UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE TECNOLOGIA E GEOCIÊNCIAS
DEPARTAMENTO DE ELETRÔNICA E SISTEMAS
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

VERUSCA SEVERO DE LIMA

GENERALIZAÇÃO DE TRANSFORMADAS DO COSSENO BASEADA EM ROTAÇÕES: contribuições teóricas e cenários de aplicação

Recife
2020

VERUSCA SEVERO DE LIMA

GENERALIZAÇÃO DE TRANSFORMADAS DO COSSENO BASEADA EM ROTAÇÕES: contribuições teóricas e cenários de aplicação

Tese apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Pernambuco, Centro de Tecnologia e Geociências, como requisito parcial para obtenção do título de Doutor em Engenharia Elétrica.

Área de Concentração: Comunicações.

Orientador: Prof. Dr. Juliano Bandeira Lima

Coorientador: Prof. Dr. Francisco Madeiro Bernardino Junior

Recife

2020

Catalogação na fonte:
Bibliotecária Sandra Maria Neri Santiago, CRB-4 / 1267

L732g Lima, Verusca Severo de.
Generalização de transformadas do cosseno baseada em rotações: contribuições teóricas e cenários de aplicação / Verusca Severo de Lima. – 2020.
101 f.: il., figs., tabs., abrev. e siglas.

Orientador: Prof. Dr. Juliano Bandeira Lima.
Coorientador: Prof. Dr. Francisco Madeiro Bernardino Junior.
Tese (Doutorado) – Universidade Federal de Pernambuco. CTG. Programa de Pós-Graduação em Engenharia Elétrica. Recife, 2020.
Inclui referências e apêndice.

1. Engenharia elétrica. 2. Transformada de Fourier sobre grafos. 3. Transformadas discretas manobráveis do cosseno. 4. Transformadas numéricas manobráveis do cosseno. 5. Compressão de imagens tridimensionais. 6. Cifragem de imagens tridimensionais. I. Lima, Juliano Bandeira (Orientador). II. Bernardino Junior, Francisco Madeiro (Coorientador). III. Título.

UFPE

621.3 CDD (22. ed.) BCTG/2022-268

VERUSCA SEVERO DE LIMA

GENERALIZAÇÃO DE TRANSFORMADAS DO COSSENO BASEADA EM ROTAÇÕES: contribuições teóricas e cenários de aplicação

Tese apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Pernambuco, Centro de Tecnologia e Geociências, como requisito parcial para obtenção do título de Doutor em Engenharia Elétrica.

Área de Concentração: Comunicações.

Aprovado em: 09 / 12 / 2020 .

BANCA EXAMINADORA

Prof. Dr. Juliano Bandeira Lima (Orientador)
Universidade Federal de Pernambuco

Prof. Dr. Ricardo Menezes Campello de Souza (Examinador Interno)
Universidade Federal de Pernambuco

Prof. Dr. Renato José de Sobral Cintra (Examinador Interno)
Universidade Federal de Pernambuco

Prof. Dr. Carlos Alexandre Barros de Mello (Examinador Externo)
Universidade Federal de Pernambuco

Prof. Dr. Fernando José Ribeiro Sales (Examinador Externo)
Universidade Federal de Pernambuco

Dedico este trabalho à minha mãe, Verônica Neves (*in memoriam*), uma mulher guerreira e de muita fé, que me ensinou o significado da palavra perseverança e de amar a Deus de todo coração, mesmo diante de qualquer sofrimento. Obrigada, mãezinha, por tudo que deixaste em mim... “E o mundo que eu levar será tudo que você me ensinou, muita garra pra lutar e honestidade que eu só devo ao seu amor”.

AGRADECIMENTOS

Agradeço a Deus, acima de tudo, pelo dom da vida, por ser meu sustento e por guiar meus passos, me fazendo acreditar que Nele tudo posso.

Agradeço, com todo meu amor e gratidão, à minha família: aos meus pais, Miguel e Verônica (*in memoriam*), por toda dedicação e amor ofertados ao longo da minha vida; aos meus irmãos, Miélix (e sua amada família, Lidiane e Bento) e Raquel, companheiros de sonhos, tristezas e vitórias; à Quitéria, por toda sua dedicação e cuidado maternal; aos meus avós, de forma especial, minha avó Marinez, por seu carinho, suas orações e incentivo constante.

Aos amigos, presentes da vida, Thereza, Tayná, Huga e João Antônio pelo companheirismo e pelas palavras de incentivo em todos os momentos da vida.

Agradeço imensamente ao Prof. Juliano pela orientação desta Tese, pela dedicação e por seus ensinamentos, sem dúvida, é um grande exemplo de educador a ser seguido. Ao meu coorientador, Prof. Madeiro, por seus sábios ensinamentos, sua dedicação e disponibilidade, e por ser um grande incentivador de seus alunos: serei eternamente grata ao senhor.

Aos professores e amigos do Grupo de Pesquisa em Processamento de Sinais, pelos ensinamentos compartilhados, de forma especial, aos colegas Arquimedes, Ravi, Guilherme, Neto, Geraldo e Felipe. Ao Programa de Pós-Graduação em Engenharia Elétrica: aos professores e funcionários, em especial, Andréa Tenório por sua disponibilidade e presteza; e às amizades construídas, que se tornaram presentes, as quais quero levar para o resto da vida: Jamile, Tarcísio e Kádna.

À família POLI-UPE (Escola Politécnica de Pernambuco, Universidade de Pernambuco): às amizades da graduação e do mestrado cultivadas até hoje, em especial, aos amigos Jair, Israel, Cilena e Lúcia; aos amigos do grupo de pesquisa do mestrado, de forma especial, aos amigos Charles (*in memoriam*), Arthur, Ana Paula e Rodrigo; aos alunos e orientandos que tanto torceram por minha formação; e aos amigos professores pelos ensinamentos, palavras amigas e conselhos.

Por fim, agradeço à Coordenação de Aperfeiçoamento de Pessoal de Ensino Superior (CAPES) pelo apoio financeiro a este trabalho.

RESUMO

Transformadas como a de Fourier desempenham um papel fundamental no processamento de sinais. No entanto, quando os sinais são definidos sobre estruturas irregulares, as quais podem ser modeladas por meio de um grafo arbitrário, seu processamento pode ser feito empregando ferramentas próprias voltadas para a sua interpretação e análise. Nesse contexto, um tópico emergente é o do processamento de sinais sobre grafos (GSP, do inglês *graph signal processing*), que estende a teoria clássica de processamento de sinais para o domínio dos grafos. Também em GSP uma transformada de Fourier foi definida, a transformada de Fourier sobre grafos (GFT, do inglês *graph Fourier transform*), que resulta da autodecomposição do operador Laplaciano do grafo. Uma característica peculiar em GSP é que a GFT para grafos com topologias específicas coincide com transformadas discretas para sinais sobre domínios usuais. Esta característica é explorada nesta Tese com o propósito de definir novas transformadas discretas baseadas em rotações, as quais são denominadas transformadas manobráveis. Mais especificamente, o que se faz é rotacionar os vetores de base da transformada discreta que coincide com a GFT de um grafo específico. É definida a transformada discreta manobrável do cosseno para o espaço tridimensional (3D-SDCT, do inglês *three-dimensional steerable discrete cosine transform*). Um método de compressão de imagens tridimensionais baseado na 3D-SDCT é apresentado; os resultados obtidos superam aqueles conseguidos empregando a 3D-DCT (utilizando a mesma estratégia de quantização e codificação). Esta Tese também apresenta o estudo da multiplicidade dos autovalores do Laplaciano do produto de quatro grafos em caminho. Essa análise é o ponto chave para a definição de uma versão 4D da SDCT. Sobre corpos finitos, são apresentadas versões da SDCT e da 3D-SDCT, identificadas, respectivamente, pelos acrônimos SCNT (do inglês *steerable cosine number transform*) e 3D-SCNT, e que são definidas, respectivamente, a partir de rotações dos vetores de base da 2D-CNT e da 3D-CNT, usando um operador de rotação sobre corpos finitos. É apresentado um esquema de cifragem de imagens médicas tridimensionais baseado na 3D-SCNT, que usa os ângulos de rotação como parâmetros secretos. O referido esquema mostra-se robusto contra os principais ataques criptográficos e sensível a mudanças na chave secreta.

Palavras-chave: transformada de Fourier sobre grafos; transformadas discretas manobráveis do cosseno; transformadas numéricas manobráveis do cosseno; compressão de imagens tridimensionais; cifragem de imagens tridimensionais.

ABSTRACT

Transforms, such as the Fourier transform, play an essential role in signal processing. However, when we define signals over irregular structures, which can be modeled by an arbitrary graph, their processing can be performed using specific tools for their interpretation and analysis. In this context, graph signal processing (GSP) represents an emerging research topic, which extends the classical theory of signal processing to the domain of graphs. A Fourier transform was defined in GSP, the graph Fourier transform (GFT), which results from the graph Laplacian operator's eigendecomposition. A particular characteristic in GSP is that the GFT for graphs with specific topologies coincides with discrete transforms for signals over usual domains. Based on this fact, this Thesis defines new rotation-based discrete transforms, which are called steerable transforms. More specifically, a rotation is applied to the basis vectors of the discrete transform that coincides with the GFT for a specific graph. The three-dimensional steerable discrete cosine transform (3D-SDCT) is defined. A three-dimensional image compression method based on the 3D-SDCT is presented; the obtained results outperform those achieved using 3D-DCT (employing the same quantization and coding strategy). This Thesis also presents the study of the multiplicity of the Laplacians' eigenvalues of the product among four path graphs. This study is the key to define a 4D version of the SDCT. Versions of the SDCT and the 3D-SDCT over finite fields, respectively identified by the acronyms SCNT (steerable cosine number transform) and 3D-SCNT, are presented; they are defined, respectively, from the rotations of the basis vectors of the 2D-CNT and the 3D-CNT, using a finite field rotation operator. A three-dimensional medical image encryption scheme based on the 3D-SCNT is presented, using rotation angles as secret parameters. The proposed encryption scheme is robust against cryptographic attacks and sensitive to changes in the secret-key.

Keywords: graph Fourier transform; steerable discrete cosine transforms; steerable cosine number transforms; 3D image compression; 3D image encryption.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

2D	Espaço bidimensional (*Two-dimensional*)
3D	Espaço tridimensional (*Three-dimensional*)
4D	Espaço quadridimensional (*Four-dimensional*)
2D-DCT	Transformada discreta bidimensional do cosseno (*Two-dimensional discrete cosine transform*)
2D-DFT	Transformada discreta bidimensional de Fourier (*Two-dimensional discrete Fourier transform*)
2D-SDFT	Transformada discreta bidimensional manobrável de Fourier (*Two-dimensional steerable discrete Fourier transform*)
3D-CNT	Transformada numérica tridimensional do cosseno (*Three-dimensional cosine number transform*)
3D-DCT	Transformada discreta tridimensional do cosseno (*Three-dimensional discrete cosine transform*)
3D-SCNT	Transformada numérica tridimensional manobrável do cosseno (*Three-dimensional steerable cosine number transform*)
3D-SDCT	Transformada discreta tridimensional manobrável do cosseno (*Three-dimensional steerable discrete cosine transform*)
4D-DCT	Transformada discreta quadridimensional do cosseno (*Four-dimensional discrete cosine transform*)
BD	Delta de Bjøntegaard (*Bjøntegaard delta*)
bpp	*Bits* por *pixel* (*Bits per pixel*)
CNT	Transformada numérica do cosseno (*Cosine number transform*)
DCT	Transformada discreta do cosseno (*Discrete cosine transform*)

DFT	Transformada discreta de Fourier (*Discrete Fourier transform*)
DHT	Transformada discreta de Hartley (*Discrete Hartley transform*)
DST	Transformada discreta do seno (*Discrete sine transform*)
DWT	Transformada discreta de wavelet (*Discrete wavelet transform*)
FFFT	Transformada de Fourier sobre corpos finitos (*Finite field Fourier transform*)
FT	Transformada de Fourier (*Fourier transform*)
GFT	Transformada de Fourier sobre grafos (*Graph Fourier transform*)
GSP	Processamento de sinais sobre grafos (*Graph signal processing*)
LSB	*Bit* menos significativo (*Least significant bit*)
NPCR	Taxa do número de *pixels* modificados (*Number of pixels change rate*)
PSNR	Relação sinal-ruído de pico (*Peak signal-to-noise ratio*)
RD	Taxa-distorção (*Rate-distortion*)
SCNT	Transformada numérica manobrável do cosseno (*Steerable cosine number transform*)
SDCT	Transformada discreta manobrável do cosseno (*Steerable discrete cosine transform*)
SDFT	Transformada discreta manobrável de Fourier (*Steerable discrete Fourier transform*)
SSIM	Índice de similaridade estrutural (*Structural similarity index*)

TCIA	*The cancer imaging archive*
UACI	Intensidade média de mudança unificada (*Unified average changing intensity*)

LISTA DE SÍMBOLOS

$\mathcal{G}$	Grafo.
$\mathcal{V}$	Conjunto de vértices de $\mathcal{G}$.
$\mathcal{E}$	Conjunto de arestas de $\mathcal{G}$.
$\mathbf{A}(\mathcal{G})$	Matriz de adjacência de $\mathcal{G}$.
$\mathbf{D}(\mathcal{G})$	Matriz de grau de $\mathcal{G}$.
$\mathcal{P}_N$	Grafo em caminho com N vértices.
$\mathbf{L}(\mathcal{G})$	Matriz Laplaciana de $\mathcal{G}$.
$\square$	Produto Cartesiano de grafos.
$\otimes$	Produto de Kronecker.
$\mathcal{C}_N$	Grafo em ciclo com N vértices.
$\tau_{N,N}$	Grafo em grade toroidal com N^2 vértices.
$\mathcal{L}_N$	Grafo em grade cúbica com N^3 vértices.
$\mathbf{C}$	Matriz de transformação da 3D-DCT.
$\mathbf{F}$	3D-DCT de um sinal $\mathbf{f}$ com dimensão $N \times N \times N$.
$\bar{\mathbf{F}}$	Vetor formado pelos elementos de $\mathbf{F}$ tomados na ordem lexicográfica.
$\oplus$	Soma de Kronecker.
$\mathbf{I}_N$	Matriz identidade de ordem N.
$\mathbf{C}_{\mathrm{S}}(\boldsymbol{\Theta})$	Matriz de transformação da 3D-SDCT.
$\mathbf{R}(\boldsymbol{\Theta})$	Matriz de rotação da 3D-SDCT.
$\boldsymbol{\Theta}$	Vetor contendo todos os pares de ângulos empregados nas rotações das triplas de autovetores de $\mathbf{C}$.
M	Número de triplas de autovetores de $\mathbf{C}$ a serem rotacionados.
$\mathbf{F}_{\mathrm{S}}(\boldsymbol{\Theta})$	3D-SDCT de um sinal $\mathbf{f}$ com dimensão $N \times N \times N$.
$\mathbf{C}_{\text{4D-DCT}}$	Matriz de transformação da 4D-DCT.
$\mathcal{Z}_N$	Produto Cartesiano de quatro grafos em caminho.

$\mathbb{F}_p$	Corpo finito de característica p.
ζ	Elemento pertencente a $\mathbb{F}_p$.
$\mathbf{C}_{\mathbf{C}}$	Matriz de transformação da CNT.
$\mathrm{GI}(p)$	Conjunto dos inteiros Gaussianos módulo p.
$\mathbf{S}_{\boldsymbol{\alpha},\boldsymbol{\theta}}$	SCNT de um sinal s com dimensão $N \times N$.
$\boldsymbol{\alpha}$	Vetor contendo todos os elementos em relação aos quais os cossenos e senos em corpos finitos de ângulos de rotação são calculados.
R	Taxa de *bits*.
D	Distorção.
J	Função Lagrangeana.
γ	Multiplicador de Lagrange.
$\|\|.\|\|_i$	Norma l_i.
$\lceil x \rceil$	Converte um número real x no menor número inteiro maior ou igual a x.
$\|.\|$	Retorna a cardinalidade de seu argumento.
q	Passo de quantização.
$\mathbf{Q}$	Matriz de quantização.
$\mathbf{Q}'$	Matriz de quantização ordenada.
round(x)	Retorna o inteiro mais próximo de x.
$\mathbf{A}_{3D}$	Matriz da transformada de Arnold 3D.
r	Coeficiente de correlação.
cov(x, y)	Covariância.
var$(.)$	Variância.
$\overline{H}$	Entropia normalizada.

SUMÁRIO

1 INTRODUÇÃO

As transformadas têm um papel crucial em processamento e análise de sinais, permitindo o mapeamento de funções de um domínio para outro por meio de um conjunto de vetores (ou funções) de base. Parte da importância das transformadas deve-se ao fato de que no domínio transformado algumas propriedades relevantes do sinal ficam mais evidentes (SCHAFER; OPPENHEIM, 2010; POULARIKAS, 2010).

Uma classe importante de transformadas é a das transformadas discretas, as quais incluem a bem conhecida transformada discreta de Fourier (DFT, do inglês *discrete Fourier transform*). A DFT possui grande destaque na área de processamento de sinais graças à existência de algoritmos eficientes empregados para o seu cálculo. A transformada de um sinal discreto de comprimento finito N corresponde à representação deste sinal na base de funções que define a transformada em questão. As funções de base da DFT são exponenciais complexas $e^{j\frac{2\pi k}{N}}$, em que o índice k é associado ao domínio da frequência. A partir da substituição das funções de base da DFT por outras bases ortogonais, diferentes transformadas são definidas, tais como a transformada discreta de Hartley (DHT, do inglês *discrete Hartley transform*) (BRACEWELL, 1983), cujas funções de base são definidas pela função $\mathrm{cas}(.) = \cos(.) + \mathrm{sen}(.)$; a transformada discreta de wavelet (DWT, do inglês *discrete wavelet transform*) (HEIL; WALNUT, 1989; DAUBECHIES, 1990), que utiliza funções de base de suporte compacto, ou seja, de duração limitada; as transformadas discretas do cosseno (DCT, do inglês *discrete cosine transform*) e do seno (DST, do inglês *discrete sine transform*) (AHMED; NATARAJAN; RAO, 1974; STRANG, 1999; MARTUCCI, 1994), cujas funções de base correspondem, repectivamente, às funções cosseno e seno; entre outras.

As transformadas supracitadas foram, inicialmente, definidas sobre corpos infinitos, seja sobre o conjunto dos números reais ou dos complexos. No entanto, após a definição da transformada de Fourier sobre corpos finitos (FFFT, do inglês *finite field Fourier transform*) apresentada por John M. Pollard, em 1971, em seu artigo intitulado "The fast Fourier transform in a finite field" (POLLARD, 1971), versões sobre corpos finitos das transformadas clássicas têm sido definidas (CAMPELLO DE SOUZA et al., 1998; CAMPELLO DE SOUZA; H. M. DE OLIVEIRA; KAUFFMAN, 2000; POOR, 1996; CAMPELLO DE SOUZA et al., 2004; CAMPELLO DE SOUZA et al., 2005; LIMA; CAMPELLO DE SOUZA, 2011). Basicamente, um corpo finito denotado por $\mathbb{F}_q$ ou $\mathrm{GF}(q)$ (do inglês, *Galois Field*) é constituído por um conjunto F de $q < \infty$ elementos ($q_{\min} = 2$, ou seja, contém no mínimo dois elementos), em que q é uma potência de um número primo p ($q = p^m$, com $m \geq 1$), munido de duas operações (multiplicação e adição) que possuem inversa (BLAHUT, 2010). O estudo de transformadas sobre corpos finitos tem ganho destaque devido ao universo de aplicações possíveis em que ela pode ser utilizada, aplicações para as quais, em contrapartida, as transformadas definidas no domínio clássico não são adequadas. Esse destaque vem, em parte, do fato de as transformadas sobre corpos finitos não exigirem operações de ponto flutuante, uma vez que as operações de adição e multiplicação

sobre o corpo em questão envolvem apenas operações da aritmética modular, além do que, é possível reduzir a complexidade computacional envolvida no cálculo da transformada, a partir da implementação das operações modulares por meio de deslocamentos. Dentre as diversas áreas de aplicação das transformadas sobre corpos finitos, pode-se destacar, por exemplo, esquemas de cifragem de imagens digitais (LIMA; LIMA; MADEIRO, 2013; LIMA; MADEIRO; SALES, 2015; LIMA; NOVAES, 2014), sistemas de múltiplo acesso (MIRANDA; DE OLIVEIRA, 2001; DE OLIVEIRA; MIRANDA; CAMPELLO DE SOUZA, 2001), entre outras.

É notório, pelo universo de aplicações encontrado na literatura, que as transformadas desempenham um papel fundamental no processamento de sinais. No entanto, quando os sinais são definidos sobre estruturas irregulares, as quais podem ser modeladas por meio de um grafo arbitrário, o seu processamento pode ser realizado empregando ferramentas próprias voltadas para sua interpretação e análise. Nesse contexto, um tópico que vem se tornando objeto de estudo para muitos pesquisadores é o do processamento de sinais sobre grafos (GSP, do inglês *graph signal processing*) (SHUMAN et al., 2013; ORTEGA et al., 2018), que busca estender a teoria clássica de processamento de sinais para o domínio dos grafos, preocupando-se com a modelagem, representação e processamento de sinais definidos sobre grafos.

Grafos têm sido utilizados para modelar vários sistemas reais. No campo de processamento de imagem, por exemplo, um grafo pode ser utilizado para modelar uma imagem, em que *pixels* ou regiões da imagem podem ser modelados como os vértices do grafo e a conectividade desses elementos pode ser modelada como as arestas do grafo (SHUMAN et al., 2013). A modelagem de sinais sobre grafos exige o uso de ferramentas especializadas no processamento de sinais sobre grafos. Nesse cenário, uma transformada de Fourier foi definida, sendo resultado da autodecomposição do operador Laplaciano do grafo e identificada pelo acrônimo GFT (do inglês *graph Fourier transform*) (SHUMAN et al., 2013). A GFT de um sinal definido sobre um grafo corresponde à representação deste sinal em uma base formada por autovetores da matriz Laplaciana do grafo em questão. Uma característica peculiar em GSP é explorada em (FRACASTORO; FOSSON; MAGLI, 2017; FRACASTORO; MAGLI, 2017): são identificadas coincidências entre a GFT para grafos com topologias específicas e as transformadas discretas para sinais sobre domínios regulares (transformadas do processamento clássico de sinais); essa coincidência foi explorada e novas transformadas discretas correspondentes a versões rotacionadas de transformadas discretas já definidas no cenário de processamento digital de sinais foram definidas. Essas novas transformadas baseadas em rotações são obtidas, fundamentalmente, a partir da rotação de vetores de base da transformada discreta em sua versão primitiva (original), os quais são agrupados segundo o autovalor ao qual estão associados na matriz Laplaciana de um grafo particular.

Motivada pelo cenário exposto, esta Tese tem como objetivo principal a definição de novas transformadas discretas basedas em rotações, seja sobre corpos infinitos ou finitos, estendendo a metodologia utilizada em (FRACASTORO; FOSSON; MAGLI, 2017; FRACASTORO; MAGLI, 2017), a qual, por sua vez, lança mão do paralelo entre as transformadas de sinais

definidos sobre grafos e sobre o domínio clássico de sinais para projetar novas trasformadas. Além disso, também é objetivo desta Tese avaliar a aplicação dessas novas transformadas em cenários de compressão e cifragem de imagens. Com isso, busca-se contribuir com avanços na área de transformadas discretas, apresentando novas ferramentas para a análise e processamento de sinais. A seguir, são apresentadas as contribuições e descrita a estrutura desta Tese.

1.1 CONTRIBUIÇÕES

As seguintes contribuições desta Tese podem ser elencadas:

- A definição de uma transformada discreta manobrável do cosseno (SDCT, do inglês *steerable discrete cosine transform*) para o espaço tridimensional (3D-SDCT), que corresponde à extensão da SDCT previamente definida em (FRACASTORO; FOSSON; MAGLI, 2017).
- A análise da multiplicidade dos autovalores da transformada discreta quadridimensional do cosseno (4D-DCT, do inglês *four-dimensional discrete cosine transform*), que constitui uma possível autobase para o Laplaciano do produto de quatro grafos em caminho. Essa análise é o ponto chave para a definição de uma versão 4D da SDCT.
- A extensão da SDCT para o cenário de corpos finitos, com a definição de uma transformada numérica manobrável do cosseno (SCNT, do inglês *steerable cosine number transform*), obtida a partir do emprego de funções trigonométricas sobre corpos finitos.
- A extensão da SCNT para o espaço tridimensional, resultando na definição da 3D-SCNT.
- Proposta de um método de compressão de imagens tridimensionais baseado na 3D-SDCT.
- Proposta de um esquema para cifragem de imagens médicas tridimensionais baseado na 3D-SCNT.

1.2 ESTRUTURA DA TESE

Após esta introdução, a presente Tese está estruturada da seguinte maneira:

- O Capítulo 2 apresenta uma breve revisão sobre grafos, com foco no processamento de sinais sobre grafos, apresentando a definição da transformada de Fourier sobre grafos e sua relação com transformadas clássicas existentes. Também é apresentado o método proposto em (FRACASTORO; FOSSON; MAGLI, 2017; FRACASTORO; MAGLI, 2017) para definir a SDCT e as transformadas discretas manobráveis de Fourier (SDFT, do inglês *steerable discrete Fourier transform*) para uma dimensão, a 1D-SDFT, e para duas dimensões, a 2D-SDFT. Por fim, o capítulo apresenta uma generalização proposta na literatura para projetar transformadas manobráveis a partir de qualquer transformada bidimensional separável.

- No Capítulo 3, é apresentado o desenvolvimento da SDCT para o espaço tridimensional (3D-SDCT), e estudada a multiplicidade dos autovalores do Laplaciano do produto de quatro grafos em caminho, que é essencial para a definição de uma possível versão 4D da SDCT. A 3D-SDCT é obtida a partir da rotação da base da transformada discreta em sua versão original (3D-DCT). Neste capítulo, é abordado também, para o espaço tridimensional, o conceito de rotação "ótima" (em termos de possibilidade de compactar energia de forma mais eficiente do que a 3D-SDCT com rotação não ótima), que permite obter um maior número de coeficientes nulos da 3D-SDCT; mostra-se, por meio de uma escolha conveniente de ângulos de rotação, que $\frac{2}{3}$ dos coeficientes 3D-SDCT rotacionados podem ser anulados.

- O Capítulo 4 apresenta a extensão das transformadas SDCT e 3D-SDCT para o cenário de corpos finitos. As abordagens propostas exploram as propriedades da diagonalização da CNT para realizar a definição das transformadas. O cálculo da SCNT sobre uma estrutura bidimensional é ilustrado como forma de exemplificar a construção da transformada.

- O Capítulo 5 apresenta dois cenários de aplicação para as transformadas tridimensionais propostas nesta Tese. Para o primeiro cenário, é apresentado um método de compressão de imagens tridimensionais baseado na 3D-SDCT, considerando o caso em que um único par de ângulos de rotação é utilizado para cada bloco, rotacionando todos os vetores de base 3D-DCT pelo mesmo par. Os resultados são comparados com a 3D-DCT usual, utilizando a mesma estratégia de quantização e codificação. Para o segundo cenário, é introduzido um esquema de cifragem de imagens médicas tridimensionais baseado na 3D-SCNT, que usa os ângulos de rotação como parâmetros secretos do esquema, mais especificamente, usados para transformar o primeiro bloco da imagem. A sequência de ângulos usada nos blocos seguintes são versões sucessivamente deslocadas ciclicamente da primeira sequência. O método é avaliado a partir da análise de sua resistência contra alguns ataques criptográficos, incluindo o estudo de sua sensibilidade a mudanças nos parâmetros empregados no esquema.

- Por fim, no Capítulo 6, são apresentadas as conclusões, com uma sumarização das principais contribuições desta pesquisa, as publicações resultantes desta Tese e uma relação de possíveis trabalhos futuros.

2 TRANSFORMADAS MANOBRÁVEIS

Este é um capítulo de revisão de literatura que tem por objetivo apresentar as definições necessárias para o desenvolvimento desta Tese. O capítulo encontra-se dividido em três seções.

A Seção 2.1 apresenta a definição da transformada discreta manobrável do cosseno (SDCT, do inglês *steerable discrete cosine transform*). Explorando as propriedades da GFT de um grafo em grade (produto entre dois grafos em caminho), em (FRACASTORO; FOSSON; MAGLI, 2017) os autores definiram a SDCT a partir da relação entre a transformada discreta bidimensional do cosseno (2D-DCT, do inglês *two-dimensional discrete cosine transform*) e a GFT de um grafo em grade. A SDCT parte do princípio de que os vetores de base da 2D-DCT formam uma autobase para o Laplaciano do grafo em grade e é definida pela rotação da base da 2D-DCT.

Em (FRACASTORO; MAGLI, 2017), por sua vez, os autores exploraram a GFT em grafos dos tipos ciclo e toroidal e propuseram uma nova generalização para a DFT, a transformada discreta manobrável de Fourier (SDFT, do inglês *steerable discrete Fourier transform*), que pode ser definida em uma ou duas dimensões. A transformada é apresentada na Seção 2.2. Para uma dimensão, a 1D-SDFT parte da definição da GFT de um grafo em ciclo, enquanto, para duas dimensões, a 2D-SDFT parte da definição da GFT de um grafo em grade toroidal. A SDFT pode ser relacionada com outras transformações conhecidas, como, por exemplo, as transformadas Fourier-seno e Fourier-cosseno.

A Seção 2.3 apresenta o método proposto em (MASERA et al., 2019), que corresponde a uma generalização dos métodos utilizados em (FRACASTORO; FOSSON; MAGLI, 2017) e em (FRACASTORO; MAGLI, 2017), para projetar transformadas manobráveis a partir de qualquer transformada bidimensional separável.

Para a definição da SDCT e da SDFT, o capítulo inicia com uma revisão dos fundamentos do processamento de sinais sobre grafos, apresentando o conceito da GFT.

2.1 TRANSFORMADA DISCRETA MANOBRÁVEL DO COSSENO

Esta seção apresenta uma revisão sobre a SDCT. Inicialmente é feita uma introdução sobre grafos, com foco no processamento de sinais sobre grafos, buscando uma relação entre a transformada de Fourier sobre grafos e a transformada discreta do cosseno.

2.1.1 Fundamentos do Processamento de Sinais sobre Grafos

Grafos são considerados uma importante e poderosa ferramenta de abstração que facilita a compreensão, modelagem e solução de problemas em que exista um conjunto de elementos de algum modo relacionados. A primeira evidência da utilização de grafos remete-se ao ano de 1736, pelo matemático suíço Leonhard Euler, que fez uso dos grafos para resolver o problema clássico das pontes de Königsberg, problema hoje conhecido como “As sete pontes de Königsberg” (EU-

LER, 1736). Desde então, grafos vem sendo extensivamente utilizados para analisar uma grande variedade de sistemas reais, como por exemplo: tráfego em redes de transporte (MOHAN et al., 2014; HUANG et al., 2016; DERI; MOURA, 2016; HACKL; ADEY, 2019; AHMADZAI; RAO; ULFAT, 2019), a dinâmica da rede cerebral (BULLMORE; SPORNS, 2009; RUBINOV; SPORNS, 2010; SPORNS, 2018; FARAHANI; KARWOWSKI; LIGHTHALL, 2019; ATAL; SINGH, 2020), dados de usuários em mídias sociais (GRANDO; NOBLE; LAMB, 2016; PEREIRA; AMO; GAMA, 2016; ZHANG; MOURA, 2014; CHAKRABORTY et al., 2018), entre outros.

Seja $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ um grafo definido por um conjunto de N vértices $\mathcal{V} = \{v_i, i = 0, 1, \ldots, N-1\}$ e um conjunto de arestas $\mathcal{E}$, em que $\mathcal{E} \subset \mathcal{V}^2$ ($\mathcal{E}$ é um subconjunto de $\mathcal{V}^2$). A matriz de adjacência $\mathbf{A}(\mathcal{G})$, que armazena o relacionamento entre os vértices do grafo, é a matriz quadrada de ordem N cujas entradas são definidas por (DIESTEL, 1997)

$$a_{ij} = \begin{cases} 1, & \text{se} \quad \{v_i, v_j\} \in \mathcal{E}, \\ 0, & \text{caso contrário.} \end{cases} \tag{1}$$

Denota-se grau, ou valência, do vértice v_i de um grafo $\mathcal{G}$ por $g(v_i)$, que corresponde ao número de arestas adjacentes a cada vértice v_i de $\mathcal{G}$. $\mathbf{D}(\mathcal{G})$ é uma matriz diagonal, que contém os graus dos vértices de $\mathcal{G}$, cujas entradas são definidas por

$$d_{ij} = \begin{cases} g(v_i), & \text{se} \quad i = j, \\ 0, & \text{caso contrário.} \end{cases} \tag{2}$$

Por exemplo, para um grafo em caminho (*path graph*), $\mathcal{P}_4$, com 4 vértices (grafo que apresenta topologia em linha) ilustrado pela Figura 1, as matrizes de adjacência e de grau de $\mathcal{P}_4$ são dadas, respectivamente por

$$\mathbf{A}(\mathcal{P}_4) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{3}$$

e

$$\mathbf{D}(\mathcal{P}_4) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{4}$$

A matriz Laplaciana de $\mathcal{G}$, denotada por $\mathbf{L}(\mathcal{G})$, desempenha um papel relevante em diversas aplicações (SHUAI; ZHENG; YANGMING, 2013; LIU; CHEUNG; WU, 2015; BATABYAL; ACTON, 2017; TANG et al., 2016; YU et al., 2016), e é obtida pela subtração matricial (CHUNG, 1997)

$$\mathbf{L}(\mathcal{G}) = \mathbf{D}(\mathcal{G}) - \mathbf{A}(\mathcal{G}). \tag{5}$$

Figura 1 – Grafo em caminho $\mathcal{P}_4$.

Fonte: A autora (2020).

A teoria de processamento de sinais sobre grafos (GSP) (SHUMAN et al., 2013) foi desenvolvida a partir da investigação do espectro de $\mathbf{L}(\mathcal{G})$ para o caso de grafos não direcionados (que não são orientados) e com arestas de peso real não-negativo, em que $\mathbf{A}(\mathcal{G})$ se apresenta como uma matriz simétrica e real. Para esse tipo de grafo, $\mathbf{L}(\mathcal{G})$ também será uma matriz simétrica e real, pois $\mathbf{D}(\mathcal{G})$ é uma matriz diagonal; portanto, $\mathbf{L}(\mathcal{G})$ é diagonalizável por uma matriz ortogonal

$$\mathbf{L}(\mathcal{G}) = \mathbf{U}\mathbf{\Lambda}\mathbf{U}^{-1}, \tag{6}$$

em que as colunas $\mathbf{u_0}, \mathbf{u_1}, \ldots, \mathbf{u_{N-1}}$ da matriz $\mathbf{U} = \{\mathbf{u_0}\mathbf{u_1} \ldots \mathbf{u_{N-1}}\} \in \mathbb{R}^{N \times N}$ correspondem aos autovetores de $\mathbf{L}(\mathcal{G})$ e $\mathbf{\Lambda} \in \mathbb{R}^{N \times N}$ é a matriz diagonal dos autovalores correspondentes $\lambda_0, \ldots, \lambda_{N-1}$ de $\mathbf{L}(\mathcal{G})$ (SHUMAN et al., 2013).

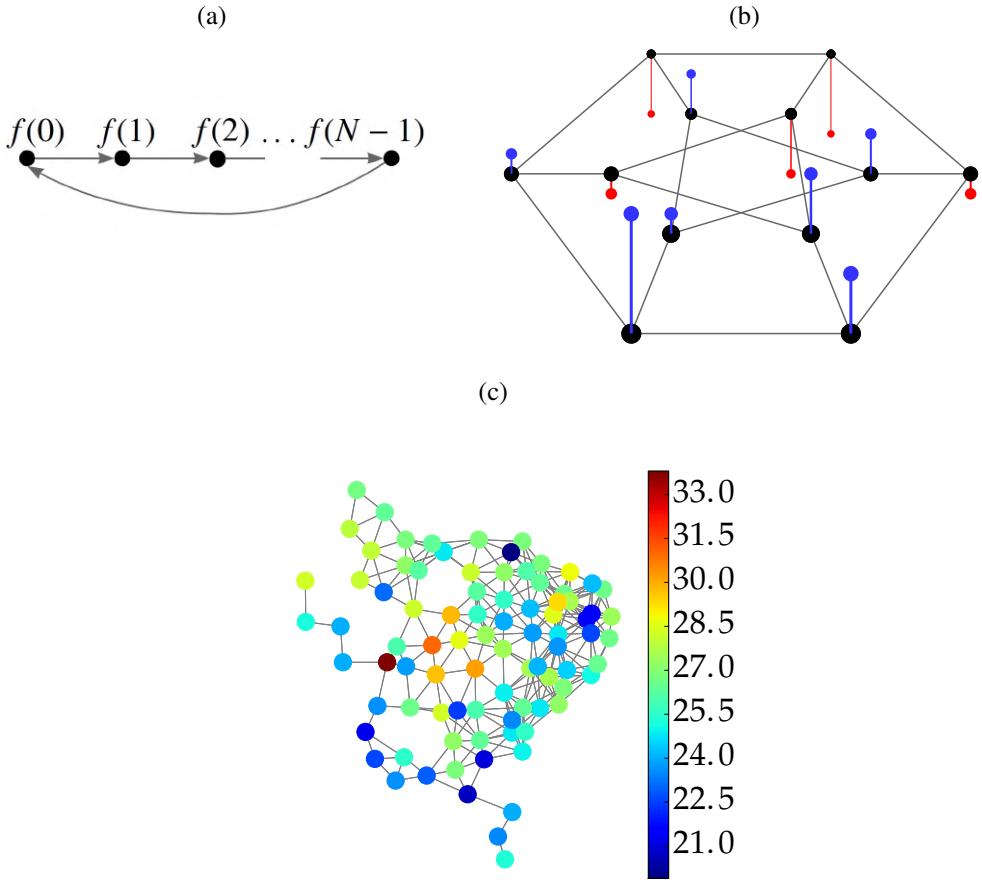
Em GSP, define-se um sinal $\mathbf{f}$ sobre o grafo $\mathcal{G}$ como sendo um mapeamento de $\mathbf{f}$ nos vértices de $\mathcal{G}$, em que $f(i)$, $i = 0, 1, \ldots, N-1$, está associado ao vértice $v_i \in \mathcal{V}$. O sinal sobre o grafo pode ser escrito como um vetor, como segue

$$\mathbf{f} = [f(0), f(1), \ldots, f(N-1)] \in \mathbb{R}^N. \tag{7}$$

A Figura 2 fornece exemplos de representações de sinais sobre grafos, nos quais a rotulação do vértice é omitida por uma questão de simplicidade, pois é assumido que $f(i)$ é atribuída ao vértice v_i. O grafo em ciclo $\mathcal{C}_N$, ilustrado na Figura 2a, modela o domínio de tempo discreto de comprimento finito; suas arestas direcionadas modelam a causalidade do domínio do tempo, enquanto a aresta de *feedback* considera a condição de contorno da periodicidade imposta pela análise DFT. O valor numérico de cada amostra de sinal $f(i)$ é indicado ao lado do vértice v_i ao qual a amostra está associada. A Figura 2b ilustra o grafo de Dürer, em que o tamanho (altura) do pulso em cada vértice v_i representa o valor da amostra do sinal em v_i. A Figura 2c mostra um exemplo de sinal definido por uma rede de sensores em malha, com as arestas ponderadas usando o inverso da distância Euclidiana, que surge em muitos cenários, como aplicações da Internet das Coisas (IoT) (MA; YAO; YAO, 2016); os valores das amostras do sinal são representados com o uso de codificação (escala) de cores.

O GSP busca estender a teoria clássica de processamento de sinais para o domínio dos grafos, preocupando-se com a modelagem, representação e processamento de sinais definidos em grafos. Entre as ferramentas de processamento de sinais, transformadas como a de Fourier (FT, do inglês *Fourier transform*) desempenham um papel fundamental na análise de sinais. Também em GSP, uma transformada de Fourier foi definida, a transformada de Fourier sobre

Figura 2 – Representações de sinais sobre grafos: (a) grafo em ciclo direcionado, (b) grafo de Dürer não direcionado e (c) grafo de cidades da região Nordeste do Brasil sobre o qual foi definido um sinal de medições de temperatura a partir de 1° de Fevereiro de 2012, extraído do Banco de Dados Meteorológicos para Ensino e Pesquisa, disponível em: http://www.inmet.gov.br/portal/index.php?r=bdmep/bdmep.



Fonte: Ribeiro (2018).

grafos (GFT), que, de certo modo, pode ser vista como uma generalização da FT, que consiste, basicamente, em representar um sinal em termos de exponenciais complexas $e^{2\pi i\xi t}$, que são autofunções do operador unidimensional de Laplace $\frac{d^2}{dt^2}$. A GFT corresponde à representação de um sinal sobre um grafo em uma autobase do operador Laplaciano do respectivo grafo. Mais especificamente, para um sinal $\mathbf{f} \in \mathbb{R}^N$ sobre o grafo $\mathcal{G}$, a GFT consiste na expansão de $\mathbf{f}$ em termos dos autovetores do Laplaciano de $\mathcal{G}$, como segue

$$\hat{f}(\lambda_l) \coloneqq \langle \mathbf{f}, \mathbf{u}_l \rangle = \sum_{i=0}^{N-1} f(i) u_l^*(i). \tag{8}$$

A GFT inversa é obtida por

$$f(i) = \sum_{l=0}^{N-1} \hat{f}(\lambda_l) u_l(i). \tag{9}$$

A GFT para um grafo com uma topologia específica pode ser relacionada com algumas transformadas existentes. Por exemplo, a DCT é equivalente à GFT de um grafo em caminho

(Figura 1 para $N = 4$). Os autovetores de $\mathbf{L}(\mathcal{P}_\mathcal{N})$ são iguais aos vetores de base da DCT, mais precisamente a DCT tipo 2 (STRANG, 1999), e são definidos como

$$\mathbf{v}_j^{(k)} = \cos\left(\frac{\pi k}{N}\left(j + \frac{1}{2}\right)\right),\ j, k = 0, 1, \ldots, N-1. \tag{10}$$

Cada $\mathbf{v}_j^{(k)}, j = 0, 1, \ldots, N-1$, é um autovetor de $\mathbf{L}(\mathcal{P}_\mathbf{N})$ associado ao autovalor

$$\lambda_k = 4\,\mathrm{sen}^2\left(\frac{\pi k}{2N}\right). \tag{11}$$

Como a multiplicidade dos autovalores λ_k é sempre igual a 1, a base DCT é a única autobase para $\mathbf{L}(\mathcal{P}_\mathbf{N})$. Logo, a GFT para um sinal representado por um grafo em caminho é equivalente à transformada DCT.

O produto Cartesiano entre dois grafos em caminho, $\mathcal{P}_N \square \mathcal{P}_N$, em que $\square$ denota o produto Cartesiano de grafos, corresponde a um grafo em grade, com N^2 vértices, como mostrado na Figura 3 para $N = 4$. Os vetores de base da 2D-DCT formam uma autobase de $\mathbf{L}(\mathcal{P}_\mathbf{N} \square \mathcal{P}_\mathbf{N})$ (ZHANG; FLORÊNCIO, 2013).

De acordo com (MERRIS, 1994; MERRI, 1998), os autovalores de $\mathbf{L}(\mathcal{P}_\mathbf{N} \square \mathcal{P}_\mathbf{N})$ são todas as possíveis somas

$$\lambda_{k,l}(\mathcal{P}_N \square \mathcal{P}_N) = \lambda_k(\mathcal{P}_N) + \lambda_l(\mathcal{P}_N) \tag{12}$$

e os autovetores correspondentes são determinados pelo produto de Kronecker entre os respectivos autovetores de $\mathcal{P}_N$, isto é,

$$\mathbf{v}^{(k,l)} = \mathbf{v}^{(k)} \otimes \mathbf{v}^{(l)}, \qquad k, l = 0, 1, \ldots, N-1, \tag{13}$$

em que $\mathbf{v}^{(k)}$ é o autovetor de $\mathcal{P}_N$ correspondente a λ_k e $\mathbf{v}^{(l)}$ é o autovetor correspondente a λ_l.

2.1.2 Análise da Multiplicidade dos Autovalores

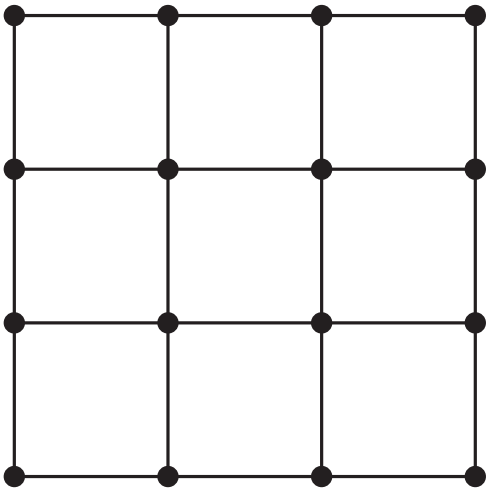
De acordo com (12), os autovalores de $\mathbf{L}(\mathcal{P}_N \square \mathcal{P}_N)$ são dados por

$$\lambda_{k,l}(\mathcal{P}_N \square \mathcal{P}_N) = 4\,\mathrm{sen}^2\left(\frac{\pi k}{2N}\right) + 4\,\mathrm{sen}^2\left(\frac{\pi l}{2N}\right). \tag{14}$$

Nota-se que alguns autovalores aparecem repetidos devido à simetria $\lambda_{k,l} = \lambda_{l,k}$ para $k \neq l$. Analisando a multiplicidade algébrica em (14), tem-se:

- O autovalor $\lambda_{k,l} = 4$ tem multiplicidade $N - 1$ e corresponde a todos os autovalores $\lambda_{k,N-k}$ com $1 \leq k \leq N - 1$.
- O autovalor $\lambda_{k,l}$ é igual a $\lambda_{l,k}$ quando $k \neq l$. Devido à simetria, $\lambda_{k,l} = \lambda_k + \lambda_l = \lambda_l + \lambda_k = \lambda_{l,k}$, apresentando multiplicidade igual a 2.

Figura 3 – Grafo em grade $\mathcal{P}_4 \square \mathcal{P}_4$.



Fonte: A autora (2020).

- O autovalor $\lambda_{k,l}$ tem multiplicidade igual a 1, quando $k = l$ com $k \neq \frac{N}{2}$ (recai no caso de $\lambda_{k,l} = 4$). Logo, no espectro de $\mathbf{L}(\mathcal{P}_\mathbf{N} \square \mathcal{P}_\mathbf{N})$ há $N - 1$ autovalores com multiplicidade algébrica igual a 1.

De acordo com (13), os autovetores de $\mathbf{L}(\mathcal{P}_\mathbf{N} \square \mathcal{P}_\mathbf{N})$ são obtidos a partir do produto de Kronecker. Os autovetores $\mathbf{v}^{(k,l)}$ e $\mathbf{v}^{(l,k)}$ são linearmente independentes (ainda que $\lambda_{k,l} = \lambda_{l,k}$, quando $k \neq l$) pois o produto de Kronecker não é comutativo. Portanto, a multiplicidade geométrica é igual à multiplicidade algébrica. A dimensão do autoespaço correspondente aos autovalores é maior do que 1. Assim, a base da 2D-DCT não é a única autobase para $\mathbf{L}(\mathcal{P}_\mathbf{N} \square \mathcal{P}_\mathbf{N})$.

2.1.3 Definição da Transformada

A partir da relação entre a 2D-DCT e a GFT de um sinal sobre um grafo em grade $\mathcal{P}_N \square \mathcal{P}_N$, em (FRACASTORO; FOSSON; MAGLI, 2017), os autores propuseram a SDCT, utilizando o fato de que os vetores de base da 2D-DCT formam uma possível autobase para o Laplaciano do grafo em grade $\mathbf{L}(\mathcal{P}_\mathbf{N} \square \mathcal{P}_\mathbf{N})$. Uma vez que a base da 2D-DCT não é a única autobase para $\mathbf{L}(\mathcal{P}_\mathbf{N} \square \mathcal{P}_\mathbf{N})$, é possível encontrar outras autobases a partir da rotação dos autovetores.

Seja $\lambda_{k,l}$ um autovalor de $\mathbf{L}(\mathcal{P}_\mathbf{N} \square \mathcal{P}_\mathbf{N})$ com multiplicidade 2 e sejam $\mathbf{v}^{(k,l)}$ e $\mathbf{v}^{(l,k)}$ dois vetores de base da 2D-DCT que são autovetores de $\mathbf{L}(\mathcal{P}_\mathbf{N} \square \mathcal{P}_\mathbf{N})$ associados a $\lambda_{k,l}$. Substituindo $\mathbf{v}^{(k,l)}$ e $\mathbf{v}^{(l,k)}$, com suas componentes rearrajandas em vetores linha com N^2 componentes, por suas respectivas versões rotacionadas $\mathbf{v}^{(k,l)'}$ e $\mathbf{v}^{(l,k)'}$, como segue

$$\begin{bmatrix} \mathbf{v}^{(k,l)'} \\ \mathbf{v}^{(l,k)'} \end{bmatrix} = \begin{bmatrix} \cos\theta_{k,l} & \operatorname{sen}\theta_{k,l} \\ -\operatorname{sen}\theta_{k,l} & \cos\theta_{k,l} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{v}^{(k,l)} \\ \mathbf{v}^{(l,k)} \end{bmatrix}, \tag{15}$$

em que $\theta_{k,l}$ é um ângulo em $[0, 2\pi]$, uma nova base é obtida, à qual está associada a transformada discreta manobrável do cosseno, identificada como SDCT.

Os $N-1$ autovetores correspondentes a $\lambda_{k,N-k}=4$ são rotacionados aos pares $\mathbf{v}^{(k,N-k)}$ e $\mathbf{v}^{(N-k,k)}$. Se N for par, $\mathbf{v}^{\left(\frac{N}{2},\frac{N}{2}\right)}$ não é rotacionado. O operador matricial associado à SDCT pode ser expresso como

$$\mathbf{V}(\boldsymbol{\theta})=\mathbf{R}(\boldsymbol{\theta})\mathbf{V}, \tag{16}$$

em que $\mathbf{V}=\mathbf{V}(\mathbf{0})\in\mathbb{R}^{N^2\times N^2}$ é a matriz da 2D-DCT, $\mathbf{R}(\boldsymbol{\theta})\in\mathbb{R}^{N^2\times N^2}$ é uma matriz esparsa de rotação, construída de acordo com (15), $\boldsymbol{\theta}\in\mathbb{R}^{\text{ang}_1}$, com $\text{ang}_1=N(N-1)/2$, é o vetor contendo todos os ângulos utilizados, e $\mathbf{0}$ é um vetor nulo com comprimento igual ao do vetor $\boldsymbol{\theta}$.

Para qualquer sinal $\mathbf{f}\in\mathbb{R}^{N^2}$, a SDCT é dada por

$$\hat{\mathbf{f}}=\mathbf{V}(\boldsymbol{\theta})\mathbf{f}=\mathbf{R}(\boldsymbol{\theta})\mathbf{V}\mathbf{f}. \tag{17}$$

A Expressão (17) mostra que a SDCT pode ser decomposta como um produto da matriz de rotação $\mathbf{R}(\boldsymbol{\theta})$ e a matriz de transformação $\mathbf{V}$ da 2D-DCT. Portanto, seja $\hat{\mathbf{f}}_{DCT}\in\mathbb{R}^{N^2}$ o vetor de coeficientes DCT do sinal $\mathbf{f}$, a SDCT desse sinal pode ser obtida por

$$\hat{\mathbf{f}}=\mathbf{R}(\boldsymbol{\theta})\hat{\mathbf{f}}_{DCT}. \tag{18}$$

De acordo com (18), dado os coeficientes $\hat{\mathbf{f}}_{DCT}$, a complexidade adicional para obtenção da SDCT se resume ao produto entre a matriz esparsa de rotação $\mathbf{R}(\boldsymbol{\theta})$ e $\hat{\mathbf{f}}_{DCT}$, o qual envolve, no máximo, um total de $N(N-1)$ operações de soma e $2N(N-1)$ operações de multiplicação (um total de $N(N-1)/2$ pares de vetores são rotacionados no cálculo da SDCT). Logo, assintoticamente, a complexidade total envolvida no cálculo de uma SDCT é a mesma para o cálculo da respectiva 2D-DCT.

2.2 TRANSFORMADA DISCRETA MANOBRÁVEL DE FOURIER

Nesta seção, é revisada a definição da transformada discreta manobrável de Fourier que pode ser definida em uma dimensão (1D-SDFT) e em duas dimensões (2D-SDFT).

2.2.1 1D-SDFT

A transformada discreta de Fourier (DFT) de um sinal $f\in\mathbb{R}^N$ é definida por

$$\hat{\mathbf{f}}_k=\sum_{n=0}^{N-1}f_n e^{-j\frac{2\pi kn}{N}},\ k=0,1,\ldots,N-1. \tag{19}$$

A transformada inversa é calculada por

$$f_n=\frac{1}{N}\sum_{k=0}^{N-1}\hat{\mathbf{f}}_k e^{j\frac{2\pi kn}{N}},\ n=0,1,\ldots,N-1. \tag{20}$$

Na forma matricial, o cálculo da DFT de $\mathbf{f}$ pode ser expresso como

$$\hat{\mathbf{f}}=\mathbf{V}\mathbf{f}, \tag{21}$$

em que $\mathbf{V} \in \mathbb{C}^{N\times N}$ é a matriz de transformação da DFT, com $\mathbf{V}_{kn} = e^{-j\frac{2\pi kn}{N}} = \rho_k^n$ para $k, n = 0, 1, \ldots, N-1$, que apresenta a propriedade de suas linhas serem autovetores de qualquer matriz circulante (GRADY; POLIMENI, 2010).

Uma matriz quadrada $\mathbf{M}$ de ordem N é chamada de circulante quando cada uma de suas linhas (após a primeira) é obtida por um deslocamento cíclico de uma posição da linha anterior, de modo que se tem

$$\mathbf{M} = \begin{bmatrix} l_0 & l_1 & l_2 & \ldots & l_{N-1} \\ l_{N-1} & l_0 & l_1 & \ldots & l_{N-2} \\ l_{N-2} & l_{N-1} & l_0 & \ldots & l_{N-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ l_1 & l_2 & l_3 & \ldots & l_0 \end{bmatrix}. \tag{22}$$

A matriz circulante $\mathbf{M}$ apresenta N autovetores ortogonais (TEE, 2007)

$$\mathbf{v}^k = \begin{bmatrix} 1 \\ \rho_k \\ \rho_k^2 \\ \vdots \\ \rho_k^{N-1} \end{bmatrix}, \tag{23}$$

para $k = 0, 1, \ldots, N-1$, e N autovalores dados por

$$\lambda_k = l_0 + l_1\rho_k + l_2\rho_k^2 + \cdots + l_{N-1}\rho_k^{N-1}. \tag{24}$$

O grafo em ciclo (ou anel) $\mathcal{C}_N$, cuja estrutura é mostrada na Figura 4, é chamado circulante porque sua matriz de adjacência e, portanto, sua matriz Laplaciana $\mathbf{L}(\mathcal{C}_\mathbf{N})$ são circulantes. Sabe-se que um conjunto válido de autovetores para qualquer matriz circulante é o conjunto de linhas da matriz DFT. Então, a GFT para um sinal representado por um grafo em ciclo é equivalente à transformada DFT.

Alguns autovalores aparecem repetidos devido à simetria

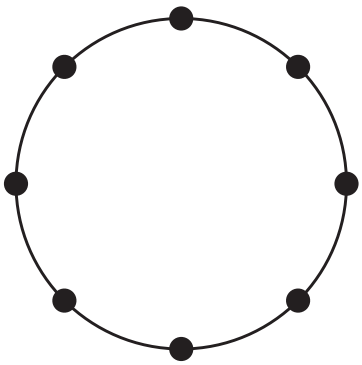
$$\lambda_k = \lambda_{N-k}, \tag{25}$$

em que λ_k corresponde ao k-ésimo autovalor de $\mathbf{L}(\mathcal{C}_\mathbf{N})$ com $k = 1, 2, \ldots, \frac{N}{2} - 1$. Analisando a multiplicidade algébrica em (24), tem-se que, se N é par:

- Os autovalores λ_0 e $\lambda_{\frac{N}{2}}$ têm multiplicidade 1.
- O autovalor $\lambda_k = \lambda_{N-k}$, quando $1 \leq k \leq \frac{N}{2} - 1$, apresenta multiplicidade igual a 2.

Como os autovetores de $\mathbf{L}(\mathcal{C}_\mathbf{N})$ são ortogonais, a multiplicidade geométrica é igual à multiplicidade algébrica. A dimensão do autoespaço correspondente aos autovalores é maior do

Figura 4 – Grafo em ciclo $\mathcal{C}_8$.



Fonte: A autora (2020).

que 1. Assim, a DFT não é a única autobase para $\mathbf{L}(\mathcal{C}_\mathbf{N})$. Esse fato é explorado para definir a SDFT.

Seja λ_k um autovalor de $\mathbf{L}(\mathcal{C}_\mathbf{N})$ com multiplicidade 2 e sejam $\mathbf{v}^{(k)}$ e $\mathbf{v}^{(N-k)}$ dois vetores da DFT que são autovetores de $\mathbf{L}(\mathcal{C}_\mathbf{N})$ associados a λ_k. Pode-se obter um novo par de autovetores $\mathbf{v}^{(k)'}$ e $\mathbf{v}^{(N-k)'}$ para o autoespaço correspondente a λ_k a partir da rotação de $\mathbf{v}^{(k)}$ e $\mathbf{v}^{(N-k)}$, como segue:

$$\begin{bmatrix} \mathbf{v}^{(k)'} \\ \mathbf{v}^{(N-k)'} \end{bmatrix} = \begin{bmatrix} \cos\theta_k & \operatorname{sen}\theta_k \\ -\operatorname{sen}\theta_k & \cos\theta_k \end{bmatrix} \cdot \begin{bmatrix} \mathbf{v}^{(k)} \\ \mathbf{v}^{(N-k)} \end{bmatrix}, \tag{26}$$

em que θ_k é um ângulo em $[0, 2\pi]$.

Se cada par de autovetores $\mathbf{v}^{(k)}$ e $\mathbf{v}^{(N-k)}$ correspondentes a λ_k, com $1 \leq k \leq \frac{N}{2} - 1$, for rotacionado de acordo com (26), uma nova transformada é definida, empregando uma base que consiste na substituição dos pares $\mathbf{v}^{(k)}$ e $\mathbf{v}^{(N-k)}$ da DFT por suas respectivas versões rotacionadas $\mathbf{v}^{(k)'}$ e $\mathbf{v}^{(N-k)'}$. A nova transformada é denominada transformada discreta manobrável de Fourier (SDFT) e sua matriz pode ser escrita como

$$\mathbf{V}(\boldsymbol{\theta}) = \mathbf{R}(\boldsymbol{\theta})\mathbf{V}, \tag{27}$$

em que $\mathbf{V} = \mathbf{V}(\mathbf{0})$ é a matriz da DFT, $\mathbf{R}(\boldsymbol{\theta}) \in \mathbb{R}^{N \times N}$ é uma matriz esparsa de rotação, construída de acordo com (26), $\boldsymbol{\theta} \in \mathbb{R}^{\text{ang}_2}$, com $\text{ang}_2 = \frac{N}{2} - 1$ (número de pares rotacionados), é o vetor contendo todos os ângulos utilizados, e $\mathbf{0}$ é um vetor nulo com comprimento igual ao do vetor $\boldsymbol{\theta}$.

Para qualquer sinal $\mathbf{f}$, a SDFT é dada por

$$\hat{\mathbf{f}}_{SDFT} = \mathbf{V}(\boldsymbol{\theta})\mathbf{f} = \mathbf{R}(\boldsymbol{\theta})\mathbf{V}\mathbf{f} = \mathbf{R}(\boldsymbol{\theta})\hat{\mathbf{f}}_{DFT}, \tag{28}$$

em que $\hat{\mathbf{f}}_{DFT}$ é o vetor de coeficientes da DFT do sinal $\mathbf{f}$.

Uma vez que os coeficientes $\hat{\mathbf{f}}_{DFT}$ de um sinal $\mathbf{f} \in \mathbb{R}^N$ apresentam a propriedade de simetria

$$\hat{\mathbf{f}}_{DFT_k} = \hat{\mathbf{f}}^*_{DFT_{N-k}}, \tag{29}$$

em que $1 \leq k \leq \frac{N}{2} - 1$ e o símbolo "*" denota o conjugado, é possível, a partir do uso de um determinado ângulo de rotação θ_k em (26), separar completamente a parte real e a parte imaginária da SDFT. Por exemplo, aplicando uma rotação com $\theta_k = \frac{\pi}{4}$ em (26), obtém-se como novos coeficientes da transformada

$$\begin{aligned}\begin{bmatrix}\hat{\mathbf{f}}_{SDFT_k}\\ \hat{\mathbf{f}}_{SDFT_{N-k}}\end{bmatrix} &= \begin{bmatrix}\mathbf{v}^{(k)'}\\ \mathbf{v}^{(N-k)'}\end{bmatrix}\mathbf{f} = \begin{bmatrix}\cos\frac{\pi}{4} & \operatorname{sen}\frac{\pi}{4}\\ -\operatorname{sen}\frac{\pi}{4} & \cos\frac{\pi}{4}\end{bmatrix}\begin{bmatrix}\mathbf{v}^{(k)}\\ \mathbf{v}^{(N-k)}\end{bmatrix}\mathbf{f}\\ &= \begin{bmatrix}\frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2}\\ -\frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2}\end{bmatrix}\begin{bmatrix}\hat{\mathbf{f}}_{DFT_k}\\ \hat{\mathbf{f}}_{DFT_{N-k}}\end{bmatrix} = \begin{bmatrix}\frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2}\\ -\frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2}\end{bmatrix}\begin{bmatrix}\hat{\mathbf{f}}_{DFT_k}\\ \hat{\mathbf{f}}^{*}_{DFT_k}\end{bmatrix}\\ &= \begin{bmatrix}\sqrt{2}\,\mathrm{Re}(\hat{\mathbf{f}}_{DFT_k})\\ -j\sqrt{2}\,\mathrm{Im}(\hat{\mathbf{f}}_{DFT_k})\end{bmatrix}. \end{aligned} \tag{30}$$

A SDFT pode ser relacionada com outras transformadas. Por exemplo, em (30) tem-se que, para um ângulo $\theta_k = \frac{\pi}{4}$, $\hat{\mathbf{f}}_{SDFT_k} = \sqrt{2}\hat{\mathbf{f}}_{\cos_k}$ para $1 \leq k \leq \frac{N}{2} - 1$ e, analogamente, $\hat{\mathbf{f}}_{SDFT_k} = -j\sqrt{2}\hat{\mathbf{f}}_{\operatorname{sen}_k}$ para $\frac{N}{2} + 1 \leq k \leq N - 1$, em que $\hat{\mathbf{f}}_{\cos_k}$ e $\hat{\mathbf{f}}_{\operatorname{sen}_k}$ correspondem, respectivamente, ao k-ésimo coeficiente da transformada de Fourier-cosseno e ao k-ésimo coeficiente da transformada de Fourier-seno (POULARIKAS, 2010).

2.2.2 2D-SDFT

Como dito na introdução deste capítulo, a definição da 2D-SDFT parte da sua relação com a DFT bidimensional (2D-DFT), que é dada pela expressão

$$\hat{\mathbf{f}}_{rq} = \sum_{n=0}^{N-1}\sum_{m=0}^{N-1} f_{mn} e^{-j2\pi\left(\frac{r}{N}m + \frac{q}{N}n\right)}, r, q = 0, 1, \ldots, N-1. \tag{31}$$

A transformada inversa da 2D-DFT é calculada por

$$f_{mn} = \frac{1}{N^2}\sum_{r=0}^{N-1}\sum_{q=0}^{N-1} \hat{\mathbf{f}}_{rq} e^{j2\pi\left(\frac{r}{N}m + \frac{q}{N}n\right)}, m, n = 0, 1, \ldots, N-1. \tag{32}$$

A 2D-DFT pode ser expressa na forma matricial como

$$\hat{\mathbf{f}} = \mathbf{V}\mathbf{f}, \tag{33}$$

em que $\mathbf{V} \in \mathbb{C}^{N^2 \times N^2}$ é a matriz de transformação da 2D-DFT, dada por

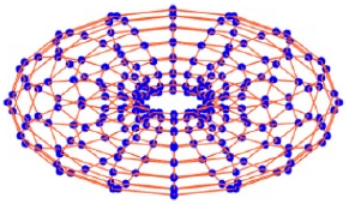
$$\mathbf{V}_{ks} = e^{-j2\pi\left(\frac{r}{N}m + \frac{q}{N}n\right)} = \rho_r^m \rho_q^n, \tag{34}$$

em que $k = mN + n$, $s = rN + q$, com $0 \leq r, m \leq N-1$ e $0 \leq q, n \leq N-1$.

O grafo em grade toroidal $\tau_{N,N}$ com N^2 vértices, cuja estrutura é mostrada na Figura 5, pode ser visto como o resultado do produto Cartesiano entre dois grafos em ciclo, $\mathcal{C}_N \square \mathcal{C}_N$.

Em (FRACASTORO; MAGLI, 2017), os autores mostraram que a 2D-DFT é uma autobase do Laplaciano do grafo em grade toroidal, $\mathbf{L}(\tau_{\mathbf{N},\mathbf{N}})$, de forma que o autovetor $\mathbf{v}^{(r,q)}$,

Figura 5 – Grafo em grade toroidal $\tau_{16,16}$.



Fonte: Fracastoro e Magli (2017).

com $0 \leq r, q \leq N-1$, do $\mathbf{L}(\tau_{\mathbf{N},\mathbf{N}})$ corresponde ao produto de Kronecker entre os autovetores $\mathbf{v}^r$ e $\mathbf{v}^q$, correspondendentes aos autovalores λ_r e λ_q, do $\mathbf{L}(\mathcal{C}_\mathbf{N})$. O autovetor $\mathbf{v}^{(r,q)}$ do $\mathbf{L}(\tau_{\mathbf{N},\mathbf{N}})$ corresponde ao autovalor $\lambda_{r,q}$ que é determinado pela soma dos autovalores λ_r e λ_q, do $\mathbf{L}(\mathcal{C}_\mathbf{N})$, ou seja

$$\lambda_{r,q} = \lambda_r + \lambda_q, \tag{35}$$

em que $0 \leq r, q \leq N-1$.

Como $\lambda_{r,q} = \lambda_{q,r}$ e devido à propriedade de simetria apresentada em (25) para os autovalores do $\mathbf{L}(\mathcal{C}_\mathbf{N})$, tem-se que

- O autovalor $\lambda_{r,q}$ tem multiplicidade algébrica igual a 1, quando $r = q$ com $r, q = 0, \frac{N}{2}$;
- O autovalor $\lambda_{r,q}$ tem multiplicidade algébrica igual a 2, quando $r \neq q$ com $r, q = 0, \frac{N}{2}$, devido à simetria: $\lambda_{0,\frac{N}{2}} = \lambda_{\frac{N}{2},0}$;
- O autovalor $\lambda_{r,q}$ tem multiplicidade algébrica igual a 4, quando $r = 0, \frac{N}{2}$ e $1 \leq q \leq \frac{N}{2} - 1$ (ou, $q = 0, \frac{N}{2}$ e $1 \leq r \leq \frac{N}{2} - 1$), devido à simetria: $\lambda_{r,q} = \lambda_{q,r} = \lambda_{r,N-q} = \lambda_{N-q,r}$ ($\lambda_{r,q} = \lambda_{q,r} = \lambda_{N-r,q} = \lambda_{q,N-r}$);
- O autovalor $\lambda_{r,q}$ tem multiplicidade algébrica igual a 4, quando $r = q$, com $1 \leq r \leq \frac{N}{2} - 1$, devido à simetria: $\lambda_{r,r} = \lambda_{r,N-r} = \lambda_{N-r,r} = \lambda_{N-r,N-r}$;
- O autovalor $\lambda_{r,q}$ tem multiplicidade algébrica igual a 8, quando $r \neq q$ com $1 \leq r, q \leq \frac{N}{2} - 1$, devido à simetria: $\lambda_{r,q} = \lambda_{q,r} = \lambda_{r,N-q} = \lambda_{N-q,r} = \lambda_{N-r,q} = \lambda_{q,N-r} = \lambda_{N-r,N-q} = \lambda_{N-q,N-r}$.

Como os autovetores de $\mathbf{L}(\tau_{\mathbf{N},\mathbf{N}})$ são determinados pelo produto de Kronecker entre os autovetores de $\mathbf{L}(\mathcal{C}_\mathbf{N})$, e esse produto apresenta a característica de ser não comutativo, tem-se que a multiplicidade geométrica de cada autovalor de $\mathbf{L}(\tau_{\mathbf{N},\mathbf{N}})$ é igual à multiplicidade algébrica correspondente, ou seja, a dimensão do autoespaço associado a cada autovalor de $\mathbf{L}(\tau_{\mathbf{N},\mathbf{N}})$ é maior do que 1 (exceto para o cenário $r = q$). Logo, pode-se concluir que a base da 2D-DFT não é a única base de autovetores de $\mathbf{L}(\tau_{\mathbf{N},\mathbf{N}})$. Se os vetores de base da 2D-DFT forem rotacionados, uma nova autobase para $\mathbf{L}(\tau_{\mathbf{N},\mathbf{N}})$ será obtida.

Se cada par de autovetores $\mathbf{v}^{(r,q)}$ e $\mathbf{v}^{(q,r)}$ da 2D-DFT associados ao autovalor $\lambda_{r,q}$, com $r \neq q$, com suas componentes rearrajandas em vetores linha com N^2 componentes, for rotacionado, um novo par de autovetores $\mathbf{v}^{(r,q)'}$ e $\mathbf{v}^{(q,r)'}$ para o mesmo autoespaço é obtido a partir de

$$\begin{bmatrix} \mathbf{v}^{(r,q)'} \\ \mathbf{v}^{(q,r)'} \end{bmatrix} = \begin{bmatrix} \cos\theta_{r,q} & \operatorname{sen}\theta_{r,q} \\ -\operatorname{sen}\theta_{r,q} & \cos\theta_{r,q} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{v}^{(r,q)} \\ \mathbf{v}^{(q,r)} \end{bmatrix}, \tag{36}$$

em que $\theta_{r,q}$ é um ângulo em $[0, 2\pi]$. Assim, uma nova base é obtida, substituindo os pares $\mathbf{v}^{(r,q)}$ e $\mathbf{v}^{(q,r)}$ da 2D-DFT por suas respectivas versões rotacionadas $\mathbf{v}^{(r,q)'}$ e $\mathbf{v}^{(q,r)'}$, à qual está associada a transformada discreta bidimensional manobrável de Fourier (2D-SDFT). A matriz de transformação da 2D-SDFT pode ser escrita como

$$\mathbf{V_{2D}}(\boldsymbol{\theta}) = \mathbf{R_{2D}}(\boldsymbol{\theta})\mathbf{V_{2D}}, \tag{37}$$

em que $\mathbf{V_{2D}} = \mathbf{V_{2D}}(\mathbf{0})$ é a matriz 2D-DFT, $\mathbf{R_{2D}}(\boldsymbol{\theta}) \in \mathbb{R}^{N^2 \times N^2}$ é a matriz de rotação, construída de acordo com (36), $\boldsymbol{\theta} \in \mathbb{R}^{\text{ang}_2}$, com $\text{ang}_2 = \frac{N(N-1)}{2}$ (número de pares rotacionados), é o vetor contendo todos os ângulos utilizados, e $\mathbf{0}$ denota o vetor nulo com comprimento ang_2.

2.3 OUTRAS TRANSFORMADAS DISCRETAS BIDIMENSIONAIS MANOBRÁVEIS

Em (MASERA et al., 2019), os autores propuseram uma generalização dos métodos utilizados em (FRACASTORO; FOSSON; MAGLI, 2017) e em (FRACASTORO; MAGLI, 2017) (apresentados nas Seções 2.1 e 2.2, respectivamente) para projetar transformadas manobráveis a partir de qualquer transformada bidimensional separável.

Uma transformada n-dimensional é dita separável se seu cálculo puder ser obtido a partir de n transformadas unidimensionais. Para o caso em que $n = 2$, uma matriz de transformação separável $\mathbf{W} \in \mathbb{C}^{N^2 \times N^2}$ pode ser definida como

$$\mathbf{W} = \mathbf{W_1} \otimes \mathbf{W_2}, \tag{38}$$

em que $\mathbf{W_1} \in \mathbb{C}^{N \times N}$ e $\mathbf{W_2} \in \mathbb{C}^{N \times N}$ correspondem a transformadas unidimensionais que operam, de forma isolada, nas colunas e linhas, respectivamente, de um sinal $\mathbf{X} \in \mathbb{C}^{N \times N}$ ($\mathbf{W} = \mathbf{W_1 X W_2}^H$, em que H denota o transposto Hermitiano). Se $\mathbf{W_1} = \mathbf{W_2}$, então (38) torna-se

$$\mathbf{W} = \mathbf{W_1} \otimes \mathbf{W_1}, \tag{39}$$

A partir de (39), pode-se definir as matrizes $\mathbf{W}^{(l,k)} \in \mathbb{C}^{N \times N}$ e $\mathbf{W}^{(k,l)} \in \mathbb{C}^{N \times N}$, com $0 \leq l, k \leq N-1$ como seguem

$$\mathbf{W}^{(l,k)} = \begin{bmatrix} w_1^{(l,k)} & w_{N+1}^{(l,k)} & \cdots & w_{(N-1)N+1}^{(l,k)} \\ \vdots & \vdots & & \vdots \\ w_N^{(l,k)} & w_{2N}^{(l,k)} & \cdots & w_{N^2}^{(l,k)} \end{bmatrix} \tag{40}$$

e

$$\mathbf{W}^{(k,l)} = \begin{bmatrix} w_1^{(k,l)} & w_{N+1}^{(k,l)} & \cdots & w_{(N-1)N+1}^{(k,l)} \\ \vdots & \vdots & & \vdots \\ w_N^{(k,l)} & w_{2N}^{(k,l)} & \cdots & w_{N^2}^{(k,l)} \end{bmatrix}, \tag{41}$$

em que $\mathbf{w}^{(l,k)} = [w_1^{(l,k)}, w_2^{(l,k)}, \ldots, w_{N^2}^{(l,k)}]$ corresponde à i-ésima linha de $\mathbf{W}$, com $i = lN + k$ e $\mathbf{w}^{(k,l)} = [w_1^{(k,l)}, w_2^{(k,l)}, \ldots, w_{N^2}^{(k,l)}]$ corresponde à j-ésima linha de $\mathbf{W}$, com $j = kN + l$.

Observa-se que $\mathbf{W}^{(l,k)} = \mathbf{W}^{(k,l)T}$. Isso indica que, se $l \neq k$, tem-se que $\mathbf{W}^{(l,k)}$ e $\mathbf{W}^{(k,l)}$ representam a mesma componente no domínio da transformada em direções diferentes (direção horizontal e vertical). Logo, é possível obter uma nova transformada a partir da rotação desses vetores.

Seja o par de vetores $\mathbf{w}^{(l,k)}$ e $\mathbf{w}^{(k,l)}$, com $0 \leq l, k \leq N-1$ e $l \neq k$. Sua versão rotacionada, para o ângulo $\theta_{k,l} \in [0, 2\pi]$, é dada por

$$\begin{bmatrix} \mathbf{w}^{(l,k)'} \\ \mathbf{w}^{(k,l)'} \end{bmatrix} = \begin{bmatrix} \cos\theta_{k,l} & \operatorname{sen}\theta_{k,l} \\ -\operatorname{sen}\theta_{k,l} & \cos\theta_{k,l} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{w}^{(l,k)} \\ \mathbf{w}^{(k,l)} \end{bmatrix}. \tag{42}$$

Se todos os pares de vetores $\mathbf{w}^{(l,k)}$ e $\mathbf{w}^{(k,l)}$, com $0 \leq l, k \leq N-1$ e $l \neq k$, ou seja $\frac{N(N-1)}{2}$ pares, forem subtituídos por suas respectivas versões rotacionadas, uma nova transformada $\mathbf{W}(\boldsymbol{\theta})$ é obtida, em que a i-ésima linha de $\mathbf{W}(\boldsymbol{\theta})$, com $i = lN + k$, corresponde a $\mathbf{w}^{(l,k)'}$ se $l \neq k$, e a $\mathbf{w}^{(l,k)}$ se $l = k$. O operador matricial da nova transformada pode ser dado por

$$\mathbf{W}(\boldsymbol{\theta}) = \mathbf{R}(\boldsymbol{\theta})\mathbf{W}, \tag{43}$$

em que $\mathbf{R}(\boldsymbol{\theta}) \in \mathbb{R}^{N^2 \times N^2}$ é a matriz de rotação, construída de acordo com (42) e $\boldsymbol{\theta}$ é o vetor contendo todos os ângulos utilizados.

3 TRANSFORMADAS DISCRETAS MULTIDIMENSIONAIS MANOBRÁVEIS DO COSSENO

Este capítulo apresenta a definição da transformada discreta manobrável do cosseno para o espaço tridimensional (3D-SDCT) e o conceito de rotação "ótima", que permite obter um maior número de coeficientes nulos da 3D-SDCT. Neste capítulo, é apresentado também, para o espaço quadridimensional, o estudo da multiplicidade dos autovalores do Laplaciano do produto de quatro grafos em caminho, que é essencial para a definição de uma possível versão 4D da SDCT.

3.1 TRANSFORMADA DISCRETA TRIDIMENSIONAL MANOBRÁVEL DO COSSENO

Esta seção apresenta uma nova transformada direcional denominada transformada discreta tridimensional manobrável do cosseno (3D-SDCT, do inglês *three-dimensional steerable discrete cosine transform*) que corresponde a uma extensão da ideia originalmente introduzida em (FRACASTORO; FOSSON; MAGLI, 2017). Tal transformada é obtida pela rotação da base da transformada discreta tridimensional do cosseno (3D-DCT, do inglês *three-dimensional discrete cosine transform*) e parte do princípio de que a 3D-DCT é uma autobase para o Laplaciano do produto de três grafos em caminho (grafo em grade cúbica). A definição da 3D-SDCT é iniciada pela investigação da auto-estrutura do Laplaciano do grafo em grade cúbica.

3.1.1 Uma Autobase para o Laplaciano do Produto de Três Grafos em Caminho

O ponto-chave para a definição da 3D-SDCT é perceber que a base 3D-DCT é uma possível autobase para o Laplaciano do produto de três grafos em caminho. Se três grafos em caminho possuem o mesmo número de vértices, seu produto Cartesiano $\mathcal{L}_N = \mathcal{P}_N \square \mathcal{P}_N \square \mathcal{P}_N$, em que $\square$ denota o produto Cartesiano de grafos, corresponde a um grafo em grade cúbica com N^3 vértices (a Figura 6 ilustra o exemplo de um grafo em grade cúbica para $N = 4$). Nesse sentido, primeiro faz-se necessário revisar a definição da 3D-DCT.

Definição 3.1. A transformada discreta tridimensional do cosseno de um sinal $\mathbf{f}$ com dimensão $N \times N \times N$ é definida como

$$F(k,l,m) = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1}\sum_{z=0}^{N-1} f(x,y,z)\alpha(k)\alpha(l)\alpha(m)u_{x,y,z}(k,l,m), \tag{44}$$

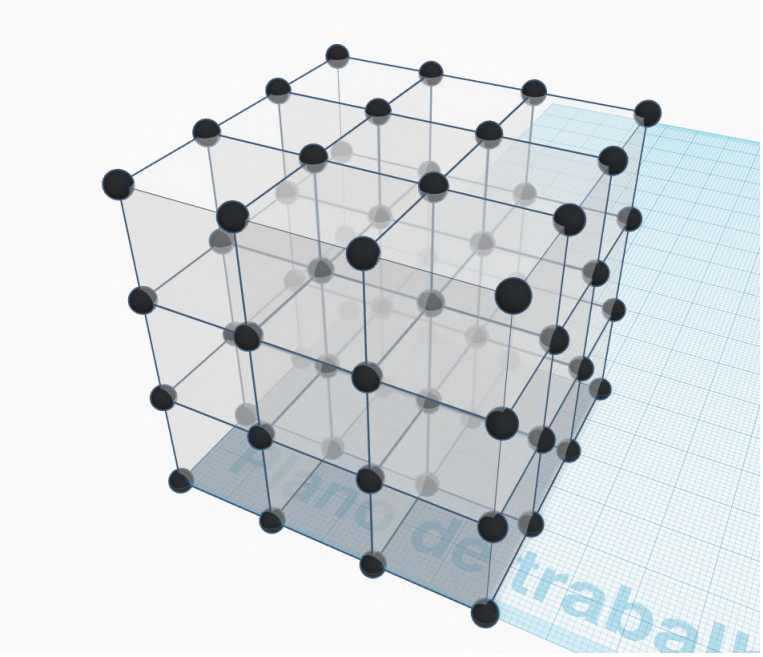
em que

$$\alpha(k) = \begin{cases} \sqrt{\frac{1}{N}}, & k = 0, \\ \sqrt{\frac{2}{N}}, & k = 1, 2, \ldots, N-1, \end{cases} \tag{45}$$

e

$$u_{x,y,z}(k,l,m) = \cos\left[\frac{\pi(2x+1)k}{2N}\right]\cos\left[\frac{\pi(2y+1)l}{2N}\right]\cos\left[\frac{\pi(2z+1)m}{2N}\right]. \tag{46}$$

Figura 6 – Grafo em grade cúbica $\mathcal{L}_N = \mathcal{P}_N \square \mathcal{P}_N \square \mathcal{P}_N$.



Fonte: A autora (2020).

A transformada inversa é calculada por

$$f(x,y,z) = \sum_{k=0}^{N-1} \sum_{l=0}^{N-1} \sum_{m=0}^{N-1} F(k,l,m)\alpha(k)\alpha(l)\alpha(m)u_{x,y,z}(k,l,m). \tag{47}$$

Na forma matricial, o cálculo da 3D-DCT de $\mathbf{f}$ pode ser expresso como $\bar{\mathbf{F}} = \mathbf{C}\bar{\mathbf{f}}^T$, em que

$$\bar{\mathbf{f}} = [f(0,0,0) \ldots f(0,0,N-1)\ f(0,1,0) \ldots f(N-1,N-1,N-1)] \tag{48}$$

é um vetor $1 \times N^3$ formado pelos elementos de $\mathbf{f}$ tomados na ordem lexicográfica; analogamente, $\bar{\mathbf{F}}$ é formado pelos elementos de $\mathbf{F}$; a matriz de transformação é $\mathbf{C}$, que tem dimensão $N^3 \times N^3$ e cujas entradas são dadas por

$$C_{x,y,z}(k,l,m) = \alpha(k)\alpha(l)\alpha(m)u_{x,y,z}(k,l,m), \tag{49}$$

com índices x, y, z e k, l, m variando na ordem lexicográfica ao longo das colunas e linhas, respectivamente.

Em geral, dados dois grafos, $\mathcal{G}_1$ e $\mathcal{G}_2$, com N_1 e N_2 vértices, e cujas matrizes Laplacianas são $\mathbf{L}(\mathcal{G}_1)$ e $\mathbf{L}(\mathcal{G}_2)$, respectivamente, a matriz Laplaciana de $\mathcal{G}_1 \square \mathcal{G}_2$ é expressa como (MERRI, 1998)

$$\mathbf{L}(\mathcal{G}_1) \oplus \mathbf{L}(\mathcal{G}_2) = \mathbf{L}(\mathcal{G}_1) \otimes \mathbf{I}_{N_1} + \mathbf{I}_{N_2} \otimes \mathbf{L}(\mathcal{G}_2), \tag{50}$$

em que $\oplus$ e $\otimes$ denotam, respectivamente, a soma de Kronecker e o produto de Kronecker, e $\mathbf{I}_N$ denota a matriz identidade de ordem N. Além disso, supondo que $\mathbf{L}(\mathcal{G}_n)$ tenha autovalores

não negativos $\{\lambda_k^{(n)}\}$, $k = 0, \ldots, N_n - 1$, e autovetores ortonormais $\{\mathbf{v}_k^{(n)}\}$, $k = 0, \ldots, N_n - 1$, para $n = 1, 2$, a soma de Kronecker $\mathbf{L}(\mathcal{G}_1) \oplus \mathbf{L}(\mathcal{G}_2)$ tem um autovalor $\lambda_{k_1}^{(1)} + \lambda_{k_2}^{(2)}$ e o autovetor correspondente $\mathbf{v}_{k_1}^{(1)} \otimes \mathbf{v}_{k_2}^{(2)}$. Estendendo estes fatos para o grafo em grade cúbica $\mathcal{L}_N$, pode-se concluir que o Laplaciano $\mathbf{L}(\mathcal{L}_N)$ pode ser determinado por

$$\mathbf{L}(\mathcal{L}_N) = \mathbf{L}(\mathcal{P}_N) \otimes \mathbf{I}_N \otimes \mathbf{I}_N + \mathbf{I}_N \otimes \mathbf{L}(\mathcal{P}_N) \otimes \mathbf{I}_N + \mathbf{I}_N \otimes \mathbf{I}_N \otimes \mathbf{L}(\mathcal{P}_N). \tag{51}$$

Sabe-se também que os autovalores de $\mathbf{L}(\mathcal{L}_N)$ são todas as possíveis somas entre os autovalores de cada grafo em caminho, ou seja,

$$\lambda_{k,l,m} = 4\left[\operatorname{sen}^2\left(\frac{\pi k}{2N}\right) + \operatorname{sen}^2\left(\frac{\pi l}{2N}\right) + \operatorname{sen}^2\left(\frac{\pi m}{2N}\right)\right], \tag{52}$$

para $k, l, m = 0, \ldots, N-1$. Além disso, como $\mathbf{v}_k = [v_k(n)]$, $n = 0, \ldots, N-1$, em que

$$v_k(n) = \alpha(k) \cos\left(\frac{\pi k}{2N}(2n+1)\right), \tag{53}$$

é um autovetor de $\mathcal{P}_N$ (e vetor base da DCT do tipo 2) relacionado ao autovalor λ_k, $k = 0, \ldots, N-1$, então

$$\mathbf{v}_{k,l,m} = \mathbf{v}_k \otimes \mathbf{v}_l \otimes \mathbf{v}_m \tag{54}$$

é um autovetor de $\mathcal{L}_N = \mathcal{P}_N \square \mathcal{P}_N \square \mathcal{P}_N$ relacionado ao autovalor $\lambda_{k,l,m}$, $k, l, m = 0, \ldots, N-1$. Isso significa que os vetores de base da 3D-DCT constituem uma autobase para o Laplaciano $\mathbf{L}(\mathcal{L}_N)$ do grafo em grade cúbica.

3.1.2 Análise da Multiplicidade dos Autovalores

De (52), derivam-se os seguintes fatos a respeito das multiplicidades dos autovalores de $\mathbf{L}(\mathcal{L}_N)$:

- O autovalor $\lambda_{k,l,m}$ tem multiplicidade igual a 1, quando $k = l = m$, com $0 \leq k, l, m \leq N-1$. Logo, no espectro de $\mathbf{L}(\mathcal{L}_N)$, há N autovalores com multiplicidade algébrica igual a 1;

- O autovalor $\lambda_{k,l,m}$ apresenta multiplicidade igual a 3, quando:

  1. $k = l$ e $l \neq m$, ou seja, $\lambda_{k,k,m} = \lambda_{k,m,k} = \lambda_{m,k,k}$, um total de $N(N-1)$ autovalores;
  2. $k = m$ e $m \neq l$, ou seja, $\lambda_{k,l,k} = \lambda_{k,k,l} = \lambda_{l,k,k}$, um total de $N(N-1)$ autovalores;
  3. $m = l$ e $l \neq k$, ou seja, $\lambda_{m,m,k} = \lambda_{m,k,m} = \lambda_{k,m,m}$, um total de $N(N-1)$ autovalores;

  Logo, no espectro de $\mathbf{L}(\mathcal{L}_N)$, há $3N(N-1)$ autovalores com multiplicidade algébrica igual a 3;

- O autovalor $\lambda_{k,l,m}$ apresenta multiplicidade igual a 6, quando $k \neq l \neq m$. Devido à simetria: $\lambda_{k,l,m} = \lambda_{k,m,l} = \lambda_{l,k,m} = \lambda_{l,m,k} = \lambda_{m,k,l} = \lambda_{m,l,k}$. Logo, no espectro de $\mathbf{L}(\mathcal{L}_N)$, há $N(N-1)(N-2)$ autovalores com multiplicidade algébrica igual a 6.

Uma vez que os autovetores de $\mathbf{L}(\mathcal{L}_N)$ são determinados pelo produto de Kronecker entre os respectivos autovetores de $\mathcal{P}_N$, e esse produto é não comutativo, a dimensão de cada autoespaço, ou seja, a multiplicidade geométrica de cada autovalor é igual à multiplicidade algébrica correspondente. Isso significa que há autoespaços cuja dimensão é maior que um e, portanto, a base 3D-DCT não é a única autobase para $\mathbf{L}(\mathcal{L}_N)$. A seguir, explora-se esse fato para definir a 3D-SDCT.

3.1.3 Definição da Transformada 3D-SDCT

Seja $\lambda_{k,l,m}$, com $k = l$ e $l \neq m$, um autovalor de $\mathbf{L}(\mathcal{L}_N)$ com multiplicidade igual a três, e $\mathbf{v}_{k,k,m}$, $\mathbf{v}_{k,m,k}$ e $\mathbf{v}_{m,k,k}$ três vetores de base da 3D-DCT que são autovetores de $\mathbf{L}(\mathcal{L}_N)$ associados a $\lambda_{k,l,m}$. Pode-se obter outra base para o autoespaço correspondente a $\lambda_{k,l,m}$ rotacionando $\mathbf{v}_{k,k,m}$, $\mathbf{v}_{k,m,k}$ e $\mathbf{v}_{m,k,k}$ em torno de um eixo arbitrário em um espaço tridimensional. Se a referida rotação é expressa por meio de duas rotações sequenciais em torno dos eixos z e y[1], os respectivos vetores rotacionados $\mathbf{v}'_{k,k,m}$, $\mathbf{v}'_{k,m,k}$ e $\mathbf{v}'_{m,k,k}$ são dados por[2]

$$\begin{bmatrix} \mathbf{v}'_{k,k,m} \\ \mathbf{v}'_{k,m,k} \\ \mathbf{v}'_{m,k,k} \end{bmatrix} = \begin{bmatrix} \cos\theta_y & 0 & \operatorname{sen}\theta_y \\ 0 & 1 & 0 \\ -\operatorname{sen}\theta_y & 0 & \cos\theta_y \end{bmatrix} . \begin{bmatrix} \cos\theta_z & \operatorname{sen}\theta_z & 0 \\ -\operatorname{sen}\theta_z & \cos\theta_z & 0 \\ 0 & 0 & 1 \end{bmatrix} . \begin{bmatrix} \mathbf{v}_{k,k,m} \\ \mathbf{v}_{k,m,k} \\ \mathbf{v}_{m,k,k} \end{bmatrix}, \tag{55}$$

em que θ_y e θ_z são ângulos no intervalo $[0, 2\pi]$.

Uma modificação semelhante à descrita em (55) pode ser aplicada aos autovetores de $\mathbf{L}(\mathcal{L}_N)$ associados aos autovalores cuja multiplicidade é igual a 6, agrupando-os em duas triplas $(\mathbf{v}_{k,l,m}, \mathbf{v}_{l,m,k}, \mathbf{v}_{m,k,l})$ e $(\mathbf{v}_{k,m,l}, \mathbf{v}_{m,l,k}, \mathbf{v}_{l,k,m})$. Se cada uma dessas triplas for rotacionada independentemente, uma nova base para o autoespaço associado ao respectivo autovalor é obtida. A nova transformada é denominada como transformada discreta tridimensional manobrável do cosseno (3D-SDCT) e consiste em substituir os vetores de base da 3D-DCT por suas respectivas versões rotacionadas. Desta forma, a matriz 3D-SDCT pode ser escrita como

$$\mathbf{C}_{\mathrm{S}}(\boldsymbol{\Theta}) = \mathbf{R}(\boldsymbol{\Theta})\mathbf{C}, \tag{56}$$

em que $\mathbf{C}$ corresponde à matriz da 3D-DCT, $\mathbf{R}(\boldsymbol{\Theta})$ é uma matriz esparsa que rotaciona cada tripla de autovetor e cuja estrutura é determinada a partir de (55), e $\boldsymbol{\Theta} = [(\theta_{y,i}, \theta_{z,i})]$, $i = 0, 1, \ldots, M-1$, é um vetor contendo todos os pares de ângulos necessários para realizar as referidas rotações. A partir dos resultados derivados na Seção 3.1.2, sabe-se que o número de

[1] Tais rótulos de eixos são usados aqui com o propósito de distinguir as coordenadas em um espaço tridimensional; não se referem aos eixos x, y e z geralmente empregados para caracterizar $\mathbb{R}^3$.

[2] A não ser que seja de outra forma declarado, a partir daqui, os autovetores de $\mathbf{L}(\mathcal{L}_N)$ são expressos como vetores $1 \times N^3$, formados pelas entradas da estrutura $N \times N \times N$ correspondente tomadas na ordem lexicográfica.

triplas de autovetores a serem rotacionados por um par de ângulos é igual a $M = (N^3 - N)/3$. Se $\mathbf{\Theta}$ for igual ao vetor nulo, a 3D-SDCT coincide com a 3D-DCT, isto é, $\mathbf{C}_{\mathrm{S}}(\mathbf{0}) = \mathbf{C}$.

Portanto, um sinal $\mathbf{f} \in \mathbb{R}^{N^3}$ tem sua 3D-SDCT, denotada por $\mathbf{F}_{\mathrm{S}}(\mathbf{\Theta})$, calculada por

$$\bar{\mathbf{F}}_{\mathrm{S}}(\mathbf{\Theta}) = \mathbf{C}_{\mathrm{S}}(\mathbf{\Theta})\bar{\mathbf{f}}^T = \mathbf{R}(\mathbf{\Theta})\mathbf{C}\bar{\mathbf{f}}^T = \mathbf{R}(\mathbf{\Theta})\bar{\mathbf{F}}, \tag{57}$$

em que $\mathbf{F}$ é a 3D-DCT de $\mathbf{f}$.

A complexidade envolvida no cálculo da 3D-SDCT depende basicamente da complexidade envolvida no cálculo da 3D-DCT correspondente, que pode ser eficientemente obtida por meio de algoritmos rápidos usuais. Como a matriz de rotação $\mathbf{R}(\mathbf{\Theta})$ é esparsa, seu produto por $\bar{\mathbf{F}}$ não envolve um número significativo de operações aritméticas. Mais especificamente, um total de $(5N^3 - 5N)/3$ operações de adição e $(8N^3 - 8N)/3$ operações de multiplicação, uma vez que, para cada tripla de autovetores, são necessárias 5 operações de adição e 8 operações de multiplicação para obter a versão rotacionada da tripla. Isso indica que, assintoticamente, a complexidade total não é alterada.

As Figuras 7 e 8 apresentam, respectivamente, as 64 primeiras funções de base da 3D-DCT e da 3D-SDCT com ângulos de rotação θ_y e θ_z iguais a $45°$, para $N = 8$. Para esse valor de N, tem-se um total de $8^3 = 512$ funções de base da 3D-DCT e da 3D-SDCT. A Figura 7 permite visualizar a natureza oscilante das funções de base da 3D-DCT. Cada elemento da Figura 7 é um cubo de tamanho $8 \times 8 \times 8$, em que os valores dos elementos de base $u_{x,y,z}(k, l, m)$ definidos em (46), com $0 \leq k, l, m \leq 7$, são plotados. O bloco superior esquerdo corresponde à função base $u_{x,y,z}(000)$, que é constante.

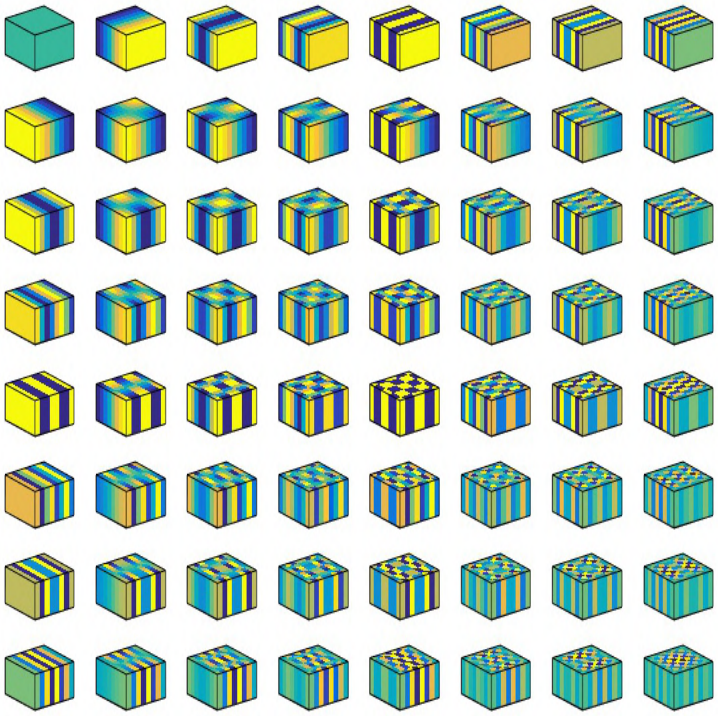
A Figura 8 apresenta os vetores de base obtidos a partir da rotação das triplas de autovetores que apresentam multiplicidade 3 e do par de triplas de autovetores que apresentam multiplicidade igual a 6. Esses autovetores foram rotacionados com ângulos θ_y e θ_z iguais a $45°$. Pode-se observar que o vetor de base $u_{x,y,z}(000)$, representado pelo bloco superior esquerdo da Figura 8, é o mesmo da 3D-DCT. Isso se deve ao fato de que o autovalor associado a este autovetor apresenta multiplicidade igual a 1 e, por esse motivo, não sofre rotação na 3D-SDCT.

3.1.4 Correspondência entre ângulos de rotação e coeficientes 3D-DCT

Na definição da 3D-SDCT, na Seção 3.1.3, foi indicado que os ângulos usados para rotacionar cada tripla de vetores de base da 3D-DCT são declarados no vetor $\mathbf{\Theta} = [(\theta_{y,i}, \theta_{z,i})]$, $i = 0, 1, \ldots, M - 1$. No entanto, é necessário identificar qual tripla é rotacionada por cada par de ângulos $(\theta_{y,i}, \theta_{z,i})$, $i = 0, 1, \ldots, M$. Equivalentemente, devido a (57), pode-se identificar qual tripla de coeficientes 3D-DCT é rotacionada por cada ângulo; isso permite fornecer visualizações 3D interessantes, que ajudam a entender a ação da 3D-SDCT e dão suporte para introduzir o conceito de rotação ótima, que será apresentado na próxima seção.

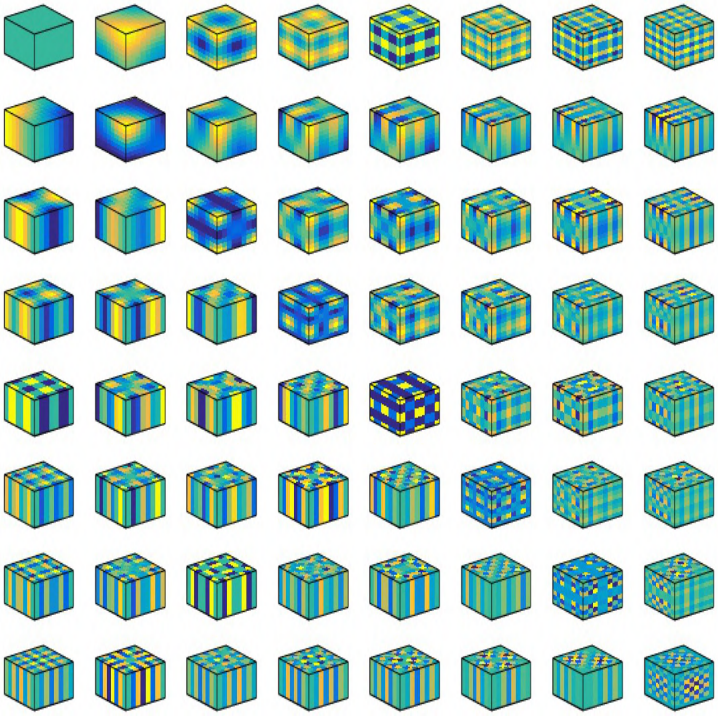
Como um exemplo, a Figura 9 apresenta uma estrutura cúbica $4 \times 4 \times 4$ representando a disposição espacial dos coeficientes 3D-DCT de um sinal com a mesma dimensão; os eixos

Figura 7 – Base ortogonal com os 64 primeiros vetores da 3D-DCT.



Fonte: A autora (2020).

Figura 8 – Base ortogonal com os 64 primeiros vetores da 3D-SDCT com ângulos de rotação θ_y e θ_z iguais a $45°$.



Fonte: A autora (2020).

associados aos índices k, l e m, que variam de 0 a 3, também são indicados[3], de modo que um

[3] Os índices são os mesmos usados para identificar os autovalores e autovetores de $\mathbf{L}(\mathcal{L}_N)$.

coeficiente pode ser denotado inequivocamente por $F_{k,l,m}$. Na figura, quatro cores são usadas: os 4 coeficientes de cor *cinza*, na diagonal principal do cubo, são aqueles que possuem $k = l = m$; esses coeficientes não são modificados pela matriz de rotação $\mathbf{R}(\mathbf{\Theta})$, pois estão associados aos vetores de base $\mathbf{v}_{k,l,m}$ também tendo $k = l = m$, aos quais as rotações não são aplicadas. O restante do cubo é dividido em 3 partes iguais (*vermelho*, *verde* e *amarelo*), de modo que cada tripla de coeficientes a serem rotacionados tem um coeficiente em cada uma dessas partes. Na Figura 9b, é proporcionada uma vista explodida da Figura 9a e as referidas partes podem ser melhor visualizadas.

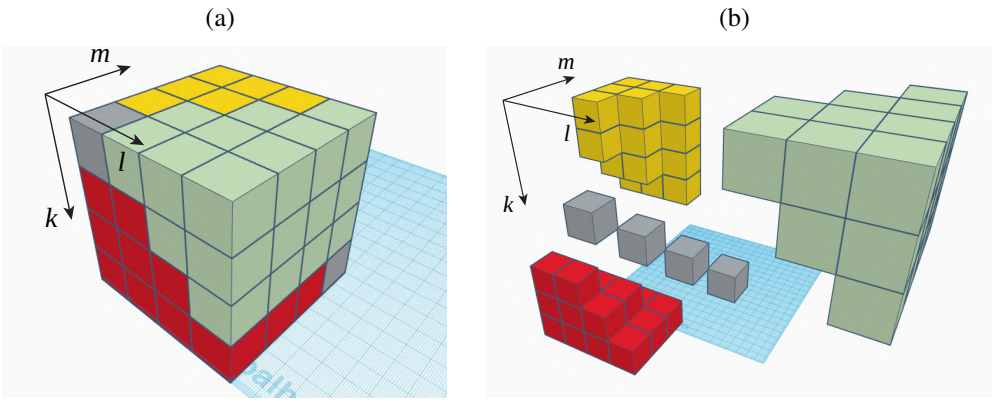
De modo mais específico, seja $F_{k,k,m}$, $k \neq m$, o coeficiente situado na parte em *vermelho* da estrutura $4 \times 4 \times 4$ mostrada na Figura 9; formará uma tripla com os coeficientes $F_{k,m,k}$ na parte em *amarelo* e $F_{m,k,k}$ na parte em *verde* do cubo. Por exemplo, o coeficiente $F_{2,2,0}$ indicado na Figura 10 formará uma tripla juntamente com os coeficientes $F_{2,0,2}$ e $F_{0,2,2}$ indicados nas Figuras 10a e 10b, respectivamente. Como mostrado nas mesmas figuras, as posições de $F_{2,0,2}$ e $F_{0,2,2}$ são simétricas à de $F_{2,2,0}$ em relação aos planos diagonais $l = m$ e $k = m$, respectivamente.

Um coeficiente $F_{k,l,m}$, $k \neq l \neq m$, situado na parte em *vermelho* da estrutura $4 \times 4 \times 4$ mostrada na Figura 9, formará uma tripla junto com $F_{l,m,k}$ na parte em *amarelo* e $F_{m,k,l}$ na parte em *verde* do cubo. Correspondentemente, $F_{k,m,l}$, também na parte em *vermelho* do cubo, formará uma tripla junto com $F_{m,l,k}$ na parte em *amarelo* e $F_{l,k,m}$ na parte em *verde*. Veja, por exemplo, o coeficiente $F_{3,1,0}$ indicado na Figura 10c, que pode ser relacionado ao autovetor $\mathbf{v}_{3,1,0}$ e, consequentemente, ao autovalor $\lambda_{3,1,0}$ com multiplicidade igual a 6; formará uma tripla juntamente com os coeficientes $F_{1,0,3}$ e $F_{0,3,1}$ indicados na Figura 10c. Conforme mostrado na mesma figura, as posições de $F_{1,0,3}$ e $F_{0,3,1}$ são simétricas à de $F_{3,1,0}$ em relação aos planos diagonais $l = m$ e $k = m$, respectivamente. Adicionalmente, tem-se o coeficiente $F_{3,0,1}$, também relacionado ao referido autovetor e autovalor, e ocupando uma posição simétrica à ocupada por $F_{3,1,0}$ em relação ao plano diagonal $m = 4 - l$, como indicado na Figura 10c; $F_{3,0,1}$ formará uma tripla juntamente com os coeficientes $F_{0,1,3}$ e $F_{1,3,0}$ indicados na Figura 10c. As posições de $F_{0,1,3}$ e $F_{1,3,0}$ são simétricas à de $F_{3,0,1}$ em relação aos planos diagonais $l = m$ e $k = m$, respectivamente.

Isso permite concluir que é suficiente escolher uma ordem para endereçar cada coeficiente 3D-DCT na parte em *vermelho* do cubo considerada nas Figuras 9 e 10, de modo que os outros dois coeficientes na tripla correspondente serão resolvidos automaticamente[4]. Logo, foi escolhida a ordem ilustrada na Figura 11, que endereça sequencialmente os coeficientes 3D-DCT na parte em *vermelho* do cubo, para cada plano $m = 0, 1, 2, 3$, de cima para baixo e da esquerda

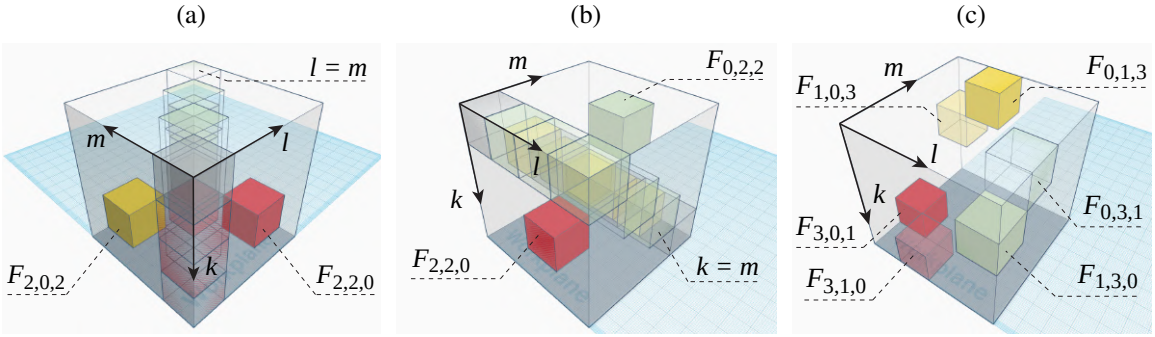
[4] Uma regra prática para obter os outros dois coeficientes de uma tripla, a partir de um coeficiente $F_{k,l,m}$ localizado na parte em *vermelho* das estruturas cúbicas consideradas, é aplicar dois deslocamentos cíclicos sequenciais à esquerda para os índices k, l, m; desta maneira, obtêm-se os coeficientes $F_{l,m,k}$ e $F_{m,k,l}$.

Figura 9 – Arranjo espacial dos coeficientes no domínio da transformada de uma estrutura cúbica $4 \times 4 \times 4$: (a) Estrutura $4 \times 4 \times 4$ representando o arranjo espacial (particionamento em quatro conjuntos) dos coeficientes no domínio da transformada e (b) sua vista explodida.



Fonte: A autora (2020).

Figura 10 – (a) e (b) Um autovetor em um autoespaço de dimensão 3 e (c) um autovetor em um autoespaço de dimensão 6, em uma estrutura $4 \times 4 \times 4$ representando o arranjo espacial dos coeficientes.



Fonte: A autora (2020).

para a direita. Desta forma, a sequência obtida de coeficientes é dada por

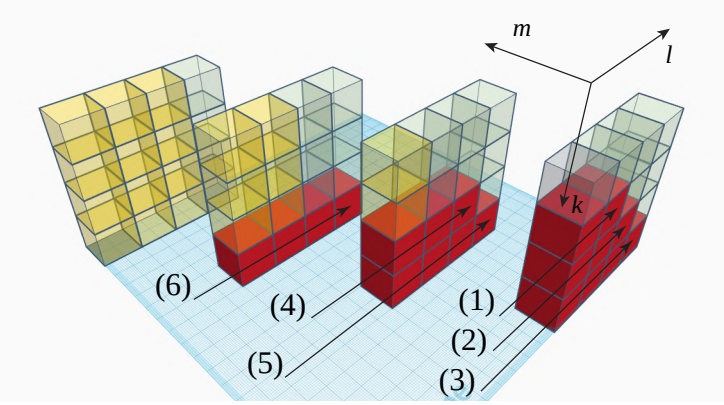
$$(1)\ F_{1,0,0},\ F_{1,1,0},\ (2)\ F_{2,0,0},\ F_{2,1,0},\ F_{2,2,0},\ (3)\ F_{3,0,0},\ F_{3,1,0},\ F_{3,2,0},\ F_{3,3,0},$$
$$(4)\ F_{2,0,1},\ F_{2,1,1},\ F_{2,2,1},\ (5)\ F_{3,0,1},\ F_{3,1,1},\ F_{3,2,1},\ F_{3,3,1},$$
$$(6)\ F_{3,0,2},\ F_{3,1,2},\ F_{3,2,2},\ F_{3,3,2}.$$

Isso fornece a seguinte regra referente à correspondência entre os ângulos de rotação e os coeficientes 3D-DCT na parte em *vermelho* do cubo $4 \times 4 \times 4$, usado como referência de cada tripla de coeficientes (ou autovetores) a serem rotacionados:

$$(\theta_{y,i}, \theta_{z,i}) \longrightarrow F_{k,l,m},\ \ i = 0, \ldots, 19;\ m = 0, \ldots, 2;\ k = m+1, \ldots, 3;\ l = 0, \ldots, k.$$

A Figura 12 apresenta várias subfiguras correspondentes àquelas apresentadas nas Figuras 9-11, mas considerando $N = 8$, ou seja, uma estrutura cúbica $8 \times 8 \times 8$. Nesse caso, a partir das explicações anteriores, sabe-se que $M = 168$ (ver Figura 12f); a regra que indica a correspondência entre os pares de ângulos de rotação e os coeficientes 3D-DCT na parte em

Figura 11 – Ordem em que os coeficientes (parte em *vermelho*) usados como referência de cada tripla de coeficientes a serem rotacionados são tomados e consequentemente relacionados a um par de ângulos de rotação.



Fonte: A autora (2020).

vermelho do cubo, usada como referência de cada tripla de coeficientes a serem rotacionados, é dada por

$$(\theta_{y,i}, \theta_{z,i}) \longrightarrow F_{k,l,m},\ \ i = 0, \ldots, 167;\ m = 0, \ldots, 6;\ k = m+1, \ldots, 7;\ l = 0, \ldots, k.$$

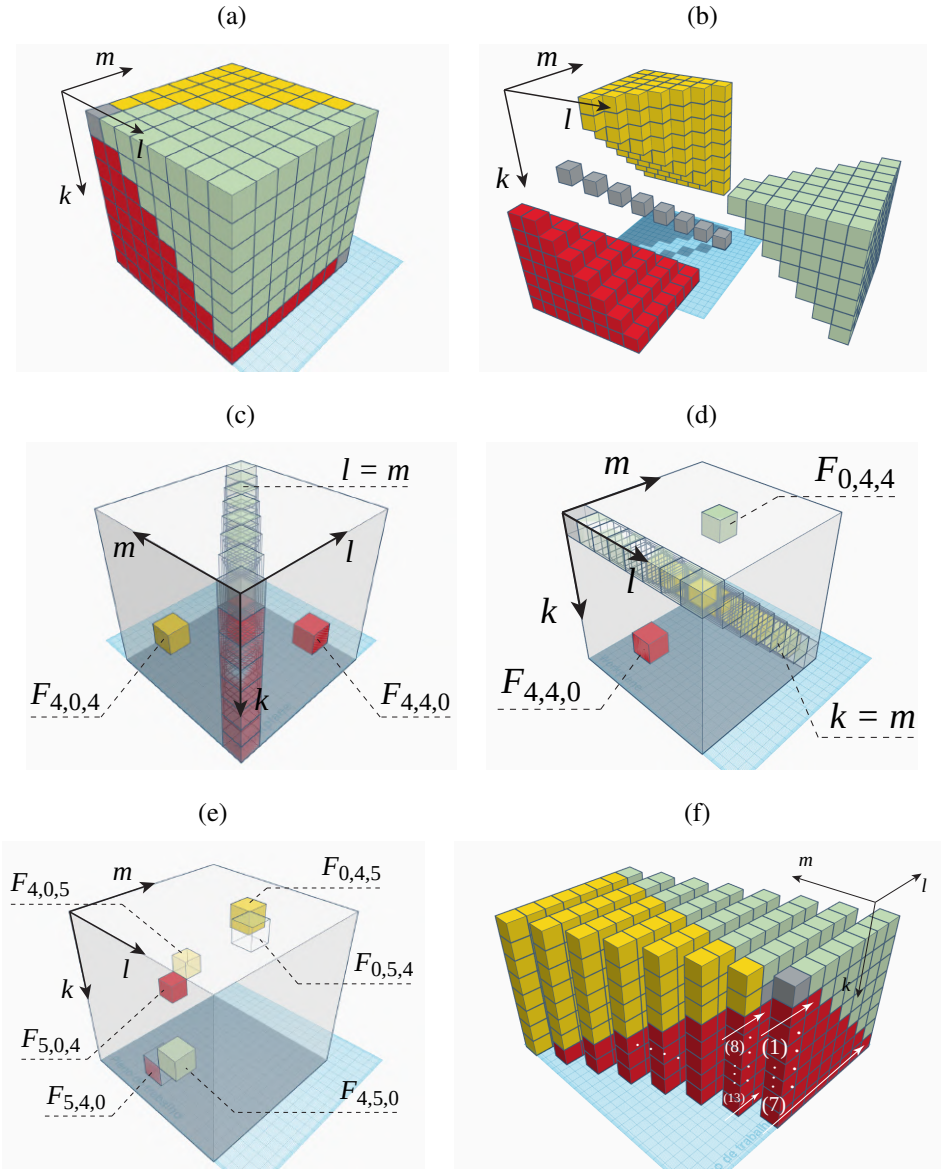
Em geral, para um dado N, a regra que indica a correspondência entre os ângulos de rotação e os coeficientes 3D-DCT usados como referência de cada tripla de coeficientes a serem rotacionados pode ser descrita como

$$\begin{aligned}(\theta_{y,i}, \theta_{z,i}) \longrightarrow F_{k,l,m},\ i = 0, \ldots, \frac{N^3 - N}{3} - 1; \qquad & m = 0, \ldots, N-2; \\ k = m+1, \ldots, N-1; \qquad & l = 0, \ldots, k. \end{aligned} \tag{58}$$

Isso fornece os detalhes necessários para o cálculo efetivo de $\mathbf{F}_{\mathrm{S}}(\boldsymbol{\Theta})$, a 3D-SDCT de um sinal $\mathbf{f}$ de dimensão $N \times N \times N$, de acordo com (57). Em resumo, é necessário realizar as seguintes etapas:

1. Calcule a 3D-DCT de $\mathbf{f}$, obtendo $\mathbf{F} = [F_{k,l,m}]$, $k, l, m = 0, 1, \ldots, N-1$;
2. Escolha um vetor $\boldsymbol{\Theta} = [(\theta_{y,i}, \theta_{z,i})]$, $i = 0, 1, \ldots, M-1$, $M = \frac{N^3-N}{3}$, de pares de ângulos de rotação;
3. Use o i-ésimo par de ângulos $(\theta_{y,i}, \theta_{z,i})$ para aplicar a rotação mostrada em (55) à tripla de coeficientes $[F_{k,l,m}\ \ F_{l,m,k}\ \ F_{m,k,l}]$, em que, de acordo com (58), $m = 0, \ldots, N-2$, $k = m+1, \ldots, N-1$ e $l = 0, \ldots, k$. A tripla rotacionada correspondente é denotada como $[F'_{k,l,m}\ \ F'_{l,m,k}\ \ F'_{m,k,l}]$. Além disso, se $k = l = m$, então $F'_{k,l,m} = F_{k,l,m}$.
4. Obtenha a 3D-SDCT de $\mathbf{f}$ como $\mathbf{F}_{\mathrm{S}}(\boldsymbol{\Theta}) = [F'_{k,l,m}]$, $k, l, m = 0, 1, \ldots, N-1$.

Figura 12 – (a) Estrutura $8 \times 8 \times 8$ representando o arranjo espacial dos coeficientes, (b) sua vista explodida, (c) e (d) um autovetor em um autoespaço de dimensão 3, (e) um autovetor em um autoespaço de dimensão 6 e (f) ordem na qual os coeficientes (parte em *vermelho*) usados como referência de cada tripla de coeficientes a serem rotacionados são tomados e consequentemente relacionados a um par de ângulos de rotação.



Fonte: A autora (2020).

3.1.5 Rotação Ótima

Como discutido na seção anterior, um vetor Θ formado por pares de ângulos deve ser escolhido para rotacionar a 3D-DCT e obter a sua versão manobrável. Neste contexto, o conceito de rotação ótima pode ser introduzido. Mais especificamente, pode-se mostrar que, por meio de uma escolha conveniente para cada par de ângulos de rotação, dois coeficientes em cada tripla dos coeficientes 3D-DCT são anulados; essa escolha, que aqui é identificada como *rotação ótima*, sugere a possibilidade de compactar energia de forma mais eficiente do que a 3D-SDCT com

rotação não ótima ou a 3D-DCT.

Neste cenário, seja a tripla $[F_{k,l,m} \;\; F_{l,m,k} \;\; F_{m,k,l}]$ inicialmente rotacionada em torno do eixo z pelo ângulo $\theta_z = \arctan(F_{l,m,k}/F_{k,l,m})$ de acordo com (55). Isto produz claramente a tripla rotacionada $[F''_{k,l,m} \;\; 0 \;\; F''_{m,k,l}]$. Em seguida, aplicando uma rotação em torno do eixo y pelo ângulo $\theta_y = \arctan(F''_{m,k,l}/F''_{k,l,m})$, obtém-se a tripla rotacionada $[F'_{k,l,m} \; 0 \; 0]$. Esse procedimento é ilustrado na Figura 13. Se a rotação ótima for empregada, somente $M + N = (N^3 + 2N)/3$ coeficientes 3D-SDCT serão diferentes de zero; isso equivale a preservar, após a aplicação da rotação, apenas os coeficientes localizados nas regiões de cor *vermelho* e *cinza* das estruturas cúbicas apresentadas na seção anterior.

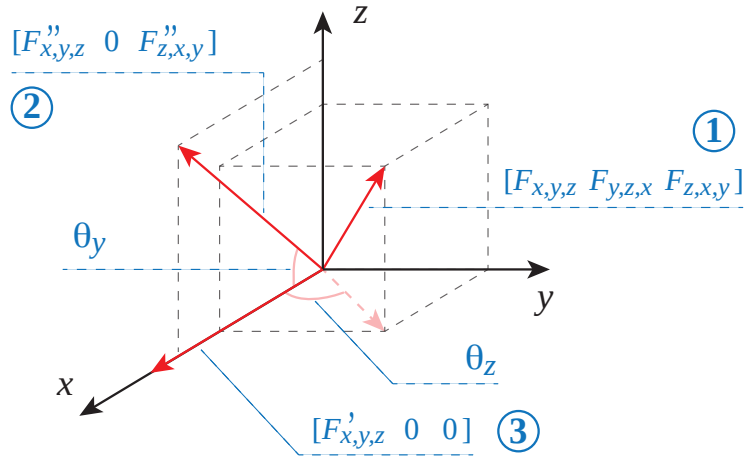
O uso da rotação ótima permite que $\frac{2}{3}$ dos coeficientes rotacionados da 3D-SDCT se tornem nulos. A Figura 14 ilustra a posição de cada coeficiente em um bloco de tamanho $4 \times 4 \times 4$ transformado. Para verificar se $\frac{2}{3}$ dos coeficientes rotacionados são anulados, as Figuras 16, 17, 18 e 19 fornecem uma visualização dos coeficientes 3D-DCT e 3D-SDCT de um bloco $4 \times 4 \times 4$ selecionado arbitrariamente da imagem apresentada na Figura 15.

Pode-se observar nas Figuras 16, 17, 18 e 19 que os coeficientes com multiplicidade igual a 1, ou seja, os coeficientes $F_{k,l,m}$ com $k = l = m$, permanecem inalterados, pois eles não são rotacionados. Esses coeficientes são: o $F_{0,0,0}$, que se encontra na 1ª linha e 1ª coluna da Figura 16; o $F_{1,1,1}$, na 2ª linha e 2ª coluna da Figura 17; o $F_{2,2,2}$, na 3ª linha e 3ª coluna da Figura 18; e o $F_{3,3,3}$, na 4ª linha e 4ª coluna da Figura 19.

Os coeficientes com multiplicidade igual a 3, ou seja, os coeficientes $F_{k,l,m}$ com $k = l$ e $l \neq m$ ou $k = m$ e $m \neq l$ ou $m = l$ e $l \neq k$ são rotacionados e dois dos três coeficientes são anulados. Por exemplo, para $k = l$ e $l \neq m$ a tripla de coeficientes que será rotacionada é $F_{k,k,m}$, $F_{k,m,k}$ e $F_{m,k,k}$. Tomando $k = l = 0$ e $m = 1$, o coeficiente $F_{1,0,0}$ deve ser diferente de zero e os coeficientes $F_{0,0,1}$ e $F_{0,1,0}$ iguais a zero. Nas Figuras 16 e 17 é possível observar que isso acontece. O coeficiente rotacionado $F_{1,0,0}$ encontra-se na 2ª linha e 1ª coluna da Figura 16b com valor igual a -64,1912 e os coeficientes rotacionados $F_{0,0,1}$ e $F_{0,1,0}$ encontram-se, respectivamente, na 1ª linha e 1ª coluna da Figura 17b e na 1ª linha e 2ª coluna da Figura 16b e apresentam valores iguais a zero. Isso acontece com os demais coeficientes que apresentam multiplicidade igual a 3, como pode ser visto na Tabela 1.

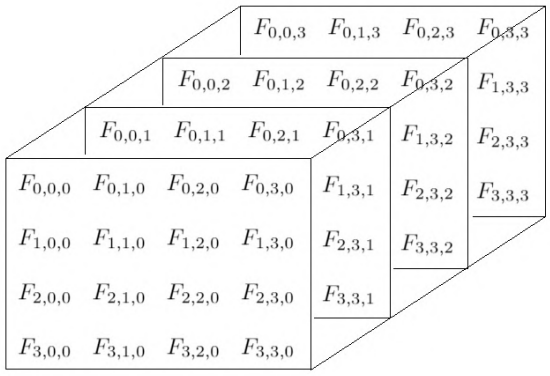
Para os coeficientes que apresentam multiplicidade igual a 6, ou seja, quando $k \neq l \neq m$, o par de triplas é rotacionado e dois dos três coeficientes de cada par devem ser anulados ao se utilizar a abordagem de rotação ótima. Por exemplo, para $k = 0$, $l = 1$ e $m = 2$, o par de triplas de coeficientes que será rotacionado é ($F_{2,1,0}$, $F_{1,0,2}$, $F_{0,2,1}$) e ($F_{2,0,1}$, $F_{0,1,2}$, $F_{1,2,0}$). Na tripla ($F_{2,1,0}$, $F_{1,0,2}$, $F_{0,2,1}$), o coeficiente $F_{2,1,0}$ deve ser diferente de zero e os coeficientes $F_{1,0,2}$ e $F_{0,2,1}$ iguais a zero, e na tripla ($F_{2,0,1}$, $F_{0,1,2}$, $F_{1,2,0}$), o coeficiente $F_{2,0,1}$ deve ser diferente de zero e os coeficientes $F_{0,1,2}$ e $F_{1,2,0}$ iguais a zero. O coeficiente rotacionado $F_{2,1,0}$ encontra-se na 3ª linha e 2ª coluna da Figura 16b, com valor igual a 52,0518, e os coeficientes rotacionados $F_{1,0,2}$ e $F_{0,2,1}$ encontram-se, respectivamente, na 2ª linha e 1ª coluna da Figura 18b e na 1ª linha e 3ª coluna da Figura 17b e apresentam valores iguais a zero. O coeficiente rotacionado $F_{2,0,1}$

Figura 13 – Rotação ótima: tripla $[F_{x,y,z}\ F_{y,z,x}\ F_{z,x,y}]$ rotacionada em torno do eixo z com $\theta_z = \arctan(F_{y,z,x}/F_{x,y,z})$ e em torno do eixo y com $\theta_y = \arctan(F''_{z,x,y}/F''_{x,y,z})$.



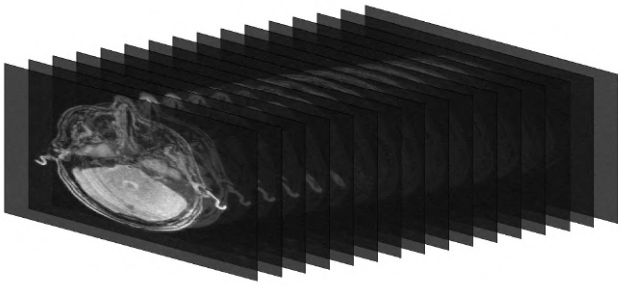
Fonte: A autora (2020).

Figura 14 – Bloco $4 \times 4 \times 4$ de coeficientes.



Fonte: A autora (2020).

Figura 15 – Imagem utilizada para exemplificar a 3D-SDCT com rotação ótima: *brain cancer* (BARBORIAK, 2015) ($256 \times 256 \times 16$ *pixels*).



Fonte: A autora (2020).

Figura 16 – Coeficientes da fatia 1 do bloco $4 \times 4 \times 4$: (a) 3D-DCT; (b) 3D-SDCT. (O coeficiente na cor cinza, com multiplicidade 1, permanece inalterado, pois não sofre rotação.)

(a)

225,1250	37,2294	13,8750	5,2798
-52,2249	-51,0412	-21,4838	-14,1285
25,1250	39,8618	23,8750	15,5546
-16,6574	-23,8785	-12,3430	-20,4588

(b)

225,1250	0	0	0
-64,1912	-52,2338	0	0
47,9210	52,0518	42,3990	0
-18,1818	-24,8573	-18,4239	-22,0415

Fonte: A autora (2020).

Figura 17 – Coeficientes da fatia 2 do bloco $4 \times 4 \times 4$: (a) 3D-DCT; (b) 3D-SDCT. (O coeficiente na cor cinza, com multiplicidade 1, permanece inalterado, pois não sofre rotação.)

(a)

-2,6547	2,0581	4,1855	6,0669
-10,9058	2,2106	-2,4079	1,3080
10,1539	3,8436	-9,1643	3,7563
4,3007	8,9000	-12,4723	-11,0920

(b)

0	0	0	0
0	2,2106	0	0
48,0237	49,5296	-52,2046	0
15,6517	9,4744	-21,6973	-11,0920

Fonte: A autora (2020).

Figura 18 – Coeficientes da fatia 3 do bloco $4 \times 4 \times 4$: (a) 3D-DCT; (b) 3D-SDCT. (O coeficiente na cor cinza, com multiplicidade 1, permanece inalterado, pois não sofre rotação.)

(a)

-38,3750	-41,7327	-23,6250	-12,8854
33,2101	49,3215	28,3297	17,0375
-25,8750	-42,8808	-20,1250	-15,6571
14,5214	17,7875	21,6843	17,6785

(b)

0	0	0	0
0	0	0	0
0	0	-20,1250	0
21,3209	21,0080	26,7493	17,9101

Fonte: A autora (2020).

encontra-se na 3ª linha e 1ª coluna da Figura 17b, com valor igual a 48,0237, e os coeficientes rotacionados $F_{0,1,2}$ e $F_{1,2,0}$ encontram-se, respectivamente, na 1ª linha e 2ª coluna da Figura 18b

Figura 19 – Coeficientes da fatia 4 do bloco $4 \times 4 \times 4$: (a) 3D-DCT; (b) 3D-SDCT. (O coeficiente na cor cinza, com multiplicidade 1, permanece inalterado, pois não sofre rotação.)

(a)

5,0233	-5,1831	-1,3278	2,9419
3,3007	2,9740	10,5277	-6,4609
4,5886	-4,9937	0,4135	2,3436
7,6558	-4,4643	1,6579	0,4373

(b)

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0,4373

Fonte: A autora (2020).

e na 2ª linha e 3ª coluna da Figura 16b e apresentam valores iguais a zero. Esse comportamento ocorre com os demais pares de triplas de coeficientes que apresentam multiplicidade igual a 6, conforme pode ser visto na Tabela 2.

Portanto, para o bloco de tamanho $4 \times 4 \times 4$ definido na Figura 14, tem-se um total de $4^3 = 64$ coeficientes 3D-DCT não nulos e $(\frac{1}{3}60) + 4 = 24$ coeficientes 3D-SDCT diferentes de zero (usando rotação ótima), ou seja, $\frac{2}{3}(64 - 4) = 40$ coeficientes 3D-SDCT são anulados.

3.2 ANÁLISE DA MULTIPLICIDADE DOS AUTOVALORES DO LAPLACIANO DO PRODUTO CARTESIANO DE QUATRO GRAFOS EM CAMINHO

Light fields (campos de luz) são estruturas quadridimensionais (4D) que possuem resolução espacial e angular, e que são compostas por subimagens bidimensionais (2D). Resumidamente, uma imagem *light field* é criada através da inserção de fatias 2D na representação 4D; múltiplas vistas de uma cena são utilizadas para criar novos pontos de vista (LEVOY; HANRAHAN, 1996; NG et al., 2005; ALVES; PEREIRA; da Silva, 2016). O processamento de *light fields* é um tema de pesquisa desafiador devido à alta dimensionalidade desse tipo de dado. No cenário de representação e codificação de *light fields*, há diversos trabalhos que fazem uso da 4D-DCT (CARVALHO et al., 2018; CONTI; SOARES; NUNES, 2016; LIU et al., 2016; CONTI; NUNES; SOARES, 2018; SANTOS et al., 2018). Isso sugere a definição de uma versão 4D da SDCT para ser avaliada no cenário mencionado, que pode levar a um melhor desempenho em relação aos resultados obtidos com a 4D-DCT.

Para a definição de uma versão 4D da SDCT, o ponto central é analisar a multiplicidade dos autovalores da 4D-DCT associados aos autovetores que constituem uma possível autobase para o Laplaciano do produto de quatro grafos em caminho. A definição da 4D-DCT é apresentada a seguir.

Definição 3.2. A transformada discreta quadridimensional do cosseno de um sinal $\mathbf{f}$ com dimensão $N \times N \times N \times N$ é definida como uma extensão direta do caso unidimensional (DCT), como segue

$$F(j,k,l,m) = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1}\sum_{z=0}^{N-1}\sum_{t=0}^{N-1} f(x,y,z,t)\alpha(j)\alpha(k)\alpha(l)\alpha(m)u_{x,y,z,t}(j,k,l,m), \tag{59}$$

em que

$$\alpha(k) = \begin{cases} \sqrt{\frac{1}{N}}, & k = 0, \\ \sqrt{\frac{2}{N}}, & k = 1, 2, \ldots, N-1, \end{cases} \tag{60}$$

e

$$u_{x,y,z,t}(j,k,l,m) = \cos\left[\frac{\pi(2x+1)j}{2N}\right]\cos\left[\frac{\pi(2y+1)k}{2N}\right]\cos\left[\frac{\pi(2z+1)l}{2N}\right] \cos\left[\frac{\pi(2t+1)m}{2N}\right]. \tag{61}$$

A transformada inversa, 4D-DCT inversa (do inglês *inverse 4D-DCT*), é dada por

$$f(x,y,z,t) = \sum_{j=0}^{N-1}\sum_{k=0}^{N-1}\sum_{l=0}^{N-1}\sum_{m=0}^{N-1} F(j,k,l,m)\alpha(j)\alpha(k)\alpha(l)\alpha(m)u_{x,y,z,t}(j,k,l,m). \tag{62}$$

O cálculo da 4D-DCT do sinal $\mathbf{f}$ pode ser expresso, na forma matricial, como $\bar{\mathbf{F}}_{\text{4D-DCT}} = \mathbf{C}_{\text{4D-DCT}}\bar{\mathbf{f}}^T$, em que

$$\bar{\mathbf{f}} = [f(0,0,0,0)\ldots f(0,0,0,N-1)\ f(0,0,1,0)\ldots f(N-1,N-1,N-1,N-1)]$$

é um vetor $1 \times N^4$ formado pelos elementos de $\mathbf{f}$ tomados na ordem lexicográfica; de forma análoga, $\bar{\mathbf{F}}_{\text{4D-DCT}}$ é formado pelos elementos de $\mathbf{F}_{\text{4D-DCT}}$; $\mathbf{C}_{\text{4D-DCT}}$ é a matriz de transformação de dimensão $N^4 \times N^4$ com suas entradas dadas por

$$C_{x,y,z,t}(j,k,l,m) = \alpha(j)\alpha(k)\alpha(l)\alpha(m)u_{x,y,z,t}(j,k,l,m), \tag{63}$$

com índices x, y, z, t e j, k, l, m variando na ordem lexicográfica ao longo das colunas e linhas, respectivamente.

O ponto de partida para a definição de uma versão 4D da SDCT é considerar o produto Cartesiano de quatro grafos em caminho ($\mathcal{Z}_N$, em que $\mathcal{Z}_N = \mathcal{P}_N \square \mathcal{P}_N \square \mathcal{P}_N \square \mathcal{P}_N$), cada um com N vértices, e fazer a análise espectral de sua matriz Laplaciana $\mathbf{L}(\mathcal{Z}_N)$. Analogamente à definição do Laplaciano de um grafo em grade cúbica, $\mathbf{L}(\mathcal{L}_N)$ (ver Subseção 3.1.1), o Laplaciano $\mathbf{L}(\mathcal{Z}_N)$ pode ser determinado por

$$\begin{aligned}\mathbf{L}(\mathcal{Z}_N) =& \mathbf{L}(\mathcal{P}_N)\otimes\mathbf{I}_N\otimes\mathbf{I}_N\otimes\mathbf{I}_N + \mathbf{I}_N\otimes\mathbf{L}(\mathcal{P}_N)\otimes\mathbf{I}_N\otimes\mathbf{I}_N + \\ &+ \mathbf{I}_N\otimes\mathbf{I}_N\otimes\mathbf{L}(\mathcal{P}_N)\otimes\mathbf{I}_N + \mathbf{I}_N\otimes\mathbf{I}_N\otimes\mathbf{I}_N\otimes\mathbf{L}(\mathcal{P}_N).\end{aligned} \tag{64}$$

Os autovalores de $\mathbf{L}(\mathcal{Z}_N)$ são todas as possíveis somas entre os autovalores de cada grafo em caminho, ou seja,

$$\lambda_{j,k,l,m} = 4\left[\operatorname{sen}^2\left(\frac{\pi j}{2N}\right) + \operatorname{sen}^2\left(\frac{\pi k}{2N}\right) + \operatorname{sen}^2\left(\frac{\pi l}{2N}\right) + \operatorname{sen}^2\left(\frac{\pi m}{2N}\right)\right], \tag{65}$$

para $j, k, l, m = 0, \ldots, N-1$. Além disso, como $\mathbf{v}_j = [v_j(n)]$, $n = 0, \ldots, N-1$, em que

$$v_j(n) = \alpha(j)\cos\left(\frac{\pi j}{2N}(2n+1)\right) \tag{66}$$

é um autovetor de $\mathcal{P}_N$ (e vetor base da DCT do tipo 2) relacionado ao autovalor λ_j, $j = 0, \ldots, N-1$, então

$$\mathbf{v}_{j,k,l,m} = \mathbf{v}_j \otimes \mathbf{v}_k \otimes \mathbf{v}_l \otimes \mathbf{v}_m \tag{67}$$

é um autovetor de $\mathcal{Z}_N$ relacionado ao autovalor $\lambda_{j,k,l,m}$, $j, k, l, m = 0, \ldots, N-1$. Isso significa que os vetores de base da 4D-DCT constituem uma autobase para o Laplaciano $\mathbf{L}(\mathcal{Z}_N)$.

Os autovalores do Laplaciano $\mathbf{L}(\mathcal{Z}_N)$ são determinados a partir de (65). Analisando a multiplicidade algébrica, tem-se, para $0 \leq j, k, l, m \leq N-1$, os seguintes casos:

- O autovalor $\lambda_{j,k,l,m}$ apresenta multiplicidade igual a 1, quando $j = k = l = m$;
- O autovalor $\lambda_{j,k,l,m}$ apresenta multiplicidade igual a 4, para os seguintes cenários:
  1. $j = k = l$ e $l \neq m$, ou seja, $\lambda_{j,j,j,m} = \lambda_{j,j,m,j} = \lambda_{m,j,j,j} = \lambda_{j,m,j,j}$;
  2. $j = k = m$ e $m \neq l$, ou seja, $\lambda_{j,j,l,j} = \lambda_{j,j,j,l} = \lambda_{l,j,j,j} = \lambda_{j,l,j,j}$;
  3. $j = l = m$ e $m \neq k$, ou seja, $\lambda_{j,k,j,j} = \lambda_{k,j,j,j} = \lambda_{j,j,k,j} = \lambda_{j,j,j,k}$;
  4. $k = l = m$ e $m \neq j$, ou seja, $\lambda_{j,k,k,k} = \lambda_{k,j,k,k} = \lambda_{k,k,k,j} = \lambda_{k,k,j,k}$;
- O autovalor $\lambda_{j,k,l,m}$ apresenta multiplicidade igual a 6, para os seguintes cenários:
  1. $(j = k) \neq (l = m)$, ou seja,
     $\lambda_{j,j,l,l} = \lambda_{l,l,j,j} = \lambda_{j,l,j,l} = \lambda_{j,l,l,j} = \lambda_{l,j,j,l} = \lambda_{l,j,l,j}$;
  2. $(j = l) \neq (k = m)$, ou seja,
     $\lambda_{j,k,j,k} = \lambda_{j,k,k,j} = \lambda_{k,k,j,j} = \lambda_{j,j,k,k} = \lambda_{k,j,j,k} = \lambda_{k,j,k,j}$;
  3. $(m = j) \neq (k = l)$, ou seja,
     $\lambda_{m,k,k,m} = \lambda_{m,k,m,k} = \lambda_{k,m,k,m} = \lambda_{k,m,m,k} = \lambda_{m,m,k,k} = \lambda_{k,k,m,m}$;
- O autovalor $\lambda_{j,k,l,m}$ apresenta multiplicidade igual a 12, para os seguintes cenários:
  1. $j = k$ e $k \neq l \neq m$, ou seja,
     $\lambda_{j,j,l,m} = \lambda_{j,j,m,l} = \lambda_{l,m,j,j} = \lambda_{m,l,j,j} = \lambda_{l,j,m,j} = \lambda_{l,j,j,m} = \lambda_{j,l,m,j} = \lambda_{j,l,j,m} = \lambda_{j,m,j,l} = \lambda_{j,m,l,j} = \lambda_{m,j,j,l} = \lambda_{m,j,l,j}$;

2. $j = l$ e $l \neq k \neq m$, ou seja,

   $\lambda_{j,k,j,m} = \lambda_{j,k,m,j} = \lambda_{k,j,j,m} = \lambda_{k,j,m,j} = \lambda_{m,j,k,j} = \lambda_{m,j,j,k} = \lambda_{j,m,k,j} = \lambda_{j,m,j,k} = \lambda_{j,j,k,m} = \lambda_{j,j,m,k} = \lambda_{m,k,j,j} = \lambda_{k,m,j,j}$;

3. $j = m$ e $m \neq k \neq l$, ou seja,

   $\lambda_{j,k,l,j} = \lambda_{j,k,j,l} = \lambda_{k,j,l,j} = \lambda_{k,j,j,l} = \lambda_{j,l,k,j} = \lambda_{j,l,j,k} = \lambda_{l,j,k,j} = \lambda_{l,j,j,k} = \lambda_{j,j,k,l} = \lambda_{j,j,l,k} = \lambda_{k,l,j,j} = \lambda_{l,k,j,j}$;

4. $k = l$ e $l \neq j \neq m$, ou seja,

   $\lambda_{j,k,k,m} = \lambda_{j,k,m,k} = \lambda_{k,j,k,m} = \lambda_{k,j,m,k} = \lambda_{m,k,k,j} = \lambda_{m,k,j,k} = \lambda_{k,m,k,j} = \lambda_{k,m,j,k} = \lambda_{k,k,j,m} = \lambda_{k,k,m,j} = \lambda_{j,m,k,k} = \lambda_{m,j,k,k}$;

5. $k = m$ e $m \neq j \neq l$, ou seja,

   $\lambda_{j,k,l,k} = \lambda_{j,k,k,l} = \lambda_{k,j,l,k} = \lambda_{k,j,k,l} = \lambda_{k,l,k,j} = \lambda_{k,l,j,k} = \lambda_{l,k,k,j} = \lambda_{l,k,j,k} = \lambda_{k,k,j,l} = \lambda_{k,k,l,j} = \lambda_{j,l,k,k} = \lambda_{l,j,k,k}$;

6. $l = m$ e $m \neq j \neq k$, ou seja,

   $\lambda_{j,k,l,l} = \lambda_{k,j,l,l} = \lambda_{l,l,j,k} = \lambda_{l,l,k,j} = \lambda_{k,l,j,l} = \lambda_{k,l,l,j} = \lambda_{l,k,j,l} = \lambda_{l,k,l,j} = \lambda_{l,j,l,k} = \lambda_{l,j,k,l} = \lambda_{j,l,l,k} = \lambda_{j,l,k,l}$;

- O autovalor $\lambda_{j,k,l,m}$ apresenta multiplicidade igual a 24, quando $j \neq k \neq l \neq m$. Devido à simetria:

  $\lambda_{j,k,l,m} = \lambda_{j,k,m,l} = \lambda_{j,l,k,m} = \lambda_{j,l,m,k} = \lambda_{j,m,k,l} = \lambda_{j,m,l,k} = \lambda_{k,j,l,m} = \lambda_{k,j,m,l} = \lambda_{k,l,j,m} = \lambda_{k,l,m,j} = \lambda_{k,m,j,l} = \lambda_{k,m,l,j} = \lambda_{l,j,k,m} = \lambda_{l,j,m,k} = \lambda_{l,k,j,m} = \lambda_{l,k,m,j} = \lambda_{l,m,j,k} = \lambda_{l,m,k,j} = \lambda_{m,j,k,l} = \lambda_{m,j,l,k} = \lambda_{m,k,j,l} = \lambda_{m,k,l,j} = \lambda_{m,l,k,j} = \lambda_{m,l,j,k}$.

No espectro de $\mathbf{L}(\mathcal{Z}_N)$ existem N autovalores com multiplicidade algébrica igual a 1, $4N(N-1)$ autovalores com multiplicidade algébrica igual a 4, $3N(N-1)$ autovalores com multiplicidade algébrica igual a 6, $6N(N-1)(N-2)$ autovalores com multiplicidade algébrica igual a 12 e $N(N-1)(N-2)(N-3)$ autovalores com multiplicidade algébrica igual a 24. Uma vez que os autovetores de $\mathbf{L}(\mathcal{Z}_N)$ são dados pelo produto de Kronecker entre os respectivos autovetores de $\mathcal{P}_N$, e o produto de Kronecker não é comutativo, a multiplicidade geométrica de cada autovalor é igual à multiplicidade algébrica correspondente. Isso significa que a dimensão de cada autoespaço correspondente aos autovalores é maior do que 1 (com exceção de $\lambda_{j,k,l,m}$, com $j = k = l = m$) e, portanto, a 4D-DCT não é a única autobase para $\mathbf{L}(\mathcal{Z}_N)$.

De forma análoga à definição da 3D-SDCT, a versão 4D da SDCT pode ser obtida pela aplicação de rotações aos vetores de base da 4D-DCT. A partir da análise da multiplicidade dos autovalores, percebe-se que há várias possibilidades para agrupar os autovetores e rotacioná-los. No entanto, o estudo e a descrição de tais possibilidades ficarão como trabalhos futuros.

Seguindo a mesma metodologia, partindo da análise da multiplicidade dos autovalores de uma transformada nD-DCT e do agrupamento dos autovetores a serem rotacionados, transformadas manobráveis do cosseno em dimensões maiores que 4, nD-SDCT para $n \geq 5$, podem ser

definidas. A definição dessas transformadas envolve um trabalho adicional à medida em que se aumenta o número de dimensões (n). No entanto, essa definição acontece de forma sistemática.

Tabela 1 – Coeficientes com multiplicidade igual a 3.

Tripla	Coeficiente	3D-DCT	3D-SDCT	Posição	Figura
1	$F_{1,0,0}$	-52,2249	-64,1912	3ª linha, 1ª coluna	16
	$F_{0,0,1}$	-2,6547	0	1ª linha, 1ª coluna	17
	$F_{0,1,0}$	37,2294	0	1ª linha, 3ª coluna	16
2	$F_{1,1,0}$	-51,0412	-52,2338	2ª linha, 2ª coluna	16
	$F_{1,0,1}$	-10,9058	0	2ª linha, 1ª coluna	17
	$F_{0,1,1}$	2,0581	0	1ª linha, 2ª coluna	17
3	$F_{2,0,0}$	25,1250	47,9210	3ª linha, 1ª coluna	16
	$F_{0,2,0}$	13,8750	0	1ª linha, 3ª coluna	16
	$F_{0,0,2}$	-38,3750	0	1ª linha, 1ª coluna	18
4	$F_{2,2,0}$	23,8750	42,3990	3ª linha, 3ª coluna	16
	$F_{2,0,2}$	-25,8750	0	3ª linha, 1ª coluna	18
	$F_{0,2,2}$	-23,6250	0	1ª linha, 3ª coluna	18
5	$F_{3,0,0}$	5,2798	-18,1818	4ª linha, 1ª coluna	16
	$F_{0,0,3}$	5,0233	0	1ª linha, 1ª coluna	19
	$F_{0,3,0}$	-16,6574	0	1ª linha, 4ª coluna	16
6	$F_{3,3,0}$	-20,4588	-22,0415	4ª linha, 4ª coluna	16
	$F_{3,0,3}$	7,6558	0	4ª linha, 1ª coluna	19
	$F_{0,3,3}$	2,9419	0	1ª linha, 4ª coluna	19
7	$F_{2,1,1}$	3,8436	49,5296	3ª linha, 2ª coluna	17
	$F_{1,1,2}$	49,3215	0	2ª linha, 2ª coluna	18
	$F_{1,2,1}$	-2,4079	0	2ª linha, 3ª coluna	17
8	$F_{2,2,1}$	-9,1643	-52,2046	3ª linha, 3ª coluna	17
	$F_{2,1,2}$	-42,8808	0	3ª linha, 2ª coluna	18
	$F_{1,2,2}$	28,3297	0	2ª linha, 3ª coluna	18
9	$F_{3,1,1}$	8,9000	9,4744	4ª linha, 2ª coluna	17
	$F_{1,1,3}$	2,9740	0	2ª linha, 2ª coluna	19
	$F_{1,3,1}$	1,3080	0	2ª linha, 4ª coluna	17
10	$F_{3,3,1}$	-7,8332	-11,0920	4ª linha, 4ª coluna	17
	$F_{3,1,3}$	-4,4643	0	4ª linha, 2ª coluna	19
	$F_{1,3,3}$	-6,4609	0	2ª linha, 4ª coluna	19
11	$F_{3,2,2}$	21,6843	26,7493	4ª linha, 3ª coluna	18
	$F_{2,2,3}$	0,4135	0	3ª linha, 3ª coluna	19
	$F_{2,3,2}$	-15,6571	0	3ª linha, 4ª coluna	18
12	$F_{3,3,2}$	17,6785	17,9101	4ª linha, 4ª coluna	18
	$F_{3,2,3}$	1,6579	0	4ª linha, 3ª coluna	19
	$F_{2,3,3}$	-2,3436	0	3ª linha, 4ª coluna	19

Fonte: A autora (2020).

Tabela 2 – Coeficientes com multiplicidade igual a 6.

Par de Tripla	Coeficiente	3D-DCT	3D-SDCT	Posição	Figura
1	$F_{2,1,0}$	39,8618	52,0518	3ª linha, 2ª coluna	16
	$F_{1,0,2}$	33,2101	0	2ª linha, 1ª coluna	18
	$F_{0,2,1}$	4,1855	0	1ª linha, 3ª coluna	17
	$F_{2,0,1}$	10,1539	48,0237	3ª linha, 1ª coluna	17
	$F_{0,1,2}$	-41,7327	0	1ª linha, 2ª coluna	18
	$F_{1,2,0}$	-21,4838	0	2ª linha, 3ª coluna	16
2	$F_{3,1,0}$	-23,8785	-24,8573	4ª linha, 2ª coluna	16
	$F_{1,0,3}$	3,3007	0	2ª linha, 1ª coluna	19
	$F_{0,3,1}$	6,0669	0	1ª linha, 4ª coluna	17
	$F_{3,0,1}$	4,3007	15,6517	4ª linha, 1ª coluna	17
	$F_{0,1,3}$	-5,1831	0	1ª linha, 2ª coluna	19
	$F_{1,3,0}$	-14,1285	0	2ª linha, 4ª coluna	16
3	$F_{3,2,0}$	-12,3430	-18,4239	4ª linha, 3ª coluna	16
	$F_{2,0,3}$	4,5886	0	3ª linha, 1ª coluna	19
	$F_{0,3,2}$	-12,8854	0	1ª linha, 4ª coluna	18
	$F_{3,0,2}$	14,5214	21,3209	4ª linha, 1ª coluna	18
	$F_{0,2,3}$	-1,3278	0	1ª linha, 3ª coluna	19
	$F_{2,3,0}$	15,5446	0	3ª linha, 4ª coluna	16
4	$F_{3,2,1}$	-12,4723	-21,6973	4ª linha, 3ª coluna	17
	$F_{2,1,3}$	-4,9937	0	3ª linha, 2ª coluna	19
	$F_{1,3,2}$	17,0375	0	2ª linha, 4ª coluna	18
	$F_{3,1,2}$	17,7875	21,0080	4ª linha, 2ª coluna	18
	$F_{1,2,3}$	10,5277	0	2ª linha, 3ª coluna	19
	$F_{2,3,1}$	3,7563	0	3ª linha, 4ª coluna	17

Fonte: A Autora, 2020.

4 TRANSFORMADAS NUMÉRICAS MANOBRÁVEIS DO COSSENO

Este capítulo apresenta a definição de uma transformada manobrável do cosseno sobre corpos finitos primos, $\mathrm{GF}(p)$, empregando uma metodologia análoga à utilizada na definição da SDCT (ver Capítulo 2). A transformada proposta é identificada como transformada numérica manobrável do cosseno (SCNT, do inglês *steerable cosine number transform*), e pode ser vista como uma generalização da transformada numérica do cosseno (CNT, do inglês *cosine number transform*), em que uma nova base é construída a partir da rotação, empregando funções trigonométricas sobre corpos finitos, de pares de vetores de base da CNT. Os vetores de base da CNT estão associados ao mesmo autovalor, em $\mathrm{GF}(p)$, do Laplaciano de um grafo em caminho com N vértices.

A extensão da SCNT para o cenário tridimensional também é apresentada neste capítulo, e é identificada como transformada numérica tridimensional manobrável do cosseno (3D-SCNT, do inglês *three-dimensional steerable cosine number transform*). Tal transformada é obtida a partir do fato de que os vetores de base da transformada numérica tridimensional do cosseno (3D-CNT, do inglês *three-dimensional cosine number transform*) constituem uma possível autobase para o Laplaciano do grafo em grade cúbica avaliado em um corpo finito. A 3D-SCNT é definida empregando a rotação dos vetores de base da 3D-CNT, usando um operador de rotação sobre corpos finitos.

4.1 A TRANSFORMADA NUMÉRICA DO COSSENO

Para a definição da CNT, faz-se necessário definir as funções trigonométricas sobre corpos finitos. A CNT considerada nesta Tese tem uma estrutura análoga àquela da DCT tipo 2 (STRANG, 1999).

4.1.1 Trigonometria sobre corpos finitos

Os principais conceitos relacionados à trigonometria sobre corpos finitos foram apresentados pela primeira vez em (CAMPELLO DE SOUZA et al., 1998), como premissa para a definição de uma transformada de Hartley sobre corpos finitos. Em trabalhos posteriores, a teoria foi estendida, e novas aplicações foram surgindo (CINTRA et al., 2009; LIMA; CAMPELLO DE SOUZA, 2011; LIMA; CAMPELLO DE SOUZA; PANARIO, 2011; LIMA; CAMPELLO DE SOUZA, 2013). A seguir, é revisada a definição das funções cosseno e seno sobre corpos finitos. A particularidade deste trabalho é que optou-se por restringir à pertinência ao corpo finito primo $\mathbb{F}_p$ os elementos ζ em relação aos quais as referidas funções são calculadas. Na verdade, em contextos mais gerais, ζ pode ser um elemento pertencente a um corpo de extensão.

Definição 4.1. Seja ζ um elemento não nulo de um corpo finito $\mathbb{F}_p$, em que p é um primo ímpar. As funções cosseno e seno sobre corpos finitos relacionadas ao ângulo do elemento ζ^θ, $\theta = 0, 1, \ldots, \mathrm{ord}(\zeta) - 1$, em que $\mathrm{ord}(\zeta)$ corresponde à ordem multiplicativa de ζ, são dadas

respectivamente por

$$\cos_\zeta(\theta) = \frac{\zeta^\theta + \zeta^{-\theta}}{2} \tag{68}$$

e

$$\mathrm{sen}_\zeta(\theta) = \frac{\zeta^\theta - \zeta^{-\theta}}{2i}, \tag{69}$$

em que $i \equiv \sqrt{-1} \pmod{p}$.

As funções sobre corpos finitos definidas acima satisfazem propriedades análogas àquelas satisfeitas pelas respectivas funções definidas sobre os números reais. Em particular, cossenos e senos sobre corpos finitos possuem, correspondentemente, simetria par e ímpar, satisfazem

$$\mathrm{sen}^2_\zeta(\theta) + \cos^2_\zeta(\theta) = 1, \tag{70}$$

bem como as identidades relacionadas à soma e à diferença de ângulos. Também é relevante notar que, se $p \equiv 3 \pmod{4}$, $i \equiv \sqrt{-1} \pmod{p}$ pertence ao corpo de extensão $\mathbb{F}_{p^2}$ (BURTON, 2010), em que as operações aritméticas podem ser realizadas empregando inteiros Gaussianos sobre $\mathbb{F}_p$ (LIMA; CAMPELLO DE SOUZA, 2011).

4.1.2 Definição da CNT

Definição 4.2. Seja $\mathbf{s}$ um sinal com N pontos cujas componentes pertencem a $\mathbb{F}_p$; seja $\zeta \in \mathbb{F}_p$ um elemento com ordem multiplicativa $\mathrm{ord}(\zeta) = 2N$. A transformada numérica do cosseno de $\mathbf{s}$ é calculada por

$$\mathbf{s_C} = \mathbf{C_C}\mathbf{s}, \tag{71}$$

em que $\mathbf{C_C}$ é a matriz cujos elementos são dados por

$$C_\mathrm{C}(k,n) = \sqrt{\frac{2}{N}}\beta_k \cos_\zeta\left(k\left(n + \frac{1}{2}\right)\right), \tag{72}$$

$k, n = 0, 1, \ldots, N-1$, em que $\beta_0 = \sqrt{2^{-1}}$ e $\beta_k = 1$, para $k = 1, 2, \ldots, N-1$.

Mostra-se que a matriz da CNT inversa é dada por $\mathbf{C}_\mathbf{C}^{-1} = \mathbf{C}_\mathbf{C}^T$ (LIMA; CAMPELLO DE SOUZA; PANARIO, 2011; LIMA; MADEIRO; SALES, 2015).

4.2 PROPRIEDADES DE DIAGONALIZAÇÃO DA CNT

Até onde o autor dessa Tese tem conhecimento, até recentemente, resultados a respeito de matrizes diagonalizáveis pela matriz da CNT ainda não tinham sido apresentados na literatura. Em (RIBEIRO; LIMA, 2017), os autores propuseram considerar um grafo em caminho $\mathcal{P}_N$

não-direcionado com N vértices, como o apresentado na Figura 1 para $N = 4$, mas avaliado sobre um corpo finito. Neste caso, a respectiva matriz Laplaciana é

$$\mathbf{L} = \begin{bmatrix} 1 & -1 & & & & \\ -1 & 2 & -1 & & & \\ & -1 & 2 & -1 & & \\ & & \ddots & \ddots & \ddots & \\ & & & -1 & 2 & -1 \\ & & & & -1 & 1 \end{bmatrix} \tag{73}$$

$$\equiv \begin{bmatrix} 1 & p-1 & & & & \\ p-1 & 2 & p-1 & & & \\ & p-1 & 2 & p-1 & & \\ & & \ddots & \ddots & \ddots & \\ & & & p-1 & 2 & p-1 \\ & & & & p-1 & 1 \end{bmatrix} \pmod{p}. \tag{74}$$

Os referidos autores, então, demonstraram que $\mathbf{C_c}$ diagonaliza $\mathbf{L}$, conforme enunciado no teorema a seguir.

Teorema 4.1. *Seja $\zeta \in \mathbb{F}_p$ um elemento com ordem multiplicativa $\mathrm{ord}(\zeta) = 2N$; seja $\mathbf{C_c}$ a matriz com dimensões $N \times N$ da CNT, construída conforme a Definição 4.2. A Laplaciana $\mathbf{L}$ do grafo em caminho não-direcionado sobre $\mathbb{F}_p$ é diagonalizada por $\mathbf{C_c}$.*

Demonstração. Ver Apêndice A. □

Como se esperava, o Teorema 4.1 pode ser visto como uma versão sobre corpos finitos do resultado bem conhecido que estabelece que os autovetores de $\mathbf{L}$ (avaliada sobre os números reais) coincidem com os vetores de base da DCT (STRANG, 1999).

4.3 TRANSFORMADA NUMÉRICA MANOBRÁVEL DO COSSENO

Considerando o resultado dado pelo Teorema 4.1, é possível, então, usar de uma abordagem análoga àquela empregada no contexto da DCT, para definir a SCNT. Em todo caso, conforme se demonstrou, também no cenário de corpos finitos, as multiplicidades dos autovalores da Laplaciana do grafo em caminho são unitárias, o que significa que a base formada pelos respectivos autovetores (os vetores de base da CNT) é única. Diante disso, a possibilidade de definição de uma SCNT requer que se considere, como ponto de partida, uma CNT bidimensional. Os Teoremas 2 e 3 em (FRACASTORO; MAGLI, 2017) também são válidos para matrizes avaliadas sobre um corpo finito, ao mesmo tempo em que a CNT pode ser estendida para duas dimensões de modo análogo àquele empregado para definição da 2D-DCT a partir da DCT

unidimensional. Assim, os autovalores do Laplaciano de um grafo em grade, $\mathcal{P}_N \square \mathcal{P}_N$, avaliado sobre um corpo finito, resultante do produto entre dois grafos em caminho $\mathcal{P}_N$, são dados por

$$\lambda_{k,l}(\mathcal{P}_N \square \mathcal{P}_N) = 4\,\mathrm{sen}_\zeta^2\left(\frac{k}{2}\right) + 4\,\mathrm{sen}_\zeta^2\left(\frac{l}{2}\right). \tag{75}$$

É importante ressaltar que as operações envolvidas são realizadas utilizando aritmética módulo p.

As multiplicidades dos autovalores são dadas por:

- O autovalor $\lambda_{k,l} = 4$ tem multiplicidade $N-1$ e corresponde a todos os autovalores $\lambda_{k,N-k}$ com $1 \leq k \leq N-1$.
- O autovalor $\lambda_{k,l}$ é igual a $\lambda_{l,k}$ quando $k \neq l$. Devido à simetria, $\lambda_{k,l} = \lambda_k + \lambda_l = \lambda_l + \lambda_k = \lambda_{l,k}$, apresentando multiplicidade igual a 2.
- O autovalor $\lambda_{k,l}$ tem multiplicidade igual a 1, quando $k = l$ com $k \neq \frac{N}{2}$ (recai no caso de $\lambda_{k,l} = 4$). Logo, no espectro de $\mathbf{L}(\mathcal{P}_N \square \mathcal{P}_N)$ há $N-1$ autovalores com multiplicidade algébrica igual a 1.

Os autovetores de $\mathbf{L}(\mathcal{P}_N \square \mathcal{P}_N)$, isto é, os vetores de base da 2D-CNT, são obtidos pelo produto de Kronecker entre os vetores de base da CNT unidimensional. Como os autoespaços em questão, com exceção daquele ao qual estão associados os autovalores descritos no último dos casos acima, possuem dimensão maior que a unidade, novas autobases para $\mathbf{L}(\mathcal{P}_N \square \mathcal{P}_N)$ podem ser obtidas por meio da rotação aos pares dos respectivos autovetores. No caso, devem ser consideradas rotações sobre corpos finitos, as quais são implementadas empregando o operador (GONDIM; OLIVEIRA NETO; LIMA, 2019)

$$\mathbf{R}_\alpha(\theta) = \begin{bmatrix} \cos_\alpha \theta & \mathrm{sen}_\alpha \theta \\ -\mathrm{sen}_\alpha \theta & \cos_\alpha \theta \end{bmatrix}, \tag{76}$$

em que $\alpha \in \mathrm{GI}(p)$ e $\theta \in \mathbb{Z}_{\mathrm{ord}(\alpha)}$[1]. Utilizando propriedades das funções trigonométricas sobre corpos finitos, mostra-se que $\mathbf{R}_\alpha(\theta)^{-1} = \mathbf{R}_\alpha(\theta)^T$. Assim, se as componentes dos autovetores $\mathbf{v}^{(k,l)}$ e $\mathbf{v}^{(l,k)}$ forem dispostas de forma unidimensional, como vetores-linha com dimensão $1 \times N^2$, o respectivo novo par de autovetores $\mathbf{v}^{(k,l)'}$ e $\mathbf{v}^{(l,k)'}$ é calculado por

$$\begin{bmatrix} \mathbf{v}^{(k,l)'} \\ \mathbf{v}^{(l,k)'} \end{bmatrix} = \begin{bmatrix} \cos_{\alpha_{k,l}}(\theta_{k,l}) & \mathrm{sen}_{\alpha_{k,l}}(\theta_{k,l}) \\ -\mathrm{sen}_{\alpha_{k,l}}(\theta_{k,l}) & \cos_{\alpha_{k,l}}(\theta_{k,l}) \end{bmatrix} \cdot \begin{bmatrix} \mathbf{v}^{(k,l)} \\ \mathbf{v}^{(l,k)} \end{bmatrix}. \tag{77}$$

Na última expressão, os cossenos e senos dos ângulos $\theta_{k,l}$ são calculados com relação aos elementos $\alpha_{k,l} \in \mathrm{GI}(p)$, $k = 0, \ldots, N-2$, $l = k+1, \ldots, N-1$, isto é, até $N(N-1)/2$ ângulos podem ser especificados. Substituindo os pares originais de autovetores por aqueles resultantes das rotações, obtém-se uma nova base, à qual está associada a transformada numérica

[1] $\mathbb{Z}_{\mathrm{ord}(\alpha)}$ denota o conjunto de inteiros módulo $\mathrm{ord}(\alpha)$.

manobrável do cosseno (os autovetores associados aos autovalores com multiplicidades iguais a 1 não são alterados). Os demais detalhes relativos ao cálculo propriamente dito da SCNT são análogos àqueles relativos ao cálculo da SDCT e, por isso, não serão apresentados aqui; esses incluem (i) a possibilidade de computar a transformada a partir do cálculo inicial da 2D-CNT e de um posterior produto por uma matriz contendo todos os cossenos e senos sobre corpos finitos associados às rotações que se deseja impor a cada par de vetor de base e (ii) a estratégia para cálculo da transformada inversa.

O Exemplo 4.1 apresenta o cálculo da SCNT da estrutura bidimensional sobre $\mathrm{GF}(257)$

$$\mathbf{s} = \begin{bmatrix} 1 & 130 & 80 & 45 \\ 20 & 254 & 92 & 50 \\ 46 & 78 & 99 & 160 \\ 20 & 80 & 121 & 200 \end{bmatrix} \tag{78}$$

de dimensão $N \times N = 4 \times 4$. A SCNT de $\mathbf{s}$ é obtida por $\mathbf{S}_{\boldsymbol{\alpha},\boldsymbol{\theta}} = \mathbf{R}_{\boldsymbol{\alpha},\boldsymbol{\theta}}\bar{\mathbf{S}}_{\mathbf{C}}$, em que $\boldsymbol{\theta}$ é um vetor contendo todos os ângulos empregados nas rotações dos pares de vetores, $\boldsymbol{\alpha} = (\alpha_{k,l})$ é um vetor contendo todos os elementos em relação aos quais os cossenos e senos dos referidos ângulos são calculados e $\mathbf{S}_{\mathbf{C}}$ corresponde a 2D-CNT de $\mathbf{s}$ que é dada por

$$\mathbf{S}_{\mathbf{C}} = \mathbf{C}_{\mathbf{C}}\mathbf{s}\mathbf{C}_{\mathbf{C}}^{T} = \begin{bmatrix} S_{00} & S_{01} & S_{02} & S_{03} \\ S_{10} & S_{11} & S_{12} & S_{13} \\ S_{20} & S_{21} & S_{22} & S_{23} \\ S_{30} & S_{31} & S_{32} & S_{33} \end{bmatrix}, \tag{79}$$

$\bar{\mathbf{S}}_{\mathbf{C}}$ é um vetor $N^2 \times 1$ formado pelos elementos de $\mathbf{S}_{\mathbf{C}}$ obtidos na ordem lexicográfica, ou seja

$$\bar{\mathbf{S}}_{\mathbf{C}} = \begin{bmatrix} S_{00} \\ S_{01} \\ S_{02} \\ S_{03} \\ S_{10} \\ S_{11} \\ S_{12} \\ S_{13} \\ S_{20} \\ S_{21} \\ S_{22} \\ S_{23} \\ S_{30} \\ S_{31} \\ S_{32} \\ S_{33} \end{bmatrix} \tag{80}$$

e $\mathbf{R}_{\boldsymbol{\alpha},\theta}$ é a matriz de rotação construída a partir dos senos e cossenos dos ângulos de rotação que compõem o vetor θ e que são calculados em relação ao elemento α.

Exemplo 4.1. *Seja* $\zeta = 4 \in \mathrm{GF}(257)$ *um elemento com ordem multiplicativa igual a* $\mathrm{ord}(\zeta) = 2N = 8$, $\boldsymbol{\alpha} = (\alpha_{k,l}) = \zeta$ *e* $\theta = [3 \quad 4 \quad 5 \quad 2 \quad 7 \quad 1]$. *A partir da matriz da CNT unidimensional com núcleo* $\zeta = 4$,

$$\mathbf{C_C} = \begin{bmatrix} 128 & 128 & 128 & 128 \\ 166 & 154 & 103 & 91 \\ 128 & 129 & 129 & 128 \\ 154 & 91 & 166 & 103 \end{bmatrix}, \tag{81}$$

tem-se a 2D-CNT de $\mathbf{s}$, *dada por*

$$\mathbf{S_C} = \mathbf{C_C s C_C^T} = \begin{bmatrix} 112 & 233 & 159 & 180 \\ 103 & 212 & 124 & 57 \\ 98 & 99 & 154 & 87 \\ 24 & 189 & 84 & 76 \end{bmatrix}. \tag{82}$$

A partir do produto da versão vetorizada de $\mathbf{S_C}$, *que de acordo com (80) é escrita como*

$$\bar{\mathbf{S}}_{\mathbf{C}} = \begin{bmatrix} 112 \\ 233 \\ 159 \\ 180 \\ 103 \\ 212 \\ 124 \\ 57 \\ 98 \\ 99 \\ 154 \\ 87 \\ 24 \\ 189 \\ 84 \\ 76 \end{bmatrix}, \tag{83}$$

com a matriz $\mathbf{R}_{\boldsymbol{\alpha},\theta}$ *contendo os cossenos e senos sobre corpos finitos dos elementos de* θ *para*

rotacionar os pares de autovetores, conforme descrito em (77), obtém-se a SCNT de $\mathbf{s}$

$$\mathbf{S}_{\boldsymbol{\alpha},\theta} = \mathbf{R}_{\boldsymbol{\alpha},\theta}\bar{\mathbf{S}}_{\mathbf{C}} = \begin{bmatrix} 112 \\ 45 \\ 98 \\ 209 \\ 57 \\ 212 \\ 99 \\ 105 \\ 159 \\ 133 \\ 154 \\ 10 \\ 203 \\ 73 \\ 90 \\ 76 \end{bmatrix}, \tag{84}$$

que apresenta-se na estrutura bidimensional como

$$\mathbf{S}_{\boldsymbol{\alpha},\theta} = \begin{bmatrix} 112 & 45 & 98 & 209 \\ 57 & 212 & 99 & 105 \\ 159 & 133 & 154 & 10 \\ 203 & 73 & 90 & 76 \end{bmatrix}. \tag{85}$$

4.4 TRANSFORMADA NUMÉRICA TRIDIMENSIONAL MANOBRÁVEL DO COSSENO

A SCNT tridimensional pode ser definida de forma análoga à SCNT e requer a consideração de uma CNT tridimensional como ponto de partida. Uma vez que a CNT pode ser estendida para três dimensões de forma semelhante àquela usada para definir a 3D-DCT a partir da DCT unidimensional, usando o Teorema 1 apresentado em (FRACASTORO; FOSSON; MAGLI, 2017), que também é válido para matrizes avaliadas em corpo finito, e usando o Teorema 4.1, temos que os autovalores de $\mathbf{L}(\mathcal{L}_N)$, o Laplaciano do grafo em grade cúbica ($\mathcal{L}_N = \mathcal{P}_N \square \mathcal{P}_N \square \mathcal{P}_N$ é o resultado do produto cartesiano entre três grafos em caminho avaliado sobre um corpo finito), são todas as possíveis somas entre os autovalores de cada grafo em caminho, ou seja,

$$\lambda_{k,l,m}(\mathcal{P}_N \square \mathcal{P}_N \square \mathcal{P}_N) = 4\,\mathrm{sen}^2_{\zeta}\left(\frac{k}{2}\right) + 4\,\mathrm{sen}^2_{\zeta}\left(\frac{l}{2}\right) + 4\,\mathrm{sen}^2_{\zeta}\left(\frac{m}{2}\right). \tag{86}$$

É importante ressaltar que as operações envolvidas são realizadas utilizando aritmética módulo p.

Analisando a multiplicidade algébrica em (86), tem-se que:

- O autovalor $\lambda_{k,l,m}$ tem multiplicidade igual a 1, quando $k = l = m$, com $0 \leq k, l, m \leq N-1$. Logo, no espectro de $\mathbf{L}(\mathcal{L}_N)$ há N autovalores com multiplicidade algébrica igual a 1;

- O autovalor $\lambda_{k,l,m}$ apresenta multiplicidade igual a 3, quando:

  1. $k = l$ e $l \neq m$, ou seja, $\lambda_{k,k,m} = \lambda_{k,m,k} = \lambda_{m,k,k}$, um total de $N(N-1)$ autovalores;
  2. $k = m$ e $m \neq l$, ou seja, $\lambda_{k,l,k} = \lambda_{k,k,l} = \lambda_{l,k,k}$, um total de $N(N-1)$ autovalores;
  3. $m = l$ e $l \neq k$, ou seja, $\lambda_{m,m,k} = \lambda_{m,k,m} = \lambda_{k,m,m}$, um total de $N(N-1)$ autovalores;

  Logo, no espectro de $\mathcal{L}_N = \mathcal{P}_N \square \mathcal{P}_N \square \mathcal{P}_N$ há $3N(N-1)$ autovalores com multiplicidade algébrica igual a 3;

- O autovalor $\lambda_{k,l,m}$ apresenta multiplicidade igual a 6, quando $k \neq l \neq m$. Devido à simetria: $\lambda_{k,l,m} = \lambda_{k,m,l} = \lambda_{l,k,m} = \lambda_{l,m,k} = \lambda_{m,k,l} = \lambda_{m,l,k}$. Logo, no espectro de $\mathbf{L}(\mathcal{L}_N)$ há $N(N-1)(N-2)$ autovalores com multiplicidade algébrica igual a 6.

Os autovetores de $\mathbf{L}(\mathcal{L}_N)$ são determinados pelo produto de Kronecker entre os vetores de base da CNT unidimensional (autovetores de $\mathcal{P}_N$). Como o produto de Kronecker não é comutativo, a dimensão de cada autoespaço, ou seja, a multiplicidade geométrica de cada autovalor é igual à respectiva multiplicidade algébrica. Isso significa que há autoespaços cuja dimensão é maior que um e, portanto, a base da 3D-CNT não é a única autobase para $\mathbf{L}(\mathcal{L}_N)$. Logo, uma nova autobase para $\mathbf{L}(\mathcal{L}_N)$ pode ser obtida rotacionando as triplas dos respectivos autovetores.

Utilizando o operador de rotação sobre corpos finitos definido em (76) para rotacionar a tripla de componentes dos autovetores $\mathbf{v}^{(k,k,m)}$, $\mathbf{v}^{(k,m,k)}$ e $\mathbf{v}^{(m,k,k)}$, organizadas como vetores-linha de dimensão $1 \times N^3$, tem-se como nova tripla de autovetores, respectivamente, os vetores $\mathbf{v}^{(k,k,m)'}$, $\mathbf{v}^{(k,m,k)'}$ e $\mathbf{v}^{(m,k,k)'}$, calculados por

$$\begin{bmatrix} \mathbf{v}^{(k,k,m)'} \\ \mathbf{v}^{(k,m,k)'} \\ \mathbf{v}^{(m,k,k)'} \end{bmatrix} = \begin{bmatrix} \cos_{\alpha_{k,l,m}}(\theta_{k,l,m}) & 0 & \operatorname{sen}_{\alpha_{k,l,m}}(\theta_{k,l,m}) \\ 0 & 1 & 0 \\ -\operatorname{sen}_{\alpha_{k,l,m}}(\theta_{k,l,m}) & 0 & \cos_{\alpha_{k,l,m}}(\theta_{k,l,m}) \end{bmatrix} \begin{bmatrix} \mathbf{v}^{(k,k,m)} \\ \mathbf{v}^{(k,m,k)} \\ \mathbf{v}^{(m,k,k)} \end{bmatrix}. \tag{87}$$

Os autovetores de $\mathbf{L}(\mathcal{L}_N)$ associados aos autovalores cuja multiplicidade é igual a 6 podem ser rotacionados utilizando a estrutura descrita em (87), agrupando-os em duas triplas, $(\mathbf{v}_{k,l,m}, \mathbf{v}_{l,m,k}, \mathbf{v}_{m,k,l})$ e $(\mathbf{v}_{k,m,l}, \mathbf{v}_{m,l,k}, \mathbf{v}_{l,k,m})$. Os autovetores associados aos autovalores com multiplicidade igual a 1 não são rotacionados. Assim, o número de triplas de autovetores a serem rotacionados por θ é igual a $\frac{N^3-N}{3}$, que corresponde aos autovetores associados aos autovalores com multiplicidades iguais a 3 (precisamente, $3(N-1)$ autovalores) e 6 (precisamente, $N(N-1)(N-2)$ autovalores). Logo, substituindo as triplas originais de autovetores por aqueles resultantes das rotações, uma nova base é obtida, a qual é utilizada pada definir a 3D-SCNT.

5 APLICAÇÕES

Neste capítulo, é apresentado um método de compressão de imagens tridimensionais baseado na 3D-SDCT, considerando o caso em que apenas um par de ângulos de rotação por bloco é utilizado, rotacionando todos os vetores de base da 3D-DCT pelo mesmo par de ângulos. Este capítulo também introduz um esquema de cifragem de imagens médicas tridimensionais baseado na 3D-SCNT, que usa os ângulos de rotação como parâmetros secretos do esquema. As seções a seguir descrevem as aplicações supracitadas.

5.1 COMPRESSÃO DE IMAGENS TRIDIMENSIONAIS

Esta seção apresenta a aplicação da transformada 3D-SDCT em compressão de imagens. Os resultados são comparados com a 3D-DCT usual, utilizando a mesma estratégia de quantização e codificação.

Como discutido na Subseção 3.1.5 do Capítulo 3, a 3D-SDCT permite anular $\frac{(N^3+2N)}{3}$ coeficientes dentre os N^3 coeficientes que compõem a 3D-DCT. Se isso for usado em um CODEC (codificador e decodificador) de imagem baseado em transformada, a quantidade de coeficientes a serem enviados ao decodificador será reduzida. No entanto, faz-se necessário enviar também ao decodificador os $\frac{N^3-N}{3}$ ângulos ótimos empregados nas rotações.

Tendo em vista a alta taxa necessária para transmitir todos os pares de ângulos de rotação, o emprego de versões subótimas que levem a um menor número de coeficientes nulos ou próximos de zero pode levar a uma solução eficiente. Essa estratégia pode ser analisada a partir de uma perspectiva de taxa-distorção (RD, do inglês *rate-distortion*), cujo objetivo é escolher a versão comprimida mais eficiente para cada bloco da imagem, no sentido de quantidade de *bits* para representação *versus* qualidade da imagem reconstruída (SULLIVAN; WIEGAND, 1998; ORTEGA; RAMCHANDRAN, 1998).

5.1.1 Modelo RD

No cálculo da 3D-SDCT, a distribuição de energia e o grau de esparsidade no domínio da transformada dependem diretamente da escolha dos ângulos de rotação correspondentes. Esses ângulos também devem ser informados ao decodificador para que a transformada inversa seja calculada. A taxa de *bits* total da 3D-SDCT é, portanto, dada por

$$R(\mathbf{F}_{\mathrm{S}}(\boldsymbol{\Theta}), \boldsymbol{\Theta}) = R_{\mathbf{F}_{\mathrm{S}}(\boldsymbol{\Theta})} + R_{\boldsymbol{\Theta}}, \tag{88}$$

em que $R_{\mathbf{F}_{\mathrm{S}}(\boldsymbol{\Theta})}$ corresponde à taxa de *bits* referente aos coeficientes transformados e $R_{\boldsymbol{\Theta}}$ à taxa de *bits* referente aos ângulos de rotação.

Tanto os coeficientes transformados quanto os ângulos de rotação devem ser quantizados em conjuntos finitos de valores, de modo que $Quant_{\mathbf{F}_{\mathrm{S}}(\boldsymbol{\Theta})} \in \mathbb{R}^{N^3}$ e $Quant_{\boldsymbol{\Theta}} \in [0, 2\pi]$ correspondem, respectivamente, aos conjuntos de valores de reconstrução disponíveis para cada

componente, ou seja, $\mathbf{F}_{\mathrm{S}}(\mathbf{\Theta}) \in Quant^{N^3}_{\mathbf{F}_{\mathrm{S}}(\mathbf{\Theta})}$ e $\mathbf{\Theta} \in Quant^{ang}_{\mathbf{\Theta}}$, em que ang corresponde ao número de ângulos usados.

Assim como o número de diferentes ângulos de rotação influencia a taxa de *bits* necessária para codificar a imagem, a quantidade e a escolha desses ângulos também afetam a distorção da imagem original. Logo, a distoção total $D = D(\mathbf{F}_{\mathrm{S}}(\mathbf{\Theta}), \mathbf{\Theta})$ é função dos coeficientes transformados, $\mathbf{F}_{\mathrm{S}}(\mathbf{\Theta}) = (F_{000}, \ldots, F_{N-1N-1N-1})$, e dos ângulos de rotação utilizados, $\mathbf{\Theta} = (\theta_0, \ldots, \theta_{ang-1})$.

A escolha de um conjunto adequado de ângulos para a 3D-SDCT pode ser analisada a partir de uma perspectiva de RD. Idealmente, o codificador deve representar a imagem usando o mínimo possível de *bits*, preservando o nível de qualidade necessário para a aplicação, ou seja, minimizar a distorção D sujeitando-se a uma restrição R à taxa de *bits* R_0:

$$\min\{D\}, \text{ sujeito a } R < R_0. \tag{89}$$

O problema de otimização apresentado em (89) pode ser resolvido usando a otimização Lagrangeana, na qual um termo de distorção D é ponderado contra um termo de taxa R, isto é,

$$\min\{J\}, \text{em que } J = D + \gamma R, \tag{90}$$

em que J é a função Lagrangeana distorção-taxa que será minimizada para um valor particular do multiplicador de Lagrange, γ.

Em (FRACASTORO; FOSSON; MAGLI, 2017), os autores propõem como medida de distorção o uso do erro de reconstrução, dado por

$$D(\mathbf{F}_{\mathrm{S}}(\mathbf{\Theta}), \mathbf{\Theta}) = ||\mathbf{f} - \mathbf{C}_{\mathrm{S}}(\mathbf{\Theta})^T \mathbf{F}_{\mathrm{S}}(\mathbf{\Theta})||_2^2, \tag{91}$$

em que $\mathbf{f} \in \mathbb{R}^{N^3}$ corresponde ao bloco da imagem original e $\mathbf{C}_{\mathrm{S}}(\mathbf{\Theta})^T \mathbf{F}_{\mathrm{S}}(\mathbf{\Theta})$ é o bloco reconstruído a partir do cálculo da 3D-SDCT inversa.

Existe uma relação aproximadamente linear entre a taxa de *bits* de codificação R e a norma-l_0 de $\mathbf{F}_{\mathrm{S}}(\mathbf{\Theta})$ (quantidade de coeficientes não nulos) para as transformadas DCT, em que

$$R_{\mathbf{F}_{\mathrm{S}}(\mathbf{\Theta})} = \kappa ||\mathbf{F}_{\mathrm{S}}(\mathbf{\Theta})||_0, \tag{92}$$

e κ é a constante de proporcionalidade que pode ser encontrada empiricamente (MITRA; HE, 2001 apud FRACASTORO; FOSSON; MAGLI, 2017).

A taxa $R_{\mathbf{\Theta}}$ depende da quantidade de ângulos de rotação diferentes utilizados. Utilizando um único ângulo, isento de compressão e quantizado sobre os valores $q_\theta \in [0, 2\pi]$, para rotacionar todas a triplas de autovetores, a taxa referente à transmissão desse único ângulo é dado por

$$R_\theta = \lceil \log_2 q_\theta \rceil, \tag{93}$$

em que $q_\theta = |Quant_\theta|$ corresponde à cardinalidade do conjunto $Quant_\theta$.

Cada solução obtida em (90) para um dado valor de γ corresponde a uma solução ótima para a equação (89) para um valor específico de R (SHOHAM; GERSHO, 1988 apud

SULLIVAN; WIEGAND, 1998). O fator γ deve levar em conta o passo de quantização uniforme utilizado pelo codificador, uma vez que o passo do quantizador influencia a taxa final R obtida no processo de compressão. Tendo em vista essa influência, Le Pennec e Mallat definiram em (LE-PENNEC; MALLAT, 2005) que um fator γ ótimo está relacionado ao passo de quantização q da seguinte forma:

$$\gamma = \frac{3q^2}{4\kappa}, \tag{94}$$

em que κ corresponde a constante de proporcionalidade da equação (92).

5.1.2 Codificador e estratégia de quantização

Para a utilização da 3D-SDCT faz-se necessário transmitir ao decodificador os coeficientes transformados e os ângulos de rotação. Os coeficientes são submetidos à quantização e ao método de varredura proposto em (LEE; CHAN; ADJEROH, 1997). Os ângulos, por sua vez, são quantizados uniformemente no intervalo de $[0, \pi]$.

Para a codificação dos coeficientes e ângulos foi utilizado o QM-coder, que é um codificador aritmético adaptado para trabalhar com entradas binárias, utilizado no JPEG. O QM-coder é um codificador livre de multiplicações e opera com aproximações dos intervalos fazendo uso somente de operações de adição, subtração e deslocamento com precisão fixa, o que faz dele um codificador simples e veloz (SALOMON; MOTTA, 2009).

5.1.2.1 Quantização

Em (LEE; CHAN; ADJEROH, 1997), os autores propuseram uma técnica para definição dos níveis de quantização para coeficientes 3D-DCT. Segundo os autores, a magnitude dos coeficientes decresce exponencialmente à medida que se afastam dos eixos principais x, y e z, de modo que os coeficientes mais significativos estão concentrados em uma região curva nomeada pelos autores de complemento de um hiperboloide deslocado, apresentado na Figura 20a. A região é definida pela equação

$$(x+1)(y+1)(z+1) \leq Cte, \tag{95}$$

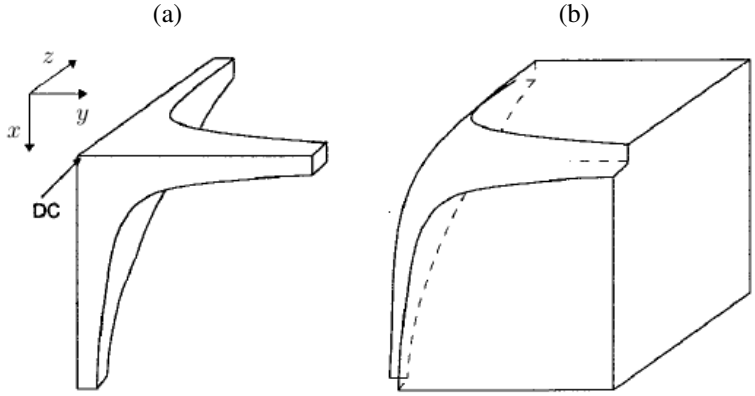
em que Cte é uma constante positiva que define o tamanho da região (define a forma da região), modificando assim o número de coeficientes a serem considerados mais significativos.

O hiperboloide deslocado (Figura 20b) captura os coeficientes menos significativos e é definido pela equação

$$(x+1)(y+1)(z+1) > Cte. \tag{96}$$

Com a modelagem da distribuição dos coeficientes em duas regiões do cubo, hiperboloide deslocado e complemento do hiperboloide deslocado, uma função para geração dos valores

Figura 20 – Distribuição dos coeficientes 3D-DCT: (a) Complemento do hiperboloide deslocado (concentra os coeficientes dominantes) e (b) hiperboloide deslocado (concentra os coeficientes menos significativos).



Fonte: Adaptado de Lee, Chan e Adjeroh (1997).

de quantização para o interior e o exterior do complemento do hiperboloide deslocado foi definida por Lee, Raymond e Donald. Enquanto na região externa ao complemento do hiperboloide deslocado deve-se ter altos valores de quantização que tendem a quantificar os coeficientes para zero, na região interna os valores de quantização devem aumentar à medida que se avança na ordem de varredura. Para isso, definiu-se a função exponencial

$$Q_{x,y,z} = \begin{cases} K_i \left(1 - \frac{e^{-\eta_i(x+1)(y+1)(z+1)}}{e^{-\eta_i}}\right) + 1, & (x+1)(y+1)(z+1) \leq Cte \\ \\ K_o \left(1 - e^{-\eta_o(x+1)(y+1)(z+1)}\right), & (x+1)(y+1)(z+1) > Cte, \end{cases} \tag{97}$$

em que i e o são índices das constantes (K_i, η_i) e (K_o, η_o) e se referem, respectivamente, à região interna e à externa do complemento do hiperboloide deslocado, a constante K é a amplitude inicial da região selecionada e o parâmetro η é a taxa de decaimento.

Em (LEE; CHAN; ADJEROH, 1997), os autores também definiram uma ordem de varredura para os coeficientes 3D-DCT quantizados, que faz uso dos valores de quantização gerados por (97). No esquema de varredura proposto, ordenam-se inicialmente os coeficientes inseridos no complemento do hiperboloide deslocado e, em seguida, os que se encontram fora dessa região (coeficientes do hiperboloide deslocado). A ideia é que mais zeros consecutivos dos coeficientes quantizados possam ser agrupados para uma codificação mais eficiente. O esquema de varredura é definido nos seguintes passos:

- **Passo 1 - Definir parâmetros para gerar valores de quantização:** Defina os valores dos parâmetros (K_i, η_i), (K_o, η_o) e Cte em (97) e gere os valores de quantização $Q_{x,y,z}$ com $0 \leq x, y, z \leq N-1$.

- **Passo 2 - Ordenar coeficientes do complemento do hiperboloide deslocado:** Gere o vetor $\mathbf{N_{interno}}$ com os números dos coeficientes, definidos por $xN^2 + yN + z$, com $(x+1)(y+1)(z+1) \leq Cte$, que corresponde à posição de cada coeficiente do complemento

do hiperboloide deslocado. Ordene $\mathbf{N_{interno}}$ de acordo com a ordem decrescente dos correspodentes valores de quantização $Q_{x,y,z}$ cujas coordenadas satisfazem $(x+1)(y+1)(z+1) \leq Cte$.

- **Passo 3 - Ordenar coeficientes do hiperboloide deslocado:** Gere o vetor $\mathbf{N_{externo}}$ com os números dos coeficientes, definidos por xN^2+yN+z, com $(x+1)(y+1)(z+1) > Cte$, que corresponde à posição de cada coeficiente do hiperbolóide deslocado. Ordene $\mathbf{N_{externo}}$ de acordo com a ordem decrescente dos correspodentes valores de quantização $Q_{x,y,z}$ cujas coordenadas satisfazem $(x+1)(y+1)(z+1) > Cte$.

O vetor ordenado $\mathbf{N_{interno}}$ (resultante do **Passo 2**) seguido pelo vetor ordenado $\mathbf{N_{externo}}$ (resultante do **Passo 3**) forma a ordem de varredura. Seguindo a ordem de varredura supracitada, obtém-se a matriz de quantização ordenada $\mathbf{Q}'$.

Os coeficientes 3D-DCT e 3D-SDCT são divididos pelos elementos correspondentes da matriz de quantização ordenada $\mathbf{Q}'$. A quantização dos coeficientes resultantes da aplicação da 3D-DCT ao bloco $N \times N \times N$ é dada por

$$Q(\bar{F}_{x,y,z}) = \text{round}\left[Q_1(\bar{F}_{x,y,z})\right], \tag{98}$$

com

$$Q_1(\bar{F}_{x,y,z}) = \frac{\bar{F}_{x,y,z}}{Q'_{x,y,z}q}, \tag{99}$$

em que q é o passo de quantização uniforme e $\bar{\mathbf{F}}$ é a 3D-DCT de $\bar{\mathbf{f}}$ e tem a entrada na posição (x, y, z) denotada por $\bar{F}_{x,y,z}$.

Uma vez que a 3D-SDCT tem por característica o desbalanceamento de energia dos coeficientes transformados (mas mantendo a energia total inalterada), o processo de quantização definido em (98) pode ser inadequado porque não leva em conta tal distribuição de energia. Para resolver este problema, optou-se neste trabalho por aplicar a divisão dos coeficientes 3D-DCT pelos elementos correspondentes da matriz de quantização ordenada antes de multiplicar pela matriz de rotação $\mathbf{R}(\mathbf{\Theta})$ para produzir a 3D-SDCT, como segue:

$$Q(\bar{\mathbf{F}}') = \text{round}\left[\mathbf{R}(\mathbf{\Theta})\mathbf{Q}_{\bar{\mathbf{F}}}\right], \tag{100}$$

com

$$\mathbf{Q}_{\bar{\mathbf{F}}} = Q_1(\bar{F}_{x,y,z}), \text{ para } 0 \leq x, y, z \leq N-1, \tag{101}$$

em que $\bar{\mathbf{F}}'$ é a 3D-SDCT de $\bar{\mathbf{f}}$ e tem a entrada na posição (x, y, z) denotada por $\bar{F}'_{x,y,z}$.

Os parâmetros utilizados na definição da matriz de quantização foram $K_i = K_o = 255$, $\eta_i = 0,0001$, $\eta_o = 0,0002$ e $Cte = 8$. Esses valores foram definidos experimentalmente a partir de uma análise prévia do desempenho (PSNR e SSIM *versus* taxa de *bits*) do método de compressão proposto, sendo escolhidos os que geraram melhor desempenho. Quanto ao passo de quantização uniforme q, foram utilizados vinte e cinco passos. Quanto maior o passo, menor a taxa de *bits* da imagem codificada.

5.1.3 Faixa para escolha dos ângulos de rotação

Os ângulos de rotação para o cálculo da 3D-SDCT são definidos no intervalo $[0, 2\pi]$. No entanto, buscando uma representação mais esparsa dos coeficientes (sabe-se que isso é conseguido por meio dos ângulos ótimos, conforme definido na seção 3.1.5 do Capítulo 3), é suficiente escolher os ângulos no intervalo $[0, \pi]$, excluindo o $\frac{\pi}{2}$.

Escolhendo duas rotações, a primeira em torno do eixo z e a segunda em torno do eixo y, verificou-se que as triplas de vetores 3D-SDCT apresentam a seguinte propriedade de simetria:

$$\begin{aligned} \mathbf{v}'_{k,k,m}{}^{(\theta_y+\frac{\pi}{2},\theta_z)} &= \mathbf{v}'_{m,k,k}{}^{(\theta_y,\theta_z)}, \\ \mathbf{v}'_{k,m,k}{}^{(\theta_y+\frac{\pi}{2},\theta_z)} &= \mathbf{v}'_{k,m,k}{}^{(\theta_y,\theta_z)}, \\ \mathbf{v}'_{m,k,k}{}^{(\theta_y+\frac{\pi}{2},\theta_z)} &= -\mathbf{v}'_{k,k,m}{}^{(\theta_y,\theta_z)}, \end{aligned} \tag{102}$$

indicando que a redução da faixa para escolha do ângulo θ_y não altera a esparsidade da matriz de coeficientes resultante de uma rotação $(\theta_y + \frac{\pi}{2}, \theta_z)$. O que ocorre é apenas uma possível troca de sinal (positivo para negativo) de coeficientes ou transferência de energia entre os coeficientes que compõem a tripla rotacionada, mas que pode levar a um ganho em termos de resolução de escolha do ângulo θ_y no intervalo $[0, \frac{\pi}{2})$.

5.1.4 Resultados

Para as simulações foram utilizadas dez imagens médicas no padrão DICOM em escala de cinza (65536 níveis de cinza) com dimensões distintas do repositório *The Cancer Imaging Archive* (TCIA) (CLARK et al., 2013), listadas na Tabela 3. As transformadas 3D-SDCT e 3D-DCT foram calculadas sobre blocos de tamanho $4 \times 4 \times 4$ sem sobreposição, e as mesmas estratégias de quantização e codificação entrópica foram utilizadas.

A 3D-SDCT foi calculada utilizando duas rotações consecutivas, a primeira em torno do eixo z e a segunda em torno do eixo y, com (θ_y, θ_z) como ângulos de rotação . Foram utilizados $q_\theta = 8$ ângulos uniformente espaçados no intervalo $[0, \frac{\pi}{2})$ para θ_y e $[0, \pi]$ para θ_z, ou seja, 64 pares (θ_y, θ_z).

Os resultados são apresentados em curvas RD, usando as métricas de distorção objetiva relação sinal-ruído de pico (PSNR, do inglês *peak signal-to-noise ratio*) e índice de similaridade estrutural (SSIM, do inglês *structural similarity index*). O PSNR é expresso como

$$\mathrm{PSNR} = 10 \log_{10} \left(\frac{\mathrm{MAX}^2}{\mathrm{MSE}} \right), \tag{103}$$

em que $\mathrm{MAX} = 65535$ (todas as imagens usadas são em escala de cinza de 16 *bits*) e MSE indica o erro médio quadrático entre a imagem original e a imagem reconstruída. O SSIM é calculado de acordo com (WANG et al., 2004)

$$\mathrm{SSIM}(\mathrm{I}, \mathrm{I}_{\mathrm{rec}}) = \frac{(2\mu_I \mu_{I_{rec}} + c_1)(2\sigma_{II_{rec}} + c_2)}{(\mu_I^2 + \mu_{I_{rec}}^2 + c_1)(\sigma_I^2 + \sigma_{I_{rec}}^2 + c_2)}, \tag{104}$$

Tabela 3 – Imagens utilizadas nas simulações.

Imagem	**Tipo**	**Dimensão**	**Referência**
I_1	*prostate cancer*	$176 \times 176 \times 100$	(LITJENS et al., 2017; LITJENS et al., 2014)
I_2	*astrocytoma*	$132 \times 132 \times 12$	(JANSEN; TERRY, 2015)
I_3	*breast cancer*	$144 \times 144 \times 108$	(LI et al., 2016; LI et al., 2015)
I_4	*lower abdomen*	$128 \times 128 \times 80$	(LUCCHESI; AREDES, 2016)
I_5	*astrocytoma*	$132 \times 132 \times 12$	(JANSEN; TERRY, 2015)
I_6	*breast cancer*	$144 \times 144 \times 108$	(LI et al., 2016; LI et al., 2015)
I_7	*brain cancer*	$256 \times 256 \times 16$	(BARBORIAK, 2015)
I_8	*breast cancer*	$320 \times 320 \times 16$	(JANSEN et al., 2015)
I_9	*prostate cancer*	$256 \times 256 \times 12$	(LITJENS et al., 2017; LITJENS et al., 2014)
I_{10}	*soft tissue sarcoma*	$256 \times 256 \times 24$	(VALLIÈRES et al., 2015)

Fonte: A autora (2020).

em que I e I_{rec} são as imagens originais e reconstruídas, respectivamente, μ e σ são a média e covariância da intensidade de *pixel* das imagens, respectivamente, e c_1 e c_2 são constantes positivas usadas para evitar instabilidade no parâmetro de qualidade SSIM (KANDHWAY; BHANDARI, 2019).

Os resultados de desempenho das transformadas são comparados usando as métricas Bjøntegaard BD-Rate, BD-PSNR e BD-SSIM. As métricas Bjøntegaard são normalmente usadas para facilitar a comparação de dois algoritmos de compressão, observando as melhorias de distorção para uma determinada taxa de *bits* ou medindo a economia de taxa de *bits* para uma distorção fixa (BJONTEGAARD, 2001). A taxa delta de Bjøntegaard (BD-Rate) representa a economia média de taxa de *bits* para a mesma qualidade de imagem (por exemplo, PSNR, SSIM), de modo que um valor negativo representa o ganho de compressão, enquanto um valor positivo representa a perda de compressão. BD-PSNR e BD-SSIM medem, respectivamente, a diferença média de PSNR e SSIM entre duas curvas RD. Um valor positivo de BD-PSNR ou BD-SSIM indica um aumento de PSNR/SSIM na mesma taxa de *bits*, do método proposto em relação ao método de referência.

A Tabela 4 apresenta os resultados da métrica BD-Rate para as imagens utilizadas nas simulações, com a economia percentual média na taxa de *bits* em comparação com a 3D-DCT. A economia média na taxa de *bits* da 3D-SDCT é maior que 1% para a imagem I_4 e igual a $0{,}68\%$ para a imagem I_8. Para as outras imagens, a 3D-SDCT supera a 3D-DCT em valores maiores que 2% em termos de economia de taxa de *bits*.

A métrica de Bjøntegaard BD-Rate utilizada permite que seja feita uma comparação numérica de redução de taxa de *bits* entre as transformadas. Para uma análise mais detalhada, as Figuras 21 e 22 apresentam as curvas RD em termos de valores de PSNR para toda a faixa

Tabela 4 – Métrica Bjøntegaard (BD-Rate): resultados de BD-Rate da 3D-SDCT em comparação com a 3D-DCT (economia de taxa de *bits*).

Imagem	**BD-Rate**
I_1	$-2,67$
I_2	$-2,18$
I_3	$-2,25$
I_4	$-1,06$
I_5	$-2,26$
I_6	$-2,13$
I_7	$-2,96$
I_8	$-0,68$
I_9	$-2,11$
I_{10}	$-2,25$

Fonte: A autora (2020).

experimental de taxa de codificação para as imagens I_7 (maior ganho BD-Rate) e I_8 (menor ganho BD-Rate), respectivamente. O desempenho em termos de PSNR obtido para a 3D-SDCT em relação a 3D-DCT para a imagem I_8 é praticamente o mesmo, enquanto que para a imagem I_7 a 3D-SDCT apresenta um ganho em PSNR, que aumenta com o aumento da taxa de *bits*.

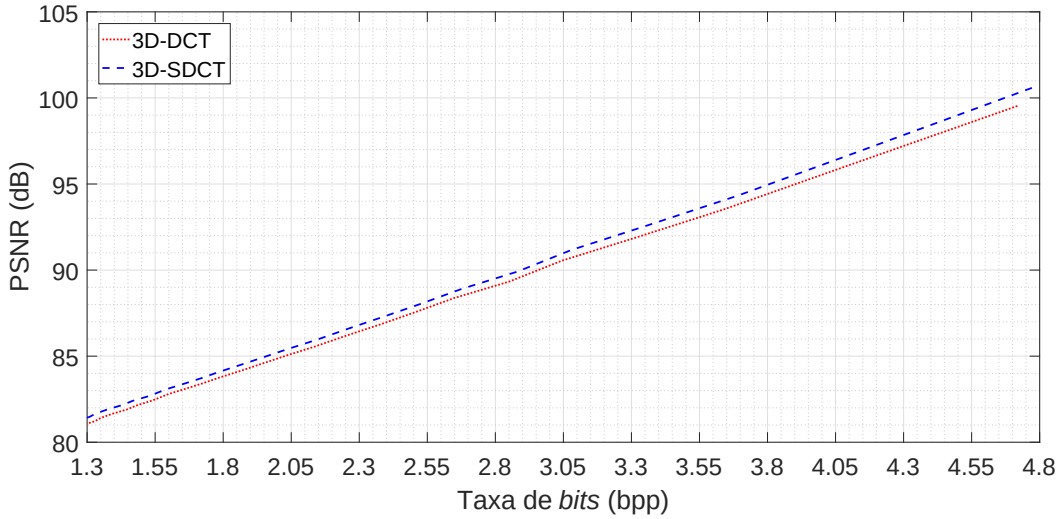
As Figuras 23 e 24 apresentam as curvas RD em termos da métrica de distorção SSIM. Para a imagem I_7, a 3D-SDCT apresenta uma leve superioridade em termos de SSIM. Para a imagem I_8, a 3D-SDCT não apresenta ganho em termos de SSIM sobre a 3D-DCT.

A Tabela 5 apresenta os resultados das métricas BD-PSNR e BD-SSIM para cada uma das imagens utilizadas. Os resultados mostram que a 3D-SDCT oferece melhores resultados de PSNR e uma leve superioridade em termos de SSIM em comparação ao uso da 3D-DCT.

Para avaliar os resultados obtidos com o uso da 3D-SDCT, foram levantados os histogramas dos ângulos utilizados na 3D-SDCT. As Figuras 25 e 26 apresentam os histogramas do uso dos ângulos para a 3D-SDCT nas imagens I_7 (maior ganho BD-Rate) e I_8 (menor ganho BD-Rate), respectivamente.

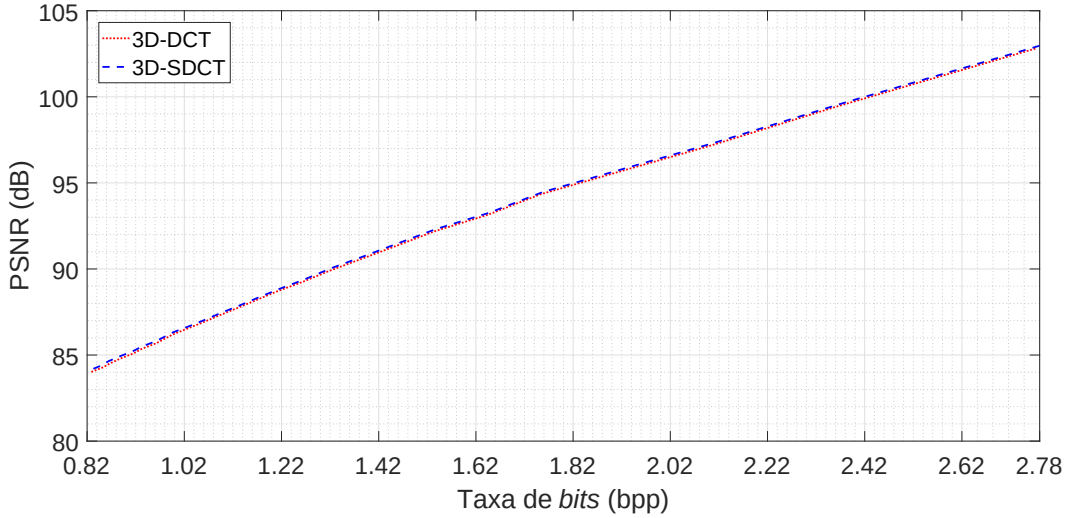
Cada uma das imagens utilizadas foi codificada usando 25 diferentes valores de passos de quantização q, que está diretamente relacionado à taxa de *bits* final, resultando em um total de aproximadamente 409600 e 640000 blocos de imagem $4 \times 4 \times 4$ processados pela 3D-SDCT para as imagens I_7 e I_8, respectivamente. A 3D-SDCT utilizou o par de ângulos $(\theta_y, \theta_z) = (0, 0)$ em $6{,}80\%$ dos 409600 blocos processados para a imagem I_7 e em $68{,}46\%$ dos 640000 blocos para a imagem I_8, isso significa que a 3D-DCT foi efetivamente utilizada nesses blocos. No caso da imagem I_7, o par de ângulos mais utilizado foi $(\theta_y, \theta_z) = (\frac{\pi}{16}, 0)$, que foi usado por $6{,}92\%$ do blocos processados. A Tabela 6 mostra os resultados do uso dos pares de ângulos para a 3D-SDCT (o par de ângulos mais utilizado, sua frequência e a frequência com que o par de ângulos $(\theta_y, \theta_z) = (0, 0)$ é utilizado) para todas as imagens. Apenas a imagem I_7 apresenta o par

Figura 21 – Curva PSNR $\times$ taxa de *bits* para a imagem I_7.



Fonte: A autora (2020).

Figura 22 – Curva PSNR $\times$ taxa de *bits* para a imagem I_8.



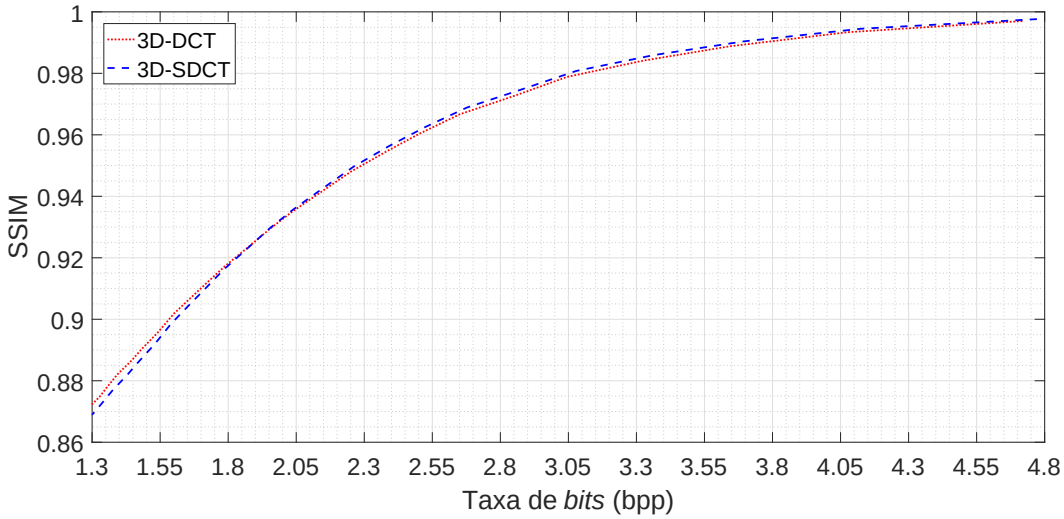
Fonte: A autora (2020).

de ângulos mais utilizado diferente de $(\theta_y, \theta_z) = (0, 0)$.

5.2 CIFRAGEM DE IMAGENS TRIDIMENSIONAIS BASEADA NA 3D-SCNT

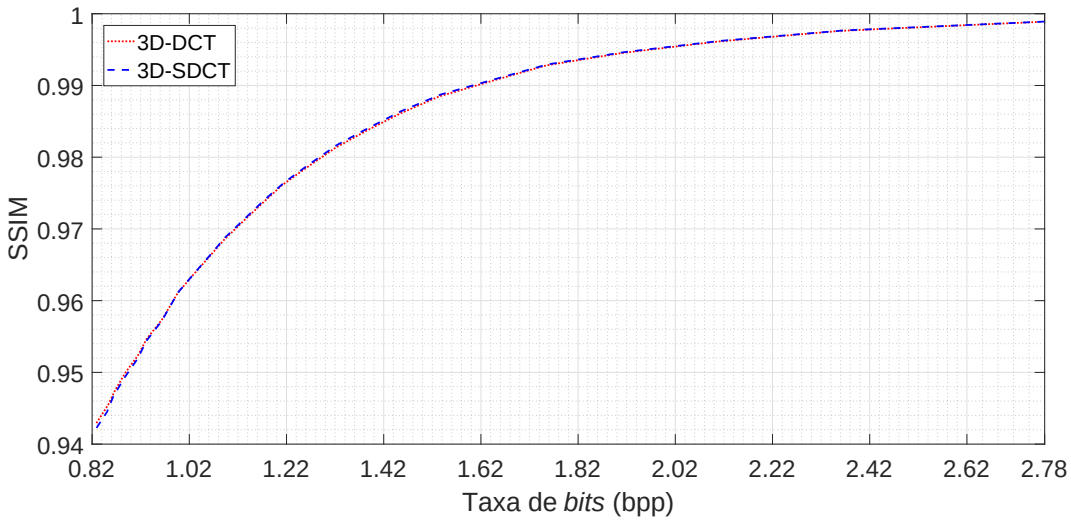
Cifragem é um dos mecanismos conhecidos para preservar a confidencialidade das imagens médicas, em que apenas pessoas autorizadas podem acessar os dados do paciente (BELKAID et al., 2015; BRINDHA, 2018; NORCEN et al., 2003). Isso leva a uma modificação visual das imagens, transformando-as em imagens com aspecto ruidoso, que apresentam uma distribuição aproximadamente uniforme dos valores de *pixel*. A cifragem de imagens médicas

Figura 23 – Curva SSIM $\times$ taxa de *bits* para a imagem I_7.



Fonte: A autora (2020).

Figura 24 – Curva SSIM $\times$ Taxa de *bits* para a imagem I_8.

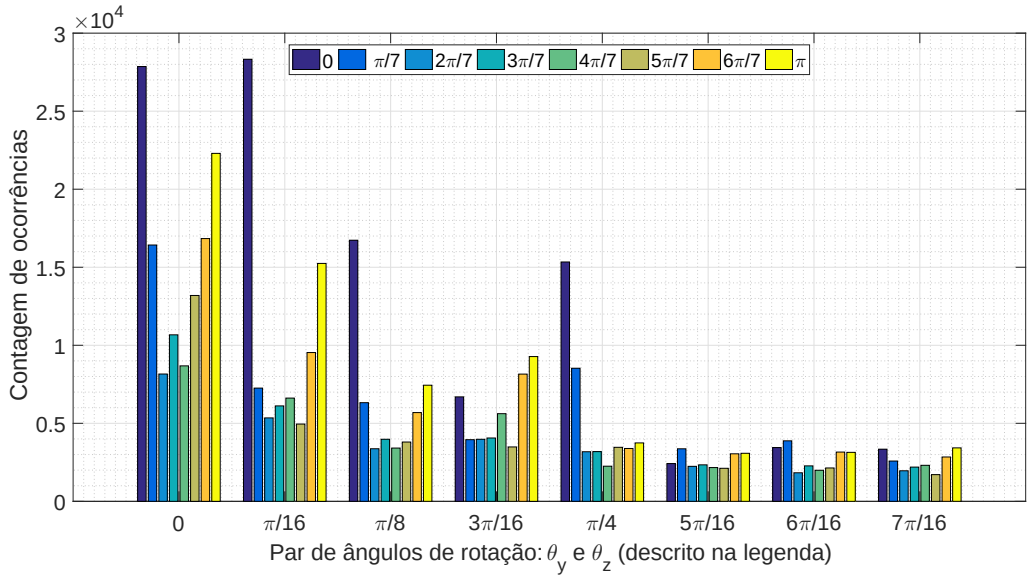


Fonte: A autora (2020).

pode ser realizada usando várias técnicas, como embaralhamento (HUA; YI; ZHOU, 2018), métodos baseados no caos (GATTA; AL-LATIEF, 2018; ABD-EL-LATIF; ABD-EL-ATTY; TALHA, 2018), mapas logísticos (DAI; WANG, 2012), algoritmos genéticos (NEMATZADEH et al., 2018), transformada discreta de wavelet (ABDMOULEH; KHALFALLAH; BOUHLEL, 2017; DAGADU et al., 2016) e transformada numérica do cosseno (LIMA; MADEIRO; SALES, 2015). Embora haja na literatura muitos trabalhos sobre cifragem de imagens médicas, a maioria destes contempla a cifragem no espaço bidimensional ou fatia por fatia das imagens médicas tridimensionais, com um número restrito de aplicações em imagens médicas 3D.

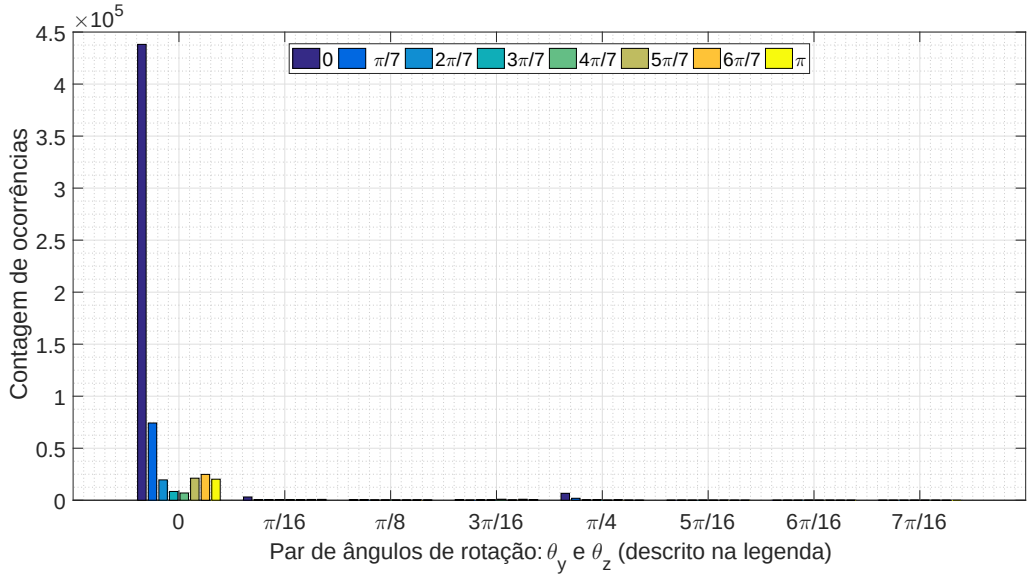
Motivada pela grande importância da cifragem de imagens médicas e pela escassez

Figura 25 – Histograma de escolha do par de ângulos para a 3D-SDCT na imagem I_7.



Fonte: A autora (2020).

Figura 26 – Histograma de escolha do par de ângulos para a 3D-SDCT na imagem I_8.



Fonte: A autora (2020).

de trabalhos de cifragem que levem em conta as imagens médicas tridimensionais, esta Tese apresenta, nesta seção, um esquema para cifragem de imagens médicas tridimensionais baseado na 3D-SCNT. O esquema proposto consiste basicamente em dividir uma imagem 3D em blocos e calcular a 3D-SCNT de cada bloco, usando uma chave secreta para obter os ângulos de rotação usados para transformar o primeiro bloco. A sequência de ângulos usada nos seguintes blocos 3D são versões sucessivamente deslocadas ciclicamente da primeira sequência. Posteriormente, a imagem é embaralhada, levando em consideração a imagem como um todo. Por fim, os blocos de

Tabela 5 – Métrica Bjøntegaard BD-PSNR e BD-SSIM.

Imagem	**BD-PSNR**	**BD-SSIM**
I_1	0,21	0,00110
I_2	0,24	0,00040
I_3	0,19	0,00051
I_4	0,14	0,00098
I_5	0,23	0,00046
I_6	0,17	0,00043
I_7	0,43	0,00006
I_8	0,10	0,00004
I_9	0,28	0,00079
I_{10}	0,50	0,00008

Fonte: A autora (2020).

Tabela 6 – Percentual de vezes que o par de ângulos $(\theta_y, \theta_z) = (0, 0)$ foi utilizado (PER$_{(\theta_y,\theta_z)=(0,0)}$), par de ângulos mais utilizado ((θ_y, θ_z)) e percentual de vezes que o par de ângulos (θ_y, θ_z) foi utilizado (PERmax$_{(\theta_y,\theta_z)}$).

Imagem	PER$_{(\theta_y,\theta_z)=(0,0)}$	(θ_y, θ_z)	PERmax$_{(\theta_y,\theta_z)}$
I_1	27,55%	$(0, 0)$	27,55%
I_2	74,84%	$(0, 0)$	74,84%
I_3	63,39%	$(0, 0)$	63,39%
I_4	20,22%	$(0, 0)$	20,22%
I_5	73,83%	$(0, 0)$	73,83%
I_6	68,09%	$(0, 0)$	68,09%
I_7	6,80%	$(\frac{\pi}{16}, 0)$	6,92%
I_8	68,46%	$(0, 0)$	68,46%
I_9	43,73%	$(0, 0)$	43,73%
I_{10}	28,09%	$(0, 0)$	28,09%

Fonte: A autora (2020).

imagens são novamente submetidos ao cálculo da 3D-SCNT. A decifragem é realizada aplicando, na ordem inversa, as mesmas etapas usadas na cifragem. O método se mostra eficaz, fornecendo resistência contra ataques criptográficos e alta sensibilidade à mudanças nos parâmetros secretos ou na própria imagem.

5.2.1 Esquema proposto

Na Figura 27, é apresentado um diagrama de blocos do método proposto, o qual recebe como entrada uma imagem tridimensional, e envolve os seguintes passos:

- **PASSO 1:** Divida a imagem tridimensional original em blocos 3D menores com a dimensão $N \times N \times N$. A imagem original pode ser preenchida com zeros para fornecer a divisão exata. Por exemplo, para dividir uma imagem com uma dimensão de $90 \times 90 \times 90$ *pixels* em blocos de tamanho $8 \times 8 \times 8$, a imagem é preenchida com zeros, de modo que tenha uma dimensão de $96 \times 96 \times 96$ *pixels*.

- **PASSO 2:** Gere a chave secreta (gerador de números pseudo-aleatórios), que corresponde a um vetor de comprimento $\frac{N^3-N}{3}$, com a sequência de ângulos usada na transformação do primeiro bloco 3D. As sequências usadas nos blocos 3D seguintes são versões sucessivamente deslocadas ciclicamente da primeira sequência;

- **PASSO 3:** Calcule a 3D-SCNT de cada bloco de I usando a sequência de ângulos destinada ao bloco em questão (conforme descrito no **PASSO 2**) e obtenha a imagem intermediária $I^{'}$.

- **PASSO 4:** Embaralhe os *pixels* da imagem intermediária $I^{'}$ para inserir difusão no sistema. Inicialmente, é realizada uma etapa de adição, na qual cada *pixel* é substituído pela soma do *pixel* atual pelo anterior (o primeiro *pixel* é adicionado a zero e a adição é executada módulo p, de modo que o valor de cada *pixel* esteja no intervalo de 0 a $p-1$). A operação de adição é realizada da esquerda para a direita, de cima para baixo, em cada fatia da imagem. Em seguida, uma permutação é aplicada às posições de *pixel* usando a transformada de Arnold (a permutação leva em consideração a imagem como um todo, não sendo realizada separadamente em cada bloco) (ARNOLD; AVEZ, 1968). A imagem é novamente submetida à etapa de soma;

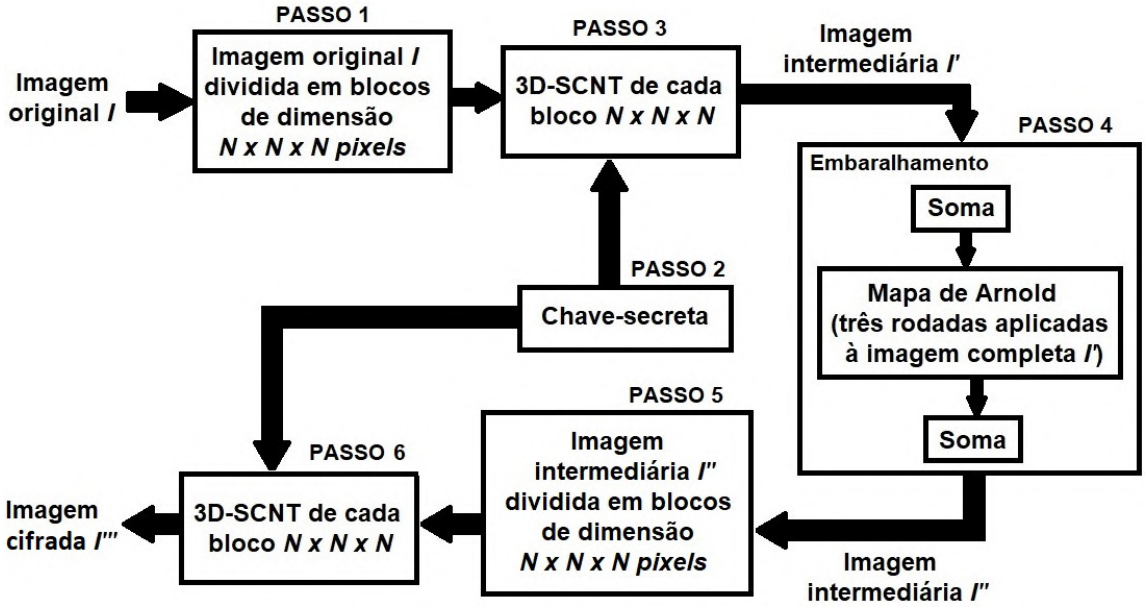
- **PASSO 5:** Divida a imagem intermediária $I^{''}$ em blocos 3D menores com a dimensão $N \times N \times N$;

- **PASSO 6:** Calcule a 3D-SCNT de cada bloco de $I^{''}$ usando o mesmo vetor com a sequência de ângulos usada no **PASSO 3** e obtenha a imagem cifrada $I^{'''}$.

A combinação de duas etapas de transformações lineares aplicadas aos blocos 3D da imagem e a etapa de embaralhamento aplicada à estrutura 3D, como um todo, tornam o esquema não linear; esse arranjo é realizado com o objetivo de obter confusão e difusão, necessárias ao esquema. Conforme será demonstrado, o fato de a chave usada para transformar cada bloco 3D corresponder a uma versão ciclicamente deslocada da chave usada para transformar o bloco anterior torna o esquema robusto contra certos tipos de ataques criptográficos clássicos, como de texto-claro escolhido.

A decifragem é realizada aplicando os passos descritos na Figura 27 na ordem inversa. A primeira etapa do procedimento de decifragem é a divisão da imagem cifrada em blocos com dimensões $N \times N \times N$ *pixels*. Em seguida, a 3D-SCNT inversa é aplicada a cada um dos blocos da imagem, usando a chave secreta informada. Na etapa inversa de embaralhamento, inicialmente,

Figura 27 – Diagrama de blocos do esquema de cifragem de imagem proposto. Os números indicam cada etapa executada para obter a imagem cifrada I''' da imagem original correspondente I.



Fonte: A autora (2020).

é executada uma etapa de soma inversa, na qual cada *pixel* é substituído pela subtração do *pixel* atual pelo anterior (o primeiro *pixel* anterior é igual a zero). A subtração é executada no módulo p, para que o valor de cada *pixel* esteja no intervalo de 0 a $p-1$. Em seguida, a transformada inversa de Arnold é aplicada e, finalmente, a etapa de soma inversa é aplicada novamente. O processo de decifragem é finalizado com a aplicação da 3D-SCNT inversa em cada bloco da imagem novamente.

5.2.1.1 Implementação do esquema

Para implementação do esquema proposto, diversos parâmetros precisam ser definidos. Assume-se que a 3D-SCNT será aplicada a uma imagem digital tridimensional, por exemplo imagens no padrão DICOM, cujo tamanho seja $W \times W \times W$ e cujos valores de *pixel* sejam codificados em palavras de 16 *bits* que representam os 65536 níveis de cinza. Os blocos 3D nos quais a imagem será dividida ao longo da cifragem têm dimensões $8 \times 8 \times 8$.

Com a configuração supracitada, é conveniente definir 3D-SCNTs sobre $\mathbb{F}_{65537}$, visto que $p = 65537$ é o menor número primo que permite acomodar toda a faixa de valores inteiros $[0, 65535]$[1] sem realização de redução modular. Na referida estrutura algébrica, pode-se escolher

[1] Os valores de *pixels* das imagens cifradas não poderão ser representados a partir de uma codificação usual de 16 *bits*, uma vez que $p = 65537$ permite acomodar a faixa de valores dos *pixels* $[0, 65536]$. Uma alternativa para contornar essa limitação é representar os valores de *pixels* no intervalo $[0, 65534]$ usando dois *bytes* no intervalo $[0000000000000000, 1111111111111110]$, e representar os valores 65535 e 65536 por meio do *flag* 1111111111111111 em que se esse for seguido pelo *bit* 0, ou seja, 1111111111111110, representa o valor de *pixel* 65535 ou se for seguido pelo *bit* 1, ou seja, 1111111111111111, representa o valor de *pixel* 65536. Isso implica um número médio de *bits* por *pixel* igual a $(65535 \times 16\ \textit{bits} + 2 \times 17\ \textit{bits}\ )/65557 = 16,0000305171\ \textit{bits}$,

$\zeta = 4$, o qual possui ordem multiplicativa $\mathrm{ord}(\zeta) = 2 \times 8 = 16$ e, portanto, pode ser utilizado para definição de uma 3D-CNT com dimensões $8 \times 8 \times 8$ (as mesmas dos blocos nos quais a imagem original é dividida). Para calcular as 3D-SCNTs com duas rotações (θ_y e θ_z) dos blocos em questão, é necessário escolher (secretamente) $2 \times M = 2 \times \frac{8^3-8}{3} = 336$ ângulos de rotação. Nas implementações realizadas nesta Tese, esses ângulos correspondem a números inteiros na faixa $[0, 15]$, produzidos por um gerador de números pseudo-aleatórios. Os cossenos e senos sobre corpos finitos desses ângulos foram calculados, também, com relação ao elemento $\alpha = 4$.

Na etapa de permutação do **PASSO 4** (Figura 27), foram empregadas três rodadas da transformada de Arnold 3D. A transformada de Arnold foi proposta por Vladimir Igorevich Arnold e corresponde a uma transformação linear nos índices i e j do nível de intensidade de um *pixel* $I(i, j)$ de uma imagem I. Seja I uma imagem com dimensão $N \times N$ *pixels*, a transformada de Arnold aplicada aos índices i e j de $I(i, j)$ pode ser expressa como (LIU et al., 2011)

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} \pmod{N}, \tag{105}$$

em que $0 \leq i, j \leq N - 1$ e (i', j') representam a nova posição do nível de intensidade do *pixel* $I(i', j')$. A transformada pode ser aplicada recursivamente, resultando em uma imagem mais embaralhada.

Em (CHEN; MAO; CHUI, 2004), os autores estenderam a transformada de Arnold para 3D, que consiste em três estágios nos quais cada uma das coordenadas x, y e z é fixada. A matriz de transformação é dada por

$$\mathbf{A}_{3D} = \mathbf{A}_{xy}\mathbf{A}_{yz}\mathbf{A}_{zx}, \tag{106}$$

em que a matriz $\mathbf{A}_{xy}$ é obtida fixando o eixo z e aplicando a transformada de Arnold no plano $x - y$, para a matriz $\mathbf{A}_{yz}$ é fixado o eixo x e a transformada de Arnold é aplicada no plano $y - z$ e, por fim, fixado o eixo y e a transformada de Arnold é aplicada no plano $z - x$ para obter a matriz $\mathbf{A}_{zx}$, como seguem

$$\mathbf{A}_{xy} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \tag{107}$$

$$\mathbf{A}_{yz} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 2 \end{bmatrix} \tag{108}$$

e

$$\mathbf{A}_{zx} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 2 \end{bmatrix}. \tag{109}$$

ou seja, o número de *bits* adicionais devido à cifragem é insignificante.

A etapa de embaralhamento no processo de cifragem é executada para evitar um ataque diferencial, de modo que uma pequena alteração na imagem a ser cifrada ou na chave secreta gere uma imagem cifrada consideravelmente diferente da imagem cifrada original. Para aplicar a transformada de Arnold 3D a uma imagem, a imagem deve ser cúbica. O preenchimento com zero pode ser usado para converter uma imagem retangular, por exemplo, $I(W, U, G)$ com $W > U > G$, em um tamanho cúbico, $I(W, W, W)$.

5.2.2 Experimentos e análise de segurança

Análise estatística

Empregando os parâmetros indicados na Subseção 5.2.1.1, foram submetidas à cifragem por meio do esquema proposto as imagens I_1, I_2, I_3, I_4, I_5 e I_6 da Tabela 3 e as imagens listadas na Tabela 7; na Figura 28, são apresentadas suas respectivas versões cifradas. Visualmente, observa-se que o aspecto das imagens cifradas é completamente ruidoso, sem conservar vestígios visuais das imagens originais correspondentes.

É desejável que os histogramas das imagens cifradas tenham distribuição uniforme, de modo a impossibilitar a extração de informações da imagem original. Analisando os histogramas das imagens originais e das imagens cifradas nas Figuras 29 e 30, observa-se que, independentemente do histograma da imagem original, o histograma da imagem cifrada correspondente possui aspecto próximo ao de uma distribuição uniforme, o que mostra a robustez do método a ataque estatístico.

Visto que uma imagem digital apresenta alta correlação entre *pixels* de uma certa vizinhança, um ataque que leve em consideração essa característica deve ser evitado. Para isso, um esquema de cifragem deve ocultar a correlação entre *pixels* adjacentes da imagem cifrada. O coeficiente de correlação, r_{xy}, entre dois *pixels* adjacentes (horizontal, vertical ou diagonal) x e y é calculado selecionando arbitrariamente T *pixels* de uma imagem a partir de

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{\text{var}(x)\text{var}(y)}}, \tag{110}$$

em que

$$\text{cov}(x, y) = \frac{1}{T}\sum_{t=1}^{T}(x_t - \text{E}(x))(y_t - \text{E}(y)), \tag{111}$$

$$\text{var}(x) = \frac{1}{T}\sum_{t=1}^{T}(x_t - \text{E}(x))^2, \tag{112}$$

e

$$\text{E}(x) = \frac{1}{T}\sum_{t=1}^{T}x_t, \tag{113}$$

Tabela 7 – Imagens utilizadas no esquema de cifragem.

Imagem	Tipo	Dimensão	Referência
I_A	*brain cancer*	$256 \times 256 \times 16$	(BARBORIAK, 2015)
I_B	*astrocytoma*	$132 \times 132 \times 24$	(JANSEN; TERRY, 2015)
I_C	*lower abdomen*	$128 \times 128 \times 70$	(LUCCHESI; AREDES, 2016)
I_D	*lower abdomen*	$128 \times 128 \times 90$	(LUCCHESI; AREDES, 2016)

Fonte: A autora (2020).

em que x_t é o valor do t-ésimo *pixel* selecionado e y_t é o valor do *pixel* adjacente correspondente.

Espera-se que a imagem original tenha um coeficiente de correlação alto, próximo a 1, e a imagem cifrada apresente um coeficiente de correlação próximo a 0. Foram utilizados arbitrariamente $T = 10000$ *pixels* para análise de correlação da imagem 3D para realizar a análise ao longo das componentes verticais, horizontais e diagonais. Para ser mais específico, se for considerado que cada imagem 3D é dividida em planos verticais (fatias 2D), a análise de correlação ao longo da direção vertical leva em consideração um *pixel* e seu *pixel* vizinho de cima ou de baixo, na mesma fatia; a análise de correlação ao longo das direções horizontal e diagonal considera um *pixel* e seus *pixels* vizinhos ao longo das direções correspondentes, obtidos de fatias adjacentes. Isso permite capturar a correlação na estrutura tridimensional. A Tabela 8 apresenta o coeficiente de correlação, r_{xy}, para as imagens originais e o coeficiente de correlação, $\widetilde{r}_{xy}$, para as imagens cifradas correspondentes. Como observado, as imagens originais têm altos coeficientes de correlação, enquanto os coeficientes de correlação para as imagens cifradas são próximos de zero. Valores semelhantes são obtidos se outras direções de adjacência forem consideradas (adjacências horizontais e diagonais na mesma fatia 2D, por exemplo).

A entropia das imagens é calculada por

$$H = \sum_{n=0}^{p-1} \frac{N_n}{N_N} \log_2 \frac{N_N}{N_n}, \tag{114}$$

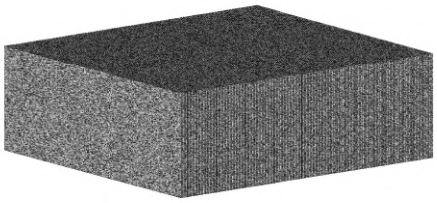
em que N_n corresponde a quantidade de *pixels* na imagem que assume o valor n e N_N é o número total de *pixels* na imagem. Uma vez que cada *pixel* da imagem pode assumir p valores diferentes de *pixels*, o valor resultante da entropia pertence ao intervalo $[0, \log_2(p)]$. Para uma comparação justa das entropias das imagens originais e suas respectivas versões cifradas, visto que os valores dos *pixels* das imagens originais se encontram no intervalo $[0, 65535]$ (16 bpp) e os das imagens cifradas em $[0, 65536]$, é usada a versão normalizada definida por

$$\overline{H} = \frac{H}{\log_2(p)}, \tag{115}$$

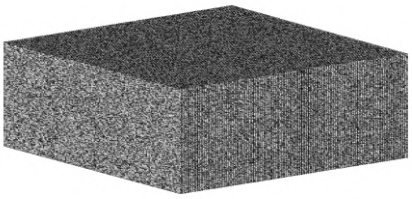
com valor máximo igual a 1, que representa o caso em que as intensidades dos *pixels* são equiprováveis. A Tabela 8 apresenta os resultados de entropia normalizada, $\overline{H}$, das imagens

Figura 28 – Imagens cifradas.

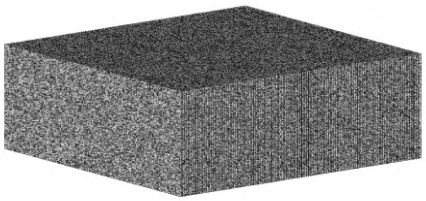
(a) Imagem $I_1^{'''}$



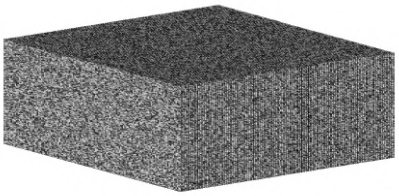
(b) Imagem $I_2^{'''}$



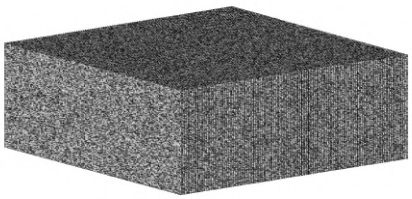
(c) Imagem $I_3^{'''}$



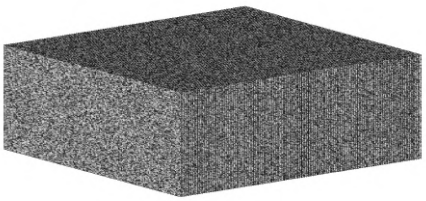
(d) Imagem $I_4^{'''}$



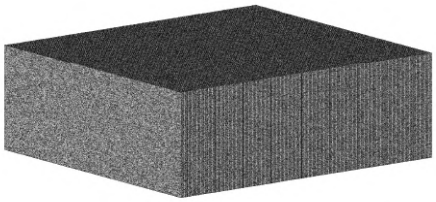
(e) Imagem $I_5^{'''}$



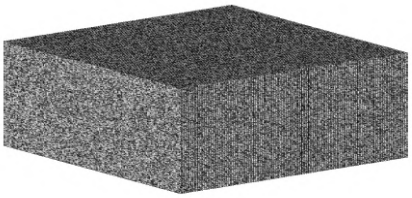
(f) Imagem $I_6^{'''}$



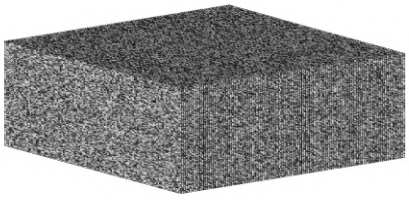
(g) Imagem $I_A^{'''}$



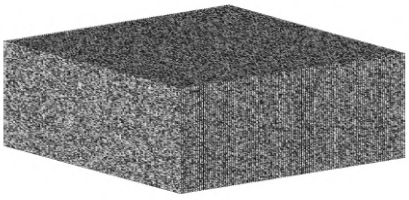
(h) Imagem $I_B^{'''}$



(i) Imagem $I_C^{'''}$



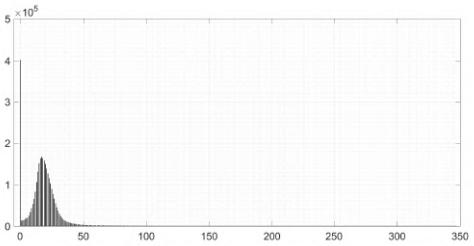
(j) Imagem $I_D^{'''}$



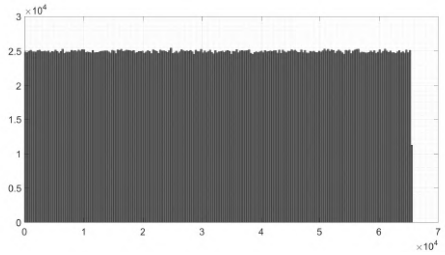
Fonte: A autora (2020).

Figura 29 – Histogramas das imagens originais I_1, I_2, I_3, I_4 e I_5 (coluna da esquerda) e de suas respectivas versões cifradas (coluna da direita).

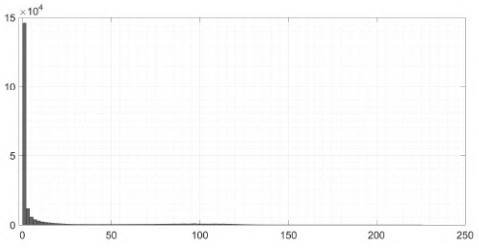
(a) Histograma da imagem I_1



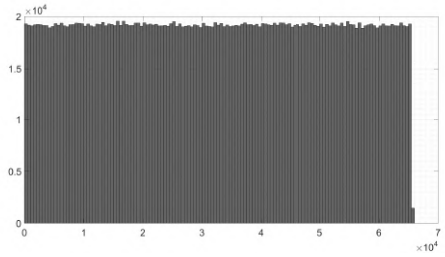
(b) Histograma da imagem $I_1^{'''}$



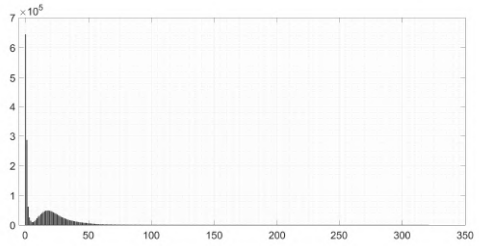
(c) Histograma da imagem I_2



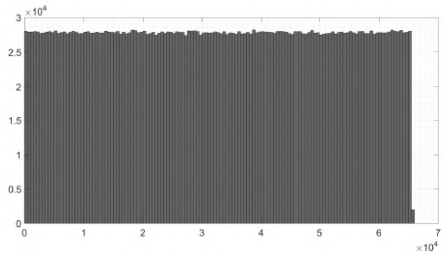
(d) Histograma da imagem $I_2^{'''}$



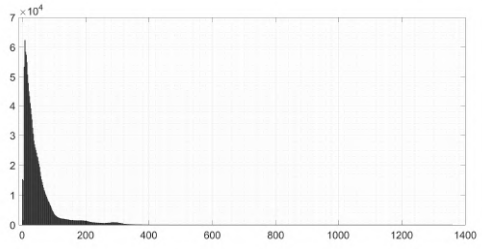
(e) Histograma da imagem I_3



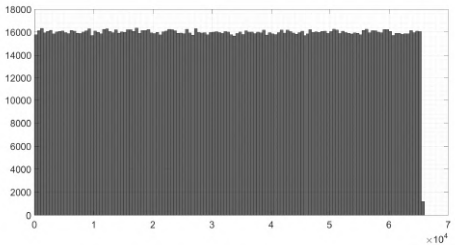
(f) Histograma da imagem $I_3^{'''}$



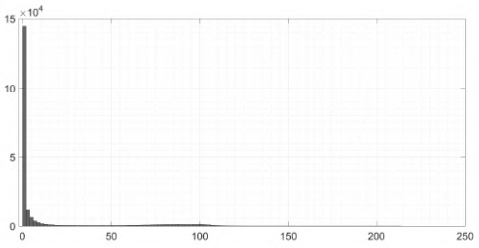
(g) Histograma da imagem I_4



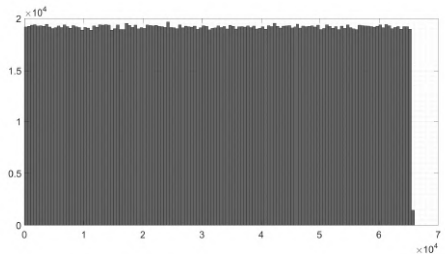
(h) Histograma da imagem $I_4^{'''}$



(i) Histograma da imagem I_5



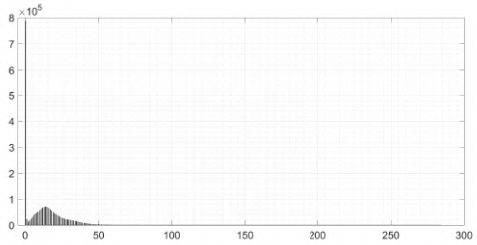
(j) Histograma da imagem $I_5^{'''}$



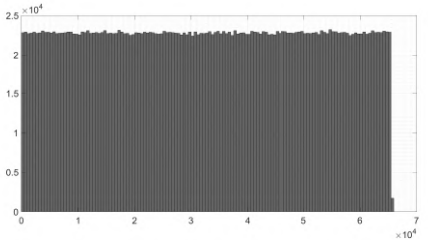
Fonte: A autora (2020).

Figura 30 – Histogramas das imagens originais I_6, I_A, I_B, I_C e I_D (coluna da esquerda) e de suas respectivas versões cifradas (coluna da direita).

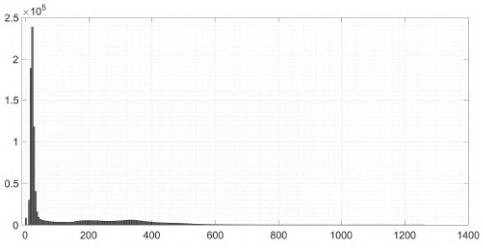
(a) Histograma da imagem I_6



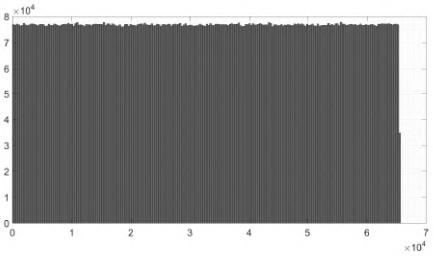
(b) Histograma da imagem $I_6^{'''}$



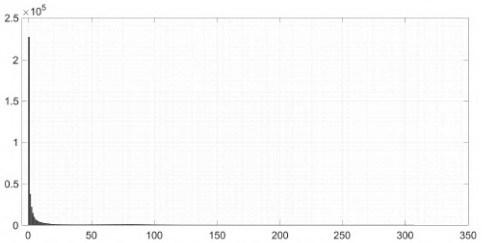
(c) Histograma da imagem I_A



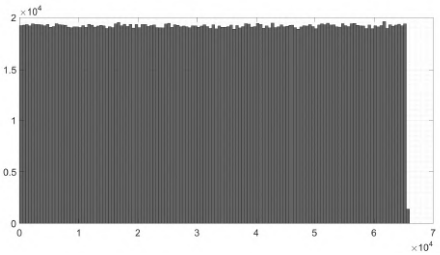
(d) Histograma da imagem $I_A^{'''}$



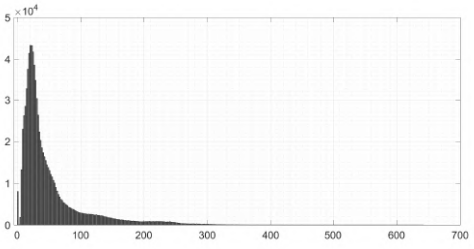
(e) Histograma da imagem I_B



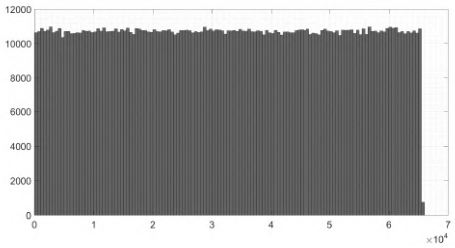
(f) Histograma da imagem $I_B^{'''}$



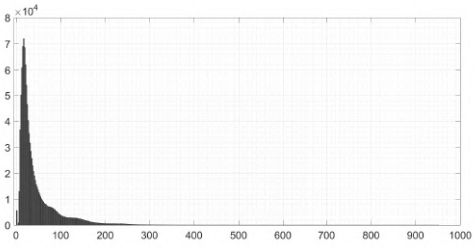
(g) Histograma da imagem I_C



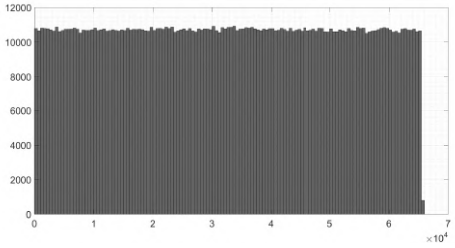
(h) Histograma da imagem $I_C^{'''}$



(i) Histograma da imagem I_D



(j) Histograma da imagem $I_D^{'''}$



Fonte: A autora (2020).

originais e as de suas versões cifradas correspondentes, $\overline{H'}$. Como desejado, os valores da entropia normalizada para as imagens cifradas são próximos a 1, revelando que cada *pixel* da imagem cifrada tem a mesma probabilidade de assumir qualquer um dos valores possíveis.

Robustez a ataques diferenciais

A avaliação da robustez do esquema contra ataques diferenciais pode ser realizada comparando imagens cifradas geradas a partir de imagens originais minimamente diferentes, por exemplo, imagens que diferem apenas no *bit* menos significativo (LSB, do inglês *least significant bit*) de um *pixel*. A diferença entre essas imagens pode ser mensurada por meio duas métricas: a taxa do número de *pixels* modificados (NPCR, do inglês *number of pixels change rate*) e a intensidade média de mudança unificada (UACI, do inglês *unified average changing intensity*), respectivamente definidas por (WU; NOONAN; AGAIAN, 2011)

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{N_1 \times N_2} \times 100\%, \tag{116}$$

e

$$\text{UACI} = \frac{1}{N_1 \times N_2} \left[\frac{\sum_{i,j} \left| I'''(i,j) - I'''_{mod}(i,j) \right|}{p-1} \right] \times 100\%, \tag{117}$$

em que N_1 e N_2 denotam, respectivamente, os números de linhas e de colunas das imagens cifradas I''' e I'''_{mod}, com as imagens originais correspondentes diferindo em apenas um LSB; $I'''(i,j)$ e $I'''_{mod}(i,j)$ correspondem ao nível de intensidade dos *pixels* da i-ésima linha e j-ésima coluna das imagens I''' e I'''_{mod}, respectivamente; e $D(i,j)$ definido como

$$D(i,j) = \begin{cases} 0, & I'''(i,j) = I'''_{mod}(i,j), \\ 1 & \text{caso contrário.} \end{cases} \tag{118}$$

Para cada uma das imagens utilizadas, 100 imagens modificadas foram geradas alterando um LSB de um *pixel* escolhido aleatoriamente. Foram calculados o NPCR e o UACI, para cada uma das 100 imagens modificadas, a partir das versões cifradas de cada imagem original, I''', e a versão cifrada da imagem modificada correspondente, I'''_{mod}. A Tabela 9 apresenta os valores mínimo, máximo e médio do NPCR e o UACI obtidos para as imagens. Os valores obtidos são muito próximos dos desejados (NPCR $\approx 99{,}61\%$ e UACI $\approx 33{,}46\%$) (WU; NOONAN; AGAIAN, 2011). Um valor de NPCR próximo a $99{,}61\%$ e de UACI próximo a $33{,}46\%$ indicam uma grande diferença entre as imagens cifradas I''' e I'''_{mod}, revelando que uma pequena modificação na imagem original resulta em uma mudança considerável na imagem cifrada, provando que o esquema é robusto a ataques diferenciais.

Espaço de chaves e sensibilidade da Chave

Para inviabilizar um ataque de força bruta, um esquema de cifragem deve ter um espaço de chave suficientemente grande. Como discutido anteriormente (ver Subseção 5.2.1.1), o cálculo da 3D-SCNT com duas rotações (θ_y e θ_z) requer a escolha de $2 \times \frac{8^3-8}{3} = 336$ ângulos de rotação. Se esses ângulos forem tomados como a chave secreta do esquema, essa chave poderá ser

Tabela 8 – Coeficientes de correlação ($r_{x,y}$) das imagens originais e os ($\widetilde{r}_{x,y}$) das imagens cifradas correspondentes ((v), (h) e (d) correspondem à adjacência vertical, horizontal e diagonal, respectivamente), entropia normalizada ($\overline{H}$) das imagens originais e ($\overline{H'}$) das imagens cifradas correspondentes.

Imagem	$r_{x,y}(v)$	$\widetilde{r}_{x,y}(v)$	$r_{x,y}(h)$	$\widetilde{r}_{x,y}(h)$	$r_{x,y}(d)$	$\widetilde{r}_{x,y}(d)$	$\overline{H}$	$\overline{H'}$
I_1	0,9567	4,6917e-04	0,8869	7,1302e-04	0,8568	3,7280e-04	0,2204	0,9995
I_2	0,9821	-9,6197e-05	0,9060	7,6000e-04	0,9150	6,5981e-04	0,0237	0,9988
I_3	0,9661	-6,7009e-04	0,9552	-6,1857e-04	0,9281	-7,9474e-04	0,2429	0,9990
I_4	0,9782	-9,5327e-04	0,9533	-2,7982e-04	0,9593	3,7276e-04	0,3269	0,9986
I_5	0,9845	2,7671e-05	0,9402	3,9854e-04	0,9421	3,3375e-04	0,0236	0,9988
I_6	0,9691	1,2225e-04	0,9605	1,0567e-04	0,9368	1,2977e-04	0,2254	0,9990
I_A	0,9787	-5,4773e-04	0,9712	-7,0050e-04	0,9626	1,7291e-04	0,0488	0,9998
I_B	0,9692	4,6283e-05	0,8919	6,8759e-04	0,8801	-3,0294e-04	0,0502	0,9988
I_C	0,9824	-1,2206e-04	0,9165	-2,1515e-04	0,9083	3,6401e-04	0,3251	0,9979
I_D	0,9703	5,5730e-04	0,9167	4,4633e-04	0,9265	-9,1081e-04	0,3764	0,9979

Fonte: A autora (2020).

representada como uma sequência com $336 \times 4 = 1344$ *bits* (assumindo que cada número inteiro no intervalo $[0, 15]$ seja representado por 4 *bits*). Vale ressaltar que os parâmetros usados na transformada de Arnold 3D para embaralhar a imagem não são levados em consideração para o cálculo do espaço da chave. Assim, o tamanho do espaço da chave é 2^{1344}, o que é suficiente para inviabilizar ataques de força bruta. Pode-se também optar por produzir os ângulos de rotação a partir de sequências caóticas, por exemplo; nesse caso, a chave secreta corresponderia aos parâmetros iniciais dessas sequências. Mais detalhes sobre essa abordagem podem ser obtidos em (STOJANOVSKI; KOCAREV, 2001; STOJANOVSKI; PIHL; KOCAREV, 2001; BEIRAMI; NEJATI; CALLEGARI, 2014; LIU; MIAO, 2016).

Em um esquema de criptografia, a imagem original deve ser recuperada corretamente se e somente se a chave exata for usada durante o processo de decifragem. Qualquer pequena alteração na chave deve causar alterações significativas na imagem recuperada correspondente, isto é, o esquema deve ser altamente sensível à chave. Essa sensibilidade pode ser avaliada a partir dos valores de NPCR das imagens decifradas utilizando a chave secreta usada para a cifragem (chave correta) e as imagens decifradas com chaves "minimamente" diferentes das corretas, diferindo, por exemplo, em apenas um *bit* menos significativo. Para isso, 100 chaves modificadas foram geradas, alterando apenas o LSB de uma das componentes da chave secreta original. As imagens cifradas foram decifradas utilizando cada uma das chaves modificadas; foram obtidos os resultados do NPCR entre a imagem original e cada uma das 100 imagens decifradas. A Tabela 10 apresenta os valores máximo, mínimo e médio para as imagens decifradas com as 100 chaves modificadas. Os resultados mostram que as imagens decifradas usando as chaves erradas são completamente diferentes das originais (veja o exemplo mostrado na Figura 31 para

Tabela 9 – Robustez a ataques diferenciais: valores mínimo (min), máximo (max) e médio (med) do NPCR e do UACI obtidos nos experimentos.

Imagem	NPCR_{max}	NPCR_{min}	NPCR_{med}	UACI_{max}	UACI_{min}	UACI_{med}
I_1	99,9992	99,9972	99,9984	33,3765	33,2908	33,3378
I_2	99,9990	99,9521	99,9958	33,3675	33,2911	33,3306
I_3	99,9992	99,9976	99,9984	33,3767	33,2957	33,3350
I_4	99,9992	99,9973	99,9985	33,3874	33,2859	33,3408
I_5	99,9991	99,9790	99,9967	33,3845	33,2843	33,3353
I_6	99,9991	99,9972	99,9984	33,3747	33,3006	33,3421
I_A	99,9991	99,9969	99,9984	33,3789	33,2836	33,3365
I_B	99,9991	99,9790	99,9967	33,3819	33,2978	33,3458
I_C	99,9994	99,9971	99,9985	33,3946	33,3040	33,3446
I_D	99,9992	99,9975	99,9985	33,3882	33,2773	33,3354

Fonte: A autora (2020).

a imagem I_C), o que significa que o esquema é altamente sensível a mudanças mínimas na chave secreta, provando que o esquema é robusto a ataques diferenciais à chave.

Comparação com outros esquemas de cifragem

Existem vários trabalhos na literatura sobre cifragem de imagens médicas. No entanto, a maioria desses trabalhos é para imagens bidimensionais ou executam a cifragem em cada fatia da imagem tridimensional. No último cenário, é possível que haja uma desvantagem no resultado da cifragem executada fatia por fatia da imagem tridimensional, no caso, por exemplo, de uma fatia nula (*pixels* iguais a zero), que é comum em se tratando de imagens médicas. Nesse caso específico, a versão cifrada correspondente também será uma fatia nula. No esquema proposto nesta Tese, isso não acontece porque o esquema de cifragem proposto atua diretamente na imagem 3D, ou seja, nos *voxels* que definem a imagem.

Além disso, até onde se sabe, não existem trabalhos na literatura sobre cifragem de imagens médicas tridimensionais com base, especificamente, em transformadas que realizam a cifragem diretamente nos *voxels* da imagem.

Na Tabela 11, o esquema de cifragem proposto é comparado com três métodos existentes na literatura, que também realizam a cifragem diretamente na estrutura 3D. As comparações foram feitas a partir das imagens mostradas na Figura 32.

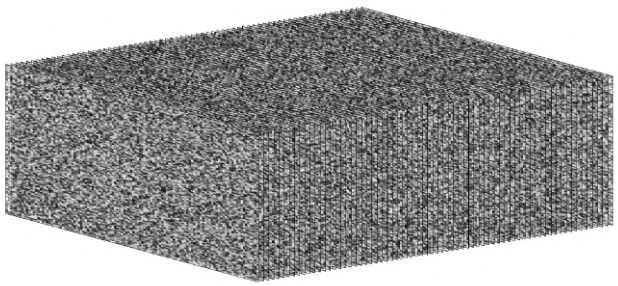
Na tabela, o texto em negrito é utilizado para destacar o melhor resultado para cada métrica. Embora os três métodos tenham atingido valores satisfatórios do ponto de vista das questões de segurança, pode-se observar que os resultados fornecidos pelo esquema proposto são os melhores, com exceção da UACI, que apresenta uma diferença de $0{,}1235$ em relação ao método introduzido em (BANIK; SHAMSI; SINGH, 2019). A Figura 33 mostra as imagens decifradas utilizando o método proposto com uma alteração de um *bit* na chave secreta. Os resultados mostram que as imagens decifradas são completamente diferentes das imagens originais.

Tabela 10 – Sensibilidade da chave: valores mínimo (min), máximo (max) e médio (med) do NPCR obtidos nos experimentos.

Imagem	$NPCR_{max}$	$NPCR_{min}$	$NPCR_{med}$
I_1	99,9988	99,9981	99,9985
I_2	99,9991	99,9979	99,9958
I_3	99,9991	99,9980	99,9985
I_4	99,9992	99,9978	99,9985
I_5	99,9990	99,9981	99,9985
I_6	99,9991	99,9979	99,9985
I_A	99,9987	99,9983	99,9985
I_B	99,9990	99,9977	99,9985
I_C	99,9992	99,9974	99,9985
I_D	99,9994	99,9978	99,9985

Fonte: A autora (2020).

Figura 31 – Imagem I_C''' decifrada com uma chave diferente da chave original em apenas um *bit* menos significativo.



Fonte: A autora (2020).

Para uma comparação mais ampla, se considerarmos algoritmos de cifragem 2D, por exemplo (GONDIM; OLIVEIRA NETO; LIMA, 2019; KAUR; KUMAR, 2018; MIKHAIL; ABOUELSEOUD; ELKOBROSY, 2017; LIMA; MADEIRO; SALES, 2015), em termos de tamanho do espaço da chave, coeficiente de correlação, NPCR, UACI e entropia normalizada, observa-se que os resultados apresentados pelo método proposto são semelhantes.

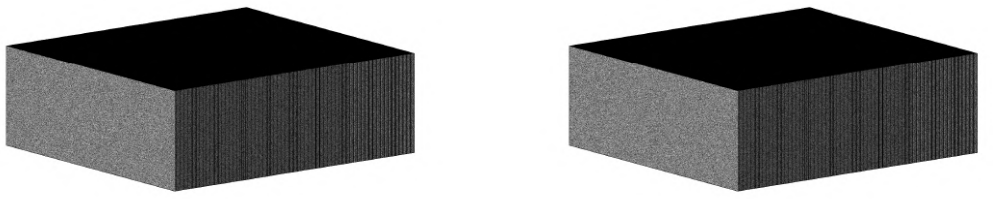
Figura 32 – Imagens usadas para comparação entre técnicas: (a) *abdomen CT scan* (SAMPLE MEDICAL IMAGES, Accessed: 2020-03-27) ($256 \times 256 \times 56$ *pixels*); (b) *abdomen CT scan* (LUNG IMAGE DATABASE CONSORTIUM (LIDC),) ($512 \times 512 \times 512$ *pixels*).

(a) (b)

Fonte: A autora (2020).

Figura 33 – Imagens decifradas com uma chave diferente da original em apenas um *bit* menos significativo: (a) Figura 32a; (b) Figura 32b.

(a) (b)



Fonte: A autora (2020).

Tabela 11 – Comparação com métodos existentes (Referência A (BANIK; SHAMSI; SINGH, 2019), Referência B (WANG et al., 2016) e Referência C (WANG et al., 2017)): coeficiente de correlação ($\widetilde{r}_{x,y}$) das imagens cifradas ((v), (h) e (d) correspondem à adjacência vertical, horizontal e diagonal respectivamente), entropia normalizada para imagens cifradas ($\overline{H'}$), NPCR e UACI para teste de ataque diferencial, e dimensão do espaço de chaves. O símbolo "-" em algumas entradas da tabela indica que a métrica de segurança correspondente não é fornecida claramente pelos autores do trabalho mencionado.

$\widetilde{r}_{x,y}(v)$				
Figura 32a		Figura 32b		
Referência A	Método proposto	Referência B	Referência C	Método proposto
1,3600e-03	**-4,3946e-05**	-6,0000e-04	-6,0000e-04	**-9,2176-05**
$\widetilde{r}_{x,y}(h)$				
Figura 32a		Figura 32b		
Referência A	Método proposto	Referência B	Referência C	Método proposto
1,3170e-02	**-7,3538e-05**	-2,0000e-04	2,0000e-04	**5,7838e-05**
$\widetilde{r}_{x,y}(d)$				
Figura 32a		Figura 32b		
Referência A	Método proposto	Referência B	Referência C	Método proposto
2,2400e-03	**1,9398e-05**	5,0000e-04	-3,0000e-04	**-5,3937e-05**
$\overline{H'}$				
Figura 32a		Figura 32b		
Referência A	Método proposto	Referência B	Referência C	Método proposto
0,9999	**0,9999**	**1,0000**	-	**1,0000**
NPCR				
Figura 32a		Figura 32b		
Referência A	Método proposto	Referência B	Referência C	Método proposto
99,6073	**99,9990**	-	-	99,9973
UACI				
Figura 32a		Figura 32b		
Referência A	Método proposto	Referência B	Referência C	Método proposto
33,4715	33,3480	-	-	33,3354
Espaço de chave				
Figura 32a		Figura 32b		
Referência A	Método proposto	Referência B	Referência C	Método proposto
2^{512}	$\mathbf{2^{1344}}$	$> 10^{39} \cdot 18$	$> 10^{135} \cdot 18$	$\mathbf{2^{1344} = 10^{404} \cdot 3{,}8394}$

Fonte: A autora (2020).

6 CONCLUSÕES

O presente trabalho apresentou a definição de novas transformadas discretas baseadas em rotações que surgiram a partir de um paralelo feito entre o processamento de sinais sobre grafos e o processamento digital de sinais, mais especificamente, a partir da equivalência identificada entre a GFT para grafos com topologias específicas e as transformadas discretas para sinais sobre domínios regulares.

Sobre corpos infinitos, foi proposta a transformada 3D-SDCT e foi apresentada a análise da multiplicidade dos autovalores da 4D-DCT, que constituem uma possível autobase para o Laplaciano do produto de quatro grafos em caminho. O estudo da multiplicidade dos autovalores da 4D-DCT tem utilidade na definição de uma versão 4D da SDCT. Para a transformada proposta 3D-SDCT foi apresentado o conceito de rotação "ótima" que permite compactar melhor a energia do sinal em relação à 3D-DCT, escolhendo, entre todas as rotações que podem ser realizadas, aquelas que fornecem um maior número de coeficientes nulos. Foi mostrado que, para cada autoespaço com multiplicidade maior do que um, é possível encontrar os ângulos de rotação que permitem compactar toda a energia em um coeficiente da tripla rotacionada, reduzindo os outros dois a zero; isso resulta na anulação de $\frac{2(N^3-N)}{3}$ coeficientes dentre os N^3, representando uma melhoria, em relação à 3D-SDCT com rotação não-ótima ou à 3D-DCT, no quesito compactação de energia do sinal.

No quesito aplicabilidade, foi apresentado um método de compressão de imagens tridimensionais baseado na 3D-SDCT em que, para contornar o problema da alta taxa de transmissão necessária para o envio ao decodificador dos $\frac{N^3-N}{3}$ ângulos ótimos empregados nas rotações (para o caso da 3D-SDCT com rotação ótima), foram utilizadas versões subótimas que levam a um menor número de coeficientes nulos ou próximos de zero. Essas versões subótimas foram obtidas a partir de uma modelagem RD, que busca escolher a versão comprimida mais eficiente para cada bloco da imagem. Foi considerado o uso de um único par de ângulos de rotação por bloco. Os resultados foram comparados com os resultados obtidos com a 3D-DCT usual, utilizando a mesma estratégia de quantização e codificação, e mostraram que a 3D-SDCT pode ser utilizada de forma eficiente no referido cenário de aplicação e supera a 3D-DCT clássica.

Foi apresentada também uma versão em corpos finitos da 3D-SDCT. A transformada proposta é identificada pelo acrônimo 3D-SCNT e é definida pela rotação dos vetores de base da 3D-CNT, usando um operador de rotação sobre corpos finitos. Foi avaliada a aplicabilidade da 3D-SCNT no cenário de cifragem de imagens médicas tridimensionais. Vale ressaltar aqui, de forma a enaltecer a importância da aplicabilidade da 3D-SCNT no cenário de cifragem, que, até onde se sabe, não existem trabalhos na literatura sobre cifragem de imagens médicas tridimensionais com base, especificamente, em transformadas que realizam a cifragem diretamente nos *voxels* da imagem; a maioria dos trabalhos de cifragem tridimensional encontrados na literatura executa a cifragem em cada fatia da imagem tridimensional, o que pode acarretar em versões cifradas nulas de fatias com *pixels* todos iguais a zero (fato comum em imagens médicas). A estratégia do

esquema de cifragem proposto é usar uma chave secreta para obter os referidos ângulos de rotação do primeiro bloco de imagem a ser transformado. A sequência de ângulos usada nos blocos seguintes é formada por versões sucessivamente deslocadas ciclicamente da primeira sequência. O esquema mostrou-se robusto contra os principais ataques criptográficos, sendo altamente sensível a mudanças na chave secreta. Isso se deve principalmente ao fato de que a 3D-SCNT é altamente dependente dos ângulos de rotação. O esquema de cifragem foi ainda comparado com três métodos existentes na literatura, e os resultados proporcionados pelo esquema proposto se apresentaram superiores em termos de tamanho do espaço de chaves, coeficiente de correlação, NPCR e entropia normalizada.

6.1 TRABALHOS FUTUROS

Como continuidade deste trabalho, pode-se destacar os seguintes pontos:

- **Algoritmos rápidos para as SDCT's e SCNT's:** As transformadas manobráveis propostas correspondem, basicamente, a versões rotacionadas das bases de suas correspondentes transformadas discretas originais. Embora as versões originais das transformadas propostas sejam separáveis, as transformadas manobráveis não são, o que acarreta uma complexidade maior em seu cálculo se comparada à versão não manobrável. Tendo em vista essa complexidade, um objeto de investigação interessante é a caracterização das transformadas propostas com relação à complexidade aritmética envolvida nos seus cálculos, propondo algoritmos rápidos neste cenário;

- **Aperfeiçoar a escolha dos ângulos de rotação:** A 3D-SDCT admite mais de um par de ângulos de rotação por bloco, e permite, a partir da escolha adequada dos ângulos de rotação (rotação ótima), compactar a energia do sinal em apenas $\frac{N^3+2N}{3}$ coeficientes. No entanto, o uso da rotação ótima acarreta uma elavada taxa de codificação dos ângulos utilizados. Diante desse cenário, torna-se de grande importância a utilização de métodos para sistematizar a escolha dos ângulos de rotação. Pode-se citar aqui, por exemplo, o uso de inteligência artifical, como algoritmos genéticos, para otimizar a forma de escolha dos ângulos visando uma rotação ótima;

- **Codificação de vídeo:** Como trabalhos futuros é interessante investigar a aplicação da 3D-SDCT no cenário de codificação de vídeo e realizar uma comparação com métodos baseados em transformadas encontrados na literatura;

- **4D-SDCT e codificação de *light fields*:** Em investigações futuras, pode-se, a partir da análise dos atutovalores do Laplaciano do produto de quatro grafos em caminho, apresentada na Seção 3.2, caracterizar uma 4D-SDCT e avaliar a sua aplicabilidade no cenário de representação e codificação de *light fields*, com o objetivo de obter um conjunto de coeficientes esparso e compacto (no sentido de que a energia está concentrada em poucos

coeficientes transformados), que pode ser usado com o objetivo de melhorar os resultados de codificação de trabalhos recentes, tais como (CARVALHO et al., 2018; CONTI; SOARES; NUNES, 2016; LIU et al., 2016; CONTI; NUNES; SOARES, 2018; SANTOS et al., 2018);

- n**D-SCNT com** $n \geq 4$**:** Como trabalhos futuros, visando o cenário de processamento de *light fields*, é de grande relevância a definição de SCNT's em espaços cujas dimensões são maiores que três, por exemplo, uma 4D-SCNT, que pode ser aplicada à cifragem de *light fields*;

- **Outras transformadas manobráveis:** A definição de novas transformadas a partir da exploração da GFT, fazendo uso da mesma abordagem utilizada nesta Tese, é um tópico de interesse para investigações futuras; propor, por exemplo, uma generalização da transformada de Hartley (BRACEWELL, 1983).

6.2 ARTIGOS RELACIONADOS À TESE

Como frutos deste trabalho, os seguintes artigos foram publicados:

Artigos em periódicos:

- LIMA, V. S.; MADEIRO, F.; LIMA, J. B. Encryption of 3D medical images based on a novel multiparameter cosine number transform. *Computers in Biology and Medicine*, v. 121, p. 103772-103783, 2020.

- LIMA, V. S.; MADEIRO, F.; LIMA, J. B. Three-dimensional steerable discrete cosine transform with application to 3D image compression. *Multidimensional Systems and Signal Processing*, p. 1-29, 2020.

Artigo completo em anais de eventos:

- LIMA, V. S.; MADEIRO, F.; LIMA, J. B. Transformada discreta do cosseno manobrável em três dimensões. *XXXVI Simpósio Brasileiro de Telecomunicações e Processamento de Sinais (SBrT 2018)*, Sep 16-19, 2018, Campina Grande, Brasil.

  – Vale destacar que o trabalho acima mencionado foi premiado como um dos melhores trabalhos do SBrT 2018.

REFERÊNCIAS

ABD-EL-LATIF, A. A.; ABD-EL-ATTY, B.; TALHA, M. Robust encryption of quantum medical images. **IEEE Access**, v. 6, p. 1073–1081, 2018. Citado na página 72.

ABDMOULEH, M. K.; KHALFALLAH, A.; BOUHLEL, M. S. A novel selective encryption DWT-based algorithm for medical images. In: **2017 14th International Conference on Computer Graphics, Imaging and Visualization (CGiV)**. [S.l.: s.n.], 2017. p. 79–84. Citado na página 72.

AHMADZAI, F.; RAO, K. M. L.; ULFAT, S. Assessment and modelling of urban road networks using integrated graph of natural road network (a GIS-based approach). **Journal of Urban Management**, v. 8, n. 1, p. 109–125, 2019. Citado na página 23.

AHMED, N.; NATARAJAN, T.; RAO, K. R. Discrete cosine transform. **IEEE Transactions on Computers**, C-23, n. 1, p. 90–93, Jan 1974. Citado na página 18.

ALVES, G.; PEREIRA, F.; da Silva, E. A. B. Light field imaging coding: Performance assessment methodology and standards benchmarking. In: **2016 IEEE International Conference on Multimedia Expo Workshops (ICMEW)**. [S.l.: s.n.], 2016. p. 1–6. Citado na página 48.

ARNOLD, V.; AVEZ, A. **Ergodic Problems of Classical Mechanics**. Benjamin: [s.n.], 1968. Citado na página 75.

ATAL, D. K.; SINGH, M. A hybrid feature extraction and machine learning approaches for epileptic seizure detection. **Multidimensional Systems and Signal Processing**, v. 31, p. 503–525, August 2020. Citado na página 23.

BANIK, A.; SHAMSI, Z.; SINGH, L. An encryption scheme for securing multiple medical images. **Journal of Information Security and Applications**, v. 49, 12 2019. Citado 2 vezes nas páginas 85 e 88.

BARBORIAK, D. **Data From RIDER NEURO MRI**. 2015. <http://doi.org/10.7937/K9/TCIA.2015.VOSN3HN1>. Citado 3 vezes nas páginas 46, 69 e 79.

BATABYAL, T.; ACTON, S. T. Neurosol: Automated classification of neurons using the sorted Laplacian of a graph. In: **2017 IEEE 14th International Symposium on Biomedical Imaging (ISBI 2017)**. [S.l.: s.n.], 2017. p. 397–400. Citado na página 23.

BEIRAMI, A.; NEJATI, H.; CALLEGARI, S. Fundamental performance limits of chaotic-map random number generators. In: **52nd Annual Allerton Conference on Communication, Control, and Computing (Allerton 2014)**. [S.l.: s.n.], 2014. p. 1126–1131. Citado na página 84.

BELKAID, B. M. et al. Secure transfer of medical images using hybrid encryption: authentication, confidentiality, integrity. In: **International Conference on Computer Vision and Image Analysis Applications (ICCVIA)**. [S.l.: s.n.], 2015. p. 1–6. Citado na página 71.

BJONTEGAARD, G. Calculation of average PSNR differences between RD-curves. **ITU-T VCEG-M33**, 2001. Citado na página 69.

BLAHUT, R. E. **Fast Algorithms for Signal Processing**. [S.l.]: Cambridge University Press, 2010. ISBN 0521190495. Citado na página 18.

BRACEWELL, R. N. Discrete Hartley transform. **Journal of the Optical Society of America**, OSA, v. 73, n. 12, p. 1832–1835, December 1983. Citado 2 vezes nas páginas 18 e 91.

BRINDHA, M. Confidentiality, integrity and authentication of DICOM medical images. In: **2nd International Conference on Inventive Systems and Control (ICISC)**. [S.l.: s.n.], 2018. p. 71–75. Citado na página 71.

BULLMORE, E.; SPORNS, O. Complex brain networks: Graph theoretical analysis of structural and functional systems. **Nature Reviews Neuroscience**, v. 10, n. 3, p. 186–198, 2009. Citado na página 23.

BURTON, D. M. **Elementary Number Theory**. 7th. ed. [S.l.]: McGraw-Hill Education, 2010. Citado na página 56.

CAMPELLO DE SOUZA, M. M. et al. The discrete cosine transform over prime finite fields. In: **Telecommunications and Networking - 11th International Conference on Telecommunications (ICT 2004)**. Fortaleza, Brazil: Springer Berlin Heidelberg, 2004. p. 482–487. Citado na página 18.

CAMPELLO DE SOUZA, R. M. et al. A transformada discreta do seno em um corpo finito. In: **Anais do XXVIII Congresso Nacional de Matemática Aplicada e Computacional (CNMAC)**. [S.l.: s.n.], 2005. São Paulo, Brasil. Citado na página 18.

CAMPELLO DE SOUZA, R. M. et al. Trigonometry in finite fields and a new Hartley transform. In: **Proceedings. 1998 IEEE International Symposium on Information Theory (Cat. No.98CH36252)**. [S.l.: s.n.], 1998. p. 293. Citado 2 vezes nas páginas 18 e 55.

CAMPELLO DE SOUZA, R. M.; H. M. DE OLIVEIRA; KAUFFMAN, A. N. The complex finite field Hartley transform. In: HERTFORDSHIRE (Ed.). **Coding, Communications and Broadcasting**. [S.l.]: Research Studies Press (RSP), John Wiley, 2000. p. 267–276. Citado na página 18.

CARVALHO, M. B. et al. A 4D-DCT-based lenslet light field codec. In: **2018 25th IEEE International Conference on Image Processing (ICIP)**. [S.l.: s.n.], 2018. p. 435–439. Citado 2 vezes nas páginas 48 e 91.

CHAKRABORTY, A. et al. Application of graph theory in social media. **International Journal of Computer Sciences and Engineering**, v. 6, p. 722–729, October 2018. Citado na página 23.

CHEN, G.; MAO, Y.; CHUI, C. K. A symmetric image encryption scheme based on 3d chaotic cat maps. **Chaos, Solitons & Fractals**, v. 21, n. 3, p. 749–761, July 2004. Citado na página 77.

CHUNG, F. R. K. **Spectral Graph Theory**. [S.l.]: American Mathematical Society, 1997. Citado na página 23.

CINTRA, R. J. et al. Fragile watermarking using finite field trigonometrical transforms. **Signal Processing: Image Communication**, v. 24, p. 587–597, August 2009. Citado na página 55.

CLARK, K. et al. The cancer imaging archive (TCIA): Maintaining and operating a public information repository. **Journal of Digital Imaging**, v. 26, n. 6, p. 1045–1057, 2013. Citado na página 68.

CONTI, C.; NUNES, P.; SOARES, L. D. Light field image coding with jointly estimated self-similarity bi-prediction. **Signal Processing: Image Communication**, v. 60, p. 144–159, 2018. Citado 2 vezes nas páginas 48 e 91.

CONTI, C.; SOARES, L. D.; NUNES, P. HEVC-based 3D holoscopic video coding using self-similarity compensated prediction. **Signal Processing: Image Communication**, v. 42, p. 59–78, 2016. Citado 2 vezes nas páginas 48 e 91.

DAGADU, J. C. et al. DWT based encryption technique for medical images. In: **2016 13th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)**. [S.l.: s.n.], 2016. p. 252–255. Citado na página 72.

DAI, Y.; WANG, X. Medical image encryption based on a composition of logistic maps and Chebyshev maps. In: **2012 IEEE International Conference on Information and Automation (ICIA)**. [S.l.: s.n.], 2012. p. 210–214. Citado na página 72.

DAUBECHIES, I. The wavelet transform, time-frequency localization and signal analysis. **IEEE Transactions on Information Theory**, v. 36, n. 5, p. 961–1005, September 1990. Citado na página 18.

DE OLIVEIRA, H. M.; MIRANDA, J. P. C. L.; CAMPELLO DE SOUZA, R. M. Spread-spectrum based on finite field Fourier transforms. In: **Proceedings of the ICSECIT - International Conference on Systems Engineering**. Punta Arenas: [s.n.], 2001. v. 1. Citado na página 19.

DERI, J. A.; MOURA, J. M. F. New York city taxi analysis with graph signal processing. In: **2016 IEEE Global Conference on Signal and Information Processing (GlobalSIP)**. [S.l.: s.n.], 2016. p. 1275–1279. Citado na página 23.

DIESTEL, R. **Graph Theory**. [S.l.]: Springer, 1997. (Graduate Texts in Mathematics, 173). Citado na página 23.

EULER, L. Solutio problematis ad geometriam situs pertinentis. **Commentarii Academiae Scientiarum Imperialis Petropolitanae**, v. 8, p. 128–140, 1736. Citado na página 23.

FARAHANI, F. V.; KARWOWSKI, W.; LIGHTHALL, N. R. Application of graph theory for identifying connectivity patterns in human brain networks: A systematic review. **Frontiers in Neuroscience**, v. 13, June 2019. Citado na página 23.

FRACASTORO, G.; FOSSON, S. M.; MAGLI, E. Steerable discrete cosine transform. **IEEE Transactions on Image Processing**, v. 26, n. 1, p. 303–314, January 2017. Citado 8 vezes nas páginas 19, 20, 22, 27, 33, 35, 61 e 64.

FRACASTORO, G.; MAGLI, E. Steerable discrete Fourier transform. **IEEE Signal Processing Letters**, v. 24, n. 3, p. 319–323, March 2017. Citado 6 vezes nas páginas 19, 20, 22, 31, 33 e 57.

GATTA, M. T.; AL-LATIEF, S. T. A. Medical image security using modified chaos-based cryptography approach. **Journal of Physics: Conference Series**, IOP Publishing, v. 1003, May 2018. Citado na página 72.

GONDIM, M. A. A.; OLIVEIRA NETO, J. R. de; LIMA, J. B. Steerable Fourier number transform with application to image encryption. **Signal Processing: Image Communication**, v. 74, p. 89–95, 2019. Citado 2 vezes nas páginas 58 e 86.

GRADY, L.; POLIMENI, J. R. **Discrete Calculus - Applied Analysis on Graphs for Computational Science**. 1st. ed. [S.l.]: Springer Publishing Company, Incorporated, 2010. Citado na página 29.

GRANDO, F.; NOBLE, D.; LAMB, L. C. An analysis of centrality measures for complex and social networks. In: **IEEE Global Communications Conference (GLOBECOM)**. [S.l.: s.n.], 2016. p. 1–6. Citado na página 23.

HACKL, J.; ADEY, B. T. Estimation of traffic flow changes using networks in networks approaches. **Applied Network Science**, v. 4, n. 28, 2019. Citado na página 23.

HEIL, C.; WALNUT, D. Continuous and discrete wavelet transforms. **SIAM Review**, v. 31, p. 628–666, December 1989. Citado na página 18.

HUA, Z.; YI, S.; ZHOU, Y. Medical image encryption using high-speed scrambling and pixel adaptive diffusion. **Signal Processing**, v. 144, p. 134–144, 2018. Citado na página 72.

HUANG, X. et al. TrajGraph: A graph-based visual analytics approach to studying urban network centralities using taxi trajectory data. **IEEE Transactions on Visualization and Computer Graphics**, v. 22, n. 1, p. 160–169, January 2016. Citado na página 23.

JANSEN, S. et al. **TCIA Mouse-Mammary Collection**. [S.l.]: The Cancer Imaging Archive, 2015. <http://doi.org/10.7937/K9/TCIA.2015.9P42KSE6>. Citado na página 69.

JANSEN, S.; TERRY, V. D. **TCIA Mouse-Astrocytoma Collection**. [S.l.]: The Cancer Imaging Archive, 2015. <https://doi.org/10.7937/K9TCIA.2017.SGW7CAQW>. Citado 2 vezes nas páginas 69 e 79.

KANDHWAY, P.; BHANDARI, A. K. An optimal adaptive thresholding based sub-histogram equalization for brightness preserving image contrast enhancement. **Multidimensional Systems and Signal Processing**, v. 30, n. 4, p. 1859–1894, October 2019. Citado na página 69.

KAUR, M.; KUMAR, V. Color image encryption technique using differential evolution in non-subsampled contourlet transform domain. **IET Image Processing**, v. 12, p. 1273–1283, March 2018. Citado na página 86.

LE-PENNEC, E.; MALLAT, S. Sparse geometric image representations with bandelets. **IEEE Transactions on Image Processing**, v. 14, n. 4, p. 423–438, April 2005. Citado na página 65.

LEE, M.; CHAN, R. K.; ADJEROH, D. A. Quantization of 3D-DCT coefficients and scan order for video compression. **Journal of Visual Communication and Image Representation**, v. 8, n. 4, p. 405–422, December 1997. Citado 2 vezes nas páginas 65 e 66.

LEVOY, M.; HANRAHAN, P. Light field rendering. In: **Proceedings of the 23rd Annual Conference on Computer Graphics and Interactive Techniques**. [S.l.]: Association for Computing Machinery, 1996. (SIGGRAPH '96), p. 31–42. Citado na página 48.

LI, X. et al. Multiparametric magnetic resonance imaging for predicting pathological response after the first cycle of neoadjuvant chemotherapy in breast cancer. **Investigative Radiology**, v. 50, n. 4, p. 195–204, 2015. Citado na página 69.

LI, X. et al. **TCIA Data From QIN-Breast.** [S.l.]: The Cancer Imaging Archive, 2016. <http://doi.org/10.7937/K9/TCIA.2016.21JUebH0>. Citado na página 69.

LIMA, J. B.; CAMPELLO DE SOUZA, R. M. Finite field trigonometric transforms. **Applicable Algebra in Engineering, Communication and Computing**, v. 22, n. 5-6, p. 393–411, December 2011. Citado 3 vezes nas páginas 18, 55 e 56.

LIMA, J. B.; CAMPELLO DE SOUZA, R. M. Fractional cosine and sine transforms over finite fields. **Linear Algebra and its Applications**, v. 438, n. 8, p. 3217–3230, April 2013. Citado na página 55.

LIMA, J. B.; CAMPELLO DE SOUZA, R. M.; PANARIO, D. The eigenstructure of finite field trigonometric transforms. **Linear Algebra and its Applications**, v. 435, n. 8, p. 1956–1971, October 2011. Citado 2 vezes nas páginas 55 e 56.

LIMA, J. B.; LIMA, E. A. O.; MADEIRO, F. Image encryption based on the finite field cosine transform. **Signal Processing: Image Communication**, v. 28, n. 10, p. 1537–1547, November 2013. Citado na página 19.

LIMA, J. B.; MADEIRO, F.; SALES, F. J. R. Encryption of medical images based on the cosine number transform. **Signal Processing: Image Communication**, v. 35, p. 1–8, 2015. Citado 4 vezes nas páginas 19, 56, 72 e 86.

LIMA, J. B.; NOVAES, L. F. G. Image encryption based on the fractional Fourier transform over finite fields. **Signal Processing**, v. 94, n. 1, p. 521–530, January 2014. Citado na página 19.

LITJENS, G. et al. Computer-aided detection of prostate cancer in MRI. **IEEE Transactions on Medical Imaging**, v. 33, n. 5, p. 1083–1092, 2014. Citado na página 69.

LITJENS, G. et al. **ProstateX Challenge data**. [S.l.]: The Cancer Imaging Archive, 2017. <https://doi.org/10.7937/K9TCIA.2017.MURS5CL>. Citado na página 69.

LIU, D. et al. 3D holoscopic image coding scheme using HEVC with Gaussian process regression. **Signal Processing: Image Communication**, v. 47, p. 438–451, 2016. Citado 2 vezes nas páginas 48 e 91.

LIU, L.; MIAO, S. A new image encryption algorithm based on logistic chaotic map with varying parameter. **SpringerPlus**, v. 5, December 2016. Citado na página 84.

LIU, X.; CHEUNG, G.; WU, X. Joint denoising and contrast enhancement of images using graph Laplacian operator. In: **2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)**. [S.l.: s.n.], 2015. p. 2274–2278. Citado na página 23.

LIU, Z. et al. Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains. **Optics Communications**, v. 284, n. 1, p. 123–128, 2011. Citado na página 77.

LUCCHESI, F. R.; AREDES, N. D. **Radiology Data from The Cancer Genome Atlas Cervical Squamous Cell Carcinoma and Endocervical Adenocarcinoma TCGA-CESC collection**. [S.l.]: The Cancer Imaging Archive, 2016. <http://doi.org/10.7937/K9/TCIA.2016.SQ4M8YP4>. Citado 2 vezes nas páginas 69 e 79.

LUNG IMAGE DATABASE CONSORTIUM (LIDC). **National Cancer Institute**. <http://imaging.cancer.gov/programsandresources/InformationSystems/LIDC>. Accessed: 2020-03-27. Citado na página 87.

MA, F.; YAO, B.; YAO, M. Non-planar unclustered Peterson graphs as scale-free models of the internet of things. In: **2016 IEEE Information Technology, Networking, Electronic and Automation Control Conference (ITNEC 2016)**. [S.l.: s.n.], 2016. p. 1040–1043. Citado na página 24.

MARTUCCI, S. A. Symmetric convolution and the discrete sine and cosine transforms. **IEEE Transactions on Signal Processing**, v. 42, n. 5, p. 1038–1051, 1994. Citado na página 18.

MASERA, M. et al. A novel framework for designing directional linear transforms with application to video compression. In: **IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)**. [S.l.]: IEEE, 2019. p. 1812–1816. Citado 2 vezes nas páginas 22 e 33.

MERRI, R. Laplacian graph eigenvectors. **Linear Algebra and its Applications**, v. 278, n. 1, p. 221–236, 1998. Citado 2 vezes nas páginas 26 e 36.

MERRIS, R. Laplacian matrices of graphs: a survey. **Linear Algebra and its Applications**, v. 197, p. 143–176, 1994. Citado na página 26.

MIKHAIL, M.; ABOUELSEOUD, Y.; ELKOBROSY, G. Two-phase image encryption scheme based on FFCT and fractals. **Security and Communication Networks**, v. 2017, p. 1–13, January 2017. Citado na página 86.

MIRANDA, J. P. C. L.; DE OLIVEIRA, H. M. On Galois-division multiple access systems: Figures of merit and performance evaluation. In: **Proceedings of the 19 Brazilian Telecommunication Symposium (BTSym)**. Fortaleza, Brazil: [s.n.], 2001. Citado na página 19.

MITRA, S. K.; HE, Z. A novel linear source model and a unified rate control algorithm for H.263/MPEG-2/MPEG-4. In: **2001 IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings (Cat. No.01CH37221)**. [S.l.: s.n.], 2001. (ICASSP '01, v. 3), p. 1777–1780. Citado na página 64.

MOHAN, D. M. et al. Wavelets on graphs with application to transportation networks. In: **17th International IEEE Conference on Intelligent Transportation Systems (ITSC)**. [S.l.: s.n.], 2014. p. 1707–1712. Citado na página 23.

NEMATZADEH, H. et al. Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices. **Optics and Lasers in Engineering**, v. 110, p. 24–32, 2018. Citado na página 72.

NG, R. et al. Light field photography with a hand-held plenopic camera. **Technical Report CTSR 2005-02**, CTSR, 2005. Citado na página 48.

NORCEN, R. et al. Confidential storage and transmission of medical image data. **Computers in Biology and Medicine**, v. 33, n. 3, p. 277–292, 2003. Citado na página 71.

ORTEGA, A. et al. Graph signal processing: overview, challenges, and applications. **Proceedings of the IEEE**, v. 106, n. 5, p. 808–828, 2018. Citado na página 19.

ORTEGA, A.; RAMCHANDRAN, K. Rate-distortion methods for image and video compression. **IEEE Signal Processing Magazine**, v. 15, n. 6, p. 23–50, 1998. Citado na página 63.

PEREIRA, F. S. F.; AMO, S.; GAMA, J. Evolving centralities in temporal graphs: a twitter network analysis. In: **IEEE 17th International Conference on Mobile Data Management (MDM)**. [S.l.: s.n.], 2016. p. 43–48. Citado na página 23.

POLLARD, J. M. The fast Fourier transform in a finite field. **Mathematics of Computation**, American Mathematical Society (AMS), v. 25, n. 114, p. 365–374, May 1971. Citado na página 18.

POOR, H. V. Finite-field wavelet transforms. In: **Information Theory and Applications II: 4th Canadian Workshop Lac Delage, Québec, Canada**. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996. p. 225–238. Citado na página 18.

POULARIKAS, A. D. **Transforms and Applications Handbook**. [S.l.]: CRC Press, 2010. Citado 2 vezes nas páginas 18 e 31.

RIBEIRO, G. B.; LIMA, J. B. Fractional shift of graph signals. In: **5th IEEE Global Conference on Signal and Information Processing (GlobalSIP 2017)**. [S.l.: s.n.], 2017. Citado na página 56.

RUBINOV, M.; SPORNS, O. Complex network measures of brain connectivity: Uses and interpretations. **NeuroImage**, v. 52, n. 3, p. 1059–1069, 2010. Citado na página 23.

SALOMON, D.; MOTTA, G. **Handbook of Data Compression**. 5th. ed. [S.l.]: Springer Publishing Company, Incorporated, 2009. Citado na página 65.

SAMPLE MEDICAL IMAGES. **VIA Image and Data Management System**. Accessed: 2020–03–27. <https://veet.via.cornell.edu/cgi-bin/datac/logon.cgi>. Citado na página 87.

SANTOS, J. M. et al. Lossless coding of light field images based on minimum-rate predictors. **Journal of Visual Communication and Image Representation**, v. 54, p. 21–30, July 2018. Citado 2 vezes nas páginas 48 e 91.

SCHAFER, A. V.; OPPENHEIM, R. W. **Discrete-time Signal Processing**. 3rd. ed. [S.l.]: Prentice Hall, 2010. Citado na página 18.

SHOHAM, Y.; GERSHO, A. Efficient bit allocation for an arbitrary set of quantizers (speech coding). **IEEE Transactions on Acoustics, Speech, and Signal Processing**, v. 36, n. 9, p. 1445–1453, September 1988. Citado na página 64.

SHUAI, L.; ZHENG, W.; YANGMING, L. Using Laplacian eigenmap as heuristic information to solve nonlinear constraints defined on a graph and its application in distributed range-free localization of wireless sensor networks. **Neural Processing Letters**, v. 37, n. 3, p. 411–424, June 2013. Citado na página 23.

SHUMAN, D. I. et al. The emerging field of signal processing on graphs: extending high dimensional data analysis to networks and other irregular domains. **IEEE Signal Processing Magazine**, v. 30, n. 3, p. 83–98, May 2013. Citado 2 vezes nas páginas 19 e 24.

SPORNS, O. Graph theory methods: applications in brain networks. **Dialogues in Clinical Neuroscience**, v. 20, n. 2, p. 111–121, June 2018. Citado na página 23.

STOJANOVSKI, T.; KOCAREV, L. Chaos-based random number generators-part i: analysis [cryptography]. **IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications**, v. 48, n. 3, p. 281–288, 2001. Citado na página 84.

STOJANOVSKI, T.; PIHL, J.; KOCAREV, L. Chaos-based random number generators. part ii: practical realization. **IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications**, v. 48, n. 3, p. 382–385, 2001. Citado na página 84.

STRANG, G. The discrete cosine transform. **SIAM Review**, v. 41, n. 1, p. 135–147, March 1999. Citado 4 vezes nas páginas 18, 26, 55 e 57.

SULLIVAN, G. J.; WIEGAND, T. Rate-distortion optimization for video compression. **IEEE Signal Processing Magazine**, v. 15, n. 6, p. 74–90, November 1998. Citado 2 vezes nas páginas 63 e 65.

TANG, J. et al. A local structural descriptor for image matching via normalized graph Laplacian embedding. **IEEE Transactions on Cybernetics**, v. 46, n. 2, p. 410–420, February 2016. Citado na página 23.

TEE, G. J. Eigenvectors of block circulant and alternating circulant matrices. **New Zealand Journal of Mathematics**, v. 36, p. 195–211, 2007. Citado na página 29.

VALLIÈRES, M. et al. A radiomics model from joint FDG-PET and mri texture features for the prediction of lung metastases in soft-tissue sarcomas of the extremities. **Physics in Medicine & Biology**, v. 60, n. 14, p. 5471–5496, 2015. Citado na página 69.

WANG, Q. et al. Simultaneous encryption and compression of medical images based on optimized tensor compressed sensing with 3D Lorenz. **BioMedical Engineering OnLine**, v. 15, December 2016. Citado na página 88.

WANG, Q. et al. Joint encryption and compression of 3D images based on tensor compressive sensing with non-autonomous 3D chaotic system. **Multimedia Tools and Applications**, v. 77, January 2017. Citado na página 88.

WANG, Z. et al. Image quality assessment: from error visibility to structural similarity. **IEEE Transactions on Image Processing**, v. 13, n. 4, p. 600–612, 2004. Citado na página 68.

WU, Y.; NOONAN, J. P.; AGAIAN, S. NPCR and UACI randomness tests for image encryption. **Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications**, v. 2, p. 31–38, April 2011. Citado na página 83.

YU, Y. et al. Graph Laplacian and dictionary learning, Lagrangian method for image denoising. In: **2016 IEEE International Conference on Signal and Image Processing (ICSIP)**. [S.l.: s.n.], 2016. p. 236–240. Citado na página 23.

ZHANG, C.; FLORÊNCIO, D. Analyzing the optimality of predictive transform coding using graph-based models. **IEEE Signal Processing Letters**, v. 20, n. 1, p. 106–109, January 2013. Citado na página 26.

ZHANG, J.; MOURA, J. M. F. Diffusion in social networks as SIS epidemics: beyond full mixing and complete graphs. **IEEE Journal of Selected Topics in Signal Processing**, v. 8, n. 4, p. 537–551, August 2014. Citado na página 23.

APÊNDICE A – PROVA DO TEOREMA 4.1

A prova do Teorema é realizada em três etapas, as quais consistem, basicamente, da manipulação dos elementos $LC_{\mathrm{C}}^{(k)}(n)$, a n-ésima componente do vetor resultante do produto entre $\mathbf{L}$ e a k-ésima linha (transposta) $\mathbf{C}_{\mathbf{C}}^{(k)}$ de $\mathbf{C}_{\mathbf{C}}$, para (a) $n = 0$, (b) $n = 1, \ldots, N-2$ e (c) $n = N-1$.

(a) A componente $LC_{\mathrm{C}}^{(k)}(0)$ pode ser escrita como

$$LC_{\mathrm{C}}^{(k)}(0) = C_{\mathrm{C}}(k,0) - C_{\mathrm{C}}(k,1) = \sqrt{\frac{2}{N}}\beta_k \left[\cos_\zeta\left(2\frac{k}{2} - \frac{k}{2}\right) - \cos_\zeta\left(2\frac{k}{2} + \frac{k}{2}\right)\right].$$

Usando a fórmula para o cosseno (sobre corpos finitos) da adição de dois arcos, a última expressão pode ser reescrita como

$$LC_{\mathrm{C}}^{(k)}(0) = 4\,\mathrm{sen}_\zeta^2\left(\frac{k}{2}\right) C_{\mathrm{C}}(k,0). \tag{119}$$

(b) Para $n = 1, \ldots, N-2$, a componente $LC_{\mathrm{C}}^{(k)}(n)$ é dada por

$$\begin{aligned} LC_{\mathrm{C}}^{(k)}(n) &= -C_{\mathrm{C}}(k,n-1) + 2C_{\mathrm{C}}(k,n) - C_{\mathrm{C}}(k,n+1) \\ &= \sqrt{\frac{2}{N}}\beta_k \left[2\cos_\zeta\left(k\left(i+\frac{1}{2}\right)\right) - \cos_\zeta\left(k\left(i-1+\frac{1}{2}\right)\right)\right. \qquad (120) \\ &\qquad \left. - \cos_\zeta\left(k\left(i+1+\frac{1}{2}\right)\right)\right], \qquad (121) \end{aligned}$$

a qual, fazendo $a = k\left(n+\frac{1}{2}\right)$ e $b = k$ fornece

$$\begin{aligned} LC_{\mathrm{C}}^{(k)}(n) &= \sqrt{\frac{2}{N}}\beta_k \left[2\cos_\zeta a - \cos_\zeta(a-b) - \cos_\zeta(a+b)\right] \\ &= \sqrt{\frac{2}{N}}\beta_k \left[2\cos_\zeta a - 2\cos_\zeta a \cos_\zeta b\right]. \end{aligned}$$

Após algumas manipulações, a última equação se torna

$$LC_{\mathrm{C}}^{(k)}(n) = \sqrt{\frac{2}{N}}\beta_k 2\cos_\zeta a \left[2\,\mathrm{sen}_\zeta\frac{k}{2}\,\mathrm{sen}_\zeta\frac{k}{2}\right] = 4\,\mathrm{sen}_\zeta^2\left(\frac{k}{2}\right) C_{\mathrm{C}}(k,n). \tag{122}$$

(c) Finalmente, a componente $LC^{(k)}(N-1)$ é dada por

$$\begin{aligned} LC_{\mathrm{C}}^{(k)}(N-1) &= C_{\mathrm{C}}(k,N-1) - C_{\mathrm{C}}(k,N-2) \\ &= \sqrt{\frac{2}{N}}\beta_k \left[\cos_\zeta\left(k\left(N-1+\frac{1}{2}\right)\right) - \cos_\zeta\left(k\left(N-2+\frac{1}{2}\right)\right)\right]. \end{aligned} \tag{123}$$

Empregando a variável auxiliar $a = k\left(N-1+\frac{1}{2}\right)$, a última equação pode ser reescrita como

$$\begin{aligned} LC_{\mathrm{C}}^{(k)}(N-1) &= \sqrt{\frac{2}{N}}\beta_k \left[\cos_\zeta a - \cos_\zeta(a-k)\right] \\ &= \sqrt{\frac{2}{N}}\beta_k \left[\cos_\zeta a \underbrace{(1-\cos_\zeta k)}_{=2\,\mathrm{sen}_\zeta^2\frac{k}{2}} - \mathrm{sen}_\zeta a\,\mathrm{sen}_\zeta k\right]. \end{aligned} \tag{124}$$

Neste ponto, são consideradas algumas identidades que serão empregadas mais à frente na demonstração. Primeiramente, o cosseno e o seno cujos argumentos são múltiplos da metade da ordem de ζ são dados respectivamente por

$$\cos_\zeta\left(k\frac{\mathrm{ord}(\zeta)}{2}\right) = \frac{\zeta^{k\frac{\mathrm{ord}(\zeta)}{2}} + \zeta^{-k\frac{\mathrm{ord}(\zeta)}{2}}}{2} = (-1)^k, \tag{125}$$

$$\mathrm{sen}_\zeta\left(k\frac{\mathrm{ord}(\zeta)}{2}\right) = \frac{\zeta^{k\frac{\mathrm{ord}(\zeta)}{2}} - \zeta^{-k\frac{\mathrm{ord}(\zeta)}{2}}}{2\jmath} = 0. \tag{126}$$

Uma vez que $\mathrm{ord}(\zeta) = 2N$, tem-se $\cos_\zeta(kN) = (-1)^k$ e $\mathrm{sen}_\zeta(kN) = 0$. Isso é usado para demonstrar que as seguintes igualdades são satisfeitas:

$$\cos_\zeta a = \cos_\zeta(kN)\cos_\zeta\left(\frac{k}{2}\right), \tag{127}$$

$$\mathrm{sen}_\zeta a = -\cos_\zeta(kN)\,\mathrm{sen}_\zeta\left(\frac{k}{2}\right). \tag{128}$$

Agora, retornando à prova, substituindo (128) em (124), obtém-se

$$\begin{aligned} {LC_{\mathrm{C}}}^{(k)}(N-1) &= \sqrt{\frac{2}{N}}\beta_k\left[\cos_\zeta(a)2\,\mathrm{sen}_\zeta^2\left(\frac{k}{2}\right) + \cos_\zeta(kN)\,\mathrm{sen}_\zeta\left(\frac{k}{2}\right)\underbrace{\mathrm{sen}_\zeta\left(\frac{k}{2}+\frac{k}{2}\right)}_{=2\,\mathrm{sen}_\zeta\left(\frac{k}{2}\right)\cos_\zeta\left(\frac{k}{2}\right)}\right] \\ &= 2\,\mathrm{sen}_\zeta^2\left(\frac{k}{2}\right)\sqrt{\frac{2}{N}}\beta_k\left[\cos_\zeta(a) + \cos_\zeta(kN)\cos_\zeta\left(\frac{k}{2}\right)\right], \end{aligned}$$

e, finalmente, de (127),

$$LC_{\mathrm{C}}^{(k)}(N-1) = 2\,\mathrm{sen}_\zeta^2\left(\frac{k}{2}\right)\sqrt{\frac{2}{N}}\beta_k 2\cos_\zeta a = 4\,\mathrm{sen}_\zeta^2\left(\frac{k}{2}\right)C_{\mathrm{C}}(k, N-1). \tag{129}$$

A partir de (119), (122) e (129), segue que

$$\mathbf{LC}_{\mathbf{C}}^{(k)} = \lambda_k \mathbf{C}_{\mathbf{C}}^{(k)}, \tag{130}$$

com

$$\lambda_k = 4\,\mathrm{sen}_\zeta^2\left(\frac{k}{2}\right), \tag{131}$$

o que implica que $\mathbf{C_C}$ é uma matriz de autovetores da Laplaciana, como se queria demonstrar.