Cifragem de Imagens Baseada na Transformada Fracional de Fourier sobre Corpos Finitos

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

***Resumo*— Neste artigo, a transformada fracional de Fourier sobre corpos finitos (GFrFT) baseada em funções de matrizes é usada no projeto de um esquema de cifragem de imagens. A abordagem é mais simples que a baseada na construção de conjuntos de autovetores, e assim permite o desenvolvimento de sistemas de menor custo computacional. O esquema é um cifrador de bloco de chave secreta, que usa uma arquitetura de confusão-difusão e a GFrFT para a cifragem de imagens. Simulações são realizadas para avaliar aspectos de segurança da informação. Uma análise teórica e métricas de segurança são usadas para verificar o desempenho do esquema em aspectos de segurança.**

***Palavras-Chave*— Transformada fracional de Fourier sobre corpos finitos; cifragem de imagens.**

***Abstract*— The fractional Fourier transform over finite fields (GFrFT) based on the matrix function approach is used to design an image encryption scheme. The approach is simpler than the approach based on the construction of an eigenvector set, therefore allowing lower-cost computation systems. The scheme is a secret-key block cipher, that uses a confusion-diffusion architecture and the GFrFT for image encryption. Computer simulations are performed in order to analyze security aspects. A theoretical analysis and security metrics are used to evaluate the scheme security.**

***Keywords*— Fractional Fourier transforms Finite fields; Image encryption.**

I. Introdução

A transformada fracional de Fourier (FrFT, *fractional Fourier transform*) vem se consolidando como uma importante ferramenta matemática em diversas áreas do conhecimento. A FrFT pode ser interpretada como uma rotação no plano tempo-frequência por um ângulo arbitrário [1]. O conceito de transformada fracional se refere à generalização do operador transformada clássica, em que potências fracionais (reais) do operador são permitidas.

A transformada discreta fracional de Fourier (DFrFT, *discrete fractional Fourier transform*) foi definida por duas abordagens. Na primeira, é usada a teoria de funções de matrizes para se calcular potências não inteiras da matriz da DFT [2]. Na segunda, a DFrFT é obtida utilizando a expansão espectral da matriz da DFT,

$$\mathbf{F} = \mathbf{V}\mathbf{\Lambda}\mathbf{V}^t, \tag{1}$$

em que $\mathbf{V}$ é uma matriz cujas colunas são autovetores de $\mathbf{F}$ e $\mathbf{\Lambda}$ é uma matriz diagonal em que os elementos não nulos são autovalores de $\mathbf{F}$. Para se obter a matriz da DFrFT, computa-se potências fracionais de $\mathbf{\Lambda}$. Os autovetores de $\mathbf{F}$ que preenchem a matriz $\mathbf{\Lambda}$ são obtidos, por exemplo, por meio de sequências generalizadas completas de Legendre [3] ou de matrizes comutantes [4].

As transformadas definidas em corpos finitos não envolvem truncagem ou arredondamento e possibilitam o uso de estratégias que diminuem sua complexidade aritmética. Em função disso, essas transformadas têm sido empregadas no cálculo rápido de convoluções e noutras aplicações de processamento digital de sinais [5]. Nos últimos anos, foram introduzidas transformadas fracionais de Fourier sobre corpos finitos (GFrFT, *Galois field fractional Fourier transform*) baseadas na expansão espectral de $\mathbf{F}$ [3], [4] e em funções de matrizes [6], [7]. Essas transformadas têm sido utilizadas em esquemas de cifragem de imagens como aquele proposto por Lima [8]; nesse esquema, que emprega a GFrFT proposta em [4], o parâmetro fracional usado na transformação de cada bloco da imagem é obtido de uma chave secreta.

Neste trabalho, é apresentado um novo esquema para cifragem de imagens baseado na GFrFT proposta em [6]. Na Seção II são revisados alguns conceitos relacionados a GFrFT. Na Seção III é descrito o esquema de cifragem de imagens proposto, o qual é avaliado sob algumas métricas de segurança de informação na Seção IV. Na Seção V, são apresentadas as considerações finais do trabalho.

II. Preliminares

A. A transformada de Fourier sobre corpos finitos

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 j^2 não é um resíduo quadrático sobre $\mathrm{GF}(p)$.

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

Definição 3: Seja $\zeta \in \mathrm{GI}(p)$ um elemento de ordem multiplicativa denotada por $\mathrm{ord}(\zeta) = N$. As funções cosseno e seno sobre $\mathrm{GI}(p)$ relacionadas a ζ são, respectivamente, dadas por

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

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

Definição 4: Seja $\zeta \in \mathrm{GF}(p^m)$ um elemento unimodular de ordem multiplicativa $\mathrm{ord}(\zeta) = N$. A transformada de Fourier sobre corpos finitos (FFFT, *finite fields Fourier transform*) do vetor $\mathbf{x} = (x[i])$, $x[i] \in \mathrm{GF}(p)$, de comprimento N, é o vetor $\mathbf{X} = (X[k])$, $X[k] \in \mathrm{GF}(p^m)$, em que

$$X[k] := \sqrt{N^{-1}} \sum_{i=0}^{N-1} x[i]\zeta^{ki}, \quad k = 0, 1, \ldots, N-1. \tag{3}$$

Departamento de Eletrônica e Sistemas, Universidade Federal de Pernambuco, Recife-PE, Brasil, E-mails: paulohugos@gmail.com, juliano_bandeira@ieee.org, ricardo@ufpe.br.

A expressão (3) pode ser escrita na forma matricial como $\mathbf{X} = \mathbf{Fx}$, em que $[\mathbf{F}]_{i,k} = \sqrt{N^{-1}}\zeta^{ki}$ é A matriz de transformação da FFFT.

Proposição 1: A matriz $\mathbf{F}$ tem, no máximo, quatro autovalores distintos, $\left\{\pm 1, \pm\sqrt{-1}\right\}$, cujas multiplicidades podem ser encontradas em [6], [9].

B. A transformada fracional de Fourier sobre corpos finitos

Em linhas gerais, para definir uma transformada fracional, é necessário computar uma potência não inteira da matriz de transformação. Assim, pode-se empregar a teoria de funções de matrizes [10][11], usando a função $f(t) = t^a$, com a racional, para obter $\mathbf{F}^a$; utiliza-se um polinômio de interpolação $r(t)$ para substituir a função $f(t) = t^a$ definida para escalares. Desde que os autovalores da matriz $\mathbf{A}$ tenham a mesma imagem na função $f(\cdot)$ e no polinômio de interpolação $r(t)$, a substituição pode ser realizada [10, pp. 5].

A matriz da FFFT possui quatro autovalores distintos, de forma que a expressão do polinômio interpolador para calcular $\mathbf{F}^a$, como pode ser visto em [7], é

$$r(t) = l_1(t) + (\sqrt{-1})^{\,a} l_2(t) + (-1)^{\,a} l_3(t) + (-\sqrt{-1})^a l_4(t),$$

em que

$$\begin{array}{ll} l_1(t) = \frac{t^3+t^2+t+1}{4}, & l_2(t) = \frac{\sqrt{-1}\,t^3-t^2-\sqrt{-1}\,t+1}{4}, \\ l_3(t) = \frac{-t^3+t^2-t+1}{4}, & l_4(t) = \frac{-\sqrt{-1}\,t^3-t^2+\sqrt{-1}\,t+1}{4}. \end{array} \quad (4)$$

Substituindo t por $\mathbf{F}$ na expressão do polinômio interpolador, mostra-se que a matriz de transformação da GFrFT com parâmetro fracional $a = (a_1/a_2)$ é

$$\mathbf{F}^a = r(\mathbf{F}) = \alpha_0(a)\mathbf{I} + \alpha_1(a)\mathbf{F} + \alpha_2(a)\mathbf{F}^2 + \alpha_3(a)\mathbf{F}^3, \quad (5)$$

em que

$$\begin{aligned} \alpha_0(a_1,a_2) &= \frac{1+(\sqrt[2a_2]{-1})^{a_1}}{2}\cos_{\,\sqrt[2a_2]{-1}}(a_1), \\ \alpha_1(a_1,a_2) &= \frac{1-\sqrt{-1}(\sqrt[2a_2]{-1})^{a_1}}{2}\sin_{\,\sqrt[2a_2]{-1}}(a_1), \\ \alpha_2(a_1,a_2) &= \frac{-1+(\sqrt[2a_2]{-1})^{a_1}}{2}\cos_{\,\sqrt[2a_2]{-1}}(a_1), \text{ e} \\ \alpha_3(a_1,a_2) &= \frac{-1-\sqrt{-1}(\sqrt[2a_2]{-1})^{a_1}}{2}\sin_{\,\sqrt[2a_2]{-1}}(a_1). \end{aligned}$$

III. ESQUEMA DE CIFRAGEM DE IMAGENS

A Figura 1 apresenta um diagrama em blocos do esquema de cifragem que envolve cinco estágios: (I) embaralhamento, (II) formação de $\mathbf{Bq}$, bloco a ser cifrado, (III) seleção dos elementos da chave, (IV) expansão da chave e (V) aplicação da GFrFT. Resumidamente, a imagem é dividida em blocos de dimensão 8×8, que são combinados entre si e com elementos da chave secreta, e ao bloco resultante é aplicada a GFrFT de parâmetro fracional a. O parâmetro a varia a cada bloco, sendo determinado por alguns elementos da chave secreta.

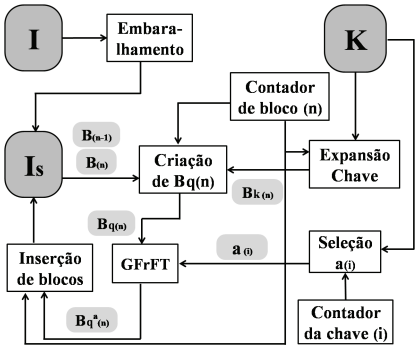

Fig. 1. Diagrama em blocos do esquema de cifragem de imagens no domínio fracional usando a GFrFT.

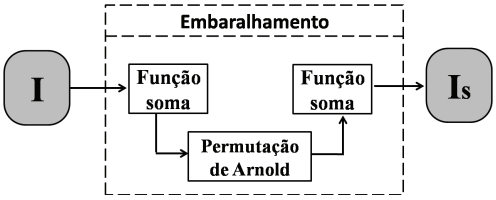

Fig. 2. Diagrama em blocos do estágio de embaralhamento.

1) Estágio (I): Em imagens digitais os *pixels* de certas regiões apresentam alta correlação. Com o intuito de diminuir esta correlação, inicialmente é realizado um embaralhamento nos *pixels* da imagem original $\mathbf{I}$, resultando na imagem $\mathbf{Is}$. Esta é uma das estratégias para prover difusão [12] ao esquema, com o propósito de dificultar a criptoanálise diferencial [13, p. 89]. Esse estágio é subdividido na etapa de *Soma* e na etapa de *Permutação*, conforme se observa na Figura 2.

Na etapa de *Soma*, percorrendo-se as linhas, o n-ésimo *pixel* é substituído por sua soma com o $(n-1)$-ésimo *pixel*, sendo o 0-ésimo *pixel* definido como zero. Na etapa de *Permutação* é usado o algoritmo de Arnold [14], o qual provê uma distribuição uniforme de energia da imagem. A etapa de *Soma* ocorre mais uma vez, percorrendo agora as colunas da imagem, de forma que a alteração de um único *pixel* modifique todos os *pixels* da imagem. Como os *pixels* são codificados a 8 *bpp* (intervalo de 0 a 255), a adição é módulo 256.

2) Estágio (II): A imagem embaralhada, $\mathbf{Is}$, é dividida em blocos $\mathbf{B}_n$, $n = \{1, 2, \ldots, N\}$, de dimensão 8×8. Pode-se prover difusão ao sistema com sobreposições entre os blocos conforme a proposta apresentada em [15], porém isso eleva a complexidade aritmética, uma vez que um número maior de blocos seria processado.

Na Figura 3, é apresentado o esquema de formação do n-ésimo bloco $\mathbf{Bq}$, ao qual é efetivamente aplicada a GFrFT. A partir de $\mathbf{K}$ são formados dois blocos $\mathbf{Bk}$ e $\mathbf{Bk}'$, através dos quais é inserido confusão ao esquema. Esses blocos têm dimensão 8×8 e elementos codificados a 8 *bits*, e sua construção é detalhada no estágio (IV) que trata da expansão da chave.

As Equações (6) e (7) descrevem a combinação feita entre os blocos selecionados:

$$\mathbf{Bq}'_n = (\mathbf{B}_n \oplus \mathbf{B}_{n-1}) + \mathbf{Bk}_n \pmod{256}, \quad (6)$$

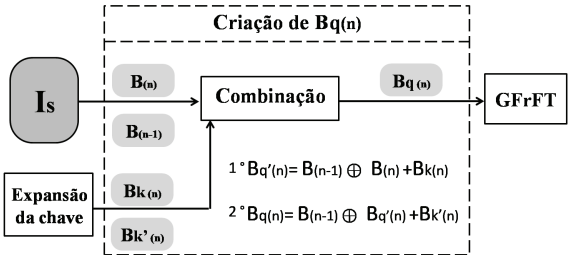

Fig. 3. Diagrama em blocos do esquema de formação de $\mathbf{Bq}_n$.

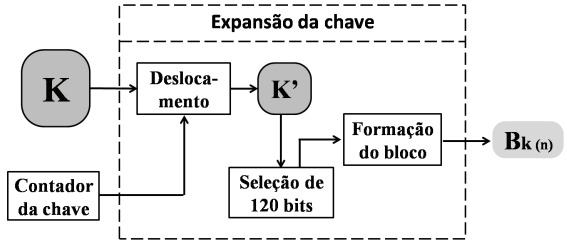

Fig. 4. Diagrama em blocos da expansão da chave para formação de $\mathbf{Bk}_n$.

$$\mathbf{Bq}_n \quad = \quad (\mathbf{Bq}'_n \oplus \mathbf{B}_{n-1}) + \mathbf{Bk}'_n \pmod{256}, \qquad (7)$$

em que $\oplus$ denota a operação XOR (ou-exclusivo binária).

Na Equação (6), com os blocos $\mathbf{B}_n$, $\mathbf{B}_{n-1}$ e $\mathbf{Bk}_n$ é construído o bloco $\mathbf{Bq}'(n)$. Observe que $\mathbf{B}_{n-1}$ é um bloco de $\mathbf{Is}$ mas cifrado anteriormente, e com o qual também se insere difusão ao esquema.

O bloco $\mathbf{B}_0$ é construído com todos os elementos da chave $\mathbf{K}$. Em sua construção, todos os *bits* de $\mathbf{K}$ são agrupados em *bytes*, e cada *byte* representa um *pixel* de $\mathbf{B}_0$. $\mathbf{K}$ é deslocada ciclicamente à direita em um *bit* e novamente os *bits* são agrupados em *bytes*, até se obter os 64 *pixels* de $\mathbf{B}_0$.

Na Equação (7), novamente é selecionado o bloco $\mathbf{B}_{n-1}$ e são usados os blocos $\mathbf{Bk}'_n$ e $\mathbf{Bq}'_n$ para formar $\mathbf{Bq}_n$. Observe que a adição é módulo 256 para que os *pixels* continuem a ser codificados a 8 *bpp*.

3) Estágio (III): A chave secreta $\mathbf{K}$ tem comprimento 256 *bits*. A partir desta são construídos os blocos $\mathbf{Bk}_n$ e $\mathbf{Bk}'_n$ a serem usados no estágio (IV), e formado um inteiro a_n a ser usado no estágio (V).

No estágio (IV), são selecionados os primeiros 120 *bits* de $\mathbf{K}$ para formar $\mathbf{Bk}_n$. Em seguida, a chave é deslocada ciclicamente à direita em um *bit* e são selecionados os primeiros 120 *bits* para formar $\mathbf{Bk}'_n$.

No estágio (V), são selecionados os primeiros 6 *bits* de $\mathbf{K}$ para formar o parâmetro a usado na construção de $\mathbf{F}^a$. Em seguida, a chave é deslocada ciclicamente à direita em três *bits*. Os deslocamentos nestes estágios são independentes.

4) Estágio (IV): A Figura 4 apresenta um diagrama em blocos do processo de expansão da chave, no qual se constrói $\mathbf{Bk}$. A cada bloco $\mathbf{Bk}$, com os primeiros 120 *bits* da chave são formados 15 *bytes*: $k1, k2, \ldots, k15$.

Os oito primeiros *bytes*, $k1$ a $k8$, correspondem aos oito primeiros *pixels* da primeira coluna, $c1$, de $\mathbf{Bk}$. As colunas seguintes são obtidas por um XOR entre os *bits* da coluna anterior e o próximo *byte* construído. Nas colunas $c4$ e $c8$ é feita uma multiplicação módulo 256 com contador de blocos, n, para que não haja repetições dos valores de $\mathbf{Bk}$, independentemente do comprimento da chave e do tamanho da imagem. A Figura 5 ilustra a composição dos elementos de $\mathbf{Bk}$ em relação aos *bytes* $k1, k2, \ldots, k15$.

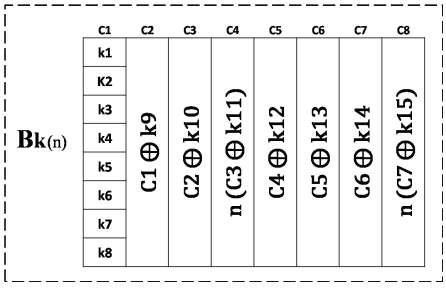

Fig. 5. Composição dos elementos do n-ésimo bloco $\mathbf{Bk}$.

5) Estágio (V): A matriz de transformação a ser aplicada a $\mathbf{Bq}_n$ tem parâmetro fracional dado por $a_n = \left(\frac{a_{1,n}}{a_2}\right)$. O termo a_2 é constante e especifica o número de *bits* de a_n, que, neste caso, é igual 6. O valor máximo de a_2 é dado pela ordem do elemento ζ com o qual se constrói a matriz $\mathbf{F}$. O termo $a_{1,n}$ é um número inteiro formado pelos primeiros 6 *bits* da chave, e deve estar no intervalo $1 \leq a_1 \leq a_2 - 1$. O bloco $\mathbf{B}_n^{a_n}$ representa o espectro fracional do bloco $\mathbf{Bq}_n$ e é dado por

$$\mathbf{B}_n^{\alpha_n} = \mathbf{F}^{a_{1,n}}\, \mathbf{Bq}_n\, \left(\mathbf{F}^{a_{1,n}}\right)^t. \qquad (8)$$

A Equação (8) é aplicada recursivamente até que os elementos de $\mathbf{B}_n^{a_n}$ estejam no intervalo de 0 a 255. Isso ocorre porque a transformada é definida em $\mathrm{GF}(257)$, de modo que os *pixels* dos blocos podem assumir valores entre 0 e 255. Em seguida, o bloco $\mathbf{B}_n^{a_n}$ substitui o bloco $\mathbf{B}_n$ em $\mathbf{Is}$.

O processo de decifragem é exatamente o inverso do processo de cifragem. O último bloco da imagem na cifragem deve ser o primeiro bloco a ser decifrado, e os deslocamentos da chave devem ser realizados de maneira coerente.

IV. Experimentos e análise de segurança

Com o próposito de avaliar a resistência do esquema de cifragem à criptoanálise, foram realizados diversos testes em imagens, com dimensões 512×512 *pixels*, em escala de cinza obtidas em [16]. Foram realizados testes nas mesmas condições com o algoritmo AES (*Advanced Encryption Standard*) modo CBC (*Cipher Block Chaining*). No AES, a imagem foi convertida num vetor de comprimento 512^2, para então ser cifrada. Em ambos os casos, é usada uma chave de 256 *bits*, $\mathbf{K} = (129, 130, 63, 224, 12, 30, 73, 48, 29, 32, 163, 24, 112, 103, 173, 148, 5, 3, 4, 233, 8, 35, 67, 28, 1, 2, 44, 64, 28, 11, 27, 44)$, a qual foi gerada aleatoriamente.

Os algoritmos foram implementados e os testes realizados em ambiente *Matlab*®. Em virtude do espaço limitado para redação do artigo são apresentados e discutidos os resultados para apenas uma imagem.

No esquema proposto, para construir as matrizes de dimensão 8×8 da GFrFT, $\mathbf{F}^{a_1/64}$, utilizou-se a matriz da FFFT,

$[F]_{k,i} = \sqrt{8^{-1}}4^{ki}$, com $\zeta = 4$. Neste caso, $a_2 = 64 = 2^6$, de forma que o parâmetro a_1 tem 6 *bits*, isto é, o intervalo de valores de $a_{1,n}$ é 1 a 63.

A. Análise estatística

A imagem original é mostrada na Figura 6 e seu histograma na Figura 8. A imagem cifrada tem um aspecto ruidoso como se observa na Figura 7. Observe que a aplicação da GFrFT leva a uma uniformização do histograma da imagem cifrada (Figura 9), sugerindo que ataques estatísticos não são viáveis.

Fig. 6. Imagem original de dimensão 512×512, 8 *bpp*.

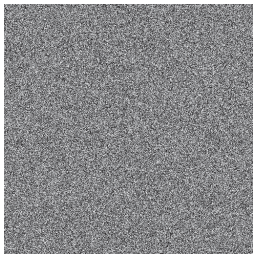

Fig. 7. Imagem cifrada.

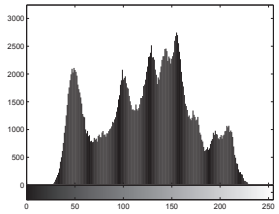

Fig. 8. Histograma da imagem original.

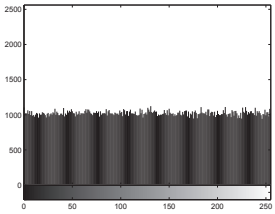

Fig. 9. Historgrama da imagem cifrada.

A alta correlação entre *pixels* adjacentes permite uma análise estatística da imagem, com a qual é possível promover um ataque. O esquema de cifragem deve reduzir a correlação entre *pixels* adjacentes. Nos testes, foram selecionados aleatoriamente 2^{15} *pixels* e calculados seus coeficientes de correlação horizontal, r_h, vertical, r_v, e diagonal, r_d [17].

Para a imagem original da Figura 6, os coeficientes de correlação calculados ficaram próximos a 1: $r_h = 0,9844$, $r_v = 0,9692$ e $r_d = 0,9567$. Na imagem cifrada com o esquema proposto, os coeficientes de correlação calculados ficaram próximos a 0: $r_h = -0,0038$, $r_v = 0,0016$ e $r_d = -0,0058$. De forma similar, na imagem cifrada com o AES, os coeficientes de correlação calculados ficaram próximos a 0: $r_h = 0,0078$, $r_v = -0,0039$ e $r_d = -0,0047$.

Pode-se também promover uma análise estatística com informações de entropia da imagem. Neste caso, deseja-se que os valores de entropia da imagem cifrada estejam próximos a 8 *bits* (máximo teórico), que representa uma fonte com emissão equiprovável de 256 símbolos. O valor da entropia para a imagem original é de $7,4473$ *bits*, para a imagem cifrada com o AES é de $7,9994$ *bits*, e de $7,9993$ *bits* para a imagem cifrada com o esquema proposto. Com esse valor, verifica-se que o esquema proposto é seguro contra ataques de entropia [18].

B. Espaço de chaves

Num esquema de cifragem de bloco, deve-se analisar o número de possibilidades para se decifrar cada bloco. Analisando a Equação (8), obtem-se o n-ésimo bloco $\mathbf{Bq}$ com

$$\mathbf{Bq}_n = \mathbf{F}^{a'_n}\, \mathbf{B}_n^{a_{1,n}}\, \left(\mathbf{F}^{a'_n}\right)^t$$

em que $a'(n) = 4 - a(n)$, e $a'(n) = \left(\frac{a'_1(n)}{a_2}\right)$. Como $a'_1(n)$ também tem 6 *bits*, há 2^6 combinações possíveis. No estágio (II), a partir da Equações (6) e (7) tem-se que

$$\mathbf{Bq}_n = [((\mathbf{B}_n \oplus \mathbf{B}_{n-1}) + \mathbf{Bk}_n) \oplus \mathbf{B}_{n-1}] + \mathbf{Bk}'_n, \quad (9)$$

$$\mathbf{B}_n = \left[(\mathbf{Bq}_n - \mathbf{Bk}'_n) \oplus \mathbf{B}_{n-1} - \mathbf{Bk}_n\right] \oplus \mathbf{B}_{n-1}, \quad (10)$$

em que a soma é módulo 256.

Dessa maneira, é necessário descobrir os blocos $\mathbf{Bk}'_n$ e $\mathbf{Bk}_n$ para obter a igualdade. Como cada um desses blocos é formado por 120 *bits* da chave, tem-se 2^{120} possibilidades. Então, o espaço de chaves tem cardinalidade $2^{246}\,(2^6 \times 2^{120} \times 2^{120})$.

Embora não se garanta a impossibilidade de um ataque por força bruta, pelos padrões atuais de segurança, o presente esquema é resistente a este tipo de ataque, uma vez que seu espaço de chaves é maior que 2^{100} [18]. O esquema apresenta também resistência ao ataque por texto claro escolhido [13, pp. 36]. Analisando a Equação (10), mesmo conhecendo $\mathbf{B}_n$ e $\mathbf{B}_{n-1}$, é necessário descobrir $\mathbf{Bk}_n$ e $\mathbf{Bk}'_n$, havendo 2^{240} possibilidades para isso.

C. Ataques diferenciais

Uma maneira de avaliar o "nível de difusão" do esquema é através do ataque diferencial. A imagem original, $\mathbf{I}_1$, e uma imagem modificada, $\mathbf{I}_2$, são cifradas usando a mesma chave secreta. A imagem $\mathbf{I}_2$ é obtida invertendo-se o *bit* menos significativo de um único *pixel* de $\mathbf{I}_1$ escolhido aleatoriamente. É desejável que as imagens obtidas pelas cifragens sejam *consideravelmente* diferentes.

A diferença entre essas imagens pode ser mensurada através da taxa do número de *pixels* modificados (NPCR, *number of pixels change rate*) e da média unificada da intensidade de modificação (UACI, *unified average changing intensity*) [17]. Um valor de NPCR próximo a 100% indica uma grande quantidade de *pixels* modificados, ou seja, indica uma grande diferença entre as imagens C_1 e C_2; já o valor ideal para a UACI é próximo a $33,33\%$ [17].

Foram criadas 100 versões modificadas para a imagem original e computados os valores de NPCR e de UACI de cada imagem cifrada. A Tabela I apresenta os valores médio, máximo e mínimo para a imagem da Figura 6. Com os resultados, é possível constatar a resistência do esquema a um ataque diferencial.

Outra maneira de avaliar a difusão inserida pelo esquema é analisar o quanto uma pequena variação da chave influencia na imagem cifrada, ou seja, a sensibilidade da chave. Como os blocos $\mathbf{B}_0$ e $\mathbf{Bk}$ são formados por elementos da chave, uma mudança na chave provoca uma alteração da imagem cifrada logo no início da cifragem/decifragem.

Nos testes, as imagens são decifradas com uma chave $\hat{\mathbf{K}} = (129, 130, 63, 224, 12, 30, 73, 48, 29, 32, 163, 24, 112, 103, 173,$

TABELA I
VALORES MÉDIO, MÁXIMO E MÍNIMO DE NPCR E UACI OBTIDOS DE UM CONJUNTO DE 100 IMAGENS.

	Proposto		AES	
Métrica	NPCR	UACI	NPCR	UACI
Máximo (%)	99,64	33,61	99,07	16,63
Mínimo (%)	99,58	30,41	4,03	48,68
Médio (%)	99,61	33,50	0,67	8,16

$148, 5, 3, 4, 233, 8, 35, 67, 28, 1, 2, 44, 64, 28, 11, 27, \underline{43})$, que difere de $\mathbf{K}$ somente no *bit* menos significativo. Observe que o valor na posição destacada é 43, enquanto que, em $\mathbf{K}$ é 44.

Com a relação sinal-ruído de pico (PSNR - *Peak signal-to-noise ratio*) pode-se mensurar a diferença entre duas imagens. Quanto maior for a PSNR mais semelhantes são as imagens. O valor da PSNR obtido para a imagem da Figura 6 foi de $9,68dB$, e com o AES a PSNR foi de $9,27dB$. Para efeito de comparação, compactando essa imagem com o padrão JPG, a PSNR obtida é de $37,40dB$.

D. Complexidade computacional

A complexidade aritmética das transformadas representa a parte mais importante no custo computacional do esquema proposto. Para cada imagem dos testes são obtidos 4096 blocos. Como cada GFrFT é aplicada recursivamente, não há uma expressão analítica para se contabilizar a complexidade aritmética envolvida na cifragem de uma imagem arbitrária. Analisando a Equação (5), cada bloco requer 44 multiplicações e 48 adições para ser cifrado.

Foi implementado um esquema de cifragem com sobreposição de blocos similar ao porposto em [8], usando blocos 8×8, a GFrFT baseada em funções de matrizes e aritmética em $\mathrm{GF}(257)$. Para a imagem da Figura 6, o número de GFrFT no esquema proposto (sem sobreposição) foi de 5316, enquanto que no esquema com sobreposição foi de 13821.

Um aspecto importante no uso das transformadas fracionais é a existência de algoritmos rápidos e cálculos em aritmética inteira, que contribuem para a diminuição do custo computacional do esquema. É possível reduzir esta complexidade usando outras transformadas fracionais com a de Hartley, do cosseno e do seno sobre corpos finitos, visto que seus polinômios de interpolação têm menos constantes multiplicativas [7].

V. CONCLUSÕES

Neste artigo foi apresentado um novo esquema de cifragem de imagens digitais baseado na transformada fracional de Fourier sobre corpos finitos. Foram realizados experimentos e analisadas diversas métricas de segurança para avaliar o desempenho do esquema de cifragem. Observa-se que o esquema é resistente aos principais ataques estatísticos, e que seu espaço de chave atende aos requisitos necessários para inviabilizar ataques de força bruta, por texto escolhido e diferenciais. Outras métricas de segurança serão analisadas para investigar o desempenho do esquema de cifragem.

Um dos aspectos positivos do esquema é que sua complexidade aritmética é menor que do esquema similar proposto em [8]. Outro aspecto importante é a flexibilidade do esquema, uma vez que se pode aumentar o espaço de chave sem comprometer sua complexidade aritmética.

Pode-se também empregar outras transformadas fracionais sobre corpos finitos como a de Hartley, a do coseno e a do seno. Além da existência de algoritmos rápidos, a complexidade aritmética associada a essas transformadas pode ser menor devido a uma menor quantidade de termos no polinômio de interpolação que as define [7]. Essas transformadas e seus algoritmos rápidos serão implementados de forma a avaliar a complexidade aritmética do esquema de cifragem proposto.

AGRADECIMENTOS

O primeiro e o segundo autores agradecem o apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq).

REFERÊNCIAS

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

[2] B. Dickinson and K. Steiglitz, "Eigenvectors and functions of the discrete Fourier transform," *IEEE Transactions on Acoustics, Speech and Signal Processing*, vol. 30, no. 1, pp. 25–31, 1982.

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

[4] 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, 2012.

[5] S. Güdvangen, "Practical applications of number theoretic transforms," 2006. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.46.1921

[6] J. B. Lima, R. M. Campello de Souza, and P. H. E. S. Lima, "Fractional number-theoretic transform based on matrix functions," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, vol. 24, no. 7, Florence, Italy, 2014, pp. 587–597.

[7] P. H. E. S. Lima, J. B. Lima, and R. M. Campello de Souza, "Hartley, cosine and sine fractional transforms over finite fields," in *Proceedings of the International Telecommunications Symposium (ITS)*, São Paulo, Brazil, 2014, pp. 1–5.

[8] J. B. Lima and L. Novaes, "Image encryption based on the fractional Fourier transform over finite fields," *Signal Processing*, vol. 94, pp. 521–530, 2013.

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

[10] N. J. Higham, *Functions of Matrices: Theory and Computation*. Society for Industrial and Applied Mathematics, 2008.

[11] P. Lancaster and M. Tismenestsky, *The Theory of Matrices: With Applications*, 2nd ed. Academic Press, 1985.

[12] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[13] W. Stallings, *Cryptography and Network Security: Principles and Practice*. Prentice Hall, 2011.

[14] Q. Guo, Z. Liu, and S. Liu, "Color image encryption by using Arnold and discrete fractional random transforms in IHS space," *Optics and Lasers in Engineering*, vol. 48, no. 12, pp. 1174 – 1181, 2010.

[15] J. B. Lima, E. Lima, and F. Madeiro, "Image encryption based on the finite field cosine transform," *Signal Processing: Image Communication*, vol. 28, pp. 1537–1547, 2013.

[16] S. I. P. I. University of Southern California, "The USC-SIPI image database," 2015. [Online]. Available: http://www.sipi.usc.edu

[17] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Applied Soft Computing*, vol. 11, pp. 514–522, 2011.

[18] A. Akhshani, S. Behnia, A. Akhavan, H. A. Hassan, and Z. Hassan, "A novel scheme for image encryption based on 2D piecewise chaotic maps," *Optics Communications*, vol. 283, no. 17, pp. 3259–3266, 2010.