Transformada Fracional do Cosseno em Corpos Finitos

Juliano B. Lima, Ricardo M. Campello de Souza e Paulo Hugo E. S. Lima

***Resumo*— Neste artigo, é apresentada uma definição para a transformada fracional do cosseno em corpos finitos. A transformada proposta é derivada a partir do conhecimento da autoestrutura da transformada discreta do cosseno e de suas relações com a autoestrutura da transformada discreta de Fourier. Uma possível aplicação da nova transformada em cifragem de imagens é discutida.**

***Palavras-Chave*— Autovetores, corpos finitos, transformadas fracionais, transformada do cosseno.**

***Abstract*— In this paper, we present a definition for the fractional cosine transform over finite fields. The proposed transform is derived from the knowledge of the eigenstructure of the discrete cosine transform and its relations with the eigenstructure of the discrete Fourier transform. A possible application of the new transform in the field of image encryption is discussed.**

***Keywords*— Eigenvectors, finite fields, fractional transforms, cosine transform.**

I. Introdução

Transformadas fracionais têm recebido considerável atenção de pesquisadores de diferentes áreas do conhecimento. O desenvolvimento deste tema iniciou-se com a transforma fracional de Fourier (FRT), cujo cálculo pode ser visto como a rotação de um *sinal* por um ângulo arbitrário no plano tempo-frequência [1]. A partir desta intepretação, diversas definições para a FRT e para outras transformadas fracionais foram propostas [2], [3]. Essas ferramentas têm encontrado aplicações em cifragem de imagens, amostragem e filtragem de sinais, esquemas de marca d'água e de multiplexação, por exemplo [4], [5], [6].

Em vários contextos, transformadas definidas sobre corpos finitos também desempenham um importante papel. Em processamento de sinais, versões numéricas dessas transformadas são comumente usadas para calcular convoluções eficientemente [7]. Em codificação de canal, transformadas sobre corpos finitos podem ser usadas para realizar decodificação no *domínio da frequência* e para construir códigos de bloco lineares baseados em transformadas [8], [9]. Aplicações de transformadas de corpo finito em criptografia, sequências multinível para espalhamento espectral e comunicação multiusuário também são possíveis [10], [11].

Recentemente, versões em corpo finito da transformada fracional de Fourier foram propostas. Em [12], transformadas numéricas fracionais são definidas a partir de sequências de Legendre completas generalizadas. Em [13], a transformada discreta fracional de Fourier introduzida em [2], a qual é baseada num método de matriz comutante, é estendida ao cenário de corpo finito e a transformada fracional de Fourier sobre corpos finitos (GFrFT[1]) é definida. Neste artigo, a abordagem desenvolvida em [14] é utilizada para definir a transformada fracional do cosseno em corpos finitos (GFrCT). Tal definição requer o conhecimento da autoestrutura da transformada do cosseno de corpo finito, a qual foi analisada em [15]. Mais precisamente, a GFrCT proposta está relacionada à transformada do cosseno de corpo finito do tipo 1, cuja autoestrutura está fortemente ligada à autoestrutura da transformada de Fourier de corpo finito.

Juliano B. Lima, Departamento de Matemática, Centro de Ciências Exatas e da Natureza, Universidade Federal de Pernambuco, Recife, Brasil, E-mail: juliano@dmat.ufpe.br.

Ricardo M. Campello de Souza e Paulo Hugo Espírito Santo Lima, Departamento de Eletrônica e Sistemas, Centro de Tecnologia e Geociências, Universidade Federal de Pernambuco, Recife, Brasil, E-mail: ricardo@ufpe.br, paulohugos@gmail.com.

II. Preliminares

A. Trigonometria em Corpos Finitos

Nesta subseção, os principais conceitos de trigonometria em corpos finitos são revisados [16]. Neste artigo, $\mathrm{GF}(q)$ representa um corpo finito com q elementos.

Definição 1: O conjunto de inteiros Gaussianos sobre $\mathrm{GF}(p)$ é o conjunto $\mathrm{GI}(p) = \{a + jb, a, b \in \mathrm{GF}(p)\}$, em que p é um número primo tal que $j^2 \equiv -1 \pmod p$ não seja um resíduo quadrático sobre $\mathrm{GF}(p)$, i.e., $p \equiv 3 \pmod 4$.

Definição 2: O conjunto unimodular $\mathrm{GI}(p)$, denotado por G_1, é o conjunto de elementos $\zeta = (a + jb) \in \mathrm{GI}(p)$, tal que $a^2 + b^2 \equiv 1 \pmod p$.

Definição 3 (funções trigonométricas em corpos finitos): Seja ζ um elemento unimodular de $\mathrm{GI}(p)$, $p \equiv 3 \pmod 4$, com ordem multiplicativa denotada por $\mathrm{ord}(\zeta)$. As funções trigonométricas cosseno e seno em corpos finitos relacionadas a ζ são calculadas módulo p, respectivamente, por

$$\cos_\zeta(x) := \frac{\zeta^x + \zeta^{-x}}{2} \quad \text{e} \quad \sin_\zeta(x) := \frac{\zeta^x - \zeta^{-x}}{2j},$$

$x = 0, 1, \ldots, \mathrm{ord}(\zeta) - 1$.

B. Transformadas Trignométricas em Corpos Finitos

A família das transformadas trigonométricas em corpos finitos (FFTT) inclui oito tipos de transformadas do cosseno (FFCT) e oito tipos de transformadas do seno (FFST) [17]. A construção das FFTT é baseada em extensões simétricas de uma sequência (ou vetor) com elementos num corpo finito e requer a função peso β_r dada por

$$\beta_r = \begin{cases} \sqrt{2^{-1}} \pmod p, & r = 0 \text{ or } N, \\ 1, & r = 1, 2, \ldots, N-1. \end{cases}$$

[1]No acrônimo GFrFT, "G" faz alusão a "Galois field".

O parâmetro N está relacionado ao comprimento da transformada. A FFCT do tipo 1 é dada pela seguinte definição.[2]

Definição 4 (FFCT): Seja ζ um elemento unimodular de $\mathrm{GI}(p)$, com ordem multiplicativa denotada por $\mathrm{ord}(\zeta) = 2N$. A transformada do cosseno de corpo finito do vetor $\mathbf{x} = (x_i)$, $i = 0, 1, \ldots, N$, $x_i \in \mathrm{GI}(p)$, é o vetor $\mathbf{X} = (X_k)$, $k = 0, 1, \ldots, N$, $X_k \in \mathrm{GI}(p)$, de elementos

$$X_k := \sqrt{2N^{-1}} \sum_{i=0}^{N} \beta_i \beta_k x_i \mathrm{cos}_\zeta(ki). \tag{1}$$

Na Definição 4, observa-se que o comprimento da FFCT é $N+1$. Observa-se, também, que esta transformada é involutiva, isto é, sua inversa é calculada pela mesma expressão dada na definição. Em geral, a transformada de um vetor $\mathbf{x} = (x_i)$, $x_i \in \mathrm{GI}(p)$, é um vetor $\mathbf{X} = (X_k)$, $X_k \in \mathrm{GI}(p)$, obtido pela equação matricial

$$\mathbf{X} = \mathbf{x} \cdot \mathbf{M}^T. \tag{2}$$

Na Equação (2), $\mathbf{M}$ é uma matriz de transformação, a qual pode ser substituída por $\mathbf{C}$, que denota a matriz de transformação da FFCT. Mostra-se que a matriz $\mathbf{C}$ é unitária.

C. Autoestrutura da FFCT

A transformada do cosseno de corpo finito do tipo 1 e a transformada de Fourier de corpo finito (FFFT) possuem autoestruturas fortemente associadas. Com o propósito de descrever esta relação, apresenta-se inicialmente a definição da FFFT [13].

Definição 5 (FFFT): Seja ζ um elemento unimodular de $\mathrm{GI}(p)$, com ordem multiplicativa denotada $\mathrm{ord}(\zeta) = N$. A transformada de Fourier de corpo finito do vetor $\mathbf{x} = (x_i)$, $i = 0, 1, \ldots, N-1$, $x_i \in \mathrm{GI}(p)$, é o vetor $\mathbf{X} = (X_k)$, $k = 0, 1, \ldots, N-1$, $X_k \in \mathrm{GI}(p)$, de elementos

$$X_k := \sqrt{N^{-1}} \sum_{i=0}^{N-1} x_i \zeta^{-ki}. \tag{3}$$

A transformada inversa é dada por

$$x_i = \sqrt{N^{-1}} \sum_{i=0}^{N-1} X_k \zeta^{ki}. \tag{4}$$

Uma FFFT pode ser calculada pela Equação (2), com a matriz $\mathbf{M}$ substituída pela matriz $\mathbf{F}$, cujos elementos são obtidos pela Definição 5. A matriz $\mathbf{F}$ é também unitária.

As Proposições 1 e 2 fornecem informações referentes à autoestrutura da FFFT [18], [19].

Proposição 1: A matriz da FFFT possui, no máximo, quatro autovalores distintos, $\{1, -1, j, -j\}$, cujas multiplicidades são apresentadas na Tabela I.

Proposição 2: Todo autovetor associado à matriz da FFFT possui simetria par ou ímpar. Autovetores pares estão relacionados aos autovalores 1 ou -1; autovetores ímpares estão relacionados aos autovalores j ou $-j$.

Com base nos resultados apresentados, as seguintes proposições relacionadas à autoestrutura da FFCT são apresentadas [15].

[2]Como neste artigo é considerada apenas a transformada do tipo 1, deste ponto em diante, omite-se o tipo de transformada usado nos desenvolvimentos apresentados.

TABELA I: Multiplicidades dos autovalores da matriz de uma FFFT com dimensões $N \times N$.

N	Mult. 1	Mult. -1	Mult. j	Mult. $-j$
$4n$	$n+1$	n	n	$n-1$
$4n+1$	$n+1$	n	n	n
$4n+2$	$n+1$	n	$n+1$	n
$4n+3$	$n+1$	$n+1$	$n+1$	n

Proposição 3: Se $\mathbf{x} = [x_0, x_1, \ldots, x_{N-2}, x_{N-1}, x_N, x_{N-1}, x_{N-2}, \ldots, x_1]$ é um autovetor par da matriz $\mathbf{F}$, com dimensões $(2N) \times (2N)$, então

$$\hat{\mathbf{x}} = \left[x_0, \sqrt{2}x_1, \ldots, \sqrt{2}x_{N-2}, \sqrt{2}x_{N-1}, x_N\right] \tag{5}$$

é um autovetor da matriz $\mathbf{C}$, com dimensões $(N+1) \times (N+1)$, isto é, $\mathbf{C} \cdot \hat{\mathbf{x}}^T = \lambda \hat{\mathbf{x}}^T (\lambda = 1, -1)$.

Proposição 4: A matriz da FFCT possui apenas os autovalores 1 and -1. Suas multiplicidades são apresentadas na Tabela II.[3]

TABELA II: Multiplicidades dos autovalores da matriz de uma FFCT com dimensões $N' \times N'$.

N'	Mult. 1	Mult. -1
ímpar	$\frac{N'+1}{2}$	$\frac{N'-1}{2}$
par	$\frac{N'}{2}$	$\frac{N'}{2}$

III. Transformada Fracional de Fourier sobre Corpos Finitos

A transformada fracional de Fourier sobre corpos finitos (GFrFT) considerada neste artigo foi introduzida em [13]. Esta transformada é baseada na expansão espectral da matriz $\mathbf{F}$, a qual pode ser escrita como

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

Na equação acima, $\mathbf{V}$ é uma matriz cujas colunas são autovetores de $\mathbf{F}$; $\mathbf{\Lambda}$ é uma matriz diagonal cujo elemento na k-ésima linha e na k-ésima coluna é o autovalor $(-j)^k$. O autovetor na k-ésima coluna de $\mathbf{V}$, o qual é denotado por $\mathbf{v}_k$, deve estar associado ao autovalor $(-j)^k$. A matriz $\mathbf{F}^a$, em que a é um número racional, define a transformada fracional de Fourier sobre corpos finitos e pode ser escrita como

$$\mathbf{F}^a = \mathbf{V}\mathbf{\Lambda}^a\mathbf{V}^T. \tag{6}$$

Escrevendo o parâmetro a como $a = a_1/a_2$, em que a_1 e a_2 são inteiros, os possíveis valores para a, num dado corpo, dependem da existência de uma a_2-ésima raiz unimodular de $-j$. Este ponto é detalhado no Teorema 1 de [13].

O ponto-chave para escrever a expansão espectral de $\mathbf{F}$ é escolher um conjunto ortogonal de autovetores para construir $\mathbf{V}$. Uma vez que os autovalores de $\mathbf{F}$ são degenerados, são

[3]As multiplicidades dos autovalores são dadas em termos do comprimento da transformada N', em vez de N, para evitar confusão com a notação anteriormente utilizada. Dessa forma, se um elemento $\zeta \in \mathrm{GI}(p)$ com ordem multiplicativa $\mathrm{ord}(\zeta) = 2N$ é usada para construir a transformada, tem-se $N' = N + 1$, para a FFCT.

possíveis diferentes escolhas para tal conjunto. Para remover esta ambiguidade, define-se a matriz $N \times N$

$$\widetilde{\mathbf{D}} = \begin{bmatrix} \widetilde{D}_0 & 1 & 0 & \dots & 1 \\ 1 & \widetilde{D}_1 & 1 & \dots & 0 \\ 0 & 1 & \widetilde{D}_2 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \dots & \widetilde{D}_{N-1} \end{bmatrix}, \quad (7)$$

em que $\widetilde{D}_n = 2[\cos_\zeta(n) - 2]$ e $\zeta \in \mathrm{GI}(p)$ tem ordem multiplicativa $\mathrm{ord}(\zeta) = N$. As matrizes $\mathbf{D}$ e $\mathbf{F}$ comutam, o que significa que elas possuem um conjunto de autovetores em comum [20]. Portanto, o que se tem a fazer é encontrar os autovetores de $\widetilde{\mathbf{D}}$. Para isso, emprega-se a matriz

$$\mathbf{P} = \sqrt{2^{-1}} \left[\begin{array}{c|ccc|c|ccc} \sqrt{2} & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \hline 0 & 1 & & & 0 & & & 1 \\ \vdots & & \ddots & & \vdots & & \iddots & \\ 0 & & & 1 & 0 & 1 & & \\ \hline 0 & 0 & \cdots & 0 & \sqrt{2} & 0 & \cdots & 0 \\ \hline 0 & & & 1 & 0 & -1 & & \\ \vdots & & \iddots & & \vdots & & \ddots & \\ 0 & 1 & & & 0 & & & -1 \end{array}\right], \quad (8)$$

a qual satisfaz $\mathbf{P} = \mathbf{P}^T = \mathbf{P}^{-1}$. A transformação de similaridade

$$\mathbf{P}\widetilde{\mathbf{D}}\mathbf{P}^{-1} = \begin{bmatrix} \mathbf{Ev} & 0 \\ 0 & \mathbf{Od} \end{bmatrix} \quad (9)$$

produz as matrizes tridiagonais simétricas $\mathbf{Ev}$ e $\mathbf{Od}$ com dimensões $\left\lfloor \frac{N}{2} \right\rfloor + 1$ e $\left\lfloor \frac{N-1}{2} \right\rfloor$ respectivamente (o símbolo $\lfloor \cdot \rfloor$ denota a parte inteira do argumento).

O conjunto ortogonal de autovetores pares e ímpares de $\widetilde{\mathbf{D}}$ é único porque, também em corpos finitos, matrizes tridiagonais possuem todos os autovalores distintos [21, p. 134]. Especificamente, os autovetores pares de $\widetilde{\mathbf{D}}$ são obtidos por

$$\mathbf{u}_{2k} = \mathbf{P}\left[\mathbf{e}_k^T \mid 0 \dots 0\right]^T, k = 0, \dots, \left\lfloor \frac{N}{2} \right\rfloor, \quad (10)$$

em que $\mathbf{e}_k$ é um autovetor de $\mathbf{Ev}$; os autovetores ímpares de $\widetilde{\mathbf{D}}$ são obtidos por

$$\mathbf{u}_{2k+1} = \mathbf{P}\left[0 \dots 0 \mid \mathbf{o}_k^T\right]^T, k = 0, \dots, \left\lfloor \frac{N-3}{2} \right\rfloor, \quad (11)$$

em que $\mathbf{o}_k$ é um autovetor de $\mathbf{Od}$. Se N for par, o vetor $\mathbf{u}_{N-1}$ é nulo. Os autovetores $\mathbf{v}_k$, $k = 0, 1, \dots, 2\lfloor N/2 \rfloor$, a serem usados como colunas de $\mathbf{V}$ correspondem aos autovetores $\mathbf{u}_k$, $k = 0, 1, \dots, 2\lfloor N/2 \rfloor$, ordenados de maneira que o autovetor $\mathbf{v}_k$ esteja relacionado ao autovalor $(-j)^k$, conforme foi observado previamente.

Com isso, a Equação (6) pode ser escrita com mais detalhes. O elemento da m-ésima linha e na n-ésima coluna de $\mathbf{F}^a$ é calculado por

$$\mathbf{F}^a_{m,n} = \sum_{\substack{k=0 \\ (\|\mathbf{v}_k\| \neq 0)}}^{2\lfloor N/2 \rfloor} \|\mathbf{v}_k\|^{-2} v_{k,m} (-j)^{ka} v_{k,n}, \quad (12)$$

para $m, n = 0, \dots, N-1$; $\mathbf{v}_k$, $\|\mathbf{v}_k\| \neq 0$, é um autovetor de $\widetilde{\mathbf{D}}$ relacionado ao autovalor $(-j)^k$; $\|\mathbf{v}_k\|$ é a norma do vetor $\mathbf{v}_k = (v_{k,i})$, $i = 0, \dots, N-1$, $v_{k,i} \in \mathrm{GI}(p)$, a qual é definida por

$$\|\mathbf{v}_k\| = \sqrt{v_{k,0}^2 + v_{k,1}^2 + \dots + v_{k,N-1}^2} \,(\mathrm{mod}\ p).$$

O termo $\|\mathbf{v}_k\|$ é incluído na Equação (12), de modo a tornar unitária a matriz $\mathbf{F}^a$. Em [13], diversos exemplos da GFrFT são apresentados.

IV. GFrCT: Definição e Aplicação

Nesta seção, os resultados apresentados nas Seções II e III são usados para definir a transformada fracional do cosseno em corpos finitos. A ideia é semelhante à usada para definir a GFrFT e emprega uma expansão espectral da matriz $\mathbf{C}$. A matriz da GFrCT é escrita como

$$\mathbf{C}^a = \widetilde{\mathbf{V}}\widetilde{\mathbf{\Lambda}}^a\widetilde{\mathbf{V}}^T. \quad (13)$$

Na equação acima, o parâmetro a é racional e $\widetilde{\mathbf{V}}$ é uma matriz cujas colunas são autovetores de $\mathbf{C}$; $\widetilde{\mathbf{\Lambda}}$ é uma matriz diagonal cujo elemento na k-ésima linha e na k-ésima coluna é o autovalor $(-1)^k$; isso se deve ao resultado da Proposição 4. O autovetor na k-ésima coluna da matriz $\widetilde{\mathbf{V}}$ deve estar associado ao autovalor $(-1)^k$ da matriz $\mathbf{C}$.

Uma vez que os autovalores de $\mathbf{C}$ também são degenerados, a escolha dos autovetores a serem usados na construção de $\widetilde{\mathbf{V}}$ deve seguir passos similares àqueles usados na construção da GFrFT. Mais precisamente, os autovetores $\tilde{\mathbf{v}}$ usados para construir a matriz $\widetilde{\mathbf{V}}$, com dimensões $(N+1) \times (N+1)$, são derivados dos autovetores $\mathbf{v}$ da matriz $\mathbf{F}$, com dimensões $(2N) \times (2N)$, associados aos autovalores $\lambda = \pm 1$ e obtidos por meio do método descrito na Seção III. A relação entre $\mathbf{v}$ e $\tilde{\mathbf{v}}$ é dada pela Proposição 3. Observando que o procedimento para construir os autovetores $\tilde{\mathbf{v}}$ a partir dos autovetores $\mathbf{v}$ *cancela* as operações com os vetores $\mathbf{e}_k$ na Equação (10), isto é, o preenchimento com zeros e a multiplicação pela matriz $\mathbf{P}$, verifica-se que os vetores $\mathbf{e}_k$ podem ser diretamente tomados como os autovetores $\tilde{\mathbf{v}}_k$.

O procedimento descrito funciona porque a ortogonalidade entre $\mathbf{v}_m$ e $\mathbf{v}_n$, $m \neq n$, os quais são ambos autovetores pares de $\mathbf{F}$, implica na ortogonalidade entre os autovetores correspondentes da matriz $\mathbf{C}$, ou seja, $\tilde{\mathbf{v}}_m$ e $\tilde{\mathbf{v}}_n$. Isso pode ser concluído com base na regra para construção dos autovetores $\tilde{\mathbf{v}}$ a partir dos autovetores $\mathbf{v}$ (vide Proposição 3). Após ajustar a Equação (13) incluindo os termos de normalização $\|\tilde{\mathbf{v}}_k\|$, pode-se calcular o elemento na m-ésima linha e na n-ésima coluna de $\mathbf{C}^a$ por

$$\mathbf{C}^a_{m,n} = \sum_{k=0}^{N} \|\tilde{\mathbf{v}}_k\|^{-2} \tilde{v}_{k,m} (-1)^{ka} \tilde{v}_{k,n}, \quad (14)$$

para $m, n = 0, \dots, N$.

De modo semelhante à GFrFT, se o parâmetro a for escrito como $a = a_1/a_2$, em que a_1 e a_2 são inteiros, os possíveis valores de a dependem da existência de uma a_2-ésima raiz de -1. Mais especificamente, o elemento $(-1)^{1/a_2} = \sqrt[a_2]{-1} \in \mathrm{G}_1$ se, e somente se, $2a_2 | (p+1)$. Este resultado pode ser demonstrado seguindo passos análogos aos empregados na prova do Teorema 1 de [13]; a_1 pode ser qualquer número inteiro.

Adicionalmente, uma vez que a FFCT é uma involução, a relação

$$\mathbf{C}^{a} = \mathbf{C}^{a+2}$$

é válida. Isso corresponde à propriedade de periodicidade da GFrCT. Em geral, a relação

$$\mathbf{C}^{a'}\mathbf{C}^{a''} = \mathbf{C}^{a'+a''}$$

também é válida e corresponde à propriedade de adição de *ângulo*. Devido aos termos de normalização incluídos na Equação (14), a matriz $\mathbf{C}^{a}$ é unitária. Na Tabela III, os passos necessários para a construção desta matriz são apresentados de forma sucinta. A seguir, é desenvolvido um pequeno exemplo numérico da GFrCT e sugerida uma aplicação desta ferramenta na cifragem de imagens digitais

A. Exemplo

Neste exemplo, constrói-se uma GFrCT utilizando o elemento unimodular $\zeta = 24+6j$, o qual possui ordem multiplicativa $2N = 6$ em $\mathrm{GI}(47)$. A partir da Equação (7), obtém-se

$$\widetilde{\mathbf{D}} = \begin{bmatrix} 45 & 1 & 0 & 0 & 0 & 1 \\ 1 & 44 & 1 & 0 & 0 & 0 \\ 0 & 1 & 42 & 1 & 0 & 0 \\ 0 & 0 & 1 & 41 & 1 & 0 \\ 0 & 0 & 0 & 1 & 42 & 1 \\ 1 & 0 & 0 & 0 & 1 & 44 \end{bmatrix}.$$

Seguindo o procedimento descrito na Tabela III, a matriz

$$\mathbf{P} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 27 & 0 & 0 & 0 & 27 \\ 0 & 0 & 27 & 0 & 27 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 27 & 0 & 20 & 0 \\ 0 & 27 & 0 & 0 & 0 & 20 \end{bmatrix}$$

é construída e, a partir da transformação de similaridade $\mathbf{PSP}^{-1}$, a matriz

$$\mathbf{Ev} = \begin{bmatrix} 45 & 7 & 0 & 0 \\ 7 & 44 & 1 & 0 \\ 0 & 1 & 42 & 7 \\ 0 & 0 & 7 & 41 \end{bmatrix}$$

é obtida. Os autovalores de $\mathbf{Ev}$ são $\{2, 12, 27, 37\}$. Os autovetores $\mathbf{e}_k = \tilde{\mathbf{v}}_k$, $k = 0, 1, 2, 3$, de $\mathbf{Ev}$, correspondentes aos autovetores da matriz $\mathbf{C}$ que se deseja fracionalizar, são apresentados na Tabela IV. Utilizando, por exemplo, $a = 1/2$, a matriz da GFrCT

$$\mathbf{C}^{1/2} = \begin{bmatrix} 21+24j & 21+37j & 31+5j & 16+16j \\ 21+37j & 9+6j & 46+46j & 42+16j \\ 31+5j & 46+46j & 41+38j & 37+21j \\ 16+16j & 42+16j & 37+21j & 23+26j \end{bmatrix}$$

é obtida.

TABELA IV: Autovetores da matriz tridiagonal $\mathbf{Ev}$ ($p = 47$, $\zeta = 24+6j$, $2N = 6$).

k	$\mathbf{e}_k$
0	[1 14 16 14]
1	[1 2 23 22]
2	[1 31 30 32]
3	[1 19 1 10]

B. Aplicação em Cifragem de Imagens

Ferramentas matemáticas definidas sobre corpos finitos são comumente empregadas em técnicas relacionadas à segurança de informação. Quando se trata de imagens digitais, recebem destaque as técnicas de marca d'água, esteganografia e cifragem. O objetivo desta última técnica é *embaralhar* e transformar os *pixels* de uma imagem, a fim de que as suas propriedades estatísticas e o seu aspecto visual originais sejam modificados. Para isso, são normalmente empregados procedimentos que dependem de uma chave secreta.

Em [22], foi proposta uma técnica para formatação de histogramas de imagens digitais baseada na transformada do cosseno em corpos finitos. Entretanto, por si só, o procedimento não produz uma imagem cifrada, uma vez que não são empregadas chaves. Utilizando a transformada fracional do cosseno em corpos finitos, é possível atrelar uma chave secreta à técnica proposta. A sugestão é empregar como chave o vetor de números inteiros

$$\mathbf{a} = \begin{bmatrix} a_1 & a_2 & \dots & a_n \end{bmatrix}.$$

O i-ésimo bloco da imagem a ser cifrada seria, então, processado pela matriz de transformação $\mathbf{C}^{1/a_i}$. O procedimento de cifragem completo é ilustrado na Figura 1.

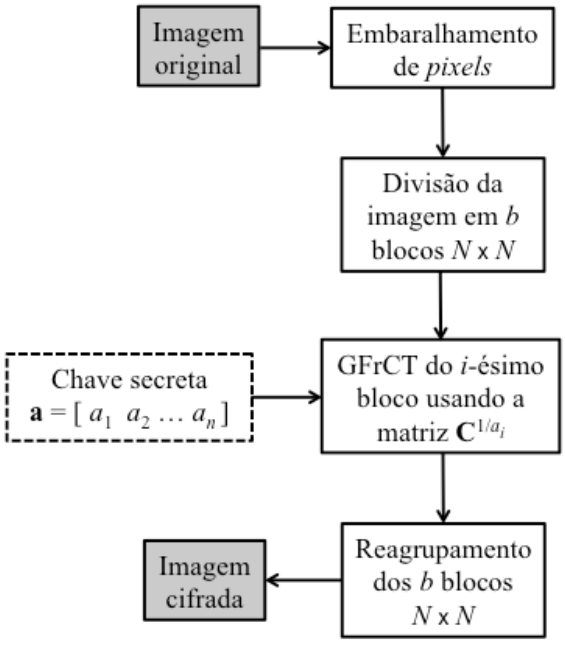

Fig. 1: Diagrama de blocos da técnica de cifragem de imagens baseada na GFrCT proposta.

TABELA III: Construção da matriz de uma GFrCT com dimensões $(N+1) \times (N+1)$.

1.	Dado um número primo p, escolha um elemento unidomular $\zeta \in \mathrm{GI}(p)$, tal que $\mathrm{ord}(\zeta) = 2N$;
2.	Construa a matriz $\widetilde{\mathbf{D}}$ de acordo com a Equação (7);
3.	Construa a matriz $\mathbf{P}$ de acordo com a Equação (8);
4.	Obtenha a matriz $\mathbf{Ev}$ a partir da Equação (9), e calcule seus autovalores;
5.	Calcule $\mathbf{e}_k$, os autovetores de $\mathbf{Ev}$;
6.	Use os vetores $\mathbf{e}_k$ como os autovetores $\tilde{\mathbf{v}}_k$ da matriz $\mathbf{C}$ (o autovetor $\tilde{\mathbf{v}}_k$ deve estar associado ao autovalor $(-1)^k$);
7.	Escolha o parâmetro a e construa a matriz $\mathbf{C}^a$ de acordo com a Equação (14).

Na Figura 1, a imagem original é inicialmente submetida a um embaralhamento de *pixels*, que pode ser realizado, por exemplo, pela transformada de Arnold [23]. O objetivo deste procedimento é diminuir a correlação entre cada *pixel* e seus vizinhos. Em seguida, a imagem é dividida regularmente em b blocos com dimensões $N \times N$; estas são as dimensões da matriz da transformada que será posteriormente empregada. Na etapa seguinte, os blocos são selecionados numa sequência previamente definida (da esquerda para a direita e de cima para baixo, por exemplo) e sua GFrCT é calculada; o i-ésimo bloco é submetido ao cálculo da GFrCT cuja matriz é $\mathbf{C}^{1/a_i}$, em que a_i é obtido da chave secreta $\mathbf{a}$. Finalmente, os blocos são reagrupados e a imagem cifrada é construída.

A decifragem é realizada empregando, de forma invertida, os mesmos passos da cifragem. Como não se faz arredondamento em nenhuma das etapas envolvidas na técnica proposta, a imagem recuperada coincide exatamente com a imagem original. A implementação efetiva deste método de cifragem requer a consideração de diversos aspectos práticos que fogem ao escopo do presente trabalho e, atualmente, encontra-se em desenvolvimento.

V. Conclusões

Neste artigo, foi introduzida uma definição para a transformada fracional do cosseno em corpos finitos. As propriedades da GFrCT e seus possíveis cenários de aplicação foram investigados. De modo particular, foram investigados aspectos práticos envolvidos na implementação do método de cifragem proposto. Isso inclui a definição da GFrCT sobre um corpo adequado ao processamento das imagens a serem cifradas, a especificação do comprimento da chave secreta empregada e a avaliação da resistência do método a ataques criptográficos. Por fim, observa-se que uma transformada fracional do seno em corpo finito (GFrST) pode ser definida utilizando passos semelhantes aos utilizados para definir a GFrCT.

Agradecimentos

O desenvolvimento deste trabalho foi apoiado pela Fundação de Amparo à Ciência e Tecnologia de Pernambuco (FACEPE), com recursos do processo APQ 1196-3.04/10.

Referências

[1] L. B. Almeida, "The fractional Fourier transform and time-frequency representations," *IEEE Transactions on Signal Processing*, vol. 42, no. 11, pp. 3084–3091, November 1994.

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

[3] G. Cariolaro, T. Erseghe, and P. Kraniauskas, "The fractional discrete cosine transform," *IEEE Trans. on Signal Processing*, vol. 50, no. 4, pp. 902–911, April 2002.

[4] R. Tao, X.-Y. Meng, and Y. Wang, "Image encryption with multiorders of fractional Fourier transforms," *IEEE Transactions on Information Security and Forensics*, vol. 5, no. 4, pp. 734–738, December 2010.

[5] R. Tao, X.-Y. Meng, and Y. Wang, "Transform order division multiplexing," *IEEE Transactions on Signal Processing*, vol. 59, no. 2, pp. 598–609, February 2011.

[6] M. Fan and H. Wang, "Chaos-based discrete fractional sine transform domain audio watermarking scheme," *Computers & Electrical Engineering*, vol. 35, no. 3, pp. 506–516, May 2009.

[7] I. S. Reed and T. K. Truong, "The use of finite fields to compute convolutions," *IEEE Trans. on Information Theory*, vol. 21, no. 2, pp. 208–213, March 1975.

[8] R. E. Blahut, *Algebraic Codes for Data Transmission*, Cambridge University Press, 1st edition, 2003.

[9] R. M. Campello de Souza, E. S. V. Freire, and H. M. de Oliveira, "Fourier codes," in *Proc. of the tenth International Symposium on Communication Theory and Applications*, pp. 370–375. Ambleside, UK, 2009.

[10] K. S. Chan and F. Fekri, "A block cipher cryptosystem using wavelet transforms over finite fields," *IEEE Trans. on Signal Processing*, vol. 52, no. 10, pp. 2975–2991, October 2004.

[11] H. M. de Oliveira and R. M. Campello de Souza, "Orthogonal multilevel spreading sequence design," in *Coding, Communications and Broadcasting*, P. G. Farnell, M. Darnell, and B. Honary, Eds., pp. 291–303. Research Studies Press, Jonh Wiley, Hertfordshire, 1st edition, 2000.

[12] S.-C. Pei, C.-C. Wen, and J. J. Ding, "Closed form orthogonal number theoretic transform eigenvectors and the fast fractional NTT," *IEEE Trans. on Signal Processing*, vol. 59, no. 5, pp. 2124–2135, May 2011.

[13] J. B. Lima and R. M. Campello de Souza, "The fractional Fourier transform over finite fields," *Signal Processing*, vol. 92, no. 2, pp. 465–476, February 2012.

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

[15] J. B. Lima, R. M. Campello de Souza, and D. Panario, "The eigenstructure of finite field trigonometric transforms," *Linear Algebra Appl.*, vol. 435, no. 8, pp. 1956–1971, October 2011.

[16] R. M. Campello de Souza, H. M. de Oliveira, A.N. Kauffman, and A. J. A. Paschoal, "Trigonometry in finite fields and a new Hartley transform," in *Proc. IEEE Int. Symp. Information Theory*, p. 293. 1998.

[17] J. B. Lima and R. M. Campello de Souza, "Finite field trigonometric transforms," *Applicable Algebra in Engineering, Communication and Computing*, vol. 22, no. 5-6, pp. 393–411, December 2011.

[18] D. T. Birtwistle, "The eigenstructure of the number theoretic transforms," *Signal Processing*, vol. 4, no. 4, pp. 287–294, July 1982.

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

[20] J. H. Wilkinson, *The Algebraic Eigenvalue Problem*, Oxford University Press, 1st edition, 1988.

[21] B. N. Parlett, *The Symmetric Eigenvalue Problem*, Society for Industrial and Applied Mathematics, 1998.

[22] J. B. Lima and R. M. Campello de Souza, "Formatação de histogramas para cifragem de imagens digitais," in *Anais do XXIX Simpósio Brasileiro de Telecomunicações*. Curitiba, Brasil, 2011.

[23] Z. H. Guan, F. J. Huang, and W. J. Guan, "Chaos-based image encryption," *Physics Letters A*, vol. 346, no. 1-3, pp. 153–157, 2005.