados a um autovalor específico dessa matriz, partindo de vetores arbitrários. Para tanto, considera-se a definição a seguir.

Definição 2.2 – Vetor par e vetor ímpar

O vetor $\mathbf{e} = (e[n])$, $n = 0, 1, \ldots, N-1$, *é um vetor par se* $e[n] = e[-n \pmod N]$; *o vetor* $\mathbf{o} = (o[n])$, $n = 0, 1, \ldots, N-1$, *é um vetor ímpar se* $e[n] = -e[-n \pmod N]$. □

Com isso, os resultados a seguir podem ser demonstrados [14].

Lema 2.1

Todos os autovetores da DFT são vetores pares ou vetores ímpares. Os autovetores pares têm como autovalor 1 *ou* -1, *e os autovetores ímpares têm como autovalor* i *ou* $-i$. □

De modo mais específico, tem-se:

Proposição 2.2

Seja $\mathbf{e} = (e[n])$, $n = 0, 1, \ldots, N-1$, *um vetor par e* $\mathbf{E} = (E[k])$, $k = 0, 1, \ldots, N-1$, *sua DFT. Então,* $\mathbf{u} = (u[n])$, *com* $u[n] = e[n] \pm E[n]$, $n = 0, 1, \ldots, N-1$, *é um autovetor da DFT associado ao autovalor* ± 1. □

Proposição 2.3

Seja $\mathbf{o} = (o[n])$, $n = 0, 1, \ldots, N-1$, *um vetor ímpar e* $\mathbf{O} = (O[k])$, $k = 0, 1, \ldots, N-1$, *sua DFT. Então,* $\mathbf{u} = (u[n])$, *com* $u[n] = o[n] \mp iO[n]$, $n = 0, 1, \ldots, N-1$, *é um autovetor da DFT associado ao autovalor* $\pm i$. □

Como um vetor par $\mathbf{e}$ com N componentes pode ser construído a partir de um vetor arbitrário $\mathbf{v} = (v[n])$ por meio de $e[n] = v[n] + v[-n \pmod N]$, $n = 0, 1, \ldots, N-1$, e, de modo semelhante, um vetor ímpar $\mathbf{o}$ com N componentes pode ser construído a partir de um vetor arbitrário $\mathbf{v} = (v[n])$ por meio de $e[n] = v[n] - v[-n \pmod N]$, $n = 0, 1, \ldots, N-1$, um autovetor da matriz da DFT associado a um autovalor específico pode ser construído, a partir de um vetor arbitrário $\mathbf{v}$, empregando a Proposição 2.2 ou a 2.3.

Construção de Autovetores da DFT via Matrizes Geradoras

Uma estratégia mais específica para construir autovetores da matriz da DFT é empregar as chamadas matrizes geradoras [7]. Este método merece um destaque particular, visto que, conforme mencionado na parte inicial desta dissertação, a principal contribuição deste trabalho é estender a referida técnica de construção de autovetores a certos tipos de transformadas trigonométricas discretas. A proposta consiste basicamente no seguinte:

dado um autovetor $\mathbf{v}$ da matriz da DFT relacionado a um autovalor $\lambda_{\mathbf{v}}$, mostra-se como obter uma matriz $\mathbf{S_A}$ tal que o vetor $\mathbf{v}' = \mathbf{S_A}\mathbf{v}$ seja também um autovetor da matriz da DFT associado a um autovalor $\lambda_{\mathbf{v}'}$; os autovalores $\lambda_{\mathbf{v}}$ e $\lambda_{\mathbf{v}'}$ não são necessariamente iguais.

A construção de matrizes geradoras de autovetores da DFT considera $\mathbf{J} = \mathbf{F}^2$ e $\mathbf{I} = \mathbf{F}^4$, em que

$$\mathbf{J} = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ \vdots & \cdots & 0 & 1 & 0 \\ \vdots & 0 & \iddots & \iddots & \vdots \\ 0 & 1 & 0 & \cdots & 0 \end{pmatrix} \tag{2.5}$$

e $\mathbf{I}$ é a matriz identidade; é necessária, ainda, uma matriz $\mathbf{A}$ que satisfaça

$$\mathbf{JAJ} = \lambda\mathbf{A}. \tag{2.6}$$

A matriz geradora $\mathbf{S_A}$ associada à matriz $\mathbf{A}$ é dada por

$$\mathbf{S_A} = \lambda^{1/2}\mathbf{F}^{-1}\mathbf{AF} + \mathbf{A}. \tag{2.7}$$

O principal resultado sobre a geração de autovetores da DFT empregando matrizes como $\mathbf{S_A}$ é enunciado a seguir.

Proposição 2.4

Seja $\mathbf{v}$ um autovetor da DFT com autovalor $\lambda_{\mathbf{v}}$. Então, $\mathbf{S_A}\mathbf{v}$ é um autovetor da DFT com autovalor $\lambda^{1/2}\lambda_{\mathbf{v}}$. □

2.2 Transformada discreta de Hartley

Nesta seção, são apresentados os principais resultados relacionados à autoestrutura da transformada discreta de Hartley (DHT, do inglês *discrete Hartley transform*). Inicia-se pela definição dessa transformada, a qual é dada a seguir.

Definição 2.3 – Transformada discreta de Hartley

A DHT de um vetor $\mathbf{x} = (x[n])$, com componentes $x[n] \in \mathbb{C}$, $n = 0, 1, \ldots, N-1$, é o vetor $\mathbf{X} = (X[k])$ com componentes

$$X[k] = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x[n]\mathrm{cas}\left(\frac{2\pi}{N}nk\right), \tag{2.8}$$

$k = 0, 1, \ldots, N-1$, em que $\mathrm{cas}(\cdot) = \cos(\cdot) + \mathrm{sen}(\cdot)$. □

Teorema 2.2 – Transformada discreta de Hartley inversa

A DHT inversa do vetor $\mathbf{X} = (X[k])$*, com componentes* $X[k] \in \mathbb{C}$*,* $k = 0, 1, \ldots, N-1$*, é o vetor* $\mathbf{x} = (x[n])$ *com componentes*

$$x[n] = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} X[k] \operatorname{cas}\left(\frac{2\pi}{N} nk\right), \tag{2.9}$$

$n = 0, 1, \ldots, N-1$. □

Pode-se relacionar um vetor $\mathbf{x}$ e a sua DHT $\mathbf{X}$ por meio da equação matricial

$$\mathbf{X} = \mathbf{H}\mathbf{x}, \tag{2.10}$$

em que a entrada na k-ésima linha e na n-ésima coluna da matriz $\mathbf{H}$ da DHT é dada por

$$H[k,n] = \frac{1}{\sqrt{N}} \operatorname{cas}\left(\frac{2\pi}{N} nk\right), \tag{2.11}$$

$k, n = 0, 1, \ldots, N-1$. Além disso, cabe observar que a DHT é uma involução, isto é, as expressões para calcular a transformada direta e a inversa coincidem. Equivalentemente, tem-se $\mathbf{H}^2 = \mathbf{I}$.

Autoestrutura da matriz da DHT

Os principais resultados a respeito da autoestrutura da matriz da DHT são enunciados a seguir [42].

Proposição 2.5

Os autovalores da matriz da DHT são 1 *e* -1*. Suas multiplicidades são listadas na Tabela Tabela - 2.2 .* □

Tabela Tabela - 2.2 – *Multiplicidades dos autovalores da matriz da DHT (m é um número inteiro).*

N	Mult. 1	Mult. -1
$4m$	$2m+1$	$2m-1$
$4m+1$	$2m+1$	$2m$
$4m+2$	$2m+1$	$2m+1$
$4m+3$	$2m+2$	$2m+1$

Proposição 2.6

Os autovetores da DHT com autovalor 1 *correspondem aos autovetores da DFT com autovalores* 1 *e* $-i$*; os autovetores da DHT com autovalor* -1 *correspondem aos autovetores da DFT com autovalores* -1 *e* i*.* □

A última proposição indica que, utilizando alguma das abordagens anteriormente apresentadas, pode-se construir autovetores da DFT e, naturalmente, esses serão também autovetores da DHT. Porém, autovetores da DHT podem ser diretamente obtidos de vetores arbitrários por meio do procedimento descrito a seguir, que consiste numa contribuição deste trabalho.

Proposição 2.7

Seja $\mathbf{v} = (v[n])$, $n = 0, 1, \ldots, N-1$, *um vetor arbitrário. Os vetores* $\mathbf{v}^+ = \mathbf{v} + \mathbf{Hv}$ *e o vetor* $\mathbf{v}^- = \mathbf{v} - \mathbf{Hv}$ *são autovetores da matriz da DHT com os autovalores* 1 *e* -1, *respectivamente.* □

Prova 2.1

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

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

Vale a pena ressaltar que o resultado da proposição 2.7, embora seja de simples demonstração, não se encontra apresentado explicitamente em [42], principal referência acerca da autoestrutura da matriz da DHT. A sua prova depende, basicamente, do fato de a matriz $\mathbf{H}$ ser involutiva. Isso permite, antecipadamente, afirmar que autovetores das matrizes da DCT e da DST dos tipos I e IV, que também são involuções (vide seções a seguir), também podem ser construídos usando a Proposição 2.7 com as respectivas matrizes de transformação substituindo $\mathbf{H}$.

2.3 Transformadas discretas do cosseno e do seno do tipo I

Nesta seção, são apresentados os principais resultados relacionados às autoestruturas das transformadas discretas do cosseno e do seno do tipo I, respectivamente referidas como DCT-I (do inglês *discrete cosine transform of type I*) e DST-I (do inglês *discrete sine transform of type I*).

Definição 2.4 – Transformada discreta do cosseno do tipo I

A DCT-I de um vetor $\mathbf{x} = (x[n])$, *com componentes* $x[n] \in \mathbb{C}$, $n = 0, 1, \ldots, N-1$, *é o*

vetor $\mathbf{X} = (X[k])$ *com componentes*

$$X[k] = \sqrt{\frac{2}{N'}} \sum_{n=0}^{N'} x[n]\beta[n]\cos\left(\frac{kn\pi}{N'}\right),$$

$k = 0, 1, \ldots, N'$, *em que*

$$\beta[n] = \begin{cases} \frac{1}{\sqrt{2}}, & n = 0 \text{ e } n = N', \\ 1, & \text{caso contrário.} \end{cases}$$

□

Teorema 2.3 – Transformada discreta do cosseno do tipo I Inversa

A DCT-I inversa de um vetor $\mathbf{X} = (X[k])$, *com componentes* $X[k] \in \mathbb{C}$, $k = 0, 1, \ldots, N$, *é o vetor* $\mathbf{x} = (x[n])$ *com componentes*

$$x[n] = \sqrt{\frac{2}{N'}} \sum_{k=0}^{N'} X[k]\beta[k]\cos\left(\frac{kn\pi}{N'}\right), \tag{2.12}$$

$n = 0, 1, \ldots, N'$. □

Definição 2.5 – Transformada discreta do seno do tipo I

A DST-I de um vetor $\mathbf{x} = (x[n])$, *com componentes* $x[n] \in \mathbb{C}$, $n = 0, 1, \ldots, N-1$, *é o vetor* $\mathbf{X} = (X[k])$ *com componentes*

$$X[k] = \sqrt{\frac{2}{N}} \sum_{n=0}^{N-1} x[n]\operatorname{sen}\left(\frac{kn\pi}{N}\right), \tag{2.13}$$

$k = 0, 1, \ldots, N-1$. □

Teorema 2.4 – Transformada discreta do seno do tipo I inversa

A DST-I inversa de um vetor $\mathbf{X} = (X[k])$, *com componentes* $X[k] \in \mathbb{C}$, $k = 0, 1, \ldots, N-1$, *é o vetor* $\mathbf{x} = (x[n])$ *com componentes*

$$x[n] = \sqrt{\frac{2}{N}} \sum_{k=0}^{N-1} X[k]\operatorname{sen}\left(\frac{kn\pi}{N}\right), \tag{2.14}$$

$n = 0, 1, \ldots, N-1$. □

De forma análoga ao que se apresentou anteriormente para as transformadas discretas de Fourier e de Hartley, a relação entre um vetor e a sua transformada discreta do cosseno ou do seno do tipo I também pode ser expressa por meio de uma equação matricial. As matrizes

da DCT-I e da DST-I são denotadas, respectivamente, por $\mathbf{C}_I$ e $\mathbf{S}_I$, e têm suas entradas dadas pelas expressões apresentadas nas definições das transformadas correspondentes. Assim como a DHT, a DCT-I e a DST-I também são involuções. Dessa forma, tem-se $\mathbf{C}_I^2 = \mathbf{S}_I^2 = \mathbf{I}$.

Autoestruturas das matrizes da DCT-I e da DST-I

Em [43], são demonstradas algumas propriedades da autoestrutura da DCT-I e da DST-I. Os principais resultados desenvolvidos no referido trabalho são revisados a seguir.

Proposição 2.8

Os autovalores da matriz da DCT-I *e da matriz da* DST-I *são* 1 *e* -1*. Suas multiplicidades são listadas na Tabela Tabela - 2.3 .* □

Tabela Tabela - 2.3 – *Multiplicidades dos autovalores das matrizes da DCT-I e da DST-I.*

N	Mult. 1	Mult. -1
Ímpar	$\frac{N+1}{2}$	$\frac{N-1}{2}$
Par	$\frac{N}{2}$	$\frac{N}{2}$

Proposição 2.9

Seja $\mathbf{v} = (v[0], v[1], \ldots, v[N-2], v[N-1], v[N-2], \ldots, v[1])^T$ *um autovetor par de comprimento* $2N-2$ *da DFT, associado ao autovalor* $\lambda_{\mathbf{F}} = \pm 1$*. Então*

$$\mathbf{v}_{\mathbf{C}_I} = \Big(v[0], \sqrt{2}v[1], \ldots, \sqrt{2}v[N-2], v[N-1]\Big)^T \tag{2.15}$$

é um autovetor de comprimento N *da DCT-I, associado ao autovalor* $\lambda_{\mathbf{C}_I} = \pm 1$*.* □

Proposição 2.10

Seja $\mathbf{v} = (0, v[1], v[2], \ldots, v[N], 0, -v[N], -v[N-1], \ldots, -v[1])^T$ *um autovetor ímpar de comprimento* $2N+2$ *da DFT, associado ao autovalor* $\lambda_{\mathbf{F}} = \mp i$*. Então*

$$\mathbf{v}_{\mathbf{S}_I} = \sqrt{2}\,(v[1], v[2], \ldots, v[N])^T \tag{2.16}$$

é um autovetor de comprimento N *da DST-I, associado ao autovalor* $\lambda_{\mathbf{S}_I} = \pm 1$*.* □

2.4 Transformadas discretas do cosseno e do seno do tipo IV

Nesta seção, são apresentados os principais resultados relacionados às autoestruturas das transformadas discretas do cosseno e do seno do tipo IV, respectivamente referidas

como DCT-IV (do inglês *discrete cosine transform of type IV*) e DST-IV (do inglês *discrete sine transform of type IV*). As transformadas da DHT, a DCT-I e a DST-I têm suas autoestruturas relacionadas à autoestrutura da DFT, e as transformadas da DCT-IV e a DST-IV têm suas autoestruturas relacionadas à autoestrutura da DFT generalizada (GDFT, do inglês *generalized discrete Fourier transform*). Por este motivo, inicia-se esta seção apresentando a definição desta última transformada.

Definição 2.6 – Transformada discreta de Fourier generalizada

A GDFT de um vetor $\mathbf{x} = (x[n])$*, com componentes* $x[n] \in \mathbb{C}$*,* $n = 0, 1, \ldots, N-1$*, é o vetor* $\mathbf{X} = (X[k])$ *com componentes*

$$X[k] = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x[n] W_N^{(n+0,5)(k+0,5)}, \tag{2.17}$$

$k = 0, 1, \ldots, N-1$. □

Teorema 2.5 – Transformada discreta de Fourier generalizada inversa

A GDFT inversa de um vetor $\mathbf{X} = (X[k])$*, com componentes* $X[k] \in \mathbb{C}$*,* $k = 0, 1, \ldots, N-1$*, é o vetor* $\mathbf{x} = (x[n])$ *com componentes*

$$x[n] = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} X[K] W_N^{-(n+0,5)(k+0,5)}, \tag{2.18}$$

$n = 0, 1, \ldots, N-1$. □

A matriz da GDFT é denotada por $\mathbf{G}$ e tem suas entradas dadas por

$$G[k,n] = \frac{1}{\sqrt{N}} W_N^{(n+0,5)(k+0,5)}, \tag{2.19}$$

$k, n = 0, 1, \ldots, N-1$.

A seguir, são apresentadas as principais propriedades dos autovalores e autovetores da GDFT [44].

Proposição 2.11

Os autovalores da matriz da GDFT são 1*,* -1*,* i *e* $-i$*. Suas multiplicidades são listadas na Tabela Tabela - 2.4 .* □

Proposição 2.12

Seja $\mathbf{v}$ *um autovetor da GDFT. Se* $\mathbf{v}$ *for par, seu autovalor associado será* i *ou* $-i$*; se* $\mathbf{v}$ *for ímpar, seu autovalor associado será* 1 *ou* -1*.* □

Tabela Tabela - 2.4 – *Multiplicidades dos autovalores da GDFT (m é um número inteiro).*

N	Mult. 1	Mult. $-i$	Mult. -1	Mult. i
$4m$	m	m	m	m
$4m+1$	m	m	m	$m+1$
$4m+2$	$m+1$	m	m	$m+1$
$4m+3$	$m+1$	m	$m+1$	$m+1$

Uma das maneiras de construir autovetores da GDFT é considerar matrizes comutantes com $\mathbf{G}$, uma vez que duas matrizes que comutam têm pelo menos um conjunto de autovetores em comum [44]. Se a referida matriz comutante possuir todos os autovalores distintos, esta possuirá um conjunto único de autovetores; para formar tal conjunto, basta que se tome um autovetor associado a cada autovalor. Como a dimensão de cada autoespaço é unitária, dois autovetores de um mesmo autoespaço diferem apenas pelo produto por um fator de escala. Considerar uma matriz comutante com esta propriedade permite estabelecer um critério para tratar a ambiguidade oriunda de se ter infinitos conjuntos completos de autovetores de $\mathbf{G}$: basta que se tome o conjunto único de autovetores da matriz comutante como o conjunto completo em questão. Isso acontece se a matriz comutante for, por exemplo,

$$\mathbf{S_G} = \begin{bmatrix} 2\cos(\omega) & 1 & 0 & \dots & 0 & -1 \\ 1 & 2\cos(3\omega) & 1 & \dots & 0 & 0 \\ 0 & 1 & 2\cos(5\omega) & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 2\cos((2N-3)\omega) & 1 \\ -1 & 0 & 0 & \dots & 1 & 2\cos((2N-1)\omega) \end{bmatrix}, \tag{2.20}$$

em que $\omega = (\pi/N)$. Detalhes sobre como construir autovetores da GDFT podem ser verificados em [44].

Definição 2.7 – Transformada discreta do cosseno do tipo IV

A DCT-IV de um vetor $\mathbf{x} = (x[n])$*, com componentes* $x[n] \in \mathbb{C}$*,* $n = 0, 1, \dots, N-1$*, é o vetor* $\mathbf{X} = (X[k])$ *com componentes*

$$X[k] = \sqrt{\frac{2}{N}} \sum_{n=0}^{N-1} x[n] \cos\left(\frac{\pi(n+0,5)(k+0,5)}{N}\right), \tag{2.21}$$

$k = 0, 1, \ldots, N-1$. □

Teorema 2.6 – Transformada discreta do cosseno do tipo IV inversa

A DCT-IV inversa de um vetor $\mathbf{X} = (X[k])$*, com componentes* $X[k] \in \mathbb{C}$*,* $k = 0, 1, \ldots, N-1$*, é o vetor* $\mathbf{x} = (x[n])$ *com componentes*

$$x[n] = \sqrt{\frac{2}{N}} \sum_{k=0}^{N-1} X[k] \cos\left(\frac{\pi(n+0,5)(k+0,5)}{N}\right) \tag{2.22}$$

$n = 0, 1, \ldots, N-1$. □

Definição 2.8 – Transformada discreta do seno do tipo IV

A DST-IV de um vetor $\mathbf{x} = (x[n])$*, com componentes* $x[n] \in \mathbb{C}$*,* $n = 0, 1, \ldots, N-1$*, é o vetor* $\mathbf{X} = (X[k])$ *com componentes*

$$X[k] = \sqrt{\frac{2}{N}} \sum_{n=0}^{N-1} x[n] \operatorname{sen}\left(\frac{(\pi(n+0,5)(k+0,5)}{N}\right), \tag{2.23}$$

$k = 0, 1, \ldots, N-1$. □

Teorema 2.7 – Transformada discreta do seno do tipo IV inversa

A DST-IV inversa de um vetor $\mathbf{X} = (X[k])$*, com componentes* $X[k] \in \mathbb{C}$*,* $k = 0, 1, \ldots, N-1$*, é o vetor* $\mathbf{x} = (x[n])$ *com componentes*

$$x[n] = \sqrt{\frac{2}{N}} \sum_{n=0}^{N-1} X[k] \operatorname{sen}\left(\frac{(\pi(n+0,5)(k+0,5)}{N}\right), \tag{2.24}$$

$n = 0, 1, \ldots, N-1$. □

De forma análoga ao que se apresentou anteriormente para as transformadas discretas de Fourier, de Hartley, do cosseno e do seno do tipo I, a relação entre um vetor e a sua transformada discreta do cosseno ou do seno do tipo IV também pode ser expressa por meio de uma equação matricial. As matrizes da DCT-IV e da DST-IV são denotadas, respectivamente, por $\mathbf{C}_{IV}$ e $\mathbf{S}_{IV}$, e têm suas entradas dadas pelas expressões apresentadas nas definições das transformadas correspondentes. Assim como a DHT, a DCT-I e a DST-I, a DCT-IV e a DST-IV também são involuções. Dessa forma, tem-se $\mathbf{C}_{IV}^2 = \mathbf{S}_{IV}^2 = \mathbf{I}$.

Autoestrutura da matrizes da DCT-IV e da DST-IV

Nesta seção, são apresentadas algumas propriedades importantes das autoestruturas da DCT-IV e da DST-IV.

Proposição 2.13

Os autovalores da matriz da DCT-IV e da matriz da DST-IV são $\lambda = \pm 1$*. Suas multiplicidades são listadas na Tabela Tabela - 2.5 .* □

Tabela Tabela - 2.5 – *Multiplicidades dos autovalores da matriz da DCT-IV e da matriz da DST-IV.*

N	Mult. 1	Mult. -1
$2m$	m	m
$2m+1$	$m+1$	m

Proposição 2.14

Seja $\mathbf{v}$ *um vetor ímpar, definido como* $\mathbf{v} = (v[0], \ldots, v[N-1], -v[N-1], \ldots, -v[0])^T$*. Se* $\mathbf{v}$ *é um autovetor de comprimento* $2N$ *da matriz da GDFT, então o vetor* $\mathbf{v}_{\mathbf{C}_{IV}} = (v[0], v[1], \ldots, v[N-1])^T$ *é um autovetor de comprimento* N *da matriz da DCT-IV.*

Proposição 2.15

Seja $\mathbf{v}$ *um vetor par, definido como* $\mathbf{v} = (v[0], \ldots, v[N-1], v[N-1], \ldots, v[0])^T$*. Se* $\mathbf{v}$ *é um autovetor de comprimento* $2N$ *da matriz da GDFT, então o vetor reduzido* $\mathbf{v}_{\mathbf{S}_{IV}} = (v[0], v[1], \ldots, v[N-1])^T$ *é um autovetor de comprimento* N *da matriz da DST-IV.* □

3 Construção de Autovetores de Transformadas Trigonométricas Discretas Baseada em Matrizes Geradoras

Neste capítulo, é apresentada a principal contribuição desta dissertação: um método baseado em matrizes geradoras para construção de autovetores de transformadas trigonométricas discretas. As transformadas contempladas pelo método são a transformada discreta de Hartley e as transformadas discretas do cosseno e do seno dos tipos I e IV. Conforme previamente indicado em capítulos anteriores deste trabalho, o que basicamente se propõe é um método para construir uma matriz $\mathbf{S_A}$, tal que, dado um autovetor $\mathbf{v}$ de uma das transformadas mencionadas, associado ao autovalor λ_v, obtém-se um outro autovetor $\mathbf{v}' = \mathbf{S_A}\mathbf{v}$ da mesma transformada, associado a um autovalor $\lambda_{v'}$ possivelmente diferente de λ_v.

Comparando o método proposto com o método correspondente para geração de autovetores da transformada discreta de Fourier [7], a principal distinção é que a matriz $\mathbf{A}$, a qual origina a matriz $\mathbf{S_A}$ geradora de autovetores das transformadas trigonométricas, não possui restrições como aquela dada em (2.6). Isso significa que, no presente caso, todas as N^2 entradas de $\mathbf{A}$ podem ser escolhidas independentemente, não sendo necessário respeitar certas condições de simetria requeridas quando da geração de autovetores da DFT. Tal possibilidade é particularmente importante quando o objetivo é utilizar essas entradas como componentes de uma chave-secreta em esquemas criptográficos baseados nessas transformadas, pois o tamanho da chave é incrementado.

Ainda neste capítulo, são propostos procedimentos sistemáticos para obter conjuntos de autovetores de uma transformada trigonométrica específica produzidos por meio do método proposto. Tal caracterização tem o propósito de atender as condições necessárias para que os referidos conjuntos formem bases a serem empregadas na diagonalização das matrizes das transformadas correspondentes. As expansões espectrais obtidas são, então, utilizadas para definir versões fracionárias das respectivas transformadas. Por fim, são indicadas estratégias para que tais versões fracionárias sejam representadas por operadores matriciais com componentes reais.

3.1 Matrizes geradoras de autovetores de transformadas trigonométricas discretas

Seja $\mathbf{M}$ uma matriz correspondente à matriz de transformação da DCT-I ou -IV, da DST-I ou -IV, ou da DHT. Conforme indicado no Capítulo 2, cada uma dessas transformadas corresponde a uma involução, isto é, o cálculo da transformada direta e o da inversa são realizados empregando a mesma expressão. Equivalentemente, pode-se escrever

$$\mathbf{M}^{-1} = \mathbf{M} \quad \text{ou} \quad \mathbf{M}^2 = \mathbf{I}. \tag{3.1}$$

A propriedade 3.1 é empregada na demonstração da proposição a seguir, a qual constitui o principal resultado deste capítulo.

Proposição 3.1

Seja $\mathbf{A}$ *uma matriz* $N \times N$ *e* $\mathbf{v}$ *um autovetor de* $\mathbf{M}$ *com o autovalor* λ*. Então,* $\mathbf{v}' = \mathbf{S_A v}$*, em que* $\mathbf{S_A}$ *é a matriz geradora dada por*

$$\mathbf{S_A} = \pm\mathbf{MAM} + \mathbf{A},$$

é um autovetor de $\mathbf{M}$ *com autovalor* $\pm\lambda$*.* □

Prova 3.1

Considerando $\mathbf{S_A} = -\mathbf{MAM} + \mathbf{A}$*, obtém-se o seguinte desenvolvimento:*

$$\begin{aligned} \mathbf{MS_A v} &= \mathbf{M}(-\mathbf{MAM} + \mathbf{A})\mathbf{v} \\ &= -\mathbf{AMv} + \mathbf{MAv}. \end{aligned}$$

Como $\mathbf{Mv} = \lambda\mathbf{v}$*, tem-se, da última expressão:*

$$\begin{aligned} &= -\mathbf{A}\lambda\mathbf{v} + \mathbf{MAM^2 v} \\ &= -\mathbf{A}\lambda\mathbf{v} + \mathbf{MAM}\lambda\mathbf{v} \\ &= -\lambda(\mathbf{A} - \mathbf{MAM})\mathbf{v} \\ &= -\lambda(\mathbf{S_A v}) \\ &= -\lambda\mathbf{v}'. \end{aligned}$$

Um desenvolvimento similar pode ser obtido se considerar $\mathbf{S_A} = \mathbf{MAM} + \mathbf{A}$*.* □

Da Proposição 3.1, considerando as transformadas para as quais os únicos autovalores possíveis são 1 e -1, conclui-se que há duas possibilidades para geração de um novo

autovetor a partir de um autovetor dado: a primeira consiste em construir a matriz geradora $\mathbf{S_A} = \mathbf{MAM} + \mathbf{A}$ e, dado um autovetor $\mathbf{v}$ com o autovalor ± 1, obter o autovetor $\mathbf{v}' = \mathbf{S_A v}$ com o mesmo autovalor ± 1; a segunda consiste em construir a matriz geradora $\mathbf{S_A} = -\mathbf{MAM} + \mathbf{A}$ e, dado um autovetor $\mathbf{v}$ com o autovalor ± 1, obter o autovetor $\mathbf{v}' = \mathbf{S_A v}$ com o autovalor ∓ 1. O uso recursivo de uma ou de outra possibilidade permite a obtenção de conjuntos de autovetores, conforme explicado a seguir.

Pode-se construir um conjunto $\{\mathbf{v}_r\}_{r=0,1,\ldots,N-1}$ com N autovetores de $\mathbf{M}$ escolhendo uma matriz $\mathbf{A}$, a partir da qual se obtenha $\mathbf{S_A}$, um autovetor de partida $\mathbf{v}_0$ e calculando, para $r = 1, 2, \ldots, N-1$,

$$\mathbf{v}_r = \mathbf{S_A v}_{r-1}. \tag{3.2}$$

Se utilizar $\mathbf{S_A} = -\mathbf{MAM} + \mathbf{A}$, são criados autovetores cujos autovalores associados 1 e -1 se alternam. Assim, abre-se uma possibilidade para que esses autovetores formem uma base de $\mathbb{R}^N$; para isso, a condição fornecida a seguir é necessária.

Proposição 3.2

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,

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

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 3.2 é apenas necessária, ainda que ela seja satisfeita, ao se obter um conjunto $\{\mathbf{v}_r\}_{r=0,1,\ldots,N-1}$ pela multiplicação recursiva entre uma matriz geradora e um autovetor, sua possível independência linear precisa ser verificada. De qualquer forma, para as transformadas trigonométricas discretas em questão, exceto para a DHT de comprimento $N = 4m$[1], a construção de uma base para $\mathbb{R}^N$, formada por

[1] Este caso será tratado separadamente.

autovetores obtidos por meio de matrizes geradoras, pode ser realizada conforme os passos a seguir.

1. Construa um autovetor $\mathbf{v}_0$ com o autovalor 1 da transformada trigonométrica discreta escolhida usando algum método descrito no Capítulo 2. Para as transformadas que correspondem a uma involução, isso pode ser feito usando a Proposição 2.7.
2. Escolha uma matriz arbitrária $\mathbf{A}$, com dimensão $N \times N$, para criação da matriz geradora $\mathbf{S_A} = -\mathbf{MAM} + \mathbf{A}$ (Proposição 3.1);
3. Obtenha, para $r = 1, 2, 3, \ldots, N-1$, os autovetores

$$\mathbf{v}_r = \mathbf{S_A}\mathbf{v}_{r-1} \tag{3.3}$$

   e verifique se o conjunto $\{\mathbf{v}_r\}_{r=0,\ldots,N-1}$ é LI;
4. Se o conjunto gerado no passo anterior for LI e se se desejar que ele seja também ortogonal, aplique algum processo de ortogonalização (o algoritmo de Gram-Schmidt, por exemplo); o referido processo pode ser aplicado em separado a subconjuntos contendo todos os autovetores associados a um mesmo autovalor. Normalizando os vetores resultantes, obtém-se, finalmente, o conjunto identificado por $\{\widetilde{\mathbf{v}}_r\}_{r=0,\ldots,N-1}$ e que corresponde a uma base ortonormal para $\mathbb{R}^N$.

A seguir, são apresentados exemplos de construção de bases formadas por autovetores das transformadas trigonométricas discretas consideradas.

Exemplo 3.1

Construção de uma base para $\mathbb{R}^8$ formada por autovetores da matriz da DCT-I: seja $\mathbf{u}$ um vetor 8-dimensional arbitrário dado por

$$\mathbf{u} = \begin{pmatrix} -0,9362 & -0,2333 & 0,4641 & -0,7027 & 0,6332 & -0,9088 & -0,7817 & 0,3529 \end{pmatrix}.$$

Utilizando um procedimento como aquele descrito na Proposição 2.7, gera-se o autovetor $\mathbf{v}_0 = \mathbf{u} + \mathbf{C}_I\mathbf{u}$ da DCT-I, associado ao autovalor 1 e dado por

$$\mathbf{v}_0 = \begin{pmatrix} -1,6702 & -0,1577 & -0,0083 & -1,3407 & 0,7245 & -2,3856 & -0,6533 & 0,8249 \end{pmatrix}.$$

Para obter a matriz geradora de autovetores da DCT-I, constrói-se de forma arbitrária

a matriz $\mathbf{A}$*, de tamanho* 8×8*, dada por*

$$\mathbf{A} = \begin{pmatrix} -0,9489 & -0,9736 & -0,4544 & -0,3295 & 0,0679 & -0,2498 & -0,8748 & 0,9705 \\ -0,7768 & 0,9620 & -0,6114 & 0,2044 & 0,5858 & 0,6756 & 0,4005 & -0,0343 \\ -0,1763 & -0,2625 & -0,9160 & 0,0642 & -0,9876 & -0,0555 & 0,1883 & 0,3082 \\ 0,0149 & 0,8987 & 0,0256 & 0,4043 & 0,5459 & -0,1717 & -0,9302 & 0,1126 \\ 0,1182 & -0,4902 & 0,9053 & 0,7073 & -0,1234 & -0,6239 & 0,9249 & -0,2368 \\ 0,8040 & 0,3472 & -0,0104 & -0,6259 & -0,8381 & -0,0493 & 0,2640 & 0,7560 \\ -0,1266 & -0,6850 & -0,4423 & 0,6897 & 0,9483 & -0,9249 & 0,6235 & 0,0280 \\ -0,9571 & -0,6627 & -0,1428 & 0,4821 & -0,0417 & 0,2062 & -0,8980 & 0,3136 \end{pmatrix}.$$

Utilizando a Proposição 3.1, encontra-se a matriz geradora de autovetores $\mathbf{S_A}$*, dada por*

$$\mathbf{S_A} = \begin{pmatrix} -1,0735 & -1,5333 & -0,6160 & -0,9564 & 0,8229 & -0,3813 & -1,2044 & 0,4783 \\ -0,9632 & 0,7005 & -0,5059 & 0,7199 & 0,1760 & 0,0934 & 0,1240 & -0,9913 \\ -0,8703 & -1,5091 & -1,6977 & 0,2254 & -0,6976 & -0,7018 & 0,1867 & -0,1927 \\ 0,3192 & 0,7707 & 0,8052 & 0,1530 & 0,3011 & -0,1935 & -0,6583 & 0,8524 \\ -0,0091 & -0,319 & -0,7193 & 0,1300 & -0,0308 & -1,3042 & 1,3053 & -0,2030 \\ 0,4594 & 0,6246 & 0,0817 & -0,3599 & 0,0015 & -0,8532 & 0,6040 & 0,7428 \\ -1,3728 & -0,9462 & 0,2513 & 0,2725 & 0,7446 & -0,9931 & 2,0282 & -0,6929 \\ -1,5467 & -1,3789 & -0,4308 & -0,3564 & 0,4847 & 1,0845 & -0,9654 & 1,3051 \end{pmatrix}.$$

Os autovetores $\{\mathbf{v}_r\}_{r=1,\ldots,N-1}$ *são construídos a partir de* $\mathbf{v}_0$ *e* $\mathbf{S_A}$ *conforme descrito no passo 3 do procedimento que se acabou de apresentar. Um processo de ortogonalização de Gram-Schmidt é então aplicado ao conjunto* $\{\mathbf{v}_r\}_{r=0,\ldots,N-1}$*. Se nenhum vetor tiver sido anulado (como ocorre neste exemplo), o conjunto resultante, após a normalização dos vetores obtidos, é identificado por* $\{\tilde{\mathbf{v}}_r\}_{r=0,\ldots,N-1}$ *e constitui uma base ortonormal. Esses vetores são apresentados nas linhas da matriz*

$$\mathbf{V}^T = \begin{pmatrix} -0,5224 & 0,5441 & -0,3655 & 0,3969 & -0,2227 & 0,2032 & -0,1574 & 0,1554 \\ 0,3253 & -0,4942 & -0,2529 & 0,1830 & -0,4182 & 0,3169 & -0,3967 & 0,3457 \\ 0,6178 & 0,4814 & 0,3795 & 0,4183 & 0,1116 & 0,1954 & 0,0087 & 0,1288 \\ -0,4879 & -0,3285 & 0,6757 & 0,2761 & 0,1286 & 0,2385 & -0,0554 & 0,2109 \\ -0,5517 & 0,2206 & -0,4229 & 0,3954 & -0,5333 & 0,1379 & -0,0862 & 0,0275 \\ -0,1281 & 0,3982 & -0,1629 & 0,4476 & 0,6378 & -0,2179 & 0,3531 & -0,1377 \\ 0,1595 & 0,0153 & -0,0726 & 0,2742 & 0,2881 & 0,2736 & -0,8063 & -0,2927 \\ -0,2538 & -0,0593 & -0,4068 & -0,4269 & 0,3970 & 0,5863 & 0,0807 & 0,2760 \end{pmatrix}.$$

□

Exemplo 3.2

Construção de uma base para $\mathbb{R}^8$ *formada por autovetores da matriz da DST-I: seja* $\mathbf{u}$ *um vetor* 8*-dimensional arbitrário dado por*

$$\mathbf{u} = \begin{pmatrix} -0,8385 & 0,6785 & 0,9244 & -0,6528 & 0,6146 & -0,1355 & 0,8641 & -0,2469 \end{pmatrix}.$$

Utilizando um procedimento como aquele descrito na Proposição 2.7, gera-se o autovetor $\mathbf{v}_0 = \mathbf{u} + \mathbf{S}_I\mathbf{u}$ *da DST-I, associado ao autovalor* 1 *e dado por*

$$\mathbf{v}_0 = \begin{pmatrix} -0,2416 & 0,6415 & 1,1267 & -1,0060 & -0,4715 & -0,8187 & 0,1472 & 0,7350 \end{pmatrix}.$$

Usando a mesma matriz $\mathbf{A}$ *do Exemplo (3.1), encontra-se, a partir da Proposição 3.1, a matriz geradora*

$$\mathbf{S_A} = \begin{pmatrix} -1,4220 & -1,2630 & -0,6083 & -0,5880 & 0,8307 & 0,2436 & -0,2848 & -0,2005 \\ -0,3737 & -0,2507 & 0,5864 & 0,1814 & 0,2723 & -1,4360 & -0,4415 & 0,4802 \\ 0,3810 & 0,6704 & -1,2540 & -0,8655 & 0,3115 & 0,1361 & 0,6478 & 0,7825 \\ -0,1874 & -1,2640 & -0,3617 & 0,1479 & -1,1390 & -0,6982 & -0,4628 & 0,2129 \\ -1,0970 & -0,0563 & -2,1250 & -0,0410 & 0,8004 & 0,1811 & 0,1807 & 0,0030 \\ 0,2883 & -1,0590 & 0,0693 & -0,3043 & -1,2610 & -0,1239 & 0,5483 & -0,3099 \\ -0,9420 & -0,2633 & 0,5176 & 1,0260 & 0,2594 & 0,7184 & 0,2626 & 0,3573 \\ 1,1430 & -1,6710 & 0,0528 & 1,3040 & -0,1919 & -1,6440 & -1,3530 & -0,6479 \end{pmatrix}.$$

A base ortonormal obtida, aplicando o procedimento descrito anteriormente, é formada pelos autovetores da DST-I apresentados nas linhas da matriz

$$\mathbf{V}^T = \begin{pmatrix} -0,1476 & 0,2166 & 0,6414 & -0,5873 & -0,3766 & -0,0703 & -0,0308 & -0,1647 \\ -0,3883 & -0,0432 & 0,2209 & 0,2512 & 0,1174 & -0,3030 & 0,7929 & -0,0321 \\ 0,0493 & 0,4462 & 0,4776 & 0,6940 & -0,0283 & 0,1771 & -0,2342 & -0,0393 \\ -0,2117 & -0,2259 & 0,1847 & -0,1001 & 0,1198 & 0,8504 & 0,1835 & 0,2978 \\ -0,7222 & 0,4942 & -0,4289 & -0,0391 & -0,1329 & 0,0660 & -0,1470 & 0,0699 \\ -0,4166 & -0,3478 & 0,3016 & -0,0088 & 0,4952 & -0,3012 & -0,4843 & 0,2090 \\ -0,2095 & -0,5343 & -0,0099 & 0,3082 & -0,7397 & -0,0528 & -0,1338 & 0,0863 \\ 0,2025 & 0,2240 & 0,0487 & -0,0590 & -0,1380 & -0,2253 & 0,0876 & 0,9085 \end{pmatrix}.$$

□

Exemplo 3.3

Construção de uma base para $\mathbb{R}^8$ *formada por autovetores da matriz da DCT-IV: seja* $\mathbf{u}$ *um vetor* 8*-dimensional arbitrário dado por*

$$\mathbf{u} = \begin{pmatrix} -0,8738 & -0,4453 & -0,3588 & 0,9020 & -0,5274 & 0,9961 & 0,2202 & 0,1955 \end{pmatrix}.$$

Utilizando um procedimento como aquele descrito na Proposição 2.7, gera-se o autovetor $\mathbf{v}_0 = \mathbf{u} + \mathbf{C}_{IV}\mathbf{u}$ *da DCT-IV, associado ao autovalor* 1 *e dado por*

$$\mathbf{v}_0 = \begin{pmatrix} -1,2223 & -1,6115 & -0,5107 & 0,6082 & -0,4306 & 1,5909 & -0,3626 & -0,7884 \end{pmatrix}.$$

Usando a mesma matriz aleatória $\mathbf{A}$ *dos exemplos anteriores, obtém-se a matriz gera-*

dora

$$\mathbf{S_A} = \begin{pmatrix} -0,0796 & -0,6966 & -0,7841 & -0,6924 & 0,4605 & 0,3655 & 1,0910 & -1,2810 \\ 0,5382 & -0,6313 & -0,3664 & -0,7002 & 0,0881 & 0,1312 & -0,8323 & 0,7827 \\ 1,4810 & 2,0180 & -0,5732 & -0,0187 & -1,0300 & -1,5970 & -0,4684 & -0,3178 \\ -0,3317 & 1,6430 & -0,2132 & 0,2124 & 0,9067 & -0,4027 & -0,1469 & -1,4990 \\ -0,0564 & 0,8098 & 0,0013 & -1,0650 & 1,1730 & 0,7640 & 1,4380 & -0,5174 \\ 0,0942 & -1,0090 & 0,5846 & 1,3630 & -0,4035 & -1,0590 & 0,7311 & -0,6166 \\ -0,7692 & -1,0760 & 0,0726 & -1,0090 & -0,9032 & 0,9302 & 1,3560 & 0,0206 \\ 0,4724 & 0,3233 & -2,1130 & 1,7630 & 1,4450 & -0,6230 & -0,9481 & -0,3981 \end{pmatrix}.$$

Procedendo de forma análoga aos exemplos anteriores, obtém-se uma base ortonormal formada pelos autovetores da DCT-IV apresentados nas linhas da matriz

$$\mathbf{V}^T = \begin{pmatrix} -0,4936 & 0,1779 & 0,7859 & -0,0623 & -0,1622 & -0,1829 & 0,0028 & 0,2080 \\ -0,7668 & -0,4929 & -0,3234 & 0,1403 & 0,1842 & 0,0575 & 0,0617 & 0,0595 \\ -0,1251 & -0,0352 & 0,2023 & 0,0676 & -0,2679 & 0,5257 & 0,1124 & -0,7594 \\ 0,0951 & -0,1840 & 0,3132 & -0,2017 & 0,6888 & 0,3125 & -0,4944 & -0,0415 \\ 0,0068 & 0,2106 & 0,1049 & 0,5982 & 0,4959 & -0,4114 & 0,2064 & -0,3589 \\ 0,3534 & -0,7339 & 0,3197 & 0,3972 & -0,2341 & -0,0964 & -0,0146 & 0,1100 \\ 0,1325 & -0,2047 & 0,1546 & -0,4175 & 0,2933 & 0,0509 & 0,8073 & 0,0429 \\ 0,0313 & 0,2556 & 0,0380 & 0,4910 & 0,0812 & 0,6387 & 0,2109 & 0,4815 \end{pmatrix}.$$

□

Exemplo 3.4

Construção de uma base para $\mathbb{R}^8$ *formada por autovetores da matriz da DST-IV: seja* $\mathbf{u}$ *um vetor* 8*-dimensional arbitrário dado por*

$$\mathbf{u} = \begin{pmatrix} 0,6071 & -0,9221 & 0,1596 & -0,3290 & 0,3591 & -0,7413 & -0,2932 & 0,9285 \end{pmatrix}.$$

Utilizando um procedimento como aquele descrito na Proposição 2.7, gera-se o autovetor $\mathbf{v}_0 = \mathbf{u} + \mathbf{S}_{IV}\mathbf{u}$ *da DST-IV, associado ao autovalor* 1 *e dado por*

$$\mathbf{v}_0 = \begin{pmatrix} 0,5699 & -1,486 & 0,4520 & -1,2030 & 1,0260 & -0,8295 & -0,0595 & 2.0700 \end{pmatrix}.$$

Usando a mesma matriz ateatória $\mathbf{A}$ *dos exemplos anteriores, obtém-se a matriz geradora*

$$\mathbf{S_A} = \begin{pmatrix} -0,5083 & -0,7706 & 0,0238 & -0,0705 & 0,9196 & -1,0970 & 1,0180 & -0,6396 \\ 0,2786 & 0,0887 & -0,5318 & -1,1320 & -0,6628 & -0,2208 & 0,5677 & 0,9786 \\ 1,7920 & 1,2200 & -1,3220 & 0,2806 & -1,3370 & -0,7826 & -0,4863 & 0,0329 \\ -1,3260 & 0,9446 & 0,0105 & 0,5803 & 1,0220 & -0,4554 & -0,4228 & -1,4250 \\ -0,4977 & 0,8769 & 0,6607 & -0,8599 & 0,3519 & 0,9595 & 1,8460 & -0,3861 \\ 0,1984 & -0,6559 & 0,9807 & 1,1700 & 1,2470 & 0,2796 & 1,0830 & -0,3016 \\ 0,2198 & -1,1080 & 1,3550 & 0,9585 & -0,6962 & -0,5058 & 0,8699 & -0,2045 \\ 0,1903 & 0,1117 & -0,4390 & -0,3474 & 0,2226 & -0,9638 & -0,0787 & -0,3395 \end{pmatrix}.$$

Procedendo de forma análoga aos exemplos anteriores, obtém-se uma base ortonormal formada pelos autovetores da DST-IV apresentados nas linhas da matriz

$$\mathbf{V}^T = \begin{pmatrix} 0,2601 & -0,6022 & 0,3124 & -0,4006 & 0,02837 & -0,1778 & 0,4065 & -0,3375 \\ -0,7593 & -0,3485 & -0,2379 & -0,0252 & -0,28980 & 0,1464 & 0,3399 & 0,1544 \\ 0,1661 & 0,1243 & 0,0773 & 0,1191 & -0,89250 & -0,3695 & -0,0130 & -0,0596 \\ -0,3009 & 0,5598 & 0,1527 & -0,4222 & -0,06734 & 0,2022 & 0,0975 & -0,5828 \\ 0,1049 & 0,3655 & -0,0311 & 0,3454 & 0,17790 & -0,1972 & 0,8108 & 0,0851 \\ -0,0628 & 0,0975 & 0,7880 & -0,0739 & -0,09641 & 0,2941 & 0,0650 & 0,5101 \\ -0,4553 & -0,0706 & 0,4219 & 0,3911 & 0,23700 & -0,5376 & -0,2156 & -0,2554 \\ 0,1242 & -0,1978 & 0,1292 & 0,6071 & -0,13080 & 0,5961 & 0,0384 & -0,4316 \end{pmatrix}.$$

□

O procedimento para obtenção de bases ortonormais de $\mathbb{R}^N$ formadas por autovetores de matrizes de transformadas trigonométricas anteriormente descrito e ilustrado por meio dos Exemplos 3.1 a 3.5 também funciona para a DHT com comprimentos $N \neq 4m$. Porém, se $N = 4m$, as multiplicidades dos autovalores da matriz da DHT diferem em duas unidades (vide Tabela Tabela - 2.2). Como, pelo método proposto, autovetores associados aos autovalores 1 e -1 são gerados de forma alternada, na tentativa de obter uma base, ter-se-ia que proceder da seguinte forma:

1. Construir um autovetor inicial $\mathbf{v}_0$ da DHT, associado ao autovalor 1, e uma matriz geradora $\mathbf{S_A} = -\mathbf{HAH} + \mathbf{A}$;
2. Obter, para $r = 1, 2, 3, \ldots, N$, os autovetores $\mathbf{v}_r = \mathbf{S_A}\mathbf{v}_{r-1}$;
3. Descartar o autovetor $\mathbf{v}_{N-1}$ associado ao autovalor -1, restando o conjunto de autovetores $\{\mathbf{v}_r\}_{r=0,\ldots,N,\, r\neq N-1}$.

O fato é que o conjunto mencionado no passo 3 acima, embora possua $2m+1$ e $2m-1$ autovetores associados aos autovalores 1 e -1, respectivamente, é linearmente dependente (LD). Isso se explica pelo fato de o conjunto obtido no passo 2, que possui $N+1$ autovetores, ser, obviamente, LD e de tal condição não ser modificada pelo descarte realizado no passo 3.

Diante da restrição descrita, são propostos os passos a seguir para construção de uma base para $\mathbb{R}^N$, $N = 4m$, formada por autovetores da matriz da DHT:

1. Construa autovetores iniciais $\mathbf{v}_0^+$ e $\mathbf{v}_0^-$ da DHT associados aos autovalores 1 e -1, respectivamente (isso pode ser feito usando a Proposição 2.7);

2. Escolha uma matriz arbitrária $\mathbf{A}$, com dimensão $N \times N$, para criação da matriz geradora $\mathbf{S_A} = \mathbf{HAH} + \mathbf{A}$ (Proposição 3.1). Conforme indicado anteriormente, realizando o produto entre a matriz $\mathbf{S_A}$ construída dessa forma e um autovetor, gera-se um novo autovetor associado ao mesmo autovalor;

3. Obtenha, para $r = 1, 2, 3, \ldots, 2m$, os autovetores

$$\mathbf{v}_r^+ = \mathbf{S_A}\mathbf{v}_{r-1}^+ \tag{3.4}$$

associados ao autovalor 1 e verifique se o conjunto $\{\mathbf{v}_r^+\}_{r=0,\ldots,2m}$ é LI; obtenha para $r = 1, 2, 3, \ldots, 2m-2$, os autovetores

$$\mathbf{v}_r^- = \mathbf{S_A}\mathbf{v}_{r-1}^- \tag{3.5}$$

associados ao autovalor -1 e verifique se o conjunto $\{\mathbf{v}_r^-\}_{r=0,\ldots,2m-2}$ é LI;

4. Se os conjuntos gerados no passo anterior forem LI e se se desejar que eles sejam também ortogonais, aplique algum processo de ortogonalização (o algoritmo de Gram-Schmidt, por exemplo) a cada um deles. Normalizando os vetores resultantes, são obtidos os conjuntos identificados por $\{\widetilde{\mathbf{v}}_r^+\}_{r=0,\ldots,2m}$ e $\{\widetilde{\mathbf{v}}_r^-\}_{r=0,\ldots,2m-2}$;

5. Obtenha a base ortonormal $\{\widetilde{\mathbf{v}}_r\}_{r=0,\ldots,N-1}$ para $\mathbb{R}^N$, em que $\widetilde{\mathbf{v}}_{2r} = \widetilde{\mathbf{v}}_r^+$, $r = 0, \ldots, 2m-1$, $\widetilde{\mathbf{v}}_{N-1} = \widetilde{\mathbf{v}}_{2m}^+$ e $\widetilde{\mathbf{v}}_{2r+1} = \widetilde{\mathbf{v}}_r^-$, $r = 0, \ldots, 2m-2$.

O procedimento que se acabou de descrever pode, naturalmente, ser adaptado para a obtenção de bases formadas por autovetores de outras transformadas trigonométricas e com comprimentos $N \neq 4m$. Basta observar que a ideia consiste, basicamente, em gerar em separado os autovetores associados a cada um dos autovalores. Nesse contexto, é relevante mencionar que, no passo 2 do referido procedimento, em vez de se empregar a mesma matriz geradora para obter os autovetores de cada autoespaço, matrizes geradoras distintas podem ser usadas.

Exemplo 3.5

Construção de uma base para $\mathbb{R}^8$ formada por autovetores da matriz da DHT: seja $\mathbf{u}$ um vetor 8-dimensional arbitrário dado por

$$\mathbf{u} = \begin{pmatrix} 0,8593 & 0,8663 & 0,4377 & -0,5928 & 0,4304 & 0,7022 & 0,8615 & 0,3747 \end{pmatrix}.$$

Utilizando a Proposição 2.7, gera-se o autovetor $\mathbf{v}_0^+ = \mathbf{u} + \mathbf{Hu}$ da DHT, associado ao

autovalor 1 *e dado por*

$$\mathbf{v}_0^+ = \begin{pmatrix} 2,252 & 0,9501 & 1,066 & -0,7752 & 0,8684 & 0,6219 & 0,2264 & 1,1599 \end{pmatrix},$$

e o autovetor $\mathbf{v}_0^- = \mathbf{u} - \mathbf{Hu}$ *da DHT, associado ao autovalor* -1 *e dado por*

$$\mathbf{v}_0^- = \begin{pmatrix} -0,5334 & 0,7824 & -0,1906 & -0,4105 & -0,0074 & 0,7824 & 1,4966 & -0,4105 \end{pmatrix}.$$

Usando a mesma matriz aleatória $\mathbf{A}$ *dos exemplos anteriores, obtém-se a matriz geradora*

$$\mathbf{S_A} = \begin{pmatrix} -1,7260 & -1,426 & -0,7793 & -0,0137 & 1,2410 & -0,8070 & 1,0300 & -0,4686 \\ -0,3117 & 0,1671 & 0,6207 & -0,8462 & -0,3379 & -0,6976 & 0,4879 & 1,2460 \\ 1,1060 & -0,3151 & -0,9119 & -0,8074 & 0,2920 & -0,7134 & -0,5039 & 0,4850 \\ -0,9244 & -0,2898 & -1,4190 & -0,0958 & 0,0048 & -0,2892 & -1,3840 & -1,3080 \\ -0,1502 & -0,4838 & -0,4858 & -1,0760 & 0,7625 & 0,0789 & -0,2863 & 0,4884 \\ 0,0292 & -0,5989 & 0,4546 & 1,3760 & 0,2417 & -0,6041 & 1,0340 & -0,6413 \\ -1,2810 & -1,555 & 1,7170 & 0,1777 & -0,6381 & -0,6675 & 0,8679 & -0,6555 \\ 0,3092 & -1,1510 & -1,6830 & 0,7719 & 0,9158 & -0,2023 & -0,2322 & -0,9466 \end{pmatrix}.$$

Seguindo os últimos passos apresentados, obtém-se uma base ortonormal formada pelos autovetores da DHT apresentados nas linhas da matriz

$$\mathbf{V}^T = \begin{pmatrix} 0,6764 & 0,3341 & 0,3119 & 0,4844 & 0,3071 & 0,0593 & -0,0263 & -0,0140 \\ -0,4235 & 0,3184 & 0,2618 & -0,1980 & 0,7035 & -0,3142 & 0,0498 & 0,1234 \\ 0,2250 & -0,0549 & -0,3922 & -0,3040 & 0,4034 & 0,3227 & 0,5038 & -0,4234 \\ -0,3687 & 0,5149 & -0,5460 & 0,5318 & -0,0504 & 0,0949 & 0,0385 & -0,0688 \\ 0,4073 & 0,1523 & -0,5086 & -0,2373 & -0,0366 & -0,6399 & -0,0208 & 0,2907 \\ -0,0361 & -0,6510 & -0,3024 & 0,3863 & 0,4738 & -0,0069 & -0,2607 & 0,2038 \\ -0,0947 & -0,2639 & 0,1789 & 0,3794 & -0,1381 & -0,4719 & 0,7007 & -0,1118 \\ -0,0123 & -0,0449 & 0,0025 & 0,0345 & 0,0202 & -0,3901 & -0.4266 & -0,8136 \end{pmatrix}.$$

□

3.2 Transformadas trigonométricas fracionárias discretas

Conforme mencionado no capítulo inicial desta dissertação, transformadas fracionárias correspondem a uma generalização da transformada ordinária correspondente, em que se admite calcular potências não-inteiras do respectivo operador de transformação. Quando se trata de uma transformada discreta, tal operador pode ser expresso por meio de uma matriz; assumindo que a referida matriz, denotada aqui por $\mathbf{M}$, é diagonalizável, ela pode ser expandida como

$$\mathbf{M} = \mathbf{V}\blacksquare\mathbf{V}^T, \tag{3.6}$$

em que $\mathbf{V}$ é uma matriz contendo em suas colunas uma base ortonormal de autovetores de $\mathbf{M}$, $\mathbf{V}^T$ denota a matriz $\mathbf{V}$ transposta e $\blacksquare$ é uma matriz diagonal contendo os autovalores

correspondentes a cada autovetor empregado na construção de $\mathbf{V}$. Com isso, pode-se escrever

$$\mathbf{M}^a = \mathbf{V}\blacksquare^a\mathbf{V}^T, \tag{3.7}$$

em que $a \in \mathbb{R}$ é um parâmetro identificado como ordem fracionária. A transformada fracionária de um vetor $\mathbf{x}$ associada à matriz $\mathbf{M}$ com ordem fracionária a é denotada por $\mathbf{X}_a$ e calculada por

$$\mathbf{X}_a = \mathbf{M}^a\mathbf{x}. \tag{3.8}$$

Dentre as propriedades desejáveis para uma transformada fracionária discreta, as mais importantes são a de redução à respectiva transformada ordinária quando $a = 1$ e a de aditividade de índices, que consiste, basicamente, em se ter

$$\mathbf{M}^{a_1+a_2} = \mathbf{M}^{a_1}\mathbf{M}^{a_2}, \tag{3.9}$$

em que $a_1, a_2 \in \mathbb{R}$. Assumindo a validade da propriedade de aditividade de índices para a transformada fracionária associada ao operador $\mathbf{M}$, tem-se que a transformada inversa de $\mathbf{X}_a$ é calculada por

$$\mathbf{x} = \mathbf{M}^{-a}\mathbf{X}_a. \tag{3.10}$$

Uma versão bidimensional de uma transformada fracionária admite o uso de duas ordens fracionárias, impostas a matrizes de transformação com dimensões coerentes com as dimensões da matriz que se deseja transformar; a transformada fracionária bidimensional de uma matriz $\mathbf{x}$ é expressa por

$$\mathbf{X}_{a_1,a_2} = \mathbf{M}_1^{a_1}\mathbf{x}(\mathbf{M}_2^{a_2})^T, \tag{3.11}$$

em que $a_1, a_2 \in \mathbb{R}$ são as ordens fracionárias das transformadas aplicadas, respectivamente, às colunas e às linhas de $\mathbf{x}$. Naturalmente, a_1 e a_2 podem coincidir e, se $\mathbf{x}$ for uma matriz quadrada, $\mathbf{M}_1$ e $\mathbf{M}_2$ também podem ser iguais. As propriedades anteriormente mencionadas também podem ser estendidas ao contexto de duas dimensões.

Transformadas fracionárias multiordem

Em trabalhos recentes, têm sido propostas transformadas fracionárias multiordem. Como o próprio termo sugere, numa transformada desse tipo, múltiplas ordens fracionárias são empregadas. Tal possibilidade é viabilizada pelo uso de um vetor $\mathbf{a} = (a_0, a_1, \ldots, a_{N-2}, a_{N-1})$,

$a_n \in \mathbb{R}$, $n = 0, 1, \ldots, N-1$, com elementos independentes, em substituição à ordem $a \in \mathbb{R}$. Assim, em (3.7), $\blacksquare^a$ é substituída por

$$\blacksquare^{\mathbf{a}} = \begin{pmatrix} \lambda_0^{a_0} & 0 & \cdots & 0 & 0 \\ 0 & \lambda_1^{a_1} & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda_{N-2}^{a_{N-2}} & 0 \\ 0 & 0 & \cdots & 0 & \lambda_{N-1}^{a_{N-1}} \end{pmatrix} \tag{3.12}$$

e, consequentemente, tem-se

$$\mathbf{M}^{\mathbf{a}} = \mathbf{V}\blacksquare^{\mathbf{a}}\mathbf{V}^T. \tag{3.13}$$

Em geral, as seguintes propriedades são válidas para uma transformada fracionária multiordem [45]:

1. Se $\mathbf{a} = (a, a, \ldots, a)$, a transformada fracionária multiordem degenera-se para a transformada fracionária correspondente, a qual pode ser vista como um caso particular da primeira;
2. Uma transformada fracionária multiordem cuja matriz possui dimensão $N \times N$ pode ter até N diferentes ordens fracionárias. A transformada fracionária correspondente possui ordem fracionária única;
3. A complexidade computacional de uma transformada fracionária e a de sua versão multiordem coincidem.

Além disso, as seguintes propriedades são desejáveis [45]:

1. Unitariedade:

$$(\mathbf{M}^{\mathbf{a}})^H(\mathbf{M}^{\mathbf{a}}) = \left(\mathbf{V}\blacksquare^{\mathbf{a}}\mathbf{V}^T\right)^H \left(\mathbf{V}\blacksquare^{\mathbf{a}}\mathbf{V}^T\right)\left(\mathbf{V}\blacksquare^{-\mathbf{a}}\mathbf{V}^T\right)^H \left(\mathbf{V}\blacksquare^{\mathbf{a}}\mathbf{V}^T\right) = \mathbf{V}\mathbf{V}^T = \mathbf{I}, \tag{3.14}$$

   em que H denota o operador conjugado transposto.
2. Matriz identidade: se $\mathbf{a} = \mathbf{0} = (0, 0, \ldots, 0)$, então $\mathbf{M}^{\mathbf{a}} = \mathbf{V}\blacksquare^{\mathbf{0}}\mathbf{V}^T = \mathbf{V}\mathbf{V}^T = \mathbf{I}$.
3. Transformada ordinária: se $\mathbf{a} = \mathbf{1} = (1, 1, \ldots, 1)$, então $\mathbf{M}^{\mathbf{a}} = \mathbf{V}\blacksquare^{\mathbf{1}}\mathbf{V}^T = \mathbf{V}\blacksquare\mathbf{V}^T = \mathbf{M}$.
4. Aditividade: se $\mathbf{a}_1$ e $\mathbf{a}_2$ são dois vetores com o mesmo número de múltiplas ordens fracionárias, então

$$\mathbf{M}^{\mathbf{a}_1} \cdot \mathbf{M}^{\mathbf{a}_2} = (\mathbf{V}\blacksquare^{\mathbf{a}_1}\mathbf{V}^T)(\mathbf{V}\blacksquare^{\mathbf{a}_2}\mathbf{V}^T) = \mathbf{V}\blacksquare^{\mathbf{a}_1+\mathbf{a}_2}\mathbf{V}^T = \mathbf{M}^{\mathbf{a}_1+\mathbf{a}_2}. \tag{3.15}$$

5. Comutatividade:

$$\mathbf{M}^{\mathbf{a}_1} \cdot \mathbf{M}^{\mathbf{a}_2} = \mathbf{V}\blacksquare^{\mathbf{a}_1+\mathbf{a}_2}\mathbf{V}^T = \mathbf{V}\blacksquare^{\mathbf{a}_2+\mathbf{a}_1}\mathbf{V}^T = \mathbf{M}^{\mathbf{a}_2} \cdot \mathbf{M}^{\mathbf{a}_1}. \tag{3.16}$$

6. Transformada inversa: a matriz da transformada fracionária multiordem inversa com parâmetro $\mathbf{a}$ é dada por $(\mathbf{M}^{\mathbf{a}})^{-1} = \mathbf{M}^{-\mathbf{a}}$.
7. Periodicidade da ordem $\mathbf{a}$: se ℓ for o menor inteiro positivo tal que $\mathbf{M}^{\ell} = \mathbf{I}$, então $\mathbf{M}^{\mathbf{a}+k\ell} = \mathbf{M}^{\mathbf{a}}$, em que $k \in \mathbb{Z}$.

Naturalmente, as bases ortonormais formadas por autovetores de transformadas trigonométricas discretas obtidas empregando os procedimentos propostos na Seção 3.1 podem ser utilizadas na expansão dos respectivos operadores matriciais (como em (3.6)) e, consequentemente, em sua fracionarização simples (como em (3.7)) ou com múltiplas ordens (como em (3.13)). É essa a possibilidade que se considera deste ponto em diante. Assim, de modo distinto do que tem sido proposto noutros trabalhos da literatura, pode-se definir versões fracionárias da DHT, da DCT-I, da DST-I, da DCT-IV e da DST-IV que, além da(s) ordem(ns) fracionária(s) especificada(s), dependem das escolhas que se faz com relação aos autovetores iniciais e à matriz geradora. Detalhes relacionados ao número total de parâmetros livres em tais definições serão abordados em seções futuras desta dissertação.

Transformadas fracionárias multiordem reais

Diferentemente da DFT, que pode originar resultados com componentes complexas, as transformadas consideradas neste trabalho são todas reais. Isso se reflete nas autoestruturas dos respectivos operadores: os autovetores e os autovalores das transformadas trigonométricas discretas são todos reais. Por outro lado, versões fracionárias dessas transformadas podem ser complexas; para confirmar tal possibilidade, basta observar que o autovalor -1, que necessariamente figura ao longo da diagonal de $\blacksquare$, ao ser elevado a um número não-inteiro (ordem fracionária), resulta num número complexo. O aparecimento de tais números quando da aplicação de uma DFT fracionária a um vetor ou matriz real envolve maior complexidade aritmética e, além disso, é indesejável em determinados cenários de aplicação (processamento e cifragem de imagem, por exemplo) [46]. Diante disso, têm sido investigadas estratégias para definir transformadas fracionárias (multiordem ou com ordem única) cujas matrizes sejam reais [41, 46, 47].

Pelo método proposto em [46], uma matriz real com dimensões $N \times N$, N par, para a

DCT com ordem fracionária a pode ser obtida por

$$\mathbf{C}^a = \mathbf{V}\left(\mathbf{G}_{1_{N/2}}(\theta(a)) \oplus \mathbf{G}_{2_{N/2}}(\eta(a))\right)\mathbf{V}^T, \tag{3.17}$$

em que $\mathbf{G}_{1_{N/2}}(\theta(a))$ e $\mathbf{G}_{2_{N/2}}(\eta(a))$ são matrizes bloco-diagonais com dimensões $N/2 \times N/2$; os referidos blocos são denotados, respectivamente, por $\mathbf{G}_1(\theta(a))$ e $\mathbf{G}_2(\eta(a))$ e dados por

$$\mathbf{G}_1(\theta(a)) = \begin{pmatrix} \cos(\theta(a)) & \text{sen}(\theta(a)) \\ -\text{sen}(\theta(a)) & \cos(\theta(a)) \end{pmatrix} \tag{3.18}$$

e

$$\mathbf{G}_2(\eta(a)) = \begin{pmatrix} \cos(\eta(a)) & \text{sen}(\eta(a)) \\ -\text{sen}(\eta(a)) & \cos(\eta(a)) \end{pmatrix}, \tag{3.19}$$

em que $\theta(a) = 2a\pi$ e $\eta(a) = a\pi$; o símbolo $\oplus$ representa uma soma direta, de modo que o termo $\mathbf{G}_{1_{N/2}}(\theta(a)) \oplus \mathbf{G}_{2_{N/2}}(\eta(a))$ em (3.17), que substitui a matriz $\blacksquare^a$, é dado por

$$\mathbf{G}_{1_{N/2}}(\theta(a)) \oplus \mathbf{G}_{2_{N/2}}(\eta(a)) = \begin{pmatrix} \mathbf{G}_{1_{N/2}}(\theta(a)) & \mathbf{0} \\ \mathbf{0} & \mathbf{G}_{2_{N/2}}(\eta(a)) \end{pmatrix} \tag{3.20}$$

A matriz $\mathbf{V}$, por sua vez, tem como suas $N/2+1$ primeiras colunas autovetores da matriz da DCT associados ao autovalor 1 e como suas $N/2-1$ últimas colunas autovetores associados ao autovalor -1.

Em [41], é proposta uma DHT fracionária multiordem e real para o caso em que $N = 4m+1$. A matriz da referida transformada é expressa por

$$\mathbf{H}^{\mathbf{e},\mathbf{g}} = \mathbf{V}\blacksquare^{\mathbf{e},\mathbf{g}}\mathbf{V}^T, \tag{3.21}$$

em que os vetores $\mathbf{e} = (e_0, e_1, \ldots, e_{2m-2}, e_{2m-1})$ e $\mathbf{g} = (g_0, g_1, \ldots, g_{2m-2}, g_{2m-1})$ possuem componentes reais e independentes. A matriz $\mathbf{V}$ é preenchida da primeira até a $((N+1)/2)$-ésima coluna com autovetores relacionados ao autovalor 1; nas demais colunas, são colocados autovetores relacionados ao autovalor -1. A transformada multiordem definida dessa forma possui todas as propriedades mencionadas na Seção 3.2.1 e permite escolher $(N-1)$ ordens correspondentes às componentes dos vetores $\mathbf{e}$ e $\mathbf{g}$. A matriz de autovalores é dada por

$$\blacksquare^{\mathbf{e},\mathbf{g}} = \begin{pmatrix} \mathbf{W}_{1_{2m}}(\mathbf{e}) & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \mathbf{W}_{2_{2m}}(\mathbf{e}) \end{pmatrix}, \tag{3.22}$$

em que

$$\mathbf{W}_{1_{2m}}(\mathbf{e}) = \begin{pmatrix} \begin{matrix} \cos(\theta(e_1)) & \operatorname{sen}(\theta(e_1)) \\ -\operatorname{sen}(\theta(e_1)) & \cos(\theta(e_1)) \end{matrix} & \begin{matrix} 0 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 0 \end{matrix} \\ \begin{matrix} 0 \\ 0 \end{matrix} & \begin{matrix} \cos(\theta(e_2)) & \operatorname{sen}(\theta(e_2)) \\ -\operatorname{sen}(\theta(e_2)) & \cos(\theta(e_2)) \end{matrix} & \begin{matrix} 0 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 0 \end{matrix} \\ \begin{matrix} 0 & 0 \end{matrix} & \begin{matrix} 0 & 0 \end{matrix} & \ddots & \begin{matrix} 0 \\ \cos(\theta(e_{2m})) & \operatorname{sen}(\theta(e_{2m})) \\ -\operatorname{sen}(\theta(e_{2m})) & \cos(\theta(e_{2m})) \end{matrix} \end{pmatrix}$$

e

$$\mathbf{W}_{2_{2m}}(\mathbf{g}) = \begin{pmatrix} \begin{matrix} \cos(\theta(g_1)) & \operatorname{sen}(\theta(g_1)) \\ -\operatorname{sen}(\theta(g_1)) & \cos(\theta(g_1)) \end{matrix} & \begin{matrix} 0 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 0 \end{matrix} \\ \begin{matrix} 0 \\ 0 \end{matrix} & \begin{matrix} \cos(\theta(g_2)) & \operatorname{sen}(\theta(g_2)) \\ -\operatorname{sen}(\theta(g_2)) & \cos(\theta(g_2)) \end{matrix} & \begin{matrix} 0 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 0 \end{matrix} \\ \begin{matrix} 0 & 0 \end{matrix} & \begin{matrix} 0 & 0 \end{matrix} & \ddots & \begin{matrix} 0 \\ \cos(\theta(g_{2m})) & \operatorname{sen}(\theta(g_{2m})) \\ -\operatorname{sen}(\theta(g_{2m})) & \cos(\theta(g_{2m})) \end{matrix} \end{pmatrix}.$$

Considerando a estrutura das matrizes $\mathbf{W}_{1_{2m}}(\mathbf{e})$ e $\mathbf{W}_{2_{2m}}(\mathbf{g})$, verifica-se que, em relação à definição original de transformadas fracionárias multiordem, cada par de autovalores iguais, posicionados de forma sucessiva ao longo da diagonal da matriz $\blacksquare$, que seriam elevados a expoentes fracionários componentes do vetor $\mathbf{a}$, é substituído pelo operador matricial de rotação no plano; a exceção é o autovalor na posição $(2m+1, 2m+1)$, que é igual a 1 e que permanece inalterado, não sendo elevado a qualquer parâmetro ou substituído por outro operador. De qualquer maneira, pela forma como os autovetores são construídos em [41], tal estratégia se limita ao caso $N = 4m+1$.

Diferentemente do método para construção de autovetores da DHT considerado em [41], o método proposto neste trabalho e descrito em detalhes em 3.1, permite obter bases de $\mathbb{R}^N$ formadas por autovetores da DHT para qualquer N. Assim, torna-se possível construir matrizes reais com formato semelhante ao de $\blacksquare^{\mathbf{e},\mathbf{g}}$ em (3.22), respeitando, naturalmente, as multiplicidades dos autovalores 1 e -1 conforme apresentado na Tabela Tabela - 2.2 . Para a DHT de tamanho $N = 4m+2$, por exemplo, pode ser empregada a matriz $\blacksquare^{\mathbf{e},\mathbf{g}}$ seja dada por

$$\blacksquare^{\mathbf{e},\mathbf{g}} = \begin{pmatrix} \mathbf{W}_{1_{2m}}(\mathbf{e}) & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \mathbf{W}_{2_{2m}}(\mathbf{g}) & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}; \tag{3.23}$$

para a DHT de tamanho $N = 4m+3$, propõe-se que a matriz $\blacksquare^{\mathbf{e},\mathbf{g}}$ seja dada por

$$\blacksquare^{\mathbf{e},\mathbf{g}} = \begin{pmatrix} \mathbf{W}_{1_{2m+2}}(\mathbf{e}) & 0 & 0 \\ 0 & \mathbf{W}_{2_{2m}}(\mathbf{g}) & 0 \\ 0 & 0 & -1 \end{pmatrix}; \tag{3.24}$$

finalmente, para a DHT de tamanho $N = 4m$, propõe-se que a matriz $\blacksquare^{\mathbf{e},\mathbf{g}}$ seja dada por

$$\blacksquare^{\mathbf{e},\mathbf{g}} = \begin{pmatrix} \mathbf{W}_{1_{2m+2}}(\mathbf{e}) & 0 \\ 0 & \mathbf{W}_{2_{2m-2}}(\mathbf{g}) \end{pmatrix}. \tag{3.25}$$

Transformadas fracionárias de Hartley discretas, multiordem e reais, com operador dado pela expansão espectral (3.21), empregando as matrizes bloco-diagonais $\blacksquare^{\mathbf{e},\mathbf{g}}$ propostas para $N \neq 4m+1$, também satisfazem as propriedades listadas na Seção 3.2.1. Além disso, transformadas do cosseno e do seno dos tipos I e IV com os mesmos requisitos também podem ser construídas de forma análoga; para isso, é suficiente construir bases de $\mathbb{R}^N$ formadas por autovetores dessas transformadas, aplicando os procedimentos anteriormente descritos, e respeitar as respectivas multiplicidades dos autovalores 1 e -1, para determinado valor de N, na construção das matrizes $\blacksquare^{\mathbf{e},\mathbf{g}}$.

4 Aplicação à Cifragem de Imagens

Neste capítulo, é apresentada uma aplicação dos procedimentos introduzidos no Capítulo 3 desta dissertação. Mais especificamente, é proposto um esquema para cifragem de imagens baseado numa DHT fracionária multiordem real. Na implementação do referido esquema, poderiam ser utilizadas versões fracionárias de transformadas como a DCT-I, DST-I, DCT-IV e a DST-IV, também consideradas anteriormente. Porém, como, conceitualmente, a simples substituição da DHT por uma versão equivalente de uma dessas outras ferramentas não representaria uma mudança relevante no esquema mencionado, neste trabalho, o uso apenas da primeira é de fato considerado.

A principal motivação para considerar a aplicação que é tema central do presente capítulo vem do fato de que, nas últimas décadas, o emprego de transformadas fracionárias em cifragem de imagens tem sido bastante difundido e documentado num grande número de publicações. Tal possibilidade advém, basicamente, da aleatoriedade que pode estar envolvida na construção de bases de autovetores da DFT, conforme indicado, por exemplo, em [39]. Isso também se verifica para outras transformadas discretas que admitem infinitas escolhas para bases formadas por seus autovetores, em função de as respectivas matrizes de transformação possuírem autovalores repetidos (vide Capítulo 2).

O esquema de cifragem de imagens considerado aqui é semelhante aos propostos em [40] e [41]. Nestes trabalhos, são utilizadas DFT fracionárias definidas usando autovetores construídos segundo o método de matrizes comutantes generalizadas, introduzido em e tratado também em [40]. No presente caso, utiliza-se a metodologia apresentada no Capítulo 3, a qual, conforme será demonstrado, envolve um número maior de parâmetros livres; isso é interessante em aplicações de Criptografia, uma vez que se pode atrelar tais parâmetros aos valores componentes de uma chave-secreta. Além disso, diferentemente do que ocorre com a DFT, é possível definir com mais naturalidade uma DHT fracionária real; tal definição parece mais adequada quando se deseja processar um sinal originalmente real, como é o caso de imagens digitais.

Uma das tecnicas usada em cifragem de imagem é baseado em mapas caóticos, pois provê de uma boa combinação entre velocidade, alta segurança, complexidade, overhead

computacional razoável e potência computacional razoável [48]. Além disso, um mapa caótico apresenta algumas propriedades que são desejáveis a um sistema de cifragem, órbitas com comportamento pseudo-aleatório, grande sensibilidade aos parâmetros iniciais, ergodicidade etc. [49]. Embora um estudo aprofundado desses mapas esteja fora do escopo desta dissertação, alguns deles são considerados neste capítulo e empregados no esquema proposto [28], [50].

Como introdução a este capítulo, ainda é importante dizer que os resultados obtidos dos experimentos computacionais realizados dão suporte apenas a uma avaliação preliminar acerca da segurança do esquema proposto. Uma análise mais completa, levando em conta, inclusive, as restrições que o uso de transformadas definidas sobre os números reais no contexto considerado possui em comparação ao uso de ferramentas definidas sobre estruturas algébricas finitas, por exemplo, é deixada para trabalhos futuros. A delimitação de tal escopo, que, de alguma forma, abdica de uma análise profunda de certos aspectos práticos do contexto de Criptografia, é justificada pelo fato de que, nesta dissertação, são apresentados como principais contribuições os resultados e os procedimentos desenvolvidos no Capítulo 3; o conteúdo apresentado no presente capítulo tem o intuito maior de ilustrar uma possibilidade de extrapolar o campo teórico em que os resultados mencionados foram desenvolvidos, permitindo sugestões e revelando direções para melhoria das métricas consideradas.

4.1 Cifragem de imagens baseada em transformadas fracionárias multiordem reais

Seguindo uma abordagem semelhante à apresentada noutros trabalhos [39–41, 51], o que se propõe é cifrar uma imagem em escala de cinzas $\mathbf{Im}$ aplicando uma versão bidimensional da DHT fracionária multiordem definida conforme apresentado na parte final do Capítulo 3. A respectiva imagem cifrada é obtida por

$$\mathbf{P} = \mathbf{H}^{\mathbf{e},\mathbf{g}}_{\mathbf{A}^+,\mathbf{A}^-,\mathbf{v}_0^+,\mathbf{v}_0^-} \cdot \mathbf{Im} \cdot \left(\mathbf{H}^{\mathbf{e}',\mathbf{g}'}_{\mathbf{A}'^+,\mathbf{A}'^-,\mathbf{v}'^+_0,\mathbf{v}'^-_0}\right)^T. \tag{4.1}$$

Na última equação, as matrizes $\mathbf{H}^{\mathbf{e},\mathbf{g}}_{\mathbf{A}^+,\mathbf{A}^-,\mathbf{v}_0^+,\mathbf{v}_0^-}$ e $\mathbf{H}^{\mathbf{e}',\mathbf{g}'}_{\mathbf{A}'^+,\mathbf{A}'^-,\mathbf{v}'^+_0,\mathbf{v}'^-_0}$ são análogas à matriz $\mathbf{H}^{\mathbf{e},\mathbf{g}}$ em (3.21); porém, na notação empregada aqui, além dos vetores $\mathbf{e}$, $\mathbf{g}$, $\mathbf{e}'$ e $\mathbf{g}'$, são explicitados os vetores iniciais $\mathbf{v}_0^+$ e $\mathbf{v}_0^-$ (resp. $\mathbf{v}'^+_0$ e $\mathbf{v}'^-_0$) e as matrizes $\mathbf{A}^+$ e $\mathbf{A}^-$ (resp. $\mathbf{A}'^+$ e $\mathbf{A}'^-$) a partir das quais se obtém as matrizes geradoras empregadas. Todos esses parâmetros podem estar atrelados a uma chave-secreta. O fato de se permitir o emprego

de parâmetros diferentes na construção das matrizes que multiplicam $\mathbf{Im}$ à esquerda e à direita indica que as transformadas aplicadas às colunas e às linhas da imagem podem ser distintas. Naturalmente, também se pode fazer $\mathbf{A}^{+} = \mathbf{A'}^{+}$, $\mathbf{A}^{-} = \mathbf{A'}^{-}$, $\mathbf{v}_0^{+} = \mathbf{v'}_0^{+}$, $\mathbf{v}_0^{-} = \mathbf{v'}_0^{-}$, $\mathbf{e} = \mathbf{e'}$ e $\mathbf{g} = \mathbf{g'}$, diminuindo o número de parâmetros necessários à construção das duas matrizes mencionadas e, consequentemente, o comprimento da chave à qual estes parâmetros estejam atrelados.

Para o processo de decifragem, utiliza-se a propriedade de aditividade de índices da transformada descrita na Seção 3.2.1. A mesma chave empregada na cifragem é utilizada, porém, as componentes dos vetores correspondentes às múltiplas ordens fracionárias das matrizes de transformação envolvidas têm seus sinais invertidos. De qualquer forma, tem-se um esquema criptográfico simétrico, de modo que se espera recuperar $\mathbf{Im}$ por

$$\mathbf{Im} = \mathbf{H}^{-\mathbf{e},-\mathbf{g}}_{\mathbf{A}^{+},\mathbf{A}^{-},\mathbf{v}_0^{+},\mathbf{v}_0^{-}} \cdot \mathbf{P} \cdot \left(\mathbf{H}^{-\mathbf{e'},-\mathbf{g'}}_{\mathbf{A'}^{+},\mathbf{A'}^{-},\mathbf{v'}_0^{+},\mathbf{v'}_0^{-}}\right)^{T}. \tag{4.2}$$

Conforme indicado, 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:

1. $m+1$ 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 $N = 4m$ parâmetros;
2. N componentes de cada um dos autovetores de partida $\mathbf{v}_0^{+}$, $\mathbf{v}_0^{-}$, $\mathbf{v'}_0^{+}$ e $\mathbf{v'}_0^{-}$, totalizando $4N$ parâmetros (supõe-se que cada um desses autovetores de partida foi construído a partir de vetores arbitrários N-dimensionais distintos);
3. N^2 componentes de cada uma das quatro matrizes arbitrárias $\mathbf{A}^{+}$, $\mathbf{A}^{-}$, $\mathbf{A'}^{+}$ e $\mathbf{A'}^{-}$ utilizadas na obtenção de quatro matrizes geradoras empregadas na geração dos conjuntos de autovetores associados aos autovalores 1 e -1, nas transformadas aplicadas às colunas e às linhas de $\mathbf{Im}$, totalizando $4N^2$ parâmetros.

Somando os números de parâmetros de cada um dos itens acima, obtém-se um total de $4N^2 + 5N$ parâmetros reais. Em suma, a partir de uma chave-secreta, pode-se determinar, no esquema descrito, os autovetores iniciais, as matrizes geradoras e as múltiplas ordens fracionárias empregadas; todos esses parâmetros influenciam, de alguma maneira, as matrizes de transformação obtidas e, consequentemente, o resultado que se obtém ao se transformar a imagem $\mathbf{Im}$.

Como forma de visualizar os efeitos da cifragem de uma imagem segundo o método descrito nesta seção, as imagens apresentadas na Figura Figura - 4.1 foram obtidas. Para isso, considerou-se $\mathbf{A} = \mathbf{A}^{+} = \mathbf{A'}^{+} = \mathbf{A}^{-} = \mathbf{A'}^{-}$, $\mathbf{e} = \mathbf{e'}$ e $\mathbf{g} = \mathbf{g'}$; os autovetores iniciais $\mathbf{v}_0^{+}$, $\mathbf{v'}_0^{+}$, $\mathbf{v}_0^{-}$ e $\mathbf{v'}_0^{-}$ foram todos construídos a partir de um mesmo vetor arbitrário $\mathbf{v}$. Na Figura Figura - 4.1a, é exibida a imagem em escala de cinzas conhecida como *cameraman*, a qual possui dimensões 256×256 pixels; a imagem na Figura Figura - 4.1b é a que resultado processo de cifragem. Conforme esperado, o aspecto da imagem é completamente ruidoso e não revela qualquer traço visual da imagem original; a imagem na Figura Figura - 4.1c é o resultado da decifragem quando todos os parâmetros envolvidos estão corretos. A Figura Figura - 4.1d é o resultado da decifragem quando se usa uma matriz $\mathbf{A}$, gerada aleatoriamente, diferente daquela empregada na cifragem; a Figura Figura - 4.1e é o resultado da decifragem quando se usa um vetor $\mathbf{v}$, gerado aleatoriamente, diferente daquele usado na cifragem; finalmente, a Figura Figura - 4.1f é o resultado da decifragem quando é usado um vetor de múltiplas ordens fracionárias, gerado aleatoriamente, diferente daquele usados na cifragem. De modo preliminar, presume-se que não se pode obter nenhuma informação sobre a imagem original a partir das imagens decifradas com as chaves incorretas. De qualquer forma, uma análise mais criteriosa acerca da segurança do esquema é necessária. Um esboço de tal análise é desenvolvido a seguir.

4.2 Análise preliminar de segurança

O grau de segurança de esquemas de cifragem de imagens é predominantemente avaliado por meio de métricas obtidas em experimentos de computador. Tais experimentos podem produzir números relacionados, por exemplo, à correlação entre pixels vizinhos e à entropia na imagem cifrada. Quando se trata de cifragem de imagens baseada em transformadas definidas sobre os números reais ou complexos, o exame da literatura relacionada indica que o experimento mais relevante é o da sensibilidade da chave [41]; o propósito de tal experimento é medir o máximo desvio δ sobre os parâmetros empregados como chave-secreta do esquema, tal que ainda seja possível decifrar a imagem corretamente. A partir dessa sensibilidade, pode-se estimar o espaço de chaves e, consequentemente, caracterizar o esquema quanto à robustez contra ataques de força-bruta. O fato é que, quando o esquema de cifragem considerado tem sua chave ligada a diversos parâmetros, como é o caso do esquema em questão, mesmo o experimento voltado à medição da sensibilidade da chave

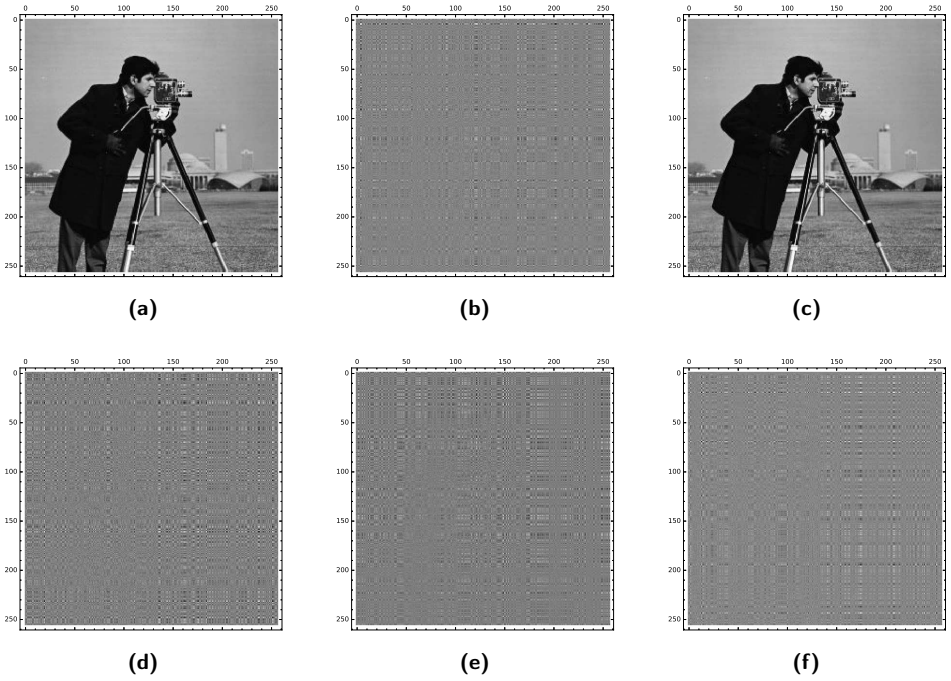


Figura Figura - 4.1 – *Resultados preliminares do esquema de cifragem descrito: (a) imagem original, (b) imagem resultante da cifragem, (c) decifragem usando todos os parâmetros corretos, (d) decifragem usando a matriz* $\mathbf{A}$ *incorreta, (e) decifragem usando o vetor* $\mathbf{v}$ *incorreto, (f) decifragem usando ordens fracionárias incorretas.*

pode ser conduzido de diferentes maneiras. Algumas dessas metodologias são concisamente descritas e têm seus resultados exibidos a seguir.

Sensibilidade da decifragem a desvios na chave

Seguindo [41], para analisar a sensibilidade da matriz $\mathbf{A}$ como chave, adiciona-se à matriz originalmente empregada na cifragem uma matriz $\mathbf{E}$ em que todos os elementos são iguais a $\delta \in \mathbb{R}$, obtendo-se uma nova matriz $\hat{\mathbf{A}} = \mathbf{A} + \mathbf{E}$. O que se faz é tentar decifrar a imagem empregando $\hat{\mathbf{A}}$ em vez de $\mathbf{A}$ (os demais parâmetros não são alterados). A diferença entre a imagem obtida na tentativa de decifragem e a imagem original é medida pelo erro médio quadrático (MSE, do inglês *mean squared error*), o qual é calculado por

$$\mathrm{MSE} = \frac{1}{M \times N} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} | C_1(i,j) - C_2(i,j) |^2;$$

na última equação, M e N são a largura e a altura da imagem e $C_1(i,j)$ e $C_2(i,j)$ são os valores dos pixels na posição (i,j) nas duas imagens a serem comparadas.

Na Figura Figura - 4.2, apresenta-se um gráfico que demonstra o crescimento do MSE

à proporção em que se aumenta o valor absoluto do desvio δ (a imagem de referência continua sendo a *cameraman*). O MSE calculado entre a imagem original e a cifrada Figura - 4.1b é de 34520, já o MSE entre a imagem original e a decifrada é de 0.0004085. Esse comportamento já era esperado e é necessário à caracterização da segurança do esquema em questão. No entanto, a determinação da faixa de valores de δ para a qual a imagem obtida na tentativa de decifragem com parte da chave incorreta é suficientemente diferente da imagem original requer uma análise mais criteriosa. Porém, a consideração apenas do referido limiar pode gerar conclusões falsas, uma vez que, ainda que valores relativamente altos sejam obtidos para o MSE, a imagem recuperada pode revelar traços da imagem original. Na Figura Figura - 4.3a, por exemplo, mostra-se a imagem obtida da decifragem com $\delta = 0,005$; mesmo com o MSE maior que 20.000 (vide Figura Figura - 4.2), é possível observar elementos da imagem original. Algo semelhante ocorre quando $\delta = 0,01$ (vide Figura Figura - 4.3b). Apenas quando $\delta = 0,02$, a imagem decifrada apresenta-se visualmente irreconhecível, como mostrado na Figura Figura - 4.3c.

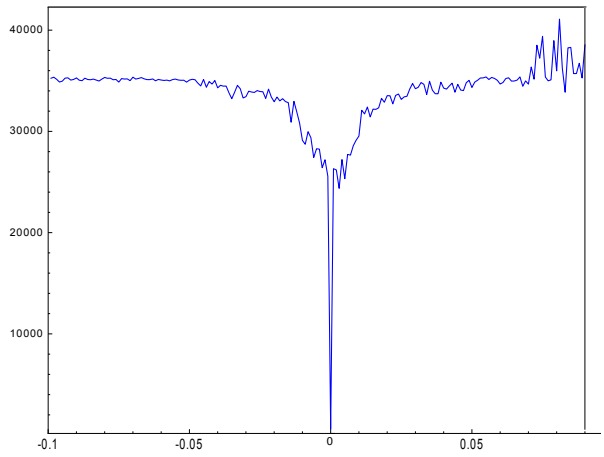


Figura Figura - 4.2 – *MSE entre a imagem original e a imagem obtida da tentativa de decifragem, quando um desvio δ é imposto aos elementos da matriz $\mathbf{A}$.*

Uma análise similar pode ser realizada também para os outros parâmetros usados como chave. Na Figura Figura - 4.4, mostra-se a variação do MSE à medida em que um desvio δ é somado a cada componente do vetor inicial $\mathbf{v}$. Mais uma vez, a partir dos resultados do experimento realizado, conclui-se que valores elevados de MSE não implicam, necessariamente, que a tentativa de decifrar a imagem com uma chave incorreta foi completamente frustrada; vestígios da imagem original podem aparecer. É o que ocorre, por exemplo, com

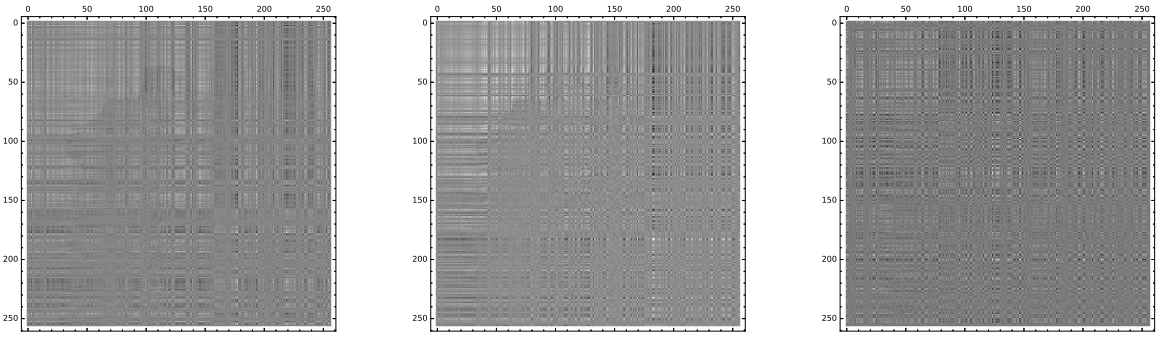


Figura Figura - 4.3 – *Decifragem com desvios sobre todas as entradas da matriz* $\mathbf{A}$*: (a) decifragem com desvio* $\delta = 0,005$ *na matriz* $\mathbf{A}$*, (b) decifragem com desvio* $\delta = 0,01$ *na matriz* $\mathbf{A}$*, (c) decifragem com desvio* $\delta = 0,02$ *na matriz* $\mathbf{A}$*.*

a imagem apresentada na Figura Figura - 4.5a; mesmo com um valor relativamente alto para o MSE, obtido quando $\delta = 0,05$, é possível observar rastros visuais da imagem original na imagem resultante da tentativa de decifragem. Por outro lado, na imagem apresentada na Figura Figura - 4.5b, obtida quando $\delta = 0,15$, a imagem produzida não revela traços da imagem original.

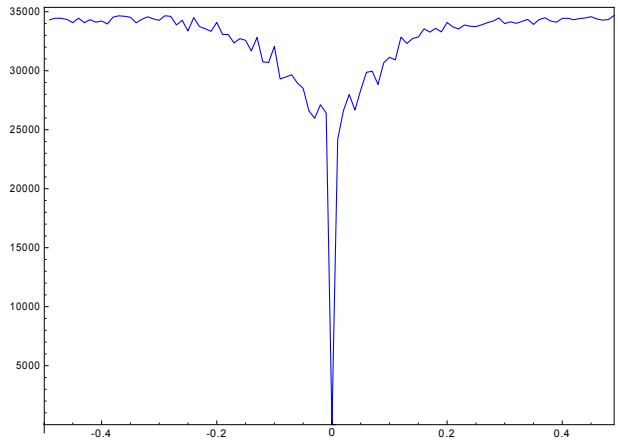


Figura Figura - 4.4 – *MSE entre a imagem original e a imagem obtida da tentativa de decifragem, quando um desvio* δ *é imposto aos elementos do vetor inicial* $\mathbf{v}$*.*

Na Figura Figura - 4.6, é apresentado o MSE entre a imagem original e a imagem obtida da tentativa de decifragem, quando um desvio δ é adicionado às componentes dos vetores com múltiplas ordens fracionárias. A partir de resultados experimentais, verificou-se que a imagem obtida passa a não conter rastros da imagem original quando $|\delta| > 0,3$, conforme ilustrado nas Figuras Figura - 4.7a e Figura - 4.7b.

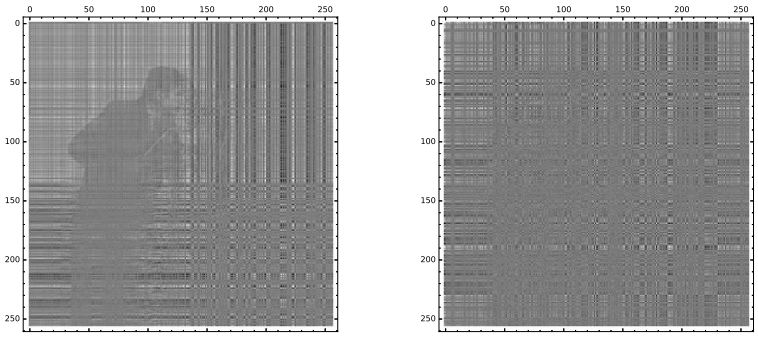


Figura Figura - 4.5 – *Decifragem com desvios sobre todas as componentes do vetor inicial* $\mathbf{v}$*: (a) decifragem com desvio de* $\delta = 0,05$ *no vetor inicial* $\mathbf{v}$*, (b) Decifragem com desvio* $\delta = 0,15$ *no vetor inicial* $\mathbf{v}$*.*

Emregando um raciocínio análogo ao considerado em [41] e levando em conta os resultados dos experimentos realizados, é possível afirmar que, para obter sucesso em um ataque de força-bruta contra o esquema proposto, é necessário que o erro em cada elemento da matriz $\mathbf{A}$ seja menor que $\delta = 0,02$ e o erro em cada elemento do vetor inicial $\mathbf{v}$ seja menor que $\delta = 0,1$. Assim, a probabilidade de sucesso de um ataque de força bruta é menor que $p = (0,02/2)^{256\times256} \times (0,1/2)^{128} = 1,018^{-131216}$, mesmo que a chave fracionária seja conhecida. Consequentemente, o espaço de chaves é dado por $1,018^{131216} \approx 2^{3385}$.

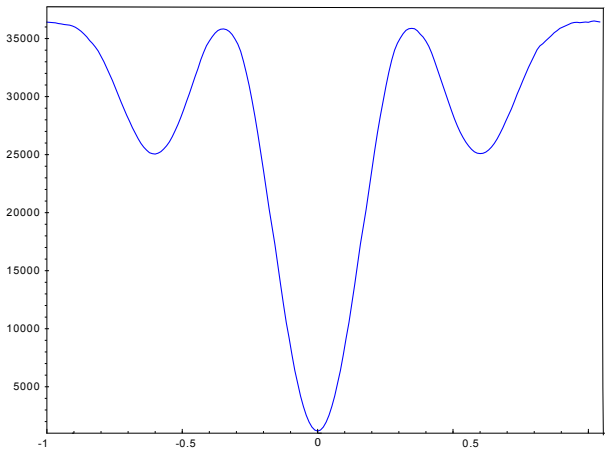


Figura Figura - 4.6 – *MSE entre a imagem original e a imagem obtida da tentativa de decifragem, quando um desvio* δ *é adicionado às componentes dos vetores de múltiplas ordens fracionárias.*

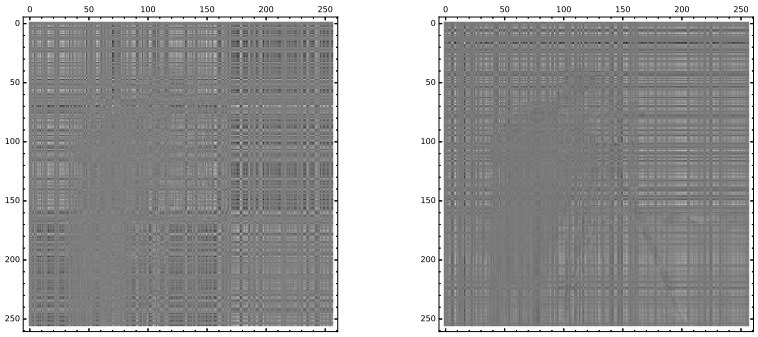


Figura Figura - 4.7 – *Decifragem com desvios sobre todas as componentes dos vetores com múltiplas ordens fracionárias: (a) imagem decifrada com desvio de $\delta = 0,35$ na chave fracionária, (b) imagem decifrada com desvio $\delta = 0,2$ na chave fracionária.*

Sensibilidade da decifragem a elementos desconhecidos na chave

Em [41], é empregado um outro procedimento para avaliar a robustez de um criptossistema para imagens baseado em transformadas. Tal procedimento consiste em calcular o MSE entre a imagem original e a imagem resultante da tentativa de decifragem quando alguns elementos das chaves são desconhecidos (ou, equivalentemente, quando alguns elementos das chaves são substituídos por valores aleatórios); o processo é iniciado com os valores corretos atribuídos a todos os elementos da chave. Numa primeira iteração, substitui-se o valor de um elemento da chave por um valor aleatório e calcula-se o MSE. A cada iteração, mais um elemento tem o seu valor substituído por um valor incorreto e um novo MSE é calculado. Tal estratégia é aplicada a determinado parâmetro da chave (matriz $\mathbf{A}$, vetor inicial $\mathbf{v}$ ou vetores com múltiplos parâmetros fracionários), ao passo em que os outros parâmetros são tomados de forma correta e mantidos inalterados.

O gráfico apresentado na Figura Figura - 4.8 apresenta a variação do MSE entre a imagem original e a imagem resultante da tentativa de decifragem à medida em que se aumenta a quantidade de elementos desconhecidos na chave $\mathbf{A}$. Neste caso, o que importa é estimar o número mínimo de elementos desconhecidos, tal que a imagem obtida numa tentativa de decifragem possua aspecto visual degradado, não revelando traços da imagem original; naturalmente, quanto menor este número mínimo, maior a segurança do criptossistema sob esse aspecto. Essa avaliação é ilustrada por meio da Figura Figura - 4.9. A Figura Figura - 4.9a sugere que, se apenas um elemento for desconhecido na matriz $\mathbf{A}$, ainda é possível obter informação visual da imagem original. Por outro lado, a Figura Figura - 4.9b indica que,

se 30 elementos de $\mathbf{A}$ forem desconhecidos, quase nenhuma informação visual da imagem original é recuperada. A medida que se incrementa o número de elementos desconhecidos, é possível obter menos informação visual da imagem, que a partir de 30 elementos, não é possível reconhecer a imagem original. Estes 30 elementos representam menos de 1% do total de elementos da chave $\mathbf{A}$, ou seja, é necessário conhecer a maior parte da chave para obter alguma informação da imagem.

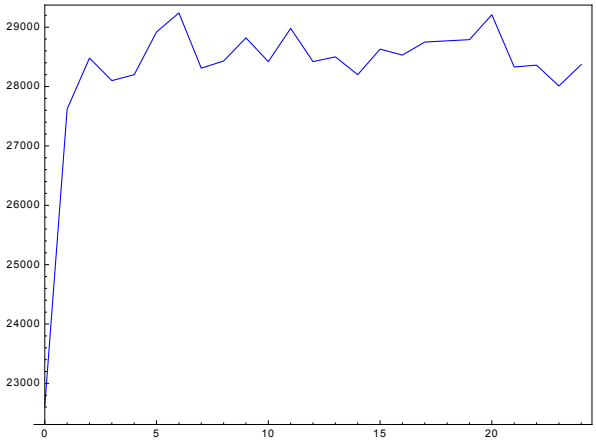
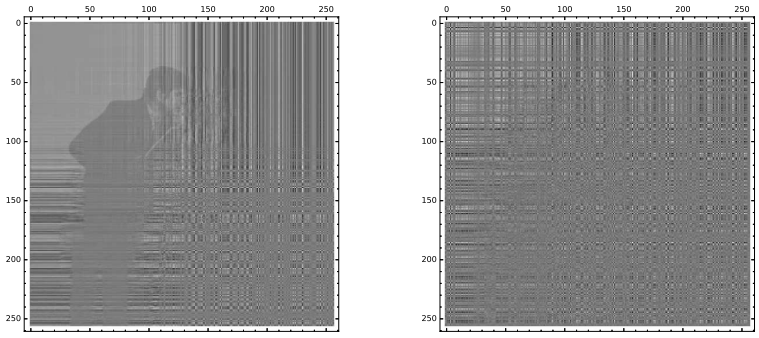


Figura Figura - 4.8 – *Evolução do MSE da imagem decifrada enquanto se incrementa o número de desconhecidos de* $\mathbf{A}$.

O gráfico da Figura Figura - 4.10 apresenta o resultado do experimento que se acabou de descrever, mas considerando elementos desconhecidos no vetor inicial $\mathbf{v}$, que também é usado como chave. Quando o número de elementos desconhecidos é igual a 1, ainda é possível obter informação visual da imagem, como mostrado na Figura Figura - 4.11a; quando o referido número é incrementado para 9, a informação visual da imagem original que se esperava recuperar é comprometida, conforme mostrado na Figura Figura - 4.11b.

A mesma análise foi feita para o vetor com múltiplas ordens fracionárias $\mathbf{a}$, que é composto pela concatenação entre os dois vetores $\mathbf{e}$ e $\mathbf{g}$ (vide descrição do esquema de cifragem na Seção 4.1). O gráfico apresentado na Figura Figura - 4.12 mostra a variação do MSE à medida em que se incrementa o número de elementos desconhecidos em $\mathbf{a}$. Quando este número é menor que 100, ainda é possível obter alguma informação visual da imagem original, como mostrado na Figura Figura - 4.13a; quando este número é maior que 100, tal informação é comprometida, conforme mostrado na Figura Figura - 4.13b.

As análises feitas até o momento consideram cada parâmetro da chave em separado. Porém, uma avaliação considerando mais de um parâmetro da chave simultaneamente



(a) **(b)**

Figura Figura - 4.9 – *Decifragem com substituição de elementos da matriz* $\mathbf{A}$ *por valores arbitrários (desconhecidos): (a) imagem decifrada para 01 elemento desconhecido na matriz* $\mathbf{A}$*, (b) imagem decifrada para* 30 *elementos desconhecidos na matriz* $\mathbf{A}$*.*

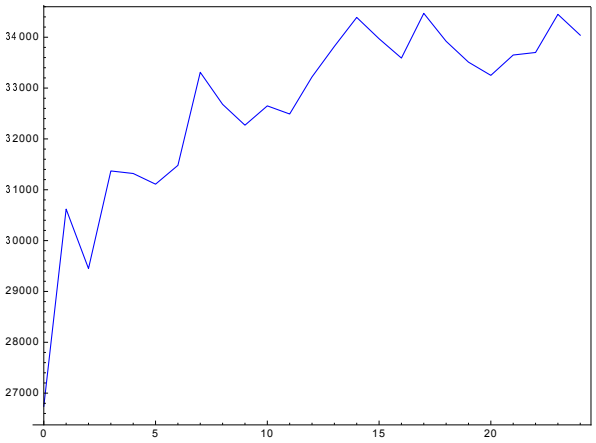
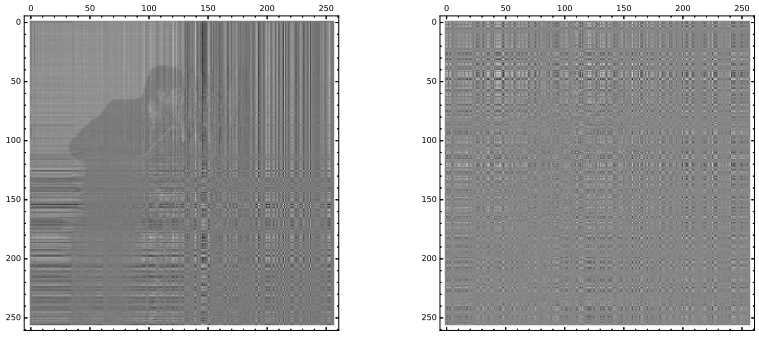


Figura Figura - 4.10 – *Evolução do MSE da imagem decifrada enquanto se incrementa o número de elementos desconhecidos de* $\mathbf{v}$*.*



(a) **(b)**

Figura Figura - 4.11 – *Decifragem com substituição de elementos do vetor inicial* $\mathbf{v}$ *por valores arbitrários (desconhecidos): (a) imagem decifrada quando o número de elementos desconhecidos em* $\mathbf{v}$ *é* 1*, (b) imagem decifrada quando o número de elementos desconhecidos em* $\mathbf{v}$ *é* 9*.*

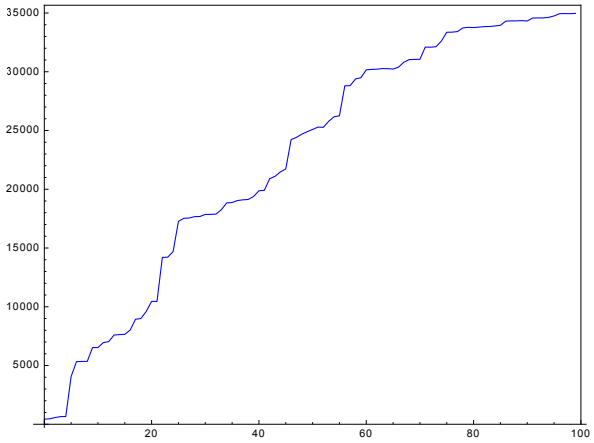


Figura Figura - 4.12 – *Evolução do MSE da imagem decifrada enquanto se incrementa o número de elementos desconhecidos de* $\mathbf{a}$.

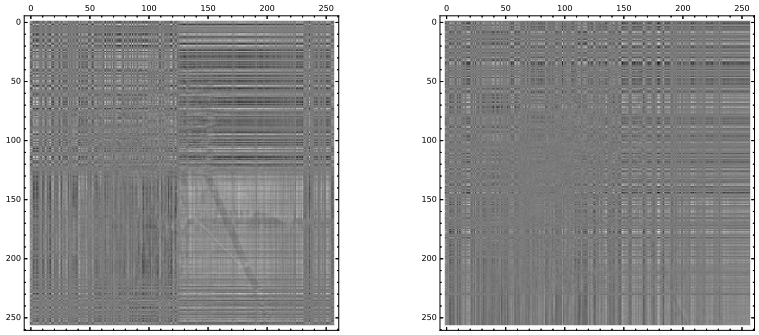


Figura Figura - 4.13 – *Decifragem com substituição de elementos do vetor de múltiplas ordens fracionárias* $\mathbf{a}$ *por valores arbitrários (desconhecidos): (a) imagem decifrada quando o número de elementos desconhecidos na chave* $\mathbf{a}$ *é igual a* 80 *elementos, (b) imagem decifrada quando o número de elementos desconhecidos na chave* $\mathbf{a}$ *é igual a* 100 *elementos.*

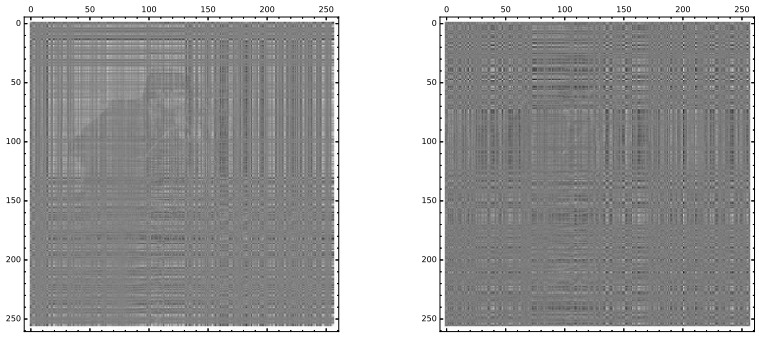


Figura Figura - 4.14 – *Decifragem com substituição de elementos de mais de um parâmetro da chave secreta por valores arbitrários (desconhecidos): (a) imagem decifrada quando a quantidade de elementos desconhecidos nas chaves é $n_{\mathbf{A}} = 1$, $n_{\mathbf{v}} = 1$ e $n_{\mathbf{a}} = 15$, (b) imagem decifrada quando a quantidade de elementos desconhecidos nas chaves é $n_{\mathbf{A}} = 1$, $n_{\mathbf{v}} = 1$ e $n_{\mathbf{a}} = 25$.*

também pode ser realizada. Por exemplo, na Figura Figura - 4.14a, obtida ao se substituir um elemento de chave correto em $\mathbf{A}$ por um elemento desconhecido $(n_{\mathbf{A}} = 1)$, um elemento em $\mathbf{v}$ $(n_{\mathbf{v}} = 1)$ e 15 elementos em $\mathbf{a}$ $(n_{\mathbf{a}} = 15)$, é possível perceber algumas características da imagem original; por outro lado, na Figura Figura - 4.14b, em que $n_{\mathbf{A}} = 1$, $n_{\mathbf{v}} = 1$ e $n_{\mathbf{a}} = 25$, não se observa visualmente nenhuma informação correlacionada à imagem original.

Naturalmente, várias combinações entre $n_{\mathbf{A}}$, $n_{\mathbf{v}}$ e $n_{\mathbf{a}}$ são possíveis, o que torna difícil mensurar a influência que o valor atribuído a cada um desses parâmetros tem na segurança do esquema como um todo. De qualquer forma, a partir dos resultados apresentados para o experimento do "elemento desconhecido", é possível concluir que nem todos os elementos da chave têm impacto significativo na segurança do esquema de cifragem. O pior cenário é o caso em que as chaves $\mathbf{A}$ e $\mathbf{v}$ são conhecidas, pois a chave do esquema se resumiria ao vetor fracionário $\mathbf{a}$; conforme observado anteriormente, mesmo que se desconheçam 100 elementos deste vetor, alguma informação visual da imagem pode ser recuperada. Isso sugere que, utilizando apenas o vetor com múltiplas ordens fracionárias como chave, a cifragem pode não ser eficaz.

Sensibilidade da decifragem à adição de ruído

Outro experimento importante é o que permite avaliar a robustez do sistema a ataques com ruídos [52]. No presente contexto, este teste é realizado adicionando à representação matricial da imagem cifrada um ruído Gaussiano com média zero e desvio padrão unitário multiplicado por um fator de ponderação α, e realizando uma tentativa de decifragem;

o que se espera é que a imagem decifrada, mesmo após a adição do ruído à respectiva imagem cifrada, conserve a informação visual da imagem original.

Na figura Figura - 4.15, é apresentado um gráfico que demonstra o crescimento do MSE enquanto aumenta-se o fator de ponderação α do ruído gaussiano. É esperado o incremento do MSE enquanto o fator de ponderação é incrementado. Nas imagens da Figura Figura - 4.16, são apresentados os resultados da decifragem para fatores de ponderação $\alpha = 10$ e $\alpha = 30$. A partir do aspecto dessas imagens, conclui-se que o esquema possui alguma robustez a ataques com ruído Gaussiano.

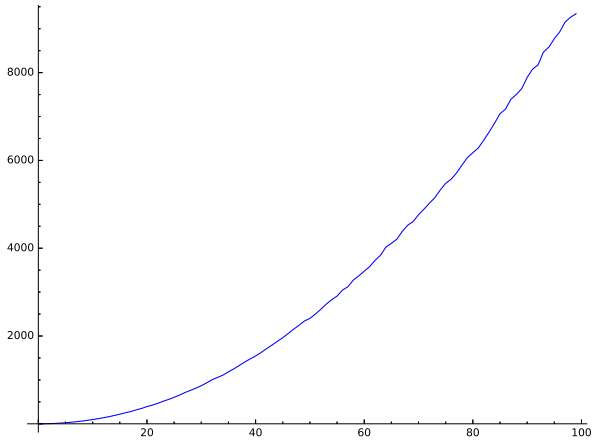


Figura Figura - 4.15 – *MSE entre a imagem original e a imagem obtida da tentativa de decifragem quando adiciona-se um ruído gaussiano a imagem cifrada.*

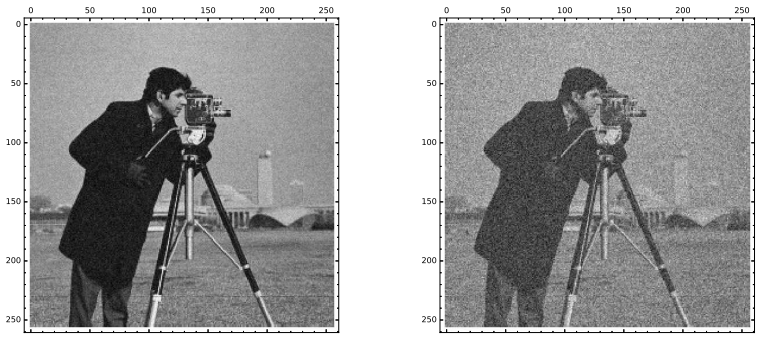


Figura Figura - 4.16 – *Imagens recuperados após um ataque a imagem cifrada com um ruído gaussiano com um fator de escala* (a) $\alpha = 10$ *e* (b) $\alpha = 30$.

4.3 Uso de sequências caóticas como chave

Uma possibilidade diferente da que se tem considerado até este ponto é gerar os elementos tomados como componentes da chave-secreta do esquema a partir de mapas caóticos [48]. Uma discussão detalhada a respeito dos diferentes tipos de sequências caóticas e de suas aplicações está fora do escopo deste trabalho. De qualquer forma, pode-se afirmar que essas sequências têm sido amplamente consideradas na implementação de diverssas classes de criptossistemas [28]. A principal razão para isso é que sequências caóticas são, normalmente, muito sensíveis a mudanças nos parâmetros empregados em sua inicialização, o que é desejável do ponto de vista de segurança [53].

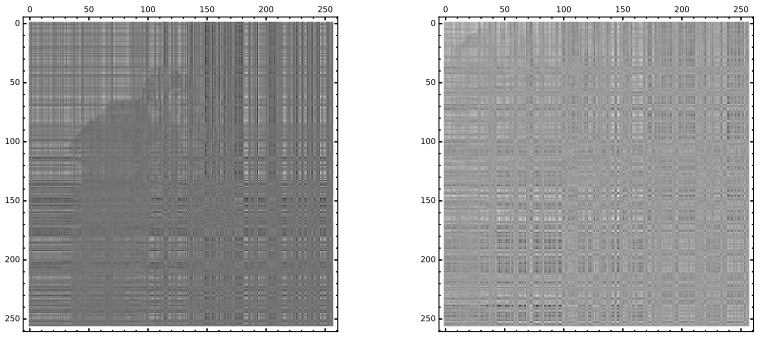
O mapa caótico considerado neste trabalho é o mapa da tenda (do inglês *tent map*), que é definido como [28]

$$x_{n+1} = \gamma \cdot x_n, \quad 0 \leq x_0 < 0,5, \tag{4.3}$$

$$x_{n+1} = \gamma(1 - x_n), \quad 0,5 \leq x_0 \leqslant 1, \tag{4.4}$$

em que x_0, $0 < x_0 \leq 1$, é o valor inicial e γ, $0 < \gamma \leqslant 2$, é uma constante. O que se faz aqui é gerar um mapa da tenda e empregar a sequência de valores obtidos tanto como componentes do vetor inicial $\mathbf{v}$ e como do vetor com múltiplas ordens fracionárias $\mathbf{a}$ (o vetor $\mathbf{a}$ é formado pela concatenação dos vetores $\mathbf{e}$ e $\mathbf{g}$). Os parâmetros iniciais empregados são $\gamma = 1,8$ e $x_0 = 0,3$. Neste caso, o que se analisa é a sensibilidade da decifragem quando se usa uma chave-secreta obtida de uma sequência caótica com parâmetros iniciais diferentes daqueles utilizados na cifragem. A mudança nos parâmetros iniciais gera desvios grandes nas sequências geradas, que tornam-se descorrelacionadas. Tal análise pode ser realizada adicionando um desvio δ a γ ou a x_0, gerando uma chave incorreta para uso na decifragem e medindo o erro entre a imagem original e aquela obtida da tentativa de decifragem.

A Figura Figura - 4.17a mostra a imagem obtida da decifragem quando um desvio $\delta = 10^{-55}$ é adicionado ao valor inicial x_0 da sequência caótica cujos termos são empregados como componentes de $\mathbf{v}$; neste caso, ainda é possível reconhecer traços da imagem original. Por outro lado, tais traços são significativamente reduzidos na Figura Figura - 4.17b, em que se tentou decifrar a imagem após se ter adicionado um desvio $\delta = 10^{-53}$ a x_0. A partir disso, é possível estimar um espaço de chaves relacionado ao parâmetro inicial x_0. Para um criptosistema em segurança de imagens, o espaço de chaves deve ser grande o suficiente para garantir que um ataque de força bruta seja inviável [53, 54]. Considerando



(a) (b)

Figura Figura - 4.17 – *Decifragem com desvios de (a) $\delta = 10^{-55}$ e (b) $\delta = 10^{-53}$ na chave x_0.*

que o intervalo dentro do qual se pode escolher x_0 a fim de que a sequência gerada tenha comportamento caótico tem largura igual a 1 e observando que o desvio $\delta = 10^{-53}$ pode ser adicionado ou subtraído de x_0, tal estimativa é obtida por

$$K_{x_0} = \frac{1}{2 \times 10^{-53}} = 5 \times 10^{52}.$$

O gráfico da Figura Figura - 4.18 mostra a mudança do MSE à medida em que se incrementa o valor absoluto do desvio δ sobre o valor inicial x_0 usado para produzir a sequência caótica correspondente ao vetor $\mathbf{v}$ (o parâmetro γ é mantido inalterado).

Uma estratégia similar é aplicada considerando-se o parâmetro inicial γ. A Figura Figura - 4.19a mostra o resultado obtido quando um desvio $\delta = 10^{-25}$ é aplicado e uma chave incorreta é gerada; na figura, observa-se que a informação visual da imagem original é parcialmente conservada. Por outro lado, na Figura Figura - 4.19b, resultante da adição de $\delta = 10^{-20}$ a γ, não se observa conteúdo visual da imagem original. O espaço de chaves da constante γ é calculado semelhantemente ao de x_0, sendo dado por

$$K_\gamma = \frac{1}{2 \times 10^{-20}} = 5 \times 10^{19}$$

O gráfico na Figura Figura - 4.20 mostra a mudança do MSE à medida em que se incrementa o valor absoluto do desvio δ sobre o parâmetro inicial γ do mapa da tenda (o valor de x_0 é mantido inalterado).

A mesma avaliação de sensibilidade é feita para o vetor com múltiplas ordens fracionárias $\mathbf{a}$. Foram adicionados desvios δ ao valor inicial x_0 e à constante γ. Com base nos resultados obtidos, é possível concluir que, do ponto de vista de segurança, a sensibilidade da decifragem aos parâmetros iniciais do mapa caótico usado é insuficiente; Na imagem da Figura Figura - 4.21a, por exemplo, obtida da decifragem após a adição de um desvio

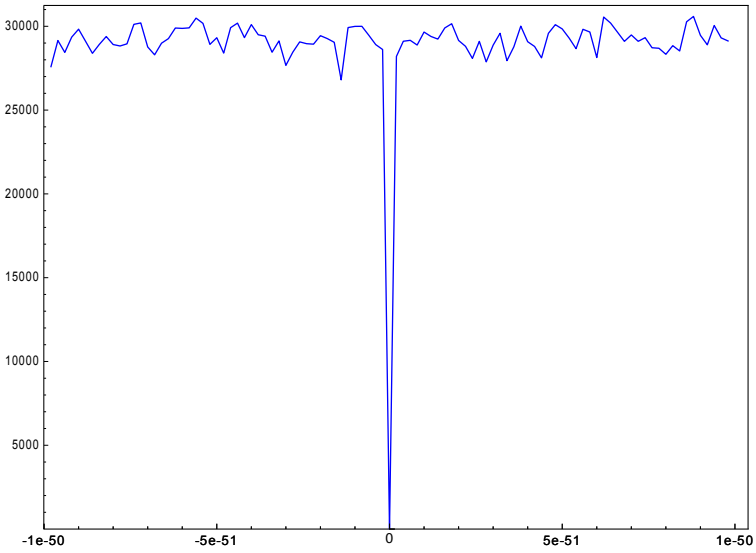


Figura Figura - 4.18 – *MSE obtido ao se adicionar um desvio δ ao parâmetro inicial x_0 do mapa da tenda no vetor inicial* $\mathbf{v}$.

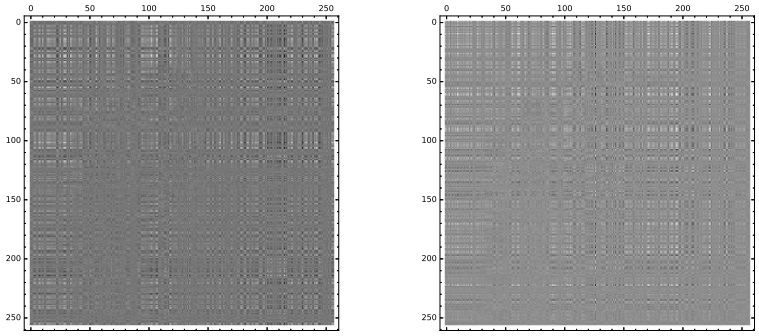


Figura Figura - 4.19 – *Decifragem com desvios de (a) $\delta = 10^{-25}$ e (b) $\delta = 10^{-20}$ na constante γ.*

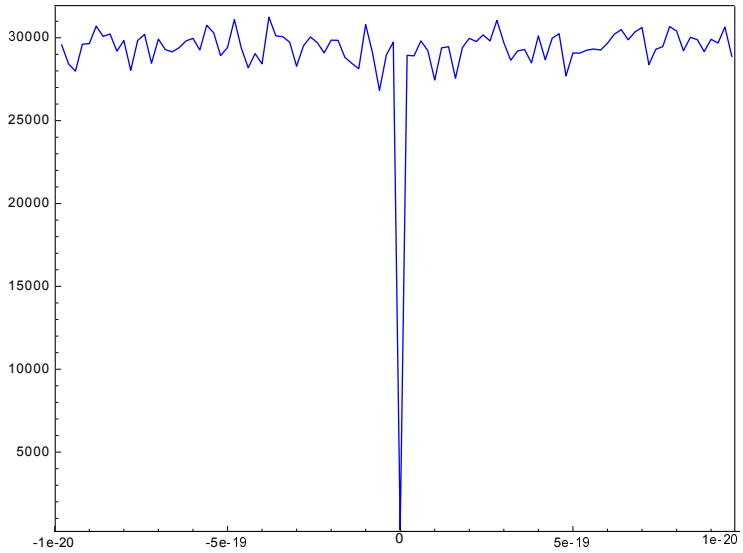


Figura Figura - 4.20 – *MSE obtido ao se adicionar um desvio δ à constante γ do mapa da tenda no vetor inicial* $\mathbf{v}$.

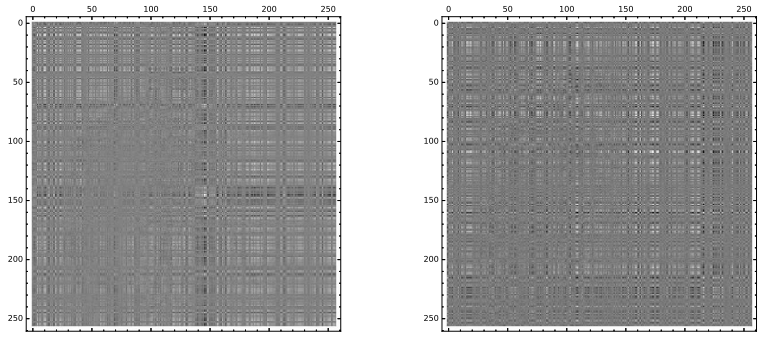


Figura Figura - 4.21 – *Decifragem com desvios de (a) $\delta = 0,5$ em x_0 e (b) $\delta = 1$ na constante γ.*

$\delta = 0,5$ em x_0, ainda é possível observar vestígios da imagem original. Algo similar ocorre se se adicionar um desvio $\delta = 1$ ao parâmetro γ (vide Figura Figura - 4.21b). Diante disso e considerando as larguras dos intervalos dentro dos quais podem ser escolhidos os valores de x_0 e de γ, é como se o espaço de chaves referente ao vetor com múltiplas ordens fracionárias $\mathbf{a}$ fosse binário; na prática, é como se a escolha das componentes de tal vetor não exercesse influência na segurança do esquema.

A partir dos resultados apresentados, conclui-se que, se desvios maiores que $\delta = 10^{-53}$ e $\delta = 10^{-20}$ forem respectivamente adicionados ao parâmetro inicial x_0 e à constante a, de forma não necessariamente simultânea, na geração da sequência caótica cujos elementos são

usados como componentes do vetor inicial $\mathbf{v}$, a imagem resultante da tentativa de decifragem não revela traços visuais significativos da imagem original. Assim, o espaço de chaves do esquema como um todo, considerando o uso do mapa da tenda, é dado por $5 \times 10^{52} \times 5 \times 10^{19} = 2,5 \times 10^{72} \approx 2^{240}$. Neste caso, assume-se que a chave aleatória $\mathbf{A}$ é conhecida, porém, seus elementos também poderiam ser gerados por meio de sequências caóticas; isso, provavelmente, aumentaria consideravelmente o espaço de chaves do esquema. Tal possibilidade, que não foi implementada neste trabalho, tem sido investigada a fim de que possa ser incluída em trabalhos futuros.

Como comentário final a respeito do conteúdo desenvolvido ao longo deste capítulo, pode-se dizer que os resultados apresentados sugerem que é possível aplicar o método de matrizes geradoras de autovetores de transformadas trigonométricas discretas para construir transformadas fracionárias multiordem e aplicá-las em cifragem de imagens. Os resultados expostos assemelham-se aos apresentados em [41], porém com mais parâmetros livres pelo fato de se poder escolher N^2 elementos da matriz $\mathbf{A}$, em vez de se poder escolher apenas $N^2/4$ em métodos baseados na transformada de Fourier. Conforme já se indicou anteriormente, mais investigações são necessárias para dar suporte a conclusões definitivas sobre o tamanho mínimo da chave para o qual o esquema é seguro, pois existe a possibilidade de o tamanho da chave ser menor e mesmo assim seguro. Além disso, faz-se necessário considerar outras métricas para caracterização do esquema como um todo, como o tempo de cifragem / decifragem, a entropia da imagem cifrada em comparação com a da respectiva imagem original e a correlação entre pixels vizinhos antes e a após a cifragem.

5 Conclusões

NESTA dissertação, foram propostas metodologias para construção de autovetores de transformadas trigonométricas discretas empregando matrizes geradoras. Além de descrever como as referidas matrizes são obtidas, foram apresentados procedimentos para que os autovetores construídos possam formar bases ortogonais. Mostrou-se como utilizar essas bases na diagonalização dos respectivos operadores matriciais de transformação, o que permitiu obter versões fracionárias dessas transformadas. Formas multiordem reais dessas transformadas foram propostas e seu potencial de aplicação à cifragem de imagem foi estudado de maneira preliminar. A partir de resultados de simulações computacionais, constatou-se que os esquemas de cifragem considerados preenchem alguns dos requisitos de segurança necessários ao uso em cenários práticos reais. Isso é proporcionado, dentre outros motivos, pelo fato de se ter, nas transformadas utilizadas como base desses esquemas, a possibilidade de escolher um grande número de parâmetros.

5.1 Trabalhos futuros

Como trabalhos relacionados a esta dissertação e que podem ser desenvolvidos em oportunidades futuras, podem ser elencados os seguintes:

- ▷ Avaliar a possibiliadde de empregar, para determinado tipo de transformada discreta, matrizes geradoras e autovetores de partida que assegurem a produção de conjuntos de vetores linearmente independentes;
- ▷ Analisar de forma mais completa os aspectos de segurança dos esquemas de cifragem considerados;
- ▷ Investigar outras aplicações das transformadas fracionárias multiordem reais, como a marca d'água e a esteganografia digitais.

5.2 Artigos publicados

Os resultados obtidos nesta dissertação foram publicados nos dois artigos listados a seguir e aceitos para apresentação num evento internacional e noutro nacional:

- ▷ Ravi B. D. Figueiredo, Juliano B. Lima, José R. de Oliveira Neto. Matrices Generating Eigenvectors for Constructing Fractional Trigonometric Transforms. In: 40th IEEE International Conference on Telecommunications and Signal Processing (Barcelona, Espanha, Julho de 2017);
- ▷ Ravi B. D. Figueiredo, Juliano B. Lima, José R. de Oliveira Neto. Matrizes Geradoras de Autovetores para Construção de Transformadas de Hartley Fracionárias. In: XXXV Simpósio Brasileiro de Telecomunicações e Processamento de Sinais (São Pedro, São Paulo, Setembro de 2017).

Bibliografia

[1] J. Lima, "A transformada fracional de Fourier: Conceitos e cenários de aplicação," *Revista de Tecnologia da Informação e Comunicação*, vol. 1, Abril 2012.

[2] R. L. Herman, *An Introduction to Fourier Analysis*. 1 ed., Agosto 2016.

[3] B. Dickinson, "Eigenvectors and functions of the discrete Fourier transform," *IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. 30, pp. 25–31, Feb 1982.

[4] S. C. Pei, W. L. Hsue, and J. J. Ding, "Discrete fractional Fourier transform based on new nearly tridiagonal commuting matrices," *IEEE Transactions on Signal Processing*, vol. 54, pp. 3815–3828, Oct 2006.

[5] Ç. Candan, "On higher order approximations for Hermite;Gaussian functions and discrete fractional Fourier transforms," *IEEE Signal Processing Letters*, vol. 14, pp. 699–702, Oct 2007.

[6] B. Santhanam and T. S. Santhanam, "Discrete Gauss-Hermite functions and eigenvectors of the centered discrete Fourier transform," in *2007 IEEE International Conference on Acoustics, Speech and Signal Processing - ICASSP '07*, vol. 3, pp. III–1385–III–1388, April 2007.

[7] S. C. Pei and K. W. Chang, "Generating matrix of discrete Fourier transform eigenvectors," in *2009 IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 3333–3336, April 2009.

[8] N. Wiener, "Hermitian polynomials and Fourier analysis," *Journal of Mathematics and Physics*, vol. 8, no. 1-4, pp. 70–73, 1929.

[9] E. Condon, "Immersion of the Fourier transform in a continuous group of functional transformations," *Proceedings of National Academy of Sciences of the United States of America*, vol. 23, no. 3, pp. 158–164, 1937.

[10] A. C. McBRIDE and F. H. KERR, "On namias's fractional Fourier transforms," *IMA Journal of Applied Mathematics*, vol. 39, no. 2, p. 159, 1987.

[11] D. A. MUSTARD, *The fractional Fourier transform and a new uncertainty principle*. Kensington, 1987.

[12] D. A. MUSTARD, *The fractional Fourier transform and the Wigner distribution*. Kensington, 1989.

[13] D. Mustard, "Uncertainty principles invariant under the fractional Fourier transform," *The Journal of the Australian Mathematical Society. Series B. Applied Mathematics*, vol. 33, no. 02, pp. 180–191, 1991.

[14] J. McClellan and T. Parks, "Eigenvalue and eigenvector decomposition of the discrete Fourier transform," *IEEE Transactions on Audio and Electroacoustics*, vol. 20, pp. 66–74, Mar 1972.

[15] H. M. Ozaktas, D. Mendlovic, L. Onural, and B. Barshan, "Convolution, filtering, and multiplexing in fractional Fourier domains and their relation to chirp and wavelet transforms," *JOSA A*, vol. 11, no. 2, pp. 547–559, 1994.

[16] H. M. Ozaktas and D. Mendlovic, "Fourier transforms of fractional order and their optical interpretation," *Optics Communications*, vol. 101, no. 3-4, pp. 163–169, 1993.

[17] H. M. Ozaktas and D. Mendlovic, "Fractional Fourier transforms and their optical implementation. ii," *JOSA A*, vol. 10, no. 12, pp. 2522–2531, 1993.

[18] D. Mendlovic and H. M. Ozaktas, "Fractional Fourier transforms and their optical implementation: I," *JOSA A*, vol. 10, no. 9, pp. 1875–1881, 1993.

[19] X. Kang, F. Zhang, and R. Tao, "Multichannel random discrete fractional Fourier transform," *IEEE Signal Processing Letters*, vol. 22, pp. 1340–1344, Sept 2015.

[20] R. Tao, X. Y. Meng, and Y. Wang, "Image encryption with multiorders of fractional Fourier transforms," *IEEE Transactions on Information Forensics and Security*, vol. 5, pp. 734–738, Dec 2010.

[21] J. Li, "Low noise reversible MDCT (RMDCT) and its application in progressive-to-lossless embedded audio coding," *IEEE Transactions on Signal Processing*, vol. 53, pp. 1870–1880, May 2005.

[22] D. Dragoman, "Fractional Fourier-related functions," *Optics communications*, vol. 128, no. 1-3, pp. 91–98, 1996.

[23] A. W. Lohmann, D. Mendlovic, Z. Zalevsky, and R. G. Dorsch, "Some important fractional transformations for signal processing," *Optics Communications*, vol. 125, no. 1-3, pp. 18–20, 1996.

[24] G. Cariolaro, T. Erseghe, and P. Kraniauskas, "The fractional discrete cosine transform," *IEEE Transactions on Signal Processing*, vol. 50, pp. 902–911, Apr 2002.

[25] S.-C. Pei and J.-J. Ding, "Fractional cosine, sine, and Hartley transforms," *IEEE Transactions on Signal Processing*, vol. 50, pp. 1661–1680, Jul 2002.

[26] M. Arora, K. Singh, and G. Mander, "Discrete fractional cosine transform based online handwritten signature verification," in *2014 Recent Advances in Engineering and Computational Sciences (RAECS)*, pp. 1–6, March 2014.

[27] Y. Tao and Y. Bao, "Speech information hiding using fractional cosine transform," in *2009 First International Conference on Information Science and Engineering*, pp. 1864–1867, Dec 2009.

[28] N. Singh and A. Sinha, "Optical image encryption using fractional Fourier transform and chaos," *Optics and Lasers in Engineering*, vol. 46, no. 2, pp. 117 – 123, 2008.

[29] L. Durak and S. Aldirmaz, "Adaptive fractional Fourier domain filtering," *Signal Processing*, vol. 90, pp. 1188–1196, April 2010.

[30] M. F. Erden, M. A. Kutay, and H. M. Ozaktas, "Applications of the fractional Fourier transform to filtering, estimation and restoration," in *Proc. of the IEEE-EURASIP Workshop on Nonlinear Signal and Image Processing (NSIP'99)*, (Antalya, Turkey), pp. 481–485, June 1999.

[31] L. Deng, M. Cheng, X. Wang, H. Li, S. Fu, P. Shum, and D. Liu, "Secure OFDM-PON system based on chaos and fractional Fourier transform techniques," *Journal of Lightwave Technology*, vol. 32, pp. 2629–2635, August 2014.

[32] T. Wang, H. Huan, R. Tao, and Y. Wang, "Security coded OFDM system based on multiorder fractional Fourier transform," *IEEE Communications Letters*, vol. PP, pp. 1–4, September 2016.

[33] R. Pelich, N. Longepe, G. Mercier, G. Hajduch, and R. Garello, "Vessel refocusing and velocity estimation on SAR imagery using the fractional Fourier transform," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 54, pp. 1670–1684, March 2015.

[34] 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, pp. 5396–5408, October 2016.

[35] D. M. J. Cowell and S. Freear, "Separation of overlapping linear frequency modulated (LFM) signals using the fractional Fourier transform," *IEEE Transactions on Ultrasonics, Ferroeletrics and Frequency Control*, vol. 57, pp. 2321–2333, October 2010.

[36] U. Singh and S. N. Singh, "Application of fractional Fourier transform for classification of power quality disturbances," *IET Science, Measurement & Technology*, vol. 11, pp. 67–76, January 2017.

[37] S. Harput, T. Evans, N. Bubb, and S. Freear, "Diagnostic ultrasound tooth imaging using fractional Fourier transform," *IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control*, vol. 58, pp. 2096–2106, October 2011.

[38] D. Shi, L. Zheng, and J. Liu, "Advanced Hough transform using a multilayer fractional Fourier method," *IEEE Transactions on Image Processing*, vol. 19, pp. 1558–1566, June 2010.

[39] Z. Liu and S. Liu, "Randomization of the Fourier transform," *Opt. Lett.*, vol. 32, pp. 478–480, Mar 2007.

[40] S. C. Pei and W. L. Hsue, "Random discrete fractional Fourier transform," *IEEE Signal Processing Letters*, vol. 16, pp. 1015–1018, Dec 2009.

[41] 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, pp. 2594–2605, Oct 2015.

[42] 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, pp. 665–675, Jun 1998.

[43] S.-C. Pei and M.-H. Yeh, "The discrete fractional cosine and sine transforms," *IEEE Transactions on Signal Processing*, vol. 49, pp. 1198–1207, Jun 2001.

[44] C.-C. Tseng, "Eigenvalues and eigenvectors of generalized DFT, generalized DHT, DCT-IV and DST-IV matrices," *IEEE Transactions on Signal Processing*, vol. 50, pp. 866–877, Apr 2002.

[45] S.-C. Pei and W.-L. Hsue, "The multiple-parameter discrete fractional Fourier transform," *IEEE Signal Processing Letters*, vol. 13, pp. 329–332, June 2006.

[46] I. Venturini and P. Duhamel, "Reality preserving fractional transforms [signal processing applications]," in *2004 IEEE International Conference on Acoustics, Speech, and Signal Processing*, vol. 5, pp. V–205–8 vol.5, May 2004.

[47] W. L. Hsue and W. C. Chang, "Multiple-parameter real discrete fractional Fourier and Hartley transforms," in *2014 19th International Conference on Digital Signal Processing*, pp. 694–698, Aug 2014.

[48] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image and vision computing*, vol. 24, no. 9, pp. 926–934, 2006.

[49] H. Huang and S. Yang, "Colour image encryption based on logistic mapping and double random-phase encoding," *IET Image Processing*, vol. 11, no. 4, pp. 211–216, 2017.

[50] X. Wu, B. Zhu, Y. Hu, and Y. Ran, "A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps," *IEEE Access*, vol. 5, pp. 6429–6436, 2017.

[51] X. Kang, R. Tao, and F. Zhang, "Multiple-parameter discrete fractional transform and its applications," *IEEE Transactions on Signal Processing*, vol. 64, pp. 3402–3417, July 2016.

[52] 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, 2015.

[53] L. Liu and S. Miao, "A new image encryption algorithm based on logistic chaotic map with varying parameter," *SpringerPlus*, vol. 5, no. 1, p. 289, 2016.

[54] H. M. Elhoseny, H. E. Ahmed, A. M. Abbas, H. B. Kazemian, O. S. Faragallah, S. M. El-Rabaie, and F. E. A. El-Samie, "Chaotic encryption of images in the fractional fourier transform domain using different modes of operation," *Signal, Image and Video Processing*, vol. 9, no. 3, pp. 611–622, 2015.