Formatação de Distribuições de Probabilidade sobre os Inteiros

J. B. Lima, H. M. de Oliveira e R. M. Campello de Souza

***Resumo*— Este trabalho investiga a propriedade das transformadas definidas sobre corpos finitos de formatar a distribuição de probabilidade de uma fonte de informação, convertendo-a numa distribuição uniforme. São discutidos alguns aspectos teóricos dessa ferramenta e apresentadas simulações no contexto mencionado. Alguns cenários de aplicação desse método são sugeridos.**

***Palavras-Chave*— Transformadas de corpo finito, distribuição de probabilidade.**

***Abstract*— This work investigates the ability of finite field transforms in formatting the probability distribution of an information source, by converting it into uniform distribution. Theoretical aspects of this tool are discussed and simulation presented. Some application scenarios of that property are suggested.**

***Keywords*— Finite field transforms, probability distribution.**

I. INTRODUÇÃO

Em Engenharia, as transformadas definidas sobre corpos finitos (chamadas transformadas digitais) têm sido empregadas em diversas aplicações, proporcionando vantagens relacionadas à precisão e à complexidade computacional. Esses aspectos englobam fatores como a existência de transformadas sem multiplicação, o uso da aritmética de ponto-fixo para a realização de cálculos e a conseqüente precisão infinita com que os mesmos são efetuados, uma vez que arredondamentos não são necessários [7].

A transformada digital mais conhecida é a de Fourier. Em sua versão numérica (NTT, *number theoretic transform*), essa transformada relaciona vetores com componentes em GF(p), o campo de Galois de ordem p. Entre as propriedades das NTTs, destaca-se a convolução cíclica, útil para calcular a convolução linear entre uma determinada informação em tempo discreto e um filtro FIR [1].

No contexto de Códigos Corretores de Erros, a transformada de Fourier de corpo finito pode ser utilizada para descrever códigos de bloco. Neste caso, a ferramenta recebe o nome de transformada de campo de Galois (GFT, *Galois field transform*), que é análoga à de Fourier, mas relaciona vetores com componentes em corpos finitos GF(p^m) [2].

Além da NTT / GFT, outras transformadas digitais têm sido propostas. Um exemplo é a transformada de Hartley de corpo finito, para a qual se propôs aplicações no projeto de sistemas de multiplexação digital, em sistemas de múltiplo acesso e no espalhamento espectral multinível de seqüências [3]. Outro exemplo é a transformada *wavelet* digital, que propicia a expansão da aplicação das *wavelets* ao campo dos Códigos Corretores de Erro e da Criptografia [4]. Mais recentemente, foram introduzidas as transformadas digitais do cosseno (FFCTs, *finite field cosine transforms*) e do seno (FFSTs, *finite field sine transforms*), cujas aplicações estão sendo investigadas [5].

Uma outra transformada definida sobre corpos finitos é a I_2I-KLT (*integer to integer Karhunen-Loève transform*), apresentada como uma ferramenta capaz de converter a distribuição de probabilidade de determinada fonte de informação numa distribuição uniforme [6]. Isso permitiria introduzir, em um sistema de comunicação digital, um bloco de interface entre o receptor, projetado segundo uma distribuição uniforme, e a informação que, muitas vezes, comporta-se segundo uma curva normal.

Assim como a KLT sobre os reais, a I_2I-KLT não é prática, pois sua matriz de transformação depende dos dados que se deseja processar. Sendo a única transformada digital a apresentar essa dificuldade, esse fato motivou o estudo da propriedade de formatação de distribuições de probabilidade que outras transformadas sobre corpos finitos teriam, particularmente, as NTTs e as FFCTs. As definições dessas transformadas são revisadas na seção a seguir.

Na seção III, a formatação de distribuições de probabilidade proporcionada pelas transformadas de corpo finito é discutida. Descreve-se alguns aspectos teóricos que ilustram o funcionamento da propriedade e fundamentam a sua utilização. Resultados das simulações realizadas são apresentados. A obtenção de uma distribuição uniforme a partir de uma distribuição qualquer significa esconder o comportamento estatístico de uma fonte de informação, o que é desejável em muitas situações no contexto de Criptografia. Com base nisso, algumas sugestões de aplicações da propriedade são apresentadas na seção IV. Por fim, são mencionadas conclusões e perspectivas para trabalhos futuros.

II. TRANSFORMADAS DIGITAIS

Nesta seção, são apresentadas as transformadas cuja propriedade de formatação de distribuições de probabilidade é investigada. Naturalmente, para que tais transformadas sejam aplicadas, são consideradas fontes discretas, onde cada símbolo pode ser associado a um número inteiro cuja freqüência de ocorrência possa ser observada. Assim, são consideradas apenas transformadas numéricas, uma vez que, em corpos finitos GF(p^m), os elementos são polinômios.

Juliano Bandeira Lima, Hélio Magalhães de Oliveira e Ricardo M. Campello de Souza, Grupo de Processamento de Sinais, Departamento de Eletrônica e Sistemas, Universidade Federal de Pernambuco, Recife, Brasil, E-mails: juliano_bandeira@ieee.org, hmo@ufpe.br, ricardo@ufpe.br.

A. Transformada Numérica de Fourier.

A transformada numérica de Fourier da seqüência $f = (f_i),\ i = 0, 1, \ldots, N-1,\ f_i \in GF(p)$, é a seqüência $F = (F_k),\ k = 0, 1, \ldots, N-1,\ F_k \in GF(p)$, de elementos

$$F_k \triangleq \sqrt{\frac{1}{N \pmod p}} \sum_{i=0}^{N-1} f_i\, \alpha^{i\,k}. \tag{1}$$

Sua transformada inversa é dada por

$$f_k = \sqrt{\frac{1}{N \pmod p}} \sum_{i=0}^{N-1} f_i\, \alpha^{-i\,k}. \tag{2}$$

Nas Equações (1) e (2), $\alpha \in GF(p)$ tem ordem multiplicativa N e todos os cálculos são efetuados módulo p; o fator de escalonamento $\sqrt{1/N \pmod p}$, cuja condição de existência é que N seja um resíduo quadrático sobre GF(p), tem a função de tornar a transformada unitária, o que simplifica o seu emprego em muitas abordagens [9]. Se p for um primo de Mersenne ou de Fermat, é possível reduzir significativamente a complexidade computacional associada às NTTs, recorrendo a algoritmos rápidos e realizando multiplicações através de deslocamentos [7].

B. Transformadas do Cosseno.

Em [5], foi introduzida a família completa de transformadas trigonométricas sobre corpos finitos (FFTTs, *finite field trigonometric transforms*), a qual é constituída de oito transformadas do cosseno e oito do seno. Um vez que as propriedades dessas transformadas são semelhantes, neste artigo, são consideradas apenas duas delas, cujas definições são apresentadas a seguir.

Definição 1: O conjunto de inteiros gaussianos sobre GF(p) é o conjunto GI(p) $= \{a + jb, a, b \in GF(p)\}$, onde p é um primo tal que $j^2 = -1$ é um resíduo não-quadrático sobre GF(p). Só um primo $p \equiv 3(mod\,4)$ atende a este requisito [8].

O corpo de extensão GF(p^2) é isomórfico à estrutura "complexa" GI(p). A partir da definição acima, os elementos de GI(p) podem ser representados na forma $a+jb$ e denominados números complexos sobre corpos finitos.

Definição 2: Os elementos $\zeta = (a + jb) \in GI(p)$, tais que $a^2+b^2 \equiv 1(mod p)$ são chamados de elementos unimodulares.

Definição 3: Seja ζ um elemento não-nulo de GI(p), onde $p \equiv 3(mod\ 4)$. A função k-trigonométrica cosseno de $\angle(\zeta^i)$ (arco do elemento ζ^i) sobre GI(p) é

$$\cos_k(\angle\zeta^i) \triangleq (2^{-1} \text{mod } p)(\zeta^{ki} + \zeta^{-ki}), \tag{3}$$

$i, k = 0, 1, \ldots, N-1$, onde ζ tem ordem N. Para simplificar, tal função é denotada por $\cos_k(i)$.

Para definir as transformadas do cosseno de corpo finito unitárias, é necessário introduzir a função peso

$$\beta_r = \begin{cases} \sqrt{2^{-1}} \pmod p, & r = 0 \text{ or } N, \\ 1, & r = 1, 2, \ldots, N-1. \end{cases} \tag{4}$$

Definição 4 (FFCT-2): Se $\zeta \in GI(p)$ tem ordem multiplicativa $4N$, então a transformada do cosseno de corpo finito do tipo 2 da seqüência $c = (c_i),\ i = 0, 1, \ldots, N-1,\ c_i \in GF(p)$, é a seqüência $C = (C_k),\ k = 0, 1, \ldots, N-1,\ C_k \in GF(p)$, de elementos

$$C_k \triangleq \sqrt{\frac{2}{N \pmod p}} \sum_{i=0}^{N-1} \tilde{\beta}_k c_i \cos_k(i + 1/2). \tag{5}$$

Teorema 1 (FFCT-2^{-1}): A transformada do cosseno de corpo finito do tipo 2 inversa da seqüência $C = (C_k),\ k = 0, 1, \ldots, N-1,\ C_k \in GF(p)$, é a seqüência $c = (c_i),\ i = 0, 1, \ldots, N-1,\ c_i \in GF(p)$, de elementos

$$c_i = \sqrt{\frac{2}{N \pmod p}} \sum_{k=0}^{N-1} \tilde{\beta}_k C_k \cos_k(i + 1/2). \tag{6}$$

Demonstração: Vide [5]. ■

Definição 5 (FFCT-4): Se $\zeta \in GI(p)$ tem ordem multiplicativa $8N$, então a transformada do cosseno de corpo finito do tipo 4 da seqüência $c = (c_i),\ i = 0, 1, \ldots, N-1,\ c_i \in GF(p)$, é a seqüência $C = (C_k),\ k = 0, 1, \ldots, N-1,\ C_k \in GF(p)$, de elementos

$$C_k \triangleq \sqrt{\frac{2}{N \pmod p}} \sum_{i=0}^{N-1} c_i \cos_{k+1/2}(i + 1/2). \tag{7}$$

Teorema 2 (FFCT-4^{-1}): A transformada do cosseno de corpo finito do tipo 4 inversa da seqüência $C = (C_k),\ k = 0, 1, \ldots, N-1,\ C_k \in GF(p)$, é a seqüência $c = (c_i),\ i = 0, 1, \ldots, N-1,\ c_i \in GF(p)$, de elementos

$$c_i = \sqrt{\frac{2}{N \pmod p}} \sum_{k=0}^{N-1} C_k \cos_{k+1/2}(i + 1/2). \tag{8}$$

Demonstração: Vide [5]. ■

É relevante mencionar que, para definir transformadas do cosseno sobre corpos finitos, considerar elementos ζ com ordem multiplicativa $2N$ seria suficiente. No entanto, para garantir que as transformadas sejam numéricas, nas definições 4 e 5, respectivamente, é necessário que $\zeta^{\frac{1}{2}}$ e $\zeta^{\frac{1}{4}}$ sejam unimodulares. Por isso, a necessidade de selecionar elementos ζ com ordens multiplicativas mais elevadas [5]. Além disso, 2 e N devem ser resíduos quadráticos sobre GF(p).

III. Formatação de Distribuições de Probabilidade

A descrição dos efeitos que uma transformada digital tem sobre uma distribuição de probabilidade pode ser feita considerando alguns aspectos da aritmética modular. Uma ilustração simples disso consiste em associar cada símbolo de uma fonte a um número inteiro de 0 a $q-1$, $q \leq p$, e multiplicá-lo, módulo p, por uma constante K. O produto modular desloca as freqüências de ocorrência dos símbolos.

Considere, por exemplo, um mapeamento em que $p = q = 13$ e $K = 5$. Imaginando que a fonte possua uma distribuição similar à normal, os números 6 e 7 devem possuir altas probabilidades de ocorrência em relação aos demais. Multiplicando

6 e 7 por 5 (módulo 13), obtém-se, respectivamente, 4 e 9. As freqüências de ocorrência permanecem as mesmas, mas, agora, estão associadas a outros símbolos, de maneira que o formato da distribuição original foi descaracterizado.

Quando o produto modular direto entre cada símbolo e uma constante é substituído por uma combinação linear que envolve um bloco de símbolos, o processo torna-se mais complexo. No entanto, o aspecto observado na situação apresentada como exemplo persiste. Ainda que seja considerável a diferença entre as freqüências de emissão dos símbolos de uma fonte (distribuição não-uniforme), a tendência é que a aplicação de uma transformada de corpo finito produza blocos transformados compostos por símbolos uniformemente distribuídos.

Para avaliar o efeito de uma transformada em GF(p) sobre o comportamento estatístico de uma fonte, gera-se amostras de números inteiros, com valores de 0 a $p-1$, com distribuições de probabilidade conhecidas. Neste trabalho, são apresentados os resultados da aplicação das transformadas a fontes que, originalmente, atendem a uma distribuição aproximadamente normal e a uma distribuição binomial. No caso da normal, que é uma função inerentemente contínua, realiza-se procedimentos de escalonamento e aproximação, para que se tenha uma amostra com as características mencionadas. A distribuição binomial, sendo discreta, não requer tal manipulação.

A fim de ser processada, a amostra é segmentada em blocos de tamanhos iguais ao da transformada que se vai aplicar. Os resultados desse procedimento são ilustrados através de histogramas da amostra antes e após a transformação. Um teste de aderência é realizado, com o objetivo de quantificar a proximidade entre a distribuição obtida e a uniforme.

A. Formatação Via FFCTs.

No contexto dos números reais, em termos de compactação de energia, a transformada de Karhunen-Loève (KLT) é a que apresenta melhores resultados, produzindo vetores transformados cujas componentes são descorrelacionadas. No entanto, na prática, seu uso é restrito, uma vez que é preciso calcular a matriz de covariância do bloco que se deseja transformar. Diante dessa limitação, em aplicações como codificação de imagem e vídeo digitais, emprega-se a transformada discreta do cosseno (DCT), a qual apresenta um desempenho próximo à KLT e pode ser calculada por algoritmos rápidos com complexidade $O(N \log N)$ multiplicações reais [10].

Nesse sentido, o conhecimento da existência da KLT de corpo finito sugere a reapresentação da implementável transformada do cosseno de corpo finito como uma versão subótima da primeira. Esse aspecto é analisado sob o ponto de vista da capacidade da FFCT de formatar distribuições de probabilidade, ilustrada através dos exemplos que seguem. Para simplificar a FFCT-2 e a FFCT-4 são denotadas, respectivamente, por $\mathcal{FC}_2$ e $\mathcal{FC}_4$.

Exemplo 1: Na primeira situação considerada, gerou-se uma amostra com 2^{14} números de 0 a 126 distríbuidos de modo aproximadamente normal. Utilizou-se a transformada $\mathcal{FC}_2$ de comprimento $N = 8$ sobre GF(127). Os histogramas da amostra antes e após a transformação são apresentados na Figura 1. Usando o teste chi-quadrado de Pearson, que permite verificar a aderência de dados a uma distribuição teórica, assumiu-se um valor de probabilidade $P \leq 0,05$ como justificativa para rejeitar a hipótese nula de que os dados não aderem à distribuição proposta [11]. Verificou-se que a amostra resultante adere a uma distribuição uniforme (vide Tabela I).

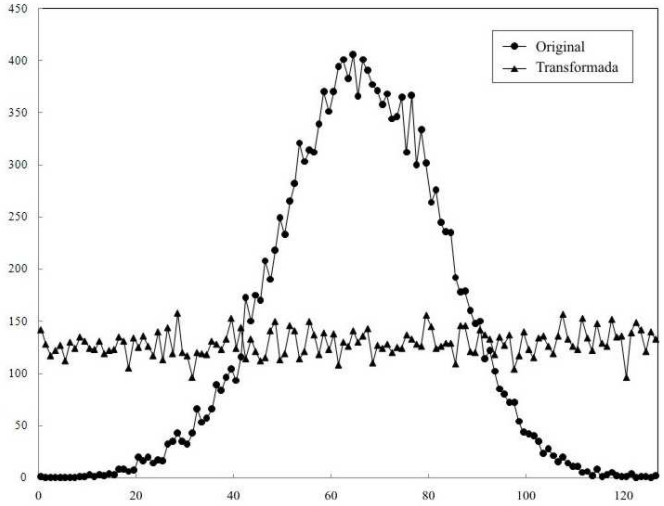

Fig. 1. Histogramas de uma amostra com 2^{14} números antes e após a aplicação da transformada $\mathcal{FC}_2$ de comprimento $N = 8$ sobre GF(127).

Exemplo 2: Numa segunda simulação, também foi gerada uma amostra com 2^{14} números de 0 a 126, no entanto, de acordo com uma distribuição binomial. Novamente, utilizou-se a transformada $\mathcal{FC}_2$ de comprimento $N = 8$ sobre GF(127). Os histogramas da amostra antes e depois de duas transformações iterativas são apresentados na Figura 2. O cálculo repetido da transformada foi necessário, pois o fato da distribuição binomial ser mais esparsa que a considerada no exemplo anterior não favoreceu a produção de uma distribuição uniforme na primeira iteração. Após este procedimento, a amostra obtida foi testada, tendo sido comprovada a sua aderência à distribuição uniforme (vide Tabela I).

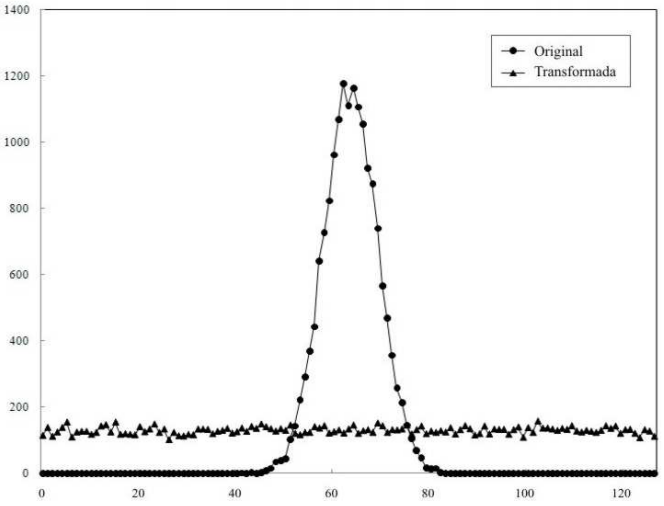

Fig. 2. Histogramas de uma amostra com 2^{14} números antes e após a aplicação da transformada $\mathcal{FC}_2$ de comprimento $N = 8$ sobre GF(127). Neste caso, a transformada foi aplicada duas vezes.

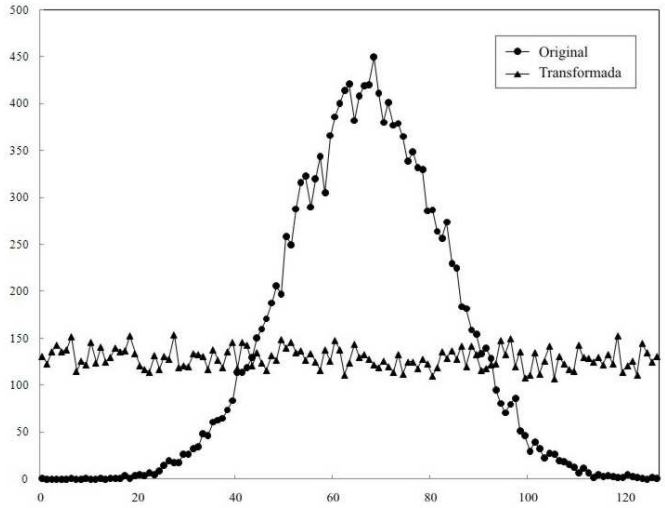

Fig. 3. Histogramas de uma amostra com 2^{14} números antes e após a aplicação da transformada $\mathcal{FC}_4$ de comprimento $N = 8$ sobre GF(127).

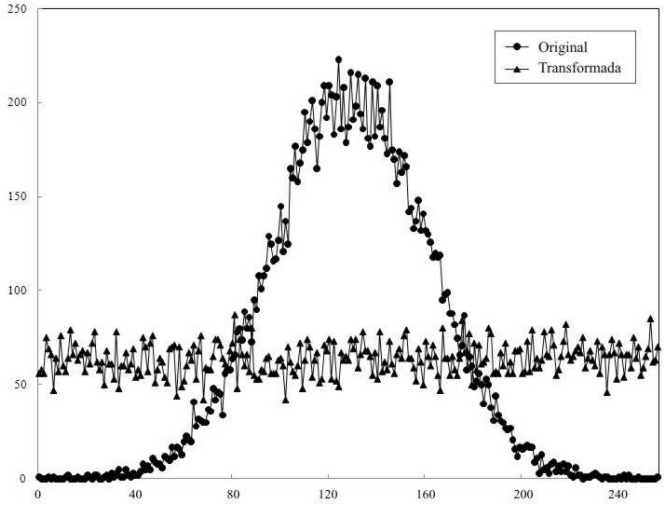

Fig. 4. Histogramas de uma amostra com 2^{14} números antes e após a aplicação da transformada NTT de comprimento $N = 8$ sobre GF(257).

Exemplo 3: Nesta situação, realizou-se um procedimento análogo ao descrito nos exemplos anteriores. No entanto, foi utilizada a transformada $\mathcal{FC}_4$. Os resultados obtidos são apresentados na Figura 3. Após a transformação, a amostra foi testada, fornecendo forte aderência à distribuição uniforme (vide Tabela I).

Nos Exemplos 1, 2 e 3, um aspecto interessante é que as transformadas utilizadas possuem um ciclo finito. Isso significa que, se um vetor for transformado iterativamente, em algum momento, o resultado produzido será igual ao vetor original. No caso da transformada $\mathcal{FC}_4$, que é involucionária (o ciclo é igual a 2), se uma amostra for processada duas vezes, obter-se-á como resultado a própria amostra. Assim, essa transformada não pode ser usada para processar distribuições que requeiram mais de uma iteração para alcançar o formato uniforme. Para a transformada $\mathcal{FC}_2$, é possível verificar que a mesma possui ciclos maiores que 2. Dessa forma, é necessário um número maior de iterações para que se retorne à amostra original.

B. Formatação Via NTTs.

O fato de se ter verificado a propriedade da formatação de distribuições de probabilidade para as FFCTs motivou a investigação de outras transformadas sob esse aspecto. No exemplo que segue, utiliza-se uma transformada numérica de Fourier para implementar o procedimento anteriormente descrito.

Exemplo 4: Aplicando a NTT de comprimento 8 em GF(257) a blocos da amostra original, obtém-se os resultados apresentados na Figura 4. Testou-se a amostra obtida e verificou-se que a mesma também adere a uma distribuição uniforme (vide Tabela I).

Utilizando a propriedade da dualidade, observa-se que o ciclo da transformada de Fourier é igual a 4 [9]. Assim, após quatro processamentos iterativos da amostra original pela NTT, retorna-se à distribuição original.

TABELA I

RESULTADOS DO TESTE CHI-QUADRADO DE PEARSON PARA VERIFICAR A ADERÊNCIA DE UMA AMOSTRA À DISTRIBUIÇÃO UNIFORME (APÓS A APLICAÇÃO DA TRANSFORMADA DIGITAL INDICADA).

Transformada	Distribuição original	P ($\leq 0,05$, rejeição da aderência)
FFCT-2	Normal	$0,4482$
	Binomial	$0,4577$
FFCT-4	Normal	$0,7792$
NTT	Normal	$0,4643$

IV. APLICAÇÕES EM CRIPTOSSISTEMAS

Conforme discutido ao longo deste trabalho, o uso de uma transformada de corpo finito conduz à uniformização de uma distribuição de probabilidade. No campo da Criptografia, essa propriedade possui potencial aplicação, uma vez que um conhecimento prévio do comportamento estatístico de uma informação facilita a criptoanálise de textos cifrados a partir da mesma.

Existem algumas ferramentas que objetivam modificar as probabilidades de ocorrência dos símbolos de uma fonte. Um exemplo é a substituição homofônica [12], que tem sido parte integrante de criptossistemas em que a modificação mencionada é empregada. Essa técnica visa reduzir a redundância da mensagem cifrada, aumentando, portanto, a distância de unicidade da cifra [12]. Assim, uma seqüência de símbolos da fonte com uma distribuição de freqüência arbitrária é transformada em uma seqüência unicamente decodificável de símbolos, tendo, todos, a mesma freqüência.

Especificamente, a substituição homofônica associa a cada símbolo s da fonte, $s \in A$, um conjunto H_s de novos símbolos, denominados homófonos, pertencentes a um alfabeto maior que A, dentre os quais se escolhe um substituto para s. A cardinalidade de H_s é proporcional à freqüência relativa de s no alfabeto original A e um homófono é escolhido aleatoriamente de modo a gerar uma "nova" fonte uniformemente distribuída,

cujos símbolos são então cifrados [12].

A técnica de formatação de distribuições introduzida nesse trabalho vem sendo investigada como uma ferramenta alternativa para a substituição clássica descrita acima. Assim, por exemplo, ao se transformar, nos moldes dos exemplos descritos na seção III, blocos de símbolos de uma fonte binária com probabilidades p_1 e p_2, produz-se uma fonte com distribuição uniforme ($p_1 = p_2 = 1/2$). Para se obter o efeito de uma substituição homofônica, é necessário não apenas uniformizar a distribuição da fonte, mas também estabelecer uma independência estatística entre os símbolos da mensagem e os produzidos pela substituição. Isso requer a expansão do alfabeto da mensagem e a introdução de um mecanismos aleatório, que não se encontra presente em transformações lineares como as consideradas aqui. Dois procedimentos atualmente sendo analisados para atender essa exigência são:

i) Usar diferentes versões de transformadas para processar diferentes blocos de mensagem. A seqüência das transformadas a ser usada seria aleatória e funcionaria como uma chave secreta. A mesma poderia ser obtida não só dos diversos tipos possíveis de FFCTs, por exemplo, mas também pelo uso de diferentes elementos unimodulares empregados na definição da transformada. Além disso, ao se usar $p > q$, a expansão do alfabeto original é obtida.

ii) Acrescentar a cada bloco de mensagem um bloco aleatório de comprimento fixo, o que significa uma expansão do texto claro. A transformação é então aplicada ao bloco expandido. Na decodificação, após a transformação inversa, o bloco aleatório, cuja posição é previamente conhecida, é simplesmente desconsiderado. Como anteriormente, a expansão do alfabeto original é obtida ao se usar $p > q$. Uma combinação dos dois procedimentos também é possível.

Um outro cenário de aplicação, ainda no campo da Criptografia, é o de mecanismos para promover difusão [13] em criptossistemas de chave secreta. O objetivo é fazer com que pequenas mudanças no texto claro ou na chave se propaguem rapidamente para o texto cifrado. Isso torna o criptossistema mais resistente a ataques, permitindo que um menor número de iterações seja usado para atingir um dado nível de segurança. Classicamente, a difusão é obtida pelo uso de permutações no algoritmo de cifragem [14]. Em 1993, um novo procedimento foi proposto, baseado no uso de transformadas lineares. Especificamente, três camadas da pseudo-transformada de Hadamard (PHT) foram usadas para promover difusão no criptossistema SAFER [15].

As transformadas digitais são escolhas naturais para se obter difusão por meio de transformações lineares. Propõe-se aqui o uso das transformadas trigonométricas digitais como uma alternativa a transformadas como a PHT. As propriedades de difusão da FFCT precisam ser investigadas. Em função das características de formatação de distribuições que foram discutidas nesse trabalho, espera-se que a FFCT proporcione, com um número menor de camadas, a difusão necessária.

V. Conclusões

Nesse artigo, discutiu-se a formatação da distribuição de probabilidade de uma fonte pelas transformadas de corpo finito. Nesse sentido, foram observados aspectos teóricos e práticos do uso das transformadas numéricas de Fourier e do cosseno e realizadas simulações a fim de ilustrar a formatação mencionada. Através dos resultados obtidos, pôde-se avaliar a capacidade uniformizar uma distribuição, a partir do processamento de uma informação distribuída de uma maneira específica, por uma ferramenta baseada em aritmética modular.

Os números alcançados nos experimentos permitiram a sugestão de cenários de aplicação da propriedade. No campo da Criptografia, tem sido investigada a possibilidade de se introduzir a NTT e a FFCT em sistemas nos quais existe o interesse de modificar a estatística de um texto claro. No mesmo contexto, sugere-se a investigação das características de difusão dessas transformadas.

Agradecimentos

Os autores agradecem ao Prof. Dr. Valdemar Cardoso da Rocha Jr. pelas valiosas sugestões e a André Leite Wanderley pelo auxílio nas simulações.

Referências

[1] W. Li and M. Peterson, "FIR Filtering by the Modified Fermat Number Theoretic Transform", *IEEE Trans. on Acoustics, Speech and Signal Processing*, v. 38, p. 1641-1645, Setembro 1990.

[2] R. M. Campello de Souza, "Transformadas em Corpos Finitos para Codificação de Canal", *Revista da Sociedade Brasileira de Telecomunicações*, N. 1, vol. 5, p. 41-57, 1990.

[3] R. M. Campello de Souza and H. M. de Oliveira, "The Complex Hartley Transform Over a Finite Field", in *Coding, Communicaitons and Broadcasting* (P. G. Farnell, M. Darnell e B. Honary, eds.), p. 267-276, Hertfordshire: Research Studies Press, John Wiley, 1st ed., 2000.

[4] F. Fekri, S. W. McLaughlin, R. M. Mersereau and R. W. Schafer, "Block Error Correcting Codes Using Finite-Field Wavelet Transforms", *IEEE Trans. on Signal Processing*, v. 54, p. 991-1004, Março 2006.

[5] J. B. Lima and R. M. Campello de Souza, "New Trigonometric Transforms over Prime Finite Fields for Image Filtering", in *VI International Telecommunications Symposium (ITS'2006)*, Fortaleza, Brasil, 2006.

[6] G. Z. Karabulut, D. Panario and A. Yongaçoglu, "Integer to Integer Karhunen-Loève Transform over Finite Fields", in *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, v. 5, Quebec, Canada, p. 213-216, 2004.

[7] D. G. Myers, *Efficient Convolution and Fourier Transform Techniques*. Prentice Hall, 1990.

[8] D. M. Burton, *Elementary Number Theory*. Addison-Wesley Publishing Company, 1994.

[9] R. M. Campello de Souza and H. M. de Oliveira, "Eigensequences for Multiuser Communication over the Real Adder Channel", in *VI International Telecommunications Symposium (ITS'2006)*, Fortaleza, Brasil, 2006.

[10] N. Ahmed, T. R. Natarajan and K. R. Rao, "Discrete Cosine Transform", *IEEE Transactions on Computers*, IT-23, p. 90-93, Janeiro 1974.

[11] G. Casella and R. Berger, *Statistical Inference*. IE-Thomson, 2nd ed., 2002.

[12] H. N. Jendal, Y. J. B. Kuhn and J. L. Massey, "An Information-Theoretic Approach to Homophonic Substitution", *Advances in Cryptology-Eurocrypt'89* (Eds. J.-J. Quisquater and J. Vandewalle), LNCS N. 434. Springer, p. 382-394, 1990.

[13] C. E. Shannon, "Communication Theory of Secrecy Systems", *Bell Syst. Tech. J.*, v. 28, p. 656-715, Outubro 1949.

[14] "Data Encryption Standard", *FIPS PUB 46*, National Bureau of Standards, Washington, D.C., Janeiro 1977.

[15] J. L. Massey, "SAFER K-64: A Byte Oriented Block-Ciphering Algorithm", in *Proc. Cambridge Algorithms Workshop*, Cambridge, England, Dezembro 1993.